

BRIDGES - Publishable summary

The Security dimension of Copernicus encompasses three main areas: Border Surveillance, Maritime Surveillance and Support to EU External Action (SEA). The Copernicus Security services are envisaged to be deployed in 2015; therefore their governance structures and the operational services need to be in place.

The overall objective of the BRIDGES project, coordinated by the EU Satellite Centre (EU SatCen), was the development of several potential models of governance for future Copernicus Security services in particular in support to EU External Action.

In order to support the EC in the smooth implementation of the service while ensuring the continuity and scaling-up of service provision, the BRIDGES consortium has studied the legal and political framework, evaluated different governance options and defined a roadmap for the future development of the services beyond the BRIDGES project.

During the project lifetime, particular attention was given to follow the political framework evolution in accordance with the progressive adoption of the Copernicus Regulation.

The involvement of the stakeholders during the entire project duration was also of strategic importance and has been very successful since the beginning of the project. Many stakeholders, such as European External Action Service (EEAS) including Crisis Management and Planning Directorate (CMPD), MD Crisis Response and Operational Coordination (MD CROC) and EU Intelligence Analysis Centre (INTCEN); European Commission (including DG ENTR, DG ECHO, Joint Research Centre, etc.), ESA, EDA and Member States, participated actively in the project.

One of the main concerns expressed during the BRIDGES stakeholder consultation was the issue of the protection of the Security interests of the Union and its Member States. SEA services address sensitive topics usually related to the foreign policies of Member States.

Governance options studied within the project were put in practice in the framework of the G-NEXT and G-SEXTANT FP7 projects, the two projects implementing the pre-operational services for Support to EU External Action.

These projects clearly indicate that the users require a fully operational service accompanied by appropriate governance as soon as possible, as the current pre-operational services do not have the capacity to fully meet their needs.

The main conclusion and policy recommendation is that the most promising and cost-effective governance model is based on a decentralized approach in which the SatCen has the role of operator of Copernicus services in support to EU External Action.

Summary description of project context and objectives

In the context of the GMES/Copernicus programme (Global Monitoring for Environment and Security), BRIDGES was aimed at developing scenarios and implementation options for the future governance of the security dimension of GMES/COPERNICUS. Taking into account the current institutional framework, the project has also considered the potential role of the European Union Satellite Centre (EUSC), the only operational EU Agency supporting EU Missions and Operations as well as decision-making by delivering geospatial information.

GMES/COPERNICUS services for Security applications are approaching operational maturity. Pre-operational services in the fields of border control, maritime surveillance and support to external action are benefitting from development and user engagement through a number of FP projects.

BRIDGES has therefore examined, by means of a structured stakeholder dialogue, the technical, financial and legal implications of several governance scenarios in the context of future operational deployment of GMES/COPERNICUS services in the field of Security.

BRIDGES was aimed at supporting the definition of the future governance of operational GMES/COPERNICUS services for Security applications including a possible role of the European Union Satellite Centre, through a structured dialogue among stakeholders.

The EUSC could serve as the natural interface between GMES/COPERNICUS services and Common Foreign and Security Policy (CFSP)/CSDP users. In addition, it is ideally situated to support the identification of options for a coordinated approach to Space data access in the Security field.

Governance relates to consistent management, cohesive policies, guidance, processes and decision-rights for a given area of responsibility.

A fair governance implies that mechanisms function in a way that allows the executives (the "agents") to respect the rights and interests of the stakeholders (the "principals").

Main S & T results

The Copernicus Services in Support to EU External Action entered their pre-operational phase in the framework of the G-NEXT and G-SEXTANT FP7 projects.

A service portfolio has been issued within the SEA Working Group under the leadership of DG ENTR following an extensive and detailed consultation with the user community, building on the considerable user engagement work performed by precursor projects (e.g. G-MOSAIC). The experience acquired through the G-NEXT and G-SEXTANT projects clearly indicates that the users require a fully operational service as soon as possible, as the current pre-operational services do not have the capacity to fully meet their needs. State of play of

the legal and political framework: In regard to the political and legal framework, there has been some debate about the framework in which the services in Support to EU External Action should operate during the legislative procedure for the adoption of the Copernicus Regulation. The field of EU External Action is mentioned in the proposed Regulation without restriction or further definitions of the field of application. It includes consequently the support to CFSP/CSDP policies:

“(f) the security service, which shall provide information in support of the civil security challenges of Europe improving crisis prevention, preparedness and response capacities, in particular for border and maritime surveillance, but also support for the Union’s external action, without prejudice to cooperation arrangements which could be concluded between the Commission and various Common Foreign and Security Policy bodies, notably the European Union Satellite Centre (EUSC).”

Particular attention was therefore paid to this consideration during the process of defining the potential governance structures. This situation also evolved during the legislative procedure of the Copernicus Regulation. The Regulation stipulates that specific measures be taken by the Council in order to counteract risks and threats to the Security of the Union or its Member States. This stipulation is intended to reassure Member States that any sensitivity issues that could potentially arise from the use of high-resolution imagery or Copernicus information service would be addressed appropriately. Another central question which has been extensively discussed with the stakeholders in BRIDGES concerns the modus operandi of service implementation. The Regulation proposes two approaches: (i) a centralised approach, if the expertise required for the effective operation of the services exists within the Commission; (ii) a decentralised approach if the operation of the services would require expertise from EU stakeholders not directly employed by Commission Directorates General (DG). An example of the centralised approach is the Emergency Management Service (EMS) operated by DG ECHO and the JRC. If the decentralised approach is adopted, the Commission has already selected several agencies that may become responsible for the implementation of Copernicus services, such as the European Maritime Safety Agency (EMSA), Frontex and SatCen. These three agencies are renowned for their expertise in the Security domain; the Commission has already indicated that Frontex and EMSA could have a role in the operations of the Copernicus Border Control and Maritime Surveillance services respectively. In purely logical terms, SatCen would be associated with the field of Support to EU External Action. Given, however, that the SatCen is also a Common Foreign and Security Policy (CFSP) agency, its cooperation with the Commission is a more delicate matter, seen from a legal and financial perspective. The work carried out in the context of the BRIDGES project provided clarity on some of these points which are reflected in the Governance Options and the Roadmap proposed by the project.

The work carried out in the context of the BRIDGES project provided clarity on some of these points which are reflected in the Governance Options and the Roadmap proposed by the project.

Governance options were proposed by BRISGES. Governance is widely understood to denote the rules and the organisational structures set up to govern a system or an entity. The governance framework adopted for the Security services should respect the rights and interests of the wide range of stakeholders involved in this area, embodying the principles of fairness and consistency. The provision of Copernicus Security services presents a range of challenges that do not necessarily arise in other areas of application, or in some cases only marginally (for example, the Emergency Management Service does not address the potential security classification of products). In some cases, a well-defined and functioning governance structure play a decisive role in the services being accessible to the users, in particular if users already have pre-existing or preferred channels for accessing or exchanging information and data. In addition, the governance model has a significant impact on the confidence the users have in the service and therefore on the extent of user uptake. For example, if governance structures are improperly set up, the following two potential problems – representing opposite and extreme scenarios - may arise:

(i) “Overprotection” (i.e. unnecessary restrictions on distribution) of information, and (ii) Uncontrolled dissemination of sensitive information.

The consequences of both scenarios are equally undesirable because they contradict two very important principles:

1. On the one hand, the principle of full and open access to Copernicus data; 2. On the other, the protection of sensitive information that could potentially compromise the Security of the EU, Member States and other stakeholders (e.g. a map showing of the location of an Internally Displaced Persons (IDP) camp could be used by hostile forces to plan an attack).

Both scenarios (i) and (ii) have a direct impact on the work of the users and on the Security of EU citizens in a more general sense. The model of governance selected for the Copernicus Security services must strike a balance between the two extreme situations referred by the scenarios, taking into account the importance of ensuring appropriate access to data for stakeholders while also ensuring that any sensitive information is not distributed. These aspects have been extensively analysed in particular in the context of SEA. One of the key issues is the selection of an appropriate operator for the service. The operator will be responsible for implementing the service in line with the Commission’s directives, coordinating user access through a single point of entry and organising service provision in collaboration with industry. Additionally, the operator will also have to ensure that the service activations are authorised by the relevant authorities and that during the provision and distribution of products, sensitive information is treated appropriately. During the BRIDGES final workshop, held on the 30th of January 2014 on the EEAS premises in Brussels, the three governance options assessed by the project were presented to stakeholders. Following further feedback and analysis, two of these options remain under consideration for their potential implementation in the future.

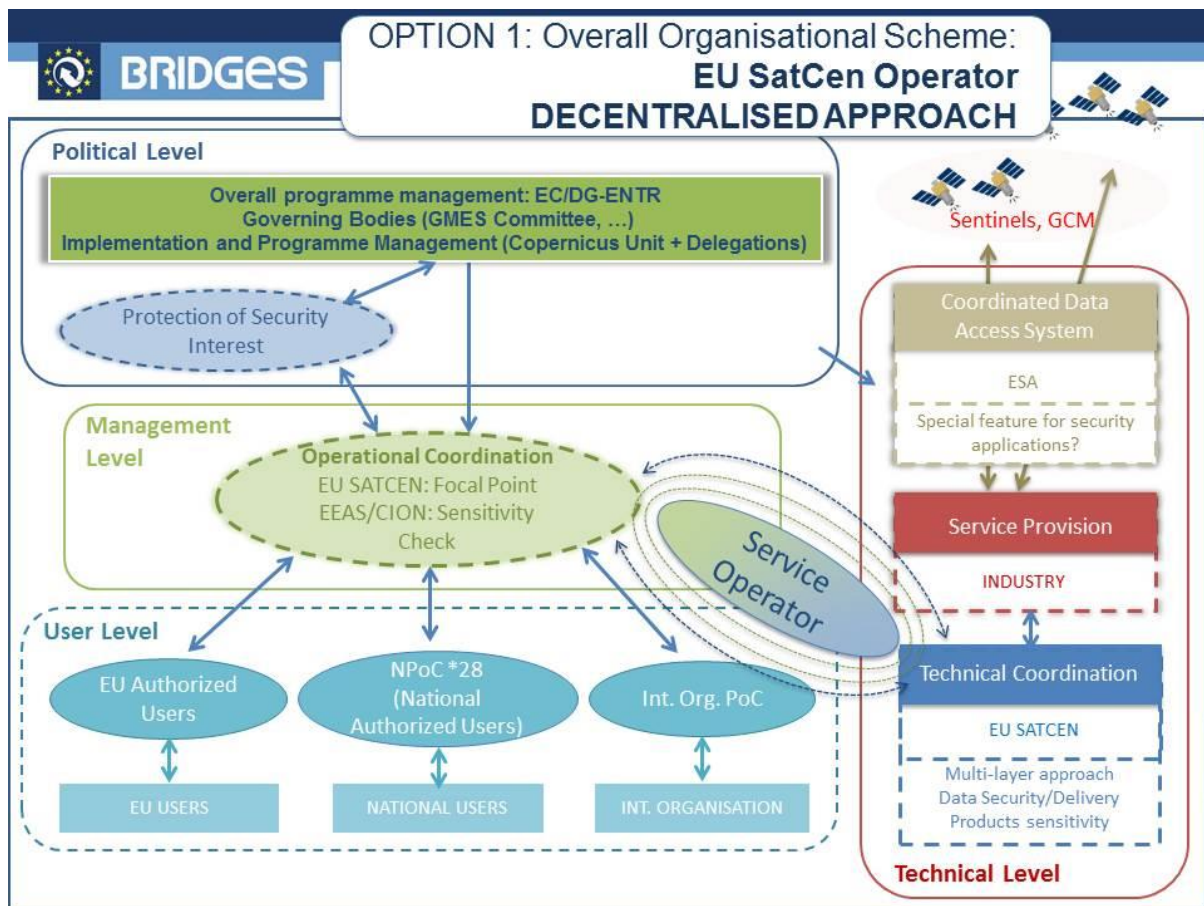


Figure 1 Option 1: EU SatCen Operator decentralised Approach

Option 1: The first option is based on a decentralised approach relying on the expertise of SatCen to operate the service. This option is the option preferred by stakeholders, and the one which offers the best cost/benefit ratio, according to the cost/benefit analysis conducted within BRIDGES. According to stakeholders, there are a number of advantages to this approach. The option is in line with the orientation of the Copernicus Regulation involving identifying an agency as a potential operator. This takes into account user requirements and ensures user uptake; SatCen has been involved in the development of the service for several years, and is trained as a service operator (Service Coordinator in G-NEXT). Such an approach generates economies of scale and facilitates synergies by using existing EU infrastructure. Information provided by SatCen image analysts could be overlaid with Copernicus data creating integrated EU information services to support EU External Action. However, there are factors that may compromise the implementation of this option in case the necessary institutional discussions and procedures would suffer delays. An update of the legal text which describes the functioning of SatCen (the EU SatCen Council Decision) is currently being discussed within the EU institutions and is likely to incorporate measures aimed at facilitating the participation of SatCen in Commission Space programmes; SatCen's role in Copernicus will depend to a large extent on the approval of this text. In addition, the financial rules of SatCen would have to be compatible with the delegation of funds from the Commission (although this issue was examined in BRIDGES and not found to create a major obstacle). The cooperation between Commission and CFSP bodies is a complex issue; it is

nevertheless possible, this being confirmed by the text of the latest draft of the Regulation, in which SatCen is mentioned as a potential operator.

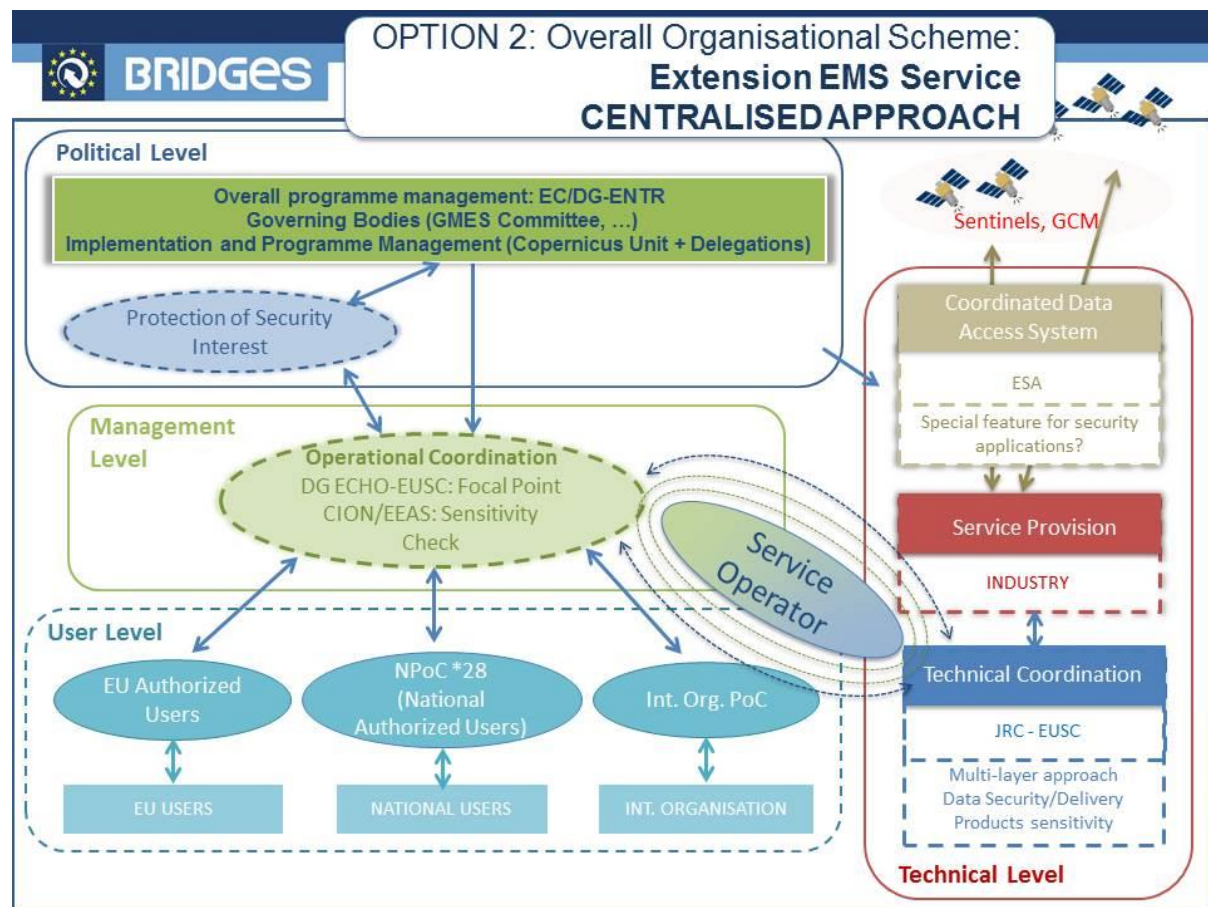


Figure 2 Option 2: Extension EMS Service Centralised Approach

Option 2: The second option is a centralised approach which would seek to use the existing operational structures of the Emergency Management Service. This approach has both advantages and disadvantages, which should be considered and compared with those of the first option, if the second is considered for implementation. The main advantage of the second option is that it might be implemented rapidly as it builds on an existing Copernicus service and the fact that there are no legal obstacles to its direct implementation by the Commission DGs. However as with the first option, there are factors that could delay or hamper the implementation of this second approach. There are currently no mechanisms in place to fully address data sensitivity in the Emergency Management Service; EMS operators (DG ECHO and JRC) do not have existing mechanisms or channels to coordinate access for the External Action user community, and this could lead to the risk of an overlap with SatCen activities. The full feasibility of implementing either of the two options cannot be assessed at present, since the two key legal documents are still in the process of being adopted: 1) the EU SatCen Council Decision 2) the Copernicus Regulation. In conclusion, the work undertaken in the context of the BRIDGES project shall now be continued at an institutional level (SatCen, EC, EEAS, etc.) and at a technical level (G-NEXT and G-SEXTANT). A roadmap for this ongoing activity is proposed hereafter.

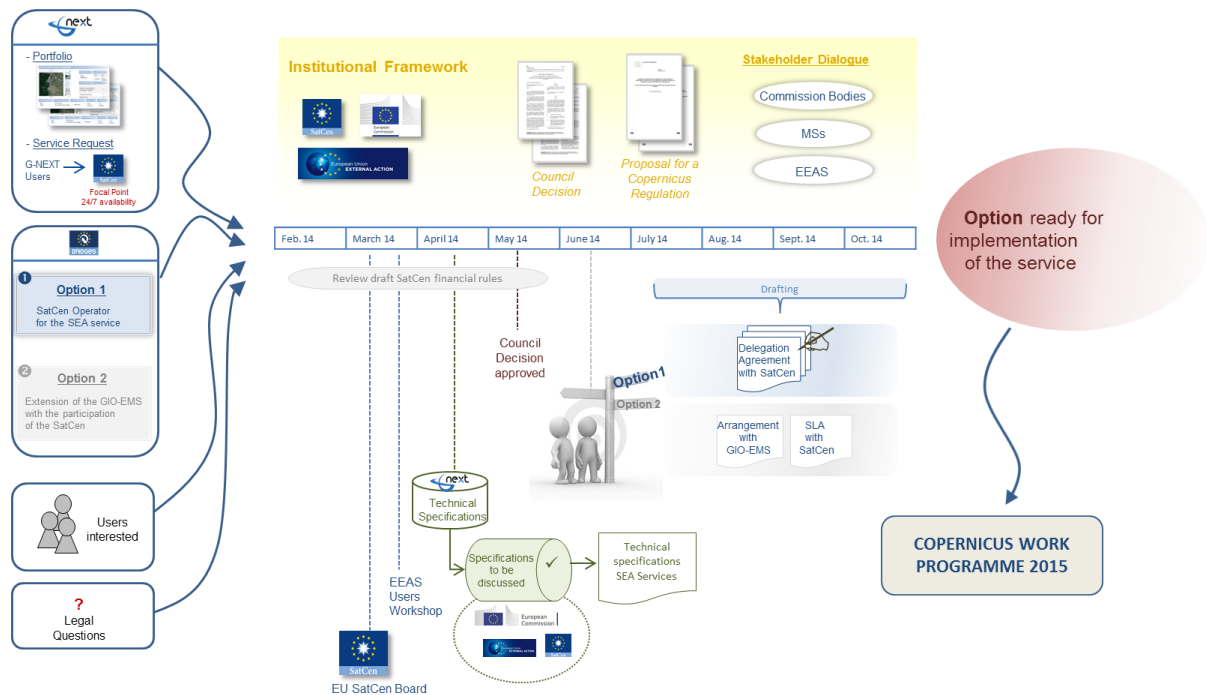


Figure 3 Copernicus Services in Support to EU External Action – Roadmap 2014

Roadmap: The roadmap in Figure 3 is proposed in order to progressively implement the Copernicus Services in support to EU External Action. This roadmap needs to fit into the more general deployment of the suite of Copernicus Security services (which also include Maritime Surveillance and Border Surveillance). The roadmap is designed to prepare for the launch of the services in Support to EU External Action in 2015. More precisely, the roadmap proposes key actions that will be undertaken in a phased process of implementation, from February to September 2014, to deliver the following results to the Commission at the end of 2014: • A clearly-defined governance model; • Detailed technical specifications for the service; • Draft legal documents for the implementation of the service (e.g. SLA, Delegation Agreement, etc.).

The governance model would be selected from the two options proposed after having clarified the legal framework and further discussed the BRIDGES project outputs within the SatCen Board, EEAS and the Commission. The timeframe is compatible with the ongoing legislative process including the adoption of the SatCen Council Decision and the Copernicus Regulation, and indicates that the governance option could be ready by June 2014. The detailed technical specifications for the service could be made available by G-NEXT in April / May 2014. These would then need to be discussed further with stakeholders and users including EEAS, SatCen and the Commission, in order to have a comprehensive document ready by June 2014. From June to September 2014, on the basis of the governance option and technical specifications chosen, legal documents such as administrative arrangements, service level agreements or delegation agreements could be prepared. A possible response from SatCen to a Call for Expressions of Interest in operating the service in Support to EU External Action may also have to be factored in, as well as the possible fine-tuning of SatCen's internal financial rules, if deemed necessary. During this process it will be crucial to intensify the dialogue in the spirit of transparency amongst all the main actors, particularly

between the EEAS, the Commission and SatCen, in order to reach sound decisions respecting both the interests of the stakeholders and the objectives of the programme. This dialogue is the most effective vehicle for the implementation of the user-driven approach while also safeguarding the integrity of the Security interests of Member States.

Expected final results and their potential impact and use (including the socio-economic impact and the wider societal implications of the project so far)

The FP7 Space Work Programme 2011 clearly defines guidelines for the expected impacts of the BRIDGES project:

- ☐ *Significantly contribute to the identification of options available for implementing a coordinated approach to Space data access in the security field*
- ☐ *Provide an overview of National and European stakeholder positions*
- ☐ *Deliver insights on how GMES as a civilian system under civilian control can contribute in an operational capacity in the CFSP/ESDP context*

The Work Programme also insists on the fact that the involvement of stakeholders is expected to contribute directly to the impact.

BRIDGES has achieved many of these expected impacts, in particular through stakeholder's engagement and consultation. Additionally it should be underlined that most of the final results can also be derived into concrete applications/procedures supporting the work of the GMES/Copernicus Unit at EC DG-ENTR and the setup of pre-operational services in Security. For example, the work on the governance model implied the identification and role of stakeholders within the activation mechanism of the G-NEXT project that is paving the way to GMES/Copernicus operational Services for Security.

The scenario(s) for the governance model identified by BRIDGES are directly applicable to the setup of the operational GMES/Copernicus Services for Security Applications, in particular for Support to EU External Actions.

BRIDGES provided useful inputs to the debate occurring in the GMES/Copernicus governance bodies (e.g. the User Forum and the GMES/Copernicus Committee) and should be an important source of information to be taken into account when implementing security domain related items of the regulation that will define the future operations of GMES/Copernicus in 2014 and beyond.

Being one of the objectives of BRIDGES to create awareness on the GMES/COPERNICUS Services for Security applications, it is worth to mention the effort put in dissemination activities, such as the organisation of two workshop, publications (e.g. article on the 1st User Committee Meeting held at the European Satellite Centre in Madrid on the June 14th, 2012 was prepared by the WP230 team and published on the GMES/Copernicus Observer Newsletter) and the development of the project website (<http://www.gmes-bridges.eu/>).

Furthermore, the main results of the project have been included in the issue of Windows on Copernicus published by BRIDGES: Discover the Security dimension of Copernicus – FOCUS ON WHAT COPERNICUS CAN DO FOR THE SECURITY OF THE EU AND ITS CITIZENS.

Address of the project public website

<http://www.gmes-bridges.eu/>

Project partners



Contact details

Denis Bruckert
GMES/Copernicus Coordinator
European Union Satellite centre
denis.bruckert@satcen.europa.eu