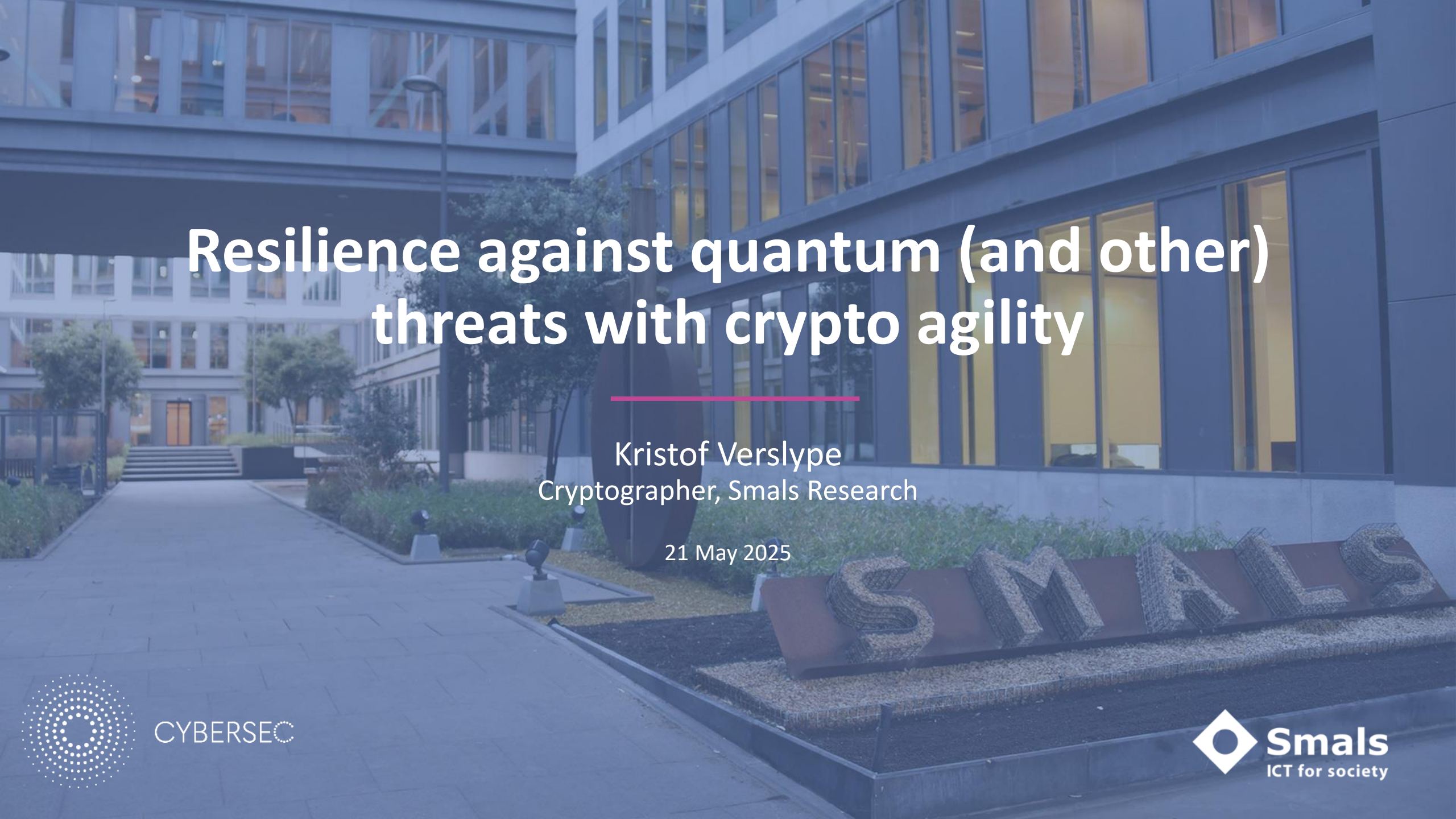


Resilience against quantum (and other) threats with crypto agility

Kristof Verslype
Cryptographer, Smals Research

21 May 2025

CYBERSEC

Smals
ICT for society

Cryptography is Everywhere

Devices

- IoT
- Smartcard (eId, bank)
- Smartphone
- Servers
- House
- Car
- Plane
- Satellite
- …

Interactions

- Financial transactions
- Secure communication
- Document signing
- Authentication
- …

Domain

- Defense / military
- Public sector
- Private sector
- Individuals
- …

WITHOUT SECURE CRYPTOGRAPHY, OUR SOCIETY COLLAPSES

Cryptography Under Threat

Cryptographically relevant quantum computers

Would be able to break modern (public-key) cryptography

"To ensure an acceptable level of readiness, we recommend that [the most sensitive use cases] should be protected against 'store now, decrypt later' attacks as soon as possible, latest by the end of 2030."

Joint statement from partners from 18 EU member states (11/2024)

Other threats

- Increasing computing power
- Cryptanalysis
- Side-channel attacks in implementations

Applies on modern and post-quantum cryptography

Smals ICT for society

IEEE Spectrum FOR THE TECHNOLOGY INSIDER

NEWS | COMPUTING

“Quantum-Safe” Crypto Hacked by 10-Year-Old PC

›Many challenges still lie ahead for postquantum cryptography

BY CHARLES Q. CHOI | 19 AUG 2022 | 7 MIN READ |

Charles Q. Choi is a contributing editor for IEEE Spectrum.

SHARE THIS STORY

TAGS

QUANTUM COMPUTING

CRYPTOGRAPHY | NIST

POST-QUANTUM CRYPTOGRA…

FUTURE QUANTUM COMPUTERS may rapidly break modern cryptography. Now researchers find that a promising algorithm designed to protect computers from these advanced attacks could get broken in just 4 minutes. And the catch is that 4-minute time stamp was not achieved by a cutting-edge machine but by a regular 10-year-old desktop computer. This latest, surprising defeat highlights the many hurdles postquantum cryptography will need to clear before adoption, researchers say.

Cryptography Under Threat

Cryptographically relevant quantum computers

Would be able to break modern (public-key) cryptography

"To ensure an acceptable level of readiness, we recommend that [the most sensitive use cases] should be protected against 'store now, decrypt later' attacks as soon as possible, latest by the end of 2030."

Joint statement from partners from 18 EU member states (11/2024)

Other threats

- Increasing computing power
- Cryptanalysis
- Side-channel attacks in implementations

Applies on modern and post-quantum cryptography

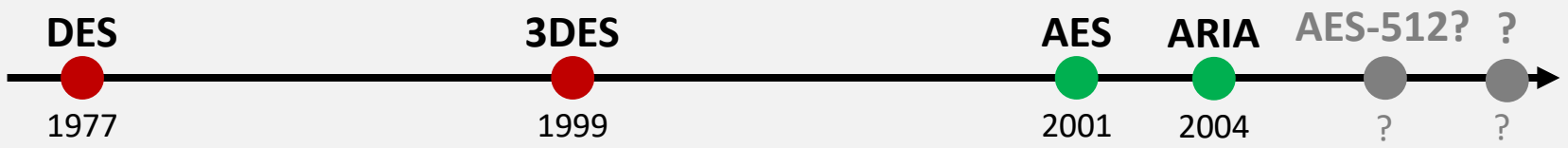
→ **MIGRATE ON TIME TO RECOMMENDED CRYPTOGRAPHY**

Smals ICT for society

Cryptographic migrations

- Insecure
- Phase-out
- Secure / Recommended
- Planned

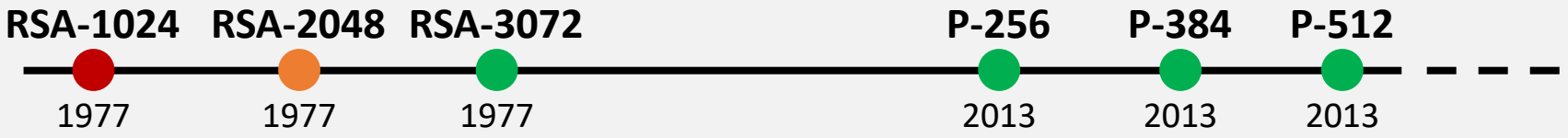
Symmetric encryption



Secure hash function

Public key cryptography

(E.g., digital signatures, key agreement, authentication)



Multiple crypto migrations in the past

Slow, cumbersome and expensive process - Takes 5 to 15 years to migrate

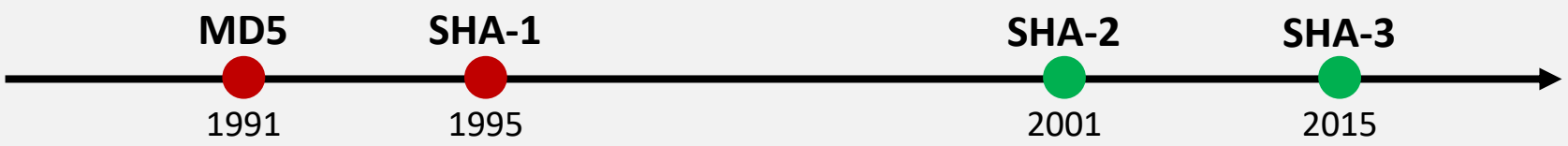
Smals ICT for society

Cryptographic migrations

- Insecure
- Phase-out
- Secure / Recommended
- Planned

Symmetric encryption

Secure hash function



Public key cryptography

(E.g., digital signatures, key agreement, authentication)

Potentially multiple crypto migrations in the not-so-distant future!

Becoming quantum-ready may not be a one-time shot

Smals ICT for society

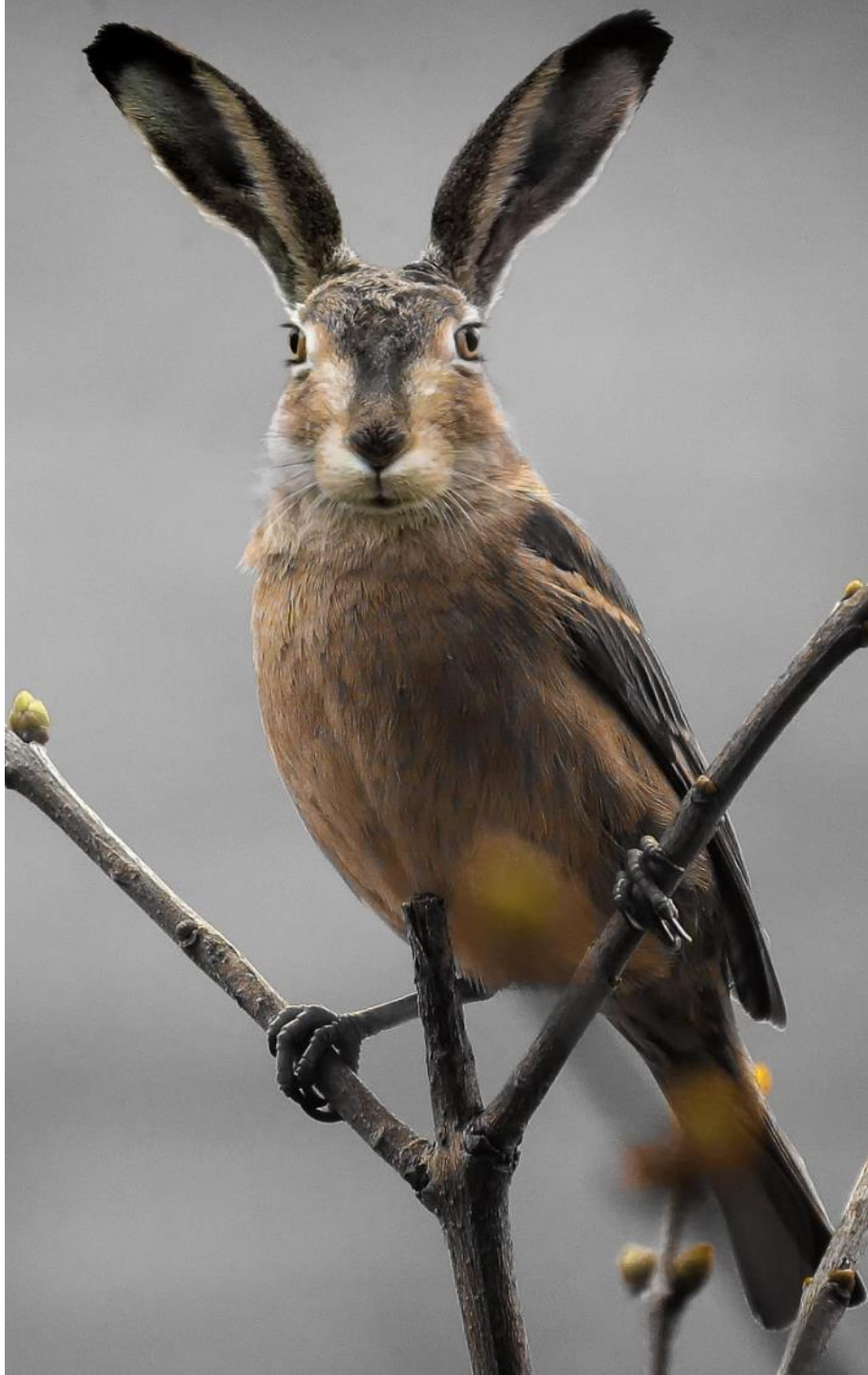
Transitional period in Hybrid Mode

Bundesamt
für Sicherheit in der
Informationstechnik

The quantum-safe algorithms that are currently being standardized are not yet as well researched as the "classical" methods *(for example RSA and ECC). This applies in particular to weaknesses that largely only become apparent in applications, such as typical implementation errors, possible side-channel attacks, etc.* ***BSI therefore recommends that post-quantum cryptography should not be used in isolation if possible, but only in hybrid mode, i.e. in combination with classical algorithms****. […] Hash-based signatures can in principle also be used on its own (i.e., not in hybrid mode).*

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

→ **EVEN MORE MIGRATIONS!**



Crypto migrations

Challenge

- Multiple in the past & multiple in the future
- Slow and cumbersome process - Takes 5 to 15 years to migrate

→ **How to facilitate smooth migrations?**

Approach

Cryptographic algorithms have a life cycle
Recommended → Secure → Phase out → Insecure

Cryptographic mechanisms are assets that need to be managed

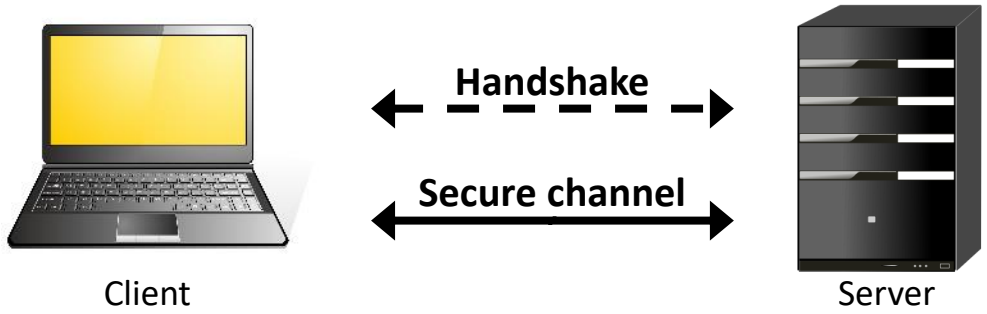
We should accept this and act on it!

Improve cryptographic maturity

Insight	Guidance	Flexibility
Crypto inventory	**Crypto policy**	**Crypto agility**
Where what crypto for which purpose?	What cryptography should (not) be used?	Migrate easily from/to crypto mechanisms

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
Deactivated

Cryptographic service offers **abstract API** to application / service

Cryptographic functions **selected in real-time**

Add and **remove** Cryptographic functions

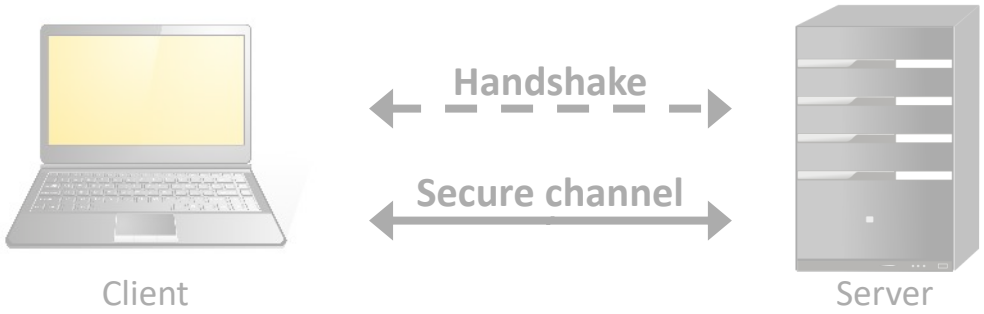
Cryptographic functions: *Hardware, software, firmware, algorithms, parameters, …*

Smals ICT for society

National Academies of Sciences, Engineering, and Medicine (2016) Cryptographic Agility and Interoperability: Proceedings of a Workshop. Forum on Cyber Resilience Workshop Series. (The National Academies Press, Washington, DC). https://doi.org/10.17226/24636

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

Supported cipher suites

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1205_SHA256

Recommended
Secure
Phase out

Cryptographic Agility

On the level of an IT system

Cryptographic service offers **abstract API** to application / service

Cryptographic functions **selected in real-time**

Add and **remove** Cryptographic functions

At runtime – No impact on system availability

Cryptographic functions: *Hardware, software, firmware, algorithms, parameters, …*

National Academies of Sciences, Engineering, and Medicine (2016) Cryptographic Agility and Interoperability: Proceedings of a Workshop. Forum on Cyber Resilience Workshop Series. (The National Academies Press, Washington, DC). https://doi.org/10.17226/24636

Sepia - Service for digital signatures

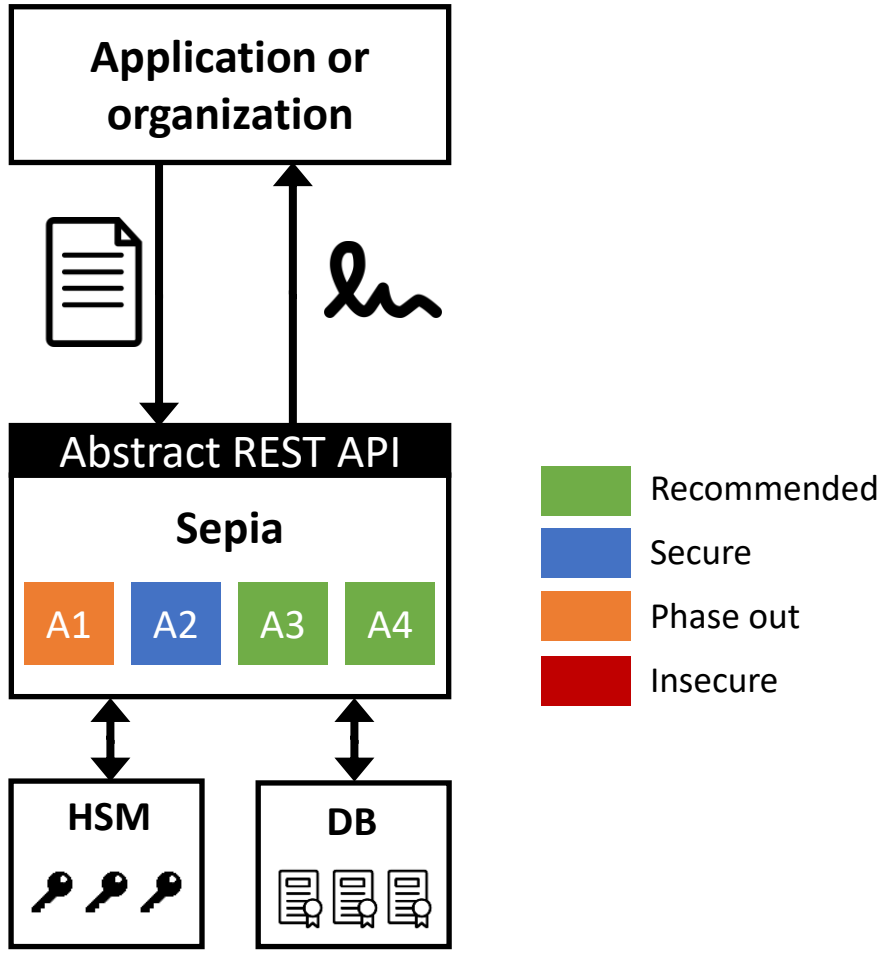
Service developed by Smals

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!**

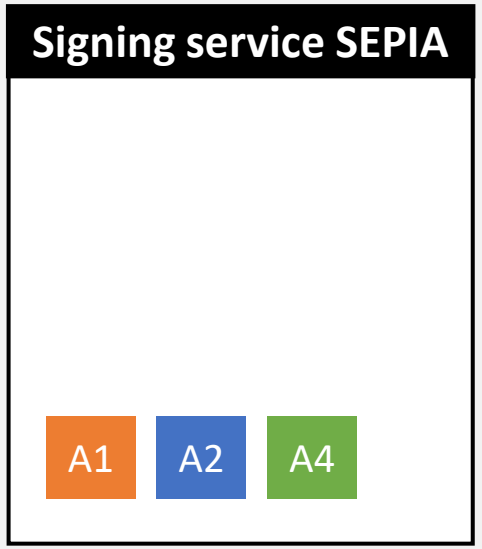


CRYPTO AGILITY AND COST EFFICIENCY CAN COEXIST

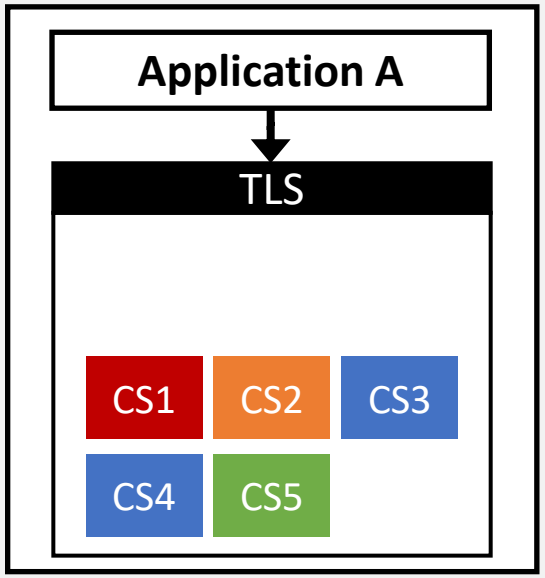
[1] https://www.ict-reuse.be/nl/service/sepiadocumentsigner

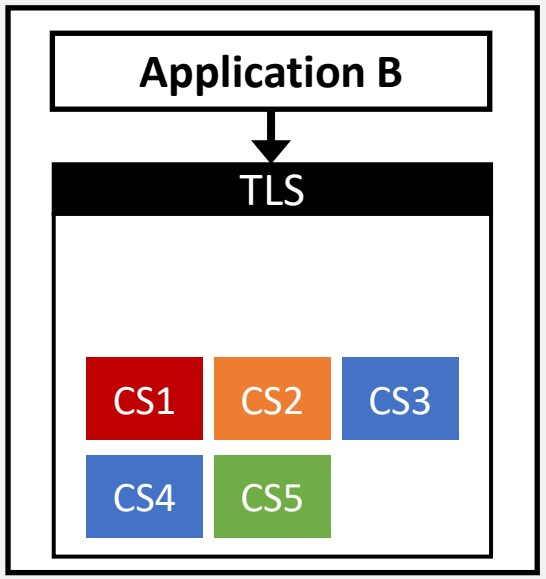
Possible Future Architecture

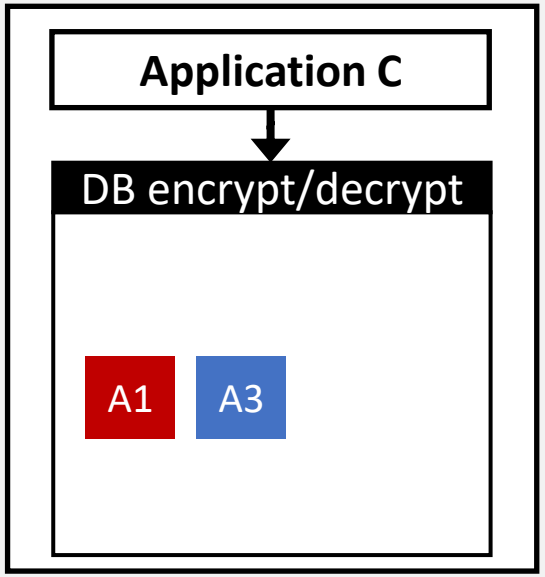
CENTRAL



LOCAL







Possible Future Architecture

CENTRAL

Implementation service

Cipher suites

CS1 CS2 CS3
CS4 CS5 CS6

Algorithms

A1 A2 A3 A4 A5

Policy service

Policy

Policy + Dev. SEPIA = Policy SEPIA

Deviations

Dev. app A
Dev. app B
Dev. SEPIA

Signing service SEPIA

A1 A2 A4

Certificate mgt.

Policy

A1 A2 A3 A4

Crypto inventory

LOCAL

Application A

TLS

Policy app A

CS1 CS2 CS3
CS4 CS5

Application B

TLS

Policy app B

CS1 CS2 CS3
CS4 CS5

Application C

DB encrypt/decrypt

Policy app C

A1 A3

"A1 only to decrypt"

Possible Future Architecture

CENTRAL

Implementation service

Cipher suites

CS1 CS2 CS3 CS4 CS5 CS6

Algorithms

A1 A2 A3 A4 A5

Policy service

Policy

Policy + Dev. SEPIA =

Deviations

Dev. app A Dev. app B Dev. SEPIA

Signing service SEPIA

Policy SEPIA

A2 A4

Certificate mgt.

Policy

A1 A2 A3 A4

Crypto inventory

CRYPTOGRAPHIC AGILITY

IMPLIES

CENTRALIZATION AND AUTOMATED PROCESSES

LOCAL

Application A

TLS

Policy app A

CS1 CS2 CS3 CS4 CS5 CS6

Application B

TLS

Policy app B

CS1 CS2 CS3 CS4 CS5 CS6

Application C

DB encrypt/decrypt

Policy app C

A1 A3 A5

"A1 only to decrypt"

Crypto-Agility Maturity Model (CAMM)

Proposal – not yet standardized or adopted – for IT-systems

Initial / Not possible

At least one subsystem or component violates L1 requirements

0

Possible

Systems can be adapted to respond dynamically to future crypto challenges

1

Knowledge

- System knowledge
- Cryptography inventory

Process

- Updateability
- Reversibility

System property

- Extensibility

Prepared

Actual crypto migration still requires some preparatory work

2

Knowledge

- Algorithm IDs

System property

- Cryptographic modularity (API)
- Algorithm intersection
- Algorithm exclusion
- Opportunistic security
- Usability of crypto agility

Practiced

Crypto migration demonstrable, effectively and securely feasible

3

Knowledge

- Performance awareness
- Secure crypto agility

Process

- Policies
- Compliance testing
- Enforceability of CA
- Transition mechanism
- Effectiveness

System property

- Hardware modularity
- Backwards compatibility

Sophisticated

Enables fast crypto migration, applied on broader infrastructure

4

Process

- Automation
- Scalability
- Real-time

System property

- Context independence
- Cross-system interoperability

https://camm.h-da.io/

Smals ICT for society

Crypto-Agility Maturity Model (CAMM)

Proposal – not yet standardized or adopted – for IT-systems

Initial / Not possible

At least one subsystem or component violates L1 requirements

0

Possible

Systems can be adapted to respond dynamically to future crypto challenges

Knowledge
- System knowledge
- Cryptography inventory

Process
- Updateability
- Reversibility

System property
- Extensibility

1

Prepared

Actual crypto migration still requires some preparatory work

Knowledge
- Algorithm IDs
- Algorithm modularity (API)
- Cryptographic modularity (alg.)
- Algorithm intersection
- Algorithm exclusion
- Opportunistic security
- Usability of crypto agility

2

Practiced

Crypto migration demonstrable, effectively and securely feasible

Knowledge
- Performance awareness
- Usability of crypto agility

Process
- Policies
- Compliance testing
- Enforceability of CA
- Transition mechanism
- Effectiveness

System property
- Hardware modularity
- Backwards compatibility

3

Sophisticated

Enables fast crypto migration, applied on broader infrastructure

Process
- Automation
- Scalability
- Real-time

System property
- Context independence
- Cross-system interoperability

4

CRYPTOGRAPHIC AGILITY IS A JOURNEY

(NO OFFICIAL MAPS AVAILABLE YET)

https://camm.h-da.io/

Smals ICT for society

Challenges & open questions

Research on CA

Performance

Middleboxes

Legacy

Standards

Downgrade attacks

QR-codes

IoT

Incompatibilities

Advanced cryptography

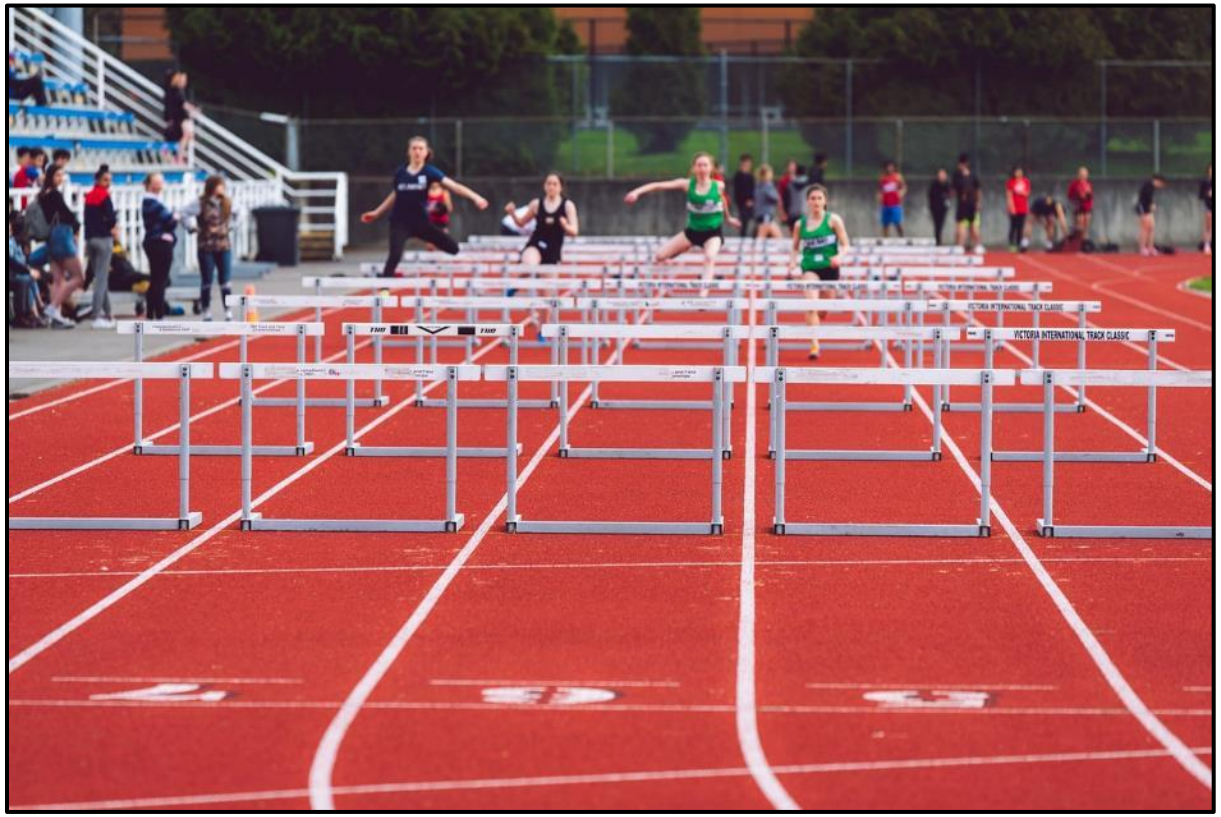
Guidance

X.509 certificates

Smartcards

HSMs

Cryptographic accelerators



BECOMING QUANTUM-READY IS HARD, BECOMING CRYPTO AGILE EVEN HARDER

BUT… IT PAYS OFF IN THE LONG RUN!

Smals ICT for society

Takeaways

- Crypto migration is not a one-time operation
- Crypto mechanisms have a life cycle
- Crypto migrations can be slow, cumbersome and expensive
- Crypto agility introduces flexibility in your organization to better deal with this
- **We are early**

BECOME A CHEETAH: EMBRACE CRYPTO AGILITY!

IT WILL BE YOUR CORNERSTONE IN ADAPTING TO YOUR FUTURE CRYPTOGRAPHIC NEEDS

Smals ICT for society

Thanks for your attention!

Feedback / questions / discussions welcome!
See you at our booth (05.F034, next to theatre 1)!

kristof.verslype@smals.be
+32(0)2 7875376
linkedin.com/in/verslype

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

CYBERSEC

Smals
ICT for society