Privacy-Enhancing Cryptography In the Post-Quantum Era

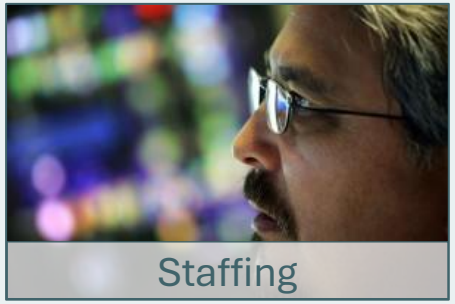
Kristof Verslype (PhD)
Smals Research - Belgian public sector

Smals
ICT for society

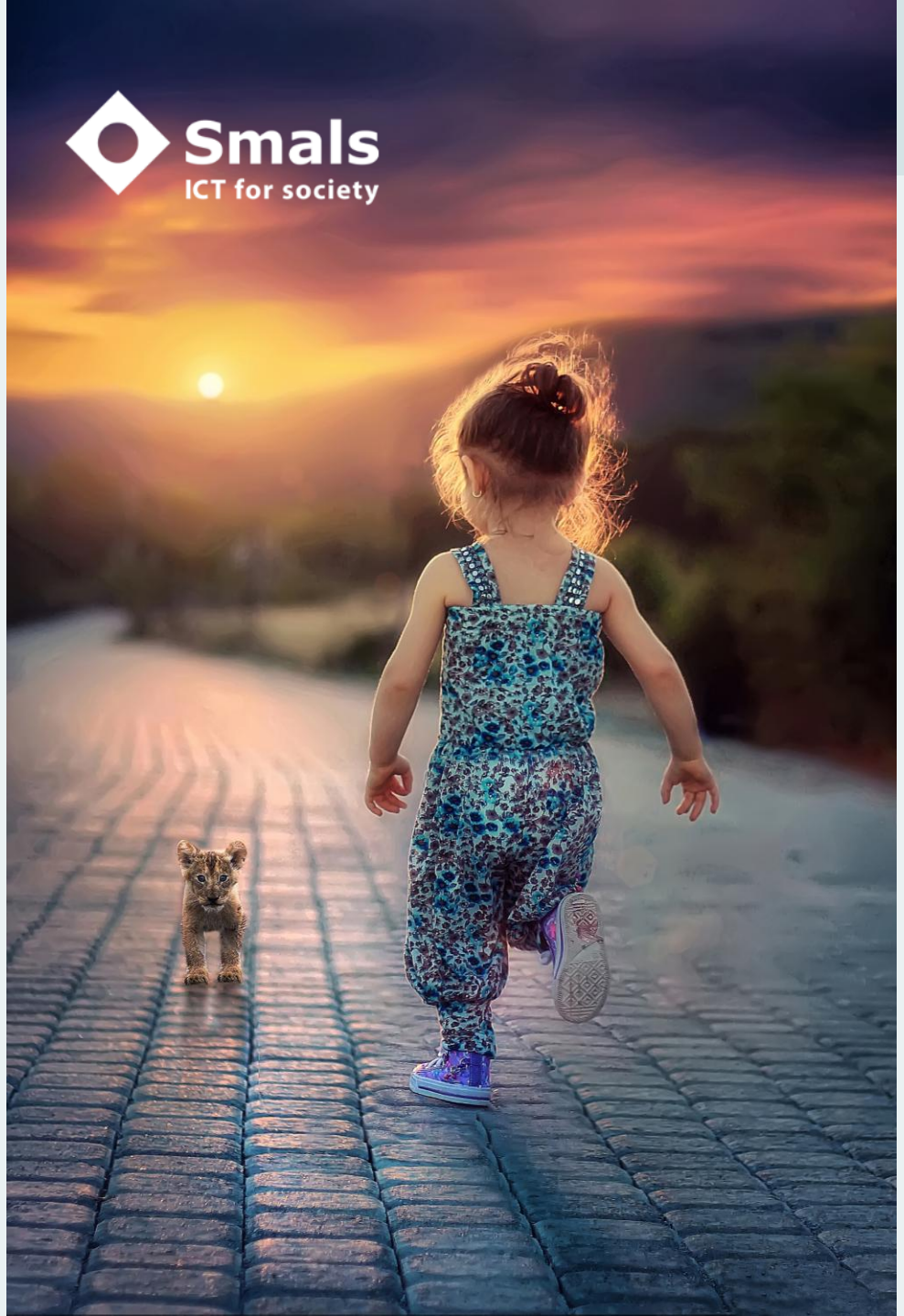
Support e-government


Knowhow


Development


Staffing


Infrastructure



g-cloud

top EMPLOYER BELGIË BELGIQUE
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

The workhorses of cryptography

All standardized

Cryptography class	Primitive type
Symmetric cryptography	❖ Symmetric encryption ❖ Message authentication code (MAC)
Hash functions	❖ Hash functions
Public-key cryptography	❖ Key Exchange Mechanism (KEM) ❖ Digital signatures

Quantum vulnerable. PQC alternatives (being) standardized



Is this the full story for PQC migration?

An extensive wildlife of non-standardized cryptography



Privacy-enhancing cryptography (PEC)

Zero-Knowledge Proofs

Prove that you know/have something that you want to keep secret

Oblivious transfer

Request a record out of a list without disclosing which record

Private Set Intersection

Parties find items they have in common while hiding any other data from their private sets

Fully Homomorphic Encryption

Computing on encrypted data

Anonymous credentials

Selectively disclosing personal properties

Multi-Party Computation

Collectively computing a function on secret inputs

Blind Identifier Pseudonymisation

Convert citizen id from/to pseudonym (=unique code) without seeing these data

Oblivious Pseudo-random Function

Calculate pseudorandom function, only client learns output, server hides key

Very powerful cryptography with potential
How quantum safe is this?

Zero-Knowledge Proof (ZKP)

One party to proves a claim to another party without disclosing further details about that claim

Google

Google's 2026 paper on breaking ECC with CRQC: Prove benchmarks without disclosing details.

Zcash Aztec STARKNET ZKsync

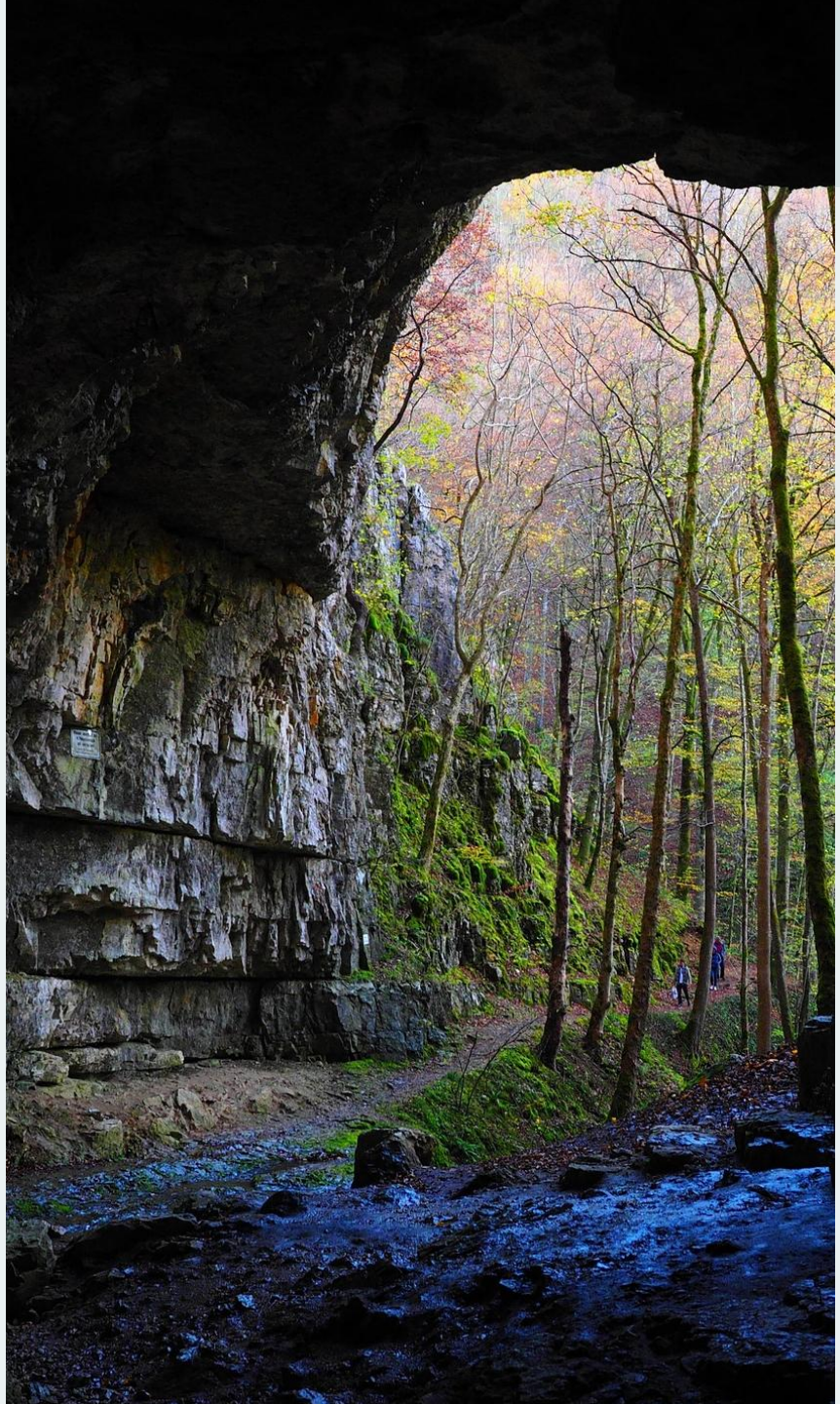
Prevalent on blockchain networks for privacy/confidentiality, but also scalability

Google VUB VRIJE UNIVERSITEIT BRUSSEL

Selectively disclose personal properties of legacy identity documents (e.g. Google Longfellow)

In summary

- Prevalent ZKP technologies quantum vulnerable
  - E.g. zk-SNARKs, Bulletproofs
- Quantum-safe alternatives
  - zk-STARKs. Proofs orders of magnitude larger
  - LaZer. Efficient, but still research library

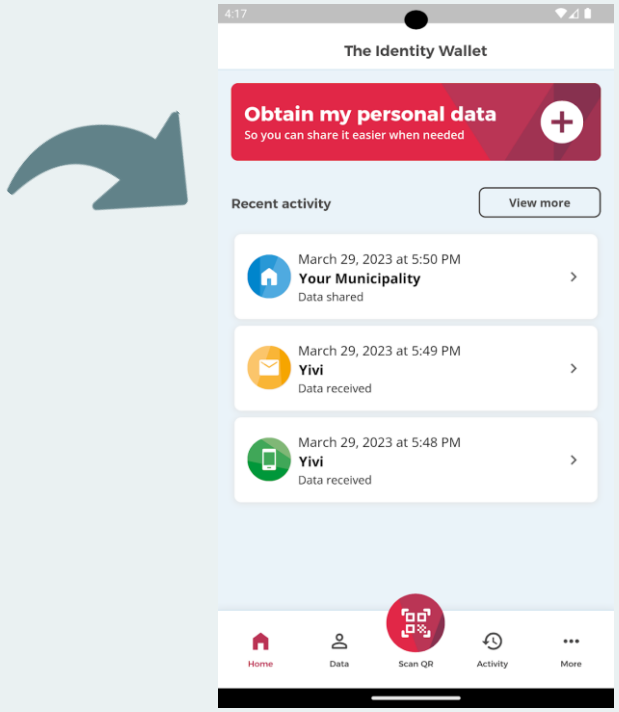


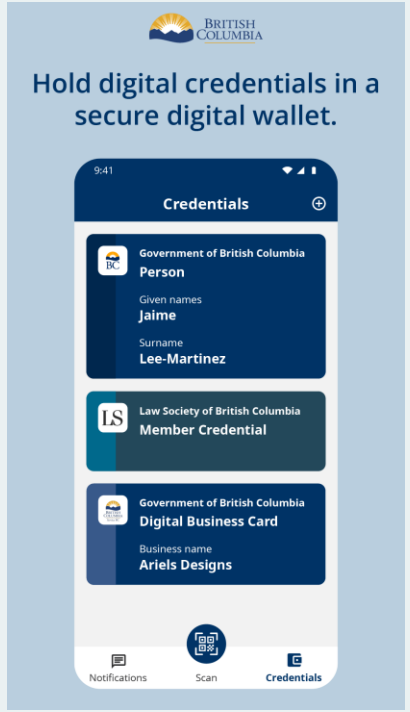
Anonymous credentials

- Selectively disclosing personal properties, derived from a digital identity document
- E.g., prove age > 18 based on document that contains social security number, year of birth, address, …

yivi

- Identity solution for citizens
- Municipality of Nijmegen, KYC in the banking sector, experiments in healthcare sector





Signal

Private groups where membership information is only visible to group members, hidden from service provider or anyone outside the group

intel

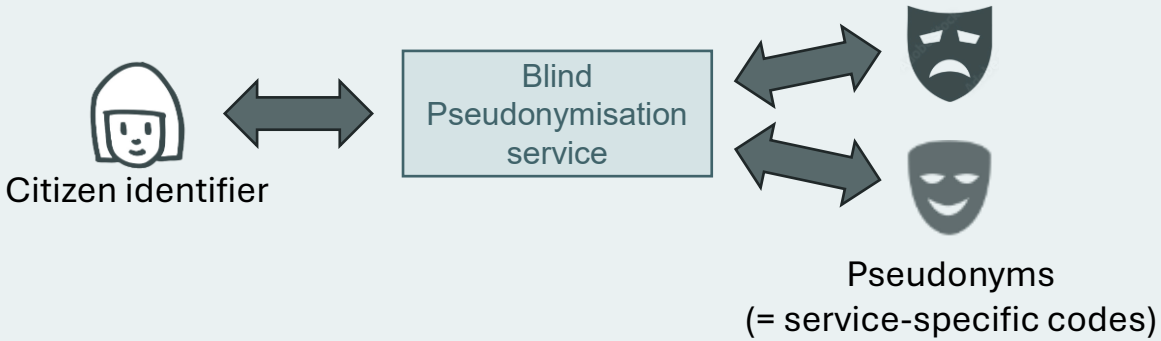
- Authenticity of Trusted Execution Environments
- On hyperscalers (Azure, AWS, Google Cloud, …)
- > 2.5 billion EPID credentials issued

In summary

- All quantum vulnerable
- Only a few quantum-resistant systems proposed
  - Much less efficient in computation and communication (50x)
  - Less mature / research phase

Blind Identifier Pseudonymisation

- Each service knows you / your data only under a unique code, not under your identifier (e.g. BSN, RRN, Steuer-ID, ΠΑ, …)
- Citizen ids and pseudonyms hidden for Pseudonmisation service



egezondheid

Storage of medical data under pseudonyms

DigiD

Main tool for citizen authentication

In summary

- Current solutions quantum vulnerable
- Attempts being made to devise efficient quantum-safe alternatives



Fully Homomorphic Encryption (FHE)

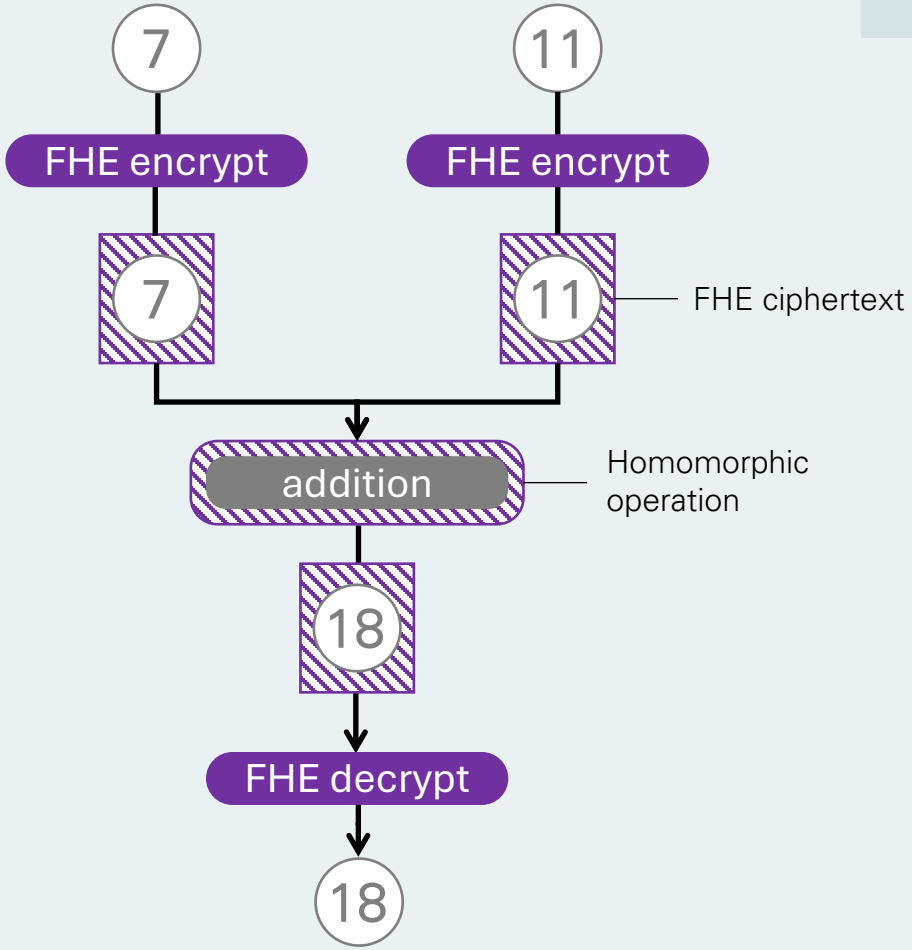
Compute on encrypted data

Microsoft

- Password Monitor in Microsoft Edge
- Check if password is on server-side list of compromised passwords

- Private information retrieval (PIR)
- Caller ID and spam blocking (E.g URL to adult content).

- Private Nearest Neighbor Search (PNNS)
- Identifying points of interest (POI) on picture taken with smart phone



In summary

- ✓ Quantum safe
- ✓ Very active field
- ✗ Still slow
- ✗ Hard to use
- ✗ Not standardized

→ Uptake today minimal

Privacy-enhancing cryptography (PEC)

Zero-Knowledge Proofs

Prove that you know/have something that you want to keep secret

Oblivious transfer

Request a record out of a list without disclosing which record

Private Set Intersection

Parties find items they have in common while hiding any other data from their private sets

Fully Homomorphic Encryption

Computing on encrypted data

Anonymous credentials

Selectively disclosing personal properties

Multi-Party Computation

Collectively computing a function on secret inputs

Blind Identifier Pseudonymisation

Convert citizen id from/to pseudonym (=unique code) without seeing these data

Oblivious Pseudo-random Function

Calculate pseudorandom function, only client learns output, server hides key

Competitive quantum-safe schemes available

Quantum-safe alternatives come with serious performance penalty (computational and/or communication)

No practical, enterprise-ready quantum-safe alternatives

In summary

- Doesn't look great now, but a lot of progress being made
- PEC lagging behind standardized public-key cryptography (KEMs & digital signatures)
- Quantum-safe alternatives often based on lattices

Privacy-enhancing cryptography (PEC)

Zero-Knowledge Proofs

Prove that you know/have something that you want to keep secret

Oblivious transfer

Request a record out of a list without disclosing which record

Private Set Intersection

Parties find items they have in common while hiding any other data from their private sets

Fully Homomorphic Encryption

Computing on encrypted data

Anonymous credentials

Selectively disclosing personal properties

Multi-Party Computation

Collectively computing a function on secret inputs

Blind Identifier Pseudonymisation

Convert citizen id from/to pseudonym (=unique code) without seeing these data

Oblivious Pseudo-random Function

Calculate pseudorandom function, only client learns output, server hides key

Can all be realized with FHE

- Smals research experimented with FHE-based blind identifier pseudonymization
- By extrapolation: Does it make sense to realize multiple PEC categories with FHE?

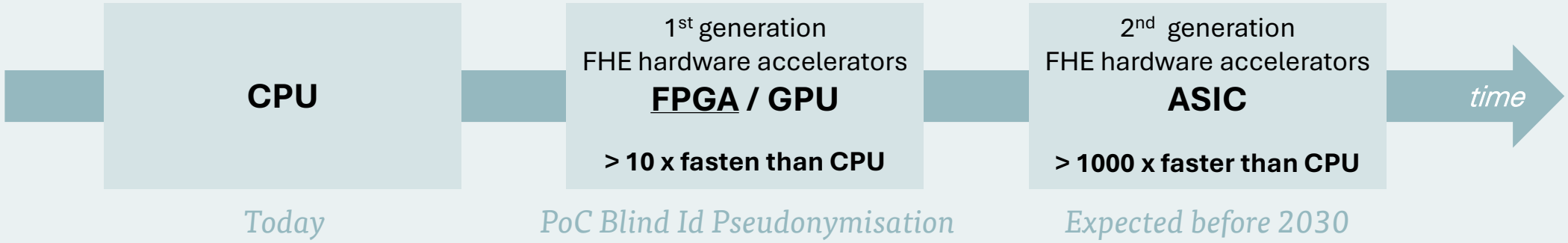
But FHE is slower than a snail!



FHE is becoming faster

Drivers

- Efficiency improvements of algorithms
- Efficiency improvements of algorithm implementations
- FHE Hardware accelerators being developed



Broader adoption of FHE expected

FHE Hardware Acceleration



Our partner in the blind id pseudonymisation PoC

Ambitions

- Accelerate FHE by multiple orders of magnitude
- Make FHE practical

Commercial sector most interested in

1. FHE
2. ZKP

Other players: Cornami, Intel, Optalysis, …

FHE Standardization efforts

NIST

- National Institute for Standards and Technologies
- Preparing possible future standardization

https://csrc.nist.gov/projects/pec/fhe

ISO/IEC

- ISO/IEC 28033 series (under development)
- BGV/BFV, CKKS, and TFHE

https://www.iso.org/standard/87638.html

FHE Technical Consortium on Hardware

- The industry body for Fully Homomorphic Encryption hardware
- Ensure Inter-compatibility

https://csrc.nist.gov/projects/pec/fhe

HomomorphicEncryption.org

- An Open Industry / Government / Academic Consortium to Advance Secure Computation
- https://homomorphicencryption.org/



Most likely 1st privacy-enhancing cryptography to be standardized (before ZKPs)

FHE as building block?

Properties

- **Quantum-safe**
- **Generic:** Enables to easily realize many other PEC types
- But needs **hardware acceleration** (like GPUs)

Current state

- Today generally **too slow,** but a lot of **progress** ongoing
- Most **interest** from **commercial sector** & **standardization bodies**



Enterprise view

Does it make sense to realize multiple PECs with FHE?

One standardized core solution

- ❖ Simplifies maintenance
- ❖ Reduces cost
- ❖ Reduces risks & liabilities

Conditions

- ❖ Fast
- ❖ Cost-efficient
- ❖ Standardized

Maybe, but it will take time to get there…

Back to the reality of today …



EU Roadmap

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

23 June 2025



31/12/2026

- National PQC transition roadmap
- Perform quantum risk analysis
- Support and promote mature cryptographic asset management (crypto inventory)

31/12/2030

- **Transition completed of high-risk use cases**
- **Support crypto agility**
- Allocate resources for transition

31/12/2035

- **Transition completed of medium-risk use cases**
- Transition completed of low-risk use cases as much as feasible

Very challenging timeline for PEC!

Conclusions

Privacy-enhancing cryptography under siege

- Deployed in real-world use cases
- Not standardized
- Often quantum-vulnerable
- Efficient & mature alternatives often unavailable today
- A lot of research ongoing

→ **Migration lags behind standardized cryptography**

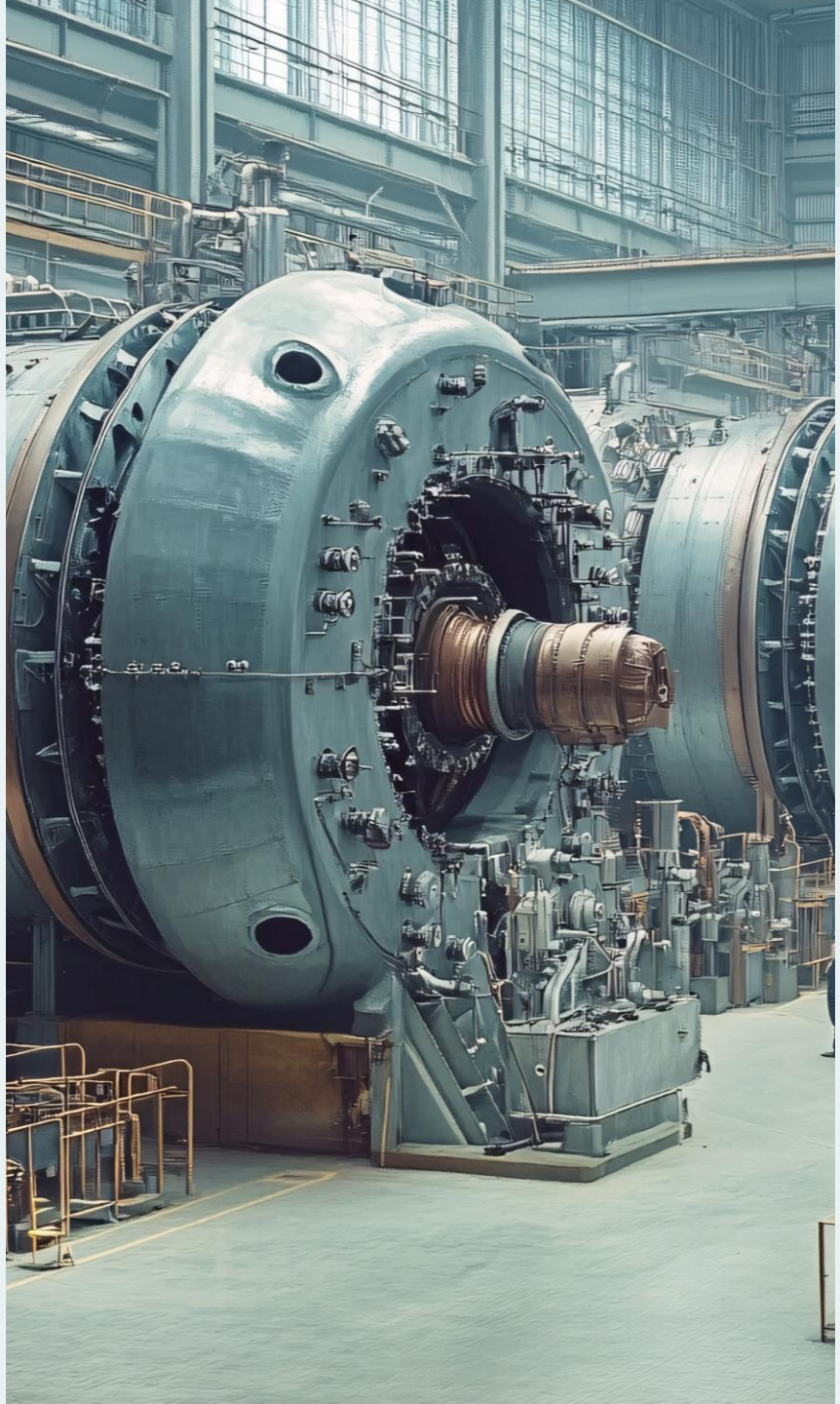
Our approach

✓ Prioritize [1]

1. Standardized public-key cryptography
2. Other crypto, including privacy-enhancing crypto
3. Symmetric cryptography

✓ Prepare

- Risk assessment
- Roadmap
- Crypto agility
- Experiment



[1] https://bughunters.google.com/blog/googles-threat-model-for-post-quantum-cryptography

QUANTUM-SAFE BLIND ID PSEUDONYMISATION

Interested? Contact us!

Together, we increase the chance to have a cost-efficient, fast and flexible solution that is enterprise-ready on time!

BLOGPOST

Sharing healthcare data without exposing patients' identity

Stay tuned!
https://belfortlabs.com/blog



BELGIUM

Guide on preparing for the quantum era and transitioning to postquantum cryptography

VOLUME 01

Preparing for the Quantum Era

Updated Strategic Guidance

Introduces quantum threat, raises awareness, provides updates on timelines, policy developments, and the urgency of post-quantum migration.

Target audience: decision-makers.

Publication date: 22 September

VOLUME 02

Managing the PQC Transition

Governance, Planning and Investment

Explains what is needed to initiate a PQC transition within an organisation, including governance, planning, responsibilities, funding considerations, and coordination across stakeholders.

Target audience: security, risk and compliance (GRC) teams, project managers and technical coordinators.

Publication date: 20 October

VOLUME 03

Implementing the PQC Migration

Technical and Migration Guidance

Technical guidance on postquantum cryptography and PQC migrations, including algorithm choices, implementation considerations, interoperability, testing, and operational deployment.

Target audience: engineers, developers, IT architecture and operations teams.

Publication date: 20 November

CYBER SECURITY COALITION

quantum circle



Thank you!

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