Information Security

V1.0

Table of contents:

Data protection and security issues

This report is part of the EWP WP3 deliverables, and is a recommendation on methods to secure data transfer and outputs in the EWP network. The following security issues are discussed:

- Protection of the contidentiality, authenticity and integrity of the data being exchanged
- Methods agnostic to the data format
- Independence to the underlying messaging and transport system
- Compliance to relevant EU legislations
- Security recommendations for developers

Confidentiality

Certain data must be kept confidential, i.e., inaccessible to unauthorized recipients.

Authenticity

Mechanisms need to be present to ensure the truthfullness of the data source.

Integrity

It must be ensured that no one can manipulate the data by, e.g., changing its contents before retransmitting it.

Non-repudiation

The solution should have the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Addressing the security issues in EWP

There are mechanisms to address the abovementioned security concerns in a data agnostic way (gpg is one example taking care of all these concerns). These mechanisms, however, might be highly impractical or even unfeasible in the EWP scenario where a lot of data exchange is done automatically.

There exist well described and standardized mechanisms to address these concerns for the types of data we handle:

- Transport layer: TLS (takes care of all the concerns)
- Data: XMLDsig (xml), PDF signatures (pdf) – this makes it possible to save data locally and verify authenticity, integrity and non-repudiation at a later point in time

We also see that the legal framework eIDAS might contain what EWP needs, or at least in part, and it seems that eIDAS will be enforced in Europe by 2018. eIDAS is a vast area and it has to be studied in more detail with regards to both the legal issues and the technical issues.

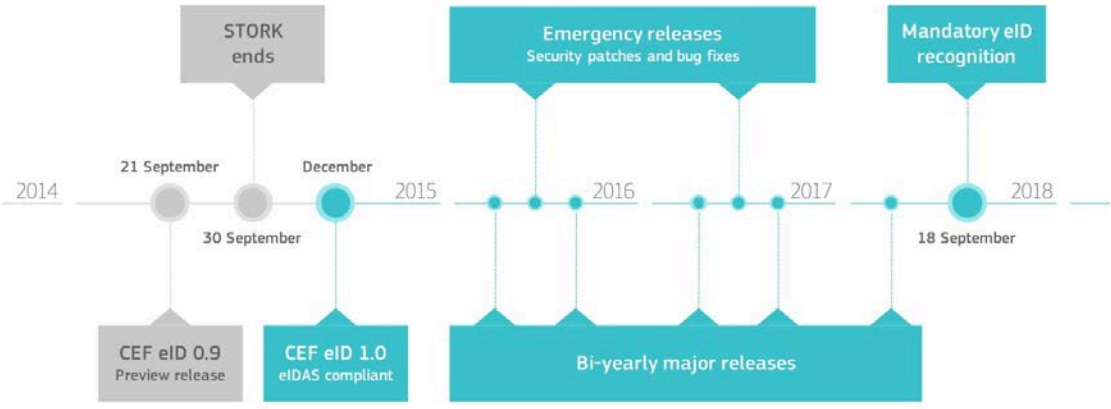
eIDAS

eIDAS (a new regulation for electronic identification and trust services for electronic transactions in the internal market), also known as the Regulation (EU) N°910/2014, is designed to replace the EU 1999/93 Directive, and update the legislative structure that governs electronic identification, documentation, and signatures across all members of the European Union.

The regulation addresses two main areas: *electronic identification systems* and *electronic signatures*.

The regulation defines a range of trust services (eSignatures, eDelivery-services, web site authentication and more), and these are required to be legally recognized across borders.

eIDAS aims to solve a range of electronic identity related issues and facilitate cross-border access to public services. eIDAS has been enforced as of July 1st 2016. The deadline for implementation is September 2018.



Source: https://joinup.ec.europa.eu/software/cefeid/news/eidas-sample-implementation-v10

eIDAS and eID

Electronic identification (eID[1]) and electronic Trust Services (eTS) are key enablers for secure cross-border electronic transactions and central building blocks[2] of the Digital Single Market. eID is based on Stork/Stork2.0 projects[3].

The aim of the STORK project was to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. Both Stork 1.0 and 2.0 are finished projects and the results are absorbed into eIDAS.

The eIDAS regulation adopted by the co-legislators on July 23rd 2014 is a milestone to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public

authorities. From July 1st 2016, people, businesses and public administrations are able to carry out convenient, secure and legally valid electronic transactions across borders. In this regard, the eIDAS regulation

- ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available.
- creates an European internal market for eTS - namely electronic signatures, electronic seals, time stamps, electronic delivery services and web site authentication - by ensuring that they will work across borders and have the same legal status as traditional paper based processes. Only by providing certainty on the legal validity of all these services, businesses and citizens will use the digital interactions as their natural way of interaction.

eIDAS and eSignature

Considerable confusion stems from the fact that "signature" is both a legal and a technical term[5]:

- An "electronic signature" is the legal term for the act of signing, i.e. giving consent to, something. An electronic signature is a replacement for a handwritten signature.
- A "digital signature" is a technical term for a signature created by public key cryptography, supported by PKI certificates issued by a recognised certification authority. This technology is currently needed to support "advanced" and "qualified" signatures.

eIDAS regulation defines several types of signatures, all of them legal terms:

- An "electronic signature" can be created by any technical mechanism that creates a link between the data/information/document that is signed, and the act of the user. Notably, a "click to consent" user interface where an authenticated user explicitly confirms their intention by clicking a button on a web page can be used, preferably in combination with a sufficiently strong audit log record of the event. Even a plaintext "signature" at the bottom of an email may constitute an electronic signature.
- An "advanced electronic signature" (**AdES**) is in reality not a technology neutral term but requires a "digital signature" and use of PKI technology. A "basic" AdES has no quality requirements, e.g. no requirement on the quality of the PKI certificate used.
- An "advanced electronic signature with qualified certificate" (**AdESQC**) adds the requirement for use of a qualified certificate, i.e. a certificate issued by a certification authority that is nationally supervised and present in the Trusted List system of the EU.
- A "qualified electronic signature" (**QES**) additionally requires use of a "qualified signature creation device" (**QSCD**) holding the signer's private signing key. A QSCD can be based on various technologies; although a smart card was initially foreseen, server-based solutions are increasingly being used

eIDAS across borders

E-signature is an area that has been defined by cryptologists and technicians. The eIDAS legal framework describes very carefully the demands you have to follow when you are going to accept and verify electronic signatures, but says nothing about what an e-signature should look like. For instance, in Norway there is no requirement for a qualified signature.

In 1999 the EU commission said that if an electronic document were to be signed and have the same legal binding as a handwritten signature, it would have to be signed with the electronic qualified signature (QES). This decision might have been the reason why e-signatures did not get as widespread that one might have wished in 1999 due to the arguing on how this signature should look like.

If someone sends you a signed document, and the signing is trusted according to trusted lists and standards and rules that are in use, you cannot reject it. In the future, there will be a country specific service to verify a e-signature. Every country has different ways of e-signing. Almost none of the Nordic countries uses QES because it is not in their legislation.

General security recommendations for implementers

The Open Web Application Security Project (OWASP) is an online community which creates freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security. They offer open source tools such as a security scanner, Code Review Guide, Application Security Verification Standard, testing guide and much more. The OWASP Top Ten is a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Recommendation for EWP

The project has different security requirements depending on what data are secured at what point in time during the student's mobility. To ensure confidentiality of data travelling through the network, we recommend encryption of all traffic by means of TLS (that is, enforcing https when calling web services). To ensure that only authorized hosts have access to the network, and to verify a request's origin, certificates should be stored centrally and delivered by each party in a secure way.

Regarding electronic signatures, to ensure that as many as possible will want to use EWP, we would recommend to use the lowest level of electronic signature (that is, "click to consent") wherever this is feasible and good enough for all the parts involved. Examples for this might be inter-institutional agreements or learning agreements. XML and PDF documents can be signed on a higher level, either using AdES, which can be done automatically by a machine, or AdESQC where a personal signature is required. The chosen level of security should be based on a legal justification, including a risk analysis.

Regarding Erasmus one should ask the following question: How would the Erasmus community like to sign data? If this decision is on a country level, you will get 30 different signature solutions. We should consider having a signing and validating service on an Erasmus level, solved in a way that works well for all the involved countries.

eIDAS wants to free themselves from the equipment users would need to have (such as card readers and smart cards) in order to make good enough signatures. So the definition: "The signature must be fully under user's control" is now reformulated to "The signature must be as fully under user's control as possible". This means that one can get centralized services, and Erasmus might decide to provide such a service. In that case, all the countries could use their national eIDs to access the service, and data would be signed in a way all the Erasmus countries agree on as sufficient/secure enough to be accepted. There are usually only a few cases where you really need heavy crypto security.

In the future there will possibly be several operators wishing to offer signature verification solutions. This needs not be a national service and there are open source solutions out there already that you can take advantage of and build your own service. An example of such a solution is DSS[4]. It is possible for Erasmus to implement DSS and it would also be possible to look up in a trusted list to see whether a document comes from somebody we trust. This could be done within the universities and/or schools and provide it as a service.

Regardless of the solutions chosen for EWP, we recommend to follow the guidelines and recommendations provided by OWASP closely and actively.

Glossary

AdES	Advanced Electronic Signature, an electronic signature that has met the requirements set forth under EU Regulation No 910/2014 (eIDAS-regulation) on electronic identification and trust services for electronic transactions in the internal market.
AdESQC	Advanced Electronic Signature with Qualified Certificate, adds the requirement for use of a qualified certificate.
Digital certificate	An electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.
Digital signature	The technical term for a signature created by public key cryptography.
eID	An electronic identification solution of citizens or organizations, for example in view to access benefits or services provided by government authorities, banks or other companies.
eIDAS	Regulation (EU) N°910/2014 on electronic identification and trust

	services for electronic transactions in the European internal market.
Electronic signature	The legal term for the act of signing, i.e. giving consent to, something. An electronic signature is a replacement for a handwritten signature.
Hash	The result of a one-way cryptographic function, often used to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption.
OWASP	Open Web Application Security Project, an online community which creates freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.
PDF	Portable Document Format, a file format used to present documents in a manner independent of application software, hardware, and operating systems. Each PDF file encapsulates a complete description of a fixed-layout flat document, including the text, fonts, graphics, and other information needed to display it.
PKI	A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
Qualified certificate	A public key certificate issued by a qualified trust service provider that ensures the authenticity and data integrity of an electronic signature and its accompanying message and/or attached data.
QES	Qualified Electronic Signature, requires use of a qualified signature creation device holding the signer's private signing key (smart card or a dedicated server-based solution)
STORK	A project whose aim was to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID.
TLS	Transport Layer Security, a cryptographic protocol that provides communications security over a computer network, a successor of Secure Sockets Layer (SSL).
XMLDsig	XML Signature (also called XML-DSig, XML-Sig) defines an XML syntax for digital signatures and is defined in the W3C recommendation XML Signature Syntax and Processing.

References

[1] https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

[2] https://joinup.ec.europa.eu/community/cef/og_page/catalogue-building-blocks#eSignature

[3] https://www.eid-stork2.eu/

[4] https://joinup.ec.europa.eu/asset/sd-dss/description

[5] Hansteen, K., Ølnes, J., Alvik, T., "Nordic digital identification (eID): Survey and recommendations for cross border cooperation", Nordic Council of Ministers, Feb 10 2016, TemaNord 2016:508, http://dx.doi.org/10.6027/TN2016-508