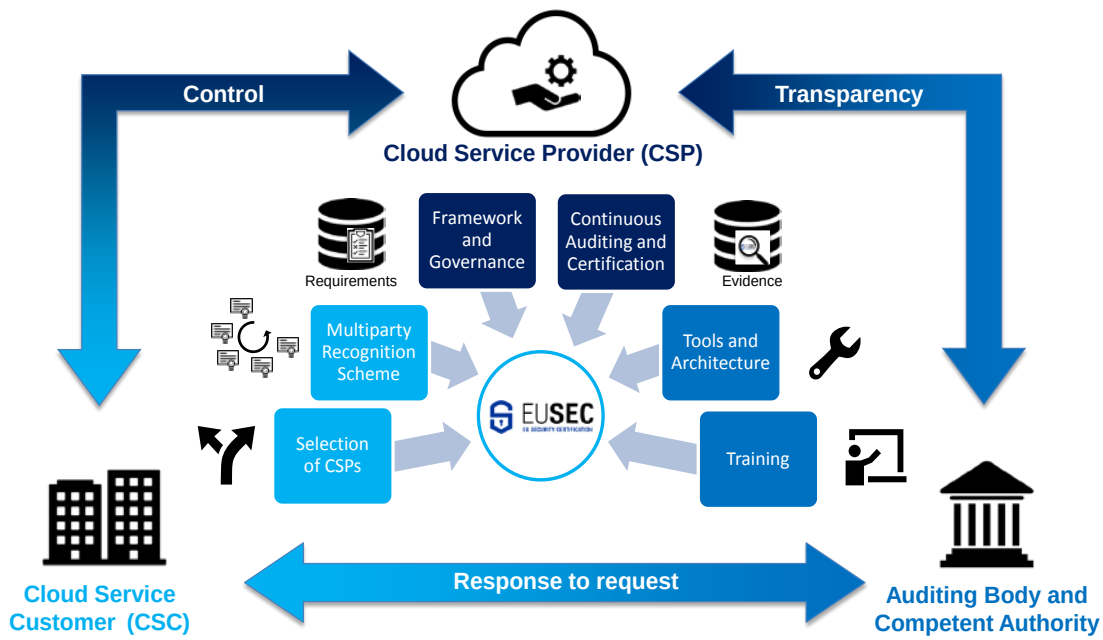
Dear Reader,

I am delighted to present you the first issue of our newsletter. Our goal is to keep you in touch with news and developments from the EU-SEC project that started its work in January 2017. The project provides an innovative approach to trust, assurance and compliance in the cloud market. Cloud customers, especially from the public and banking sectors, require a high level of trust in IT-security. But, despite of a high level of standardisation in cloud computing, customers in general are not aware of these safeguards. Different standards and certifications cause further confusion. This is where the EU-SEC comes into play. The project will improve the effectiveness and efficiency of existing certifications by creating a framework for Mutual recognition between different certification schemes. Requirements and controls from the public sector and the banking sector will be incorporated into the framework. After one year of collecting requirements from the respective sectors and hard work we are happy to present you the first project highlights.

I wish you an exciting read!

Linda Strick

EU-SEC Project Coordinator, Fraunhofer FOKUS



Implementation of EU Data Protection Regulation (GDPR) Makes a Mutually-recognisable, European Certification Framework More Important

On May 25 2018, the General Data Protection Regulation (GDPR) will come into force in Europe. The GDPR is designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organisations across the region approach data privacy. With the introduction of GDPR, Cloud Service Providers (CSPs) and cloud customers need guidance to comply with the new law in the cloud environment. CSPs will be responsible for self-determining the level of protection required for the personal data they process.

The Privacy Code of Conduct (CoC) aims at increasing the level of transparency and accountability from the privacy and security point of view. As such, it will play a fundamental role in the context of the EU-SEC framework, since it will be the tool that helps address one of the main limitations of existing certifications for cloud services, i.e., focusing almost exclusively on information security and not providing a means to show compliance with privacy requirements.

Moreover, it is meant to offer a free tool for those organisations seeking guidance when assessing their level of adherence to GDPR requirements as well as a mechanism of compliance. You can read more of this in D2.3 Privacy Code of Conduct (http://www.sec-cert.eu/downloads/).

The EU-SEC project focuses on addressing issues related to security and privacy governance, risk management and compliance in the cloud. Existing certifications for cloud services focus almost exclusively on information security and do not cover compliance with privacy requirements. EU-SEC will improve the effectiveness and efficiency of existing security certification processes by bridging the requirement gaps between them and minimising the lack of transparency toward cloud service customers. Furthermore, it aims at providing support to the European industry through the development and introduction of the multiparty recognition framework for cloud security certifications. The framework is based on mutual recognition criteria identified between widely known certification schemes. The technical requirements are collected in the form of EU-SEC controls/requirements repository and are described in detail within the documents D1.2 Security and Privacy Requirements and Controls and D1.3 Auditing and assessment requirements. Based on the standards and frameworks considered in D1.2 and D1.3 respectively, it was found that they are based on the auditing processes – either ISO27001 or ISAE 3000 frameworks. You can find all relevant documents in our website (http://www.sec-cert.eu/downloads/).

EU-SEC - Towards a Framework of Certification Schemes

Currently, national governments of the EU member countries develop and maintain their own standards, guidelines and define requirements, controls and conditions for obtaining a certificate or demonstrate compliance. This creates a high degree of confusion among cloud consumers and duplication of compliance efforts for CSPs. The EU-SEC project aims to resolve this by developing a framework that enables and ensures interoperability and compatibility between existing certification schemes and requirements.

EU-SEC Repository of Controls: Creating the Basis for an EU-wide Security Certification Framework

In the first phase in the design of a new security certification framework, EU-SEC has collected security and privacy requirements and controls, analysed and integrated them into a common repository of controls. The scope of input sources used for requirements collection was set to the international and national standards related to cloud computing legislation (related to public sector), technical specifications, and guidelines and documents important for the banking sector. The common repository used is the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM). The mapping led to three different levels – no, partial or full - gaps in the mapping to the CCM controls. Partial or full gaps served as a basis for updating the existing CCM controls or to define new controls. The experiences from this process also indicated the need to ensure that the new requirements could be continuously captured and covered by the up-to-date security and privacy controls in a transparent way. More information can be found in D1.2 Security and Privacy Requirements and Controls (http://www.sec-cert.eu/downloads/).

EU-SEC Auditing and Assessment Requirements: A European Harmonization of Certification Schemes

The EU-SEC project contributes to an enhanced mapping of laws, regulation and industry requirements to standard cloud controls. We have studied differences in professionally-conducted audit and assessment engagements, and applied audit criteria. In order to audit IT operations of a customer, a CSP may assign an independent audit and assessment firm to certify or attest on its information security management system (ISMS) and controls. Certification and attestation processes are governed with well-defined standards such as ISO/IEC 27000 and ISAE 3000. A CSP seeking for multiple accreditations may benefit from an EU-SEC designed multiparty audit and assessment engagement, to meet not one but several audit criteria with one engagement and possibly lowering the “unit” cost of compliance for the CSP. EU-SEC recommends building a control environment in compliance with CCMv3 and structured according to ISO/IEC 27001 topics, which would allow for ISO/IEC 27001 certification. This is in good alignment with most requirements, including ISAE 3000, and does not limit the cloud service provider from seeking an attestation on controls according to SOC 2, BSI C5 and/or SecNumCloud, which would require further efforts to comply. Read more in deliverable D1.3 auditing and assessment requirements (http://www.sec-cert.eu/downloads/).

Conference Attendance

Consortium partners have attended several conferences as part of our drive to spread the word about EU-SEC. The Slovenian Ministry of Public Administration presented the EU-SEC project at the yearly Informatics in Public Administration Conference: Administration 4.0 - Gaap, which was held at Congress Centre Brdo pri Kranju, on 4 and 5 December 2017. Partners of the consortium, CSA and Fraunhofer, attended the Digital Single Market cloud stakeholder meeting in Brussels on 12 December. There is interesting work going on within the European Commission to discuss about the European cloud certification scheme. The EU-SEC partners will stay in close contact with that initiative.

Publications

The Ministry of Public Administration of the Republic of Slovenia has published information about EU-SEC project development:

• on its web site in Slovenian and English version:

http://www.mju.gov.si/si/delovna_podrocja/informatika/mednarodni_projekti/eu_sec/ , and:

• in the conference proceedings of Informatics in Public Administration Conference 2017

Coming Up Next

In 2018, partners of the consortium will present the EU-SEC project at following events. Stop by and see us if you are participating too.

• RSA Conference in April 2018

• Days of Slovenian Informatics in April 2018

• CSA Japan Summit & Government Cybersecurity Forum in May 2018

• Infosecurity Europe in June 2018

• CSA Swiss Chapter Forum in September 2018

• CSA Netherlands Chapter and Nordic Chapter Forums in October 2018

• CSA Italy Chapter and Spain Chapter Forums in November 2018

• Informatics in Public Administration Conference in December 2018

Please feel free to subscribe to our newsletter by sending us an email at **contact@sec-cert.eu**

THE PROJECT

The European Security Certification Framework (EU-SEC) strives to address the security, privacy and transparency challenges associated with the greater externalisation of IT to Cloud services.

EU-SEC will create a certification framework under which existing certification and assurance schemes can co-exist. Furthermore, it will feature a tailored architecture and provide a set of tools to improve the efficiency and effectiveness of current assurance schemes targeting security, governance, risks management and compliance in the Cloud. It will be tested and validated in pilots involving industrial partners.

PARTNERS

Caixa Bank, Spain

CSA, UK

Fabasoft Cloud, Austria

Fraunhofer, Germany

Ministry of Finance, Slovakia

Ministry of Public Administration, Slovenia

NIXU, Finland

PwC, Germany

SIXSQ, Switzerland

CONTACT

Linda Strick (Fraunhofer FOKUS)
http://www.sec-cert.eu
contact@sec-cert.eu

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