ecsec and LuxTrust contribute new protocol for Qualified Electronic Signatures to OASIS

[Michelau, Germany / Capellen, Luxembourg, 16.02.2017] Leading experts from ecsec GmbH and LuxTrust S.A. joined forces to develop a novel "ChipGateway Protocol", which enables generation of qualified electronic signatures in cloud-based environments and contributed this to OASIS to foster the development of open standards for electronic signatures.

Browser-based generation of Qualified Electronic Signatures increasingly challenging

Browser vendors are progressively blocking plug-in interfaces, which particularly prevents using Java-applets, that are merely used for accessing smartcards in web applications. The proposed innovative "ChipGateway Protocol" provides a suitable solution to this problem, allowing to use smartcards and to sign electronically in any browser without using plug-ins, and particularly without using Java in the browser. Today, this protocol, which has jointly be developed by LuxTrust and ecsec, has been submitted to the non-profit consortium OASIS, which drives the development, convergence and adoption of open standards for the global information society and is committed to creating open standards for digital signature services.

eIDAS Regulation enables the ease of Qualified Electronic Signatures on the Cloud

The Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions (eIDAS) is fully applicable in all European Member States since July 2016. The eIDAS Regulation addresses, among other things, qualified electronic signatures, which shall replace their handwritten equivalents. While generation of qualified electronic signatures traditionally required using local smartcards, or similar cryptographic devices, the eIDAS Regulation introduced "remote electronic signatures", which enable generating qualified signatures within cloud applications. *"Unfortunately, until now there is no common and convenient approach on the market for accessing local signature creation devices from cloud-based applications,"* stated Stefan Hagen, Co-Chair of the OASIS Digital Signature Services eXtended (DSS-X) TC.

"ChipGateway Protocol" enables Cloud-based Applications to Sign Locally

The "ChipGateway Protocol" fills in the gap of the eIDAS standards for using local signature creation devices from cloud-based applications. Using the "ChipGateway Protocol", which

was inspired by the protocols used for the German eID card as specified in BSI TR-03124 and implemented in the certified Open eCard App, it is possible to generate qualified electronic signatures in browser-based web and cloud applications. *"The 'ChipGateway Protocol' makes it now possible for a remote signing server to access the locally connected signature creation devices using simple functions for listing available tokens as well as certificates and for requesting a signature in order to provide a seamless and user-friendly signing experience"*, explains Dr. Detlef Hühnlein, CEO of ecsec GmbH.

Contribution to OASIS is a starting point for Development of an Open eIDAS-Ecosystem

The innovative "ChipGateway Protocol" has today been contributed to the OASIS Digital Signature Services eXtended (DSS-X) Technical Committee (TC), which is committed to creating open standards for electronic signature services. *"It has been a pleasure to join forces with ecsec GmbH to develop the 'ChipGateway Protocol"*, explains Thomas Kopp, Chief Scientist at LuxTrust S.A.. *"As we are convinced that open standards are crucial for the prospering development of the eIDAS-Ecosystem, we are pleased to contribute the 'ChipGateway Specification' to OASIS in order to foster the development of an open ecosystem for trust services and electronic transaction services in Europe and beyond. This also demonstrates the innovative approach of LuxTrust as European Trust Services Provider of eIDAS Qualified Electronic Signatures."*

EU-funded FutureTrust project is proudly supporting eIDAS-related standardization

"We warmly welcome the contribution of the 'ChipGateway Protocol' as input for standardization and heartily invite all interested stakeholders to join us and contribute to the development of an open eIDAS-Ecosystem", added Stefan Hagen, Co-Chair of the OASIS Digital Signature Services eXtended (DSS-X) TC. As multiple DSS-X experts are also active within the EU-funded FutureTrust project, it is not surprising that this project is committed to supporting the forthcoming standardization efforts. *"We are proudly supporting the development of eIDAS-related standards and additionally aim at providing an Open Source reference implementation of the novel 'ChipGateway Protocol'"*, added Jon Shamah, FutureTrust Associate Partner Manager. *"FutureTrust invites all interested parties to benefit from these exciting developments and join the project as associated partner."*

About ecsec GmbH

ecsec is a specialized vendor of innovative solutions in the sector of security in the information and communication technology, security management, smart card technology, identity management, web security and electronic signature technology. Based on experiences from several consulting projects with international reach ecsec GmbH counts to the leading providers in this sector and supports well known customers within the

conception and implementation of tailor-made solutions. Due to the observance of current results of science and technology and current and future international standards, an excellent consulting quality and sustainable customer prosperity are guaranteed. ecsec for example developed the Open eCard App, which has been the first and only Open Source eID-Client, which has been certified by the German Federal Office for Information Security, and has received numerous international awards for its SkIDentity service, which offers "Mobile eID as a Service".

https://ecsec.de

About LuxTrust S.A.

Founded in 2005, LuxTrust is the Trust Services Provider operating from Luxembourg. It provides digital identity management, qualified electronic signature services and other trust services in line with eIDAS European regulations. LuxTrust manages digital identities, which are interoperable and multi-applicative, and today serves the entire population of Luxembourg. Trust Services are securely delivered through the cloud, based on user devices including hardware elements as well as mobile solutions to the highest certifications and standards. By virtue of its portfolio combining high-value trust services, a mobile user experience, and innovation, LuxTrust is expanding its international reach.

https://luxtrust.lu/

About OASIS

OASIS is a non-profit, international consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for security, privacy, cloud computing, IoT, SmartGrid, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology. OASIS members broadly represent the marketplace of public and private sector technology leaders, users, and influencers. The consortium has more than 5,000 participants representing over 600 organizations and individual members in 65+ countries.

https://www.oasis-open.org

About the FutureTrust project

Against the background of the regulation 2014/910/EU on electronic identification (eID) and trusted services for electronic transactions in the internal market (eIDAS), the FutureTrust project, which is funded within the EU Framework Programme for Research and Innovation (Horizon 2020) under Grant Agreement No. 700542, aims at supporting the practical implementation of the regulation in Europe and beyond. For this purpose the FutureTrust project will address the need for globally interoperable solutions through basic research with respect to the foundations of trust and trustworthiness, actively support the standardization process in relevant areas, and provide Open Source software components and trustworthy services which will ease the use of eID and electronic signature technology in real world applications.

https://futuretrust.eu

Number of Words: 1200

Contact

Dr. Detlef Hühnlein
ecsec GmbH
Sudetenstraße 16
96247 Michelau
Germany
Phone: +49 9571-6048014
E-Mail: info@ecsec.de
Web: https://ecsec.de

Stéphanie Dermience
LuxTrust S.A.
IVY Building, 13-15 Parc d'Activités
L-8308 Capellen
Luxembourg
Phone: +352 26 68 15-892
E-Mail: stephanie.dermience@luxtrust.lu
Web: https://luxtrust.lu

Carol Geyer
OASIS

Phone: +1.941.284.0403
E-Mail: carol.geyer@oasis-open.org

Jon Shamah
FutureTrust Partner Manager

Phone: +44 78 13 111 290
E-Mail: jon.shamah@eema.org

Press Release