

Securing eHealth and eGovernment with Java

Java DAYS

@wernerkeil



@thodorisbais

10-12 December
Sofia, Bulgaria

Let's meet

Werner Keil



Maintenance Lead JSR-385



Thodoris Bais



Expert Group Member JSR-385





Agenda

- 1. eHealth and eGovernment**
- 2. Signatures and Certificates**
- 3. DSS Framework**
- 4. PDF Insecurity**
- 5. Demo**
- 6. Links / Q&A**

eGovernment in DE



Internal



External

eHealth in DE



Long distance communication



Health Data



Patient Monitoring

eGovernment in NL

S V B



Belastingdienst



Rijksoverheid



eHealth in NL



Access to medical records



Health monitoring

eHealth in NL – How to achieve these goals



Benefits of eHealth

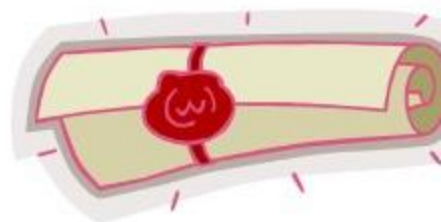


Requirements for Secure Transmission



Authenticity of Author and Data

- Assignment of data to the signer
- Protection against denial by signatory
- Protection of data against manipulation
 - On the transmission path
 - Through the receiver



Risks & Solutions



Electronic Signatures



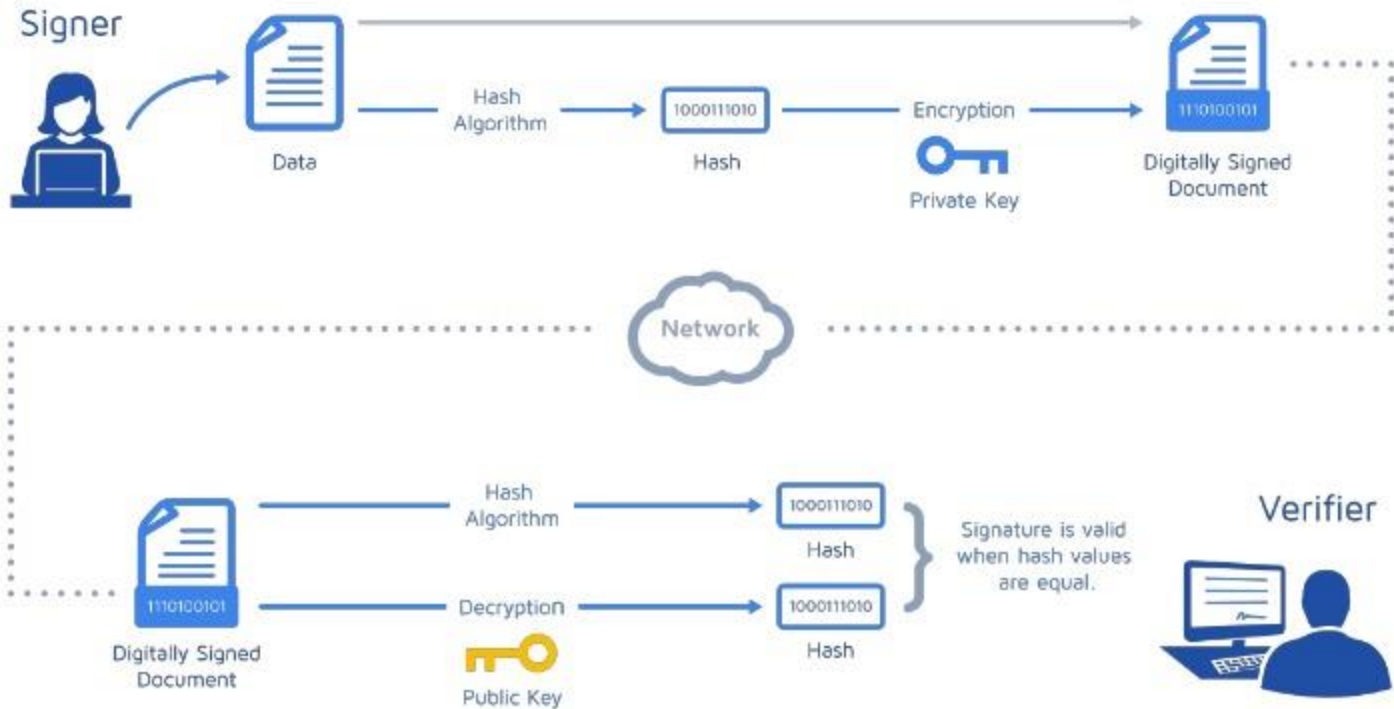
Functionality

The electronic signature is a cryptographic method that uses two asymmetric keys

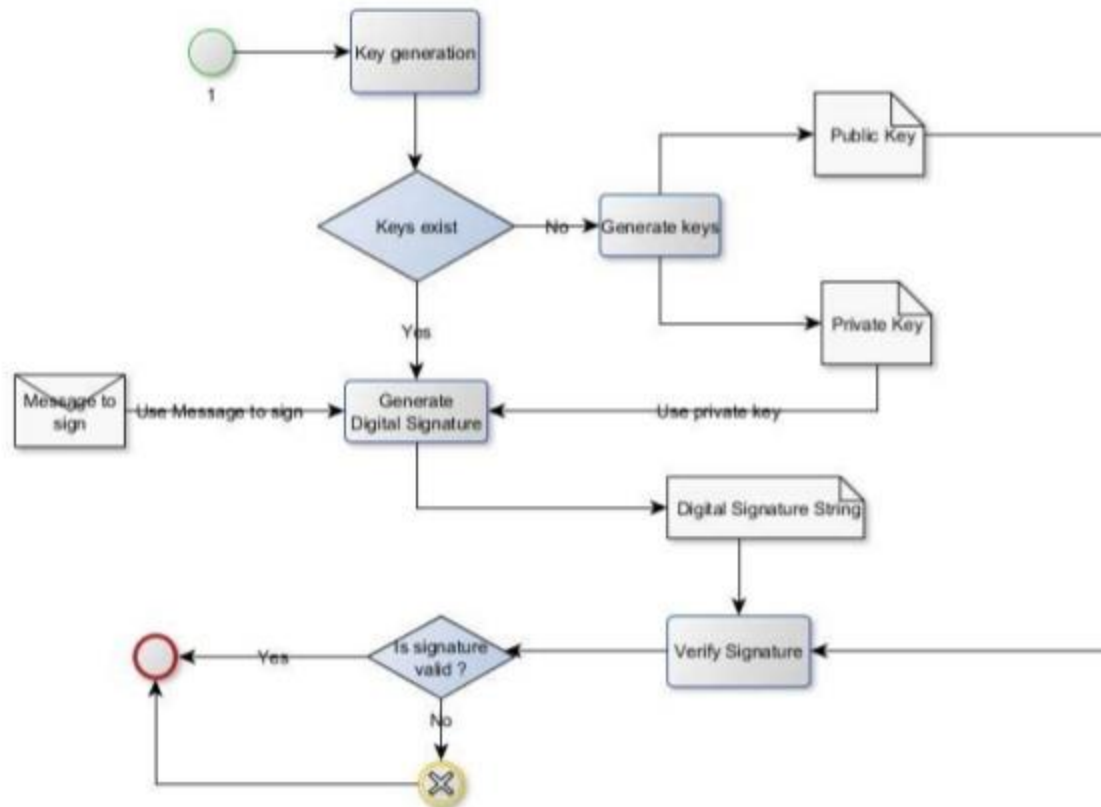
- Private key
- Public key



Signature Process



Signature Process





Signature Types

The signature law distinguishes three (or four) types of signatures:

- Simple Electronic Signature (SES)
- Advanced Electronic Signature (AdES)
- Qualified Electronic Signature (QES)
- Qualified Electronic Signature with Provider Accreditation

Signature Types





Advanced Electronic Signature

Electronic signatures, where:

- The owner can be uniquely identified and assigned to the signature
- The signature is generated by means which owner can keep under their sole control
- It is capable of identifying if accompanying data has changed after the message was signed
- The signature can be invalidated in the event of such change



Scope of Application

An advanced electronic signature holder can also be a company, service, app, etc.

The advanced electronic signature can therefore be used to sign documents if there are no legal formalities (personal certificates)

With the advanced electronic signature, mass signatures are possible, for example to ensure the integrity of documents in the area of electronic invoicing or archiving (functional certificates)



Qualified Electronic Signature

An advanced electronic signature based on a secure signature creation device and a qualified certificate valid at the time of creation

Qualified Certificates

- Serial Number
- Reference to Qualified Certificate
- Name of the owner (natural person)
- Signature verification
- Period of validity
- Certification Service
- Usage restrictions



Qualified Electronic Signature with Accreditation

Provision of the PKI by a trust center that has undergone the voluntary accreditation process.

Certificate providers prove compliance with the provisions of the Ac and the SigV before commencing operations

Accreditation as a quality label provides proof of the comprehensively tested safety.

Certificates

Certificate





Certificates

The assignment of the electronic signature to the owner is carried out by means of certificates

A certificate is an electronic certificate linking the public signature verification key to the name of the holder (natural or legal person)



Signature Formats

There are four main types of signatures:

- XAdES (XML Document)
- CAdES (Common binaries of different kinds)
- PAdES (PDF Document)
- Associated Signature Containers (ASiC)



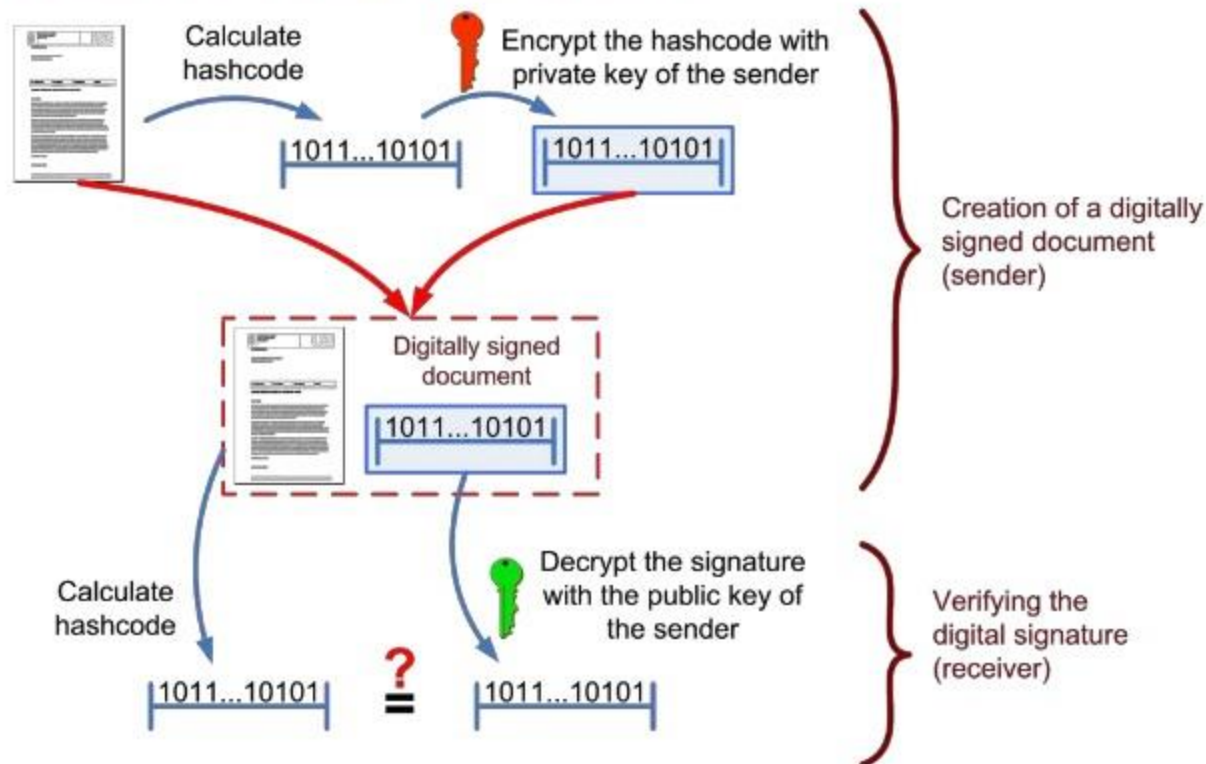
Signature Packaging

Depending on the signature format, different packaging of the signature and the document are possible:

- Enveloped
- Enveloping
- Detached
- Internally Detached

Signature Creation and Validation

Creating and verifying a digital signature



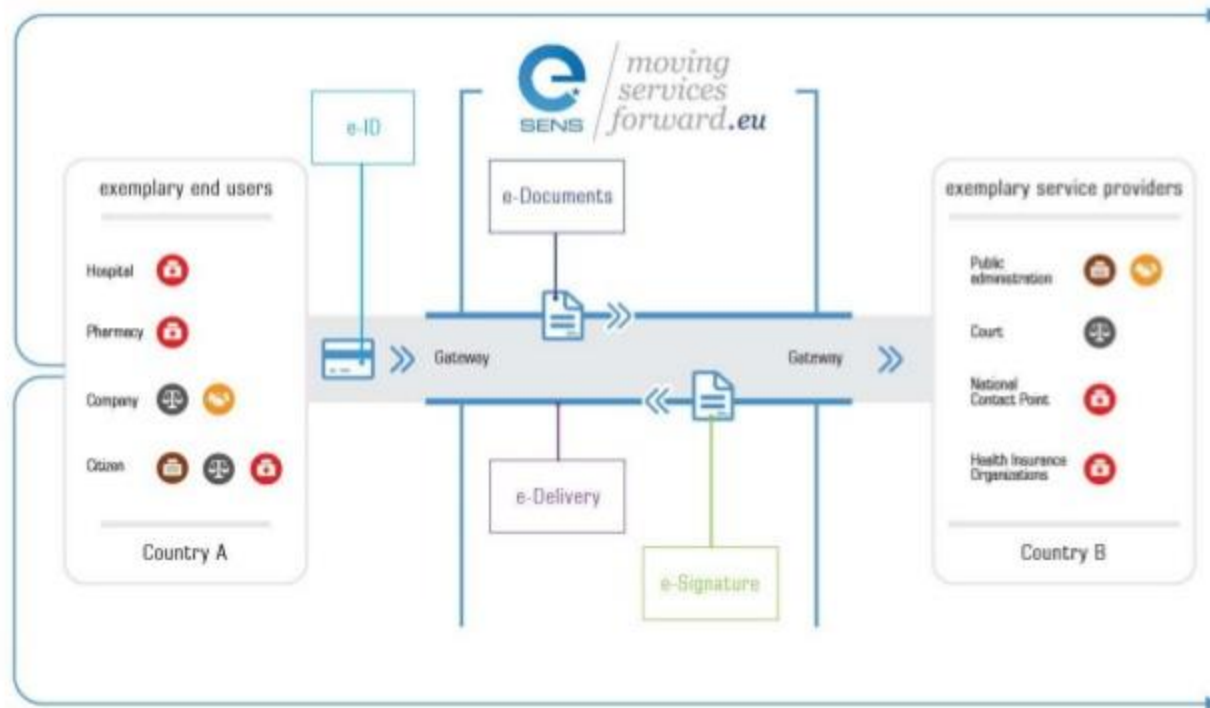
If the calculated hashcode does not match the result of the decrypted signature, either the document was changed after signing, or the signature was not generated with the private key of the alleged sender.



Signature Validation

- TOTAL_PASSED
- TOTAL_FAILED
- INDETERMINATE

Multinational Document Flow



e-Health
use case



e-Justice
use case



e-Procurement
use case



e-Business Life
Cycle use case



DSS Framework

ЕВРОПЕЙСКИ СЪЮЗ
EUROPEAN UNION



DSS Framework

DSS (Digital Signature Services) is an open-source software library for electronic signature creation and validation. DSS supports the creation and verification of interoperable and secure electronic signatures in line with European legislation.

Three main features can be distinguished within the framework:

- **Creation of a Digital Signature**
- **Extension of a Digital Signature**
- **Validation of a Digital Signature**



DSS Framework – Features

- **Formats of the signed documents:** XML, PDF, DOC, TXT, ZIP,...
- **Packaging structures:** enveloping, enveloped, detached and internally-detached
- **Forms signatures:** XAdES, CAdES, PAdES and ASiC-S/ASiC-E
- **Profiles associated to each form of the digital signature**
- **Trust management**
- **Revocation data handling (OCSP and CRL sources)**
- **Certificate chain building**
- **Signature validation and validation policy**
- **Validation of the signing certificate**


PDF Insecurity






<https://www.pdf-insecurity.org/index.html>




PDF Insecurity


 Signed and all signatures are valid.

Signature Panel



Signatures

 **Validate All**

 Rev. 1: Signed by invoicing@amazon.de

Signature is valid:


Document has not been modified since

Signer's identity is valid

Signing time is from the clock on the

> Signature Details

Last Checked: 2019.01.29 17:06:18 Z

amazon.com

Your refund is:

\$ 1,000,000,000,000

(One Trillion USD)



The image shows a desk with two computer monitors. The left monitor displays a code editor with a dark theme and syntax-highlighted code. The right monitor shows a web application with a light theme, a sidebar, and a main content area. In the foreground, a smartphone is mounted on a stand, displaying a social media feed. A keyboard and mouse are also visible on the desk. The background is a solid red wall with some blurred plants on the left.

Demo Time



Links



CEF Digital Home:

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature>

eGov EU Twitter Account: [@eGov_EU](#)

CEF DSS:

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/DSS>

DSS Framework on GitHub: <https://github.com/esig/dss>

Bouncy Castle for Java:

<https://www.bouncycastle.org/java.html>

Apache Sanctuario:

<https://santuario.apache.org/>

Apache PDFBox:

<https://pdfbox.apache.org/>


THANK YOU

@wernerkeil  @thodorisbais





Own your Developer Career



@thodorisbais