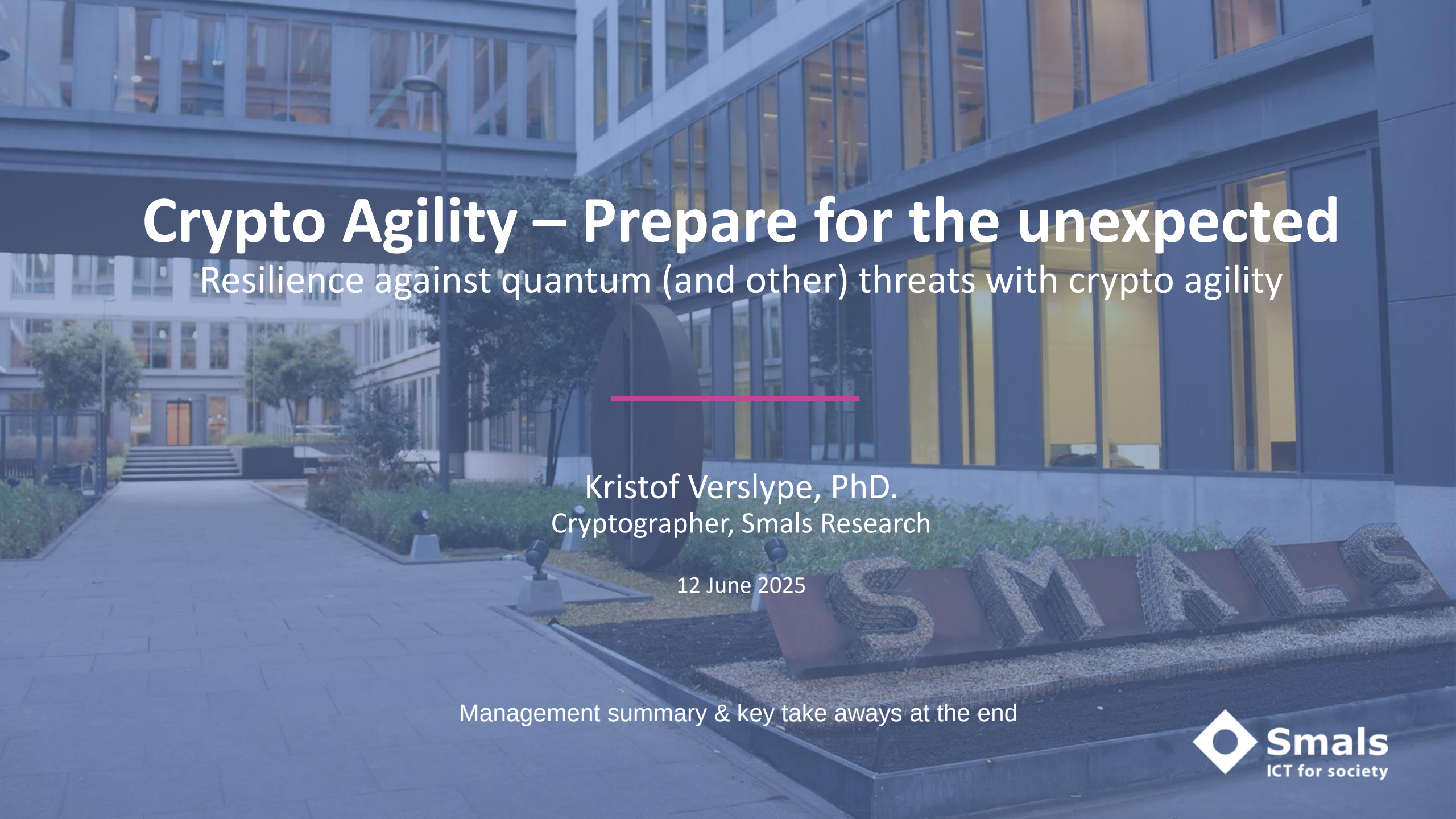


Crypto Agility – Prepare for the unexpected

Resilience against quantum (and other) threats with crypto agility

Kristof Verslype, PhD.
Cryptographer, Smals Research

12 June 2025

Management summary & key take aways at the end

Smals
ICT for society

Smals Research

Innovation with new technologies

Consultancy & expertise

Internal & external knowledge transfer

Support for going live

GraphRAG

Agentic AI

Code security assistants

Knowledge Graphs

Guardrails & Evaluations for RAG

Agent-Computer Interaction

Native Graph ML

Crypto migration

Administrative Digital Twins

Semantic Search

Rules and code generation

2025

Crypto policy as code

Metadata Management Solutions

Neuro-symbolic AI

Legacy code & AI

Zero-Knowledge proofs

Confidential cross-institutional collaboration

Dark & Deep Web

Verifiable Credentials & EU Digital Wallet

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

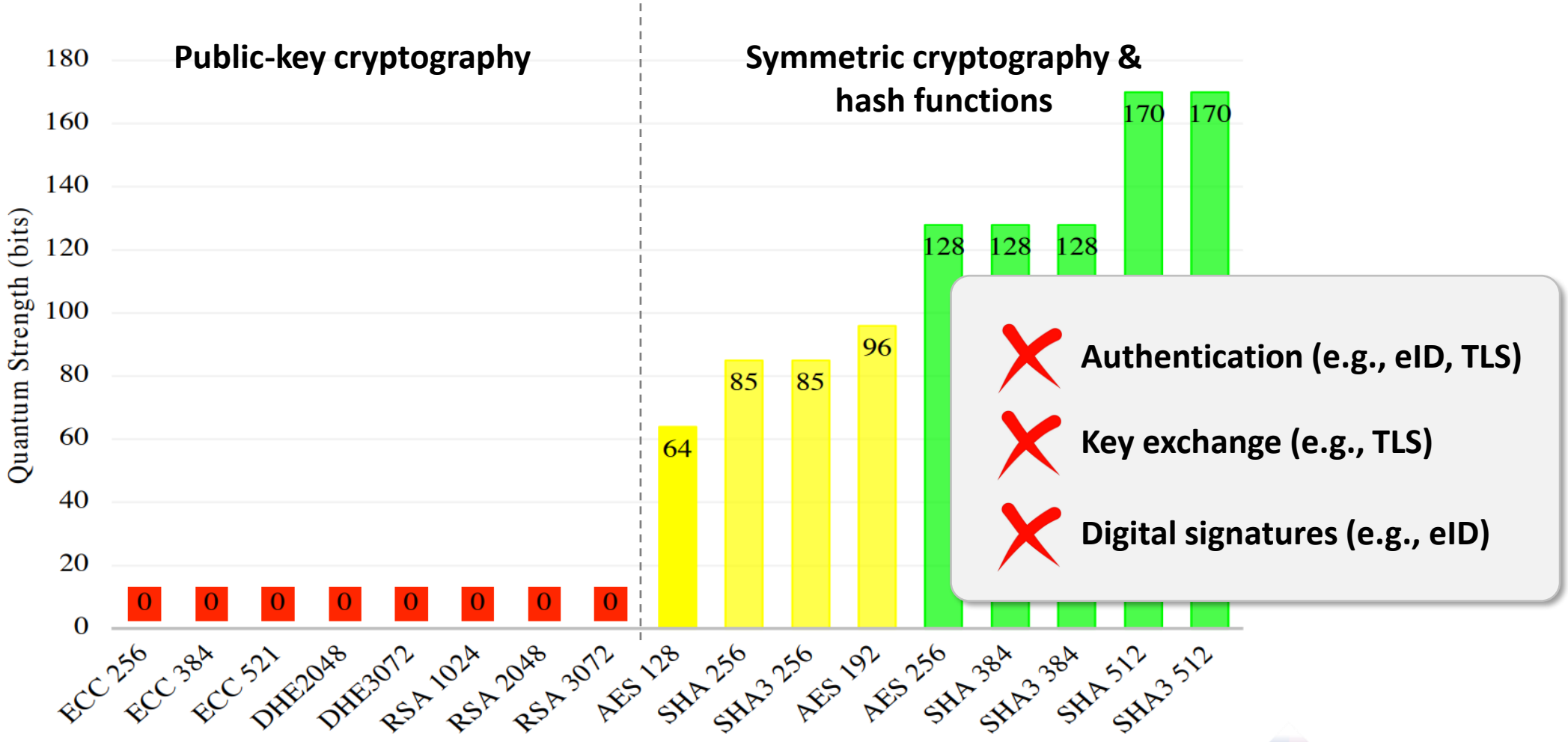
Would be able to break modern (public-key) cryptography

"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)

Smals
ICT for society

Impact cryptographically relevant quantum computers on modern cryptography

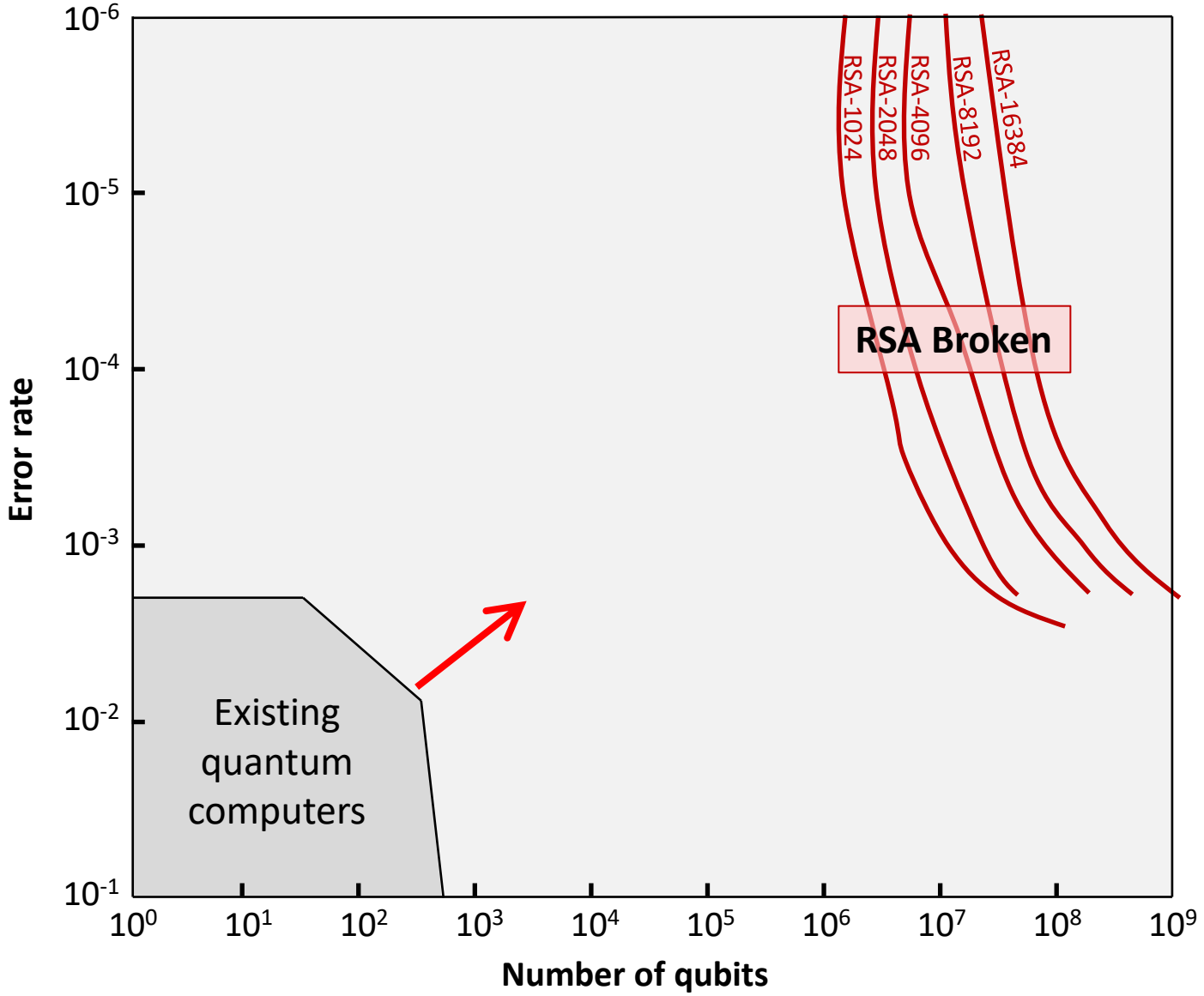


Expected Impact of Quantum Threat for Classic Cryptography

Smals ICT for society

Baseri, Y., Chouhan, V., Ghorbani, A., & Chow, A. (2024). Evaluation Framework for Quantum Security Risk Assessment: A Comprehensive Study for Quantum-Safe Migration. *arXiv preprint arXiv:2404.08231*.

Quantum computers Vs. Modern public-key cryptography



"We need Moore's-law type scaling for quantum computers to ever be useful"

Figure inspired by Samuel Jaques
https://sam-jaques.appspot.com/quantum_landscape

Smals
ICT for society

How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

Google Quantum AI, Santa Barbara, California 93117, USA

May 28, 2025

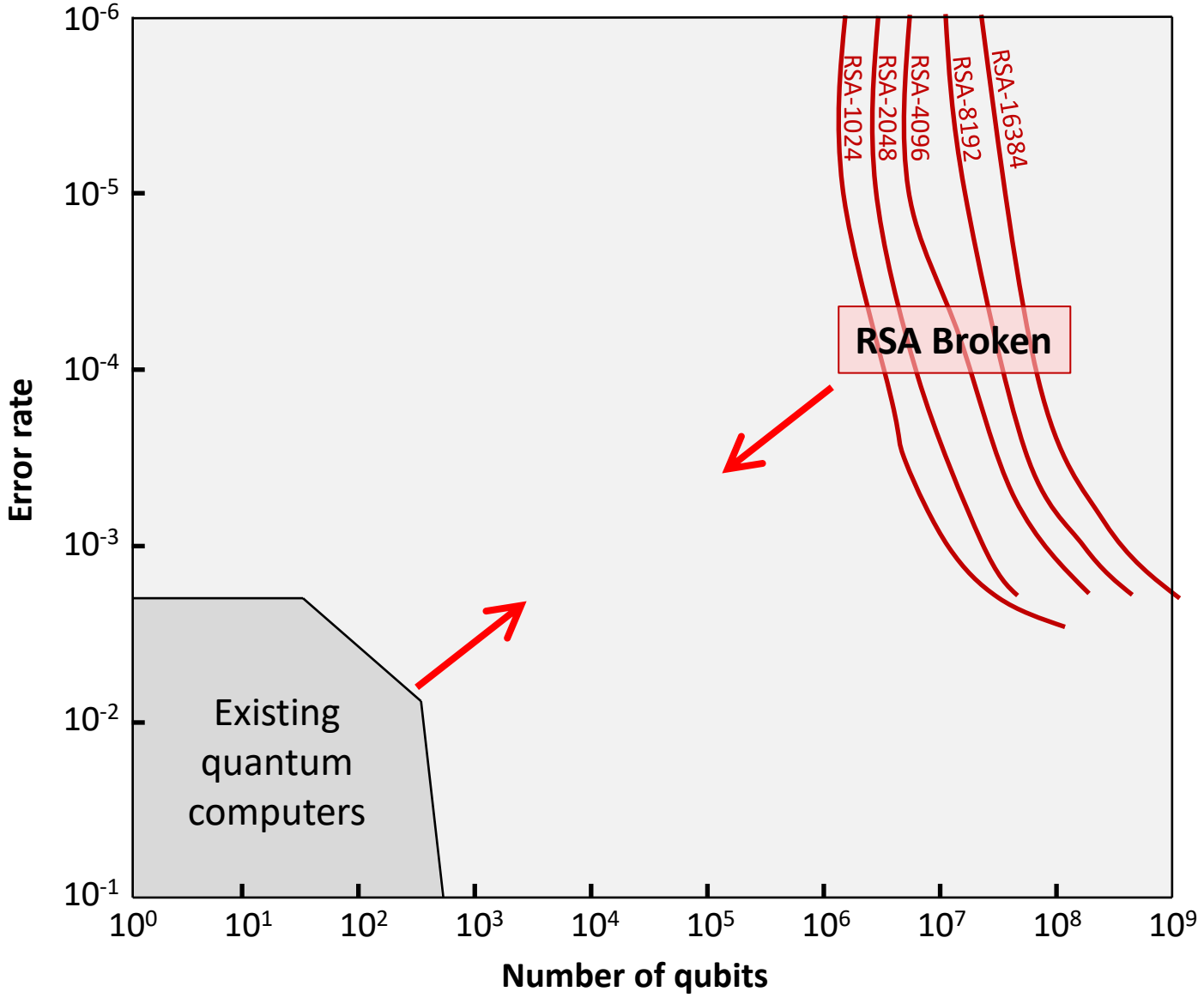
Planning the transition to quantum-safe cryptosystems requires understanding the cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ekerå 2019, I co-published an estimate stating that 2048 bit RSA integers could be factored in eight hours by a quantum computer with 20 million noisy qubits. In this paper, I substantially reduce the number of qubits required. I estimate that a 2048 bit RSA integer could be factored in less than a week by a quantum computer with less than a million noisy qubits. I make the same assumptions as in 2019: a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds.

The qubit count reduction comes mainly from using approximate residue arithmetic (Chevignard+Fouque+Schrottenloher 2024), from storing idle logical qubits with yoked surface codes (Gidney+Newman+Brooks+Jones 2023), and from allocating less space to magic state distillation by using magic state cultivation (Gidney+Shutty+Jones 2024). The longer runtime is mainly due to performing more Toffoli gates and using fewer magic state factories compared to Gidney+Ekerå 2019. That said, I reduce the Toffoli count by over 100x compared to Chevignard+Fouque+Schrottenloher 2024.

Smals
ICT for society

https://arxiv.org/pdf/2505.15917

Quantum computers Vs. Modern public-key cryptography



"We need Moore's-law type scaling for quantum computers to ever be useful"

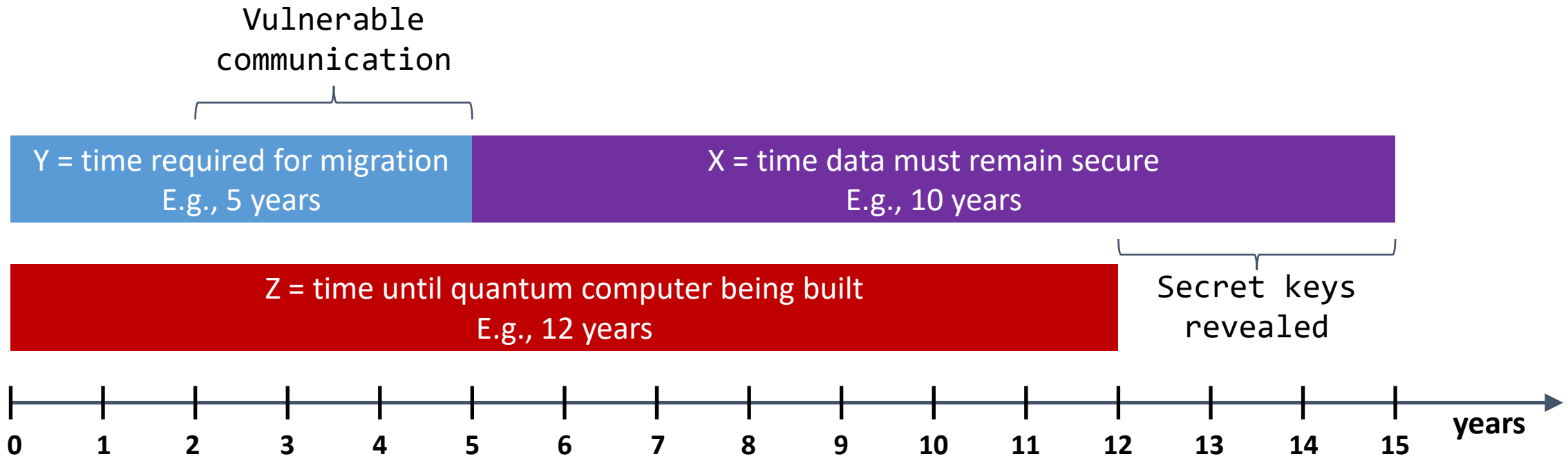
Improvements of the quantum algorithms & implementations to break modern public-key cryptography possible

Figure inspired by Samuel Jaques,
https://sam-jaques.appspot.com/quantum_landscape

Smals
ICT for society

Harvest now, decrypt later

Encrypted communication intercepted today can be encrypted in the future



Mosca's Theorem

if X + Y > Z
then Sensitive data exposed

Take attack scenario into account

Harvest now, decrypt later

→ Forced to think a long time in advance!
→ Primarily key-agreement schemes (data in transit)
→ **Don't panic! Not an easy attack!**

Smals ICT for society

Source: Quantum-safe cryptography – fundamentals, current developments and recommendations

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

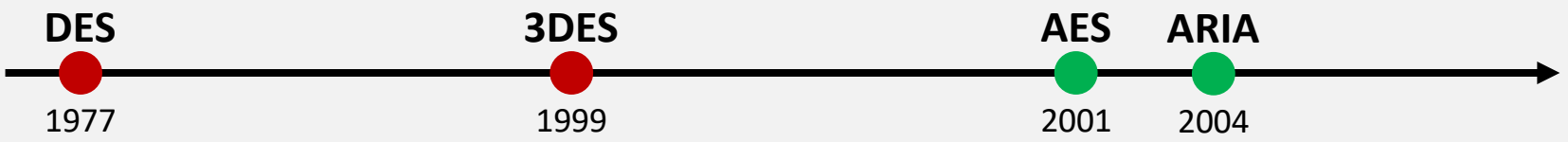
→ **MIGRATE ON TIME TO RECOMMENDED CRYPTOGRAPHY**

Smals ICT for society

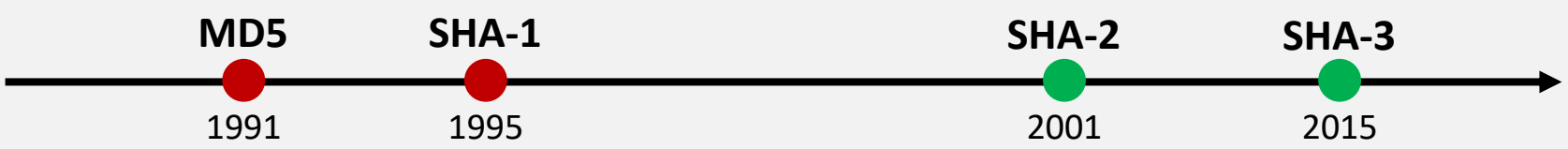
Cryptographic migrations

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

Symmetric encryption

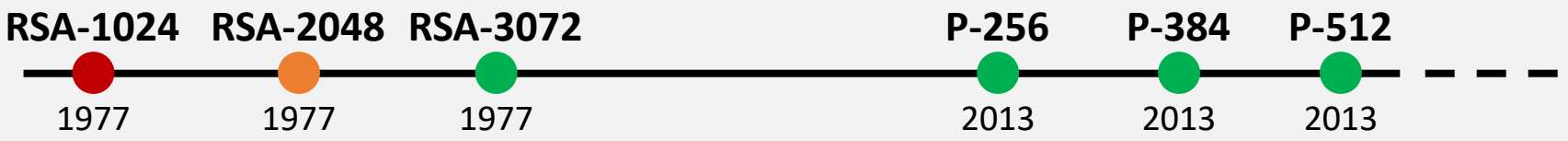


Secure hash function



Public key cryptography

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



Multiple crypto migrations in the past

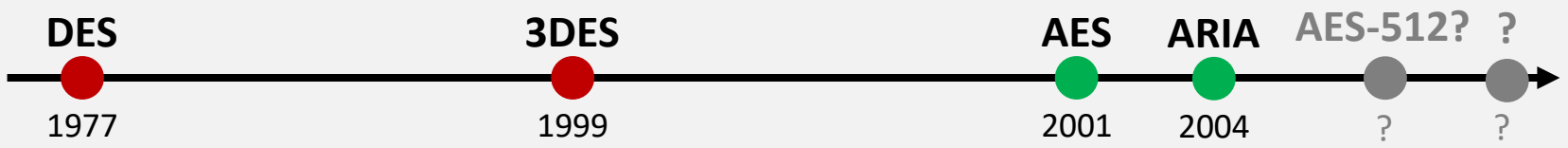
Slow, cumbersome and expensive process - Takes 5 to 15 years to migrate

Smals ICT for society

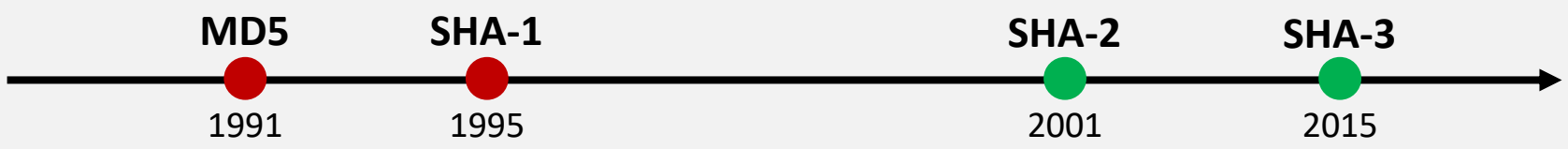
Cryptographic migrations

- 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

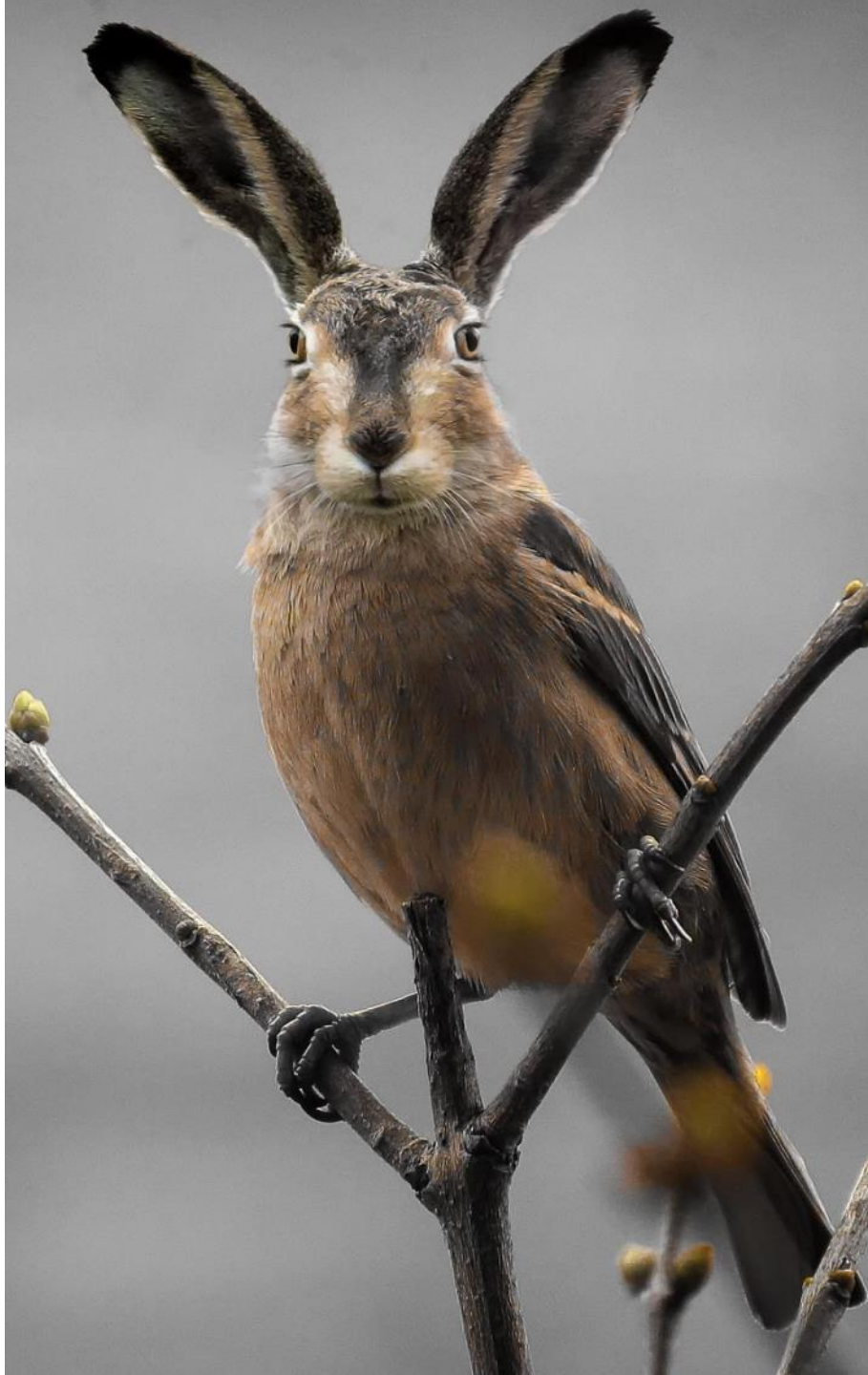
Transitional period in Hybrid Mode

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

Cryptography: Assets that need to be managed

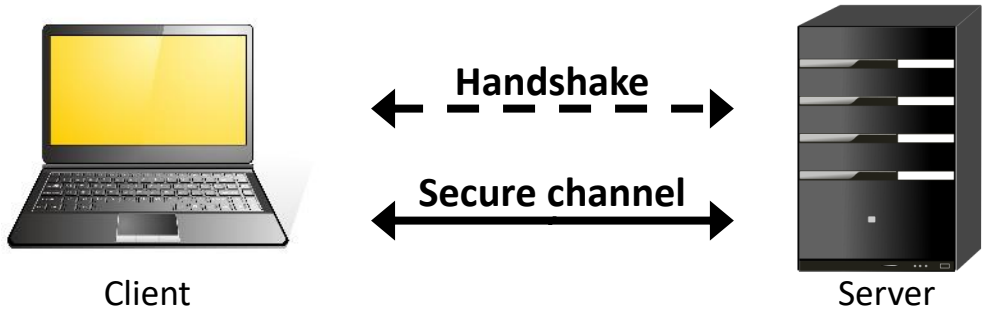
We should accept this and act on it!

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

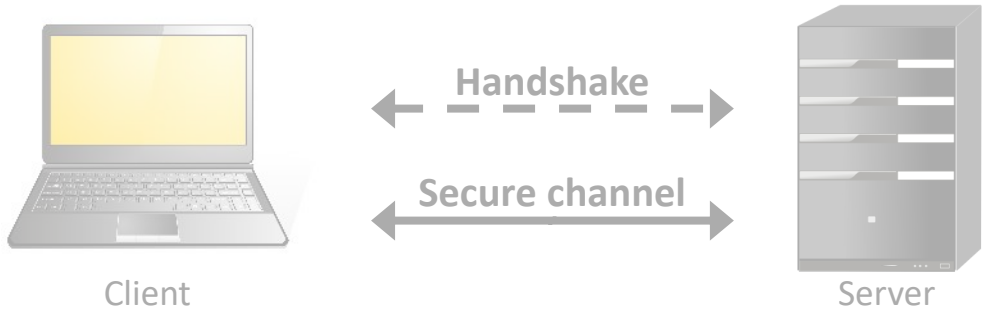
Cryptographic functions: *Hardware, software, firmware, algorithms, parameters, …*

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
Insecure

Cryptographic Agility

On the level of an IT infrastructure

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

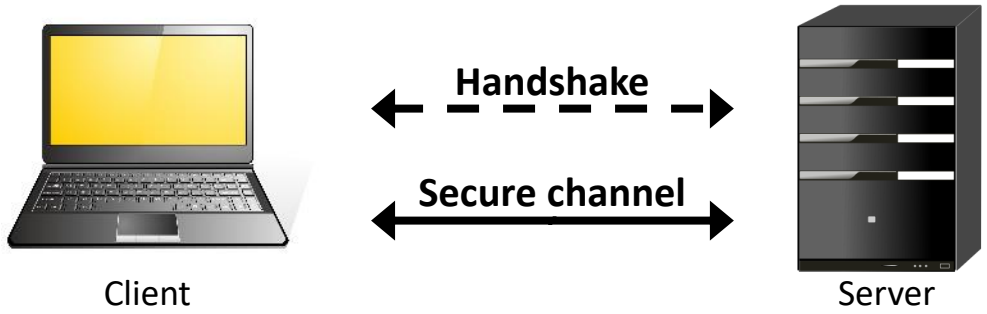
Agenda

- Why & What?
- **In the Public Sector**
- Crypto Inventory
- Crypto Policy as Code
- Cryptography in Hybrid Mode
- Outlook & Challenges
- Wrapping Up

Smals
ICT for society

Transport Layer Security (TLS)

Concept being developed by Smals Research



Handshake

- Agree on TLS version
- 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

Policy service

Policy + **Deviation** => **TLS Config**
- Cipher suites
- Parameters
- Extensions

CRYPTO AGILITY BY AUTOMATING AND CENTRALIZING TLS CONFIGURATION

OVERVIEW OF POLICY DEVIATIONS

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

Sepia - Service for digital signatures

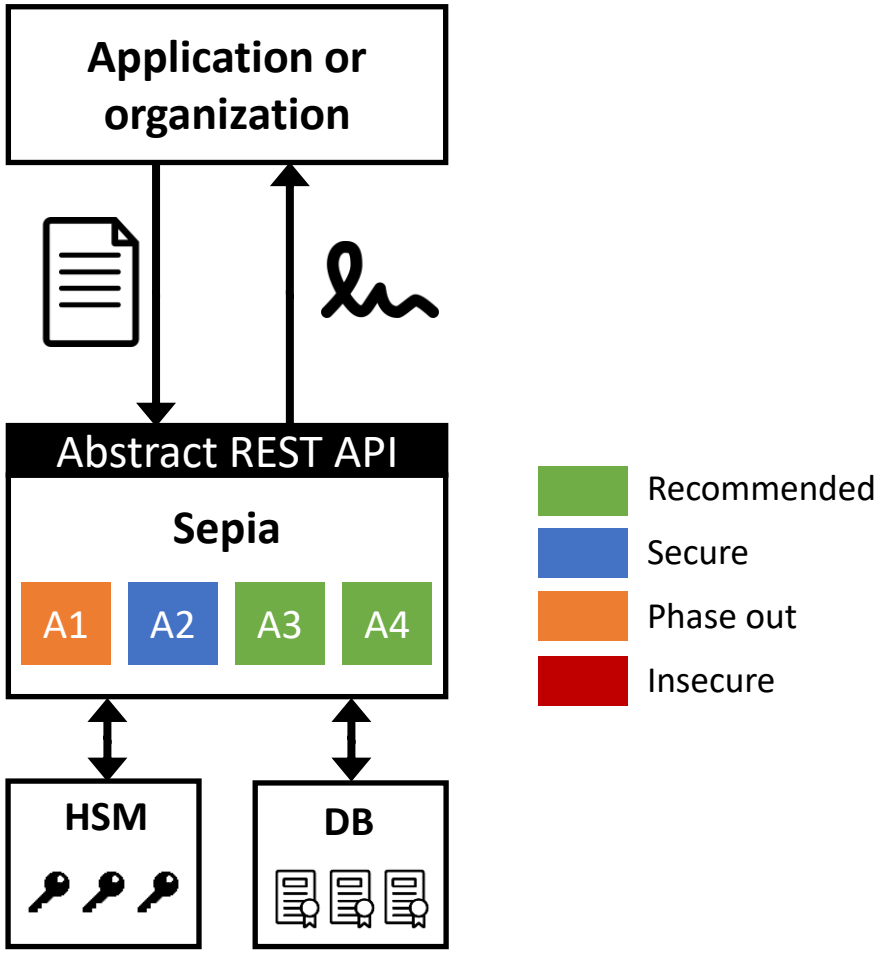
Service developed by Smals

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

Smals ICT for society

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

Blind Pseudonimisation Service eHealth

Runner-up for *Best Cybersecurity Innovation Europe* award issued by Cybersec Europe

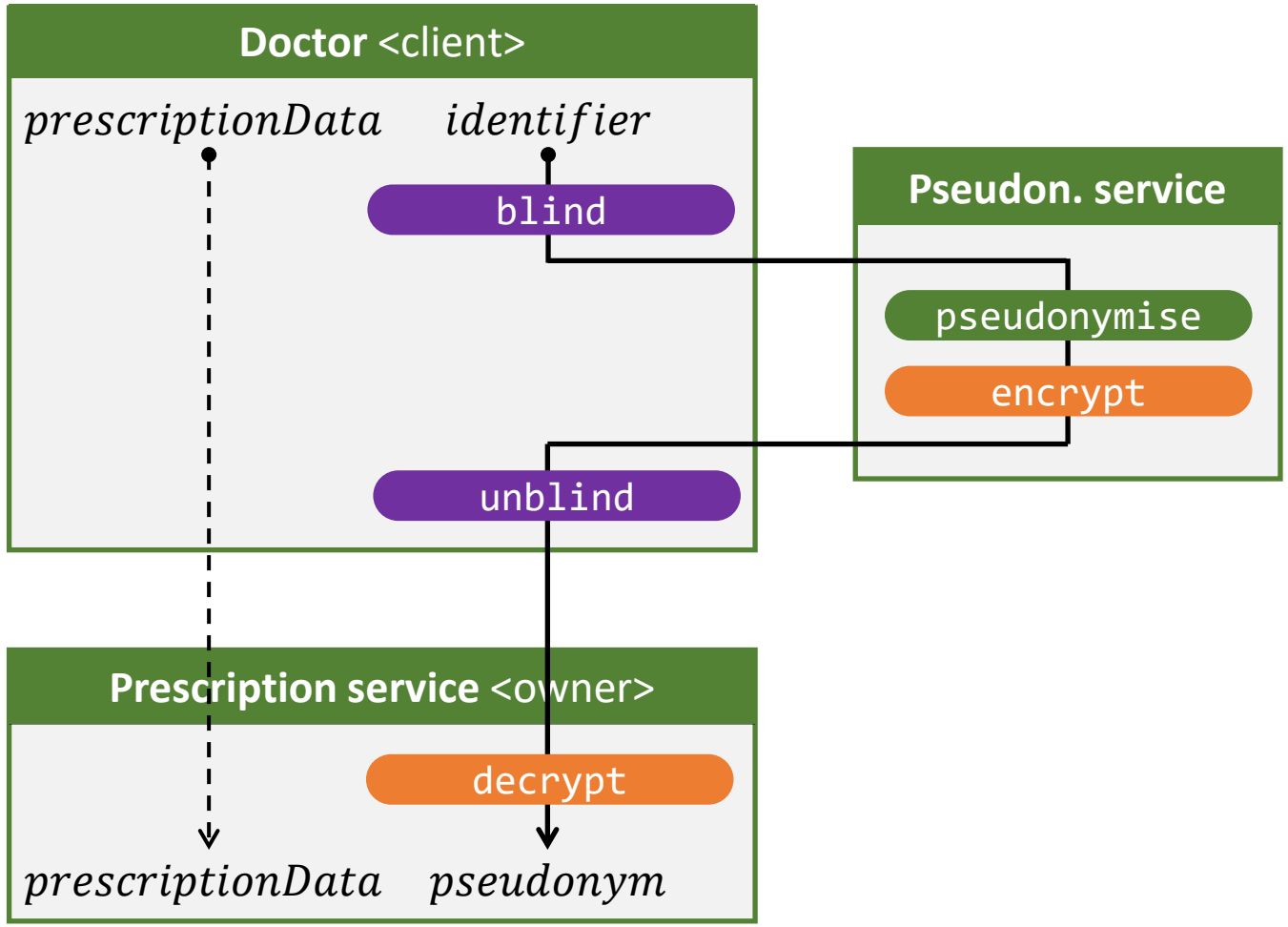
Data minimisation
- Doctor only sees identifiers
- Backend only sees pseudonyms
- Pseudon. service sees neither

Reduced overhead
- Direct communication between healthcare professional and prescription service
- No in-between entity

Low-intrusive side professional
- No extra keys required
- Relatively simple implementation

Scenario

Doctor requests *Prescription service* to register medical prescription



HOW QUANTUM RESISTANT IS THIS SOLUTION?

Smals ICT for society

Blind Pseudonimisation Service eHealth

Cryptography

- Mix of symmetric and public-key crypto
- Designed before NIST PQC standards
  (like close to all applications in the world)

Analysis

Communication (red lines)

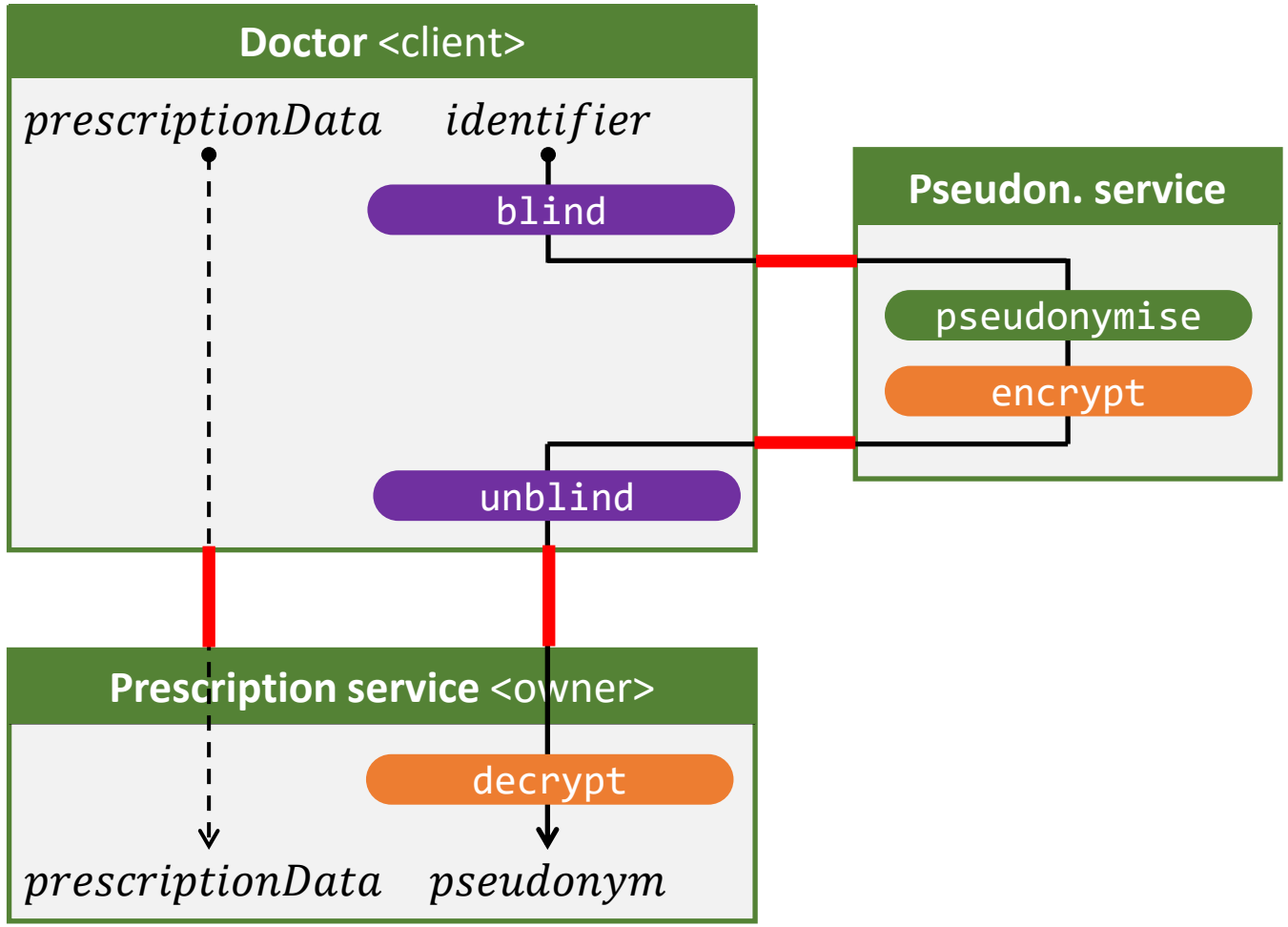
- Most important → harvest now decrypt later
- Update TLS clients
- Not different from other applications

Pseudonymisation

- Single quantum risk: backend-stored pseudonyms
- Roadmap to mitigate risk
  1. Alternative based on lattices (PQC)
  2. Integration of crypto agility
  3. Defining procedures
  4. Actual migration

Scenario

Doctor requests *Prescription service* to register medical prescription



SMALS IS EARLY BY PROACTIVELY WORKING ON QUANTUM-READINESS & CRYPTO AGILITY

Smals ICT for society

Cryptographic Agility in the Belgian Public Sector

TLS

- Deriving TLS configs from central policy-as-code and deviations-as-code
- Status: Research

Blind pseudon. service

- Quantum-resistant pseudonymisation being developed
- Crypto-agility being examined
- Status: Research

Sepia

- Central, flexible service for document signing
- Status: Live

Key Vault

- Storing middleware keys in a central vault
- Status: Soon live

Central certificate mgt.

- Automatic TLS certificate install & updates
- Status: Soon live

SMALS IS EARLY WITH CRYPTO-AGILITY & TAKING INITIATIVES

NEVERTHELESS, A LONG ROAD AHEAD OF US!

Smals
ICT for society

Agenda

- Why & What?
- In the Public Sector
- **Crypto Inventory**
- Crypto Policy as Code
- Cryptography in Hybrid Mode
- Outlook & Challenges
- Wrapping Up

Smals
ICT for society

Cryptography inventory

What cryptography is used where in the IT-infrastructure (and for what purpose)

Purpose

- ✓ Prepare crypto migrations
- ✓ Intervene quickly in case of vulnerability
- ✓ Demonstrate compliance

Keys	Certificates	Algorithms	Protocols
Cipher suites	Crypto libraries	Algorithm implementations	Services
Hardware	IoTs	…	

IMPOSSIBLE MANUALLY – AUTOMATED PROCESSES REQUIRED

EXPRESS CRYPTOGRAPHY INVENTORY IN MACHINE-READABLE WAY

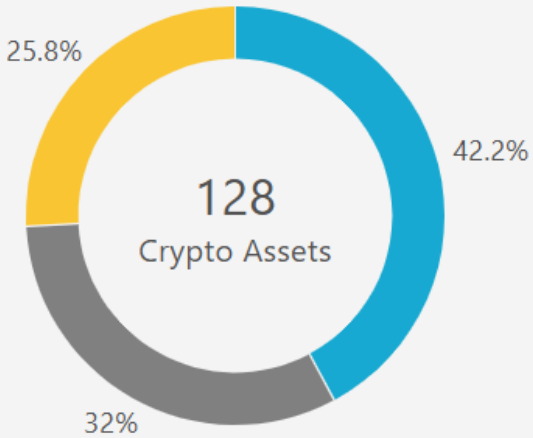
github.com/keycloak/keycloak

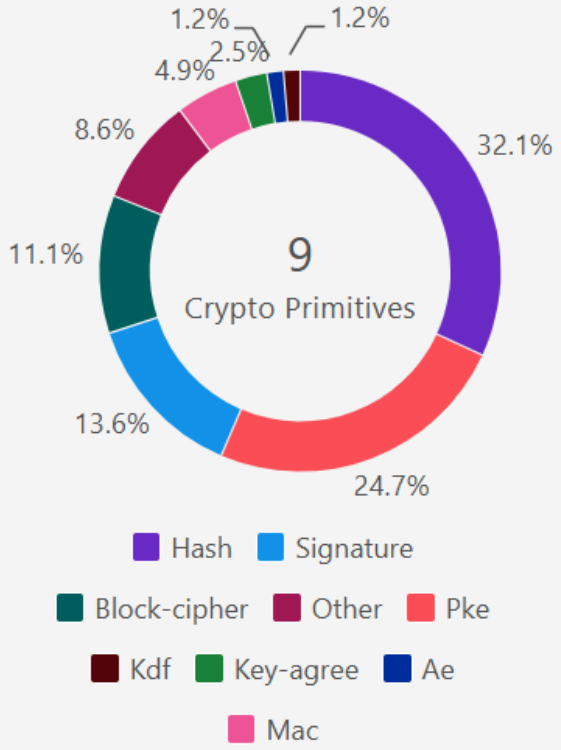
CBOMkit

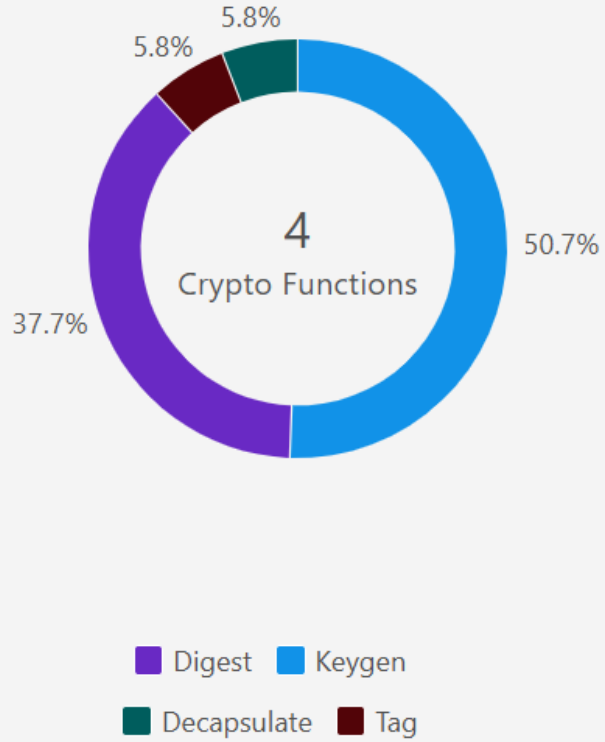
128 cryptographic assets found. Scanned **616.7K** lines of code across **5.3K** files. Took **2m 21s** to scan (**4m 7s** in total).

gitUrl: https://github.com/keycloak/keycloak | revision: main | commit: f8a4a8d

Not compliant – This CBOM does not comply with the policy "quantum_safe".
Source: Basic Backend Compliance Service







List of all assets

Scan finished

Download CBOM

Cryptographic asset	Type	Primitive	Location
PUBLIC-KEY	Related Crypto Material	*Unspecified*	BCFIPSECDSACryptoProvider.java:85
RAW	Algorithm	Other	HmacOTP.java:159
EDDSA	Algorithm	Digital Signature	GeneratedEddsaKeyProvider.java:50
EDDSA	Algorithm	Digital Signature	GeneratedEddsaKeyProviderFactory.java:133
HMAC-SHA256	Algorithm	Message Authentication Code	HMACProvider.java:41
HMAC-SHA256	Algorithm	Message Authentication Code	KeycloakModelUtils.java:215
SECRET-KEY	Related Crypto Material	*Unspecified*	AesCbcHmacShaEncryptionProvider.java:170
PUBLIC-KEY	Related Crypto Material	*Unspecified*	BCECDSACryptoProvider.java:80
RSA-2048	Algorithm	Public Key Encryption	KeyUtils.java:69
RSA-2048	Algorithm	Public Key Encryption	RSAKeyValueType.java:103

Items per page: 10 | 11-20 of 128 items | 2 of 13 pages

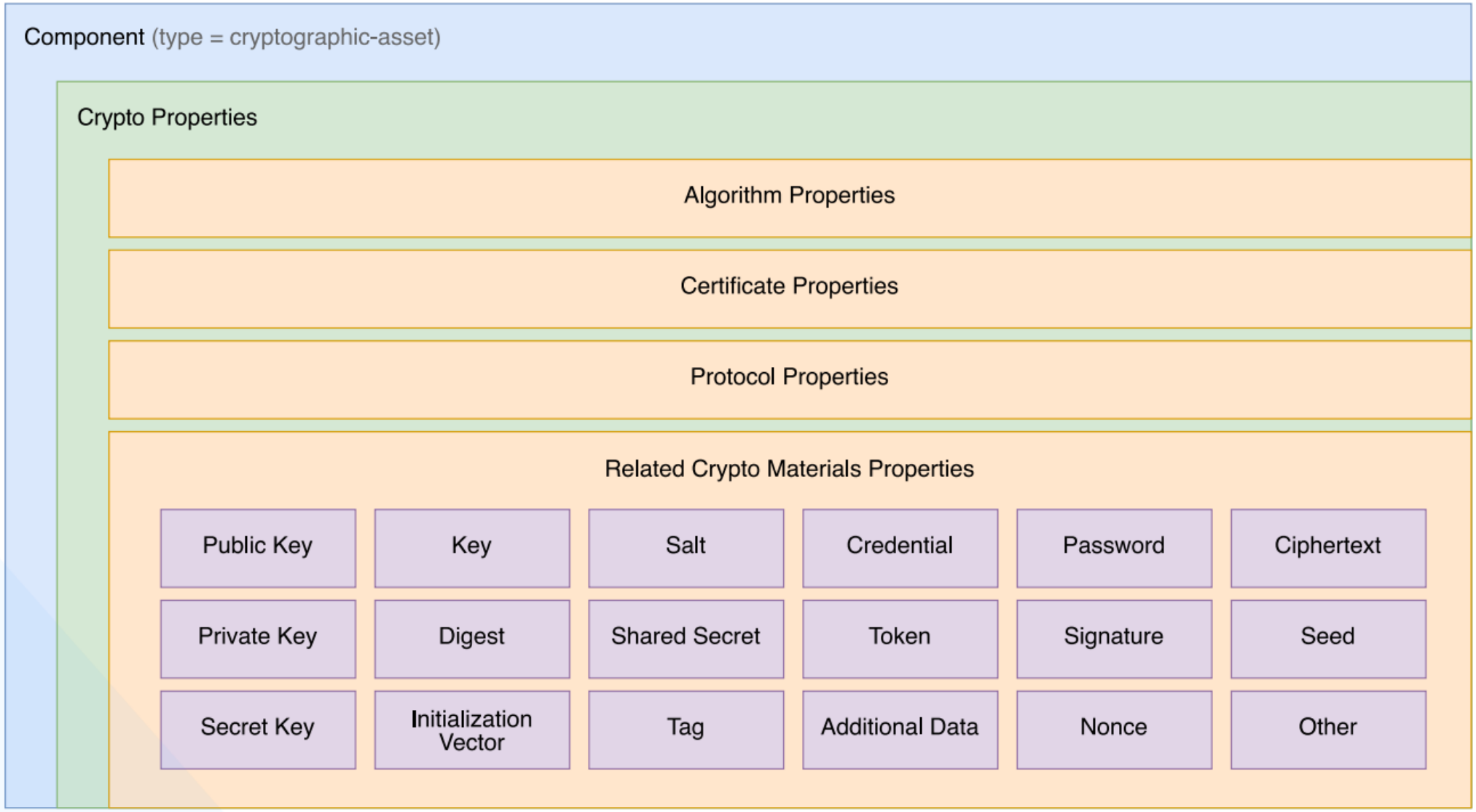
Cryptography Bill of Materials (CBOM)

Object model to describe cryptographic assets and their dependencies. Developed by IBM, now OWASP standard


```
{
    "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/AbstractJWKParser.java",
                "additionalContext": "java.security.KeyFactory#getInstance(Ljava/lang/String;)Ljava/security/KeyFactory;"
            },
            {
                "line": 103,
                "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;"
            },
            {
                "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;"
            }
        ]
    }
}
```

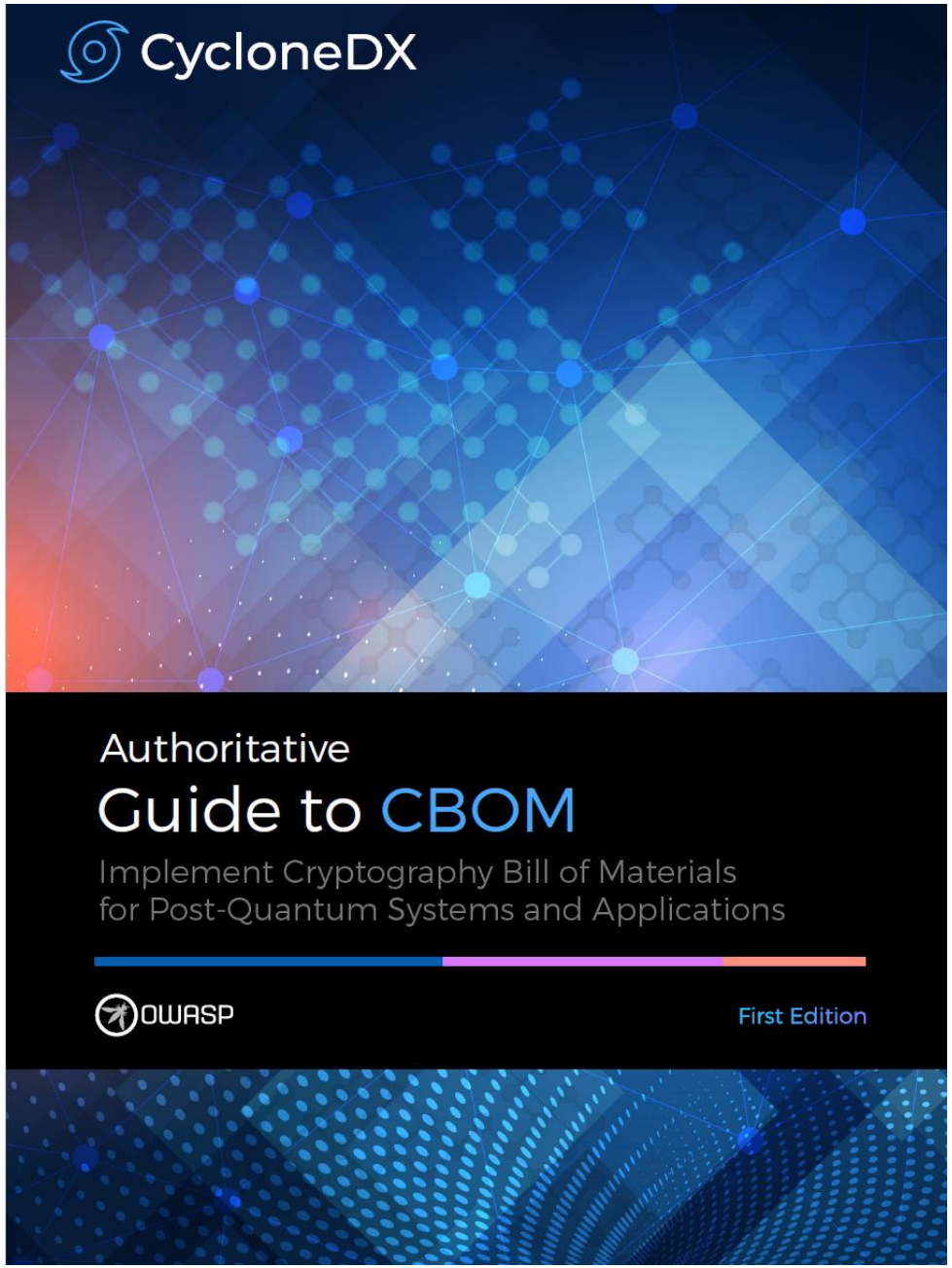

https://github.com/IBM/cbomkit/blob/main/example/keycloak-cbom.json

CBOM - Structure and Cryptographic Asset Types



mals
ICT for society

CBOM Authorative Guide



https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-CBOM-en.pdf

Smals
ICT for society

Consolidating Crypto Inventory

DISCOVERY

Dynamic scanning

- External network
- Internal network

→ **NOT CBOM**

Static scanning

- IT assets (IoT, servers, …)
- Databases
- Code

→ **CBOM**

DELIVERY

Internal import

- In-house applications
- Certificate management

→ **CBOM**

External import

- Cloud services
- External libraries
- Operating systems
- Hardware (HSM, firewalls, …)

→ **CBOM**

NEED TO CONSOLIDATE EVERYTHING IN ONE INVENTORY & KEEP IT UP-TO-DATE
REQUIRES AUTOMATED, INTEGRATED PROCESSES → LONG SHOT

START SIMPLE, WITH A FOCUS ON YOUR MOST VALUABLE ASSETS & EXTERNAL COMMUNICATION
CONSOLIDATE WHAT YOU ALREADY HAVE

Smals
ICT for society

Agenda

- Why & What?
- In The Public Sector
- Crypto Inventory
- **Crypto Policy as Code**
- Cryptography in Hybrid Mode
- Outlook & Challenges
- Wrapping Up

Smals
ICT for society

Crypto policy – Current situation

Symmetric Encryption Schemes

Created by Kristof Verslype, last updated on Jul 29, 2024 • 5 minute read

Corresponds to section 3. Symmetric Encryption Schemes in BSI TR-02102-1 (version 2024).

Symmetric encryption schemes are used to guarantee the confidentiality of data that is transmitted, for example, via a public chann ntegrity guaranteed. For integrity protection, see Chapter 6 and Section A.1. Even in cases where at first glance the protection of the confide even th integrity-securing mechanisms can easily lead to weaknesses in the overall cryptographic system, which then also makes the system h vulne active side-channel attacks,

3.1 Block ciphers

A *block cipher* is an algorithm that encrypts a plaintext of fixed bit length (for example 128 bits) by means of a key to a ciphertext of the same bit length. This bit length is also called *block size* of th of other lengths, block ciphers are applied in different *modes*.

3.1.1 Algorithm

Recommended

For new cryptographic applications, only block ciphers whose block size is at least 128 bits should be used. The following block ciphers are recommended for use in new cryptographic systems:

Algorithm name	Security level	Key Size	Block size	Reference
AES-128	128	128	128	FIPS PUB 197 [3]
AES-192	192	192	128	FIPS PUB 197 [3]
AES-256	256	256	128	FIPS PUB 197 [3]

So far, there are no negative findings on Serpent and Twofish, however, the security of those block ciphers has been examined much less intensively.

The best known attacks against AES that do not require related-keys achieve only a slight advantage over generic attacks.

Curent situation

- Smals has cryptographic recommendations.
- Based on recommendations German BSI
- Helps us to anticipate change
- Next step: express as code

Crypto policy as code - AES-128-GCM

CBOM model

```
"components": [
  {
   "type": "cryptographic-asset",
   "name": "AES-128-GCM",
   "cryptoProperties": {
    "assetType": "algorithm",
    "algorithmProperties": {
     "primitive": "ae",
     "parameterSetIdentifier": "128",
     "mode": "gcm",
     "executionEnvironment": "software-plain-ram",
     "implementationPlatform": "x86_64",
     "certificationLevel": [ "none" ],
     "cryptoFunctions": [ "keygen", "encrypt", "decrypt", "tag" ],
     "classicalSecurityLevel": 128,
     "nistQuantumSecurityLevel": 1
    },
    "oid": "2.16.840.1.101.3.4.1.6"
   }
  }
]
```

Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as AES192 (exhaustive key search)
V	At least as hard to break as AES256 (exhaustive key search)

Recommendation

```
"components": [
  {
   "type": "cryptographic-asset",
   "name": "AES-128-GCM",
   "cryptoProperties": {
    "assetType": "algorithm",
    "algorithmProperties": {
     "primitive": "ae"
    },
   "recommendation": {
     "level": "recommended",
     "standardization": ["FIPS PUB 197 (2001)", "NIST SP 800-38D (2007)"],
     "conditions": [
       "For initialization vectors, a bit length of 96 bits is recommended.",
       "A key change is required after at most 2^32 calls of the authenticated
                                                                    within the lifetime of a key.",
                                                                    ",
                                                                    th IV = j, we never take a
   }
  }
]
```

Design principles

- **Maximize CBOM compatibility**
  - Keep structure
  - Keep names and identifiers
  - No information-duplication
- **Recommendations as guide**
  - Include additional information, s.a., conditions of use

Deviations

Ensure in a controlled, managed way availability for users and compatibility with systems

```
{
 "deviations": [
  {
   "scope": {
    "type": "application",
    "name": "Quatro",
    "info": "https://...",
    "module": "…"
   },
   "approval": {
    "approvalDate": "01/05/2023",
    "from": "01/05/2025",
    "until": "31/12/2025",
    "reference": "…",
    "justification": "Ensure availability for …"
   },
   "assessment": {
    "risk": "low",
    "impact": " low",
    "probability": "medium",
    "data": "…",
    "explanation": "..."
   },
```

```
"allow": {
   "type": "cryptographic-asset",
   "name": "TLSv1.3",
   "cryptoProperties": {
    "oid": "1.3.18.0.2.32.111",
    "assetType": "protocol",
    "protocolProperties": {
     "type": "tls",
     "version": "1.2",
     "cipherSuites": [
      {
       "name": "TLS_DH_RSA_WITH_AES_128_CBC_SHA256",
       "identifiers": [
        "0x00",
        "0x3F"
       ]
      }
     ]
   }
  }
 }
]
}
```

CBOM Model

Smals
ICT for society

Crypto policy as code

Recommendations as Code

Deviations as Code

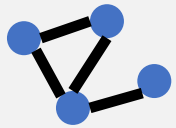
Inventory as Code

Up-to-date PDFs

Auto-generated config files

REST API (E.g., browser)

Bespoke query



Graph analytics

RECOMMENDATIONS + EXCEPTIONS + INVENTORY AS CODE = A POWERFUL COMBINATION

mals for society

EVERYTHING AS CODE

ENABLES A HIGH DEGREE OF AUTOMATION AND INSIGHT

SMALS RESEARCH IS WORKING ON THIS

Smals
ICT for society

Agenda

- Why & What?
- In the Public Sector
- Crypto Inventory
- Crypto Policy as Code
- **Cryptography in Hybrid Mode**
- Outlook & Challenges
- Wrapping Up

Smals
ICT for society

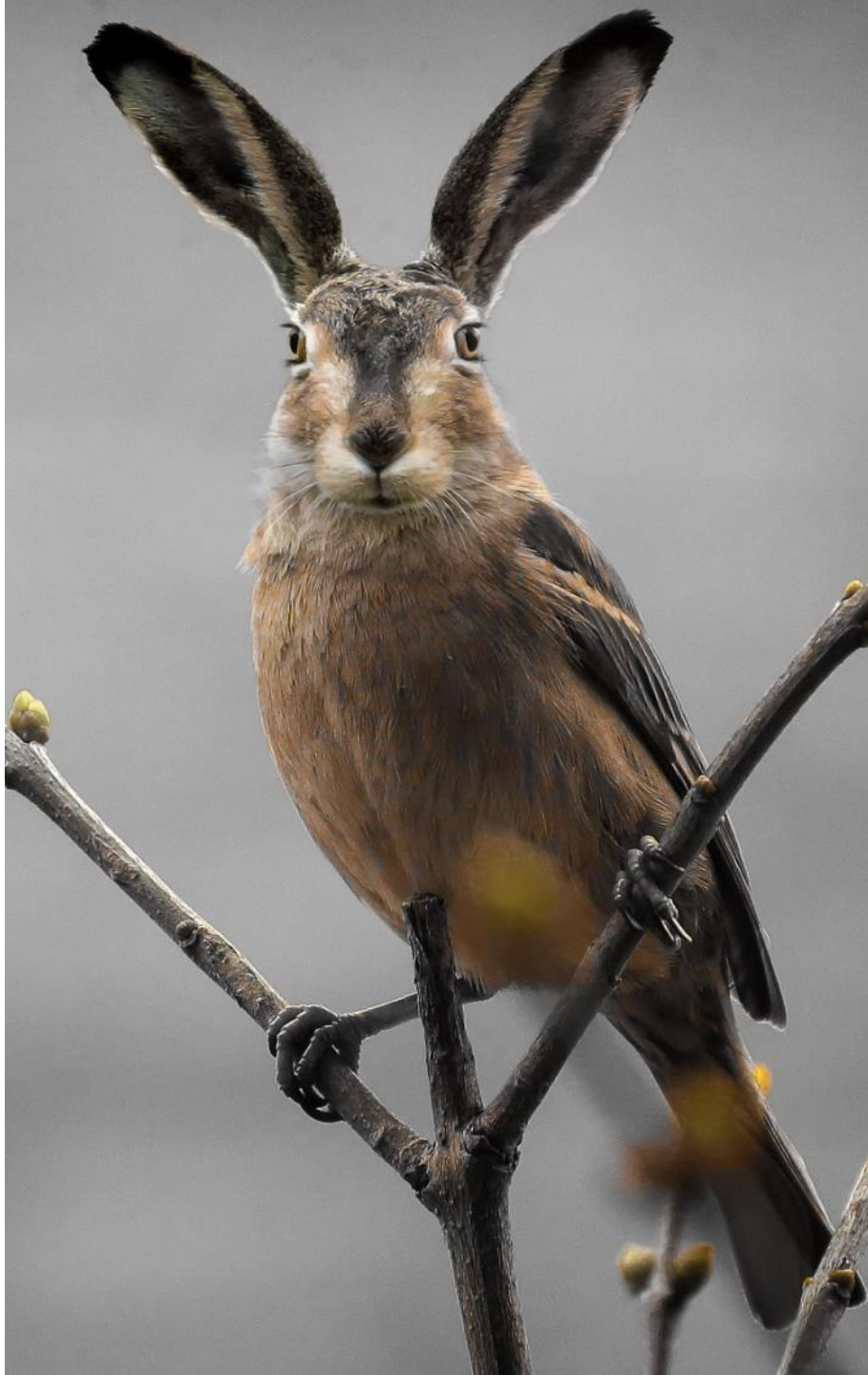
Transitional period in Hybrid Mode

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).*

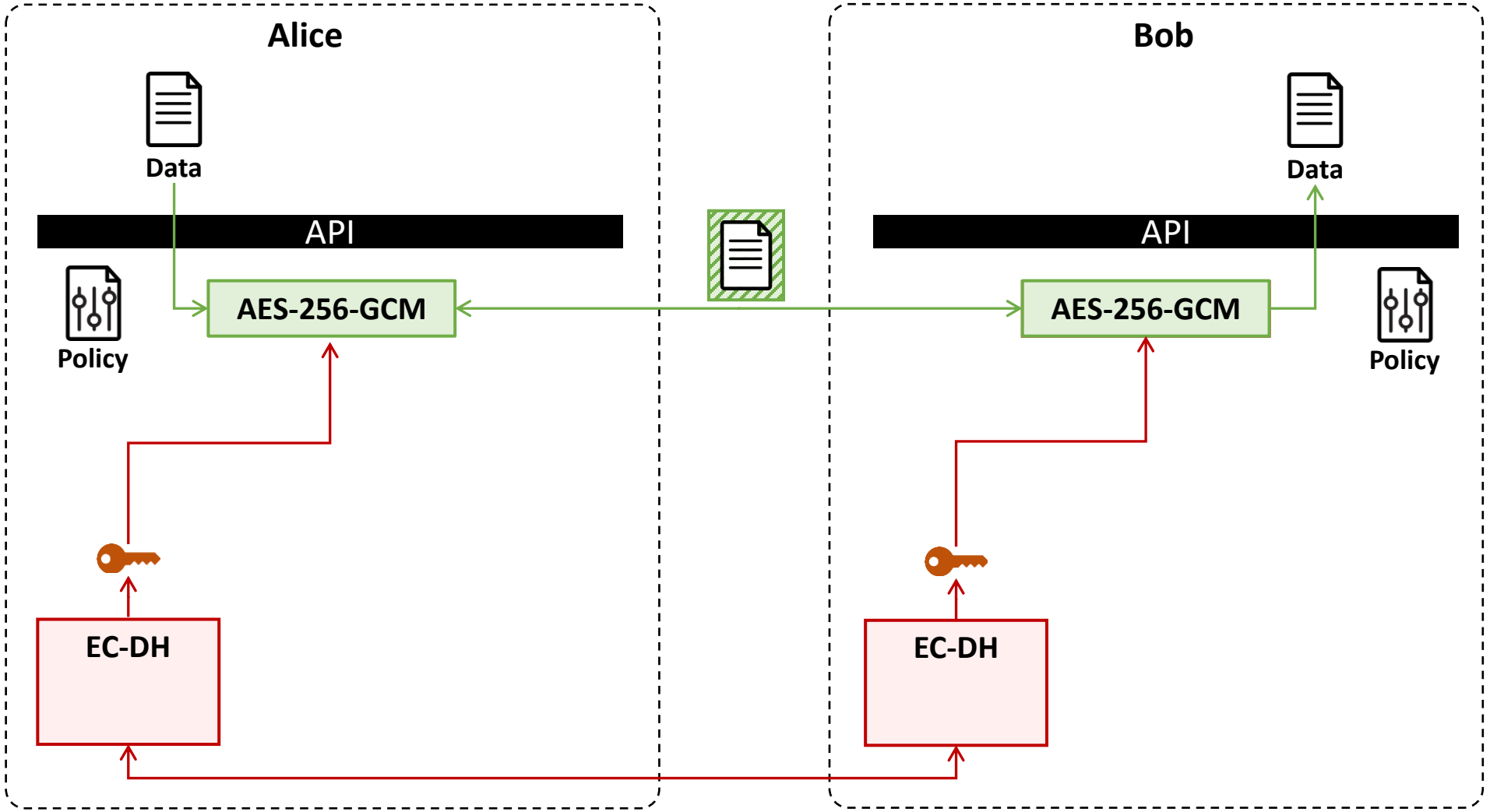
Quantum-safe cryptography –fundamentals, current developments and recommendations. October 2022

→ **EVEN MORE MIGRATIONS!**



Key agreement with classical cryptography

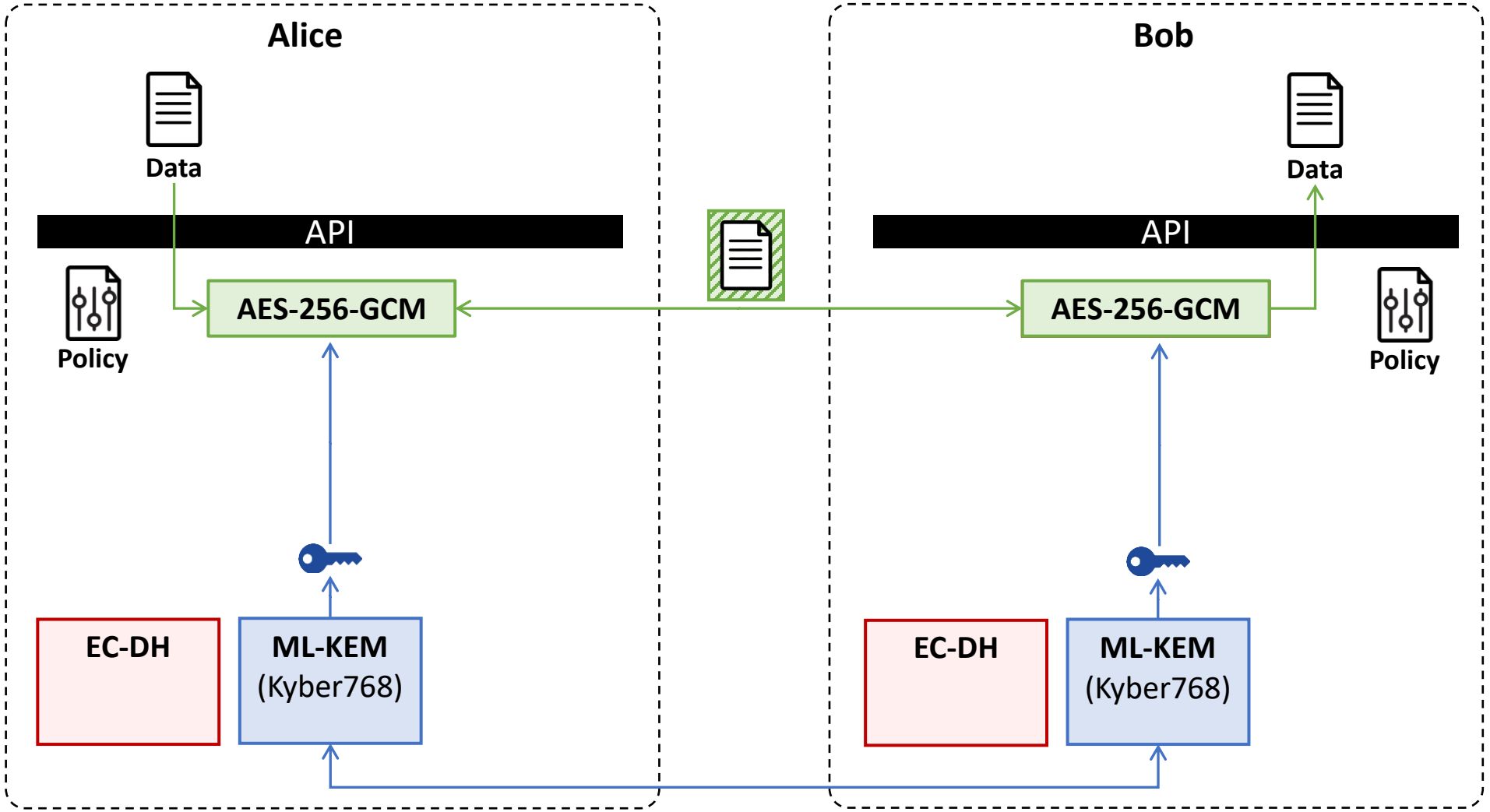
Highly trusted, but quantum vulnerable



Smals
ICT for society

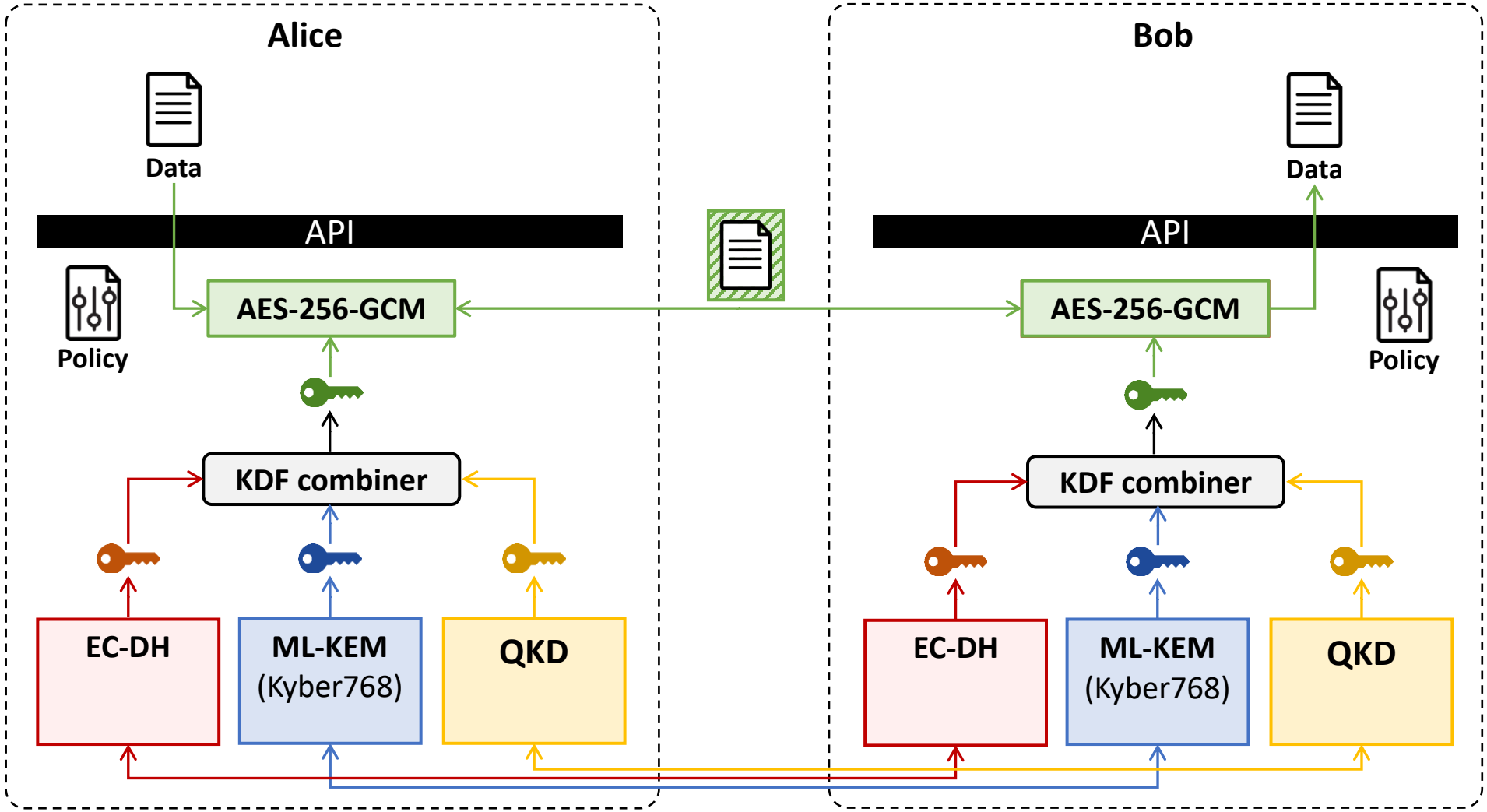
Key agreement with PQC (Post-Quantum Cryptography)

Quantum resistant, but not yet sufficiently trusted



Smals
ICT for society

Key agreement – Hybrid mode with Crypto Agility



HYBRID MODE HELPS NAVIGATING CRYPTO MIGRATION TRANSITION PERIODS

CRYPTO AGILITY FACILITATES HYBRID MODE

ALREADY IMPLEMENTED BY VENDORS

Smals ICT for society

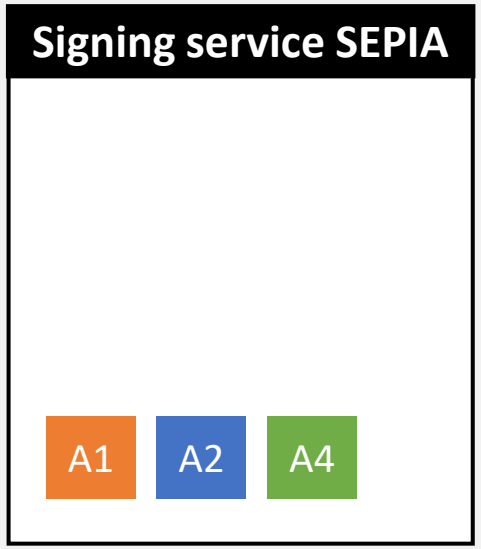
Agenda

- Why & What?
- In the Public Sector
- Crypto Inventory
- Crypto Policy as Code
- Cryptography in Hybrid Mode
- **Outlook & Challenges**
- Wrapping Up

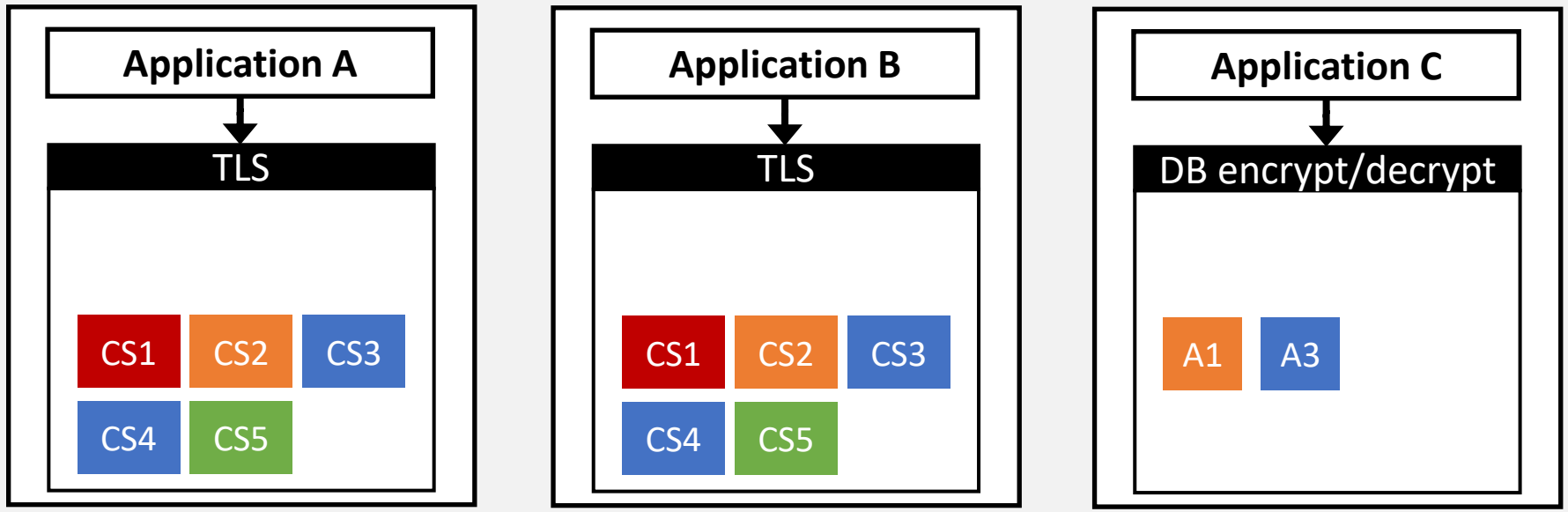
Smals
ICT for society

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

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 (alg.)
- 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

(NO OFFICIAL ROADMAPS AVAILABLE YET)

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

Increased Overhead

Digital signature algorithms

	Quantum Resistant	Public key size (in bytes)	Signature size (in bytes)	CPU time - sign (lower is better)	CPU time- verify (lower is better)
Ed25519 (Elliptic curves)	No	32	64	1 (baseline)	1 (baseline)
RSA-2048	No	256	256	70	0,3
ML-DSA-44 (Dilitium2)	Yes	1 312	2 420	4,8	0,5
FN-DSA-512 (Falcon512)	Yes	897	666	8	0,5
SLH-DSA-128s (SPHINCS+128s)	Yes	32	7 856	8 000	2,8
SLH-DSA-128f (SPHINCS+128f)	Yes	32	17 088	550	7

Impact

PKIs / X.509 certs

Contains public key and signature

Handshake

TLS handshake: + 15 KB

Smartcards

E.g. Belgian eID Limited resources

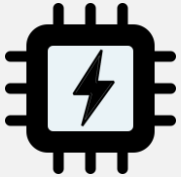
IoT

Limited resources & bandwidth

QR codes

Encode signature in QR code

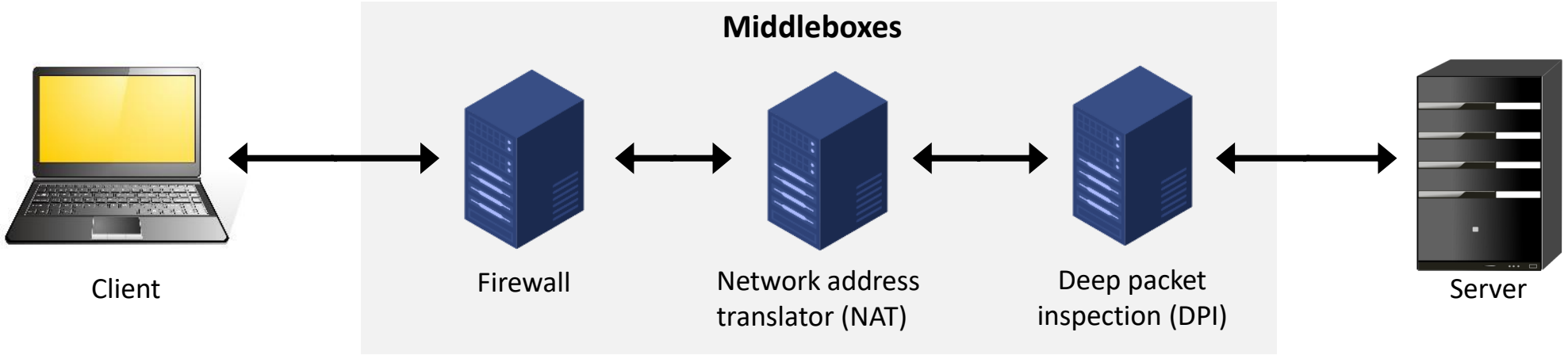
Hardware



Acceleration, resources

Protocol Ossification

Loss of flexibility, extensibility and evolvability of network protocols.



Slow adoption by OS Kernel

Middlebox interference

Protocols implemented in hardware

PROTOCOL OSSIFICATION HINDERS CRYPTO AGILITY

IMPORTANCE OF TESTING BEFORE MIGRATION IN LIFE PRODUCTION ENVIRONMENT

Smals ICT for society

Agenda

- Why & What?
- In the Public Sector
- Crypto Inventory
- Crypto Policy as Code
- Cryptography in Hybrid Mode
- Outlook & Challenges
- **Wrapping Up**

Smals
ICT for society

Advice by the BSI

If I could give companies and organisations three pieces of advice as they prepare for quantum safety, they would be:

- **Include the threat in your risk management system**
- **Create a crypto inventory**
- **Implement and use crypto-agility**

Dr. Gerhard Schabhüser
Vice President, BSI

Bundesamt
für Sicherheit in der
Informationstechnik

Crypto inventory

Start simple, with a focus on your most valuable assets & external communication. Consolidate what you already have.

Crypto agility

- In-house development → focus on cases that may save money
- Stimulate your vendors / suppliers! What are their plans?

Smals
ICT for society

Source: KPMG, BSI. *Market Survey on Cryptography and Quantum Computing*. 22/08/2023.

Recommendations by the NSA

"IAD [Defensive branch of NSA] will initiate a transition to quantum resistant algorithms in the not-too-distant future. […] For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition."

NAS-CSS. Commercial National Security Algorithm Suite. 19 August 2015.

Smals ICT for society

Some more advice on quantum-readiness

Fear is a bad guide

We are not sure if quantum computers will ever be strong enough to break classical public-key cryptography (for sure not in the next 5 years)
Nevertheless, we should mitigate the risk.

Have your priorities right

- **Focus on (external) communication**
  Harvest now decrypt later attack: Intercepted encrypted communication is decrypted later
- **Focus on most sensitive assets**

Prepare to go with the flow

Public-key crypto often relies on certificates.
Certificate authorities will determine when to introduce new and phase-out old crypto.
Be sure to be ready for this!

Smals
ICT for society

Some more advice on cryptographic maturity

Improve cryptography asset management

- Assumption in the past: "*RSA and elliptic curve cryptography rock-solid*" → Historical neglect
- Crypto inventory / policy / agility → *No-regret moves*

Think long-term

Crypto inventory and crypto agility prevent further expenses in the long run. They are long-term investments → Insight, compliance, quick vulnerability response

Don't get stuck in the past. Focus on the future

- Don't waste resources on refactoring legacy that reaches end-of-life in a few years
- Embrace crypto agility as design principle for new applications

Smals ICT for society

Quantum readiness & crypto agility @ Smals

- **Central focus Smals Research**
  Post-quantum cryptography, Crypto inventory, Crypto agility and crypto policy as code
- **Smals is already taking initiatives**
  Sepia, Middleware key vault, automated certificate management
- **Plan of action Smals**
  Coming later this year
  Awareness, inventory, risk analysis, next steps, …
- **We are early!**

Smals
ICT for society

In summary - Crypto Migrations

Cryptography

- Is everywhere → Need for secure cryptography
- Public-key cryptography required for, among others, key-exchange (communication), authentication and digital signatures
- Classical public-key cryptography based mainly on RSA and elliptic curves

Cryptography under attack

- Future quantum computers may break classical public-key cryptography
- Also other threats, such as cryptanalysis and side-channel attacks (cfr. SIKE, a NIST post-quantum finalist, broken in 2022)
- Focus on communication, due to *harvest now, decrypt later attack.* Encrypted data intercepted today may be decryptable in the future

Cryptography migrations

- Multiple migrations in the past
  → slow, cumbersome & expensive (5-15 years)
- Most likely, multiple migrations in the future
- **Need to facilitate migrations**
  → make applications & infrastructure crypto agile!

Smals
ICT for society

In summary – Crypto Agility

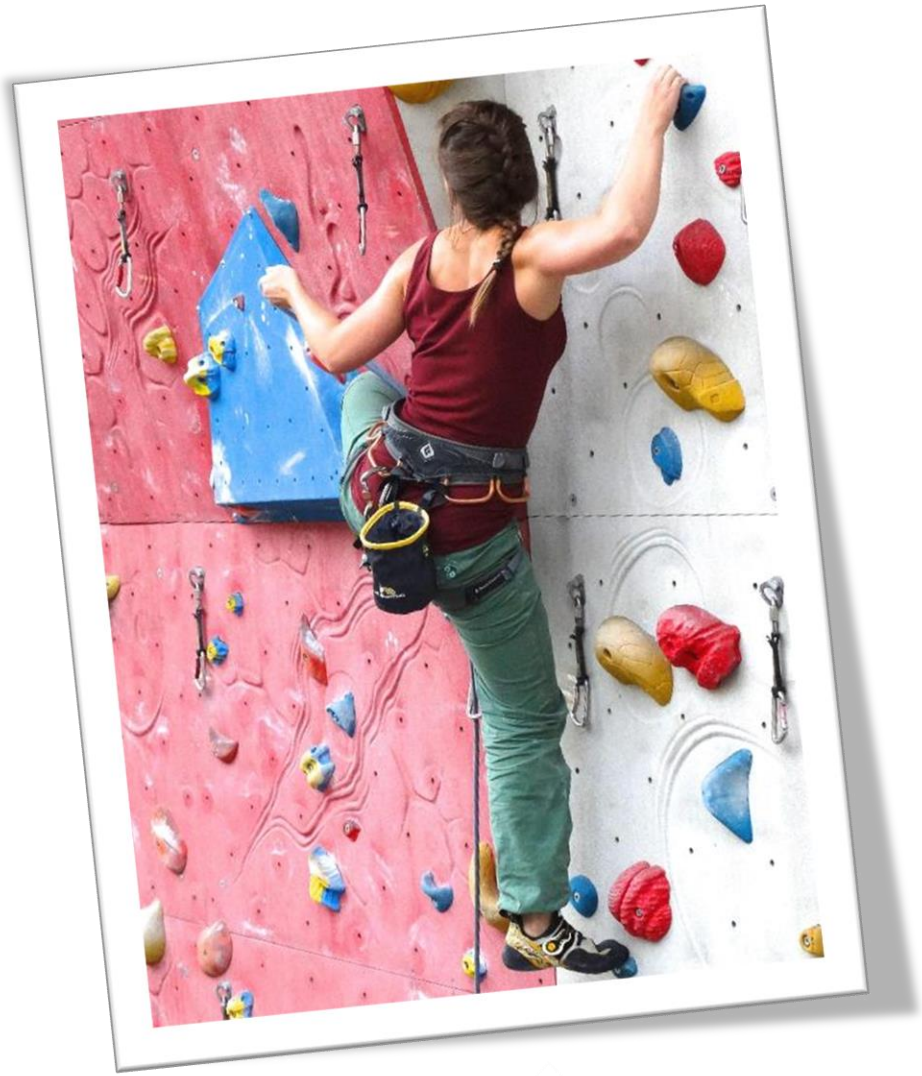
Properties

- Applications no longer embed crypto logic, but instead consume cryptography by using APIs that hide crypto details
- Multiple cryptographic functions supported simultaneously
- Systems can choose/negotiate in real-time which ones to use
- New cryptographic functions can be easily added and removed
- Without affecting system availability

Cryptographic functions: algorithms, implementations, cipher suites, hardware, …

History

- **Cryptographic *protocol* agility** already adopted, for instance by TLS clients.
- **Crypto agility** is on the level of a broader infrastructure
- Term only recently more widely adopted, due to the quantum threat
  → Still al lot of work to be done by industry
- Quantum resistant and/or crypto agile systems are still rare
  Smals is early!



Smals
ICT for society

In summary – Lessons

Cryptographic maturity

- Crypto agility requires a
  - Crypto inventory: what crypto is used where?
  - Crypto policy: what crypto is recommended, insecure, …

→ Agility / inventory / policy improve organisation's crypto maturity

Everything as code

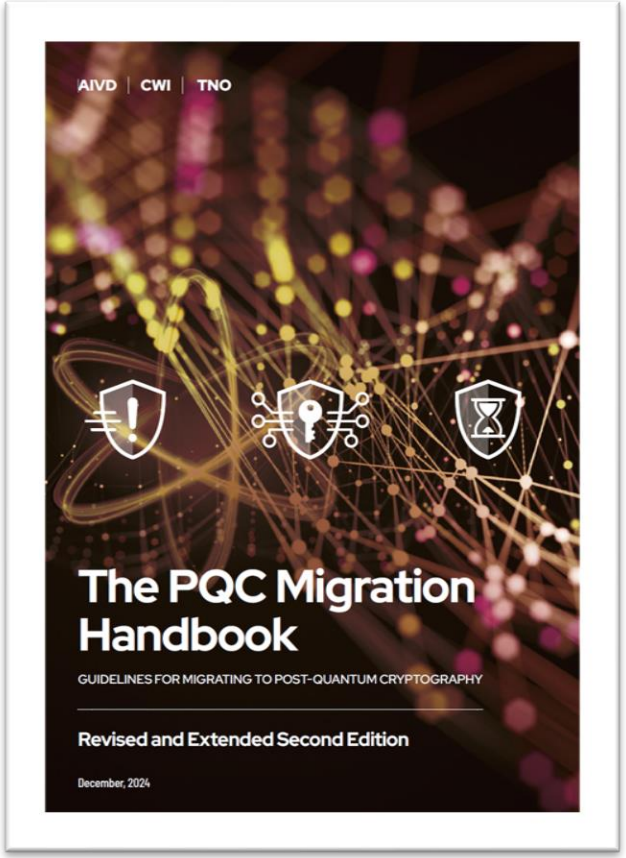
- Crypto inventory as code & policy as code enable automated processes and management of complexity related to cryptography asset management
- Standards required for interoperability: CBOM (Cryptography Bill Of Materials) to express crypto inventory. Likely adopted by industry
- Smals Research is working on CBOM-inspired crypto policy as code

Lessons

- Cryptographic agility implies centralization and automated processes
- Importance of testing before migration in life production environment
- Cryptographic agility is a journey (No adopted maturity model yet)

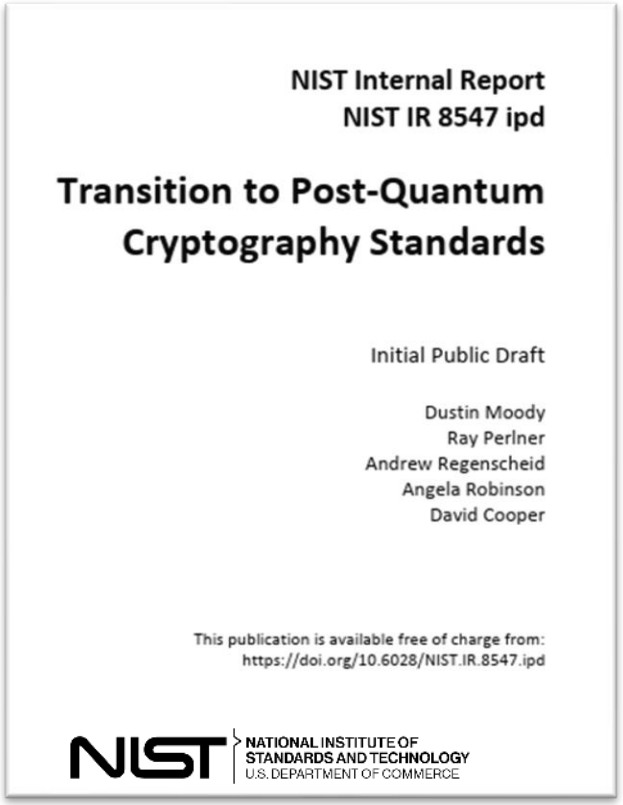
Smals
ICT for society

Crypto migration handbook (AIVD)



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

NIST report


NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8547.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

Articles Smals Research

www.smalsresearch.be/tag/quantum-computing/

Smals
ICT for society

BECOME A CHEETAH: EMBRACE CRYPTO AGILITY

Smals
ICT for society

Thanks for your attention!

Feedback / questions / discussions welcome!

Please share your feedback with us!

kristof.verslype@smals.be

+32(0)2 7875376

linkedin.com/in/verslype

www.smals.be

www.smalsresearch.be