Towards Cryptographic Agility in the Public Sector

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

Crypto migrations

Past

-
-
-
-

Future

-
-
-

We should accept this an act on it

Crypto Agility

Bundesamt
für Sicherheit in der
Informationstechnik

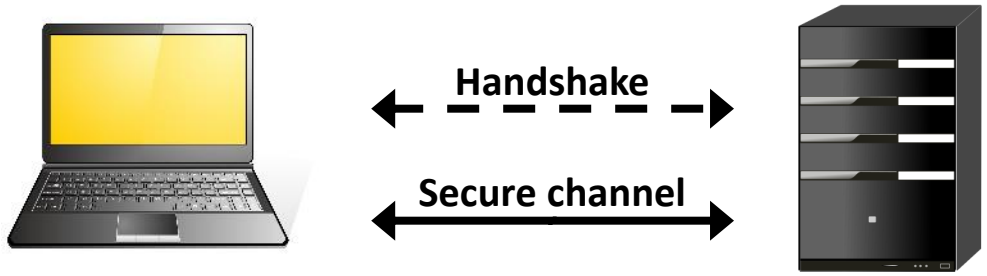
Cryptographic agility

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.



Handshake

-
-
-
-

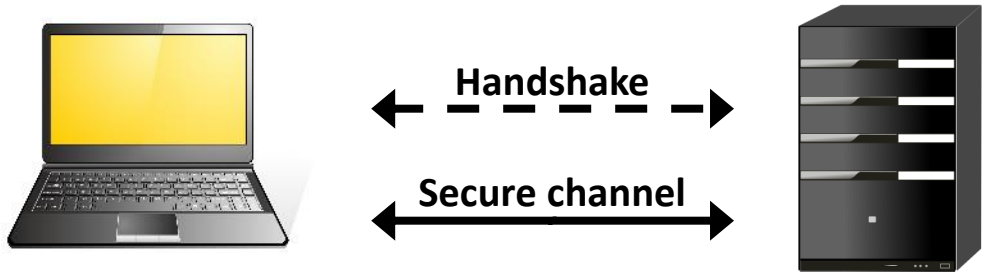
Supported cipher suites

TLS_AES_128_GCM_SHA256

Supported cipher suites

TLS_AES_128_GCM_SHA256

abstract interface	**Config file**	**quantum resistant**	



Handshake

-
-
-
-

Supported cipher suites

TLS_AES_128_GCM_SHA256

Supported cipher suites

TLS_AES_128_GCM_SHA256

Technology

- ❖
- ❖

Processes

- ❖
- ❖

Policy

- ❖
- ❖

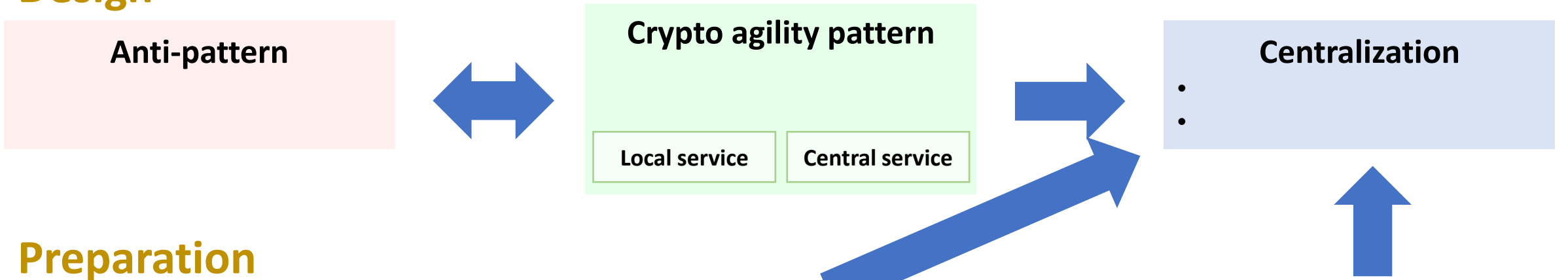
Crypto Agility – A technical definition

Properties

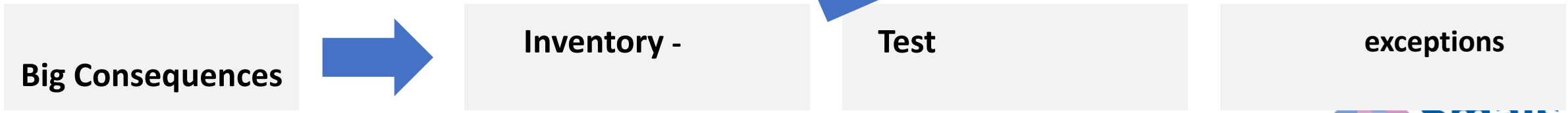
negotiate	add	retire	At runtime

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

Design



Preparation



[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			
Crypto agility			
Migration			

Smals is working on these three domains

Smals
ICT for society

Cryptography Bill of Materials (CBOM)


```
{
    "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

-
-

Quantum and other threats

Inventory in a perfect world

-
-
-
-

Asset management is complicated

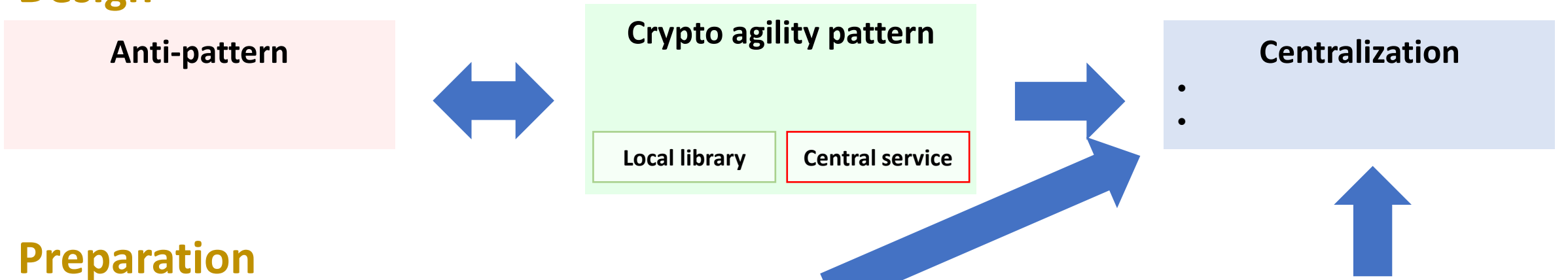
Crypto Agility – A technical definition

Properties

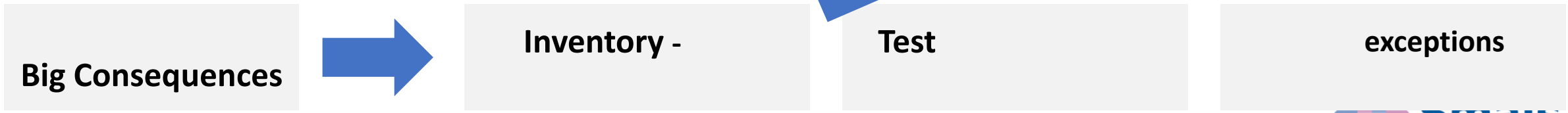
negotiate	add	retire	At runtime

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

Design



Preparation



[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.

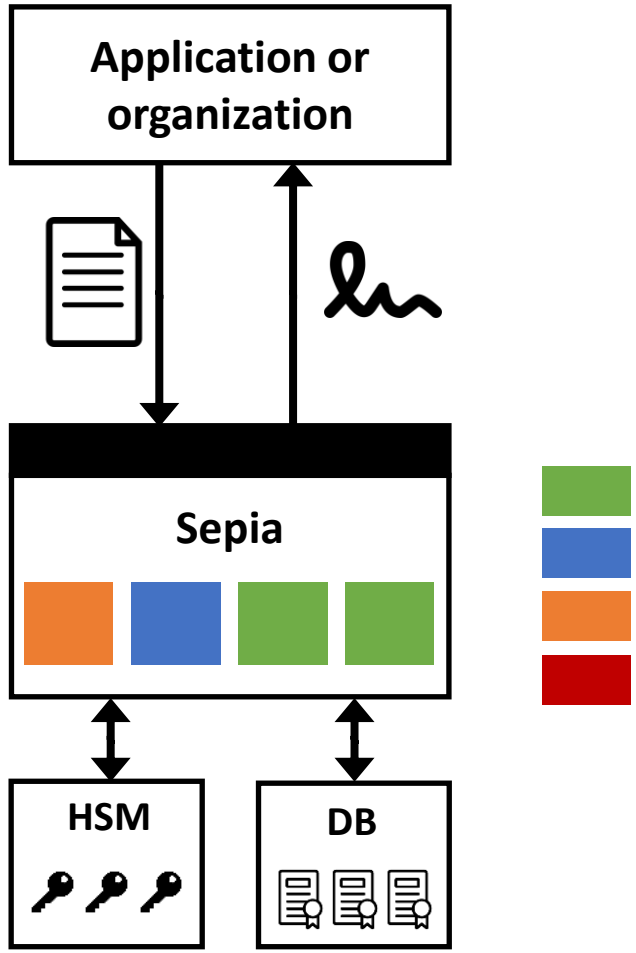
Service being developed by Smals

Functionality

-
-
-
-

Motivation

- Cost reduction by reuse
- Increase security
- Crypto agility!



Smals
ICT for society

Screenshot of prototype

eSign

Electronic Signature

- Accueil
- Certificats
- Historique de signature

Liste des certificats / **Création d'une demande de certificat**

DEMANDE DE CERTIFICAT

Type de certificat*

Certificat institution

Type des clés*

RSA - 2048

Common Name* (CN)

Organization (O)

SMALS

Organizational Unit (OU)

Belgian federal Governme

Country (C)

BE

Précédent | Suivant

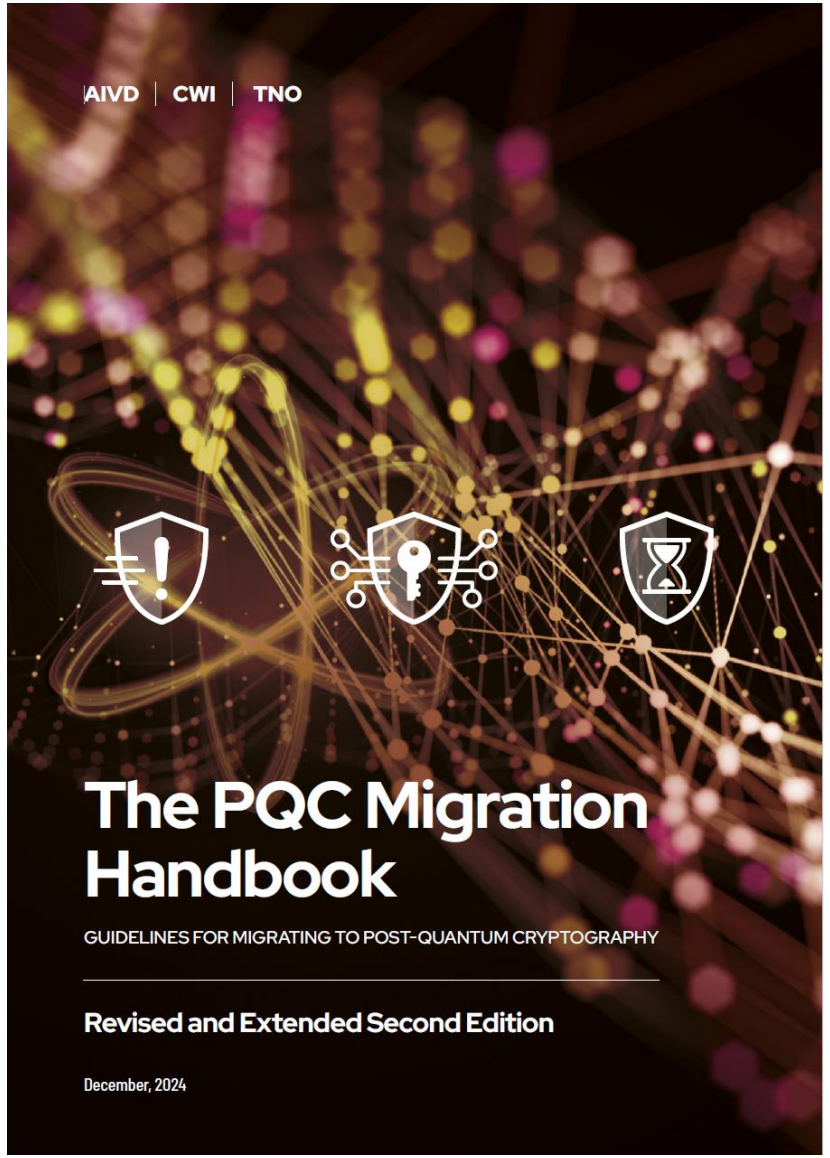
Conclusions

What?

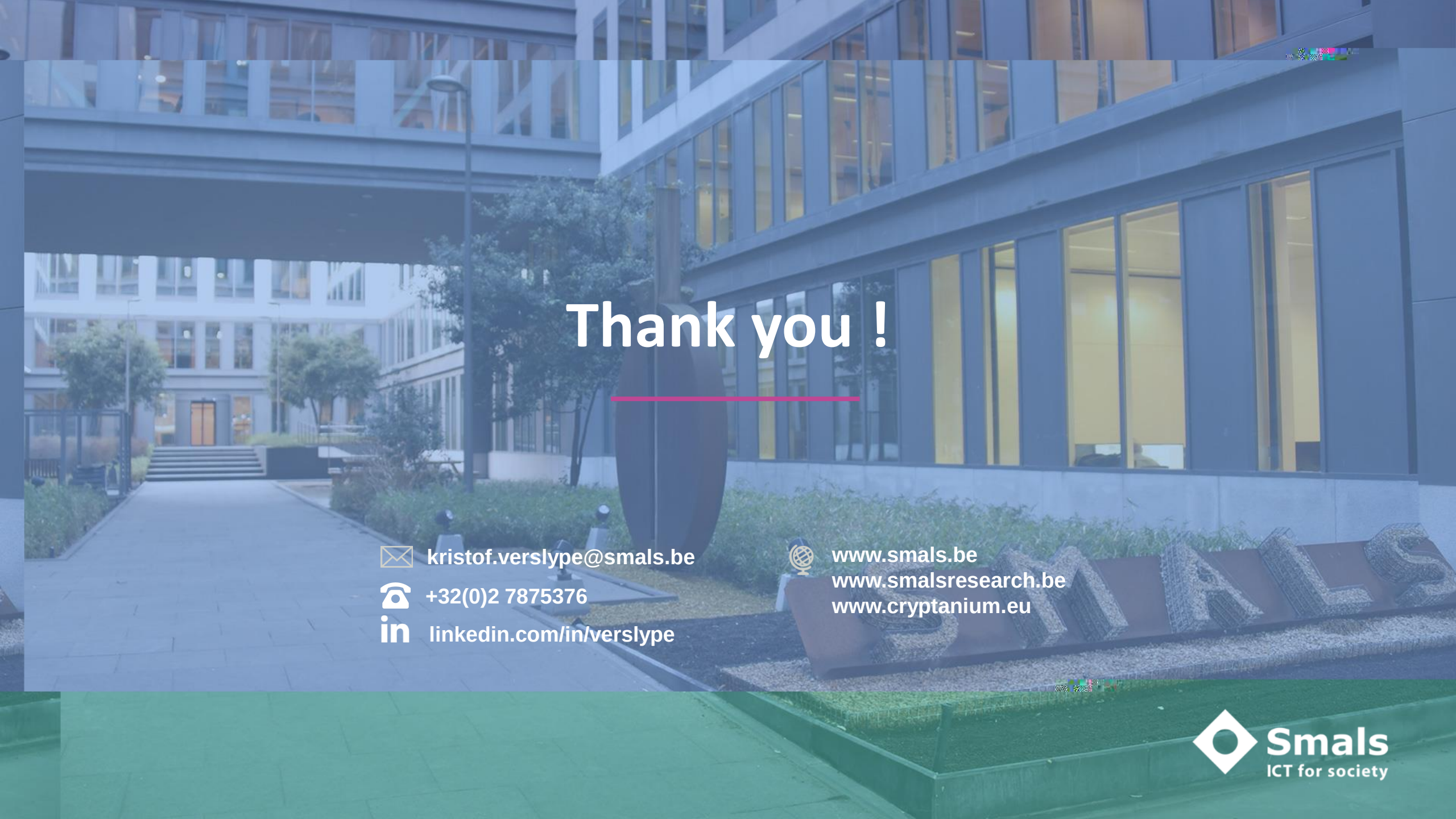
-
-
-
-
-

Why?

-
-
-



Smals
ICT for society



Thank you !

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