Post-Quantum

Cryptography Conference

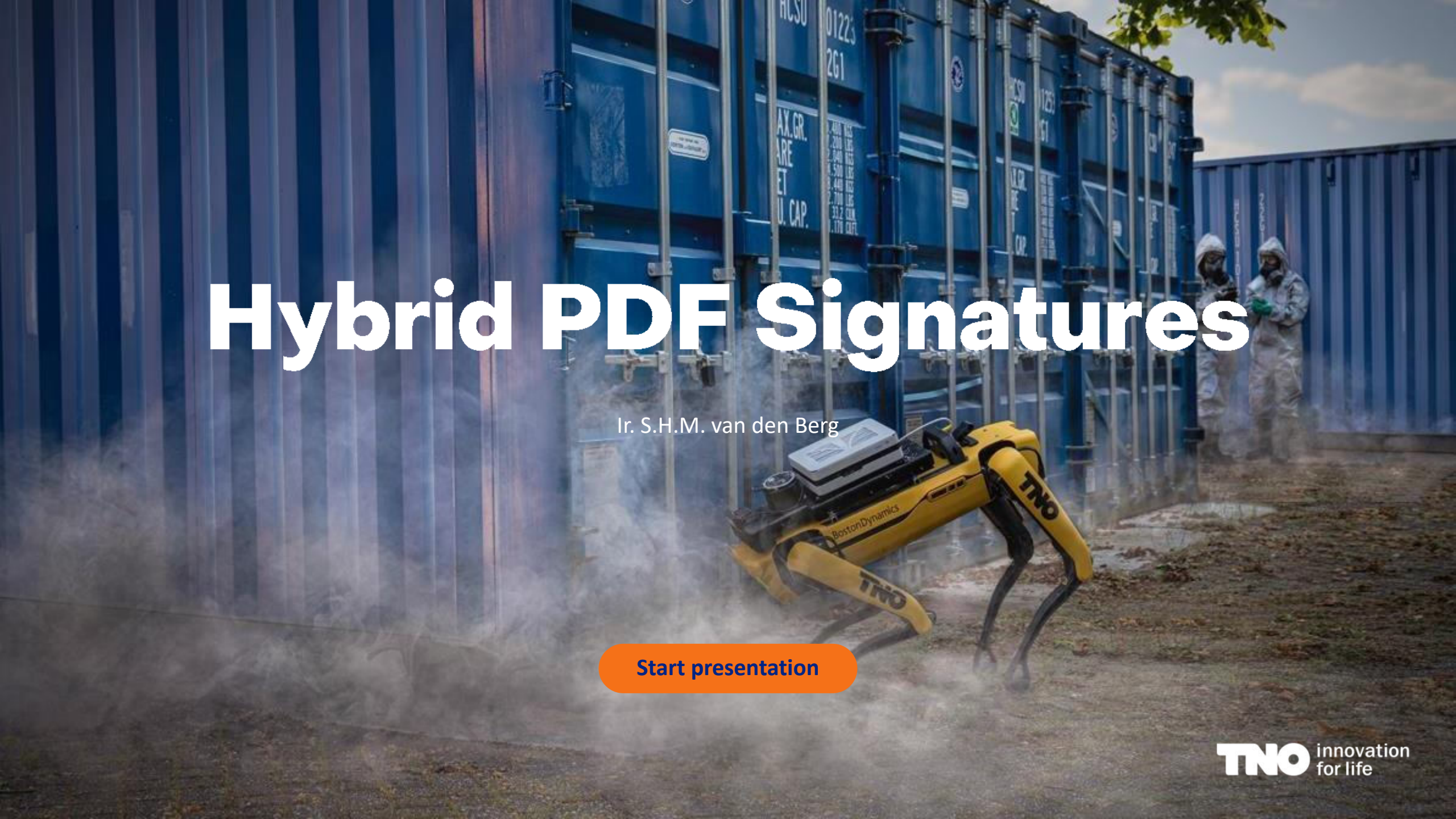
Using quantum-safe hybrid certificates for signing documents

Stefan van den Berg
Cryptographer at TNO

ENTRUST HID PKI Consortium

Hybrid PDF Signatures

Ir. S.H.M. van den Berg



Start presentation

TNO innovation for life

Hybrid PDF Signatures

HAPKIDO

Ir. S.H.M. van den Berg |


TNO innovation for life

1. Contracts

- Basis for legal agreements
  - Valid for long periods

- Many are digitalized
  - My contract with TNO is digitally signed

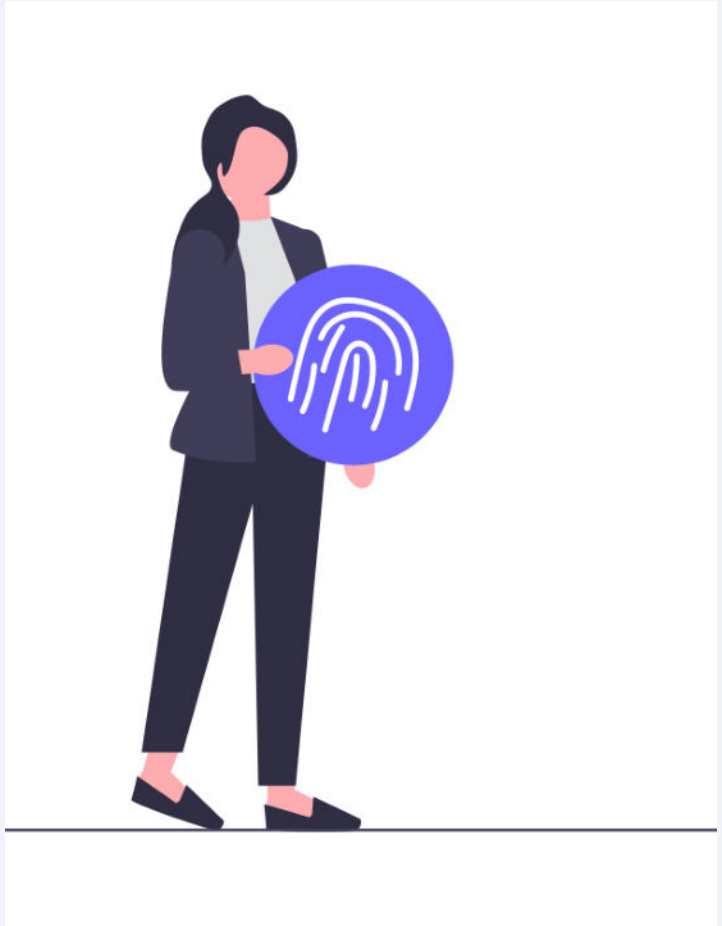
2. Quantum computer

- Allows for many amazing things:
  - Optimizations
  - Simulations
  - Factorization of numbers

- Impact on cyber security
  - Threatens classical cryptography

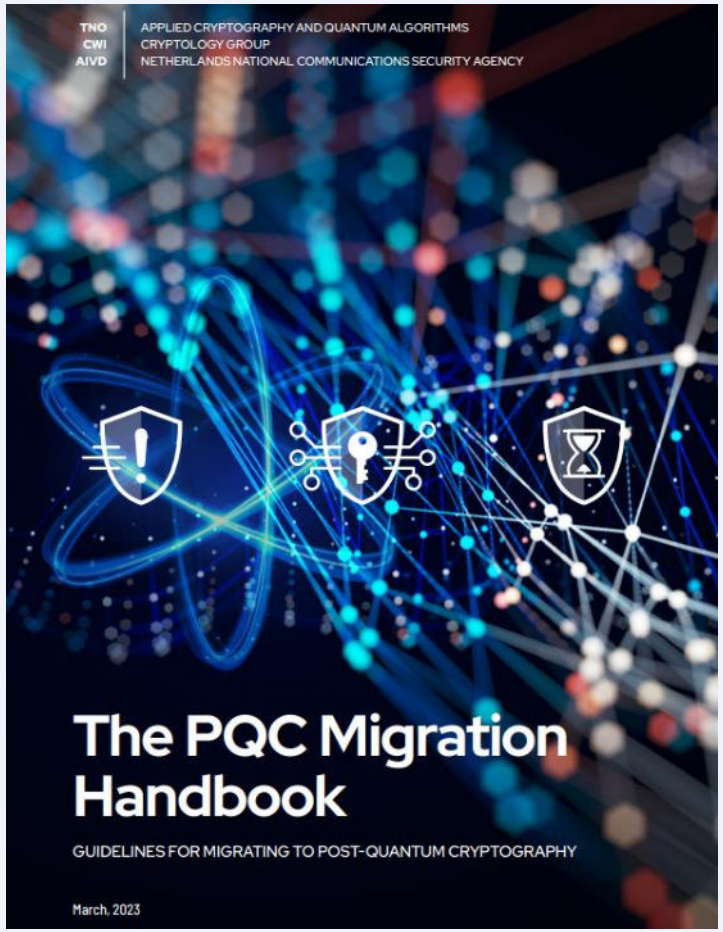
Impact

- Forge contracts
  - Recalculating signature
- Loss of trust in classical signatures
- Solutions:
  - Reissue all contracts
    - Impractical due to number of documents
  - Transition a.s.a.p. to Post-Quantum Cryptography



Transition to Post-Quantum Cryptography

- PQC migration handbook
  - AIVD, CWI and TNO
  - Help companies transition to PQC
- Crypto-agility
  - Minimal effort to change cryptographic algorithms
- Asymmetric Cryptography strategy
  - Hybrid solutions

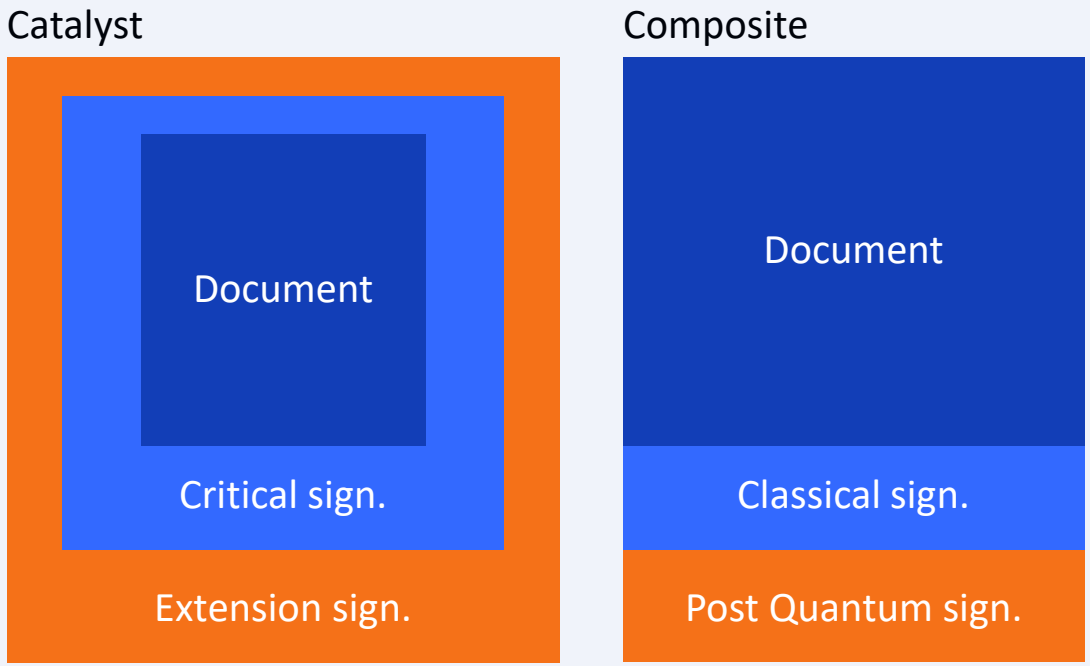


Hybrid solutions

- Combination between classical and quantum cryptography

- Catalyst (X.509 ITU-T)
  - Critical algorithm
  - Extension algorithm

- Composite (IETF Draft)
  - Multiple keys in certificate
  - Standardization under development
  - No adoption yet…



Applying signatures to PDF's

- Most digital contracts PDF format

- Legally compliant across borders
  - eIDAS Regulation (Europe)

- PAdES standard
  - Information inside of pdf
    - Visible signature
    - Invisible signature
  - Different profiles for different use-cases

What is inside the PDF

- Add byte range used for message digest
  - Should be entire document excluding signature dictionary
- Message digest
- Certificate used

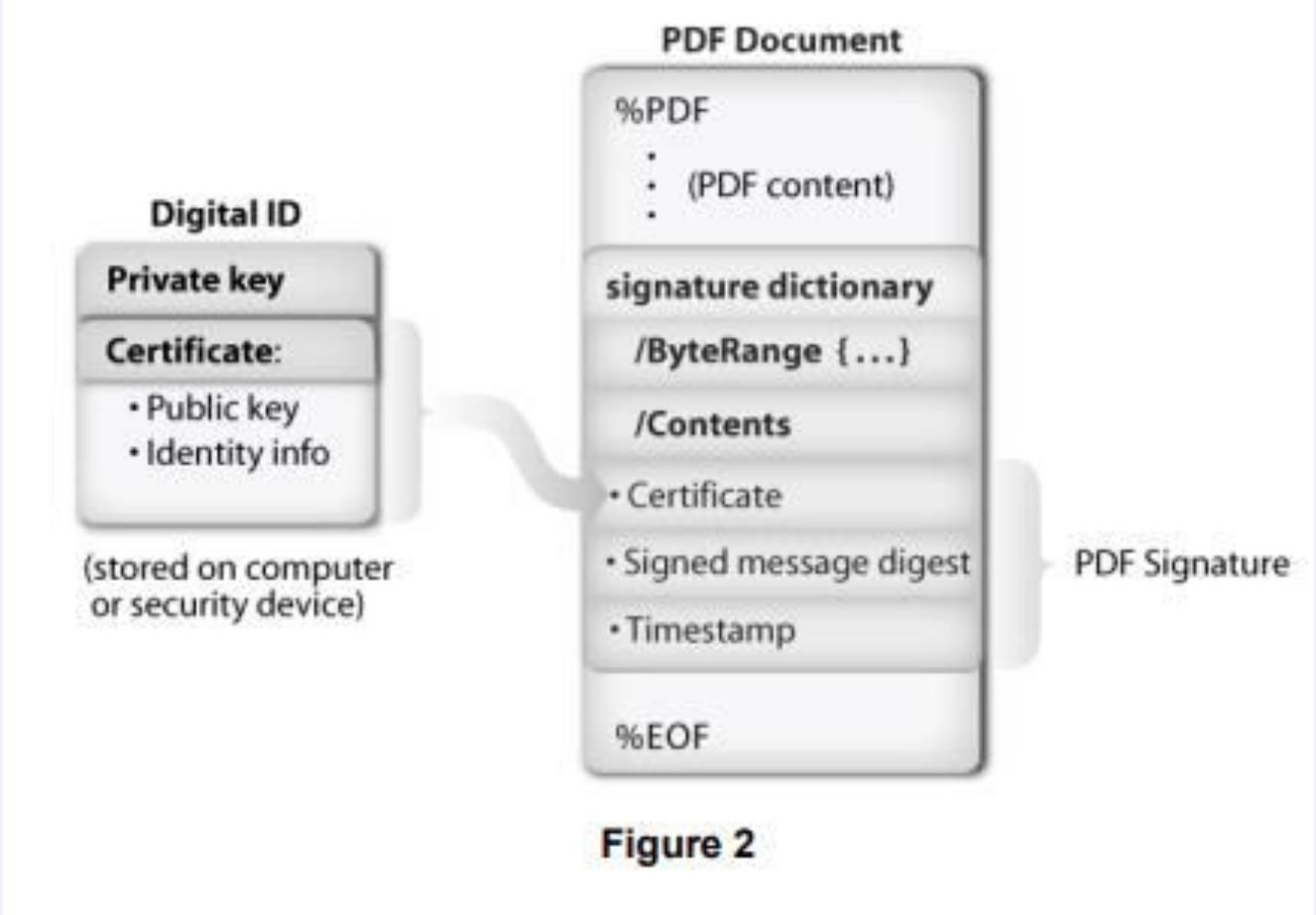
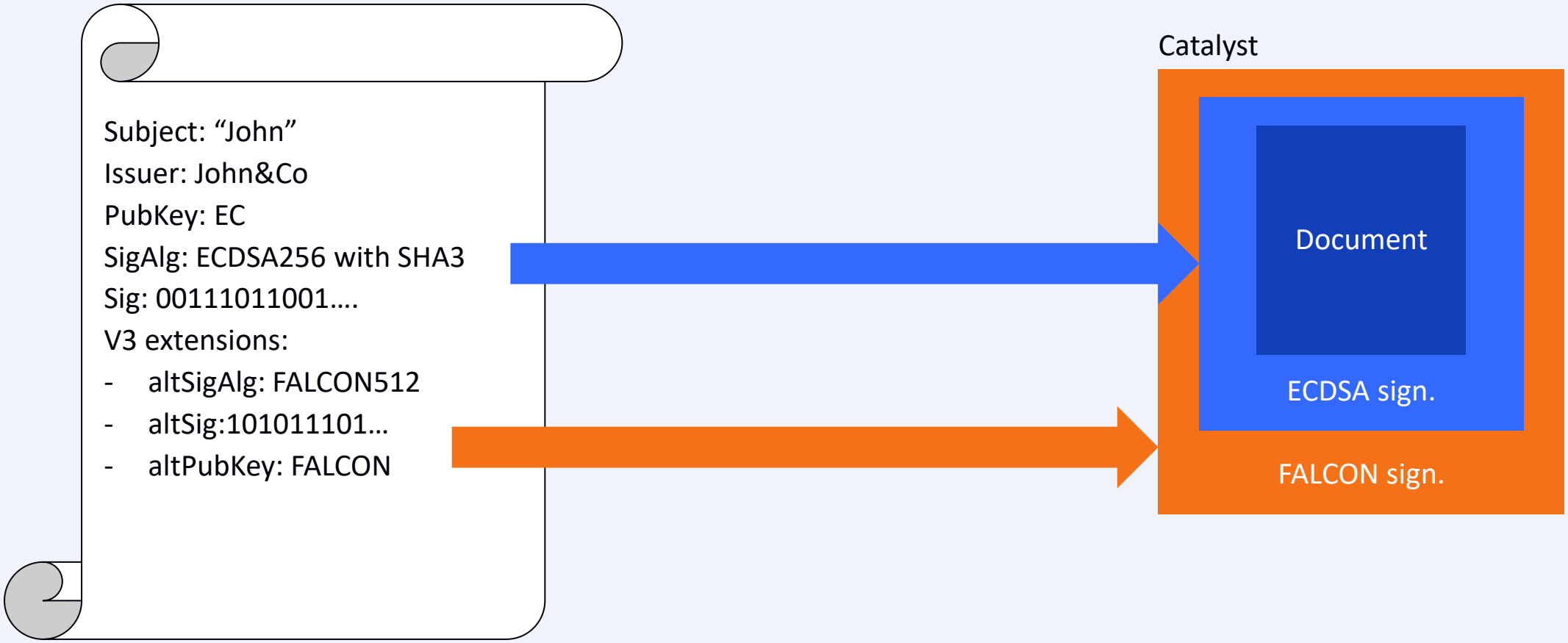


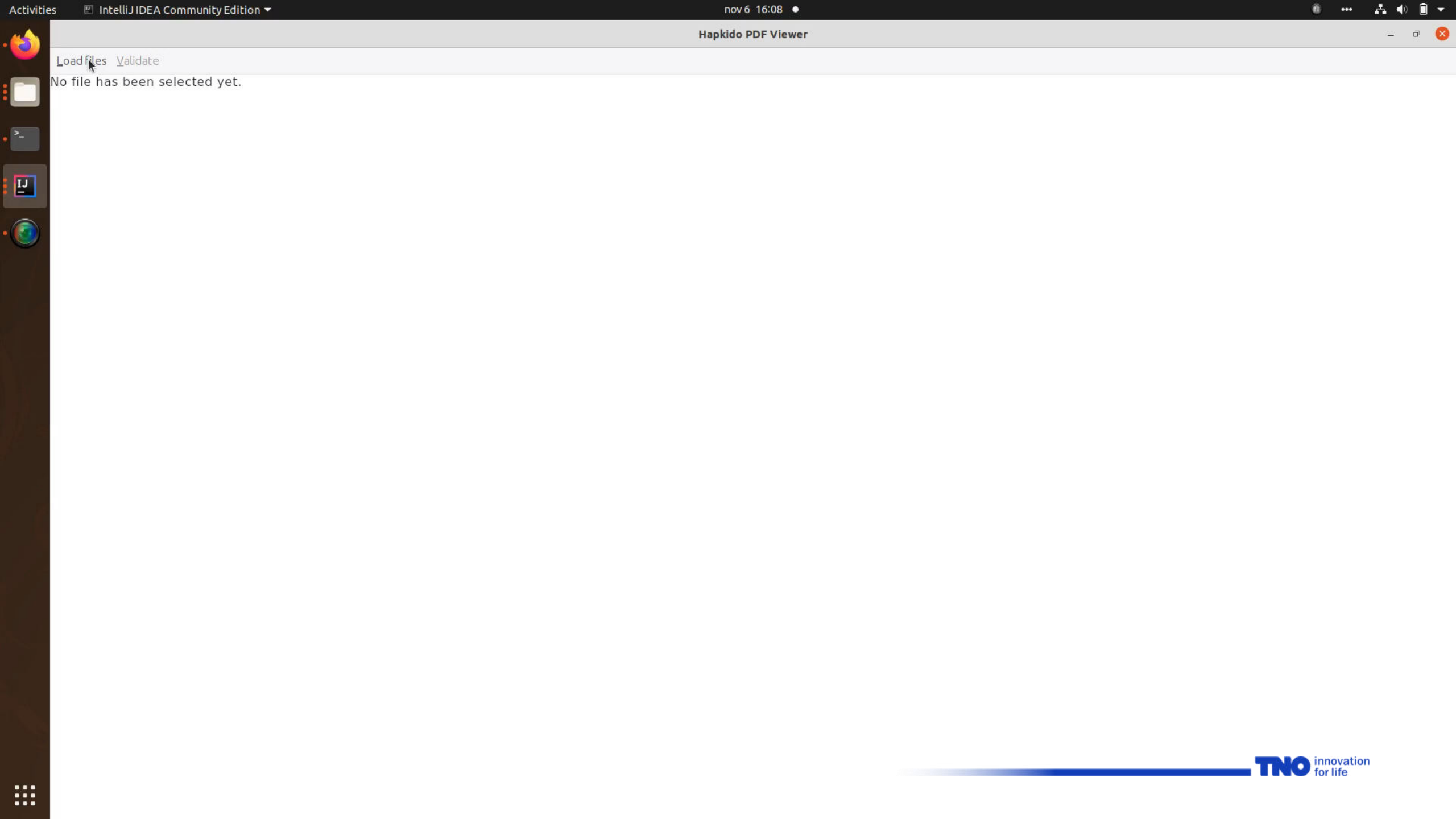
Figure 2

DSS PAdES

- ‘Implementation from the EU
- Digital Signature Service
- Our contribution:
  - Extended with Catalyst hybrid solution
  - Both for signing as for validation

Demo explanation



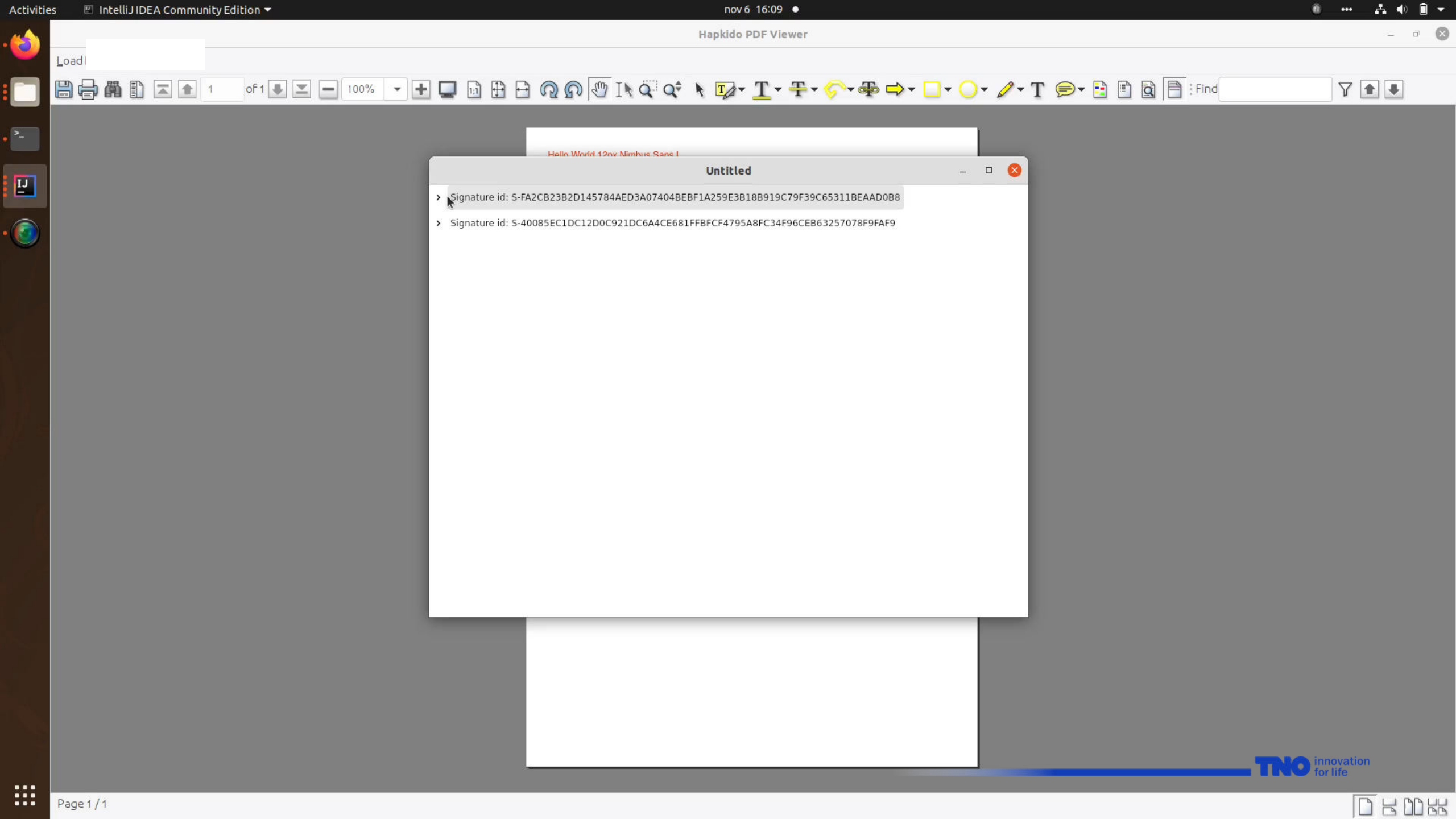

Activities
IntelliJ IDEA Community Edition
nov 6 16:08
Hapkido PDF Viewer
Load files
Validate
No file has been selected yet.
TNO innovation for life

Hapkido PDF Viewer

Load files Validate

1 of 1 100% Find

Hello World 12px Nimbus Sans L
Hello World 12px DejaVu Sans
Hello World 12px FreeSans
Hello World 12px DejaVu Serif
Hello World 12px Liberation Serif
Hello World 12px chocolate


Activities
IntelliJ IDEA Community Edition
nov 6 16:09
Hapkido PDF Viewer
Load
1
of 1
100%
Find
Hello World 12px Nimbus Sans L
Untitled
Signature id: S-FA2CB23B2D145784AED3A07404BEBF1A259E3B18B919C79F39C65311BEAAD0B8
Signature id: S-40085EC1DC12D0C921DC6A4CE681FFBFCF4795A8FC34F96CEB63257078F9FAF9
TNO innovation for life
Page 1 / 1

Hapkido PDF Viewer

Load files Validate

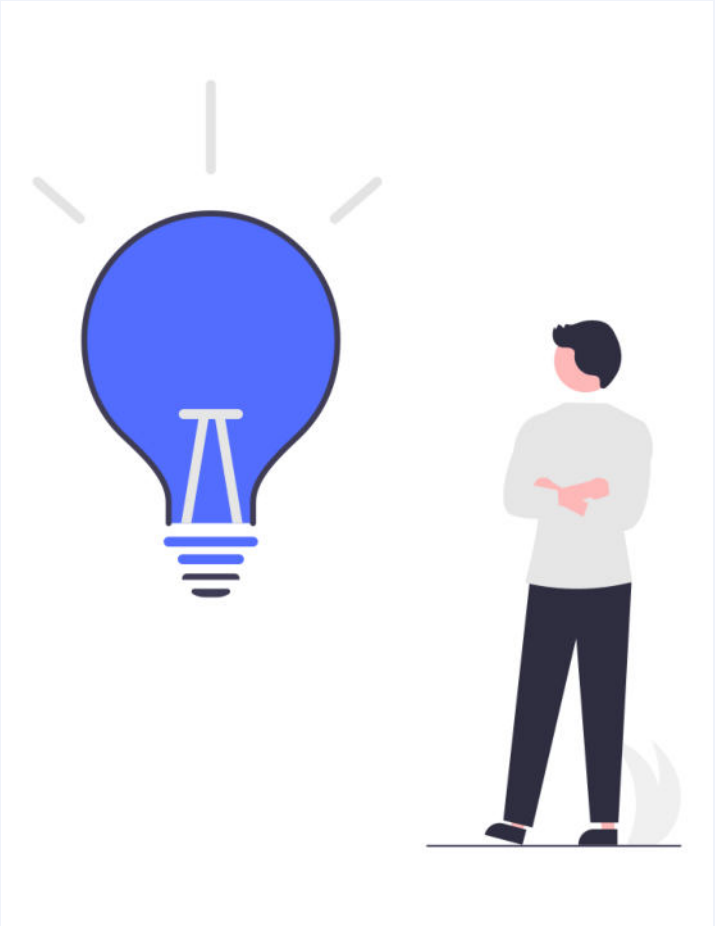
1 of 1 100% Find

Hello World 12px Nimbus Sans L
Hello World 12px DejaVu Sans
Hello World 12px FreeSans
Hello World 12px DejaVu Serif
Hello World 12px Liberation Serif
Hello World 12px chocolate

TNO innovation for life

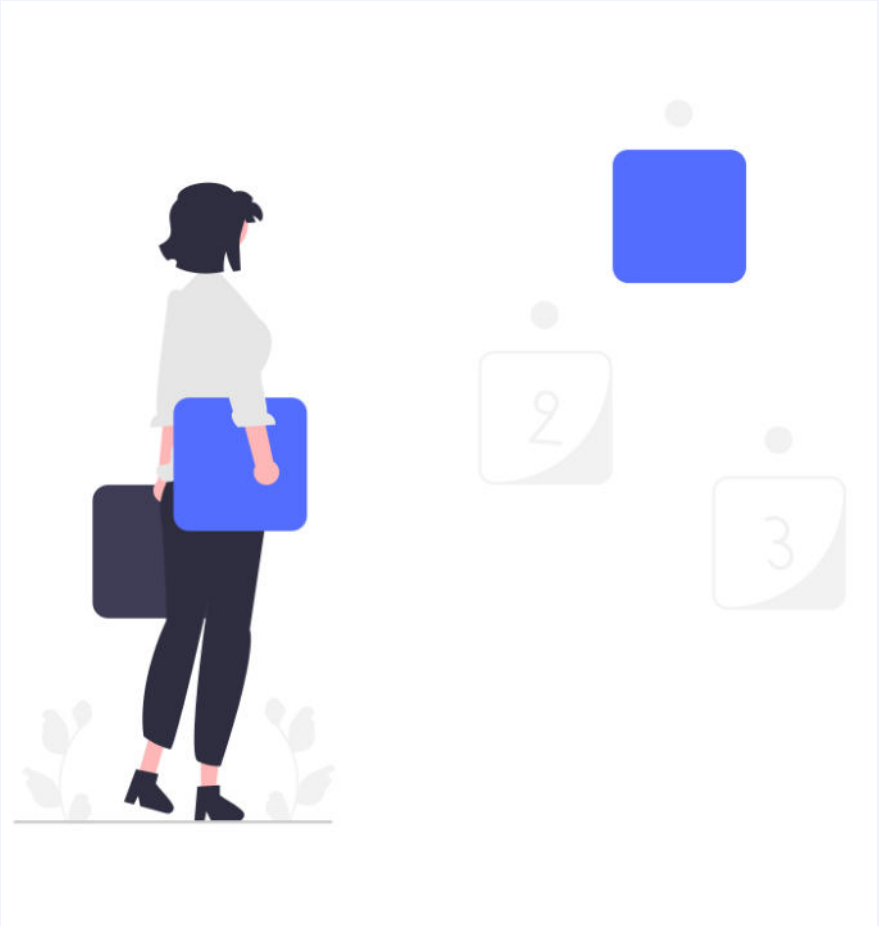
Lessons learned

- Hybrid difficult to integrate
  - not replacing one but replacing by two algorithms
- Lot of focus on TLS
  - AdES/ non-internet proctocols
  - eIDAS very little attention
- Patching your libraries not enough
  - Ecosystem needs to change
  - Plan carefully ahead



Possible future steps

- PoC improve robustness
  - Integrate with other PDF readers
- Extend to other AdES services
- Open sourcing DSS-fork



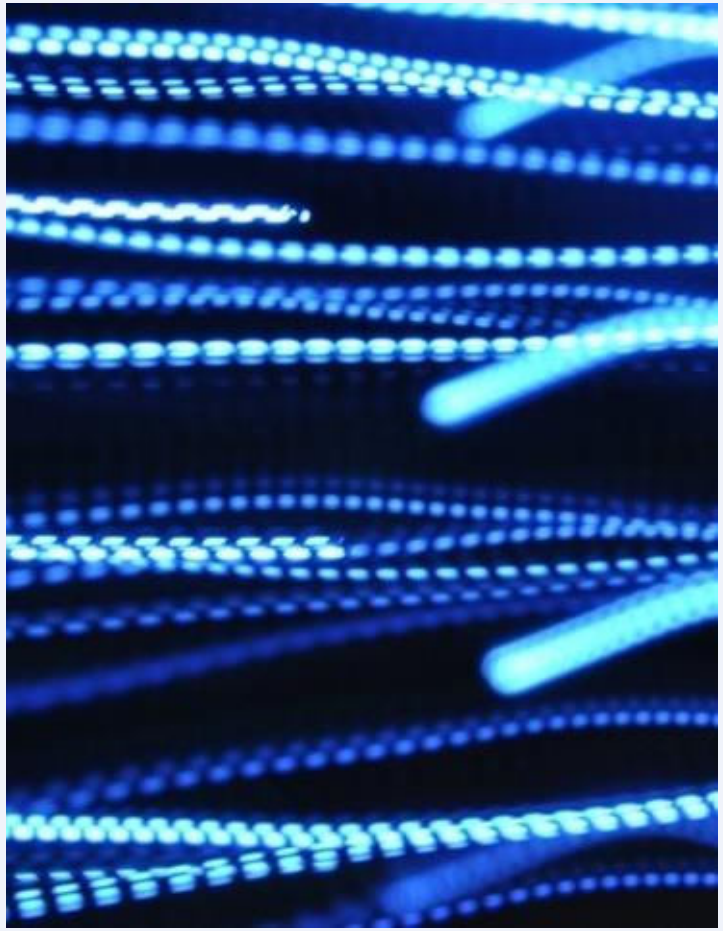
PKIC

HAPKIDO

- HAPKIDO: for quantum-safe Public Key Infrastructures (tno.nl)

- More information can be found on:
  - hapkido.tno.nl
  - Work package 4

- If you have any questions reach out to me at:
  - stefan.vandenberg@tno.nl



Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia