THE QUANTUM SPACE

WIBU SYSTEMS

TQS EXECUTIVE INTELLIGENCE

SOVEREIGN BY DESIGN

How Europe Can Secure its Digital Future in the Post-Quantum Age

OCTOBER 2025

A Whitepaper from Wibu-Systems & The Quantum Space

Edited by
Daniela Previtali, Wibu-Systems
Steve Atkins, The Quantum Space

Exploring how quantum computing threatens today's cryptography and why post-quantum migration is urgent. It examines Europe's strategic challenge of balancing digital sovereignty with innovation, regulatory deadlines, and global competition—framing the critical questions leaders must answer to secure trust, competitiveness, and independence in a quantum future.

Sovereign by Design:
How Europe Can Secure Its Digital Future in the Post-Quantum Age

Examining how Europe can balance regulation, innovation, and security to remain sovereign in the post-quantum era.

A WIBU-SYSTEMS AG & The Quantum Space Whitepaper

Edited by:

Daniela Previtali,
WIBU-SYSTEMS AG

Steve Atkins,
The Quantum Space (Krowne Communications GmbH)

CONTENTS

Table of Contents

Executive Summary

We are living through a quiet revolution. Cryptography, the invisible scaffolding of digital life, is under threat from a new class of machines that still sit in research labs but already shape today's security decisions: quantum computers. Their promise is scientific; their threat is systemic. The prospect of breaking RSA and ECC algorithms doesn't just endanger bank transfers or VPNs. It undermines the entire trust fabric of our digital economy.

The urgency is sharpened by regulation. The U.S. NIST has finalized post-quantum cryptography standards. The EU has set explicit migration milestones: national roadmaps by 2026, high-risk systems migrated by 2030, medium-risk by 2035. At the same time, the Cyber Resilience Act, NIS2, and DORA are raising the floor of security expectations across Europe.

Yet Europe's challenge is not just technical. It is strategic. Digital sovereignty—the ability to act with independence, under European values, in a world dominated by U.S. and Chinese technology—is both an ambition and a constraint. Regulation provides a shield, but it can also become a cage if it outpaces innovation.

This report brings those two threads together. Part 1 explains the cryptographic shift: why post-quantum migration is urgent, why it's hard, and how organizations can act now. Part 2 situates that shift inside Europe's sovereignty project: the mix of regulation, investment, and geopolitics that will determine whether Europe leads or lags in the next digital decade. The roundtable transcript (Part 3) captures these issues as they were debated in real time—experts from industry, academia, and government grappling with the trade-offs, timelines, and practicalities.

Our purpose is not to provide every answer, but to frame the questions that matter most. How do we migrate before the clock runs out? How do we balance sovereignty with competitiveness? And, ultimately, how do we secure Europe's place in a quantum future?

Part 1 — The Coming Cryptographic Shift: Why Post-Quantum Migration Matters Now

Imagine someone steals your locked diary today because they're confident that tomorrow they'll own the master key. That, in one sentence, is the quantum threat: "harvest-now, decrypt-later." Attackers capture sensitive data today (banking, health records, IP, diplomatic cables), store it, and wait for sufficiently powerful quantum computers to peel open the classical encryption that protects it. Whether that capability arrives in ten, fifteen, or twenty years is not the point; the shelf life of your data is. If the information must remain confidential for a decade or more, the risk is live now.

This first part is a straight-talk guide for tech leaders who need to make sense of the regulatory clock, the engineering pain, the business case, and the practical steps. The bottom line: the post-quantum migration has started. Standards exist, deadlines are public, and boards are asking questions. Waiting until "it's clearer" will just make the eventual retrofit more expensive and more disruptive. The window to move deliberately—rather than frantically—is open, but not wide.

The Quantum Threat, Without the Hype

Let's strip it down.

- **What breaks?** Public-key cryptography based on RSA and ECC is theoretically vulnerable to quantum algorithms (notably Shor). That means the mechanisms we use for key exchange, digital signatures, code-signing, and certificates are at risk in the long term.
- **What doesn't?** Symmetric crypto (e.g., AES) and hash functions (e.g., SHA-2/3) fare better; they may require larger parameters but aren't fundamentally broken by the same algorithms.
- **Why act now?** Because of the harvest-now, decrypt-later pattern and because standards and regulation have started the clock.

On the standards front, the U.S. National Institute of Standards and Technology (NIST) finalized the first three post-quantum cryptography (PQC) standards in August 2024: FIPS 203 (ML-KEM) for key establishment, FIPS 204 (ML-DSA) for digital signatures (module-lattice, a.k.a. Dilithium family), and FIPS 205 (SLH-DSA) for stateless hash-based signatures. These are no longer research curiosities; they're formal, deployable standards with parameter sets, test vectors, and compliance pathways.

Across the Atlantic, the European Commission published a Coordinated Implementation Roadmap in June 2025, setting out a staged EU-wide PQC migration with explicit milestones (more on those in Section 3). The message is clear: act early, act in concert, act with agility.

Why Post-Quantum Migration Is Harder Than It Looks

If you've ever swapped a database engine or lifted a legacy monolith into microservices, you know: the technology is the easy part; the dependencies are the pain. PQC is similar—except the dependencies are everywhere.

The brownfield reality

Most organizations operate complex estates: on-prem systems, cloud workloads, SaaS integrations, IoT fleets, industrial control systems, and partner APIs. Cryptography is baked into each layer (protocols, libraries, HSMs, firmware, signed containers, update chains). Few estates were built with crypto-agility in mind—the ability to swap algorithms and parameters without rebuilding the world. Retrofitting agility after the fact is slower than anyone likes to admit, especially where hardware and certification are involved. ENISA's guidance calls out exactly these issues and frames migration as a multi-year program that starts with inventory and risk analysis, not with ripping out TLS stacks on day one.

The performance and footprint trade-offs

PQC algorithms typically have larger keys and signatures and different performance profiles than RSA/ECC. On a modern server, the impact is often acceptable; in constrained environments—smartcards, sensors, medical devices—it can be non-trivial. That's why both NIST and ETSI emphasize composite approaches (classical + PQC in tandem) during transition, so systems maintain current assurances while gaining quantum resistance, allowing time to optimize stacks and hardware.

Certificates, chains of trust, and signed updates

It's not just TLS. Your PKI, code-signing, firmware update mechanisms, container signing, and secure boot all rely on digital signatures and certificate profiles that expect RSA/ECDSA today. Migrating means re-tooling CAs, revamping issuance policies, updating device trust anchors, and validating OTA update paths with PQC signatures. The U.S. federal ecosystem (via CNSA 2.0 policy and guidance) and the EU regulatory stack both press for updateability and crypto-agility as foundational properties—because these migrations will not be one-and-done.

The Deadlines You Can't Ignore

You can debate quantum timelines. You can't debate regulatory ones. Here are the ones that matter for boards and budgets:

- NIST PQC standards are final. FIPS 203/204/205 were published Aug 13, 2024, with effective notice in the U.S. Federal Register the following day. This is the green light many vendors (and auditors) were waiting for.
- EU PQC Roadmap milestones. The Commission's June 23, 2025 roadmap calls for:
  (a) By end-2026: every Member State should have national roadmaps and pilots underway;
  (b) By end-2030: complete migration for high-risk use cases (including critical infrastructures);
  (c) By end-2035: complete migration for medium-risk use cases, aligning broadly with U.S./UK timelines.
  It also recommends composite schemes deployment first and stresses crypto inventories and upgradeability.
- Cyber Resilience Act (CRA). The CRA entered into force 10 December 2024; its main obligations apply from 11 December 2027. In practice, that means products with digital elements shipped into the EU must meet security-by-design requirements, including secure update mechanisms—a precursor to PQC agility. This is not a PQC mandate per se, but you won't clear CRA compliance if your products can't be updated as cryptographic requirements evolve.
- DORA (financial sector). The Digital Operational Resilience Act applies from 17 January 2025 to banks, insurers, and other financial entities. While DORA doesn't name PQC, it raises the bar for "state-of-the-art" cyber controls, incident reporting, and third-party risk management—factors that make crypto inventories and upgrade paths mandatory in all but name.
- NIS2 (horizontal critical sectors). The revised EU cybersecurity directive had to be transposed by 17 October 2024; it tightens obligations on risk management and incident reporting across essential and important entities. Again, not a PQC rulebook—but a strong hand on the rudder toward current, robust cryptography, which by definition now includes PQC plans.
- U.S. National Security timelines (signal, not mandate). The NSA's CNSA 2.0 materials and CNSSP-15 policy signal an accelerating shift: new acquisitions for National Security Systems move to CNSA-2.0 algorithms before the end of the decade, with end-state "quantum-resistant" requirements by the mid-2030s. Even if you don't sell into NSS, these milestones influence commercial vendor roadmaps and procurement norms.

Translation for your roadmap: you don't need a crystal ball—you need a Gantt chart. The dates above are the anchors.

The Cost of Waiting (and Why It Balloons)

Delaying PQC runs a tab in four ways:

1. **Retrofitting is pricier than designing-in**. If you ship products without crypto-agility and with hard-coded RSA/ECC dependencies, you'll pay to refactor later—often under certification and customer pressure. Anyone who navigated TLS 1.0/1.1 deprecations knows the pattern.
2. **Certification and supply-chain friction.** CRA compliance, sectoral schemes, or customer security questionnaires will increasingly ask for PQC plans and update mechanisms. Lacking those creates deal friction and, in some markets, simple exclusion.
3. **Technical debt accumulates quietly.** Keys expire, certificates roll, devices get field-upgraded. If those processes aren't retooled to accommodate PQC (or composite schemes) in routine operations, you're effectively compounding debt with each cycle.
4. **Opportunity cost.** Vendors that advertise PQC-ready features (even as composite schemes) signal resilience and foresight. In regulated procurement, that's often the tie-breaker. The EU roadmap explicitly frames PQC migration steps as "no-regret" controls that improve cyber posture overall—i.e., you're not doing this only for quantum.

In practical terms, migrations of this kind take years—not months. Even optimistic playbooks put "identify → pilot → scale → certify" well past a single budget cycle, especially for embedded and industrial fleets. Independent migration handbooks from national labs and standards bodies echo this: start with inventories and governance, then phase in composite schemes while you stabilize your reference architectures.

What "Good" Looks Like: An Executable Migration Plan

You've heard "inventory first" a dozen times for a reason. Here's a pragmatic plan you can stand up in a quarter and keep running for the next five years.

Establish governance and scope (Weeks 0–4)

- **Name an owner (CTO/CISO office**): create a cross-functional crypto steering group (security architecture, PKI, product, firmware, legal/compliance, procurement).
- **Define the risk lens:** classify data by confidentiality horizon (≥10 years ⇒ high quantum risk). The EU roadmap's milestone language maps naturally to this classification.
- **Agree reference standards you'll track:** NIST FIPS 203/204/205; ETSI composite key exchange guidance; your sector's schemes (e.g., payment, medical, automotive).

Inventory and dependency mapping (Weeks 2–12)

- Catalog cryptographic assets: algorithms, key sizes, protocols, libraries/SDKs, HSMs, trust anchors, certificate profiles, signed update chains.
- Map where crypto lives: endpoints, services, APIs, devices, CI/CD signing, boot chains.
- Record constraints: memory/CPU limits, certificate size limits, protocol support in partners' systems, regulator-mandated cert paths.
- Create a "composite scheme-ready" checklist for each component (can it support ML-KEM + classical today? What breaks? What must be re-compiled?).

NIST's migrations work (e.g., NCCoE projects) provides practical test profiles for composite TLS, IKEv2, and SSH—use these to seed your lab work.

Prioritize and pilot (Months 3–9)

- Triage by risk and reach: focus first on systems that protect data with long confidentiality requirements (customer PII, IP, health/financial records), and on choke points (gateways, VPNs, inter-DC links, PKI roots). This aligns cleanly with the EU's 2030 high-risk milestone.
- Pilot composite schemes in TLS and IKE: start with ML-KEM-768 composites that balance footprint and assurance (mind your handshake size and certificate chain blow-ups). Document performance and interoperability issues; you will find some.
- Harden your signing pipeline: introduce ML-DSA or SLH-DSA for internal artifacts (containers, firmware), even if your external distribution still uses ECDSA during transition. This derisks your supply-chain attack surface early.

Build crypto-agility into product and platform (Months 6–18)

- Abstract algorithm choice behind policy and configuration; rip out hard-coded assumptions.
- Version your trust anchors to support rotations without bricking devices.
- Design for larger artifacts: ensure MTU, message framing, and storage accommodate bigger keys/signatures/certificates.
- Updateability by design: CRA obligations around secure updates effectively make agility a compliance requirement for EU-bound products in 2027 and beyond.

Align with regulation and certification (Months 6–24)

- Map controls to CRA, NIS2, and DORA for your products and services; bind migration milestones to audit checkpoints.
- Engage your CA and HSM vendors on PQC roadmaps and FIPS 140 validations; check when mixed-mode certificates and ML-DSA/SLH-DSA support will be production-grade.
- Plan for customer communications: what changes when, how you'll support dual-stack/composite operations, and what the eventual cut-over policy looks like.

Engineering Realities: Composite Schemes, Profiles, and “Gotchas”

Composite schemes are your friend (for a while)

Composite key exchange (classical + ML-KEM) and composite signatures (ECDSA + ML-DSA/SLH-DSA) let you maintain current assurances while gaining quantum resistance. They buy time for performance tuning, interoperability work, and policy convergence. ETSI and industry groups have published guidance and profiles; use them rather than inventing your own.

Watch the size limits

Bigger keys and signatures can trigger silent failures: handshake messages that exceed limits; intermediaries that drop oversized cert chains; database schemas that truncate fields; MTU/PMTU issues leading to fragmentation and packet loss. Bake size-stress tests into your pilots. The fact that NIST standards are final doesn’t mean every middlebox, library, or SaaS endpoint in your ecosystem is ready for them.

Side-channel and implementation hygiene

Standards don’t guarantee safe code. Timing leaks and bad randomness remain perennial risks. Follow the FIPS 203/204 implementation notes and known-issue trackers; pay attention to constant-time requirements and vetted parameter handling.

Device and embedded constraints

In medical, industrial, and automotive environments, device lifecycles can run into decades. That means you must design now for field replaceability (dongles, secure elements, modules) and for attested updates that support new algorithms over time. This is where CRA’s secure-update obligations and sectoral regimes intersect with PQC: agility is not a luxury feature; it’s how you stay legal and safe.

The Business Case: Compliance, Trust, and Competitive Advantage

A sober view: few customers will pay a premium just for “quantum-safe.” But many will choose a vendor who reduces their risk and compliance burden without drama. That’s the play.

- Compliance tailwind. CRA, NIS2, and DORA collectively raise expectations for security-by-design, incident preparedness, and supplier assurance. A visible PQC roadmap and working composites help you pass audits and win procurement points.

- **Procurement signaling.** “PQC-ready” on datasheets and RFP responses is becoming shorthand for engineering maturity. In public sector and critical infrastructure bids, that often breaks ties. The EU’s 2030/2035 milestones institutionalize this expectation.
- **Supply-chain stability.** Re-keying and certificate rotations triggered by quantum guidance will ripple through ecosystems. Vendors who can handle mixed-mode operations smoothly will win renewals and expand footprint.
- **Strategic optionality.** Once crypto-agility is in place, you’re better positioned for future changes—be that new PQC algorithms, parameter shifts, or sector-specific certification schemes.

In other words: PQC is a forcing function. It nudges you toward the kind of secure-by-default architecture you wanted anyway.

A Board-Level Narrative You Can Use

When you brief leadership, avoid speculative quantum timelines. Anchor the conversation in standards and regulation:

1. Standards exist and are stable: NIST FIPS 203/204/205 are final; vendors are shipping support; federal and defense ecosystems are aligning.
2. EU milestones are public: 2026 (national plans and pilots), 2030 (high-risk migrated), 2035 (medium-risk). These dates will echo through procurement and certification.
3. Other regulations are “PQC-adjacent”: CRA’s 2027 application date drives updateability; DORA and NIS2 push state-of-the-art security and supplier oversight.
4. Migration takes years: inventories, composites, PKI refits, re-signing and update chains—especially for embedded fleets and certified devices. Start now to avoid a future cliff.

Then ask for three things:

- A multi-year PQC budget line (tools, lab hardware, vendor upgrades, certification).
- A policy decision to adopt composites in priority protocols within 12–18 months.
- A quarterly report on crypto inventory coverage and pilot progress.

Frequently Asked “But What About…?”

Q: Should we wait for more algorithms before we commit?
A: No. ML-KEM and ML-DSA are the workhorses for most deployments, with SLH-DSA as an additional signature tool where you need hash-based properties. Start with composite schemes to de-risk and leave room to incorporate future selections as NIST rounds continue.

Q: Can we just use longer RSA/ECC keys for a while?
A: Longer keys extend classical security margins but do nothing against a sufficiently capable

quantum adversary. They may be part of near-term hardening, but they're not a strategy for long-life confidentiality. Use composites to bridge.

Q: How do we handle partners who aren't ready?
A: That's why composite profiles exist: maintain classical interoperability while adding PQC. Negotiate timelines in SLAs and bake upgrade clauses into contracts.

Q: Isn't this all going to be too slow for our devices?
A: Benchmark, don't assume. Many footprints are manageable with careful parameter choices (e.g., ML-KEM-768 as a balanced default), and you can offload some functions to gateways or accelerators. Where devices are too tight, plan for hardware refresh cycles—better on your schedule than on a regulator's.

Closing: The Countdown Has Started

Quantum computers don't need to exist today to create today's risk. The combination of finalized PQC standards, published EU milestones, and adjacent regulatory obligations means the window for orderly migration is here. Use it.

Treat PQC as you would any major platform shift: establish governance, get the inventory right, pilot composite schemes where they matter, build agility into your products and pipelines, and align with the certifications and regulations that govern your market. None of that requires hype. It just requires leadership—and a plan.

Next up: Part 2 explores the bigger stage on which all this plays out: Europe's push for digital sovereignty—how regulation, identity, and supply-chain assurance intertwine with post-quantum security, and how to balance trust with speed.

References & Further Reading

NIST PQC Standards (Finalized Aug 13, 2024):
ML-KEM (FIPS 203), ML-DSA (FIPS 204), SLH-DSA (FIPS 205). U.S. Federal Register notice confirms effective date. These are the primary technical references for implementation and validation.
https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf
https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.204.pdf
https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.205.pdf
Federal Register: https://www.federalregister.gov/documents/2024/08/14/2024-17956

EU Coordinated Implementation Roadmap for PQC (June 23 2025):
Sets EU migration milestones (2026 / 2030 / 2035) and emphasizes composite scheme deployments and crypto inventories.
https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
Press note: https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography

Cyber Resilience Act (CRA):
Entered into force Dec 2024; main obligations apply from Dec 11 2027, requiring secure updates and state-of-the-art protection for products with digital elements.
Official text (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
Commission explainer: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

DORA (Digital Operational Resilience Act):
Applies from Jan 17 2025 to EU financial entities; elevates operational resilience expectations and supplier oversight (implications for crypto governance and upgradeability).
Official text: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
Summary: https://eur-lex.europa.eu/EN/legal-content/summary/digital-operational-resilience-for-the-financial-sector.html

NIS2 Directive:
Transposition deadline Oct 17 2024; strengthens horizontal cybersecurity obligations across sectors, indirectly pushing organizations toward modern cryptography practices.
Official text: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
Overview: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

ETSI Composite Guidance:

Technical reports and standards on composite key exchanges and migration patterns (e.g., TR 103 966; press releases on composite key exchange standards). Useful for protocol profiles and real-world deployments.

ETSI TR 103 966 (v1.1.1):
https://www.etsi.org/deliver/etsi_tr/103900_103999/103966/01.01.01_60/tr_103966v010101p.pdf
ETSI TS 103 744 (v1.2.1):
https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.02.01_60/ts_103744v010201p.pdf
Press release: https://www.etsi.org/newsroom/press-releases/2513-etsi-launches-new-standard-for-quantum-safe-composite-key-exchanges-to-secure-future-post-quantum-encryption

NIST NCCoE PQC Migration Profiles / Practice Guides:

Draft practice guides and test profiles for composite TLS, IKEv2, SSH, with interoperability and performance notes—useful for lab pilots.

Project hub: https://csrc.nist.gov/pubs/sp/1800/38/iprd
SP 1800-38A (draft): https://www.nccoe.nist.gov/sites/default/files/2023-04/pqc-migration-nist-sp-1800-38a-preliminary-draft.pdf
SP 1800-38B (draft): https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf
SP 1800-38C (draft): https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf

Part 2 – Europe's Digital Sovereignty: Between Regulation and Innovation

"Does Europe want to lead in digital technology—or merely regulate those who do?" This question frames one of the great strategic choices facing the continent. Europe's vision of digital sovereignty is not about shutting borders or going it alone. It's about ensuring trusted independence: the ability to make choices about infrastructure, identity, and security without being beholden to foreign suppliers or legal regimes.

The paradox is obvious: Europe has the world's most comprehensive regulatory toolkit but lags in scaling the technologies that regulation seeks to tame. Can sovereignty be both a shield and a springboard?

What Digital Sovereignty Really Means

At its core, digital sovereignty is about control over the systems that underpin the digital economy. Analysts typically describe three layers:

1. Physical infrastructure – chips, data centers, networks, satellites.
2. Code and standards – operating systems, cryptographic libraries, cloud frameworks.
3. Data ownership and flows – where data is stored, who can access it, under which laws.

Europe cannot manufacture all of these domestically. Nor should it try. Sovereignty doesn't mean autarky—it means trusted independence. For instance, cloud services may run on U.S. hardware, but if they are bound by European governance frameworks like Gaia-X, then Europe retains control where it matters: trust, certification, compliance.

This distinction—between self-sufficiency and self-determination—is what policymakers often struggle to explain. The point is not to exclude international partners, but to ensure Europe's critical choices remain Europe's to make.

Europe's Toolbox: Regulation as Sovereignty

Europe's sovereignty drive is built in Brussels, not Silicon Valley. Its tools are legal codes rather than venture capital. Consider the regulatory stack:

- GDPR (2018): set the global benchmark for data protection, forcing companies worldwide to adjust privacy practices.
- Digital Services Act (DSA, 2022): accountability for online platforms.
- Digital Markets Act (DMA, 2022): limiting gatekeeper power.

- Cyber Resilience Act (CRA, 2024): requiring security-by-design and secure updateability in all products with digital elements.
- NIS2 Directive (2024): strengthening cybersecurity obligations across critical sectors.
- AI Act (2024/25): the world's first comprehensive regulatory framework for artificial intelligence.
- eIDAS 2.0 (2024): mandating the rollout of the European Digital Identity Wallet by 2026.
- Digital Product Passport (DPP, pilots 2024–2026): requiring traceable lifecycle data on products like batteries, textiles, and electronics.

Together, these measures create a sovereignty shield: a trusted, regulated digital environment that reflects European values of privacy, fairness, and sustainability.

Critics argue the shield risks becoming a cage. Regulation can be heavy-handed, slow innovation, and create compliance burdens that SMEs struggle to bear. Yet it is also true that Europe has exported its values globally through regulation—the Brussels Effect. GDPR reshaped privacy norms worldwide. Sovereignty is as much about influence as it is about independence.

Strategic Investments: Muscle Behind the Rules

Sovereignty cannot be legislated into existence alone—it requires industrial muscle. The EU has responded with large-scale programs:

- European Chips Act (2023): €43 billion to boost Europe's semiconductor share from under 10% to 20% of the global market by 2030. Compared to the U.S. CHIPS Act and China's state subsidies, this is modest, but it signals recognition that chips are sovereignty's bedrock.
- Gaia-X (2019–): a federated cloud and data initiative, designed to embed European values into infrastructure. Its progress has been slow, but its federated governance model remains influential.
- EuroQCI (Quantum Communication Infrastructure): creating a pan-European secure quantum-based communications backbone.
- Horizon Europe (2021–2027): €95 billion R&D program funding AI, cybersecurity, and quantum projects.
- EuroStack (2025): an emerging movement for independent European digital stacks—an echo of Gaia-X, but with more grassroots momentum.

These investments matter because sovereignty without capacity is hollow. The Chips Act, Gaia-X, and EuroQCI are not perfect, but they give Europe a stake in the technologies of the next decade.

Case Studies: Sovereignty in Action

Gaia-X: Launched with fanfare, Gaia-X aimed to create a European alternative to hyperscaler cloud services. In reality, adoption has lagged. Critics note it risks being co-opted by the very U.S. players it sought to balance. Yet, Gaia-X achieved something important: it reframed the debate. Cloud is not just about compute; it's about governance and trust.

Chips Act: Europe's semiconductor share has been declining for decades. The Chips Act is a belated attempt to reverse that. Compared with the U.S. and China, Europe's investment is smaller, but it reflects recognition that sovereignty without silicon is impossible. Success will depend on execution: aligning funding, research, and private capital.

EUDI Wallet pilots: The European Digital Identity Wallet is a sovereignty milestone. By 2026, every Member State must provide wallets to citizens. Pilots in banking, travel, and healthcare show the potential for frictionless, cross-border trust. The challenge: uptake. If citizens don't use the wallets, sovereignty on paper will mean little in practice.

The Global Context: Between Washington and Beijing

Europe positions itself as the third way.

- United States: innovation-first, regulation-later. U.S. dominance in cloud, chips, AI models, and platforms gives it global leverage. Sovereignty is exercised through market power and standard-setting.
- China: sovereignty through control. Heavy state involvement, industrial subsidies, and regulatory barriers ensure domestic dominance of key technologies, at the cost of openness.
- Europe: sovereignty through regulation. Values and legal frameworks define the digital environment.

This balancing act gives Europe influence—its regulatory standards often become global defaults—but also fragility. If Europe cannot scale its own champions in AI, chips, and quantum, it risks being a "rule-taker" in innovation while remaining a "rule-maker" in regulation.

The Regulation–Innovation Tension

Europe's strength lies in its ability to anchor the digital economy in trusted frameworks. Regulation provides legitimacy, ensures a fair playing field, and projects European values—privacy, fairness, and sustainability—onto the global stage. This approach has given Europe a unique role as a regulatory superpower, exporting its standards far beyond its borders. Yet, the same scaffolding that creates trust can slow innovation. Startups often complain that compliance absorbs more resources than product development, and fragmentation across 27 Member States magnifies the burden.

Sovereignty is supposed to empower, not inhibit. The path forward is not deregulation but smarter regulation: certification sandboxes that let innovators test under controlled conditions, EU-funded compliance toolkits that reduce costs for smaller firms, and harmonized standards that prevent national divergence. Regulation must evolve in lockstep with innovation, not run ahead of it.

SMEs and the Sovereignty Gap

For small and medium-sized enterprises, sovereignty can feel less like empowerment and more like a wall. Certification under frameworks such as the MDR, CRA, or eIDAS is often prohibitively expensive and time-consuming. Large incumbents can absorb the cost, but SMEs—the very pipeline of European innovation—struggle to keep pace. This creates what might be called a “sovereignty gap”: Europe succeeds in establishing sovereignty on paper while losing the very innovators who could make it meaningful in practice.

Closing this gap requires practical measures: shared certification services for SMEs, publicly funded compliance labs, streamlined conformity routes for low-risk products, and targeted grants to offset the costs of implementing PQC, CRA, and AI Act requirements. Europe cannot afford to hollow out its startup ecosystem. Without SMEs, sovereignty risks becoming a brittle construct, dependent on regulation without renewal.

AI and Sovereignty

Artificial intelligence represents the sharp edge of sovereignty. With the AI Act, Europe has sought to embed its values—risk-based oversight, transparency, and prohibitions on practices such as social scoring—into the governance of AI. This positions the EU as the world’s ethical regulator. Yet the risk is clear: while Europe regulates, innovation may shift elsewhere. If the continent becomes reliant on AI models trained in the United States or hardware produced in China, sovereignty becomes rhetorical rather than real.

The answer lies in balance: regulation must be paired with investment in infrastructure, compute, datasets, and skills that allow European AI to flourish. Post-quantum cryptography also plays a role here: sovereign AI requires sovereign trust anchors, ensuring that models, updates, and training pipelines can be verified securely and independently.

Where Post-Quantum Security Meets Sovereignty

Post-quantum cryptography is not only a technical necessity but a strategic one. Relying solely on U.S.-driven NIST standards risks ceding control of Europe’s security foundations. The EU’s post-quantum roadmap, with milestones in 2026, 2030, and 2035, is therefore as much about sovereignty as about cryptography.

Sovereign PQC libraries, validated by European bodies such as BSI, ANSSI, and ENISA, help retain competence at home. Composite deployments allow alignment with global norms while preserving optionality. And as regulations such as the CRA, NIS2, and DORA make PQC a matter of compliance rather than choice, sovereignty and security converge. If Europe falters in this migration, its sovereignty will be undermined at the most basic level: the ability to secure its own data.

Geopolitics of Standards

Standards are sovereignty by another name. The entities that define cryptographic parameters, AI risk categories, or identity protocols effectively set the terms of global trade. Europe cannot afford to be absent from these processes. To safeguard influence, it must push its regulatory frameworks into global standards bodies such as ISO, ITU, and ETSI; promote sovereign infrastructure models like the European Digital Identity Wallet and the Digital Product Passport abroad; and align selectively with U.S. initiatives while retaining the freedom to diverge.

Digital sovereignty, in other words, is as much about projecting influence externally as it is about control internally.

Scenarios for 2030

Europe's future could unfold along sharply diverging paths. In one scenario, the continent successfully deploys sovereign PQC libraries, completes a EuroQCI backbone, sees EUDI Wallets widely adopted, restores a 20% global share in chip manufacturing, and fields AI models that compete globally. Sovereignty in this version is not defensive but a brand: trusted, resilient, and privacy-first. In the alternative, regulation multiplies while uptake stagnates. SMEs exit to friendlier jurisdictions, Gaia-X is forgotten, the EUDI Wallet gathers dust in app stores, and Europe remains dependent on Taiwanese chips, American AI, and Chinese hardware. Sovereignty in this case is rhetorical—asserted, but not lived. Which path Europe follows will depend less on vision than on execution: harmonization, investment, and sustained political will.

Closing: Europe at the Crossroads

Europe stands at a pivotal moment. Digital sovereignty is neither fortress nor fantasy; it is the capacity to act independently in a world of superpower competition and quantum disruption. The balance is delicate. Excessive regulation could stifle the very innovation sovereignty is meant to protect; insufficient oversight could entrench dependency. Yet the choice is unavoidable. In an age where security, identity, and infrastructure are contested domains, sovereignty is not a luxury but survival. If Europe aligns regulation with investment, embeds PQC into its critical infrastructure, nurtures SMEs, and harmonizes across Member States, it can go beyond regulating the digital future—it can shape it.

References & Further Reading

European Commission Coordinated Implementation Roadmap for PQC (2025):
Outlines EU-wide milestones (2026, 2030, 2035) and emphasizes composite deployments, crypto inventories, and harmonized migration strategies.
https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
Press release: https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography

European Chips Act (2023):
€43 billion initiative to boost Europe's semiconductor production share to 20% by 2030—treating chips as a pillar of digital sovereignty.
Official text (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2023/1781/oj/eng
Commission overview: https://digital-strategy.ec.europa.eu/en/policies/european-chips-act

Cyber Resilience Act (CRA, 2024):
Establishes mandatory security-by-design and updateability for digital products; obligations apply from December 2027.
Official text (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
Commission explainer: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Digital Operational Resilience Act (DORA, applies 2025):
Applies to EU financial entities, raising expectations for operational resilience, supplier oversight, and crypto-governance.
Official text (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
Policy summary: https://eur-lex.europa.eu/EN/legal-content/summary/digital-operational-resilience-for-the-financial-sector.html

NIS2 Directive (2024):
Extends cybersecurity obligations across critical sectors and reinforces quantum-ready infrastructure planning.
Official text: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
Overview: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Artificial Intelligence Act (2024/25):
The world's first comprehensive AI regulatory framework—anchored in risk-based oversight, transparency, and European values.

Official text (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
Commission overview: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

ENISA — Post-Quantum Migration Guidance (2024):
Offers practical steps for PQC deployment, composite schemes, and compliance pathways within European organizations.
ENISA publication page: https://www.enisa.europa.eu/publications/post-quantum-cryptography-migration
Direct PDF: https://www.enisa.europa.eu/publications/post-quantum-cryptography-migration/download

ETSI — Composite Key Exchange Profiles (2024):
Defines standards for phased migration and interoperability between classical and quantum-safe systems.
ETSI TR 103 966 v1.1.1:
https://www.etsi.org/deliver/etsi_tr/103900_103999/103966/01.01.01_60/tr_103966v010101p.pdf
ETSI TS 103 744 v1.2.1:
https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.02.01_60/ts_103744v010201p.pdf

World Economic Forum:
Europe’s Digital Sovereignty (2025):
Examines Europe’s digital autonomy strategy amid global competition between Washington and Beijing.
https://www.weforum.org/publications/europes-digital-sovereignty

Reuters (2025) :
“EU rejects U.S. pressure on sovereignty regulation.”
Highlights the geopolitical tension surrounding Europe’s digital-sovereignty agenda.
https://www.reuters.com/world/europe/eu-rejects-us-pressure-sovereignty-regulation-2025-03-14

Part 3 – Quantum Computing & Digital Sovereignty: Securing Europe's Future

Introduction

In early July of 2025, at the Wibu-Systems INNO DAYS meeting, an expert roundtable gathered leaders specializing in cybersecurity, cryptography, semiconductor technologies, enterprise software, and quantum research.

The title of the roundtable was: Quantum Computing & Digital Sovereignty: Building Secure and Independent IT Infrastructure. Together, they explored practical strategies for building quantum-resistant IT infrastructures and strategies for PQC migration, highlight initiatives aimed at securing sensitive data against quantum threats such as the "harvest now, decrypt later" approach and discussed Europe's roadmap toward digital autonomy (e.g., EuroQCI, Quantum Flagship). Those representative companies and organizations were:

Infineon Technologies: A semiconductor manufacturer specializing in security solutions, focusing on hardware for PQC and public key infrastructure (PKI) migration. They were represented by Dr. Detlef Houdeau, Senior Director Business Development, Infineon Technologies AG

SAP: A leader in enterprise software, with expertise in entitlement management systems (EMS) and their integration with secure licensing solutions. Represented by Thomas Depeweg, Chief Product Manager, SAP Deutschland SE & Co. KG

Karlsruhe Institute of Technology (KIT): A research institution (via KASTEL Security Research Labs) advancing PQC and quantum technology research. Represented by Prof. Dr. Joern Mueller-Quade, Professor for IT Security at Karlsruhe Institute of Technology, and IT Security chairman at the Institute for Theoretical Computer Science (ITI)

Wibu-Systems: A specialist in software protection and license management systems, in the process of integrating PQC into their flagship technology, CodeMeter, for secure monetization of digital assets and represented by Oliver Winzenried, CEO and founder of WIBU-SYSTEMS AG.

The session was chaired by Steve Atkins, CEO, Krowne Communications GmbH and Publisher and Editor of The Quantum Space. What follows is an edited version (for readability) of the conversation that took place during the roundtable session between the participants.

PART A – Understanding Quantum Threats to IT Security

Steve Atkins – Without further ado, let's begin. Let me start with Prof. Dr. Joern Mueller-Quade. It's a question that gets asked a lot these days. When do you think we will have quantum computers with sufficient power available to crack today's asymmetrical cryptography?

Prof. Dr. Joern Mueller-Quade – In terms of when I'm actually expecting quantum computers to arrive, I'm a little bit pessimistic because there are huge challenges, but we've also seen great breakthrough lately. There's a risk that quantum computers could be here in, say, 10, 15 years, if it continues like this. I would say the risk of that happening is maybe in the single-digit percentage-wise, but that's a risk we cannot take because as you said, we have this harvest now, decrypt later approach, and even if it comes in 20 years, it's still a threat for the secrets we have today.

Actually, there was a time when people thought quantum computers would be impossible because those quanta are too fragile. But then quantum error correction was invented and became possible in principle. Now these error-correcting codes are being implemented. We are now on track to realize quantum computers. I think we should keep this in mind that we have to go to post-quantum cryptography because we will not be safe anymore in the 10, 15 years.

SA – Well, let's just stay with you there. If some of the current algorithms will be broken after a few years and need to be updated, how do you feel about this constant updating? What does that mean for the design of products?

JMQ - I think that's a necessity because we saw that there were isogeny-based crypto systems[1] which were thought to be safe against quantum computers, but they were later broken on the laptop. This shows that we do not really fully understand the post-quantum crypto assumptions if problems are truly hard. We cannot just jump to the next best solution, but we have to be very careful when changing. First, it's recommended that maybe the next systems should combine quantum-saved crypto with a new scheme, such that you combine the best of both worlds. But also, we have to use what's called crypto agility. We have to design the products in a way that you can safely exchange the crypto. For example, the digital signatures you use to sign the updates, those should be quantum safe in the nearest future because this is what you really rely on when replacing your crypto.

SA - Let me pass that over to Detlev. You've heard Joern's comments about the timelines. How do these timelines affect your hardware development strategy? What does that mean?

[1] Isogenic-based crypto system: Isogeny Based Crypto
Isogeny-based cryptography relies on the difficulty of finding mappings (isogenies) between elliptic curves. Once seen as promising for post-quantum security, schemes like SIDH/SIKE were broken in 2022 and are no longer considered viable. A newer variant, CSIDH, remains under study but has performance issues. Its main advantage is small key sizes, though it is generally slower than lattice-based cryptography.

Dr. Detlef Houdeau – From the semiconductor point of view, you are looking for some guideline from public authorities. First of all, we have recognized in 2017 that NIST in the United States, which is the father of elliptic curve of the Aeron encryption[2], started the standardization on PQC algorithms in 2017. Last year, 2024, we saw that the standardization came to a first milestone, where the first algorithm was published and communicated. Then we heard from the European Commission last year that they have implemented a European dedicated Working Group to create a European PQC roadmap. This was published on the 23rd June 2025. The UK roadmap follows the same timeline, and the US roadmap shows also exactly the same timeline.

From an industry point-of-view, if you are looking for critical infrastructure for public procurement, we must follow these timelines exactly. It was our intention to make a first try last year, 2024, and bring the first algorithm from the NIST standardization into real hardware, into a real accelerator, and combine a conventional ECC accelerator plus PQC accelerator on the same hardware platform.

In December of last year, we got the first PSI certified product[3] from the BSI. It's a learning journey for TÜV, it's a learning journey for BSI, and it's a learning journey for us how long this needs and what new technical areas will come later, down the road.

The deadline for critical infrastructure in the United States, UK, and Europe is 2030. This is what has been announced. But the procurement in the United States starts in 2027. This is in two years. When this happens, traditional, conventional, certified, secure products can no longer be sold. This is, from our point of view, very challenging for the industry because we are starting from the semiconductor perspective. Then we must go to the software application, and finally to the real ecosystem application. That means we must start first, but we need all the other stakeholder along the value chain.

SA – Okay. Let me pass that over to you, Oliver. Why is PQC so important for licensing?

Oliver Winzenried – Licensing makes only sense if the deployed licenses are secure. Otherwise, all these efforts are lost. And if you are looking at existing products, you cannot immediately change everything. But the license deployment process and the license creation process must be PQC-secure very soon. Otherwise, what's happening, device manufacturers or software vendors put a lot of energy in doing a flexible licensing for their product, and then illegal third parties are able to create license generators that can issue licenses in a correct way. The original product will work with a license issued not by the software vendor or device manufacturer, but by the illegal third party. Having a secure

[2] Aeron Encryption
Aeron is a high-performance messaging system used in low-latency environments like trading and IoT. Its encryption layer is modular: AES-GCM for symmetric encryption, pluggable key exchanges (classical or post-quantum), and replay protection for UDP traffic. It's not a monolithic security standard but a framework that users can adapt with PQC mechanisms as needed.

[3] PSI Certification (Germany)
The German BSI's Produkt-Sicherheits-Initiative (PSI) is a certification scheme for IT products. It ensures compliance with defined security requirements—cryptography, secure updates, and vulnerability management. Compared with Common Criteria, PSI is faster and more pragmatic, tailored for critical infrastructure and industrial IoT. Certification applies to specific product versions and must be renewed when major changes occur.

license creation and license deployment process is the first priority and the first step in upgrading to a higher level of security.

PART B – Practical Strategies for Quantum-Resistant IT Infrastructures

SA – Let me just jump back to Detlef. In some domains, PKI infrastructures are in use. Why is the inventory important as a first step for migration from conventional to PQC encryption? What would be the next step after?

DH – We have learned that large companies don't just have one single IT system. They have different IT systems that have been developed over a long period. A German high-speed railway company, for example, have different IT systems that have been developed over time. They must first consider what PKI is behind the system, what is the age of the PKI, and how liable is the system to hacking. Airbus have made the same analysis for the Airbus group. It means you have different domains, you have different divisions, and each of them have their own IT system. And for the military we have different development paths and they must also take time to analyze what is currently in existence.

The second point is before you begin any changes to the front-end, you must start with the back-end. In PKI, infrastructure is the first step and must support both the old crypto keys and certificates as well as the new ones. In some domains, between five and ten years, this must be done in parallel because you have the old system running and you must implement a new system in the field, and the PQI must support both. So, in terms of inventory, you must consider any new modification while thinking about running a parallel mode; the old and the new system together.

SA – Last December, 18 European states signed a joint statement on a composite approach. What's the technical challenge for this?

DH – If you have knowledge of 20 years of elliptic curve and RSA, 1K, 2K, 4K, and so on, and then you hear about a new standard, or about a new risk but you have no learning curve, it makes sense that public authorities would want to combine existing security systems with some elements from this new world. The document you are referring to was the first letter in December last year, that 18 member states in Europe have signed, including Germany and BSI, confirming that they will follow this model, and it's completely understood from the industry point-of-view to be on the safe side.

From the implementation side, as I explained, if you have hardware which supports both technologies, for example, designs and accelerator, you need a more powerful IC chip, and more computing power because you must create this for both. Finally, if this algorithm and combination comes to life, we must also think about performance, because the calculations need more time.

We have a lot of real-world implementations where a citizen has an idea of timing for a particular process. I will give you two examples – starting with payment. If you go to a point-of-sales, today it is 300 milliseconds for the transaction check. If you go to a border control, the passport reading time is three seconds. If we have a new modification of algorithm, it may require more time. This could equate to a doubling of processing time for border controls and payments. And this is for us one of the big challenges of bringing this composite, or combination, of old and new algorithms to full future implementation.

SA – How important is the research on the post-quantum cryptography at Kastel, at KIT, when the algorithms are mostly recommended by NSIT.

JMQ – It's true that NSIT is leading this standardization process, but it is an open process and everybody can contribute. A colleague did indeed eliminate one of the candidates. So, we had an actual impact on this process. In another example, he also did a very thorough quantitative analysis of the time you would need for a quantum computer to break Kyber[4], which was one of the candidates. Kyber looks good in his analysis, and this supports the standardization of Kyber, which also happened. Many researchers worldwide are contributing to this process by showing weaknesses, eliminating candidates, and supporting claims.

SA – So it’s very much a case of optimizing the algorithms for specific use cases?

JMQ – No, we don't change the algorithm. We improve the analysis and maybe the algorithms of the attacker. That's indeed what researchers do, they look at how could certain attacks work, what are the best-known attacks and could we improve on those attacks? If it’s a case that the improved security doesn't hold anymore, then the candidate is taken out.

SA – Technical migration to post-quantum cryptography looks and addresses at many markets. What are the key parameters for PQC algorithm selection from an industry point-of-view? Can you name some examples?

DH – The first point is: We would expect that 95% or more are brownfield migrations. That means we have an existing ecosystem, you have existing applications, and they must migrate. We have less than 5% new applications. Maybe Galileo, satellite or ground communication could be one, 6G could also be a new one. So, we have this relation, and that is my first point.

Point two: You need to have the technical standards and the application standards. For example, for banking, we have EMVCo (Integrated Circuit Card Specifications for Payment Systems). They must migrate this in their standardization. ICAO must also bring these standards into travel documents. So, we have different organizations and different responsibilities to bring technical standards to application standards and to protocols to life. This is for us, one of the boundary conditions. And from existing real field applications, we see today that there are different topics which are also relevant. One was mentioned before – performance – how long we need for this encryption/decryption, because we have some existing real-system in place. There is also the increasing of security and agility for the next 5 to 10 years. This is for us, an important point.

[4] Kyber (ML-KEM)
Kyber is the lattice-based key encapsulation mechanism selected by NIST and standardized as ML-KEM (FIPS 203, 2024). It provides quantum-safe key exchange. Three variants balance performance and security: ML-KEM-512, -768, and -1024. It’s expected to be the default post-quantum KEM, with broad adoption in TLS, VPNs, and software updates by 2030.

Point three is that today, we have limited resources on micro-electronic chips. That means the computer power is not big, it's very small. The chip, for example, in the passport is 4 square millimeters today worldwide. We do not have a big chip that has big computing power with a big memory.

Point four, we have many applications and mobile devices where you have a simple battery. For encryption and decryption, you need energy. That requires real energy efficiency. Encryption/decryption is important, for example, in smartphones. It's important in smart cars which use batteries because any energy you need for such decryption/encryption reduces the lifetime of your smartphone or the distance of your car. As explained earlier, in more than 95% cases, we have an existing system and now we must implement this new technical topic into this framework in different domains.

SA – Would anybody else like to comment on that in terms of looking at this from an industry point of view?

OW – For us, upgrading to Post-Quantum Cryptography is much more than changing some easy ECC algorithms by hardened PQC ECC algorithms. One of the biggest challenges might be what was referred to as ‘Brownfield‘. In our case, our customers have deployed millions of licenses, millions of CodeMeter dongles in the field. They have a security controller which is several years old, which might be not upgradeable to PQC. That's one issue. Our next step is hardening the license deployment process so that this is using PQC schemes while still using it a compatible way for the next 5 to 10 years, with the existing CodeMeter dongles in the field. That's a requirement from the customers that have applications in the field that need to continue to operate.

In parallel, our new hardware – our new CodeMeter dongles – and the complete ecosystem with License Central, with CmActLicenses, and with cloud-based licenses will be upgraded to PQC. So not only the license deployment, but also the license storage will use PQC, to reach a higher level of security. We have the performance issue, of course, but we work intensively with Infineon and using their latest, already certified, crypto-controller series that has some PQC acceleration.

The performance issue might be doable, but on the other side, the keys are much larger. If we talk today about a 256-bit ECC key, this will expand to 2 times 2 kilobit of keys for PQC algorithms. That's much, much more. In our solution, we need to be able to store multiple keys for multiple different licenses, for multiple different products for one software vendor or device manufacturer. We need clever combinations of having a PQC key per Firm Item – per company, and not using a PQC key for each product item.

That’s possible in practice. On a PC and in the cloud, you have enough memory and you have enough resources to do it differently. But if you also have a piece of secure hardware, you need to take care about this memory restrictions and so on. Of course, we want to have one system – we don't want to have an incompatibility with the licenses stored in the cloud or stored in an activation-base and stored in a secure hardware device. So, lots of challenges in implementation above only changing an algorithm.

DH – Maybe I can add two topics. Number one, from an industry point of view, it's very important that we have, in the future, one European PQC library and not national-specific frameworks that we have today. If you go to the BSI TR 02102[5], it's a German library. If you go to ANSSI in France, you have a French library. Eventually, we would like to implement one mainstream library on the hardware and go into one certification. This is a positive thing. The negative thing is we have learned that this first publication from DG Connect of the European Commission (that's a high-level document created by ENISA plus member states) is step one. They will create a step two publication, second half of next year, which is created from the member states level. I have the impression that this will not be a harmonized view. It's coming more from top down than bottom up. If this is the case then we will have national-specific definitions of their priority risks. This is for me, the main negative point-of-view, which we must keep in mind while we all work at different speeds.

SA – Joern, let me ask you this. How does your research help Infineon address technical challenges of this transition from a classical cryptographic method to these more composite approaches?

JMQ – We currently have no direct collaboration, but what we actually do is we think a lot about digital sovereignty, and so we are currently building a cyber-vault where we try to make security explainable such that you can explain the architecture and you can convince someone that your data is secure in there. Of course, we would like to maybe build on Infineon chips. I think some are in there, but we bought them regular way. They are incorporated in the product. We actually built on their research and on their knowledge to build a system where we want to later convince the legal people that it's GDPR compliant to execute algorithms on medical data, on sensitive data in this cyber world.

SA – Has anybody in the live audience started a cryptographic inventory? Would the speakers like to comment on the fact that nobody started anything yet?

DH – Maybe it's not visible, but the BSI organizes every six months a brainpool meeting and invites some large companies. The last meeting was some weeks ago in Frankfurt. The next will be in November in Berlin at the Bundesdruckerei. In these meetings, the Ministry of Interior participates, the BSI is participating, and some large companies are participating in order to exchange the views of large German companies, what they are doing for their own purposes, and also what's of interest for the German Federal Government and for German projects. This exchange is running, but it's not visible and you see not many publications are covering it.

SA – Are they normally well-attended? I mean, are they growing in attendance for these meetings?

DH – Yeah, it's growing. There are more and more companies participating, but it's a closed event, you can say. It's not an open event where you have journalists but in terms of corporations that are now being included, it is taken very seriously. The main aspect is to have this informal platform

[5] BSI TR 02102
BSI TR 02102 is Germany’s technical guideline for cryptography, covering key lengths, protocols, and recommended algorithms. The 2025 update incorporated PQC readiness, advising a shift to quantum-safe methods by 2030 in sensitive use cases. It forms the baseline for German and EU implementations of PQC in TLS and related systems.

between industry and government to have a view from both sides; what are the next milestones from the industry point of view and what are the milestones from the public authority. For us, the European regulations and also the national regulations are a must. We cannot ignore this. I hope that most of these regulations fit well with the requirements from the industry like Wibu-Systems, so that we can take exactly the products that we developed for these markets and they can be reused in the private sector.

PART C – Software and Licensing in the Quantum Era

SA – Thomas, can you very briefly summarize what the SAP Entitlement solution is about and how it works with Wibu-Systems CodeMeter?

Thomas Depeweg – When you have followed the earlier session with Roche, what Roche is doing is about the integration of the complete service chain from ordering until the end delivery of the product or service. SAP is a company who would like to provide its clients with the entire business suite. That means a complete integration of all your business processes. Because our customers are moving more and more from the physical world to the digital world, it means that there is not necessarily a physical product in the center anymore. I would say that with this shift from the physical to the digital world, entitlement management becomes more and more important. And the core element of entitlement management is the entitlement.

What is an entitlement? It is a right. Entitlement means it is a right you give someone, and we take the term ‘entitlement’ very broadly. But it is not just a license. Even though a license is a very important type of entitlement – but it could be any other right, especially in the digital world. An example could be the right of service, of maintenance. It's the entitlement for warranty. It's the right to get access to a learning model. It's the right to get access to your parking garage. It’s a right – it’s an entitlement. Companies who are dealing more and more with rights need a repository to handle all these rights very centrally, to determine what rights have been given to a certain customer and what are the exact elements of these rights. These rights are best automated rather than be manually approved. They should be completely automated from order entry until securing and executing on the right. This is what entitlement management is all about. Therefore, of course, we need Wibu-Systems because all the security aspects, the ‘last mile’, we call it, can only be done by companies such as Wibu-Systems, from our point of view.

DH – Some years ago we heard the phrase Digital Twin[6]. Back then it was only a figure of speech, but now we have some standardization, the title has become more concrete. Number one, with the digital twin, we will see a digital identity, not for people, but for products and for machines. Some new descriptions will arrive, like digital product passport[7], through European regulation. This type of digital world must be also implemented in the IT system like SAP, from the shop floor as well as in the office world. Most areas must deal in the future not for people identities, but also for objects and for software because each of these elements need identities.

[6] Digital Twins
A digital twin is a real-time virtual model of a physical asset, connected via sensors and data streams. It allows simulation, monitoring, and optimization across a product’s lifecycle. In cybersecurity, digital twins help detect anomalies by comparing expected digital behavior with physical performance. EU industry initiatives are embedding PQC and security-by-design into digital twin frameworks.

[7] Digital Product Passport (DPP)
The EU’s Digital Product Passport initiative creates a standardized data record for products (materials, repairability, compliance, sustainability). Pilots are already underway for batteries, textiles, and electronics. For cybersecurity, the DPP links to CRA and supply chain transparency, ensuring product data is verifiable and portable across the EU market.

SA – Why do you think the combination of SAP's entitlement solution with Wibu's CodeMeter, creates such significant value for the consumer?

TD – You want to automate where possible and you want to make sure that the content of your economical contract you have with your customer – your promise to your customer – find its way through the complete chain until you really have a license which is secure and that your customer is not overusing it. Because SAP is not providing this last mile, as we call it, we have this very close relationship to Wibu-Systems. And entitlement management, EMS, it's called in our world, is the orchestrator of this world. We distribute the rights to Wibu-Systems, if it's a license, but also to a cloud tenant (if you have a right for a cloud tenant) or be distributed to any system. My example is a parking garage. Maybe a parking garage needs to know who has the right to enter. And this is a spider in the web, to say, that it's EMS.

SA – Oliver, security of software licensing is often considered less important than flexible licensing. Now, how does post-quantum cryptography play a role in software protection?

QW – It's a little bit similar to what I said before. If somebody else is able to generate licenses, then all our efforts make no sense. We often hear that software vendors and device manufacturers start to think about licensing because they want to implement new business models. They want to sell additional elements to perpetual licenses, so that means a one-time sale. They want to use the new business models like subscriptions, like pay-per-use. They want to have it very modular so that they can offer a product with some basic functionality to a very competitive price to the market, and then add features on demand depending on the user's requirements and licensing these additional features in a different way. That's the main driver, and showing the return on investment for the device manufacturer for the software vendor quite quickly is why they start thinking about using such a licensing system. We have the discussion quite often that the device manufacturer or software vendors, think they know their customers and their customers are okay. They don't think that their customers will actively bypass the licensing they provide to them. But as soon as their pirated products are available, in China for example, and in a way that the original product doesn't need to be changed because they have been able to create a license or to modify it a little bit, modify the application a little bit, so that it's working – then the customers can use it without paying for it. They buy only a few licenses, but they are using much, much more.

Some of our famous customers – I will not mention their names – are also in the automotive area, and have witnessed this a lot in China. And it's not just a simple thing, either. Chinese organized crime, or I don't know how you want to call it, have spent a lot of effort to make the copy product, the pirate product, look exactly the same as the original. They try to copy electronic devices from our customers, by buying our original dongle and modifying the case so that it looks exactly the same. You see that when this happens, security becomes very important. Then, a lot of efforts are done to increase the security level. If this becomes standard, and we've used asymmetric cryptography for the license transfer and for the license creation, as soon as it can be broken by these criminals, then it's more-or-less worthless. We need to be able to have this hardened way of creation and deployment of licenses prior to the technical possibility to bypass the existing schemes.

DH – Maybe Oliver, we can expand a little bit that view. For me, software today is not only a simple software for, for example, machines. We have also the combination of software plus artificial intelligence in this software now. And AI will continue to moves further and further into edge, into healthcare, into consumer electronics, automotive – even smartphones. Each smartphone has today 10 algorithms. Not everybody knows this. So, we now have this in the edge. And AI every quarter gets some updates about performance, about quality and so on. With this, you have sped up not only traditional software, but also on software which have an AI function and must move further into the edge. For me, this is a driver to bring more software updates into the field for connected devices.

OW – Yes, that's completely right. And licensing is only one issue. The other issue is that through the protection schemes for data, AI models and program code that protect and enable not only different licenses, but also protect the integrity of the application, the integrity of the code, and makes it harder to do reverse engineering because it's protected. These are additional factors that require a high level of security. In fact, we have applications today that protect the AI application and the AI models. For example, in medical equipment today, these AI models help the doctor to analyze, for example, the results from computer radiography equipment and helps them to see critical points much faster. These AI models needs to be frozen with the certification of the medical device according to MDR[8]. We can help to do this integrity protection for the models as well. We work on monetizing AI models. There is an ecosystem coming from NVIDIA for that purpose as well, where we are working on providing the secure licensing for this purpose. That's one. It can be extended to other licensing of data, for example, for additive manufacturing for 3D printing data.

SA – Can I ask, Oliver, in terms of CodeMeter, what are the actual technical hurdles for introducing post-quantum cryptography?

OW – There are several. It needs to be implemented in all types of our license containers – in the CodeMeter dongle with the security controller from Infineon. It needs to be implemented for the CmActLicense for the activation-based software-based licensing scheme. It needs to be implemented in the CmCloud server. That's only the site where the license containers are stored. It needs to be also integrated in the whole ecosystem. Therefore, creating the licenses, deploying the licenses in License Central and with the other tools, everything needs to be upgraded to PQC – with the difficulty of the larger key length. What is very important with this difficulty is creating an upgrade pass for our existing customers that are users of our systems today, from today's solution to future solutions without replacing everything in the field, which would be not possible.

SA – Are there any other hardware constraints?

OW – Yeah, in terms of the hardware, there will be a new hardware probably in 2027 with new security controllers that have special accelerators for the PQC algorithms. But today's hardware that is in the field will be used for the next 10 years as well. We need to improve the security level for licensed

[8] Medical Device Regulation (MDR)
The MDR is the EU framework for medical device certification. It applies to hardware, software, and AI-based tools used for diagnosis or treatment. Devices are risk-classified, require CE marking, and must support traceability and post-market monitoring. For AI, “frozen” models are certified to guarantee reproducibility, though adaptive AI remains a regulatory challenge.

deployment and license updating for this existing hardware also. That's very important for the customer base.

SA – Let me throw this over to the panel: How does SAP and Wibu-Systems' solution align with PQC migration strategies that's already been discussed by both Infineon and KIT? What are the opportunities for collaboration?

TD – I'm coming from a purely business angle. For our end, we hand this over to Wibu-Systems because they are experts in developing secured software for whatever challenge is coming next. We tell our customers that it's important that there is a close technical relationship between these two systems and the business relationship between us and Wibu-Systems. Now we just direct our clients to Wibu-Systems when asked these critical questions.

OW – That's true. We also need to upgrade the authentication of the SAP ERP system to our License Central so that no-one else can create that license. Only the EMS is able to send the order to create the license. Everything else – how the license is created, what technology is used behind that, and what technology is used to protect the software or data – is outside of the ERP system and outside of the business process.

TD – Of course, in our technical relationship, we have to be state-of-the-art, and whatever is needed, we have to do it. We have a specific security department in SAP with a lot of experts who are doing this. We are the biggest software company in Europe, so you can be sure that these problems definitely are on the radar of my colleagues. With the help of my colleagues, my department will take care that everything will be future safe.

SA – Joern, you have spoken about migration, and how this migration might not be a one-step approach.

JMQ – It might be a more continuous process. To give you an example, you can even harden non-quantum safe key exchange protocols by over-encrypting the communication with a symmetric key. If you have a symmetric key from the past, from a previous usage, you can just use it to do an encrypted key exchange. An encrypted key exchange is already a huge hurdle for someone having a quantum computer because for this attack the hacker doesn't even have the data because it's encrypted. This is just one tiny step. Then one has to go step by step until we fully replace the non-quantum state crypto.

DH – We have not discussed one area that is also important. We've been speaking about crypto agility, but we also need to speak about products which have different lifetimes. Crypto agility for a product which has a three years lifetime is less flexible. If you are looking for products which have 20 years and more in the field you need a different strategy. A one-solution-fits-all doesn't work in this scenario. We must also think about industry applications. We must think about automotive applications. We must also think about consumer electronic applications which have different product lifetimes. Then you must bring a different level of agility of hardware, of software and of hardware-software codesign down the line. A single solution for everything is not possible.

JMQ – Yeah, I can only emphasize this. We have a joint project with Wibu-Systems, where we think about crypto agility in medical devices. And there we also have several steps. And one is to be able to replace the hardware, to pull out the dongle and replace it with a new one capable of handling all the advanced post-quantum elements. But it has, so to speak, a software-based migration up to a certain point. And beyond that, because medical devices are usually used for a long time, we even take into account that the hardware will have to be replaced, and then you will need a secured authentication process to ensure that you know that it's not a malicious third-party replacing the hardware.

SA – Okay. Anybody else want to comment on that? I understand what you're saying, that there's no one-approach-fits-all. You have different products with different lifecycles over them. But how would a small or medium company be able to adopt these solutions cost-effectively? Is there some plan or roadmap or is there some process? How do you plan for something like this over a product lifetime?

TD – I can only speak for EMS. We are a cloud solution. Our price model is based on the number of entitlements, which does not change if you're a small company and you might have just a small number of entitlements and the price is pretty cheap. If you're a larger company the price will increase accordingly, but you have deeper pockets. That's the idea of our price model. Because our software, EMS, is running in the cloud it is being updated constantly meaning the latest version is always available – with the latest security, that we have implemented as SAP. Our customers who are using our EMS cloud service can be sure they are using the very latest security methods that are available on the market.

OW – I think in our case, it's not so difficult for our customers. It's more or less our task to provide the tools and to provide any new dongles that can handle the new PQC algorithms as well as the cloud server and the software-based licenses. In our business model with customers – with the software vendors or the device manufacturers, we either count the number of licenses that are issued, or we have a small percentage, something like 0.5% or something like that, of the value of the products that are licensed with our technology as a flat rate and without counting the number of licenses issued. Then it will make no difference if the vendor is creating a new license in a compatible way for the existing dongles, for example, in the field, or if perhaps he's creating a new license with PQC schemes.

DH – Maybe I can add two topics. Number one, we have had some change in policies. For example, in industrial IoT, we have seen the change from the perimeter protection five years ago. Now we are talking only on the subject of zero trust. That means you need credentials before you start machine-to-machine communication. Credentials must be stored and secured. You have some new framework that goes into the shop floor, or goes in the operation OT, and no longer this traditional old perimeter protection part of your number.

Number two, and this is very important, we have heard recently about the Cyber Resilience Act. Some products are not able to create software updates over five years, but five years is a must in this regulation. I have heard some washing machines are not able to do this. When buying a washing machine, you normally have a warranty of only one year. However, the Commission requires a five-year software update cycle. These examples show you that also there are some migration obstacles in many markets to fulfill this Cyber Resilience Act, which will be enacted in two years from now. The

European Commission have mandated It is a must that software updates in the future should take place.

And for critical infrastructure, you need a third-party certification by, for example, TÜV. That creates a certain restriction for consumers when choosing products. In the past, the CE label was placed on product safety aspects. Now, manufacturers of consumer good must look toward a security certification if they want to trade within the European market. This change will also need some modification to incorporate the concept of PQC or software algorithms into any future products. The Commission is aware that some products and companies will be forced out of the market. But this is a clearing situation as the commissioners step up security for consumer products. This will happen. It is unlikely the program will be reversed, so changes should be considered and implementation made as soon as possible.

PART D – Europe’s Roadmap to Digital Sovereignty

SA – What measures should the European Union take to avoid falling behind in this quantum race? Do you already know of any measures that you can share with us?

JMQ – I think the European Union is not badly placed in the quantum race. We have very terrific researchers, very successful researchers. I think the main problem is that a lot of the ideas do not fully go from academia to the market. My fears are that we will miss another market, not the quantum market, but the AI market, which is also going to be huge in the future. It could be that there we will have some the winner-takes-it-all development. Perhaps by the big companies who invest billions in models which are hosted in huge giga-factories, which are next to some power plants who we, in Europe, will not be able to catch up with. I think energy is very expensive here, and energy is one of the main ingredients of these AI models. I fear that we have to really think about what to do there.

I even heard of a proposal to house computer centers outside of Europe – where energy is much cheaper, and then discuss whether IT security solutions must still have sovereignty, even though they are not located physically in Germany. I think we should focus purely on a convincing concept for IT security, rather than digital sovereignty in the sense of every component in the chain of value is to be produced in Germany. It’s a nice idea to have everything built here in Germany for security reasons, but there must be some way to convince us that if we do this outside of Germany, foreign powers (of the country we are doing this in) are not harming us, that they are leaving our compute center alone and that they are not committing espionage on us.

Then I think there will be much more collaboration, and then we will be able to have an extended vision of what digital sovereignty means. It does not mean we have to do it ourselves. It means we understand what other people are doing. We understand it so deeply, and they can explain it so well that we can use their knowledge and resources without harm to ourselves.

SA – Nice idea, but what time frames would you put on this approach?

JMQ – I think this idea of building compute centers outside of Germany, which are still trusted, could be something which we could do quite soon. I would propose that we build racks and computers together with security measures in containers and then seal the containers in a very secure way and then simply move them to build a modular AI supercomputer built from these trusted containers.

DH – Maybe from my point of view, it's important to know that Ursula von der Leyen (the President of the European Commission) stated in 2021, that any devices which can be connected to an information system, can be hacked. This was the initial point to create the Cyber Resilience Act. As of 2022, we now have this Russian-Ukraine war; since this time period and the Ministry of Interior and Ministry of Defense are talking about composite threats, not just cyber security, now. This means we have multiple attack situation in Europe, not only from the criminal area, but also from some foreign public government authorities. They have money, they have budgets, and they have a little bit power. So, from my point-of-view we have a new game. We are no longer speaking about traditional hackers or traditional blackhats or even a traditional cyber security situation. We now have to consider that some government agency or a group related to a specific government, will create some attacks in the future. This would be aimed at critical infrastructure. For me, it's a new game-changer that becomes a high priority in terms of digital sovereignty.

JMQ – I completely agree. I think that before the Ukraine war, we thought a lot about espionage, but not so much specifically about kill switches, where everything is simply turned off – communications, infrastructure and so on. I think we were too relaxed in the past and felt too safe, and we didn't see this coming early enough, and so we have to take care right now.

SA – Speaking specifically about timing there is a Coordinated Implementation Roadmap[9] for the transition to post-quantum cryptography from the NIS Group. I know that they've put out a report that covers timings and miles stones. Can you comment on this?

DH – There were two deadlines defined. This was published two weeks ago. They say high risk areas must be ready by 2030. That means high risk for public sector as well as for the private sector. The United States defined only public procurement in the United States for 2030 for high risk. For medium risk in Europe, the deadline is 2035. Safe timing for the United States as well as the UK. They have a very synchronized framework about risk approach and implementation deadlines. These timings have been around for a while now. This report was expected, by the way, in April, but there was a lot of overwork of this document and modification, and we have heard some friction, let me say, between different agencies on the European level, like ENISA, DG Connect, and so on. Policy could now be changed so that national bodies create the next level of paper which goes deeper into detail. For example, in Germany, we have Toll Collect. This is a PKI system. It's only working in Germany. It's a critical infrastructure to us here in Germany. Is this deadline 2030 or what? Such national priorities could be pushed to the front of the queue, so to speak, as we need to onboard and update trucks and bus onboard units in two years or in three years, with PQC technology solutions. Then you have to replace all the existing equipment.

Such national-driven programs come next year with the next report. Then we will see more solid proposals, which domains and which risk approaches are pushed by member states and what is their concrete deadlines. Today, we have this higher level, umbrella view. But from my point of view, this next level of documentation will make everything more concrete.

OW – I think there are even more deadlines. For PQC, the 2030 and 2035 deadlines are defined now. But if you are looking at the Cyber Resilience Act, with the deadline of 2027, that doesn't require that the products have post-quantum crypto inside, but it merely requires that the products fulfill many requirements that allow this updatability and so on. For products, for device manufacturers, for software vendors, there are a lot of tasks to do in the next two years or to have finished in the next two years. It needs to be done maybe earlier, finished earlier so that it can be certified and everything.

[9] EU PQC Roadmap
The NIS Cooperation Group’s roadmap (2025) sets EU-wide milestones for PQC adoption: 2026: National roadmaps and pilots launched. 2030: Migration completed for high-risk systems. 2035: Migration completed for medium-risk, aligned with US/UK. The roadmap stresses composite deployments first, mandatory crypto inventories, and regulatory alignment with NIS2, DORA, and the CRA.

DH – Maybe we can make it a little bit more concrete. In the Cyber Resilience Act, most of the companies must look to their own product portfolios and at the risk concerning existing sold products in the market and must decide which of them must be upgraded to get the CE label as soon as possible. This must be decided this year. Next year, all the important implementations that are important for the purchase department, for the development department, for the quality department, for the sales and after-sales department will need a lot of changing. This must be implemented next year, in 2026. In 2027, you need to incorporate the CE approval process. It's a tight deadline but it's important that you have CE certified stock ready before the deadline is reached.

SA – It appears that after some of the discussions on Quantum Computing that we've had today, that real-world, external, factors are causing increased attention and focus on the subject to try and get things moving as quickly as possible. Let's just switch back to products for a moment. Can I ask, Thomas, what's the SAP strategy for entitlement management in the future?

TD – In general, of course, our strategy is in line with the overall company strategy. I think there are two main areas. One area I have covered earlier is that we are the best in terms of software suites. We dominate the market not by being very good in a specific field, but by ensuring that we deliver the most value to our customers with our integrated suite of products. That's one area. The second area is clearly Artificial Intelligence. It's clear that SAP will move into AI, and we are doing a lot of things every day towards this move. AI is really our top priority at the moment. Why? Because the role of a business user will change completely. We do not see it today, but we will see it change very soon.

By that, I mean you are not doing transactions anymore, but you are somehow the manager of identity with AI. It's all these AI agents which we currently see in the scientific world. When these AI agents become real, you as a user will only do the exceptional process rather than the mundane processes. You will be managing this AI agent, or you will be the one who's implementing them and making the decisions. You're moving as a user into the role of a decision maker. That's the future of cloud ERP. This is a strategy coming from the board, and that we are following today.

Going down now to EMS, what does it mean? Well, we are not a user-centric application. Our implementations run in the back-end. Ideally, nobody cares, because everything is running fine. We are already there today, and we will support this by enabling our users with some AI tools to be even more productive when configuring our solution. And then also giving data to other solutions so that they can then use it to build their own agents. Some of this data is within Entitlement Management. Combining that with other data enables us to create the database to build the AI agents.

DH – AI is a far more complex topic than PQC or quantum computing, because we are talking about different bridges between cybersecurity and AI. You can define three classes: cybersecurity for AI, which already covered by Oliver, cybersecurity with AI, and cybersecurity against AI, because also cyber-attackers use AI. These are three different domains, and there are a lot of research topics in this area. Also, we are not talking about this AI but rather conventional AI, anomaly-AI, large and small language AI, and now agentic AI. These are different boxes with different algorithms with different applications behind them. AI can be a driver for new business, but can also be a driver for software update topics and a driver to bring more security into the IT system – not only in the network, but also in the edge – we call this endpoint security. Both, network security and endpoint security must be solved on this topic.

SA – Why will physical CodeMeter dongles still be needed in the future? Along with software and cloud-based licensing procedures?

OW – It always depends on the application and on the threat scenario, for which container is best suited for the application. But we see many applications that need to run with a high level of security in an offline scenario. For example, engineering tools used in the office area might often use cloud licensing. They don't need a dongle connected to the PC workstation while the engineer is working with the engineering tool. But we also have PLCs in process automation systems that cannot be securely switched off; they need to shut down the process in defined steps to be able to shut down in a safe way. In that case, licensing needs to be local, and cannot be used from the cloud, probably. Other offline scenarios also exist in other schemes as well. Having a small piece of hardware is something which, with limited complexity, evaluated and certified according to Common Criteria in regard of the crypto algorithms, is something that works well for these manufacturing floor machines. They are not so well suited for a high-end PC, because the complexity is so big that an evaluation is no longer possible. This small piece of trust anchor is still very valuable in many applications.

DH – I think there's one trend expected in the next couple of years in Europe; the so-called business wallet[10]. The Commission have published the specification on the business wallet. It means that for people who are working in a company they will get a wallet on the smartphone. You will see also the driving license on the smartphone. You will see the future travel credential on smartphone. This business wallet is used to bring digital identities to the factories and also for the people in the office domain, and this is a digital transformation. The combination of the dongle access along with this business wallet, which is an app on smartphone, could be a new game changer to bring the digital identity of software, of objects, and people together. This was what SAP was talking about when they spoke about the 'digital twin'. We are now getting a more concrete understanding on what that means. By the way, this business wallet will be tested by a large-scale group with more than 100 participants starting in September 2025. It's funded by the European Commission under the eIDAS 2.0 regulation[11]. They will bring out this real implementation to show up how this can be incorporated into business models in industries. For me, this is a game changer, the creation of new business models. It is a window of opportunity to bring authentication and identification into the market. The dongle is one piece in this scenario.

[10] EU Business Wallet
As part of eIDAS 2.0, the EU Business Wallet (EUBW) extends the European Digital Identity Wallet to companies. It will hold verifiable credentials such as registrations, tax IDs, licenses, and conformity certificates. Pilot programs start in 2025, aiming to streamline compliance, procurement, banking, and supply chain transparency with cross-border recognition.

[11] eIDAS 2.0
eIDAS 2.0 (2024) introduces the European Digital Identity Wallet (EUDI Wallet) for citizens and businesses. It stores and presents verifiable credentials (IDs, licenses, diplomas, payment details) with legal standing equal to paper documents. Member States must roll out wallets by 2026–27. They will be mandatory in regulated sectors and interoperable across the EU.

SA – If you don't mind, I'd just like to circle back to the subject of AI, and especially with SAP and Entitlement Management. What is SAP’s strategy for dealing with AI, especially when talking about Entitlement Management.

TD – I think I outlined already the overall idea behind our strategy. With the EMS especially, there are two dimensions. One thing is that our customers, the customers of EMS, of course, would like to be offered AI-based services more and more. For us, we see that as part of an entitlement. Here, you are entitled to use an AI, you are entitled to different kinds of coins, of tokens, whatever. This is, I would say, a use case for EMS, but it's not something completely different. It's one use-case further than a lot of other use-case, but it shows to our customers that EMS for digital products is becoming more and more important because AI is becoming more important.

What is interesting for us is software. We are a software product, of course, and as I already said, we would like to add AI capabilities for our users, which would mean we have rule generation and scripting capabilities. These tasks are traditionally carried out by hand. We already have a working prototype. You just put in natural language and our AI agent will automatically translate this into the right script. This script is now the basis for a rule in Entitlement Management. This is can be done during your design and entitlement model, and with AI capability, you are much faster.

SA – I'm going to pass this over to Wibu-Systems. What is monetization of AI models and 3D printing data all about?

OW – Yeah, that's similar to monetization of a software-realized function in devices or in software. On AI models, you want to measure the usage of the AI model. That's a monetization that can be realized with the same mechanisms and with the same principles. The additive manufacturing area or 3D models, that's in fact very similar, but a totally different use-case.

For example, Daimler Trucks is doing the spare part logistics in 3D printing. In the past, the automotive industry had to produce a lot of spare parts, that had to put on stock for 20 years, then you wasted any remaining parts after that time. If you needed a spare part within these 20 years, it was sent by air freight to any location in the world so that the repair station could put it into the car or truck or bus. That is not a very good example for sustainability for the environment. If you are able to produce the spare part by 3D printing at the place where you need it, then, of course, it's much, much better. The spare part business is a business with a good margin, and no manufacturer wants to give away his spare part business.

So, the protection of the 3D models is very important. And in addition, the protection of the printer that uses the part needs to be controlled in terms of parts volume. From the licensing point-of-view, it's quite similar like pay-per-use models with software. So, it's pay-per-use models for the digital rights and for using and handling this production data for additive manufacturing.

SA – Can Europe achieve digital sovereignty without relying on non-European tech, or is a global collaboration essential?

DH – I think from a European point-of-view, we are telling the story that Europe must be open, number one. Number two, we have a lot of regulation in Europe; GDPR for example, the Cyber Security Act, the Cyber Resilience Act, AI Act, and so on. Such numbers of regulation are not existing, for example, in the United States. They can have their business models. They create different ecosystems. You have the Android world, you have the iOS world, you have the Windows world. In each of these areas, companies have no standardized solution. They create their own framework, and at the end, high propriety security architecture in hardware and software. This is, for me, a completely different policy.

In China, they use, from my point-of-view, cybersecurity as a barrier to non-Chinese companies. Let's say we have a local certification. If you are not a Chinese company, you cannot get the certification because you have no local access. China takes security and cybersecurity as a barrier-to-entry. The United States is completely different, and Europe is now opening up their markets a little bit more. We have spent some years discussing the topic of sovereignty because we have learned that some products are not developed in Europe and are not produced in Europe. We cannot know or control if there is any backdoor solution inside the products or if there are any functions which don't conform. At least that is my worry and suspicion. In the terms of the military, they are concerned about 'sleeping electronics' in potentially high-risk and critical devices and areas.

Fundamentally, Europe is now thinking more about what are the key technologies which we can control, develop and analyze in Europe and what is not so important? This makes the idea of digital sovereignty more concrete and immediate as we incorporate this approach into products, systems, infrastructures, communication, and finally, for chips.

SA – How do we balance innovation with regulation in Europe? How are we able to do it? Europe is a very regulated area. How do we achieve a balance enough to participate in the quantum race?

DH – I would expect that sooner or later we have not only a European roadmap with deadlines for risks but as a regulation to have a clear implementation plan for clear application areas. And from my point-of-view, they will start with a public domain or public sector, and then move onto critical infrastructure, then to the essential infrastructure and so on, step-by-step in a top-down approach. Sooner or later, I would expect to also have a PQC migration regulation on the table. The roadmap is a front runner. It's there to make the industry and governments aware about what's going on and bring it all on the same page. But later on, you will still need a clear regulation topic about real deadlines and penalties for non-compliance.

JMQ – I think balancing regulation and innovation is very, very hard. It might be easier for post-quantum crypto because there, we know what we want. We want this transition to happen. But if we look at AI, I fear that we will regulate everything, and then the models produced in the US will be better, and then we will use those instead of the models produced in Europe. It's the same with our secret services. In our research we very constrained and not allowed to do this and that, and then we get a hint from a friendly secret service source who got this by ignoring all the rules we have to follow ourselves, and we use it.

SA – Do you think we push ourselves into a corner through over regulation?

OW – In my view, we cannot do everything ourselves in Europe. We should continue the co-operation in research and we should continue the cooperation in business for sure, because we want to make business. We need to work with the US, we need to work with the Asian countries and with China. What politicians might do best is to try to get international standards, and then we can follow these international standards, and we should have the competence and the people to do the implementations according to these international standards by ourselves. That way can have a say in the direction to go and create our own competence and sovereignty in these areas.

SA – Just to bring it back to individual companies, how should a small business prioritize its PQC investments? How do they go about prioritization when confronted with different timelines, especially when talking about SMEs?

DH – I would start from the value chain, from the micro-electronic point of view, from the discrete secure element, from the embedded security point-of-view. We must bring this into our roadmap. We must bring these different products and different platforms and different applications, and we must offer these in different markets. We cannot ignore this. We know that many customers, for example in automotive, are asking specific questions on these topics. That's because they are thinking about generations of cars, and they must think about the next generation and the one after that and need to bring such elements into the field. We have many such discussions in other industries as well. In automation, machine producers are asking today when we will be able to sell them these next-generation ICs for their computers.
As we continue to talk with a variety of companies their requests are getting more and more specific and we must ensure that we convey these requests to become mandatory features that are needed in the market. If we don't, we remain out of this game.

OW – Maybe SMEs don't need to focus so much on PQC today. So the first thing, if companies have products that are somehow networked with electronics, they need to focus on the Cyber Resilience Act, which is very close to deadline. And regarding PQC, if they are using licensing with CodeMeter, we are happy to help them in the journey to upgrade to PQC-ready licensing solutions that give a higher level of security for their products as well.

SA –Is there a significantly higher cost for a company migrating up to a PQC compliance for a legacy system?

OW – If they want to replace the CodeMeter dongle with one that is PQC ready, they need to buy a new one, yes.

SA – That's sounds fairly simple.

OW – It is fairly simple, yes.

DH – As we said before, Steve, everything needs to be ready for 2030. Keep in mind that today we have in many government agencies, so-called 'Connectors', which decrypt and encrypt information and communications. Every German embassy have such connectors worldwide. And by 2030, they must replace them. So, we have some major challenges in the market.

SA – Do you think they're as ready as everybody else is?

DH – No. But this is a clear deadline, and the German government will see products at this time, even if they are only appearing on PowerPoint slides today.

Roundtable Sum-Up

SA – Okay. Well, I'm going to do a very, very quick sum up from my notes that I have here. There is a real urgency now, for PQC migration. The European Commission have released their report on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography and these time frames are now set in stone. The Cyber Resilience Act will have a real impact on products coming to the market. If companies have products that are going to be connected to something, they have to be secured. There's very much an urgency for this now.

Also, the importance of crypto agility, is now becoming incredibly important to enable a move from traditional cyber-security to crypto-based secured solutions. We need a European-harmonized roadmap that needs to be Europe-wide and not individual country-driven, which is even more important these days. Finally, from what I've picked up, certainly from Wibu-Systems and SAP, there are some fairly industry-specific solutions that have to be incorporated in the mix.

Would any of you gentlemen like to give a final statement on the encroaching quantum revolution?

DH – From an industry point of view, PQC is coming and will be present, so we cannot stop this train. You must jump on this.

JMQ – We have to switch to PQC, but we don't yet fully understand everything, so there's a lot of research to be done.

TD – We rely on partners like Wibu-Systems. Our customers are taking their commercial process into our systems and for what comes then, which is relevant for this topic, I hand it over to Wibu-Systems.

OW – I can repeat that we try to incorporate our customers in the journey, that we involve them early. Especially for this migration path. We do not necessarily throw away everything, but instead increasing the security level step-by-step, using existing, rolled out licensed containers as well. That's a smooth migration for the software vendors, for the device manufacturers, and for their customers.

SA – Gentlemen, thank you very much for participating today.

Conclusion

The cryptographic clock is ticking. Whether large-scale quantum computers arrive in 2030 or 2040, the regulatory deadlines and security imperatives are here now. Post-quantum migration is no longer optional; it is a survival strategy.

Europe faces a double challenge: move fast enough to secure its infrastructures, while also navigating its unique path of digital sovereignty. Regulation has given Europe a shield. Investments in chips, cloud, quantum, and identity systems have given it some muscle. But execution—harmonization, SME support, innovation at scale—will determine whether sovereignty becomes an asset or a liability.

The roundtable discussions in this volume show both the urgency and the diversity of perspectives. Some see PQC as an engineering project, others as a compliance milestone, others as a sovereignty test. All are correct. That's the point: this is not a single-issue transition. It's a reshaping of the digital ecosystem itself.

If there is a single takeaway, it is this: start now, and start together. No organization can migrate alone; no Member State can achieve sovereignty in isolation. Europe's advantage lies in acting as a bloc, aligning its standards, investments, and regulations to create a trusted, quantum-safe, sovereign digital future.

The coming decade will decide whether Europe is remembered as the world's most effective regulator—or as a trusted innovator that turned values into competitive advantage. The difference will be made by the choices we start making today.

About Wibu-Systems

Wibu-Systems is a recognized leader in security technologies for the global software licensing market. Established in 1989 by technology entrepreneurs Oliver Winzenried and Marcellus Buchheit, the company has built its reputation on a singular mission: to provide the highest levels of protection, licensing, and security for digital assets and intellectual property in an increasingly connected world.

Its solutions are used worldwide by software publishers and manufacturers of intelligent devices, spanning PCs, mobile platforms, embedded systems, PLCs, and microcontrollers. Wibu-Systems emphasizes platform independence, interoperability, and rigorous quality standards rooted in German engineering.
The company's leadership, products, and technologies have earned numerous industry awards. Its flagship platform, CodeMeter, has been internationally recognized both as a content rights and entitlement solution for office applications and as an endpoint management solution for industrial environments. In 2014, Wibu-Systems, the FZI Research Center, and the Karlsruhe Institute of Technology (KIT) jointly received top honors for the development of Blurry Box, a breakthrough encryption technology later integrated into CodeMeter.

Research and development remain a central pillar of Wibu-Systems' strategy. The company collaborates with leading technology vendors in areas such as Industry 4.0, the Industrial Internet of Things (IIoT), and OPC UA, while also contributing to industry bodies including the Association for Advancing Automation, the Open Industry 4.0 Alliance, and the Trusted Computing Group. Through these initiatives, Wibu-Systems continues to advance security best practices and strengthen trust in the digital economy.

https://wibu.com

About The Quantum Space

The Quantum Space (TQS) is an independent research and intelligence platform dedicated to quantum computing, post-quantum cryptography, cybersecurity, and digital sovereignty. Our mission is to equip Europe's decision-makers with actionable, evidence-based insights to anticipate and adapt to the quantum era.

We specialise in sector-specific strategic analysis that bridges the gap between technical depth and boardroom priorities — supporting leaders in technology, defence, finance, and infrastructure with intelligence that is:

- Technically rigorous — grounded in verifiable data, technical standards, and leading-edge research.
- Strategically relevant — framed in the context of sovereignty, resilience, and competitive advantage.
- Forward-looking — identifying not just immediate threats, but the emerging opportunities of quantum technologies.

Our research methodology integrates:

1. Primary source analysis — EU directives, national strategies, and industry technical publications.
2. Sector engagement — consultation with vendors, regulators, and operators across critical industries.
3. Comparative intelligence — mapping Europe's positioning against global competitors in quantum readiness.

TQS operates as an independent voice, committed to transparency and neutrality in its assessments. We work with public-sector agencies seeking to set resilient quantum migration policies and private-sector leaders integrating quantum-safe technologies into mission-critical systems. We also work with industry consortia shaping international standards and collaborative innovation.

https://thequantumspace.org