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

cryptovision

Your last mistake is the best teacher

Applet Suite certified on
NXP
Infineon
Veridos

We offer more control and no regrets for your next eID project

We all have regrets sometimes. Choose your party wisely and you won't wake up with a hangover. Working with cryptovision for your next eID project means that you will stay in control. Your customers will appreciate the flexibility and ingenuity of our solutions.
Don't make the same mistake twice – get in touch with us.

Find out more on cryptovision.com/eID

- Java Card™ Applet Suite
- Personalization Middleware
- Certificate Management
- Public Key Infrastructures

Atos

Contents

Securing the future: The next generation chip Operating System for eID applications 4
Achim-Florian Gornik, AUSTRIACARD

A New Era in Customer Communications – Brands, Fashion and Art now talk NFT 8
Kay Plaumann, AdvanIDe

Physical art on chain 14
Steve Atkins, Silicon Trust

Building links for a digitally secure and sovereign value chain in electronics 16
Ralf Fust, Wibu-Systems

Cybercriminals conquer the Metaverse – secure identities can stop them 22
Adam Ross and Klaus Schmeh, Atos BDS Cybersecurity Products

TrustSEC's journey to secure identities 26
Manal Ashraf, TrustSEC

Flow instead of falter: Seamless travel made easy 30
Katharina Schuldt, Mühlbauer Group

Silicon Trust Directory 2022 34

Imprint

THE VAULT ISSUE 34
Published by Krowne Communications GmbH, Berlin.
PUBLISHER: Krowne Communications GmbH, Steve Atkins, Kurfürstendamm 194, 10707 Berlin
EDITOR-IN-CHIEF: Steve Atkins
ART DIRECTOR: Lana Petersen
PARTNER DIRECTOR: Yvonne Runge
EDITORIAL CONTRIBUTIONS: Achim-Florian Gornik, Kay Plaumann, Lambert Lang, Ralf Fust, Adam Ross, Klaus Schmeh, Katharina Schuldt, Manal Ashraf
PHOTOS: ISTOCKPHOTO, PIXELBAY, ARTSY APES, STEBOART, WIBU-SYSTEMS, TRUSTSEC, MÜHLBAUER KROWNE COMMUNICATIONS ,
EDITION: August 2022.

SECURING the *future*: The *next* generation Chip *Operating* SYSTEM for e-ID *applications*

By Achim-Florian Gornik, AUSTRIACARD

□ There is no doubt that secure identification has become a matter of course at a global scale. Increased security requirements for electronic travel documents (for instance EAC and PACE) on the one hand and evolution of the regulatory framework, such as eIDAS in the EU on the other, have played a key role in this transformation.

In the past, primarily optical security features have been used as a guarantor for the document's counterfeit protection and trustworthiness, whereas today the chip on which the document holder's data is stored, becomes even more essential to the document's overall security. The centrepiece of every machine-readable e-ID document is the operating system, since it forms the backbone of the actual secure identification and authentication process and at the same time enables the combination of various applications.

By rolling out its next generation Chip Operating System ACOS-ID v2.0, AUSTRIACARD has responded to these market needs for enhanced security in identification, by creating a holistic solution that is able to cover most e-ID use cases. ACOS-ID v2.0 has been especially developed for passports,

> *“By rolling out its next generation Chip Operating System ACOS-ID v2.0, AUSTRIACARD has responded to these market needs for enhanced security in identification by creating a holistic solution that is able to cover most e-ID use cases.*

identity cards and residence permits, as well as driver's licenses and eIDAS-compliant signature cards, with state of the art new technologies and elevated security certification confirming the highest security level according to Common Criteria for applications at a global level.

ACOS-ID implements functionality based on international standards such as ICAO 9303, EAC v1&v2, PACE v1&v2, eSign, ISO 18013 (EU electronic Driving License) and benefits from its 40 years of experience in the highly complex and sensitive field of payment, covering the entire contact only, dual interface and contactless application scenarios for online and offline data authentication.

ACOS-ID was developed to ensure maximum flexibility for the customers, hence AUSTRIACARD is able to provide tailor-made solutions in relation to the chip’s memory size, operating system and applications that can be added or developed: Therefore, ACOS-ID is a distinctively resource efficient OS with small memory footprint, through which the customer obtains a fully sustainable solution for long-lifetime ID/government projects, without compromising performance or usability.

This unique combination makes it possible to create a secure and globally recognized digital solution with an optimum cost efficiency and availability in different memory sizes and various delivery forms or licensing options like wafer, modules on reel or sheets/transponder.

No matter what the final product looks like, whether a passport booklet, a card or simply an inlay, AUSTRIACARD will be glad to be once more the partner of choice.

For further information please contact our ID team at ID.contact@austriacard.com ☒

AC
AC IDENTITY CARD
AUSTRIACARD ID - DIGITAL SECURITY

A *New* ERA in Customer *Communication* – Brands, FASHION and *Art* NOW talk NFT.

By Kay Plaumann, AdvanIDe

□ You've likely heard recently how the metaverse will usher in a new era of digital connectivity, virtual reality (VR) experiences and e-commerce. Tech companies, Brands and Banks are betting big on it: Microsoft's massive US$68.7 billion acquisition of game developing giant Activision Blizzard reflected the company's desire to bolster its position in the interactive entertainment space. Prior to this, Facebook's parent company rebranded itself as Meta — a key pillar of founder Mark Zuckerberg's grand ambitions to reimagine the social media platform as "a metaverse company, building the future of social connection." In fact, the global "metaverse" first appeared in 1982, before everyone was as comfortable, or even aware of, the Internet (Web 1.0). Today, however, big money, backed by even bigger companies are intent on making the metaverse (Web 3.0) as acceptable and utilized as the internet we know today. In this emerging Web 3.0 iteration, users consume, create, and own content; the networks (and the money exchanged) are decentralized, with blockchain technology replacing centralized intermediaries and providing the trust that enables both consumption and exchange. In fact, The global metaverse market size is projected to grow from USD 61.8 billion in 2022 to USD 426.9 billion by 2027, at a Compound Annual Growth Rate (CAGR) of 47.2% during the forecast period.

To see the metaverse in action, we can look at popular massively multiplayer virtual reality games such as Rec Room or Horizon Worlds, where participants use avatars to interact with each other and manipulate their environment. But the wider applications beyond gaming are staggering. Musicians and entertainment labels are experimenting with hosting concerts in the metaverse. Fashion brands are releasing on-line collections for virtual reality avatars. The sports industry is following suit, with franchises like Manchester City building virtual stadiums so fans can watch games and, presumably, purchase virtual merchandise. Artists are developing online art collections and of course, allowing for the purchase and trading of Non-Fungible Tokens (NFTs) connected to such projects and art items.

But before we talk about the metaverse and the role that NFTs play there, it is vital that we briefly touch upon where the metaverse lies within the web iterations of 1, 2 and 3 and what we mean when we talk about Web 1.0, 2.0 and 3.0.

Basically, this first version of the Web consisted of a few people creating web pages and content and web pages for a large group of readers, allowing them to access facts, information, and content from the sources. It was designed to help people better find information. This web version was dedicated to users searching for data. This web version is sometimes called “the read-only Web” because it lacks the necessary forms, visuals, controls, and interactivity we enjoy on today’s Internet. People use the term “Web 1.0” to describe the earliest form of the Internet.

If Web 1.0 was made up of a small number of people generating content for a larger audience, then Web 2.0 is many people creating even more content for a growing audience. Web 1.0 focused on reading; Web 2.0 focused on participating and contributing. This Internet form emphasizes User-Generated Content (UGC), ease of use, interactivity, and improved compatibility with other systems and devices. Web 2.0 is all about the end user's experience. Consequently, this Web form was responsible for creating communities, collaborations, dialogue, and social media. As a result, Web 2.0 is considered the primary form of web interaction for most of today's users. If Web 1.0 was called “the read-only Web,” Web 2.0 is known as “the participative social Web.”

And finally, we come to the latest Web iteration. Although there are elements of Web 3.0 currently available today, it still has a way to go before it reaches full realization. Web 3.0, which is also referred to as Web3, is built on a foundation consisting of the core ideas of decentralization, openness, and more excellent user utility. Web 1.0 is the "read-only Web," Web 2.0 is the "participative social Web," and Web 3.0 is the "read, write, execute Web."

> *“Web 3.0 ultimately lets users interact, exchange information, and securely conduct financial transactions without a centralized authority or coordinator. As a result, each user becomes a content owner instead of just a content user.*

This web interaction and utilization stage moves users away from centralized platforms like Meta, Google, or Twitter and towards decentralized, nearly anonymous platforms. Web 3.0 ultimately lets users interact, exchange information, and securely conduct financial transactions without a centralized authority or coordinator. As a result, each user becomes a content owner instead of just a content user. Web 3.0 isn't entirely in place yet, however, we are already seeing elements of Web 3.0 moving into our Internet experiences, such as NFTs, blockchain, distributed ledgers, and the metaverse as a concept.

Blockchains are a vital part of Web 3.0 – some would also call them the ‘backbone and foundation of Web 3.0’. A blockchain is, in the simplest of terms, a time-stamped series of chained records of data that is managed by a cluster of computers not owned by a single entity. Each of these blocks of data (i.e., blocks) is secured and bound to each other using cryptographic principles (i.e., chain). The blockchain network has no central authority – it is the very definition of a democratized system. Since it is a shared ledger, the information in it is open for anyone and everyone to see. Hence, anything that is built on the blockchain is by its very nature transparent and everyone involved is accountable for their actions.

The blockchain is a simple yet ingenious way of passing information from A to B in a fully automated and safe manner. One party to a transaction initiates the process by creating a block. This block is verified by thousands, perhaps millions of computers distributed around the net. This verified block is added to a chain, which is stored across the net, creating not just a unique record, but a unique record with a unique history.

Most of us have heard of blockchain when talking about crypto-currencies, such as Bitcoin. However, if we look beyond fintech services, it can also be used in many other applications such, as logistics, energy supplies, social networks, messaging, gaming, online market-places, storage platforms, voting systems, predictive markets, online shops and brand protection. There is one very important area that blockchain is vital for though – the

development, collection and trading interactions concerning Non-Fungible Tokens (NFTs). These items are what everyone is considering the 'hot ticket' today, and are playing a major role in the growth of Web 3.0's metaverse.

The term "Non-Fungible" means that it is completely unique. "Token" means that it can be transferred on a blockchain. Essentially, NFTs are assets that carry a unique digital identity and can be traded between users on a public blockchain like Ethereum. Common examples of NFTs include artwork, trading cards, comic books, sports collectibles, games and more. Although NFTs tend to be associated with artwork, they actually represent much more. NFTs can actually unlock a lot of things including digital and in-person experiences, etc. It works like this - because NFT ownership can be instantly and easily verified on the blockchain, NFTs can act as proof of ownership. This is helpful in categories like art, where provenance is such an important part of the collectability of a piece. But this provenance, or proof of ownership is even more useful when applying NFTs to things like experiences; for example, you might in the future use an NFT to unlock access to a digital or in-person gallery or event for a specific artist, with the NFT acting as a ticket or pass to grant you access. The possibilities are really endless.

Regardless of whether you are a brand, an institution, an artist or collector, NFTs work in the same way. NFTs empower creators to connect directly with fans and enable new types of exclusive experiences that can be virtual, in-person, or both. NFTs offer further utility over traditional art pieces. NFTs can be traded on online marketplaces or exchanged directly between individuals. NFTs also provide a variety of specific benefits for artists, such as royalties. NFTs can be programmed with royalty features that reward artists for every sale in specific marketplaces, allowing artists to sometimes even be able to get royalties for secondary marketplace sales if their work is resold–this is one of the biggest attractions of NFTs for artists. Additional information related to each NFT can be stored within the NFT's metadata, giving each asset a unique history.

> *“ The issuance of NFTs can blur the lines between the physical and digital worlds and enables individuals and companies from various industries to cater to specific audiences and deliver personalized consumer interactions.*

We are currently seeing many big-name brands moving into the metaverse and offering a digital version of their ‘real-world’ products. Be they sneakers, clothes or even real-estate. The luxury fashion house, Balenciaga, entered the metaverse in late 2021 through a partnership with the video game makers Epic Games. The Fortnite x Balenciaga collab contained in-game limited-edition skins and outfits for avatars in the Fortnite game, which boasts a staggering 350 million users worldwide. The collab also featured an accompanying real-world Fornite x Balenciaga clothing line.

Nike acquired the non-fungible token studio RTFKT in December 2021 as a tool to access the metaverse. RTFKT produces NFT collectibles and memes, most notably digital sneakers, and aims to merge culture and gaming. Their most famous collab was with teenage artist FEWOCiOUS, to sell physical sneakers paired with their digital counterparts. RTFKT managed to sell 600 pairs/NFTs in seven minutes as part of the venture and netted more than $3.1 million.

Other interesting NFT project co-operations include Coca-Cola and Tafi, Gucci (and Hyundai) and Roblox. Other brands also making entry into the metaverse include Nike, Louis Vuitton, Adidas, Wendy’s, Samsung, Burberry, Dolce & Gabbana, Ferrari, Tommy Hilfiger, Vas and Ralph Lauren to name but a few.

The metaverse is ripe with marketing and advertising possibilities. While it is still in its early stages, the community is now more open to experimenting on various projects, which brands, artists, musicians and sports teams can leverage for a successful breakthrough in the digital space – even through the issuing of a digital product that is NFT based. The issuance of NFTs can blur the lines between the physical and digital worlds and enables individuals and companies from various industries to cater to specific audiences and deliver personalized consumer interactions.

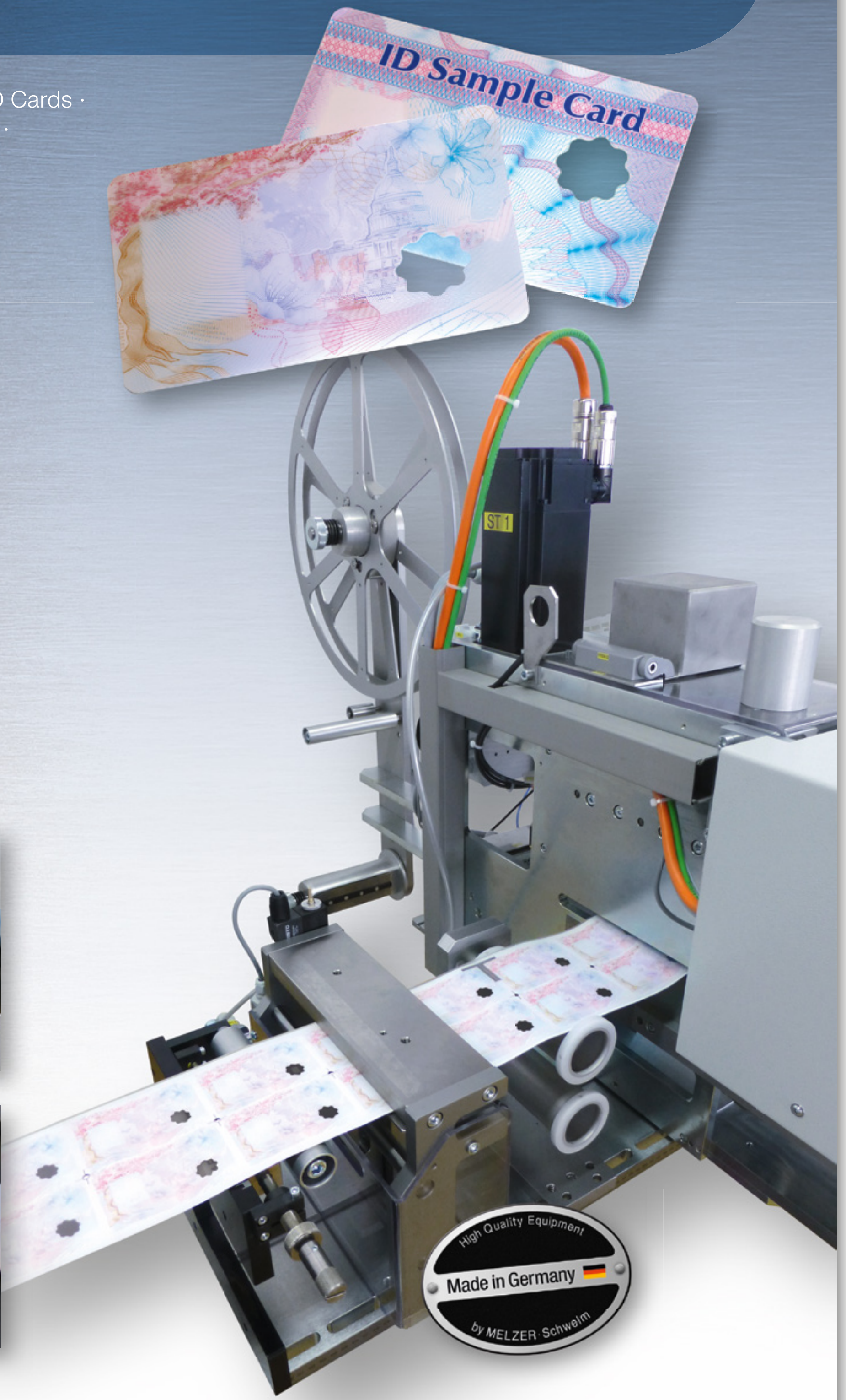
The metaverse may be young and volatile, but this is a chance to pioneer a new era of marketing. The future appears bright for a marketing model based in the digital world. The technology shift into the metaverse has started, and brands continue to find new ways to reach and communicate with Generation Z and beyond. ☒

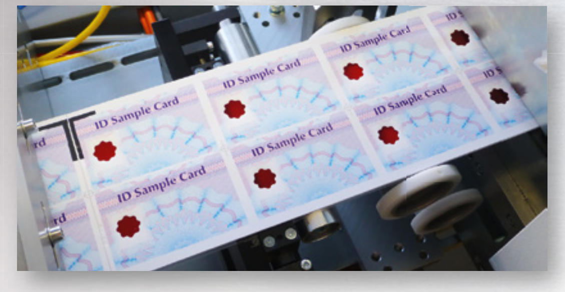
Inline Window Application

IPS

Inline Production System for ID Cards · Data Pages · Driving Licenses · Resident Permit Cards

- ▷ Fully automatic punching and inserting
- ▷ For cards and data pages
- ▷ Zero gap technology
- ▷ Full lamination for utmost durability





ARTSYAPES: Physical *ART* ON Chain

By Steve Atkins, Silicon Trust

> *“We are convinced that the dynamic and diversity of the Ethereum ecosystem is optimal for pushing the boundaries of what NFTs can be.*
>
> *– Lambert Lang, ArtsyApes*

□ ArtsyApes is the first project, realized by SteboArt located in Graz, that brings digital Non-Fungible Tokens (NFTs) on the Ethereum Blockchain, back into the real world for collectors to own, with a super-tribe of 3,777 Apes.

Each NFT consists only of completely handmade elements. The process begins with sketches of single attributes that are translated to canvas to be painted by the Austrian artist and founder of ArtsyApes – Stebo. In the second stage, all hand painted attributes are then photographed in high resolution and turned into digital files so they can be processed into separate layers.

“In the end, the final collection is created using an algorithm that combines the layers into a whole, matching picture. This is how all ArtsyApes are created”, explains ArtsyApes Art Director, Marta Viegas.

However, this is no simple blockchain NFT offering. The ArtsyApes team are bringing these pieces of art back from the blockchain and into the real world. Every NFT owner will have the opportunity to redeem or commission physical art made from their own ArtsyApe.

There is a whole selection of ArtsyApes items available that are split up into three tiers.

Tier 3 is a hand signed art print on recycled paper with a certificate that is free for any token holder that will depict their Ape and its traits in a stylish manner. Tier 2 is a signed high resolution canvas print that will include an ArtsyApes signature Crypto NFC Chip that will be directly linked to the owners’ ArtsyApes NFT, to provide proof of ownership, origin and uniqueness. A quick scan with a smartphone also allows the owner to pull up information about the artwork, making it ideal for showing it off to friends or other interested parties and for gallery spaces. The chips are provided by Infineon Technologies and can be found in the artworks by Stebo’s signature in the bottom right of the piece.

Tier 1 ArtsyApes are fully hand painted 100 cm x 100 cm masterpieces on canvas, painted by Stebo from scratch, coated with epoxy resin and an ArtsyApes staple, 24 Carat gold. The NFC Chip is also included in the artwork.

“What’s worth mentioning is that every physical Tier of an ArtsyApe will only ever be available a limited number of times to create interesting dynamics in the secondary market, with the Tier 1 paintings being a one-and-done deal. So, if a collector claims their NFT as a handmade painting, no one else will ever be able to do it ever again.” Says ArtsyApes Team Lead, Lambert Lang. “We are convinced that the dynamic and diversity of the Ethereum ecosystem is optimal for pushing the boundaries of what NFTs can be.”

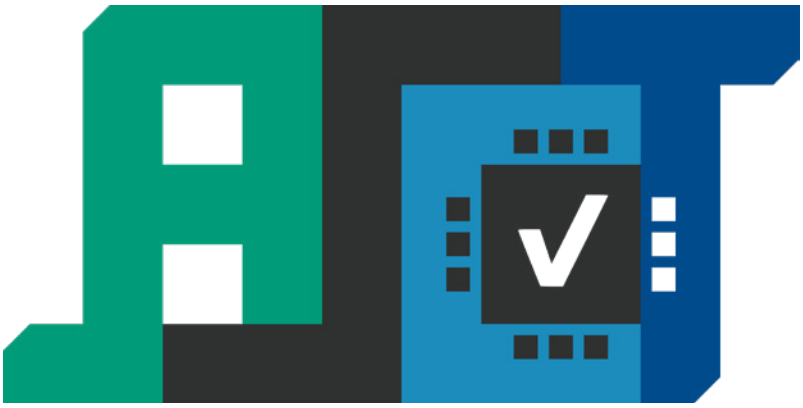
With companies such as Meta creating more urgency and interest in the potential of the Metaverse, expect more assets based on NFTs to be generated in the Metaverse, but have an NFC-protected physical twin in this world too.

Discover more about ArtsyApes at www.artsyapes.com. ☒

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. ☒

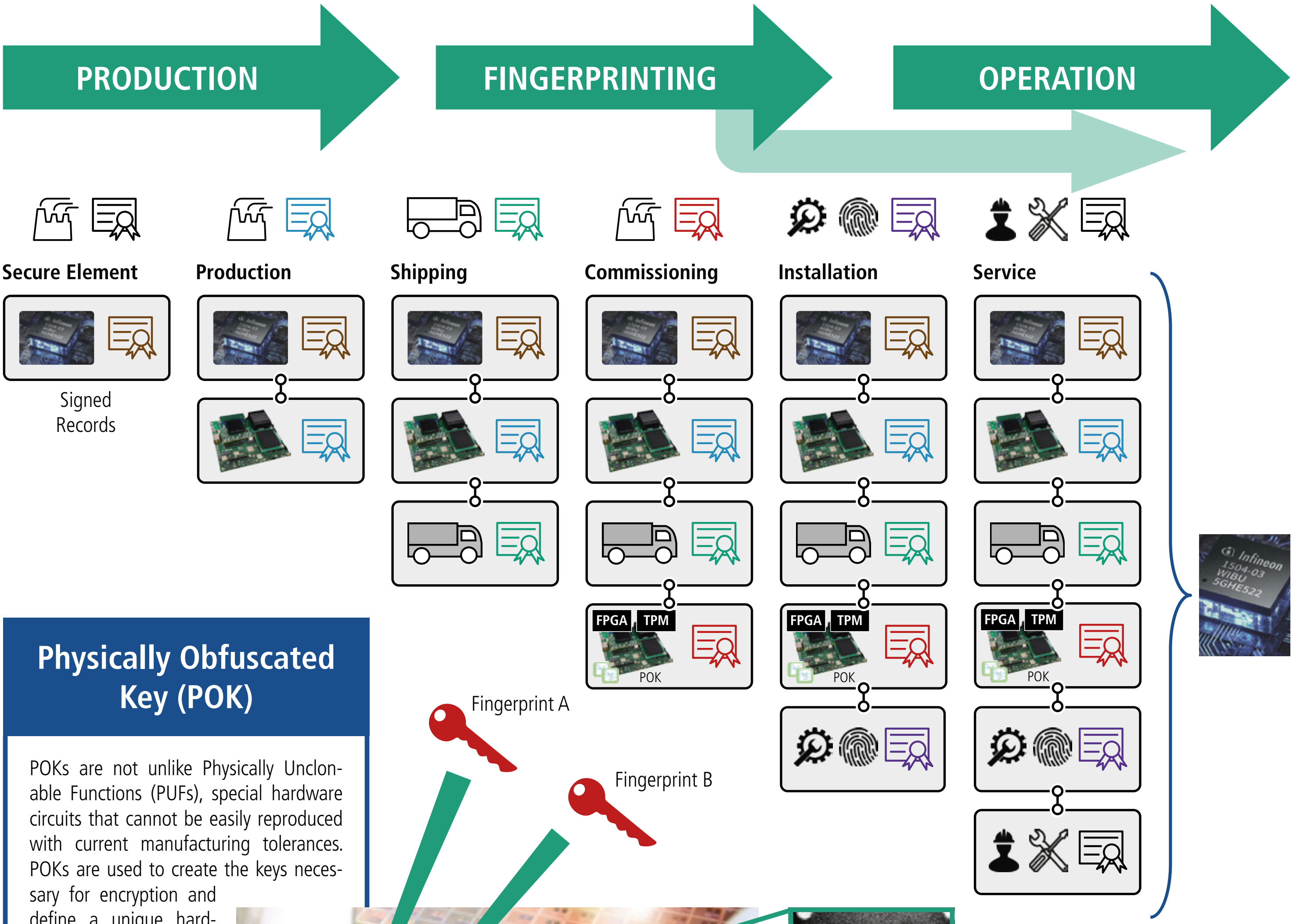
CodeMeter by Wibu-Systems is the company's award-winning family of IT security solutions that monetize the know-how of any software-powered business by safeguarding their digital assets and distributing them via versatile licensing models. Using unbeaten encryption technology and an underlying interoperability 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.

Exploitation of manufacturing tolerances (Infineon)

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

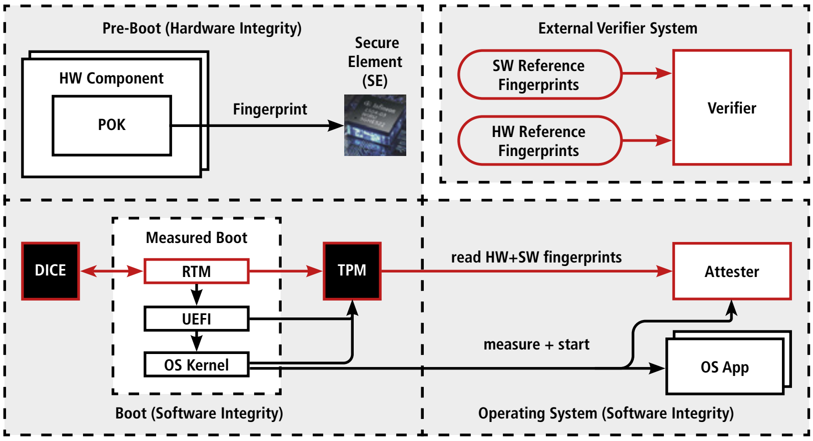
Industrial Use Case

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.

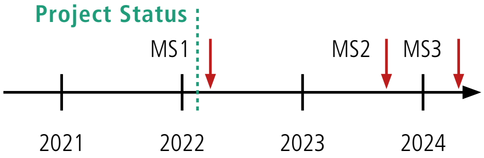
Trusted Computing & Integrity Verification



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.

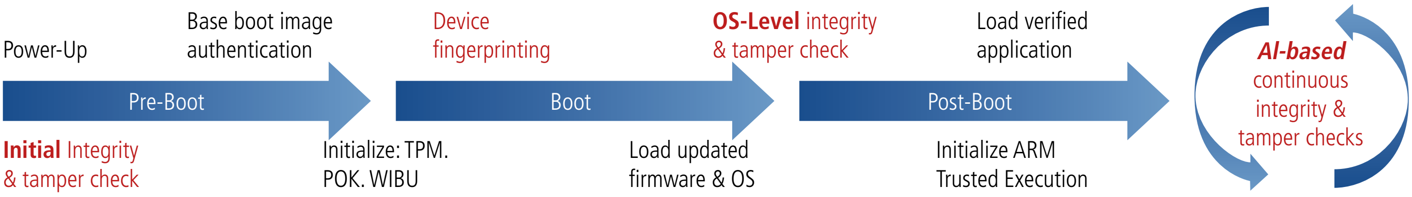
VE-ASCOT at a Glance

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



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.


Power-Up
Base boot image authentication
Device fingerprinting
OS-Level integrity & tamper check
Load verified application
Pre-Boot
Boot
Post-Boot
Initial Integrity & tamper check
Initialize: TPM. POK. WIBU
Load updated firmware & OS
Initialize ARM Trusted Execution
AI-based continuous integrity & tamper checks

SIEMENS Ingenuity for life

Fraunhofer SIT

Schölly EXCELLENCE INSIDE (Associate partner)

Rev One
RevisionOne Engineering GmbH
RevOne (Subcontractor)

Cybercriminals *CONQUER* the *Metaverse* – Secure IDENTITIES can *STOP* them

By Adam Ross and Klaus Schmeh, Atos BDS Cybersecurity Products

The Metaverse is booming. While this attracts gamers, shoppers, and art lovers, it also arouses the interest of individuals from the dark side of the law. Specifically, Non-Fungible Tokens (NFTs) have become attractive targets for cybercriminals. Some of these tokens have high values, while their owners are lacking cybersecurity experience. To protect Metaverse users from attacks of this kind, appropriate identity and authentication technology must be established. This development is still in its infancy.

□ The American actor Seth Green recently faced a serious problem. Green, who played Dr. Evil's son in the Austin Powers movie series, was planning to develop a TV show "White House Tavern" around a number of NFTs he had purchased for a sum of hundreds of thousands of dollars. However, these plans were derailed when a hacker stole the key NFTs from him via using a phishing technique and then sold them to clueless new owners. The theft included Bored Ape #8398 of the Bored Ape Yacht Club from Yuga Labs. This theft represented a significant setback for Green, as this NFT was the main character of the animated series in development; giving rise to the question if Green still had the rights to use this NFT art as the basis for his TV project.

Many were hoping Green would go to court and get a ruling over whether or not he was still the owner of the tokens, as they represented stolen art. As creators of the NFTs, Yuga Labs retain ownership of the brand copyright, but the company gives the owner of the individual NFTs a broad license to use the image they own. This includes unlimited, worldwide license to use, copy, and display the purchased art. But how is ownership verified? Does possession of the NFT in a wallet convey these usage rights if the NFT was nefariously obtained? A high-profile lawsuit might have clarified several legal questions around digital assets ownership and established some legal precedent. Rather than going to court, Green, chose a pragmatic solution by repurchasing the NFT from the new owner, paying a price of $300,000. Industry observers were disappointed about Green's discouraged reaction of paying this virtual ransom.

The Metaverse as a crime scene

The story about Seth Green's stolen TV show character illustrates that NFTs have become an alluring target for cybercriminals. While some NFTs have reached high values and are held by wealthy individuals, these owners may not have a high degree of digital literacy and often know little about cybersecurity. This dangerous combination, combined with rather lax persecution of cybercrime, has created an enormous potential for crime and fraud. Another example of NFT-related crime, the NFT-based game "Evolved Apes", is worth mentioning. The developer promised a rich gaming ecosystem of battling NFTs which initially sold out a collection of 10,000 pieces. But within one week of launching, the project suddenly disappeared with total digital assets of over $2.7 million. Currently, this case remains unsolved.

In many respects, NFT-related crime resembles the hacks that have been witnessed for years in the cryptocurrency world, with many of these scams evolving from real world fraud. The aforementioned "Evolved Apes" scam can be categorized as a "rug pull" – a case where the operator simply takes the money and runs. The history of cryptocurrency is littered with swindles of this kind. Another attack vector for digital assets includes stealing secret keys or recovery phrases which can empty entire wallets of their owners. This phishing happened in the Seth Green case and unfortunately to many other wallet holders.

Cryptocurrencies and NFTs are important building blocks of the Metaverse, a completely digital world based on virtual reality. The Metaverse is currently booming, with Microsoft and other companies investing billions in this new technology. Facebook's parent company even rebranded as "Meta" to emphasise their claim to be a leading player in this market. Attacks on cryptocurrency and NFTs need to be seen as crimes that threaten not only the Metaverse, but are in fact 'real world crimes'.

Cryptocurrencies and NFTs can be regarded as one of the Metaverse's ways to cope with a well-known problem: that digital data can be copied easily and perfectly. The identical copy trait is not desirable when it comes to digital money and valuables. As both cryptocurrencies and NFTs are based on blockchain technology, one can expect that blockchains will become another indispensable part of the Metaverse.

One positive aspect is that the cryptography used in the Metaverse appears to be secure. To date there have been no significant successful attacks on the ciphers, signature algorithms, and hashing functions involved in NFTs, cryptocurrency, or other blockchain systems. This is largely due to the fact that the core cryptography for these systems is mature and well-known from more conventional crypto applications, such as email encryption, code signing, and file protection. While there have been attacks on these components, the cryptography they are based on has never been the weak point.

While many of the aforementioned attacks work on both NFTs and cryptocurrency systems, some hacking methods can only be employed on the latter. This is because NFTs are unique and cannot be swapped atomically, while Bitcoin or Ether are fungible assets that can be easily sent from address to address. To address this challenge many NFTs and sales and trading platforms rely on some smart contract to enable transfer of NFT assets. There is always a risk that untrusted sites use this malicious code to perform actions that are not intended when transacting for NFT purchase or sale. Criminals can not only use such a weakness to steal the NFTs themselves, but also other digital assets held in the wallet of the owner.

Technology from secure identities is key

"While crime in the Metaverse, just like the Metaverse itself, is a new phenomenon, the methods to prevent it are not", says Dan Butnaru, Senior Advisor Digital Identity, Atos. "The core task to fight cryptocurrency and NFT offenses is to implement robust security which can be replicated from the technology used to secure identity documents." If an avatar in the Metaverse can be identified in a secure way and ownership can be validated, then identity theft becomes infeasible.

To establish secure identities in the Metaverse, advanced multifactor authentication techniques need to be established. Passwords are not sufficient for this task. For instance, the

> “ *While crime in the Metaverse is a new phenomenon, the methods to prevent it, are not. The core task is to create reliable identities.*
>
> *– Dan Butnaru, Senior Advisor Digital Identity, Atos.*

phishing attack on Seth Green targeted the knowledge-based authentication he used to access his NFT wallet. If traditional protection techniques such as a hardware based secure elements were used, such as a smart card or an embedded SIM card, the hacker would not have been successful. By using custodial wallets that allow the holder to retain control over their private key and recovery phrases, it becomes nearly impossible for remote attackers to exploit such vulnerabilities, as they need to be in physical possession of such a wallet.

Because of the transparent nature of the blockchain, it is well suited for creating reliable identities and secure authentication schemes that can be verified by anyone. As blockchain is the major underlying technology present in the Metaverse, a major task will be determining how to use it for authentication across different blockchains. Current initiatives like the European Blockchain Services Infrastructure (EBSI) and the European Self-Sovereign Identity Framework (ESSIF), are attempting to solve this problem in the real world. In a self-sovereign-identity environment, every citizen can decide with whom their name, age, academic credentials, or purchase data is shared on an individual basis. This allows for citizens to have a far greater degree of control over their personally identifiable information. Dan Butnaru states: “Self-sovereign identities are well suited for the Metaverse and might become another important building block of it.”

Finally, future eID-document-based digital identities may serve as solutions to protect the Metaverse. Many current eID documents are based on Java Card platforms that could allow for additional applications to be stored on the eID card. By loading an additional applet, a digital asset wallet could be paired with the eID card and benefit from the secure element as a keystore. Such a solution is considerably more secure and more user-friendly than a password alone and this would also serve as a means to address challenges of linking crypto-wallets with their owners to discourage money laundering or other financial crime.

“It appears that we are heading for a Metaverse, in which cryptocurrencies and NFTs are used to implement money and valuables, while trusted digital identities, blockchains and eID documents serve as technology enablers”, concludes Dan Butnaru. This development is still in an early stage, but it is justified to say: while the Metaverse may be attractive for criminals, there are already powerful tools to fight them. ☒

Trust SEC
CCESS CARDS
red by
COS

TrustSEC's *journey* to SECURE identities

By Manal Ashraf, TrustSEC

□ Digitalization has decisively penetrated all industries, changing the day-to-day business operational security boundaries. One of the key enablers to maintaining secure processes is authentication. High authentication measures ensure secure digitalized services in our hyper-connected world, including communications, access-right management, online payments, and so on.

Many companies have focused on providing products and solutions that serve the digital transformation in general. TrustSEC, however, has chosen to adopt the concept of innovating products and solutions of a value-added proposition in terms of security specifically. TrustSEC's vision is to provide the most secure solution that will serve for the securing of identities.

The rise of the PKI Multifactor Authentication USB device

Passwords were considered the primary method by which users authenticated themselves in computers and systems logins. But passwords proved over time that they were weak and incapable of protecting identities in the right way. Based on the concept of two-factor authentication, which requires the user to both own a hardware token and possess a password that no one else knows, TrustSEC provided its first standard secure authentication PKI device, to secure a user's identity as a first milestone on its journey to secure identities.

Public Key Infrastructure (PKI) is a framework established to issue, maintain, and revoke public key certificates, including systems, processes and people. Public key certificates provide digital signature and encryption capabilities, which can be used to implement the following security services:

- **Identification and Authentication:** PKI provides for identification and authentication through digital signature. If the signature is valid, then the Relying Party (the person or system relying on the presented certificate for authentication or other security services) has assurance that the entity participating in the transaction is the Subscriber (the identity asserted by the certificate).
- **Data Integrity:** PKI provides for data integrity through digital signature of information. If the recipient of digitally signed information is able to verify the signature on the information using the public key of the certificate used to generate the signature, then the recipient knows that the content has not changed since it was signed.
- **Confidentiality:** PKI provides confidentiality through encryption. If the public key in a certificate is used to encrypt information, only the associated private key, held (and kept secret) by the entity named in the certificate, can decrypt that information.
- **Technical Non-Repudiation:** PKI assists with technical non-repudiation through digital signatures. Technical non-repudiation can be considered a form of attribution, namely that the digitally signed information can be attributed to the entity identified in the certificate used to generate the signature.

The challenges from the theft of tokens or the sharing of passwords were also considered. It was these considerations that pushed the evolution of the TrustSEC high-secure authentication devices toward Multi-Factor Authentication (MFA). TrustSEC MFA PKI Tokens were developed to enable high-security procedures based on available biometric features. The TrustSEC MFA PKI Tokens are considered a highly secure device for individuals. It authenticates and enables the authorization of the users to access systems containing sensitive information, by using the user's unique fingerprint. With this biometric feature added, only the legitimate owner of the fingerprint and the tokens can authenticate their identity.

The first generation of TrustSEC PKI tokens were based on MicroControl chips, but later TrustSEC adopted new technology. In the process of developing their innovative hardware and optimized software solutions with the highest level of cryptography, it became clear that a smartcard's secure element is the most secure component. The secure element encrypts all the keys, uses techniques to implement tamper resistance (making it harder to extract data by disassembling or analysing the chip) and is designed to frustrate attempts to extract any information from the card beyond what the intended interface exposes.

A smart card is essentially a minimal computing environment on a single chip, complete with a CPU, ROM, EEPROM, RAM and I/O port. The latest generation of cards are supplied with cryptographic co-processors that implement common algorithms.

Securing identities using Bio Smart Card Operating system and Applets

In parallel to the PKI Tokens, TrustSEC was also developing its smartcard operating system – SLCOS. This operating system allowed the independence and flexibility of code upgrade to handle rising security measures. It also allowed the ability to add more than one applet in a safe and secure environment, the facility to make any customization to SLCOS and the capability to port on any chip.

SLCOS is smart card operating system that incorporates the latest secure technology in a smart card, offering an open platform that combines the best in security, flexibility Native/Java, and hardware independence. SLCOS manages the internal file system, I/O, and the interactions between these components and various applications. It supports contact/ contactless/dual/USB Interfaces, can be preloaded or programmed with fixed applications or accepts post application-uploads using the Card Manager Module.

> “*TrustSEC has recently released its biometric access control card that secures identities’ authentication over physical access points and logical access.*

TrustSEC integrated its smart card operating system, SLCOS, with biometrics technology to provide a multi-factor authentication device that verifies the card holder’s identity by their fingerprint, to facilitate a higher security measure. TrustSEC used the Match-on-Card (MoC) feature that stores the holder's biometric data on the card – eliminating the possibility of revealing private fingerprint data on any network or local databases. Based on this milestone, TrustSEC has now added a PKI applet to the smart card to provide Multi Factor Authentication PKI, that supports secure communication and client certificate authentication with a fingerprint tap.

When it’s time to log into a system, the user presses his finger to the biometric sensor, while the card is either inserted into a reader or through an NFC-enabled reader. The card captures the user's fingerprint, (through the smart card embedded fingerprint sensor), then uses algorithms to extract the data needed to compare the captured print to the stored template. If the data matches, the user's identity is authenticated and access is granted or the process is completed.

Multi-application smart card with biometric validation

TrustSEC has recently released its biometric access control card that secures identities’ authentication over physical access points and logical access. TrustSEC’s Bio Access control cards combine both functionalities. It provides a simple and easy user experience – simplifying the authentication process by successfully authenticating the person’s identity over physical access points and logical access with the user’s unique fingerprint.

Multi Factor Authentication against cryptocurrency wallet attacks

A cryptocurrency wallet is an application that functions as a wallet for your digital currency. The term wallet is used to create the image of a physical wallet that can store cash and cards. However, instead of holding physical assets and items, it stores the passkeys individuals use to sign for their cryptocurrency transactions and provides the interface that lets users access their crypto.

TrustSEC decided to be part of this new technology provider community and used its capabilities, expertise and experience in PKI and smart cards to support its partners in achieving great milestones in this field.

In partnership with eSignus, TrustSEC has brought to market a very high secure environment, which includes a biometric card system that combines security and flexibility, serving to sign any crypto transaction with the card holder's fingerprint; Thereby helping to bring 'HASHWallet’ – the first non-programmable hardware wallet – to the market. ☒

You can find out more about HASHWallet at
www.gethashwallet.com

and TrustSEC’s Biometric Access Control Card at
www.trustsec.net

SCAN ME

TO WATCH OUR
LATEST VIDEO

FLOW *instead* of falter SEAMLESS travel made *easy*

By Katharina Schuldt, Mühlbauer Group

□ We live in the digital age; all our devices are smart, count our steps, measure our pulse. They remind me to leave my apartment early enough and manage to avoid every traffic jam so that I arrive at the airport on time. Once there, however, neither my smartphone nor my smartwatch come up with a plan B: there is no detour for the way through check-in and security control. The waiting game begins.

After a study from the US luggage storage company Bounce between March 2021 and March 2022, the average security wait time at Miami International Airport – the largest gateway from the US to Latin America – was 24 minutes and 54 seconds. Average passport control wait time was 22 minutes and 3 seconds. That means a passenger was waiting 47 minutes only for these two control stations, not to mention the waiting time to drop off or pick up the luggage and passing through the terminal!

Are there also examples where you can speed through the airport quickly? Indeed, there are! It does not always depend on the airport's size or passenger number how long the travelers have to queue up. The system is crucial. More and more people use electronic passports, but an alarming number of airports and border crossing stations still control every passport manually. Automated border control (ABC) systems though are more efficient and offer higher security, because they avoid human mistakes and match the data within seconds. Flow instead of falter!

> *“ The benefits of automated border control systems like Muehlbauer’s Easy Flow are not only appealing for the traveler. Replacing manual processes saves time and reduces operating costs and personnel expenses.*

Fast check-in at smart kiosks

The German innovative technology specialist Muehlbauer has developed an airport and border crossing solution, where automated security systems take over the verification and authentication of travelers and their identity documents. The MB Easy Flow system allows the passenger to fill out the digital declaration forms before starting the journey via smartphone or computer. At the airport or border crossing checkpoint, the passenger can directly check-in at a smart kiosk. The high-tech kiosk reads the traveler’s biometric data from their ePassport or eID and performs a quick presence check via facial recognition, liveness and fever detection. For this purpose, the sophisticated system automatically moves to the height of the traveler's face and uses a built-in camera and thermometer to take the required data and match it with the appropriate database. Officials will immediately be notified if a passenger is considered unfit to pass or has incomplete travel documents. Of course, manual intervention is possible at any time, but the majority of passengers pass through the station without personal contact. This speeds up the process enormously and brings further advantages like contact reduction during pandemic conditions.

Passport control without standstill

The intelligent system automatically passes on the information to the relevant authorities and the flight operator receives a notification when check-in and verification have been completed. After the flight crew gives their OKAY, the boarding gate is activated automatically. To board the aircraft, passengers now seamlessly pass through the last control station: Muehlbauer’s smart gate. There is no need for stopping, the traveler just walks through the gate, pointing the head to the integrated camera screen. The gate checks if this person is allowed to access by facial verification on the fly and the passenger can proceed to the aircraft.

The benefits of automated border control systems like Muehlbauer’s Easy Flow are not only appealing for the traveler. Replacing manual processes saves time and reduces operating costs and personnel expenses. Eliminating human mistakes protects against forgery and increases data security. As a cloud-based application, the system can be connected with a closed and secured network. This allows the operator to monitor and intervene in real-time from anywhere. These smart solutions can be integrated in the existing infrastructure and do not need expensive alteration. Essentially, we could use and utilize our digital resources and our knowledge about artificial intelligence to offer a satisfying and comfortable experience to both the passenger and the employee. ☒

SILICON TRUST DIRECTORY 2022

THE SILICON TRUST

THE INDUSTRY'S PREMIER SILICON BASED SECURITY PARTNER PROGRAM

The Silicon Trust is a well-established marketing program for smart card solutions with high visibility in the worldwide government and identification (ID) markets. With over 30 companies along the value chain, the Silicon Trust forms a strong community of like-minded companies.

THE SILICON TRUST PROGRAM FOCUSES PRIMARILY ON:

- Educating government decision makers about technical possibilities of ID systems and solutions
- Development and implementation of marketing material and educational events
- Bringing together leading players from the public and private sectors with industry and government decision makers
- Identifying the latest ID projects, programs and technical trends

EXECUTIVE COUNCIL

The Executive Council has been the steering committee of the Silicon Trust since 2008. It drives the Silicon Trust by defining the topics and directions of the program's publications, workshops and meetings.

INFINEON TECHNOLOGIES

Infineon Technologies AG is a world leader in semiconductors. Infineon offers products and system solutions addressing three central challenges to modern society: energy efficiency, mobility, and security. In the 2016 fiscal year (ending September 30), the company reported sales of Euro 6,5 billion with about 36,000 employees worldwide. Infineon is the world's leading vendor of secure chip card ICs used for passports, ID cards, payment cards, mobile subscriber authentication (SIM cards), access cards and trusted-computing solutions as well as being a technology driver in the hardware-based security field.

www.infineon.com

ADVISORY BOARD

The Silicon Trust Advisory Board supports the Executive Council in defining the direction of the program in terms of public policy and scientific relevance.

BSI

Bundesamt für Sicherheit in der Informationstechnik – The German Federal Office for Information Security (BSI) is an independent and neutral authority for IT security. It has been established in 1991 as a high level federal public agency within the area of responsibility of the Ministry of the Interior. The BSI's ultimate ambition is the protection of information and communication.

Especially in the area of smart card technology, BSI is responsible for the design and definition of secure solution requirements for governmental identification documents. The German ePassport has been introduced in 2005, the second ePassport generation followed 2007, and starting in 2010 the all-new German eID card has opened a new trustworthy approach to Internet authentication for all German citizens. Security of all these documents is based on BSI specifications, developed in close collaboration with European/international standardization bodies and leading industry partners.

www.bsi.bund.de

FRAUNHOFER AISEC

Fraunhofer AISEC supports firms from all industries and service sectors in securing their systems, infrastructures, products and offerings. The institution develops qualitatively high-value security technologies, which increase the reliability, trustworthiness and tamper-resistance of IT-based systems and products. The approximately 80 members of the Fraunhofer AISEC scientific and technical staff balance economic needs, user-friendliness, and security requirements to develop optimally tailored concepts and solutions.

The security test labs are equipped with state-of-the-art equipment, and highly qualified security experts evaluate and analyze the security of products and hardware components as well as software products and applications. In our laboratories, functionality, interoperability and compliance are tested to give clients targeted, effective advice. Strategic partnerships with global corporations as well as with internationally recognized universities guarantee scientific excellence as well as its market-driven implementation.

www.aisec.fraunhofer.de

SILICON TRUST PARTNERS

Partners of the Silicon Trust are a vital element of the program. The partners represent all aspects of the value chain and are international representatives of the ID industry. They all share one common goal – to create awareness, to educate and to promote the need for silicon-based security technologies.

AdvanIDe

Advanced ID Electronics – is one of the leading silicon distributors, focused on components for RFID transponders, chip cards and RFID readers and terminals. Thanks to its optimized semiconductor supply chain, AdvanIDe can guarantee manufacturers of smart cards, RFID transponders and readers the most efficient access to the latest semiconductors.

www.advanide.com

ATOS

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of over € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries..

www.atos.net

AUSTRIACARD

AUSTRIACARD AG is a holding company of businesses providing end-to-end solutions and products in the field of Digital Security and Information Management. The Group brings together the century-long heritage in printing services and state-of-the-art digital data solutions (Information Management division) with the well-established production and personalization of smart cards and the offer of cutting-edge digital payment solutions (Digital Security division). The combination of well-established industrial roots with an expanding services portfolio that meets the needs of the increasingly digital and mobile economy is at the very core of the Group's confidence in its future.

www.austriacardag.com

AUTHENTON

authenton (a EU + CH + UK registered Trademark and authenton GmbH) is a new (2022) Sales & Marketing arm of AIXecutive, which was founded in 2012. AIXecutive's management and its technology-partners have been an integral part of the global Smart Card industry since the mid 1990s. Since 2012 AIXecutive provides and supports global players with customer specific developments.

The company helps to manage high security Identification & Authentication solutions for Government eID, Mobile-, Payment-, and high secure IoT (IoT SAFE) as well as security certified Web-Authentication solutions (incl. FIDO2.1). The authenton#1 Token is a result of AIXecutive & its technology partners' latest security certified developments for Government eID and Mobile Security.

Munich based authenton GmbH represents all Marketing & Sales activities for the registered authenton brand, its first product -the authenton#1 FIDO2.1 Token – as well as subsequent products.

www.authenton.com

AVATOR

AVTOR LLC is an integrator of cybersecurity solutions and the leading Ukrainian developer in the field of cryptographic protection of confidential information. The AVTOR's hardware secure tokens and HSMs are based on smartcard technology and own smartcard operating system "UkrCOS" are compliant for operations with qualified digital signatures and classified information.

AVTOR provides services for development and integration of complex cybersecurity systems for automated systems for different purposes and any level of complexity and predominantly deals with: protection of data transfer (IP-traffic); secure electronic document management; developing corporate and public certifying authorities (CA) in public key infrastructure (PKI); integration of complex information security systems; development of special secure communications systems.

http://www.avtor.ua

CARDLAB

CardLab is a world leading data and privacy protection and Cyber security company by use of its biometric card technology provided to the powered smart card industry having developed and commercialized ISO 7810 compliant secure card products including:

- Full "System on Card" biometric authentication solution based on Fingerprints™ FPC1300 T-shape™ touch sensor", for payment, ID, Access control, blockchain and Cyber Security.
- Communication controlled RFID cards (Jammer & Mute-Cards),
- "All In One" card solution platform and other card solutions customized to customer specifications for secure and sustainable card production.

CardLab is a Denmark based card development and manufacturing company with manufacturing partners in Asia and USA and own card lamination factory in Thailand. CardLab offers unparalleled technical design and manufacturing support for card solutions including scalable security levels and existing infrastructure compatibility making implementation cost affordable for end users.

www.cardlab.com

CARDPLUS

CardPlus is a consulting firm with a focus on customized, enterprise level, Identity and Security Management Solutions. We offer a full range of Professional services to build, transform, implement and manage our customized enterprise level security and identity solutions. Due to our vast hands-on experience in designing and implementing secure travel and identification systems for governments and large public sector customers, we are uniquely positioned to understand your highly complex security requirements and translate the same into practical, workable solutions.

www.cardplus.de

COGNITEC

Cognitec develops market-leading face recognition technology and applications for industry customers and government agencies around the world. In various independent evaluation tests, our FaceVACS® software has proven to be the premier technology available on the market. Cognitec's portfolio includes products for facial database search, video screening, and biometric portrait capturing.

www.cognitec-systems.de

CRYPTOVISION

cryptovision is a leading supplier of innovative cryptography & public key infrastructure (PKI) products. The lean and intelligent design of the complete product range makes it possible to integrate the most modern cryptography and PKI application into any IT system. cryptovision PKI products secure the IT infrastructures of diverse sectors, from private enterprise to government agencies. The consultancy service spectrum ranges from the risk analysis of subsystems or standalone systems to the design of complete cross-platform cryptographic architectures. Since August 2021, cryptovision is part of Atos.

www.cryptovision.com

GEMALTO

Gemalto, a Thales company, is a global leader in digital security, bringing trust to an increasingly connected world. We design and deliver a wide range of products, software and services based on two core technologies: digital identification and data protection.Our solutions are used by more than 30,000 businesses and governments in 180 countries enabling them to deliver secure digital services for billions of individuals and things. Our technology is at the heart of modern life, from payment to enterprise security and the Internet of Things.We have built a unique portfolio of technology and expertise including physical and digital identity credentials, multiple methods of authentication – including biometrics – and IoT connectivity as well as data encryption and cloud service protection. Together, these technologies help organizations protect the entire digital service lifecycle from sign-up to sign-in and account deletion with data privacy managed throughout.Gemalto is part of the Thales group, a €19bn international organization with more than 80,000 employees in 68 countries worldwide.

HBPC

Pénzjegynyomda Zrt. (Hungarian Banknote Printing Shareholding Company) is the exclusive producer of 'Forint' banknotes, and is one of the leading security printers in Hungary, specializing in the production of documents and other products for protection against counterfeiting. Currently, HBPC produces passports, visa, ID documents, driving licenses, securities, duty and post stamps, tax stamps and banderols, paper- and plastic-based cards, with or without chip, and is aiming to provide complex system solutions.

www.penzjegynyomda.hu

HID GLOBAL

HID Global Government ID Solutions is dedicated to delivering highly secure, custom government-to-citizen ID programs worldwide. HID Global Government ID Solutions offers government customers an end-to-end source for their most demanding state and national ID projects. With Genuine HID™, customers benefit from the industry's broadest portfolio of trusted, interoperable secure identity solutions across all aspects of the government identification market. Government ID Solutions offerings include expert consulting services, data capture, credential management and issuance solutions, world-leading credentials and e-documents, readers, inlays, prelaminates, LaserCard® optical security media technology, and FARGO® card printers.

www.hidglobal.com

MASKTECH

MaskTech is the leading independent provider of high secure system on chip designs, embedded ROM masked products, security middleware, certification and integration services focused on human credential applications. MTCOS – MaskTech Chip Operating System – is a high performance and high security operating system, especially designed for secure semiconductors with powerful crypto co-processor and RFID, dual interface or contact interface. MTCOS is available on a unique variety of microcontrollers of different silicon vendors. MTCOS is a fully open standard (ISO/IEC) compliant multiapplications OS, used in more than 40 eID projects worldwide.

www.masktech.de

MELZER

For decades, MELZER has been internationally known as the leading production equipment supplier for cutting-edge ID Documents, Smart Cards, DIF Cards, RFID Inlays and e-Covers for Passports. Customised solutions in combination with the unique modular inline production processes ensure the highest productivity, flexibility and security, leading to maximum yield and the lowest per unit costs. Numerous governmental institutions, as well as private companies, rely on industrial solutions supplied by MELZER. The Melzer product portfolio also includes advanced RFID converting equipment for the production of Smart Labels/Tickets and Luggage Tags.

www.melzergmbh.com

MICROPROSS

Established in 1979, Micropross is the leading company in the supply of test and personalization solutions for the business of RFID, smartcard, and Near Field Communication (NFC). Micropross has proven expertise in the design of laboratory and manufacturing test tools which are all considered as references in their domains. These tools allow users to fully characterize and test the electrical and protocol performance of products such as smartcards and smartphones in design, conformance, and production. In 2015, National Instruments acquired Micropross.

www.micropross.com

MK SMART

Established in 1999 in Vietnam, MK Group is the leading company in Southeast Asia with years of experience in providing Digital security solutions and Smart card products for the following industries: Government, Banking and Fintech, Transport, Telecom, IoT, Enterprises, and the Consumer market.

With production capacity of over 300 mio. card per annum and more than 700 employees, MK Smart (a member of MK Group) is ranked under the Top 10 largest card manufacturers globally. The companies production facilities and products are security certified by GSMA, Visa, Mastercard, Unionpay, ISO 9001 and FIDO.

www.mksmart.com

MÜHLBAUER ID SERVICES GMBH

Founded in 1981, the Mühlbauer Group has grown to a proven one-stop-shop technology partner for the smart card, ePassport, RFID and solar back-end industry. Further business fields are the areas of micro-chip die sorting, carrier tape equipment, as well as automation, marking and traceability systems. Mühlbauer's Parts&Systems segment produces high precision components.

The Mühlbauer Group is the only one-stop-shop technology partner for the production and personalization of cards, passports and RFID applications worldwide. With around 2,800 employees, technology centers in Germany, Malaysia, China, Slovakia, the U.S. and Serbia, and a global sales and service network, we are the world's market leader in innovative equipment- and software solutions, supporting our customers in project planning, technology transfer and production ramp up.

http://www.muehlbauer.de

OVD KINEGRAM

OVD Kinegram protect government documents and banknotes. More than 100 countries have placed their trust in the KINEGRAM® security device to protect their high security documents. OVD Kinegram is a Swiss company and a member of the German Kurz group. The company has accumulated over three decades of experience in the protec- tion against counterfeiting and maintains close contacts with police forces, customs authorities and internationally reputed security specialists. OVD Kinegram offers a full range of services: consulting, design, engineering, in-house production, application machines and support as well as after-sales service.

www.kinegram.com

PARAGON ID

Paragon ID is a leader in identification solutions, in the e-ID, transport, smart cities, traceability, brand protection and payment sectors. The company, which employs more than 600 staff, designs and provides innovative identification solutions based on the latest technologies such as RFID and NFC to serve a wide range of clients worldwide in diverse markets.Paragon ID launched its eID activity in 2005. Since then, we have delivered 100 million RFID inlays and covers for ePassports. 24 countries have already chosen to rely on the silver ink technology developed and patented by Paragon ID for the deployment of their biometric electronic passport programs.Today, Paragon ID delivers nearly 1 million inlays each month to the world's leading digital security companies and national printing houses, including some of the most prestigious references in the industry. Through 3 secure and certified manufacturing sites located in France (Argent sur Sauldre), USA (Burlington, Vermont) and Romania (Bucharest), Paragon ID ensures a continuous supply to its local and global clients. Visit our website for more information and our latest news.

www.paragon-id.com

PAV

PAV Card is a German, family-run business and one of the leading manufacturers for smart cards and RFID solutions. PAV products are used in many applications, ranging from hotel access, airport and stadium technology to the use in retail outlets and smart card applications, such as payment and health insurance. PAV's product range includes special heat resistant and tamper-proof ID cards as well as smart cards using the latest contactless technology for secure access solutions suitable for corporate buildings or sensitive access areas, such as airports.

www. pav.de

POLYGRAPH COMBINE UKRAINA

State Enterprise "Polygraph Combine "Ukraina" for securities' production" is a state company that has more than 40 years of experience in providing printing solutions. Polygraph Combine "Ukraina" has built up its reputation in developing unique and customized solutions that exceed the expectations of customers and partners. Moreover, the enterprise offers the full cycle of production: from prepress (design) processes to shipment of the finished products to customers.It offers the wide range of products: passports, ID documents, bank cards, all types of stamps (including excise duty and postage stamps), diplomas, certificates and other security documents. Find more information at:

www.pk-ukraina.gov.ua

PRECISE BIOMETRICS

Precise Biometrics is an innovative company offering technology and expertise for easy, secure, and accurate authentication using smart cards and fingerprint recognition. Founded in 1997, Precise Biometrics today has solutions used by U.S. government agencies, national ID card programs, global enterprises, and other organizations requiring multi-factor strong authentication. Precise Biometrics offers the Tactivo™ solution, a smart card and fingerprint reader for mobile devices.

www.precisebiometrics.com

PWPW

PWPW is a commercial company, entirely owned by the Polish Treasury, with a long tradition and extensive experience in providing security printing solutions. The company offers modern, secure-products and solutions as well as highest quality services which ensure the reliability of transactions and identification processes. It is also a supplier of state-of-the-art IT solutions.

www.pwpw.pl

SECOIA EXECUTIVE CONSULTANTS

SECOIA Executive Consultants is an independent consultancy practice, supported by an extensive global network of experts with highly specialized knowledge and skill set. We work internationally with senior leaders from government, intergovernmental organizations and industry to inspire new thinking, drive change and transform operations in border, aviation, transportation and homeland security. SECOIA provides review and analysis services for governments in the field of Civil Registry, Evidence of Identity, Security Document issuance and border management. Also, SECOIA specialises in forming and grouping companies for sustainable, ethical sales success. Adding to the consulting and coaching activities, SECOIA offers Bidmanagement-Coaching and RFP preparation / Procurement assistance for Government offices and NGOs. Try us, and join the growing family of customers.

www.secoia.ltd

SIPUA CONSULTING

SIPUA CONSULTING® is a leading and well-established consultancy company, focusing on customized e-ID solutions for government agencies and institutions around the world. Based on detailed market intelligence and long-lasting relationships within the e-ID ecosystem, SIPUA CONSULTING is in the strategic position to conceptionalize, promote and implement various projects along the value chain.

www.sipua-consulting.com

TRUSTSEC

TrustSec is a Polish information security company, founded by internationally recognized information security and cryptography experts. Through TrustSec's pool of experts and its business-driven innovative solutions, TrustSec offers its unique, in-house developed operating system for smart cards – SLCOS. The company also delivers a variety of products and solutions, that cover software protection, data encryption, OTP, and security hardware (namely PKI tokens and FIDO2 tokens). In addition to its latest fintech innovation CPA and its unique panel of professional services; of consultation, integration, testing, and outsourcing, to help the other companies benefit from the latest available advances in cryptography to improve their products and services.

www.trustsec.net

UNITED ACCESS

United Access is focused on secure, high-end smart card and RFID based solutions. We are acting as a security provider with a broad range of standard and integration components. United Access is the support partner for the Infineon smart card operating system SICRYPT. United Access provides secure sub-systems to various markets like public transport, road toll, logical access, logistics, parking systems, brand protection, physical access control and others.

www.unitedaccess.com

WCC

Founded in 1996, WCC Smart Search & Match specializes in the development of enterprise level search and match software for identity matching. Its software platform ELISE delivers meaningful identity matches using multiple biometrics and/or biographic data from a wide range of sources at sub second response times. ELISE is highly scalable and extremely robust, and is used by large health insurance companies and government agencies for immigration, border security and customs control. The company is headquartered in the Netherlands and has offices in the USA and the Middle-East.

www.wcc-group.com

WIBU-SYSTEMS

Wibu-Systems, a privately held company founded by Oliver Winzenried and Marcellus Buchheit in 1989, is an innovative security technology leader in the global software licensing market. Wibu-Systems' comprehensive and award-winning solutions offer unique and internationally patented processes for protection, licensing and security of digital assets and know-how to software publishers and intelligent device manufacturers who distribute their applications through computers, PLC, embedded-, mobile- and cloud-based models. .

www.wibu.com

X INFOTECH

X INFOTECH, a leading systems integrator and a developer of software suite Smarteo, delivers premium solutions for issuing, managing and verification of electronic ID documents and smart cards. The company's turnkey solutions are fully independent and flexible, and in combination with unrivalled team expertise, allow smart card and eID programs to be implemented easily, adapting to any environment by supporting any equipment and chip type. With successfully implemented projects in 45 countries already, X INFOTECH is now a trusted business partner and preferred solutions and services provider for hundreds of customers.

www.x-infotech.com

MASKTECH

We make chips intelligent

MTCOS®

Independent – High Secure
Card Operating System

ELECTRONIC PASSPORT

ELECTRONIC NATIONAL ID

ELECTRONIC TICKETING

ELECTRONIC HEALTH

ELECTRONIC RESIDENCE PERMIT

ELECTRONIC DRIVING LICENSE

MTCOS 2.5
EAL5+
certified on
IFX, NXP and ST

We are looking forward to seeing you at one of the upcoming events.

SecurITy made in Germany
TeleTrusT Quality Seal
www.teletrust.de/itsmig

Common Criteria

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