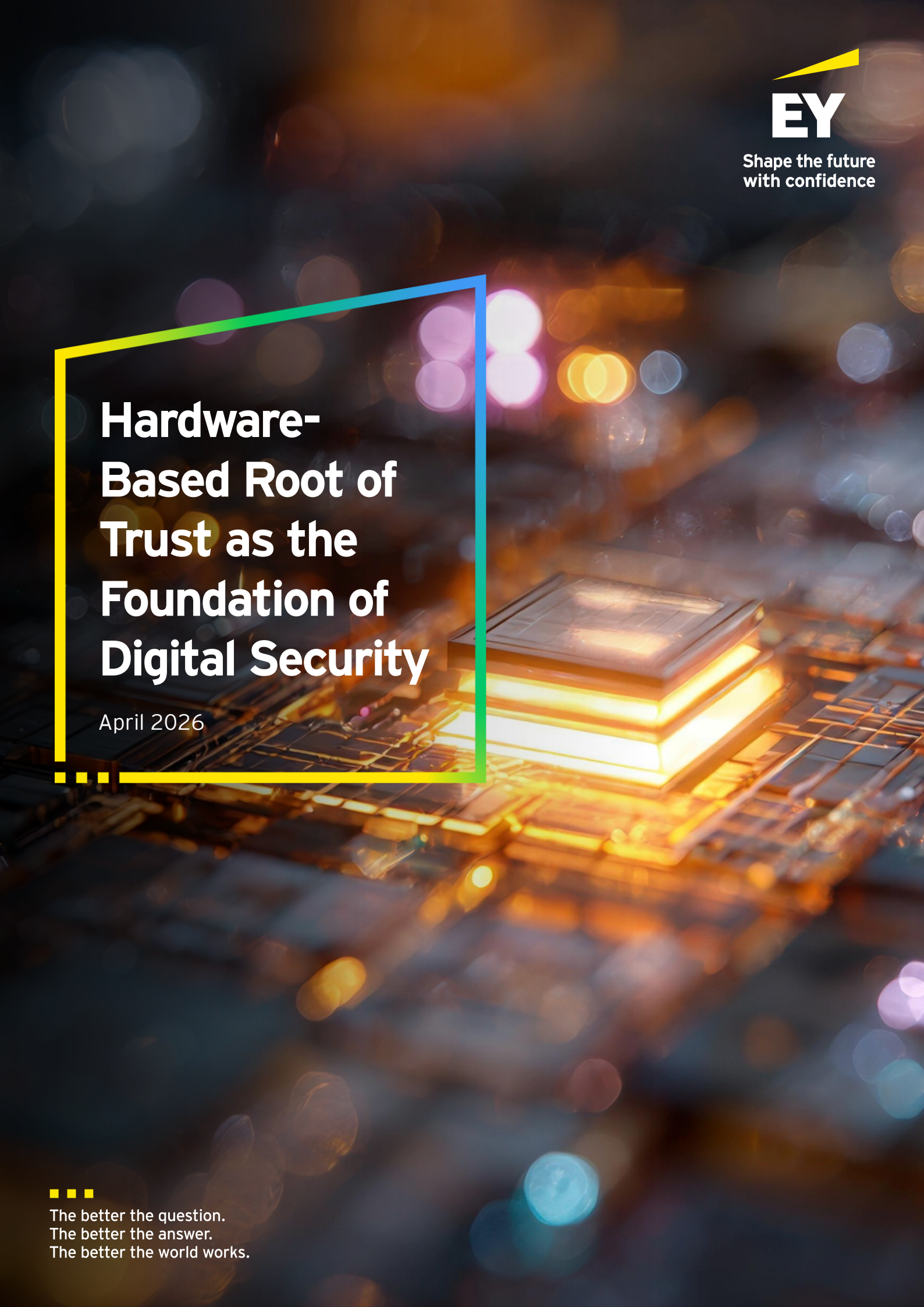

Shape the future with confidence

Hardware-Based Root of Trust as the Foundation of Digital Security

April 2026

The better the question.
The better the answer.
The better the world works.

HBRT anchors security functions in the chip and enables measured system boots, unique identities, attestation and secure updates.

- **Hardware-based roots of trust anchor central security functions directly in the chip and thus ensure a trustworthy IT architecture.**
- **They secure system boot, keys and device identity and provide verifiable proof of integrity throughout the entire lifecycle.**
- **In this way, they strengthen cyber resilience, facilitate compliance and prepare systems for post-quantum-resistant cryptography.**

Cyberattacks, regulatory pressure and quantum computing are putting pressure on classic, purely software-based security mechanisms. Organizations need a trusted function directly embedded in the chip that secures identity, integrity and cryptography throughout the entire lifecycle of a device. Hardware-based roots of trust (HBRTs) create precisely this foundation. They embed core security functions in the hardware in a way that cannot be altered, including cryptographically secured boots, key protection, device identity, remote attestation and protected firmware updates. HBRTs will thus become central building blocks of trusted computing, Zero-Trust architecture and protected data processing (confidential computing), regardless of whether workloads are run in the vehicle, in the cloud, in the industrial network or on IoT devices.

What makes a Hardware-based Root of Trust?

A root of trust (RoT) is the smallest and most protected system component that serves as a reliable starting point for trust and security functions. In the hardware version, it is anchored directly in the silicon, safe from manipulation and independent of the rest of the system architecture.

Typical functions include the following:

- Secure Boot: cryptographic verification of each firmware stage before it boots
- Cryptographic Key Protection: secure generation and storage of keys in the chip
- Zero-Trust Device Identity: immutable, hardware-anchored device identity
- Remote Attestation: verifiable transmission of the current security status of a device to external testing authorities
- Firmware Protection: approval exclusively of authorized updates, including rollback protection

In contrast to purely software-based approaches, this creates a physical foundation of trust, even if the operating system or applications are compromised. Technologies such as the Trusted Platform Module (TPM) or modern security architectures directly in the processor are already implementing this principle in practice.

> HBRTs anchor central security functions in the hardware in a way that cannot be altered.

Why HBRTs are now becoming strategically important: Regulation, compliance and post-quantum readiness

EU regulations such as the Cyber Resilience Act, the NIS2 Directive or the European Union Common Criteria-based Cybersecurity Certification (EUCC) require verifiable security and resilient update processes. HBRTs provide the technical foundation for this and deliver verifiable proof of integrity, even in regulated sectors such as automotive or industry.

Quantum computers will make today's encryption methods vulnerable in the future. With the standardization of post-quantum-resistant algorithms (FIPS 203–205), the transition to post-quantum cryptography (PQC) will begin. HBRTs support this change through crypto-agile architectures that can integrate new algorithms through secure updates – and without costly hardware redesigns.

Technology trends: Openness, Zero-Trust, and Confidential Computing

The HBRT landscape is evolving from proprietary modules to open, auditable platforms. Initiatives such as OpenTitan or Caliptra rely on transparent hardware designs and thus strengthen supply chain security as well as certifiability. Physical Unclonable Functions (PUFs) complement these approaches with physically non-clonable device identities.

In modern Zero-Trust architectures, HBRTs provide the foundation for continuous integrity checks and identity-based access control. In cloud environments, Trusted Execution Environments (TEEs) extend this principle as isolated and specially protected processor areas. Technologies such as Intel SGX, AMD SEV or Arm TrustZone protect workloads even in multi-tenant environments.

Industry focus: from vehicle to factory

Whether cloud, edge, IoT or vehicle: In a Zero-Trust architecture, no system can be trusted across the board. Security functions embedded in the hardware are the foundation of trust, regardless of location or software environment.

- Automotive: ECUs require hardware-based Secure Boot and Attestation to securely implement over-the-air software updates and meet regulatory requirements.
- IoT and industrial equipment (OT): Networked sensors, machines and controllers often have limited resources and long runtimes. HBRTs ensure a unique, non-tamperable device identity, check the integrity of the firmware at startup, and enable secure updates over many years.
- Cloud and data center: Attestations are integrated into orchestration processes to automatically establish trust in devices and workloads.

Challenges – and how they are dealt with

HBRT implementations are complex:

- Verification of modern system-on-chip architectures
- Securing global supply chains
- Certification effort (e.g. Common Criteria, FIPS 140-3)
- Protection against physical attacks such as differential power analysis or fault injection

Dr. Srdan Dzombeta
Partner Consulting
EY Consulting GmbH, Germany

Srdan.Dzombeta@de.ey.com

Dr. Samim Ahmadi
Senior Manager Consulting
EY Consulting GmbH, Germany

samim.ahmadi@de.ey.com

Michael Aulhorn
Senior Manager Consulting
EY Consulting GmbH, Germany

Michael.Aulhorn@de.ey.com

Standardization, interoperable certifications and reusable assurance artifacts are increasingly providing a remedy here. In the European standardization body ETSI TC CYBER, requirements for HBRT implementations are standardized in the technical specification ETSI TS 104 875.

What companies should do now

1. Strategically anchor HBRTs and establish them as an integral part of the long-term IT and security architecture.
2. Consider regulatory requirements at an early stage and integrate integrity certificates and secure update mechanisms right from the beginning.
3. Pay attention to crypto-agility and start thinking about the capacity for post-quantum-resistant cryptography today.
4. Establish attestation in a binding manner, especially in cloud, edge and IoT environments.
5. Opt for transparent and auditable solutions to strengthen supply chains and support certifiability.

HBRT as the foundation of digital resilience

Hardware-based root of trust is no longer a niche topic for chip developers. It is becoming a key enabler for cyber resilience, regulatory compliance, trusted supply chains and digital sovereignty.

Anyone who invests in hardware-anchored trust models today lays the technological foundation for secure and future-proof digital business models in the cloud, in the vehicle or in the factory. And this will continue far beyond the coming decade.

Conclusion

Hardware-based roots of trust anchor central security functions directly in the chip and thus create a tamper-resistant foundation of trust for digital systems. Among other things, they enable secure system boot, protected key management, unique device identities, integrity certificates and secured updates. This makes them an important component of modern security architectures in the cloud, IoT, industry and vehicles. At the same time, they help companies meet new regulatory requirements and facilitate the transition to post-quantum-resistant cryptography through crypto-agile hardware designs. HBRTs thus strengthen cyber resilience, trustworthiness of digital infrastructures and future-proofing.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

XXXXX-XXX
ED None

ey.com