D8.4 Architecture for Standardization V1

Fatbardh Veseli, Pascal Paillier, Jan Schallaböck, Ioannis Krontiris

Editor:	*Fatbardh Veseli (Goethe University Frankfurt)*
Reviewers:	*Gregory Neven (IBM Research - Zürich), Kazue Sako (NEC Japan)*
Identifier:	*D8.4*
Type:	*Deliverable*
Version:	*1.0*
Date:	*2012-03-06*
Status:	*Final*
Class:	*Public*

Abstract

This deliverable highlights the focus of ABC4Trust on standardization and studies three such standardization projects underway within ISO/IEC JTC/1 SC/27 WG 5. The main contribution of the document concentrates on developing concrete proposals to contribute to these projects, based on the research results brought by the first version of the ABC4Trust architecture. Firstly, a number of improvements to the current working draft of "ISO/IEC 24760-2 (2nd WD): Information technology - Security techniques - A framework for identity management - Part 2: Reference architecture and requirements" is proposed. Secondly, a concrete mapping of the ABC4Trust Architecture is made into the current draft of "ISO/IEC 29101 (4th CD): Privacy Architecture Framework". Thirdly, an analysis of the compatibility of the ABC4Trust architecture with the current draft of "ISO/IEC 29191 (2nd CD): Requirements for partially anonymous, partially unlinkable authentication" is given, along with suggestions on possible standard adjustments. Finally, the last part of the deliverable presents an overview of additional relevant projects within and beyond ISO, and examines prospective activities of ABC4Trust as the project matures further.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257782 for the project Attribute-based Credentials for Trust (ABC4Trust) as part of the "ICT Trust and Security Research" theme.

Members of the ABC4TRUST consortium

1.	Alexandra Institute AS	ALX	Denmark
2.	CryptoExperts SAS	CRX	France
3.	Eurodocs AB	EDOC	Sweden
4.	IBM Research – Zurich	IBM	Switzerland
5.	Johann Wolfgang Goethe – Universität Frankfurt	GUF	Germany
6.	Microsoft Research and Development	MS	France
7.	Miracle A/S	MCL	Denmark
8.	Nokia-Siemens Networks GmbH & Co. KG	NSN	Germany
9.	Research Academic Computer Technology Institute	CTI	Greece
10.	Söderhamn Kommun	SK	Sweden
11.	Technische Universität Darmstadt	TUD	Germany
12.	Unabhängiges Landeszentrum für Datenschutz	ULD	Germany

***Disclaimer**: The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.*

List of Contributors

Chapter	**Author(s)**
Executive Summary	Ioannis Krontiris (GUF)
Chapter 1 – Introduction	Jan Schallaböck (ULD), Ioannis Krontiris (GUF)
Chapter 2 – ABC4Trust contribution to ISO/IEC 24760-2	Fatbardh Veseli (GUF)
Chapter 3 – Specific relation towards ISO 29101	Fatbardh Veseli (GUF)
Chapter 4 – Contribution to ISO/IEC 29191	Pascal Paillier (CRX)
Chapter 5 – Other related projects in standardization and Outlook	Jan Schallaböck (ULD)

Executive Summary

ABC4Trust considers standardization to be a strong outreach activity, which has thus gained considerable attention from the project. This deliverable outlines the landscape of the relevant standardization bodies and projects, and takes first steps into looking into the viability of having an impact on the most relevant ones. In this regard, ABC4Trust has identified two groups of high relevance within ISO/IEC JTC 1/SC 27, namely WG 2 and WG 5.

Taking from the results of the work done on the definition of the first version of the ABC4Trust architecture, this deliverable addresses concrete proposals to three specific projects underway within WG 5, namely ISO/IEC 24760-2, ISO/IEC 29101 and ISO/IEC 29191.

"*ISO/IEC 24760-2: Information technology - Security techniques - A framework for identity management - Part 2: Reference architecture and requirements*" focuses on the description of the lifecycle model of identity information, providing guidelines for the implementation of systems for the management of identity information, and specifying requirements for the implementation and operation of a framework for identity management. This deliverable suggests a number of improvements to the current working draft of ISO/IEC 24760-2. Additionally, we also present here a mapping of some of the terms used in the two (ABC4Trust and ISO/IEC 24760-2) architectures.

The deliverable also presents the ABC4Trust Architecture in the spirit of the "*ISO/IEC 29101: Information Technology – Security Techniques – Privacy Architecture Framework*". The presented comparison takes the current version of the ABC4Trust architecture, adapting it to the structure and terminology of ISO/IEC 29101. This comparison outlines how the ABC4Trust architecture already implements many of the privacy-enhancing features by design, reducing the additional implementation burden for an application that uses this architecture to also comply with ISO/IEC 29101. In addition, the comparison presented here can also be used as an annex to the upcoming version of the ISO/IEC 29101.

A similar comparison of the ABC4Trust architecture is done with the draft of "*ISO/IEC 29191 - Requirements for partially anonymous, partially unlinkable authentication*". The overall purpose of ISO/IEC 29191 is to establish requirements for anonymous, unlinkable entity authentication. In this respect, the scope of ISO/IEC 29191 overlaps with goals of the ABC4Trust and the capabilities of the current ABC4Trust architecture. Part of this deliverable focusing on the identification of similarities and highlight the main incompatibilities between the definitions, concepts and requirements put forward by the two frameworks. Similarly, we also identify potential ABC4Trust contributions to the upcoming versions of the Draft.

There are numerous other standardization efforts underway, which are somewhat related to ABC4Trust. Although these projects have not been chosen as targets for outreach efforts at this point in time, they may nevertheless represent an outreach potential for us in the future. In particular, in WG 2 there are two multipart projects: ISO/IEC 20008, which specifies anonymous digital signature mechanisms; and ISO/IEC 20009, which delivers the descriptions of anonymous entity authentication mechanisms as a general model. In WG 5 there are also two other projects of relevance: ISO/IEC 29115, which delivers a metrics for four levels of authentication assurance; and ISO/IEC 29146, which provides a framework for the definition of access management and the secure management of the process to access information. An outlook of standardization projects and the prospective activities with ABC4Trust concludes the work on this deliverable.

Table of Contents

1 Introduction 9

1.1 Standardization and privacy legislation 9
1.2 Relevant Standards and Standardization Bodies 10
1.3 An Overview of the ABC4Trust Architecture 12

2 ABC4Trust contribution to ISO/IEC 24760-2 15

2.1 ISO/IEC 24760 – An Overview 15
2.2 ISO/IEC 24760-2 and ABC4Trust 15

2.2.1 Definition of additional terms in ISO/IEC 24760-2 15

2.2.2 Main Actors (Entities) in ISO/IEC 24760-2 16

2.2.3 Main Actors in ABC4Trust architecture 17

2.3 ABC4Trust contribution to ISO/IEC 24760-2 17

2.3.1 Mapping ISO/IEC 24760 to ABC4Trust Actors 17

2.3.2 Terms and Actors 18

2.3.3 (ISO/IEC 24760) Reference identifier vs. (ABC4Trust) pseudonyms 20

2.3.4 Non-recognition of long-lived credentials and its consequences 20

2.3.5 Processes and Information Flow 21

2.3.6 Diagram with the main IdM components 22

2.4 Conclusion 23

3 Specific relation towards ISO/IEC 29101 24

3.1 Overview 24
3.2 Brief description of the ABC4Trust architecture 24
3.3 Introduction into ISO/IEC 29101 25

3.3.1 Terminology 25

3.4 Purpose, Actors and Deployment of the ABC4Trust architecture 25
3.5 Architecture for the PII Controller 1 (Issuer) 27

3.5.1 Privacy Settings 27

3.5.2 Identity Management 27

3.5.3 Data 28

3.6 Architecture for the PII Controller 2 (Verifier) 28

3.6.1 Privacy Settings 28

3.6.2 Identity Management 29

3.6.3 Data 30

3.7 Architecture for the PII Principal (*User*) 30

3.7.1 Privacy Settings 30

3.7.2 Identity Management 30

3.7.3 Data....31

3.8 Conclusion....32

4 Contribution to ISO/IEC 29191....33

4.1 Description 33

4.2 Scope and Purpose of ISO/IEC 29191 33

4.3 Comparing Terminologies in ISO/IEC 29191 and ABC4Trust 33

4.3.1 Comparing High-Level Purposes....34

4.3.2 Comparing Roles 34

4.3.3 Comparing Operations and Data Objects....35

4.3.4 Comparing Requirements....36

4.4 Comparative Summary 37

4.5 Contributions to ISO/IEC 29191 38

4.6 ISO/IEC 29191 and Group Signatures....39

4.7 Conclusion....40

5 Other related projects in standardization and Outlook 41

5.1 ISO/IEC JTC 1/SC 27 41

5.2 Integration with current Identity Management Implementations....42

5.3 Outlook: Standardization of WP2 XML formats?....42

6 References....43

Index of Figures

Figure 1.1: An Overview of ABC4Trust-relevant standards 11
Figure 1.2: Entities and Interactions Diagram 12
Figure 1.3: A Sample Presentation Scenario 13
Figure 1.4: ABC4Trust Architecture Layers 14
Figure 2.1: A snapshot of the IdM components, as presented in ISO/IEC 24760-2 23
Figure 3.1: ABC4Trust architecture – An overview of (a subset of the main) Actors and their interactions 26

Index of Tables

Table 2-1: The list of Actors identified in Part 2 and their definitions 16
Table 2-2: ABC4Trust architecture Actors and their definitions 17
Table 2-3: (Partial) Mapping of ISO/IEC 24760-2 and ABC4Trust Actors 18
Table 2-4: Possible flows of identity information for the Revocation process, as presented in [10] 22
Table 3-1: Definition of terms for the main framework actors, as defined in ISO/IEC 29100 25
Table 3-2: Architecture at the PII Controller's (Issuer's) ICT 27
Table 3-3: An overview of the architecture at the PII Controller's ICT (Verifier)................................ 29
Table 3-4: An overview of the architecture of the PII Principal 31

1 Introduction

ABC4Trust is a research project bringing together industry, academia and others to address the federation and interchangeability of technologies that support trustworthy yet privacy-preserving Attribute-based Credentials (ABC). Attribute-based Credentials allow a holder intend to reveal just the minimal information required by the application, without giving away full identity information. These credentials thus facilitate the implementation of a trustworthy and at the same time privacy-protecting digital society.

Standardization has been chosen as a strong outreach focus of ABC4Trust Consortium [1]. This deliverable outlines the landscape of relevant standardization bodies and projects, and takes first steps into looking into the viability of impacting selected projects.

After an introduction assessing the relevancy of standardization in the field of ABC4Trust technology, especially relating this to the legal framework within the European Union (Section 1.1), an overview of standardization bodies and their roles will be given (Section 1.2), highlighting the relevancy of the International Standardization Organisation (ISO) in this context. To put the efforts in context with the ABC architecture an overview of this architecture is given in Section 1.3.

We will then outline three concrete projects underway within ISO/IEC JTC/1 SC/27 WG 5 and develop concrete proposals to contribute to these projects from a perspective of ABC4Trust. A number of improvements to the current working draft of “ISO 24760-2: Information technology - Security techniques - A framework for identity management - Part 2: Reference architecture and requirements” will be proposed in Chapter 2. Chapter 3 will try to map the ABC4Trust Architecture into the CD of “ISO 29101: Privacy Architecture Framework”. In Chapter 4, we will then analyse the compatibilities towards the current Committee Draft (CD) of “ISO 29191: Requirements for partially anonymous, partially unlinkable authentication”, and look into necessary adjustments.

Finally, an overview of other projects within ISO and beyond, their relationship to and their perspective for standardising work of ABC4Trust will be described in the outlook chapter (Chapter 5).

1.1 Standardization and privacy legislation

Especially in the European Union's privacy legislation technical standards are given significant role, e.g. when the law requires technical mechanisms to be put in place to protect the privacy of users. The specific mechanisms are usually not spelled out in the law itself, as the regulation aims to be “technology neutral”.[1] Instead, the term “state of the art” is often referred to, cf. art. 4 para 1 in [2] recital 46 and art. 17 para 1 in [3]. How is this term then related to international standards? one might ask. There is currently little legal research in this specific field, so the details may still be vague. From earlier discussions in other areas such as technical regulation as nuclear safety, waste, etc we probably can safely assume that standards give high prejudice whether or not the state of the art has been met.[2] In other words: In borderline cases, courts will draw to existing standards to determine whether or not

[1] For a more thorough discussion of the term and its implications, cf. 2.

[2] cf, eg. Bundesverfassungsgericht (Verfassungsgericht der Bundesrepublik Deutschland), Beschluß des Zweiten Senats vom 8. August 1978, Geschäftszeichen 2 BvL 8/77, amtliche Sammlung BVerfGE 49, 89; sogenannte „Kalkar I"-Entscheidung, cit. in Wikipedia: http://de.wikipedia.org/wiki/Anerkannte_Regeln_der_Technik

legal compliance has been met, whenever the understanding of the legal term “state of the art” is in question.

Likewise data protection agencies recognize international standards when inspecting the implementation of technical means of a service provider [4]. Consequentially procurement often requires products or services to meet certain standards. This even furthers the relevancy of technical standards as a whole.

In European data protection legislation the aforementioned is given emphasis already in the `95 Directive on data protection [3] as well as in the E-Privacy directive [2]. On January 25th, 2012, the European Commission officially published a first proposal for a new regulation on data protection [5] which will be superseding the `95 Directive and effectively will communitarise (as well as “lisbonize”[3] as we will describe in the following) this field of regulation. This proposal appears to further strengthen the relevancy of technical standards. Namely, its recital 66 and in Article 23 para 1 thereof explicitly refers to the state of the art, with the latter being augmented by the process of the superseded comitolgy process, cf. [6] for a more detailed analysis. The latter gives the commission the power to mandate specific standards pending lack of objection by the parliament. Effectively, such regulation would allow for a strong harmonization of technical measures in specific domains under the control of the Commission.

1.2 Relevant Standards and Standardization Bodies

The often referred-to definition of standards stems from ISO/IEC Guide 2:2004 which describes standards as “a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context” [7]. (Technical) Standards can be developed via standardization bodies or solely develop through broad acceptance. The latter are usually referred to as “de-facto” standards, and may not be considered standards in a narrower sense and are also sometimes called “quasi standards”. If standardization bodies are involved, these can be differentiated by the process of developing the standard, as well as by the entities taking part in the process. Finally the availability differs in different organisations. There also are of course national, regional and international standards.

Especially in IT, industrial consortia defining different standards are often predominant, although drawing the line towards more open forms of standards development is not often a very easy task. Basic standards of the Internet are developed through organisations like the Internet Engineering task force (IETF) or the World Wide Web Consortium, to name two of the more important entities, do rely on some industrial financing but take a mixed approach often involving other interested parties and experts. They are driving the development of the basic protocols, like the Internet-Protocol (IPv4 and IPv6), defining protocols for the exchange of E-Mail, and the presentation of Web-pages (HTML, HTML5). Both can be described as standards bodies meeting the definition above, although their internal structure, process, funding mechanisms, etc varies. However, both produce standards that are freely available at no cost.

On the other hand, the International Organisation for Standardization - ISO - does rely on selling most of its standards, but nevertheless traditionally enjoys a high level of recognition, but it could possibly be considered the “root” of standardization bodies. This stems from its history, but might also be

[3] The term has been coined for the new powers granted to the commission as part of the Lisbon treaty, which are herein referred to as the amended comitology procedure, which, of course is slightly misleading, as the underlying regulation 182/2011, cf. [6], is in fact not really amending but replacing the comitology process.

related to its structure as being strongly tied to only one recognized standardization body on a national level. Without being able to go in detail on the specific differences of the different institutions, one probably can assume, that often ISO acts as an integrator of the work of different standards bodies around the world and enjoys a high level of recognition especially with national governments and international institutions such as the World Trade Organisation, which explicitly mentions ISO in Annex 3 of the Agreement on Technical Barriers to Trade [8].

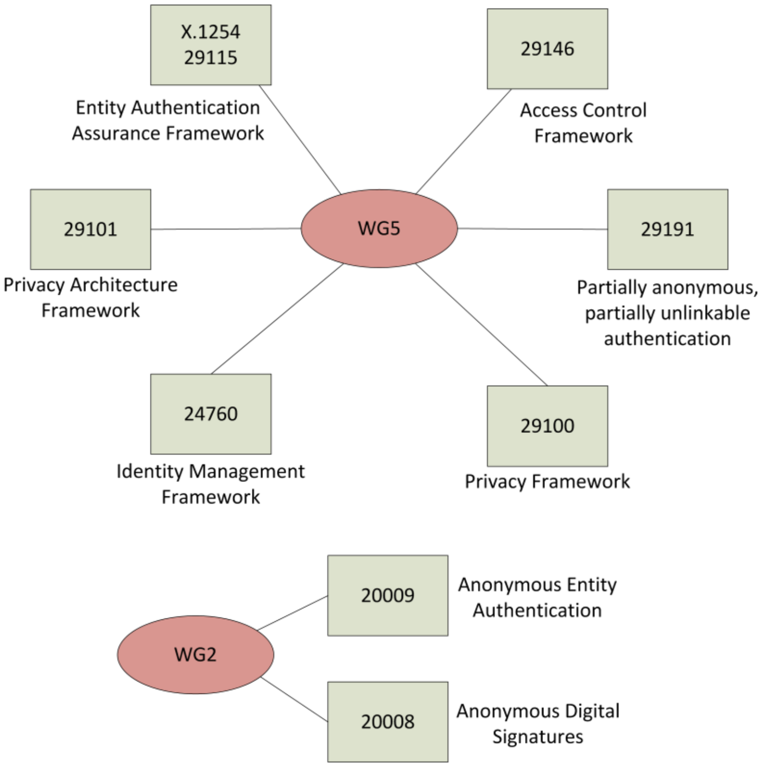
X.1254
29115
Entity Authentication Assurance Framework
29146
Access Control Framework
29101
Privacy Architecture Framework
WG5
29191
Partially anonymous, partially unlinkable authentication
24760
Identity Management Framework
29100
Privacy Framework
20009
Anonymous Entity Authentication
WG2
20008
Anonymous Digital Signatures

Figure 1.1: An Overview of ABC4Trust-relevant standards

The role of ISO is not carved in stone, and e.g. in the European Union a specific mandate is sometimes given to its own standardization body, CEN. For the scope of this deliverable, however, most relevant standards are developed and under discussion within Working Groups of either ISO, or within the Joint Technical Committee 1 (JTC 1) of ISO with the International Electrotechnical Commission, IEC, to be more correct. There is some relevant effort in a number of other bodies, such as W3C and OASIS, nevertheless, which will be briefly addressed in Chapter 5.

Subcommittee 27 of JTC 1 (ISO/IEC JTC 1/SC 27), concerned with IT-Security standardization, is the subcommittee whose scope closely related to the work of ABC4Trust. It has five working groups of which Working Group 5 (WG 5) is concentrating on identity management and privacy technologies. Obviously, this working group relates greatly to the work of ABC4Trust, but Working Group 2 (WG 2) also being of some relevance. In the following chapters a number of most relevant projects underway will be described in more detail as well as possible contributions from the research within ABC4Trust, after a brief overview of the ABC4Trust Architecture.

1.3 An Overview of the ABC4Trust Architecture

For giving an overview of the ABC4Trust architecture in a first step we need to introduce the different involved entities, and the type of interactions that they engage in.

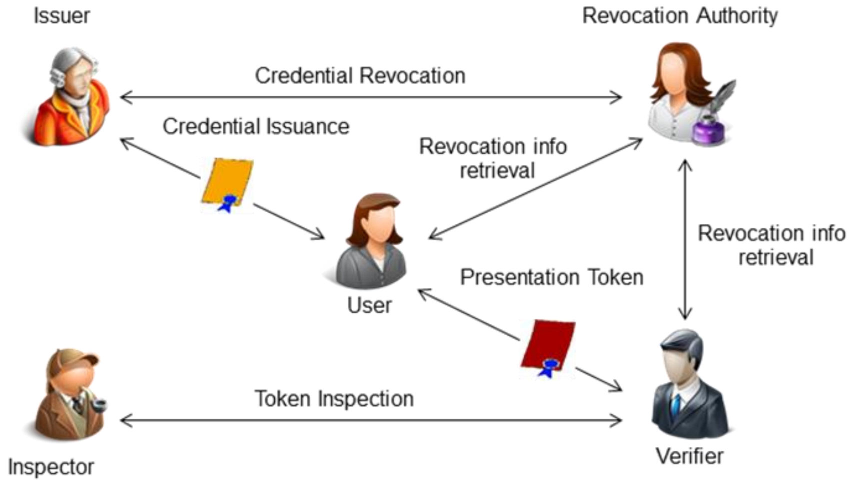

Figure 1.2: Entities and Interactions Diagram

As it is depicted in Figure 1.2, the following five architectural entities can interact in the various possible scenarios:

- The *User* is at the centre of the picture, collecting *Credentials* from various Issuers and controlling which information from which credentials she presents to which verifiers. The human User is represented by her *User Agent*, a software component running either on a local device (e.g., on the User's computer or mobile phone) or remotely on a trusted cloud service. The User may own special hardware tokens to which credentials can be bound to improve security. In the identity management literature, the User is sometimes referred to as the requestor or the subject.
- An *Issuer* issues credentials to Users, thereby vouching for the correctness of the information contained in the credential with respect to the User to whom the credential is issued. Before issuing a credential, the Issuer may have to authenticate the User, which it may do using Privacy-ABCs, using a different online mechanism (e.g., username and password), or using out-of-band communication (e.g., by requiring the User to physically present herself at the Issuer's office). In the identity management literature, the Issuer is sometimes referred to as the identity provider or attributes authority.
- A *Verifier* protects access to a resource or service that it offers by imposing restrictions on the credentials that Users must own and the information from these credentials that Users must present in order to access the service. The Verifier's restrictions are described in its presentation policy. The User generates from her credentials a presentation token that contains the required information and the supporting cryptographic evidence. In the identity management literature, the Verifier is sometimes also referred to as the relying party, the server, or the service provider.
- A *Revocation Authority* is responsible for revoking issued credentials, so that these credentials can no longer be used to generate a presentation token. The use of a particular Revocation Authority may be imposed by the Issuer, in which case the revoked credentials cannot be used with any Verifier for any purpose, or by the Verifier, in which case the effect of the revocation

is local to the Verifier and does not affect presentations with other Verifiers. Both the User and the Verifier must obtain the most recent revocation information from the Revocation Authority to generate, respectively verify, presentation tokens.

- An *Inspector* is a trusted authority who can de-anonymize presentation tokens under specific circumstances. To make use of this feature, the Verifier must specify in the presentation policy which Inspector should be able to recover which attribute(s) under which circumstances. The User is therefore aware of the de-anonymization options when the token is generated and actively participates to make this possible; therefore the User can make a conscious decision based on her trust in the Inspector.

In an actual deployment, some of the above roles may actually be fulfilled by the same entity or split among many. For example, an Issuer can at the same time play the role of Revocation Authority and/or Inspector, or an Issuer could later also be the Verifier of tokens derived from credentials that it issued.

A *credential* is a certified container of attributes issued by an *Issuer* to a *User*. An attribute is described by the *attribute type*, determining the semantics of the attribute (e.g., first name), and the *attribute value*, determining its contents (e.g., John). By issuing a credential, the Issuer vouches for the correctness of the contained attributes with respect to the User. The User can then later use her credentials to derive *presentation tokens* that reveal *partial* information about the encoded attributes to a Verifier.

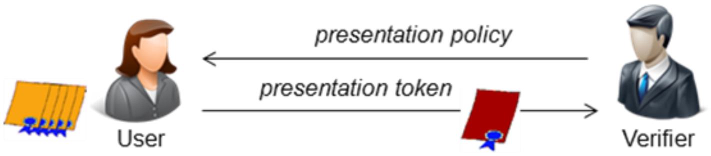

Figure 1.3: A Sample Presentation Scenario

In a typical scenario (Figure 1.3), a Verifier announces in its *presentation policy* which credentials from which Issuers it accepts and which information the presentation token must reveal from these credentials. The Verifier can cryptographically verify the authenticity of a received presentation token using the credential specifications and issuer parameters of all credentials involved in the token. The Verifier must obtain the credential specifications and issuer parameters in a trusted manner, e.g., by using a traditional PKI to authenticate them or retrieving them from a trusted location.

To provide certified information to a Verifier (for authentication or an access decision), the User uses one or more of her credentials to derive a *presentation token* and sends it to the Verifier. A single presentation token can contain information from any number of credentials. The token can reveal a subset of the attribute values in the credentials (e.g., IDcard.firstname = “John”), prove that a value satisfies a certain predicate (e.g., IDcard.birthdate < 1993/01/01) or that two values satisfy a predicate (e.g., IDcard.lastname = creditcard.lastname).

The presentation token created in response to such a presentation policy consists of the *presentation token description,* containing a mechanism-agnostic description of the revealed information, and the *presentation token evidence,* containing opaque technology-specific cryptographic data in support of the token description.

Presentation tokens based on Privacy-ABCs are in cryptographically proven to be unlinkable and untraceable, meaning that Verifiers cannot tell whether two presentation tokens were derived from the same or from different credentials, and that Issuers cannot trace a presentation token back to the issuance of the underlying credentials. However, we have considered additional mechanisms so that, with the User's consent, it enables a dedicated third party to recover this link again.

In particular, the architecture has been designed to decompose future (reference) implementations of Privacy-ABC technologies into sets of modules and specify the abstract functionality of these components in such a way that they are independent from the cryptographic mechanisms used underneath. The functional decomposition foresees possible architectural extensions to additional functional modules that may be desirable and feasible using future Privacy-ABC technologies or extensions of existing ones.

Figure 1.4 shows how ABC4Trust architectural modules are divided into the three abstract layers, namely *Application*, *ABC-Engine (ABCE)* and *CryptoEngine (CE)*. The ABCE *layer* contains all cryptography-agnostic methods and components for a Privacy-ABC system. That is, it contains e.g. the methods to parse an obtained presentation policy, perform the selection of applicable credentials for a given policy or to trigger the mechanism-specific generation or verification of the cryptographic evidence. The ABCE-layer is invoked by the application-layer and calls out the *CryptoEngine* to obtain the mechanism-specific cryptographic data.

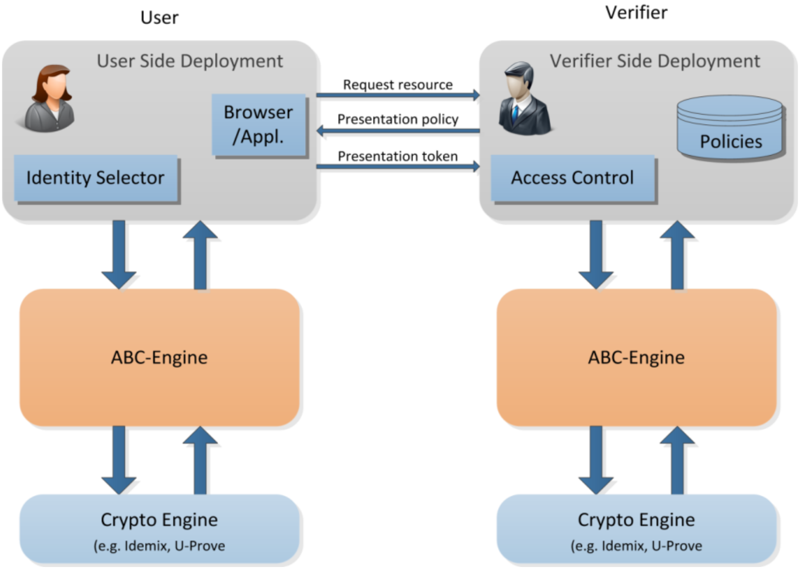

Figure 1.4: ABC4Trust Architecture Layers

Equally important in the architecture is the specification of the data artefacts exchanged between the implicated actors, in such a way that the underlying differences of concrete Privacy-ABCs are abstracted away through the definition of formats that can convey information independently from the mechanism-specific cryptographic data.

2 ABC4Trust contribution to ISO/IEC 24760-2[4]

2.1 ISO/IEC 24760 – An Overview

The text of the standard "ISO/IEC 24760 – Information Technology – Security Techniques – A framework for identity management" addresses the issue of efficient and effective implementation of systems that make identity-based decisions. This standard [9] "specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations or information technology components, which operate on behalf of individuals or organizations. Furthermore, it specifies fundamental concepts and operational structures of identity management."

The standard is organized into three parts:

- Part 1: Terminology and concepts,
- Part 2: Reference architecture and requirements, and
- Part 3: Practice

While Part 1 (ISO/IEC 24760-1) has the status of an International Standard, Part 2 and Part 3 on the other hand have the status of a Working Draft.

In 24760-1, the main focus of the standard is on the definition of terms for identity management, specification of core concepts for identity and identity management, as well as explanation of their relationships [9].

On the other hand, ISO 24760-2 focuses on the description of the lifecycle model of identity information, providing guidelines for the implementation of systems for the management of identity information, and specifying requirements for the implementation and operation of a framework for identity management [10].

Part 3 of 24760 provides guidance for practice in the design, implementation and operations systems for the management of identity information [11].

Overall, the standard deals with processes around identity management and contains some of the privacy requirements in place, while the architecture of ABC4Trust provides a specific infrastructure which has been designed having in mind the need for privacy.

2.2 ISO/IEC 24760-2 and ABC4Trust

2.2.1 Definition of additional terms in ISO/IEC 24760-2

General definition of terms is one of the scopes of the ISO/IEC 24760-1, but ISO/IEC 24760-2 also brings a list of some additional terms in Section 3 – Terms and Definitions, where the terms *principal*, *provisioning*, *revocation* and *assertion* are defined. The reason for this may be the omission of definitions of such terms in the Part 1 of the standard, which is now in a stable version (IS), but may

[4] All the contribution and references in this chapter to ISO/IEC 24760-2 refer to the "ISO/IEC 2nd Working Draft 24760-2" dated 2012-01-10.

also attribute to the fact that these terms are of some special relevance in the context of the scope of this part.

2.2.2 Main Actors (Entities) in ISO/IEC 24760-2

The two (ISO/IEC 24760-2 and ABC4Trust) architectures define their respective sets of actors. In this section we present the Actors identified in Part 2 of ISO/IEC 24760. However, not all of the presented actors in Part 2 have been provided a definition for in Part 1. Consequently, Part 2 presents a separate section in the beginning, introducing the missing terms. Therefore, for each definition, we will specify their original source of definition.

A special remark in this section concerns two new entities presented in Part 2, namely the **Identity Management Authority** and the **Auditor**, for which the definitions are missing in both parts of the standard. This is a separate feedback to Part 2, which must be corrected in the coming version. However, Table 2-1 presents the complete list of the actors introduced in Part 2. Most of the definitions are taken from Part 1 and there is a notice on the column “Note” otherwise. The text in italics in the column “Definition” is used to show that the term has merely been explained and no proper definition for it is provided in the standard.

Table 2-1: The list of Actors identified in Part 2 and their definitions

Actor	Definition	Note
Principal	Entity to which identity information pertains	Defined in Part 2.
Identity management authority	*Entity associated with a domain with the capabilities to set and enforce operational policies*	Definition missing. This is the description presented in Part 2.
Relying party	Entity that relies on the verification of identity information for a particular entity	
Identity Information Authority	Entity related to a particular domain that can make provable statements on the validity and/or correctness of one or more attribute values in an identity	
Identity Information Provider	Entity related to a particular domain that can make provable statements on the validity and/or correctness of one or more attribute values in an identity	
Verifier	Entity that performs verification	
Auditor	*Entity with capabilities to inspect operations*	Definition missing. This is the description presented in Part 2.

2.2.3 Main Actors in ABC4Trust architecture

On the other hand, actors of the ABC4Trust architecture have already been explained in Section 1.3. However, Table 2-2 list the definitions for these actors, as defined in the ABC4Trust deliverable "D2.1 Architecture" [12]:

Table 2-2: ABC4Trust architecture Actors and their definitions

Actor	Definition	Note
User	The human entity who wants to access a resource controlled by a verifier and obtains credentials from Issuers to this end.	
Verifier	The party that protects access to a resource by verifying presentation tokens to check whether a User has the requested attributes.	The Verifier only accepts credentials from Issuers that it trusts.
Issuer	The party who vouches for the validity of one or more attributes of a User, by issuing a credential to the User.	
Inspector	A trusted entity that can trace the User who created a presentation token by revealing attributes from the presentation token that were originally hidden from the Verifier.	
Revocation Authority	The entity in charge of revoking credentials.	The Revocation Authority can be an Issuer, a Relying Party, or an independent entity. Multiple Issuers or Verifiers may rely on the same Revocation Authority.

2.3 ABC4Trust contribution to ISO/IEC 24760-2

2.3.1 Mapping ISO/IEC 24760 to ABC4Trust Actors

Having introduced the list of entities for both (ABC4Trust and ISO/IEC 24760-2) architectures together with their definitions, we present a mapping of these entities in Table 2-3. Roles mapping is unilateral, since our intention is to show how the actors listed under Part 2 architecture map to the actors of the ABC4Trust architecture. This way, we can see what entity is missing in this part of the standard, which can be an additional contribution from ABC4Trust.

The first column in Table 2-3 represents the ABC4Trust entities, while the second column shows the corresponding role, which it maps to. The third column (Mapping level) is used to show if the roles map completely (Full), partially (Part) or if there is no equivalent mapping role (None).

Table 2-3: (Partial) Mapping of ISO/IEC 24760-2 and ABC4Trust Actors

ABC4Trust Actor	ISO/IEC 24760-2 Actor	Mapping level
User	Principal	Full
Verifier	Relying Party + Verifier	Partial
Inspector		None
Issuer	Identity Information Authority	Partial
Revocation Authority	Identity Management Authority	Partial

Role mapping is in most of the cases an approximate rather than a one-to-one mapping of the roles of such entities. Except for the full mapping, the explanation for this is as follows:

- The single ABC4Trust entity “Verifier” combines both functions of the ISO/IEC 24760-2 “Verifier” and “Relying Party”. In the ABC4Trust architecture, there is no explicit reference to a Relying Party. From of the definition of the Verifier in both architectures (see Table 2-1 and Table 2-2, it is clear that the two respective entities perform the same task – they map exactly to one another. In addition to that, by relying on the certification of credentials by the Issuers it trusts, the ABC4Trust Verifier also covers the role of an ISO/IEC 24760 Relying Party, which is explained in the Column “Notes” in Table 2-2.
- Part 2 of ISO/IEC 24760 does not recognize any entity with the capabilities of the ABC4Trust Inspector, since there is no designated entity that can revoke the anonymity of a User. This must be taken into account when designing the coming version of ISO/IEC 24760-2. In addition, adding this entity would introduce additional processes (Inspection) and data flows in the standard. Alternatively, this role could be assigned to the existing ISO/IEC 24760-2 Auditor, which is not defined yet.
- ISO/IEC does not recognize the process of credential issuing, nor the one of certified identity information. In ABC4Trust, these tasks belong to the Issuer. Consequently, there is no complete match between an ABC4Trust Issuer and the ISO/IEC 24760-2 Identity Information Authority. However, both entities provide assurance that the attribute values contained in a credential are valid, so there is a partial mapping of these roles. More on this will come in Section 2.3.4.
- In ABC4Trust, the role of the Revocation Authority is to invalidate a credential or a list of credentials. An equivalent specialized entity for this purpose has not been defined in ISO/IEC 24760. However, the description of the Identity Management Authority and its position in the Revocation Process as the authority deciding about the revocation in the data flow table in Part 2 brings it close to the function of the ABC4Trust Revocation Authority. A precise definition of this entity in the upcoming ISO/IEC 24760-2 to specifically include this function could clarify and confirm this mapping.

2.3.2 Terms and Actors

Given that the terminology was defined in ISO/IEC 24760-1, while partly complemented with a list of new terms in a separate section in the ISO/IEC 24760-2, the reader may get the impression that some of these terms are being re-defined later exactly in ISO/IEC 24760-2. The reader might especially get such a wrong impression in Section “5.1.1 - Actors”, where the main actors of the reference architecture (of 24760-2) are described. In this section, some of the actors have been described imprecisely, such as the roles for the (ISO/IEC 24760-2) Principal, Verifier and the Relying Party, as the following sections will show (see Subsections 2.3.2.1-2.3.2.3).

2.3.2.1 Principal

The role of the (ABC4Trust) User is equivalent to the (ISO/IEC 24760) role of an "Identity Principal". Part 2 of ISO/IEC 24760 defines a *Principal* in Section 3 – Terms and Definitions, where a Principal is described as "*an entity with the capabilities to present an **identity** to a Verifier*" [10].

In ABC4Trust, the User uses her credential(s) to generate a presentation token, which she can present to a Verifier, proving the possession of certain attribute(s), which should reveal to the Verifier only the minimum necessary (set of) values of attributes about the User. Indeed, Section 3.3.5 of ISO/IEC 24760-1 defines a *credential* as a „*representation of an identity*", whereas an *identity* is defined as a „*set of attributes related to an entity*" [9].

Therefore, taking into consideration the architecture of ABC4Trust, a more precise definition of the "Identity Principal" should incorporate a definition which incorporates presenting <u>a proof of possession of certain credentials</u> to a Verifier, rather than presenting the *identity* or even the *credential* itself.

2.3.2.2 Verifier

ISO/IEC 24760-1 defines a Verifier as "*an entity that performs verification*" [9], while in ISO/IEC 24760-2 a Verifier is described as "*an entity associated with a domain with capabilities to perform identification of an entity*" [10]. While the definition in ISO/IEC 24760-1 is in line with the ABC4Trust definition of a Verifier, the use of the term "identification" instead of "verification" in ISO/IEC 24760-2 seems to be incorrect. To support our claims, this is how ISO/IEC 24760-1 defines these two terms [9]:

- <u>Identification</u>: "*Process of recognizing an entity in a particular domain as distinct from other entities*."
- <u>Verification</u>: "*Process to determine that presented identity information associated with a particular entity is applicable for the entity to be recognized in a particular domain at some point in time.*"

2.3.2.3 Relying party

In the ABC4Trust architecture, the (ISO/IEC 24760) roles of a Verifier and a Relying Party are combined into the single role of the (ABC4Trust) Verifier (see also Table 2-3: (Partial) Mapping of ISO/IEC 24760-2 and ABC4Trust Actors). In the Part 2 of the ISO 24760, the Relying Party is described as "*an entity exposed to the risk of incorrect identity information, e.g. service provider using identity information in providing its services, or identity information provider in another domain*". This description of a Relying Party is correct as it relies on another entity to provide correct information (proof) about the User. Nevertheless, there are certain mechanisms which can be implemented to help reduce the risk level the Relying Party is exposed to and which can provide a certain level of assurance on the entity the Relying Party relies on, which should also mentioned in the description of this entity.

2.3.3 (ISO/IEC 24760) Reference identifier vs. (ABC4Trust) pseudonyms

In ABC4Trust [12], pseudonyms are used to provide controlled linkability, whenever this is desired, distinguishing between the following three types of pseudonyms:

- *Verifiable pseudonyms* allow the User to re-authenticate under the pseudonym by proving knowledge of the user secret. Presenting a verifiable pseudonym does not involve presenting a corresponding presentation token and is useful in login scenarios, e.g., to replace usernames/passwords.
- *Certified pseudonyms* are verifiable pseudonyms derived from a user secret that also underlies an issued credential. By imposing, i.e. key-binding, the User can therefore prove ownership of a credential and at the same time establish a pseudonym based on the same user secret.
- *Scope-exclusive pseudonyms* In the architecture of ABC4Trust, a scope-exclusive pseudonym is defined as „a certified pseudonym that is guaranteed to be cryptographically unique per scope string and per user secret. Meaning, from a single user-bound credential, only a single scope-exclusive pseudonym can be generated for the same scope string." This feature can be useful to implement a form of "consumption control" in situations where users must remain anonymous to the Verifier but should not be allowed to create multiple identities based on a single credential, although for different scope strings, they are still unlinkable, just like normal pseudonyms.

Related to this comes the ISO/IEC 24760-1 concept of Reference Identifier (RI), which is defined as an "*identifier in a domain that is intended to remain the same for the duration an entity is known in the domain and is not associated with another entity for a period specified in a policy after the entity ceases to be known in that domain*" [9]. An ABC4Trust scope-exclusive pseudonym gives additional guarantees for the identifier. The ISO definition does not say anything about the linkability of identifiers across different domains, or about the number of possible different identifiers per domain. Scope-exclusive pseudonyms are guaranteed to be unique for a domain and are unlinkable across domains. Verifiable pseudonyms are unlinkable but not unique.

On the other hand, such a narrow definition of a reference identifier has an impact on the privacy of the User, limiting the use of a certain identifier (pseudonym) each time they want to access a service. ABC4Trust architecture enables Users to generate as many pseudonyms as they wish and use any of them to authenticate towards the Verifier, which are unlinkable and untraceable, and consequently offer a better privacy. Therefore, incorporating such a definition or at least making such a distinction clearer is another contribution from ABC4Trust architecture to Part 2 of ISO/IEC 24760.

2.3.4 Non-recognition of long-lived credentials and its consequences

Even though the credential definition in ISO/IEC 24760-1 is in line with both short- and long-lived credentials, the architecture description in ISO/IEC 24760-2 does not fully support the concept of long-lived credentials, which are core to the ABC4Trust architecture. This can be explained by the fact that ISO/IEC 24760 does not include the following:

- No concept of issuance of a certified credential - no full functionality of an ABC4Trust Issuer
- Missing corresponding entity with the (complete) functionality of an ABC4Trust Revocation Authority
- Imprecise definition of a Principal and unused of a credential – the standard defines the concept of a credential, but it has never been used in a relation with other entities or processes, such as presentation, revocation or issuance.

Therefore, incorporating the concept of long-lived credentials in Part 2 of ISO/IEC 24760 is a major contribution which would reduce the set of inconsistencies and is essential in responding correctly to the identified issues in this chapter.

2.3.5 Processes and Information Flow

While Part 1 of the ISO/IEC 24760 recognizes the different processes of:

- identification,
- registration,
- authentication, and
- activation,

Part 2 introduces requirements for additional processes, including:

- auditing,
- generating reference identifier,
- provisioning,
- identity adjustment
- revocation
- identity information processing, and
- identity information processing authorization.

Additionally, a table presenting these processes, the actors involved and their respective actions is presented in a form of information flow in the Part 2 of ISO/IEC 24760 (Section 5.1.2 Information flow). However, a general remark in this section is that it is not easy for a reader to clearly see if the identified steps are supposed to be independent from each other or they run in a sequence. Therefore, an additional text on how to read the table would improve the understanding of such an information flow presentation (see for instance Table 2-4). The following subsections bring parts of such a table depicted from Part 2 of ISO/IEC 246760 and explain some of the identified issues in a bit more detail.

2.3.5.1 Revocation

The definition of Revocation is missing in ISO/IEC 24760-1, but is introduced as a new definition in 24760-2, where it is described as a *"process to end the validity of a particular attribute".* In the architecture of ABC4Trust, revocation ends the validity of a credential, which is more precise due to the fact that a credential is the representation of a particular attribute [10]. Therefore, a first contribution in this regard would be to re-define the term Revocation reflecting this reality.

Table 2-4 has been copied from Part 2 of ISO/IEC 24760 and presents the information flow for the revocation process and the involved actors. In ABC4Trust, we distinguish between two types of revocation of a credential, depending on which entity initiates the revocation:

1. Issuer-driven revocation
2. Verifier-driven revocation

These two types of revocation are distinct in the scope of the revocation, as well as the information flow. While the Issuer-driven revocation is initiated by the Issuer and has a "global impact", making a credential invalid for use with any Verifier, the Verifier-driven revocation is initiated by a Verifier and has a "local" impact in the sense that a credential will be invalidated for use with that Verifier only. Therefore, a contribution to the standard could be to distinguish between different types of revocation, depending on the entity initiating the revocation process and the scope of applicability of such a revocation.

Table 2-4: Possible flows of identity information for the Revocation process, as presented in [10]

	Source		**Recipient**	
Process	**Actor**	**Action**	**Actor**	**Action**
Revocation	Identity Management Authority	*Decides on identity revocation.*	Identity Register	*Stores information to effect status change.*
	Identity-Information Provider	*Initiates provisioning of the revocation.*	Relying Party	*Applies updated information to its service process.*

2.3.5.2 Identity adjustment

Identity adjustment is a process described in ISO/IEC 24760-1 as "*an update of the information in the identity register for an entity, where the new information gives rise to the modification of activation information"* [9]. However, the right term in this case would be the "*identity information adjustment*" rather than "*identity adjustment*", since, according to the same standard, identity represents "*a set of attributes related to an entity*", whereas identity information is defined as a "*set of values of attributes optionally with any associated metadata in an identity*". Since the term was merely described, but not properly defined in ISO/IEC 24760-1, the use of this term should be properly corrected in ISO/IEC 24760-2.

What is also missing in the standard is the requirement to revoke the old-credential upon receiving a request to adjust identity information. Again, this relates to the absence of a concept of long-lived credentials and the whole concept of credential issuance (see Section 2.3.4, "Non-recognition of long-lived credentials").

2.3.6 Diagram with the main IdM components

The standard already shows a diagram of the identified components of an Identity Management System, but there seems to be a flaw in it (see Figure 2.1), since the "Principals" entity is separately associated in the diagram from the other Actors, while they represent a regular Actor, as defined also in ISO/IEC 24760-2 in Section "5.1.1 - Actors".

Moreover, what would make the overall standard more readable would be the presentation of a diagram with the interactions between the Actors.

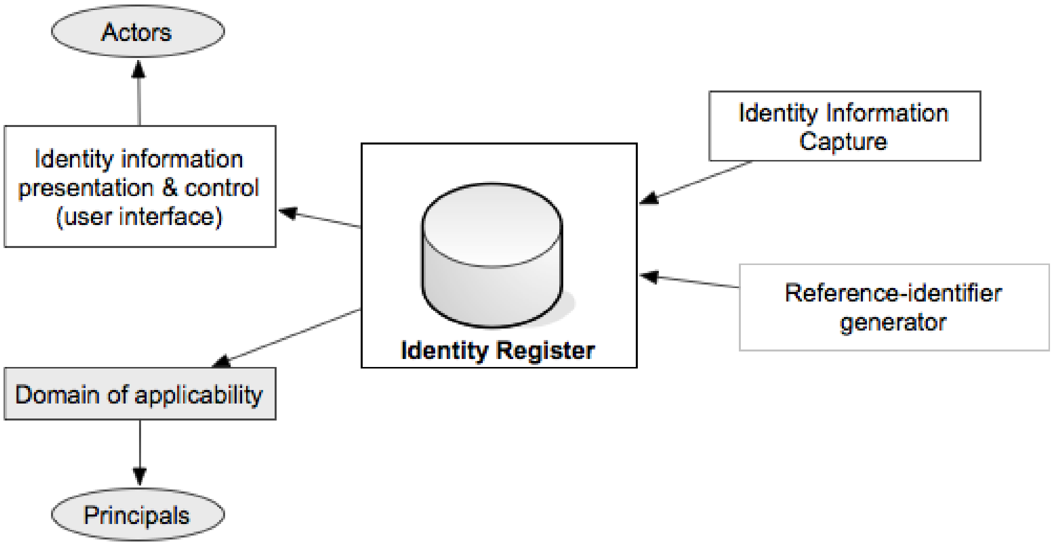
Actors
Identity information presentation & control (user interface)
Identity Register
Identity Information Capture
Reference-identifier generator
Domain of applicability
Principals

Figure 2.1: A snapshot of the IdM components, as presented in ISO/IEC 24760-2

2.4 Conclusion

ISO/IEC 24760 is a relevant standard for comparing with the architecture of ABC4Trust, since they both deal with the issue of Identity Management. In this regard, a role mapping that clarifies the different terminology used for the same actors in each of the corresponding architectures.

On the other hand, since the Reference architecture and requirements of ISO 24760 (Part 2) is still in a draft version, we also contributed with some feedback that could improve the reference architecture in the final version. Such feedback mostly concerns the inclusion of the concept of identity information certification, which ABC4Trust is based upon, and consequently recognizing the process of Issuance of a credential. . Similarly, we also provide feedback to a definition of revocation with regard to the entity initiating this process, as in the ABC4Trust: Verifier- and Issuer- driven revocation. Some additional terminology adjustment and a diagram correction that would make this part of the standard more precise have also been proposed, along with the argumentation why such a correction is necessary.

Finally, to improve the understanding of this part of the standard, we recommend building and presenting a new diagram depicting the main actors of the ISO/IEC 24760-2 reference architecture and their interactions, so as to give the reader a clearer picture of the architecture at a more concrete level.

3 Specific relation towards ISO/IEC 29101

3.1 Overview

This chapter presents the ABC4Trust Architecture in the spirit of the "ISO/IEC 29101: Information Technology – Security Techniques – Privacy Architecture Framework"[5] (ISO 29100). The presented material is based on the original version of the architecture and has been hereby adopted to fit the structure and terminology described in the standard. ABC4Trust architecture is built upon the concept of (Privacy-) Attribute-Based Credentials (ABCs), which provides a model for an Identity Management System designed with a special focus on the user privacy[6].

This chapter starts by introducing the ABC4Trust architecture (Section 3.2), a brief introduction into the scope of the ISO/IEC 29100 (Section 3.3) and continuing with a closer look at (some of the) actors (entities) of the ABC4Trust architecture (Section 3.4). Finally, in Sections 3.5-3.7 will present a more detailed architecture of the ABC4Trust entities from the perspective of ISO/IEC 29101, describing the implemented components in each of them.

Sections 3.5-3.7 have been modelled similarly to the "Annex A" of ISO/IEC 29101. Each entity's ICT system is represented in a tabular format, depicting the implemented Privacy, Identity Management and Data handling features, as defined in the Standard (ISO/IEC 29101), followed by an explanation of the implemented features. For the extensive list of the features that can be implemented in the respective entities' ICT systems, one should consult the standard ISO/IEC 29101.

3.2 Brief description of the ABC4Trust architecture

In the architecture of ABC4Trust, an *Issuer* issues a certified list of attributes (a *credential*) to a *User*, thereby vouching for the correctness of the information contained in the credential with respect to the *User* to whom the credential is issued [12]. Before issuing such a credential, the *Issuer* may have to authenticate the *User*, which it may do either using Privacy-ABCs, using a different online mechanism (e.g., username and password), or using out-of-band communication (e.g., by requiring the *User* to physically present herself at the *Issuer*'s office).

Having obtained the ABCs, a *User* is able to request a service provided by a *Verifier*.

A *Verifier* protects access to a resource or service that it offers by imposing restrictions on the credentials that Users must own and the information from these credentials that Users must present in order to access the service. The Verifier's restrictions are described in its presentation policy. The User generates from her credentials a presentation token that contains the required information and the supporting cryptographic evidence. The role of a Verifier is sometimes also referred to as a relying party (as it relies on the credential certification performed by the Issuer) or a service provider.

Note that the ABC4Trust architecture recognizes additional actors beyond those presented in this chapter, but they have been omitted here for a better understanding of its main features (for a complete description see Section 1.3).

[5] In this chapter, ISO/IEC 29101 always refers to the "ISO/IEC 29101 (4th Committee Draft) – Information technology – Security techniques – Privacy architecture framework".

[6] More information about the project and the architecture can be found at the project's website: https://abc4trust.eu/

3.3 Introduction into ISO/IEC 29101

ISO/IEC 29100 [13] "provides a high-level framework for the protection of personally identifiable information (PII) within information and communication technology (ICT) systems. It is in general nature and places organizational, technical, and procedural aspects in an overall privacy framework." On the other hand, ISO/IEC 29101 [14] builds on the privacy framework provided by ISO/IEC 29100 and more speficially "describes a privacy architecture framework that:

- Describes concerns for ICT systems that process PII;
- Lists components for the implementation of such systems; and
- Provides architectural views contextualizing these components."

ISO/IEC 29101 is primarily focused on ICT systems that are designed to interact with PII principals and shoes how privacy-enhancing technologies can be used to build better privacy controls.

3.3.1 Terminology

ISO/IEC 29101 applies the terminology defined in ISO/IEC 29100 [14].

For the purposes of the discussion presented in this chapter, the definitions presented in Table 3-1 will suffice.

Table 3-1: Definition of terms for the main framework actors, as defined in ISO/IEC 29100

Term	**Definition in ISO/IEC 29100**
Personally identifiable information (PII)	any information that (a) can be used to identify the PII Principal to whom such information relates, or (b) might be directly or indirectly used to identify the PII principal
PII Principal	natural person to whom the personally identifiable information (PII) relates
PII Controller	privacy stakeholder (or stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes
PII Processor	privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

3.4 Purpose, Actors and Deployment of the ABC4Trust architecture

The purpose of this architecture is to provide a generic model for a privacy-friendly identity management system, which can be adopted and deployed in specific target applications. The model is based on the concept of long-lived credentials (privacy- ABCs), which employ privacy-enhancing technologies that eliminate (credential usage) linkability and traceability issues that traditional IdM systems suffer from.

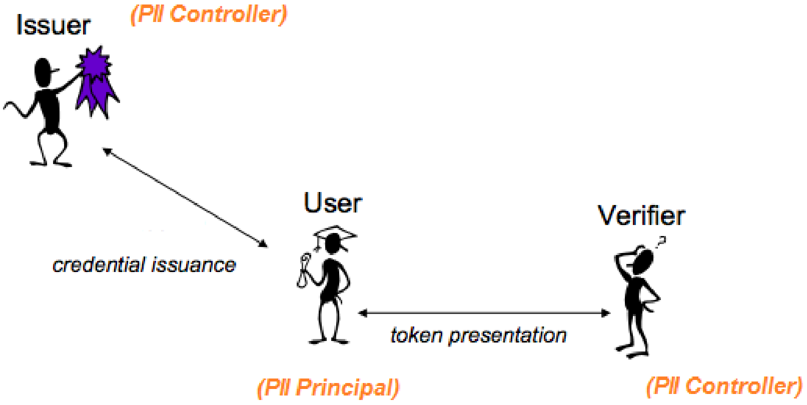

Figure 3.1: ABC4Trust architecture – An overview of (a subset of the main) Actors and their interactions

Error! Reference source not found. gives an overview of the main actors in the ABC4Trust architecture and the interactions between them:

1. The (ABC4Trust) *User* represents the PII Principal. The information system at the *User* part is typically a software component running either locally at the user's machine or located on a trusted cloud service. As PII and some corresponding user secrets will have to be kept safe, the PII principal's information system may be a combination of high-security storage component (such as a smart-card) and the respective software component.
2. We can identify two different PII controllers in this architecture:

    a. A *Verifier* is a typical PII controller, as it needs to collect and verify certain attributes about the user requesting its services. The information system at this PII controller is typically a web application, but it can also be employed in any other type of communication technology that can support ABCs.

    b. An *Issuer* can also be seen as a PII controller, as it needs to process certain information regarding the User (PII Principal) in the case when a user requests credentials issuance, which can be regarded as a service. This can be a service that is either provided through an online web application or an application running locally at the Issuer's premises and users may in this case be required to present their information in alternative means, such as paper or even direct physical contact. A major difference in the two PII controllers in this scenario is their respective trust relationship with the User (the PII Principal).

3. The current level of the architecture is not bound to the use of a PII processor, as this would be out of the scope for a generic architecture at this level of detail and consequently out of scope for this chapter. A concrete application may or may not use a PII processor.

In an actual scenario, some of the above roles may actually be fulfilled by the same actor or split among many. The flows presented here show only the big picture of the architectural model, but particular deployments may incorporate further flows.

3.5 Architecture for the PII Controller 1 (Issuer)

In the spirit of ISO 29101, the Issuer can be seen as a *PII Controller* that responds to the PII principal’s (credential issuance) requests.

Table 3-2: Architecture at the PII Controller's (Issuer's) ICT

Category	**Implemented features**		
Privacy Settings	Policy and Purpose Communication	PII Categorization	Consent Management
Identity Management	Identity Management System		Access control
	Authentication		Authorization
Data	Data Management		Data Transfer
	Data Inventory		Audit logging

3.5.1 Privacy Settings

- Privacy and Purpose Communication: The ICT of the Issuer will deliver the issuance policy and the purpose of the data collection from the User through the communication channel used during information processing.
- PII Categorization: Attribute information upon which the Issuer issues a credential is always considered to be sensitive. Therefore, the Issuer treats all the attribute information equivalently.
- Consent Management: The user will be requesting a credential to be issued and this is the explicit consent of the user. Of course, the Issuer will take care to properly handle the credential validity time and consequently sync this information in a way that both the PII Principal and the PII Controller are aware of it.

3.5.2 Identity Management

- Identity Management System: The Issuer vouches for the correctness of the information contained in a credential; therefore, the Issuer checks whether the attributes are indeed valid and may need to identify the User before being able to issue him/her a credential.[7]

[7] Note that identification here does not include uniquely identifying the user. If the credential is being issued using “carried-over” attributes, the PII principal may be anonymous and the Issuer might not know the value of such attributes.

Authentication of the User is out of the scope of the architecture and it may be provided along with the issuance messages.

- Authentication, Authorization and Access Control: In order for the Issuer to start an issuance of a credential, it needs to authenticate the User. Therefore, an appropriate access control must be in place, but this is not in the scope of the architecture and it is up to the target application to decide on this. On the other hand, the Issuer can also authenticate itself towards the User.

3.5.3 Data

- Data Management: The necessary Principal PII may already (a-priori) be available to the Issuer. The Issuer makes a decision on the issuance of a certified credential upon the attributes it already knows about a User. However, there is a special scenario when the Principal possesses a subset of attributes, which have previously been certified (carried-over from a previously certified credential), in which case the Issuer does not need to see the actual values of such attributes, but merely combines them into a newly issued credential.
- Data Transfer: In the case of the data transfer over the Internet, the Issuer ICT is capable of accepting secured connections to protect the confidentiality of the PII. This depends on the specific application and is not covered in the scope of the architecture in detail. Also, some of the Issuer data (such as credentials) may be stored in another highly-secure storage and the architecture can support such data transfer, but necessary security measures must be taken at the respective implementation, which is not in the scope of the architecture provided here.
- Data inventory: The Issuer is able to keep an inventory of the exchanged tokens, pseudonyms and other transaction logs for archiving purposes, revocation or other previously specified purposes. In such a case, it may be able to produce the total number of received tokens and used pseudonyms.
- Audit logging: An Issuer may keep a log of transaction material for audit purposes, as well as evidence for the (issuer-driven) credential(s) revocation(s).

3.6 Architecture for the PII Controller 2 (Verifier)

The (ABC4Trust) Verifier is an entity that provides services to different Users, while enabling them to authenticate using Privacy Attribute-Based Credentials issued by an/a (trusted) Issuer.

3.6.1 Privacy Settings

- Policy and Purpose Communication: The Verifier presents a Presentation Policy to the User, asking the User to present a proof of possession or (optionally) disclose values of certain attributes, in order to grant the User access to the request resource (service). Additionally, the presentation policy specifies if the presentation token can be "inspected" and/or "revoked". However, these two features will be omitted in the description of this chapter.
  In addition, ABC4Trust architecture provides the possibility for the Verifier to specify a link to the relevant privacy policy, for each attribute the User must reveal. On the other hand, the specific privacy policy and communication of the purpose of information processing are not in the scope of the ABC4Trust architecture, as this is completely application-specific and should therefore be specified in a target application that is implemented using the architecture of ABC4Trust.
- PII Categorization: In general, the Verifier receives (cryptographic) proof of possession of certain the attribute values (the PII themselves) or the values of the attributes the User must reveal. In the latter case, it is up to the specific Verifier application to employ necessary categorization of the PII it receives from the User.

- Consent Management: Application specific, not in the scope of the current level of the architecture.

3.6.2 Identity Management

- Identity Management System: Normally, the Verifier stores the user-generated tokens, presented to it and/or (possibly) a minimal subset of identity information about the PII Principal, which have been revealed by the User itself. The ICT of the Verifier may typically store information regarding credential types, credential identifiers and other user-generated cryptographically evidence, which can be used for non-repudiation purposes. This information does usually not provide linkability between different sessions a User opens, except in the case when the Verifier supports the use of scope-exclusive pseudonyms, under which a User can log in multiple times. Still, the User can still remain anonymous, but linkable. On the other hand, a special care should be taken to the presentation policy and the combination of the attributes the User reveals, since such information might be highly identifying.

Table 3-3: An overview of the architecture at the PII Controller's ICT (Verifier)

Category	Implemented features		
Privacy Settings	Policy and Purpose Communication	PII Categorization	Consent Management
Identity Management	Identity Management System		Pseudonymization scheme
	Access control	Authentication	Authorization
Data	Data Management		Data Anonymization
	PII encryption		Audit logging

- Pseudonymization scheme: The ICT system at the Verifier supports the use of cryptographic pseudonyms, which provide a controlled linkability to the user profile, but reveals nothing about the identity behind the credential. A *Pseudonym Scope* provides the ability to limit the scope of the use of a pseudonym. A Verifier can offer a User to use many unlinkable pseudonyms or it may enforce the use of a single pseudonym ("*scope-exclusive pseudonym"*) in cases when such a solution is desired or required by the business model (such as multiple voting possibilities, single vote count).
- Authentication, Authorization and Access Control: The Verifier's ICT enforces User authentication and specifies the necessary proofs the User must present in order to (be authorized) to gain access to its services. The Verifier's ICT system receives a presentation token from the User and compares it to the required presentation policy previously sent to the User to decide whether or not the presented proof makes the User eligible for its services.

3.6.3 Data

- Data Management: A Verifier data management definition is application-specific, but some requirements about data management are defined relating to maintaining local revocation lists, Issuer certificates, used presentation tokens, pseudonyms.
- Data Anonymization: This is related to the description of the Identity Management System. Data anonymization may be required when the Verifier stores the values of the PII it has received from the User. However, the ABC4Trust architecture does not define a specific mechanism for anonymizing such data, as this is left to a certain application that uses the architecture of the Verifier.
- PII encryption: For the disclosed attributes, The Verifier receives them in cleartext and no previous encryption has been implemented on these data. Encryption of such values for further processing purposes may be implemented in a specific Verifier application, but that is not defined at the ABC4Trust architecture level. For the undisclosed attributes, the Verifier receives only a cryptographic proof and PII about the User, thus no encryption is necessary for these data.
- Audit logging: The Verifier may (need to) keep logs of the performed transactions for audit purposes, as well as the list of received tokens, pseudonyms and other transaction metadata. Additionally, it may keep a local list of attributes of the revoked credentials (for the Verifier-driven revocation).

3.7 Architecture for the PII Principal (User)

3.7.1 Privacy Settings

- Policy and purpose communication: The User receives (from the Verifier) in the presentation policy a link to the respective privacy policy, for each of the attributes the User must reveal. The ICT of the User is capable of handling such a communication.
- PII Categorization: In general, the ICT of the PII Principal is capable of handling the credentials, which prove certain attributes about the User, but at this level of the architecture, it is not meant to specify if different categories are used to classify them. As for most of the other details, it is up to a certain application/scenario to specify it.
- Consent Management: The implementation of this component is not in the scope of the ABC4Trust architecture. This is also application specific, but in principle any application that uses ABCs should adhere to the legal requirement that the Principal consent should always be in place in order to initiate any further protocol steps. However, the User consent is always present in any implementation, as the ICT of the User provides a User Interface for *Identity Selection*, where the User can explicitly choose the credentials and/or values of attributes she/he wants to use to generate a proof in response to a presentation policy.
- Privacy Preference Management: In response to a presentation policy or a list of them, the ICT of the PII Principal gives the Principal the choice of selecting the desired presentation policy they want to create a presentation token for. Additionally, if different combinations of user credentials can be used to fulfil the selected presentation policy, then the user has the choice to decide which of them he/she wants to use for the token generation.

3.7.2 Identity Management

- Identity Management System: The ICT of the Principal stores information about the credentials that the Principal has in possession and the tokens it has generated. However, an Issuer can support issuance of a credential using "advanced features", such as "*self-claimed"* and/or *"carried-over"* attributes, under which the (ICT of the) User can control the attribute values it wants to have certified (in a credential).

- Pseudonymization scheme: By design, the ICT of the PII Principal implements pseudonymization schemes that are compatible with the ones that are supported by Verifier. The ICT of the PII Principal is able to differentiate between what the ABC4Trust architecture defines as "certified", "verifiable" or "scope-exclusive" pseudonyms and handle them accordingly.
- Authentication, Authorization and Access Control: the ICT of the Principal is able to authenticate the Verifier's Identity and also implement the necessary mechanisms to generate presentation tokens that fulfil the access requirements of the Verifier.

Table 3-4: An overview of the architecture of the PII Principal

Category	Implemented features			
Privacy Settings	Policy and Purpose Communication	PII Categorization	Consent Management	Privacy Preference Management
Identity Management	Identity Management System		Pseudonymization scheme	
	Access control	Authentication	Authorization	
Data	Data Management	Data Transfer	Data archiving and retention	Data pseudonymization
	Data Anonymization	Secret sharing	PII encryption	Data inventory

3.7.3 Data

- Data Management: The ICT of the PII is capable of processing the credentials the User keeps in a highly-secure location, but it need not be locally to the ICT of the PII principal.
- Data Anonymization: The ICT of the PII Principal is capable of performing the necessary cryptographic operations that transform the User credentials into tokens that reveal no PII attributes.
- Data Pseudonymization: As specified in the Pseudonymization scheme, the ICT of the Principal provides the possibility to create pseudonyms respectively.
- PII encryption: *Crypto Engine* component at the ABC Engine at the ICT of the PII Principle is responsible for creating and presenting a presentation token from the credentials, which is subsequently delivered to the Verifier. However, the encryption of the revealed PII is not covered in the current scope of the architecture.
- Secret sharing: In general, such a feature is not covered in the current architecture. However, the architecture identifies cases when it may be required that a joint creation of some random values must take place between the Issuer and the User (a sort of multi-party computation), which is then used used to generate certain features, such as credential serial number, device binding evidence and so on.

- Data Archiving and Retention: Specific data about the credentials (possibly together with the credentials) are to be stored in a highly secure storage, for instance in smart cards (optionally, but not limited to). However, it is up to the specific application to define if they want to implement certain back-up and restore mechanism for credentials.[8]
- Data Inventory: The ICT of the PII Principal can list the possessed credentials to the user, which are stored in a separate component called *Credential Store* inside the ABC Engine.
- Data Transfer: The ICT of the Principal is capable of processing data (credentials) located at external devices, such as smart cards or other location external to the ICT of the Principal. However, it is up to the specific implementation to take care of secure handling of the data on the transfer.

3.8 Conclusion

The ABC4Trust architecture, as generic as it is, presents a very good example of a technology designed with privacy features in the core of it. The architecture presented here provides a subset of the main ABC4Trust entities involved in a "normal" online transaction, but it is enough to show that it has built-in such technologies that makes most of the privacy concerns brought in the ISO 29101 solved even at this level of abstraction. Therefore, it provides a good example of how a well-designed architecture can already implement the privacy requirements independently of the target application using it, making it a lot easier for specific scenarios to adhere to the privacy principles in this part of the standard by just implementing the few remaining application-specific privacy protection mechanisms, as required in the standard.

With respect to privacy framework architecture, ABC4Trust architecture provides

- Non-linkability between the issuance and the presentation of a credential;
- A user-controlled profile traceability (when desired)
- Anonymous but highly assured authentication framework towards the Verifier;
- Protection mechanisms against malicious Issuers, Users or Verifiers (Multilateral Security);
- Minimal disclosure of only the attributes the Verifier truly needs;
- Protection against user impersonation in case the list of "customer data" (presentation tokens) get compromised by an intruder;
- Control over "multiple spending", where desired; etc.

[8] Backing up the credentials from the smart card has proven to be complex task, since the card will not (and should not) give away the secret key. However, this can be overcome by alternative solutions. In an ABC4Trust pilot, an identified solution backed up certain data that allow new credentials with identical attributes to be re-issued, thus creating a "clone" of the original data. However, the original secret key and the associated data in the smart card cannot be recovered.

4 Contribution to ISO/IEC 29191

4.1 Description

In this chapter, we compare the ABC4Trust architecture with the current Committee Draft of "ISO/IEC 29191 - Requirements for partially anonymous, partially unlinkable authentication" [15] and identify potential contributions from ABC4Trust to future versions of the Draft. This standard is an on-going project within ISO/IEC JTC 1/SC 27/WG 5 and is currently in the stage of 3rd Committee Draft. We identify the similarities and highlight the main incompatibilities between the definitions, concepts and requirements put forward by the two frameworks. Be aware, that we base our comparison on the terminologies adopted by the 2nd Committee Draft, so remarks may not apply to future and final versions. We will compare this towards ABC4Trust deliverable D2.1 [12], which thoroughly reflects the features and concepts behind attribute-based credential systems federated by the ABC4Trust architecture.

4.2 Scope and Purpose of ISO/IEC 29191

The overall purpose of ISO/IEC 29191 is to establish requirements for anonymous, unlinkable entity authentication. According to this paradigm, an entity is to be authenticated anonymously towards a verifier and authentication transactions are unlinkable in the sense that the verifier cannot tell whether two transactions are performed by the same entity. The text also introduces the notion of a designated opener, a third party who is given privileged information as per the system and can later reveal the entity's identity from authentication transcripts. The notion of an issuer, an entity who provides digital means to an entity to enable anonymous, unlinkable authentication, also appears in the current draft. In this respect, the scope of ISO/IEC 29191 is very similar in nature to the main roles and capabilities of ABC systems as described in D2.1 [12], despite a number of differences in the terminology that appear when taking a closer look at definitions, as described later on in more detail.

Interestingly, the scope of ISO/IEC 29191 covers ABC systems to some advanced degree; it also encompasses another cryptographic technology known as group signatures[9]. We think that understanding this characteristic helps capture the nature of the standard, and we therefore discuss this further in a dedicated section later in this chapter.

4.3 Comparing Terminologies in ISO/IEC 29191 and ABC4Trust

We will now first review the definitions of ISO/IEC 29191 and highlight their differences with the ones presented in ABC4Trust D2.1. To ease readability, we will make use of "curved quotes" when referring to the ISO/IEC 29191 terminology and underline the terms defined in the ABC4Trust framework. The other terms are to be taken according to their common sense.

[9] These can actually be seen as a special case of our privacy-ABCs where the signing key is a credential with one uniquely identifying attribute, and the signature is a presentation token for the signed message and inspection on the unique attribute.

4.3.1 Comparing High-Level Purposes

The purpose of ISO/IEC 29191 is to provide a general framework for what is referred to as “partially anonymous, partially unlinkable authentication”. The notions of anonymous and unlinkable authentication are omnipresent in the context of ABC4Trust and well-understood as properties achieved by the underlying ABC protocols and enforced by cryptographic means. However the standard makes use of the term “partially” which, to avoid any misinterpretation, refers in fact to the legal standpoint according to which an anonymous authentication that can later be “opened” to reveal the “Claimant”/User’s identity cannot be considered as being legally anonymous (the same remark also holds for unlinkability). From a technical viewpoint, though, the terminology “partially anonymous, partially unlinkable authentication” used in the standard refers to the exact same notion as the one of anonymous, unlinkable authentication in ABC4Trust, both notions quite explicitly considering the presence of a “Designated Opener”/Inspector in the deployed system.

4.3.2 Comparing Roles

The framework defined in ISO/IEC 29191 identifies four roles that are similar in nature to the ones described in deliverable D2.1. We refer the reader to N9914, Section 4.

“Issuer: an issuer is an entity who issues certificates to claimants“

This role is identical to the one of an Issuer in ABC4Trust D2.1, up to a reformulation of credentials as “certificates” and Users as “Claimants”. The common literature in identity management sometimes refers to this role as the identity provider or the attribute authority.

“Claimant: a claimant is one who will be authenticated by a verifier“

The term “Claimant”, as appearing in other standards in identity management, refers to an entity that claims access to a service or resource and is capable of authentication. In ABC4Trust parlance, this role is called the User and more specifically refers to a human User, who may be represented by a software User Agent and possibly make use of hardware tokens to manage and use credentials. The definition of ISO/IEC 29191 is therefore more abstract and general.

“Verifier: a verifier is one who checks whether the claimant possesses a valid certificate”

This role is similar to the definition of Verifier or Relying Party in ABC4Trust, which also refers to the conformity to a presentation policy although that notion is left unspecified in ISO/IEC 29191. In both frameworks, the “Verifier”/Verifier is assimilated in spirit to a service provider who grants or denies access to a service or resource.

“Designated opener: a designated opener is an entity who can re-identify a claimant from the transcript of authentication”

The role of the “Designated Opener” consists in “opening” a “transcript of authentication” to reveal the full identity of the “Claimant”, an operation sometimes called “re-identification of the Claimant” in N9914. In ABC4Trust, this role is played by the so-called Inspector, and the “opening” functionality is referred to as inspection. In the ABC4Trust architecture, this feature is left optional and may or may not be enforced based on the Verifier’s presentation policy. The feature is not specified as optional in ISO/IEC 29191, resulting in that the capabilities of the architecture must be voluntarily restricted if one requires full conformity to the standard.

Furthermore, the notion of **revocation** is left unaddressed in ISO/IEC 29191. This concept is supported in the ABC4Trust architecture and operated by a Revocation Authority who can revoke credentials and may be imposed either by the Issuer or the Verifier. The architecture specifies that the Revocation Authority is meant to distribute up-to-date revocation information to both the User and the

Verifier and that authentication must fail whenever the User's credential in use has previously been revoked by the authority. Therefore, the revocation information provides an additional input to the authentication procedure and some form of online update must take place prior to proceeding to authentication.

The ABC4Trust architecture allows entities to play several roles in a concurrent manner; for instance an Issuer may also behave as a Revocation Authority and/or Inspector, or an Issuer may also be a Verifier at a later time in the envisioned application. The fact that several roles may be fulfilled by the same entity in deployed applications is left unaddressed in ISO/IEC 29191.

4.3.3 Comparing Operations and Data Objects

N9914 (Section 4, page 2) defines three high-level processes whereby entities interact with each other or process data received from other entities:

1. **Process 1:** "a process between an Issuer and a Claimant to perform a certificate issuing process. After this process a user has a certificate";
2. **Process 2:** "a process between a claimant and a verifier to perform authentication. Authentication is successful if the verifier can verify the possession of a valid certificate";
3. **Process 3:** "A process by a designated opener to [re-]identify the Claimant from the transcript of authentication".

The ABC4Trust architecture supports these three processes: D2.1 (Section 1) refers to them as

- Issuance of a credential for Process 1,
- Generation of a presentation token (by the User) and Verification of a presentation token (by the Verifier) for Process 2,
- Inspection or de-anonymization of a presentation token (by the Inspector) for Process 3.

Therefore the notion of "transcript of authentication" referred to in the standard is instantiated in ABC4Trust by a presentation token, which in addition suggests that a single-pass transaction is realized between the User and the Verifier, although ISO/IEC 29191 considers that authentication may possibly have multiple transmissions back and forth between the two entities until the authentication protocol is complete.

However, ABC4Trust defines additional features and extends the semantics of ISO/IEC 29191 in several ways:

- A credential is defined as a certified container of **attributes**, an attribute being described by its attribute type (e.g. a date) and attribute value (e.g. Jan 1, 2012),
- When generating a presentation token at authentication time, the User may choose to disclose some attributes held within a credential to the Verifier and leave others undisclosed,
- The verification performed by the Verifier takes as input a presentation policy that has been transmitted to the User before the authentication actually takes place (alternatively, this can be viewed as a first pass in the authentication protocol, the transmission of the presentation token being seen as the second pass),
- ABC4Trust provides optional **user binding**[10], a mechanism that binds credentials to a private key only known to the User. The validity of a presentation token is ascertained only when the

[10] These is indeed so in architecture description in D2.1. However, in the upcoming version of the ABC4Trust architecture, there will be no difference between user and device binding, but there will only be a single "key binding". If the secret key is stored on a hardware token, then one essentially has device binding.

token contains an implicit proof of knowledge of the User's private key. This mechanism may be extended to hardware devices, meaning that a credential may be bound to a device owned by the User (notion of device binding),

- ABC4Trust supports the use of **pseudonyms**, a general-purpose identifier under which a User is known to a Verifier and that is possibly reused across several authentications over time. This feature allows a Verifier to constitute a pseudonymized profile of the User, should the User choose to present herself as a profiled user (e.g. with an account login or customer number). This allows a form of controlled linkability whereby a User lets the Verifier relate (some of) her transactions to a known pseudonym. Most importantly, it allows users to create different unlinkable pseudonyms at different providers.

  Interestingly, ISO/IEC 29191 does not consider unlinkability as being optional and presents this property as a security requirement that must be enforced by the target application. ABC4Trust is therefore more flexible and general in this respect. In Section 1.4, D2.1even defines three types of pseudonyms (verifiable, certified and scope-exclusive) which are adapted to different use cases.

- The ABC4Trust architecture extends the functionalities of the ISO/IEC 29191 framework by providing a definitional background for the revocation of credentials, cf. D2.1, Section 1.8.

4.3.4 Comparing Requirements

ISO/IEC 29191 defines four requirements in N9914, Section 5:

"REQ. a) a claimant must be authenticated by a verifier without being identifiable by the verifier"

Although the term "identifiable" seems a black-and-white property of the authentication process according to this formulation, the ABC4Trust architecture achieves a policy-driven, maximal granularity of anonymity based on the minimal disclosure of the User's attributes. We may therefore consider that this requirement (and stronger versions thereof, where identification relates to certain specific attributes instead of being taken in the broadest sense) is readily enforced.

"REQ. b) the transcript of authentication must not provide information that can link multiple authentication transactions by the same claimant"

Since the ABC4Trust architecture leaves optional the use of pseudonyms and supports unlinkable authentication, this requirement can be seen as a restriction of the architecture to certain use cases where pseudonyms are not used by Users and Verifiers. Under this functional restriction, the ABC4trust architecture fulfills the requirement.

"REQ. c) the transcript of a successful authentication must contain the information necessary for the designated opener to re-identify the claimant"

Again, this requirement can be enforced by restricting the capabilities of the ABC4Trust architecture, which in its nominal version may enable or disable token inspection according to the Verifier's presentation policy.

"REQ. d) the designated opener must be able to provide evidence that the claimed identity is correct"

This feature is not supported as such by the ABC4Trust architecture; it would imply an additional cryptographic mechanism by which an "opened" presentation token (containing the Inspector's input transcript and the generated output) can be publicly checked for consistency. This functionality would require an adaptation of the underlying cryptography and could be achieved e.g. by making use of a non-interactive proof of knowledge of the Inspector's private key. In its current definition, however, the ABC4Trust architecture does not fulfill this requirement.

4.4 Comparative Summary

Summarizing the above discussion, we report our comparison on the following table.

ISO/IEC 29191	ABC4Trust Architecture	Comments
"Partially anonymous authentication"	Anonymous authentication	**Identical notions**, "partially" being added to comply with the legal standpoint
"Partially unlinkable authentication"	Unlinkable authentication	**Identical notions**, "partially" being added to comply with the legal standpoint
"Certificate"	Credential	**Similar definition**, although a credential refers to the notion of attributes
"Transcript of authentication"	Presentation token	**Similar definition**, although a "transcript" possibly collects multiple transmissions when authentication is performed
"Issuer" ("certificate issuing process")	Issuer (credential issuance)	**Similar definition**, although an ABC4Trust Issuer has more capabilities such as imposing a Revocation Authority
"Claimant" ("performs authentication")	User (generates a presentation token)	**Similar definition**, although an ABC4Trust User is a human represented by a User Agent and possibly hardware devices
"Verifier" ("verifies possession of valid certificate")	Verifier (verifies the presentation token)	**Similar definition**, although an ABC4Trust Verifier has more capabilities
"Designated Opener" (mandatory)	Inspector (optional)	**Similar definition**, optional in ABC4Trust, mandatory in ISO 29191
Not defined in ISO/IEC 29191	Presentation Policy (part of the architecture)	
Not defined in ISO/IEC 29191	Pseudonyms (optional)	
Not defined in ISO/IEC 29191	Revocation Authority (optional)	
Not defined in ISO/IEC 29191	User and device binding (optional)	
Requirement REQ. a) ("claimant not identifiable")	Minimal disclosure of attributes (policy-driven, totally customizable)	**Achieved**; more granular and refined in ABC4Trust
Requirement REQ. b)	Unlinkability versus Pseudonyms	**Achievable** by disabling the use of

("transcripts cannot be linked")	(can choose one or the other)	pseudonyms by Users
Requirement REQ. c) ("transcripts must be openable")	Inspection (optional)	**Achievable** by always requiring inspectable tokens in the Verifier's presentation policy
Requirement REQ. d) ("verifiable correctness of opening")	**Not supported in ABC4Trust**	**Requires an adaption** of ABC systems federated by the ABC4Trust architecture

4.5 Contributions to ISO/IEC 29191

To ease closing the gap between ISO 29191 and the federated architecture of ABC4Trust, one would have to harmonize the last three lines of the above table. However, it is easily seen that

- As long as requirement REQ. b) is mandatory in ISO/IEC 29191, there is a clear incompatibility with the use of pseudonyms. Therefore, either this feature is to be excluded from a ISO-compliant version of the ABC4Trust framework, or the requirement is to be relaxed in some technically sound fashion to allow a policy-driven, controlled linkability between "authentication transactions";
- As long as requirement REQ. d) is mandatory in ISO/IEC 29191, an ISO-compliant version of the ABC4Trust architecture shall have to provide a functionality that has not yet been taken into consideration. REQ. d) is indeed useful to give claimants a guarantee that they cannot be "framed" by cheating openers. Formalizing this requirement at the cryptographic level would probably introduce a new role to the system, a judge or so, who must be convinced by the evidence. This feature is currently not supported by ABC4Trust and can be taken as an action point within ABC4Trust WP3 for future research and adaptations.

We see several contributions from ABC4Trust to ISO 29191 with respect to requirement REQ. c) and the role of the "Designated Opener":

I. We suggest that this requirement be relaxed to allow a more flexible opening functionality depending on a presentation policy;

II. A proposed feature to be added to ISO 29191 is that the cryptographic information passed to the designated opener could optionally contain so-called "re-identification grounds" describing the circumstances under which the "Claimant" agreed that she may be "re-identified". We assume that it is out of scope of ISO/IEC 29191 to define how these grounds are expressed or how the "Designated Opener" checks that they are satisfied, but a crucial aspect is that these "re-identification grounds" be cryptographically bound to the cryptographic information passed to the "Designated Opener". As a consequence, a cheating "Verifier" should not be able to change the "re-identification grounds" that the "Claimant" agreed with in the first place (the ABC4Trust framework already supports this feature, which is referred to as Inspection grounds);

III. Maybe one trusts the designated opener to verify that "re-identification" is indeed appropriate, but not to learn the identity of the "re-identified Claimant". One could require protocols that ensure that the "Designated Opener's" collaboration is required to "re-identify" the "Claimant", but in such a way that the "Designated Opener" does not see the "Claimant"'s identity in the clear. This feature is currently not supported by the ABC4Trust framework but may be considered for addition in the future.

4.6 ISO/IEC 29191 and Group Signatures

Group signatures are a cryptographic technology that also fit in the framework of ISO/IEC 29191. For completeness, we provide here a brief overview of the main concepts behind group signatures to show how they can be used to implement an ISO 29191-compliant application.

In a typical group signature scheme,

- A group manager is a trusted entity who issues individual (group member) certificates to users;
- Certified users form a group. New users may join the group by being given a certificate by the group manager;
- A user makes use of her certificate to sign messages on behalf of the group. A group signature hides the user's identity in the sense that one cannot tell which group member generated the signature;
- Any group signature can be publicly verified by any third party using the group's public key;
- A privileged key (the opening key) can be used to "open" a group signature and reveal the identity of the group member who generated it. The opening key can be made independent from the group manager's private issuing key;
- Group signatures are unlinkable in the sense that one (even group members) cannot tell whether two signatures were generated by the same user.

In this respect, the roles defined by ISO/IEC 29191 can be associated with the different parties described above:

- The group manager instantiates the "Issuer",
- A user/group member is a "Claimant",
- Any third party can play the role of the "Verifier",
- Any entity being given the opening key can play the role of the "Designated Opener". This role is a priori different from the "Issuer's".

The first three requirements described above are readily fulfilled thanks to the basic cryptographic properties of any group signature scheme. The fourth requirement REQ. d), namely that a signature opening should be publicly verifiable to avoid framing attacks whereby a certain user is wrongly incriminated, can be enforced on top of the first three by adapting the cryptography involved in the signature opening procedure. Therefore only some group signature scheme can simultaneously realize all four requirements imposed by ISO/IEC 29191.

Somehow, the definitions and scope of the standard are well-suited to group signatures, and the bibliographic references appearing in N9914 confirm that group signatures are of particular interest in targeted applications. Due to the general context of anonymous authentication, however, ABC systems also fit in the same definitional framework, making it conceivable to ensure an advanced level of compliance with the standard.

4.7 Conclusion

Overall, the ABC4Trust architecture supports more actors and features than what is defined in the framework for anonymous, unlinkable entity authentication put forward by the current draft of ISO/IEC 29191. To some extent, the model of architecture specified in D2.1 extends the functionalities introduced in the standard and allow a certain flexibility and customization of the first three requirements of ISO/IEC 29191. However, requirement REQ. d) is not supported as such by the architecture, although the underlying cryptography could probably be adapted to achieve it. We leave it as an open issue and as a potential topic for improvements and research in view of the second version of the ABC4Trust architecture.

5 Other related projects in standardization and Outlook

This deliverable highlights the relevancy of standardization for ABC4Trust as a project, followed by describing three ongoing standards projects within ISO/IEC JTC 1/SC 27 (Chapters 2-4), their implications for ABC4Trust and prospective contributions from the research carried out within the project.

There are, however, numerous other efforts underway, which are somewhat related to the project. Although, these projects have not been chosen as targets for outreach efforts at this point in time, they are maybe worth mentioning nevertheless. Finally, potential prospective activities in standardization are addressed, as the project further matures.

5.1 ISO/IEC JTC 1/SC 27

As described above, there are two groups of high relevance for ABC4Trust within ISO/IEC JTC 1/SC 27, namely WG 2 and WG 5.

In WG 2 there are two other multipart projects underway that relate to ISO/IEC 29191, which has been addressed in Chapter 4.

"ISO/IEC 20008 Information technology - Security techniques - Anonymous digital signature - Part 1: General" [16] specifies anonymous digital signature mechanisms. Its "Part 2: Mechanisms using a group public key" [17] goes in depth about those digital signatures that make use of a group public key to verify a digital signature; which could yield further input from aspects of section 4.6. Although all of the above are somewhat related to ABC4Trust work, they were not chosen as a priority for outreach activities for various reasons.

Equally, "ISO/IEC 20009 Information technology - Security techniques - Anonymous entity authentication - Part 1: General" [18] and "Part 2: Mechanisms based on signatures using a group public key" [19] has not been commented on until the date of this publication. Part 1 (ISO/IEC 20009-1) delivers the description of anonymous entity authentication mechanisms on the level of a general model (Part 1), while part 2 (ISO/IEC 20009-2) focuses more specifically on similar mechanisms using a group public key.

In WG 5 there are also two more projects of relevance, with one of them being close to publication, therefore not a plausible target for further contributions, and one being only related to ABC4Trust work.

"ISO/IEC 29115 Information technology - Security techniques - Entity authentication assurance" [20], which is currently Draft International Standard, delivers a metric for four levels of authentication assurance. How ABC credentials relate to such authentication levels might be an interesting subject for further research, since, ISO/IEC 29115 follows a traditional approach, usually matching real entities (often individuals). How this would relate to ABC technology is a subject that reaches beyond technological questions, but relates to requirements design, privacy (by design) and ultimately legal frameworks, often requiring real person authentication, where this may not necessarily the best option considering freedom and individual self-determination.

"ISO/IEC 29146 - Information technology - Security techniques - A framework for access management" [21] provides a framework for the definition of Access Management and the secure management of the process to access information. It is aimed to supplement ISO/IEC 24760 (see above) by describing the relevant services for access management. The project is, however, still under hefty development at Working Draft stage, and thus was not chosen to be a good candidate to concentrate ABC4Trust resources on, at this time. Also, the scope is slightly of topic for the core of ABC4Trust.

5.2 Integration with current Identity Management Implementations

There are, of course, numerous legacy Identity Management Implementations and elements thereof, such as X.509 [22], OAuth [23], OpenID [23, 24] with SAML, supplemented by Access Control languages such as XACML [25], and Trust Frameworks [26]. As shown in D2.1 [12], most of these integrate with ABC technology. For the latter, there already is specific work available [27], relating the U-Prove technology to WS-Trust.

5.3 Outlook: Standardization of WP2 XML formats?

Future work may approach standardizing the XML-formats developed in D2.1 [12], potentially within OASIS or W3C, although this must clearly be a deliberate decision, as there it does not make sense to standardize as a means in itself. Also concrete cryptographic schemes may be worth the effort, potentially within ISO/IEC JTC 1/SC 27/WG 2. The detailed data format mechanism of the underlying Identity Mixer technology are not yet defined well enough for standardization, but be very well be in the future.

6 References

[1] ABC4Trust Consortium, "ABC4Trust - Project description", 2010.

[2] European Commision, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)" *Official Journal of the European Communities*, 2002.

[3] European Commision, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" *Official Journal of the European Communities*, vol. 23, p. 31, 1995.

[4] T. Weichert, "Datenschutzzertifizierung - Vorteile für Unternehmen," in *ITK-Kompendium 2010: Expertenwissen, Trends und Lösungen in der Informations- und Kommunikationstechnologie*, M. Neudörffer, ed. Frankfurt am Main: FAZ-Institut, 2009, pp. 274-279.

[5] European Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" 2012.

[6] T. Christiansen and M. Dobbels, "Implementing and Delegated Acts after Lisbon-Towards the Parliamentarisation of Policy-Implementation? Paper for Presentation" in *Decision-Making in the European Union Before and After Lisbon, Leiden,* 2011.

[7] "ISO/IEC Guide 2:2004 Standardization and related activities - General vocabulary", Geneve, Switzerland, 2004.

[8] WTO, "Agreement on Technical Barriers to Trade," ed: World Trade Organization, 1979.

[9] JTC 1/SC 27/WG 5, "ISO/IEC 24760-1:2011 Information technology -- Security techniques -- A framework for identity management - Part 1: Terminology and concepts", 2011.

[10] JTC 1/SC 27/WG 5, "ISO/IEC 24760-2 (2nd WD): Information technology - Security techniques - A framework for identity management - Part 2: Reference architecture and requirements", 2011.

[11] JTC 1/SC 27/WG 5, "ISO/IEC 24760-3 (1st WD): Information technology - Security techniques - A framework for identity management - Part 3: Practice", 2011.

[12] I. Krontiris (ed.), "D2.1 Architecture for Attribute-based Credential Technologies – Version 1", 2011.

[13] JTC 1/SC 27/WG 5, "ISO/IEC 29100:2011 Information technology - Security techniques - Privacy framework", 2011.

[14] JTC 1/SC 27/WG 5, "ISO/IEC 29101 (4th CD): Privacy Architecture Framework", Geneva, Switzerland, 2011.

[15] JTC 1/SC 27 WG 5, "ISO 29191 (2nd CD): Requirements for partially anonymous, partially unlinkable authentication", 2011.

[16] JTC 1/SC 27 WG 2, "ISO/IEC 20008-1 (3rd WD): Information technology - Security techniques - Anonymous digital signature - Part 1: General", Berlin, Germany, 2011.

[17] JTC 1/SC 27 WG 2, "ISO/IEC 20008-2 (3rd WD): Information technology - Security techniques - Anonymous digital signature - Part 2: Mechanisms using a group public key", 2011.

[18] JTC 1/SC 27 WG 2, "ISO/IEC 20009-1 (3rd WD): Information technology - Security techniques - Anonymous entity authentication - Part 1: General", 2011.

[19] JTC 1/SC 27 WG 2, "ISO/IEC 20009-2 (3rd WD): Information technology - Security techniques - Anonymous entity authentication - Part 2: Mechanisms based on signatures using a group public key", 2011.

[20] JTC 1/SC 27/WG 5, "ISO/IEC DIS 29115: Information technology - Security techniques - Entity authentication assurance", 2011.

[21] JTC 1/SC 27/WG 5, "ISO/IEC WD 29146: Information technology - Security techniques - A framework for access management", 2011.

[22] ITU-T, *ITU-T. X.509 : Information technology-Open systems interconnection-The Directory: Public-key and attribute certificate frameworks*: International Telecommunications Union, 2008.

[23] Internet Engineering Task Force: *OAuth Web Resource Authorization Profiles*, 2010.

[24] OpenID: *OpenID Authentication 2.0*, 2007.

[25] T. Moses (ed.), *eXtensible Access Control Markup Language (XACML) Version 2.0* (OASIS Standard), 2005.

[26] A. Nadalin *et al.* (eds.), *WS-Trust 1.4*, OASIS, 2009.

[27] C. Paquin, *U-Trust WS-Trust Profile V1.0*, Microsoft, 2011.