Cryptographic agility in practice

Experiences from the Belgian public sector

Kristof Verslype
Cryptographer, Smals Research

21 May 2025

CYBERSEC

Smals
ICT for society

Today

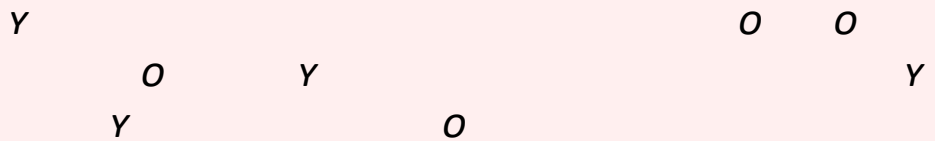
Cryptography is everywhere

- IoT, smartcard (Belgian eID, bank card), cars, planes, satellites, …
- Financial transactions, communication, document signing, authentication, ….
- Defense, public sector, private sector, individuals

→ **If broken, our society collapses**

Cryptographically relevant quantum computers

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



→ **MIGRATE ON TIME TO RECOMMENDED CRYPTOGRAPHY**

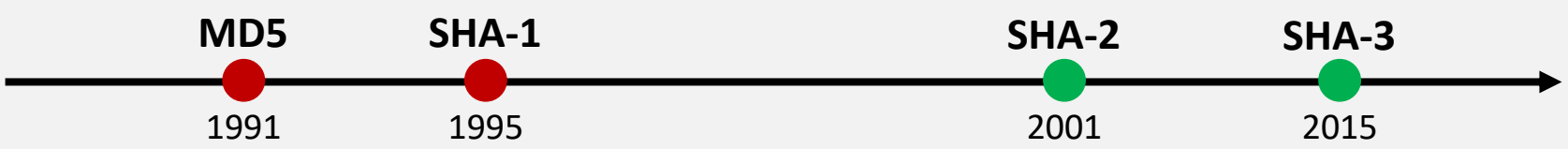
Smals
ICT for society

Cryptographic migrations

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

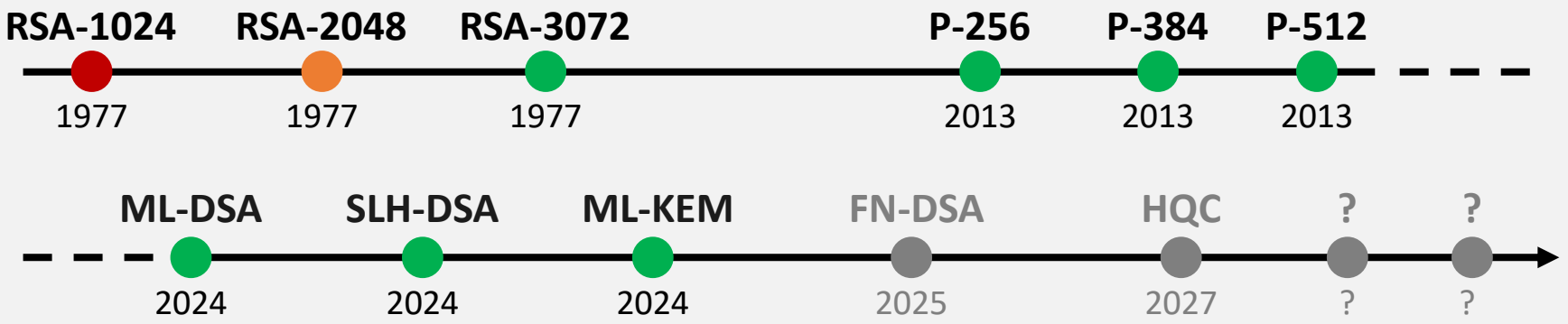
Symmetric encryption

Secure hash function



Public key cryptography

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



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

Multiple crypto migrations in the not-so-distant future!

Smals ICT for society

Crypto migrations

Challenge

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

→ **How to facilitate smooth migrations?**

Approach

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

Cryptographic mechanisms are assets that need to be managed

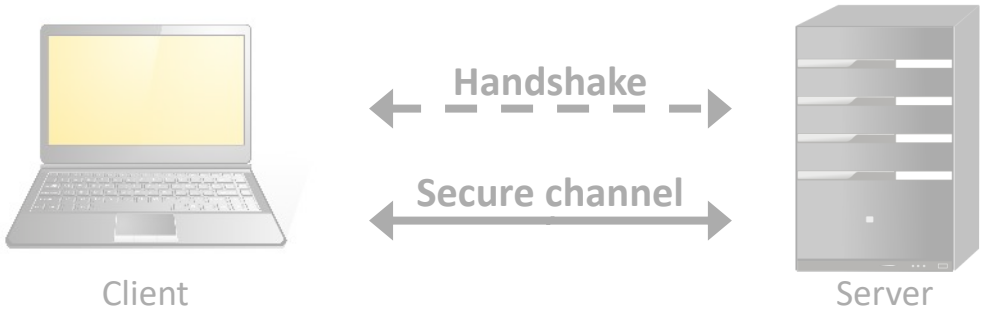
We should accept this and act on it!

Improve cryptographic maturity

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

Transport Layer Security (TLS)

Example of cryptographic protocol agility (see RFC7696)



Handshake

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

Supported cipher suites

TLS_SM4_GCM_SM3
TLS_AES_128_CCM_SHA256
TLS_AES_128_GCM_SHA256

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 system

Cryptographic service offers **abstract API** to application / service	Cryptographic functions **selected in real-time**	**Add** and **remove** Cryptographic functions	**At runtime** – No impact on system availability

Cryptographic functions: *O* *Y*

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

- Intro / recap
- Crypto Agility in the Public Sector
- Crypto inventory
- Crypto Policy as Code
- Cryptography in Hybrid mode
- Challenges
- Conclusions

Smals ICT for society

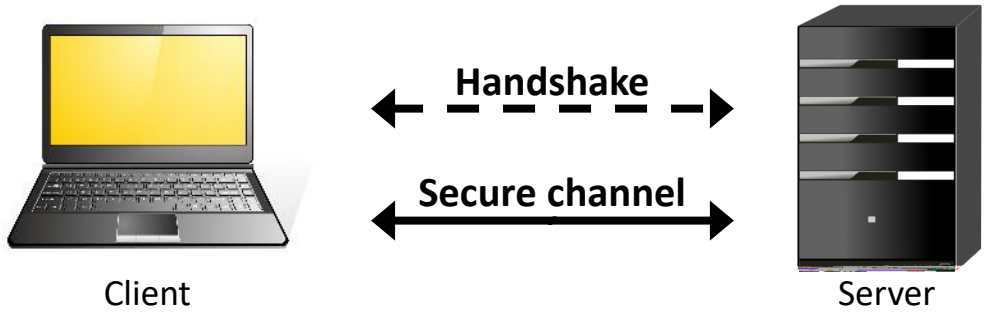
Agenda

- Intro / recap
- **Crypto Agility in the Public Sector**
- Crypto inventory
- Crypto Policy as Code
- Cryptography in Hybrid mode
- Challenges
- Conclusions

Smals ICT for society

Transport Layer Security (TLS)

Example of cryptographic protocol agility (see RFC7696)



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 CONFIG GENERATION

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

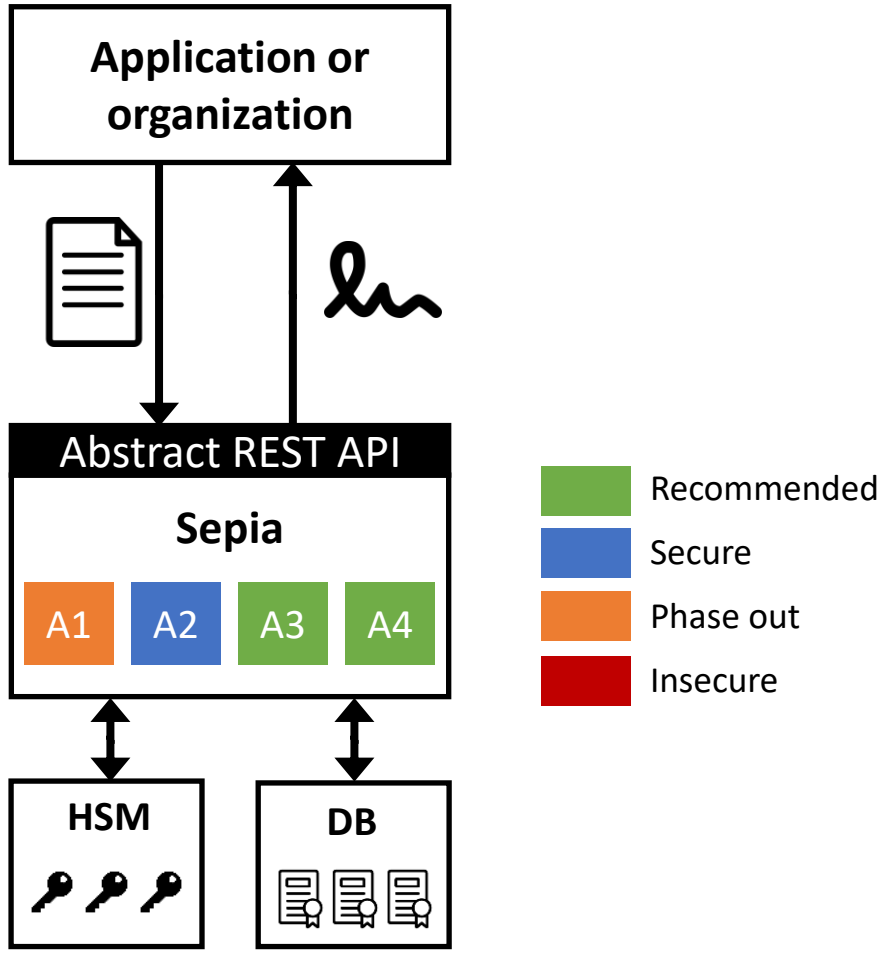
Service developed by Smals

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

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

Blind Pseudonimisation Service eHealth

Shortlisted for *Best Cybersecurity Innovation Europe* award issued by Cybersec Europe

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

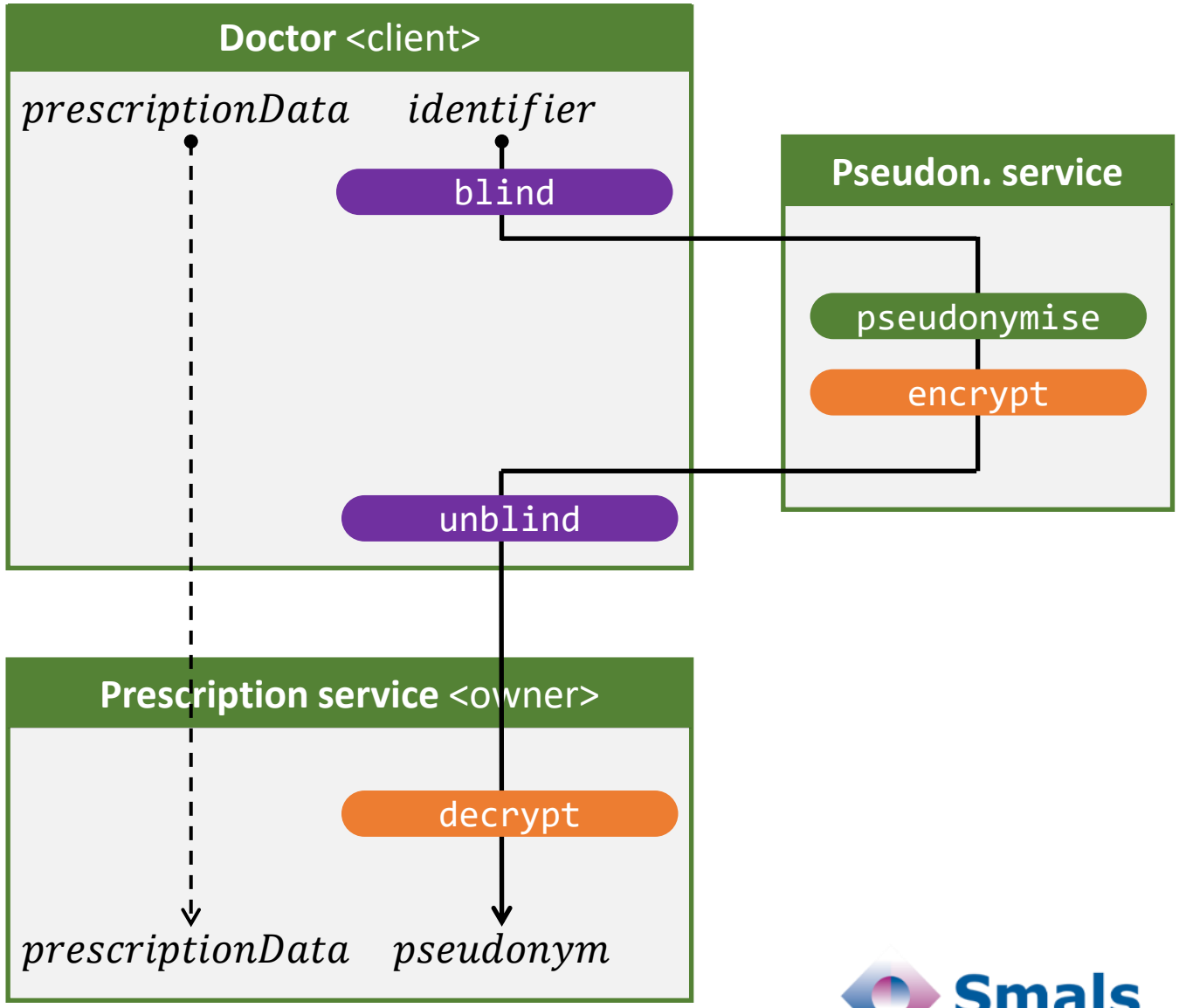
Reduced overhead
- Direct communication between healthcare professional and prescription service
- No in-between entity

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

HOW QUANTUM RESISTANT IS THIS SOLUTION?

Scenario

requests *Y* to register medical prescription



Smals ICT for society

Blind Pseudonimisation Service eHealth

Cryptography

- Mix of symmetric and public-key (EC)
- Designed before NIST PQC standards
- Deviation from standards

Analysis

Communication (red lines)

- Most important
- Upgrade TLS clients and cipher suites
- Not different from other applications

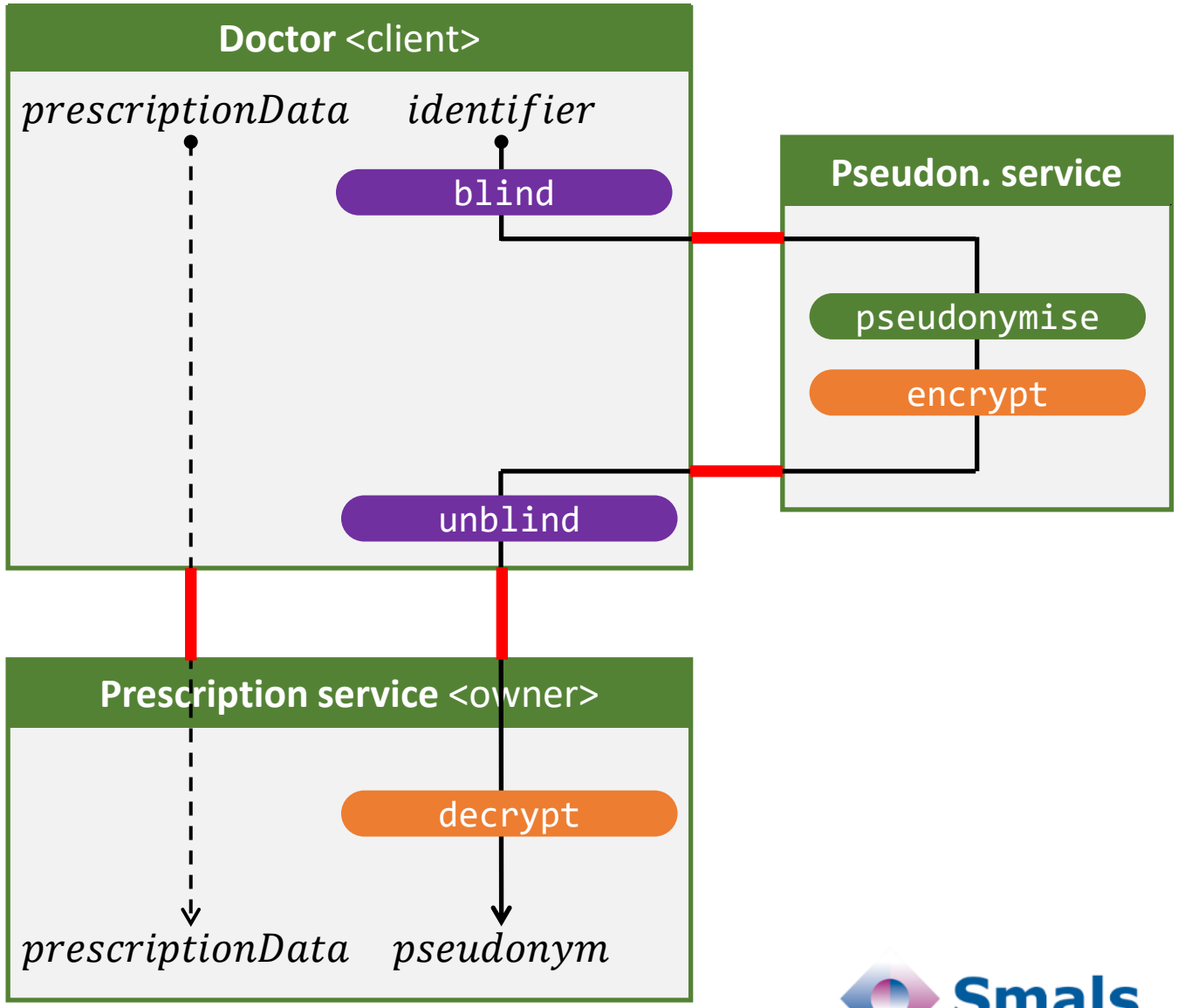
Pseudonymisation

- Quantum risk backend-stored pseudonyms to be mitigated
- Alternative based on lattices
- Integration of crypto agility to facilitate migration

DEVIATING FROM STANDARDS MAKES QUANTUM READINESS HARDER

Scenario

requests *Y* to register medical prescription



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

Sepia

- Central, flexible service for document signing
- Status: Final phase of development

Blind pseudon. service

- Quantum-resistant pseudonymization being developed
- Crypto-agility in future versions
- Status: research

SMALS IS EARLY ADOPTER OF CRYPTO-AGILITY

NEVERTHELESS, A LONG ROAD AHEAD OF US!

Smals ICT for society

Agenda

- Intro / recap
- Crypto Agility in the Public Sector
- **Crypto inventory**
- Crypto Policy as Code
- Cryptography in Hybrid mode
- Challenges
- Conclusions

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

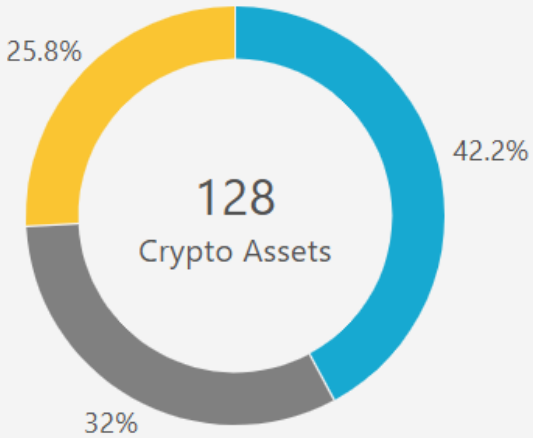
github.com/keycloak/keycloak

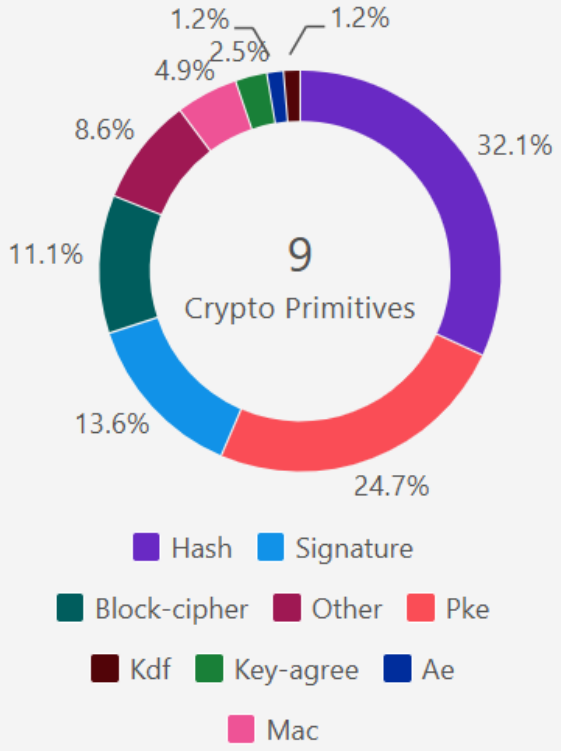
CBOMkit

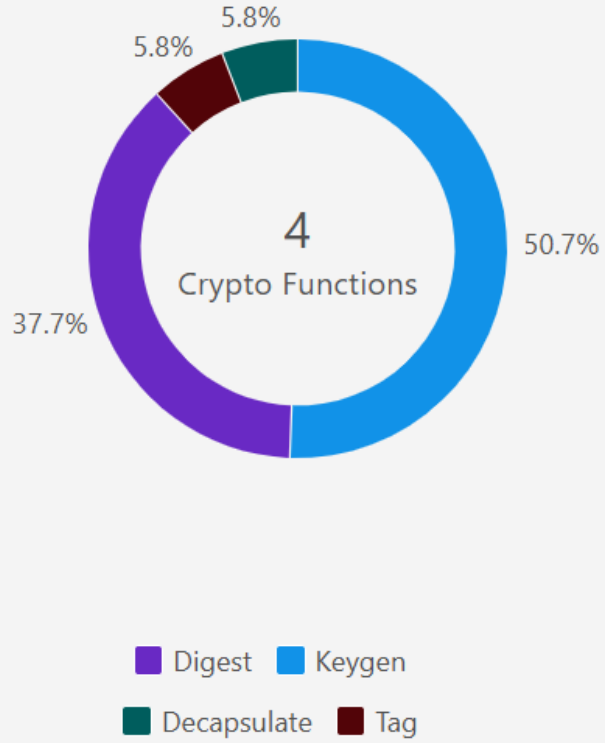
128 cryptographic assets found. Scanned **616.7K** lines of code across **5.3K** files. Took **2m 21s** to scan (**4m 7s** in total).

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

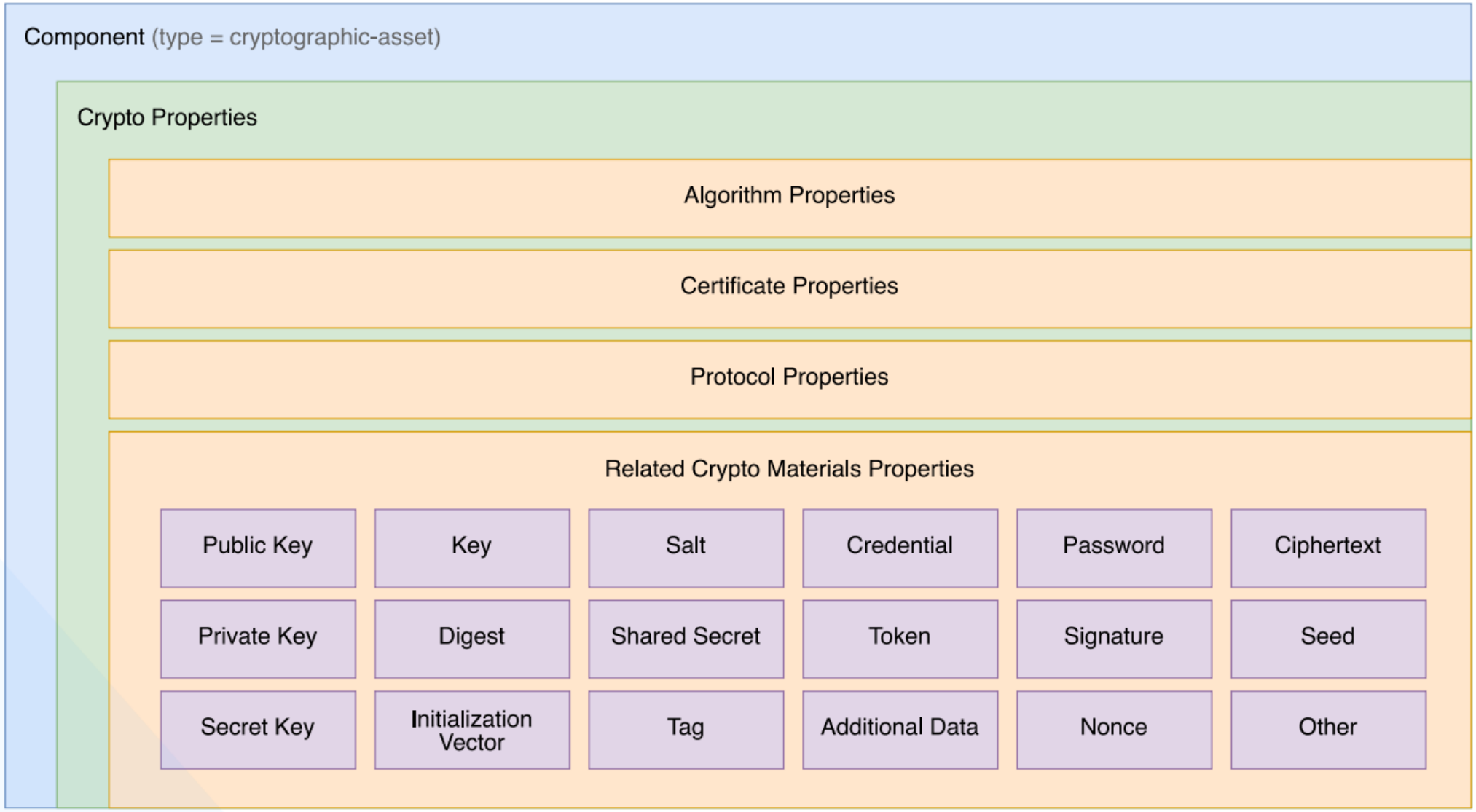
Cryptography Bill of Materials (CBOM)

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;"
```

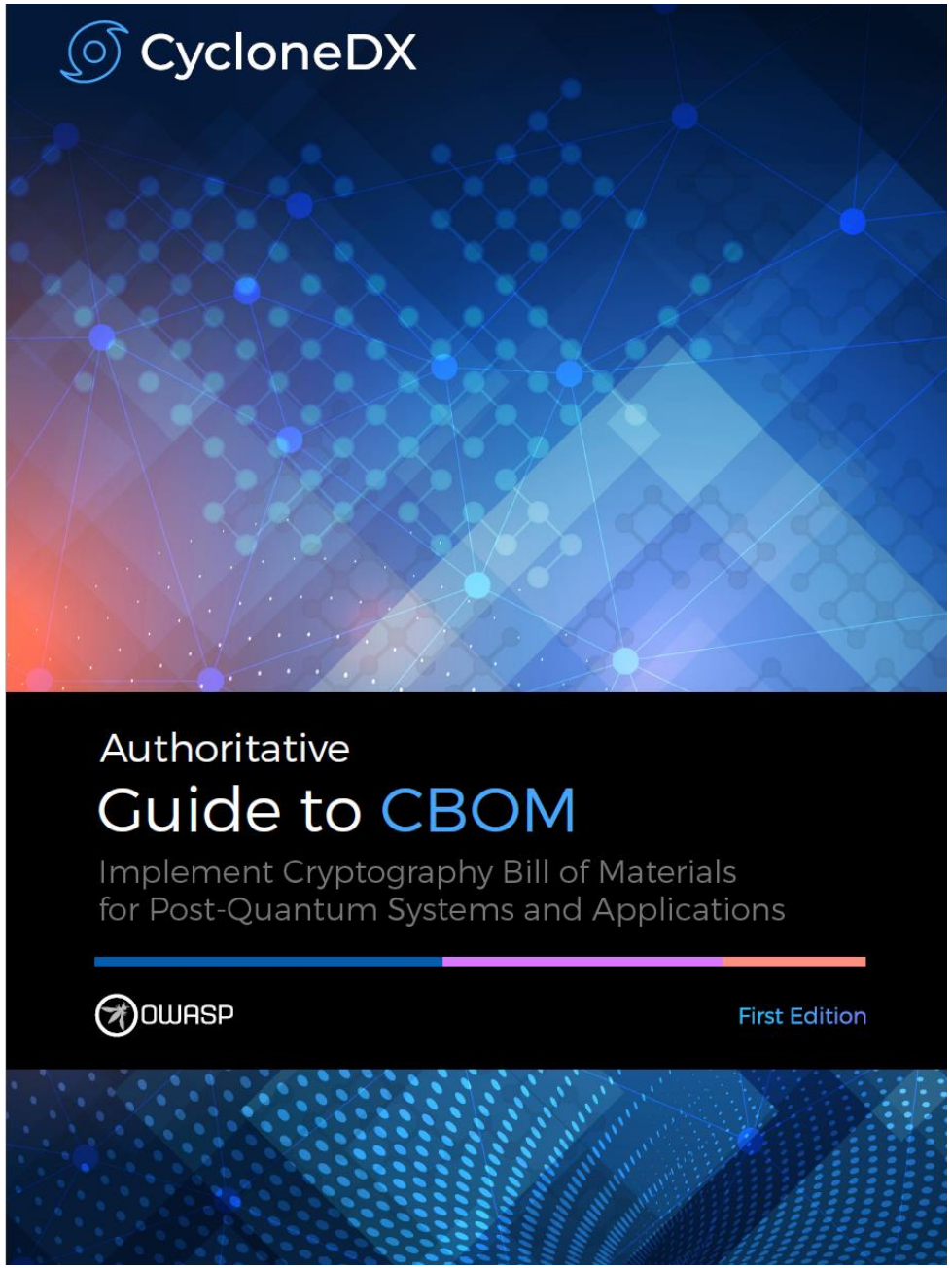

https://github.com/IBM/cbomkit/blob/main/example/keycloak-cbom.json

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

Dynamic scanning
- External network
- Internal network

→ **NOT CBOM**

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

→ **CBOM**

Internal import
- Home-build 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
CONSOLIDATE WHAT YOU ALREADY HAVE

Smals ICT for society

Agenda

- Intro / recap
- Crypto Agility in the Public Sector
- Crypto inventory
- **Crypto Policy as Code**
- Cryptography in Hybrid mode
- Challenges
- Conclusions

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 vulnerable to attacks on confidentiality. In particular, such vulne active side-channel attacks,

3.1 Block ciphers

of th 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 other lengths, block ciphers are applied in different *modes*.

3.1.1 Algorithm

Good

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
- 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 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": "medium",
    "impact": "medium",
    "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"
        ]
       }
      ]
     }
    }
   }
 ]
}
```


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 IS WORKING ON THIS

Smals ICT for society

Agenda

- Intro / recap
- Crypto Agility in the Public Sector
- Crypto inventory
- Crypto Policy as Code
- **Cryptography in Hybrid mode**
- Challenges
- Conclusions

Smals ICT for society

Transitional period in Hybrid Mode

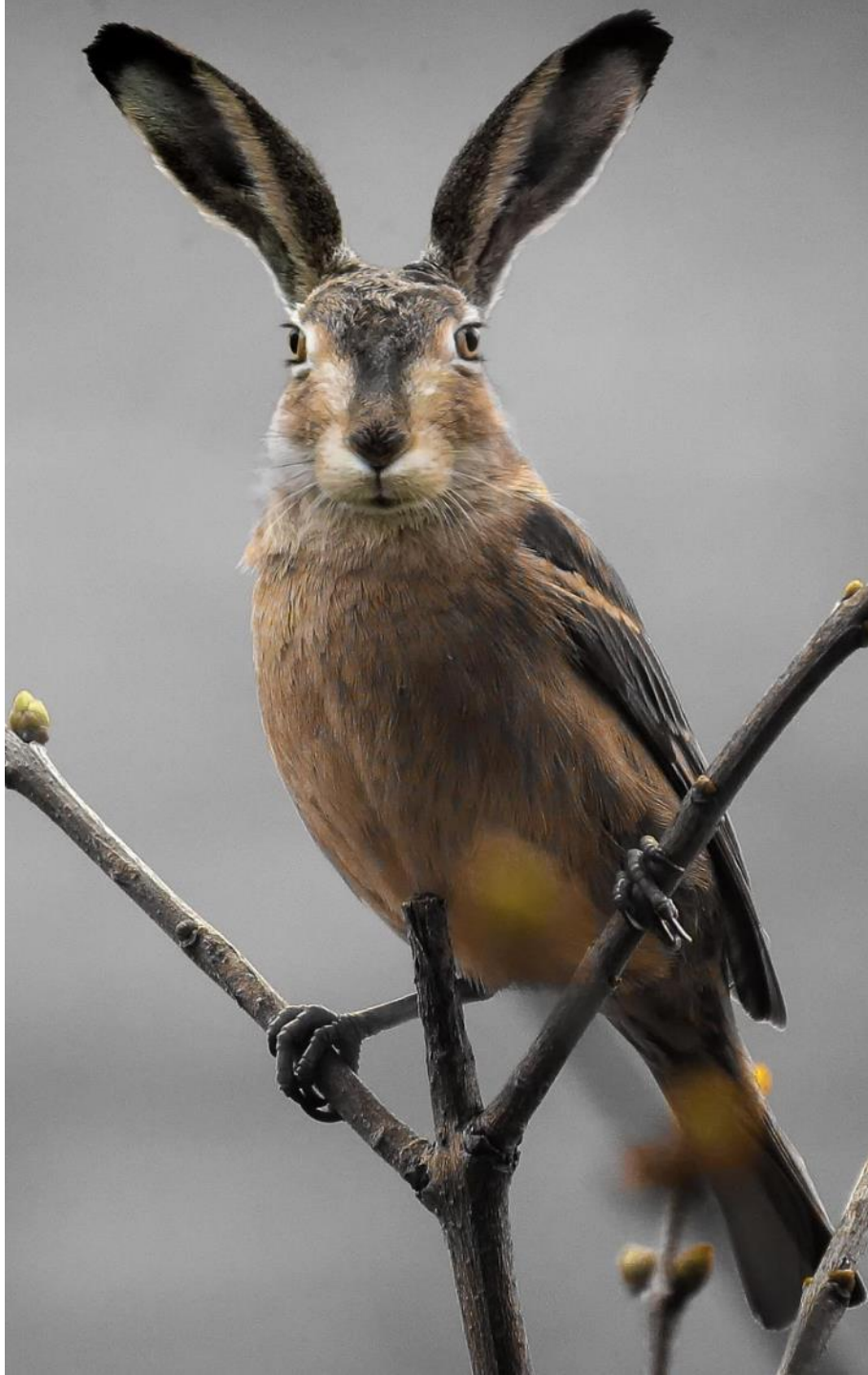
Bundesamt
für Sicherheit in der
Informationstechnik

The quantum-safe algorithms that are currently being standardized are not yet as well researched as the "classical" methods

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

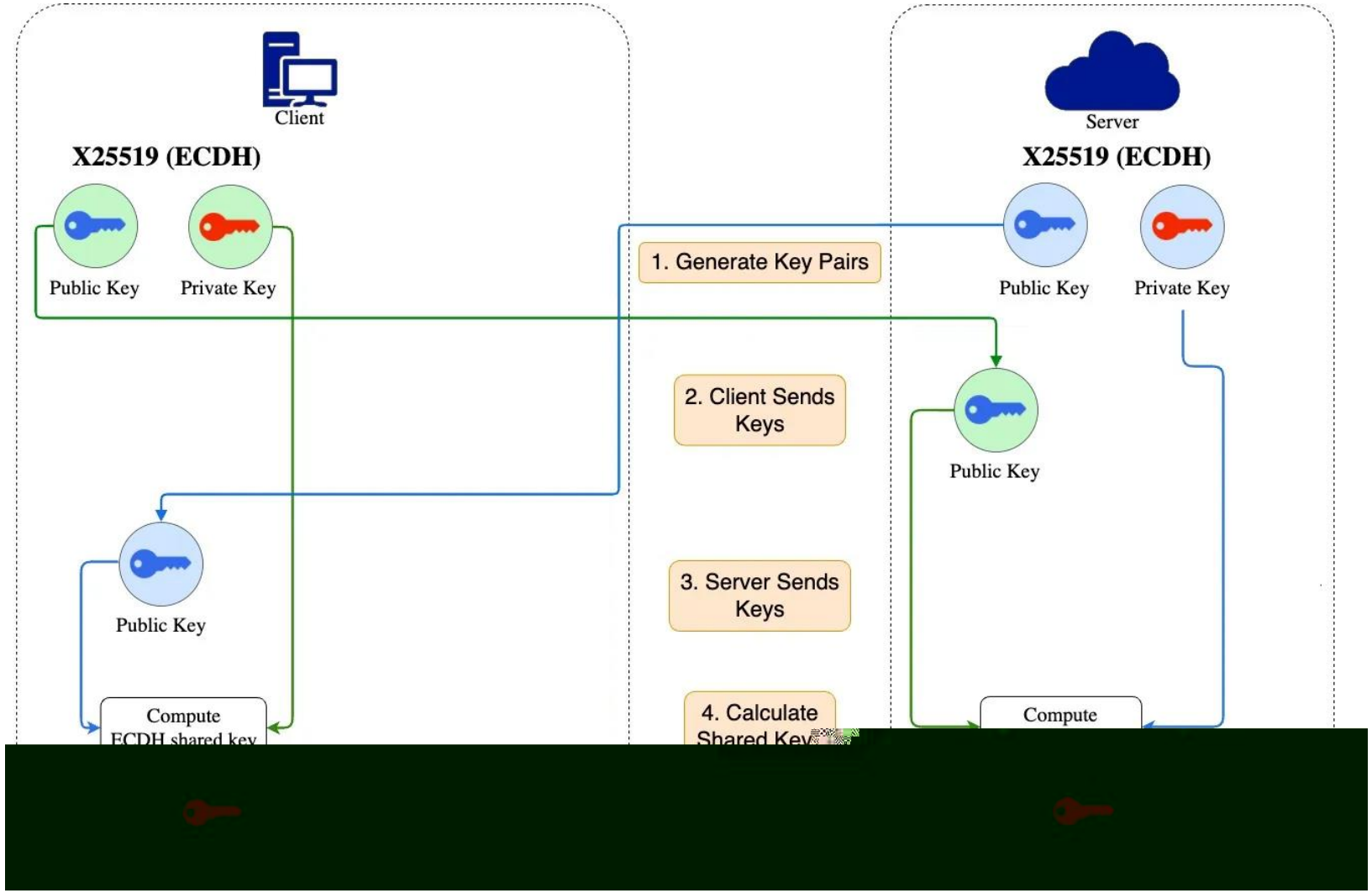
Quantum-safe cryptography –fundamentals, current developments and recommendations. October 2022

→ **EVEN MORE MIGRATIONS!**



Key Agreement – Diffie Hellman

Highly trusted, but quantum vulnerable



Symmetric protocol

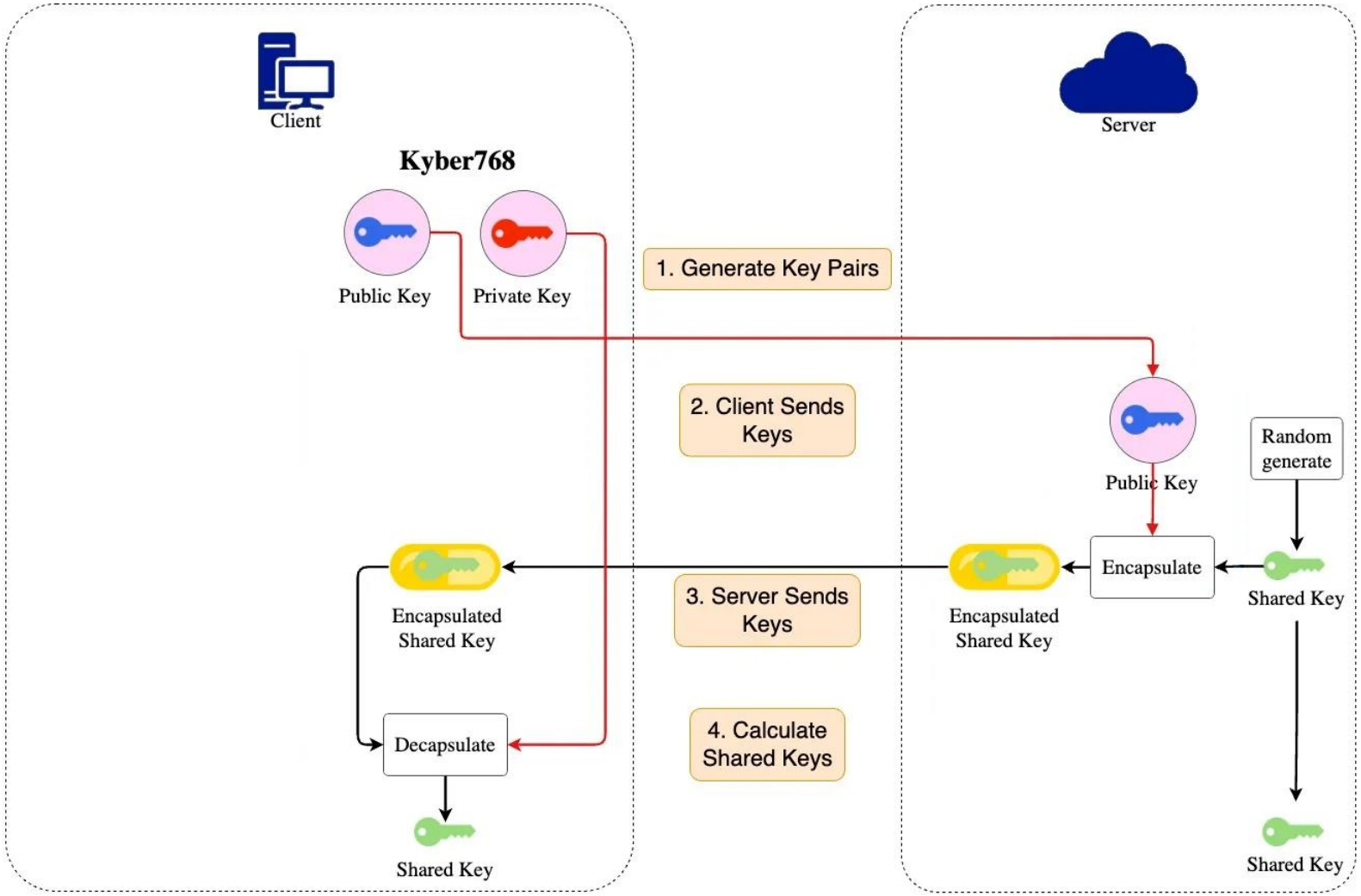
Client and server perform the same operations

https://medium.com/identity-beyond-borders/x25519kyber768-post-quantum-key-exchange-for-https-communication-70eba681931d

Smals ICT for society

Key Agreement – Kyber (ML-KEM)

Quantum resistant, but not yet sufficiently trusted



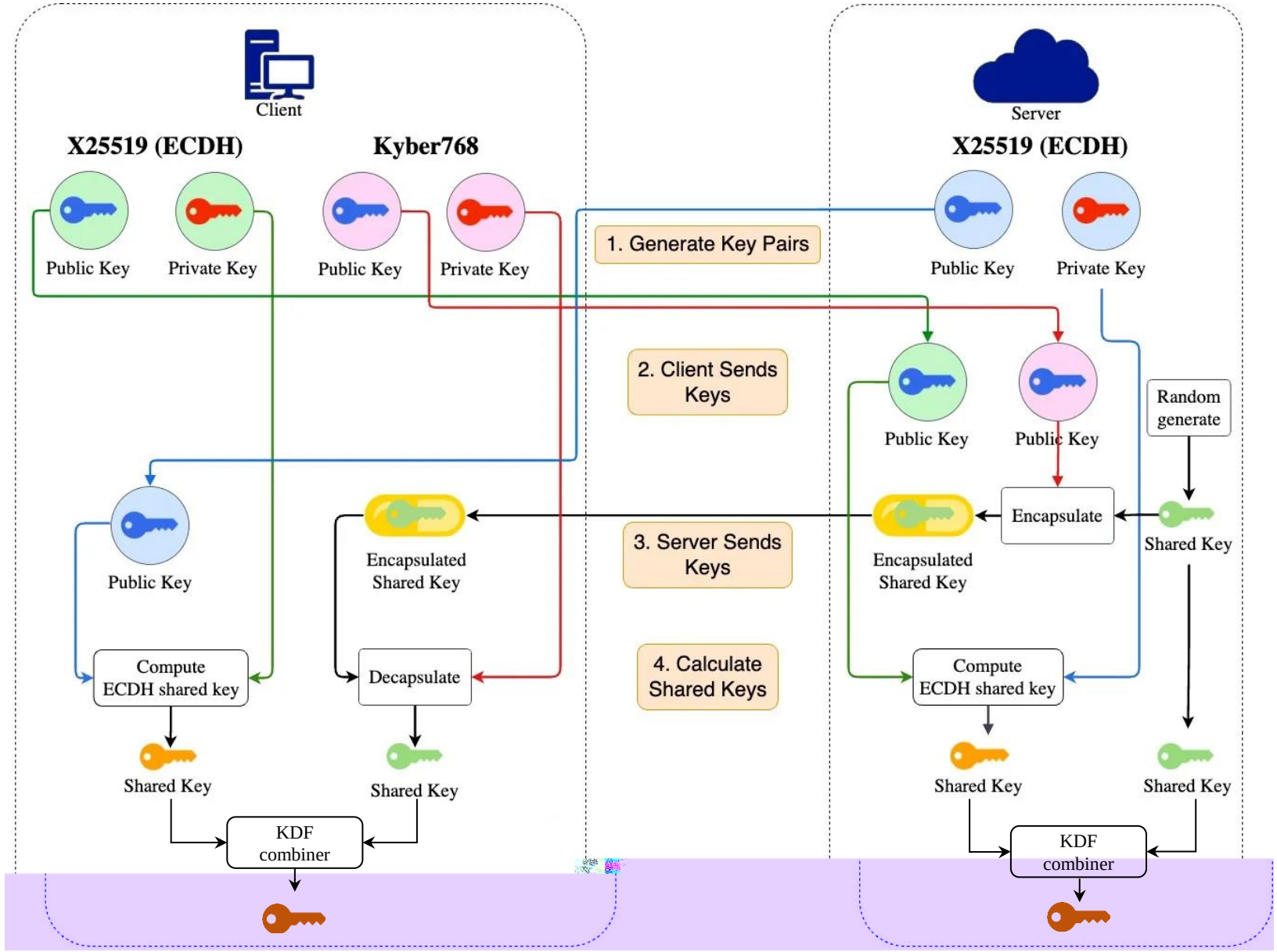
Asymmetric protocol

Client and server do different operations

https://medium.com/identity-beyond-borders/x25519kyber768-post-quantum-key-exchange-for-https-communication-70eba681931d

Smals ICT for society

Key Agreement – Hybrid mode



Combinable

Despite differing principles/flow

Migration

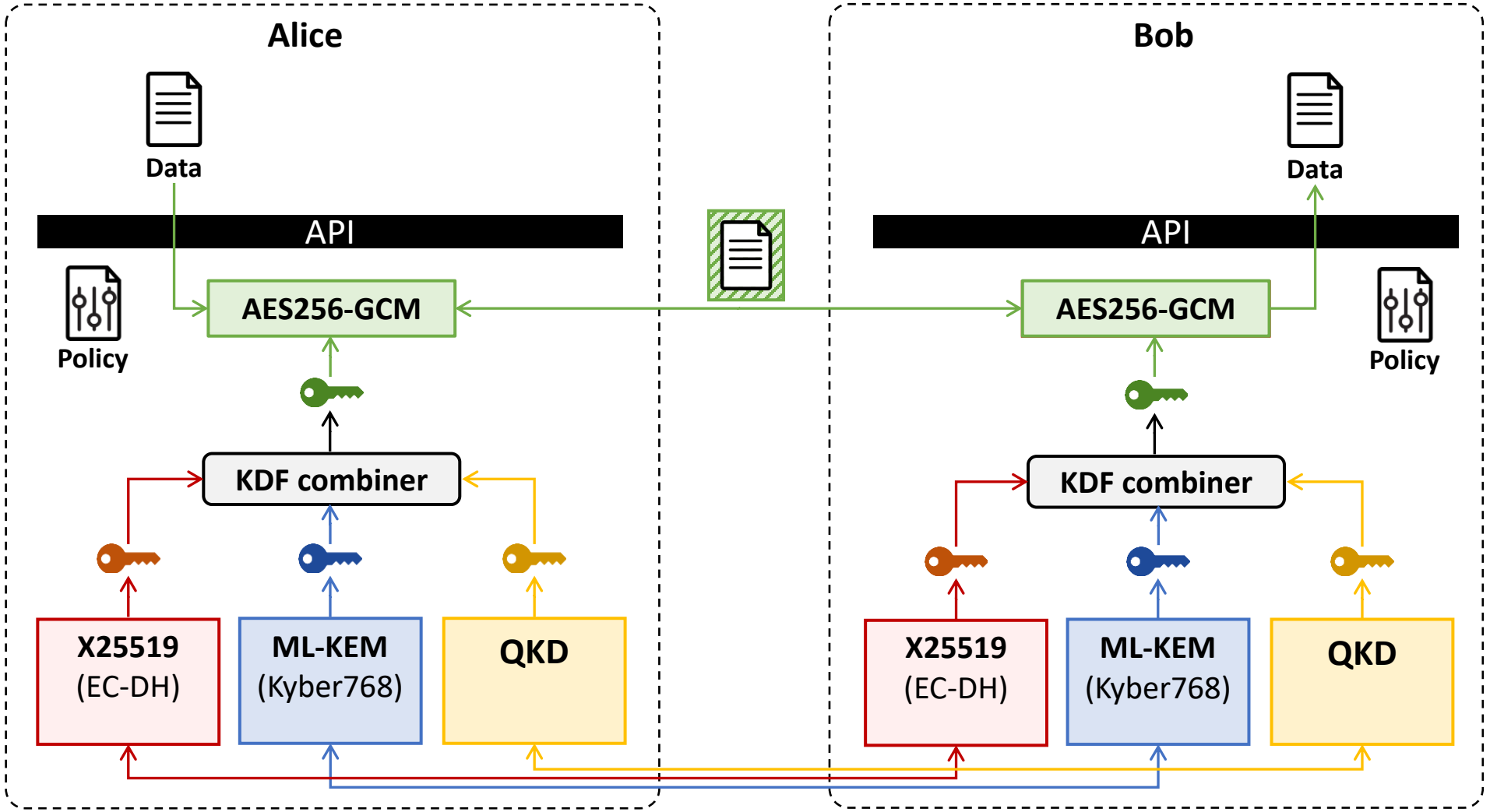
Diffie–Hellman → Hybrid → Kyber / ML-KEM)

Penalty

- Adds complexity
- Increased data transmission (not much worse than PQC only)

Smals ICT for society

Key agreement – Hybrid mode with Crypto Agility



HYBRID MODE HELPS US TO NAVIGATE CRYPTO MIGRATION TRANSITION PERIODS

CRYPTO AGILITY SUPPORTS HYBRID MODE

Smals ICT for society

Agenda

- Intro / recap
- Crypto Agility in the Public Sector
- Crypto inventory
- Crypto Policy as Code
- Cryptography in Hybrid mode
- **Challenges**
- Conclusions

Smals ICT for society

Challenges & open questions

Research on CA

Performance

Middleboxes

Legacy

Standards

Downgrade attacks

QR-codes

IoT

Incompatibilities

Advanced cryptography

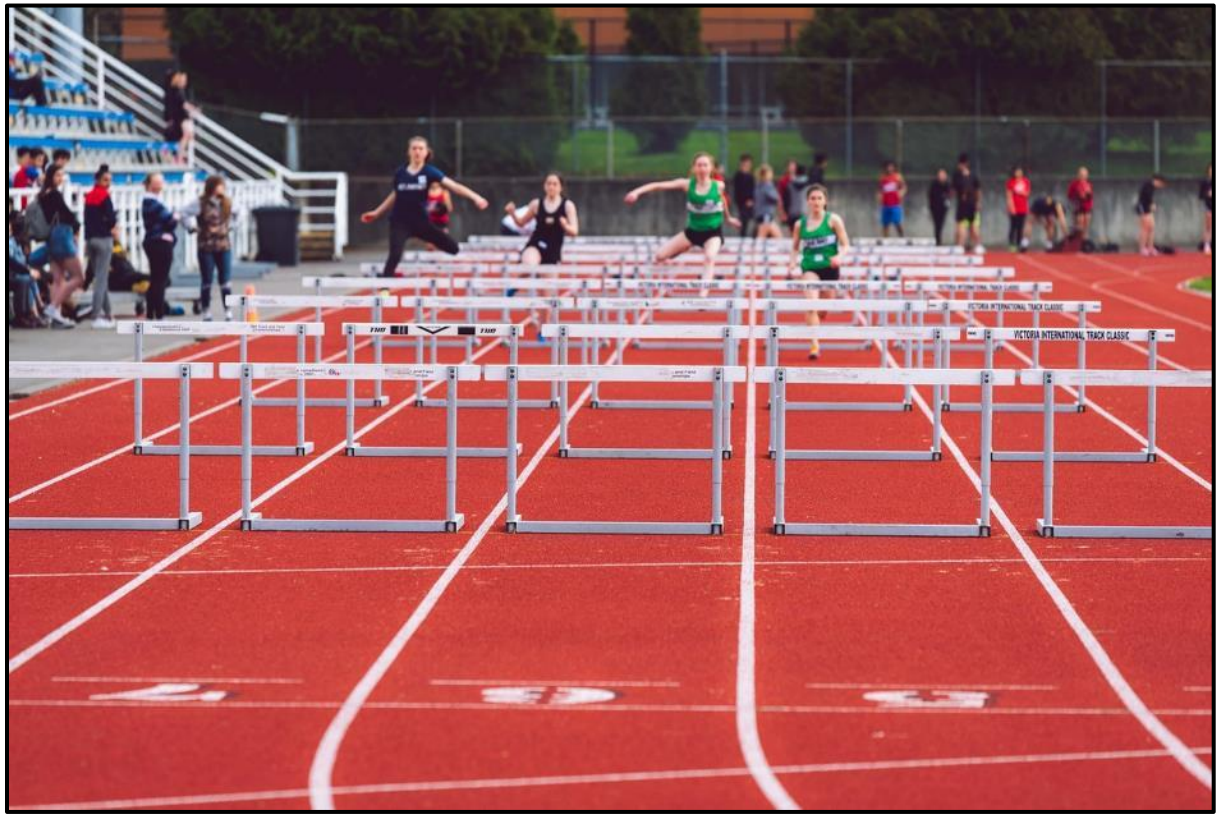
Guidance

X.509 certificates

Smartcards

HSMs

Cryptographic accelerators



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

BUT… IT PAYS OFF IN THE LONG RUN!

Smals ICT for society

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)
Y	No	32	64	1 (baseline)	1 (baseline)
	No	256	256	70	0,3
	Yes	1 312	2 420	4,8	0,5
	Yes	897	666	8	0,5
	Yes	32	7 856	8 000	2,8
	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

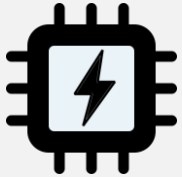
IoT

Limited resources & bandwidth

QR codes

Encode signature in QR code

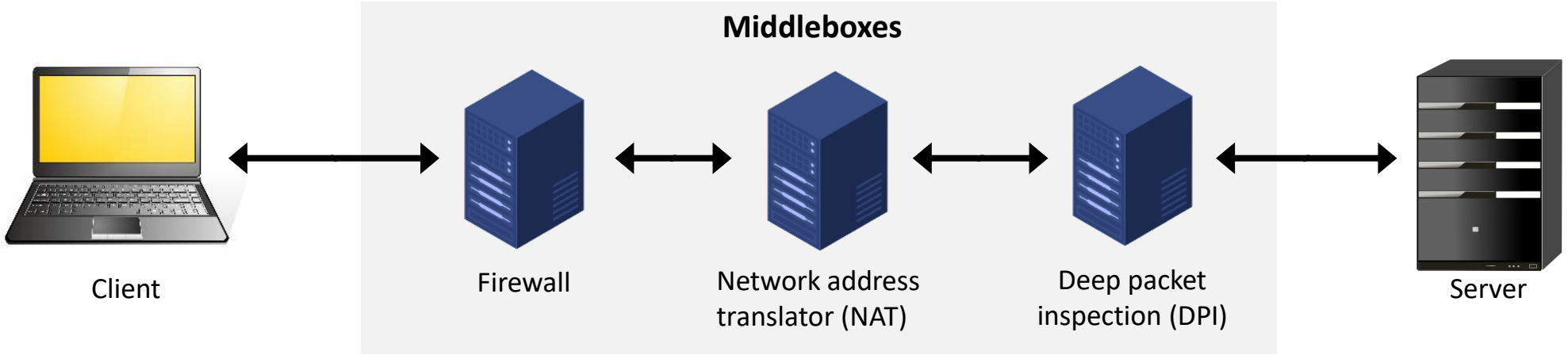
Hardware



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 LIVE PRODUCTION ENVIRONMENT

Smals ICT for society

Agenda

- Intro / recap
- Crypto Agility in the Public Sector
- Crypto inventory
- Crypto Policy as Code
- Cryptography in Hybrid mode
- Challenges
- **Conclusions**

Smals ICT for society

Crypto-Agility Maturity Model (CAMM)

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

Initial / Not possible

At least one subsystem or component violates L1 requirements

0

Possible

Systems can be adapted to respond dynamically to future crypto challenges

1

Knowledge

- System knowledge
- **Cryptography inventory**

Process

- Updateability
- Reversibility

System property

- Extensibility

Prepared

Actual crypto migration still requires some preparatory work

2

Knowledge

- Algorithm IDs

System property

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

Practiced

Crypto migration demonstrable, effectively and securely feasible

3

Knowledge

- Performance awareness
- Secure crypto agility

Process

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

System property

- Hardware modularity
- Backwards compatibility

Sophisticated

Enables fast crypto migration, applied on broader infrastructure

4

Process

- Automation
- Scalability
- Real-time

System property

- Context independence
- Cross-system interoperability

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

Smals ICT for society

Crypto-Agility Maturity Model (CAMM)

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

Initial / Not possible

At least one subsystem or component violates L1 requirements

0

Possible

Systems can be adapted to respond dynamically to future crypto challenges

Knowledge
- System knowledge
- Cryptography inventory

Process
- Updateability
- Reversibility

System property
- Extensibility

1

Prepared

Actual crypto migration still requires some preparatory work

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

2

Practiced

Crypto migration demonstrable, effectively and securely feasible

Knowledge
- Performance awareness
- Usability of crypto agility

Process
- Policies
- Compliance testing
- Interoperability PCA
- Transition mechanism
- Effectiveness

System property
- Hardware modularity
- Backwards compatibility

3

Sophisticated

Enables fast crypto migration, applied on broader infrastructure

Process
- Automation
- Scalability
- Real-time

System property
- Context independence
- Cross-system interoperability

4

CRYPTOGRAPHIC AGILITY IS A JOURNEY

(NO OFFICIAL MAPS AVAILABLE YET)

SMALS IS AN EARLY ADOPTER AND HAS STARTED THE WALK

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

Smals ICT for society

Advice from 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

Source: KPMG, BSI. Y YO Y . 22/08/2023.

Smals ICT for society

Thanks for your attention!

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

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

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

CYBERSEC

Smals
ICT for society