EUSEC
EU SECURITY CERTIFICATION

WHITEPAPER

The Multiparty Recognition Framework.

Table of Contents

What is Multiparty Recognition? **3**

State of the art in cloud service certification. *3*

EU-SEC's contribution. *0*

Use case stories: how multiparty recognition helps *1*

Benefits to Cloud Stakeholders. **2**

Cloud service providers and cloud users. *2*

Auditors *2*

Certification bodies/scheme owners. *3*

National and International Accreditation Bodies. *3*

Technical Details **4**

Reference architecture. *4*

Activities overview. *0*

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845

What is Multiparty Recognition?

State of the art in cloud service certification.

Cloud computing has emerged as the *de facto* standard when it comes to outsourcing IT infrastructure. Although it comes with many benefits like flexibility, cost-efficiency, and maintenance reduction, adopting cloud computing also means handing over control and governance of data to the Cloud Service Provider (CSP). That is a great concern for many customers. CSPs have addressed this issue to some extent by improving both their security and privacy posture and transparency, but there remains a need to establish a deeper level of trust between the CSP and the cloud customer.

Third-party audits and certifications can help to increase the level of trust around the effectiveness of a security and privacy programme. Independent standards such as ISO/IEC 27001 and ISE 3000 (SOC2) are internationally recognised. They are typically vendor-neutral, technology-agnostic, and they impose good cybersecurity practice. What's more, they require an independent third party to verify that the organisation operates its security controls the way it claims to do.

Unfortunately, however, security compliance based on third-party audit is becoming increasingly complex – especially as a result of the considerable number of national, international and industry specific standards and certification schemes present in the market.

Such a proliferation of schemes is generating 'compliance fatigue' in the industry, not to mention sometimes contradicting audit reports related to similar controls, especially for those companies operating on a global scale. That often translates into substantial costs for those service providers that can afford compliance to multiple standards, and potentially market entry barriers for smaller providers and confusion on the users/customer side, who are not necessarily experts on certification and standards, and who might have trouble in understanding which compliance seal to rely on.

At first sight, all these new certification schemes seem to be uniquely heterogeneous, since they target wider or specific application areas (e.g., national, sectorial, regulatory domains and requirements), but this might not be the case. In fact, cloud-based certification schemes are based on globally accepted and widely used standards (e.g., ISO 27000). Consequently, their very core security domains and requirements are largely homogeneous from the perspective of security requirements and objectives equivalency. As a result, many of the existing cloud security standards, especially national ones, include many overlapping requirements. To this end, it is valuable to identify those common denominators between these requirements and present them under a comprehensive framework

This work aims to show how mutual recognition between certification schemes can be achieved through their common security characteristics and showing that by terms of comparability and interoperability and under certain principles, criteria and requirements. In this context, one of the of the main objectives of the EU-SEC project is to develop such a framework for the multiparty recognition between existing cloud security certification schemes such as ISO27001, SOC2, CSA STAR Certification and Attestation, BSI C5, and other national schemes or requirements in the domain of cloud security.

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845

EU-SEC’s contribution.

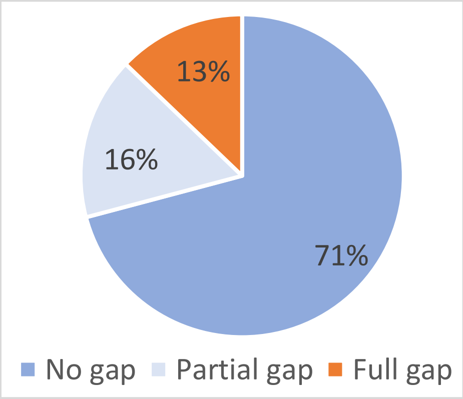
The EU-SEC project has developed a model architecture which aims to tackle the certification schemes’ proliferation side effects as a means to benefit all cloud-based stakeholders. The method we developed to achieve this goal is called multiparty recognition, and it is realised as a well-defined layered architecture called: **the multiparty recognition framework** (MPRF).

The idea behind the MPRF is not to create yet another cloud certification or auditing architecture. Instead, it aims to provide a unified method of systematic and consistent activities with the goal of minimising the burden of obtaining certification "Y" for a CSP, once it has already obtained certification "X". The MPRF’s purpose is therefore to us e and promote a comparison analysis between different security frameworks, standards, and best practices.

In EU-SEC’s study of different compliance schemes, we have observed that many of their individual security requirements and control objectives are, in fact, largely the same (see Figure 1). Consequently, when a CSP obtains a certification or attestation under two different schemes, a lot of work is duplicated, unduly increasing costs and complexity.

Therefore, it seems that in many cases, the work done under one compliance scheme should be re-usable under another. This would allow CSPs to focus instead on the differences in security requirements between multiple compliance schemes.

Figure 1: EU-SEC Security Requirements gap analysis results



The EU-SEC MPRF is intended to benefit all stakeholders in the cloud computing security and privacy compliance landscape. It should:

- guide **cloud stakeholders** in understanding the relationship between information security and privacy requirements contained in various compliance schemes such as BSI C5, CSA STAR, ISO or ISAE 3000
- support **CSPs** in selecting and adjusting their security and privacy objectives and controls in a way that several compliance schemes are applied at the same time
- offer **certification bodies** and **audit firms** the ability to present a more attractive compliance assessment portfolio through the multiparty recognition-based auditing services.

This project has received funding from the European Union’s HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845

Use case stories: how multiparty recognition helps

The MPRF is meant to streamline the cloud compliance process, bringing efficiency, increasing assurance and reducing reassessment costs.

For illustrative purposes, consider the following scenario in which a national organisation wants to conclude a contract with a foreign CSP:

1. The foreign CSP holds a CSA STAR certification
2. The national organisation wants to understand which of their national requirements are already covered by the CSA STAR certification
3. The CSP can focus on addressing the national organisation's controls that are not covered by CSA STAR.

Conversely, consider a CSP seeking to attract new customers by addressing specific regional or sectorial compliance requirements:

1. The CSP holds a SOC 2 attestation
2. The CSP wants to identify the gaps between the TSC requirements provided by the SOC 2 attestation and the regional or sectorial requirements of its new target customers
3. The CSP identifies the gaps and develops controls or adjusts processes addressing the identified gaps.

The scenarios above show the contributions, benefits and future perspectives this work aims to offer all parties involved in multiparty recognition between cloud-based security certification schemes

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845

Benefits to Cloud Stakeholders.

Cloud service providers and cloud users.

Cloud service providers are under considerable pressure to comply with several international, national, and sector specific standards and requirements. Such a proliferation of standards and requirements demands more resources be spent, increases compliance acquisition costs, and potentially also creates room for security vulnerabilities. The MPRF aims at tackling the former challenges by enabling its processes to compare two compliance schemes and output a minimum set of complementary security requirements. A CSP only needs to use this minimum set of requirements in addition to the existing certification during a third-party audit – not only reducing the overall auditing effort and costs but also the CSP's security surface exposure.

From the standpoint of **cloud users**, they need a better understanding of the extent to which a particular cloud service can be trusted and of how certifications and attestations are a good proxy of trust. In fact, due to the increasing number and diversity of certifications, cloud users often struggle to understand the level of assurance provided by each. As a result, instead of creating more trust, this overabundance of certification paradoxically leads to diminished trust due to confusion and lack of comparability. Cloud users need clear information about their CSPs' security and compliance postures so they can take informed decisions; numerous certifications and standards only seem to create more confusion rather than clarity. The MPRF is expected to add more transparency to the similarities and differences that exist between the security requirements of two certification schemes – raising awareness, improving understanding and increasing trust.

Auditors

Auditors have an active role within the context of multiparty recognition. They are considered as a qualified and trusted external party or organisation, and recognised as such by the EU-SEC governance body. They provide consultation about multiparty recognition activities performed over the compared security compliance schemes.

The MPRF gives auditors the opportunity to understand the relationship between information security and privacy requirements contained in various compliance schemes such as BSI C5, CSA STAR, ISO or ISAE 3000. This opportunity is offered by the provision of access to the EU-SEC repository, where the certification schemes' requirements comparison results and respective subsidiary guidelines are archived and made available. Throughout this collaboration, audit firms are able and expected to present and provide a more attractive compliance assessment portfolio to auditees (CSPs), in means of cost/time-effectiveness, efficiency, and as well as of increased transparency of the audit process.

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845

Certification bodies/scheme owners.

A certification body/scheme owner is a trusted party that is responsible for the correct organisation of a certification or compliance scheme, including accrediting auditors and keeping a registry of certified cloud services. Certification bodies/scheme owners, as with auditors, take over a significant consulting role within the various processes and respective activities of the framework. This will ensure that the framework will only comprise certification schemes with an equivalent level of quality and maturity and that it will keep up with changes and developments both of the schemes themselves and of the cloud ecosystem.

They need to ensure their certification schemes address the stakeholders' needs and are embedded into and connected with the legal as well as the regulatory landscape. The MPRF, through the various schemes' requirements comparison, enables certification bodies to keep track of multiple schemes' differences and their evolution, and provides the opportunity to review their own schemes on a regular basis and update them accordingly, if required.

Last but not least, the framework favours collaboration between certification bodies or compliance scheme owners. It encourages the establishment of mutual agreements between these parties, to recognise full or partial equivalences that are found between the certification and/or attestation they govern.

National and International Accreditation Bodies.

Accreditation Bodies are organizations that issue credentials or certify third parties (CBs) against official standards that are themselves formally accredited by accreditation bodies (such as UKAS or ANAB); hence they are sometimes known as "accredited certification bodies".

The accreditation process ensures that their certification practices are acceptable, typically meaning that they are competent to test and certify third parties, behave ethically and employ suitable quality assurance.

It encourages the establishment of mutual agreements between these parties and the certification bodies, to allow for recognition and acceptance of (full or partial equivalences) that are found between the certification and/or attestation they govern.

Technical Details

Reference architecture.

The framework's architecture is realised in accordance to a lifecycle process that has three main phases: "Evaluate", "Execute", "Govern", each corresponding to a set of components and underlying activities as shown in Figure 2 below.

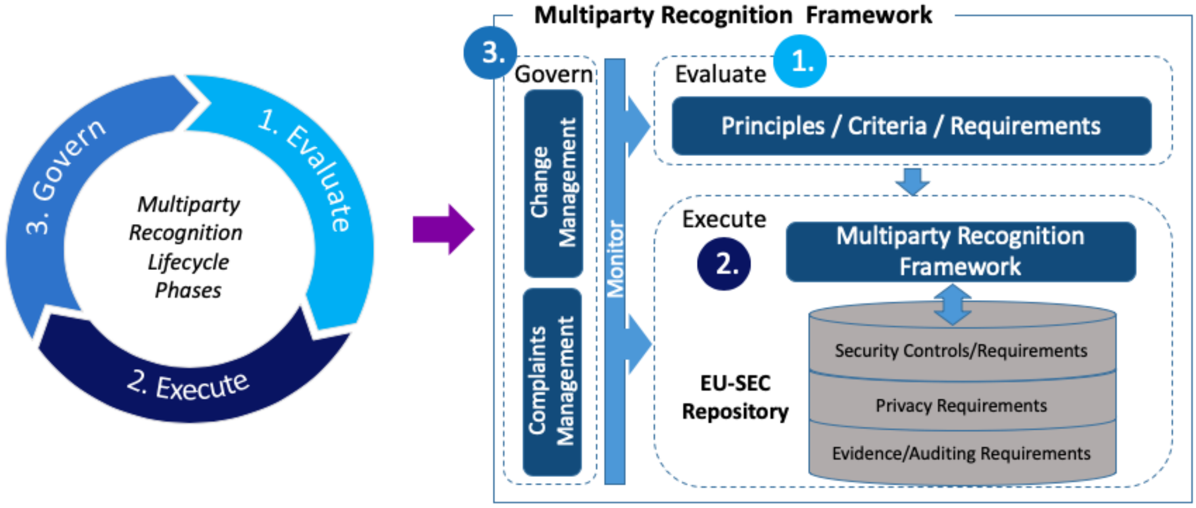

1. Evaluate
2. Execute
3. Govern
Multiparty Recognition Lifecycle Phases
Multiparty Recognition Framework
3.
Govern
Change Management
Complaints Management
Monitor
Evaluate
1.
Principles / Criteria / Requirements
Execute
2.
Multiparty Recognition Framework
EU-SEC Repository
Security Controls/Requirements
Privacy Requirements
Evidence/Auditing Requirements

Figure 2: Framework Lifecycle Phases and Components Correspondence

1. **Evaluate**: Within this phase, the EU-SEC governing body must evaluate the candidate scheme(s) for eligibility of use in the multiparty recognition process against certain principles, criteria, and requirements. The schemes' requirements comparison results are also validated for their soundness and consistency.
2. **Execute**: Within the execution step, the governance body and consulting entities (e.g., scheme owners, auditors) ensure the sound execution of the main multiparty recognition activities: requirements collection, comparison analysis, results output and dissemination.
3. **Govern**: To ensure that the MPRF reflects the current state of the art for cloud certifications and standards, a governance framework is implemented. Governance is applied throughout all framework activities in order to ensure its long-term management, maintenance and synchronisation to the evolving cloud certification landscape.

Five main activities lie at the core of the multiparty recognition framework, as illustrated in Figure 3 below.

Activities 1, 3 and 5 correspond to the “Execute” phase’s group of activities, while activities 2 and 4 corresponding to the “Evaluate” lifecycle group of activities. The “Govern” lifecycle group of activities interact with and run throughout the full multiparty recognition lifecycle phases. This group comprises two main processes: change management and complaint management (see Figure 2).

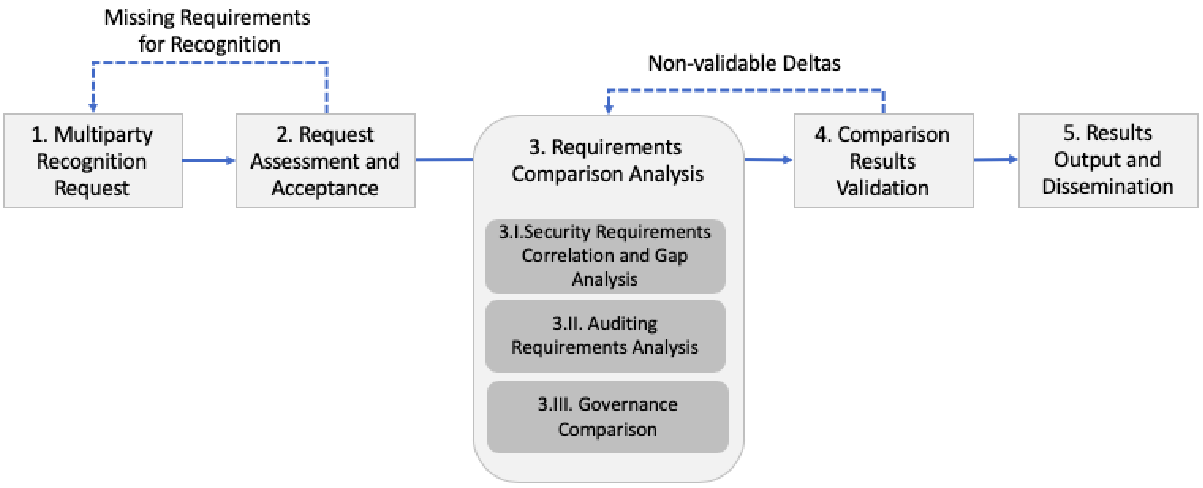

Missing Requirements for Recognition
Non-validable Deltas
1. Multiparty Recognition Request
2. Request Assessment and Acceptance
3. Requirements Comparison Analysis
3.I.Security Requirements Correlation and Gap Analysis
3.II. Auditing Requirements Analysis
3.III. Governance Comparison
4. Comparison Results Validation
5. Results Output and Dissemination

Figure 3: Multiparty Recognition Framework’s Core Processes Diagram

Activities overview.

1. ***Multiparty Recognition Request*** *is the provision and collection of inputs that will be fed to the framework, involving requests from the compliance schemes to initialise the MPRF process.*

2. ***Request Assessment and Acceptance*** *evaluates the request against the MPRF’s criteria such as comparability of the requirements and governance model, and principles such as relevancy and transparency. The request must be approved in order to initialise the correlation and gap analysis of the submitted compliance scheme.*

3. ***Requirements Comparison Analysis*** *is a critical activity that enables the multiparty recognition and involves analysing the submitted compliance scheme(s). The correlation and analysis are performed within three (3) main categories: security requirements, auditing requirements and governance requirements.*

4. ***Comparison Results Validation*** *receives input from the requirements correlation and gap analysis activity and validates the results. This is a feedback cycle that is continued until a satisfactory result is achieved.*

5. ***Results Output and Dissemination*** *releases the final results to the EU-SEC (security and auditing) requirements repository and shares them with the relevant stakeholders.*

This project has received funding from the European Union’s HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845

The developed architectural model aims at guaranteeing the manageability and scalability of the proposed framework architecture to rapidly adapt to the evolving cloud security certification landscape, the repeatability and consistency of expected multiparty recognition results, and finally the promotion of awareness and trust towards the multiparty recognition works among the participating cloud stakeholders.

This project has received funding from the European Union’s HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845

EUSEC
EU SECURITY CERTIFICATION

The European Security Certification Framework (EU-SEC)
mailto:contact@sec-cert.eu
https://www.sec-cert.eu/

Dr.-Ing. Jürgen Großmann
EU-SEC Project Manager
The Fraunhofer Institute for Open Communication Systems FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin
Phone +49 30 3463-7000
www.fraunhofer.de

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845