Electronic Signatures Standards

Workshop #1 - Standardization

1. Introduction

1.1 What is a digital signature?

A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital document or message. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent. In many countries, including the U.S., digital signatures are considered legally binding in the same way as traditional handwritten document signatures.

1.2 Pros & Cons

1.2.1 Pros

1. **Security:** Digital signatures provide a high level of security and authentication. They use encryption and cryptographic techniques to verify the identity of the signer and ensure the integrity of the signed document.
2. **Legally Binding:** In many jurisdictions, digital signatures are legally binding and hold the same legal weight as traditional handwritten signatures when used correctly. They can be used for contracts, agreements, and other legal documents.
3. **Tamper Detection:** Digital signatures include mechanisms to detect any unauthorized changes to the signed document after it has been signed. This ensures the document's integrity.

1.2.2 Cons

1. **Initial Setup:** Implementing a digital signature solution can require an initial investment in terms of technology and training. Small businesses or individuals may find this setup cost prohibitive.
2. **Legal Variability:** While digital signatures are generally legally binding in many countries, the specific legal framework and requirements may vary. Users should ensure they comply with local laws and regulations.
3. **Authentication:** The security of digital signatures depends on the protection of private keys. If a private key is compromised, it could lead to fraudulent signatures. Users must take measures to safeguard their private keys.

1.3 How is it working ?

Digital signatures are based on asymmetric cryptography: using a public key algorithm two keys are generated, creating a mathematically linked pair of keys, one private and one public.

For encryption and decryption, the person who creates the digital signature uses a private key to encrypt signature-related data. The only way to decrypt that data is with the signer's public key.

If the recipient can't open the document with the signer's public key, that indicates there's a problem with the document or the signature. This is how digital signatures are authenticated.

Now that the main concepts are said, let’s talk about the different standards behind digital signatures.

2. What are the standards ?

2.1 Electronic IDentification Authentication and trust Services

Electronic IDentification Authentication and trust Services (eIDAS) is a EU regulation on electronic identification and trust services (legal entity providing and preserving digital certificates to create and validate electronic signatures) in the European common market.

It was established in July 2014, entered into force in September 2014 and applied in July 2016.

It provides a regulatory environment for electronic signatures and it classifies it as qualified and advanced, and what characteristics they have to fulfill be on either of these groups, digital certificates and trust services, which are companies or organizations that provide these services, and creates, validates, and verifies electronic signatures, time stamps, seals, and certificates. There is a list called the European Union Trusted List with over 200 providers accredited to deliver compliance to this regulation.

2.2 XML Digital Signature

XML Digital Signature (XMLDSIG) is a specification and standard developed by the World Wide Web Consortium (W3C) that defines a format for digitally signing XML documents. XMLDSIG provides a way to ensure the integrity and authenticity of XML data by applying digital signatures to XML content. This technology is widely used in various applications, including web services, electronic commerce, and secure data exchange.

XMLDSIG plays a critical role in ensuring the authenticity and integrity of XML data in a wide range of domains. It allows organizations and systems to verify the source and integrity of

XML documents, which is essential for secure and trusted data exchange in electronic transactions and communications.

2.2.1 Key aspects

1. **XML-Based:** XMLDSIG is based on XML syntax, making it a natural fit for XML documents. It defines XML elements and attributes that represent digital signatures and signature-related information within an XML document.
2. **Multiple Signatures:** XMLDSIG supports the signing of an entire XML document or specific portions of it. This allows multiple parties to sign different parts of the same document.
3. **Applications:** XMLDSIG is used in various applications, including web services security (WS-Security), electronic document signing, secure data exchange in healthcare (HL7), and XML-based communication in government and financial sectors.

2.3 PDF Advanced Electronic Signatures

PDF Advanced Electronic Signatures (PAdES) is a set of standards and specifications that define how electronic signatures and related trust services should be applied to PDF (Portable Document Format) documents. PAdES is designed to ensure the legality, security, and interoperability of electronic signatures within PDF files. It was developed to meet the specific needs of the European Union (EU) and is often referenced in the context of eIDAS regulation.

PAdES is an important standard for organizations and individuals who use PDF documents for electronic signatures, particularly in the context of legal, financial, or government transactions within the European Union. Compliance with PAdES standards ensures that electronic signatures within PDF files meet the necessary legal and security requirements.

2.3.1 Key aspects

1. **Legally Binding Signatures:** PAdES specifies the requirements for creating legally binding electronic signatures within PDF documents, ensuring that they are equivalent to traditional handwritten signatures in a legal context.
2. **Timestamps:** PAdES allows for the inclusion of trusted timestamps in PDF documents. Timestamps provide evidence of the exact time a document was signed, helping to prevent disputes related to document modification after signing.
3. **European Union Focus:** While PAdES has broader applicability, it was initially developed with a focus on aligning with the requirements of the EU's eIDAS regulation, which governs electronic identification and trust services within the EU.

We will prioritize the eIDAS standard as it establishes uniform regulations for digital signatures across European nations, ensuring that any signature generated within Europe holds validity and recognition throughout all member countries.

3. eiDAS in details

3.1 Context

On July 23, 2014, the European Parliament and the Council of the European Union adopted Regulation No. 910/2014/EU on electronic identification and trust services for electronic transactions in the internal market, known as the "eIDAS" Regulation.

The adoption of this regulation follows the relative failure of Directive 1999/93/EC on electronic signatures. Differences in the transposition of this directive, as well as in the technical choices made by Member States, prevented the emergence of a common foundation of interoperability necessary for the development of cross-border exchanges. This state of affairs had been pointed out by the Commission on two occasions in 2010, leading the European Council in 2011 to call for the creation of a digital single market by 2015.

In June 2012, the Commission initiated work to promote e-commerce within the Union, with the aim of adopting a regulation that would apply directly to member states, without transposition into national law. It took more than two years of discussions to arrive at the final text of the eIDAS regulation.

The eIDAS regulation was published in the Official Journal of the European Union (OJEU) on August 28, 2014 and came into force on September 17, 2014.

The eIDAS regulation has been applicable since July 1, 2016 for most of its provisions. Mutual recognition of electronic means of identification has been mandatory since September 29, 2018.

3.2 Scope and Recipients

The eIDAS regulation applies to electronic identification, trust services and electronic documents. It aims to establish an interoperability framework for the various systems set up in the Member States, in order to promote the development of a digital trust market.

The regulation sets out requirements for the mutual recognition of electronic means of identification and electronic signatures, for exchanges between public sector bodies and users. It excludes internal administrative exchanges with no direct impact on third parties, as well as privately signed documents.

3.3 Main measures

The eIDAS regulation focuses primarily on electronic identification and trust services. To a lesser extent, it also deals with electronic documents, giving them legal effect.

3.3.1 Electronic identification

The eIDAS regulation aims to establish a mechanism for the mutual recognition of Member States' means of electronic identification on all online services in other Member States.

In order to benefit from this mutual recognition, an electronic means of identification must :

1. Have been issued in accordance with an electronic identification scheme notified by the Member State concerned and included on the list published by the Commission.
2. Avoir un niveau de garantie égal ou supérieur à celui requis par l'organisme du secteur public concerné pour accéder à ce service en ligne, à condition que ce niveau soit substantiel ou élevé.

3.3.2 Trusted services

The eIDAS regulation also aims to establish a legal framework for the use of trust services. It lays down requirements for trust services relating to electronic signatures, electronic stamps, electronic time stamps, electronic registered mail and website authentication.

The regulation distinguishes between qualified and non-qualified trust services. Qualified trust services meet specific requirements and may benefit from specific legal effects. Qualified trust services are provided by qualified trust service providers.