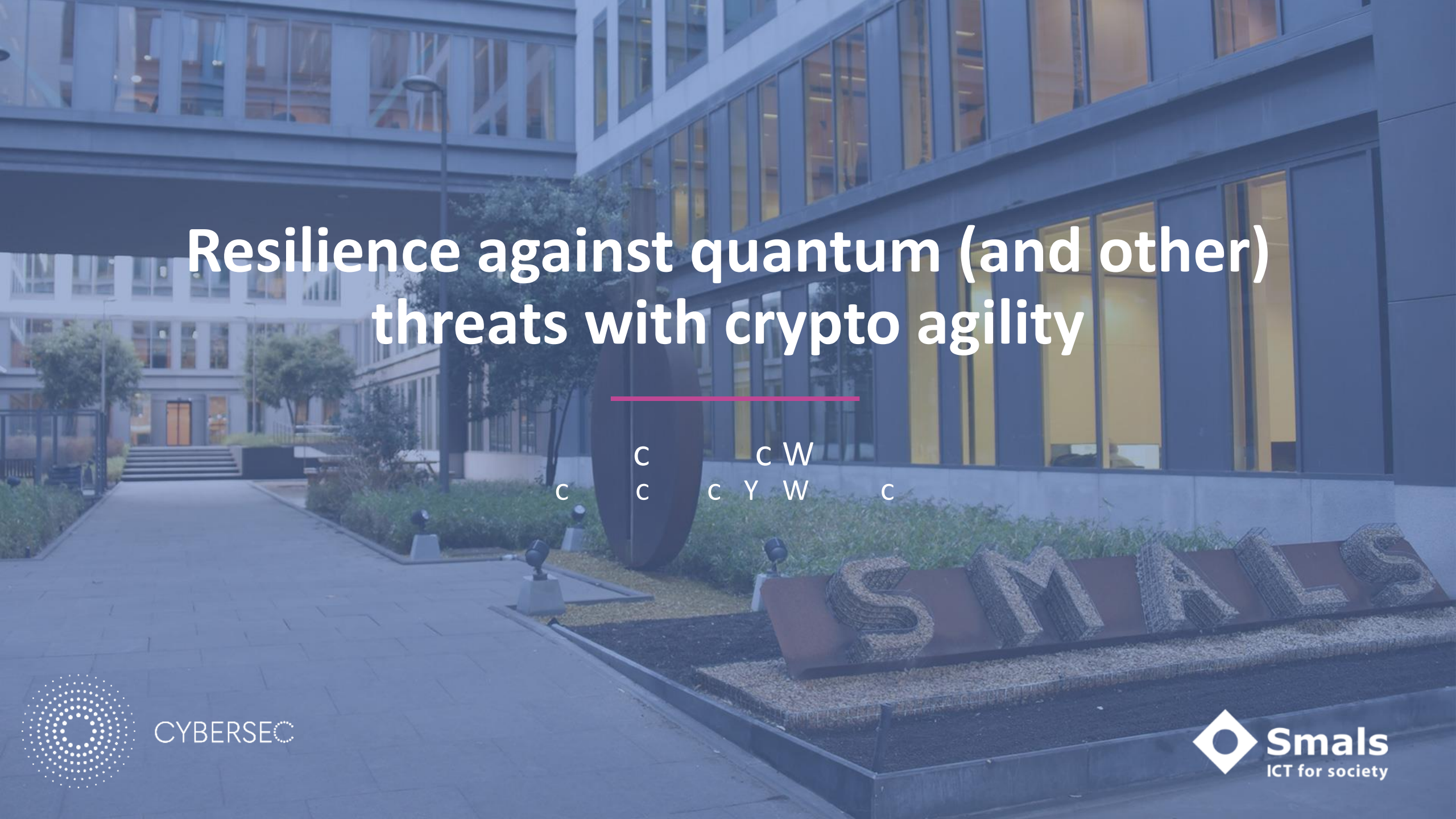
Resilience against quantum (and other) threats with crypto agility

C C W
C C C Y W C



CYBERSEC

Smals
ICT for society

Cryptography is Everywhere

Devices

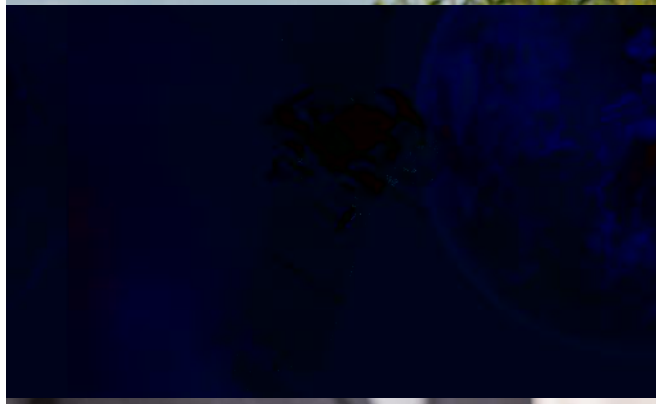
-
- Y c c
- Y c
- c c
-
- c
- W
- WW
-

Interactions

- Wc
- c Y Y
- Y
-
-

Domain

- Y W c
- W c
- c c
- W
-



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.”

Y c Y c c c Y Y Y c

Other threats

- c Y c
- c W
- W Y WY

W Y c B Y c c

Smals
ICT for society

IEEE Spectrum FOR THE TECHNOLOGY INSIDER

NEWS | COMPUTING

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

›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."

Y c Y c c c Y Y Y c

Other threats

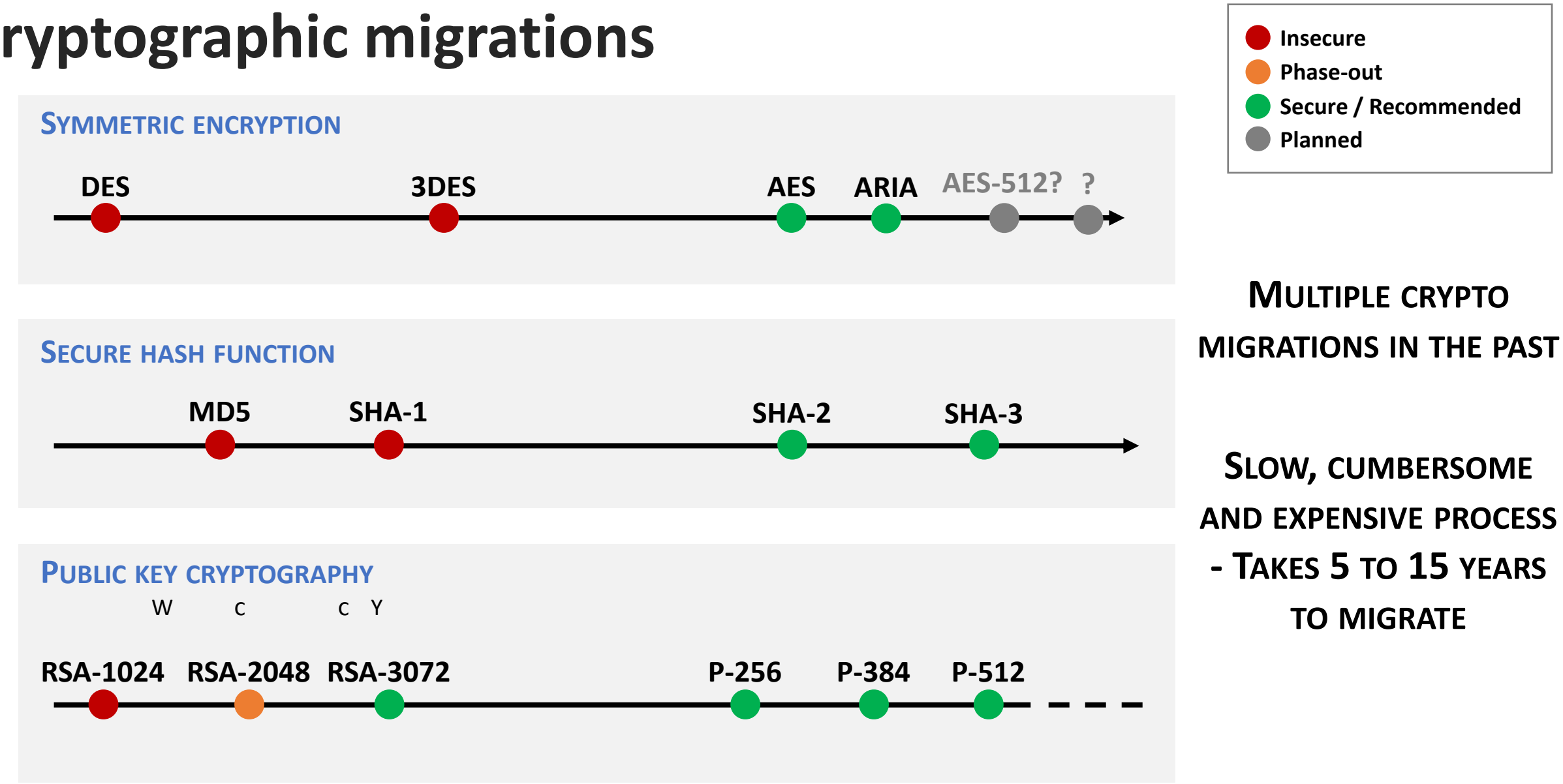
- c Y c
- c W
- W Y WY

W Y c B Y c c

→ MIGRATE ON TIME TO RECOMMENDED CRYPTOGRAPHY

Smals
ICT for society

Cryptographic migrations

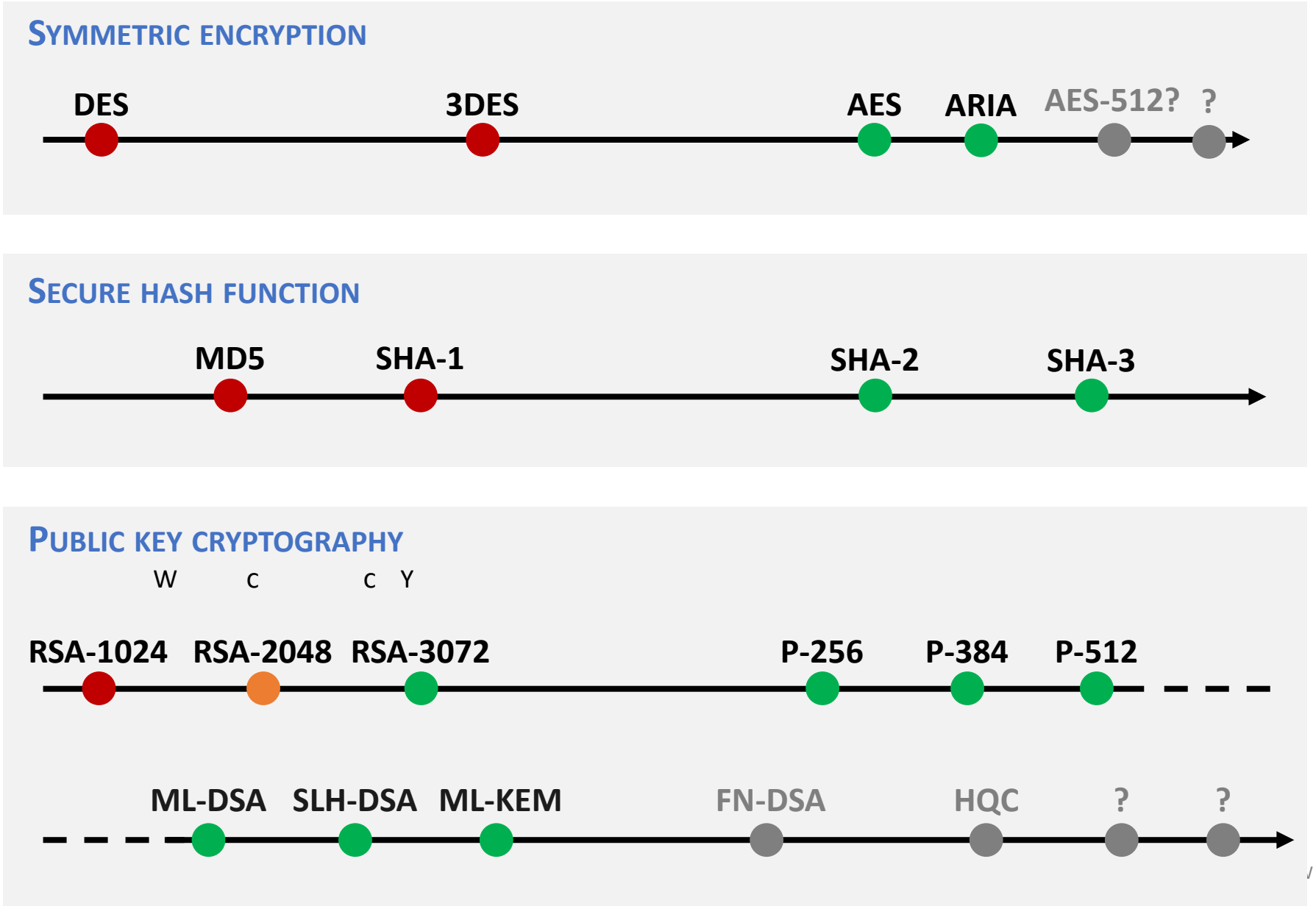


MULTIPLE CRYPTO MIGRATIONS IN THE PAST

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

Smals
ICT for society

Cryptographic migrations



POTENTIALLY MULTIPLE CRYPTO MIGRATIONS IN THE NOT-SO-DISTANT FUTURE!

BECOMING QUANTUM-READY MAY NOT BE A ONE-TIME SHOT

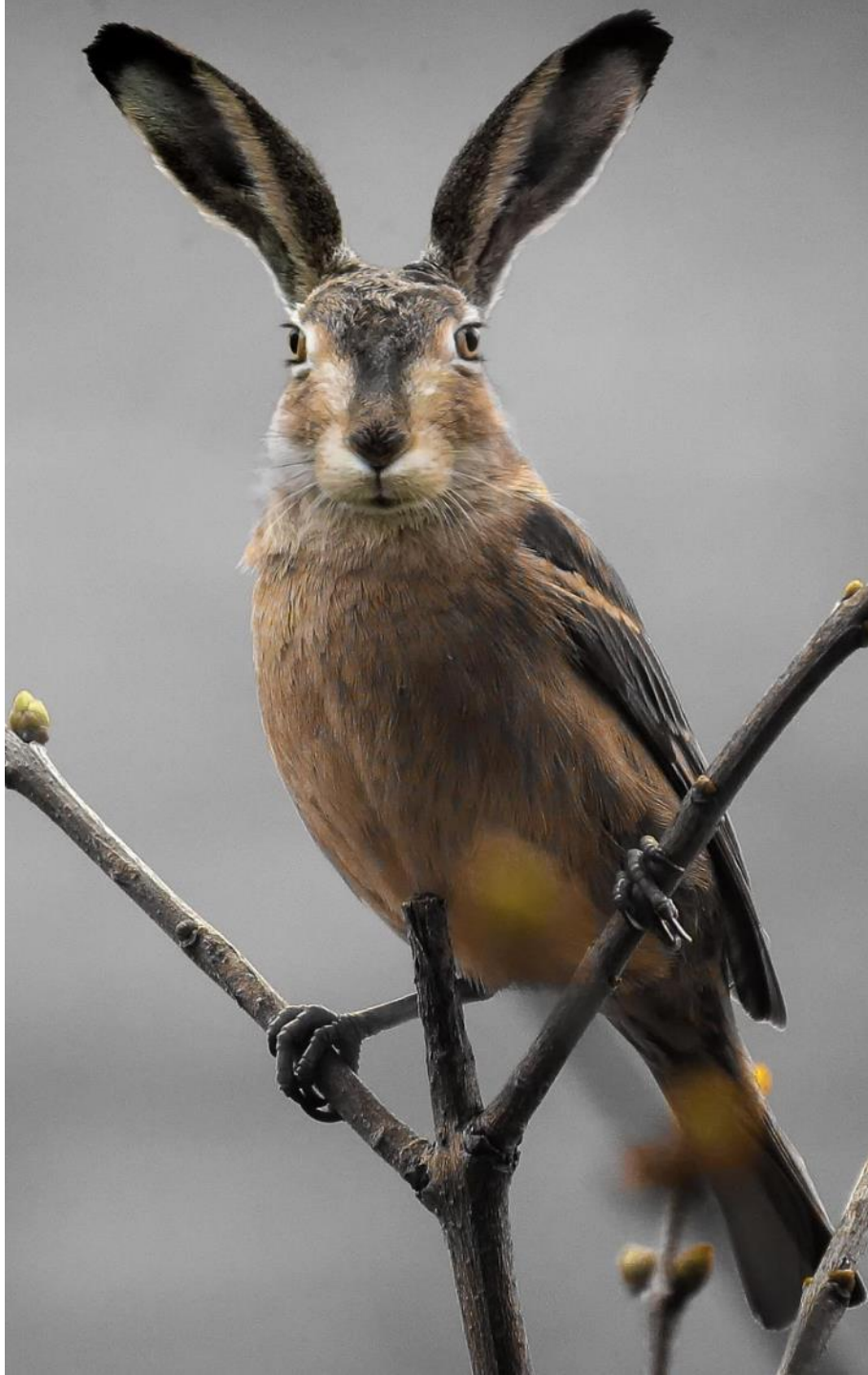
Smals
ICT for society

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).*

→ **EVEN MORE MIGRATIONS!**



Crypto migrations

Challenge

- ❖ W W Y W W c
- ❖ W Y c Y c c Y c

→ **How to facilitate smooth migrations?**

Approach

c c W c Y W W
Y Y c c
c c Y Y c Y

We should accept this and act on it!

Improve cryptographic maturity

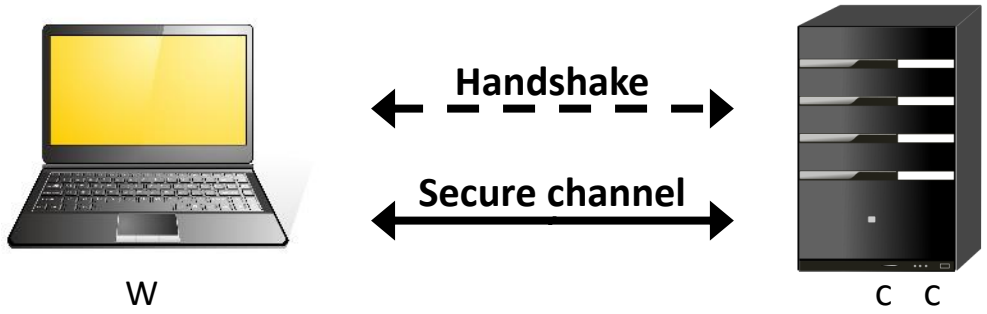
Insight
Crypto inventory
c c c
c

Guidance
Crypto policy
c c
W

Flexibility
Crypto agility
c W c Y
c Y Y

C C C C

Y W c c c W W



Handshake

- C C C
- C C
-
- C C

Supported cipher suites

TLS_AES_128_GCM_SHA256

Supported cipher suites

TLS_AES_128_GCM_SHA256

Y Y

c

c

C c abstract API W c

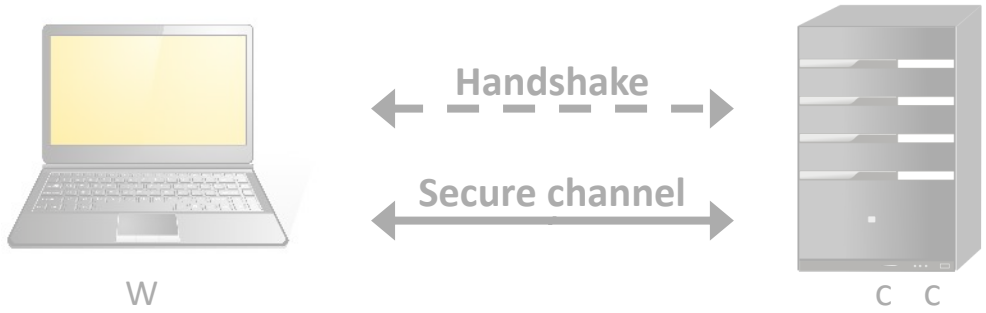
C C selected in real-time

Add remove C C

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

W Y c c c W c c W c c c Y c

W c c W Y c c



Handshake

Supported cipher suites

TLS_AES_128_GCM_SHA256

Supported cipher suites

TLS_AES_128_GCM_SHA256

Cryptographic Agility

On the level of an IT system

abstract API

selected in real-time

Add remove

At runtime

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

C C W C

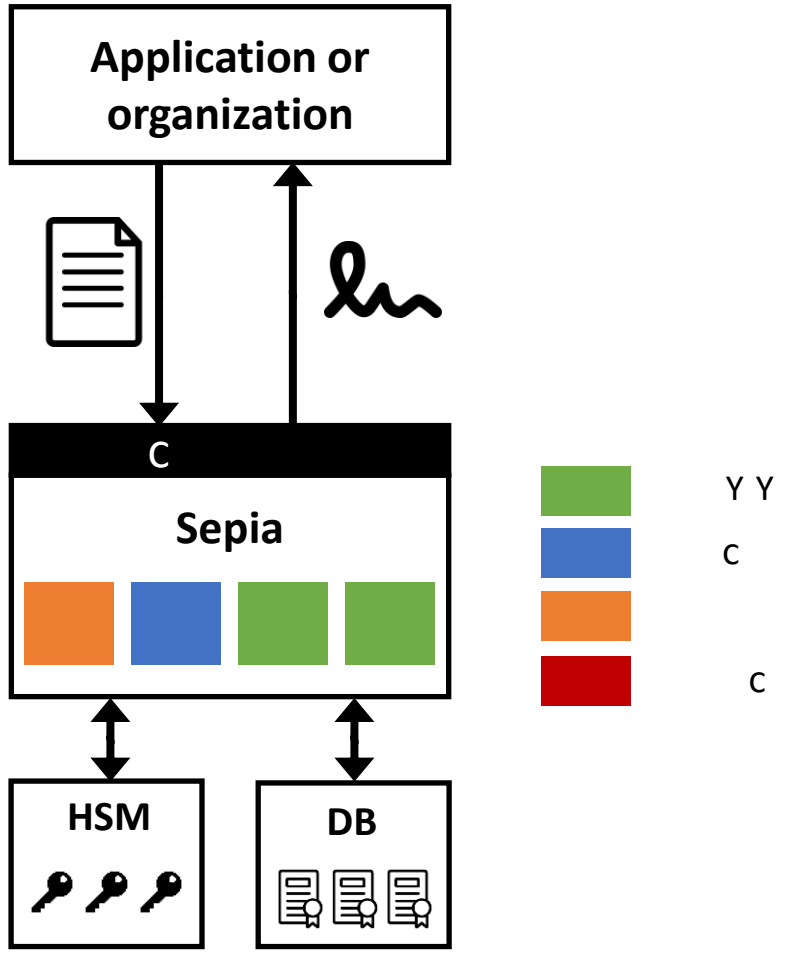
Service developed by Smals

Functionality

- C W C W W C
  C C
- Y C Y C
- C Y C
- C C C C

Motivation

- **Cost reduction by reuse**
  C W
- **Increase security**
- **Crypto agility!**



CRYPTO AGILITY AND COST EFFICIENCY CAN COEXIST

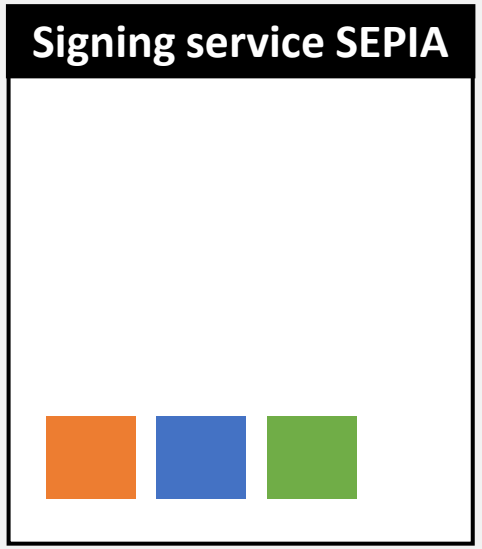
W B Y C C C W |

C W C Y C

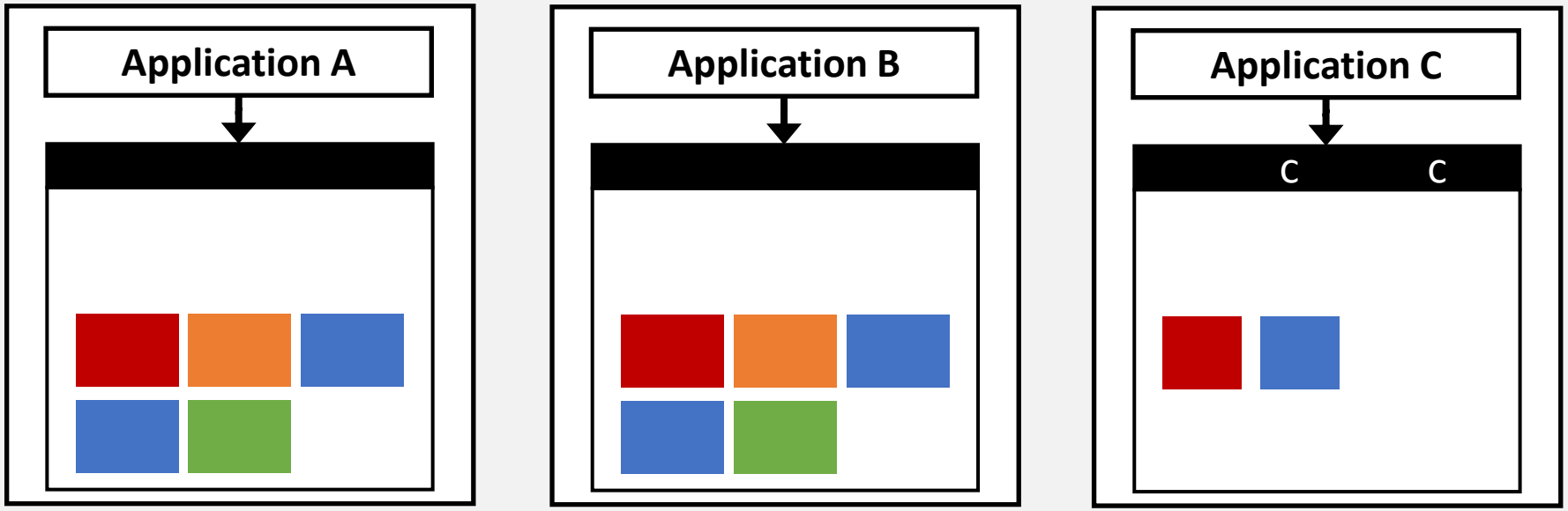
Smals
ICT for society

Possible Future Architecture

CENTRAL



LOCAL



Possible Future Architecture

CENTRAL

Implementation service

Cipher suites

Algorithms

Policy service

Policy

W + = W

Deviations

Signing service SEPIA

Certificate mgt.

W

Crypto inventory

LOCAL

Application A

W

Application B

W

Application C

C C

W

"A1 only to decrypt"

Possible Future Architecture

CENTRAL

Implementation service

Cipher suites

Algorithms

Policy service

Policy

W + =

Deviations

Signing service SEPIA

W

Certificate mgt.

W

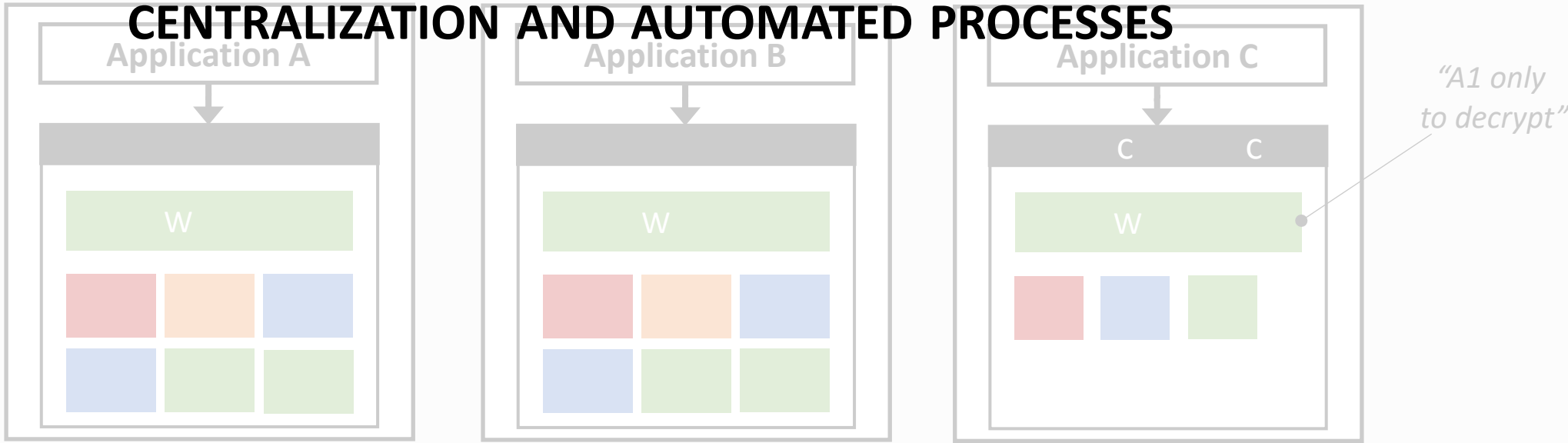
Crypto inventory

CRYPTOGRAPHIC AGILITY

IMPLIES

CENTRALIZATION AND AUTOMATED PROCESSES

LOCAL



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

W B Y C C C W |

Smals ICT for society

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

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

2

Practiced

Crypto migration demonstrable, effectively and securely feasible

Knowledge

- Performance awareness
- [illegible] 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

W B Y C C C W |

Smals ICT for society

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

Challenges & open questions

Research on CA

Performance

Middleboxes

Legacy

Standards

Downgrade attacks

QR-codes

IoT

Incompatibilities

Advanced cryptography

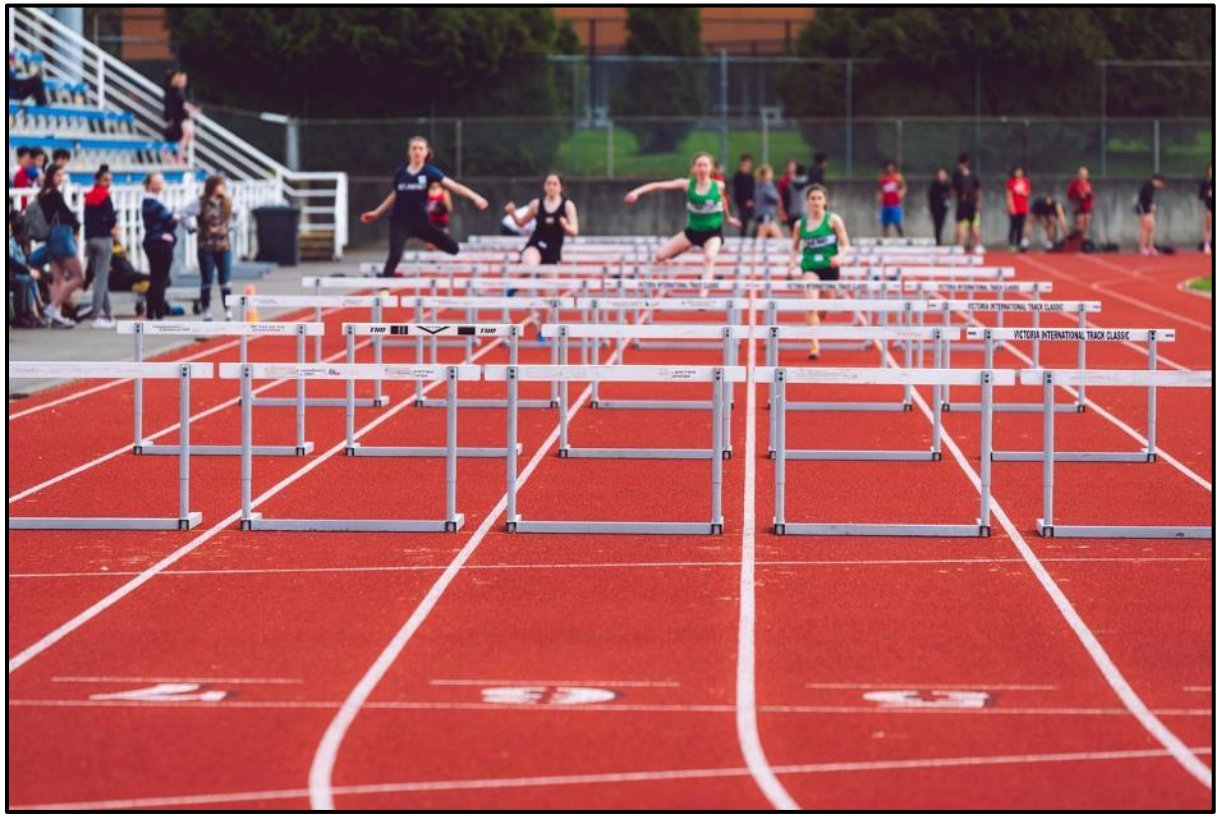
Guidance

X.509 certificates

Smartcards

HSMs

Cryptographic accelerators

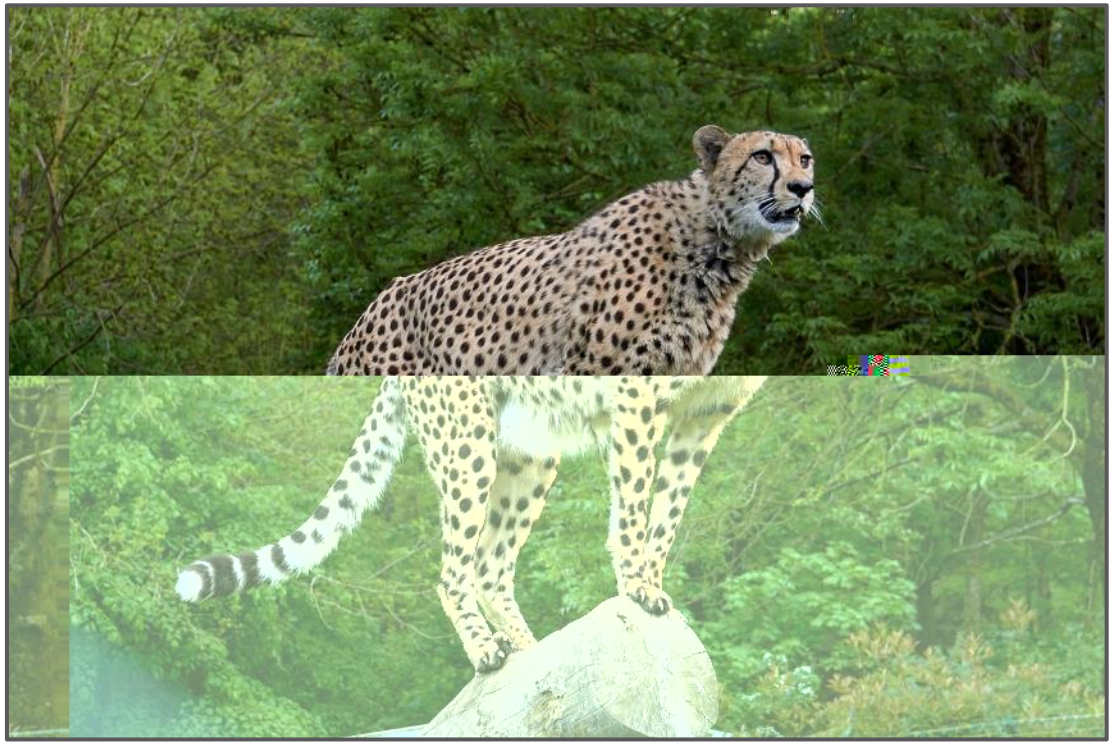


BECOMING QUANTUM-READY IS HARD, BECOMING CRYPTO AGILE EVEN HARDER

BUT… IT PAYS OFF IN THE LONG RUN!

Smals
ICT for society

Takeaways



- c Y c Y c
- c Y Y W W
- c Y c W Y c Y
- c W c W W c c
  c W
- **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!

B
C

W Y
C

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