NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

AUGUST 2022 | #34

The VAULT

NFT & NFC, ID & TOKENS

From the Metaverse to our Universe

FEATURED ARTICLE

A New Era in Customer Communications – Brands, Fashion and Art now talk NFT
AdvanIDe

ALSO IN THIS ISSUE

ArtyApes
Physical art on chain

Atos BDS Cybersecurity Products
Cybercriminals conquer the Metaverse – secure identities can stop them

Wibu-Systems
Building links for a digitally secure and sovereign value chain in electronics

Mühlbauer Group
Flow instead of falter: Seamless travel made easy

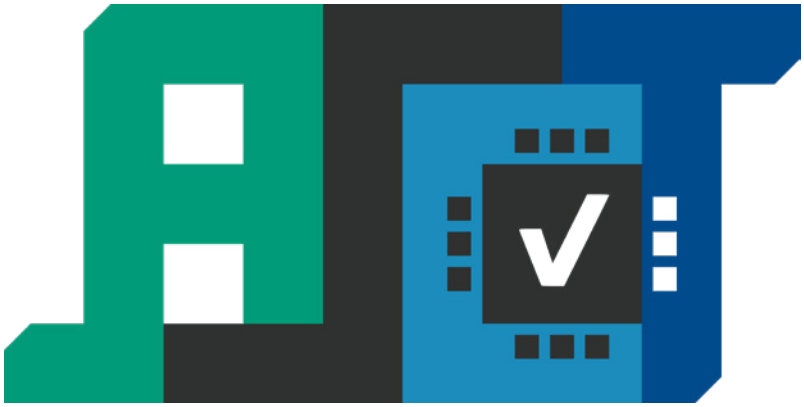
AUSTRIACARD
Securing the future: The next generation chip Operating System for eID applications

TrustSEC
TrustSEC's journey to secure identities

Building LINKS for a *Digitally* SECURE and SOVEREIGN Value CHAIN in *Electronics*

By Ralf Fust, Wibu-Systems

VE-ASCOT Consortium Partner representatives seen here from; Infineon AG, Siemens AG, Wibu-Systems AG, Universität Bielefeld, Fraunhofer SIT and Kastel Security Research Labs at the Karlsruhe Institute of Technology. Not present, Schölly Fiberoptic GmbH, Revisionone Engineering GmbH



☐ Digital identities made unique and tamper-proof with secure hardware elements

Making complex electronic systems is a challenging business at the best of times, but given today's strained supply situation, it seems to have turned into a game of whack-a-mole with a new problem turning up every time an issue has been resolved. Established supply chains always appear to be one step away from snapping. The job of getting the necessary electronic components looks to have turned from sourcing to outright scrounging. This is a time for flexibility, but flexibility comes at a cost, as every alternative choice or replacement component might bring quality or reliability issues. New suppliers might also become new threats to the integrity of one's products. This could happen by chance, as the new component's features or functions might bring new vulnerabilities, but it could also happen intentionally, as there is always a chance of falling prey to product pirates or counterfeiters.

All of these problems are particularly acute at the moment. But they are factors that should always be considered when it comes to developing or producing electronic systems.

Critical infrastructures and systems, e.g. in medical technology, demand particular trustworthiness, as people's health and wellbeing may be at stake. But even less immediately critical scenarios, like common industrial applications, rely on trustworthy electronics and sound and properly authenticated sensor systems.

The VE-ASCOT project was set up to resolve these challenges by means of a unique digital identity (DID) for electronic systems. These DIDs need to be created and be ready to grow and evolve securely over the entire lifecycle of a component or system. How can this be done? With cryptographic means to establish the necessary level of trustworthiness and integrity.

The DID proposed by the project is formed of a set of data points, called records, that are created in a chronological sequence aligned with the product lifecycle to create a cryptographic blockchain. The term found for these cryptographically secured and interlinked records is "Chain of Trust" (CoT).

Anchors of trust: The first link in the chain

Any CoT starts with a cryptographic anchor of trust, formed by a secret asymmetric key and coupled certificates, whose integrity can always be checked. The CoT should be kept in a specifically hardened hardware secure element, a chip protected against attacks. With its serial number and additional data hashed and signed, this original certificate represents the first record in the CoT, making it the principal element of the eventual DID.

All later steps, from the creation to commissioning, operation, and maintenance of the system, can be integrated as records in the CoT. In logistics, customs or certification records could be formed in a similar way, which could facilitate trade. Not all of this data needs to be part of the records in the CoT; it is even flexible enough to include a unique reference to an external data set and put a hash value instead into the record.

A signature keeps every record cryptographically secure, using a structured PKI that includes e.g. the producer, machine certificates or operator certificates. A certificate structure like this pays back immediately in terms of the benefits and trustworthiness of the CoT. A debate could be held – elsewhere – about the type and size of manufacturers' associations and the required PKI.

Over time, the CoT in the secure element grows, with each record creating an increasingly detailed identity of the electronic system. With the CoT and the producer certificates stored in the secure element, the CoT can be cryptographically verified at any point in time, allowing for local and independent checks of the systems' trustworthiness.

Copies of the CoT could also be stored in the cloud, which could form a type of digital twin of the electronic system that could carry additional information about the system's maintenance status or its firmware and software versions. This would make it possible to manage e.g. the rollout of updates for entire industrial installations from the cloud.

VE-ASCOT focuses on CoTs stored locally in secure elements, which should include specific traits, still to be determined, of the hardware. These could be stored as separate records and serve to check the integrity and authenticity of a component during bootup or active operation.

One property that has been proposed for this purpose would be a so-called "Physical Unclonable Function" (PUF). The project VE-ASCOT is looking at a related type of technology, specifically "Physically Obfuscated Keys" (POKs) developed and evaluated by Infineon. During commissioning, a POK would add an auxiliary, silicon-based source of entropy to get a unique fingerprint, which is stored as a record within the CoT.

Other physical traits of an electronic system or specific components are also checked in the research project for their suitability as additional properties for a unique and identifiable DID. Using such physical traits usually needs some tolerance, which could be provided by mathematical methods or AI-supported techniques.

New and secure identifier data, courtesy of CodeMeter

The chosen traits form a fingerprint that, in turn, becomes a record in the secure element's CoT. To store that CoT, Wibu-Systems is developing a novel Universal Data (UvD) structure for its CodeMeter license management technology on proprietary secure elements. This new format should allow flexibility for the amount of data to be stored and facilitate additional signing and validation processes, even with longer key lengths up to RSA 4096 and ECC 521.

Wibu-Systems provides the secure elements as packaged chips or USB and memory card devices (CmDongles) that can store the CoT records into CodeMeter UvD entries with a signed hash of the data separately or as already linked lists. Similarly, a list of certificates containing public keys for signature verification can be stored and used to validate the CoT records. The CmDongles used for signing the records even come with their internal key generation capabilities. For additional security, the channel through which the signed data or certificates are passed between the secure element and the machine or operator is hardened with point-to-point encryption.

The illustration (page 20-21) shows a sample CoT that can grow and evolve over the lifecycle of the electronic component it belongs to. At a minimum, the records making up the chain include the following data and information:

- Record version
- Sequential number
- Binding to the previous record
- ID of the certificate key used for signing
- Process description
- Results / Data
- Signature of the hashed record data

The producers' certificates also need to be stored in a parallel certificate list.

With all of this data at hand, the CoT can be read and cryptographically checked at any time using the CodeMeter UvD entries. This guarantees the integrity and authenticity of the data and, by extension, of the actual hardware. As all of the data is kept locally, this check can be done anytime and anywhere, without need for network or cloud access.

Security built into the boot process

Another important building block in the VE-ASCOT project's security architecture is an automated internal check of the CoT upon power-on, acting as a gatekeeper before the electronic system is allowed to start booting. For this use case, the secure element will be in charge of a multi-level boot process and checks every element of the CoT before the system gets to boot up the target system and launch applications.

The proposed process can be executed on the processor's pre-boot level. The CoT is read and cryptographically validated on the secure element. When using Trusted-Boot records, e.g. POKs, a challenge is retrieved by the secure element and passed onto the POK, where it is processed and the necessary response fed back to the secure element.

This simple, but smart process, allows different physical traits to be tested. Alternatively, the secure element itself can be authenticated in the pre-boot phase. To do so, the certificate of the secure element's serial key, acting as the basic anchor of trust, is checked in a two-step process: First, the signature of the relevant record #1 in the CoT gets checked against the PKI; next, the availability of the corresponding private key is tested by challenge-response.

The VE-ASCOT project also includes the integration of a TPM in the electronic component. The thinking behind this is that hardware traits can be integrated in a "measured boot" process and the resulting data structures fed into a new profile for such hardware properties, to be standardized by the Trusted Computing Group.

Both approaches to hardware fingerprinting are valid avenues. While a TPM tends to play a more passive role and acts as a cryptographic co-processor that measures data which allows a local or remote instance to assess the integrity of the electronic system, a secure element can more actively influence the boot process.

The Wibu-Systems' secure element is used in the project to demonstrate a range of ways to interact with the hardware or software:

- Hardware system reset: The secure element could force a hardware system reset to the electronic system and the main processor whenever a CoT cannot prove its integrity or parts of a fingerprint cannot be validated.
- Resource restrictions: Cryptographic keys that would be needed e.g. to decode the final boot image after the fingerprint check, can be blocked if that check fails. When using CodeMeter hardware with flash memory, this could also mean that the encrypted partition cannot be decrypted.
- License locks: When using the CodeMeter licensing system from Wibu-Systems, certain protected applications could be blocked with a "disabled" entry in the license if a CoT check fails or a fingerprint turns out to be not trustworthy.

These mechanisms make it possible to check hardware traits in a specially hardened secure element, to verify the results of the check, and to then influence the boot process in response to a positive or negative outcome.

Advanced Security by the Chain Of Trust, as the project's acronymic name spells out, combines hardware-specific properties of an electronic system with cryptographic means to create a unique digital identity that can grow and evolve over the entire lifecycle of a product and stay verifiable and trustworthy at any point in time. ☒

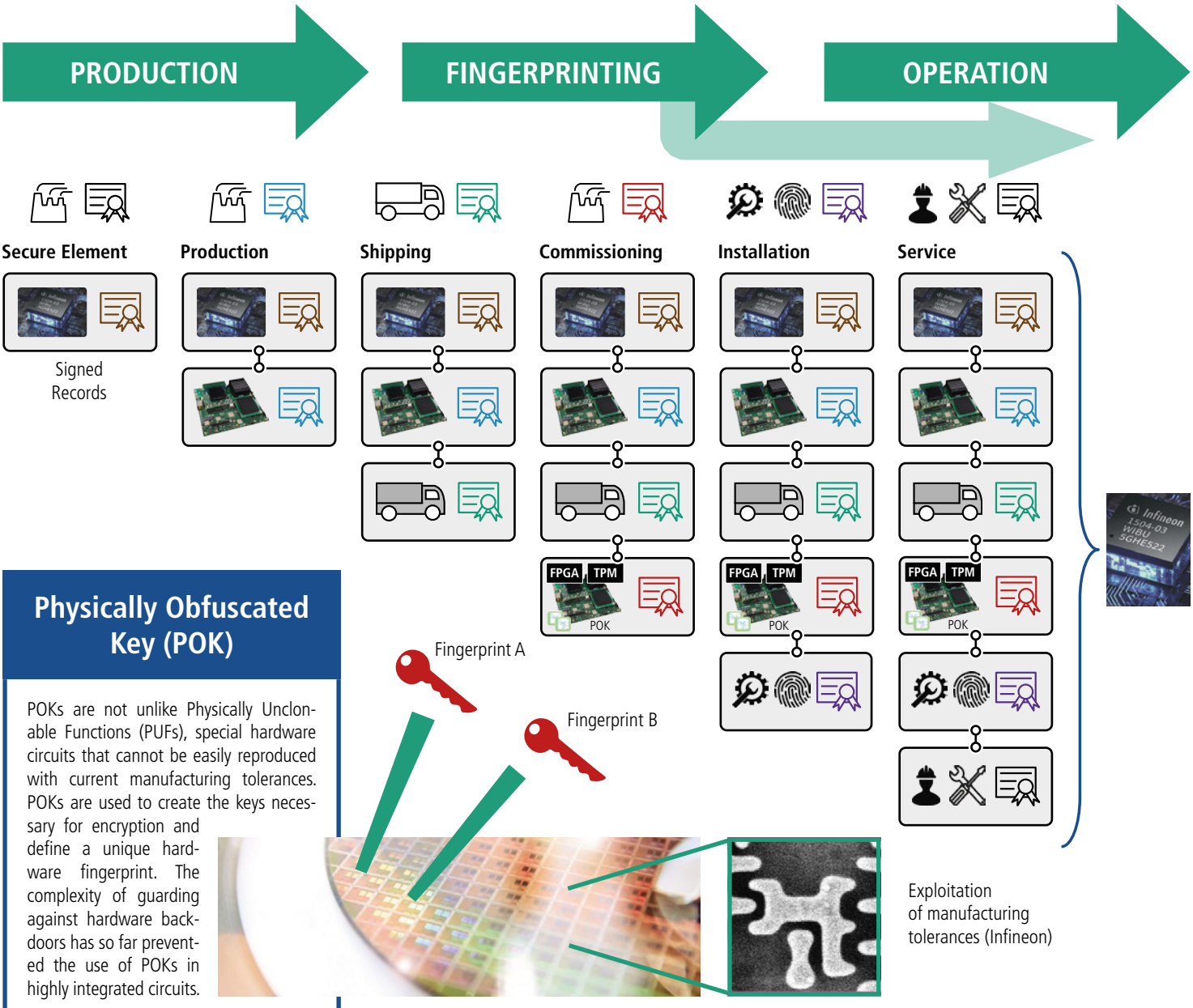
CodeMeter by Wibu-Systems is the company's award-winning family of IT security solutions that monetize the know-how of any software-powered business by safeguarding their digital assets and distributing them via versatile licensing models. Using unbeaten encryption technology and an underlying interoperability approach that embraces all the software, hardware, and cloud elements of CodeMeter's universe, the technology is supporting businesses agnostically across all verticals and is also attracting increasing attention in novel protection scenarios, including its integration in trustworthy computing schemes.

VE-ASCOT:
Advanced Security for Chains of Trust

Goals and Chain of Trust (CoT)

In the distributed manufacturing of electronic systems, trust between the actors involved is of paramount importance for producing high-quality components. This means trust in the quality of work itself and trust in the correct functioning and integrity of the entire electronic unit. The secret to establish such trust in a network of makers and producers lies in mirroring the production and commissioning process in a cryptographically secure Chain of Trust (CoT). It works by recording individual processing steps and specific traits of the hardware components as a shared, protected dataset on the component itself to be read out and cryptographically checked at any time during production or use.

Production Records within the Chain of Trust



Physically Obfuscated Key (POK)

POKs are not unlike Physically Unclonable Functions (PUFs), special hardware circuits that cannot be easily reproduced with current manufacturing tolerances. POKs are used to create the keys necessary for encryption and define a unique hardware fingerprint. The complexity of guarding against hardware backdoors has so far prevented the use of POKs in highly integrated circuits.

Contact
Ralf Fust
ralf.fust@wibu.com
www.ascot-trust.info

WIBU SYSTEMS

UNIVERSITÄT BIELEFELD

KIT Karlsruher Institut für Technologie

Infineon

Funding Code: 16ME0270K

Velektronik

Supported by the
Federal Ministry of Education and Research

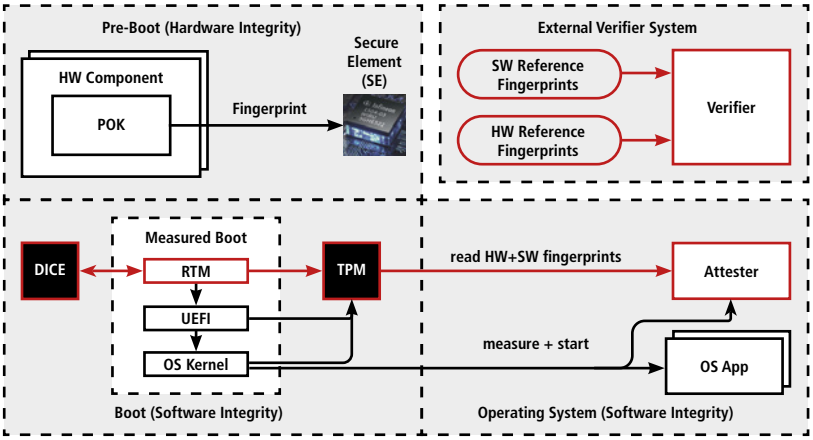
Industrial Use Case

IoT devices are used for the state monitoring of industrial facilities like the power or transport infrastructure for preventive maintenance or the reliable supply of spare parts. Alongside secure means for data transmission between these devices and the cloud, there needs to be trust in the hardware and software alike. ASCOT demonstrates this with traction transformers used in the rail sector.

Medical Use Case

SCHÖLLY is an international medical technology leader in the field of endoscopic imaging. With the company's experience in producing certified electronics, Schölly contributes to the VE-ASCOT endeavor with the development of a demonstration unit of a medical imaging device.

Trusted Computing & Integrity Verification

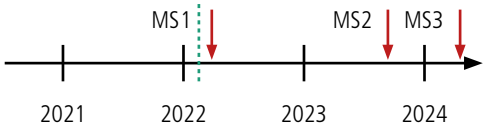


Hardware and software integrity are inextricably linked with the Trusted Platform Module (TPM) 2.0, using the TPM ecosystem (Trusted Boot, TPM 2.0 Software Stack (TSS2), and Remote Attestation). The Device Identifier Composition Engine (DICE) ensures the peripheral components' integrity on the board. Processes, protocols, and data structures are set to be standardized by the Trusted Computing Group (TCG) and the IETF.

VE-ASCOT at a Glance

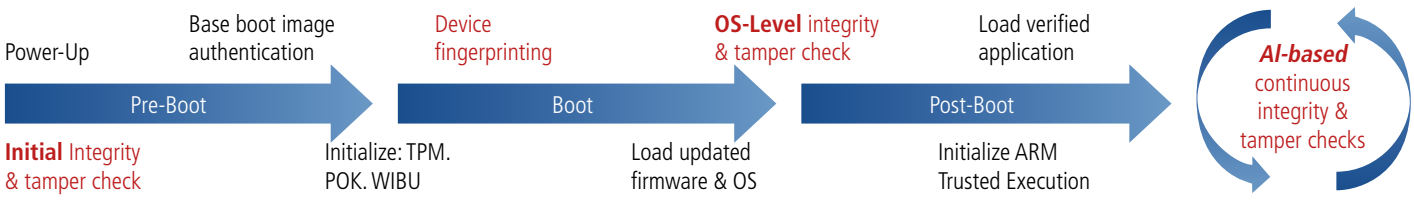
Coordinator:	WIBU-SYSTEMS AG
Contact:	Ralf Fust
Project volume:	€4.71 million
Project timeframe:	1 Mar 2021 to 29 Feb 2024
Project partner:	See logos below
Technology Readiness Level:	
Verified Boot:	3 to 5
Demonstrators:	2 to 5
POK	3 to 4
COT	2 to 4
TPM	4 to 5
AI	2 to 4

Project Status



Secure Boot & Fingerprinting

The secure boot process based on FPGA guarantees that only the authenticated hardware and software is allowed to run. The properties of the hardware components and the environment and operating parameters form a unique fingerprint of the system. By continually checking these traits during runtime also with AI support, any changes and tampering by third parties will be spotted reliably.



SIEMENS Ingenuity for life

Fraunhofer SIT

Schölly EXCELLENCE INSIDE (Associate partner)

RevOne RevisionOne Engineering GmbH (RevOne (Subcontractor))

WIBU SYSTEMS

Cybersecurity: Addressing the Global Challenge

A beacon for IT security innovations

A business enabler for all software and device makers

A guardian for all digital assets

Wibu-Systems and the House of IT Security support the local and international community for a more trustworthy, sustainable, and effective digital future.

Are you looking for thought leaders and inspiring partners to engage with?

Become a member of the IT Security Club

Are you looking for a rewarding career in IT security?

Send your application to Wibu-Systems

+49 721 931720
sales@wibu.com
www.wibu.com

SECURITY
LICENSING
PERFECTION IN PROTECTION