COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

ICT Policy Support Programme (ICT PSP)

ICT-PSP-2-Theme-3 - Consensus building, experience sharing
on internet evolution and security

ICT PSP call identifier:	ICT PSP 2nd call for proposals 2008
ICT PSP Theme/objective identifier:	3.2 Trusted information infrastructures and biometric technologies
Project acronym:	**BEST Network**
Project full title:	**Biometrics European Stakeholder Network**
Grant agreement no.:	**238955**

Deliverable D0.8

Report 2nd BEST Network Workshop vs0 2

Final version
Dissemniation level: C
Date of submission: 1st October, 2011
Author: Max Snijder

Contents

1. Project Summary & Introduction.

BEST Network, the Biometrics European Stakeholders Network, is a European Commission ICT Policy Support Programme centred on a European Thematic Network on Trusted information infrastructures and biometric technologies. To facilitate the latest information exchange and expert opinion, BEST Network has brought together key stakeholders including the finest experts from across the EU to determine how biometrics can most appropriately be applied in the context of the Charter of Fundamental Rights of the European Union.

BEST Network will focus on promoting the development of new policy implementation schemes through working groups and workshops. This will include the exchange of best practices, common cross border strategies and future pilot activities.

In its role to communicate the activities and deliverables of the BEST Network, the BEST Network Dissemination Conference was held in Darmstadt, Germany in September 2010.
The aim of the Conference, which was midway through the project, was to communicate the results of the BEST Network project to the audience and to the wider community and to stimulate interest and further contributions to the project.

2. Preparation of the 2nd BEST Network

To prepare the workshop a conference call for the chairs and co-chairs took place on September 2nd, 2011. On August 12th the coordinator received the formal confirmation from the commission that the recovery plan was accepted and that the suspension of the project was lifted as from September 1st. For that reason the conference call was moved to September 2nd.

During the conference call the agenda of the workshop was decided (see Annex 1) and administrative issues were discussed (see Annex 2 - Minutes of the Conference Call).

Furthermore it was decided that each chair/co-chair would make sure that a short introduction to their WG was done. The purpose of the introduction was to summarize the WG outcomes until now and to decide the topics and issues for further discussion at the workhsop. The goal of the workshops is to deepening the discussions which have started during the first part of the project and to prepare the November workshop based on the outcomes of the September workshop.
This report describes the discussions that took place during the workshop by providing an outline of the topics and issues that were discussed and by providing summaries of observations and conclusions. The sources used for this report have been 1) notes of the coordinator, 2) notes of chairs/co-chairs and 3) tapes. The report doesn't contain quotes from individual people as it should be seen as a joint achievement.

3. 2nd BEST Network Workshop (non public), 15-16 September 2011

The final agenda of the 2nd workshop was as follows (see also Annex 1):

Day 1, September 15th	
10.30 – 11.00	Welcome and introduction by coordinator - Administrative affaires - Agenda of the Workshop Alexander Nouak / Max Snijder
11.00 – 11.45	BEST Network: the new work program Max Snijder
11.45 – 12.30	WG1 discussion introduction: Günter Schumacher
12.30 - 13.15	WG2 discussion introduction: Dmitrios Tsovaras
13.15 – 14.15	*Lunch*
14.15 – 15.00	WG3 discussion introduction: Max Snijder
15.00 – 15.45	WG4 discussion introduction: Herbert Leitold
15.45 – 16.15	*coffee/tea*
16.15 – 17.00	Next ICT call introduction: Alexander Nouak
Day 2, September 16th	
09.30 – 10.15	WG5 discussion introduction: Juliet Lodge
10.15 – 11.00	WG6 discussion introduction: Alexander Nouak
11.00 – 11.15	*coffee/tea*
11.15 – 12.00	WG7 discussion Introduction: Emilio Mordini
12.00 – 12.30	Discussion on Eurosmart White Paper Smartcards & Biometrics: How can BEST Network contribute to next version of the White Paper? (*** see link below) introduction: Didier Chaudun
12.30 – 13.30	*Lunch*
13.30 – 14.15	plenary discussion (based on results of WG discussions) OR: separate discussion per WG (to be decided at the workshop)
14.15 – 15.00	BEST Network Final Conference: European Biometrics Summit - goals and objectives - format, structure, content - pre-conference workshop introduction: Max Snijder
15.00 – 15.30	*Coffee/tea*
15.30 – 16.00	European Technology Platform (see appendix)

	Günter Schumacher
16.00 – 16.45	BEST Network after project end: the setting up of a new European platform introduction: Max Snijder
16.45 – 17.00	Wrap up and closure Max Snijder / Alexander Nouak

4. WG Session reports

4.1. WG1

The aim of WG1 is to identify technological and conceptual gaps instead of also assessing them. The BEST Network workshops facilitate the discussion on the issues for the relevant stakeholders rather than proposing measures.

The main recognized issues of biometrics for border control are:

- Biometric spoofing of face and finger (WG6 liaising with BEAT)
- Conceptual gaps of ABCs
    - we need systematic approach on informing relevant stakeholders on the conceptual gaps.. training, but in the right way, is needed (WG5!)
    - Ageing problems (and how this affects efficiency)
    - Acceptance (of customers/travelers) and convenience
        - issue of bad publicity: the opinions/issues/risks are not openly expressed and this could significantly set back the industry if later on these issues arise due to incidents)
    - Data protection (WG7: Privacy by Design and PIA's for policy makers)
    - Quality and integrity of biometric data (fingerprints, face recognition) encaputured in passports etc. are very important, as low quality and integrity means a larger depency from manual inspection and supervision procedures at border control check points.
        - WG3 remark: at Schiphol there is a new large scale ABC project: NoQ, which will install 110 ABC gates for Schengen to non-Schengen (vice versa) by the end of 2012 (see also WG3 presentation). NoQ has solved the spoofing and quality problem by making the face recognition as a additional feature as part of a chain of measures. There is a strong supervision process (human control). The supervisor decides if there are false positives or false negatives. Another person looks at "strange behaviour" on the camera's.
        - WG6 remark: still the ABC systems have common conceptual gaps: the border guard can have a bad day so the risk of human failures remains. A deterministic system can be cheated once you know how it works. Human control (also unexpected and ad randum) will support in solving this issue. However, if the system's reject rate becomes to high, the border guards might in the end ignore it or lower down the thresholds. If there is no red flag, they are so happy, that they will just relax and not check extra. This creates perceived security (for a while), but no real security.
- Process of obtaining the biometric data (e.g. capturing fingerprints at the municipality, vs. capturing by the police); currently the process of capturing the biometrics data for the e-passport by European member states show a large variety in quality and integrity. That

means that either a discriminanitive method is needed (passports from countries with bad quality biometrics need to have additional checks) or the overall quality excaptance threshold needs to be lowered towards an exceptable level for all passports. The later means that the overall security will decrease and the amount of manual efforst will increase, thus making the ABC systems less efficient.

WG7 input: privacy should be looked at from the perspectives of different stakeholders (user/traveler, company, government):

- User: they may want privacy, but are not aware of what is happening with their data and their rights according to privacy and data protection law.
- Company: will perform a cost-benefit analysis to see to what extent compliance with (data protection) law is desirable
    - Is concerned with ideal implementation of an application.
    - Privacy/legal requirements are not always included.
- Government: interested in data (fighting crime/terrorism, national security).
    - Often difficult to assess what kind of biometric developments are deployed at present in the governmental area due to confidentiality of such information.

In the area of law enforcement and criminal investigation you have most of these issues are not present. However, if biometrics are used for authentication purposes for citizns, these issues beconme more paramount. The crucial stakeholders are the policymakers.

WG1 and WG3 will jointly seek for input to the pre-conference workshop on February 16th. The goal should be to have a structured dialogue on the requirements regarding the quality and integrity of the biometric data for ABC and how the current passport application process and the associated capturing of biometric information do meet with those requirements. Vice versa, it should be understood how the quality and integrity of the passport biometrics do impact on the usability of the e-passport for biometrics based services, such as ABC at airports.

4.2. WG2

Dimitrios Tzovaras presented the roadmap towards D2.3 of BEST Network focusing on the ideal implementation of an application which includes biometric technologies as constituting element. The presentation was prepared by Olivier Epinette and Daniela Reyes.

Guenter Schumacher commented that the methodology proposed was somehow general and could be specialized concerning the inclusion of biometric technologies. It was agreed that WG2 should clearly indicate in D2.3 which elements from *definition, enablers & drivers, implementation steps, application requirements, key players relationship and technological development* are clearly linked with the choice of the biometric technologies involved. The final D2.3 document should clearly show what is specific for biometrics in the proposed methodology.

Max Snijder proposed to add another column in the methodology called “Feasibility” which could be the intermediate step between application requirements and technological developments. This would serve as a go/no-go step in the whole implementation process. Also, participants proposed to include more elements in the methodology, i.e. the following:

- Include also “added value of introducing biometrics in the particular application” in the *Definition* column.
- Include also “legal issues” and “liability and how it related to safety and robustness” in the *application requirements* column.
- Include also “organization top level training” in the *stakeholders/participants* column.

A discussion was then initiated concerning potential overlaps with WG4 and it was agreed that the two WGs should exchange documents and also potentially plan for a common workshop in the next meeting in November.

Max also proposed to create a quick scan feasibility tool out of the proposed methodology. These tools could be useful for anyone who wants to make use of biometric technologies in new applications since it can be used as a feasibility go/no-go check before taking any decision in this direction. It was agreed that WG2 would produce this tool, which could be used also in WG5, and this would be one of the main outcomes of the project. A Privacy Impact Assesment (PIA) should also be part of the tool.

During the next workshop in November also legal requirements should be discussed.

From training and eductiona point of view (WG5) it was mentioned that top-management decision makers would benefit from a better understanding of biometrics. Managers who are involved in the development process of a biometrics application should be aware in an early stage of the various typical issues that biometrics bring foreward when being apllied in daily life. This will encompass the basic technical characteristics (e.g. the staistical nature of it), the management of the biometrics from a technical, system and operational point of view. WG5 therefore will take this on board to their further work.

4.3. WG3

ABC system are gaining grounds from RT. Ten years ago the first biometrics based border control systems at airports were RT programs (Privium, Project IRIS). The advantage of ABC over those first RT schemes is that there is no pre-registration, a common trustworthy identifier is being used (i.e. the biometrics passport) and there are no extra costs involved for the traveler. The strong development towards ABC systems at airports is because the three business drivers (security, convenience, efficiency) are equally relevant at an airport. At the same time the business drivers represent the three main stakeholders: government (security), airlines (convenience) and the airports (efficiency).

Although the three drivers are almost equally relevant, it is efficiency in the first place that drives the ABC systems at airports. ABC is not a security measure. The main driver is efficiency: the number of passengers increase, but space and resrouces remain the same.

The factor of convenience is embedded in a larger global development towards the self service travel experience, the so called self service (r)evolution: internet check-in, mobile check-in, kiosk check-in, self-tagging, baggage self drop off, transfer kiosk, self-boarding, self-recovery ... The global association of airpprts (IATA) has the following vision:

« By 2020, 80% of global passengers will be offered a complete self-service suite based on industry standards »

Biometrics based ABC fit into this vision.

An important example of this development is the program NoQ at Schiphol Airport. This program foresees the installation of more than 100 ABC gates in the Schengen/non-Schengen area (S/n-S). Within the Schengen area no regular id-check is required, so no buinsess case for ABC exists. The S/-nS gates for this moment are ment for European citizens (18+) who are in the posession of an 2nd generation e-passport.

The NoQ project raises the question about the actual security level of the ABC gates. Although no details are available, it can be assumed that the overall security level of the NoQ ABC gates (i.e. the gates plus all additional measures, such as monitoring and supervision) will be higher or at least equal to the manual process. As this project is driven by the Dutch government one can expect that proper threat analysis has been performed having resulted in a positive outcome. Nevertheless, for the sake of transparency the question remains to what extent the ABC gates provide atual security versus perceived security. Perceived security can 1) scare off perputraders and 2) provide the sensation of security with the travelers. Both can be positive for the business case. However, these positive affects of perceived will be temporarily once the flaws of the system are known, resulting in negative effect on the perception of safatey with the travelers. Therefore it is important to cleary make a difference between perceived security and real secuity.

During a WG6 conference call on ABC in February 2011 there was a discussion on the standardization of ABC. Starting point of the discussion were the D3.1 and the Frontex ABC Best Practice Guidelines. During that discussion it was remarked that 1) the Frontex guideline was not established in concertation with the airports nor the airlines and 2) that both documents took very litlle consideration about privacy and data protection issues. Therefore Paul de Hert (WG7) did send in a commenting document (see Annex 3, co-authored by Els Kindt, Unviersity of Leuven).

Given the strong presence of all three business drivers it is recommended if not inevitable that the three main stakeholders (airports, government and airline) will work together more closely.

If we speak about security of the ABC systems it is important to acknowledge that there are two main perspectives:

- security of the airport and the flight (e.g. terrorism)
- security of the data of the travelers (data subjects)

Mostly only the first one is emphasized and communicated. That means that the data security (and the associated level of privacy protection) is generally less elaborated. This is a potential threat to general privacy principles, especially because there is no common European policy on this.

The main driver for ABC is efficiency in terms of government personnel savings , not improvement of throughput speed. The assumption that ABC as we currently see them appear to do take less space is not true. In general we see that actually one ABC currently is slower than one officer, while the footprint requirements are more or less the same. However you can place more ABC's on one officer, thus compensating for processing time loss of ABC. Hence: ABC need more space to be able to have the same throughput as the manual process, while it saves government personnel (not airport/airline staff, since generally government asks airports to deliver more airport assistants helping passengers through ABC). Given this there probably will be a minimum volume of S/n-S travellers needed to reach a positive return on investement. If this minimum is not reached the ABC systems will be too expensive. It is yet unknown what this threshold currently will be, just like the answer on the question for whom the costs and benefits are. To find this out an integral business case is required involving all stakeholders. In the longer term, when the costs of ABC systems have dropped, these systems will become more attractive to the smaller airports.

Another observation is that in essence ABC will have to be able to process all groups of travellers: with ePassport EU as well as people from outside of EU (TCN) who will have to be registered. Airports and governments are looking for one size fits all solutions rather than three different piecemeal solutions. Challenge is to maximize the number of travelers that can use ABC´s in order to maximize ROI. That means a combination of ePassport and registered travelers (people who do not have (e)Passport they can use-TCN) need to be able to do that. The IATA has developed a recommendation on a international traveller scheme: RP1701 (see Annex

Aviation industry is taking the first baby steps into this new field of biometric processing. The first releases ABC do not solve the issues at hand and are still far from perfect. The good news is that there is a lot of room for improvement. Large implementations such as NoQ will learn us more about technology acceptance amongst a wider public and how to manage the systems efficiently. It is common knowledge that the group of frequent travelers benefit most from a fast and smooth border control process. For the wider public this is still unexplored.

In the meanwhile there is also a shift in the government's approach on assessing the risk regarding individual travelers. Rather than applying one type of thourrough security regime governments now are more looking into the threat which each individual poses. That requires an individual approach. The focus will shift from *"Does this person carry a knife?"* to *"Who is this person: where is he going, what are his connections, does he have a criminal record?"* Based on this profiling the travelers are being processed accordingly through different security mechanisms. IATA's check point of the future is a first attempt to bring this approach into practice (see WG3 presentation).

This immidiately raises the question: based on what information does this profiling take place and how is this information gathered? How consistent and reliable will this information be (e.g. spelling)? How search criteria aligned? Not surprisingly it can be observed that the police (government) and

airlines are searching for each other, as they might benefit to combine the police data (e.g. identity, passport number ...) with the data that airlines contain from their travelers (identity, destination ...).

Looking at the IATA's Check Point of the Fututre, which seperates the travelers for the security process based on the risk profiles they are labled to, one might ask whether travellers will be happy with cleary being separated into three different groups. Especially if somebody is indicated for the 'high security' lane this person might get an unpleasant feeling. IATA describes three types of security lanes : enhanced security, normal security and known traveller. After the presentation of the Check Point of the Future the IATA concept was seriously challenged by the airlines. The separation of risks non visible to travellers is one thing, but the different lanes for different categories led to a serious discussion over ethical issues.

Specifically for the ABC gates the question is how the quality and integrity of the biometric data affects the performance of the gates. And if a passport shows a very low quality of the biometrics information, how will the ABC gate deal with that in terms of thresholds and manual inspection. This where WG1 and WG3 converge: the efficacy of the ABC gates depends on the qualtiy and integrity of the passport application process.

Another convergence we see is that once the government will able to access the personal data from the flight information system, the ailrines might look into using the identity credentials which are being generated by the government in their ABC gates. Once the identity of a traveler has been verified the life biometric image which has been taken into the ABC gate could be reused in other passenger ground processes, e.g. for automated boarding or lounge access.

So there are several convergences to be observed:

- ABC towards RT (or vice versa)
- Airlines and governments sharing data
- Embedding ABC into the overall airport process context: airports (passively intelligent acting as a TTP) can take up the role of facilitating the exchange of information between those stakeholders to enable simplifying the business process and seamless flow at airports

A common issue of increasing security measures is that criminals will find other ways. The problem will be shifted, either to other airports that do not have these kinds of strict border controls, or to other manners of traveling.

Questions to be further discussed at the scond workshop are:

- is there European leadership; who could be the leader (Frontex?)
- is a European approach needed?
- what is the impact of the non-consistent quality/integrity of European e-passport biometrics and how can this be addressed?
- how can quality/integrity of the e-passport be harmonized in EU
- is there a standardization process on ABC going on (e.g. CEN, ISO)

- what are the (potential) consequences of merging/combining police data with flight information data?
- what is the impact of ABC gates to provide id-credentials for other processes (e.g. boarding)
- what are the risks of creating the perception of security through automation, while keeping human supervision at the background?

NOTE: Paul de Hert from WG7 (in cooperation with Els Kindt from the University of Leuven) has commented on the Frontex Best Practice Guidelines on ABC and D3.1 of WG3. These comments have been included to this report as Annex3

4.4. WG4

Herbert Leitold started the WP4 discussion on "eID and electronic Services" with a presentation on the status and the plans for the final deliverable: D4.1 and D4.2 have been delivered; D4.2 received positive remarks by the reviewers in the second deliverable. As most of the content aimed for in the Description of Work has been provided with D4.1 and D4.2, the revised work plan aims for consolidating the material already available by scrutinizing D4.1 and D4.2 in the broader BEST-NW audience.

D4.3 is due December 23rd. The presentation of Herbert said (taken from the recovery plan):
"*D4.3. shall not produce substantially new content, but scrutinize the existing material in the networking phase and report on the result.".*
Therefore, the presentation was meant to give core content on D4.1 and D4.2 and to provoke discussion on it.

The discussion following the presentation touched upon the following issues and topics:

1. Synergies might exist with WP7, e.g. on Privacy Impact Assessment (PIA). WP4 should join WP7 discussions.
2. Is it convenience that might drive usage of biometrics? This view clearly also came up later during the presentation by Günter Schumacher on the establishment of a Biometrics ETP (see further in this report), who's vision is that biometrics will only take off as an enabler of citizens oriented services once it will be adopted in non-governmental and non-security based applications.
3. As biometrics for remote access has not emerged, is there a piece of technology missing that solves this and can we describe what this piece of technology should provide?
4. The question has been raised whether we face a technology problem or an integration problem.
5. On a "*this is the problem - this is how technology should solve it*" statement on the slides, a discussion evolved whether the problem-driven approach is always the successful one. There may be other aspects why a technology sells than just solving a problem.
6. The question has been raised, whether there are areas (such as unattended remote access) where there won't be biometrics at all.
7. On discussing business cases, one needs to distinguish between two kinds of technologies:
    a. Infrastructure-driven (e.g. the Internet)
    b. Market-driven (consumer products)

8. Biometrics has been stated as a supplement to conventional technologies (see also 10. below on security)
9. The following statement in the introduction of D4.2 was considered too strong "*The conclusion of this WG, reported in this Deliverable are that there are a range of types of reason leading to the widespread practical failure of biometrics*: ….". This should be better set into the context of D4.2 (failure in remote access environment)
10. A statement was made that biometrics is wrongly considered as a security technology. It is a personalisation technology that adds security by introduction an additional factor.
11. A line of thought has been expressed whether acceptance of biometrics may be raised by applying it to social networks, where people tend to reveal personal data. This was questioned due to legal and ethical problems arising.

4.5. WG5

The first output of WG5 was concerned with producing an outline of the available biometrics-related training and education provision in Europe. In this final phase of work the focus is now on the development of a coordinated action plan to address needs and gaps regarding training and education provision on biometrics in Europe. The provisional shortcoming should be identified and suggestions for addressing them should be catalogued through Network discussions and collated to produce the final deliverable of WG5.
To this end the following discussion points are suggested for the consideration of the whole Network during its Workshop in September.

Discussion Points for this 2nd Workshop where as follows:

1. What are the skill and educational needs in the following areas of the Network's activities?
    a. Passports and public administrations (WG1)
    b. Emerging applications (WG2):
        i. time and attendance / access control
        ii. biometric payment
        iii. video surveillance
    c. European ABC and RT (WG3)
    d. Biometrics and e-ID: national eID and e-services (WG4)
2. How can these needs, in each of the above areas in turn, be addressed?
3. What common and coordinated measures may be taken to enhance the level of skills and education in the field of biometrics technologies and services?
4. How can BEST Network address these issues now and in the future, given the perspective of a new European platform on biometrics after BEST Network project end?

Important mission of a European T&E provision is 'train the trainers'.

In the discussion of training and education needs and imperatives, clear distinctions were drawn between the provision of generic curricula in universities and post-school education and the kind of training for specific purposes and specific types of personnel who might be engaged in the enrolment, processing or handling of biometric data. Computer engineering, ICTs and science curricula included biometrics more frequently but rarely expose students to consideration of the

impact of their work regarding socio-legal and ethical issues. This was seen as vital. By contrast humanities and social sciences degrees tend to stress the negative impact of new technology without sufficiently showing understanding of the science.

The biggest challenge for training and education, however, was seen to lie with the need to ensure that procurers of biometric ICT systems understood the limitations and power of biometrics in specific setting: the one-size-fits-all model was rejected as inappropriate.
It was clearly concluded that there is an urgent need to show the importance of using specific systems and use cases as opposed to grasping inappropriate legacy systems designed for different purposes (eg fingerprint forensics v. security application of biometrics). If not, false hopes are created inferred from biometrics as a panacea, causing application and system designers to start with wrong expectations.

There was discussion of the need to train the trainers with regard to the EU's specific needs and requirements which differ substantively to those of other states (like the US and China) for example in respect of privacy. The conclusion was that there should be a visible independent, credible and authoritative EU body that would be objective and seen as a trustworthy source of appropriate information regarding technology, training, education and biometrics uses.

The area's where training and education skills are mostly needed are:

- Passports and public administrations (WG1)
- Emerging applications (WG2):
    i. time and attendance / access control
    ii. biometric payment
    iii. video surveillance
- European ABC and RT (WG3)
- Biometrics and e-ID: national eID and e-services (WG4)

A risk in the current policy making concerning large scale biometric deployments is that people don't know that they don't know. This creates the risk of starting the project with the wrong expectations. Therefore people need to be informed about the basics of biometrics at early stages of a project. Usually the police is supposed to know and understand about biometrics because of their large experience with fingerprints and forensics. However, this knowledge is only partly applicable to the processing of normal citizens. Most of these issues can be addressed by building awareness.

Observed gaps and issues in Training and Education are:

- There still exists a wide persistent ignorance among policymakers and implementers at all levels
- Authoritative, informed, credible and independent EU views and training are essential for further progress
- Gaps in provision at university level owing to swift introduction of biometric outstripping slow pace of adaptation in many university degree programmes
- Insufficient number of skilled University qualified people at the technical level are available to the market
- A diverse understanding of commonly used terms that different sectors use and understand differently (eg interoperability)

Regarding education it would be desirable to establish an overview of the availability of academic curricula. In addition some kind of a structured school should deliver courses periodically. These can be developed and provide by a new European organization, but in addition this new European organization could also engage existing provisions such as the Alghero Summer School in Italy and the workshops from the Biometrics Institute. National fora as such in Germany, The Netherlands, Italy and the Scandinavia countries could also be involved.

The following gaps in academic eduction were observed:

- there are gaps at university level owing to swift introduction to biometrics
- at a technical level there are insufficiently skilled university qualified people

For the next workshop the following questions need to be addressed:

- What common and coordinated measures may be taken to enhance the level of skills and education in the field of biometrics technologies and services?
- Should there be a biometrics group modelled on the initiative in July 2011 by Net security firms who supported a new group seeking to provide cybercrime training for law enforcement officials as part of a wider fight against cybercrime. McAfee and Trend Micro pledged support for the fledgling International Cyber Security Protection Alliance (ICSPA).

If there would be a specific European body in training and education its tasks would be:

- Awareness building of the realities of biometric applications
- Overview of academic curricula availability
- Structured school able to deliver periodic courses
- Develop appropriate training materials and resources

The overall conclusions of the WG5 discussions were as follows:

- Training and education Provisions need to be developed to 'Train the Trainers' (beware of language issues in EU27+)
- There is a need for training at system (technical) level and policy level but less so at operating level (ms dependant, system specific)
- It is needed to train people so they can better understand, assess, design and evaluate their systems (link to WG6)
- product specific training plus general introduction to biometrics is generally needed

At the next workshop a concrete plan will be discussed to address these issues and needs.

4.6. WG6

WG6 work to date and status was detailed in Alexander Nouak's presentation.

D6.1

D6.1 is an inventory of testing and certification institutions in Europe.
It was noted that D6.1 is a living document and needs to be updated.

D6.2

D6.2 is the assessment of selected application scenarios on their relevant standards and evaluation schemes. NPL has done work on access control evaluation and testing, and will provide input on this for D6.2.

WG5 collaboration

Collaboration with WG5 (skills, training, and education) in the subject area of biometric testing was discussed. Many customers perform their own testing and so these customers will need to obtain the appropriate skills and training to correctly perform biometric evaluations. WG6 may be able to provide input for training courses related to biometric evaluation and testing for end users for the WG5 work on a European Biometrics Academy.

FP7 project Biometric Evaluation and Testing

Seven proposals had been submitted for EU FP7 project topic SEC-2011.5.1-1 "Evaluation of identification technologies, including biometrics". However only one project, BEAT, was funded. It was noted that sometimes the EU will fund project areas which they have also previously funded. However, it was perceived is rather dissappointed that none of the partners of BioTesting Europe are being involved in this project, although it paved the way for a sound European strategy on testing and certification of biometrics systems and components (www.biotestingeurope.eu).
The FP7 project BEAT (Biometric Evaluation and Testing) was discussed and the project coordinator will be invited to present to EU BEST. The project will be quite focused on security. The list of participants in BEAT was provided, and included Idiap research institute, Morpho, TUI IT, Universidad Autonoma de Madrid, University of Surrey, Leuven Catholic Univeristy, a Turkish research company, and Commersat-Energie in France.

BSI (D) testing work

There was a discussion on German BSI research work and standardization. BSI produce technical guidelines to advance biometric work and stimulate ISO work. However, it was felt that there was a lack of opportunity for expert or public contribution to BSI technical guidelines. It was noted that BSI have provided a document on finger spoofing, which is available for public download.

Common criteria

It was noted that common criteria standards do not really apply to biometrics, as biometrics is not a core security technology.

ISO biometric device certification

Work on a new ISO standard for certifying finger devices was briefly discussed. There will be three possible certification levels. It was agreed that something similar could be produced for face biometric devices. It may be possible to test devices and state that the device is conformant and produces conformant biometric records.

ISO-29196 "Guidance for biometric enrolment"

The draft ISO-29196 work on "Guidance for biometric enrolment" was discussed. It was noted that an earlier version of this document was reviewed and taken into consideration in preparation of D6.2 for the existing section on e-passport enrolment. The ISO report will be a set of guidelines and therefore cannot be directly evaluated against for conformance. It was proposed to invite the ISO document editor, Marek Rejman-Greene (UK), to the EU BEST pre-conference workshop in February 2012 to discuss work in this area further.

CEN/TC224/WG18

The ABC work of CEN/TC224/WG18 was discussed. This group is creating guidelines and technical reports. They are working on a draft report entitled "Recommendations for using Biometrics in European ABC". Active members of this group include experts from Austria, France, Germany, Poland, Spain, and the UK.

EUROSMART whitepaper

The Eurosmart whitepaper on "Smart Biometrics for Trust and Convenience" is of interest to WG6, and several WG6 participants agreed to participate in a joint workshop with the technical biometric committee from Eurosmart. The goal of the workshop would be to help improve the technical content of the whitepaper which may be released in as an updated version in Q1 2012. Travel to this meeting may be funded by Eurosmart (see also Chapter 6 of this report).

4.7. WG7

The discussion began with a clarification over the use of biometrics : they were pervasive and limiting or preventing their deployment was virtually impossible. The chair and co-chair agreed on this. This led to an exploration of the meaning of privacy historically and in the contemporary world: the question of nudity versus nakedness exemplified distinctions and ethical issues in relation to body scanners. The problematisation of this required an assessment of authoritative, credible, transparent and ethical use in different settings. Trust in biometrics remains contextually dependant and widespread ignorance among procurers about different aspects of biometrics led to suboptimal decisionmaking and undesirable consequences that could lead people to reject the use of biometrics per se, and to continue to confuse biometrics with the unrealistic hype surrounding the notion of inter-operability. The need for a credible, trustworthy body to provide independent objective advice and views again surfaced as an item of debate.

Privacy is knowledge about the personal sphere of a persons life. In a second manifestation, privacy is meta-knowledge about some intimate issue. In third, privacy is power to control over knowledge.

Personal data, concentrated information in raw or unorganized from about an individual, is shifting from personal knowledge understood as self-knowledge (introspection), to personal knowledge understood as knowledge about the self. If knowledge about oneself becomes detachable, it will become marketable.

Also there is a shift from privacy to data protection: data protection generates a technical conception of privacy, now framed in terms of risk management and technical ability to protect or

penetrate the private sphere. Privacy and security become counterweights in the same balance. Data protection is just one means to protect privacy. The behaviour of the data subject regarding participation to social networks or sending sensitive messages unprotected through the internet, is for a large part impacting the vulnerability regarding privacy. Most people are not sufficiently aware of this and should ideally receive more education on this.

The challenge with biometrics is that citizens have not been confronted yet with the benefits nor with the risks of using biometrics in daily life. Also large surveillance systems which are using biometrics to identify people are not directly confronting the citizens with the impact of these systems. It therefore would be helpful if services based biometric applications would be developed. That would provide experiences with citizens which are not security based, but which show the benefits of biometrics to increase the convenience of certain services.

Than the question was raised what the term Privacy by Design actually means in the daily practice of applying biometrics. Which design is this referring to? The technical or functional design? The design of the legal framework? The ov erall design? In case of the latter: where does this overall designing process exactly start and who are involved in that? How are the people advocating PbD and are they actively involved in the design process in an early stage?

It was agreed that the use of biometrics always requires the direct involvement of the senior management of an organization. In order to integrate PbD in an early stage it will be needed that the senior management is aware of the need of it. That means that it will be beneficial in many cases if the senior management would be well informed about the typical challenges that biometrics bring regarding privacy and how these could be addressed. This should be further elaborated in WG5 in connection with the establishment of education programs and courses on biometrics.

5. ICT Calls

Alexander Nouak gave an introduction to the FP7-ICT-2011 Call 8 and the security call FP7-SEC-2012-1 (see ANNEX). It was concluded that the ICT call gave very little opportunity for a biometrics project. However, the SEC-2012 call provided a very interesting call on automated border checks at airports:

SEC-2012.3.4-6 Enhancing the workflow and functionalities of Automated Border Control (ABC) gates (CP-IP). It was proposed that ideally an airport should be coordinator. Max will approach Schiphol.

6. Eurosmart white paper “Smart Biometrics for Trust and Convenience”

The Eurosmart white paper on “Smart Biometrics for Trust and Convenience” (see Annex 6) is of interest to WG6, and several WG6 participants agreed to participate into a joint workshop with the technical biometric committee from Eurosmart. The goal of the workshop would be to help improve the technical content of the whitepaper which may be released as an updated version in Q1 2012. Travel to this meeting may be funded by Eurosmart (to be confirmed). The following BEST Network members have confirmed their participation to such a workshop: Raoul, Juliet, Emilio, Olaf, Michael,

Tony, Max. More members can join by sending an email to Max. As the revised version of the White Paper is planned for February 2012, the workshop should take place as soon as possible. Max will coordinate this with Eurosmart.

7. BEST Network Final Conference (Feb. 16-17, 2012)

The concept of the BEST Network Final Conference was discussed. The following was agreed:
the conference will consist of 1 day for pre-conference workshops (1 or 2) and 1 day for a public conference

- the conference should deal with current issues as well as providing a vision for the future
- the conference will have a recognizable title, so it can be marketed with more impact. The title should also make it possible to become an annual event.
- the agreed title is: *European Biometrics Symposium 2012*.

Max will start announcing and promoting the event asap.

8. European Technology Platform (ETP) on Biometrics

Günter Schumacher from the EC-JRCT IPTS gave a presentation on the potential of setting up a European Technology Platform (ETP) on biometrics (see enclosed presentation and *Annex 4*).

The political dimension of biometrics increased dramatically with the threat of terrorism, in particular since the 9/11 event. Driven by good experience gained in the area of law enforcement, biometrics was supposed to serve for better (i.e. stronger) identification of individuals in general as a mean to improve public security. Another important driver was the increasing level of immigration which made it necessary to create efficient measures for border control and for preventing fraud. Consequently, biometrics has become an integral part of new concepts to improve identification document security, in particular focussing on fingerprint identification and face recognition.

In parallel to its wider deployment, biometrics has become subject to severe concerns about the potential harm to the fundamental rights of privacy and data protection – a controversy still ongoing by 2011. But not only the privacy concerns hampered the smooth roll-out of the technology. Questions of scalability and interoperability soon raised further doubts about the feasibility of biometric based identity management (IDM) at large. These questions are still not fully answered, despite the impressive number of already registered biometric identifiers in numerous governmental IDM systems worldwide.

With increasing number of biometric tokens (passports, ID cards) rolled out, the question about its potential “dual use” for non-governmental applications is now on the agenda of many countries. Likewise, completely new and non-security related application scenarios are under research and development. This fact has furthermore contributed to a highly diversified picture of what is still summarised under the heading “biometrics”. There is almost no question about biometrics which

could be answered without looking at its technical and non-technical context, neither about its technical capabilities, nor about its ethical implications.

The first larger scale implementations of Identity Management Systems involving biometrics have revealed the four basic problem areas:

1. Insufficient maturity level of state-of-the-art technology: performance, accuracy, scalability
2. Lack of commonly agreed quality assessment: testing, evaluation, certification
3. New security problems: protection against ID theft, privacy
4. Ethical concerns and societal acceptance

A comparison was made with the USA, where already in 2002 a coordinated approached on biometrics was developed at the highest policy level (NSTC, subcommittee on Biometrics and Identity Management). This strategy has crystallised in an impressive number of R&D support programmes which, of course, benefits mainly US companies in the sector. This strategy also provided industry with a clear perspective on future markets in order to stimulate their own investments. A similar approach never took off in Europe, although several initiatives were taken. Günter strongly advocated the establishment of a similar body on biometrics in the form of an ETP.

The envisaged ETP has to be defined along a number of different dimensions which might be grouped as follows:

1. **Mission:** What is the scope, what are the limits of actions provided by the ETP? What should be the widest context in which the ETP operates?
2. **Objectives:** What are objectives of the ETP in terms of new products and services? What vision does the ETP develop regarding the future use of biometrics and its integration into various kinds of applications?
3. **Structure:** Shall the ETP – according to its mission – work as an independent organisation or should it be integrated into or merged with another ETP (see attached list)?
4. **Operation:** How is the operational business of the ETP organised? Should there be a executive office? What kind of organisations need to be involved? How will the operational business of the ETP be financed?

The ETP should clearly look into the future developments involving new technical modalities (e.g. behavioural biometrics) and service based use cases (e.g. payment).

During the discussion it was decided to prepare some focused input for the pre-conference workshop on February 16th. The selected topics should concern immediate challenges which are directly impacting the usability, as well as the establishment of a vision on how these challenges can be addressed. It was also suggested to invite Duane Blackburn from the NSTC Subcommittee on Biometrics for the final conference.

9. BEST Network after project end: setting up a new European biometrics platform

It was discussed if a new European platform on biometrics was needed and if so, how that should look like. The conclusion was that the EBF leaves a gap which needs to be filled. However, the new platform should be membership based and should be based on a more diverse business model. The new platform should be a common meeting place, while accommodating the possibility for the partners to set up and organize a variety of activities. These activities should be able to have their own business model and should be able to be managed under the board of the platform. The activities of the new platform will be divided into three main streams:

- Community Building
- Training & Education
- Projects & Research

The activities of the new platform will carry a common 'brand', so a clear link to the new organization is always made. The board of the new platform makes sure that the brand is managed properly.

It is difficult to speak about biometrics as an industry, as biometrics is a technology which forms just a part of a large variety of applications. Nevertheless, it was concluded that the issues concerning the large scale adoption of biometrics into various application area's do need specific attention. The technology is complex due to its multidisciplinary aspects and the fact that it affects all (European) citizens. Many issues, such as a common understanding of the technology, high quality training and education, exchanges of experiences, maturation of the standardization, testing and certtification, legal and privacy aspects and many others need proper and targeted attention, rather than being part of a larger cluster of technologies, such as an ICT platform. There is some evidence that with the embedding of biometrics into broader community structures the specific issues concerning biometrics will be snowed under, leaving open a structural debate on issues as described above. It was concluded that a new platform would contribute to a faster and more responsible uptake of biometric technologies into common use application. In addition it was concluded that since the BioVision report from 2003 fragmentation of the European market place still is a fact of life.

The first activities of the new platform will be:

- Setting up training programs (workshops, courses, cooperation with existing training providers, e.g. Alghero Summer School, Biometrics Institute)
- Organizing an annual biometrics symposium
- Setting up a European newsletter (e.g. with news and updates from various member states, research centres, industry, academia, biometric fora etc.)

The partners agreed that a new European platform on biometrics should be set up according to the vision as described above. Max is mandated by the BEST Network members to take further steps

towards the formal set up of such a platform. Jean-Paul, Alexander, Christoph and Marek will provide their support (*additional help will always be more than welcome!*).

If it will be an association, the name will be 'The European Biometrics Association'. It would be desirable if the setting up such a new European platform would be announced before the Biometrics Conference in London. Max will prepare a press release.

10. ANNEX

10.1. Annex 1 – 2nd Workshop Agenda

2nd BEST Network Workshop / Darmstadt, September 15-16, 2011

AGENDA

Day 1, September 15th	
10.30 – 11.00	Welcome and introduction by coordinator - Administrative affaires - Agenda of the Workshop Alexander Nouak / Max Snijder
11.00 – 11.45	BEST Network: the new work program Max Snijder
11.45 – 12.30	WG1 discussion introduction: Günter Schumacher
12.30 - 13.15	WG2 discussion introduction: Bernadette Dorizzi
13.15 – 14.15	*Lunch*
14.15 – 15.00	WG3 discussion introduction: Nanne Onland
15.00 – 15.45	WG4 discussion introduction: Herbert Leitold
15.45 – 16.15	*coffee/tea*
16.15 – 17.00	Next ICT call introduction: Alexander Nouak
Day 2, September 16th	
09.30 – 10.15	WG5 discussion introduction: Juliet Lodge
10.15 – 11.00	WG6 discussion introduction: Alexander Nouak
11.00 – 11.15	*coffee/tea*
11.15 – 12.00	WG7 discussion
12.00 – 12.30	Discussion on Eurosmart White Paper Smartcards & Biometrics:

	How can BEST Network contribute to next version of the White Paper? (*** see link below) introduction: Didier Chaudun
12.30 – 13.30	*Lunch*
13.30 – 14.15	plenary discussion (based on results of WG discussions) OR: separate discussion per WG (to be decided at the workshop)
14.15 – 15.00	BEST Network Final Conference: European Biometrics Summit - goals and objectives - format, structure, content - pre-conference workshop introduction: Max Snijder
15.00 – 15.30	*Coffee/tea*
15.30 – 16.00	European Technology Platform (see appendix) Günter Schumacher
16.00 – 16.45	BEST Network after project end: the setting up of a new European platform introduction: Max Snijder
16.45 – 17.00	Wrap up and closure Max Snijder / Alexander Nouak

Format of the WG discussions

Each Working Group will prepare a short introduction of 10 min. This is followed by an interactive discussion. Each WG has 45 minutes. Input from all the attendees is expected so opinions and visions from different angles and area's of expertise are being collected and recorded.

Focus area's are:

- Biometrics for passports and public administrations (WG1)
- Emerging technologies and applications: access control, T&A, video surveillance biometric payment (WG2)
- Biometrics for ABC and RT (WG3)
- Biometrics and eID/eServices (WG4)
- Training & Education (WG5)
- Testing and evaluation (WG6)
- Ethics, legal and socio-technical aspects (WG7)

How to prepare for the workshop

It is advised to read the deliverables which have been finalized during the first period of the project.

Appendices:

- *Amended table of deliverbales and project schedule*
- *Minutes Conference Call Chairs/Co-chairs d.d. 2nd September 2011*
- *Discussion Paper European Technology Platform by Günter Schumacher (EC JRC)*

*** Link to Eurosmart White Paper "**Smart Biometrics for Trust and Convenience":**
http://www.eurosmart.com/images/doc/Papers/eurosmart_whitepaper_biometrics_final.pdf

10.2. Annex 2 – Minutes Conference Call September 2nd, 2011

BEST NETWORK
Biometric European Stakeholders Network

Minutes Conference Call 2 September 2001

Present:
Siliva Venier (WG7), Herbert Leitold (WG4), Farzin Deravi (WG5), Michael Peirce (WG6), Julliet Lodge (WG7), Bernadette Dorizzi (WG2), Olivier Epinette (WG2), Alexander Nouak (WG6), Paul de Hert (WG7), Günter SChumacher (WG1+3), Max Snijder (WG1)

1. Update on EC affaires and Fraunhofer coordination

- Project restart en end date
  Re-start date is September 1st as confirmed by the European Comission. Formalities are being finalized. Because the project is funded lumps sum we can start activities as planned by the Recovery Plan (see annex).
- Funding
  The remaining funding is 40%. Alexander will get confirmation from the commission.
- IMPORTANT: a pressing email will be send out to all the partners in order to make clear that everybody is expected to attend as the focus of the network is now shifted to the meetings itself and the associated discussions. All the new dates have been communicated several months ago. ***EVERYBODY HAS TO BE PRESENT!***

2. Workshop agenda

- Structrue
  Draft Agenda vs0 2 was discussed. It was concluded that in princple all sessions will be pleneray. Each WG will prepare a discussion document (max. 1 A4) that will be used as input for the discussions. These need to be send to Max before Friday September 7th so it can be included in the workshop materials. Max will set up an amended schedule.
  Each WG will do a short introductionary presentation on the proposed topics and scope of the discussion, after which the network partners will start commenting and discussing.
  A separate session for each WG should discuss the content and structure of each final deliverable.
- Eurosmart has prepared a discussion document on the use of biometrics and smartcards. This will be included in the agenda of the workshop as a separate item as potential subject for a Best Practice Guidelines discussion.
- tools to 'record' the results of the workshop
  There will be three means of recording the results of the workshop:
  1. taping the full proceedings
  2. report of the literaly text (paraphrased based on the tape)
  3. contextual report containing main issues, conclusions, next steps and actions
- External participants

It was decided that the September workshop will be BEST internal only. The results of this workshop will be used as input for the November workshop, to which external participants will be invited.

- A separate slot will be included to discus/evaluate the next ICT-call

3. Special invitees to the workshop

There will be no external invitations for the September workshop, apart from Frontex. Max will contact them to see whether a representative of Frontex can be present.

4. Final Conference

1. Dates are okay
2. Title(1st) European Biometrics Summit (other suggestion still welcome)
3. Program outline: to be decide

It could be considered to organize a pre-conference workshop (Feb 15th 2012) on biometrics for passports and public administration (+ABC?). Cooperation with Keesing Journal could be sought (media partner?). It should be avoided that the whole three days will be too exhaustive.

Max will start preparing the communication for the final conference (separate website?).

5. Setting up new European biometrics platform

All participants to this conference call supported the setting up of a new Eureopan platform for biometrics, taking BEST Network as the starting point. The Final Conference should be used to present the new organization.

The chairs and c-chairs will send a brief collection of ideas and suggestions for the new European biometrics platform to Max, who will prepare a short introductionary presentation for the discussion at the workshop. The ideas should contain suggestions on the mission, goals, objectives, activities and maybe even some ideas on the organizational structure.

ACTIONS:

EVERYBODY coordinate	-	preparing discussion document for each WG (chairs and co-chairs to within WG)
		Input on the new European biometrics platform to be sent to Max
MAX	-	send email to all partners regarding workshop and new EU platform
		Invite Frontex
		Disseminate Günter's ETP document
		Preparing new agenda
		Preparing short introduction on new European platform based on input from partners
		Start preparing thee communication on the final conference
MAX/PAUL/JULLIET/GÜNTER		prepare ideas for preconference workshop

ANNEX: amended table of deliverables and new project schedule

10.3. Annex 3 - WG7 comments on D3.1 and Frontex ABC Best Practice Guidelines

Input on Privacy and Data Protection aspects

of European ABC Systems based on E-Passports

in particular for WG6: Testing and Certification of the BEST Network. Paragraph 6: Perspectives/Recommendations/Issues on Privacy and Data Protection

by Paul de Hert and Els Kindt – 30.3.2011

1. General

First of all, it is necessary to point out that there has been very little consideration of any privacy and data protection issues in the BEST Network Deliverable D3.1 and the Frontex Best Practice Guidelines on ABC systems as starting point documents. In one document, reasons have been given ('lack of expertise and time' – Frontex), the other devotes half a page (of 17) to some limited data protection considerations (mainly about transparency) and remains very general and incomplete. The lack of focus on privacy and data protection aspects which are of major importance as these systems involve the processing of (sometimes sensitive) personal data of citizens raises serious concern. Data protection considerations have thus possibly not been as incorporated as other considerations. ABCs and e-passports present, of themselves, a range of data protection concerns both as to their own security and as to their potential social impact. These issues are part of a wider series of debates regarding the security imperative, automation of security networks, government surveillance, legitimacy of collection of biometric data etc. These discussions and concerns must be considered as a background in the development or analysis of any certification or testing. The FRONTEX document states 'the primary goal of ABC systems MUST be facilitation without disregarding security. Facilitation is thus the main objective to maximize, and security a boundary condition that has to be met'. Data protection and privacy considerations are the rights predominantly harmed by encroaching security and as such should be accorded due consideration.
Since it is impossible to cure this default in a short contribution as requested, we hereunder make general remarks and evocate some issues which need further follow up and elaboration in due course.

2. Need for clear and detailed description of data collection and use

First of all, it would be necessary for the envisaged ABC and the RT systems to describe in detail and to clarify what data collection and processing activities are taking place in combination with an explanation which external processing acts are made and by whom as required in practise. This is essential for a privacy and data protection analysis aims, but is lacking.
Similar, for the testing and certification, it is necessary to elaborate in clear terms what is to be certified and tested. Only with a greater degree of clarity and certainty on the processes of the personal data involved is it possible to clarify the data protection and privacy issues involved.

In general, all testing and certification requiring the processing of personal data (with the exception of data already anonymised or not identifying an individual as defined in data protection legislation) shall follow the principles of Directive 95/46 (laid out in article 6) and national applicable supporting legislation. The privacy rights of the individual must also be borne in mind as laid out in article 7 of the Charter of Fundamental Rights of the European Union and article 8 of the European Convention on Human Rights. Pure privacy concerns may not be so relevant here, but should be taken into account with the development of any more invasive systems (e.g., extensive profiling or data mining activities, …).
Another aspect is the aim of the testing and certification. Is it aimed at (only) testing and confirming particular functionalities/data flows/assertions made (e.g., that particular data are compared locally and after comparison deleted from particular components), or aimed at a broader goal of attesting overall or particular data protection compliance of (particular components of) the system ? Certification of the latter may be very ambitious, but an ever increasing demand as it is believed that this may enhance compliance, transparency and accountability for systems.1

3. Specific comments

a .Legal obligations for each of the specific data processing operations. Each data processing operation potentially engages the legal framework in a different and potentially unique way. The following factors may influence the specifics of engagement and the legal obligations: specific ABC design, the location of the ABC operations and the data (collection) and the national legislative issues its operation touches on, the purpose of the operation, to whom the data is distributed and who the data controller is, what data is being collected and distributed and accessed, which external/other systems are involved in processes and how they interact with these processes, etc…. The principles of the framework must thus be applied to each processing operation with the specifics of the above issues in mind.

b. Different national data protection legislations will apply and international personal data transfer issues The data protection framework is transposed differently in various countries and under certain circumstances this can lead to different engagement in different states. The potential for this must be considered as well as the difference across states in the interplay of the data protection framework and relevant local non-harmonised legislation. The data protection framework may also overlap or interact with other relevant European or international legislation. Legal boundaries and interaction should be clarified

c. Determining the controllers, the processors and the receivers. When data must be shared out or dispersed among systems or operators, designations such as controller and processor and the consequent responsibilities should be considered and determined beforehand, otherwise this risks of getting lost amongst the dispersion.

[1] Various Data Protection Authorities and the European Data Protection Supervisor ('EDPS') have stressed the opportunities that certification may offer See also European Commission, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union*, 4.11.2010, COM(2010) 609 final, pp. 12-13, available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf and the reply of the EDPS in his opinion of 14 January 2011.

d. Need to define specific purposes, re-use of data and need for a legal basis. Data may be collected toward different aims, for instance toward improving the operational effectiveness of the system, toward statistics collection or toward developing the business model. Following this, data may be transferred to different types of bodies. The legality and the legitimacy and justification of each entity's collection and processing of data and every re-use of data (in particular of additional data collections) must be carefully considered. Data collection, distribution and storage processes must be tailored with the status of likely recipients and future use in mind.
e. Data minimisation. The collection of data necessary for each operation should be kept to the minimum necessary for that operation and data should be stored only for as long as necessary. If possible, data should be anonymised (for example in statistics collection) and the possibility of 'anonymising' biometric data must be considered. Additional privacy enhancing technologies should be considered as well, as in order to make 'biometric identities' revocable, irreversible and unlinkable (with other applications to the extent feasible/desired).2 The difference between different types of biometric data must also be considered. Different types of biometric data may contain different information about the individual and alone or in combination with other categories of data this may demand their consideration under the more strenuous considerations required by article 8 (processing of special categories of data).

f. Information, transparency and rights to the data subjects. Where possible and required, it must from a legal point of view be made clear to the data subject how and why the data is being processed although, due to clear legal and practical reasons there are limits to this. This has been recommended in the FRONTEX best practises and should be defined more precisely in according with applicable data protection requirements as information and transparency are general legal rights of the data subjects.

g. Use and interaction with other data collections. In testing and certification, the interaction of ABC mechanisms with other external databases must be carefully reviewed and safeguarded. There must be particular attention when considering interoperable systems in which data may be dispersed across networks. Where data is captured and re-used, it must be considered, (beside the legal issues of e.g., re-use, profiling, transfer of data, consent, timely deletion,…) where this data will be stored, authorizations for accessing the data, and whether it will be stored with or will be easily accessible alongside other data or data sets which together may constitute a breach of the principles of the framework. It must be borne in mind that the ABC system will work in tandem with systems which themselves raise considerable data protection issues and this must be borne in mind when considering testing and certification.

h. Use of 'best available technologies' and privacy by design. ABCs and RT systems (which should properly be distinguished) operate differently depending on design and incorporate novel technologies. Thought should be given to the use of 'best available technologies', for example to restrict access or to minimize data collection (see also below) and to Privacy by Design of the systems. The specific qualities of the systems must be considered when considering the privacy

[2] About the importance of these aspects of biometric identities, see EDPS, *Opinion 1.02.2011 on a research project funded by the European Union under the 7th Framework Programme (FP 7) for Research and Technology Development (Turbine (TrUsted Revocable Biometric IdeNtitiEs),* also available at http://www.edps.europa.eu/EDPSWEB/edps/cache/off/Consultation/OpinionsC/OC2011

and data protection in testing and certification. The practicality of their setup and background layout may also be important although are probably not key concerns.
Paul de Hert (paul.de.hert@uvt.nl) & Els Kindt (els.kindt@law.kuleuven.be)

10.4. Annex 4 - JRC ETP Proposal

Discussion Paper

Establishing a European Technology Platform on Next Generation Biometrics

(Version 1.0, 07.04.2011)

Abstract

This discussion paper summarises considerations about the motivation and modalities to establish a European Technology Platform (ETP) in the area of biometrics. The paper explains why biometrics satisfies the current criteria for an ETP and why previous initiatives for this sector all fell short in relation to the real societal importance of biometrics.

Introduction

ETPs have been introduced with the start of the 7th Framework Programme[3] as a new instrument to structure and support European level R&D and to create sector specific public-private partnerships (PPP). In essence, ETPs shall be *"mechanisms to bring together all interested stakeholders to develop a long-term vision, create a coherent, dynamic strategy to achieve that vision, and steer its implementation."*[4] The so-called Strategic Research Agenda (SRA) shall form *"a crucial part of the strategy to optimise the contribution of research to the process. Technology platforms should also address both the technical and non-technical barriers to and requirements for the optimal development, deployment and use of technologies, such as regulations, standards, financial aspects, social acceptance, skills and training needs, etc., while taking into account the relevant Community policies."*[5]

[3] Decision No 1982/2006/EC of the European Parliament and of the Council of 18 December 2006 concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-2013)

[4] Investing in Research: an Action Plan for Europe, Communication from the Commission, COM (2003) 226

[5] ebit

The first steps to establish such ETPs in certain areas date back to 2003. Since then, a total of 36 ETPs have been created, with 5 of them even at the status of a so-called Joint Technology Initiative (JTI).

With up to some hundreds of organisations combined in an ETP, such an initiative is much more than a project. In fact, the aim is to reach the critical mass for tackling problems with wider impact on a large portion (if not all) of our society. Therefore, the selection process for becoming a recognised ETP with corresponding public support required the compliance with this and a number of other criteria[6]:

Response to Major European Challenges: An ETP shall be mission-oriented and address major European economic-environmental-technical-social challenges. They are not short-term, problem solving devices.

Strategic European Initiative: Platforms should be set up only when there is a well-defined, European strategic need for such an instrument, and European added value can be clearly justified.

Politically Highly Visible: To affect change across national, industrial, technological boundaries, Platforms must create strong political support and be highly visible at a European, even at a global level.

Industry Led: To be effective, Platforms must be driven by actors from the applications / problem end of the innovation process.

Well planned and executed: There must be a roadmap with a longer-term vision, a sound strategy for achieving this vision and a detailed action-plan for carrying out the necessary activities.

It is interesting to observe that among those areas selected, there is no ETP for ICT Security or even security in general. Given the fact that biometrics is still widely considered as being only “part” of ICT security or other security issues (like immigration control), any consideration about an ETP on biometrics must be seen a as being extremely temerarious.

However, this paper presents a number of arguments why biometrics satisfies all the mentioned criteria and why it well justifies an initiative of the order of an ETP. Moreover, it explains why previous initiatives for this sector all fell short in relation to its real and emerging societal importance.

The rise of biometrics

The political dimension of biometrics increased dramatically with the threat of terrorism, in particular since the 9/11 event. Driven by good experience gained in the area of law enforcement, biometrics was supposed to serve for better (i.e. stronger) identification of individuals in general as a mean to improve public security. Another important driver was the increasing level of immigration which made it necessary to create efficient measures for border control and for preventing fraud.

[6] European Research Advisory Board: Report on European Technology Platforms (January 2004)

Consequently, biometrics has become an integral part of new concepts to improve identification document security, in particular focussing on fingerprint identification and face recognition.

In parallel to its wider deployment, biometrics has become subject to severe concerns about the potential harm to the fundamental rights of privacy and data protection – a controversy still ongoing by 2011. But not only the privacy concerns hampered the smooth roll-out of the technology. Questions of scalability and interoperability soon raised further doubts about the feasibility of biometric based identity management (IDM) at large. These questions are still not fully answered, despite the impressive number of already registered biometric identifiers in numerous governmental IDM systems worldwide.

With increasing number of biometric tokens (passports, ID cards) rolled out, the question about its potential "dual use" for non-governmental applications is now on the agenda of many countries. Likewise, completely new and non-security related application scenarios are under research and development. This fact has furthermore contributed to a highly diversified picture of what is still summarised under the heading "biometrics". **There is almost no question about biometrics which could be answered without looking at its technical and non-technical context, neither about its technical capabilities, nor about its ethical implications.**

The industrial context

In accordance with the biometric diversity, the industrial situation looks similar. There is a broad span from very small companies focusing only on a specific biometric sensor system up to very large companies offering a variety of sensor systems and system integration.

Europe has acquired a high level of competencies in biometrics. The global market, however, is clearly US dominated for several reasons: Firstly, the political climate in the US fosters very much new biometric developments. Involved companies can rely on a large internal market with the US Army as one of the largest single customer in the world. Secondly, the well-known buy-out in IT industry favours again the US companies with their stronger capital base according to the first reason. Thirdly, the US industry has much stronger influence on standardisation in this field than European companies have.

On the other hand, the already started large scale public procurement in the context of biometric enhanced identification documents would offer excellent opportunities for European companies to gain significant shares. **Therefore, it seems to be a legitimate objective of European industry policy to support European biometrics industry in this global competition process.**

Support initiatives in the United States

The US support activities for biometrics are coordinated by the National Science and Technology Council's (NSTC) subcommittee on Biometrics and Identity Management[7]. Directly linked to the Executive Office of the President, it has the highest possible visibility and authoritative power. The

[7] http://www.biometrics.gov/

committee has developed since 2002 a comprehensive strategy for the usage of biometrics across all governmental departments and services. This strategy has also crystallised in an impressive number of R&D support programmes which, of course, benefits mainly US companies in the sector. This strategy also provides industry with a clear perspective on future markets in order to stimulate their own investments.

In addition, the US Army has created the Biometric Task Force (BTF) which has recently (2010) become the Biometric Identity Management Agency (BIMA)[8], a Field Operating Agency of the US Department of Defence (DoD). Its mission "is to lead DoD activities to program, integrate and synchronize biometrics technologies and capabilities and to operate and maintain the DoD authoritative biometrics database in support of the national Security Strategy".

It is remarkable that both initiatives are explicitly devoted and focussed to biometrics. Related areas like IDM systems are derived from this origin and not – as it is considered in Europe – the other way round. The total volume of governmental driven activities in the area of biometrics has to be estimated being in the billions rather than in the millions which exceeds by far comparable investments in Europe. **There is also no such dedicated initiative on biometrics ever established in Europe, despite the recognition as a "key technology".**

Existing support activities at European level

There have been a couple of important support measures in the past which were supposed to help Europe to find the most appropriate technical solutions for the most beneficial usage of biometrics. These measures were mainly based on an Action Plan[9] developed by the European Commission Directorate General for Information Society and Media (INFSO) in 2003. The Action Plan encompassed three pillars:

- Establishment of an authoritative technical body on biometrics
- Launching of a European Web Portal for biometrics
- Creation of a European network on testing and assessment of biometric technology

The following sections briefly describe the motivation behind and explain why the corresponding implementation measures turned out to be insufficient.

Establishment of an authoritative technical body on biometrics

The envisaged technical body was meant to advise European policy makers in issues related to the large scale deployment of biometric systems. This advice should include also the legal and ethical implications certain technical solutions would imply. In this way, the body – consisting of renowned experts in the field and organised as a EC experts group[10] – should have been a partner in the

[8] http://www.biometrics.dod.mil/

[9] See http://webapp.cnaemiliaromagna.it/biblioteca/files/20060313160321200603131458755320004_11_23_Tecnologie_biometrich7986.ppt

[10] See http://ec.europa.eu/transparency/regexpert/faq.cfm?aide=2 for more information on formal experts group

implementation process rather than a potential obstacle. However, the aspect of being "authoritative" has been seen sceptical by the anticipated target group, in particular as the time for its establishment fall in the period of acute public debate about the pros and cons of biometrics. "Critical advice" was seen as a potential risk for the envisaged roadmaps for the introduction of relevant systems. **The result is that no such expert board exists up to know and that unbiased and commonly shared advice is still missing.**

Launching of a European Web Portal for biometrics

The web portal was meant to serve as a platform for systematic exchange of information on pilots and other deployment relevant information rather than just another website for general biometric issues. The portal was actually created in 2005 by DG INFSO[11] and has been available under http://www.europeanbiometrics.info. It provided a restricted area in which Member States authorities could upload any type of experience documentation and share this with authorities in other countries. However, the response to this opportunity was very poor. Again, the particular public climate at the time of launching that portal could be blamed for its failure. Some Member States had delegated certain tasks in the implementation of biometric governmental system to the private sector which prevented governmental authorities in other countries to participate in the information sharing. The risk of leaking out any type of negative experience (in fact, the most interesting part of information) was considered too high. The website was shut down in 2008. **Consequently, each Member State has to gain experience through own pilots, except where such information is shared on the basis of bilateral agreements.**

Creation of a European network on testing and assessment of biometric technology

Although there exist a large number of relevant standards for the biometric technology and devices, there are still aspects not covered yet (e.g. security assessment). Moreover, the assessment of complex systems involving biometrics is still in its infancy. It was believed that at short and midterm perspective (i.e. the time frame of the most extensive introduction of biometrics at large) there will be no single organisation or (at least a suitable assessment framework) to cover all relevant aspects. Thus, the creation of a network of capable institutions was considered as a remedy.

Important preparatory work had been developed by the "BioTesting Europe" project[12], funded under the Preparatory Action for Security Research (PASR) in 2007. The project elaborated an inventory of existing activities and capabilities and developed an R&D roadmap to cover gaps. Unfortunately, at the end of the project, the overall research priorities in the area of security changed significantly with the beginning FP7. Biometrics was considered as just one aspect of the security supply chain. The already started procurement of biometric devices in the context of the large scale European IDM Systems emphasised the impression that biometrics "is done". To a large extent, only integration aspects and non-security applications became subject for further funding.

[11] The implementation has been awarded to UNISYS under the contract 2004/S 164-141520.

[12] http://www.biotestingeurope.eu/

On the other hand, the questions of proper evaluation remained unanswered and left to the existing market forces – mainly from outside Europe. It is still widely underestimated that biometrics deserves particular and focussed attention to cover all its implications. Existing attempts to cover it "top-down" as an integral part of something else (e.g. Common Criteria for general security systems) all fail for insufficient resources to address these implications sufficiently. **As a result, ad hoc methodologies are developed here and there to cover those gaps, however, dependent on the individual perspective of its developers. This is still far from being satisfying and an important obstacle for suppliers and customers to arrive at well-specified and well-deployed IDM systems.**

The BEST Network

As a kind of fusion of the above mentioned support measures, the BEST Network[13] has been created in 2009 as a project to bring together all relevant stakeholders in biometrics. Funded under the ICT Policy Support Programme[14], it combines a number of working groups on the most relevant issues of the presence and the near futures:

- Immigration and Border Control
- Emerging applications: access control, commercial services and surveillance
- European Registered Traveller programs
- Biometrics in eID and electronic transactions
- Training and Education
- Standards, Testing and Certification
- Ethical, Legal and Socio-technical aspects

The project is still ongoing but it is already foreseeable that its impact is likely to be limited as for its predecessors mentioned before. The owners of relevant pilot or even fully operational installations refuse to share their experience as the network is not considered "trustworthy" enough; the hot issues are not recognised as reopening the research agenda. **On the other hand, the discussions conducted in this network have revealed an improved understanding of this particular sector and the emerging issues ahead To some extent, the initiative to create an ETP on Next Generation Biometrics is a result of this network.**

Next generation biometrics

Despite the fact that the desire behind the mentioned support actions is still valid and not yet satisfied, it turned out during the started deployment of biometrics that the actual scope of existing open questions and problem is much wider than predicted round 2003. The massive usage of biometrics for authentication (rather than for identification in law enforcement) has created a security dimension which did not exist before in law enforcement. Also, data protection has not really been an issue for the historical roots of biometrics. **The most popular modalities fingerprint, face and iris – which are somehow "public" information – contradict fundamentally the basic**

[13] http://www.best-nw.eu/

[14] http://ec.europa.eu/information_society/activities/ict_psp/index_en.htm

concepts of security systems and constitute a factually unsolvable problem for data protection. Their fundamental deficiencies are:

Reproducibility: Whether stolen from someone else or simply changed to by-pass blacklists, the modalities fingerprint, face and iris will be increasingly subject to forgery. Because this front end of the security concept behind can never be fully protected it is likely only a matter of time until all methodologies to recover this situation have reached the limit. Either the modality in question will be dropped completely or replaced or complemented by an alternative modality without the ease of reproducibility.

Expected data breaches: With increasing number of systems deployed and with increasing number of enrolled persons, the likelihood of massive losses of registered biometric samples due to data breaches will increase. Similar to the availability of stolen credit card numbers over internet, fingerprints and other biometric identifiers will become available as well. However, unlike credit card numbers, the biometric identifiers have a much more universal usage, including governmental IDM systems.

Cooexistence of diverse biometric enhanced applications: Fingerprints used for the newly introduced European passports are considerably well-protected with cryptographic techniques inside the passport chip. However, the same fingerprint might be used for accessing leisure centres or other types of application with low level security profile. If the fingerprint gets lost in the context of one of those applications, it can be used as well in the high security application environment of a governmental IDM system. Again, only the adoption of additional security components could prevent such a situation. On the other hand, it is yet unknown to what extent such additional measures would harm the anticipated ease of use and efficiency.

Although these deficiencies have already led to significant research on “template protection”, “anti-spoofing”, and other protection techniques, it is likely that these measures will not be sufficient and research on alternative modalities (i.e. aspects inside the human body) has to be intensified.

This will be the point when this type of “first generation” biometric research will merge with research on the so-called Second Generation Biometrics, the latter concentrating on behavioural features of human beings. However, these behavioural aspects are usually obtained through the observation and measurements of information originating from inside the body. At this intersection of first and second generation biometrics, i.e. “below the skin”, things will become even more complicated and challenging than observed so far in this sector. On the other hand, the potential exploitation in terms of new products and services is still to be investigated. This is what will be referenced furthermore as **Next Generation Biometrics**.

The challenges ahead

What will be the particular challenges of Next Generation Biometrics? – What will be the differences to challenges already apparent? – The following list is tentative and subject to the further discussion on the biometric ETP:

How can the predicted obstacles in the further deployment of biometrics be moderated and a **smooth transition to Next Generation Biometrics** established? – This question requires technical, conceptual and legal considerations. If attacks to first generation biometrics solutions become too massive before suitable alternative techniques based on other modalities will be mature enough, intermediate solutions have to be found which are lawful, effective and secure.

Alternative modalities: Each alternative modality has to address (apart from the evidence of being "safer") the potential implications its usage might have.

Ageing effect of biometric identifiers: With an ageing human body, also the chosen biometric identifiers are subject to ageing. Though not even fully investigated for first generation biometrics, it would be as well important for next generation modalities to guarantee the longer term functionality of identification or verification.

Longer term impact of biometric mass deployment on ICT supported IDM: Everybody is aware of the risks when using the same login and password for a larger number of applications. If biometrics becomes a mass phenomenon, i.e. it would be used for many applications, the situation is merely the same as long as the same biometric identifier is used.

Systematic assessment of privacy and other ethical risks: The deeper biometrics will look into the human body, the more it might reveal sensitive information which is not directly linked to the purpose for which biometrics is used. How can this additional information be protected against abuse or any other unwanted disclosure? – New assessment and ethical audit techniques are necessary which have to be used already during the development of new methodologies.

This package of challenges requires a comprehensive multi-disciplinary and multi-stakeholder approach. As the envisaged timeframe for solving these challenges is in the 5-10 years range, a European Technology Platform is the most appropriate instrument to organise the necessary R&D and market preparation actions.

Dimensions to be considered for the ETP

The envisaged ETP has to be defined along a number of different dimensions which might be grouped as follows:

Mission: What is the scope, what are the limits of actions provided by the ETP? What should be the widest context in which the ETP operates?

Objectives: What are objectives of the ETP in terms of new products and services? What vision does the ETP develop regarding the future use of biometrics and its integration into various kinds of applications?

Structure: Shall the ETP – according to its mission – work as an independent organisation or should it be integrated into or merged with another ETP (see attached list)?

Operation: How is the operational business of the ETP organised? Should there be a executive office? What kind of organisations need to be involved? How will the operational business of the ETP be financed?

Tentative Timetable for the Consultation Process

What	When	Who
Informal circulation of Discussion Paper (Version 1)	**Early April 2011**	**JRC, EBF, CSSC, FhG, Sagem**
Invitation to Feasibility Workshop	**20 April 2011**	**JRC**
Feasibility Workshop	**Mid June 2011**	**All (see list attached)**
Revised Discussion Paper (Initial SRA)	**July 2011**	**All**
Wider consultation process, including Commission services	**August/September 2011**	**All**
Decision on ETP	**October 2011**	**All**
Kick-off ETP (in case of positive decision)	**November 2011**	**All + further invitees tbd**

Tentative list of organisations for the first consultation round

National initiatives
Italian Technology Platform on Biometrics (Italy)
Teletrust Working Group 6 (Germany)
Biometrics Working Group (U.K.)

European initiatives
European Biometrics Forum
BEST Network

Industry
Sagem (France)
Vision-Box (Portugal)
SECUNET (Germany)

Research
GET (France)
Fraunhofer-IGD (Germany)

European institutions
EC Joint Research Centre
EC DG INFSO (ICT Programme, ICT policy)
EC DG ENTR (SEC Programme)
EC DG RTD (Science in Society)
EC DG HOME (Passports, VIS)
EC BPAP (General EU policy)

CEN (Biometrics Focus Group)

Current list of existing ETPs15 (ICT Sector only)

ARTEMIS	**Advanced Research & Technology for EMbedded Intelligence and Systems**	**JTI**
ENIAC	**European Nanoelectronics Initiative Advisory Council**	**JTI**
ISI	**Integral Satcom Initiative**	
eMobility	**Mobile and Wireless Communications**	
NEM	**Networked and Electronic Media**	
NESSI	**Networked European Software and Services Initiative**	
EUROP	**European Robotics**	
EPoSS	**European Technology Platform on Smart Systems Integration**	
Photonics21	**European Technology Platform on Photonics**	

[15] http://cordis.europa.eu/technology-platforms/home_en.html

10.5. Annex 5 - IATA International Traveler Scheme RP 1701

Subject: **International Traveller Scheme**

Submitted by: **Lisa Angiolelli angiolellil@iata.org on behalf of Passenger Facilitation Working Group (PFWG)**

Background:

The International Traveler Scheme aims to bring registered travelers schemes together under one overall program. The purpose of an International Traveler Scheme is to expedite passenger movements of identified, pre-screened and assessed as low-risk passengers through all border controls, including immigration and customs. A registered traveler scheme is a program that allows travelers expedited passage through automated border control systems following successful background checks and the recording of biometric data.

Problem:

A number of countries world-wide have established, or are in the process of establishing national, bilateral and multilateral registered traveler schemes. Passengers applying to multiple states within the Scheme may not be accepted by all the states to which they have applied. The development of agreed criteria for the potential disqualification of participants including agreement on the eligibility and status of passengers will foster interoperability. Passengers should benefit from a standardized application process and an enhanced travel experience by gaining access to a range of registered traveler programs operated by participating states where access would be otherwise unavailable.

Proposed Action:

PSC to adopt RP 1701a as shown in ***Attachment A_B1***.

Recommended Practice 1701 l

INTERNATIONAL TRAVELER SCHEME

RECOMMEND that Governments work together to develop commonalities between national registered traveler schemes to facilitate joining these together within wider multilateral initiatives. Where Governments offer registered traveler schemes, airlines underpin Government promotional activities and the facilities offered by airport operators support these schemes.

1. INTRODUCTION

1.1 A number of countries world-wide have established, or are in the process of establishing national, bilateral and multilateral registered traveler schemes.

1.2 The concept of a registered traveler scheme is to provide pre-assessed low-risk travelers with expedited passage through border controls.

1.3 These schemes deploy an automated process to:

- Check that the passenger is in possession of a genuine, valid travel document or token
- Verify the passenger's biometric data against the travel document or token or a pre-existing biometric identifier supplied by the passenger during enrolment to ensure the travel document is presented by the rightful owner.
- Grant or deny admission according to pre-established specification.

2. SCOPE

2.1 Whilst each registered traveler scheme is unique, commonalities do exist; It is recommended that:

2.1.1 Operationally

- Registered traveler schemes may be separately developed and operated by a Government or jointly developed and operated between Government and Industry.
- Where a charge is levied, the scheme should offer travelers a more bespoke service, i.e., web-based application including forms and the ability to schedule interviews
- The scheme should facilitate an increased efficiency in traveler clearance times
- Procedurally and practically clear for travelers to understand and operate

2.1.2 Eligibility

- The scheme should be open to nationals from more than one country
- Age restrictions may apply
- Membership should to be time limited, invariably linked to the length of the travel document.
- Continued eligibility requires passing regular background checks.

2.1.3 Enrolment

- Enrolment is voluntary in all schemes
- All registered traveler schemes should collect biographic data and may request supplementary data
- Each scheme will capture a minimum of one biometric

2.1.4 Background checks

- Regular background checks are conducted against national databases
- These may include biometric data and criminality checks.

3. PURPOSE

The purpose of a Registered Traveler Scheme is to allow travelers expedited passage through automated border controls following successful background checks and the recording of biometric data.

Governments should benefit from initiating a registered traveler scheme by enhancing security of the border through the use of biometrics, reducing illegal immigration, allowing more effective deployment of resources towards potentially higher-risk travelers and being able to obtain additional advanced information on travelers. Governments may also benefit in that additional sources of information may be utilized that they would not normally have access to in the identification of low-risk travelers.

Airlines may indirectly benefit from the additional vetting of travelers within the scheme, which offers greater security on the identity of the traveler and their admissibility by border control authorities. Where schemes incorporate direct transit points, airlines should additionally benefit from on-time departures where a passenger is transiting an airport and is required to make a border crossing, leading to cost efficiencies and the provision of better customer service.

Airport operators should expect a reduction in queue length and times which will facilitate a more efficient use of space and a possible deferment of infrastructure requirements and costs.

The vision is to ultimately create an International Traveler scheme which will bring registered traveler schemes together under one overall initiative. An International Traveler Scheme should enhance a passenger's travel experience by granting them access to a range of registered traveler programs operated by participating countries where access would be otherwise unavailable. The Traveler should also benefit from a standardized application process, access to expedited automated border crossings and the creation of a more seamless journey.

The recommendations also seek to assist Governments and Industry in designing data requirements for the implementation of a registered traveler scheme which may facilitate multilateral agreements.

4. DEFINITIONS

For the purposes of this Recommended Practice, the following definitions apply;

4.1 Admission

The permission granted to a passenger to enter a State by the public authorities of that State in accordance with its national laws.

4.2 Automated Border Control (ABC)

An automated control system that authenticates travel documents and/or tokens and permits, or denies, admission to a traveler according to a pre-established specification.

The ABC may additionally verify the passengers' biometric data against the travel document and/or token or a pre-existing database containing biometric data. It may also register the entry or exit of the country.

4.3 Biometrics

Biometrics are any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include fingerprints, hand geometry, iris, retina, facial image, hand vein geometry, voice waves, DNA, and signatures.

4.4 International Traveler Scheme

An umbrella initiative that seeks to bring countries existing registered traveler schemes together.

4.5 Registered Traveler Scheme

A registered traveler scheme allows pre-assessed low-risk travelers expedited passage through automated border control system following successful background checks and the recording of biometric data.

4.6 Token

A personalized secure credential that permits the authorized traveler to gain admission via automated border controls, subject to passing background checks and, in some instances, producing a valid travel document.

4.7 Travel Document

A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel.

5. Data Fields

In an effort to facilitate multilateral agreements the following represents a composite list of the information Governments may request for the Registered Traveler Scheme application process. This list is not exhaustive.

Biographic Information

- Last, First and Middle names
- Gender
- Date of birth

Governments may additionally request;

- Surname or Academic title, prefix or suffix
- Maiden Name
- Alias
- Height
- Eye Color
- Town/State/Province of birth

Nationality and Citizenship

- Country of birth
- Country of Citizenship
- Immigration Status
- Nationality

Travel Document

- Travel Document type and number
- Expiry date
- Date of issue

Governments may additionally request;

- Government issuing the document
- Visa information
- Information on other travel documents

Contact Details

The following contact fields are primarily utilized to contact fee-paying applicants;

- Country of primary residence
- Address if different from primary residence
- Commencement date for current address
- Full current address details
- Previous address history where the above covers less than 5 years
- Mailing address if this differs from the current address
- Home, Business and Mobile Telephone Numbers
- Email Address
- Invoice Address
- Preferred language and method of communication whether email or mail

Employment

The following information may be requested to inform background checks;

- Employment status and commencement date
- Occupation
- Employer name, address and telephone number
- Additional employment history where the above covers less than 5 years

Travel History Governments may additionally request;

- Boarding Pass available at time of enrolment
- Average number of flights per year
- Travel history over a specified period

Criminality, Immigration and Customs Offences

Whilst the following information is not widely requested, it is utilized by Governments to inform background checks;

- Criminal conviction details
- Waiver of Inadmissibility details
- Customs offences
- Immigration offences

Membership and Payment Details

Those Governments operating fee-paying registered traveler schemes may seek to establish:

- Where Governments offer varying levels of membership, the type of membership the applicant requires
- Payment method and bank details

Terms and Conditions

- All Governments seek to ascertain that the applicant understands the terms and conditions of the scheme before proceeding.

10.6. Annex 6 - Eurosmart White Paper ("Smart Biometrics for Trust and Convenience")

EUROSMART

The Voice of the Smart Security Industry

White paper

Smart Biometrics for Trust and Convenience

December 2010

Disclaimer
Eurosmart has taken reasonable measures to ensure the quality of the information contained in this document. However, Eurosmart will not assume any legal liability or responsibility for the accuracy, reliability or completeness of any information contained herein or for any consequences of its use.

Index

Foreword by the Eurosmart Chairman

Our Industry has designed and developed biometric solutions for more than 10 years now. Our vision has been always that personal data and especially biometric references should be stored in a smart card.

We are now at the front of very new era with significant deployment in the eID market. And today the global privacy protection issue opens emerging opportunities in almost all Smart Security market segments.
Biometric solutions can positively contribute to reducing ID fraud or payment card skimming, reinforcing trust in electronic transactions, and improving the convenience of security solutions.

Our Biometrics Task Force has done an impressive job, gathering and formatting key expertise amongst our members and proposing many relevant use cases for the future. This White paper will become a reference document for any stakeholder or end user that wants to consider Biometric technologies.
All forms of biometrics are considered, even though some are more adapted to smart security and targeted applications. Today Eurosmart members have the capacity to industrialize the Biometric solutions described in this document, and together they have the willingness to support any interoperability definition that may be necessary.

As a natural consequence to this initiative, Eurosmart will demonstrate a host of applications at its Biometrics booth at Cartes'10!

Enjoy your reading!

Marc Bertin
EUROSMART Chairman

Introduction

The development of Biometrics is a result of political, economic and technological globalisation. The world is now a global place for trade, migrations, transfers and reliable exchanges of all kind of information and values, physically and / or remotely. This can give rise to new risks, problems, fraud, illegal traffic, identity theft or even terrorism. Biometrics is seen as the best solution for identification or authentication as it is directly linked to the person (whoever he /she is). Identity theft has been classified as the fastest growing white collar crime since the mid-1990s. For goods and documents that also need to be guaranteed as genuine or identified / authenticated, some technologies may be used that can be classified as biometrics for objects.

However there are privacy and ethical concerns that must be taken into account.

In the opinion of Eurosmart, “the Voice of the Smart Security Industry”, technology does not have an intrinsic value, either good or bad. Biometric technology must both provide security benefits and ensure respect for ethical concerns and protection of privacy. This objective will be easier to manage when biometrics is combined with smart card technology.

This paper aims to make recommendations on the use of biometrics for cases of identification and authentication of individuals and goods. It is aimed at governments and organizations that have a primary role and responsibility for implementation of electronic identities, with safeguarding of privacy and to secure themselves and their people against those who seek to do harm, travel illegally, or commit fraud.

This White paper is divided into four parts. Part 1 provides general information about biometrics and gives a tour of biometrics, i.e. a presentation of the different forms of biometrics.
In Part 2, the objective is to provide detailed and comprehensive information about biometric concepts and use.
Part 3 develops biometric use cases with a focus on the most promising markets and recommendations from the Smart Security Industry.
The appendix in Part 4 provides additional information on the documentation used for the White paper, as well as a glossary about Biometrics.

1. Information

1.1. The need for biometrics

Some thousands of years ago, Chinese pottery makers used to put their fingerprints on their products. Over a hundred years ago fingerprint analysis was introduced for criminal investigations. In the first case, the goal was to identify and authenticate the origin of the product (object), in the second case; the major concern was to identify criminals and offenders (people).

Biometrics is a characteristic of human morphology or behaviour. In the identification, or authentication process of an individual, the use of biometrics provides accuracy and eliminates many of the risks of fraud. However there may be some political, religious, public and private concerns when biometric techniques are used. Eurosmart recommends that biometrics should be used for electronic identity documents as it is certainly the most efficient technique, and also in respect of protection of privacy and other ethical concerns.

With the globalization of world trade, there is a huge flow of people and goods. In order to prevent piracy / terrorism, and counterfeiting as much as possible, there is a need to use reliable identification and authentication methods. The use of biometric techniques allows identification - for instance of one individual within a population - or authentication – that is to say verifying a claimed identity – as a result of the study of physical characteristics that vary from one individual to any other.

When we talk about biometrics, we can deal with the physical characteristics of people or objects that are used successfully, but also behavioural characteristics (for which we are more at the experimental stage).
Some are emergent like voice and smell. New technologies based on chaotic elements can be used for manufacturing what we can call the object biometrics.

In a dematerialized world the identification / authentication process is based on what you own (a key, a card …), what you know (PIN code, secret), who you are (biometric characteristics), or any combination of these. The confidence level is of course dependent on the number of methods that are used to authenticate and identify the individual. The use of one is less safe than the use of several of these methods. In general, it is better to use a combination of the "element owned and biometrics" type which gives a very high level of confidence. The use of known information can be subject to disclosure and indiscretion and is especially less reliable over time.

In this context, biometrics is emerging as essential in authentication and identification applications.

1.2. A tour of biometrics

Biometrics is a characterised result from the natural chaos that authenticates and identifies individuals. There are several forms of biometrics:

- Morphological / physiological biometrics:
  These biometric methods use a biological characteristic of the individual or object. For example, fingerprints, iris texture, shape of the face or hands, wood grain or even atomic minerals in the organization.

- Behavioural biometrics:
  These are the biometrics that measure a dynamic characteristic associated with an ability to reproduce a movement, a sound or even an electromagnetic resonance. For example, writing, handwritten signature, voice or a magnetic field of particles.

- Object biometrics:
  These are the biometric methods that reproduce a natural phenomenon for elements whose characteristics are chaotic and measurable, for example, surface states, the bubbles in the material, manufacturing defects. For instance, digital watermarking, surface aspects and

bubble tags are object biometrics.

Capturing a biometric sample is generally made by live capture but some biometric characteristics methods allow identifying from traces. For instance, we all leave fingerprint traces on objects, and a hair is a trace using DNA identification.

We shall continue this tour with a focus on the main biometric techniques used.

Fingerprints
Fingerprint recognition is based on the analysis of the ridge patterns on the tips of fingers. This biometric technique has been used for more than a century to identify criminals. The process was purely manual, carried out by experts. But this biometric technique was the first to be automated in order to enhance criminal investigation and create civilian records in countries where no population register existed. Each finger of an individual is different and it is different from the fingers of another individual. The sensors, systems and algorithms have been refined over many years giving this technique good accuracy and performance, cost effectiveness and led to the creation of huge databases. Sensors produce images of the ridges that are scanned for the search of structural features (called minutiae) such as bifurcations or terminations. The minutiae of one fingerprint can be matched against all other fingerprints.

Face
Facial recognition is based on the measurement of the positions of distinctive features of the face - including the upper outlines of the eye sockets, the areas surrounding the cheekbones, the sides of the mouth, and the location of the nose and eyes. The use of face recognition has been introduced for the electronic / biometric passport to the ICAO standard. As facial recognition works when images have a suitable quality, the ICAO has defined criteria that must be checked before accepting a facial image for recording. Accuracy is not considered as good as for fingerprints and the iris.

Iris
The iris is the coloured part of the eye that lies between the pupil and the white of the eye. It is made up of coloured tubes, each having a diameter less than the diameter of a hair. The data is so dense that individual details can only be distinguished when viewed through a microscope. The iris contains a biometric pattern. An individual's right eye is as different from his left eye as it is from the eye of another individual. The eyes of identical twins are different. The colour can vary throughout an individual's life but the pattern and the external radius do not.

Data acquisition is done by a camera. The image is filtered to remove background noise and reflection, the border of the iris is searched, and a mathematical transformation is then made. Accuracy is considered as very good.

Hand
Hand palm print recognition is similar to fingerprinting. It uses the same principles and techniques. Hand geometry is based on measuring the dimensions of fingers and the hand to generate descriptive templates. The sensing process is user friendly, which is the reason for its relatively widespread use in the areas of access control and time attendance monitoring.

Vein
Veins have also been recognised as a unique characteristic that can be applied as a biometric for verification. Veins are developed before birth and remain highly stable throughout life, even differing between twins. Vascular pattern recognition systems identify an individual by using the patterns of veins on their finger, or palm (although almost any body part with visible veins could be used). An infrared camera captures the vein pattern with a focus on the shape and location of the vein structure.

DNA
Deoxyribonucleic acid (DNA) may be the most accurate of all biometrics. DNA contains genetic identity information about an individual’s health as well as his identity. There are privacy concerns with the use of this biometric method and the process is inherently slow. So there is no real use of DNA other than for forensic applications

Multimodal biometrics
Above is a summary of the main methods of biological biometrics. Each of them has different accuracy characteristics, but it should be noted that it is more and more common to use multiple biometric techniques in systems (such as fingerprints combined with face).

Advantages of using multimodal biometrics are that overall accuracy is significantly improved and the system still works even if one of the biometric samples is damaged.

Object biometrics
Biometrics is fundamentally a characteristic of human morphology or behaviour. Physical processes can generate chaos elements that cannot be voluntarily reproduced. When tightly coupled with an object a chaos element can be interpreted with accuracy for the identification, or authentication of the object. This object, for instance a document, can then be preserved from the many risks of fraud. This characterised result from the natural chaos of objects or documents may be known as the object biometrics.

As an example, the type of natural 3 dimensional generated physical chaos known as a bubble tag is a natural and unique occurrence. Characteristics are complex and cannot be either reproduced or counterfeited. When the bubble tag is attached to an object or a document, that object or document becomes uniquely identifiable and authenticable as the one and only original.

1.3. Legal and societal aspects

Biometric systems can, by nature, invade privacy since they make it possible for authorities to track people in all their actions and travels. Privacy concerns can be real or imagined and a user's perception of the invasiveness of biometrics will impact on their acceptance of the system.

The right to privacy is the right to protect property against search and seizure and to control information about oneself, at all times. The Universal Declaration of Human Rights, in article 12 says that "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks* ". Privacy is a fundamental right that is recognised in many international instruments and regulations, for example, all European countries have enacted legislation safeguarding privacy and Directive 95/46/EC of the European Union (EU) focuses directly on protecting personal data. However, there is currently very little legislation in Europe which deals specifically with biometric technologies. Directive 95/46/EC is presently under revision to adapt the legal framework in Europe to the new context and the issues raised by the digital environment. Based on the results of the public consultation in 2010, the European Commission should present a revision in the first half of 2011.

Some very interesting papers have been published on biometrics and privacy by various organizations such as:

- The Irish Council for Bioethics,
- The BITE ('Biometric Identification Technology Ethics') project.

It is not the role of Eurosmart to introduce a new one, but it recommends either to set a task for the European Ethics Group set up by the European Commission, or to create an Ethics Committee specifically for the use of biometrics. This Ethics Committee should, in our opinion, be independent of course of any government and any industrial group. Eurosmart would be willing to answer any technological question that the group might like to ask.

In order to be constructive, Eurosmart has analyzed all its proposed use cases with regard to ethical criteria.

2. Education

2.1. Electronic Identity

The expected benefits of electronic Identity (eID) are many: reinforced security, more privacy protection, more and better services to citizens, global interoperability, cost effectiveness, etc.

Security can be seen as protection against terrorism acts, identity theft, criminal or fraudulent acts against private interests and/or public affairs.
Privacy is the ability to reassure people that their lives and personal affairs are out of undesirable public view, that they have control of the flow of their personal information, and that their individual actions cannot be tracked. Privacy is sometimes related to anonymity and can be seen as an aspect of security.
More and better services mean confidential access to electronic services and cyberspace. Besides, global interoperability is a nationwide and cross-border necessity.
All the benefits of electronic identity must be cost effective. This is actually possible, because electronic identity allows the implementation of automated processes.

The key functionalities of electronic identity are Identification, Authentication, and electronic Signature, very often referred as IAS. They allow the protection of people's data when a strong security level is deployed. In order to satisfy all the needs for security, privacy and interoperability, there is a requirement to define and adopt robust standards. Smart card technology associated to biometrics is the best answer. Digital identification and authentication, with or without an associated digital signature, where the biometrics feature ("I am") reinforces the PIN ("I know"), allows secure access control to personal data by appropriate individuals. Thus, the privacy issue is managed in a secure way and can be integrated into a complete interoperable system. The European Citizen Card (ECC) standard, as well as the ICAO standard for electronic passports are reliable fundamentals for eID.

2.2. Concepts and basics of biometrics

2.2.1. Basics of biometrics use

- **Identification**

Identifying somebody is obtaining his identity from his biometrics.

The identification system works from a collected biometric sample and compares it to all references stored in the database. The person may be known as present in the database, or not. In the first case, it is a "closed set" identification. In the second case (open set identification), the database is a watch list and then the system must determine whether the person is in the database and in case of yes provide the identity.
In terms of biometrics, it is a one-to-many matching process (1: N).

- **Authentication**

Authentication is the verification that an individual actually has the identity it claims to have. This verification process can be made by:

- Checking something the individual owns, like an Identity document with a photograph,
- Verifying something they know, a password, a PIN code, a secret,
- Verifying a biometric characteristic, such as a fingerprint (his).

The verification is said to be a 1, 2, 3 factor authentication, depending on the number of type checks made. In terms of biometrics, the authentication can be a one-to-one matching process (1:1). In this

case, a new biometrics sample is taken from the individual to be authenticated and compared to one of their previously registered biometrics sample. If it matches, the user is "authenticated".

- **Electronic Signature**

Like a hand written signature, the electronic signature is used for giving irrefutable evidence of the user's approval for an electronic contract or transaction. Electronic signatures are usually based on asymmetric cryptographic algorithms, such as the RSA algorithm. Their legal validity is governed by legislation in many countries and in Europe. Electronic signatures are also referred to as "digital signatures".

It is possible to generate strong cryptographic keys from biometrics. So, a new technology known as bio-cryptography has been developed, linking the electronic signature more firmly to the user. This then makes impossible the repudiation of an agreement or a transaction thus signed.

2.2.2. Biometrics qualification methods

Making the selection of a biometric method for identification/authentication must take full consideration of its appropriateness for the use case with regard to fundamental criteria.

Seven main criteria are generally taken into consideration when selecting a biometric method for an identification or authentication process.

- Universality: each individual or object must possess this characteristic;
- Uniqueness: the characteristic is different for each individual or object in the considered population;
- Permanence/immutability: the characteristic should be sufficiently invariable over time;
- Measurable / scalable: it can be acquired by technology that can quantify it;
- Performance: Accuracy and speed of the authentication or identification process;
- Human acceptance: General human feeling that makes people reluctant or cooperative with the use of biometric methods;
- Non circumvention: level of difficulty for hacking the system using biometric methods.

2.2.3. Biometrics use: flow process

- **Overview**

Biometric techniques are used for many reasons, but the flow process, despite some variants, always include some key steps.

- The enrolment process that captures biometric data processes it in order to transform it into reference templates that will be stored for future comparisons.
- The verification or identification process, based on a matching search. A correlation score is computed between the live template and any of the stored ones. Then, the score is compared to an application threshold to make a YES / NO decision (for example: granted /denied access).

The following figure illustrates the flow process. It is relevant to every kind of biometrics.

Fig. 1: The biometrics flow process (Global Platform source)

- **Enrolment**

The first step of the flow process of any biometric solution is the enrolment of the individual(s). The system captures biometric data, extracts unique features into a reference template and ties the reference template to the individual's identity.
The captured biometric may be recorded:

- in a large central database, such as a Automated Biometric Identification System (ABIS), that allows the performance of later operations of identification of one individual within a population or to ensure that there are no duplicated identity records and thus no identity fraud;
- In a secure individual device such as a smart card, for future 1:1 comparison (authentication).

The enrolment is the foundation of a reliable identity chain, thus some very important procedures must be observed:

- Location must be secure in order to prevent individual data theft or cloning and the operation must be performed by an authorized enrolment officer;

- The captured data must have the highest available quality. This will determine the accuracy and performance of the future matching operations. With regard to this, it is highly recommended that the operation be performed in a live and well checked process by a trusted officer.

Fig .2 Enrolment (Global Platform source)

With regards to identification solutions, the enrolment process is made either with individual's consent (civilian applications) or not (criminal investigation), live and checked, or from biometric traces.

Biometric life enrolment means capture biometric data direct from the person, for example, obtaining the facial photo or fingerprint. With this approach, the quality of the data is under control as well as the management of the biometric data. Life detection of persons could be the second key topic with this method.

- **Identification**

Biometric systems are used to identify an individual's biometric data against a large database or watch-list of individuals in a process known as a 1: n matching. The wording "Match on System" MOS) is also used. This approach is mainly used by governments for identifying their employees, as well for identifying citizens for social benefits, or for checking the uniqueness of identity document delivery.

Automated Biometric Identification system (ABIS) is both a generic word and it is also used when using multi-biometric techniques. Many systems are based on fingerprints. Such systems are named AFIS (Automated Fingerprint Identification System).

This identification process is also used for criminal investigations, from biometric tracking.

- **Authentication**

A biometric verification process includes the following steps:

  - Live data acquisition: the user presents the required biometric characteristic to the capture device, for instance a finger;
  - Live feature extraction: a unique template is extracted from the previously captured image; according to the selected biometric methodology;
  - Storage extraction: the reference template is retrieved from the secure storage memory. E.g. Smart card;
  - Matching: a correlation score is computed between the live template and the storage template;
  - Decision making: according to the score and the pre-defined policies and rules by the application, a YES / NO decision is done. Ex: granted / denied access.

The smart card technology allows performing the matching algorithm in the processor of the smart card. Then the operation is said to be "Match On Card" (MOC).

If the biometric templates are stored on a device that cannot perform the matching algorithm process, then this is a “Template On Card” case (TOC), and the templates must be transferred to a terminal / system that will carry out the matching. Depending on project type and size, this may cost less but offers a lower level of security.

- **Signature**

Digital signatures allow the user to apply an electronic stamp to a file. The file can then be sent to another person. As a result of the electronic stamp, the recipient can verify the authenticity of the file. Digital signature is part of a PKI (Public Key Infrastructure) system (infrastructure/framework that uses digital certificates as an authentication mechanism and is built to manage these certificates and their associated keys).

A PKI application (embedded on a smart card or on a PC) securely stores user’s credentials (digital certificates, keys etc.). In order to apply his signature, the user must be authenticated on the system by following the process described previously: The user is requested to enter his biometric identifier to the system and a matching is done.

Once he is authenticated, he can sign files or documents for secure data exchange. The electronic stamp contains information regarding the signatory (identity, organization...) and the signature (date, approval authority...). The recipient of the file can then verify the information (using the dedicated software) and validate the authenticity of the file.

The user's credentials can be generated from his biometric characteristics based on new technology called bio-cryptography. This reinforces the link between the user and his credentials.

2.2.4. Use of Biometrics with regard to security, privacy and ethics

Passwords and PINs can be forgotten, shared with others, or lost or stolen, which can compromise the integrity of a system. A biometric trait is part of an individual and as such it offers the best element of proof of identity (something you are). Consequently, biometric traits are thought to have a number of advantages over the above security measures: they cannot be lost or forgotten, they are difficult to copy, forge or share and they require the individual to be present at the time of identification.

The use of biometrics also makes it difficult for an individual to deny having accessed a physical location or a computer system, or having conducted a particular transaction. In fact, biometric traits are often portrayed as the ultimate form of identification or verification. They are used as a means of heightened security, efficiency and convenience and have been proposed as the solution to issues of identity theft and benefit fraud. Biometric systems are faster and more convenient to use, cheaper to implement and manage and more secure than traditional identification and verification methods.

Biometric data is more sensitive than private data. It must be used in a secure way. No unauthorized third party must be able to use it.

Automated Biometrics Identification Systems are key elements for security, but an uncontrolled or illegal use of them could infringe privacy. So a strict policy of use, procedures and security techniques must be put in place with such systems:

- Global examination by a Committee in charge of Civil liberties;
- Evaluation of the security mechanisms preventing hacking or illegal use of the systems;
- Audit of procedures :
  - Trusted officials and infrastructures to reassure individuals that the data cannot be compromised and information is not cloned;
  - Biometrics database is operated diligently and by competent official;
  - Use only in valid scenarios;
  - Biometrics systems may be certified by the data protection authorities of the Member States.

When biometrics is used with smart card technology, protection of privacy is easier to ensure.

- **Biometric Match on Card**

A smart card is a safe box of data. By storing biometrics on a smart card as opposed to a central database, there is less opportunity for compromising the biometrics data. In the case of a card if it were compromised, only the data of the card owner would be read. In case of system hacking, then the entire database could be compromised.

The biometric match on card can be used instead of or in addition to a PIN code check. The biometric template is not transferred outside of the card and cannot be caught by a hacker. When smart cards are used to store sensitive data such as medical or civil information, MOC authentication of the user is a far better method than PIN to unlock the card and read the information.

- **Matching off card with biometric or template images in the card**

ePassports store biometric images. The matching is not performed in the document, but on reliable biometrics terminals. These deployment models offer good security characteristics and accuracy, but require these terminals to be secured and attended. The model is successful as the number of checkpoints is relatively low and strict procedures are defined by the authorities which limits the risk of compromised inspection systems. As such, verification on the inspection system may be cost effective. This architecture, however, cannot be utilized in an open environment.

Other matching off card cases are made using chipless or memory cards that just store biometric templates. For instance, some welfare programs issue chipless cards with fingerprint templates registered with other data and encryption in a 2D bar code. The card reader decodes the 2D bar code and makes a match with the captured biometric sample.

- **Summary of matching processes**

Template on …. ➔ Match on … ↓	**Database**	**Card**	**Terminal**
System	ABIS AFIS Identification, forensic	Cards that can only store the template, but cannot process the matching algorithm (chipless or memory cards).	No sense
Card	No sense	The template never leaves the card	No sense
Terminal	In this case the terminal periodically receives a subset from the database (watchlist)	Cards that can only store the template, but cannot process the matching algorithm (chipless or memory cards)	Used when the expected individuals are known to be in a small database. For instance, physical access control.

Notwithstanding the fact that Eurosmart cannot be a starting point for statements on for biometric ethics, it has analyzed all its proposed use case with regards to ethical. The following table has arisen from our analysis.

Ethical criteria	Eurosmart technical questionnaire	Eurosmart recommendation to government, ID management and service providers
Role of the biometric application	Description use case per use case	Full and frank debate on the issues raised by all parties who will be involved in the proposed application, prior to establishment of the proposed programme
Transparency regarding use of biometric technology	Who has access to the biometric information at the different steps of the solution?	Describe in a public document the procedures that go with the technical measures
Relevance and necessity	*Environment*: does the nature of the workplace need a high degree of security? *Purpose*: is a biometric system required to achieve the intended purpose or could a less intrusive method be used? *Efficiency*: is the introduction of a biometric system needed to meet requirements. Which alternative, less intrusive methods have been unable to achieve them? *Reliability*: Which other methods have failed to work?	Answer in the same questionnaire.
Use of only required information to achieve a clear, limited and specified purpose.	How is this technically managed?	Appropriate information and access management procedures should be established.
Are system operators and system providers properly trained with regard to their obligations to respect and protect the information?	Description of security objective measures and control that allow the system operator to define procedures that meet the target?	Appropriate information and access management procedures should be established.
Can system operators and system providers access information other than that only required to carry out their job?	Description of security objective measures and control that allow the system operator to define procedures that meet the target?	Appropriate information and access management procedures should be established.
Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately?	Description of security objective measures and control that allow the system operator to define procedures that meet the target?	Appropriate information and access management procedures should be established.
Can the user make the decision whether or not to participate in the programme?		An individual should be fully and accurately informed and should understand all the issues and implications relating to the provision of his/her information.
What are the practical measures that ensure the integrity of an individual's personal and information privacy?	Description of technical measures.	General description and guarantee to be described in an easy to find and understand document.
The biometric data should be classified as sensitive personal information and as such afforded greater protection.	Description of technical measures.	Data protection legislation should be reviewed in order to deal sufficiently with the privacy concerns presented by the use of biometrics.
Clear knowledge of vulnerabilities	Description of security	Describe in a public document the

and protection against them.	mechanisms, countermeasures and their control. Answers to these known vulnerabilities *Spoofing,* use of a fake biometric. *Replay attacks,* recording an image from a legitimate user and inserting it back into the system. *Substitution attacks* –overwriting a stored template and replacing it with his/her own template. *Tampering*- the verification process to achieve a hit for his/her own biometric. *Masquerade attacks* , by means of . *Trojan horse attacks* , for instance, in order to get a hit for his/her own biometric. *Overriding the yes/no response,* inserting a false hit response to bypass the biometric system.	procedures that go with the technical measures.
An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary,	Technical solution must allow the subsequent actions tyo be performed with appropriate security.	Procedures must allow the individual's rights to be satisfied. Moreover, when context allows it; if an individual no longer wishes to utilise the biometric application or the original purpose of the application has been achieved, then any biometric and other personal information about that person should be deleted from the system.

2.3. Interoperability

In the past use was made of biometric technology mainly for criminal investigations or specific applications of physical access control or access to social benefits. This is changing now. The world is opening up with cross border agreements in the EU and worldwide, the international need to fight terrorism and the increasing need to securely verify the identity of users of e-commerce services.

International organizations have defined the use of biometrics for border controls. The ICAO has endorsed facial and fingerprint recognition for the e-passport and the EU has introduced a technical specification accordingly. The ISO is hosting sub-committees (SCs) relevant to the biometrics industry.

2.3.1. European Organizations Requiring Conformity and Interoperability

As a result of the freedom of movement of European citizens to live and to work across the EU, many sectors require conformity and interoperability. Here is a non exhaustive list of sectors which will require conformity and interoperability:

- Border controls and criminal justice,
- Cross border transportation,
- (e-)Healthcare,
- e-Government,
- Banking,
- Sensitive industrial site protection, such as nuclear power facilities,
- Military installations.

2.3.2. Barriers to consensus

The various sectors have different priorities and different timescales for cross interoperability. In addition, local-only solutions tend to get favoured and implemented. They are sometimes based on some standards, but every sector will benefit from a cross border consensus and from coordinated projects.

2.3.3. Current projects and Relevant Existing Standards

Here are some very important projects and infrastructures regarding EU wide interoperability of biometric systems:

- Visa Information System (VIS),
- Schengen Information System II (SIS II)
- Bio Testing Europe
- BioDev
- EURODAC (Asylum Seeker Data Base)
- Biometric passports

In the case of forensic systems that have been deployed earlier, Member States have proprietary systems. The need for standardization is not so important.

2.3.4. International standards

ISO sub-committee 37 (SC37) was set up in 2002 to develop formal international biometric standards for harmonization of vocabulary, biometric technical interfaces, biometric data interface formats, profiles for biometric applications, testing and reporting and cross-jurisdictional and societal aspects.

Smart card technology is well defined by many standards that enable it to be the most secure and interoperable means of setting up biometric solutions. These standards are produced by sub-committee 17 (SC17) at ISO, but other organizations have also defined the BioAPI (Java Card Forum),

and the European Citizen Card (CEN).
The ICAO's work on ePassports has been set out by the Technical Advisory Group on Machine Readable Travel Documents (TAG – MRTD) in ICAO document No 9303.

A list of standards is attached in the appendix.

2.4. State of the art

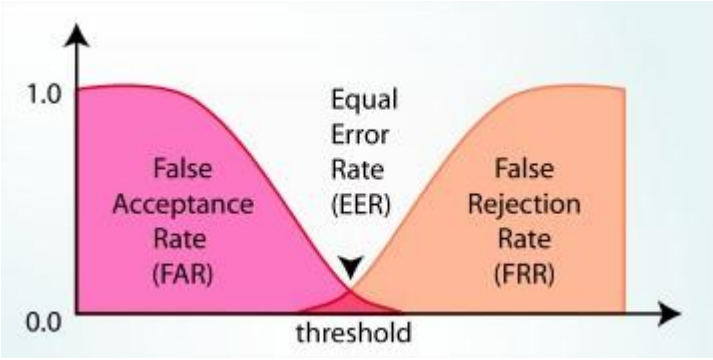
2.4.1. Performance: FAR, FRR and FTE

While it appears to simply give a yes or no answer, the biometric matching algorithm actually measures how similar a captured biometric data is to the stored reference. Biometrics uses score to express the similarity between a reference and a candidate biometric template. The higher the score, the higher the similarity between them.
Then it makes a decision according to a preset threshold as to whether the biometric sample comes from the same individual that provided the stored biometric template or not. That is to say, this process is statistical and although very accurate, it is not always exact. The security level is set by the threshold matching scores.

A false match is an erroneous conclusion by the biometric system that a reference template is from the same individual, when in fact, it is not. A False Acceptance Rate (FAR) or False Match Rate (FMR) is the statistical evaluation of false acceptances (wrong positive matches).

A false non-match is an erroneous conclusion by the biometric system that a reference template stored is not from the same individual, when in fact, it is. A False Rejection Rate (FRR) or False Non Match Rate (FNMR) is the statistical evaluation of false rejections (wrong no matches).

If we put together the curves of FAR and FRR, there is a point where both of them have the same value, it is called the Equal Error rate (EER). When setting the threshold value high, FAR reduces while FRR rises. When setting threshold score low, FAR rises whilst FRR reduces.



FAR and FRR are the main criteria for quality assessment of a biometric system. Their values are also related to the quality of the enrolment.

The failure to enrol rate (FTER) measures the probability that an individual will be unable to enrol in the biometric system. Failure to enrol may be due to:

- The biometric method that may not allow all individuals to permanently have distinctive enough biometric samples. For instance, the fingerprints of some manual workers are more often difficult to capture than for other people.
- The design of the system can make it difficult to get consistent biometric data.
- The quality of the enrolment system or the enrolment procedure. A commonly accepted rule

is that good quality enrolment must be live and well checked.

- A system design that makes it difficult to provide consistent biometric data. For instance, retina recognition systems needs to be very accurate, so is difficult to achieve in the enrolment process.

2.4.2. Comparison of techniques

The following table gives some figures for FTER, FAR an FRR for fingerprint, iris and face biometrics. These rates may vary depending on the quality of the enrolment, the sensors and the parameters selected for the system. For instance, in some cases a service provider might prefer to have more false acceptances and less false rejections, in other cases false acceptances are strictly prohibited.

	Fingerprint	Iris	Face	Face + Fingerprint
Failure to Enrol	0.1%	1-2%	0%	0,1%
False Acceptance Rate	0.01%	0.0001%	1%	1%
False Rejection Rate	0,5%	0,2%	2-10%	0,6%

The comparison of the techniques with regard to the qualification criteria of biometrics must be taken into account for the expected use case.

Biometry \ characteristics	universality	uniqueness	permanence / immutability	measurable	performance	acceptance[1]	resistance to circumvention
FACE	high	medium	medium	high	low	high	low
FINGERPRINT	high	high	high	high	high	medium	high
IRIS	high	high	high	medium	high	medium/low	high
VEIN PATTERN	medium/high	medium/high	medium/high	medium	medium	medium	unknown
HAND GEOMETRY	high	low/medium	medium	medium/high	medium	medium	medium
BUBBLE TAG	High	high	high	high	high	high	high
DNA	high	high	high	low	high	low	low
MULTIMODAL	High	high	high	high	high	high	high

2.5. Typical architectures for biometrics

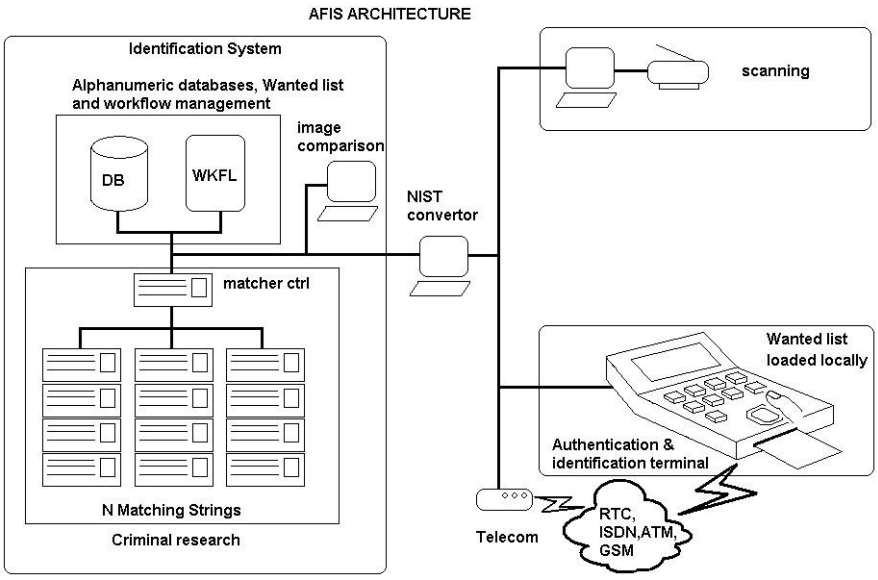
ABIS architecture (Match on System)

The architecture of such systems is independent from the biometric technique. The biometric identification is purely based on algorithms in which quality is determinant for the performance as regards accuracy and response time. In general three types of algorithms are involved:

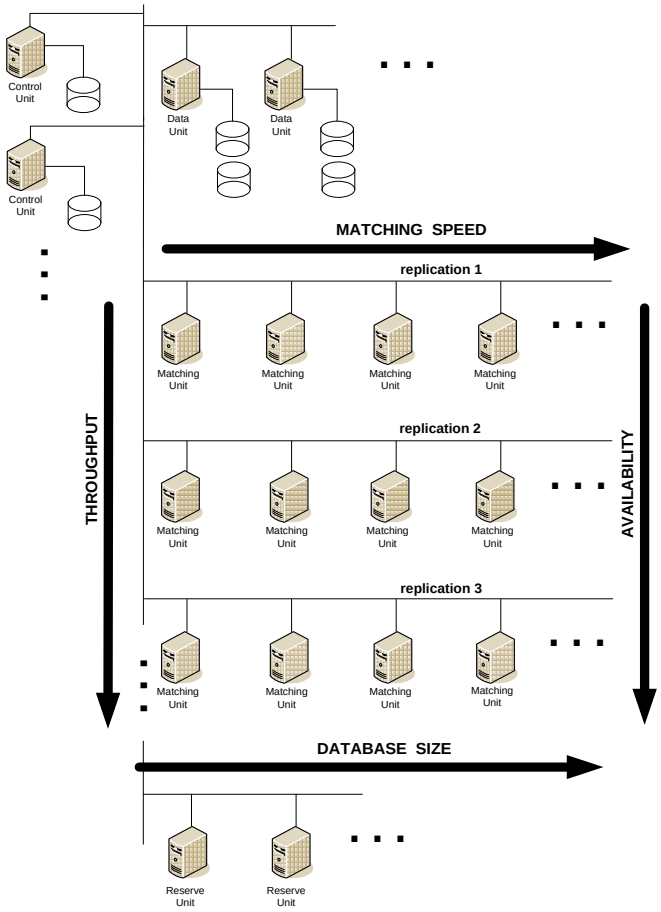
- Coding: These algorithms extract and encode information from the biometric samples, in order to prepare the next steps for high performance.
- Classification: Objective is to reduce the population of the database that will be considered for the matching process. The efficiency of these algorithms is key to the performance of a given hardware, or for the cost of the system at a given performance level.
- Matching: The aim of these algorithms, also named matchers, is to find the correct candidate for identification. For each reference they search for and evaluate the number of common minutiae and compute a score. Then the final decision will be either “no match”, “hit”, or

[1] Acceptance may vary depending on countries and culture

presentation of candidates to experts for visual inspection in the case of criminal investigations.



In order to achieve high performance when databases can be very large (millions, tens of millions, or hundreds of millions) and transaction requests numerous (tens of thousands per day), the architecture will then be based on clusters of Matching Units. This approach permits workload balancing flexibility and high reliability and availability of the system. Searches are then performed in parallel on sub-databases thus increasing the matching performance. When the search is completed on each sub-database, the results are consolidated to give the list of potential hits on the entire 1:N template database.



Match-on-Card Architecture

On-card comparison, or Match On Card (MOC) means that the biometric sample verification is performed in the card. The smart card must have sufficient processing power to perform the matching. The biometric system captures the biometric sample and extracts biometric data. The created biometric data is then uploaded to the card for verification. The verification process is executed on-card. If the biometric verification is successful the card's security state is updated and an appropriate signal sent to the back-end system.

Match On Card may be performed for fingerprint, face, iris, and almost certainly other techniques in the future.

The storage of the biometric templates in the card memory requires a few hundred bytes only for fingerprints and iris and a few kilobytes for face.

Match-on-Card fits with all available operating systems in the market such as Java, Multos, .NET and cards with proprietary Card OS´s.

Match-on-terminal architecture

Matching on Terminal may be made either by comparison of the captured biometric sample with a list of templates stored in the terminal memory (watch list) or by a 1:1 comparison with a template stored in a card.

Comparison to a watch list:

This watch list is downloaded and updated to the terminal by a system that owns a biometric database. This architecture is used, for instance, in some physical access controls where the terminals only get the biometric list of people who can access the protected area. In this case there is no need for employee badges.

Comparison by use of a token

The biometric template stored inside the card is then transferred to the terminal software for 1:1 comparison.

BioAPI

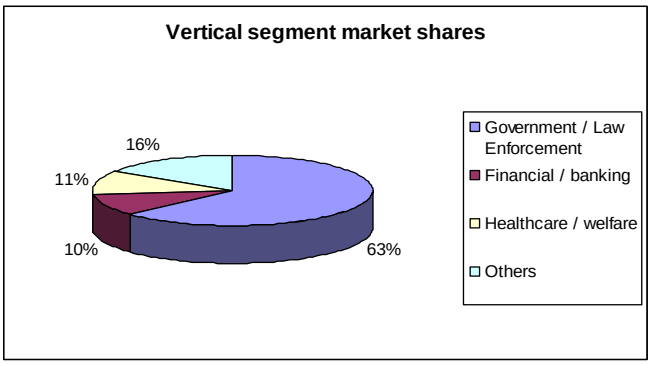
BioAPI (Biometric Application Programming Interface) is a key part of the International Standards that support systems that perform biometric enrolment and verification (or identification). It defines interfaces between modules that enable software from multiple vendors to be integrated together to provide a biometrics application within a system, or between one or more systems using a defined Biometric Interworking Protocol (BIP).

2.6. Market figures

These figures are extracted from an EMEA Biometrics market study carried out by Frost & Sullivan in July 2009.

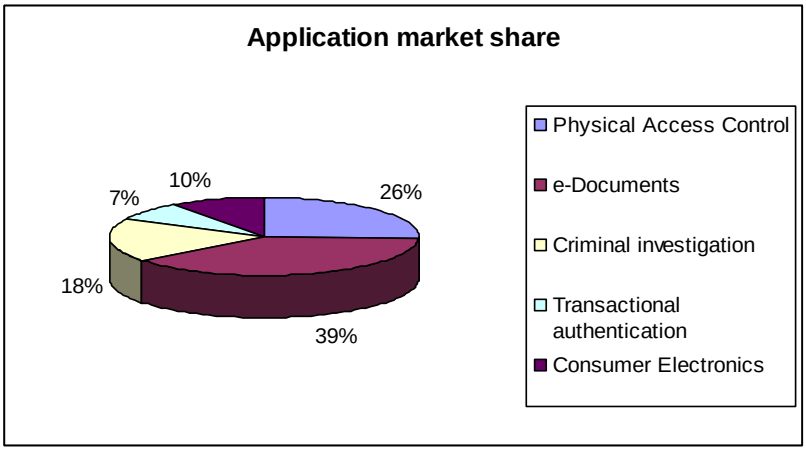
The Biometrics market in Europe is estimated at about 250 million Euros in Europe for the year 2010, with a 25% compound annual growth Rate (CAGR) from 2008 to 2015. The economic downturn in the commercial and financial segments should be counterbalanced by government projects.

Vertical markets are mainly:



- Government/Law Enforcement represents 2/3 of the market.
- Financial/Banking, at about 10%
- Healthcare, at about 10%
- Others at about 15%

Main applications are:



- Physical Access Control:
- e-Documents:
- Criminal Identification:
- Transactional Authentication
- Consumer electronics

In terms of techniques:

- Fingerprinting (non-AFIS) is the predominant biometric technology used for most applications. It is increasingly used in e-Documents like the Schengen visa and e-Passports and in consumer electronics.
- Facial recognition is linked to the adoption of biometric passports according to the International Civil Aviation Organisation (ICAO) mandate. The use of facial recognition with CCTV for security measures in the next three to five years is a potential growth area for this technique.
- Iris recognition is also likely to gain traction for airport security, registered travellers and access control in sensitive areas for airport staff.

Main market drivers are:

- Increased security concerns
- Government projects
- Use of biometrics in healthcare / welfare programs,
- Consumer electronics: Authentication of users accessing PCs, PDAs, smartphones,..

Main restraining factors are:

- Economic downturn,
- Privacy concerns and insufficient educational activity.
- Delays in government projects.

3. Biometrics use cases

Because it refers to intrinsic characteristics of the individual rather than to the ownership of an object or the knowledge of what is supposed to be a secret, biometrics has huge advantages for identification applications.

Some varied concrete case uses can be identified, enjoying the benefit of new possibilities introduced by biometrics:

- Identity verification is necessary in many cases. It can be citizenship identification at borders or on land by the police. It can also be the verification of the digital identity when accessing IT infrastructure or electronic services. Identity verification can be extended to some attributes other than first and last name and citizenship, in order to control the access to some benefits or rights.
- Strong and secure authentication purpose; to ensure that the identity claimed by an individual is really his or hers. This is a need for both face to face verification for citizenship or membership of a group and digital identity. Biometrics, contrary to PINs and passwords, is intrinsically linked to the individual and thus truly authenticates who the individual is.
- Digital signature, for the provision of a legally compliant irrefutable signature.
- Simplifying password management that is proven to be a weak and inconvenient authentication solution. A recent study revealed that French internet users have on average 12 accounts, that is to say even more passwords to remember and keep confidential. Human memory fails; some ailments prevent people using these properly; confidential preservation of these secrets is also difficult.
- Replacement of PIN code support, it is clear that PIN secrecy is very difficult to maintain. Environmental conditions and also technology available to hackers makes PIN theft easy.
- Product & document protection: Counterfeiting and forgery of documents and products is now so huge that new solutions must be put in place.
- Data protection that is adequate, relevant and not excessive.
- Civilian registration and criminal investigations: The use case has been developed for some time, but the market is still developing and technology provides enhancements.

3.1. Attempt at classification and listing of use cases

This list of use cases is not, of course, exhaustive.

Families of Use-Cases	Some concrete examples of use case
Identity Verification	Border controls
	Identity checks on land
	Secure chat for children
	Access to e-services
	Driver's license
	Tachograph card
	Physical Access Control
Strong & Secure Authentication	Secure e-mailing
	e-administration (tax declaration, call for tenders)
	e-banking
	e-health
	e-commerce
	Border controls
Digital Signature	Notary service
	e-banking
	e-administration (tax declaration, call for tenders)

	e-health
	e-mailing
Simplify Password Management	Mobile connections to e-services sites
	Application management
Replacement of Pin code Support whenever possible	Internet/Intranet web-service connection
	Internet/Intranet tools usage
	Banking/e-banking
	e-administration (tax declaration, call for tenders)
	e-commerce
Product and document protection	eID card for national
	eResident Permit for foreigners
	Documents, certificates
	Material goods
	Vehicle registration
Civilian registration & Criminal investigations	Identification

The following table provides another classification of the use cases:

Use cases	Identification	Authentication	Signature	Password simplification	PIN replacement	Product Document authenticity
Border controls	**X**	**X**				**X**
On land identity document verification						**X**
- eID card for nationals	**X**	**X**				**X**
- eResident Permit for foreigners	**X**	**X**				**X**
- Driving license checking	**X**	**X**				**X**
- Vehicle registration	**X**	**X**				**X**
- Tachograph card and data	**X**	**X**				**X**
Payment		**X**			**X**	
ID and non ID document or certificate checking						**X**
Material goods checking						**X**
Digital world						
Secure emailing	**X**	**X**	**X**			
Secure chat for children	**X**	**X**				
Age verification for purchases		**X**				
Access to e-services	**X**	**X**	**X**			
- e-administration (tax declaration, call for tenders)	**X**	**X**	**X**	**X**	**X**	
e-banking	**X**	**X**	**X**	**X**	**X**	

- e-health	**X**	**X**	**X**	**X**	**X**	
- e-commerce	**X**	**X**	**X**	**X**	**X**	
- e-billing	**X**	**X**		**X**	**X**	
- Notary service	**X**	**X**	**X**			
- On-line contract (for any of the above use cases)			**X**			
- Mobile connections to e-services sites	**X**	**X**		**X**		
Application management	**X**	**X**		**X**		
Internet/Intranet webservice connection	**X**	**X**		**X**	**X**	
Internet/Intranet tools usage	**X**	**X**		**X**	**X**	
Physical Access Control	**X**	**X**			**X**	

Below we give an informal description of the use case and provide further details for the most promising business use case

3.1.1. Civilian registration & Criminal investigation

It is often necessary to identify individuals after a crime, an accident or military action. Biometrics have been providing this type of identification for centuries. Biometric analysis can be used to identify both offenders and victims and this information can be stored on databases and used for later applications. The biometric methods used are mainly fingerprints extending to rolled fingerprints, palmprints, face, and DNA. Collection of biometric samples on crime scenes takes time of course, as well as the analysis process, and then the matching with the databases. The systems used are called ABIS (Automatic Biometric Information systems) and AFIS in the case of fingerprints.

AFIS and ABIS are used also for civilian registration and provide the assurance that a citizen is registered only once under a unique identity.

Civilian registration methods at national elections with biometric data have been made on a large scale, e.g. Bangladesh, Pakistan and the Republic of South Africa. India has started a new program of central registration in combination with fingerprint data and a UID system for 1.1 billion citizens (called UIDIA) and Brazil is also doing so for 270 Million citizens (called RIC).

3.1.2. Border Controls

In the travel and tourism sector, biometrics now plays a key role in identity management. The International Civil Aviation Organisation (ICAO) set international standards for the industry and has recommended facial recognition as the primary biometric with iris and fingerprint as backup (but not compulsory). Some countries are starting border control processing by the use of eGate systems. The systems acquire, for instance, a live image of an individual's face and use facial recognition technology to match the image with the digitised image stored in the individual's ePassport. If there is a successful match, the individual is cleared to proceed through the Customs control point. If there is not a successful match they would be referred to a Customs Official for processing in the traditional, manual way. Some eGates systems use fingerprint or iris instead of face, but the general processing is the same.

eTravel documents embed many security features that are used for checking that the document is not a faked one, and has not been forged. An additional level for guaranteeing the genuineness of the document can be done by the use of biometrics of object

3.1.3. On land Identity document verification

- **National eID cards**

These ID documents may often be used like an e-passport in some regions of the world. They are also used for accessing eServices. Resident Permits shall offer the same features as a National eID card. Thus, in Eurosmart's opinion the use of electronic e-passport technology is recommended for the use case of citizen identity verification with these cards.
In addition, checking the genuineness of the document against a biometric document image can be an additional security against counterfeiting or forgery.
Some countries have decided to include the match on card feature to these documents. This is the case, for instance, in Spain and Portugal.

- **Driving license**

Electronic driving license: Driving license document fraud is huge in many countries. Providing electronic documents that cannot be forged or counterfeited and that allow management of respect by the driver for the safety rules is a solution that can save lives. Introducing a biometric technique that

can be verified by police officers using mobile terminals with biometric ICAO checking or matching on card may well lead to a significant increase of road safety. In some countries, the driver's license has the statute of an identity document.

- **Tachograph card**

Tachograph systems record key data like driving time, speed. Respect for these by professional drivers is an important factor in guaranteeing the safety of passengers, drivers and other vehicles. This equipment uses a smart card that is general individual to a driver. Other smart cards are also distributed to authorized officials controlling the system. A level of secure authentication should be adopted equal to the one proposed for the driver's license.

- **Vehicle registration cards**

Current paper documents do not allow true authentication of the origin and history of the car (owners, accidents, periodical technical mandatory inspection results …). By preventing the possibility of shady dealing in cars, we can improve road safety. The Biometric use of document and chip technology would provide better security by ensuring the uniqueness and the integrity of the document. The solution can also be enhanced by linking object biometrics of the car to the card chip.

3.1.4. ID and non ID document checking

Even with more and more sophisticated security features in the e-ID and eTravel documents, it is not possible to conclude that powerful terrorist organizations cannot forge or counterfeit documents. The use of smart card technology combined with biometrics is the only means that can provide reliable identity verification.

Many other documents such as school certificates, proofs of ownership, issued by administration bodies, notaries, and even private institutions can have a high value. They are very often made of paper. Use of object biometrics can make forgery and counterfeiting of the document very difficult and their detection easy. The introduction of the owner's biometric characteristics would provide an even better level of security.

Authentication of objects solutions built around object biometrics can be applied in various sectors for victims of frauds such as forgery or counterfeiting:

- Identity Documents to: ID cards, Passports, Driving licenses, eResident permits …
- Secure access professional cards,
- Healthcare cards, Benefit cards, …
- Contracts,
- Property title
- Intellectual property

3.1.5. Material goods checking

In many cases it is important to be able to prove that a material good really has the claimed origin, and is not a counterfeited product. This can be for safety reasons, for instance maintenance parts for aircrafts, or IP protection for products that have required huge R&D efforts, Quality label protection.

Authentication solutions built around object biometrics can be applied to products in various sectors for victims of frauds such as forgery or counterfeiting:

The main interests of the use of the object biometrics as a seal applied to the logistics field are:

- Security of large packages (by price, know-how, confidentiality) in transportation and storage phases;
- Deterring and control of access to highly secure data (the fight against industrial espionage);
- Deterring and control of opening of the packaging.

Benefits:

- The biometric seal prevent consumers and distributors from any counterfeiting of products and brands;
- Beyond the authenticity guarantee, the Biometrics seal has a deterrent role on the opening of packages or systems;
- The biometric seal enables each package to be individually and formally identified and authenticated.

3.1.6. Payment

By using Match-on-Card fingerprint recognition as an alternative to PIN when verifying a purchase it is possible to avoid forgotten PINs and "shoulder surfing". Other advantages can also be achieved using secure distribution by enabling biometric activation of the card.

The technology fits perfectly with EMV architecture, as card holder verification is still performed inside the smart card. It offers a stronger link between the card and the card holder. The use of biometrics ties the card to one specific physical individual, removing the possibility of card usage transfer or delegation, and making the card truly personal.

3.1.7. Physical Access Control

Physical Access control can be achieved by a human (guard...), through a device which can be a mechanical key or an electronic device which uses a token such as a smart card. In order to access a restricted area, the user needs to have a sufficient access right defined in his device. But the loss of the device by the user can be a security breach in the system. If the badge is found by someone before being deactivated in the system, intruders may be able to access a restricted area.

As a result of biometrics the user needs to be at the access control point to present his biometric credential to obtain access. Users can no longer share their device. Moreover, nowadays most of the biometric techniques can differentiate between a live and dead biometric identifier avoiding the risk of identity theft. Biometric use brings the most advanced level of security to physical access control.

3.1.8. Digital world

- **Secure e-mailing**

Access to mails is one of the fundamental privacy rights that must be protected. Personal computers, and also personal storage space on servers can contain the people's entire correspondence over many years. Any attack on such a storage space may lead to serious harm.

As a secure alternative to traditional e-mailing it is possible, as a result of biometric technologies, to identify both the sender and the recipient. Usually, emails are not considered as a safe way of transmitting sensitive data. With biometric technologies associated to the secure environment of a smartcard, the e-mail is encrypted and sealed by the sender. The message can only be read by the authorized receiver who also must identify himself by fingerprint biometrics. With this solution, the authenticity and integrity of the e-mail, recipient and sender are ensured.

Another possible scenario is to drag emails to a special encrypted e-mail folder accessible only with the user's biometrics in order to avoid anyone reading the emails in his inbox. Documents and e-mails can only be opened by means of his fingerprint, face or voice.

- **Secure chatrooms for children**

The Internet can be both good and bad. Cases of paedophiles who have been able to meet children through internet chatrooms are too numerous. This must be prevented. A smart card that can deliver a status answer about a minority / majority age is a level of protection. But children do not really understand the idea of confidentiality and may disclose passwords and PINs unintentionally. A smart card with an age status delivery function protected by a match on card is a secure solution.

- **eID Verification/Age verification for purchase**

Some purchases are dependent on the age of the buyer (e.g. Alcohol). It may be necessary to first check the age of the buyer before delivering the requested purchase. For such a use, the identification does not deal with names, surnames, etc but focuses only on age in order to validate the order (off-line or on-line). The order is accepted when the Age Verification is in line with the rules associated with the purchase; it is refused when this is not the case. The same solutions as for secure chatrooms for children should be provided.

- **Access to e-services**

These services can be:

- Public e-services (Government to citizen, government to government, government to companies)
- Private e-services (business to business, business to citizen)

<u>e-administration</u>

We can assume that nobody likes to pay taxes for someone else, or that this is not a real loss. But making false declarations in lieu of the authorized individual or organization may cause losses, financial losses, consequential losses, and many legal problems for businesses.

Administration processes can be streamlined by using a digital signature. Administration employees can digitally sign electronic documents to validate forms and make requests from citizens or within the administration. Then the document can be legally sealed by the use of certified applications compliant with standards such as the "European citizen card".

On the other hand, citizens can validate their forms such as tax declaration through a digital signature online on e-government websites. Administration processes are then faster and more secure avoiding the risk of fraud based on paper documents' lack of security.

Biometric authentication or / and digital signature based on biometrics gives a higher level of security to the transaction as the signature is based on the presentation of a biometric characteristic of the signatoryr. Fraud, misuse and even corruption can then be reduced. Rejection of the transaction becomes impossible.

<u>e-banking</u>

Banks are familiar with risk management and use it to adapt the security of their system to the best compromise between ease of access their services, security costs and the risk of fraudulent use of e-banking services. But criminal organizations are looking more and more to attack e-banking with powerful IT resources and skilled people inside their organization. Access to e-services through a weak authentication mechanism is one of the preferred ways of hacking a system.

Nowadays, banks want to offer new services such as bank transfers, subscriptions to new services and, on line contract signing. Technologies are available to secure a signature and laws in most of the countries define frameworks for a legal and qualified signature.

With the biometric technologies associated to the secure environment of a smartcard for example, the customer or the sales representative can only sign a contract after identifying himself by his biometric identifier. With this solution, the authenticity and integrity of the signature is ensured

eHealth / eWelfare

For these application fields there is the need to both protect private data relative to the individual's health and ensure that the benefit of social insurance or welfare organization are actually provided to the right individual. The sums of money are important, the social impact is high.

Whether the reason is regulatory or financial, fraud reduction and security enhancement are the primary concerns for healthcare applications. Issues related to fraud are most commonly seen in countries and regions where healthcare insurance is widely used. Three of the main issues are:

- Phantom billing – a claim is submitted but no service is rendered and the patient is not physically present
- Coding errors – a claim that includes services that are not rendered or more services than those that were rendered.
- Card sharing and ID theft – uninsured individuals using another's valid identity

Utilizing biometrics and thereby binding transactions to an individual is a powerful tool to combat the abovementioned issues.

Using biometrics for welfare payments can efficiently fight against fraud. For instance, the payment of pensions in some countries where no real civilian registration or identity documents are available: Biometric use makes certain that the payment of pension has been made to the right individual.

A system that has to know and use an individual's unique social security number or an individual's medical history can be considered more invasive of privacy than other systems, including biometrics. Medical information can be stored in the tamper-proof environment of a smartcard which the holder can keep.
Granting access with the permission of the holder thanks to a Match on Card mechanism will certainly protect the confidentiality of this personal data... In order to reduce costs, electronic health records are currently being deployed in many countries. To ensure the authenticity of a prescription, the health professional can digitally sign the prescription using an electronic device such as a smart card. The digital seal is then integrated in the electronic prescription allowing pharmacists and other health professional easily to verify the authenticity of a prescription. Use of biometrics for digital signature avoids the risk of fraud with prescriptions by bringing a highly secure authentication method that prevents a shared use of a credential. In addition, access to health records on medical servers can be highly protected by biometric authentication.

e-commerce

e-commerce protection is similar to e-banking. The volume of e-commerce transactions is increasing. Hence the interest in hacking into systems is also increasing for criminal organizations acting on their own behalf or seeking to sell fraudulent access to e-commerce sites to individuals. The digital economy must also seek to prevent money-laundering.
Confidence is absolutely necessary for the development of e-commerce. Government authentication of a person's identity is the best means for instilling this confidence in both customer and service provider's minds. For a government, using a sovereign identity document and biometrics is the only certain solution.

e-billing

In almost every discussion about implementing e-billing, concerns about privacy and the protection of information quickly emerge as key issues. A company delivering invoices to its customers has the possibility to use biometric technologies in order to keep the related information confidential such as:
- Billing amounts,
- Bank accounts,
- Or the nature of the product or service bought

The chip implements some cryptographic algorithm protecting the data. The possibility of access to this sensitive information is given to the customer using biometric identification such as Match on Card fingerprint recognition.
There is no interest in stealing one invoice but attacking a server or bills website can be profitable for some hackers or some dishonest employees. Using biometrics, to sign or access this information, in such a situation, is the best way to avoid these threats.

Notary services

A document issued by a notary office may be falsified, counterfeited, and even be a fake. Use of such documents is not in general subject to strong verification. Applying object biometrics to the document is a safer mean of document direct authentication, with even the possibility proceeding to on-line supplementary checking.

On-line contract

Online contract signing is generally carried out in 2 steps. As long as the acceptance does not change the terms set out in the offer, the contract is concluded at the second step. In order to do so, those entering into the contract have to be sure that the data has not been altered by the other party or by a third party. Using biometric technologies makes certain that the contract content was created by the legitimate authority and has not been altered.
Only the two parties to a contract can access the contract as a result of a biometric authentication.

Mobile connections to e-services sites

This is a relatively new market. Some smartphones and new portable computers are embedding smart card technology and biometric sensors. This will allow local secure authentication and proof of it to the e-service site. MOC in the mobile/ Match on device.

3.2. Analysis of use cases

3.2.1. Border controls with biometric travel documents

Border controls	Biometric Travel Documents
Status	New World-Standard ICAO 9303; two regulations: US VISIT for 27 VISA WAIVER Countries (like Australia, Japan, and many EU-States), EU: 2252/2004 with deadlines in CY 2006 for 27 EU Member States. In CY 2010, 91 of 188 states worldwide issue travel documents with biometric facial or combined with biometric fingerprint data; border control equipment is only in place in 6 states (pilot scheme); Main applications are three-way-verification of the document holder and the possibility of automatic border control (ABC). Three way verifications means: - verification of document and MRZ - verification optical data set versus electronic data set - verification electronic biometric data set with document holder ABC allows the replacement of border police by an electronic gate. This gate can take over the three way verification as well as matching a data set to a wanted list. The following travel documents could be handled: a) MRP, b) RTP-tokens and c) National eID w/ biometric data, d) e-Residence Permit, e) e-Visa.
Benefits	- biometrics increases the security of the document - biometrics allows better linkage between holder and travel document - provides a profile of the traveller; identifies those on the “wanted list” ; a traveller profile captures data, such as name, given name, birthday, nationality, 10 fingerprint images, one facial image and other. - Automation of border controls
Security	Travel documents have 5 to 10 optical security elements; with an embedded microcontroller electronic HW and SW securities are captured.
Interoperability	- done thanks to a worldwide standard ICAO 9303-1, 9 global interoperability tests in the time window CY 2004 – CY 2009, organized by the ICAO (worldwide) and BIG (Europe) and conformity tests according ISO 10373-6. A test sequence on biometrics and interoperability was not done.
Privacy	Protection of electronic data by reading MRZ and hashing the value (ICAO-BAC security). Photo image as printed and fingerprint protected by access key in DG14 (BIG-EAC security).
ROI	Re-financing of production cost by increasing the fee per travel document. Automation might also reduce cost of border controls

Recommendations	a) Government recommendation: US regulation VISIT for all VWP-states, published in CY 2004. EU regulation 2252/2004 for all travel documents in EU from August 2006 onwards. b) EUROSMART's recommendation: New travel documents should be used at any SCHENGEN Border, to use the new security level and to protect against crime. Travel documents with biometric data have been issued for five years, but only three airports in Europe have it in use (some of them at the pilot stage), included biometric verification of the document holder.

Ethical criteria	**Eurosmart technical questionnaire**	**Eurosmart recommendation to government, ID management and service providers**
Role of the biometric application	Accurate verification of the traveller's identity, by an official or by means of automated inspection systems	EU and member states have discussed the subject and issued regulations and laws
Transparency regarding use of biometric technology	Enrolment: By a registration official Storage : in travel document Acquisition & matching by an authorized official or a closed system in a protected area	Describe the procedures in a public document
Relevance and necessity	This subject has been dealt with by official bodies in Europe and the Member States, and endorsed by ICAO.	
Use of only required information to achieve a clear, limited and specified purpose.	The only information linked to biometric is that required to obtain an accurate identity	Appropriate information available to travel document applicants and travellers should be easily accessible. Access management procedures should be established and made public. An individual should be fully and accurately informed and should understand all the issues and implications relating to the provision of his/her information. General description and guarantee to be described in an easy to find and understand document.
Are system operators and system providers properly trained with regard to their obligations to respect and protect the information?	Access to information can only be made by terminals linked to a key public infrastructure	
Can system operators and system providers access information other than that just required to carry out their function?	No information other than that needed to carry out the function is accessible.	
Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately?	The system does not record the information extracted from the travel document	
Can the user make the decision whether or not to participate in the programme?	Not if he wants to travel abroad.	
What are the practical measures to ensure the integrity of an individual's personal and information privacy?	The travel document stores raw images; but reading the chip information is protected by the BAC mechanism, and access to biometrics (finger/ iris) is protected by EAC protocol	
The biometric data should be classified as sensitive personal information and as such afforded greater protection.	The travel document information is protected by the BAC mechanism, and access to biometrics (finger/ iris) is protected by EAC protocol	

Clear knowledge of vulnerabilities and protection against them.	Identity verification is performed by an authorized official or by automated inspection terminals that are reliable, secure and attended.	Describe the procedures that go with the technical measures in a public document.
An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary,	?	

3.2.2. National eID card with biometrics

National eID-Card	National eID card for eGovernment Services ; biometric data for identification and/or authentication of the card holder
Status	12 States in Europe use National eID cards (Spain, Portugal, Monaco, Italy, Belgium, Austria, Netherlands, Lithuania, Estonia, Finland, Sweden, Serbia) 6 of them use biometrics for identification, 1 uses biometrics for verification (Portugal) ; Main purpose of replacing printed ID documents with electronic ID documents is to open up this document to e-government services as well to e-business services and to increase the security of the document. Alongside this application three elements are in use: identification (with a token), authentication (with a PIN or biometric verification) and optional electronic signature.
Benefits	Benefit for the user/citizens : - in the case of verification: more convenience for the user; - in the case of identification: more trust in secure documents for the police Benefit for the authorises: - user verification at the issuing procedure
Security	- in the case of verification: Match on Card - in the case of identification: protecton of the data set with access key; typically fingerprint images are stored in the 6 running national eID cards. To protect the images, the Police need the right to read the data. Typically specific access keys to this data are in use.
Interoperability	- in the case of verification: interoperability programs are not in use. - in the case of identification: test program is in progress under ICT LSP STORK; 17 EU member states participate in this; life test phase for cross border services has been running since July 2010. Biometrics is not part of these cross border interoperability tests.
Privacy	- in the case of verification: no re-building of fingerprint images; biometric data will never leave the secure token. - in the case of identification: only authorized persons, such as police have access to biometric data. In the case of using the ICAO framework, specific access conditions, such as ICAO-BAC are defined.
ROI	Refinancing by increasing the document fee. Example: new national eID card in Germany (nPA) costs 28,80€ compared with the current ID-card, at 8€. In the event of re-using part of the infrastructure for travel documents, such as the link to the population register, the bridge to trust center and the data capturing equipment, total cost for the infrastructure could be reduced dramatically.

Recommendations	a) Government's Recommendation: EU recommendation 14351/2005; this refers to ICAO 9303. b) EUROSMART's Recommendation: In the case of authentication: to maintain privacy as well as security, match-on-card would be the best approach. In the case of identification: the ICAO framework is well known and established.

Eurosmart recommendations for this use case are to use ICAO 9303 specifications for citizenship identity and another application for digital identity, the analysis with regard to ethics:

- is the same as for border controls, when the ICAO 9303 application is used,
- is given in the following table for digital identity with match on card.

Ethical criteria	**Eurosmart technical questionnaire**	**Eurosmart recommendation to government, ID management and service providers**
Role of the biometric application	Biometric application will replace PIN by matching on card	Full and frank debate on the issues raised by all parties: – Government, – Administrative service providers – Private service providers, – Citizens
Transparency regarding use of biometric technology	Enrolment: By a registry official Storage : in eID document Acquisition & matching by cardholder's terminal and PC	Describe the procedures that go with the technical measures in a public document
Relevance and necessity	*Environment*: On internet nobody knows who you are. Password / PIN easy to spoof. *Purpose*: Biometrics is the only technique that can authenticate who you are. *Efficiency*: No existing technique can replace biometrics *Reliability*: Pin and password theft Is an increasing white collar fraud.	A government policy on digital identity management should be defined, describing: – Identity theft dangers for the community, for the service providers and for citizens. – Along with identity management, use of biometrics should not be imposed, but given as a more convenient possibility when digital identities have to be relaible. MOC by itself has a privacy guarantee, but governments must provide evidence that there is no biometric database, or that their use is restricted to justified known use case, using defined procedures protecting privacy. General description and guarantee to be described in an easy to find and understand document.
Use of only required information to achieve a clear, limited and specified purpose.	MOC is the cardholder's clear consent to access his/her data	
Are system operators and system providers properly trained with regard to their obligations to respect and protect the information?	No need for system operators.	
Can system operators and system providers access information other than that required to carry out their function?	No need for system operators.	
Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately?	Use of MOC does not allow this possibility.	
Can the user make the decision	Use of MOC for accessing e-	Availability of MOC on the eID card

whether or not to participate in the programme?	services is always a voluntary act.	shall be an option decided by the citizen
What are the practical measures that ensure the integrity of an individual's personal and information privacy?	Templates and MOC are the best measures for ensuring both integrity and privacy of information	No specific concern as far as biometrics is concerned.
The biometric data must be classified as sensitive personal information and as such afforded greater protection.	Templates are never transmitted outside of the card.	Data protection legislation should be reviewed in order to deal sufficiently with the privacy concerns presented by the use of biometrics.
Clear knowledge of vulnerabilities and protection against them.	*Spoofing,* Less easy than with PIN / password *Replay attacks,* Less easy than with PIN / password. *Substitution attacks,* Not possible*. *Tampering* not possible*. *Masquerade attacks* not possible* *Overriding the yes/no response,* Not possible*. * within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum	Describe in a public document the procedures that go with the technical measures. Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum)
An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary,	Possibility to cancel a card and issue a new one.	Government must allow the individual's right to be satisfied at a cost corresponding to the legitimacy of the cardholder's claim.

3.2.3. eID document authenticity as a result of object biometrics

e-ID document authenticity	**e-ID document authenticity: guarantee of genuineness and uniqueness by linking chip and object biometrics(bubble tag for instance).**
Status	This use case has not yet been implemented, but some proof of the concept has already been developed. The interest of this prospective use case is to guarantee that the chip and the body of the document have been personalized together at the same time as a unique document. It also allows control of the document even if the chip is broken by means of a database transaction
Benefits	Benefits include : • Tying the medium to the chip • When the chip is broken, control is possible with a bubble tag through a central anonymous database • The chip and a bubble tag may moderate the number of security features • avoids the theft of rights and identity because of the impossibility of duplicating the document

Security	The chip can confirm the authenticity of the document body when it is challenged by presentation of the physical biometrics of the object sample. Reinforce the integrity check of the e-ID document: the right chip on the right medium with the right data. Allows control of the e-ID even if the chip is broken in an online transaction.
Interoperability	At the moment, no standards have been defined to use object biometrics in this way. A standard must be developed.
Privacy	Object biometrics actually protect privacy by accessing the data of the e-Id without the use of the human biometrics in a database transaction.
ROI	The bubble tag has an extra cost to integrate it, and increases the price of the smartcard reader, but it may reduce the cost of the document design by reducing the number of extra security features. The reading of object biometrics has an extra cost for the inspection terminal/system
Recommendations	Object biometrics is recommended to link the document with central anonymous databases and to ensure the link between the chip and the body of the card.

For this use case, we assume that any on card verification does not infringe civil privacy. This table focuses on on-line access to a central database, if any.

Ethical criteria	**Eurosmart technical questionnaire**	**Eurosmart recommendation to government, ID management and service providers**
Role of the biometric application	A bubble tag closely integrated with the document is linked to the smart card chip. Optionally, in the case of a broken chip a central database can provide document authentication and identity verification	In the case of a central database, full and frank debate on the issues raised by all parties who will be involved in the proposed application, prior to the establishment of the proposed programme
Transparency regarding use of biometric technology	Enrolment: Object biometrics created at document personalization Storage : in the document Acquisition & matching by an authorized officialr or a closed system in a protected area	Describe in a public document the procedures
Relevance and necessity	An attempt at fraud is breaking the chip of the document, or creating a new document using a chip that was personalized for another identity. *Environment*: The document requires a high degree of security *Purpose*: Make document forgery impossible , by establishing a unique link between document and chip. *Efficiency*: Today there is a multiplication of security features	Access to the database should be allowed in the only case of doubts over the document: Chip broken and security features difficult to verify.

	engraved on or affixed to the document. There are so many that they become difficult to check, except in laboratories. *Reliability*: Reliability is linked to human capacity	
Use of only required information to achieve a clear, limited and specified purpose.	The only information linked to the biometrics is that required to obtain an accurate identity	Appropriate information available to travel document applicants and travellers should be easily accessible. Access management procedures should be established and made public. An individual should be fully and accurately informed and should understand all the issues and implications relating to the provision of his/her information. General description and guarantee to be described in an easy to find and understand document. General description and guarantee to be described in an easy to find and understand document.
Are system operators and system providers properly trained with regard to their obligations to respect and protect the information?	Access to information can only be made by terminals linked to a public key infrastructure	
Can system operators and system providers access information other than that required to carry out their function?	No information other than that needed to carry out the function is accessible.	
Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately?	The only information linked to the biometrics is the one requested for getting an accurate identity (ICAO)	
Can the user make the decision whether or not to participate in the programme?	Not if he wants to travel abroad.	
What are the practical measures that ensure the integrity of an individual's personal and information privacy?	The record in the database can be encrypted by a key extracted from the bubble tag.	
The biometric data should be classified as sensitive personal information and as such afforded greater protection.	The record in the database can be encrypted by a key extracted from the bubble tag. The BAC protocol can also be used.	
Clear knowledge of vulnerabilities and protection against them.	Identity verification is performed by an authorized official or by automated inspection terminals that are reliable, secure and attended.	Describe the procedures that go with the technical measures in a public document.
An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary,	Technical solution must allow the subsequent actions to be performed with appropriate security.	Procedures must allow the individual's rights to be satisfied.

3.2.4. Physical / logical access control

Employee ID card for physical access control	**ID card for controlling access to restricted area, corporate or government facilities**
Status	Securing access to sensitive facilities has always been a concern. Video surveillance can give information after unauthorized access but security officers need to prevent unauthorized access. Access can be restricted to certain employee after authenticating themselves. Today some smart solutions are used such as badges based on smart card technology. Fingerprints are also used alone or linked to a database of authorized users. Combining employee ID card and biometrics offers a more convenient and reliable solution respecting the privacy of end-users. - Boeing employee card with fingerprint data (since 2007) - Case Use electronic Government Employee-eID cards with biometric data, e.g. US Department of Defence, US-Army and US-Coast Guard
Benefits	More secure for security officers as biometrics allows verification of the user instead of an object owned by the user. As the user cannot lose his biometric identifier, it is more secure than a PIN code for security officers and it provides more confidence and convenience for users. Other applications can be accessed through employee badges after a biometric authentication. For instance, e-purse for vending machines inside the building, access to the canteen…
Security	Use of biometrics enables strong authentication as the end-user needs to be present at the control point to present his biometric identifier. It reinforces the fight against fraud and unauthorized access as an employee card cannot be shared between employees and a lost card cannot be used on its own (i.e. without end-user presenting his biometrics).
Interoperability	Interoperability can be achieved using standards for biometric images and or templates (ANSI 378, ISO 19794-2, ISO 19794-4) and using standards for contactless protocols (ISO 14443).
Privacy	As a result of MoC, end-user's privacy is maintained by keeping the reference template in the proven secure environment of a smartcard. Storage of end-user's biometrics (On-Card or in databases) must be done with regard to ethics & privacy committee's recommendations for each country.
ROI	No more pin code/password loss. Cost saving for card re-issues. According to a cost/benefit analysis from US DoS, 200USD per user per year can be saved on password management by the use of biometrics.
Recommendations	Logical and physical access applications can be merged on a single dual employee ID card. Each solution must be adapted and/or customized to the needs of the different stakeholders: Military restricted area access control vs private company employees' access control.
Eurosmart Recommendations	Combination of an access badge with MoC and biometrics for two factor identification with respect for privacy. For highly sensitive areas, multimodal biometrics can be used with combination of fingerprint and iris for instance.

Employee ID card for logical access control	Digital ID for employees enabling logical access control to sensitive data and critical IT infrastructures
Status	Authentication on IT networks in companies or government agencies is mainly done through PIN code or passwords. But PIN codes and passwords are something the user knows and that he can give them to someone else or they can be retrieved against his will. As soon as someone has a password, he can be authenticated on the system with another identity until it has been deactivated by security officers. Combining employee ID card and biometrics offers a more convenient and reliable solution respecting privacy of end-users.
Benefits	More secure for security officers as biometrics allows verification of the user instead of an object owned by the user and/or a password he knows. As the user cannot lose his biometric identifier, it offers more security than a PIN code for security officers and it offers more confidence and convenience for users. Biometric can be used to cipher and sign electronic file/documents.
Security	Use of biometrics enables a strong authentication as the end-user needs to present both his employee card and his biometric identifier to be authenticated by the system. It reinforces the fight against fraud as the employee card cannot be shared between employees and a lost card cannot be used on its own (i.e. without end-user presenting his biometrics). Electronic corporate data can be encoded and protected when stored and/or sent in e-mails with biometrics ensuring their integrity. E-mails can be signed by an electronic stamp ensuring authenticity of electronic communications inside the company/government agency.
Interoperability	Interoperability can be achieved by using standards for images and or templates (ANSI 378, ISO 19794-2, ISO 19794-4) Currently, no standard is defined for employee digital identity.
Privacy	Thanks to MoC, end-user's biometrics remains in his card. It ensures end-user's privacy by keeping the reference template in the proven secure environment of a smartcard. End-user can encode his files on his desktop with his biometric identifier and prevent access to them by another user. Storage of end-user's biometrics (On-Card or in databases) must be done with regard to ethics & privacy committee's recommendations of each country.
ROI	No more pin code/password loss. Cost saving for card re-issues. Reduction of calls to help desk for password resets Reduce electronic data thrft. According to a cost/benefit analysis from US DoS, 200USD per user per year id saved on password management by the use of biometrics.
Recommendations	Logical and physical access applications can be merged on a single dual employee ID card. Each solution must be adapted and/or customized to the needs of the different stakeholders: ▪ High security infrastructure ▪ Government employee for IT network access, legal forms

	digital signature… ▪ Private company employees for IT network access…
Eurosmart Recommendations	Combination of an access badge with MoC and biometrics for two factor identification with respect of privacy. Definition of a standard for employee digital identity on corporate networks. European standard IAS-ECC can be used for digital signature application.

Ethical criteria	**Eurosmart technical questionnaire**	**Eurosmart recommendation to government, ID management and service providers**
Role of the biometric application	Biometric application is to use MOC in both cases of physical access control and PIN replacement	Full and frank debate on the issues raised by all parties in the entity concerned of a public or private organization.
Transparency regarding use of biometric technology	Enrolment: By an appointed official Storage: in the employee card only. Acquisition by means of attended terminals for physical access and cardholder's terminal for logical access control. Matching: On card	Describe in a document the procedures that go with the technical measures. Request the legal authorizations.
Relevance and necessity	*Environment, purpose*, e*fficiency*: relative to the entity that must be protected *Reliability*: MOC is more reliable than codes, PINs and passwords.	The ID management policy of the entity must comply with legislation, regulations. Information will describe – The dangers for the entity, for the employees. – The management of biometric data and procedures, confirming that no biometric database would be set up.
Use of only required information to achieve a clear, limited and specified purpose.	MOC is the clear cardholder's consent to be authenticated. No access to any further information.	
Are system operators and system providers properly trained with regard to their obligations to respect and protect the information?	Biometrics does not affect in any way the management of employee's information.	
Can system operators and system providers access information other than that required to carry out their function?	Biometrics does not affect in any way the management of employee's information.	
Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately?	Biometrics does not affect in any way the management of employee's information.	
Can the user make the decision whether or not to participate in the programme?	Use of MOC may be not the unique identification / authentication mean.	Subject to negotiation in the entity, taking into account, relevance, necessity and acceptance by users.
What are the practical measures that ensure the integrity of an individual's personal and information privacy?	Templates and MOC are the best measures for ensuring both integrity and privacy of information	No specific concern as far as biometrics is concerned.
The biometric data should be classified as sensitive personal information and as such afforded greater protection.	Templates are never transmitted outside of the card.	Templates are never stored or transmitted elsewhere other than inside the card.
Clear knowledge of vulnerabilities and protection against them.	*Spoofing,* Less easy than with PIN / password *Replay attacks,* Less easy than with PIN / password.	Describe in a public document the procedures that go with the technical measures.

	Substitution attacks Not possible*. *Tampering* not possible*. *Masquerade attacks* not possible* *Overriding the yes/no response,* Not possible*. * within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum	Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum)
An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary,	Possibility to cancel a card and issue a new one.	Entity must allow the individual's rights to be satisfied.

3.2.5. Healthcare

Healthcare	**Use of smart card + biometrics in order to enhance efficiency, prevent fraud, whilst reducing healthcare costs**
Status	eHealth card systems appeared in the early 90s, to streamline the infrastructure for transactions and processing. The objective was to reduce the administrative costs of health care coverage. Since the new millennium, security objectives became an increasingly important aspect for protecting the personal data of users and it become crucial to enhance the security of those systems aimed at protecting against fraud, on the one hand, and abuse/excessive treatment, on the other. Many European countries (France, Germany, Slovenia, Spain, Italy, etc.) have already set up modern healthcare systems. Many other initiatives are currently being pursued around the world (South Africa, Taiwan, Algeria, etc). Today a new generation of systems are arriving adding new features to the infrastructure already in place, based on PKI for example, implementing ePrescriptions management, allowing online medical data... where strong authentication is needed. Biometrics is the perfect technology to achieve this goal.
Benefits	Providers - Instant patient identification - Rapid accessibility to patient medical history - Accurate link between patients and institutional medical records - Faster care delivery in emergency care situations - Potential reduction in adverse events and medical errors due to lack of patient information - Reduction in claims denials - Integration with legacy systems with nominal IT costs - Audit trail through a course of treatment across multiple organizations - Reduction in unnecessary/duplicated diagnostic tests or procedures by providing results from other medical providers Healthcare Delivery Organizations - Reduction or elimination of mismanaged, lost or stolen electronic records - Fraud Reduction via accurate patient identity - Data Integrity -- Reduced medical record maintenance costs (duplicates/overlays) -- - Streamlined administrative procedures Healthcare Employer - Highly secure identity credential for both physical and logical access - Single sign-on capabilities (reduction in help desk calls/password management requirements) - Link to other employee services (ID badge, parking, cafeteria)
Security	- against fraud and misuse of system both from patients and health care providers - patient security – enabling quick decision making based on correct facts
Interoperability	- Regulatory Compliance: HIPAA and DEA compliance for ePrescribing controlled substances - Interoperability using standards for images and or templates (ANSI 378, ISO 19794-2, ISO 19794-4)
Privacy	- MoC with template stored on card possible, no database needed.
ROI	In France, with the Vitale card, annual administrative cost savings have been estimated at EUR 300 millions, In Germany, the annual medical cost savings have been estimated at EUR 3

	billions.
Recommendations	- combination of smart cards and biometrics for identification of both patients, doctors and other health care providers - win-win situation • Patients get more efficient and quicker help • Reduced administration and higher efficiency for health care providers • Reduced fraud, saving money for insurance and government

Ethical criteria	**Eurosmart technical questionnaire**	**Eurosmart recommendation to government, ID management and service providers**
Role of the biometric application	Biometric application is to replace PIN by matching on card	Full and frank debate on the issues raised by all parties: – Social insurance – Healthcare professionals (HP) – Patients
Transparency regarding use of biometric technology	Enrolment: By a registry official at Insurance premises. Storage : on eID card only Acquisition by HP's terminal for an electronic claim, or cardholder's terminal for access to a medical / health insurance server Matching on card.	Describe the procedures that go with the technical measures in a public and easily accessible document
Relevance and necessity	*Environment*: Medical information is very sensitive. The MOC protects privacy. *Purpose*: The requirement is actuallyto authenticate who you are. *Efficiency*: No existing technique can replace biometrics *Reliability*: Pin and password theft Is an increasing white collar fraud.	A policy on medical data and digital identity management should be defined, describing: – Identity theft dangers for the community, social insurance, healthcare professionals and for patients. – Along with identity management, use of biometrics should not be imposed, but given as a more convenient possibility when digital identities must be trusted. MOC by itself has a privacy guarantee, but health insurance management must provide evidence that there is no biometric database. General description and guarantee to be described in an easy to find and understand document.
Use of only required information to achieve a clear, limited and specified purpose.	MOC is the clear cardholder's consent to access his/her data	
Are system operators and system providers properly trained with regard to their obligations to respect and protect the information?	Introducing biometric MOC does not particularly impact this point.	
Can system operators and system providers access information other than that only required to carry out their function conduct their job?	Introducing biometric MOC does not particularly impact this point.	
Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately?	Introducing biometric MOC does not particularly impact this point.	
Can the user make the decision whether or not to participate in the programme?	Use of MOC for accessing e-services is always a voluntary act.	Availability of MOC on the eID card must be an option decided by the patient. Warning of weaker protection of personal data should

		be given in case of refusal to use MOC.
What are the practical measures that ensure the integrity of an individual's personal and information privacy?	Templates and MOC are the best measures for ensuring both integrity and privacy of information	No specific concern as far as biometrics is concerned.
The biometric data should be classified as sensitive personal information and as such afforded greater protection.	Templates are never transmitted outside of the card.	No specific concern as far as biometrics is concerned.
Clear knowledge of vulnerabilities and protection against them.	*Spoofing,* Less easy than with PIN / password *Replay attacks,* Less easy than with PIN / password. *Substitution attacks* Not possible*. *Tampering* not possible*. *Masquerade attacks* not possible* *Overriding the yes/no response,* Not possible*. * within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum	Describe in a public document the procedures that go with the technical measures. Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum)
An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary,	Possibility to cancel a card and issue a new one.	Health insurance must allow the individual's right to be satisfied at costs corresponding to the legitimacy of the cardholder's claim.

3.2.6. Welfare

Using biometrics for welfare	**Use of smart card + biometrics in order to prevent fraud, misappropriation of welfare benefits whilst protecting privacy**
Status	Welfare programs provide pension payments, distribution of goods and services to poor populations. In many cases, the people who should benefit from the program do not have any ID document. It might also be the case that no civilian registration is in place. Provision of goods and services is decentralized and very often no on-line connection is available. People must be identified in order to avoid misappropriation of the benefits. Biometrics is the most secure means to identify these people.
Benefits	For welfare organizations - Instant individual identification - Elimination of duplicate beneficiaries - Fraud Reduction via accurate patient identity - Easier administrative processing Beneficiaries - Confirmation that he/she is a beneficiary of the program -
Security	- against fraud and misappropriation by misuse of identity - Biometrics is linked to the beneficiary not to a document that can be counterfeited, stolen or lent.
Interoperability	- Interoperability using standards for biometric images and or templates
Privacy	Non Governmental organizations are not officials. They are not entitled to manage a biometric database. Then MOC is the right solution.
ROI	In all cases, there is the need to enrol all the beneficiaries. Capturing biometric data does not represent a significant cost increase in the process. It allows prevention of duplicate identities. Issuing a document for biometric matching is cheap compared to the cost of an on-line IT infrastructure.
Regulations and recommendations	
Eurosmart recommendations	- combination of smart cards and biometrics for beneficiaries - Avoid the use of biometric database for convenience and misuse by organizations that shall not be entitled to manage identities

Ethical criteria	**Eurosmart technical questionnaire**	**Eurosmart recommendation to government, ID management and service providers**
Role of the biometric application	Biometric application will verify the beneficiary's identity.	Full and frank information to all parties. – Government – Welfare organization members – Beneficiaries
Transparency regarding use of biometric technology	Enrolment: By an authorized official with only possibility of recording templates onto the beneficiary's	Describe in a public and easily accessible document the procedures that go with the

	card. Storage : on beneficiary's card only Acquisition by welfare organization terminal. Matching on card.	technical measures
Relevance and necessity	*Environment*: No civil registry able to prevent duplicated identities *Purpose*: The requirement is to authenticate who the beneficiary is *Efficiency*: No existing technique can replace biometrics *Reliability*: No other reliable solution for most cases	A policy on welfare benefits and digital identity management should be defined, describing: – The risks that must be prevented. – Alongside a clear statement on the use of biometrics MOC by itself has a privacy guarantee but welfare organization must provide evidence that there is no biometric database, General description and guarantee to be described in an easy to find and understand document, for the people concerned.
Use of only required information to achieve a clear, limited and specified purpose.	Introducing biometric MOC does not particularly impact this point.	
Are system operators and system providers properly trained with regard to their obligations to respect and protect the information?	Introducing biometric MOC does not particularly impact this point.	
Can system operators and system providers access information other than that only required to carry out their function?	Introducing biometric MOC does not particularly impact this point.	
Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately?	Introducing biometric MOC does not particularly impact this point.	
Can the user make the decision whether or not to participate in the programme?	Balanced benefits are important for beneficiaries. Biometrics is more likely to be used as a protection of privacy rather than a threat to privacy.	
What are the practical measures that ensure the integrity of an individual's personal and information privacy?	Templates and MOC are the best measures for ensuring both integrity and privacy of information	No specific concern as far as biometrics is concerned.
The biometric data should be classified as sensitive personal information and as such afforded greater protection.	Templates are never transmitted outside of the card.	No specific concern as far as biometrics is concerned.
Clear knowledge of vulnerabilities and protection against them.	*Spoofing,* Less easy than with PIN / password *Replay attacks,* Less easy than with PIN / password. *Substitution attacks* Not possible*. *Tampering* not possible*. *Masquerade attacks* not possible* *Overriding the yes/no response,* Not possible*. * within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum	Describe in a public document the procedures that go with the technical measures. Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum)
An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary,	Possibility to cancel a card and issue a new one.	Welfare organization must allow the individual's rights to be satisfied corresponding to legitimate claims.

3.2.7. eGovernment

eGovernment use case:	**Declaration of revenues of small enterprises for calculation of company's owner social contributions**
Status	e-Government Services with biometric authentication are being deployed in Portugal (since 2007). In France, this declaration can be made over the internet by an employee of the company. Security is carried out by an identifier + a password authentication. After the first declaration, the company receives a letter informing them of this identification. In small companies, the security culture is poor. Protection of identifiers and passwords may not be observed. A malicious person could create problems for the company owner with social organizations and the legal system. The use of the national eID card would make great progress in terms of security. In addition, authentication via Match On Card would provide the guarantee that the card holder is the person who made the declaration.
Benefits	For the employee: This person would feel comfortable that nobody can carry out malicious acts with his / her identity. For the company owner: His delegation of duties to a person is secure. For the service provider: Small companies will make more on-line declarations that will reduce its costs and enhance its own processes. Disputes are unlikely to happen.
Security	Security is enhanced by means of strong authentication. The benefit in terms of security is to avoid personal financial harm and unmerited problems with social declaration organizations and the legal system.
Interoperability	European Citizen Card (ECC) and electronic signature standards are applicable.
Privacy	Use of his/her own credentials might be seen as a privacy risk by the employee. Match On Card authentication, if well explained, would put his/her mind of rest.
ROI	No investment required: The company does not have to issue corporate cards. The security solution is effected by the use of the employee's ID card.
Regulations & recommendations	EC initiatives and directives in terms of eGovernment and electronic signature.
Eurosmart recommendations	For the adoption of the solution, there is a need to explain what Match On Card is. There is also a need for Ethical organizations to confirm that Match On Card does not infringe in any way card holder's privacy.

With regards to privacy and ethics, this is a special use of an eID card. So the same table applies.

3.2.8. eBanking

e-Banking	Introducing biometric authentication for on line banking use cases
Status	Banks are familiar with risk management and use in order to adapt the security of their system to the best compromise between ease of access their services, security costs and the risk of fraudulent use of e-banking services. As early adopters of biometric technology for employees it is expected that this functionality also will be made available to customers.
Benefits	Biometric technology simplifies access to services while Match-on-Card ensures end-user privacy.
Security	PINs and passwords are frail links in a security chain as they are easily written down, lost, borrowed or even stolen. With biometric Match-on-Card, you tie each transaction to a physical individual, creating traceability and reducing risks of fraud.
Interoperability	N/A – closed loop system.
Privacy	Match on card ensures end-user privacy by keeping the reference template in the proven secure environment of a smartcard.
ROI	Many laptops have built in sensors but for those who does not have one there is an investment related mainly to distribution of biometric readers. These readers, when distributed to customers without support, may also provide a branding opportunity for the bank.
Recommendations	None
Eurosmart Recommendations	Match-on-Card is strongly recommended to ensure privacy of clients. The possibility of allowing the clients to self enrol solves what would otherwise be a logistical challenge in some parts of the world.

Ethical criteria	Eurosmart technical questionnaire	Eurosmart recommendation to government, ID management and service providers
Role of the biometric application	Biometric application would replace PIN / secret code / password by matching on card	Application shall comply with the law, regulations, and necessary authorizations. The contract between the bank and the customer m,ust provide clear information on all issues. –
Transparency regarding use of biometric technology	Enrolment: By the customer him/herself in secure premises of the bank, in presence of a bank official. Storage : on eID card only Acquisition by cardholder's terminal	Describe in the contract the procedures that go with the technical measures

	to access a bank server Matching on card.	
Relevance and necessity	*Environment*: Banking information is very sensitive. The MOC protects privacy. *Purpose*: The requirement is to authenticate who you are. *Efficiency*: No existing technique can replace biometrics *Reliability*: Pin and password theft Is an increasing white collar fraud, especially for financial transactions.	The bank policy on digital identity management should be defined, describing: – Identity theft dangers for the bank, service providers and customers. – Alongside identity management, use of biometrics should not be imposed, but given as a more convenient possibility when digital identities must be trusted. MOC by itself has a privacy guarantee, but the bank must provide evidence that there is no biometric database. General description and guarantee to be described in an easy to find and understand document.
Use of only required information to achieve a clear, limited and specified purpose.	MOC is the clear cardholder's consent to access his/her data	
Are system operators and system providers properly trained with regard to their obligations to respect and protect the information?	Introducing biometric MOC does not particularly impact this point.	
Can system operators and system providers access information other than that only required to carry out their function?	Introducing biometric MOC does not particularly impact this point.	
Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately?	Introducing biometric MOC does not particularly impact this point.	
Can the user make the decision whether or not to participate in the programme?	Use of MOC for accessing e-services is always a voluntary act.	Availability of MOC on the card must be an option decided by the customer. Warning of weaker protection of personal data should be given in case of refusal to use MOC.
What are the practical measures that ensure the integrity of an individual's personal and information privacy?	Templates and MOC are the best measures for ensuring both integrity and privacy of information	No specific concern as far as biometrics is concerned.
The biometric data should be classified as sensitive personal information and as such afforded greater protection.	Templates are never transmitted outside of the card.	No specific concern as far as biometrics is concerned.
Clear knowledge of vulnerabilities and protection against them.	*Spoofing,* Less easy than with PIN / password *Replay attacks,* Less easy than with PIN / password. *Substitution attacks* Not possible*. *Tampering* not possible*. *Masquerade attacks* not possible* *Overriding the yes/no response,* Not possible*. * within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum	Describe in the contract the procedures that go with the technical measures. Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum)
An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary,	Possibility to cancel a card and issue a new one.	Banks must allow the individual's rights to be satisfied at costs corresponding to the legitimacy of the cardholder's claim.

3.2.9. Vehicle Registration card

Electronic Vehicle Registration card	**The EU Directive 2003/127/EC of December 2003, allows all member countries to introduce an electronic vehicle registration card as an alternative to the paper format. The card replaces previous documents dealing with registration and ownership of the vehicle concerned.**
Status	Electronic vehicle registration cards have been in discussion for a number of years, but up to the end of 2009, none had been introduced. Since 2009, however, member countries and their transport ministries have shown increased interest in the introduction of a highly secure electronic registration document. Slovakia, Austria and the Netherlands are leading the way and are already implementing the eVRC. Morocco has issued electronic Vehicle cards since 2007 No biometric technique is involved to date.
Benefits	For the user, for the service provider, the government, the society, … Road safety is a huge concern: It is a matter of saving lives, not simply money! Card document fraud is at very high level. In France, 200 000 cars are stolen annually and most of them are reused in France or other countries. The directive allows the addition of further data or changes to be made to the data initially created in the card. An overwrite option can, for example, be useful where vehicle modifications or tuning require registration changes that are not personalized in the card. The introduction of the eVRC will not only simplify vehicle checks by the responsible authorities at home and abroad but also make them more reliable. Smart card technology and security features printed or engraved in the document will provide a high level of security. A higher level of global security could be obtained by tying the vehicle to the document, using object biometrics. A bubble tag placed in the windscreen of the vehicle and identified in the chip of the eVRC would establish this strong link. Benefits for society: fewer accidents caused by vehicles that should no longer be used. Lives saved! Benefits for enforcement officers: Fast, easy and efficient checking of vehicle ownership, operational ability. Benefit for car owners and insurance companies: drastic reduction in vehicle thefts.
Security	Road safety is enhanced. Vehicle thefts are drastically reduced. Cost of vehicle insurance could be reduced accordingly.
Interoperability	Directive 2003/127/EC A further standardization of use of object biometrics should be provided, but not impacting on previous standards.
Privacy	Reading the biometrics of the vehicle could infringe privacy by tracking vehicle trips. However using eVRC and the vehicle together does not present such risks. O line checking with a database can be strictly allowed for enforcement officers in some very specific cases.
ROI	The cost of a smart card is of course higher than the classical paper document. But fees paid for VCR by motorists are very high in comparison of the technology costs, and thus are not really linked to it. Adding object biometricswould not add a cost to the eVRC. Introducing a bubble tag would affect the manufacturing of the vehicle part (windscreen as suggested here) but not significantly. Identity verification, including e-passports, eID cards, Driving licenses,

	eVRCs, tachograph cards, can be done with same tools. Use of object biometrics would request an additional sensor. Estimation of ROI: Most investment for eVRC can be shared by all other eID documents. Bubble tags add a marginal cost. But benefits are firstly saving of lives, and then the possibility of drastically reducing vehicle theft.
Regulations & recommendations	No regulation, no recommendation to date.
Eurosmart recommendations	Recommendations when using object biometrics are only linked to on line verification. This should be limited to police, and only in the case of non presentation of the eVRC, broken chip, or vehicle theft suspicion. Object biometrics could be used for anonymity of the data base, in this case.

The use case of a bubble tag applied to a document with the aim of guaranteeing genuineness and uniqueness of the document is very similar to the eIdentity document authenticity use case. So the same table may be reused.
In the case of a bubble tag (or any object biometrics) installed on the vehicle, we assume that any on card verification would not infringed civil privacy. So, the following table focuses on on-line access to a central database, if any.

Ethical criteria	**Eurosmart technical questionnaire**	**Eurosmart recommendation to government, ID management and service providers**
Role of the biometric application	A bubble tag integrated in the vehicle is linked to the chip of the car registration smart card. Optionally, in the case of a broken chip a central database can provide document authentication and vehicle data.	In the case of a central database, full and frank debate on the issues raised by all parties who will be involved in the proposed application, prior to the establishment of the proposed programme
Transparency regarding use of biometric technology	Enrolment: The biometrics of object is created at document personalization Storage : in the document Acquisition & matching by an authorized official or a closed system in a protected area	Describe the procedures in a public document
Relevance and necessity	An attempted fraud is breaking the document chip, *Environment*: The document requires a high degree of security *Purpose*: Make impossible to have fakes or forged documents for bad deals of vehicles. *Efficiency*: Today no real security feature exists. *Reliability*: No equivalent solution in terms of reliability	Access to the database should be allowed in well defined case uses: Upload of data, or check in the case of doubts on the document: Chip broken and security features difficult to verify.
Use of only required information to achieve a clear, limited and specified purpose.	Introducing of object biometrics does not particularly impact this point.	Appropriate information available to vehicle owners should be easily accessible. . Access management procedures should be established and made public. An individual should be fully and accurately informed and should
Are system operators and system providers properly trained with regard to their obligations to respect and protect the information?	Introducing of object biometrics does not particularly impact this point.	

Can system operators and system providers access information other than that only required to carry out their function?	Introducing of object biometrics does not particularly impact this point.	understand all the issues and implications relating to the provision of his/her information. General description and guarantee to be described in an easy to find and understand document.
Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately?	Introducing of object biometrics does not particularly impact this point.	
Can the user make the decision whether or not to participate in the programme?	Introducing of object biometrics does not particularly impact this point.	
What are the practical measures that ensure the integrity of an individual's personal and information privacy?	Introducing of object biometrics does not particularly impact this point.	
The biometric data should be classified as sensitive personal information and as such afforded greater protection.	Object biometrics of is not linked to a person.	
Clear knowledge of vulnerabilities and protection against them.	Identity verification is performed by an authorized official or by automated inspection terminals that are trusted, secured and attended.	Describe in a public document the procedures that go with the technical measures.
An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary,	Technical solution must allow the performance of the subsequent actions, with suitable security.	Procedures must allow the individual's rights to be satisfied.

3.2.10. Payments, cash withdrawals

Payments, cash withdrawals: use of biometrics instead of PIN or as a complement.	**Tailored payment solutions depending on the user Identity As aresult of biometrics, we can now adapt and tailor the payment solution for each citizen category.**
Status	Access to smartcards has historically been controlled by a simple authentication method: the PIN (Personal Identification Number). As a result of the right PIN, the cardholder has access to the card functionalities. This solution is relatively weak because the code can be easily forgotten and quickly recoverable. Biometric technologies can improve these authentication mechanisms. Indeed, a combination of both PIN and biometrics will easily improve security and privacy. Another solution is only to use biometrics to verify the user identity depending on the application. In some countries, many citizens can enjoy tax exemption on purchases. In this situation, the vendor or the authority need to verify the identity to adapt the payment. This is typically the type of application where MoC adds value.
Benefits	For the user, for the service provider, the government, the society, … - Avoids card sharing: only the cardholder can use it. Transaction only possible for the cardholder. - Easy to use and impossible to forget compared to a PIN code. - Strong authentication: the card and the cardholder are at the same place at the same time. - Easy to integrate into current systems. - Improves user confidence. - Cost saving for issuer due to the pin code loss and card reissue. - Possibility to adapt the payment as a result of the User Identity, tailored payment solution depending on the type of user. Authentication is done in advance to adapt the method of payment to the user's profile. - No database, no constraining maintenance
Security	How is security enhanced? Protection against terrorism, fraud, counterfeiting, identity theft, theft of money, … - Strong cardholder authentication - No skimming - Impossible to use a stolen payment card - Avoids people looking over the shoulder
Interoperability	done thanks to standards? Regulation, … - EMV - ISO - NFC
Privacy	What are the privacy concerns? - No database. - Only the cardholder has the record of his fingerprints. - Fingerprints secured in the tamper-proof environment of the smart card.

	- Impossibility of card sharing.
ROI	Estimate of ROI: Investment, extra recurrent costs, measurable benefits - Cost saving for issuers due to pin code loss and card reissue. - No costs for database maintenance. - Costs due to fingerprint reader to be integrated at the point of sale.
Recommendations	For adoption of the solution, for programs, support procedures, advices to regulation - Add biometric functionality when a payment solution needs to be adapted due to the user identity. - Work closer with Visa/MasterCard to integrate the Biometric PIN.

Ethical criteria	**Eurosmart technical questionnaire**	**Eurosmart recommendation to government, ID management and service providers**
Role of the biometric application	Biometric would replace PIN / secret code / password by matching on card	Application shall comply with the law, regulations, and necessary authorizations. The contract between the bank and the customer must provide clear information on all issues.
Transparency regarding use of biometric technology	Enrolment: By the customer him/herself in secure premises of the bank, in presence of a bank official. Storage : on eID card only Acquisition by payment terminal or an ATM for a payment or a cash withdrawal Matching on card.	Describe in the contract the procedures that go with the technical measures
Relevance and necessity	*Environment*: Spoofing a PIN at payment terminal or ATM is easy. *Purpose*: The requirement is to replace the PIN weakness. *Efficiency*: No existing technique can replace biometrics *Reliability*: false or true PIN theft Is increasing.	The bank policy on biometric use should be defined, describing: – Risks for the bank, retailers and customers. – Use of biometrics should not be imposed, but given as a more secure and convenient possibility when digital identities must be trusted. MOC by itself has a privacy guarantee, but the bank must provide evidence that there is no biometric database, General description and guarantee to be described in the contract.
Use of only required information to achieve a clear, limited and specified purpose.	Introducing biometric MOC does not particularly impact this point.	
Are system operators and system providers properly trained with regard to their obligations to respect and protect the information?	Introducing biometric MOC does not particularly impact this point.	
Can system operators and system	Introducing biometric MOC does	

providers access information other than that only required to carry out their function?	not particularly impact this point.	
Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately?	Introducing biometric MOC does not particularly impact this point.	
Can the user make the decision whether or not to participate in the programme?	Use of MOC for accessing e-services is always a voluntary act.	Availability of MOC on the card must be an option decided by the customer. Warning of weaker protection must be given in case of refusal to use MOC.
What are the practical measures that ensure the integrity of an individual's personal and information privacy?	Templates and MOC are the best measures for ensuring both integrity and privacy of information	No specific concern as far as biometrics is concerned.
The biometric data should be classified as sensitive personal information and as such afforded greater protection.	Templates are never transmitted outside of the card.	No specific concern as far as biometrics is concerned.
Clear knowledge of vulnerabilities and protection against them.	*Spoofing,* Less easy than with PIN / password *Replay attacks,* Less easy than with PIN / password. *Substitution attacks* Not possible*. *Tampering* not possible*. *Masquerade attacks* not possible* *Overriding the yes/no response,* Not possible*. * within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum	Describe in the contract the procedures that go with the technical measures. Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum)
An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary,	Possibility to cancel a card and issue a new one.	Banks must allow the individual's rights to be satisfied at costs corresponding to the legitimacy of the cardholder's claim.

3.2.11. Protection of children: Safe Chat

Chat	**Access control of participants to a children's chat room, by biometric authentication, in order to avoid participation by undesirable adults.**
Status	Users are not all familiar with risk management and there is the need to adapt the security of their system to the best compromise between ease of access to chatroom services, security cost and the risk of fraudulent chat. Teenagers do not perceive the risks connected with chatrooms. As early adapters to biometric technology for adults it is expected that this functionality will also be made available to teenagers.
Benefits	Biometric technology simplifies access to services while Match-on-Card ensures end-user privacy. The strong secure authentication reinforces the age validation and guarantees that teenagers are talking with appropriate persons in term of age.
Security	PINs and passwords are weak links in a security chain as they are easily written down, lost, borrowed or even stolen. With biometric Match-on-Card, you tie each chatroom to a physical individual, creating traceability and reducing risks of fraud.
Interoperability	Biometrics are not part of these cross border/systems interoperability tests. Bu, the approach as in e-Passports could be reused here.
Privacy	Match on card ensure end-user privacy by keeping the reference template in the proven secure environment of a smartcard. - in the case of verification: no re-building of fingerprint images - in the case of identification: only authorized person have access to biometric data
ROI	Many laptops have built in sensors but for those who does not have one there is an investment related mainly to distribution of biometric readers
Recommendations	The approach as in e-Passports could be reused here.
Eurosmart Recommendations	Match-on-Card strongly recommended.

Ethical criteria	Eurosmart technical questionnaire	Eurosmart recommendation to government, ID management and service providers
Role of the biometric application	Biometric application will replace PIN by matching on card	Full and frank debate on the chatroom misuses raised by all parties: – Government, – Administrative service providers – Private service providers, – Citizens
Transparency regarding use of biometric technology	Enrolment: By a registry official Storage : on eID document Acquisition & matching by	Describe in a public document adapted to teenagers the procedures that go with the

	cardholder's terminal and PC	technical measures
Relevance and necessity	*Environment*: On internet nobody knows who you are. Password / PIN easy to spoof. *Purpose*: Biometrics is the only technique that can authenticate who you are. *Efficiency*: No existing technique can replace biometrics *Reliability*: Pin and password theft Is an increasing white collar fraud.	A government policy on digital identity management should be defined, describing: – Identity theft dangers for the community, for the service providers and for teenagers. – Along with identity management, use of biometrics should not be imposed, but given as a more convenient possibility when digital identities must be trusted. MOC by itself has a privacy guarantee, but governments must provide evidence that there is no biometric database, or that their use is restricted to justified known use caseuse cases, using defined procedures protecting privacy. General description and guarantee to be described in a document easy to find and understand forteenagers.
Use of only required information to achieve a clear, limited and specified purpose.	MOC is the clear cardholder's consent to access his/her chat	
Are system operators and system providers properly trained with regard to their obligations to respect and protect the information?	No need of system operators.	
Can system operators and system providers access information other than that only required to carry out their function?	No need of system operators.	
Is there the possibility of installing profiling measures that might target particular groups within society unfairly or disproportionately?	Use of MOC does not give any possibility to do so.	
Can the user make the decision whether or not to participate in the programme?	Use of MOC for accessing e-services is always a voluntary act.	Availability of MOC on the eID teenager' card must be an option decided by the citizen
What are the practical measures that ensure the integrity of an individual's personal and information privacy?	Templates and MOC are the best measures for ensuring both integrity and privacy of information	No specific concern as far as biometrics is concerned.
The biometric data should be classified as sensitive personal information and as such afforded greater protection.	Templates are never transmitted outside of the card.	Data protection legislation must be reviewed in order to deal sufficiently with teenagers privacy concerns presented by the use of biometrics.
Clear knowledge of vulnerabilities and protection against them.	*Spoofing,* Less easy than with PIN / password *Replay attacks,* Less easy than with PIN / password. *Substitution attacks* Not possible*. *Tampering* not possible*. *Masquerade attacks* not possible* *Overriding the yes/no response,* Not possible*. * within the limits of the most up-to-date implementations, certified according to Common criteria EAL4+, as a minimum	Describe in a public document the procedures that go with the technical measures. Selection of smart card + biometric technology, security certified by CC evaluation (EAL4+ at minimum)
An individual should have the right to access any collected and/or stored information relating to him/her and to review and amend it where necessary,	Possibility to cancel a card and issue a new one.	Government must allow the individual teenager's rights to be satisfied at costs corresponding to the legitimacy of the cardholder's claim.

3.2.12. Notary Acts

Notary acts	Use of object biometrics for authentication of documents
Status	This solution is to use object biometrics and is already up and running in some countries to certify and authenticate original notary deeds as land titles. One reference solution is Benin where now object biometrics are systematically attached to the issued documents.
Benefits	Land title used to be falsified, counterfeited, and illegally delivered. Consequently the documents were questionable and lost value Offering the possibility to prove that one is in possession of the one and only unique original gives value to the documents. Benefits are many; for the benefit of the citizen, who can negotiate an investment loan with banks for his land, for the city that can identify the rightful owners, and for the economy of the society because of the trustworthy environment. The most convenient solution is to use a bubble SmartCard and an Authentication Cloud services. The bubble SmartCard allows the owner to certify the current use of the notary deed to prove and apply the right attached to the bubble SmartCard and the Authentication Cloud services with the bubbleTag reinforce the long term verification of the document.
Security	Security is enhanced by having the token proving that the document is genuine and that the information is accurate and not altered in any way. Additionally security is durable because no information is stored in the biometric element, it is just a unforgeable optical key linked to managed security information stored on an electronic medium as a Bubble SmartCard for years
Interoperability	The system is web based and accessible to all citizens according to local rules and regulations
Privacy	None, it obeys local laws and can be changed should privacy issues change
ROI	The cost of using a bubble SmartCard and Authentication Cloud services is higher than a paper document but the return on the investment lies in reducing paper document storage for the notary, reducing the cost of verifying the document and increasing the confidence in the document leading to a reduction in the financial risk.
Recommendations	Documents with high longevity (over 5 years) should carry a visible optical object biometricacting as an unforgeable optical key to access the file stored in either local or remote information storage facilities. This object biometric should ideally be linked to a human biometric when the protected information is linked to one or more individuals involved in the certification process.

3.2.13. Driving licenses

e-Driving License	**Extended EU regulations are expected in November 2010; these regulations refer to new application standards ISO 18013, as well as a harmonized document in format, security and driving class.**
Status	In CY 2010 e-Driving License are in use in 10 states outside Europe. Many programs run with biometric data stored on the document, such as in Japan, Hong Kong, India, Morocco, and El Salvador. The new extended EU regulations would foster more programs in Europe. Facial images are in use in Japan (tested in Russia), fingerprint data is in use in India and Morocco and both biometric data are used in El Salvador and Hong Kong.
Benefits	- increasing the security of the document - better tie between holder and license document - increase in road safety
Security	New EU driving licenses have a minimum of 5 optical security elements, defined by the EU Commission; with an embedded microcontroller electronic securities in HW and SW are captured.
Interoperability	If the EU-specification defines all key elements, such as data set on card, access to the data set on card, communication protocol between card and reader, interoperability should be possible, similar to the programs running for EU-Tachographs, which run today in 32 states.
Privacy	Protection of electronic data by access key. Fingerprint images must be protected by an additional access key. Card-to-Card Authentication and PIN verification by authorized persons, such as the police, should be used.
ROI	Re-financing of production costs by increasing the fee per driving license document.
Recommendations	a) Government's Recommendation EU regulation 2006/126/EC for all driving license documents in EU from 2012 onwards ID1-format, Polycarbonate, 5 optical security elements, uniform design) b) EUROSMART's Recommendation In some EU states driving licenses are equivalent to ID-cards, because ID-cards are not in use (e.g. UK, Norway, Denmark) or ID cards are voluntary (e.g. in Sweden, Finland, France). With the migration to e-Driving License a contribution to national security would be achievable.

With regard to privacy and ethics, the eDriver's license is similar to an eID card. So the same tables apply, for either identification or authentication.

3.3. Eurosmart general recommendations and position

Community and individual security risks that exist and are growing fast are not well identified and evaluated:

- Terrorism, acts of piracy are increasing,
- Illegal immigration,
- Identity theft,
- Social insurance, welfare benefit Fraud,
- White collar, organized crime,
- Misappropriation of documents, intellectual property,
- ….,

A global response for drastically reducing all of these is to reinforce identification of people and objects. Biometrics is the only means of identification that is linked to the individual or the object itself. Thus it is natural to consider its use.

Generally, the man in the street thinks that biometrics is a threat to his own privacy and an ethical risk for people.

The first recommendation of Eurosmart is to provide education:

- On security risks: nature, seriousness of harm to the community and individuals, impact on economy, growth,

- On solutions that can combat the risks, whatever they are, on the evaluation of their efficiency, costs, side effects, their intrinsic security, the misuses they can give rise to.

- On privacy: What it is, perceived and effective privacy, on proportionality: security vs privacy.

- On what is identification, digital economy, digital identity,

- On smart card technology, biometrics,

This is similar to the OECD's promotion of a security culture.

Associated with this recommendation, Eurosmart would like an Ethics Committee to elaborate and validate impartially these education documents. In a globalized world, we can assist in preventing non-use of good solutions because of unverified threats as reagrds privacy and ethics, and also in the uncontrolled use of inappropriate solutions. With regards to that, we recall the paradox of people who are afraid of sending their personal data to reliable organisations when they disclose it all to the planet via social networks on the internet.

The second recommendation of Eurosmart is to classify use cases we have tried in this document, in order to analyse and compare solutions on the basis of pragmatic criteria.

These criteria will relate to security, privacy protection, efficiency, convenience, ease of use, benefits, costs and ROI.

The third recommendation is to roll out solutions that comply with EU regulations, governmental laws, and authorizations issued by ethics committees. In our opinion, technology does not intrinsically have value, either good or bad. The proposed solution must provide countermeasures to the identified misuses that represent threats.

Linked to the third recommendation, our fourth one is to recommend the association of both smart card technology and biometrics, and in particular the use of Match On Card.

As a fifth recommendation, we note that the security of IT solutions can be evaluated and certified. The common criteria methodology has been used extensively used for smart card technology and is being adopted for Match On Card. The objective of an evaluation document forming part of the method can define what has to be protected in terms of security and in terms of privacy.

Better integration of biometrics in smart card standardization is our 6th recommendation. The European Citizen card (ECC) standard should perform this action. This will enhance interoperability at card level.

Integration recommendations deal with:

– The selection of the biometric technique according to the use case,
– The use of multimodal biometrics where necessary,
– The definition of procedures for system operators and system providers.

4. Appendix

4.1. Sources and references

- European Biometrics Portal (EBP) Trend report, “Biometrics in Europe”, Unisys, 2006.
- “EMEA Biometrics market” Frost and Sullivan, July 2009.
- [FGB09] Report on a biometric profile specific to cross-border interoperability of biometrics applicable to e-identity, 1.0, Focus Group on Biometrics, CEN, 2009.
- [TR09] Technical Report : a consensus on conformity and interoperability mechanisms; both for applications and sensors, in order to achieve security evaluated interoperable solutions between European Union Member States, v1.01, Focus Group on Biometrics, CEN, 2009.
- [IDMT07] The Global Platform Value Proposition for Identity Management, Global Platform, White Paper September 2007.
- [MOC09] The Global Platform for Biometric Match-on-Card Verification, Global.
- “The GlobalPlatform value proposition for biometrics match on card verification”, GlobalPlatform, white paper 2009.
- “Smart cards and biometrics in privacy-sensitive secure personal identification systems”, Smart Card Alliance, May 2002.
- “Biometrics enhancing security or invading privacy?” Irish Council for Biometrics, 2009.
- Ethical practices in the use of biometrics identifiers within the EU, Anne-Marie Sprokkereef and Paul de Hert.

4.2. Glossary

These definitions are part of the Eurosmart glossary (www.eurosmart.com).

ABC	**A**utomatic **B**order **C**ontrol.
ABIS	Automated Biometric Identification System. Such a system compares captured biometric samples to a database of records in order to determine the identity of an individual.
Accuracy	The accuracy of a biometric procedure or system gives the level of precision reached in the actions.
AFIS	Automated Fingerprint Identification System. Automated Biometric System that compares a submitted fingerprint record (single or multiple) to a database of records in order to determine the identity of an individual.
Authentication	A cryptographic process that validates the claimed origin of data or an identity [EMV].In biometric technique the authentication process compares the captured biometric sample with the biometric information’s previously stored on a smart secure device (epassport, smart card,…)
Biometrics	Measurable, distinct physical characteristics or personal traits that can be used to recognize the identity or verify the claimed identity of an enrolled person.
BioAPI (Biometrics Application Programming Interface)	Define the programming interface and service provider interface in order to facilitate the integration of biometric devices into the overall system architecture.

Biometric Data	A general term used to refer to any computer data that is created during a biometric process. More precisely two kinds of biometrics data can be used : * Collected Biometric Data : raw data get out of the sensors named Biometric Samples * Compressed or computed Biometric Data : in order to accelerate the automated biometric process or reduce size needed by the records in memory, raw Data are “compiled” or “compressed” by dedicated algorithms that keep accuracy while decreasing drastically size of records.
Biometrics	A general term to describe either a characteristic or a process : * A measurable biological and behavioral characteristic that can be used for automated recognition * In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes.
Biometric Sample	Raw data originating from the sensors.
Biometric template	Representations of a fingerprint or other biometrics using series of numbers and letters.
BIP	**B**iometric **I**nterworking **P**rotocol.
BITE	The BITE (‘Biometric Identification Technology Ethics’) project set out to promote research on the bioethical and ethical implications of emerging biometric identification technologies and initiate an international, public debate on the subject. The project brought together nine partners, including bioethicists and representatives of the biometric industries, from five European countries, including four EU Member States.
Capture	Process of collecting biometric samples from an individual via a sensor.
CBEFF	A standard that provides the ability for a system to identify and interface with multiple biometrics systems and to exchange data between system components.
Comparison	Process of comparing a biometric sample with a previously stored reference or references, in order to make an identification, or a verification.
Digital signature	Digital signatures are used to establish the authenticity of electronic messages and documents. They are usually based on asymmetric cryptographic algorithms, such as the RSA algorithm. The legal validity of digital signatures is governed by legislation in many countries and in Europe. Digital signatures are sometimes referred to as ‘electronic signatures’.
DNA	**D**eoxyribo**n**ucleic **A**cid.
ECC	**E**uropean **C**itizen **C**ard.
EER (Equal Error Rate)	Statistic evaluation of the biometric performance of the system where FAR and FFR are equal. In general the lower the EER is, the more accurate the biometric system is.

Enrolment	The initial process of collecting biometric data from a user and then storing it in a template for later comparison. As far as smartcard are concerned the process of originally acquiring the biometric data of a cardholder and entering it into the corresponding smart card. The data stored in the smart card then form the basis for subsequent biometric user identification.
e-Services	Or "eServices" is a highly general/generic term usually referring to the provision of services via the Internet (the prefix 'e' standing for "electronic", as it does in many other uses). It is true Web jargon, meaning just about anything done online. e-Services include "e-commerce," although they may also include non-commercial services. Non-ecommerce e-services include (at least some) "eGovernment" services.
eVRC	**e**lectronic **V**ehicle **R**egistration **C**ard.
Extraction	In a biometric security system, the process of converting a captured biometric sample into data that can be compared to a reference template and possibly stored.
Face Recognition	Biometric modality that uses an image of the visible physical structure of an individuals' face for recognition purposes.
FAR - False Acceptance Rate	A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system produces a false accept, which occurs when an individual is incorrectly matched to another individual's existing biometrics.
Fingerprint Recognition	Biometric modality that uses the physical structure of the User fingerprint for recognition. In most of Fingerprint recognition the Biometric Samples are compressed in Minutiae points that reduce the size of data and accelerate the process.
FTA (Failure To Acquire or FMR)	Failure of a biometric system to capture and/or extract usable information from a biometric sample.
FRR - False Rejection Rate	A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system produces a false reject, which occurs when an individual is incorrectly matched to his/her own existing biometrics.
FRR Rate	Statistic evaluation of the FRR of a biometric system.
FTE - Failure To Enrol	Failure of a biometric system to form a proper enrolment reference for an end user. Common failures include end users who are not properly trained to provide their biometrics, the sensor not capturing information correctly, or the sensor data insufficient quality to develop a template.
FTE Rate	Statistic evaluation of the FTE of a biometric system.
Global Platform	A non-profit organization founded in 1999 aiming at Smart Card infrastructure development to support multi-application, multi-actor and multi-business models implementations. At the end of 2008, the Global Platform association had more than 50 members.
Hacker	A person who attempts to break into computers that he or she is not authorized to use.
Hand Geometry Recognition	Biometric modality that uses the physical structure of the user's hands for recognition

HPC (Health Professional Card)	The Healthcare Professional Card (HPC) is a person specific ID Card, which allows health professionals to access to the Patient Card (PC) data and IT infrastructure available for healthcare and health insurance services.
IAS (Identification, Authentication & Signing)	The three main pillars for a 2-factor user authentication combined with electronic signature useful for all online services such as e-Government, e-Business and e-Procurement services. A smartcard with MoC (Match on Card) capability ideally provides all the necessary ingredients for identification including with biometrics and authentication (PIN verification).
IAS-ECC	Technical specification for smart card based on the European Citizen Card (ECC) standard which is a CEN standard
ICAO	**I**nternational **C**ivil **A**viation **O**rganization.
Identification	* The process, generally employing unique machine-readable names, that enables recognition of users or resources as identical to those previously described to the computer system * The assignment of a name by which an entity can be referenced. The entity may be high level (such as a user) or low level (such as a process or communication channel * In a biometric system, a task where the system searches a database for a reference matching a submitted sample, ad if found, returns a corresponding identity.
Identification card	Card identifying its holder and issuer which may carry data required as input for the intended use of the card and for transactions based thereon. [ISO 7810]
Identity	Two definitions: * Information that is unique within a security domain and which is recognized as denoting a particular entity within that domain. * Representation uniquely identifying entities (e.g. a user, a process or a disk) within the context of the TOE. An example of such a representation is a string. For a human user, the representation can be the full or abbreviated name or a (still unique) pseudonym.
Integrity	* The accuracy, completeness and validity of information in accordance with business values and expectations. The property that data or information has not been modified or altered in an unauthorized manner * A security service that allows verification that an unauthorized modification (including changes, insertions, deletions and duplications) has not occurred either maliciously or accidentally.
Interoperability	The ability to exchange requests between entities. Objects interoperate if the methods that apply to one object can request services of another object. Example: ePassports from different vendors must be readable at any border control terminal from various vendors.
Iris Recognition	Biometric modality that uses an image of the physical structure of an individual's iris (the iris muscle which is the colored portion of the eye surrounding the pupil) for recognition purposes. Only the iris structure is used by the recognition process, not the color of the iris.

ISO (International Organization for Standardization)	ISO was founded in 1947 and is based in Geneva, Switzerland. Its function is to support the generation of international standards in order to promote the free exchange of goods and services. Many ISO standards are used by the Smartcard Industry and Smart technology Industry such as * ISO 7816 series for contact card products & systems * ISO 14443 series for contactless smartcard products & systems * ISO 15693 series for "vicinity" cards * ISO18092 for the NFC interface and protocol communication modes * ISO 15408 series for IT security evaluation * Etc. Conversely "ISO" is not an acronym, but the Greek word for "equal."
JTC	**J**oint **T**echnical **C**ommittee.
LSP (Large Scale Pilot)	In the areas of electronic identity and online public procurement, many initiatives have been launched at national level to develop solutions. Bringing these sometimes divergent approaches into line and making them interoperable at European level is the focus of a series of Large-Scale Pilots (LSP) being launched with the support of the European Commission? STORK, PEPPOL, epSOS are such pilots.
Masquerade	A masquerade is where one entity pretends successfully to be a different entity. A masquerade is usually used with some form of an active attack such as replay and modification of messages or data.
Match	Decision that the biometric sample and a stored template comes from the same human source. The decision is made on the level of similarity (difference or hamming distance).
Matching	The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. The system makes decisions based on this score and its relationship (above or below) with a predetermined threshold.
Match on Card (MOC)	The process of matching a biometric sample against a previously stored template on the same smartcard. MOC is the best known approach to underwrite cardholder's privacy protection.
Match On System (MOS)	The process of matching a biometric sample against a previously stored template, performed on a system.
Match off Card	The process of matching a biometric sample against a previously stored template outside of card or any portable personal object.
Minutia (e) Point	Minutiae are the points where friction ridges begin, terminate, or split into two or more ridges. In many fingerprint systems, the minutiae are compared for recognition purposes. It accelerates the matching and can be done using a smaller memory footprint for storing them.
MRTD	**M**achine **R**eadable **T**ravel **D**ocuments.
MRZ (Machine Readable Zone)	Data on the identity page is encoded in optical character recognition (called OCR) format. Many states began to issue Id documents with MRZs in the 1980. The standardization was done by the International Civil Aviation Organization (ICAO), with the document ICAO 9303.
Multimodal Biometric System	System that uses two or more modality components (biometric characteristic, sensor type, or feature extraction algorithm) occurs in multiple. (For example: fingerprints and iris recognition).

Non-repudiation	The author of a message cannot deny an operation.
nPA	**n**euer **P**ersonal**a**usweis (German new eID card).
Objects Biometrics	A natural phenomenon of elements which characteristic is chaotic and measurable, for example, surface states, bubbles in a material, manufacturing defects, can be used a biometric characteristic of the element.
OECD	**O**rganisation for **E**conomic **C**o-operation and **D**evelopment.
One to Many, One to n	In a biometric system describes the comparison of one reference to many enrolled references. One to Many is used for identification or by watch list tasks.
One to One	In a biometric system describes the comparison of one reference to one enrolled reference to make a decision .One to One is used for authentication particularly by Match on Card.
Palm Print Recognition	Biometric Modality that uses the physical structure on an invidual's palm print for recognition purposes.
Performance	When applied to a biometric process or algorithm, this word means a measurement of a single or mixed characteristics, such as accuracy, speed, throughput.
Phishing	Phishing' refers to emails that trick people into giving out their personal and banking information; they can also be sent by SMS. These messages seem to come from legitimate businesses, normally banks or other financial institutions or telecommunications providers.
PI	Personal identification.
PIN (Personal Identification Number)	A security method used to show "what you know". Depending on the system a PIN could be used to either or verify a claimed identity.
PIV (Personal ID-Verification)	In response to HSPD 12, the NIST Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. The PIV-Card is a secure token for logical and physical access.
PKI	Public Key Infrastructure A PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.
Population	The set of people that can be concerned by a biometric application.
Replay attack	A replay attack occurs when a message, or a part of a message, is repeated to produce an authorized effect.
ROI	**R**eturn **O**n **I**nvestment.
SC	**S**ub-**C**ommittee.

Security	This term has different generic definitions: • Freedom from undesirable events, such as malicious and accidental misuse; how well a system resists penetrations by outsiders and misuse by insiders: • The protection of system resources from accidental or malicious access, use, modification, destruction, or disclosure. • The protection of resources from damage and the protection of data against accidental or intentional disclosure to unauthorized persons or unauthorized modifications or destruction. Security concerns transcend the boundaries of an automated system.
Security feature	Technical mean which permits raising the effort of exploiting a threat, or even making it impossible to exploit. It can be implemented at software, hardware or protocol level.
Sensor	Hardware of a biometric device that is able to capture a biometric sample, for instance iris, fingerprint, or face.
SIS	**S**chengen **I**nformation **S**ystem.
Skimming	Card skimming' is the illegal copying of information from the magnetic strip of a credit or ATM card. It is a more direct version of a phishing scam. In biometrics and ID it could be the act of obtaining data from an unknowing end user who is not willing to submit the sample at that time. An example could be secretly reading while in close proximity to user on a bus.
Smart Card (Smartcard)	Generally used to name a card containing a chip or an Integrated Circuit (strictly a secure microcontroller). A Smart Card is an ICC
Spoofing	Commonly used technique to break inside a network. The packets are building so that they seem to come from inside the network whereas they come from the outside. This kind of attack can be blocked by firewalls.
Tachograph	Device combining the functions of a clock and a speedometer. Fitted to a motor vehicle, a tachograph records the vehicle's speed whether it is moving or stationary. In order to avoid tampering analogue tachographs are now being replaced by digital tachographs which records data on Smart Security Devices (smartcards or other form factor).The signals from the vehicle's axle-tree sensor are encrypted which makes tampering much more difficult.
Tamper	To deliberately alter a system's logic, data, or control information to cause the system to perform unauthorized functions or services.
Template	A digital representation of an invidual's characteristics representing information extracted from a biometric sample and calculated at the enrollment phase. Accuracy of algorithm that generates Templates is the key point of the complete system.
Terminal	The device used in conjunction with the ICC at the point of transaction to perform a financial transaction. The terminal incorporates the interface device and may also include other components such as host communications [EMV].
Threat	A threat consists of an adverse action performed by a threat agent on an asset [CC] Examples of threats are: * a hacker (with substantial expertise, standard equipment, and being paid to do so) remotely copying confidential files from a company network or from card; * a worm seriously degrading the performance of a wide-area network; * a system administrator violating user privacy; * someone on the Internet listening in on confidential electronic communication.

Treshold	Setting for a biometric system. The acceptance or rejection is determined by the fact that the comparison process provides a score that is above or below the treshold.
Trojan horse	When a software program that performs a legitimate function contains a hidden unauthorized function that exploits the legitimate function, the unauthorized function is called Trojan horse.
True Rejection Rate	i.e. the percentage of times a system (correctly) rejects false claim identity. The TAR is one of the components which measures the performance of a biometric system when operating in the verification task.
Trust	A firm belief or confidence in the honesty, integrity, justice, reliability, etc., of a person, company, etc. In the security engineering, a trusted system is a system that is relied upon to a specified extent to enforce a specified security policy. As such, a trusted system is one which failure may break a specified security policy.
Trusted channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.
Verification	A task where a biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates.
VIS	**V**isa **I**nformation **S**ystem.
VISIT (USA) / US-VISIT	The U.S. Department of Homeland Security's US-VISIT program provides visa-issuing posts and ports of entry with the biometric technology that enables the U.S. government to establish and verify your identity when you visit the United States
Vulnerability	A flaw or weakness in a product and/or system's design, implementation, or operation and management that could be exploited to violate the system's security policy.
Watch list	Biometric database / list consisting of biometric data that has to be used for an identification purpose. Watch list may be a black of white list.
Web services	These are software applications running via the internet (as opposed to Client software installed on one particular platform). The main advantage is that they do not require any software installation on the user's computer. All what is needed is a web browser. Web Services work seamlessly across all platforms and all Operating Systems because they only interact with the web browser. The benefits for the users are numerous * According to W3C: A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically an XML based format named WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards. * When mentioned in the plural ("Web services", the term often refers to an interface for a service oriented architecture (SOA), in which Web-based applications dynamically interact with other Web applications using open standards that include XML running over HTTP, UDDI and SOAP. Such applications typically run behind the scenes, one program "talking to" another (server to server). Microsoft's .NET and Sun's Java System (J2EE) are the major development platforms that natively support these standards

4.3. Standards

- ISO/IEC JTC[2] 1 SC[3] 37 "Biometrics", which deals exclusively with biometrics standardization includes several Working Groups

  WG1 Harmonized biometrics vocabulary
  WG2 Biometric Technical interfaces
  WG3 Biometric data interface formats
  WG4 Profiles for biometric applications
  WG5 Biometric testing & reporting
  WG6 Cross jurisdictional and societal aspects

- ISO/IEC JTC 1 SC 27 "IT Security Techniques", which deals with specific questions on securing biometric data and on general IT security topics,
- ISO/IEC JTC 1 SC 17 "Cards and Individual Identification" deals in Working Group 3 "Machine Readable Travel Documents" with standardization of passports, ID cards, visa, and other travel documents in cooperation with the International Civil Aviation Organization (ICAO),
- ISO/IEC JTC 1 SC 17 also deals in its Working Group 11 "Application of biometrics to cards and individual identification" with topics such as comparison of biometric data on a smartcard;
- ISO TC68/SC 2 "Security management and general banking operations" offers guidelines that have already been applied to large scale heterogeneous banking systems and might also be useful in the context of biometric technology

Standards:

ISO/IEC 19794-1 Biometric data interchange formats
ISO/IEC 19794-2 Finger Minutiae Data
ISO/IEC 19794-3 Finger pattern spectral data
ISO/IEC 19794-4 Finger Image Data
ISO/IEC 19794-5 Facial image Data
ISO/IEC 19794-6 Iris image Data
ISO/IEC 19794-9 Vascular image Data
ISO/IEC 19794-10 Hand geometry silhouette data
ISO/IEC 19785 CBEFF Common Biometric Exchange Framework format
ISO/IEC 19784 BioAPI
ISO/IEC 19795 Biometric testing and reporting
Part 1: Evaluation of biometric systems in terms of error and throughput rates
Part 2 Technology and scenario evaluation
Part 3 Modality specific testing
Part 4 Interoperability and performance testing

ISO 24708, under development: syntax, semantics and encoding of messages for BIO APIs

[2] Joint Technical Committee
[3] SubCommittee

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, promoting Smart Security standards and continuously improving quality security applications and services.

Eurosmart members are suppliers and manufacturers of smart cards, semiconductors, terminals, equipment and technology for Smart Secure Devices, system integrators, application developers, issuers, associations, laboratories and independent experts. They work in dedicated working groups (communication, marketing, security, electronic identity, new form factors, and prospective emerging markets).

Eurosmart is acknowledged as representing "The Voice of the Smart Security Industry" and is heavily involved in political and technical initiatives as well as research and development projects at the European and international levels.

For more information, please visit www.eurosmart.com

EUROSMART
Rue du Luxembourg 19-21 – B-1000 Bruxelles
Tel. (+32) 2 506 88 38 / Fax. (+32) 2 506 88 25
Email : eurosmart@eurosmart.com

10.7. Annex 7 - Presentations

BEST Network

Working Group 1

Immigration and Border Control

Achievements so far

Deliverable	Date	Status
D1.1: Inventory of biometrics enabled registration processes for immigration purposes	06/2010	Delivered; first summary of existing implementations; was planned to be updated during 2011
D1.2: How EU policy requirements shall translate into daily business	05/2010	Delivered; summary of legal and technical issues related to the introduction of biometrics at borders
D1.3: Existing and developing use cases where biometrics is part of border control		Skipped in favour of new focus

The case of WG 1

- This is working group “1” in its literal sense !
- However, stronger involvement of governmental stakeholders still to be established and crucial for having any impact
- Information on implementations still considered as highly sensitive, in particular with regard to problems
- BEST mission obviously conflicts with information policy of “some” European member states

New

Mission Statement for WG1

- To understand the critical issues of biometrics related to the context of ~~border security~~ e-passports (and visa?)
- To identify ~~and assess~~ technological and conceptual gaps
- ~~To propose and communicate~~ Facilitate discussion about measures to address the issues ~~and gaps after consultation~~ with relevant stakeholders

Potential issues for WG1

- Biometric spoofing of face and finger
- Conceptual gaps of ABCs (handling of passports, one and two step approaches, etc)
- Conclusions from BIODEV on biometrics in VIS
- Ageing problems (and how this affects efficiency)
- Acceptance and convenience
- Data protection
- . . .

IDEAL IMPLEMENTATION OF AN APPLICATION

BEST Network – WG2

EPINETTE Olivier
REYES Daniela
DORIZZI Bernadette
TZOVARAS Dimitrios

September 2011

TELECOM & Management SudParis

AGENDA

- OBJECTIVES
- METHODOLOGY
- DIMENSIONS
- IDEAL SCENARIO
- HYPOTHESIS
- DISCUSSION

OBJECTIVES

Outline the ***ideal*** scenario for an application to be implemented, detailing steps and requirements.

Identify all necessary participants based on the applications previously analysed in D2.1 and D2.2. Applications restricted to: time and attendance - access control, biometric payment, video surveillance, (context for smart environments)

Provide a set of recommendations based on the gaps found for further and continuous improvements

OBJECTIVES

METHODOLOGY

Explanatory research

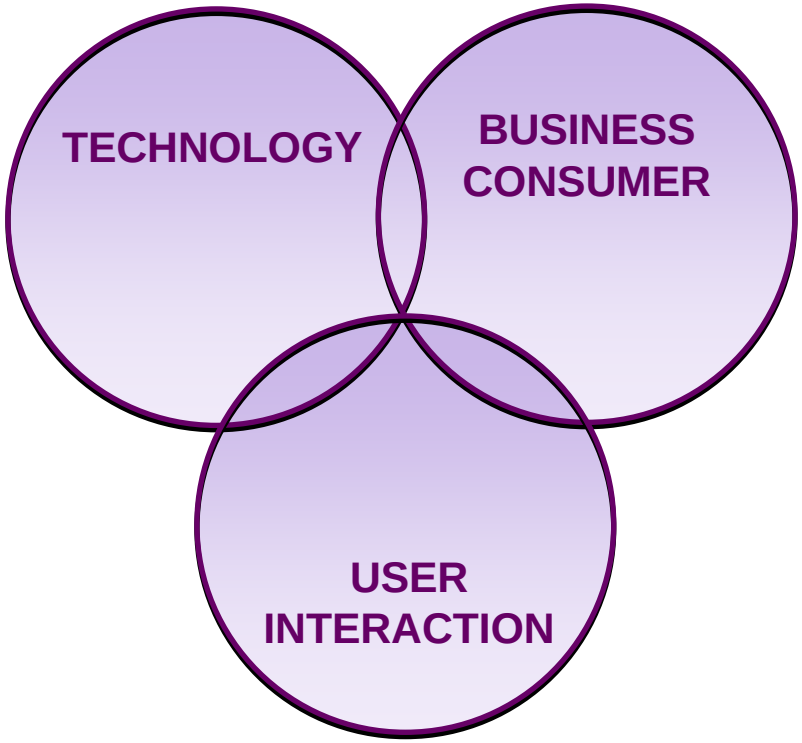
- Desk research
- Qualitative research

D2.3: Emerging applications for biometrics: opportunities and threats

OBJECTIVES

METHODOLOGY

DIMENSIONS



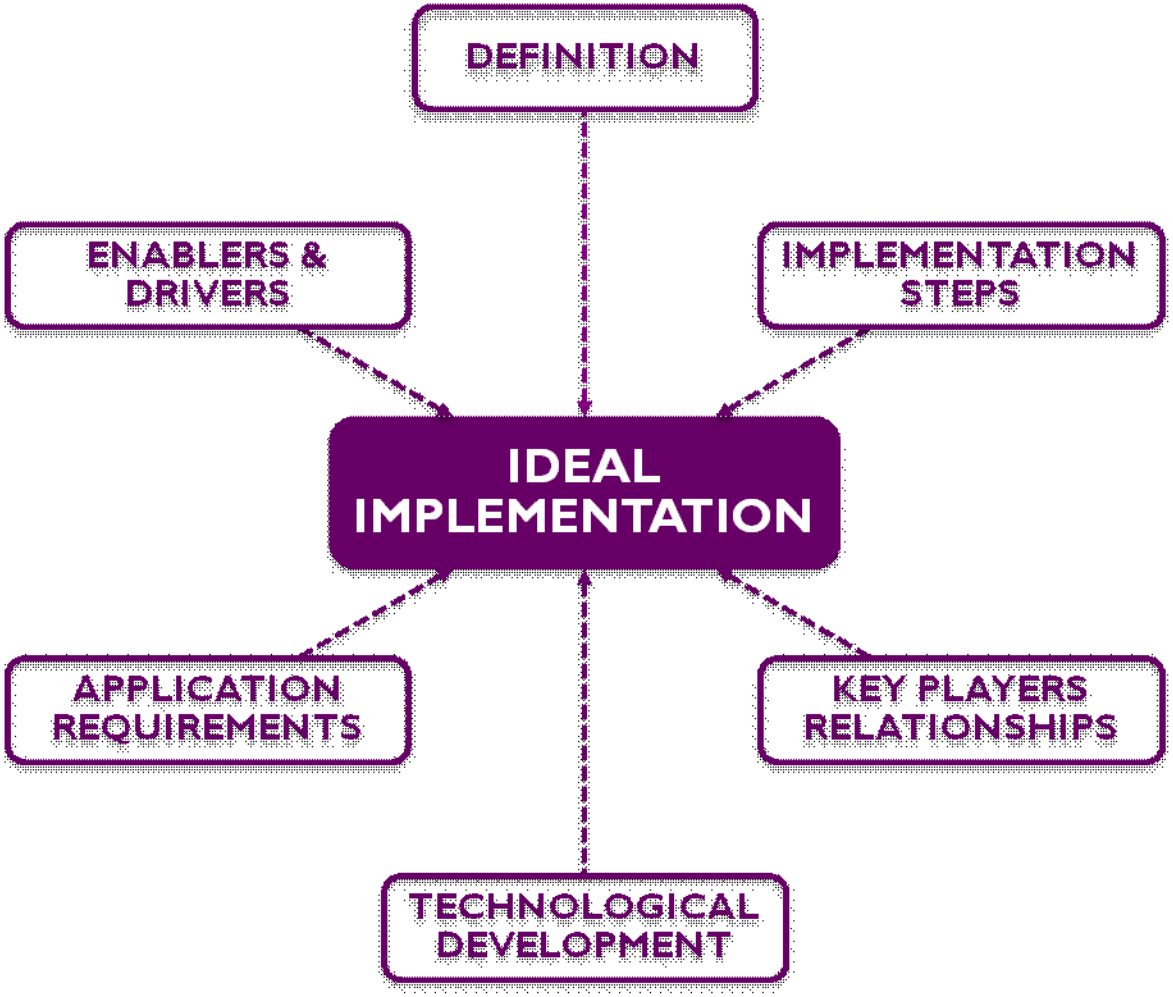
OBJECTIVES

METHODOLOGY

DIMENSIONS

“IDEAL SCENARIO”

“IDEAL SCENARIO”



HYPOTHESIS

DEFINITION

- BUSINESS FUNCTIONS TO BE PERFORMED
- CONTEXT
- SCOPE
- R.O.I.
- ORGANIZATION OBJECTIVES & GOALS
- ADDED VALUE OF INTRODUCING BIOMETRICS TO THE PARTICULAR APPLICATION

APPLICATION REQUIREMENTS

- USER FRIENDLY
- TECHNOLOGY PORTFOLIO CONGRUENT COHERENT (NO DISRUPTION NOT PLANNED)
- STANDARDIZED APPLICATION
- FUNCTIONS REQUIRED
- SAFETY
- LEGAL ISSUES
- ROBUSTNESS
- LIABILITY AND HOW IT RELATES TO SAFETY AND ROBUSTNESS
- RELIABILITY
- SCALABILITY

(ADD_FEASIBILITY) TECHNOLOGICAL DEVELOPMENT

- STANDARDIZATION STILL GOING ON
- INDUSTRIALIZATION
- MASS-PRODUCTION
- NEW TECHNOLOGICAL DEVELOPMENT "EASILY" EMBODIED TO PRODUCT / APPLICATION

DISCUSSION

- Do we have the right dimensions?
- Do we need to add more?
- Are the items for each category well placed or should they be moved to an other one?
- Are any items missing in each category?
- Clearly show in the methodology what is specific for biometrics.
- Cross-check overlaps with WG4
- Create a quick scan feasibility tool out of our methodology. This tool could be used also from WG5.

BEST NETWORK

Biometric European Stakeholders Network

WG3
European RT and ABC

Driving to Convergence

Max Snijder

2nd Workshop, Darmstadt 15-16 September 2011

BEST NETWORK

Biometric European Stakeholders Network

Agenda

- D3.1 outcomes
- Observations
- Current developments in ABC
- Questions

BEST NETWORK
Biometric European Stakeholders Network

D3.1 outcomes - 1 -

Defenitions

ABC ‘Automated’ border control for the mass based on the e-passport (no pre-registration, free of charge)

RT Service based boder control for premium travelers based on a specific token or e-passport (pre-registration to a program, membership and fee based)

BEST NETWORK
Biometric European Stakeholders Network

D3.1 outcomes - 2 -

Ciritical success factors ABC/RT

- embedding in the new operations of border/ security control authorities
- systems interoperability
- user friendly, recognisable systems, limited instructions, simple to operate
- a clear business case
- integration in the overall aviation processes (IATA Simplifying Passenger Travel , Simplifying the Business)
- a well defined and elaborated public/private partnership (airports, airlines, governments)

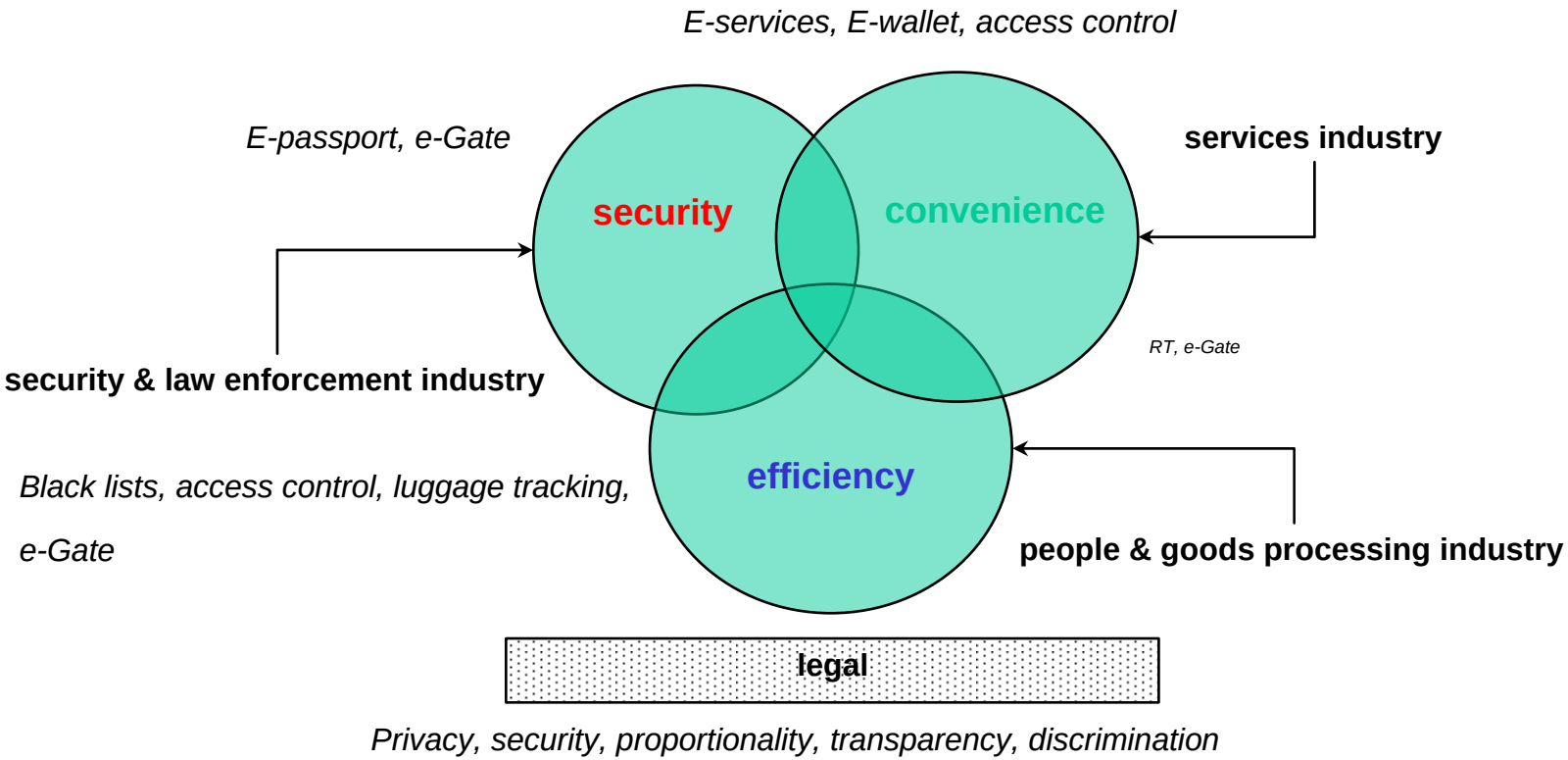
BEST NETWORK
Biometric European Stakeholders Network

D3.1 outcomes - 3 -

Biometrics business drivers at airports

- more efficient border control process
  airport, airline
- more convenient border crossing experience
  passenger, airline
- higher level of security
  government, airline

Strong interconnected interests with stakeholders


E-services, E-wallet, access control
E-passport, e-Gate
services industry
security
convenience
RT, e-Gate
security & law enforcement industry
Black lists, access control, luggage tracking,
e-Gate
efficiency
people & goods processing industry
legal
Privacy, security, proportionality, transparency, discrimination

BEST NETWORK
Biometric European Stakeholders Network

Observations

- little considerations to privacy/data protection (De Hert / Kindt)
- no European approach
- Frontex Best Practice Guidelines first attempt to harmonize ABC in EU
- ABC gates to facilitate RT and immigration (VIS)
- integration bordel control & flight information (DCS)
- traveler is known before entering airport
  (profiling, IATA Check Point of the Future)
- ABC to provide id-credential for other processes (e.g. boarding)
- integration ABC and RT (e.g. Privium & NoQ at SPL)
- biometrics as supporting technology
- perception of automation, supervision at the back ground
- no consistent quality/integrity of e-passport biometrics (WG1!)
  (application - and capturing process)
- ongoing studies on 13th data group e-passport

BEST NETWORK
Biometric European Stakeholders Network

Comments by WG7

(De Hert / Kindt)

- little considerations to privacy/data protection (De Hert / Kindt)
- need for clear and detailed description of data collection
- defining legal obligations for each of the specific data processing operations.
- different national data protection legislation will apply
- processors, controllers and receivers should be clearly defined
- need to define specific purposes, re-use of data and legal basis
- collected data should be kept to a minimum
- information, transparency and rights to the data subjects
- use and interaction with other data collections
- Privacy by Design

BEST NETWORK
Biometric European Stakeholders Network

Developments

self service (r)evolution

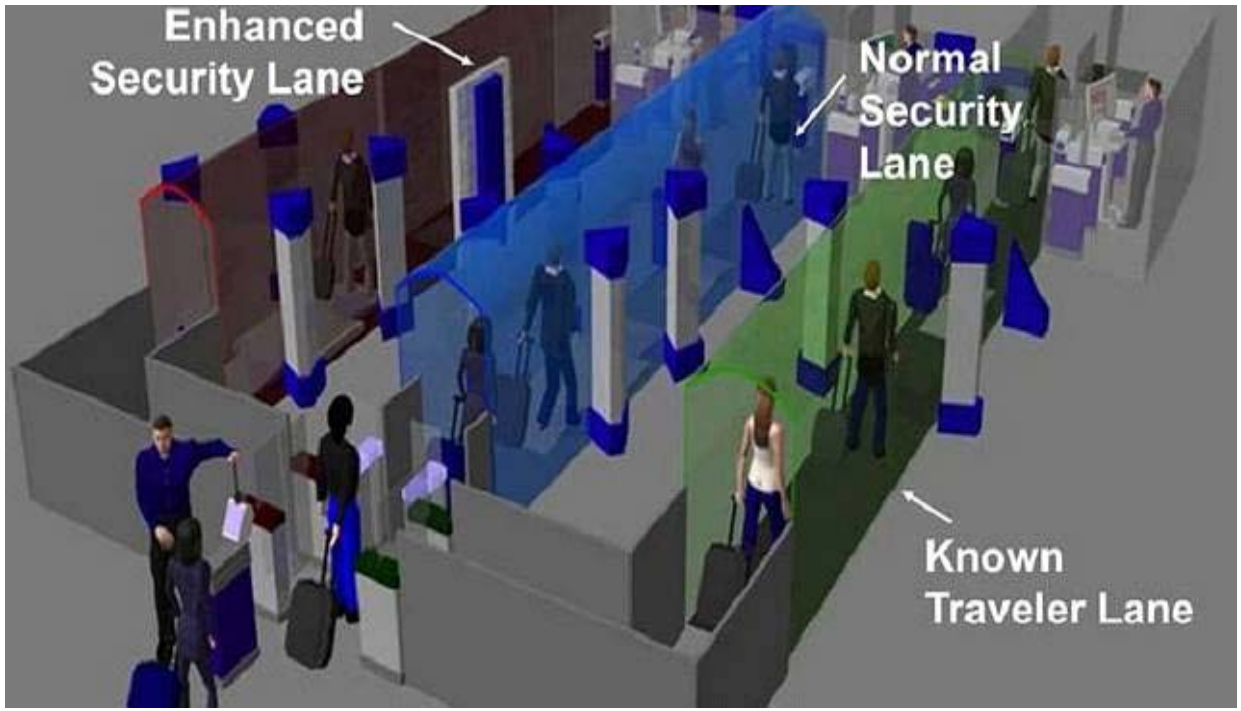
internet check-in, mobile check-in, kiosk check-in, self-tagging, baggage self drop off, transfer kiosk, self-boarding, self-recovery ...

« By 2020, 80% of global passengers will be offered a complete self-service suite based on industry standards »

BEST NETWORK
Biometric European Stakeholders Network

Developments

Check point of the Future (IATA)



BEST NETWORK

Biometric European Stakeholders Network

BEST NETWORK
Biometric European Stakeholders Network

Questions

- is there European leadership; who could be the leader (Frontex?)
- is a European approach needed
- how can quality/integrity of the e-passport be harmonized in EU
- is there a standardization process on ABC going on (e.g. CEN, ISO)
- what are the (potential) consequences of merging/combining police data with DCS data
- impact of integration bordel control & flight information (DCS)
- traveler is known before entering airport
  (profiling, IATA Check Point of the Future)
- ABC to provide id-credential for other processes (e.g. boarding)
- integration ABC and RT (e.g. Privium & NoQ at SPL)
- biometrics as supporting technology
- perception of automation, supervision at the back ground
- no consistent quality/integrity of e-passport biometrics (WG1!)
  (application - and capturing process)

BEST NETWORK

Biometric European Stakeholders Network

THANKS

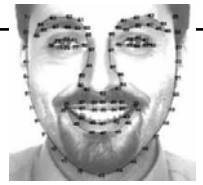
Q & A

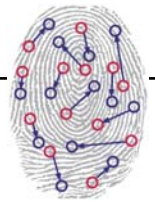
Training and Education

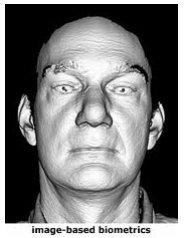
Testing and Evaluation

Legel, Ethics, Socio-technical issues

other issues?







eID and electronic Services

BEST-NW WP4

BEST Workshop, 14-15
September 2011

H. Leitold

Agenda

1. **Original Objectives**
2. **Deliverable Status**
3. **Revised Objectives**
4. **Core Content so far**
5. **Discussion**

BEST WP4 Objectives

- WP4: eID and Electronic Services

  Until now biometrics are mainly being associated with large identification systems in the criminal and law enforcement environment. This WG will look into the **requirements for using biometrics in electronic environments** from the perspectives of the end user (citizen), governments and commercial service providers, which are not yet fully understood, neither by governments that are currently implementing their national eID schemes based on a national identity card, nor by the public. However, in order to make use of the specific benefits that biometrics can provide, this WG will focus on the requirements for using biometrics in digital environments including the aspects of security, convenience, privacy, cost/benefit and adoption.

- Co-chaired by Graz University of Technology and RAND Europe Cambridge
- Contributors: European Biometrics Group, ANCITEL, EUROSMART AISBL, Università degli Studi Roma TRE, Fraunhofer-Gesellschaft

Deliverable Plan

- D4.1 State of art on Biometrics in eID
  - Delivered
  - Set the Scope including PESTLE analysis
- D4.2 Business case for biometrics in eID and el. service
  - Found not many within the defined WP4 scope
  - Delivered and still received quite positive remarks in the last review
- D4.3 Future proofing biometrics enabled eID and e-services
  - At least that was the original title
  - We refocused in the revises Work Plan
  - To be delivered **23rd December 2011**

D4.3: Revised Objectives

- D4.3 Objectives “Biometrics in eID and eServices final report”:
  - To put the core findings of D4.1 and D4.2 to debate in the networking exercise
  - To collect opinions in conference calls and the face to face workshops
  - To combine D4.1 and D4.2 together with networking outcome to a final report D.4.3

D4.3: What to be done

- Expected Content of D4.3:
  - D4.1 and D4.2 form a solid basis and already anticipated the contents that originally has been envisaged for D4.3 (i.e. policy aspects have been dealt with in the PESTLE analysis and requirements have been elaborated on in D4.2).
  - D4.3. **shall not produce substantially new content**. **but scrutinize the existing material** in the **networking phase** and report on the result.

Expectations for today

- Lively discussion on the existing D4.1 and D.4.2
- You all have read them …
- … in case not, a few core parts follow. Pick up controversial thoughts, jump in, shout and discuss …..

D4.1 Scope definition

D4.1 considerations on scope

- Electronic service
  - We assume a Internet remote access environment
- Usage in public sector vs. private sector
  - Who is providing the electronic service
  - Different assumptions on user's trust may apply
- Where is the biometric info storage taking place
  - In the user's domain?
  - In the e-service domain?

Public sector, attended environment

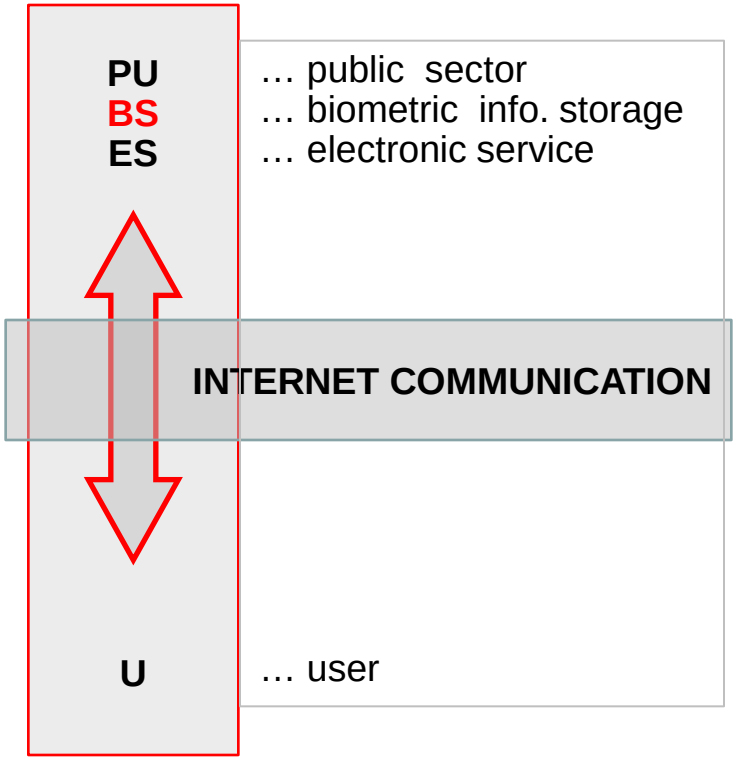
PU
BS
ES
official
U

... public sector
... biometric info. storage
... electronic service

... user

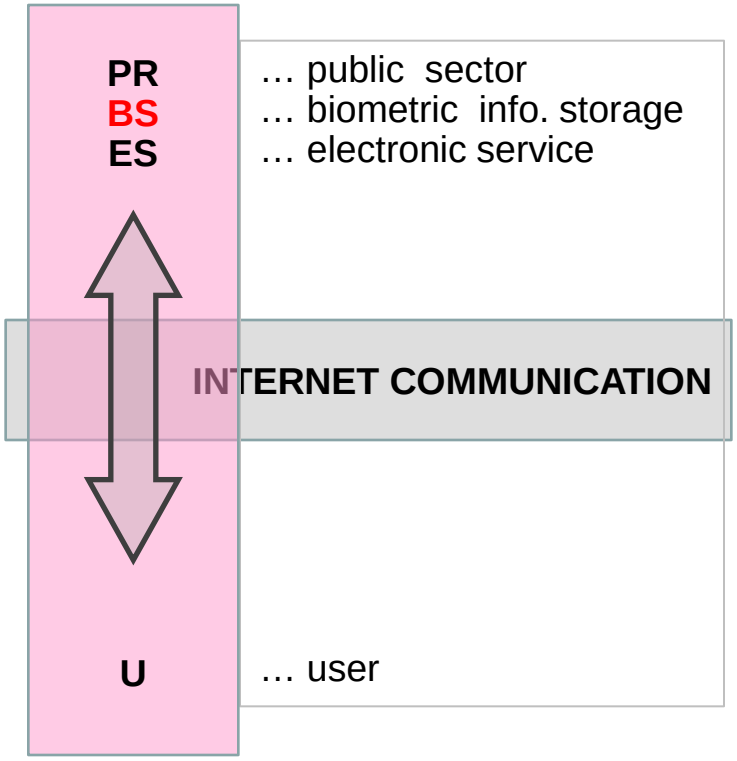
- User, biometric storage, and service in same domain
  - Typical border control scenario with face-to-face checking
- No remote access e-services
  - Out of scope

Public sector with biometric info storage



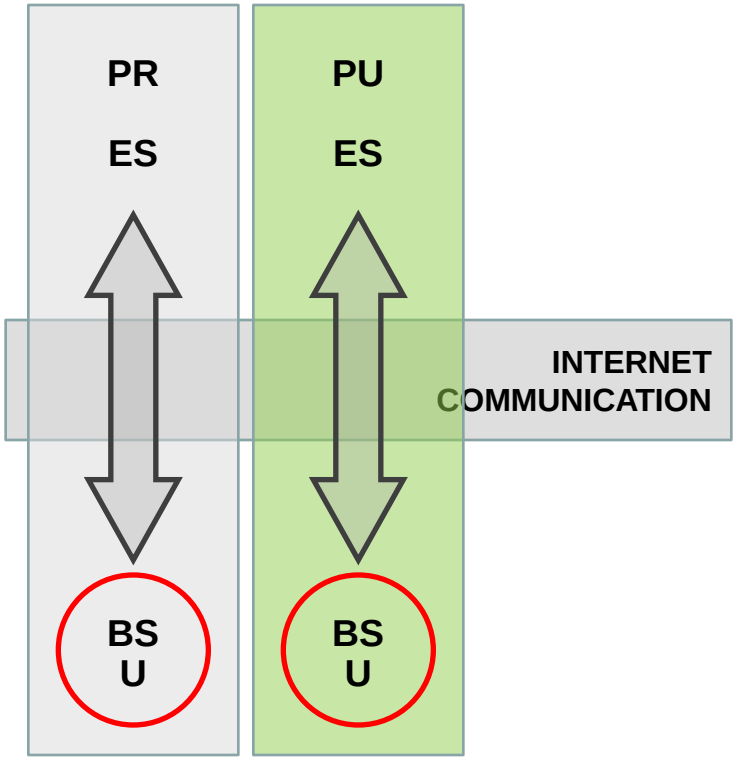
- Public sector storing biometric info in its domain
- Remote access via the Internet
- Security & data protection concern
  - Kept out of scope

Private sector with biometric info storage



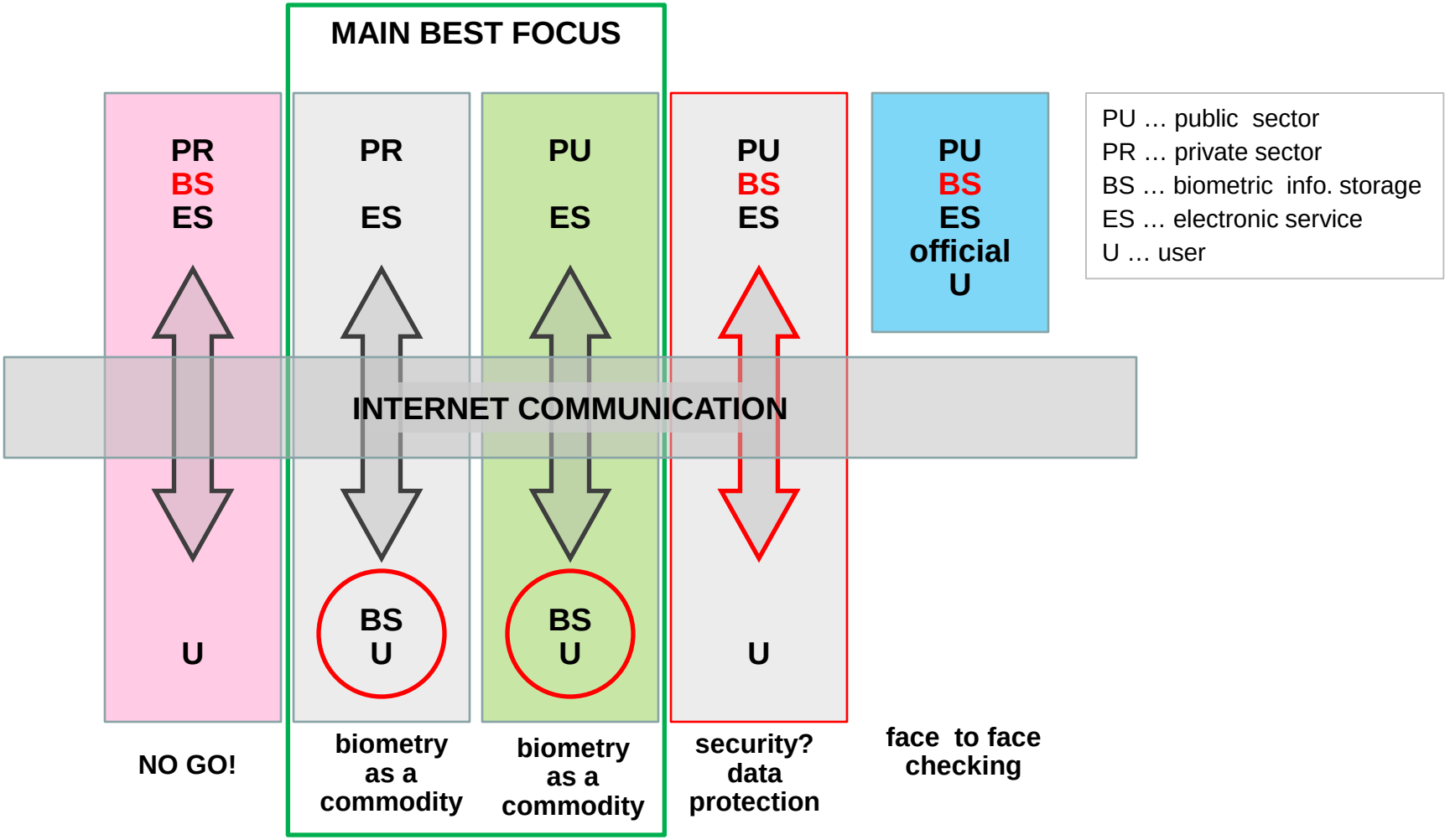
- Public sector storing biometric info in its domain
- Remote access via the Internet
- Security & data protection concern
  - Considered a no-go

Public/private sector with user storage



- Public or private organisation providing a service
- User holds the biometric inform.
  - On the PC, a token …
- Biometric as commodity

Overall scope



D4.1 PESTLE

Political

- Political acceptability hard to determine – narrow adoption so far (mainly air travel and borders)
- Increasing political focus on the ‘rights of the individual’
- Governments and public administrations may need to radically change to facilitate use of biometric data
- Large scale IT systems in the area of justice and home affairs
  - Visa Information System
  - 2nd Generation Schengen Information System (SIS II)
  - Biometric Management System

Social

- Fear of the unknown and the ‘surveillance society’
- Introduction of increasingly sophisticated privacy technology may be seen by the public as unnecessary
- But security breaches can be catastrophic for businesses and governments
- Question of inclusivity

Technological

- Current state of the art based around fingerprint, facial, retinal scans
- Degree of ubiquity of biometric infrastructure is important factor in adoption – for example the prevalence of laptops with fingerprint scanners is growing
- Form and specific biometric technology of any ubiquitous deployment will be a commercial decision, based on infrastructure cost and risk assessment.
- Backend technological developments will affect utility of biometrics, eg. cloud computing, homomorphic encryption

Economic

- ‘Derived demand’ – affected by demand for the underlying service and the availability, cost and effectiveness of substitute (non-biometric ID) technologies
- Supply side driven by R&D and linked to technological and socioeconomic ‘downstream’ development. ‘Value mesh’
- Market structure – distorting influence of patents on development and adoption of biometric technologies
- Externalities

Legal

- Legal uncertainty – rapidly changing picture
- A number of pan-European legal instruments may influence the use of biometrics
- European Framework for Data Protection and Privacy is evolving
- 1999/93 Electronic Signatures Directive – challenge and opportunity
- Private law – questions of accountability and liability

D4.2 Business Cases

Remote usage models

- Investigated ownership of data and sensor in 4 cases

eID	Biometric	
Ownership	data	sensor
Service Provider		
User	X	X

Scope as of D4.1

ATM	Biometric	
Ownership	data	sensor
Service Provider	X	X
User		

ATM

ePPs	Biometric	
Ownership	data	sensor
Service Provider		X
User	X	

Passport

	Biometric	
Ownership	data	sensor
Service Provider	X	
User		X

Security model

Understanding positives and negatives

- Compared scenarios with / without biometrics
  - For the details one might need to get into D4.2 itself
  - Input appreciated also after this workshop

With biometrics

		User	Provider
Positives	**Externalities**	• Reduced chances of identity being stolen • Reduced chance of error (false positives and false negatives) • Increased ...countability (esp.	• Less fraud • Greater confidence • Reduced regulatory impact • Less costs in dealing with security breaches • Reduction / avoidance of regulatory liabilities (fines) • Increased revenues (existing customers do ...e business for those ...urity as

Without biometrics

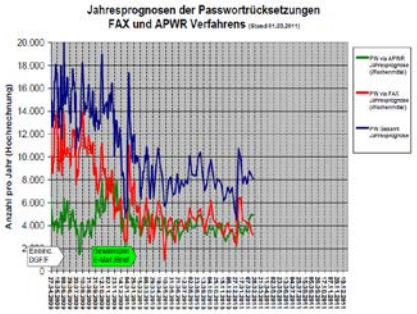
		Use...	
Positives	**Externalities**	• Convenience (mobility / device independence) • Many tools	(po... put off by ... authentication m... • Increased revenues (ex... customers do more business)
	Costs	• No investment in sensors	• Lower Capex/Opex for authentication
Negatives	**Externalities**	• Increased risk of identity theft	• Increasing identity theft and cyber-attacks on less secure authentication • Loss of customer...

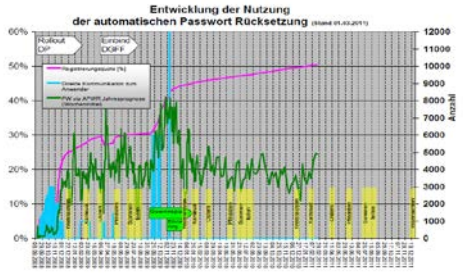
Tried to foster controversial discussion

- Why *do* biometrics fail?
  - Security and privacy concerns
  - Perception of biometrics
    - “here is the technology; what shall we do with it?”, vs.
    - “this is the problem - this is how technology should solve it“
  - (Un)clear business need
    - What is the reason of applying biometrics: adding security or making the process more convenient?
  - Operational considerations
  - Standardisation

Finally found a few business cases

1. Password reset (Deutsche Post)





2. Throwaway biometric – boarding card (SAS Airlines)
3. Voice authentication for pension plan (Philippines)
4. Remote tele-monitoring for healthcare (Clalit Health Services)

Source: Medic4all[21]

D4.2 Conclusions

- Moving the debate forward …
  - softer or ‘weaker’ biometrics to re-shape the debate away from a focus on narrow identity orientated uses? (e.g. telemonitoring)
  - positive convenience on user side should be promoted more clearly
  - Understanding the business case not a problem of the technology, but r that there remains little public robust actuarial data on security cost benefits which would inform better decision-making
  - admitting the failure of inter and intra-organisational communication may help to stave off the desire for commissioning yet another large technology project involving a centralised database with all its risks
  - value of ‘mutual biometrics’ as a way to help build trust between the data subject and the entity or agency requesting such data. (establish a mutual platform of trusted interaction between the data subject’s personal space and technology enabled infrastructure)

Food for discussion?

WG5 Skills, Training and Education

Best Network
Darmstadt, Fraunhofer Institute,
September 16 2011
Farzin Deravi (WG5) and Juliet Lodge (WG5 & 7)

WG5 Skills, Training and Education

- In the beginning WG5 produced an outline of the available biometrics-related training and education provision in Europe
- Workshop in Kent identified weaknesses & compared EU with US provision
- GAP : NEEDS NOW a coordinated action plan to address needs and gaps regarding training and education

What are the Skills and Training needs for

- Passports and public administrations (WG1)
- Emerging applications (WG2):
  - time and attendance / access control
  - biometric payment
  - video surveillance
- European ABC and RT (WG3)
- Biometrics and e-ID: national eID and e-services (WG4)

Needs for Learning on the job?

- Need for certainty in terms of recognised quality standard of diplomas or certificates or awards given to people following training
- Need for clarity regarding casual v. credible authoritative certification quality standards
- Need to differentiate requirements between

➢ System level and Operative level

➢ Agreed that generic training not feasible

Authoritative training problem areas

- Private Public Partnership arrangements v Quality institute provision
- Train the trainers : integrators in the centre could have generic training
- Face to face training : eg of the Bundespolizei on how to handle and control interaction
- Little standardisation of components bought for German agencies compared to UK, Portugal and Austria

Target training

- Question of adequacy of knowledge base and updating : people, including experts, do not know that they don’t have sufficient contemporary training and knowledge
- Target training towards specific client groups
- Training must include knowledge transfer regarding the purpose and policy context

The trap of legacy use cases

- Need to show importance of using specific systems as opposed to grasping inappropriate legacy systems designed for different purposes (eg fingerprint forensics v. security application of biometrics)
- The false hopes inferred from biometrics as a panacea

(eg Should border biometrics have a kitemark?)

Does the EU need an independent biometrics academy/body?

Tasks:

- Awareness building of the realities of biometric applications
- Overview of academic curricula availability
- Structured school able to deliver periodic courses
- Develop appropriate training materials and resources

What resources might be developed?

- Certification for FP and face?
- Combined biometrics?
- Checklist/guidelines for evaluating a system
- Identification of convergence processes and models?

Gaps to be addressed

- Gaps in provision at university level owing to swift introduction of biometric outstripping slow pace of adaptation in many university degree programmes
- Insufficient number of skilled University qualified people at the technical level
- Addressing diverse understanding of commonly used terms that different sectors use and understand differently (eg interoperability)

Future BEST Roles?

- **How can these needs be addressed?**
- **What common and coordinated measures may be taken to enhance the level of skills and education in the field of biometrics technologies and services?**
- **Should there be a biometrics group modelled on the initiative in July 2011 by Net security firms who supported a new group seeking to provide cybercrime training for law enforcement officials as part of a wider fight against cybercrime. McAfee and Trend Micro pledged support for the fledgling International Cyber Security Protection Alliance (ICSPA).**

Conclusions : meeting needs

- Train the trainers ++++ Langs in EU27+
- Need for training at system level **and policy level** but less so at operating level
- Need for training so people can better assess their systems (link to WG3)
- Product specific training plus generic intro to biometrics : at the moment the client seeks product oriented support rather than more training

CONCLUSIONS

EU needs an authoritative, informed, credible and independent body to :-

- provide EU views and training related to EU policy priorities and context
- Address ignorance and misunderstanding among procurers, officials, policymakers and users at all levels of what the ICTs and biometrics can and can‘t deliver

NEXT STEP

Pre-conference workshop suggested topics

- Conformity standards for performance quality and processes; how ID checked etc
- Designing a process/document at municipal level
- Convergence

Parallel stream?

- Biometrics in policy context
- Privacy Impact Assessment

BEST NETWORK

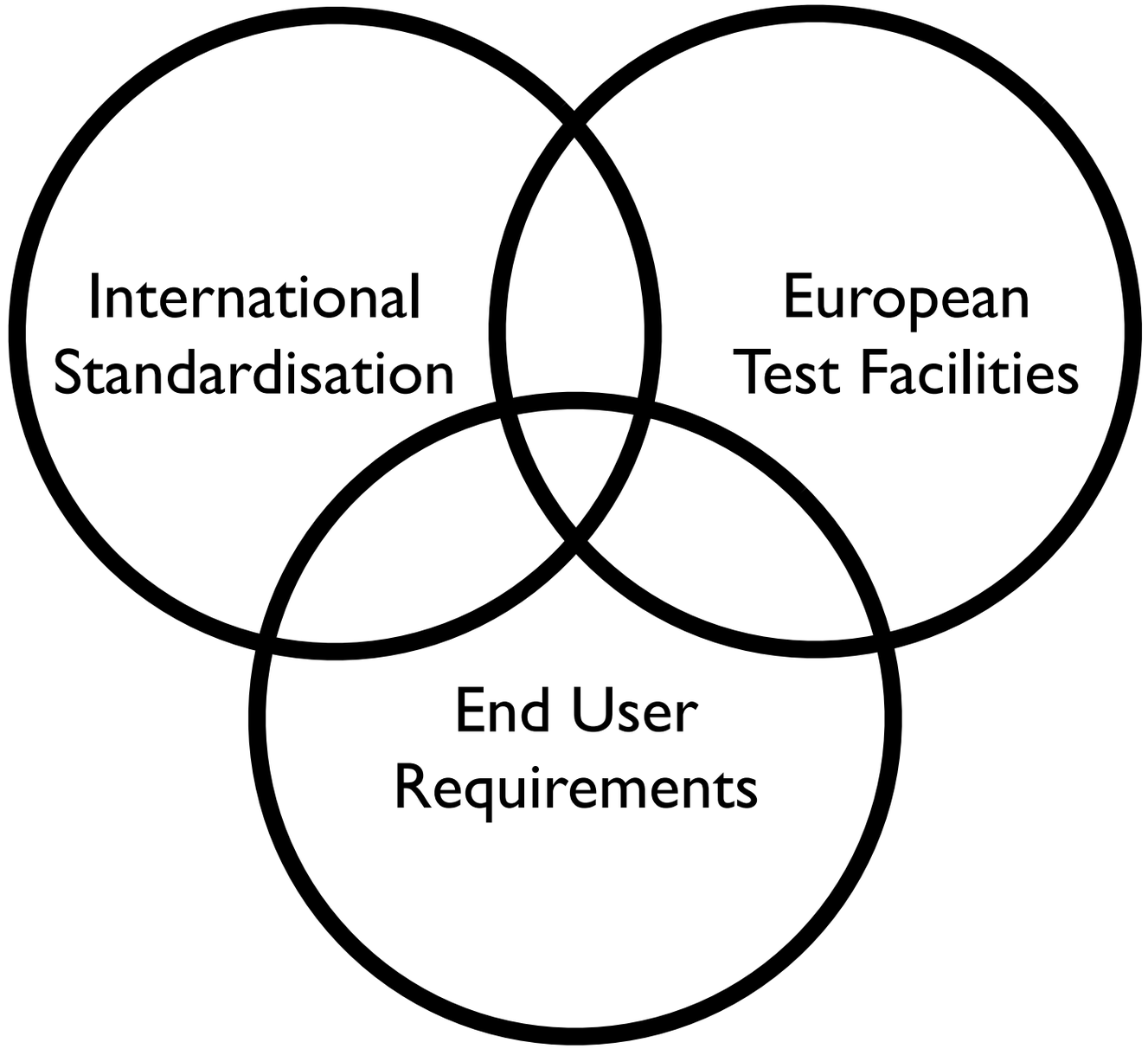
Biometric European Stakeholders Network

WG6 – Testing & Certification

2nd BEST Network Workshop, Darmstadt
September 16, 2011

Fraunhofer

Objective



BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

D6.1 – Inventory of Testing & Certification Institutions in Europe

- Inventory of standards related to biometrics and to evaluation of biometrics
- Description of accreditation and certification process in selected countries
- Inventory of evaluation and testing institutions
- Issues detected
  - Quality testing of image quality for fingerprints and facial images
  - Harmonised European certification process and responsibility

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

D6.2 – Application Scenarios, respective Standards and Evaluation Schemes

- Not an inventory of all biometric standards, but which biometric standards in specific application scenarios (from WG1, 2, 3, 4) can be tested against (e.g. for conformance, performance, usability etc.).
- Take standards inventory input from CEN/ISSS FG-Biometrics report
- Due M18

Partners and Liaisons

- *Fraunhofer* (WG 4)
- *Joint Research Center*
- DAON
- NPL
- Gjøvic University College
- University Carlos III Madrid
- Morpho (WG 1)
- Secunet Security Networks (WG 1)
- Center for research and Technology Hella (WG 2+3)
- Group des Ecoles des Télécommunications (WG 2)
- Universitá degli Studi Roma TRE (WG 1+4)
- European Biometrics Group (WG 1+3+4)

D6.3. Summary of existing biometric evaluation methodologies

- D6.3. Summary of existing biometric evaluation methodologies, not just focused on security
- Due M24

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

D6.4 – Inventory of existing tests and test results

- Will tie back to the application scenarios of D6.2. Snap-shot of test results.
- Will also maintain list of open issues on our Wiki. For example, the issue of a sequestered distributed European testing database
- Due M24

D6.2 – The assessment of selected application scenarios on their relevant standards and evaluation schemes

- Application scenarios in scope
  - Access control
  - Automated Border Control Systems
  - Border Control Equipment
  - Passport Enrolment Process

D6.2 – The assessment of selected application scenarios on their relevant standards and evaluation schemes

- Access control
  - International standards
  - National Evaluation Schemes
    - Level of spoof resistance
    - List of approved and certified products
  - Includes time and attendance control

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

D6.2 – The assessment of selected application scenarios on their relevant standards and evaluation schemes

- Automated Border Control Systems
  - FRONTEX Document
  - ABC Best Practice Guidelines
  - Harmonised Schemes
- Are European Requirements on border control equipment elaborated?

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

D6.2 – The assessment of selected application scenarios on their relevant standards and evaluation schemes

- Border Control Equipment
- Passport Enrolment Process
  - Duplicate Enrolment Check
  - Quality and Security

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

D6.2 – The assessment of selected application scenarios on their relevant standards and evaluation schemes

- Application scenarios out of scope
  - AFIS
    - Proprietary
    - National Schemes
      - Only components can be evaluated
  - eID systems – no business case
  - Biometrics in surveillance systems – no specific requirements
  - Transaction and payment systems
    - ATMs with biometrics not deployed in Europe
    - Emerging, thus we do not really know the requirements
    - Open question: why is there no rollout in Europe but in Asia

Plans for 3rd workshop

- Invite Biometric Institute to give a talk on their approach on Vulnerability Analysis
- Invite Idiap research institute to give a talk on the FP7 project BEAT – Biometric Evaluation And Testing
  - Currently in negotiation
  - Topic SEC-2011.5.1-1 – Evaluation of identification technologies, including biometrics

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

Fraunhofer
IGD

Alexander Nouak
Dipl. Informationsw. (FH), Dipl. Betriebsw. (FH)

Abteilungsleiter
Identifikation und Biometrie
Fraunhofer-Institut für Graphische Datenverarbeitung IGD

Fraunhoferstraße 5 · 64283 Darmstadt
Telefon +49 6151 155-147 · Fax -499
alexander.nouak@igd.fraunhofer.de

BEST NETWORK

Biometric European Stakeholders Network

WG7

Ethics, legal and socio-technical aspects

Participants

CSSC (Chair)
University of Leeds (Co-chair)
University Tilburg TILT (Rapporteur)
Rand Europe
EBF
Independent Centre for Privacy Protection Schleswig-Holstein
Universiteit Utrecht
EP Priv-ID

Objectives

BEST WG7 specifically deals with “ethical, legal and socio-technical aspects” that shape biometric responsible innovation. Trough the BEST Network, WG7 seeks to facilitate and structure European and international conversation in this sensitive policy area. As stated in BEST DoW, “the objective of WG7 is to incorporate ethical and legal reflection and conversation directly into the industrial and policy matrix”.

Deliverables

D7.1 Biometrics in Europe: inventory on politico legal priorities in EU27 Time 6

D7.2 Inventory on Privacy and Data Protection issues in biometric applications Time 12

D7.3 Overview of Ethical, Social and Policy Implications of Biometrics Time 24

Main Conclusions -1-

- Potentially risky is the **lack of understanding** at the political level about an unthinking adoption of a broad definition of biometrics
- The 2 rationales for the implementation of biometrics (**security and e-government**) have surprisingly been developed separately
- Concerns on **out-sourced data**
- **Interoperability** of systems is not only a technical concept

  In the EC Communication on Interoperability of European Databases it is stated that “interoperability is a technical rather than a legal or political concept”. From a mere technical perspective, the Stokholm programme’s committment to enhancing interoperability and cross border information exchange is undermined by the reality of diverse and incompatible ICT legacy systems and administrative procedures. However, the EDPS in 2006 noted that interoperability cannot be considered in a mere technical way, since it can often lead “to subsequent demands for less stringent legal requirements”.

Main Conclusions -2-

- *The **definition of biometrics** in Europe is expanding from the EU definition of a biometric as a digital expression of a given feature of a person, to include the US DHS definition that includes behaviour (data used for "intelligence" purposes). The wider definition makes the concept of biometric essentially arbitrary and contestable: if biometrics are to have legitimate uses, they have to be better specified, safeguarded and restrained. This is clear also in consideration of the fact that in Europe databases (EURODAC, SIS, VIS) have grown in size and scope.*
- This conclusion refers to the risk of **mission creep** resulting from the separation of policies related to ICTs used for security purposes and to ICTs used for other purposes (convenience).
- **EU data protection law** stipulates that personal data con only be transferred outside the EEA if it is protected as well there as it is within the EU.

D7.2 Main Conclusions

- There is an “enabling legal environment” for biometrics but it is **lacking normative content**: more specific rules needed addressing specific applications
- Regulations should address **the need for transparency** in biometric systems
- Regulations should address **the technical failures** and should determine the rights of data subjects in case of failure
- Need for **monitoring and certification procedures**
- Basic principles such as **informed consent, human dignity, equality**

D7.3 Goals

- The final deliverable by WG7 aims to deepen a **common understanding** of the main social, ethical and political challenges posed by biometrics, to integrate responses to these challenges into a wide range of **concrete proposals**, to contribute to the future development of this sensitive policy area

D7.3 Objectives

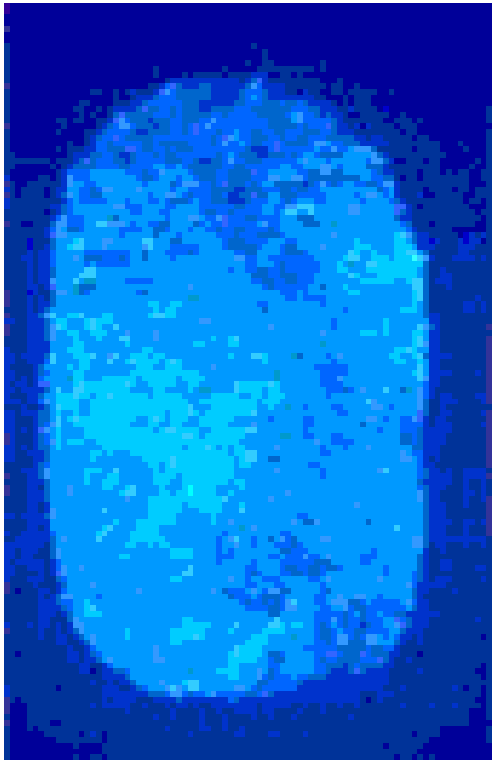
- **Reassess existing data** on biometrics in Europe from the ethical/legal/social perspectives and identify relevant issues that have not been included in D7.1 and D7.2
- **Prioritize policy and legal issues** at a European level
- **Provide benchmarks** or possible indicators of action
- Summarise considerations on the inclusion of ethical, social, cultural aspects in the ETP on **next generation biometrics**

D7.3 Timeline

- The first draft will be circulated among the BEST Network by the **first week of November**. Discussion on the first version will be carried out through email exchange, on the BEST Wiki Workspace, through conference calls within WG7 (if needed), through social network websites, and during the forthcoming BEST Network November workshop.
- **The final version will be submitted by December 23rd**.

Controversial and open issues

CONVENTIONAL BIOMETRICS



NEXT GENERATION BIOMETRICS

Benschmarking and indicators of Actions

Controversial and Open Issues

PRIVACY

DATA PROTECTION

Privacy

- What is privacy? Etymologically the word derives from the Latin *privatus*, past participle of *privo*, “I deprive”, “I cut away”. Privacy thus refers to the state of something that is separated, secluded from others. It refers to the state of being set apart, belonging to oneself, in contrast to the state of being public or common. According to the *Encyclopedia of Privacy*, it describes and demands “limits on the appropriation of others’ peaceful seclusion, personal information, intimate choice, and identities”.

Privacy as an Ethical Concept

- Privacy is an ethical concept. It involves claims about the moral status of the individual self, about its dignity and relation to others. Philosophers and legal theorists, for example, tend to talk about privacy in terms of ideas like ‘inviolate personality’. This moral core, it is argued, is the origin of social values such as autonomy, integrity, independence. Such values form a foundation for contemporary notions of human rights, citizenship and civic obligation in European public affairs.

Privacy as a Form of Knowledge

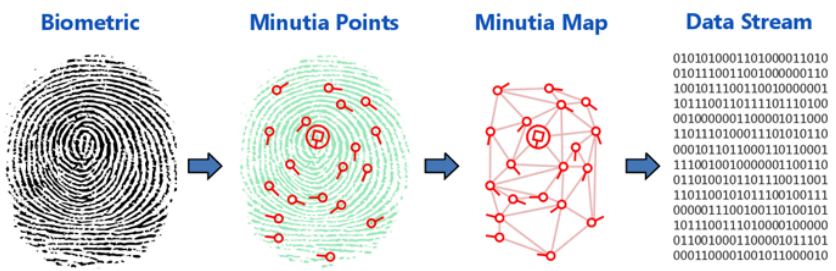
- In one manifestation, privacy is knowledge **— knowledge about the personal sphere of a person's life**. In a second manifestation, privacy is **meta-knowledge — knowledge about some intimate issue**, who knows what and where such information came from. In still a third, privacy **is power over or control of knowledge**.
- It concerns not only information about individuals, but also the right allegedly held by individuals to determine how information about them is used.

Personal Data

Articulation of the concept of personal data is a key historical event.

Data

- **1. Information** in raw or unorganized form (such as alphabets, numbers, or symbols) that refer to, or represent, conditions, ideas, or objects. Data is limitless and present everywhere in the universe.

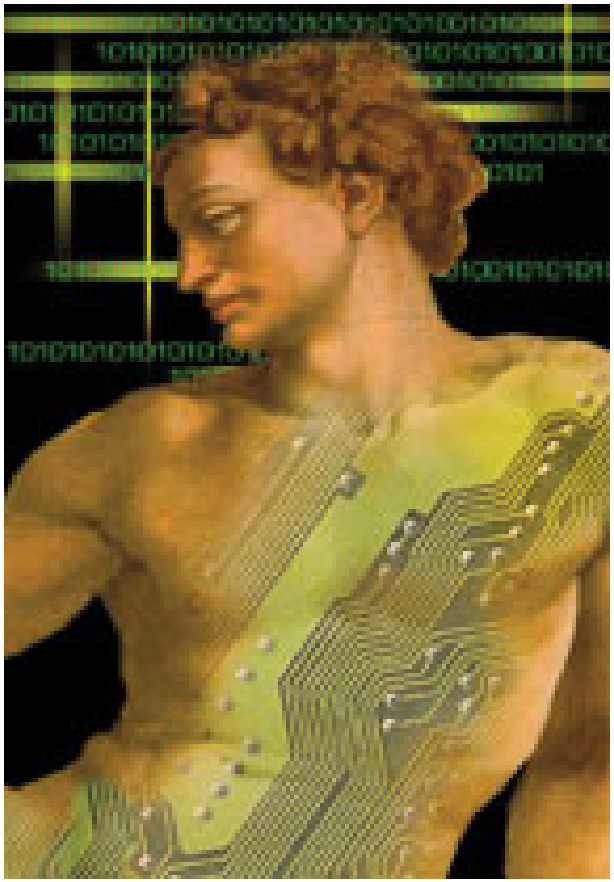


- **2. Computers: Symbols or signals that are input, stored, and processed by a computer, for output as usable information.**

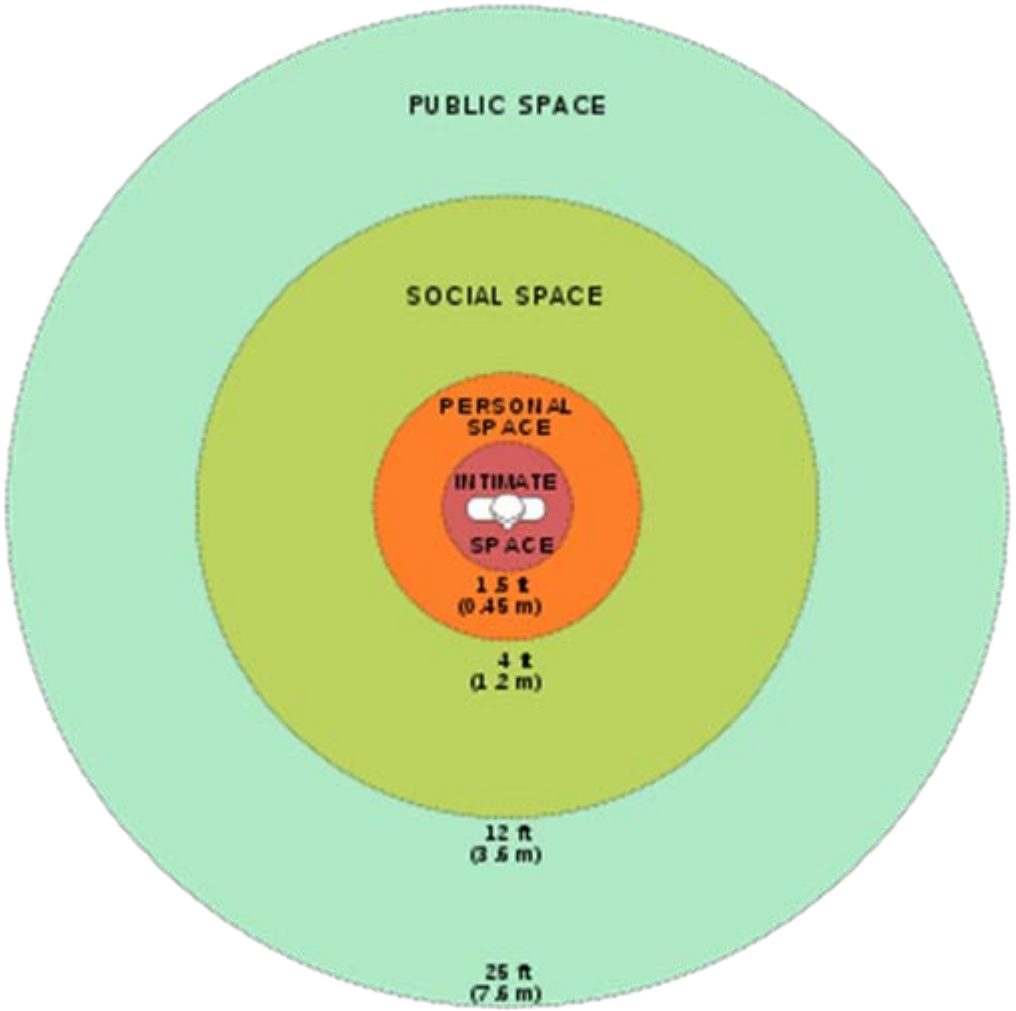
AQAAABQAAABUAQAAAQASAAMAOAAAAAAAUAEAAC1/G6Hq*OKQqstU1g6CufzsfhaU27Xs4NYa/df
1DDwtiQ*IciybaPlpEeJUz*mZfnXJuTF1w49YUkKPm9NBerAIZKDRaceVPkYsdCfEcnvmct9QcZlp*dWLCT
gltM6k3B6ab18Qlf4jqAq4hsZCki9gqJTA7CaglrBotSXqAfKCKG*sLKukWGWBm3QWTqRyHllqSsY2KzSD
mnEiyEwkJCggd8QaC76X5VoQUoZshazXfFC3t52*dSwSBVQgtg/Fk2Ck3CUu5mCy7q0Dy8DcQKcnJf0*
R/v/RYJik8LIE*2gq/mhTeh9F3NoPDxXyEDyb6Qqzl/YnRLPi57NrGfM9evl*PwclBYA7F*WR/1s7q2MGzlCTi
k9CmgicooElbjOKhMxMc/JFFhqd7zTvCu*W8yfeCniGRjjvY7SSIS1CdkO7dWQ8Eq8QQGh8rJWrQYoeA

Personal Data

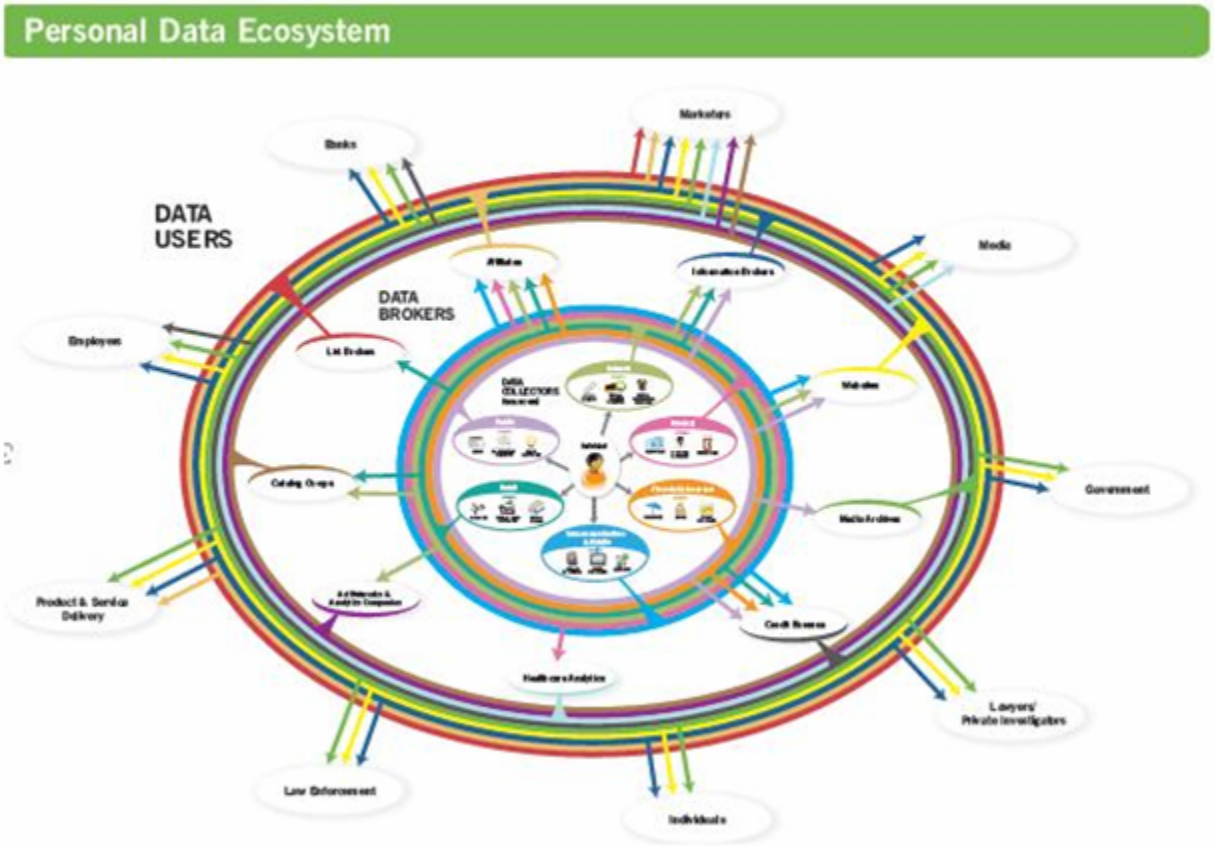
- It represents a shift from personal knowledge understood as **self-knowledge** (attained by introspection) to personal knowledge understood as **knowledge about the self** (attained by technical instruments). **Knowledge about oneself becomes detachable from the person and marketable.**



Privacy

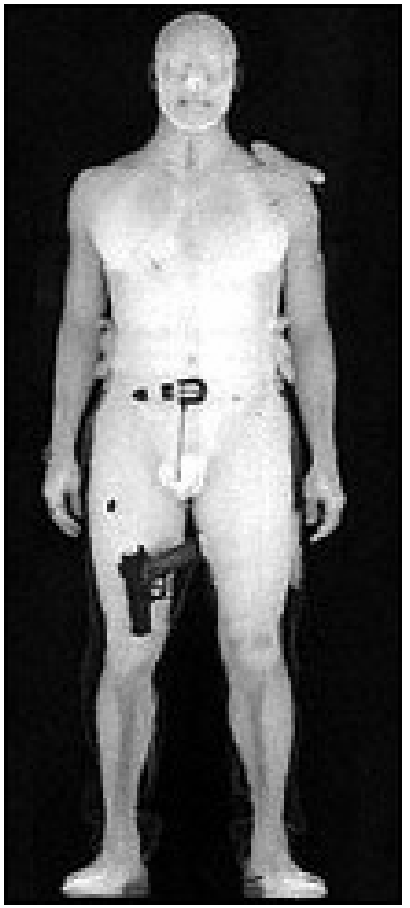

PUBLIC SPACE
SOCIAL SPACE
PERSONAL SPACE
INTIMATE SPACE
1.5 ft
(0.45 m)
4 ft
(1.2 m)
12 ft
(3.6 m)
25 ft
(7.6 m)

Personal Data



Personal Data, Privacy, Security

- Privacy gives way to personal data protection. **Data protection generates a technical conception of privacy**, now framed in terms of **risk management** and technical ability to protect or to penetrate the private sphere. Here security and privacy meet. **Privacy and security become counterweights in the same balance**.



Privacy and Security

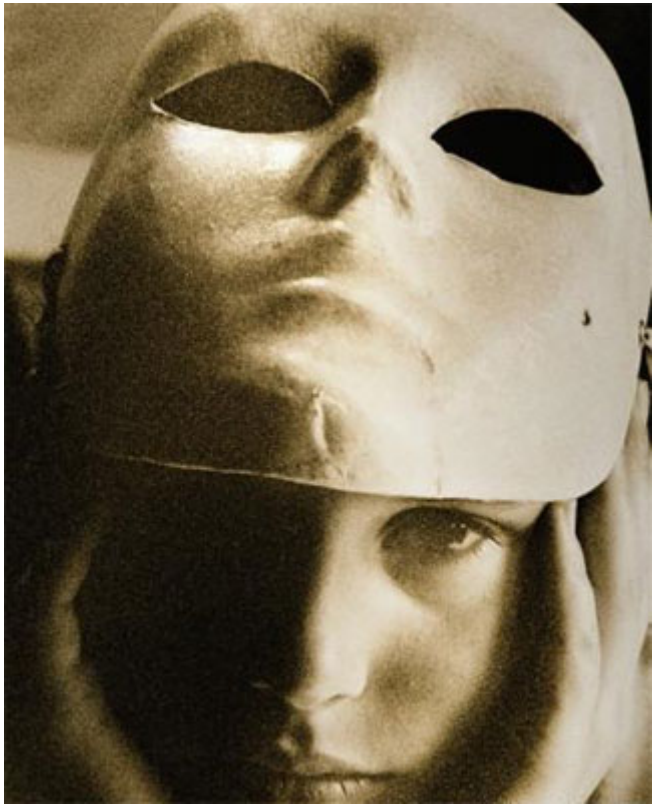
NUDITY

NAKEDNESS

BEST NETWORK
Biometric European Stakeholders Network

Protecting Privacy

- Privacy governance means to be ready to deal with all nuances and complexities of the concept of privacy, its relations with the idea of human **dignity, private sphere, intimacy, human flourishing**. Brief, privacy governance should be part of a wider strategy for protecting fundamental human rights at local and global levels.



Protecting Data -1-

- There is no data that can be truly protected in the online world. Everything has already been disclosed if it is online. Most electronic information is public or anyhow very easy to be unraveled and divulged. The best form of defense is then transparency.

Protecting Data -2-

- The race towards an increasing security at privacy expenses is a lose-lose situation, which is destined to produce at the end of the day less security and less privacy. The trade-off model of the relationship between privacy and security is obsolete in the online world.

BEST NETWORK

Biometric European Stakeholders Network

Current Calls in the

7th Framework Program for Research

2nd BEST Network Workshop, Darmstadt
September 16, 2011

Fraunhofer

FP7 Current Calls

- FP7 ICT Call 8
  - Call identifier: FP7-ICT-2011-8
  - Date of publication: July 20, 2011
  - Deadline: January 17, 2012, at 17:00 Brussels local time
- FP7-SEC Call 5
  - Call identifier: FP7-SEC-2012-1
  - Date of publication: July 20, 2011
  - Deadline: November 23, 2011 at 17.00, Brussels local time

FP7 ICT Call 8

- Call identifier: FP7-ICT-2011-8
- Date of publication: July 20, 2011
- Deadline: January 17, 2012, at 17:00 Brussels local time

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

FP7-ICT-2011-8 Challenges

- Challenge 1: Pervasive and Trusted Network and Service Infrastructures
- Challenge 3: Alternative Paths to Components and Systems
- Challenge 4: Technologies for Digital Content and Languages
- Challenge 5: ICT for Health, Ageing Well, Inclusion and Governance
- Challenge 6: ICT for a Low Carbon Economy
- Challenge 8: ICT for Learning and Ac to Cultural Resources
- Future and Emerging Technologies

FP7-ICT-2011-8
Challenge 1

- ICT 2011.1.1 Future Networks – (IP/STREP, NOE, CSA)
- ICT 2011.1.2 Cloud Computing, Internet of Services and Advanced Software Engineering – (IP/STREP, CSA)
- ICT 20011.1.4 Trustworthy ICT – (IP/STREP, NoE, CSA)
- ICT 20011.1.6 Future Internet Research and Experimentation (FIRE) – (IP, STREP, CSA)

FP7-ICT-2011-8
Challenge 3

- ICT 2011.3.1 Very advanced nanoelectronic components: design, engineering, technology and manufacturability – (IP/STREP, CSA)
- ICT 2011.3.2 Smart components and smart systems integration – (IP/STREP)
- ICT 2011.3.5 Core and disruptive photonic technologies – (IP, STREP, ERA-NET Plus, CP-CSA)

FP7-ICT-2011-8
Challenge 4

- ICT 2011.4.4 Intelligent Information Management – (IP/ STREP, CSA)

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

FP7-ICT-2011-8
Challenge 5

- ICT-2011.5.7 Support to the early implementation of the Joint Programming Initiative (JPI) 'More Years – Better Lives – the Challenges and Opportunities of Demographic Change' – (CSA)

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

FP7-ICT-2011-8
Challenge 6

- ICT 2011.6.1 Smart energy grids – (STREP, CSA)
- ICT 2011.6.3 ICT for efficient water resources management – (STREP)
- ICT 2011.6.7 Cooperative systems for energy efficient and sustainable mobility – (IP/STREP, CSA)

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

FP7-ICT-2011-8
Challenge 6

- ICT 2011.8.1 Technology-Enhanced Learning – (IP/STREP, NoE, CSA)

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

FP7-ICT-2011-8
FET

- ICT 2011.9.6 FET Proactive: Unconventional Computation (UCOMP) – (STREP)
- ICT 2011.9.7 FET Proactive: Dynamics of Multi-Level Complex Systems – (IP/STREP, CSA)
- ICT 2011.9.8 FET Proactive: Minimising Energy Consumption of Computing to the Limit (MINCON) – (STREP)
- ICT 2011.9.12 Coordinating Communities, Identifying new research topics for FET Proactive initiatives and Fostering Networking of National and Regional Research Programmes – (CSA)
- ICT-2011.9.14 'Science of Global Systems' – (STREP)

FP7-ICT-2011-8
Horizontal Actions

- ICT 2011.11.1 Pre- Commercial Procurement Actions – (CSA, CP-CSA)

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

FP7-SEC Call 5

- Call identifier: FP7-SEC-2012-1
- Date of publication: July 20, 2011
- Deadline: November 23, 2011 at 17.00, Brussels local time

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

FP7-SEC-2012-1 Activities

- Activity: 10.1 Increasing the Security of the Citizens
- Activity: 10.2 Security of infrastructures and utilities
- Activity: 10.3 Intelligent surveillance and border security
- Activity: 10.4 Restoring security and safety in case of crisis
- Activity: 10.5 Security systems integration, interconnectivity and interoperability
- Activity: 10.6 Security and society
- Activity: 10.7 Security Research coordination and structuring

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

FP7-SEC-2012-1
Activity 10.1

- SEC-2012.1.3-1 Less than Lethal Handling of PBIEDs
- SEC-2012.1.3-2 Home made explosives (HMEs) and recipes characterisation
- SEC-2012.1.5-1 CBRNE Demo Phase II
- SEC-2012.1.5-2 Improving drinking water security management and mitigation in large municipalities against major deliberate, accidental or natural CBRN-related contaminations
- SEC-2012.1.5-3 Identification and development of low-risk alternatives to high-risk chemicals
- SEC-2012.1.5-4 Securing the food chains from primary production and animal feeds to consumer ready food against deliberate, accidental or natural CBRN contamination
- SEC-2012.1.6-1 Digital, miniaturised operational tool for investigation

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

FP7-SEC-2012-1
Activity 10.2

- SEC-2012.2.1-1 Resilience of large scale urban built infrastructure
- SEC-2012.2.1-2 Criticality analysis of critical infrastructure including concepts for forgery proof and efficient facility access systems
- SEC-2012.2.2-1 Identification of measures to counter illegal export of metal-bearing waste
- SEC-2012.2.2-2 Air traffic Management/Control threat assessment model
- SEC-2012.2.2-3 Improving security in air cargo transport
- SEC-2012.2.2-4 A common EU aviation security requirement to reduce costs and facilitate passenger flows
- SEC-2012.2.3-1 Early warning security systems: physical protection of critical buildings
- SEC-2012.2.4-1 Pre-normative technology development for improved and more efficient security of the supply chain
- SEC-2012.2.5-1 Convergence of physical and cyber security
- SEC-2012.2.5-2 Cyber resilience – Secure cloud computing for critical infrastructure

FP7-SEC-2012-1
Activity 10.3

- SEC-2012.3.1-1 Increasing trustworthiness of vessel reporting systems
- SEC-2012.3.1-2 Pre-Operational Validation (POV) at EU level of common application of Surveillance tools
- SEC-2012.3.4-1 Research on "automated" comparison of x-ray images for cargo scanning with reference material (use of historic images in an automated environment) to identify irregularities
- SEC-2012.3.4-2 Research and validation for sub-surface fingerprint live scanners
- SEC-2012.3.4-3 Tools and processes for assessing the impact of policies/actions on border control
- SEC-2012.3.4-4 Innovative, cost-efficient and reliable technology to detect humans hidden in vehicles/closed compartments
- SEC-2012.3.4-5 Further research, development and pilot implementation of Terahertz passive detection techniques (T-Ray)
- SEC-2012.3.4-6 Enhancing the workflow and functionalities of Automated Border Control (ABC) gates
- SEC-2012.3.5-1 Development of airborne sensors and data link

FP7-SEC-2012-1
Activity 10.4

- SEC-2012.4.1-1 Preparedness for and management of large scale fires
- SEC-2012.4.1-2 Psycho social support in Crisis Management
- SEC-2012.4.2-1 Positioning and timing tools to guarantee security assets trace & tracking together with worker safety in a secure environment
- SEC-2012.4.2-2 Situational awareness guidance and evacuation systems for large crowds, including crowds unpredictable behaviour
- SEC-2012.4.2-3 Post crisis lesson learned exercise
- SEC-2012.4.3-1 Next generation damage and post-crisis needs assessment tool for reconstruction and recovery planning
- SEC-2012.4.4-1 Development of mobile laboratories, structures and functions to support rapid assessment of CBRN events with a cross-border or international impact
- SEC-2012.4.4-2 Means of decontamination of large groups, urban/wide areas and large, complex and/or sensitive object
- SEC-2012.4.4-3 Tools for detection, traceability, triage and individual monitoring of victims after a mass contamination

FP7-SEC-2012-1
Activity 10.5

- SEC-2012.5.2-1 Preparation of the next generation of PPDR communication network
- SEC-2012.5.3-1 Embedded protection of security systems and anti-tampering technologies
- SEC-2012.5.3-2 Establishment of a first responders platform for interoperability
- SEC-2012.5.3-3 Establishment of a interoperability platform/ centre for testing and validating decisionand intelligence systems
- SEC-2012.5.3-4 Global solution for interoperability between first responder communication systems

BEST NETWORK
Biometric European Stakeholders Network

Fraunhofer

FP7-SEC-2012-1
Activity 10.6

- SEC-2012.6.1-1 Methodologies to assess the effectiveness of measures addressing violent radicalisation
- SEC-2012.6.1-2 Tools and methodologies, definitions and strategies for privacy by design for surveillance technologies, including ICT systems
- SEC-2012.6.1-3 Use of new communication/social media in crisis situations
- SEC-2012.6.3-1 Developing an efficient and effective environmental scanning system as part of the early warning system for the detection of emerging organised crime threats
- SEC-2012.6.3-2 Criteria for assessing and mainstreaming societal impacts of security research activities
- SEC-2012.6.4-1 Fight against corruption
- SEC-2012.6.5-1 Legitimacy and effectiveness of legal measures against security threats

FP7-SEC-2012-1
Activity 10.7

- SEC-2012.7.2-1 Open topic for Small and Medium Enterprises: "Advancing contemporary forensic methods and equipment“
- SEC-2012.7.4-1 Coordination of national research programmes in the area of security research
- SEC-2012.7.4-2 Networking of researchers for a high level multi-organisational and cross-border collaboration

FP7 Current Calls

- FP7 ICT Call 8
  - Call identifier: FP7-ICT-2011-8
  - Date of publication: July 20, 2011
  - Deadline: January 17, 2012, at 17:00 Brussels local time
- FP7-SEC Call 5
  - Call identifier: FP7-SEC-2012-1
  - Date of publication: July 20, 2011
  - Deadline: November 23, 2011 at 17.00, Brussels local time

Fraunhofer
IGD

Alexander Nouak
Dipl. Informationsw. (FH), Dipl. Betriebsw. (FH)

Abteilungsleiter
Identifikation und Biometrie
Fraunhofer-Institut für Graphische Datenverarbeitung IGD

Fraunhoferstraße 5 · 64283 Darmstadt
Telefon +49 6151 155-147 · Fax -499
alexander.nouak@igd.fraunhofer.de