Towards Cryptographic Agility in the Public Sector

Kristof Verslype
Cryptographer, Smals Research

13 January 2025

Smals
ICT for society

Smals
ICT for society

SUPPORT FOR E-GOVERNMENT

Knowhow

Development

g-cloud

Staffing

Infrastructure

top EMPLOYER BELGIË BELGIQUE
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

Smals
ICT for society
www.smals.be

Crypto migrations

Past

- DES → 3DES → AES
- MD-5 & SHA1 → SHA2 & SHA3
- RSA-1024 → RSA-2048 →
- …

Future

- RSA & ECC → Hybrid mode
- Hybrid mode → PQC
- ???

SLOW AND CUMBERSOME PROCESS - TAKES 5 TO 15 YEARS TO MIGRATE

Cryptographic mechanisms have a life cycle
Recommended → Secure → Phase out → Insecure
We should accept this an act on it

Smals ICT for society

Crypto Agility

Bundesamt für Sicherheit in der Informationstechnik

Cryptographic agility

Particular attention should be paid to ***making cryptographic mechanisms as flexible as possible in order to be able to react to developments, implement upcoming recommendations and standards****, and possibly replace algorithms in the future that no longer guarantee the desired level of security ("cryptographic agility"). This is* ***particularly important due to the threat posed by quantum computers, though not exclusively****: classical attacks can also evolve and make encryption schemes or key lengths once considered secure obsolete.*

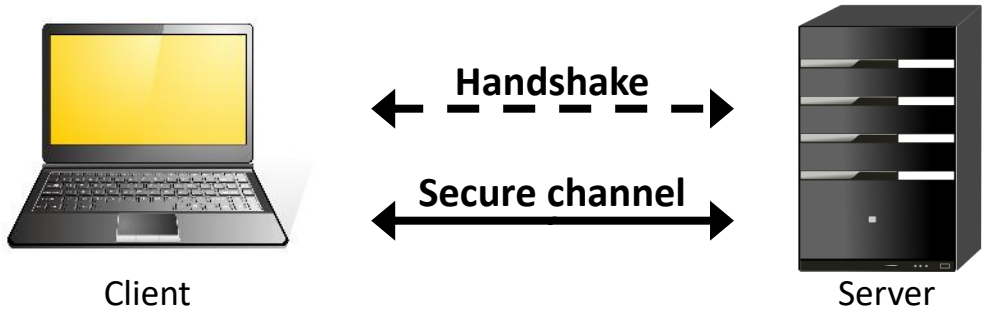
Quantum-safe cryptography –fundamentals, current developments and recommendations. October 2022

Smals ICT for society

[1] Marchesi, L., Marchesi, M., & Tonelli, R. (2025). A survey on Cryptoagility and Agile Practices in the light of quantum resistance. Information and Software Technology, 178, 107604.

Transport Layer Security (TLS)

Example of cryptographic protocol agility (see RFC7696)



Handshake

- Agree on TLS version (1.2 or 1.3)
- Agree on cipher suite
- Authenticate
- Generate shared session keys

Supported cipher suites

TLS_SM4_GCM_SM3
TLS_AES_128_CCM_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_AES_128_CCM_8_SHA256
TLS_CHACHA20_POLY1205_SHA256

Supported cipher suites

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1205_SHA256
TLS_AES_128_CCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_SM4_GCM_SM3

Recommended
Secure
Phase out
Insecure
Desactivated

TLS service offers **abstract interface** to application / service

Config file defines allowed cipher suites and their priority

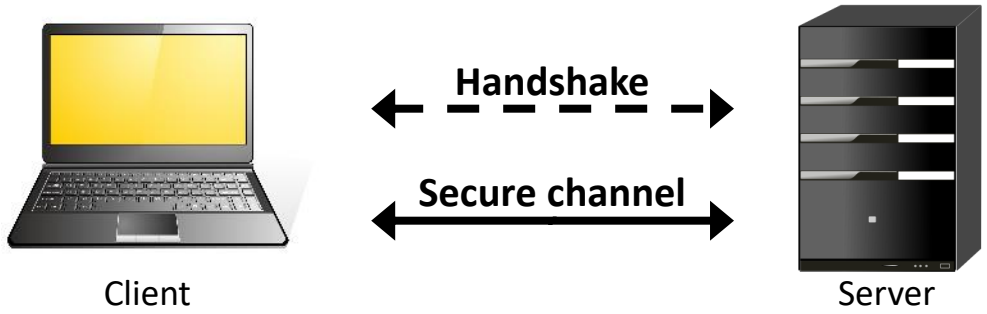
Future releases of TLS will contain **quantum resistant** cipher suites

cryptographic protocol agility is part of crypto agility

Smals ICT for society

Transport Layer Security (TLS)

Example of cryptographic protocol agility (see rfc7696)



Handshake

- Agree on TLS version (1.2 or 1.3)
- Agree on cipher suite
- Authenticate
- Generate shared session keys

Supported cipher suites

TLS_SM4_GCM_SM3
TLS_AES_128_CCM_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_AES_128_CCM_8_SHA256
TLS_CHACHA20_POLY1205_SHA256

Supported cipher suites

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1205_SHA256
TLS_AES_128_CCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_SM4_GCM_SM3

Recommended
Secure
Phase out
Insecure
Desactivated

Technology

- TLS service with config file
- On thousands of machines

Processes

- To bring policy into practice
- Ambition: Higher automation

Policy

- Cryptographic recommendations
  Recommended → secure → phase out → insecure
- Processes needed!

Crypto Agility – A technical definition

Properties

Interacting systems **negotiate** about cryptographic functions	Possibility to **add** cryptographic functions	Possibility to **retire** obsolete cryptographic functions	**At runtime** - No impact on system availability

Cryptographic functions: Hardware, software, firmware, algorithms, parameters.

Design

Anti-pattern
Hard-coding the cryptography in system

Crypto agility pattern
System uses cryptography by calling abstract interface

Local service | **Central service**

Centralization
- Central crypto policy
- Central crypto services

Preparation

One change →
Big Consequences

Inventory - What cryptography used where

Test to learn impact on performance, compatibility

Temporal **exceptions** to deal with incompatibility

[1] Marchesi, L., Marchesi, M., & Tonelli, R. (2025). A survey on Cryptoagility and Agile Practices in the light of quantum resistance. Information and Software Technology, 178, 107604.

Crypto Agility – A more holistic definition

	Technology	Processes	Policy
Inventory	Tools, infrastructure & integration	Processes to populate and keep up-to-date	Make mandatory
Crypto agility	- Application design - Products & services	- Include in public tenders - Adopt design principle	Make mandatory
Migration	Supported cryptography	Change management – define procedure and attribute roles & responsibilities.	- Crypto recommendations - Define roles / responsibilities

Smals is working on these three domains

Smals ICT for society

Cryptography Bill of Materials (CBOM)

Proposed as standard by IBM to express cryptographic assets


```
{
    "name": "RSA-2048",
    "type": "cryptographic-asset",
    "bom-ref": "e2c92908-3559-4f86-8212-2e134dfce30a",
    "evidence": {
        "occurrences": [
            {
                "line": 110,
                "offset": 28,
                "location": "core/src/main/java/org/keycloak/jose/jwk/AbstractJ
                "additionalContext": "java.security.KeyFactory#getInstance(Ljav
            },
            {
                "line": 103,
                "offset": 39,
                "location": "saml-core-api/src/main/java/org/keycloak/dom/xmlse
                "additionalContext": "java.security.KeyFactory#getInstance(Ljav
            },
            {
                "line": 122,
                "offset": 39,
                "location": "saml-core-api/src/main/java/org/keycloak/dom/xmlsec/w3/xmldsig/RSAKeyValueType.java",
                "additionalContext": "java.security.KeyFactory#getInstance(Ljava/lang/String;)Ljava/security/KeyFactory;"
            }
        ]
    }
}
```


In case of vulnerability

- Where is the organization vulnerable
- Where intervene with high priority

Quantum and other threats

Inventory in a perfect world

- Central repository
- Machine-readable → CBOM
- Automatically updated
- Includes external dependencies

Asset management is complicated

https://github.com/IBM/cbomkit/blob/main/example/keycloak-cbom.json

Crypto Agility – A technical definition

Properties

Interacting systems **negotiate** about cryptographic functions

Possibility to **add** cryptographic functions

Possibility to **retire** obsolete cryptographic functions

At runtime - No impact on system availability

Cryptographic functions: Hardware, software, firmware, algorithms, parameters.

Design

Anti-pattern
Hard-coding the cryptography in system

Crypto agility pattern
System uses cryptography by calling abstract interface

Local library | **Central service**

Centralization
- Central crypto policy
- Central crypto services

Preparation

One change →
Big Consequences

Inventory - What cryptography used where

Test to learn impact on performance, compatibility

Temporal **exceptions** to deal with incompatibility

[1] Marchesi, L., Marchesi, M., & Tonelli, R. (2025). A survey on Cryptoagility and Agile Practices in the light of quantum resistance. Information and Software Technology, 178, 107604.

Sepia - Service for digital signatures

Service being developed by Smals

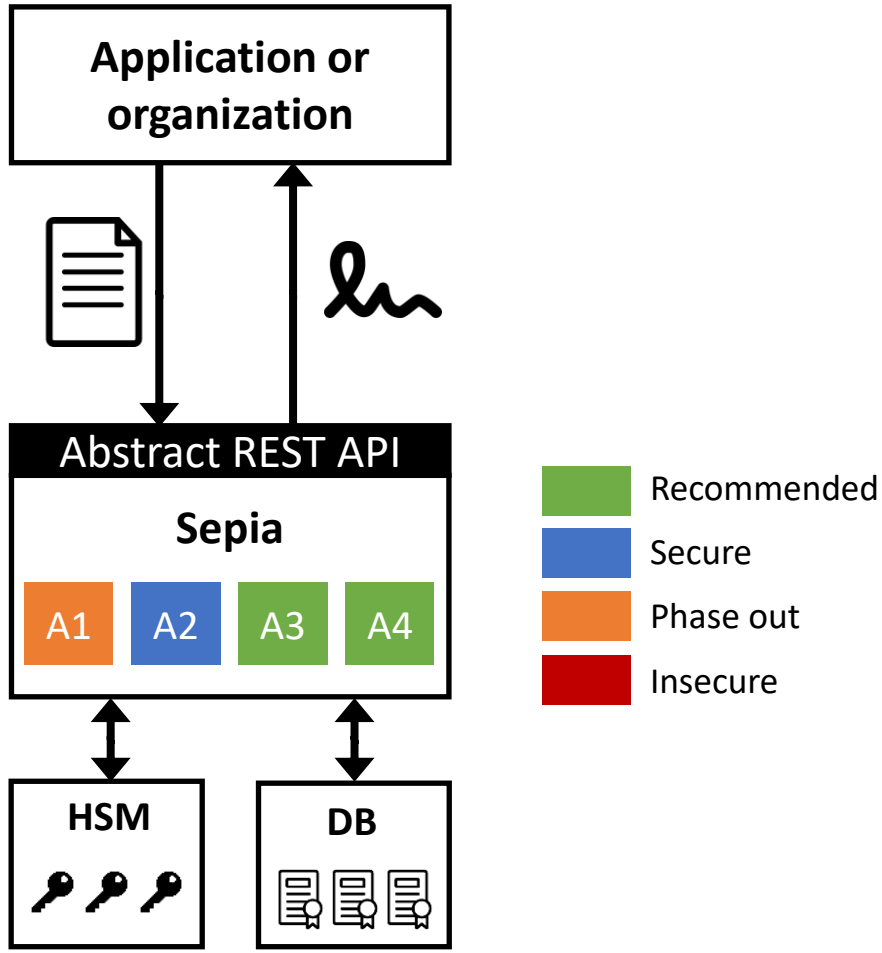
Functionality

- Creates digital signatures on behalf of public sector organisations and services
- Automated or with human intervention
- Storage of signed documents with signature
- Secure storage of certificates and secret keys

Motivation

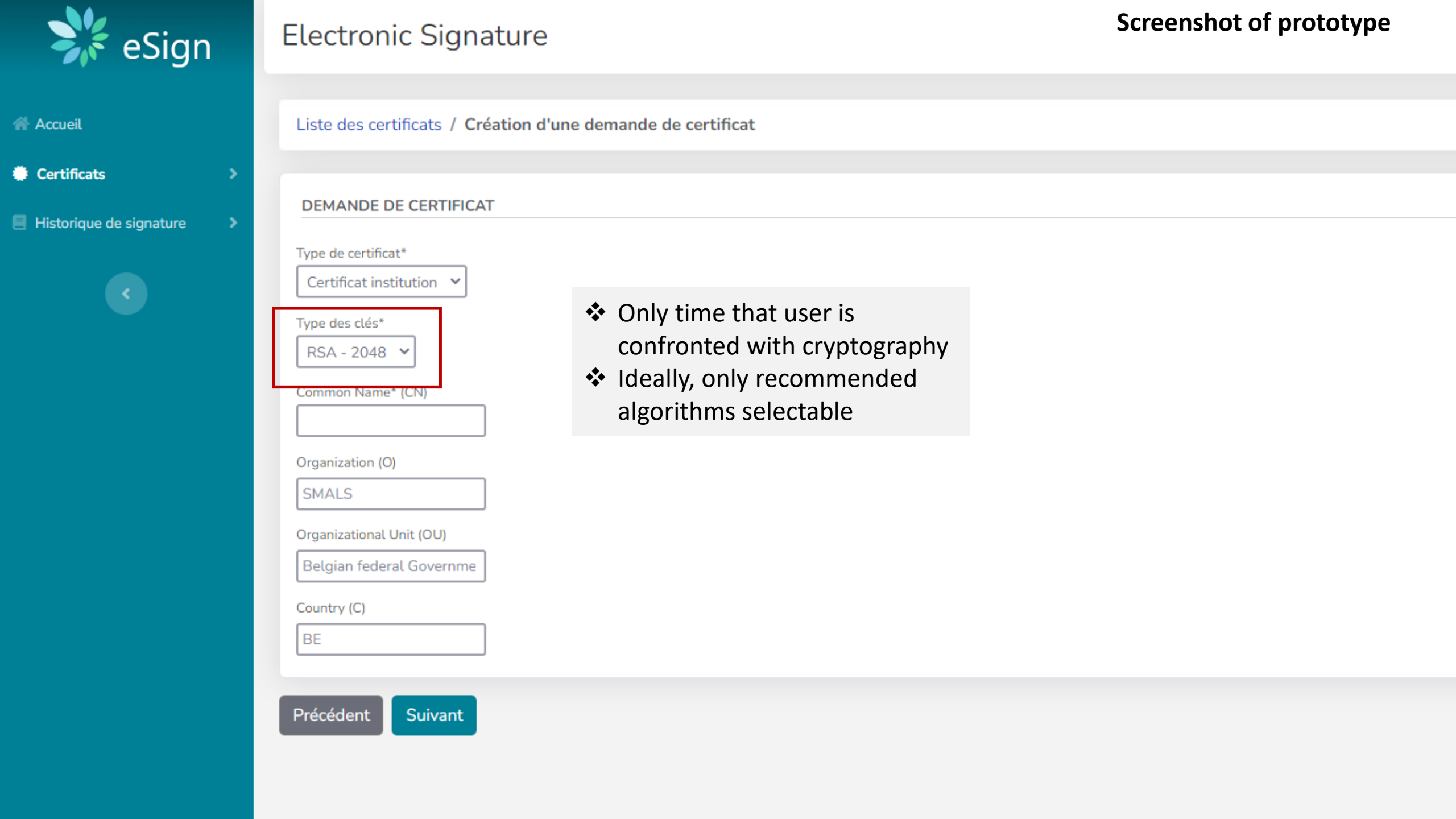
- **Cost reduction by reuse**
  See reuse catalog [1]
- **Increase security**
- **Crypto agility!**

Lesson: Crypto agility and cost efficiency can coexist



[1] https://www.ict-reuse.be/nl/service/sepiadocumentsigner

Screenshot of prototype



- Only time that user is confronted with cryptography
- Ideally, only recommended algorithms selectable

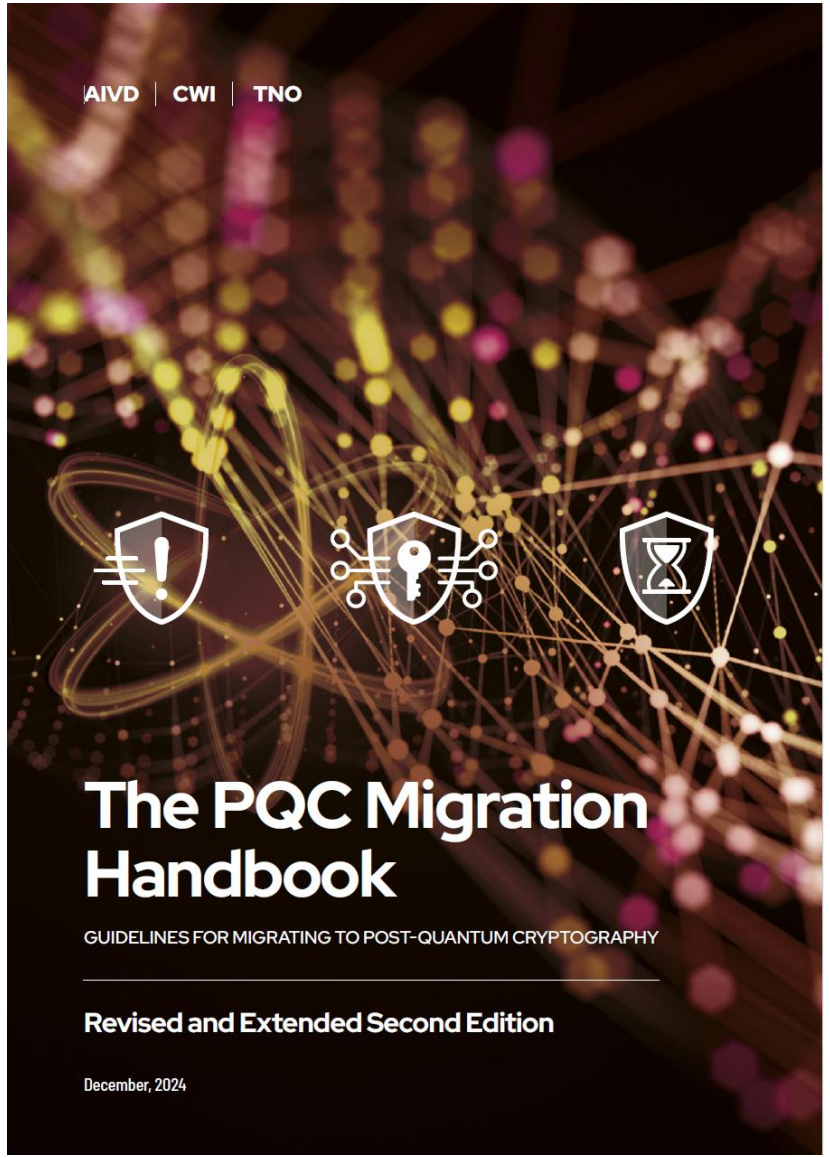
Conclusions

What?

- Crypto mechanisms have a life cycle
- Crypto agility introduces flexibility in your organization to better deal with this
- Systems call abstract interface for crypto
- Technology – Processes – Policy
- Crypto inventory essential

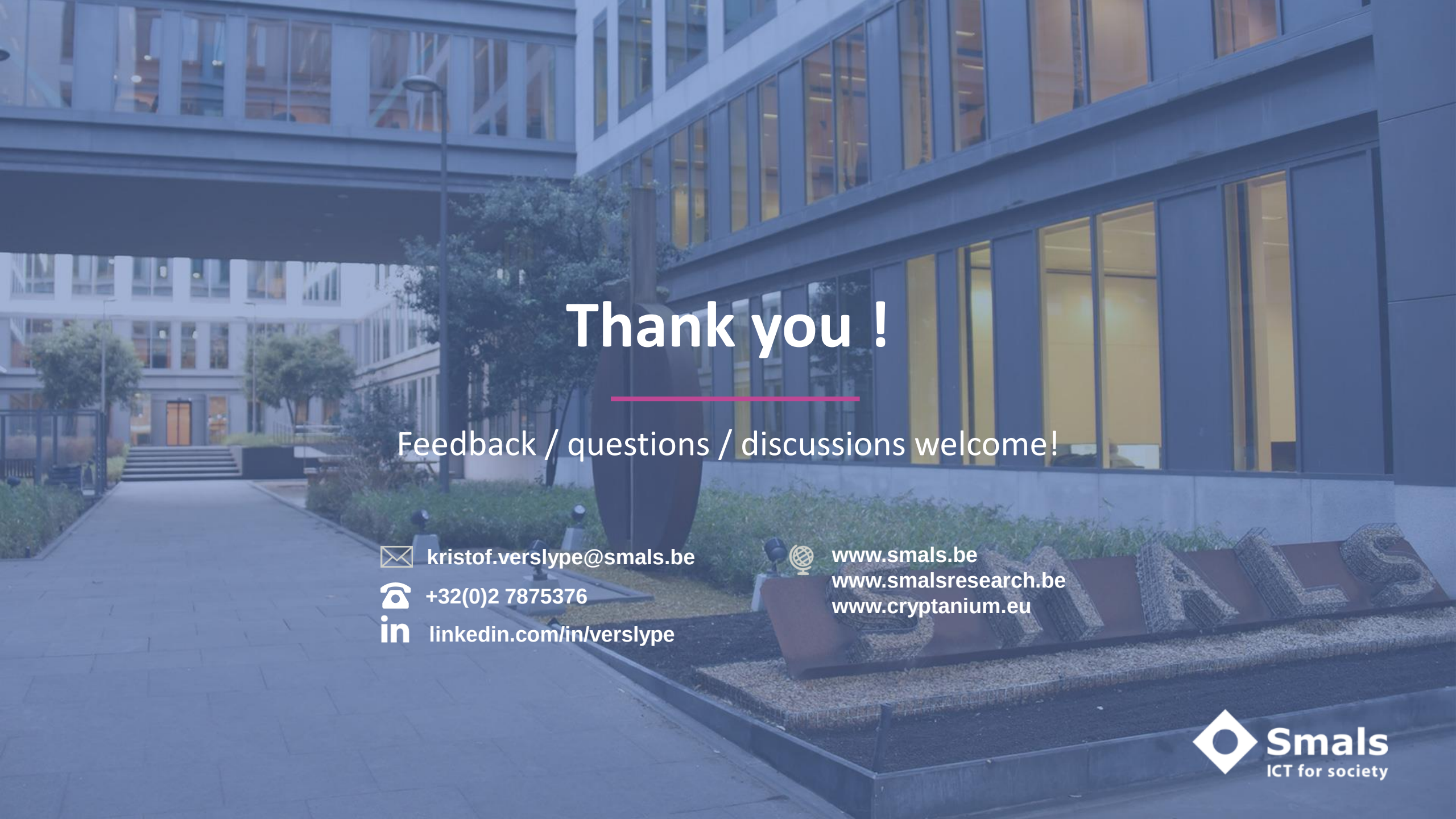
Why?

- Smoothens migration process. Not only for quantum threat
- Improves management of cryptography in the organization: Detection and resolution of vulnerabilities
- Can result in cost efficiencies



https://english.aivd.nl/publications/publications/2024/12/3/the-pqc-migration-handbook

Smals ICT for society



Thank you !

Feedback / questions / discussions welcome!

kristof.verslype@smals.be

+32(0)2 7875376

linkedin.com/in/verslype

www.smals.be
www.smalsresearch.be
www.cryptanium.eu

Smals
ICT for society