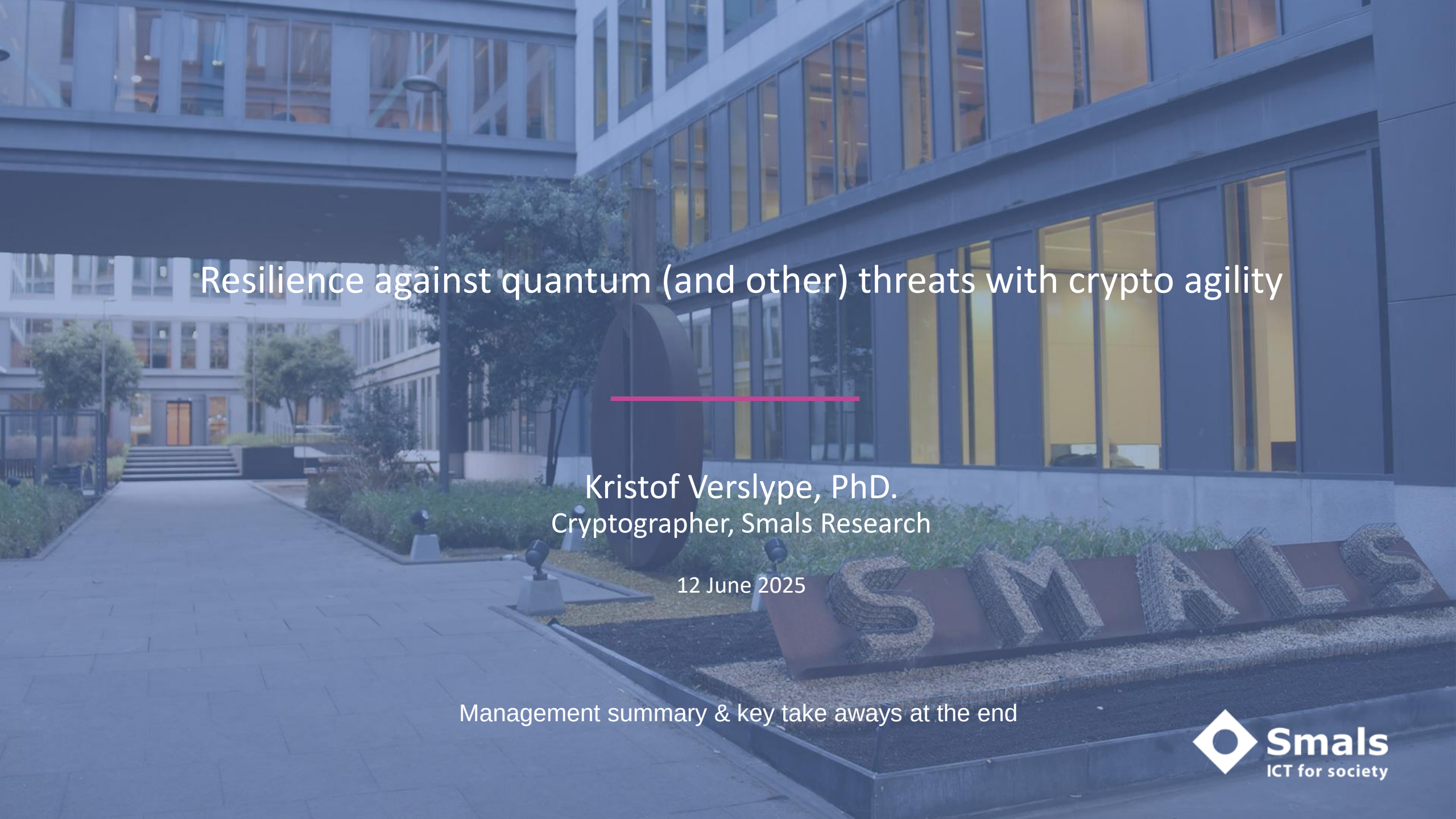


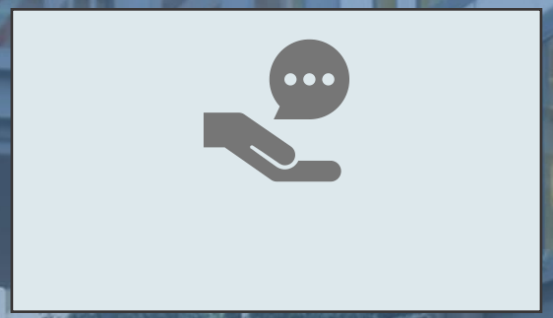
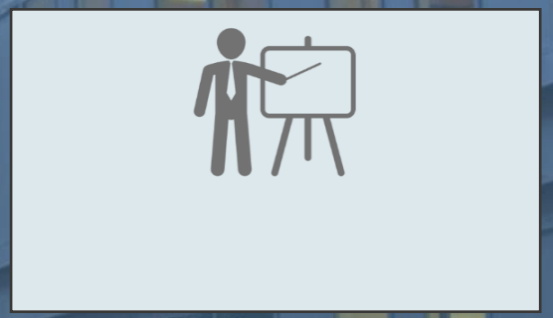
Resilience against quantum (and other) threats with crypto agility

Kristof Verslype, PhD.
Cryptographer, Smals Research

12 June 2025

Management summary & key take aways at the end

Smals
ICT for society


GraphRAG

Agentic AI

Native Graph ML

Code security assistants

Knowledge Graphs

Agent-Computer Interaction

Guardrails & Evaluations for RAG

Administrative Digital Twins

Rules and code generation

Semantic Search

Metadata Management Solutions

Zero-Knowledge proofs

Legacy code & AI

Confidential cross-institutional collaboration

Neuro-symbolic AI

Verifiable Credentials & EU Digital Wallet

Dark & Deep Web

Smals
ICT for society

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

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

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



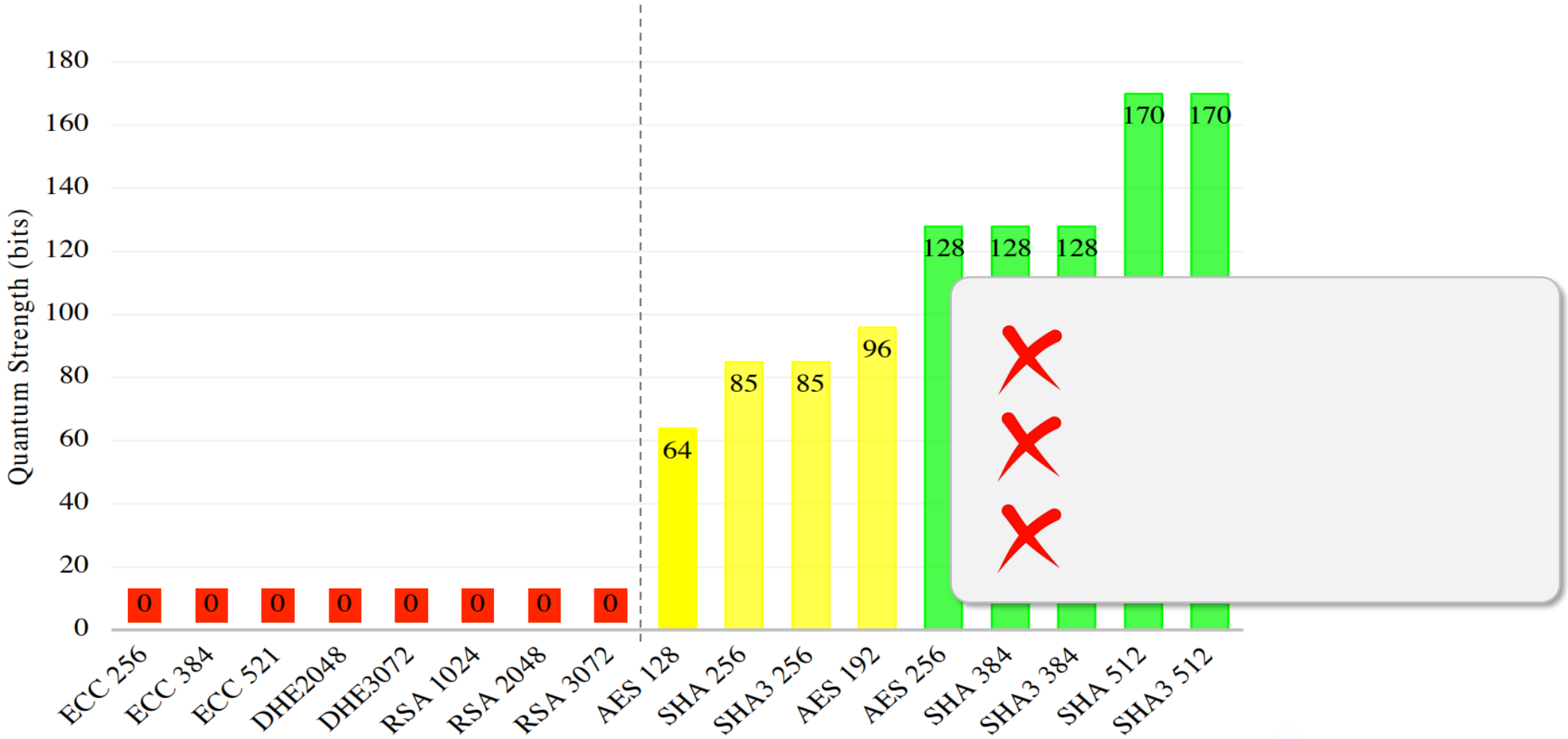




“To ensure an acceptable level of readiness, we recommend that [the most sensitive use cases] should be protected against ‘store now, decrypt later’ attacks as soon as possible, latest by the end of 2030.”

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

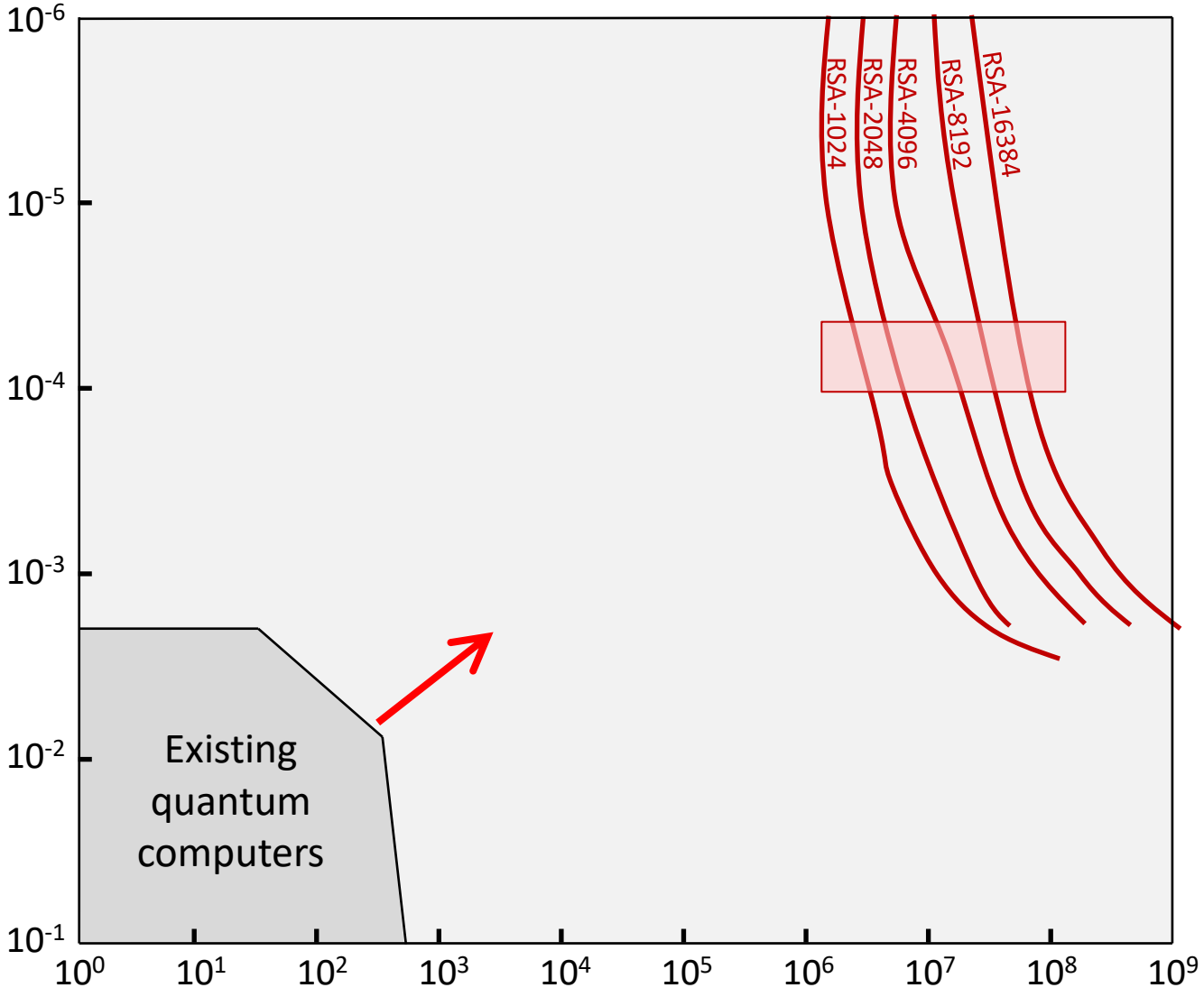
Smals
ICT for society



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*.



"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

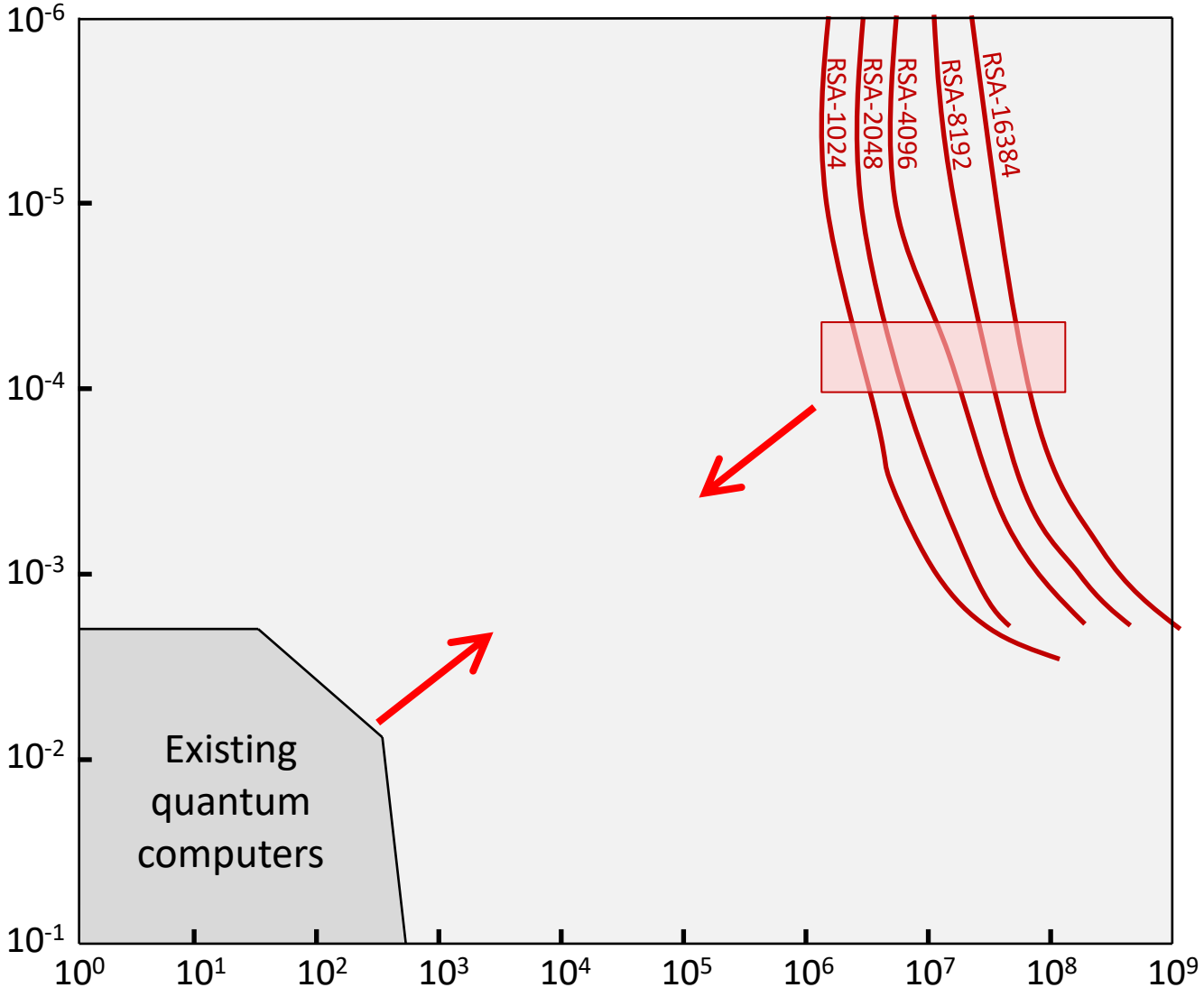
May 28, 2025

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 [illegible] compared to Chevignard+Fouque+Schrottenloher 2024. [illegible] Toffoli count by over 100× compared to Chevignard+Fouque+Schrottenloher 2024.

https://arxiv.org/pdf/2505.15917

Smals ICT for society



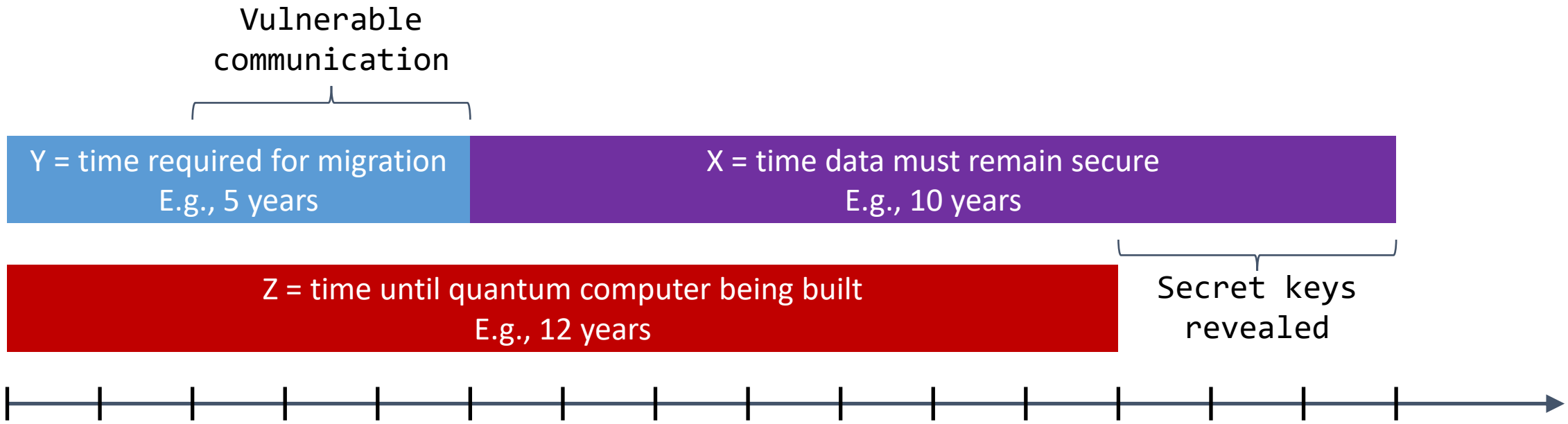
"We need Moore's-law type scaling for quantum computers to ever be useful"

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

Encrypted communication intercepted today can be encrypted in the future



if X + Y > Z
then Sensitive data exposed

Harvest now, decrypt later

→ Forced to think a long time in advance!
→ Primarily key-agreement schemes (data in transit)
→

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

“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)

- Increasing computing power
-
- 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

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.

POST-QUANTUM CRYPTOGRA…

“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)

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

Applies on modern and post-quantum cryptography

Smals
ICT for society

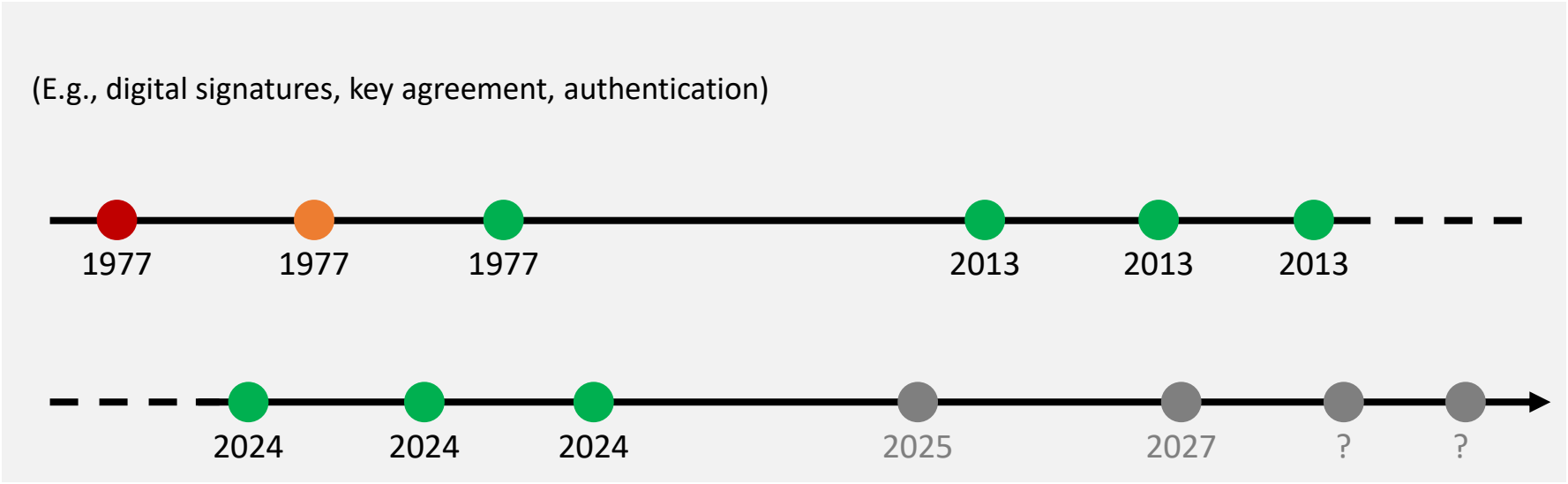
(E.g., digital signatures, key agreement, authentication)

MULTIPLE CRYPTO MIGRATIONS IN THE PAST

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

Smals
ICT for society

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



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

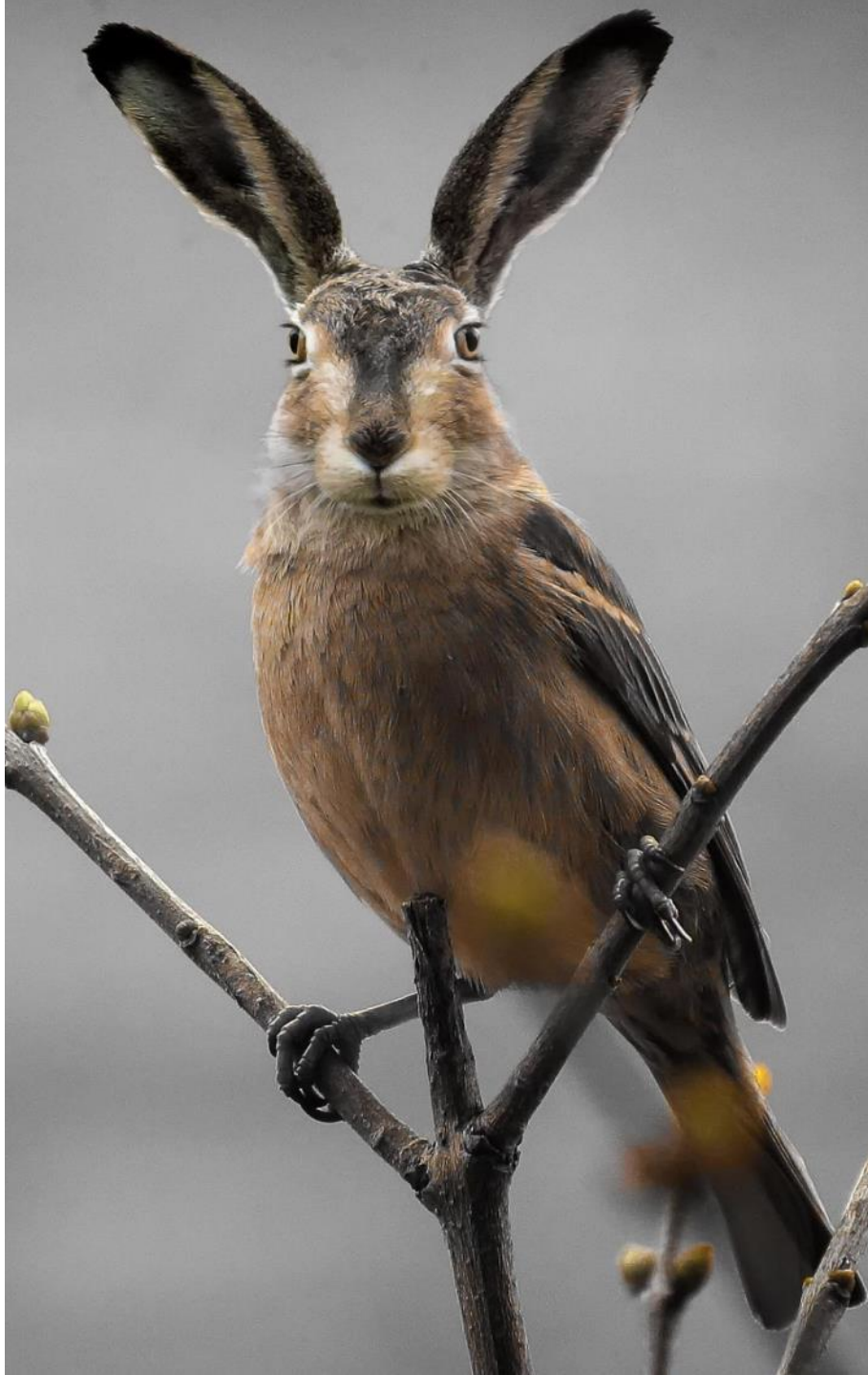
BECOMING QUANTUM-READY MAY NOT BE A ONE-TIME SHOT

Smals ICT for society

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



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

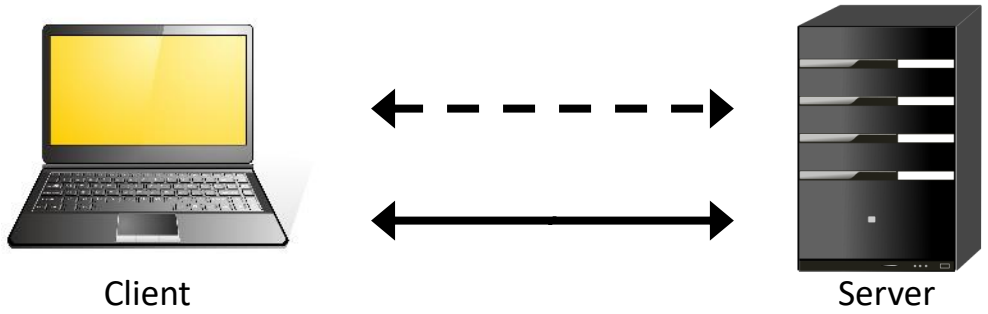
Cryptographic algorithms have a life cycle
Recommended → Secure → Phase out → Insecure

Cryptography: Assets that need to be managed

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)



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

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

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 to application / service

Cryptographic functions

and
Cryptographic functions

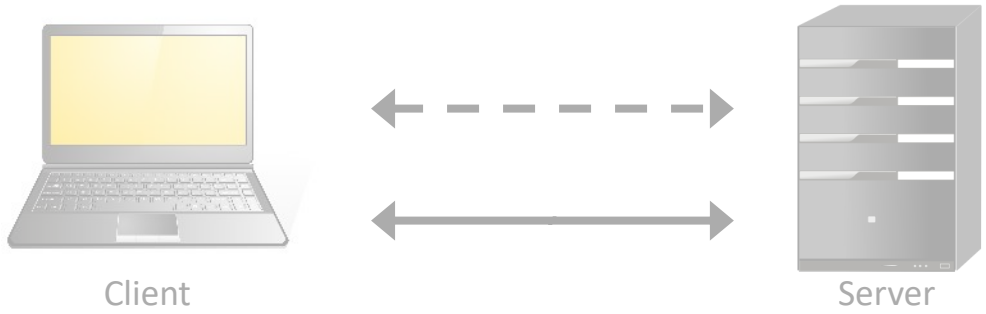
Cryptographic functions: *Hardware, software, firmware, algorithms, parameters, …*

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)



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

TLS_SM4_GCM_SM3
TLS_AES_128_CCM_SHA256
TLS_AES_128_GCM_SHA256

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1205_SHA256

Recommended
Secure
Phase out

Cryptographic service offers to application / service

Cryptographic functions

and
Cryptographic functions

–
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

Why & What?

In the Public Sector

Crypto Inventory

Crypto Policy as Code

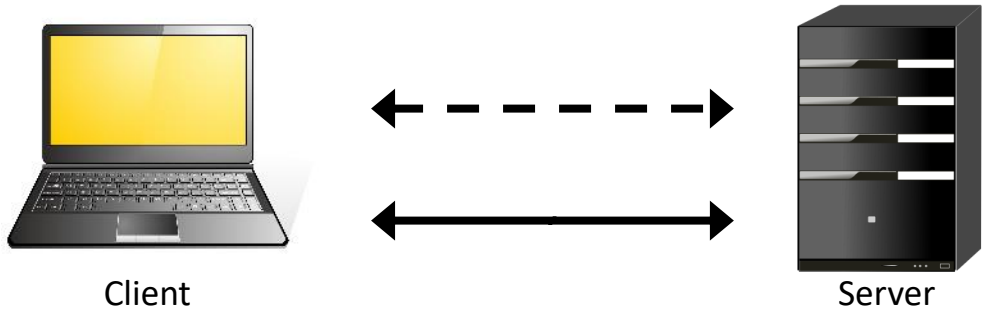
Cryptography in Hybrid Mode

Outlook & Challenges

Wrapping Up

Smals
ICT for society

Transport Layer Security (TLS)



Agree on TLS version
Agree on cipher suite
Authenticate
Generate shared session keys

TLS_SM4_GCM_SM3
TLS_AES_128_CCM_SHA256

TLS_AES_256_GCM_SHA384
TLS_AES_128_CCM_8_SHA256
TLS_CHACHA20_POLY1205_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

- 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

Smals
ICT for society

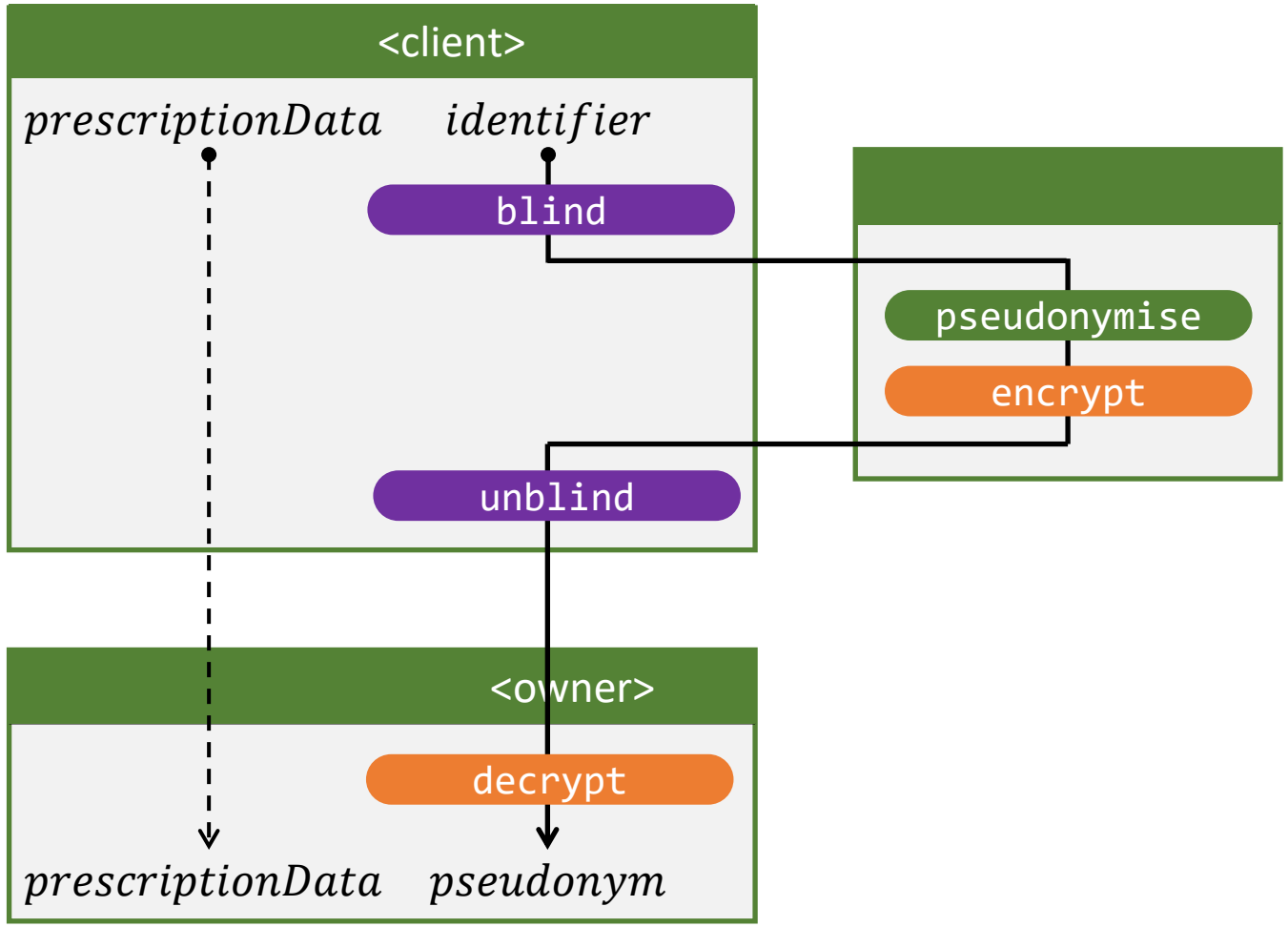
Runner-up for *Best Cybersecurity Innovation Europe* award issued by Cybersec Europe

- ❖ Doctor only sees identifiers
- ❖ Backend only sees pseudonyms
- ❖ Pseudon. service sees neither

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

- ❖ No extra keys required
- ❖ Relatively simple implementation

Doctor requests *Prescription service* to register medical prescription



How quantum resistant is this solution?

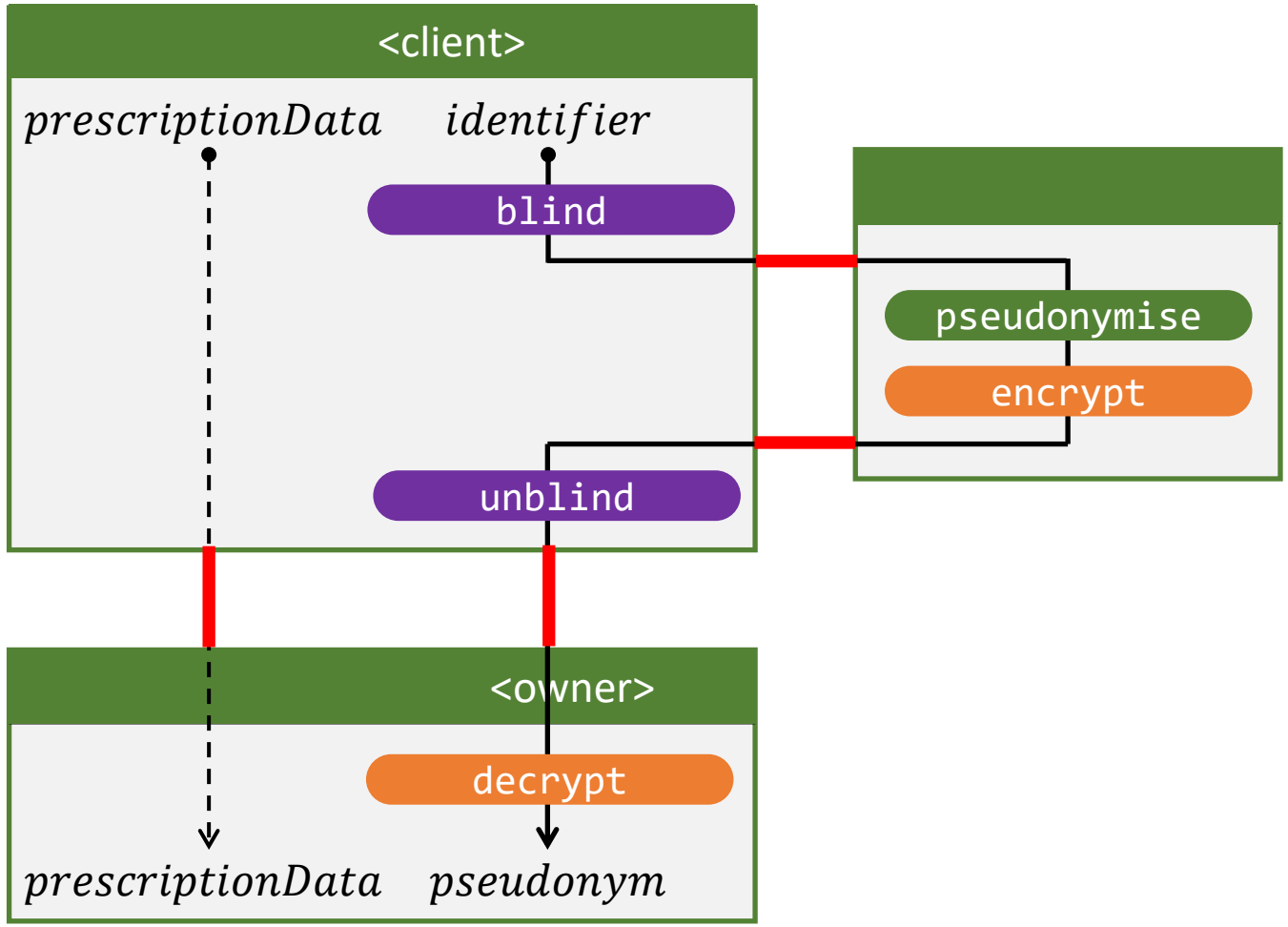
Smals ICT for society

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

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

- 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

Doctor requests *Prescription service* to register medical prescription



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

Smals ICT for society

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

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

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

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

- 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

Why & What?

In the Public Sector

Crypto Inventory

Crypto Policy as Code

Cryptography in Hybrid Mode

Outlook & Challenges

Wrapping Up

Smals
ICT for society

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

n

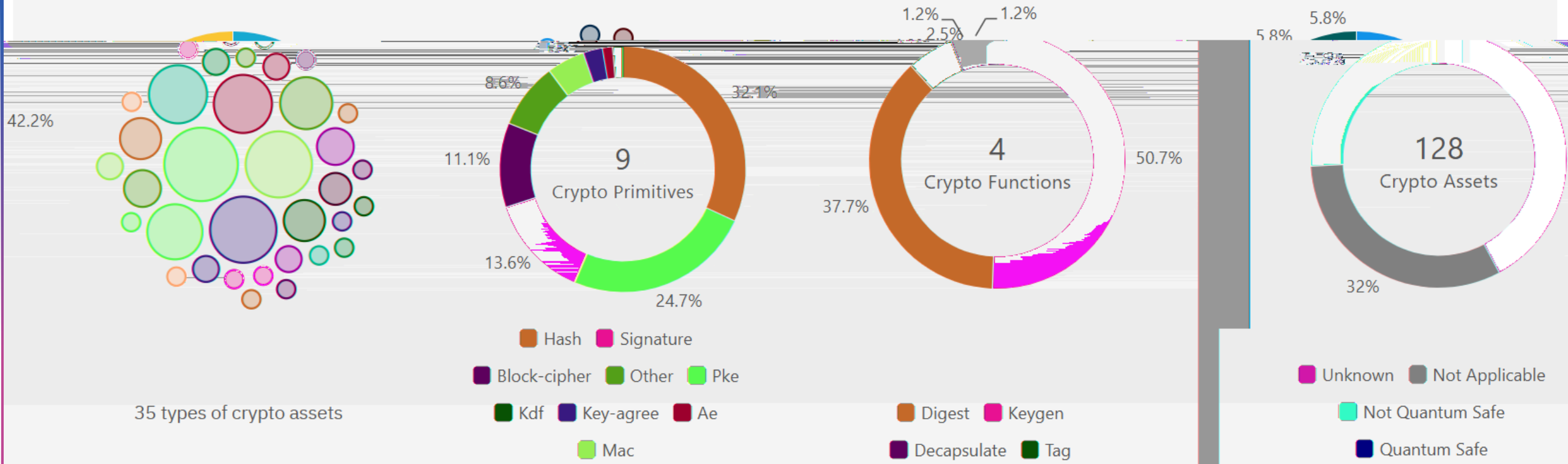
github.com/keycloak/keycloak

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

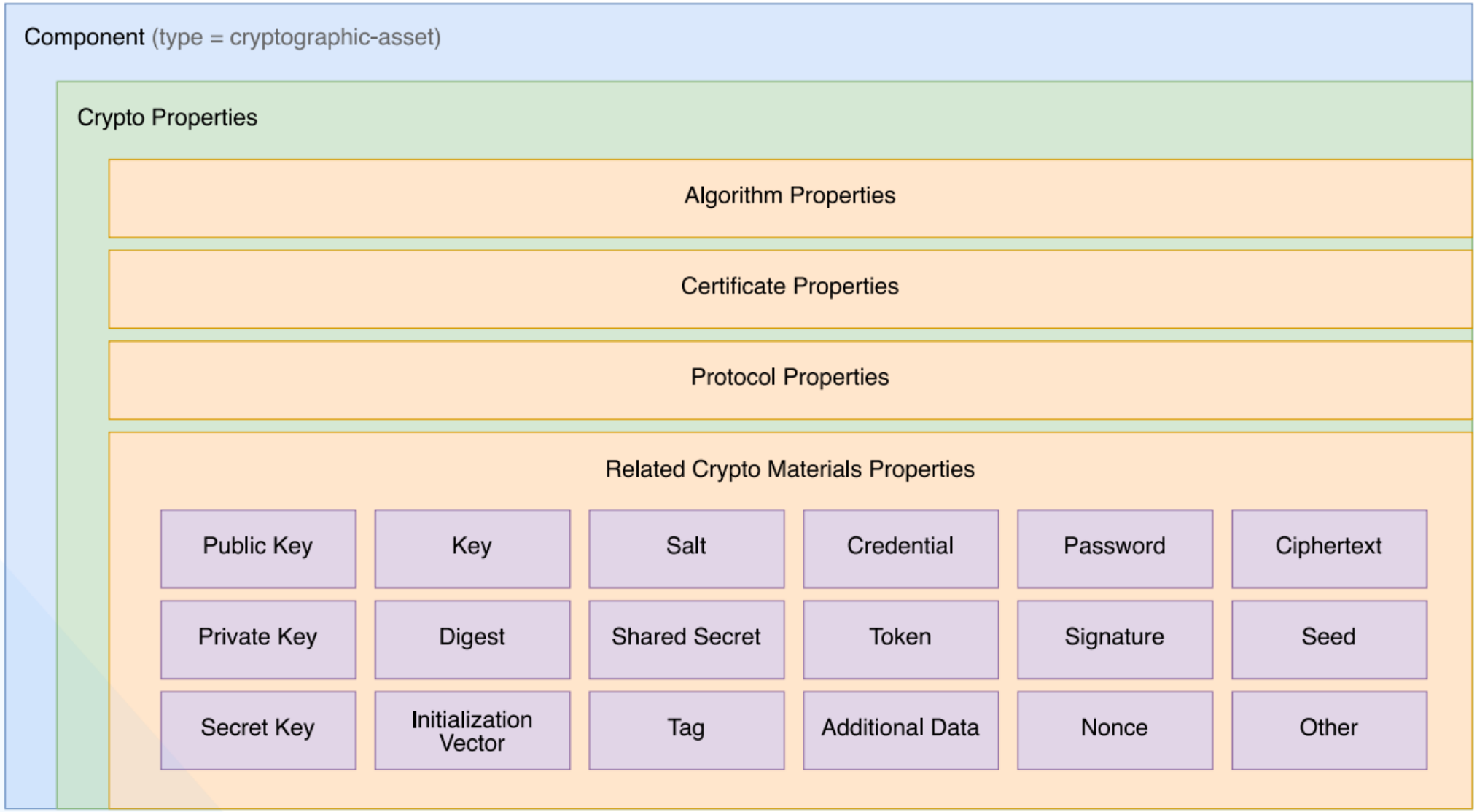
Download CBOM

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

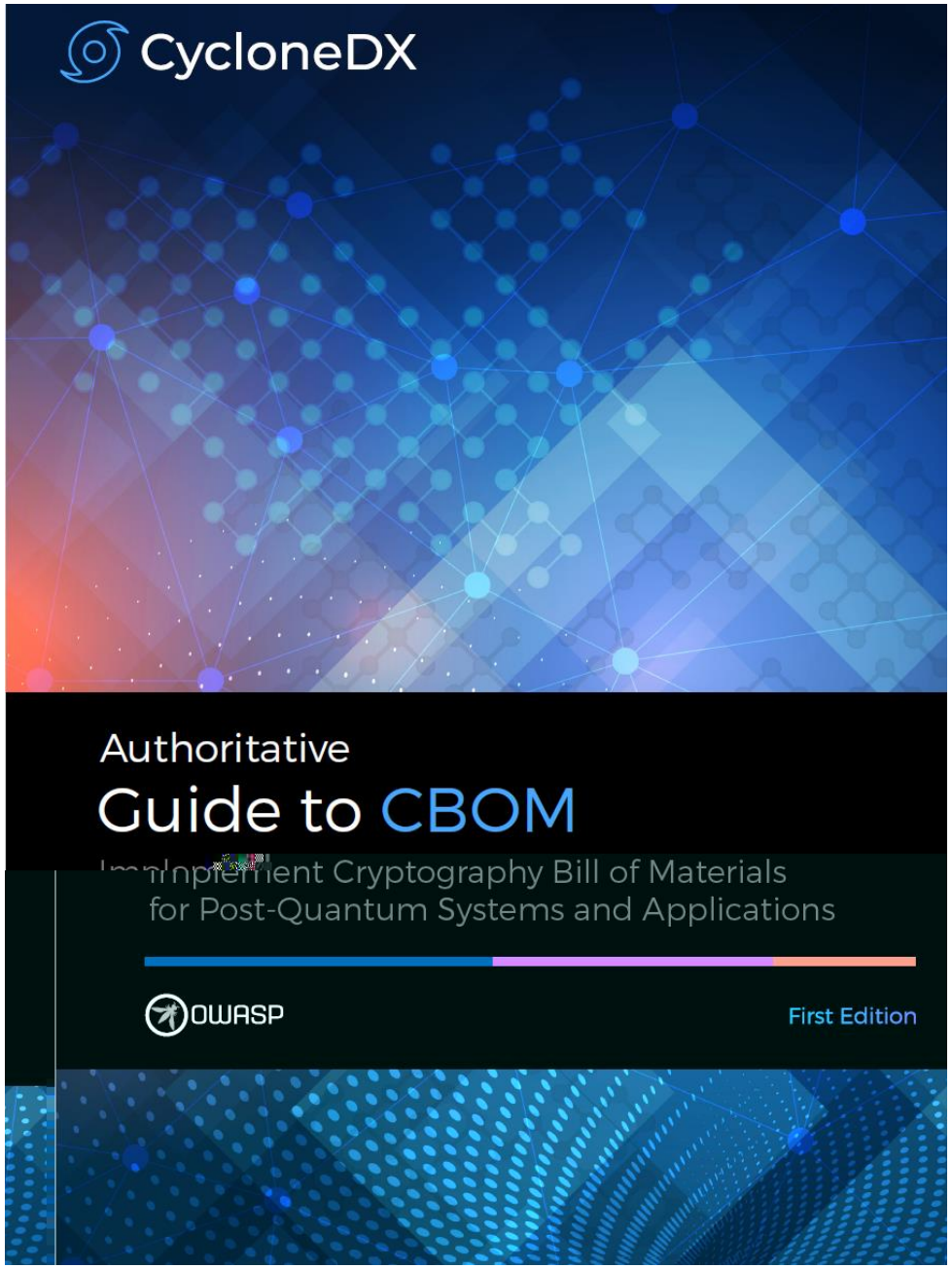
Items per page: 10 | 11-20 of 128 items | 2 of 13 pages

```
{
    "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



mals
ICT for society



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

Smals
ICT for society

- External network
- Internal network

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

- In-house applications
- Certificate management

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

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

Why & What?

In The Public Sector

Crypto Inventory

Crypto Policy as Code

Cryptography in Hybrid Mode

Outlook & Challenges

Wrapping Up

Smals
ICT for society

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 me

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

```
"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"
   }
  }
]
```

```
"components": [
  {
   "type": "cryptographic-asset",
   "name": "AES-128-GCM",
   "cryptoProperties": {
    "assetType": "algorithm",
    "algorithmProperties": {
     "primitive": "ae"
    },

                    [

  }
]
```

- Keep structure
  Keep names and identifiers
  No information-duplication
- Include additional information, s.a., conditions of use

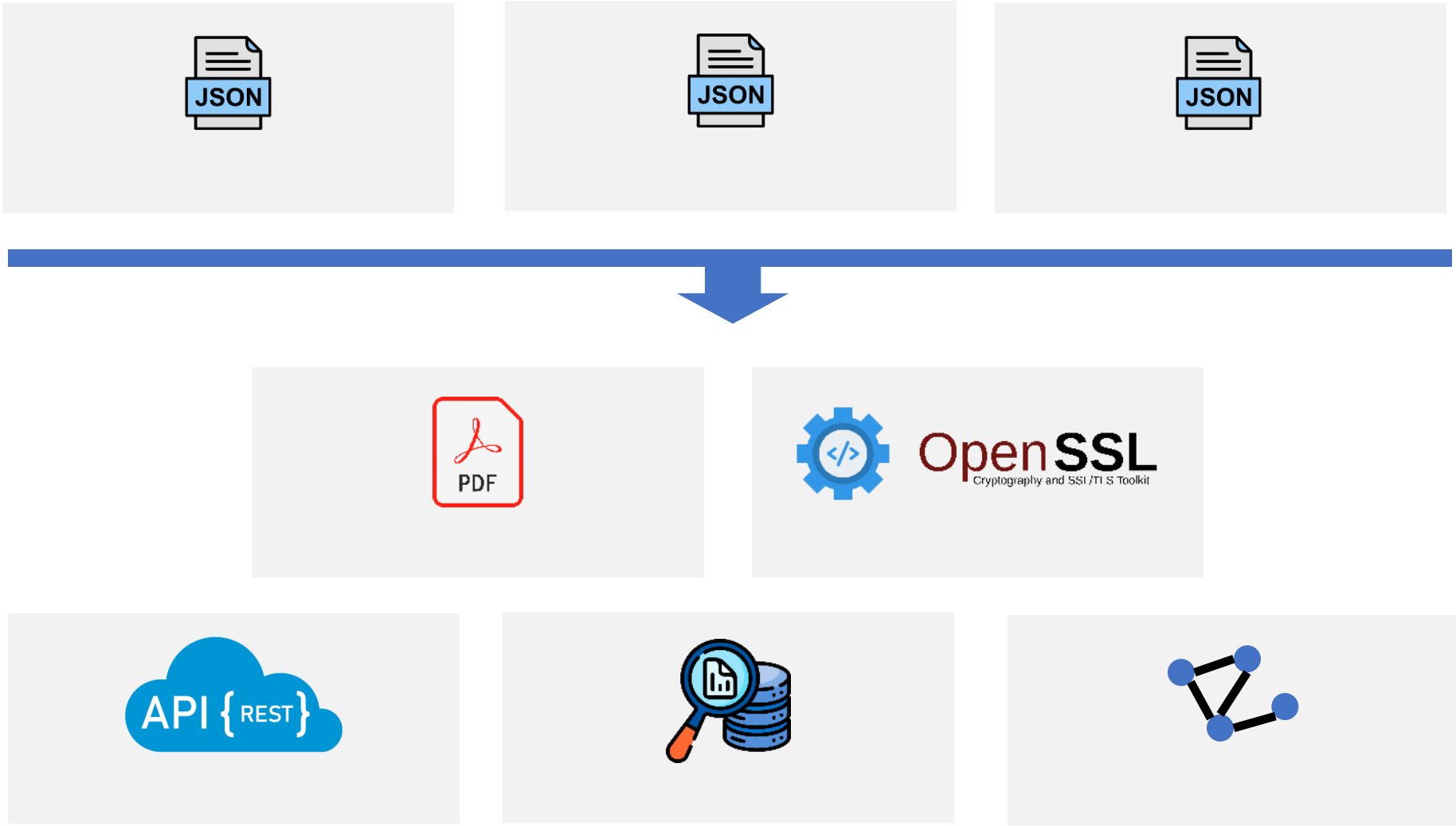
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as AES192 (exhaustive key search)
V	At least as hard to break as AES256 (exhaustive key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

```
{
 "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": "..."
   },
```

```
"       ": {
    "type": "cryptographic-asset",
    "name": "TLSv1.3",
    "cryptoProperties": {
     "oid": "1.3.18.0.2.32.111",
     "assetType": "protocol",
     "protocolProperties": {
      "type": "tls",
      "version": "1.2",
        }
       ]
     }
    }
   }
  ]
}
```

CBOM Model

Smals
ICT for society



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

Why & What?

In the Public Sector

Crypto Inventory

Crypto Policy as Code

Cryptography in Hybrid Mode

Outlook & Challenges

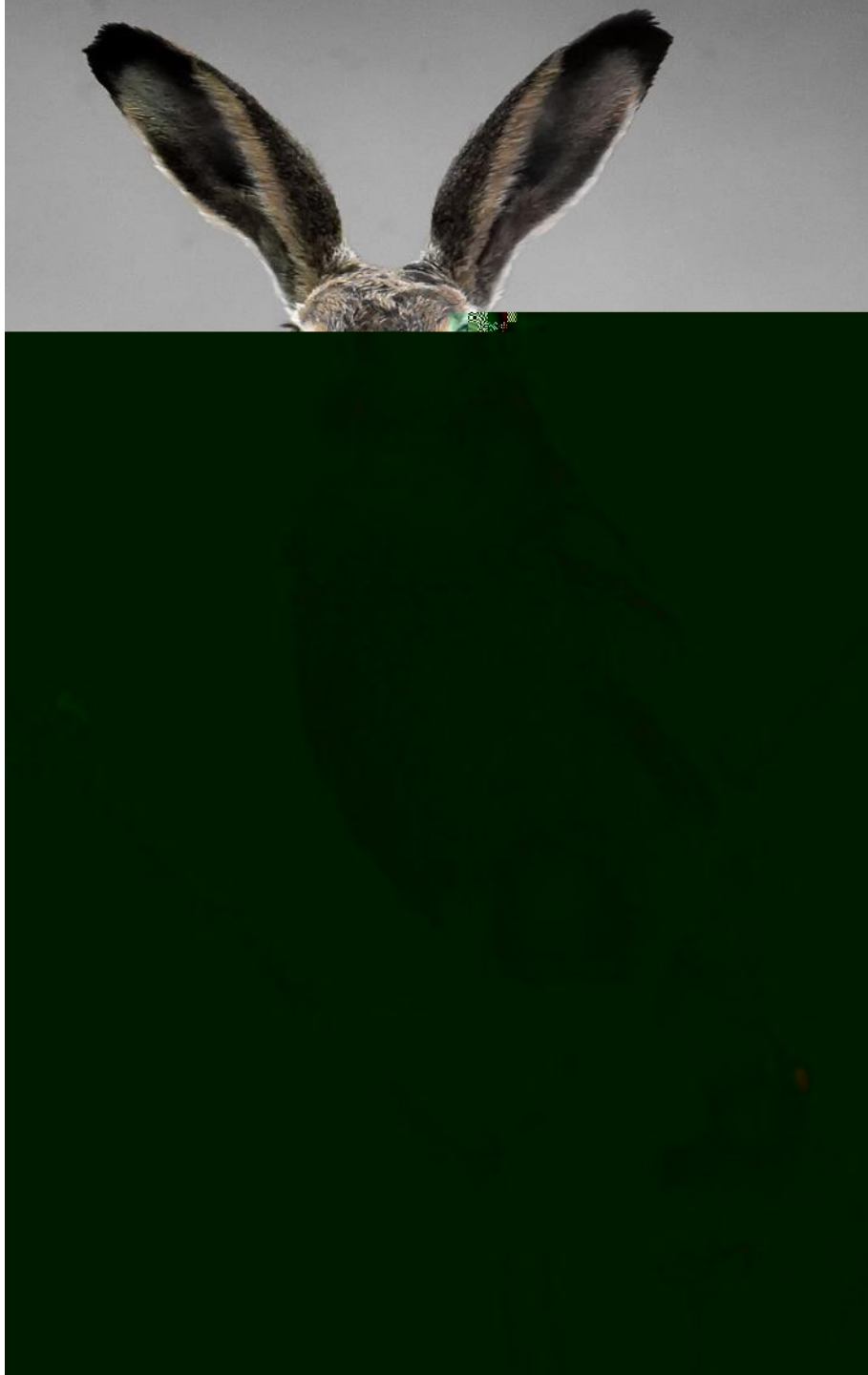
Wrapping Up

Smals
ICT for society

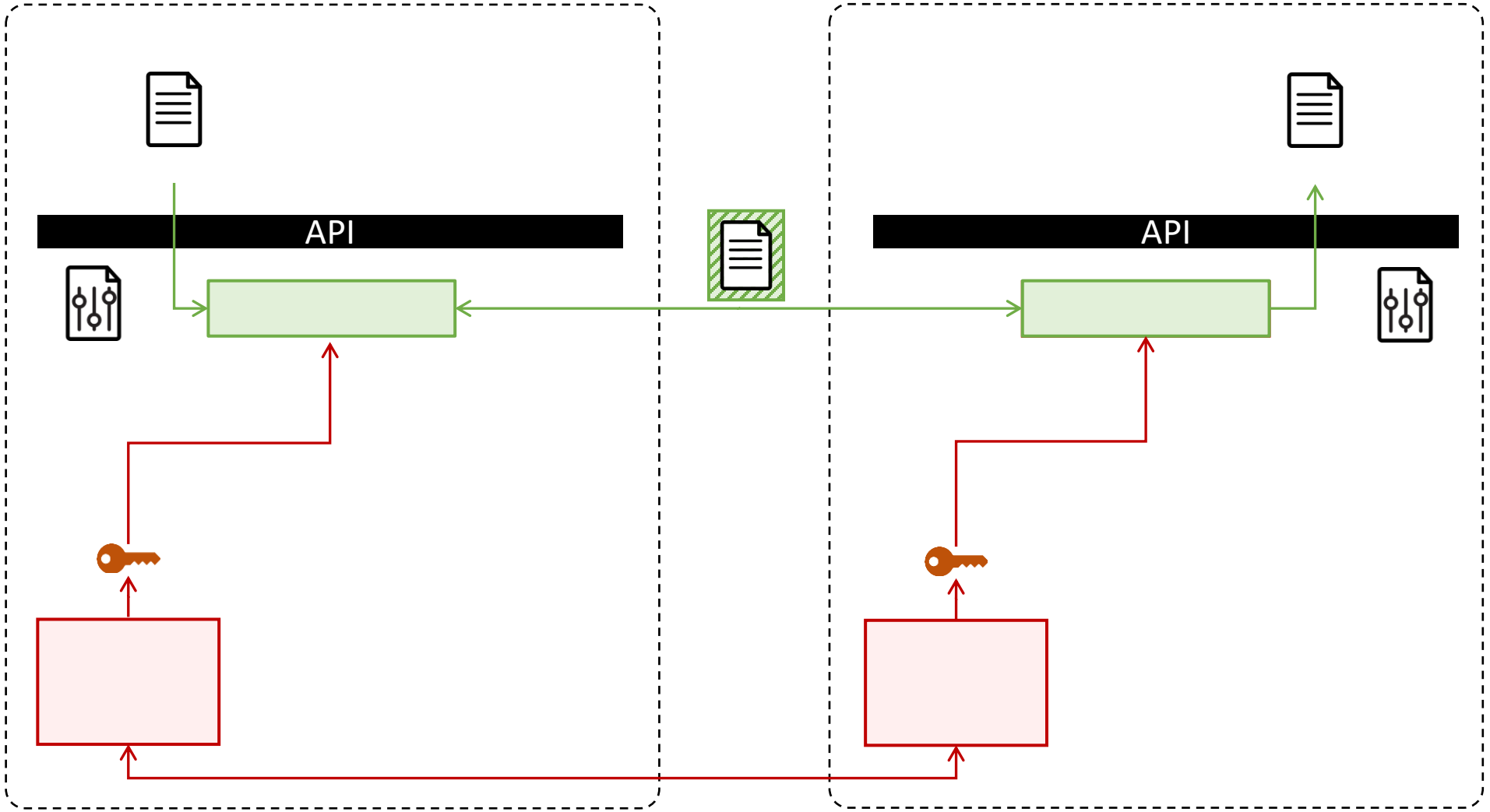
Bundesamt
für Sicherheit in der
Informationstechnik

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

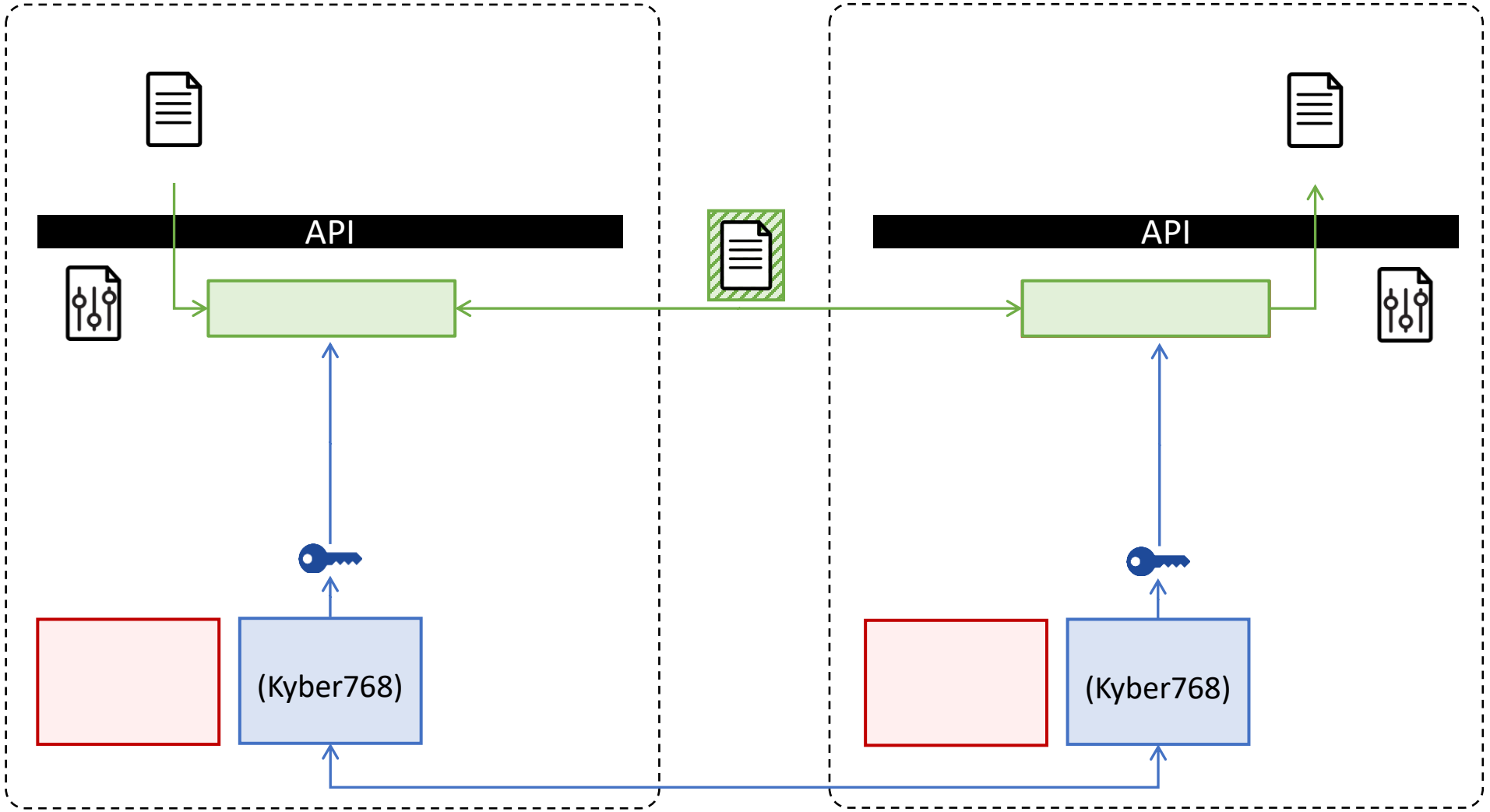


Key agreement with classical cryptography



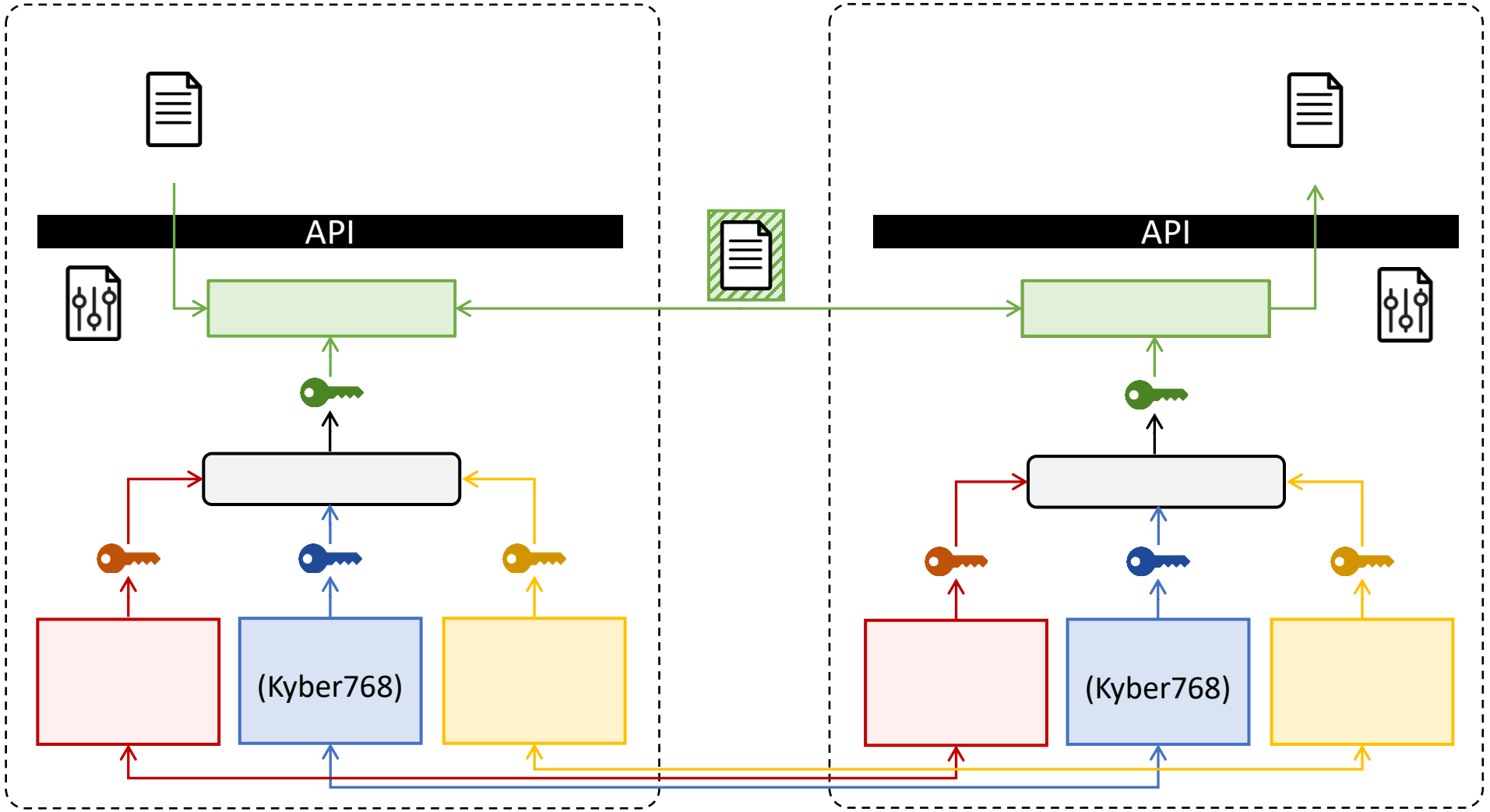
Smals
ICT for society

Key agreement with PQC (Post-Quantum Cryptography)



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

Why & What?

In the Public Sector

Crypto Inventory

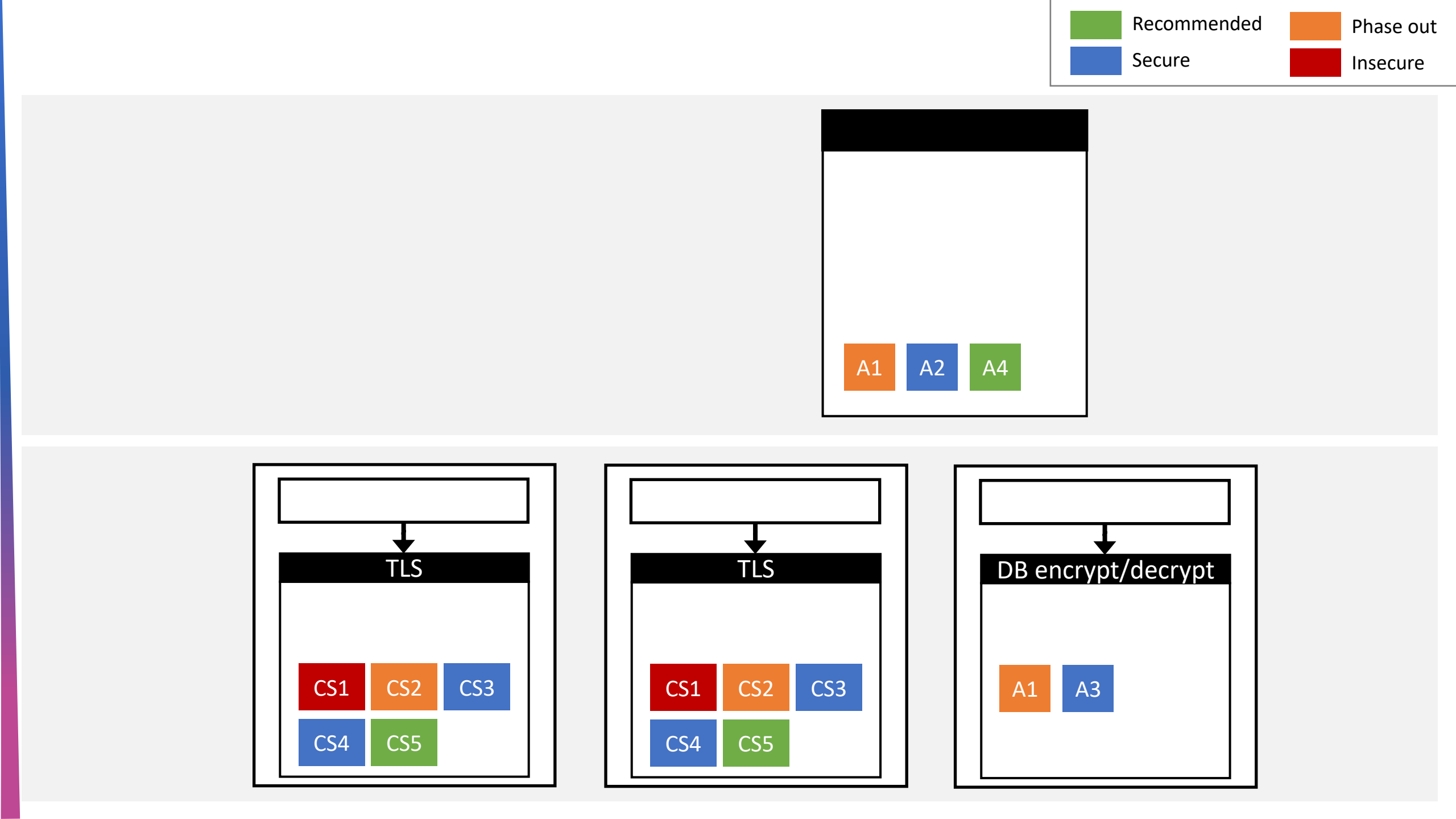
Crypto Policy as Code

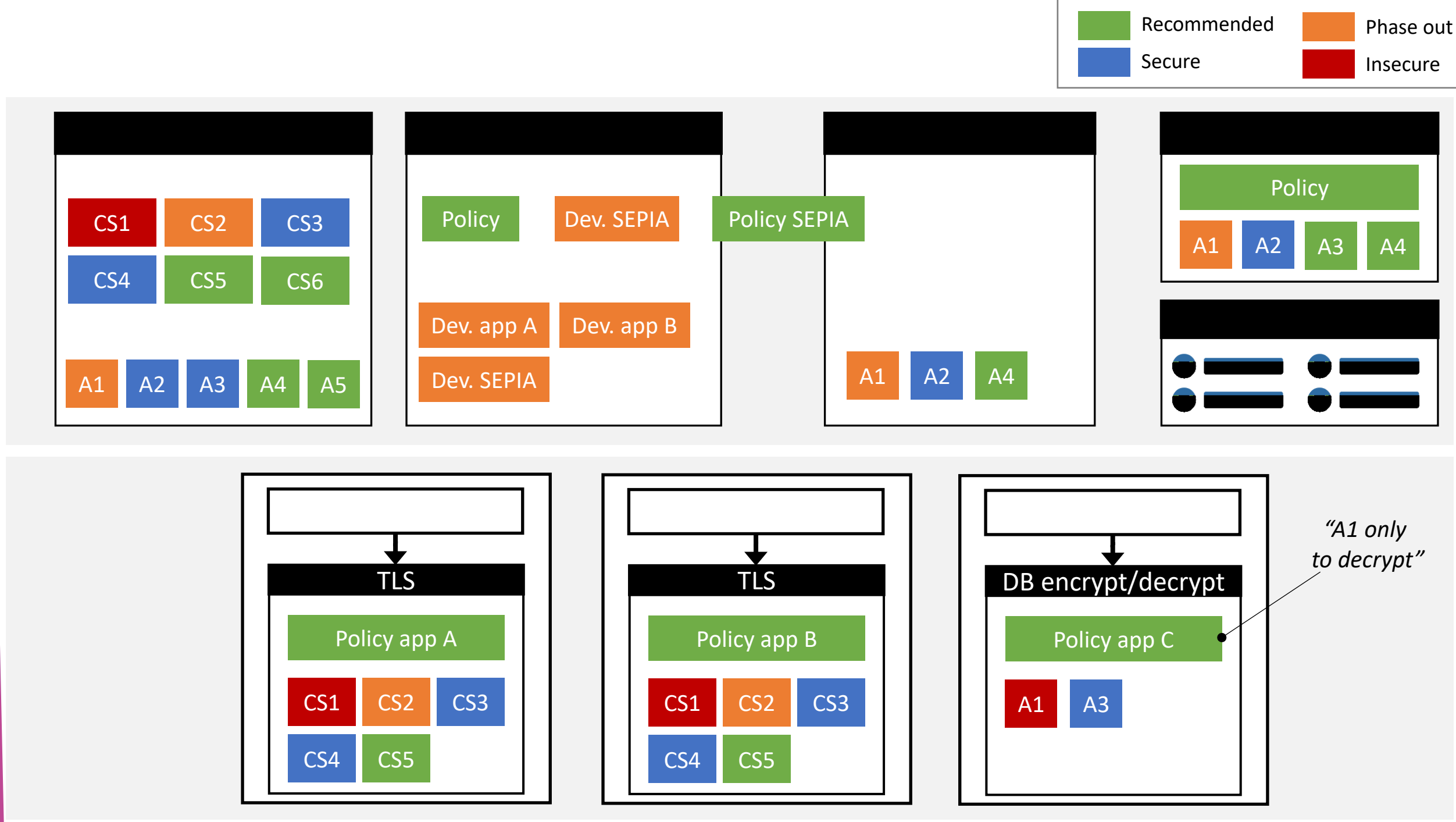
Cryptography in Hybrid Mode

Outlook & Challenges

Wrapping Up

Smals
ICT for society


Recommended
Secure
Phase out
Insecure
A1
A2
A4
TLS
CS1
CS2
CS3
CS4
CS5
TLS
CS1
CS2
CS3
CS4
CS5
DB encrypt/decrypt
A1
A3


Recommended
Secure
Phase out
Insecure
CS1
CS2
CS3
CS4
CS5
CS6
A1
A2
A3
A4
A5
Policy
Dev. SEPIA
Dev. app A
Dev. app B
Dev. SEPIA
Policy SEPIA
A1
A2
A4
Policy
A1
A2
A3
A4
TLS
Policy app A
CS1
CS2
CS3
CS4
CS5
TLS
Policy app B
CS1
CS2
CS3
CS4
CS5
DB encrypt/decrypt
Policy app C
A1
A3
"A1 only to decrypt"

Recommended
Secure
Phase out
Insecure
CS1
CS2
CS3
CS4
CS5
CS6
A1
A2
A3
A4
A5
Policy
Dev. SEPIA
Dev. app A
Dev. app B
Dev. SEPIA
Policy SEPIA
A1
A2
A4
Policy
A1
A2
A3
A4
TLS
Policy app A
CS1
CS2
CS3
CS4
CS5
CS6
TLS
Policy app B
CS1
CS2
CS3
CS4
CS5
CS6
DB encrypt/decrypt
Policy app C
A1
A3
A5
"A1 only to decrypt"

Crypto-Agility Maturity Model (CAMM)

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

System property
- 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
- Secure 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

Smals ICT for society

Crypto-Agility Maturity Model (CAMM)

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

System property
- Cryptographic modularity (alt.)

Process
- Algorithm intersection
- Algorithm exclusion
- Opportunistic security
- Usability of crypto agility

2

(NO OFFICIAL ROADMAPS AVAILABLE YET)

Practiced

Crypto migration demonstrable, effectively and securely feasible

Knowledge
- Performance awareness
- Secure 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

Smals ICT for society

n

Smals
ICT for society

		(in bytes)	(in bytes)	(lower is better)	(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

n

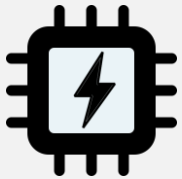
Contains public key and signature

TLS handshake: + 15 KB

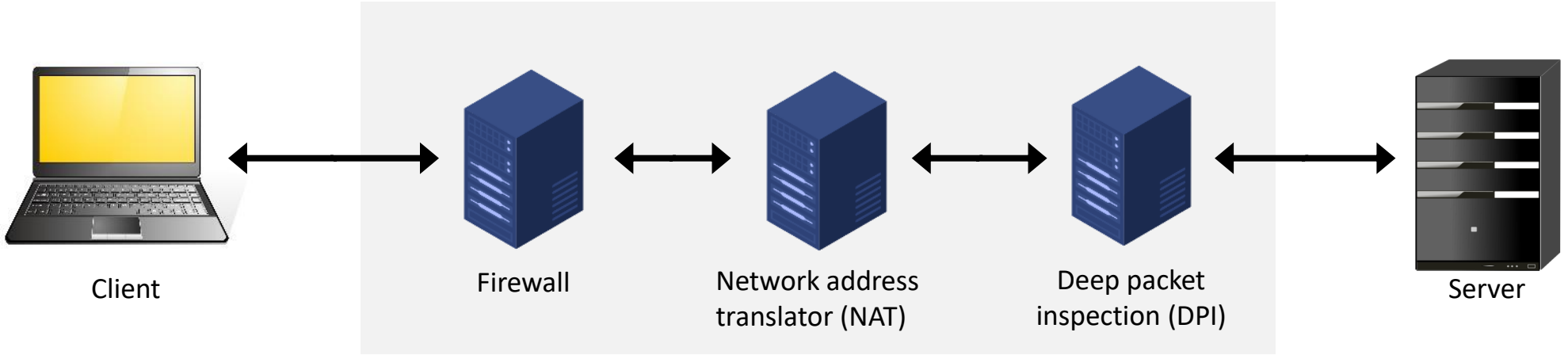
E.g. Belgian eID Limited resources

Limited resources & bandwidth

Encode signature in QR code



Acceleration, resources



Smals
ICT for society

Why & What?

In the Public Sector

Crypto Inventory

Crypto Policy as Code

Cryptography in Hybrid Mode

Outlook & Challenges

Wrapping Up

Smals
ICT for society

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

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

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.

“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.

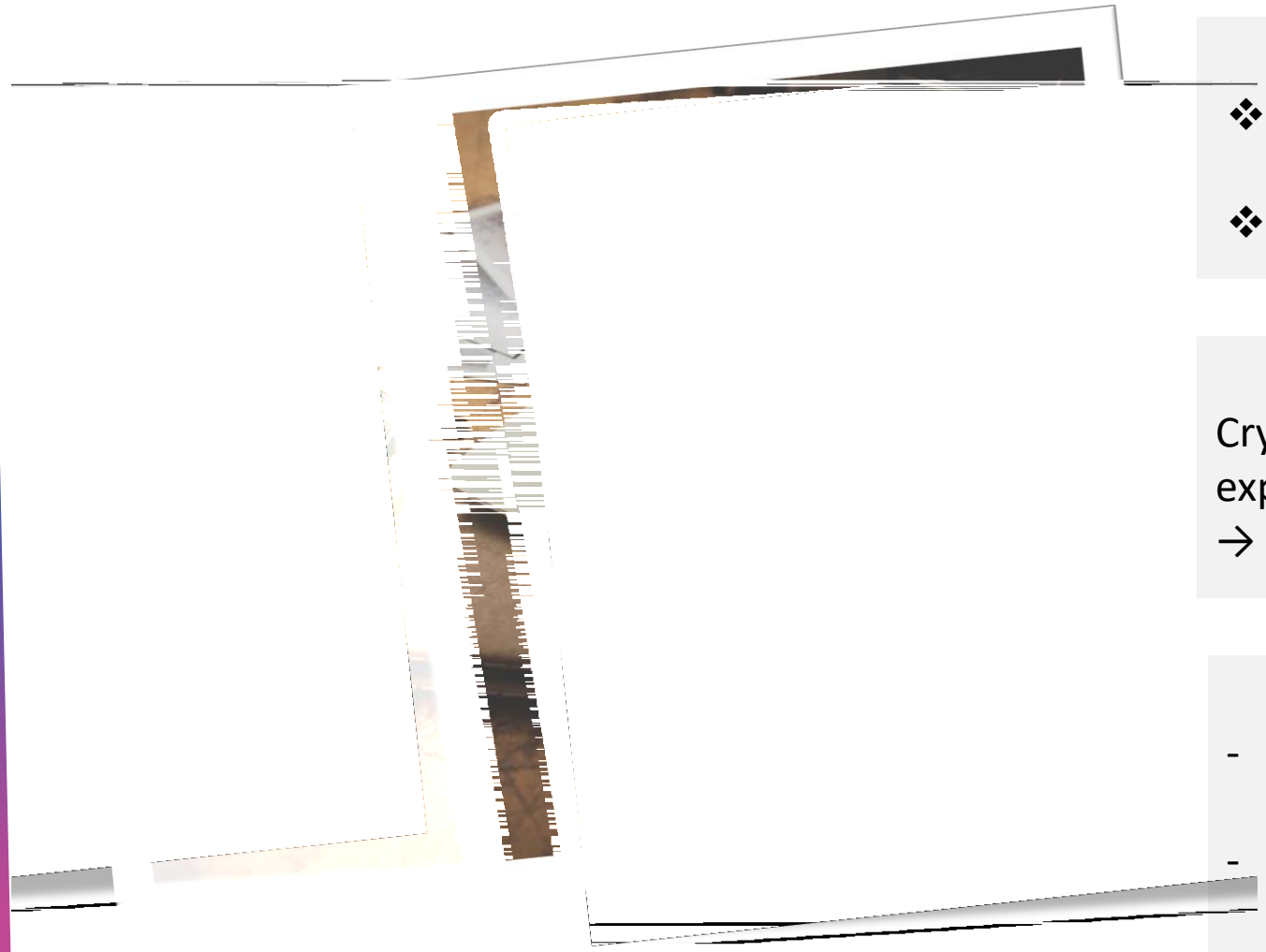
Smals ICT for society

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.

- *Harvest now decrypt later* attack: Intercepted encrypted communication is decrypted later
-

Public-key crypto often relies on certificates. Certificate authorities will determine when to introduce new and phase-out old crypto.

Smals
ICT for society

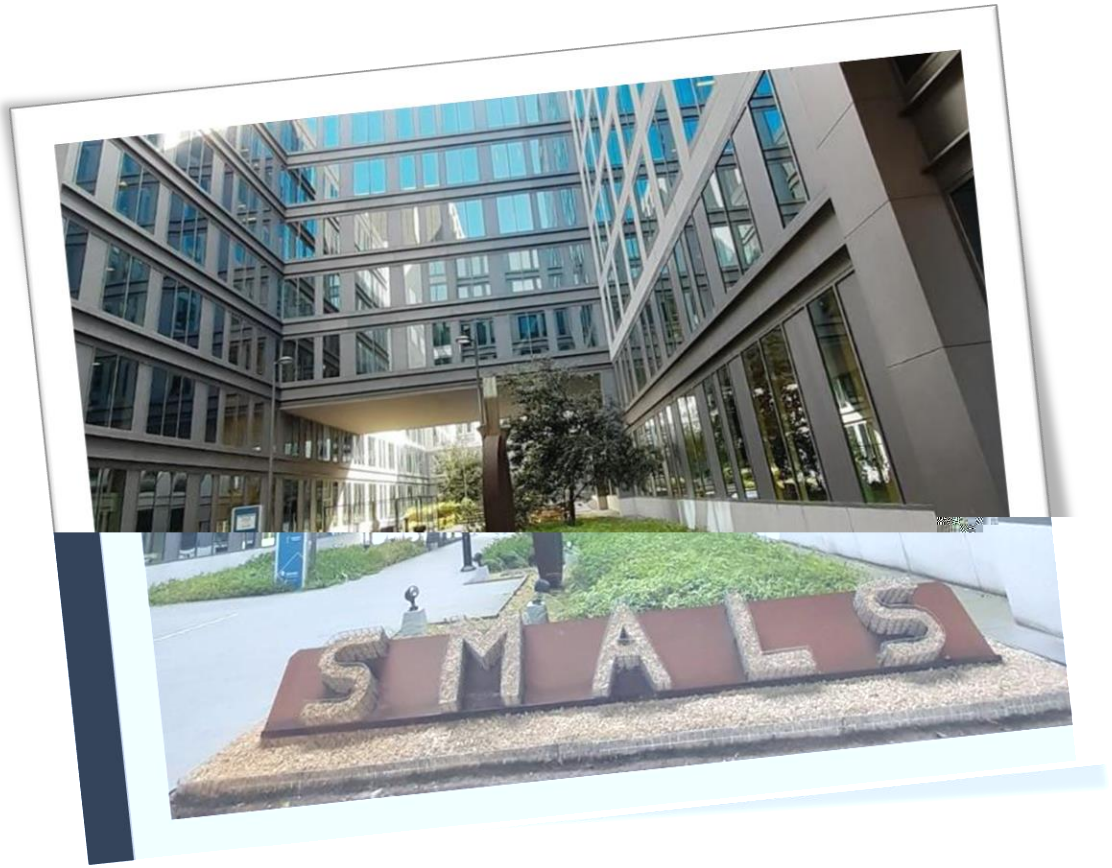


- ❖ Assumption in the past: "*RSA and elliptic curve cryptography rock-solid*" → Historical neglect
- ❖ Crypto inventory / policy / agility → *No-regret moves*

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

- 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



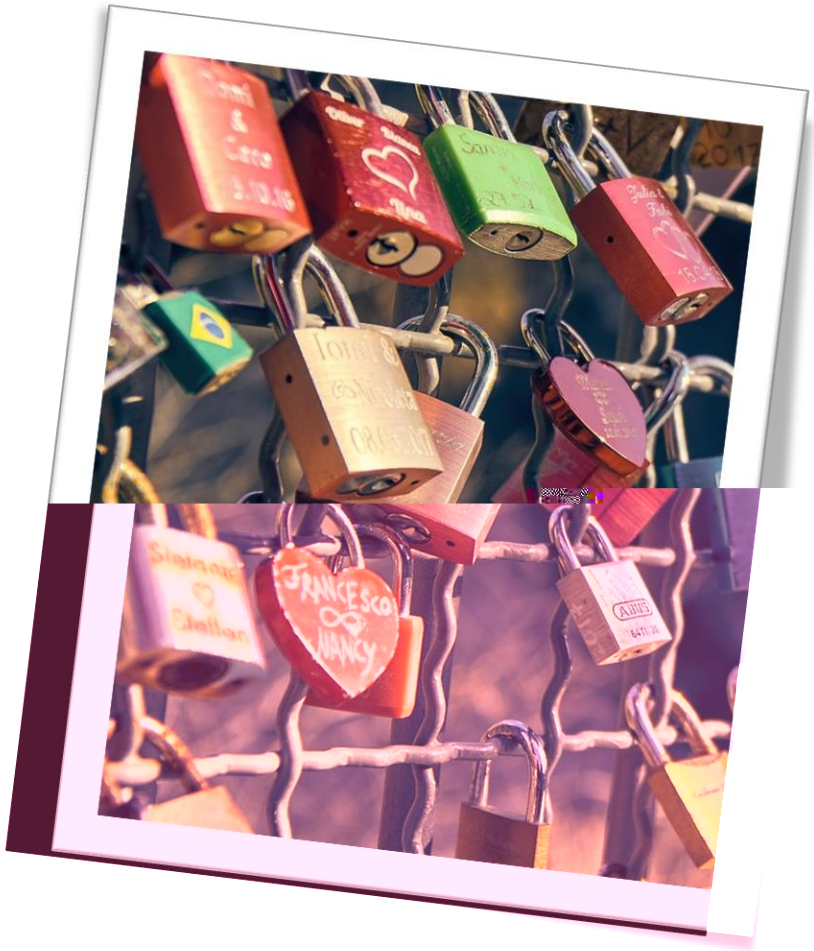
- Post-quantum cryptography, Crypto inventory, Crypto agility and crypto policy as code
- Sepia, Middleware key vault, automated certificate management
- Coming later this year
  Awareness, inventory, risk analysis, next steps, …

Smals
ICT for society

- 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

- 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

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



Smals
ICT for society

- 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, …

- ***protocol*** already adopted, for instance by TLS clients.
- 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
ICT for society

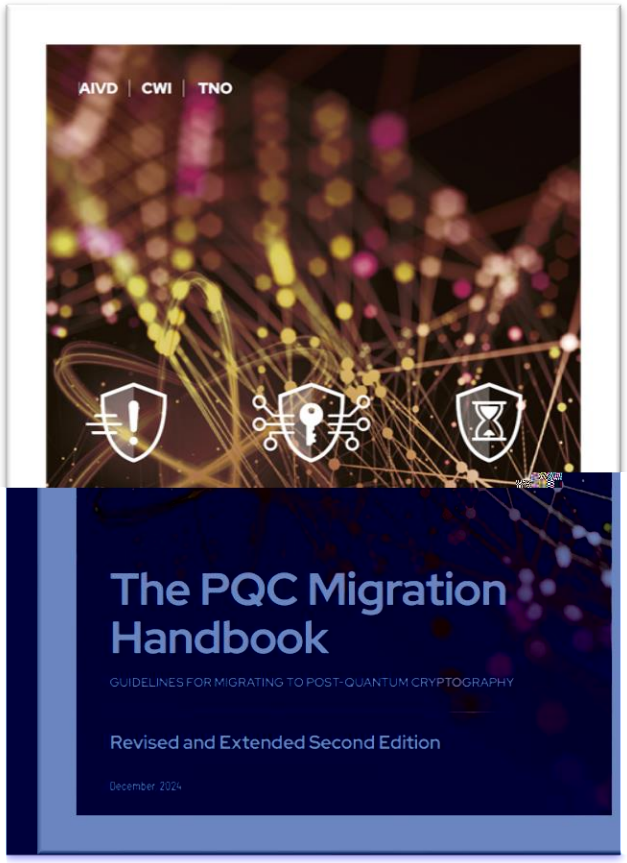
- Crypto agility requires a
  - Crypto inventory: what crypto is used where?
  - Crypto policy: what crypto is recommended, insecure, …

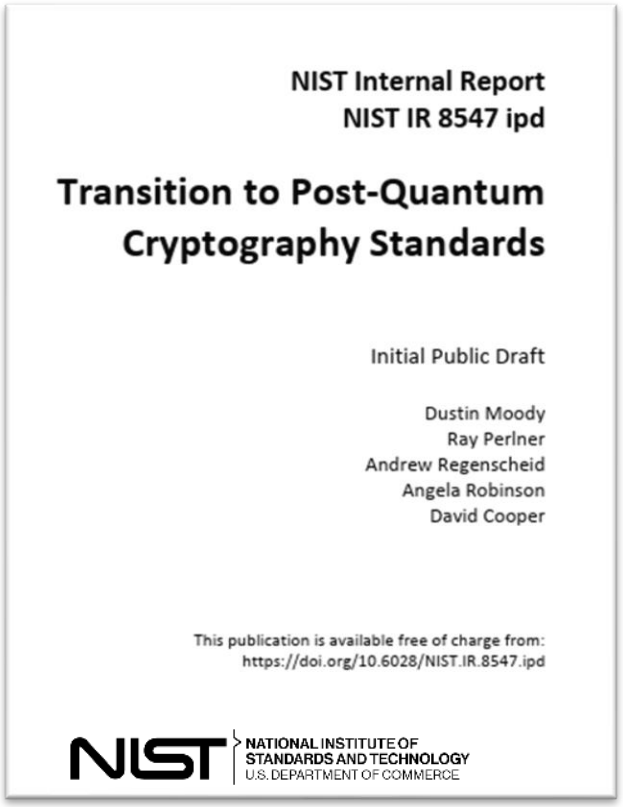
→ Agility / inventory / policy improve organisation's crypto maturity

- 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

- 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





Smals
ICT for society

BECOME A CHEETAH: EMBRACE CRYPTO AGILITY

Smals
ICT for society

Feedback / questions / discussions welcome!

kristof.verslype@smals.be

+32(0)2 7875376

linkedin.com/in/verslype

www.smals.be
www.smalsresearch.be