NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

NOVEMBER 2023

The VAULT

HOW DO YOU KNOW IF IT'S REAL OR FAKE?

FEATURED ARTICLE

CodeMeter Certificate Vault: Certified Genuine

Wibu-Systems

ALSO IN THIS ISSUE

Silicon Trust
Unmasking the Threat: AI and the future of Digital ID

Mühlbauer Group
Queuing was Yesterday

Infineon Technologies
Revolutionizing Security with Integrity Guard 32

Contents

Imprint

THE VAULT ISSUE 38
Published by Krowne Communications GmbH, Berlin.
PUBLISHER: Krowne Communications GmbH, Kurfürstendamm 194, 10707 Berlin
EDITOR-IN-CHIEF: Steve Atkins
ART DIRECTOR: Nina Eggermann
PARTNER DIRECTOR: Yvonne Runge
EDITORIAL CONTRIBUTIONS: Steve Atkins, Katharina Schuldt, Marco Blume, Comexposium, Robert Bach
PHOTOS: ISTOCKPHOTO, WIBU-SYSTEMS, MÜHLBAUER, WEPIK AI IMAGE EDITOR, KROWNE COMMUNICATIONS
EDITION: NOVEMBER 2023. No portion of this publication may be reproduced in part or in whole without the express permission, in writing, of the publisher. All product copyrights and trade- marks are the property of their respective owners. all product names, specifications, prices and other information are correct at the time of going to press but are subject to change without notice. The publisher takes no responsibility for false or misleading information or omissions.

QUEUING was YESTERDAY. How to pass BORDERS *SEAMLESSLY*?

By Katharina Schuldt

The world's airports are becoming busier and busier, facing the task to ensure safe traveling in terms of identity checking and repeatedly also in relation to health. We are not only thinking about how to combat the counterfeiting of documents and how to expose fraudsters. Today, we are figuring out how we keep the queues at the counters as short as possible. How do we limit or completely avoid contacts between travelers? How do we prevent documents from being passed from hand to hand between security staff and passenger? In other words, it's about how to pass borders seamlessly.

Automated Border Control systems (ABC systems) efficiently perform the border control process thereby expanding the control capacities within a limited investment. The Mühlbauer Group developed such a solution to unite a touchless and hassle-free travel experience with highest security standards for all stakeholders. This decentralized, permission-based solution operates from the passenger's personal mobile device. It ensures compliance with current health and hygiene standards, as well as with valid data protection regulations and fulfils all governmental security requirements.

Verification within seconds

The MB SEAMLESS TRAVEL system uses self-service kiosks as fully automated border management systems. These iKiosks feature an incorporated ePassport and ID card reader to allow for the reliable identification and verification of the traveler, also checking the data against external databases. The integrated advanced biometric technology with face and liveness detection offers high-speed screening to compare the digital image on the chip with the live photo. Optionally, a fingerprint

The MB SEAMLESS TRAVEL system *uses self-service kiosks as fully automated border management systems. The integrated advanced biometric technology with face and liveness detection offers high-speed screening to compare the digital image on the chip with the live photo. Optionally, a fingerprintreader captures the finger's pattern of ridges and valleys and then compares it with the help of the matching software ABIS (Automated Biometric Identification System) to a list of registered fingerprints.*

reader captures the finger's pattern of ridges and valleys and then compares it with the help of the matching software ABIS (Automated Biometric Identification System) to a list of registered fingerprints. Besides the whole verification tools, the MB iKiosks can be equipped with a barcode reader and a thermal printer to scan or print the flight tickets. Although it sounds like a long process with many individual security steps, the complete registration only takes around 15 seconds.

The smart kiosk can also be used to check in the passenger's luggage. He or she simply places their bag in a designated area, confirms the request on the touch screen of the kiosk and automatically receives its luggage tag in the application on its mobile device. To adequately protect all passengers' health, the smart terminal can additionally be endowed with an automatic fever detection camera technology.

After checking in at the iKiosk, the traveler receives a mobile ID on its own mobile device. This TECURE-ID can be used as a passport or ID card to pass through the airport gates. It replaces a variety of inhomogeneous travel documents and guarantees a convenient, touchless and privacy-respecting border crossing. Once issued, the Digital Travel Credential (DTC) can be used whenever passing airport gates and frequent travelers do not have to enroll at the Kiosk again. When approaching the eGates, the smart system automatically prepares an authentication process and broadcasts an identification request via Bluetooth, NFC or QR-Code for the passenger to approve on their mobile device. The gate will perform a two-factor authentication: the first factor is the enrolled smartphone (or other enrolled mobile device) with the previously issued TECURE-ID; the second factor can be a biometric screening like face recognition. The doors of the gates will automatically open and the traveler can pass completely contactless. If all airports could adopt this innovative solution, long lines could be declared a thing of the past.

KATHARINA SCHULDT *is International Marketing Manager at the German technology company Mühlbauer in Roding. Before moving to the Upper Bavarian Forest, she was responsible for the promotional videos and product catalogs of the well-known toy manufacturer PLAYMOBIL near Nuremberg. She graduated in Journalism and Business Communication at the University of Europe for Applied Sciences in Iserlohn, Germany and can now look back on 10 years of experience in internal and external communication, guerilla marketing, video production and copy writing. Today she applies her creative ideas and the collected expertise to professional articles for the Mühlbauer Group.*

TRUSTECH 2023: A Glimpse into the *EVOLVING LANDSCAPE* of Digital *Identity*?

Every year, TRUSTECH emerges as a pivotal rendezvous for the card and trust technology sectors, providing a platform for industry leaders to convene and explore the ever-evolving landscape of digital payments and identification solutions. TRUSTECH seamlessly combines elements of a trade show and conference, boasting over 200 international exhibitors and approximately 150 speakers from across the world. Together, they delve into the latest technological advancements and trends within the realms of Payments and Identification.

The years 2022 and 2023 have ushered in transformational changes, particularly in the way our society operates. The prevalence of remote operations, accelerated by the recent global health crisis, has significantly shifted our mainstream economy towards online platforms. Consequently, the demand for secure identification, authentication, and authorisation, the cornerstones of digital identity, has surged in economic and civic contexts.

Digital identity has assumed a pivotal role in verifying information remotely, confirming the presence of individuals, and validating document accuracy. Technologies like biometrics and artificial intelligence, along with data source verification orchestration, have birthed a new industry: remote identity verification (PVID), now recognised by several standards.

Authentication has witnessed significant enhancements, driven by regulatory, risk management, and fraud prevention needs. Multi-factor authentication (MFA) is now commonplace across internet accounts, payment services, and various transaction platforms. The next frontier is password-less authentication, with numerous protocols and solutions already vying for market dominance.

Authorisation, a diverse stage encompassing digital signatures, access management, and resource allocation, remains crucial. It considers trust levels in identification, authentication, and network security, while also benefiting from advanced contextual analysis of risks, customer behaviour, and remote analysis tools.

In the context of cloud service platforms and connected devices, these identity functions amalgamate and transform various certified data forms, encompassing physical and digital credentials, attribute identities, or application tokens.

Governments at the national level face the challenge of adapting digital infrastructure and architecture to the new norm. They must construct digital ecosystems capable of resiliently meeting population needs, including administration, education, health, inclusion, and assistance services. These ecosystems must prioritise security, data protection, and technological sovereignty. Collaboration between the public and private sectors is imperative for building a trusted, economically viable, and sovereign ecosystem. Governance of these ecosystems requires attention to legal aspects, cybersecurity, identity management, and data protection, often necessitating the establishment of an independent supervisory authority.

Efforts and investments in infrastructure are substantial, but they are essential for governments seeking to maintain a role in digital intermediation, which impacts economic flows, as well as citizen and social interactions.

The orchestration of these entitlements is now a key focus. Digital identity has taken the helm, managing numerous certificates and attributes related to civil status, administration, KYC, payments, diplomas, and more. Orchestration and certification of public and private data, while upholding data security and user consent, pose new challenges. Initiatives like the European Digital Identity Wallet (EUDIW) project in Europe seek to address these challenges. The electronic wallet promises to revolutionise the digital identity experience by offering more integrated paths for identification, authentication, and authorisation, creating a smoother experience for users. Mobile devices as multi-purpose mediums open up significant opportunities for digital identity development and market expansion.

To navigate the evolving landscape, solutions are required to address security, privacy, and sovereignty challenges within mobile operating systems and the cloud-mobile technology environment. Additionally, traditional cards gain prominence as reliable factors for identification and authentication, complementing mobile devices.

Architectural models, including centralised, federated, and decentralised approaches, are evolving towards greater complementarity. Standards and protocols, such as ISO for driving licenses and W3C for decentralised credentials, may converge in the future to enhance interoperability and compatibility of architectural models, particularly within mobile wallets.

As digital identity expands across diverse use cases and architectural models diversify, the pursuit of international interoperability gains prominence. Collaborative efforts to open protocols and mature market standards are underway, making 2022 and 2023 pivotal years for the digital identity landscape.

This overview underscores the growing significance of digital identity for governments, citizens, and economic stakeholders alike. TRUSTECH 2023, scheduled from November 28th to 30th in Paris, presents a unique opportunity to engage with key public and private stakeholders in the field of digital identity and technology.

Entry to TRUSTECH 2023 is free, covering both exhibition visits and conference attendance. Mark your calendars for November 28th to 30th, 2023, at Paris Expo - Porte de Versailles, Pavilion 5.2.

CODEMETER *Certificate* VAULT: *Certified* Genuine

By Marco Blume, Wibu-Systems

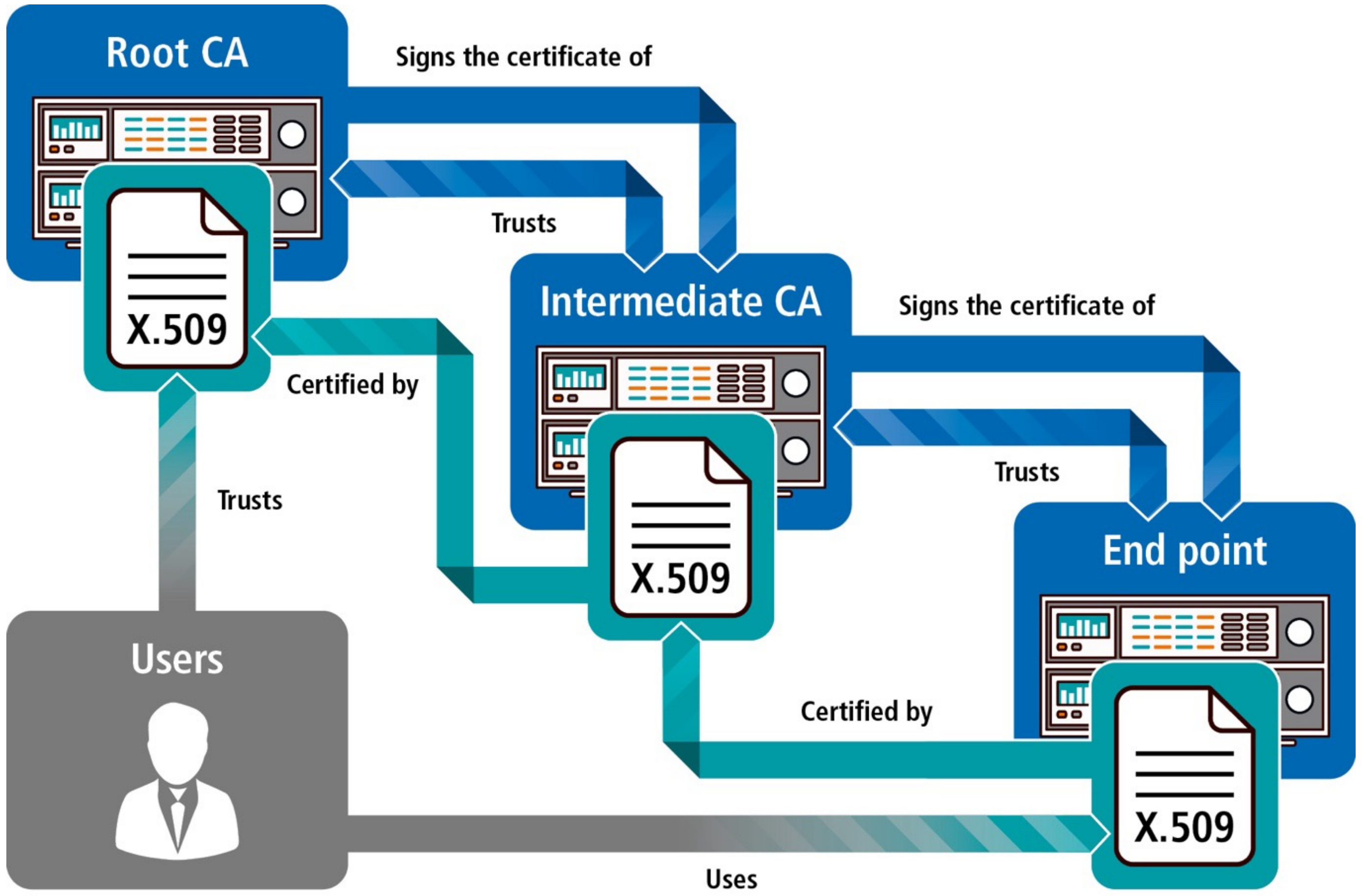
When the police came knocking on his door in 1995, John Myatt instantly knew his game was up. One of the art world's most prolific forgers confessed on the spot to creating fake works by some of modern art's greatest masters. Braques, Giacomettis, Chagalls: Myatt faked them all, made to order for the real mastermind behind the criminal enterprise: John Drewe. Where Myatt faked the paintings, Drewe faked much more. He faked their identity.

The style, technique, even the paints themselves? All fake. The reams of papers to prove the works' provenance? Fake. The previous owners listed on them? Fake. Drewe's credentials, his claimed PhDs, his entire backstory? Fake. Not even Drewe's name was genuine. He was born John Cockett in genteel Sussex in the south of England.

Certificates of Authenticity

Certificates of authenticity are not just a thing in the art world, in the jewelry business, or in the wine trade. In the digital world, certificates are also the crucial means to say: This person, this device, this program, or this line of communication is who they say they are.

Digital certificates operate by a simple principle: They are little pieces of data, issued with a set of cryptographic keys. That key pair is where the magic happens: One key is public, one is private. Both only go with each other and no other key. Having the key pair together shows that one is the real deal. In ages past, traders would make notches on sticks, split them down the middle and give one side to their trading partner in a deal. If, at a later point, the other partner had to authenticate themselves, they could bring their half of the tally stick and check if the notches match: An early form of asymmetric authentication and a (simplistic) explanation of how cryptographic key pairs work. The X.509 standard lays out what goes into the tally stick's modern successor, the digital certificate: Identity information, a serial number, information about the cryptographic algorithm, the public key, and the signature by a certificate authority (CA) that has vouched that the certificate goes with the public key for the person, device, or service it belongs to – its proof of provenance, in a way.



The rollout process of X.509 certificates

The standard practice for rolling out X.509 certificates to their destination is deceptively simple: It all begins with a root certificate authority that has the original root certificate on which all subordinate certificates depend. The root CA signs the certificates of intermediate CAs which eventually sign the certificates of end users. It is a long chain of trust, which has to be protected at all costs. As long as it holds, the end user or end point device can be sure that the certificate they are shown is genuine, that the person or machine they are communicating with is who they say they are, and so on. A simple, yet powerful way to ensure trustworthiness across our digital globe.

No Strings Attached?

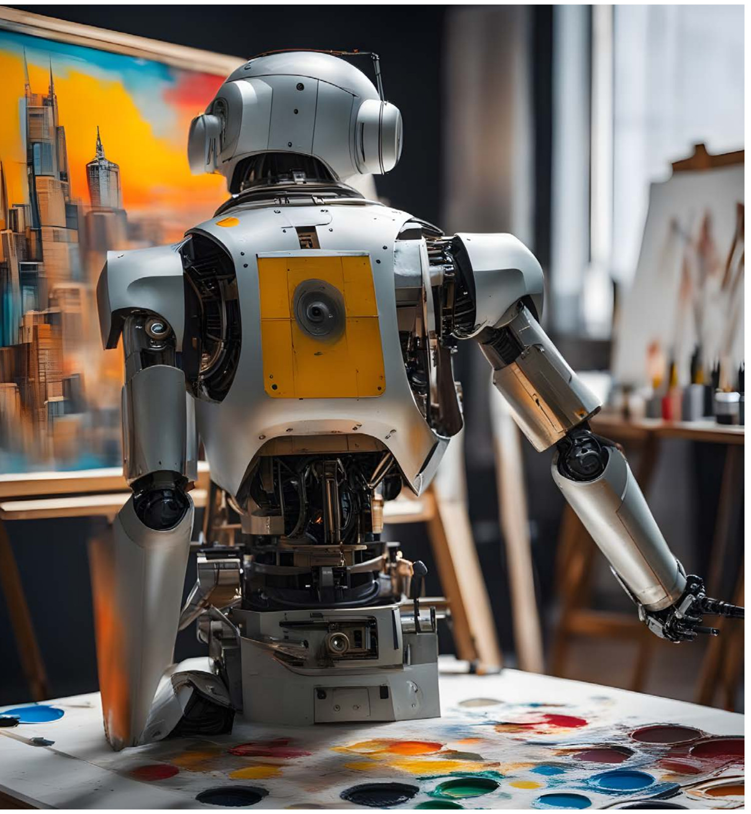
If certificates are such a great and universally accepted currency for authenticity and identity, why is the digital world not a haven of security and trustworthiness? Put simply: Digital certificates are the keys to our digital homes, vehicles, and safes. And as in the real world, even the highest walls, most complicated locks, or sturdiest safes will not guarantee security if we do not take care of our keys.

And like physical keys, keeping track of our digital certificates and keeping them secure can be a frustratingly complicated business. The private cryptographic keys that work the digital certificate wizardry must never be allowed to be lost, stolen, or otherwise tampered with. And it does not suffice to keep the digital certificates they are part of in a secure place. The private keys have to sometimes leave that safe space to be used in the cryptographic operations that make certificates do their jobs. Even if that moment is as brief as can be, a compromised system could allow an attacker to access that critical cryptographic data and get all they need to do their illicit work.

Sensible workflows, good compliance practices, and a bit of care and common sense would seem all that is needed to keep certificates secure, but that is far from true. It is not all due to human error – sophisticated hackers can find other technical means to crack even apparently safe systems – but human users often become the unwitting assistants of hackers by relying on unsafe practices or not doing their IT security homework.

Who has not shrugged off a warning message that a certificate has expired? Who among the vast masses of regular users, not trained IT professionals, understands what certificates do or how they can become problematic? As John Drewe found out when selling one of Myatt's forged Giacomettis to two art dealers: If a deal is attractive, but checking the paperwork (or, indeed, keeping your certificates up to date) is too much of a hassle, people will tell themselves that everything is alright, because it looks alright on the surface. People want to be deceived.

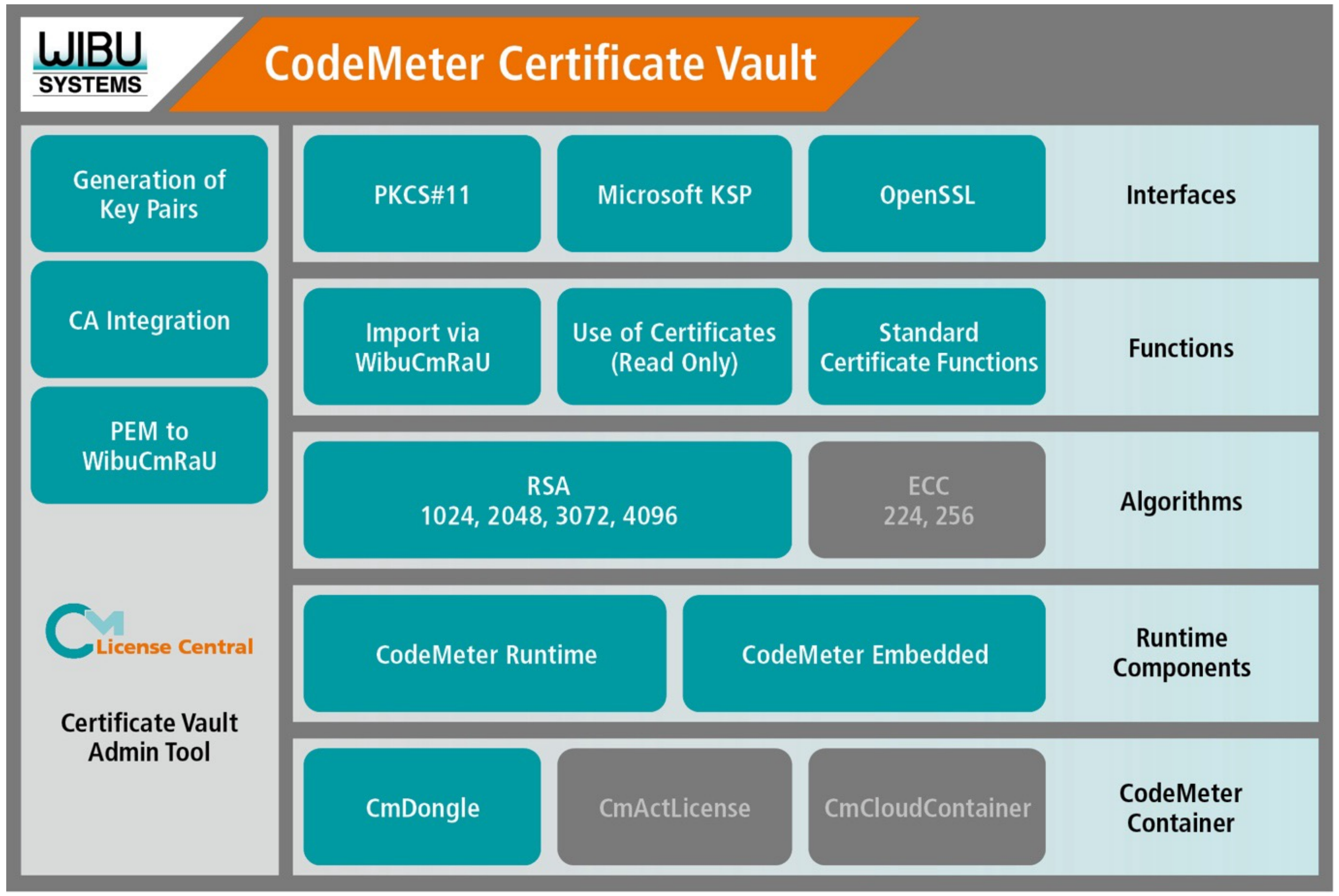
MARCO BLUME *has been with WIBU-SYSTEMS AG since 2013, as Product Manager/R&D Manager Embedded. His work covers the range of protection concerns for embedded systems and includes the development of custom concepts for manufacturers and contributions to active research ventures. He has spent his entire career with different embedded systems, including 11 years as product manager for the security of ATMs and checkout systems and previous responsibilities as embedded specialist for video systems and industrial automation..*



CodeMeter Certificate Vault: Removing the Weak Spots

Commercial certificate authorities or other sophisticated organizations have the means to protect their certificates with powerful hardware and software. Complex closed systems are used to store the certificates and cryptographic keys, and these normally never leave these secure enclaves as the necessary calculations and cryptographic operations can be run inside those systems, called Hardware Security Modules or HSMs. For less well-equipped organizations, let alone regular end users, this is not an option. They have to rely on less secure options to keep their certificates, or they had to until Wibu-Systems' launched CodeMeter Certificate Vault.

CodeMeter Certification Vault



WIBU SYSTEMS CodeMeter Certificate Vault

Generation of Key Pairs

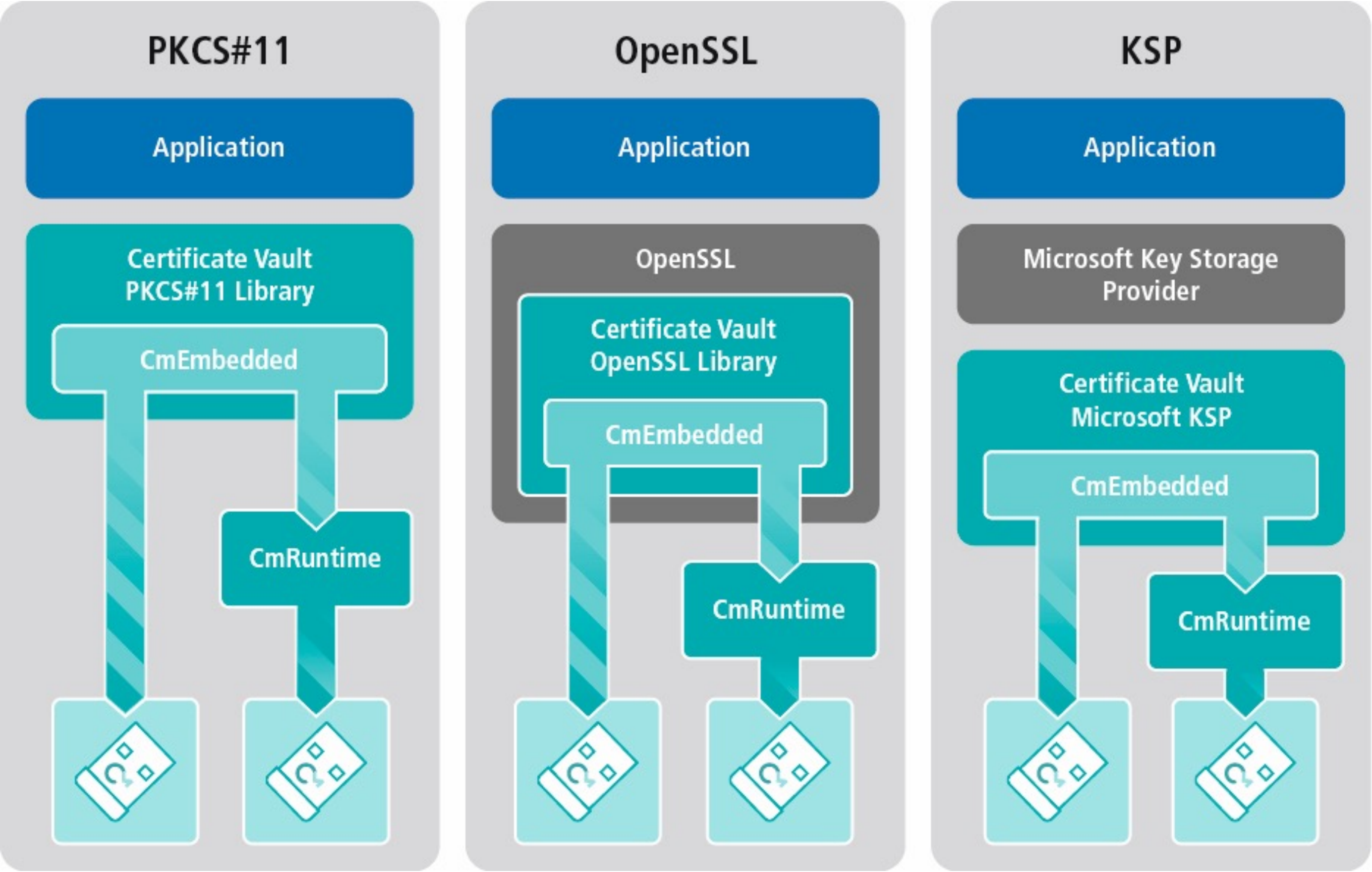
CA Integration

PEM to WibuCmRaU

License Central

Certificate Vault Admin Tool

PKCS#11	Microsoft KSP	OpenSSL	Interfaces
Import via WibuCmRaU	Use of Certificates (Read Only)	Standard Certificate Functions	Functions
RSA 1024, 2048, 3072, 4096		ECC 224, 256	Algorithms
CodeMeter Runtime	CodeMeter Embedded		Runtime Components
CmDongle	CmActLicense	CmCloudContainer	CodeMeter Container


PKCS#11
Application
Certificate Vault PKCS#11 Library
CmEmbedded
CmRuntime
OpenSSL
Application
OpenSSL
Certificate Vault OpenSSL Library
CmEmbedded
CmRuntime
KSP
Application
Microsoft Key Storage Provider
Certificate Vault Microsoft KSP
CmEmbedded
CmRuntime

CodeMeter Certificate Vault can be easily integrated into existing environments

CodeMeter Certificate Vault essentially lets regular users work with a slimmed-down version of an HSM: Certificates can be stored in secure hardware containers, so-called CmDongles in USB stick, memory card, or ASIC form factors, that come not just with a place to keep them, but even the Common Criteria EAL5+ evaluated smart card chip to run the cryptographic operations. One common standard used for that purpose is PKCS#11, which includes cryptographic algorithms like RSA and is the basis for X.509 certificates. CodeMeter Certificate Vault comes with the necessary PKCS#11 library for key storage purposes, as it does with the OpenSSL library (for securing network protocols) and with Microsoft Key Storage Provider, the Windows-specific means to manage certificates and keys for Windows applications. In all three cases, the critical jobs happen inside the secure dongle: the certificates either never leave the dongle at all or if they do, as is the case with Microsoft KSP, the private key remains hidden, and all cryptographic operations happen on the dongle.

Scan the QR Code to access a White Paper Executive Summary on CodeMeter Certificate Vault

In Practice

Whether certificates are used to identify a flesh-and-blood person or a machine in a network or to form a public key infrastructure (PKI), e.g. in email communication, CodeMeter Certificate Vault adds a new layer of security in the form of secure key storage and protected lines of communication. For human users, certificates stored on a CmDongle become more portable than ever before, not unlike the passports they resemble, which can be essential for many mobile projects or services and maintenance engineers that have to identify themselves. On the other end of the portability scale, a piece of equipment in a modern smart factory does not have to be moved around much, but it would be useless without a reliable and trustworthy certificate. In that case, a built-in CmASIC is the perfect, physically hidden-away container for that certificate.

In order to get a certificate onto the device where one needs it, the standard process works as it should, only with added CodeMeter security. For a new certificate, a key pair is created, but now by the CodeMeter chip and within the secure container. The key pair is used for the new certificate, which can now contain other identifying data about the container for added authenticity. The certificate is sent to a CA for signing and returned back into the container. During all of this, the private key never has to leave its safe home. (Figure.1)

One of the most critical moments in a certificate's life happens when an update comes around, as many Internet users will know from encountering websites with expired certificates. CodeMeter Certificate Vault again benefits from Wibu-Systems' experience with secure updating mechanisms, and the swapping of CSR and signed certificates again happens in a safe environment with no way for a would-be attacker to intercept anything of value in between: The private key stays inside the secure CodeMeter chip. (Figure. 2)

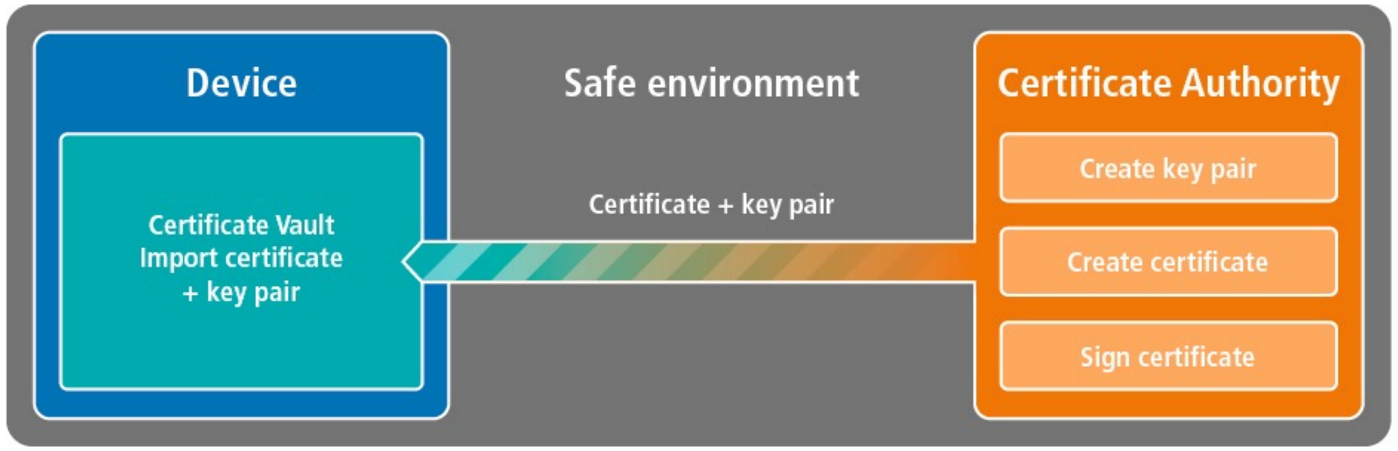
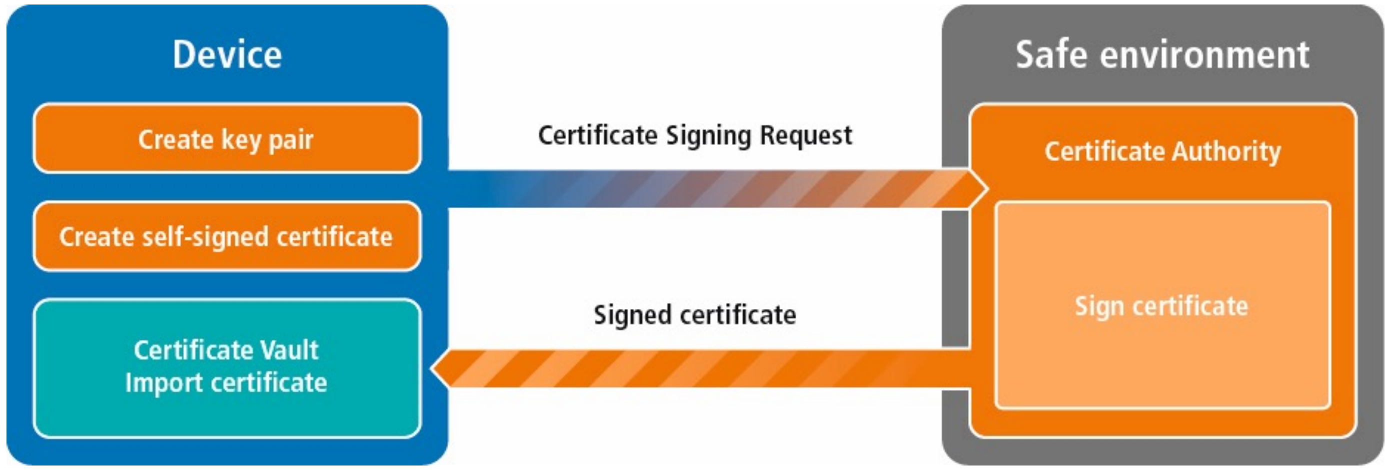


Figure. 1

Figure. 2



The secure updating process invented for CodeMeter licensing, swapping a special *.RaC update request and an encrypted *.RaU update file, works as well as an optional way to distribute new or updated certificates securely from the CA to their destination. (Figure. 3)

With CodeMeter Certificate Vault's on-board OpenSSL and PKCS#11 interfaces, all of these processes can be automated and completely taken out of the end user's hands for added reliability and easy supervision.

Conclusion: No excuses for poor practice

In a nutshell, CodeMeter Certificate Vault is the means to store and manage certificates in secure containers. But it is far more than that: As part of the CodeMeter ecosystem, CodeMeter Certificate Vault feels familiar to users of Wibu-Systems' powerful protection and licensing solution, working with hardware that is as smart as it is tough and offering a similar user experience built around comfort and flexibility coupled with powerful customization and integration capabilities.

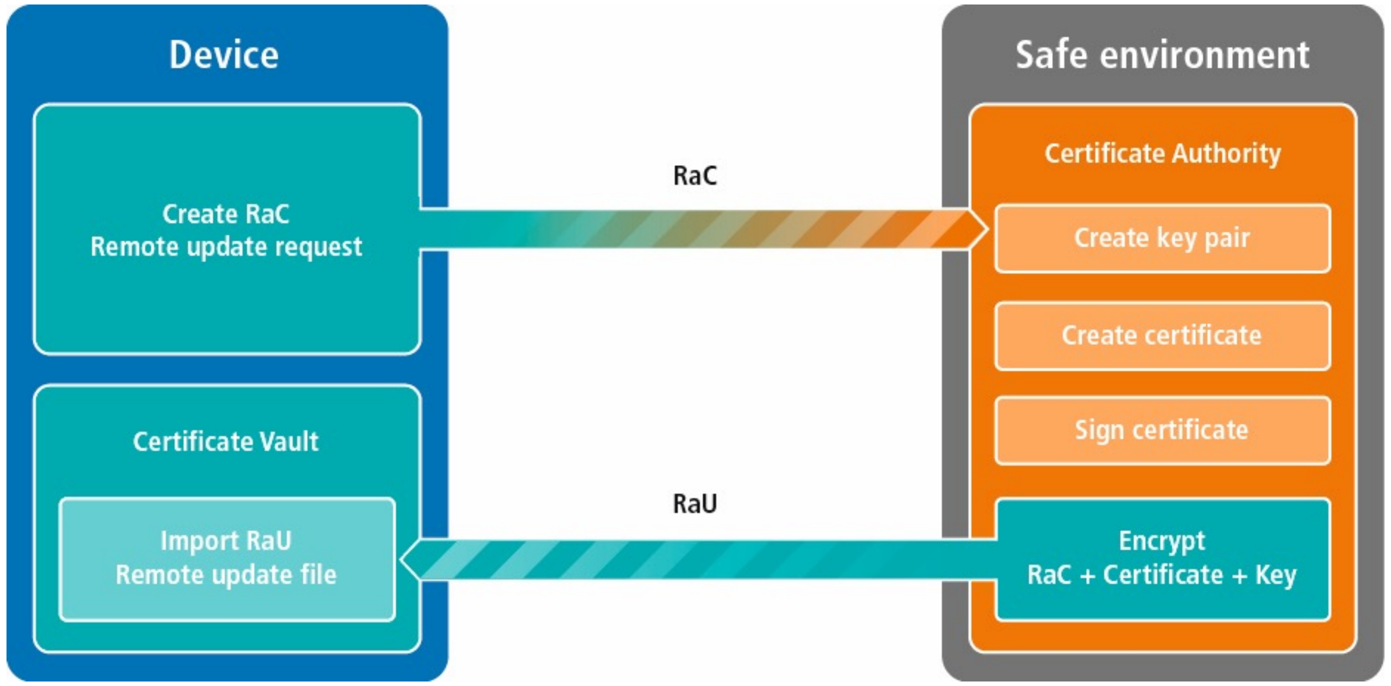
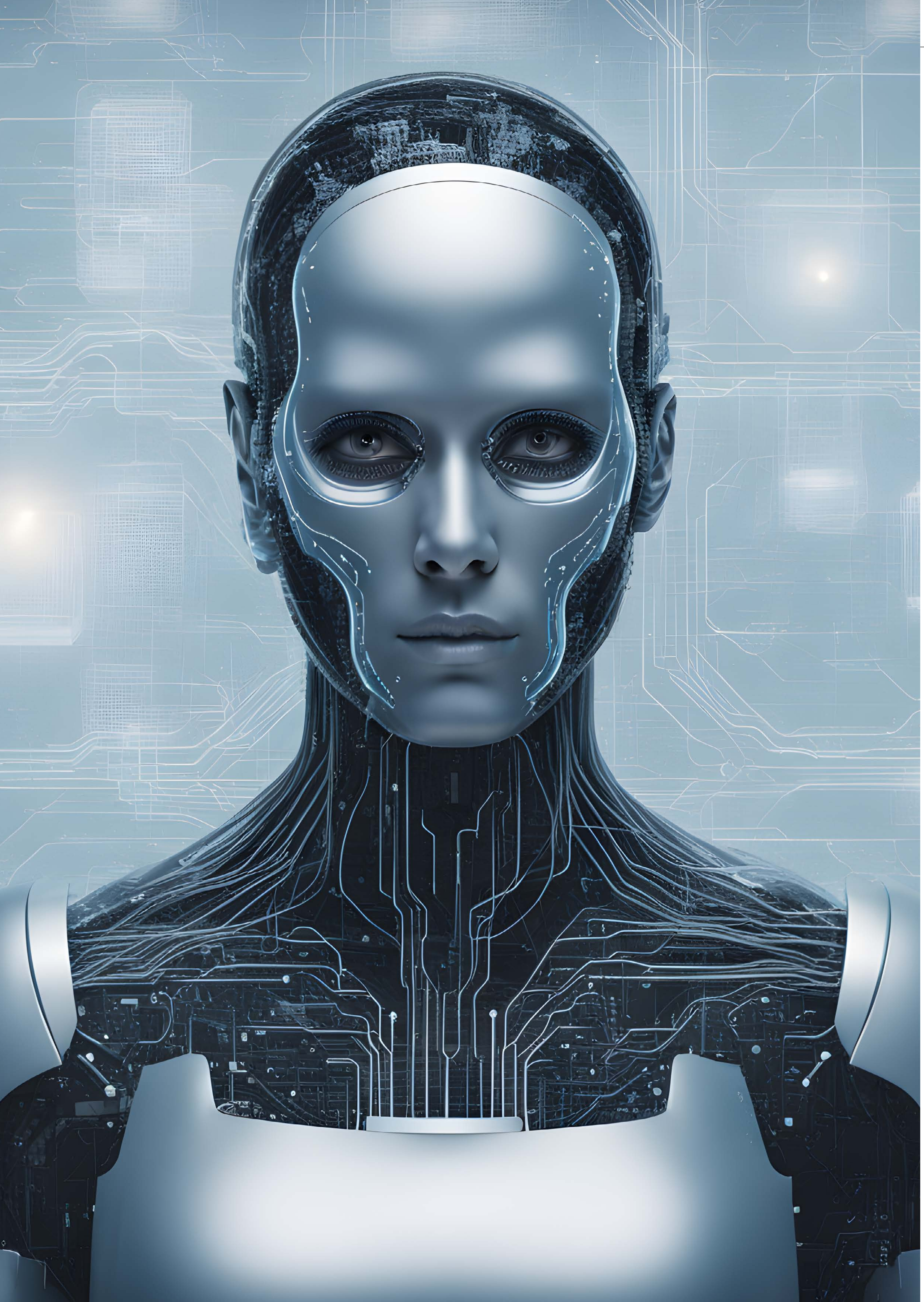


Figure. 3

CodeMeter Certificate Vault supercharges the CodeMeter universe with a solution for digital certificates that completes the IT security and protection line-up from encryption, protection, and licensing to authentication and secure communication. By removing many, if not most of the obstacles and problems caused by technology or human habit, it leaves no excuses for poor-practice certificate usage. The digital world will be more secure for it.

Postscript

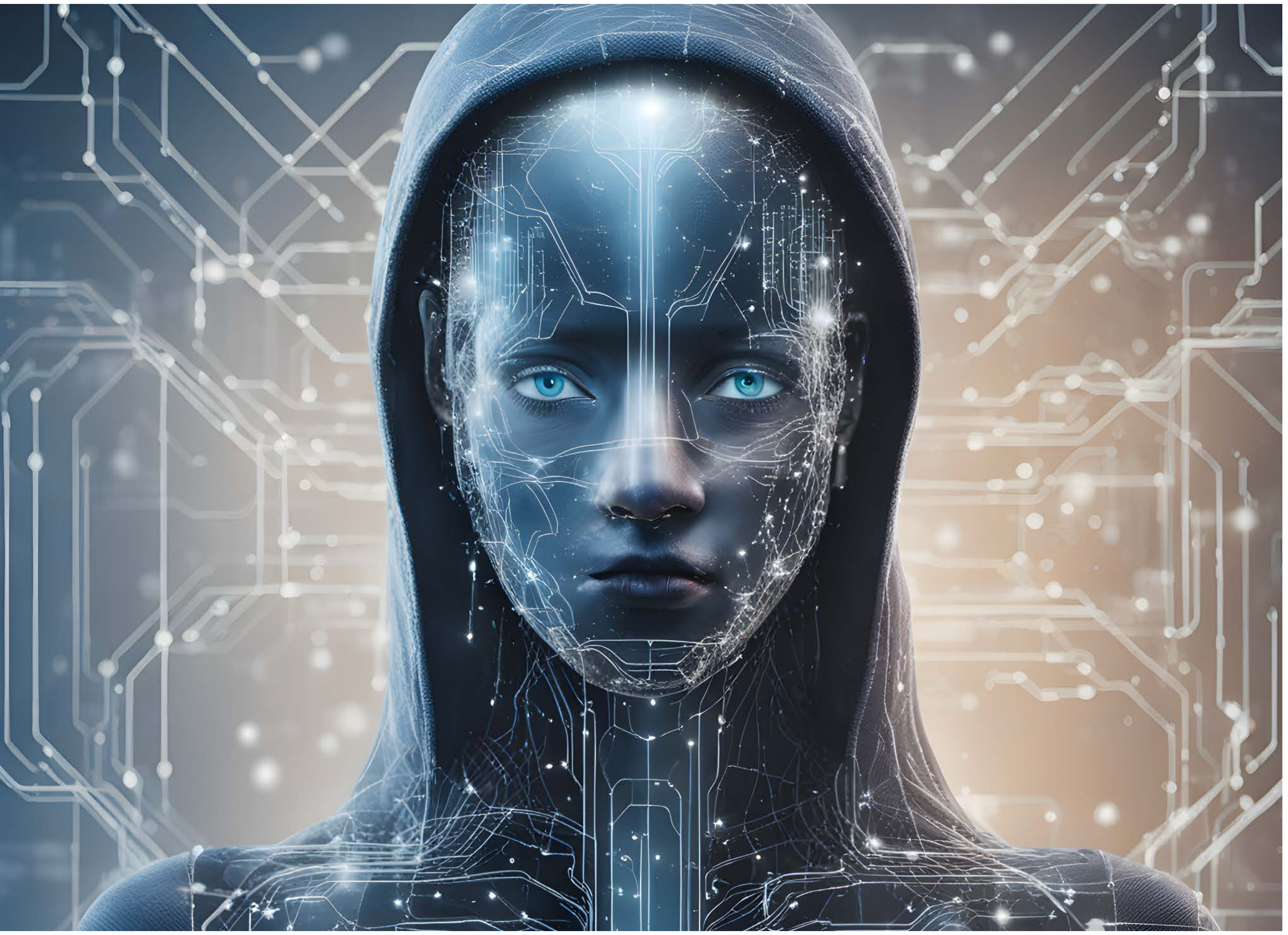
In 1999, John Myatt, art forger extraordinaire, was released from prison. He never stopped painting in the style of the great modern masters. Today, his works are sought after by collectors worldwide, not as the genuine article, but as – "genuine fakes".



UNMASKING the THREAT: AI and the Future of *DIGITAL IDENTITY*

By Steve Atkins, Silicon Trust

In today's hyper-connected world, the concept of digital identity has evolved from a mere convenience to an indispensable part of our daily lives. As we embrace the digital age, our identities are intricately tied to a complex web of online interactions, from social media accounts and online banking to e-commerce and government services. However, as we continue to digitize our lives, a growing concern emerges—the potential threat posed by artificial intelligence (AI) to our digital identities. This article delves into the technical intricacies of AI's threat to digital identity.



AI's Role in Digital Identity

AI technologies have advanced rapidly in recent years, and their impact on various sectors, including cybersecurity, has been profound. In the context of digital identity, AI plays a multifaceted role, both as a solution and a potential threat.

Biometric Authentication: AI has revolutionized biometric authentication, enhancing the security of digital identities. Facial recognition, fingerprint analysis, and voice recognition technologies powered by AI have made it difficult for unauthorized users to breach digital security.

Behavioural Analysis: AI-driven systems monitor and analyse user behaviour to detect anomalies. These behavioural biometrics approach adds an extra layer of security, helping to prevent unauthorized access to sensitive digital assets.

Personalized Services: AI-driven recommendation engines and personalized services use data from digital identities to enhance user experiences. This results in increased engagement, improved service quality, and, often, a deeper sense of attachment to one's digital identity.

The Threats Posed by AI

While AI bolsters the security of digital identity in many ways, it also raises legitimate concerns. Here are some key areas where AI poses a threat to digital identity, complete with specific (for the moment, fictional) examples:

1. **Deepfake Vulnerabilities.** Deepfake technology, driven by AI, has emerged as one of the most insidious threats to digital identity. Malicious actors can use AI algorithms to create convincingly realistic fake videos, audio recordings, or images, thereby putting unsuspecting individuals at risk. A well-known example is the case of deepfake audio of a CEO instructing a fraudulent wire transfer, leading to significant financial loss.
   Deepfake creation relies on a combination of Generative Adversarial Networks (GANs) and deep neural networks, enabling attackers to manipulate digital content with unparalleled precision. Such deepfakes can damage reputations, commit fraud, and compromise the integrity of digital identities.

2. **Spear Phishing and Social Engineering.** AI-powered spear phishing attacks have become increasingly sophisticated and targeted. By analysing vast datasets, AI can craft highly convincing messages or impersonate known contacts. For instance, an AI-driven spear phishing attack might impersonate a colleague, seeking confidential data or login credentials.
   AI-enhanced chatbots can engage in seemingly genuine conversations, adapting to user responses. This is illustrated in the case of a chatbot impersonating a tech support agent to trick users into revealing personal information, which can be used to compromise digital IDs.

3. **Predictive Analysis and Behaviour Profiling**
   Mofiles of individuals, known as behavioural biometrics. Such profiles can reveal sensitive personal information or patterns of behaviour, which attackers can then manipulate or misuse.
   For example, AI can predict a user's daily habits, online preferences, or even psychological vulnerabilities. Attackers may use this information to target users with customized phishing campaigns, leveraging insights derived from predictive analysis.

4. **Data Breach and Identity Theft.** AI plays a dual role in data breaches, both as a security measure and a threat. AI systems are increasingly used to detect and mitigate breaches. However, malicious actors are leveraging AI's capabilities to evade detection, exploit vulnerabilities, and steal data, including sensitive digital identity information. One notable case involved the use of AI to bypass security measures and gain unauthorized access to a healthcare database. The attackers extracted personal information, including social security numbers, posing a severe risk to the digital identities of thousands of individuals.

5. **Sophistication of AI Tools.** AI tools have become increasingly sophisticated, capable of mimicking human behaviour, generating convincing deepfakes, and automating attacks. As AI technology continues to advance, the threat it poses to digital ID grows.
   The seriousness of the threat is further exacerbated by the fact that attackers are increasingly using AI to enhance their malicious activities. Furthermore, the volume of sensitive personal data available online, often used to verify digital identities, provides ample opportunities for exploitation.

As well as being the CEO of Krowne Communications, **STEVE ATKINS** *is also the Program Director for the Silicon Trust and Editor of the VAULT magazine (covering hardware-based IC security, biometrics, contactless, blockchain and cloud-based technologies). Even with almost 35 years of experience in the high-tech industry, he is still fascinated with all kinds of technology and the impact it has upon end users. He is currently based in Berlin, Germany.*

Mitigating the Threats

To counter the threat, organisations are continually developing more advanced security measures, including AI-based solutions to detect and prevent AI-driven attacks. Multi-factor authentication, robust encryption, and user education are essential components of defence against AI-based threats to digital ID. Protecting your digital ID against the threat of malicious AI requires a multifaceted approach that combines advanced technology, security best practices, and user education. Here are several key strategies to safeguard your digital identity:

1. **Multi-Factor Authentication (MFA).** Implement MFA whenever possible. MFA requires users to provide multiple forms of verification before gaining access to an account or system, making it much harder for malicious actors to breach your digital identity.

2. **Deepfake Detection Algorithms:** Develop and deploy advanced deepfake detection algorithms that can identify manipulated media content. These algorithms often leverage image or video forensics and machine learning techniques.

3. **AI-Powered Threat Detection:** Utilize AI-driven threat detection systems capable of identifying malicious AI-driven attacks, such as spear phishing attempts and behaviour profiling.

4. **Privacy-Preserving AI:** Explore privacy-preserving AI techniques that allow data analysis while protecting sensitive user information, thereby reducing the risk of identity exposure.

5. **User Behaviour Analytics:** Implement user behaviour analytics tools that can identify anomalies and unauthorized access, safeguarding digital IDs against AI-driven attacks.

6. **Regular updates and patch systems.** Keep your software, operating systems, and security tools up-to-date to address known vulnerabilities. Malicious AI often targets outdated systems.

7. **Leverage Blockchain Technology.** Consider using blockchain-based solutions for digital identity verification, as they offer a high level of security and decentralization.

8. **Monitor and audit access and review and update policies.** Continuously monitor user access to sensitive data and audit access logs for suspicious activities. Automated AI-driven systems can help with real-time detection of anomalies. Familiarize yourself with privacy regulations and data protection laws, such as GDPR or CCPA, and ensure compliance with them in your digital identity practices. Keep your organization's security policies and procedures up-to-date to address evolving AI threats. Regularly review and revise these policies as needed.

The technical solutions and vigilance needed to combat these challenges are critical to safeguarding the digital identities of individuals and organizations alike. Balancing the benefits of AI with the need for safeguarding digital identities is an ongoing challenge that must be met with a combination of technology, regulation, and ethical considerations.

Conclusion

Artificial intelligence is a double-edged sword when it comes to digital identity. While it enhances security measures in many ways, it also presents new threats and challenges. As we navigate this evolving landscape, it is imperative for individuals and organizations to stay vigilant, adapt to emerging threats, and actively participate in the responsible development of AI technologies to ensure a secure and resilient digital identity ecosystem.

In summary, AI poses a significant and evolving threat to digital ID due to its ability to mimic human behaviour, generate convincing fake media, and automate attacks. As AI technology advances, the threat will continue to grow, making it imperative for individuals and organisations to remain vigilant and invest in robust security measures to protect their digital identities.

Could AI fool a Digital ID Verification Check?

AI has the potential to seriously impact digital ID verification checks, but it's important to distinguish between different aspects of digital ID verification and the capabilities of AI. Here are some key considerations:

Facial Recognition: *AI-driven facial recognition technology has advanced significantly and can accurately match a face to a registered digital ID or image. However, it is not fool-proof and can be tricked in some cases. For instance, determined attackers have used high-quality 3D printed masks or images to spoof facial recognition systems.*

Behavioral Biometrics: *AI can analyse a user's behavioural biometrics, such as typing patterns or mouse movements, to verify their identity. While these systems are robust, a sophisticated attacker who closely mimics the legitimate user's behaviour could potentially bypass them.*
Document Verification: AI-based document verification systems are highly effective at identifying forged or altered documents. However, if an attacker uses sophisticated methods to create convincing fake documents, these systems may struggle.

Voice Recognition: *AI can be used for voice recognition, which is generally reliable. But like facial recognition, attackers can use synthesized or manipulated audio to potentially fool these systems.*
Machine Learning Attacks: Attackers can also leverage AI and machine learning to learn and adapt to security measures over time. This makes it a constant cat-and-mouse game between those developing AI for verification and those trying to fool it.

It's important to note that AI's effectiveness in digital ID verification largely depends on the specific technology and the resources available to both the defenders and attackers. In practice, many digital ID verification systems use multiple layers of security, combining biometrics, document checks, behavioural analysis, and more to minimize the risk of impersonation.

To bolster security and reduce the risk of AI-based attacks, organizations often employ additional factors like multi-factor authentication (MFA) that include something the user knows (e.g., a password), something the user has (e.g., a physical token or mobile device), and something the user is (biometrics).

While AI has the potential to seriously impact digital ID verification, the ongoing advancement of security measures and AI detection systems makes it challenging for malicious actors to consistently and easily fool these checks. However, the threat is ever-evolving, and continuous improvements in AI-driven security are essential to staying one step ahead of potential threats. ☒

REVOLUTIONIZING SECURITY with *INFINEON'S Enhanced INTEGRITY GUARD 32*

By Robert Bach, Infineon Technologies

Discover the Future of Security:
the TEGRION™ Controller Family from Infineon
Redefines Efficiency, Performance, and Ease of
Implementation

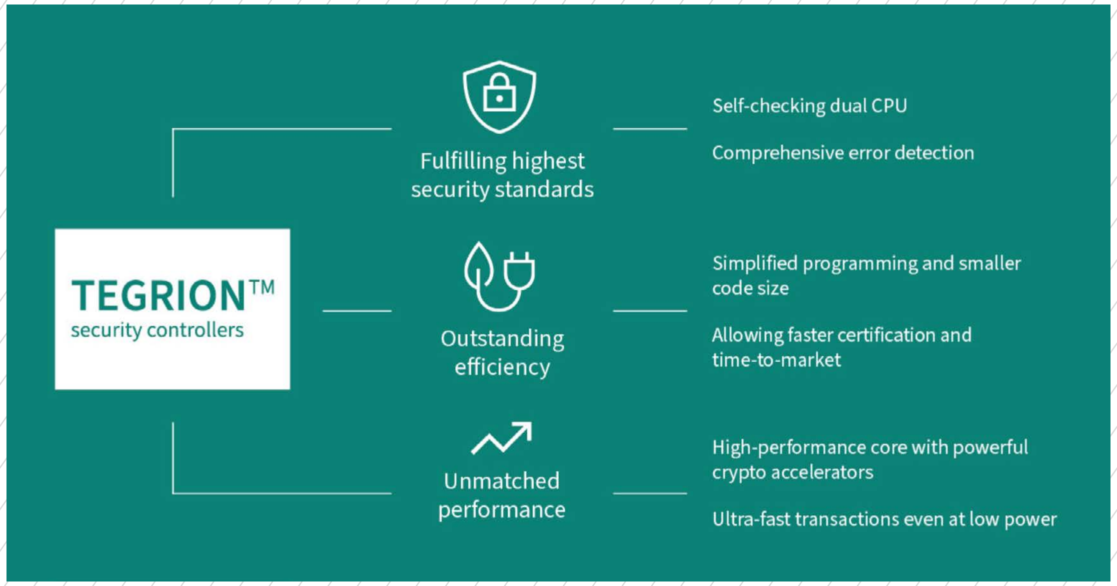
Infineon Technologies has introduced the TEGRION™ security controller family, a significant leap forward in security controller technology. At its core, this state-of-the-art family incorporates the ground-breaking Integrity Guard 32 security architecture and a powerful Arm® v8-M instruction set, promising unrivalled device performance.

But there's more to the story! TEGRION™ security controllers mark a ground-breaking shift for both developers and businesses alike. With seamless implementation and swift design integration, these controllers enable rapid time-to-market, providing a competitive advantage in the ever-evolving tech landscape. What truly sets TEGRION apart is its steadfast commitment to extended product lifecycles, enabling lasting device relevance in a world of ever-changing technology.

And the best part? The TEGRION™ security controller portfolio caters to a wide range of applications, from equipping smart homes and powering innovative smart mobility solutions to revolutionizing industries, facilitating secure payment systems, protecting identities, and enhancing lifestyles.

TEGRION™ boasts Infineon's exclusive Integrity Guard 32 hardware security architecture, a solution that greatly streamlines application development. It enables the design of security-centric conditions critical for the sustained success of both current and future connected applications. Integrity Guard 32 achieves elevated security levels without sacrificing performance and reliability. It adopts a holistic approach, seamlessly integrating the system's processing core, on-chip memories, buses, caches, crypto accelerators, and peripheral interfaces into a comprehensive security architecture.

Ioannis Kabitoglou, Senior Vice President & General Manager of Digital Security & Identity at Infineon, highlighted the company's long-term commitment to the security market with the launch of the TEGRION™ security controller family. He asserts, " By investing in and launching the TEGRION™ security controller family, Infineon is demonstrating its long-term commitment to the security market. It is the most powerful security controller family the company has ever launched. Based on the positive customer feedback, we are confident that the TEGRION™ security controller family will meet current and future security application requirements. And, as a matter of fact, our customers will be able to develop their operating systems much faster.”


TEGRION™ security controllers

Fulfilling highest security standards
- Self-checking dual CPU
- Comprehensive error detection

Outstanding efficiency
- Simplified programming and smaller code size
- Allowing faster certification and time-to-market

Unmatched performance
- High-performance core with powerful crypto accelerators
- Ultra-fast transactions even at low power

TEGRION™ features Infineon's unique Integrity Guard 32 hardware security architecture, which greatly simplifies application development. It allows design-for-security conditions that are critical to sustainable success of todays and tomorrow's connected applications. Integrity Guard 32 enables higher levels of security without compromising on performance and reliability. It is based on a holistic approach that integrates the system's processing core, on-chip memories, buses, caches, crypto accelerators and peripheral interfaces into a comprehensive security architecture.

> *“By investing in and launching the TEGRION™ security controller family, Infineon is demonstrating its long-term commitment to the security market. It is the most powerful security controller family the company has ever launched.*
>
> *– Ioannis Kabitoglou, Senior Vice President & General Manager Digital Security & Identity, Infineon*

Comprehensive Portfolio of TEGRION™ Security Controllers

Infineon's TEGRION™ offers a comprehensive portfolio of 28 nm security controllers, designed to excel in security, efficiency, performance, and ease of implementation across a wide range of secured and connected systems. By utilising Infineon's revolutionary Integrity Guard security architecture, TEGRION™ can now push the boundaries of hardware security while facilitating easy implementation, rapid design-in, and time-to-market readiness, all while supporting extended product lifetimes.

TEGRION™ security controllers combine a 32-bit high-performance CPU based on Arm® v8-M with the latest-generation crypto accelerators, power-optimized 28 nm technology, and advanced digital security technologies. Enjoy the benefits of Infineon's extensive range of next-generation security controllers, which are easy to program and design-in, thanks to an enhanced toolchain and a certified crypto suite.

High security, efficiency, and performance and a future-proof platform

TEGRION™ security controllers consistentwwWWwly deliver top-level security, speed, and performance, along with energy efficiency. Infineon's Integrity Guard digital security technology, combined with the Arm® v8-M core and powerful crypto accelerators, reaches the highest protection standards, fast communication speed, and ultra-low power consumption.

TEGRION™ security controllers are at the forefront of technological advancements. Built on the newest power-optimized 28 nm technology, TEGRION™ provides a future-proof security platform for various applications, including identity, payment, smart industry, smart mobility, smart home, and lifestyle.

ROBERT BACH comes along with a vast experience in the semiconductor industry for chip card IC´s. After finishing his university studies with a degree in industrial engineering and management at the technical university of Darmstadt, Germany he joined the Chip Card & Security IC group of Siemens AG, Germany in 1996. Mr. Bach has held various marketing and strategic marketing positions at Siemens and subsequently at Infineon Technologies AG. Currently, he is responsible for the semiconductor product marketing in the Product Line "Identity Solutions" within the Connected Secure Systems (CSS) division at Infineon.

Ease of implementation, robust support and reliable supply

TEGRION™ ICs significantly simplify and expedite software development and certification while enhancing security substantially. With a sophisticated toolchain, comprehensive crypto suites, mathematically modelled security, and a dedicated global support team, you can securely bring your project to market quickly and efficiently.

TEGRION™ security controllers build upon Infineon's extensive experience in the hardware security market, with more than three billion security controller ICs shipped annually. Infineon serves as the ideal and dependable high-volume supply partner for your long-term sourcing needs for next-gen, long-lifetime security controllers.

Infineon's TEGRION™ security controller family, featuring Integrity Guard 32, marks a breakthrough in digital security, offering unmatched performance, reliability, and adaptability for a wide range of applications. With its revolutionary architecture and commitment to long product lifecycles, TEGRION is poised to redefine the standards of digital security.

Explore more at www.infineon.com/tegrion.

SILICON TRUST DIRECTORY 2023

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.

Bundesamt
für Sicherheit in der
Informationstechnik

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

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 & MuteCards),
- "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

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

EVIDEN

Eviden designs the scope composed of Atos' digital, cloud, big data and security business lines. It will be a global leader in data-driven, trusted and sustainable digital transformation. As a next generation digital business with worldwide leading positions in digital, cloud, data, advanced computing and security, it brings deep expertise for all industries in more than 53 countries. By uniting unique high-end technologies across the full digital continuum with 57,000 world-class talents, Eviden expands the possibilities of technologies for enterprises and public authorities, helping them to build their digital future. Eviden is an Atos Group business with an annual revenue of c. € 5 billion.
www.eviden.com

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.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.
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, secureproducts 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

THALES

Thales is a global leader in advanced technologies within three domains: Defence & Security, Aeronautics & Space, and Digital Identity & Security. It develops products and solutions that help make the world safer, greener and more inclusive. The Group invests close to €4 billion a year in Research & Development, particularly in key areas such as quantum technologies, Edge computing, 6G and cybersecurity. Thales has 77,000 employees in 68 countries. In 2022, the Group generated sales of €17.6 billion.

www.thalesgroup.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

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