



Digital Signature Service

e-Contract.be BVBA
info@e-contract.be
2 september 2015

About e-Contract.be BVBA

- Consultancy
 - SOA security
- Projects: eID/security related only
 - From analysis to operational hosting
- SaaS: internal product line
 - eID Applet/Chrome, IdP, DSS, Trust Service, ...
 - MyCareNet/eHealth platform
 - IAM for bailiffs
 - Auction platform for bailiffs

Electronic Signatures

- Regulation (EU) No 910/2014

Electronic Signature

Advanced Electronic Signatures

Qualified Electronic Signatures

Qualified Electronic Signatures with SSCD

Digital
Signatures

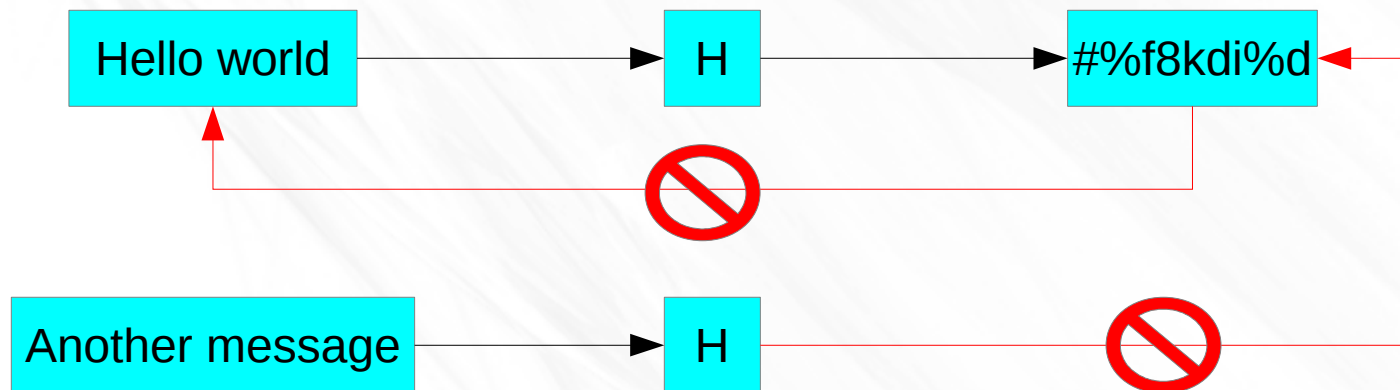
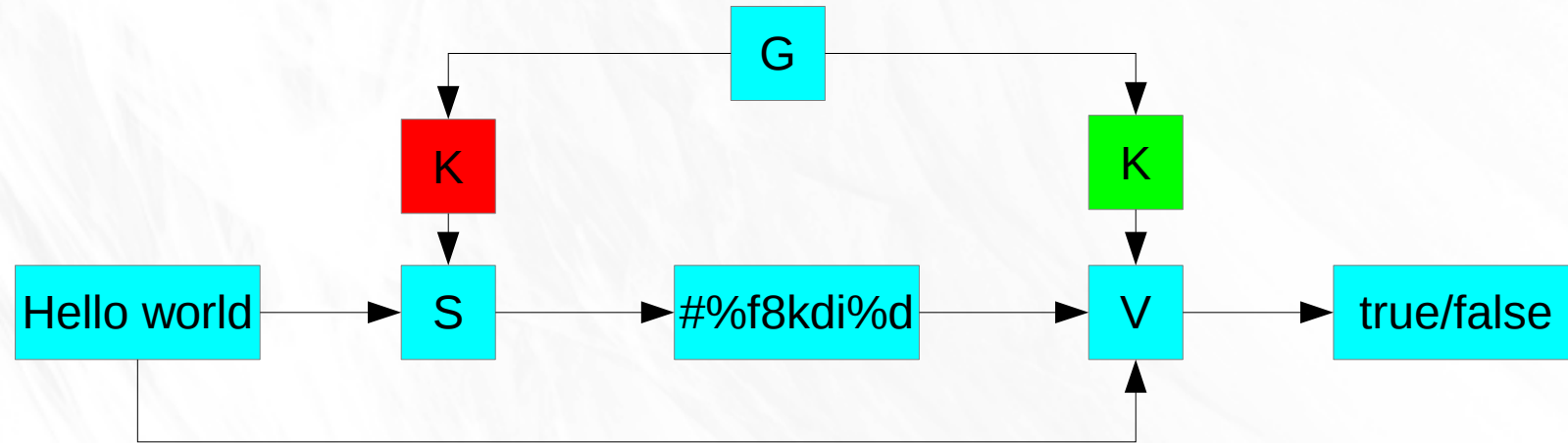
QC

eID

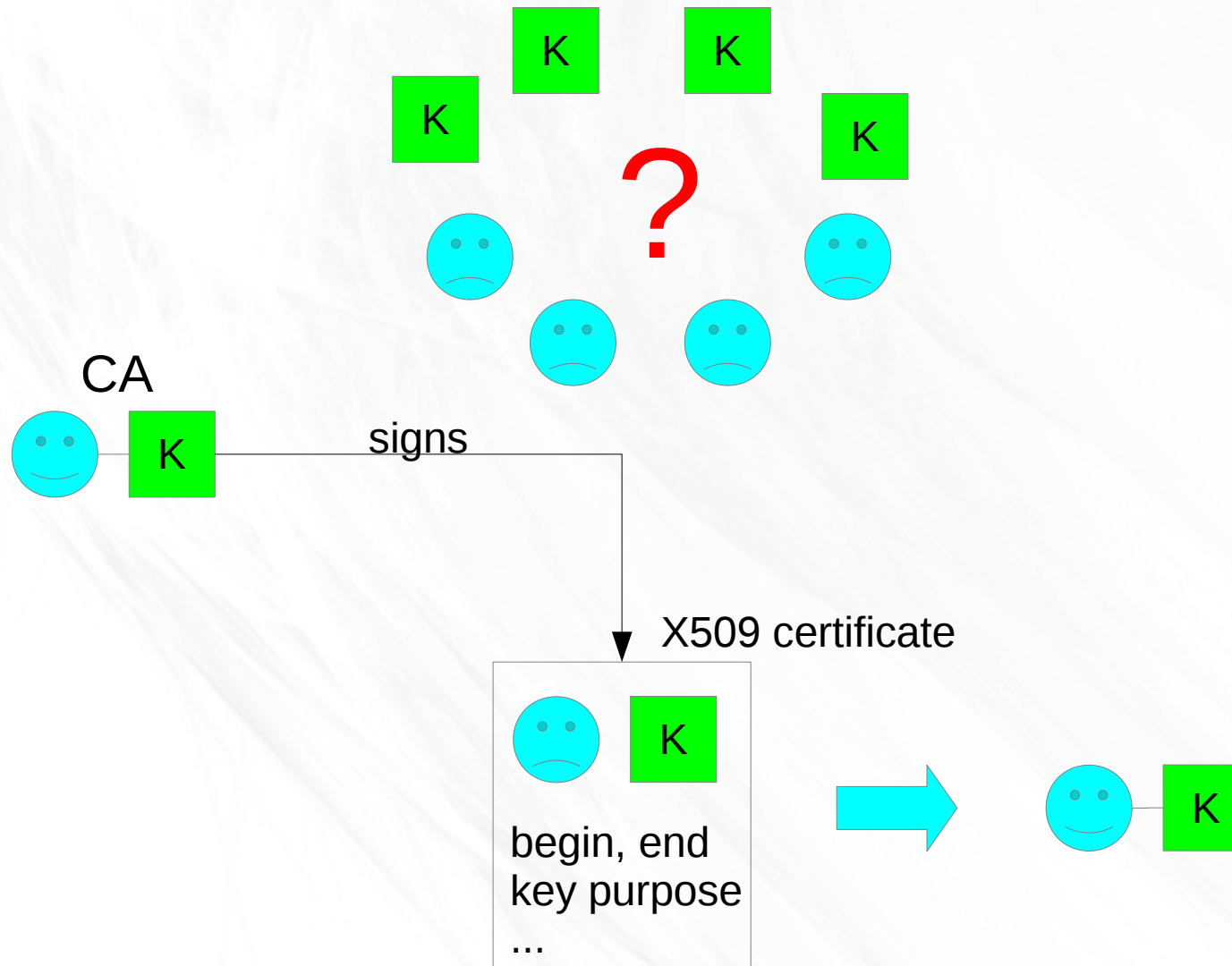
eID Functionality

- Identification
 - Who are you?
- Authentication
 - Can you prove who you are?
- Digital signatures
 - Proof of statement made in time

Digital Signatures



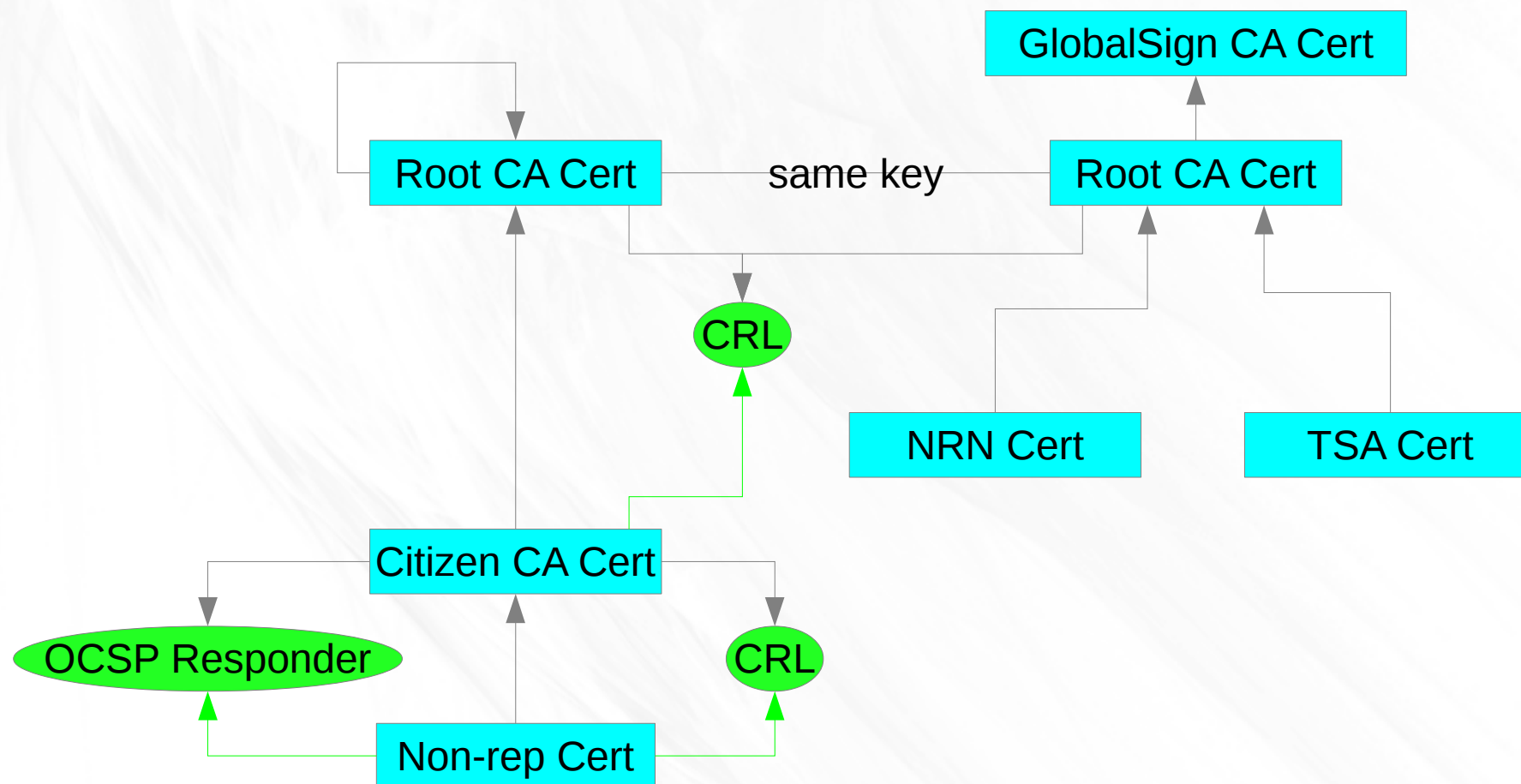
Certificates



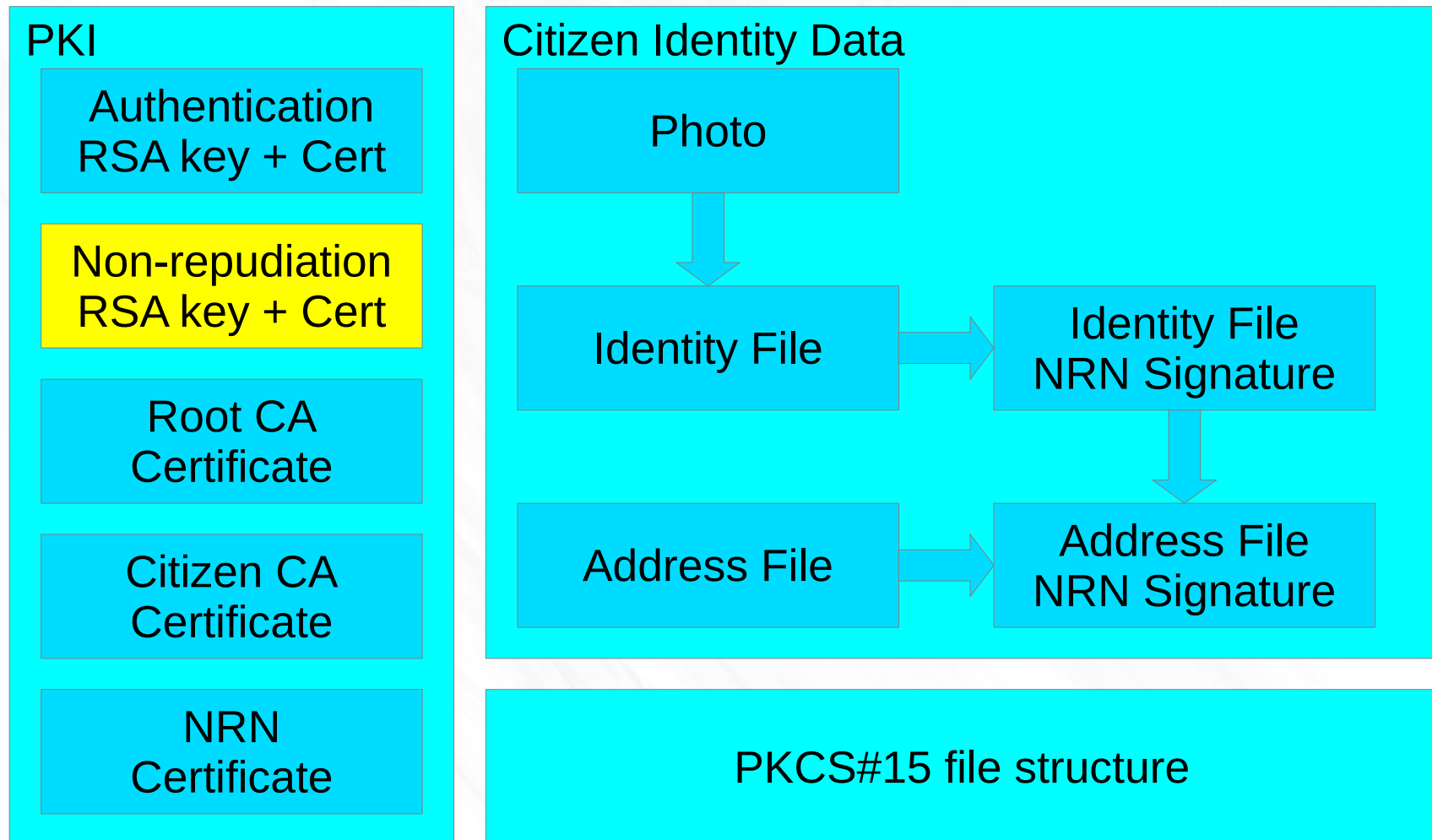
Certificate Status

- CRL: Certificate Revocation List
 - Contains serial numbers of revoked certs
 - Signed by the CA
 - Issued periodically
- Online Certificate Status Protocol
 - Online query for certificate status
 - Signed by the CA OCSP Responder

eID PKI Topology



eID Card Content



Advanced Electronic Signatures

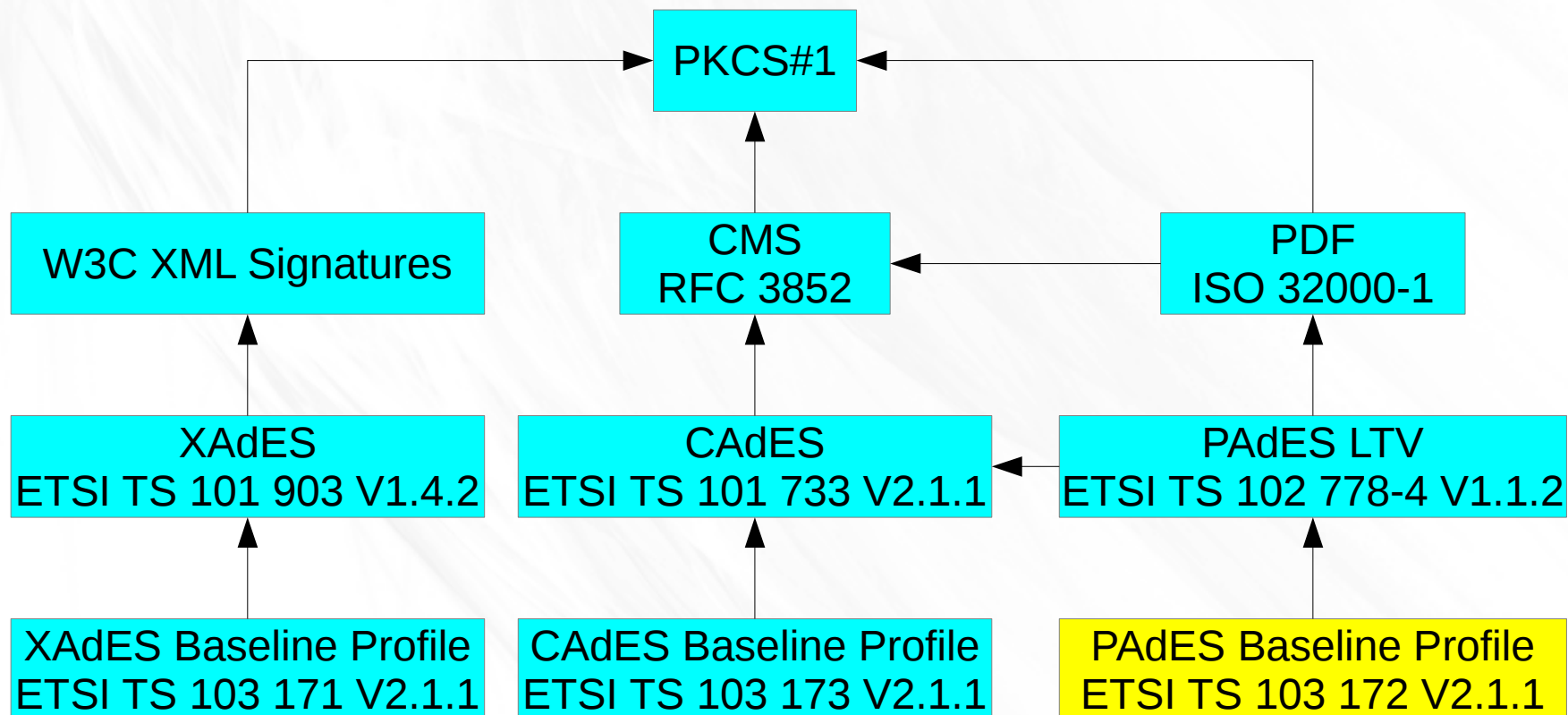
- Link a signature with an identity
 - X509 certificates
- Capable of identifying the signatory
 - AdES-BES
- Under control of signatory
 - eID as SSCD (CEN CWA 14169)
- Integrity verification possible
 - Digital signature

Qualified eID Signatures

- Equivalent with handwritten signature
- Non-repudiation
- Are admissible as evidence in legal proceedings
- Accepted accross the European Union

Signature Specifications

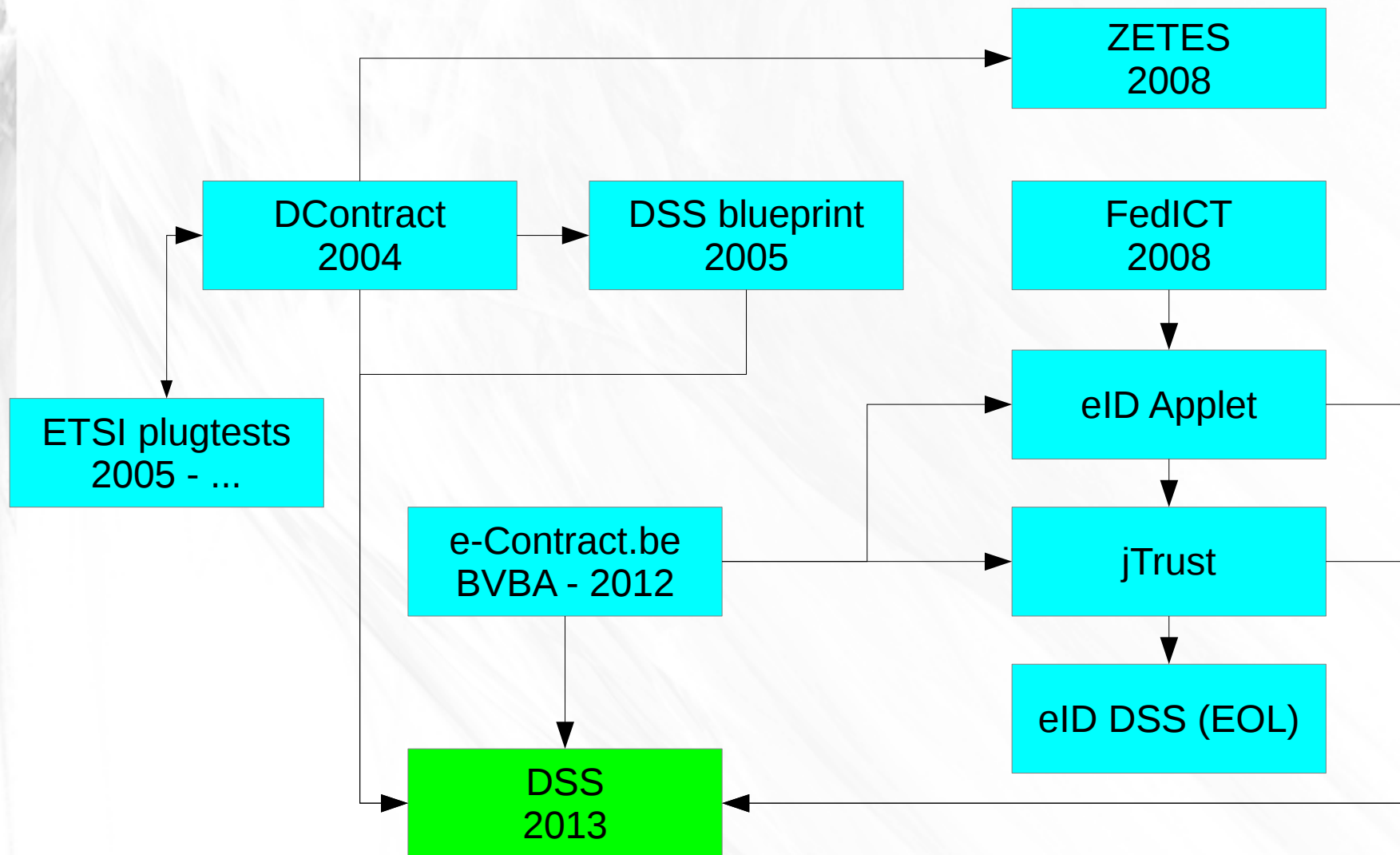
- e-Signature Expert Group: ETSI AdES



Digital Signature Service

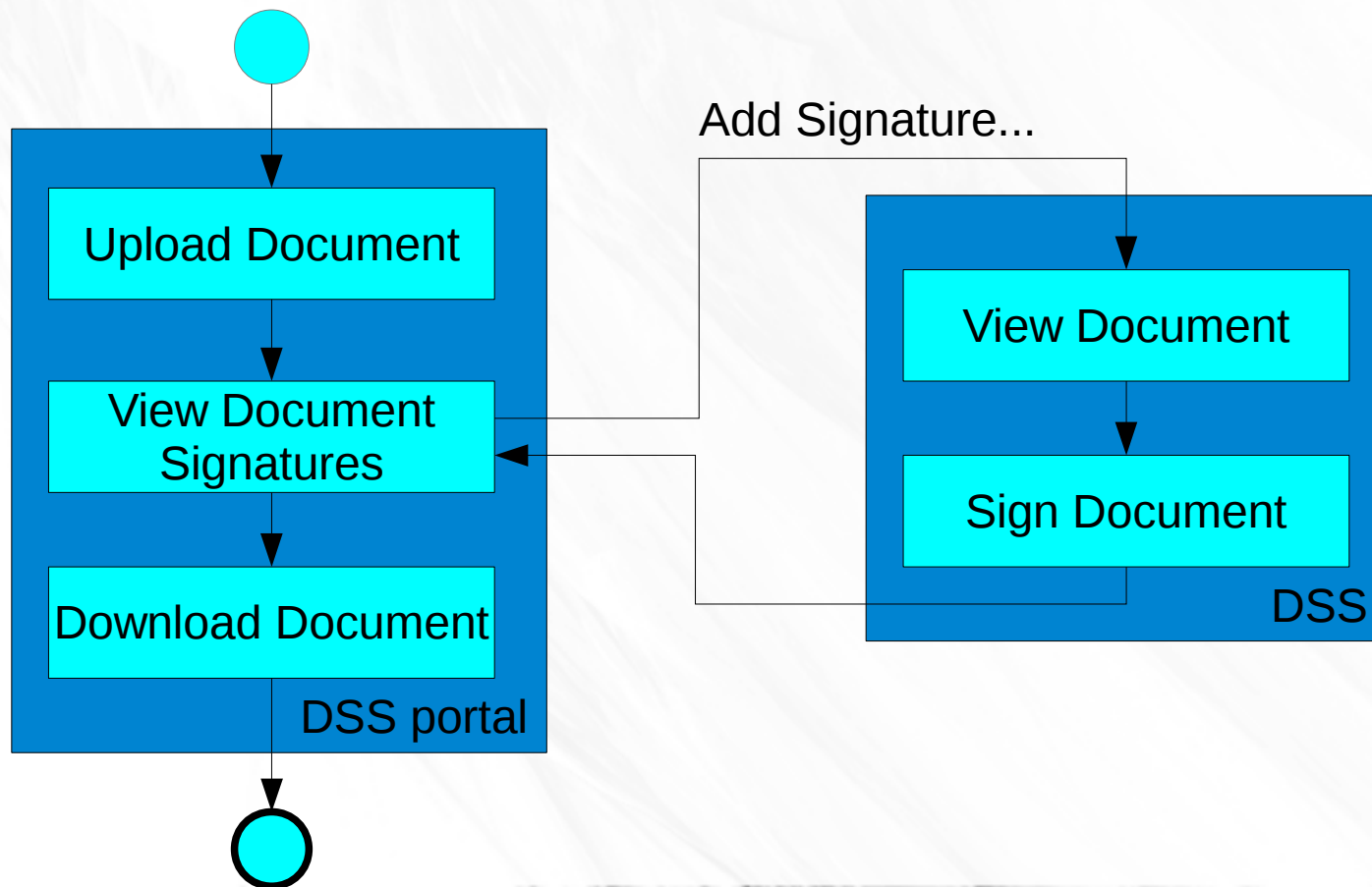
- XAdES: XML, ZIP documents
 - eID DSS compatible (XAdES-X-L)
 - ETSI XAdES Baseline Profile (long-term)
- PAdES: PDF documents
 - ETSI PAdES Baseline Profile (long-term)
- OASIS DSS based protocol
 - Secure and robust communication between DSS and your applications.

DSS History: 3rd generation

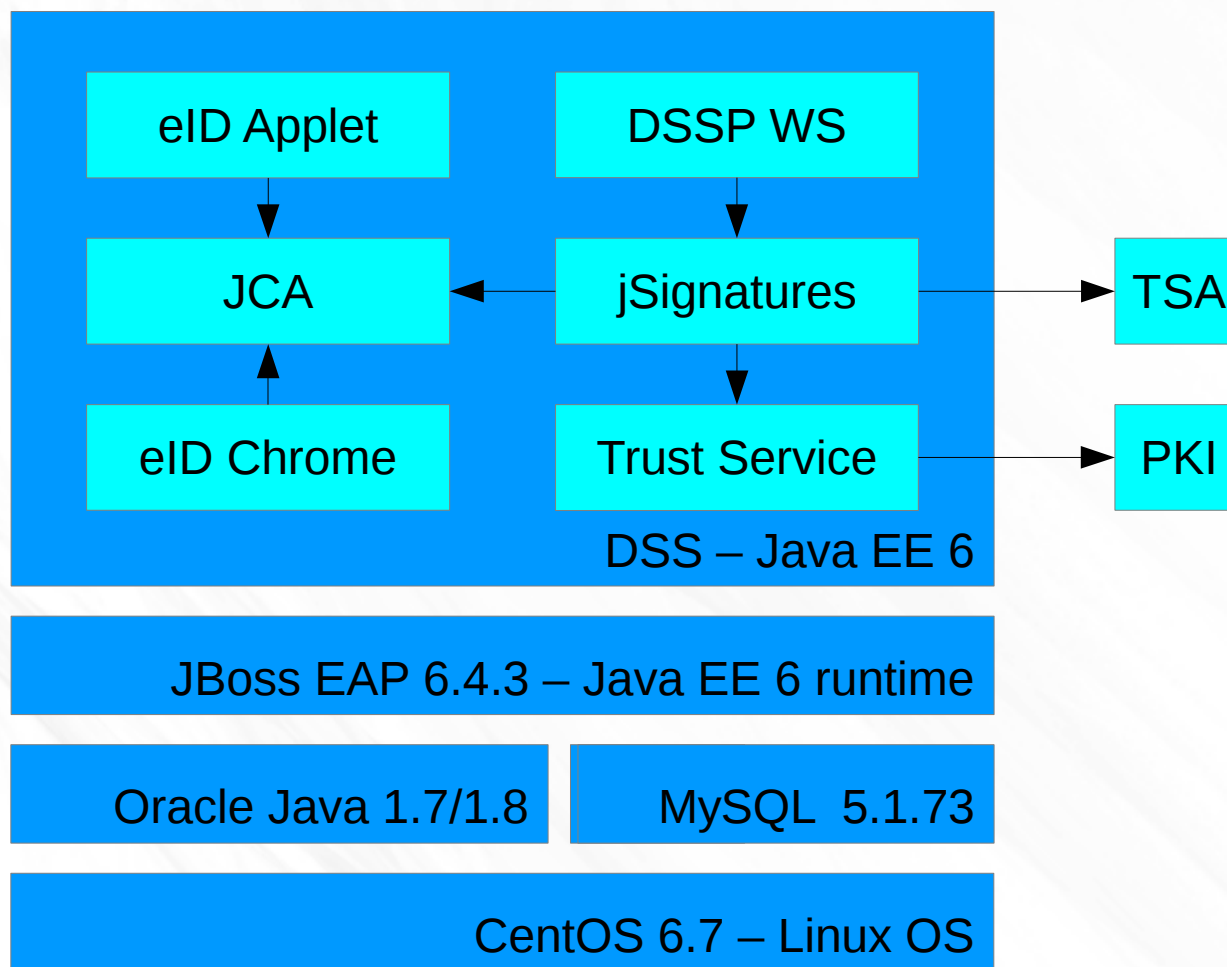


DSS Architecture

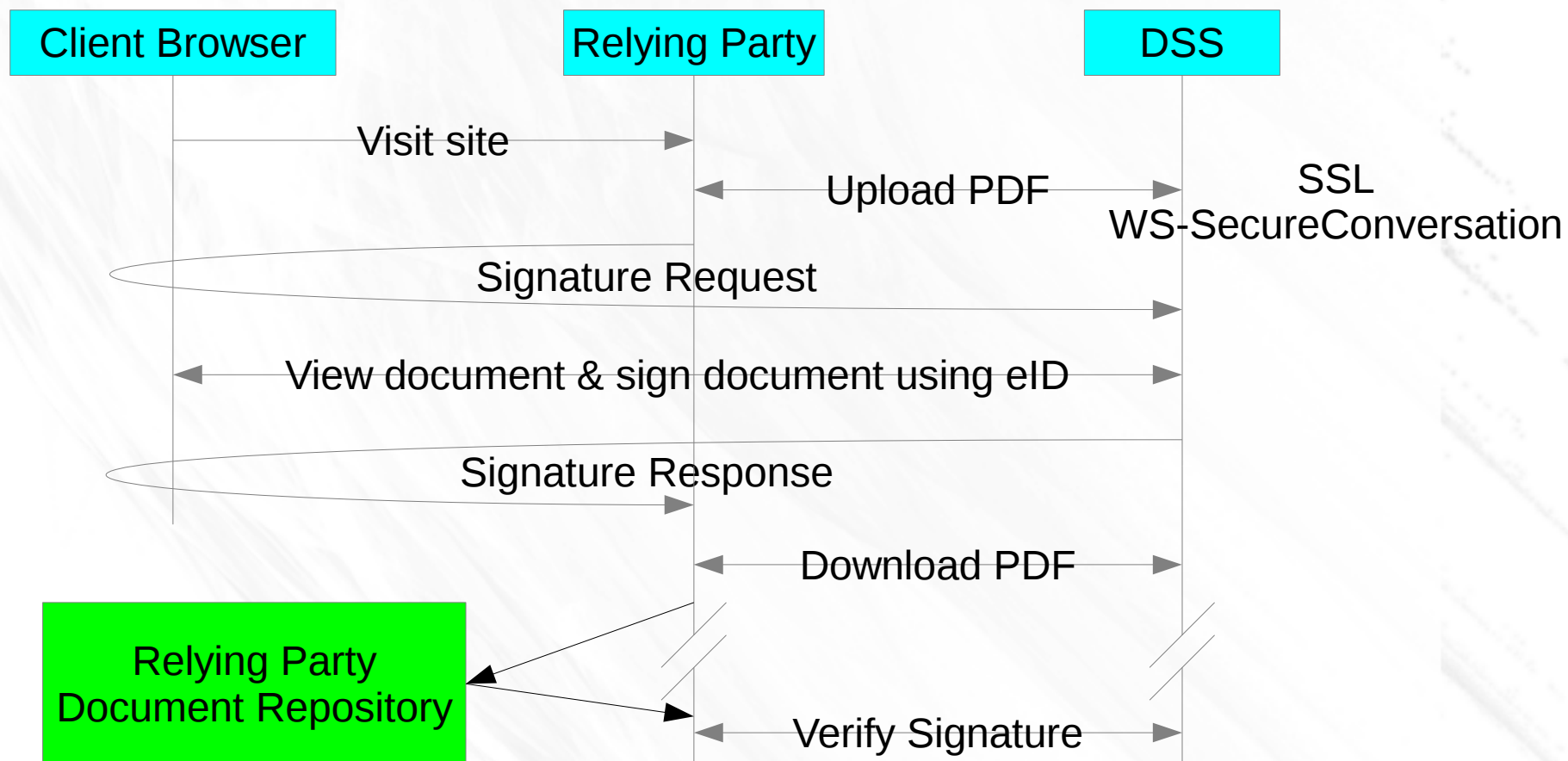
- <https://www.e-contract.be/dss/>
- <https://www.e-contract.be/dss-ws/>



DSS Design



Digital Signature Service Protocol



Service-centric versus document-centric

- Don't bother the end-user with signed documents.
- Signed documents stored in RP repository:
 - Loss of data
 - Hard-disks crash
 - Laptops get stolen
 - Accidental removal of files
 - Virus may corrupt files
 - User has multiple devices: laptop, tablet, ...
 - Signature archival (XAdES-A, PAdES document timestamp)
 - Access-control via verification portal
 - Application context-aware signature verification
 - Further processing of signed data possible

DSS Portal

Digital Signature Servi x

<https://www.e-contract.be/dss/>

English

Digital Signature Service Portal

Welcome

Welcome to the digital signature service portal.

Via this web application you can create and validate PDF and XML signatures.

The PDF signatures are compliant with PAdES LT-level as defined in ETSI PAdES Baseline Profile v2.2.2.

The default XML signatures are compliant with XAdES-X-L v1.4.2 and compatible with eID DSS 1.0.x signatures. Besides this, the DSS also supports XML signatures that are compliant with XAdES LT-level as defined in ETSI XAdES Baseline Profile v2.1.1.

This digital signature service portal serves as a demonstrator for the underlying Digital Signature Service product.

+ Choose document...

Signatures

Filename: cv-frank-cornelis-1979.pdf

Renew the time stamp before: Wednesday, January 23, 2019 12:00:00 PM

1	
Signing Time	Signer
Tuesday, February 18, 2014 3:22:32 PM	SERIALNUMBER=79102520991, GIVENNAME=Frank Henri, SURNAME=Cornelis, CN=Frank Cornelis (Signature), C=BE
1	

Add signature...
Download

DSS Web Service

Digital Signature Service

[View Document](#)

[Sign](#) [Cancel](#)

Frank Cornelis
Blaesenbergstraat 42
1800 VILVOORDE

homepage: <http://www.e-contract.be>
email: info@e-contract.be
Jabber: frank.cornelis@gmail.com
ICQ: 168372541

Degree
1997-2002 Ghent University
Licentiate (~ mas
Dissertation: Stud

College
1991-1997 Vrij Technisch In
Industrial Science
Dissertation: FA7

Feb 2012 Founded e
See [e-Contract.be BVBA Client](#)

Digital Signature Service

[Sign Document](#)

Signing...

[Details >>](#)

Please enter your PIN code

Digital Signature Service

[Welcome](#)

Welcome to the digital signature service.

Supported mime type
application/pdf
application/x-zip-compressed
application/xml
application/zip
text/xml

For information about how to integrate with the digital signature service, check out the [Digital Signature Service Protocol project](#).

[Click here to import Root CAs in Adobe Acrobat Reader](#)

Product version: 0.8.8

DSS – Google Chrome

- eID web browser runtime fragmentation

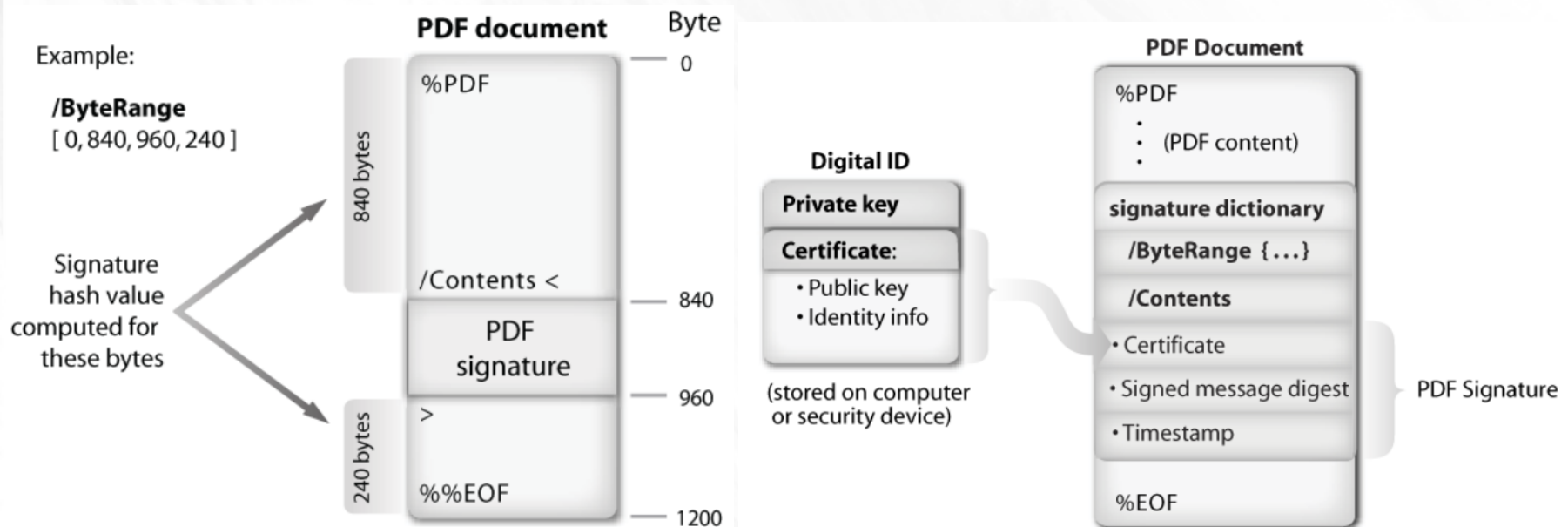


AdES implementation in DSS

- basic signature: allows multiple signatures
 - XAdES: co-signatures
 - PAdES: sign the entire PDF document
- AdES-BES: digest signatory certificate
- AdES-T: timestamp
 - 3rd party certification of signing time
- AdES-LTV: include revocation data
 - capture signing certificate validity status at signing time

ETSI PAdES

- Signature time-stamp
- Document time-stamp



Signature Validation

cv-frank-cornelis-1979.pdf - Adobe Reader

Bestand Bewerken Beeld Venster Help

Ondertekend en alle handtekeningen zijn geldig.

Handtekeningen

Alles valideren

Rev. 1: Ondertekend door Frank Cornelis (Signature)

Handtekening is geldig:

- PDF is niet gewijzigd sinds deze handtekening is toegepast
- Ondertekend door de huidige gebruiker
- De handtekening is voorzien van een ingesloten tijdstempel.
- De handtekening is geschikt voor LTV

Handtekeningdetails

Certificaatdetails...

Laatste keer gecontroleerd: 2014.04.10 03:32:04 -07'00'

Veld: Signature1 (onzichtbare handtekening)

Klik om deze versie weer te geven

Eigenschappen van handtekening

De handtekening is GELDIG en is ondertekend door Frank Cornelis (Signature).

Tijd van ondertekening: 2014/02/18 07:22:32 -07'00'

Geldigheidsoverzicht

De PDF is niet gewijzigd sinds deze handtekening is toegepast.

De certificering staat het invullen, ondertekenen en plaatsen van opmerkingen in formulieren toe voor dit document. Andere wijzigingen zijn niet toegestaan.

Het document is ondertekend door de huidige gebruiker.

De handtekening is voorzien van een ingesloten tijdstempel. Tijd tijdstempel: 2014/02/18 07:22:39 -07'00'

Handtekening werd gevalideerd op de beveiligde tijd (tijdstempel): 2014/02/18 07:22:39 -07'00'

Geavanceerde eigenschappen van handtekening

Details van handtekening

De handtekening is gemaakt met e-contract.be DSS.

Hash-algoritme: SHA256

Details van tijdstempel

Tijdstempel ingesloten in ondertekening

Tijdstempels worden op dezelfde manier ondertekend als documenten. Voor een geldige tijdstempelhandtekening moet u de tijdstempelinstantie vertrouwen die de tijdstempel heeft ondertekend. Klik op Certificaat tonen om de details van de verificatie van de tijdstempelhandtekening te bekijken.

Tijdstempelinstantie: Time Stamping Authority Certificaat tonen...

Tijdstempels worden gemaakt met een specifiek beleid dat is gedefinieerd door de tijdstempelinstantie. Met een beleid kan onder andere de betrouwbaarheid van de tijdsbron worden aangegeven. Het beleid voor deze tijdstempel wordt aangeduid met de id 2.16.56.9.3.1. Neem contact op met de tijdstempelinstantie voor meer informatie over het tijdstempelbeleid.

Sluiten

informatie over ondertekenaar

Het pad van het certificaat van de ondertekenaar naar een certificaat van de uitgever is gemaakt.

Het certificaat van de ondertekenaar is geldig en is niet ingetrokken.

Certificaat van ondertekenaar weergeven...

Geavanceerde eigenschappen...

Handtekening valideren Sluiten

Certificaat weergeven

In dit dialoogvenster kunt u de details van een certificaat en de gehele uitgaveketen bekijken. De details komen overeen met het geselecteerde item.

☐ Alle gevonden certificeringspaden tonen

- Cybertrust Global Root
 - Belgium Root CA2
 - Time Stamping Authority

Overzicht Details Intrekking Vertrouwd Beleid Juridische kennisgeving

Het geselecteerde certificaat is geldig

Details

Het geselecteerde certificaat wordt als geldig beschouwd omdat het niet voorkomt in de certificaatintrekkingslijst (CRL) die is ingesloten in het document.

De CRL is ondertekend door "Belgium Root CA2" op 2014/01/01 04:00:00 -07'00' en is geldig tot 2014/07/31 04:00:00 -07'00'.

Klik op Details van ondertekenaar voor meer informatie over de bron.

Visible PDF Signatures

pades-lt-3755602642662172823.pdf - Adobe Reader

Bestand Bewerken Beeld Venster Help

Gereedschappen Ondertekenen Opmerking

Ondertekend en alle handtekeningen zijn geldig. Handtekeningvenster

Handtekeningen

Alles valideren

Rev. 1: Ondertekend door Frank Cornelis (Signature)

Handtekening is geldig:

- PDF is niet gewijzigd sinds deze handtekening is toegepast
- De identiteit van de ondertekenaar is geldig
- De handtekening is voorzien van een ingesloten tijdstempel.
- De handtekening is geschikt voor LTV

Handtekeningdetails

Laatste keer gecontroleerd: 2014.11.18 23:03:26 -08'00'

Veld: Signature1 op pagina 1

[Klik om deze versie weer te geven](#)

Rev. 2: Ondertekend door Time Stamping Authority

Handtekening is geldig:

- PDF is niet gewijzigd sinds deze handtekening is toegepast
- De identiteit van de ondertekenaar is geldig
- Handtekening is een tijdstempelhandtekening voor een document
- De handtekening is geschikt voor LTV

Handtekeningdetails

Laatste keer gecontroleerd: 2014.11.18 23:03:07 -08'00'

Veld: Signature2 (onzichtbare handtekening)

[Klik om deze versie weer te geven](#)

Hello World

Eigenschappen van handtekening

De handtekening is GELDIG en is ondertekend door Frank Cornelis (Signature).

Tijd van ondertekening: 2014/11/11 22:48:19 -08'00'

Reden: test

Locatie: Vilvoorde

[Geldigheidsoverzicht](#)

De PDF is niet gewijzigd sinds deze handtekening is toegepast.

De certificatie staat het invullen, ondertekenen en plaatsen van de handtekening voor dit document. Andere wijzigingen zijn mogelijk.

Geavanceerde eigenschappen van handtekening

[Details van handtekening](#)

De handtekening is gemaakt met e-contract.be DSS.

Hash-algoritme: SHA256

[Details van tijdstempel](#)

[Tijdstempel ingesloten in ondertekening](#)

Tijdstempels worden op dezelfde manier ondertekend als documenten. Voor een geldige tijdstempelhandtekening moet u de tijdstempelinstantie vertrouwen die de tijdstempel heeft ondertekend. Klik op Certificaat tonen om de details van de verificatie van de tijdstempelhandtekening te bekijken.

Tijdstempelinstantie: **Stamping Authority** [Certificaat tonen...](#)

Tijdstempels worden gemaakt met een specifiek beleid dat is gedefinieerd door de tijdstempelinstantie. Met een beleid kan onder andere de betrouwbaarheid van de tijdsbron worden aangegeven. Het beleid voor deze tijdstempel wordt aangeduid met de id 2.16.56.9.3.1. Neem contact op met de tijdstempelinstantie voor meer informatie over het tijdstempelbeleid.

[Handtekening valideren](#)

Visualisation Profiles

- DSS can be extended with new profiles
- Customers can design their own profile
- Reference codes: printable PDF documents



Signatory Role

- From the contractual context
- Explicit via:
 - PAdES:
 - Reason field
 - Location field
 - XAdES:
 - SignerRole
 - SignatureProductionPlace

Authorization

- Based on OASIS XACML 2.0 Policy
- Relying party can restrict signatories
 - SERIALNUMBER=123456789,.*,C=BE
- Implemented in DSSP 1.1.0
- Doccle uses this extension

Secure Environment

- Law July 9, 2001 – chapter 4, art. 6
 - betrouwbare systemen en producten te gebruiken
- Certification Practice Statement (Citizen CA)
 - 4.5.1 Verplichtingen van de Burger
 - 9.4.1 Plichten van de Burger
 - 9.4.3 Aansprakelijkheid van de Burger ten opzichte van de Vertrouwende Partijen
- CCID Secure PIN pad readers
- CEN CWA 14170 → CC Security Target

DSS Roadmap

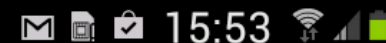
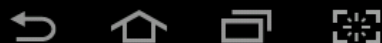


eID Viewer

Pippa
Cornelis
25-04-2010
Blaesenbergstraat 42
1800
Vilvoorde

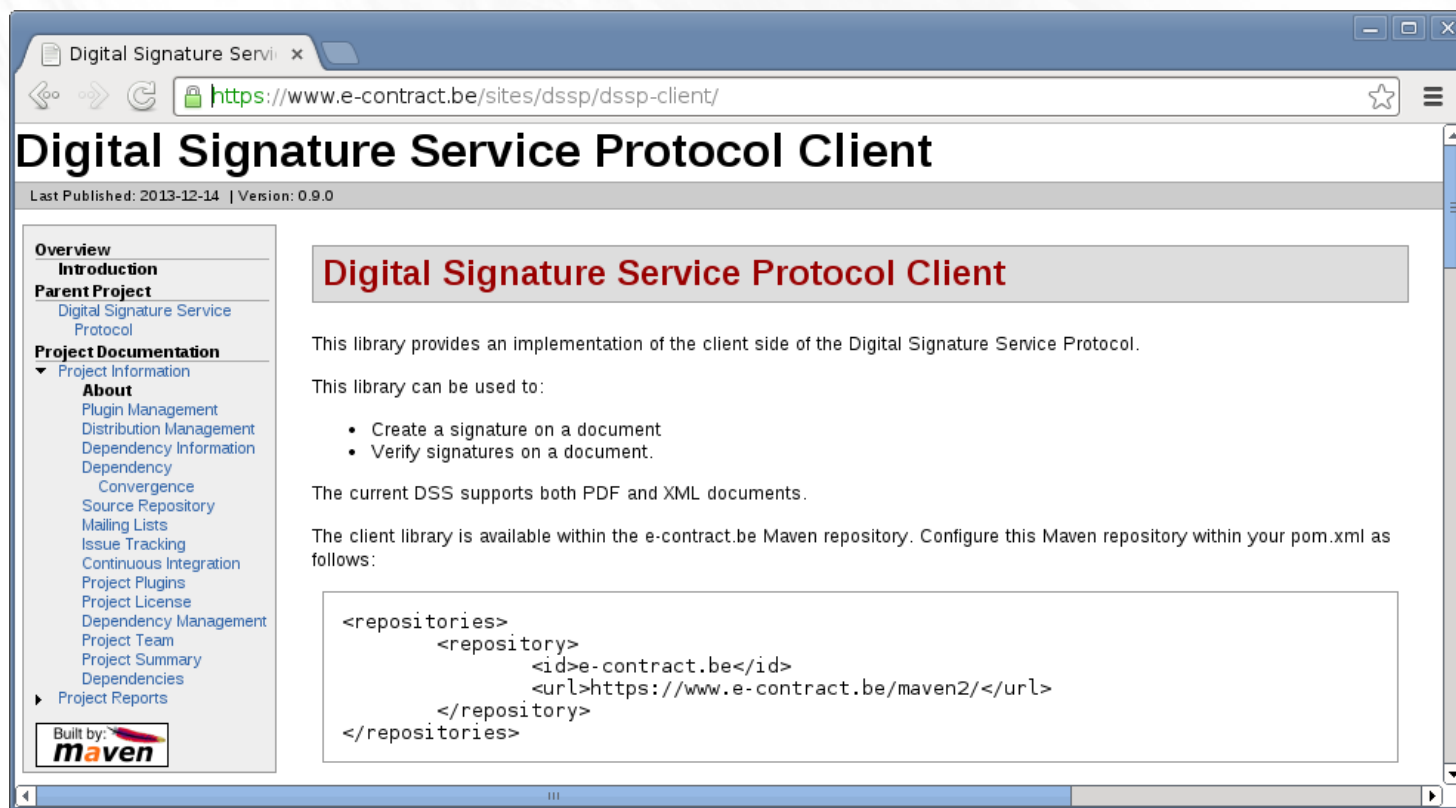


- Protocol features
 - Metadata for bootstrapping
 - Message level encryption
- PAdES-A & XAdES-A
- Android support
- Office ODF/OOXML support
- ISO 27001



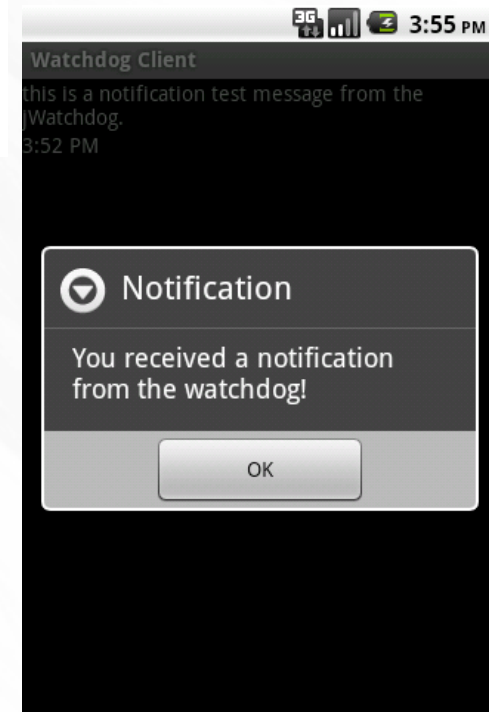
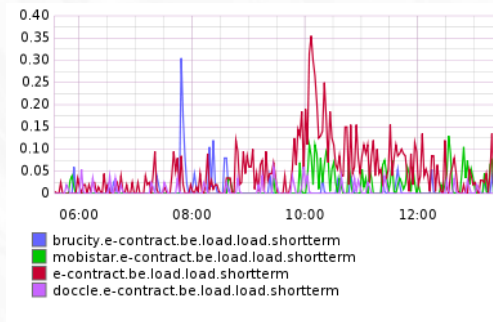
DSS Protocol SDK

- <https://www.e-contract.be/sites/dssp/>
- SDKs for Java, PHP, and .NET 3.5/4.0+
- Source code at <https://github.com/e-Contract>



DSS as a Service

- Managed service by e-Contract.be BVBA
- SLA
- 3th line support
- Regular updates:
 - Bug fixes, security fixes
 - New features
- Professional monitoring
- Fail-over system



Licensing Model

- Dedicated environment (like Mobistar, Doccile)
 - 99,95% SLA
 - Shared environment as fail-over (worst-case)
 - Set up cost
 - Maintenance cost
- Pricing per signature creation
 - Bandwidth
 - Timestamps
 - Multiple signature verifications

References

- eID Identity Provider
 - Mobistar, Proximus
 - MIVB, Air Cargo Systems
 - Van Lanschot, Bolero KBC
- DSS
 - Registratie Huurgarantiefonds
 - Subsidieloket Provincie Antwerpen
 - Doctar
 - CoronaDirect – Belfius
 - Doccle

Q&A

- e-Contract.be BVBA
- Frank Cornelis (former eID Architect FedICT)
- info@e-contract.be
- <https://www.e-contract.be>



e-contract.be
SAFE E-TRANSACTIONS