Roadmap for the Transition to Post-Quantum Cryptography

Fabiana Da Pieve

Program Manager
Unit C.4 “Emerging and Disruptive Technologies”
Directorate General for Communications Networks, Content, and Technology (DG CONNECT)

If a large quantum computer can be built … what happens ?

Devastating effects on society at all levels, economy, political stability …

At risk: everything ! Data in transit, data at rest, data-in-use

Harvest now-decrypt later attacks already occurring, forging signatures will come later

All modern public-key cryptography has to be replaced [Shor'94]

For symmetric crypto; huge devices would be needed to break it; serial algorithm does not scale impressively

You may double things … but not at the price of public-key cryptography:

Symmetric key sizes: x2 [Grover'96]

Hash function outputs x2 [Grover'96]

See Sam Jacques CHES'24: https://www.youtube.com/watch?v=eB4po9Br1YY

There are, in fact, several transitions

Confidentiality (& could authenticate):
KEY ENCAPSULATION MECHANISMs (KEMs)
Urgent !

- ML-KEM (FIPS 203) – despite some occasional difficulty with its larger key sizes, in several cases it allows for a drop-in upgrade – at least for Post-Quantum Internet
- Sectors with constrained devices: problems

Authentication, integrity and non-repudiation:
SIGNATURES & CERTIFICATES
less urgent but more complex !

- attacks in real time
- use of digital signatures more complex than key agreement
- none of the current PQC signatures scheme is ideal

Other transitions: advanced cryptographic schemes

(anonymous credentials, FHE, …attribute-based encryption, …)

EUROPEAN COMMISSION

Brussels, 11.4.2024
C(2024) 2393 final

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Having regard to Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148[1] (NIS 2 Directive).

HAS ADOPTED THIS RECOMMENDATION

1. SCOPE AND OBJECTIVES

The purpose of this Recommendation is to foster the transition to Post-Quantum Cryptography for the protection of digital infrastructures and services for public administrations and other critical infrastructures in the Union by enabling Member States to:

(1) define a 'Post-Quantum Cryptography Coordinated Implementation Roadmap' aimed at synchronising the efforts of Member States to design and implement national transition plans while ensuring cross-border interoperability;

(2) support the evaluation and selection of relevant Post-Quantum Cryptography EU algorithms with the help of cybersecurity experts, and further adoption of such algorithms as Union standards that should be implemented across the Union as part of the Post-Quantum Cryptography Coordinated Implementation Roadmap.

(3) take appropriate and proportionate measures to prepare for this transition.

2. COORDINATED IMPLEMENTATION ROADMAP ADDRESSING THE TRANSITION TO POST-QUANTUM CRYPTOGRAPHY

(4) This Recommendation encourages Member States to coordinate their actions at Union level through a dedicated Member States forum. For this purpose, the Commission recommends that Member States take advantage of existing structures at Union level in the area of cybersecurity and establish a sub-group of the NIS Cooperation Group. Such sub-group could include representatives of national security agencies and cybersecurity experts, notably from national cybersecurity authorities and ENISA. The sub-group may invite representatives of relevant stakeholders to participate in its work such as those of advisory bodies of public organisations, industry, service providers, and operators, with a view to gather input and exchange information on the transition of digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography in different sectors, coordinate their efforts at national level, and develop the Post-Quantum Cryptography Coordinated Implementation Roadmap, in accordance with the Union competition rules and Union data protection law.

(5) This sub-group on Post-Quantum Cryptography should consider appropriate, effective and proportionate measures for defining and coordinating the development of the Post-Quantum Cryptography Coordinated Implementation Roadmap. The sub-group on Post-Quantum Cryptography is encouraged to engage in discussions with other relevant bodies, such as Europol, NATO, or others, to avoid duplication of efforts and ensure a cohesive approach to addressing emerging challenges.

(6) To this effect, soon after the publication of this Recommendation, Member States are invited to establish such a sub-group on Post-Quantum Cryptography pursuant to Commission implementing decision (EU)2017/179 and to appoint expert representatives who should work in close cooperation with the Commission and who should be tasked to define and develop the Post-Quantum Cryptography Coordinated Implementation Roadmap.

(7) The Post-Quantum Cryptography Coordinated Implementation Roadmap should be available after a period of two years following the publication of this Recommendation, which will be followed by the development and further adaptation of Post-Quantum Cryptography transition plans of individual Member States, in accordance with the principles set out in the Post-Quantum Cryptography Coordinated Implementation Roadmap.

ACTIONS AT UNION LEVEL

(8) The overall work will be monitored and assessed periodically by the Commission in cooperation with the expert representatives of the Member States.

(10) On the basis of those and all other available information the Commission will assess the designed measures and the operation of the network of Member States' representatives and determine whether additional actions, including proposing binding acts of Union law, are required.

experts

targets

by when

what

active role

monitoring

who will do the work

additional measures

Roadmap for a Coordinated Transition across EU

New PQC workstream in the NIS Cooperation Group created

First version of the Roadmap released (June 2025):

Timeline:

- By 31/12/2026. PQC roadmaps defined in each MS. Planning for high- and medium-risk use cases will be underway.
- By 21/12/2030: high-risk use case migrated: critical infrastructure (eg water, energy, health care, finance and transportation) and high-risk domains. Quantum-safe software and firmware upgrades are enabled by default. Transition planning for medium-risk ones.
- By 31/12/2035. All of the migrations should be completed for every risk level.

https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

Strong hook to the Cyber Resilience Act in the Roadmap

Necessity for consideration of EU Cybersecurity Policies in National Actions

Roadmap – more in detail – first and next steps

End of 2026 | **End of 2030** | **End of 2035**

Milestone 1: 31.12.2026

- First Steps:
  - Identify and involve stakeholders.
  - Support mature cryptographic asset management.
  - Create dependency maps.
  - Perform quantum risk analysis.
  - Include the supply chain.
  - Create a national awareness and communication program.
  - Share knowledge and get involved with the NIS CG work stream on PQC.
  - Develop a timeline and an implementation plan.
- **Main achievements**:
  - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
  - Initial national PQC transition roadmaps have been established by all Member States.

Milestone 2: 31.12.2030

- Next Steps:
  - Support cryptographic agility and a quantum-safe upgrade path.
  - Allocate resources for the transition.
  - Adapt certification schemes.
  - Evolve the rules.
  - Look for opportunities within the ecosystem.
  - Considering transversal activities throughout the creation and implementation of the roadmap.
  - Implement pilot use cases and contribute to testing centres.
- **Main achievements**:
  - The PQC transition for high-risk use cases has been completed.
  - PQC transition planning and pilots for medium-risk use cases has been completed.
  - Quantum-safe software and firmware upgrades are enabled by default.

By **31.12.2035**:

The PQC transition for medium-risk use cases has been completed.

The PQC transition for low-risk use cases has been completed as much as feasible.

Strong hook to the Cyber Resilience Act in the Roadmap

Necessity for consideration of EU Cybersecurity Policies in National Actions

Roadmap builds on lessons learnt from the past

Take action as soon as possible !
We don't know when quantum computers will break today's crypto, but:

- attackers store now, decrypt later;
- devices deployed today remain in the field for decades;
- migration takes time and may not be smooth.

Use hybrid deployments

- Combine PQC with traditional schemes – traditional schemes must NOT be weakened
- Security as long as one of the two schemes is secure
- Weakened encryption impedes the migration to PQC

Supply chain security (HW and SW) – and contribute to transparent standardization activities

- Enabling Quantum-safe software and firmware upgrades by default, by 2030

Symmetric methods instead of public-key cryptography are also worthwhile to consider, depending on the application

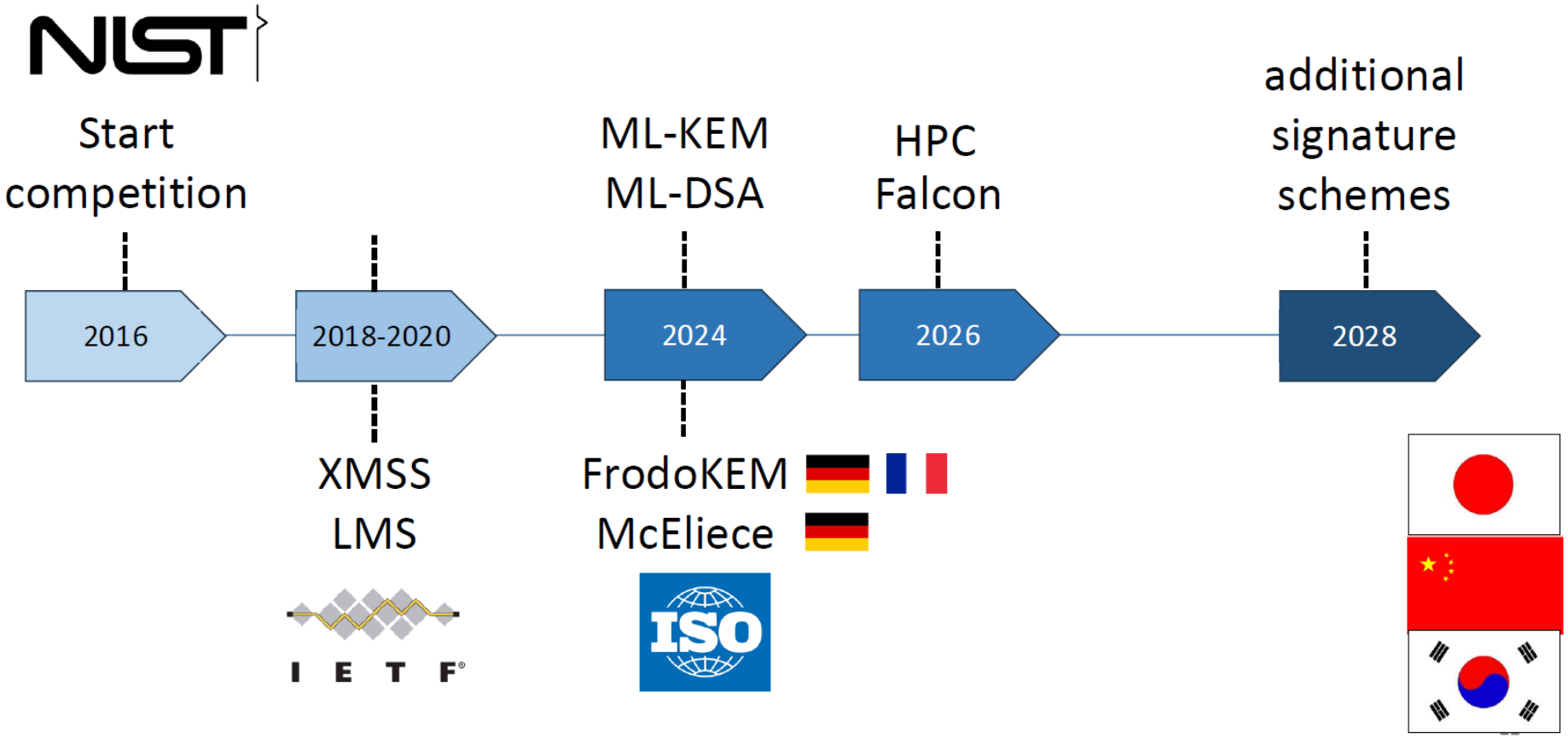
Crypto-Agility as fundamental aspect

It is important that all implementations of cryptography be “crypto-agile”: cryptographic routines and ciphers can be easily upgraded or replaced without having to completely replace the underlying application or device.

Need for: Interoperability, diverse technical requirements, rapid update cycles

Type of Agility	Definition
Implementation	The Capability to swiftly configure interfaces and implement updates across various systems or applications
Compliance	The capacity to adapt cryptographic configurations in accordance with compliance requirements.
Security Strength	The capability to dynamically adjust the level of security strength based on configuration, allowing for scalable security measures.
Migration	The capability to transition and convert between cryptographic algorithms seamlessly.
Retirement	Ability to retire obsolete or insecure cryptographic algorithms
Composability	The capability to securely integrate multiple cryptographic primitives for composability.
Platform	Ability to use assured cryptographic algorithms across different platform types
Context	Ability to use a derived cryptographic algorithm policy with the flexibility from system attributes

Timeline standardization



Impact of the PQC transition on (some of the) relevant areas related to data protection

EUDI wallet

Data and personal data processing (Cloud, AI-training, ...)

Age verification protocols

Impact of the PQC transition on EUDI Wallet is **pervasive**

https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

"Technologies used to achieve those objectives should be developed aiming towards ***the highest level of security, privacy, user convenience, accessibility, wide usability and seamless interoperability.*** *"*

"Trust in European Digital Identity Wallets would be enhanced if issuing and managing parties are required to implement appropriate technical and organisational measures to ensure ***the highest level of security that is commensurate to the risks raised for the rights and freedoms of the natural persons****, in accordance with Regulation (EU) 2016/679."*

"European Digital Identity Wallets should ensure ***the highest level of data protection and security for the purposes of electronic identification and authentication to facilitate access to public and private services, irrespective of whether such data is stored locally or on cloud-based solutions****, taking due account of the different levels of risk."*

"European Digital Identity Wallets should be secure-by-design and should implement advanced security features to protect against identity and other data theft, denial of service and any other cyber threat. Such security should include ***state-of-the-art encryption and storage methods that are accessible only to, and decryptable only by, the user and that rely on end-to-end encrypted communication with other European Digital Identity Wallets and relying parties****."*

→ at this moment PQC for such advanced applications is under strong investigation efforts, and must be ready by 2030

Impact of the PQC transition on EUDI Wallet is **pervasive**
(continuation)

https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

"To ensure that the European Digital Identity Framework is open to innovation, technological development and future-proof,"
→ seems mostly about testing ....
however, it ends with *"thus preventing the development of solutions that do not comply with Union law on data protection or that are open to security vulnerabilities."*
→ So development NOT allowed for unsecure solutions ! a quantum computer would bring an acute security vulnerability
→ And CRA anyway requires long-term security

"Trust service providers should use cryptographic methods reflecting ***current best practices and trustworthy implementations*** *of those algorithms in order to ensure security and reliability of their trust services."*

"Member States should integrate different privacy-preserving technologies, such as zero knowledge proof, into the European Digital Identity Wallet. Those cryptographic methods should allow a relying party to validate whether a given statement based on the person's identification data and attestation of attributes is true, without revealing any data on which that statement is based, thereby preserving the privacy of the user."

Impact of the PQC Roadmap on the EUDIW

Anonymous credential systems

Current plans seem to be suboptimal in terms of Security AND Privacy

- commodity random-oracle signature scheme (**ECDSA**) and hacky ad-hoc techniques to achieve (some of) the privacy properties
- users will get batches of many signatures at a time so that they only need to present each signature once

This does NOT:

- prevent linkeability with respect to the issuing party, required from the law
- offer quantum-resistance …

So … which PQC digital signatures ? Instantiated by which Zero-Knowledge Proofs ?

- Possibly, development general lattice-based zero-knowledge proof systems
- Improvement of their performance and proof sizes

Impact of the PQC transition on data and personal data processing (Cloud, AI-training, …)

Numerous cloud-based applications, where data is not only externally stored, but externally computed upon

Data confidentiality can hence be lost to the cloud provider, any entity who hacks the cloud provider, and any entity that has legal authority on the cloud provider

Protection needed for numerous cloud-based applications:

- database management
- delegation of machine learning inference and training
- delegated statistics, etc notably for financial data, medical data, government data and individuals' private data

Specific examples:

Protecting huge databases (biometrics, searches in text, searches in DNA, searches in movies) - compute on data protected via quantum-safe Fully Homomorphic Encryption (FHE) → avoid personal data leakage

Protecting machine learning queries and model training. AI requires a lot of data to be effective, but this impacts privacy. FHE allows to remove this tension between functionality and privacy.

Need for: theory, computational acceleration, standardization and certification

Conclusions

There is no 100% certainty if or when a quantum computer will break RSA & ECC

But we need to migrate:

- hybrid deployments (PQC & current public-key cryptography)
- **we need a huge efforts in pilot projects with testing PQC-solutions**
- crypto-agility is a key concept

Thank you for your attention

Quantum Risk-based approach

Perform quantum risk analysis to help prioritisation of the transition process

Three basic quantum risk levels “high”, “medium” and “low”, defined on the how an application or system is influenced by three factors:

- the quantum weakness of the cryptography used;
- the expected impact of the used cryptography being broken;
- the estimated time and effort required to migrate to PQC.

Examples of high-risk levels:

If confidentiality needs to be protected for a long time period (at least 10 years), and an attack after 10 years or more would still have significant impact

if the transition effort is high (taking more than 8 years) and the impact of an attack is high, for example for securing software updates

Global landscape

Image from PQShield - do NOT re-use

Impact of the PQC Roadmap on the EUDIW

- eIDAS Regulation mandates strong privacy guarantees
- Current plans seems to be suboptimal in terms of Security AND privacy
- Crypto-agility !
- Advanced cryptographic schemes: anonymous credentials …

- which PQC digital signatures ?

- instantiated by which zero-knowledge proofs ?

- **bring the functionality of lattice-based proof systems to the state of PCP-type ones**
- **improving their performance and proof sizes to levels that are orders of magnitude better than the state of the art**

Conclusions

We do not know with 100% certainty if or when a quantum computer will break RSA & ECC

But we can’t take the risk

Need to move:

- risk-based approach
- crypto-agility
- hybrid deployments (PQC & current public-key cryptography)
- symmetric methods instead of public-key cryptography also worthwhile to consider, depending on the application
- refinement EU-level strategy

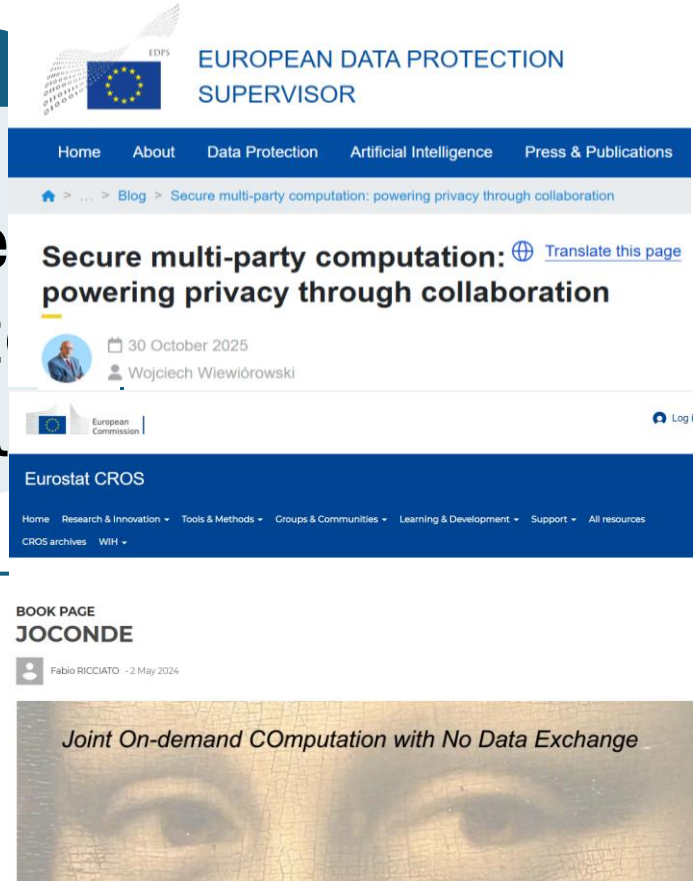
International alignment

The legislative landscape is changing

Impact of the PQC transition on (some of the) relevant areas related to data protection

Data processing (Cloud) → Secure Multiparty Computation

Cose da Damie
Stehle suggerit
per le nuove cal



[Transition to post-quantum Public Key Infrastructures (10 mln, 10 proposals)]

[JOCONDE | Eurostat CROS]

IMP - Confidential computing and cloud – ANSSI - https://cyber.gouv.fr/en/publications/technical-position-paper-confidential-computing

Mohamad HajjMohamad Hajj • 2ndVerified • 2ndCybersecurity Solution Manager | Certification & Standardization Specialist | Trainer | MBR ENISA AHWG EU 5G scheme and ORAN Security Focus Group/WG11 | (5G, Cloud, O-RAN, eUICC, IoT, QSCD, EUDI, Automotive)Cybersecurity Solution Manager | Certification & Standardization Specialist | Trainer | MBR ENISA AHWG EU 5G scheme and ORAN Security Focus Group/WG11 | (5G, Cloud, O-RAN, eUICC, IoT, QSCD, EUDI, Automotive)
Visit my website
4d • 4 days ago • Visible to anyone on or off LinkedIn

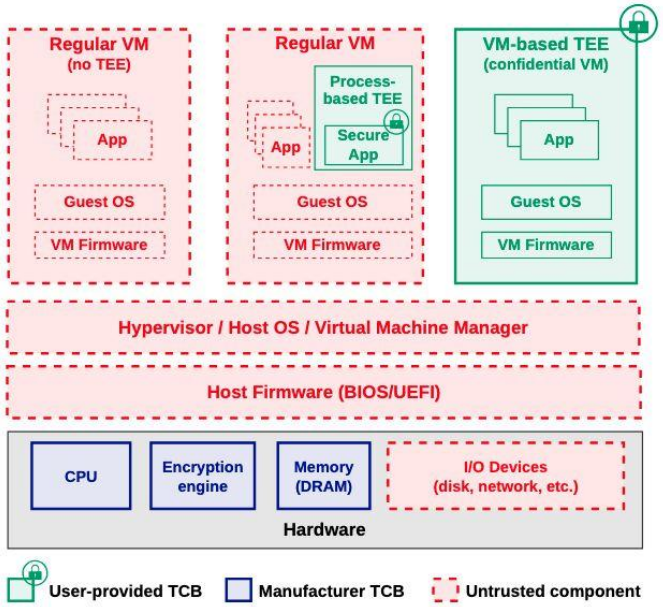
hashtag#Confidential hashtag#Computing is often presented as the missing piece for moving sensitive workloads to the cloud: protect data at hashtag#rest, in hashtag#transit, and now also "in hashtag#use".
In its new technical position paper, **ANSSI - Agence nationale de la sécurité des systèmes d'information** provides a very useful reality check:

- Confidential Computing can harden memory and reduce the Trusted Computing Base (hashtag#TCB), making some attacks from the host or other tenants more complex.
- However, it is not sufficient against a targeted, hostile administrator or a compromised supply chain. Under this threat model, dedicated hardware you can trust is still required.
- Secure use is far from trivial: workloads must be hardened against host-driven attacks, and remote attestation plus secret provisioning must be designed correctly for the entire TCB.
- Today, ecosystems and tools for end-to-end attestation and secret delivery are still immature.
- On its own, Confidential Computing is not enough to meet the expectations of hashtag#SecNumCloud 3.2 section 19.6.

The paper provides guidance both for:
- hashtag#users (how to define the threat model, design the TCB, tie attestation and secrets, and when not to rely on Confidential Computing);
- hashtag#service hashtag#providers (what is needed to make confidential VMs and enclaves verifiable, manageable and evaluable).

For anyone working on hashtag#cloud, SecNumCloud, hashtag#virtualisation, or hashtag#CRA-aligned hashtag#standards, this is an important reference.

https://cyber.gouv.fr/en/publications/technical-position-paper-confidential-computing



VERY IMPORTANT:

Johnny Da Silva • 2nd
Chef d'entreprise @ Axians | Expert MultiCloud, Cybersécurité, Services Managés & Transformation Numérique
4d
This summary by ANSSI underscores how Confidential Computing is maturing but still faces significant limitations from both a technical and regulatory perspective. While moving sensitive workloads to the cloud is now more attractive thanks to secure execution environments and attestation mechanisms, organizations cannot view Confidential Computing as a panacea. Regulations like SecNumCloud 3.2 highlight that requirements for sovereignty, confidentiality and integrity go well beyond what is possible with just TEE-based protections.

There are, in fact, several transitions

Confidentiality (& could authenticate):
KEY ENCAPSULATION MECHANISMs (KEMs)
Urgent !

- ML-KEM (FIPS 203) – despite some occasional difficulty with its larger key sizes, in several cases it allows for a drop-in upgrade – at least for Post-Quantum Internet
- Sectors with constrained devices: problems

Authentication, integrity and non-repudiation:
SIGNATURES & CERTIFICATES
less urgent but more complex !

- attacks in real time
- use of digital signatures more complex than key agreement
- none of the current PQC signatures scheme is ideal

Other transitions: advanced cryptographic schemes

(anonymous credentials, FHE, …attribute-based encryption, …)

Problems with devices with long service lifetimes, difficult to upgrade once deployed: *satellites in orbit, sensors in cars, airplanes, cell phone towers, smart water and electricity meters in people's homes, chips in a 10-year ePassport, …*

Air-gapped systems: some critical infrastructures relying on OT …

Roadmap – steps towards second release

August 2025	End September 2025	October 2025	Beginning November 2025	by 10th of April 2026
Open for public comments for feedback to 1st release	Collect comments on 1st release + interest from different sectors to contribute with new text specific for sectors for the 2nd release	Elaborate and incorporate input from first consultation Start a second round with people/sectors willing to contribute for specific sectors	Work on text together with experts from the different sectors	**Final version** after many iterative steps with experts from the different sectors

Outstanding EU contributions to NIST competitions

Chen IACR 2024/555

Purpose	Standard	Title	Scheme	Underlying Problem Class
KeyAgreement	FIPS 203	ML-KEM	CRYSTALS-Kyber	Module LWE **(structured lattice)**
Digital Signatures	FIPS 204	ML-DSA	CRYSTALS-Dilithium	Module LWE **(structured lattice)**
	FIPS 205	SLH-DSA	SPHINCS+	SHAKE, SHA-2 (symmetric primitives)
	FIPS (due 2024)		FALCON	NTRU lattice **(structured lattice)**
Key Agreement			BIKE	QC-MDPC codes (structured code)
	Fourth round reserves		HQC	QC-MDPC codes (structured code)
			Classic McEliece	Code based (well studied, v. large key)
Digital Signatures	Additional call; round one		40 entries: 8 broken, 13 attacked	Entries across seven families

Univ. Radboud, NL, Univ. Bochum, DE, NXP, BE

Univ. Radboud, NL, Univ. Eindhoven, NL, Fraunhofer Darmstadt, DE

France

SIKE broken

Univ. Bochum, DE, INRIA, FR

Univ. Toulouse, Limoges, Toulon, Bordeaux FR

Univ. Eindhoven, NL, INRIA, FR, Univ. Southern Denmark, DK

HQC chosen as new key agreement next to Kyber

Also for this additional call outstanding EU contributions

Standardization
Outstanding EU contributions to NIST competitions

(some) Ongoing, past, just started EU projects
Horizon Europe, DEP, H2020

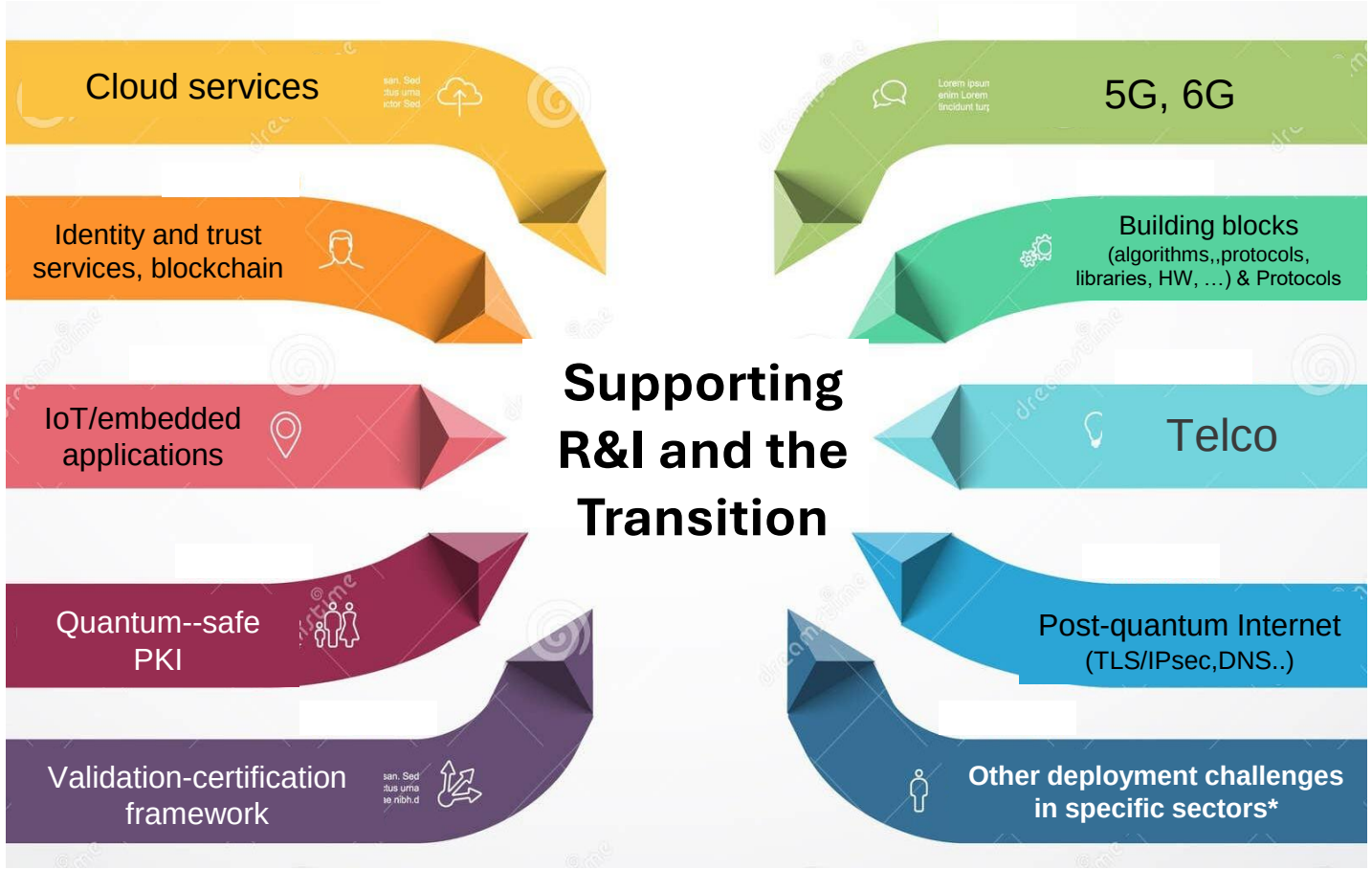
PQCRYPTO, FOCAL

QUBIP, PQC4eMRTD, PQ-REACT, PROMETHEUS, PRIViLEDGE NGI-SARGASSO PQ-NEXT POSEIDON

QUBIP, PQCRYPTO, FOCAL

PQC4eMRTD, PiQASO, HAPKIDO (NL, national)

WORK IN ECCG CHAIRED BY ENISA



CONFIDENTIAL6G, XTRUST-6G

QUBIP, ERC EPOQUE (integ. in procotols), ERC ARTICULATE (libraries), SAFECrypto, PiQASO (HW), ERC ISOCRYPT (non-lattice based), ERC BRIDGE (asymm+symm crypto) Q-FENCE (HW acceleration) QARC

QUBIP, PQ-REACT, PQ-NEXT

QUBIP, PQCRYPTO

Automotive (PQCSA)
Financial sector (NGI-TALER, EPOQUE, PQ-NEXT, FORTRESS)
Administrations (Q-PrEP)
Several industrial sectors (PIQASO)
Defence (SMiEQ)
Critical Infr. (PQ-NEXT)
Work of PQC in space, energy grids …

Digital Identity is no longer an emerging technology - it's the backbone of tomorrow's digital systems

High risk use cases and advanced cryptographic schemes

Prof Bill Buchanan OBE FRSE • Following
Old World Breaker, New World Creator | One of the World's Top 2% Scientists for ...
3d •

ZKPs (Zero Knowledge Proofs) in a browser? With the Bellman Rust library, we have a Groth16 [1] implementation, and can implement Zero Knowledge Proofs, and use WASM integration: https://lnkd.in/egKAWrdM

[1] Groth, J. (2016, April). On the size of pairing-based non-interactive arguments. In Annual international conference on the theory and applications of cryptographic techniques (pp. 305-326). Berlin, Heidelberg: Springer Berlin Heidelberg.

On the Size of Pairing-based Non-interactive Arguments*

Jens Groth**

University College London, UK
j.groth@ucl.ac.uk

Abstract. Non-interactive arguments enable a prover to convince a verifier that a statement is true. Recently there has been a lot of progress both in theory and practice on constructing highly efficient non-interactive arguments with small size and low verification complexity, so-called succinct non-interactive arguments (SNARGs) and succinct non-interactive arguments of knowledge (SNARKs).
Many constructions of SNARGs rely on pairing-based cryptography. In these constructions a proof consists of a number of group elements and the verification consists of checking a number of pairing product equations. The question we address in this article is how efficient pairing-based SNARGs can be.

COSIC (KU Leuven)COSIC (KU Leuven)3,433 followers3,433 followers4h • 4 hours ago • Visible to anyone on or off LinkedIn

Bart Preneel in **VRT** Nws podcast Het Kwartier: "Maximum **hashtag#rivacy** protection is essential for the **hashtag#MyGov** app, combining private and governmental data. There isn't enough time to get it right before the November 20 launch."

https://lnkd.in/eVqiEjKd (in Dutch)

- Put the schemes from the document from ITU-T “T25-SG17-C-0300 “ and “0410”

From Olivier

- * ZK have existed for years, with a boom in usage with cryptocurrencies, and some local anonymous credentials. (i mean... we had anonymous "credentials" on parisian metro cards during my PhD... until they realised that without the anonymity they could do statistics...)
  * Still, there are no large scale projects, and so we need extra care before deploying that (if paolo was a student i would be like "uh, you took some random code over the internet with no security proof and you are not able to explain it?")
  * Modern solutions... well, they are not tested, sometimes not proven, and/or trade real security for efficiency... so we need more time, and that's not something that can be simply fixed later on, security should have been part of the design from the start... [@Anja, i can be the mean one, and try to defend what we wanted to do in the letter]
- * We need to have PQ in mind, right now (or even yesterday), and again... there are solutions that have been published, proven, tested... why start from something new... [Abhi is planning to announce that longfellow could do ML-DSA... while Labrador has existed, and been published for FN-DSA for a while...]
- (This is mostly in line with the french position (ie the lead is more than happy if i say that), and already clash with the EUDIW team...)
- **
- The topics that might/should be interesting
- * Proper hybridization technique [We know how to do hybridization (PQ/standard) for signatures, encryption, but can we do something a little more clever for credentials / ZK ?]
  * Specific ZK for standard (i understand that considering enisa terrible stance on pq standards... it's complicated... but on the other hand, here google can say we handle circuits so yes we will be able to do whatever... so at some point... we need to be able to build and test proper ZK on a specific/specified signature)
  * And it would be nice, to have specific use cases. NIST has "won" and picked general standards, but having calls for "PQ standards" in satellite communication, or credentials for person onboarding in energy/defense contractors would allow more specific design and (oh no) would proscribed US applicants...

From anja Lehmann

- 1) Topics I want to address for the panel (actually quite similar to what I presented in Den Haag this week)
- - we should build a EUDI wallet that follows privacy-by-design, not start with non-privacy solution and then add complex crypto on top to salvage that.
- - well-understood crypto for such privacy-preserving wallets exists.
- Solutions are relatively simple and partially standardised - these schemes have post-quantum privacy, which is main priority for new crypto
- - go for most simple and most mature solution for short/mid-term. Test it on low-assurance use cases (no need to build a Level of Assurance High infrastructure for the national eID from ZKP) --> use is to understand the proper requirements, functional goals and also real-world constraints (this will also help to focus PQC research)
- - avoid dependencies of complex cryptographic libraries and inflexible solution provided by Big Tech (slightly awkward with Abhi/Google on stage)
- - understand that in a ZKP-based solution, security comes from security of signature scheme + security of ZKP
-
- - SNARKs/circuit might appear appealing/simple at first, but they hide complexity in the circuits design. Currently, no generic and easily extendible solutions exist that have an acceptable efficiency or are well-understood enough for short-term deployment
-
- - engage with research community to build PQC-ZKP solutions, and have a public and transparent process (not one driven by Big Tech behind closed
- doors) to determine the best scheme to standardise. Also here, PQC-ZKP solutions have been proposed, but probably are not fully aligned with EUDI requirements yet.
- - main bottleneck for efficient constructions at the moment is limitation coming from Secure Elements - the manufacturer would add more/better APIs if there is a market --> EU should rather lead than follow here, and make clear it wants secure hardware and phones that provides solutions for privacy.
- 2) Hybrid solutions as Olivier said are an interesting and understudied aspect. E.g., in Germany it is currently not allowed to use lattice-based signatures alone. They must be used in combination with classically-secure ones. This will be challenging for ZKP, and we need to think about proper hybrid solutions. In fact, this is yet another motivation why it still makes sense to have *simple* DL-based ZKPs standardised now --> so that they can help with efficient hybrid solutions.

FROM PAPER CRYPTOGRAPHERS ON ARF

- Due to the prevalence of the quantum threat topic and the planning to migrate to quantum safe (aka
- post-quantum) cryptography, we feel that it is important that this also needs to be discussed in context of
- anonymous credentials. We first note that anonymous credentials are used for authentication and thus the
- integrity protection is very short lived and does not need to be guaranteed for a very long time. Consequently,
- as for most use-cases of signatures (apart from specific use cases like long-term archiving), the switch to postquantum
- alternatives is not extremely urgent. This is in stark contrast to encryption schemes, where due to
- the “store now decrypt later” problematic a switch to post-quantum encryption schemes needs to happen
- timely. Otherwise data that needs to be kept confidential for a longer period of time is endangered.
- Moreover, in context of anonymous credentials there is another important aspect to note from a privacy
- perspective. Namely, if the privacy property of an anonymous credential system is unconditional then even
- when instantiated from building blocks that could be broken by a hypothetical quantum computer, the
- privacy is not endangered and will hold forever (even when given unlimited computing power). We note that
- for the BBS family of anonymous credentials, the privacy property holds unconditionally.

- Currently, there do not exist anonymous credential schemes that are plausibly post-quantum secure,
- scalable to the eIDAS setting and have high quality software implementations. At the same time, the
- hash and signature-based mechanism currently being proposed is neither post-quantum secure nor privacypreserving.
- It is therefore prudent that processes exist so that the cryptography being deployed in the EUDI
- can be updated to a new, post-quantum standard whenever it becomes necessary and possible.
- Following the success in the NIST Post-Quantum Standardization [NIS], it seems very likely that constructions
- based on lattice assumptions will form the future foundation of quantum-safe public-key cryptography.
- Hence, naturally several constructions of lattice-based anonymous credentials have recently been proposed
- [LCL+23, BLNS23, JRS23], together with a proof-of-concept implementation [LSS24]. Although, as of now,
- the current constructions do not seem well-studied enough in terms of security and efficiency for such a
- wide deployment, such lattice-based solutions for anonymous credentials may likely become one of the most

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Data protection and privacy aspects of trust services in the context of the European Union Digital Identity Wallet

11th Trust Services and eID Forum

Alicia FILIPIAK – Commission Nationale de l'Informatique et des Libertés (CNIL)

Alicia Filipiak

CNIL

Data protection aspects of trust services

A PRIVACY TYPOLOGY OF EIDAS 2.0 PROVISIONS

Article 5a, paragraph 4.(c)

European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (...) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;

Article 5a, paragraph 4.(d)

European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (...) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard (...)

Article 5a, paragraph 5.(a)(x)

European Digital Identity Wallets shall, in particular: support common protocols and interfaces: (...) for reporting a relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for data is received;

CNIL.

Alicia Filipiak

CNIL

Data protection aspects of trust services

A PRIVACY TYPOLOGY OF EIDAS 2.0 PROVISIONS

Article 5a, paragraph 4.(c)

European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (...) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;

- **Provisions with exclusively functional or security requirements.**
- **eIDAS conformity does not impede GDPR conformity.**
- **Such provisions can even ensure compliance with Articles 25 and 32 of the GDPR.**

Article 5a, paragraph 4.(d)

European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (...) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard (...)

- **doctrinal work (recommendations from DPAs, guidelines from EDPB...).**
- **No critical or complex impact on data protection and privacy principles.**
- **However, technical implementations shall be carefully reviewed by Data Protection Authorities.**

Article 5a, paragraph 5.(a)(x)

European Digital Identity Wallets shall, in particular: support common protocols and interfaces: (...) for reporting a relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for data is received;

- **Provisions that explicitly reference GDPR principles or Data Protection Authorities.**
- **Critical impact on Data Protection measures and mitigations.**
- **Critical impact on legal certainty for relevant actors of the ecosystem.**

CNIL.

Alicia Filipiak

CNIL

Data protection aspects of trust services

A PRIVACY TYPOLOGY OF EIDAS 2.0 PROVISIONS

Article 5a, paragraph 4.(c)

European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (...) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;

- **Provisions with exclusively functional or security requirements.**
- **eIDAS conformity does not impede GDPR conformity.**
- **Such provisions can even ensure compliance with Articles 25 and 32 of the GDPR.**

NO/LOW RISK OF MISALIGNMENT

Article 5a, paragraph 4.(d)

European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (...) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard (...)

- **doctrinal work (recommendations from DPAs, guidelines from EDPB...).**
- **No critical or complex impact on data protection and privacy principles.**
- **However, technical implementations shall be carefully reviewed by Data Protection Authorities.**

INTERSECTIONS WITH DPA PRACTICES

Article 5a, paragraph 5.(a)(x)

European Digital Identity Wallets shall, in particular: support common protocols and interfaces: (...) for reporting a relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for data is received;

- **Provisions that explicitly reference GDPR principles or Data Protection Authorities.**
- **Critical impact on Data Protection measures and mitigations.**
- **Critical impact on legal certainty for relevant actors of the ecosystem.**

GDPR OR DPA EXPLICIT REFERENCES

CNIL.

Alicia Filipiak

CNIL

Data protection aspects of trust services

INTERPRETING AND ENFORCING EIDAS 2.0

- The eIDAS 2.0 Regulation defines new roles for National and European administrations.
- With no cohesive and coordinated cooperation between said administrations, the Regulation's provisions can be interpreted differently.

A RISK OF LEGAL MISALIGNMENT

- Wallet providers frame the functionalities and capacities of wallet instances. However, they may neither be controllers nor processors under GDPR.
- Without strong privacy considerations in the certification schemes design, Data Protection Authorities may encounter difficulties to enforce **GDPR.**

SOME DEAD ANGLES FOR DATA PROTECTION

- Wallet providers, relying parties and other services need a clear and stabilized framework.
- Transparency and guarantees for the user to have control over their personal data are critical for the wide adoption of trust services and eID solutions.

A RISK OF LACK OF LEGAL CERTAINTY

- Privacy Enhancing Technologies can lack the maturity or the industrial incentive for strong certification guarantees in standardization bodies.
- However, for some use cases that do not require strong security, such as Age Verification, they can be relevant and shall be promoted.

A DELICATE BALANCE BETWEEN SECURITY AND PRIVACY

CNIL.

Impact of a quantum Computer on the EUDIW

From ERC Gregor Seiler

Zero-knowledge proof systems are an extremely versatile tool for the construction of advanced cryptographic protocols and especially privacy-preserving protocols. Their importance will increase in the expected post-quantum world where quantum computers break classical cryptography. Unfortunately, for many applications and despite enormous research efforts, state-of-the-art quantum-safe proof systems of PCP type do not yet offer the necessary performance required in practice. The time needed to compute a proof is often too long and the proof size too big. **An important such application that shall serve as a guiding principle in this project are privacy-preserving protocols constructed on top of standard (random-oracle) schemes. In recent research a promising new family of proof systems has emerged that is based on lattice cryptography. Especially their computational performance and proof sizes warrant more research into them. But lattice-based proof systems do not currently match the functionality of the PCP-type ones and can not be used for proving general computation**. The central objective of GLAZE is to research ways to **bring the functionality of lattice-based proof systems to the state of PCP-type ones, and then work on improving their performance and proof sizes to levels that are orders of magnitude better than the state of the art**, enabling applications that are completely beyond the reach of practicality at the moment. Concretely, this project would ideally result in lattice-based proof systems able to prove a standard post-quantum signature such as Falcon with its long unstructured full-domain hash in under 100 milliseconds prover time and 10 Kilobytes proof size on a mobile processor.

From ERC Gregor Seiler

- We are living in an era of rapid digitization where cryptography makes it possible to securely translate
- some of our core societal infrastructures into the digital realm. Cash gets translated to digital payment
- systems, signatures on paper to digital signatures, and passports to digital certificates of identity issued
- by our countries of citizenship. In this process the difficulty to fork physical artifacts is replaced by
- unforgeability based on mathematics, with the potential for higher security. But these technologies
- come with the risk of an unprecedented accumulation of private data. For example, our banks now
- learn essentially every payment we perform. Fortunately, cryptography not only enables high security
- but also provides the tools to retain privacy without any sacrifice in security or functionality. And one
- of the most versatile tools for this task are zero-knowledge proofs that I focus on in my work. Using
- efficient zero-knowledge proofs we are able to replace our current digital payment systems by cash-like
- central-bank-issued digital money where transactions do not leave any trace about the payer, payee
- or amount, but where the digital money is still as difficult to forge as before. In the case of digital
- identities, zero-knowledge proofs allow for certificates where the user can selectively disclose only some
- of their credentials in each presentation (say citizenship and age, but not name), and where different
- presentations can not be linked to the same user.
- Zero-knowledge proof systems provide algorithms that produce digital proofs of knowledge of a
- solution to any algorithmic problem such that the proofs do not reveal any other information than
- mere knowledge of a solution. So in particular no hints about the solution are revealed. The proofs are
- sound meaning it is impossible to create a valid proof for a problem without actually knowing a solution
- to it. Exemplary for privacy-preserving cryptographic algorithms are proofs showing knowledge of a
- message that hashes to a fixed value and that encodes a number above a certain threshold (possibly
- representing the age of a person), without revealing the number.

From ERC Gregor Seiler

- Let us now look at a concrete example to understand what is needed from zero-knowledge proofs when one wants to use them for protecting privacy in the real world. **In May 2024 the European Union has established new digital identity regulations that demand from the EU member states to provide interoperable digital identities to all of their residents by 2026 [eID24].**
- **The cryptographic research community has developed anonymous credential systems precisely for this task already more than 20 years ago** [CL01, BBS04]. Their high-level structure is that users get a signature for their credentials from the issuing party. In presentations, the users do not reveal all their credentials and the signature, but instead only a subset of the credentials and a zero-knowledge proof showing possession of a valid signature that includes the revealed credentials. The underlying signature schemes are specifically designed and exceptional in that they allow for simple and efficient proofs and the proofs are in turn specialized for this task. In particular, **the signature schemes avoid so-called random oracles, i.e. hash functions, since it is easier to prove the (elliptic curve) arithmetic of a signature scheme than the mathematically unstructured computation in a hash function such as SHA2.**
- Unfortunately, the EU is headed towards not using the mature anonymous credential systems for their upcoming interoperable identities. Instead, **the European solution is constructed around a**
- **commodity random-oracle signature scheme (ECDSA) and hacky ad-hoc techniques to achieve (some of) the privacy properties [ARF24]. Concretely, in the European system users will get batches of many signatures at a time so that they only need to present each signature once. This does not prevent linkeability with respect to the issuing party, which would be required from a strict reading of the law. Furthermore, it comes with other problems and does not allow for desirable features such as pseudonyms.** In short, the European digital identity system is headed for a suboptimal and scientifically unsatisfactory solution that is far behind the state of the art, see [BBC+24].
- The main reason why the EU did not choose existing anonymous credential systems is that the **hardware security chips in smartphones on the market today only support commodity random-oracle signatures such as ECDSA, but no signatures without random oracles**. It is important that digital identities can not be copied and then used by unauthorized parties. For this non-transferability property, the identities need to be bound to a secure hardware element that prevents the copying.

From ERC Gregor Seiler

an approach to cryptographic design that has a higher chance of having impact in the real world is to build protocols in a black-box way from as few standard building blocks as possible. That means already standardized commodity schemes and general zero-knowledge

proofs that are capable of proving any scheme. The hardware binding for digital identities can be achieved in this black-box paradigm by requiring the security chip to produce a fresh commodity

signature for every presentation using a secret key safely stored inside it, which in turn is proven by a general zero-knowledge proofs that can run in software on the host smartphone and does not need to be supported by the hardware security chip.

The black-box paradigm leads to more easily deployable and modular algorithms, with readily available hardware support being one reason, and it has important additional advantages. It increases the security posture because the standardized building-blocks have been subject to more cryptanalysis.

The software complexity is reduced so that cryptographic implementers can focus their efforts on fewer well-understood schemes, thereby reducing the probability for implementation bugs which are a central security challenge in the real-world. The black-box paradigm also provides for higher cryptographic agility since modular algorithms allow for subschemes to be exchanged against better or more secure alternatives once this becomes necessary. Finally, it reduces the time needed for producing standards and certification criteria.

Unfortunately, there is a catch. Despite enormous research efforts both by academia and industry, the performance of state-of-the art proof systems for proving random-oracle signatures is by far not good enough. This is especially the case for the newly standardized quantum-safe signatures such as Falcon, where the time needed to prove the SHAKE full-domain hash with long output of more than 4 KB lies in the order of tens of seconds on a server. For a smooth user experience, the time needed to prove a signature should ideally be below 100 milliseconds on a single core of the low-power mobile processor in a smartphone. This is about the barrier where operations stop to be human noticeable.

Therefore, I propose the project GLAZE where I want solve this challenge with research on proof systems that take a relatively new approach, namely *lattice-based* proof systems. I would like to develop general lattice-based zero-knowledge proof systems that are easy to use for proving standard schemes with their symmetric-key primitives, and whose performance is orders of magnitude better than the state of the art, good enough for real-word usage in black-box privacy protocols even on lowpower mobile processors. Those proof systems can then be used for a vast range of privacy-preserving applications in the real world. I am hopeful that this can lead to more adoption of advanced privacypreserving cryptography.

There are other applications where more efficient zero-knowledge proofs would have groundbreaking impact as well, and sometimes it is the size of the current proofs that hinder adoption. Also in this regard I want the proof systems coming out of GLAZE to drastically improve upon the state of the art. An important such application is signature aggregation where one wants to compress a large number of signatures by replacing them with a single proof that should be as small as possible. Here my goal is to be able to prove 10000 signatures with 10 Kilobytes proof size.

From ERC Gregor Seiler

quantum-safety is now essentially a necessity for newly designed cryptographic algorithms.

NIST: Three of the four new standards are lattice-based.

In the area of quantum-safe zero-knowledge proofs, lattice-based constructions are still a niche topic. The by far most researched quantum-safe proof systems are PCP-type systems that base their security solely on the mathematically unstructured assumption of collision resistant hash functions.

Sate-of-the-art systems are STARK [BBHR18], Aurora [BCR+19], Brakedown [GLS+23] and Orion [XZS22]. But lattice-based proof systems have made tremendous progress in the last five years. And in 2023 we proposed the Labrador system [BS23], which made a big leap forward and is the first lattice-based proof system whose proof sizes are concretely small and scale sublinearly with the witness length, which is a necessity for proving the circuits in standard schemes. In fact, Labrador's proofs are even about one order of magnitude smaller than state-of-the art PCP-type proofs. Concretely, even for very large witnesses a Labrador proof has about 50 KB, whereas state-of-the-art PCP-type proofs are at least several hundred Kilobytes in size. And in terms of runtime we have recently shown that latticebased proof systems can beat PCP-type ones as well. Our Greyhound front-end to Labrador from this year can prove polynomial evaluation statements that are also used internally in the PCP-type systems in about one order of magnitude less time [NS24].

Our recent research shows that lattice-based proofs can provide smaller proofs and faster proving times but the sizes and runtimes are still far from what is needed in practice. An most importantly, the PCP-type proofs are still far ahead in terms of ability to prove arbitrary circuits and thus standard schemes with their symmetric-key primitives. Lattice-based proof system such as Labrador are specialized to proving the cyclotomic operations in lattice schemes and can not be used for arbitrary circuits. That is, lattice-based proof systems are not yet general. The PCP-type systems are also far ahead in terms of fast verification, and software tooling.

From ERC Gregor Seiler

The central objectives of GLAZE are to build lattice-based succinct zero-knowledge proofs with around 10 KB proof size that simultaneously support cyclotomic constraints as well as arbitrary circuits formase of proving standard lattice schemes, and production-ready, high-assurance and high-performance implementations that are capable of proving a standard Falcon [FHK+18] lattice signature including its unstructured full-domain hash function in less than 100 milliseconds runtime.

In order to reach these objectives the first challenge is to make the existing systems general in theory. For this I want to find ways to make them able to efficiently prove the same statements as the leading PCP-type systems. Then the commercial tool chains for compiling high-level programming languages into proof system statements, e.g. [ac22, BIM+23], can be used to prove arbitrary circuits with lattice systems, at least in principle. Here it is also important for certain applications to achieve fast sublinear verification both for lattice statements as well as arbitrary circuits.

When these goals have been reached, the efficiency breakthroughs from our recent works on Labrador should make it possible to build general and easy-to-use lattice-based proof systems whose prover runtimes are faster by about one order of magnitude compared to the state-of-the-art PCP-type systems, and whose proof sizes of about 50 KB even for very large witnesses are smaller by another order of magnitude. From there, I hope we will be able to achieve further reductions in prover time by one to two orders of magnitude, and a reduction in proof size to ideally 10 KB through research on a combination of theoretical improvements and implementation techniques.

The cost of basic building blocks such as commitments in lattice constructions are so big that concretely small output sizes always require optimization techniques that remedy these costs. One example for a class of techniques in this domain is compressing commitments by rounding, which needs ingenious ways to retain correctness and security, e.g. [BG14]. In my experience the details of these optimization techniques are regularly the main theoretical contributions in constructive lattice cryptography and I find them to be among the most beautiful and rewarding contributions in the literature. The recently standardized signature scheme ML-DSA (Dilithium) is the result of about one decade of research on such improvements. This research has brought the scheme from a straightforward translation of the discrete-log Schnorr signature, which was clean but extremely unpractical, to a quite complicated but very practical scheme that is now the main post-quantum signature. For proof systems, I believe the groundwork of constructing basic algorithms with the potential for concrete efficiency has been laid and on a high level we understand how good lattice proof systems are constructed. On the other hand, the optimization research has only begun and there remains great potential for improvements.

Each additional optimization technique usually increases the design complexity of the protocols and introduces additional system parameters so that the parameter space gets exceedingly difficult to navigate. In a recursive protocol like Labrador there are in total hundreds of system parameters. In my research I tend to follow a very numerical and parameter-centered approach. By constantly computing the effects on sizes of various alternative and often mutually exclusive techniques and parameter changes one gets a good understanding what the concretely best techniques are, how to best parameterize them, and where potential avenues for improvement lie. Then the final system and parameterization is the result of a long effort where one tries to find an optimal combination of techniques and parameters. I have had rather good success with using this approach as one of my main research methods. It is somewhat different to what is being done in the majority of research publications, where authors strive for clean protocols that improve asymptotic characteristics. Often the proposed constructions are not parameterized at all, or when they are, this is more of an afterthought, and there was no effort to optimize the output sizes.

For optimizing the runtimes I use a double tracked approach. Firstly, there is still a lot of room for improvements by working on software optimizations in vectorized implementations that are written using intrinsics and assembly language. I have extensive experience in optimizing implementations via vectorization. I have for example designed the NTT in Kyber that is the result of my work on vectorizing signed Montgomery reductions [Sei18], which improved the runtimes of NTT implementations by a factor of more than 5 over previous highly optimized and vectorized assembly implementations. I now focus on the AVX-512 instruction set architecture on x86, but vectorization techniques can be ported to other ISAs such as NEON on ARM. Secondly, it is often possible to gain massive reductions in runtime by exploiting interactions between theoretical design decisions and computational complexity that have no or only a small impact on proof sizes. As an example, lattice-based proof systems generally work over small cyclotomic rings because in some places this is necessary for small proof sizes. But in other places this is not necessary, for example in commitments. So by using extension rings of the small rings in those places one can gain an improvement in computation time that is usually quadratic in the extension degree. Here it is crucial to note that the extension rings are modules over the small rings so that their arithmetic is compatible with the rest of the protocol. Such improvements require a very good theoretical understanding by the implementers and often require that the implementation work goes alongside the theoretical work. I view this as a particular strength of combining theoretical and optimized implementation research in one group. Moreover, less objectively quantifiable effects of design elements such as high-risk for side-channel leakage can and should also be addressed in this combined research.

After the described work on improving lattice-based zero-knowledge proof I also want to work on increasing the assurance of the implementations, including formally verifying parts of the code. And finally, I would like to showcase the groundbreaking practicality of the proof systems by using them in example applications that are currently beyond the reach of practicality. I now briefly sketch the work packages that GLAZE can naturally be divided into.

- **WP1: Theory.** The first work package is concerned with theoretical improvements that make
- lattice-based proof systems general and that drastically improve upon the proof sizes. By general
- I mean the ability to efficiently and simultaneously prove cyclotomic as well as arbitrary circuit
- computations, with sublinear verification. For arbitrary circuits it is necessary to try to achieve the
- ability of proving the same statements as the PCP-type systems. For improved proof sizes the size of opening norm proofs, and/or better parameterizations. Also a promising idea here is to make use of
- a full recursion strategy where the outer commitments are replaced by proving all prover messages
- in the next recursion layer. This would need an easy to prove (lattice-based) hash function as the
- Fiat-Shamir hash. I would like to work on such a hash function in collaboration with a cryptographer
- who is an expert on symmetric-key primitives.
- **WP2: Implementation.** In the second work package implementation techniques that greatly improve
- the runtimes are being researched. The first challenge is to improve our optimized Labrador
- implementation by vectorizing parts of the code that are still scalar, and finding better vector algorithms
- for the parts that are already vectorized. Next, it is crucial to improve the memory access
- patterns and code organization to make better use of the data and muop caches. Here different algorithmic
- approaches that need less memory overhead will also be researched. Then, a big project for
- improving the computation speed, but also for drastically simplifying the code is to research if it is
- possible to instantiate the proof system arithmetic over cyclotomic rings modulo fully splitting primes
- without going back to old repetition techniques that increase proof size.
- In this work package the goal is to also deliver a high-quality and high-performance software library
- for the proof systems from the project, including tools to compile high-level programming languages
- into the systems' statements so that the systems can be used easily in practice.
- **WP3: Assurance and Standardization.** The first topic of the third work package is to tame the
- high complexity of implementations from WP2. Methods to increase the assurance are researched,
- with the final goal of formally verifying critical parts of the code in collaboration with Prof. Bo-
- Yin Yang at Academia Sinica Taipei. The new algorithmic ideas and techniques that already exist in

ERC Gregor Seiler – part B2

Other quantum-safe proof systems:

- Similarly to signature schemes and unlike public-key encryption schemes, quantum-safe zero-knowledge proofs can also be constructed by basing their security solely on the mathematically unstructured assumption of a collision resistant hash function. The origins of this lie in probabilistically checkable proofs (PCP) using error-correcting codes and Kilian's protocol using Merkle hash trees for committing to the PCPs [Kil92].
- Examples of such systems are STARK [BBHR18], Aurora [BCR+19], Brakedown [GLS+23] and Orion [XZS22]. They all have transparent setup and sublinear proof sizes, but the proof sizes are typically at least in the order of several hundred Kilobytes, an order of magnitude worse than Labrador's.
- Their statements target arbitrary circuits. Internally the circuit and witness are compiled into polynomials via interpolation so that evaluations of the polynomials prove knowledge of the witness. The evaluations are reduced to a single random evaluation using variants of the information-theoretic sumcheck protocol. This allows these systems to construct their algorithms using a so-called polynomial commitment scheme, i.e. essentially a proof system for polynomial evaluation constraints similarly as Greyhound, where the prover first commits to the polynomials and later proves correct evaluation at the random point with little proof size.
- In the internal polynomial commitment schemes the polynomials are encoded using an error correcting code. STARK and Aurora use Reed-Solomon codes that require expensive large FFTs. Brakedown and Orion use linear-time encodable codes, but for committing to the polynomials they still use Merkle hash trees with the codeword coefficients as leaves. Such commitments are much more expensive to compute than a lattice-based commitment, as for example used in Greyhound. Also the large amount of RAM required to compute the codes and Merkle tree are a major problem in these systems. Concretely, the prover times of the fast Brakedown and Orion polynomial commitment schemes are about one order of magnitude worse than Greyhound's. And, coming back to proving standard signature schemes, Brakedown and Orion would need tens of seconds on a server to prove the full-domain hash in the Falcon signature scheme with its long output.
- **Our recent research shows that lattice-based proofs can provide smaller proofs and faster proving times, but the code-based proofs are still far ahead in terms of ability to prove arbitrary circuits, fast verification, and software tooling. There is a significant industry often associated to blockchain technology that drives the research and development of the code-based systems and provides the engineering resources for high-quality implementations and a sizeable variety of mature tool chains that are necessary for compiling high-level programming languages to circuits and polynomials, e.g. [BIM+23, ac22].**
- There are discrete-log and especially pairing-based proof systems that are typically slower than the code-based ones due to their expensive elliptic curve arithmetic but that excel with very small proof sizes that can be as small as a few hundred bytes. Because of their missing quantum-safety I consider them outside of the scope of this research project.

EUDI | Privacy Requirements in eIDAS

- eIDAS Regulation mandates strong privacy guarantees

"securely [..] authenticate to relying parties [..] while ensuring **selective disclosure of data** [..]

enable privacy-preserving techniques which ensure **unlinkability** [..]

possibility of users to access services through the use of **pseudonyms** [..]

providers should ensure **unobservability** by not collecting data and not having insight into the transactions of the users [..]

§ 16. The technical framework of the European Digital Identity Wallet shall:

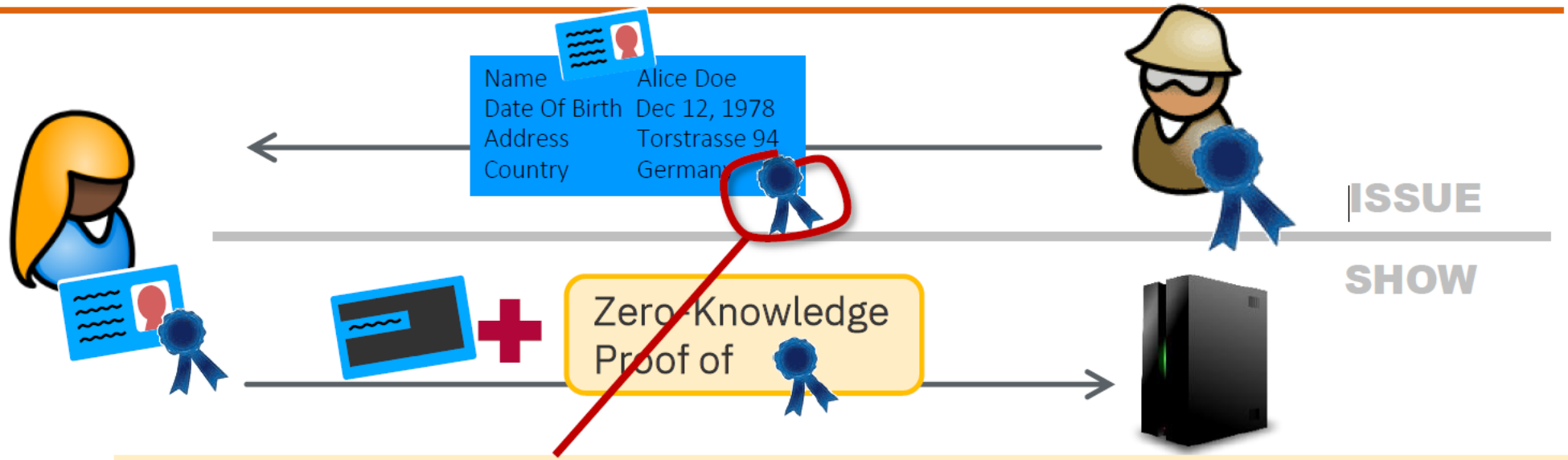
(a) **not allow providers** of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, **to obtain data that allows transactions or user behaviour** to be **tracked, linked or correlated**, or knowledge of transactions or user behaviour to be otherwise obtained, unless explicitly authorised by the user;

(b) enable privacy preserving techniques which ensure ~~unlikeability~~

Corrigendum 9.4.25: unlinkability! ☺

https://eur-lex.europa.eu/eli/reg/2024/1183/oj
https://eidas-open-letter.org/

Anonymous Credentials | Signatures with ZKPs



Needs **signature scheme** (for IdP) **that allows for efficient ZKP of a signature**

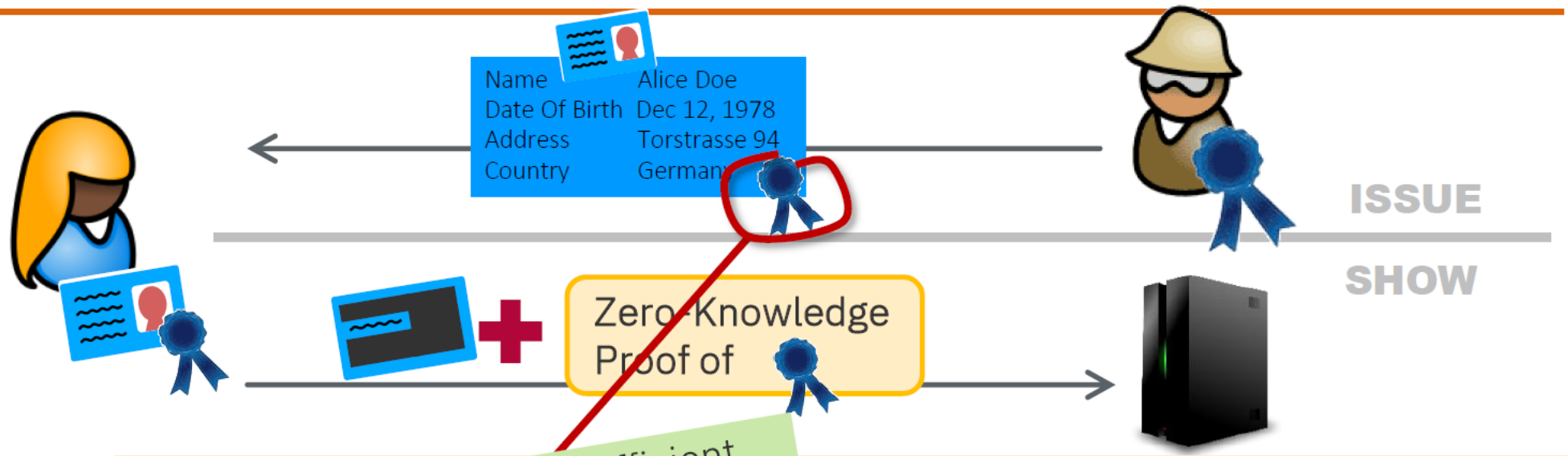
Option 1 | Dedicated signature scheme with „build-in“ ZKP-capabilities

E.g., CL/BBS/PS-signatures

Option 2 | Use any signature scheme (e.g., ECDSA) & generic (circuit-based) ZKP

Legacy-compatible, but less efficient & more complex

Anonymous Credentials | Signatures with ZKPs



Most mature (20 years), simple & efficient

Needs sig… (for IdP) that allows for efficient ZKP of a signature

Option 1 | Dedicated signature scheme with „build-in“ ZKP-capabilities

E.g., CL/BBS/PS-signatures

Option 2 | Use any signature scheme (e.g., ECDSA) & generic (circuit-based) ZKP

Legacy-compatible, but less efficient & more complex

Anonymous Credentials | From Theory to Practice

- Not used in EUDI 1.0 due to lack of standards/SOGIS approval and device binding

Primitive	Scheme	R/L	Notes
RSA	PSS (PKCS#1v2.1) [RFC8017, PKCS1, ISO9796-2]	R	
FF-DLOG	KCDSA [ISO14888-3]	R	
	Schnorr [ISO14888-3]	R	41-DSARandom
	DSA [FIPS186-4, ISO14888-3]	R	
EC-DLOG	EC-KCDSA [ISO14888-3]	R	
	EC-DSA [FIPS186-4, ISO14888-3]	R	41-DSARandom
	EC-GDSA [TR-03111]	R	
	EC-Schnorr [ISO14888-3]	R	
RSA	PKCS#1v1.5 [RFC8017, PKCS1, ISO9796-2]	L	40-PKCSFormatCheck

Credential must be bound to hardware-protected device key

EUDI Wallet requires Level-of-Assurance (LoA) High

Secure Elements/OS provide ECDSA APIs

- Ongoing standardisation activities & research to solve device binding

  BBS IETF Draft
  Pairing IETF Draft revived

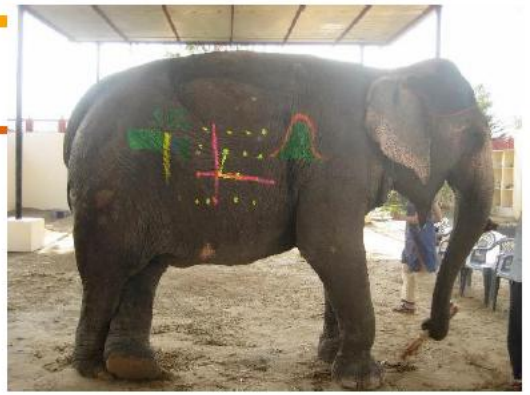
  BBS-ECDSA (legacy device binding),
  BBS-BLS (simple device binding & blind version for cloud HSM)

- ZKP-based solutions are considered for EUDI 2.0 ☺

  Technical specifications for BBS and ECDSA/Circuit based approaches have been started

... but, all considered options are DL-based

Post-Quantum vs. Post-Privacy?



- Does it make sense to deploy new DL-based crypto? PQC!
  - But, PQC less time-critical for authentication than for encryption
  - NIST 2024 report on PQC transition

    "Authentication systems may continue to use quantum-vulnerable algorithms ***until quantum computers*** *that are capable of breaking current, quantum-vulnerable algorithms* ***become available****."*

- **Main priority: EUDI Wallet should have post-quantum privacy!**

→ Anonymous Credentials from BBS-signatures have perfect privacy, but DL-based soundness

- Identity infrastructure is being built now! Based on „ECDSA mindset“

  If we don’t propose a viable ZKP-based solution now → lack of privacy will manifest

Digital Identity with Privacy

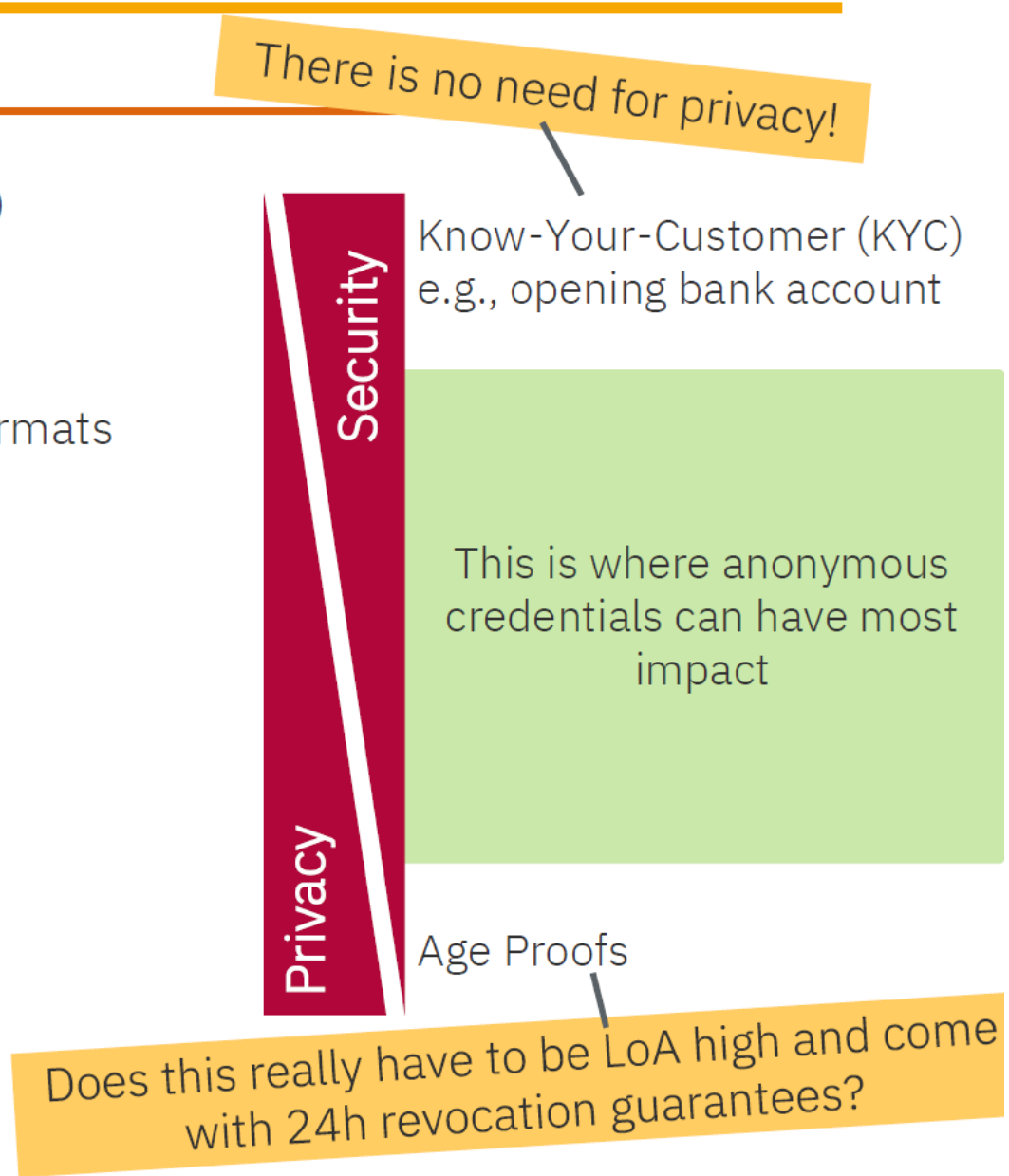
Short/Midterm (PQC-privacy, non-PQC soundness)

- Show feasibility and benefits
- Shape requirements and use cases
- ZKP-compatible protocols (OIDC4Vx) & data formats

  Ensure application layer support e.g., for:
  - Presentation ≠ Credential
  - Conditional disclosure
  - Composite proofs
  - Blind issuance
  - Pseudonyms

→ Provides concrete target for PQC research

Insights from pre-PQC serve as blueprint



Slides from Gregor from gsm

Post Carsten on anonymous credentials

Transition of the PKI (page 6 of the article feedback from cryptographers …)

Anonymous credentials for the wallet

- achieve authentication and identification that are both secure and privacy-preserving

- Article by cryptographers and post by Cloudflare

Personal data protection – Digital Omnibus

All the things about age verification and other concerns