Quantenresistente Übertragung und lange Einsatzdauer – kein Widerspruch dank Kryptoagilität

Post-quantum cryptography and a long period of use – no objections thanks to crypto agility

Gunnar Preissler | Andreas Hinterschweiger | Klaus Schmeh

Komponenten der Leit- und Sicherungstechnik (LST), die in Eisenbahnsystemen zum Einsatz kommen, sind oft Jahrzehnte in Betrieb und müssen zukünftig stets aktuelle kryptografische Verfahren nutzen. Da derzeit verbreitete Kryptoalgorithmen wie RSA oder Diffie-Hellman irgendwann mit einem Quantencomputer gebrochen werden könnten, muss es vor allem möglich sein, bei Bedarf auf Post-Quanten-Verfahren umzustellen. Gesucht sind innovative Ansätze. Dieser Beitrag stellt ein nachhaltiges Konzept auf Basis kryptoagiler Lösungen vor.

1 EULYNX

In den europäischen Schienennetzen besteht ein erheblicher Modernisierungsbedarf, zumal die Anforderungen an den Schienenverkehr in der nahen Zukunft weiter steigen werden. Die Überalterung der Bestandstechnik spielt als Ursache hierbei genauso eine Rolle wie der Fachkräftemangel für Betriebs- und Wartungsaufgaben und die angestrebte Verdopplung des Schienenverkehrs auf den bestehenden Verkehrswegen – um nur die wichtigsten Gründe zu nennen.

Hand in Hand mit der bautechnischen Erneuerung der Eisenbahninfrastrukturen geht die Digitalisierung der gesamten LST einher. In diesem Zusammenhang haben die europäischen Betreiber von Eisenbahn-Infrastruktur 2014 gemeinschaftlich eine proaktive Rolle eingenommen und mit EULYNX eine Initiative gegründet, die die Entwicklung einheitlicher Industriestandards für digitale Stellwerkstechnik zum Ziel hat. Mit der Einführung digitaler Stellwerke gelingt es unter anderem, die Vielfalt an unterschiedlichen Bedienplätzen zu reduzieren und damit den Aufwand für die Schulung des Personals, das Bevorraten unterschiedlicher Ersatzteile und somit die operativen Aufwände zu senken.

Die Digitalisierung der LST setzt auch eine Anpassung der Risikobetrachtungen und der davon abgeleiteten Schutzmaßnahmen voraus. Dabei ist zwischen Safety (Schutz vor unabsichtlichen Störungen) und Security (Schutz vor absichtlichen Manipulationen) zu unterscheiden. Die Safety ist in den aktuellen Komponenten, Geräten und Systemen umfassend implementiert.

2 Informationssicherheit in EULYNX-Systemen

Die fortschreitende Digitalisierung erfordert, dass zukünftig auch die Informationssicherheit einen hohen Stellenwert erhält. Sie erlangt ein höheres Gewicht, da nun vermehrt auch die Sicherheit von Software, Hardware und Informationen berücksichtigt werden muss. Die EULYNX-Mitglieder haben hierzu ein Positionspapier entwickelt, in dem erklärt wird, wie ein herstellerneutrales Framework

The control and safety components used in railway systems have often been in operation for decades and will have to use up-to-date cryptographic methods in the future. Since currently widespread crypto algorithms such as RSA or Diffie-Hellman could be broken with a quantum computer at some point, it must be possible to switch to post-quantum methods if necessary. Innovative approaches are therefore being sought. This article presents a sustainable concept based on crypto-agile solutions.

1 EULYNX

There is a significant need for modernisation in Europe's rail networks, especially as the demands on rail transport are set to increase in the near future. The obsolescence of existing technology plays just as significant a role as the shortage of skilled workers for operation and maintenance tasks and the targeted doubling of rail traffic on existing transport routes, to name but the most important reasons.

The digitalisation of the entire control and safety technology goes hand in hand with the structural renewal of the railway infrastructure. Within this context, the European railway infrastructure operators jointly played a proactive role and founded EULYNX in 2014, an initiative aimed at developing uniform industry standards for digital interlocking technology. The introduction of digital interlockings has enabled, amongst other things, a reduction in the variety of different operating stations, as well as reduced costs for personnel training and stocking different spare parts, meaning reduced operating expenses in general.

The digitalisation of control and safety technology also requires the adaptation of the risk assessments and the protective measures derived from them. A distinction must be made between safety (protection against accidental interference) and security (protection against deliberate manipulation). Safety has been comprehensively implemented in the current components, devices and systems.

2 Information security in EULYNX systems

Advancing digitalisation means that information security will also have to be given a high priority in the future. It is becoming increasingly important, because software, hardware and information security must also now be considered. To this end, EULYNX members have developed a position paper that explains how a vendor-neutral framework of security features and func-

von Security-Leistungsmerkmalen und -Funktionen als Ergänzung zur Safety implementiert werden kann. Ein besonderes Augenmerk gilt hierbei der Rückwirkungsfreiheit der Security auf die Safety.
Eine wichtige Rolle innerhalb der Security und speziell der Informationssicherheit spielt die kryptografische Absicherung der digitalen Kommunikation. Sie hat in diesem Zusammenhang folgende Ziele:

- Authentizität: Es darf für einen Angreifer nicht möglich sein, falsche Anweisungen zu verschicken, da dies beispielsweise das Verstellen einer Weiche oder eines Signals zur Folge haben kann. Der Authentizität kommt daher eine hohe Bedeutung zu.
- Integrität: Ein Angreifer darf nicht die Möglichkeit haben, eine Nachricht zu manipulieren, da dies ebenfalls gefährliche Eingriffe in den Schienenverkehr erlauben würde. Auch die Integrität hat in diesem Zusammenhang daher eine hohe Bedeutung.
- Vertraulichkeit: Die Vertraulichkeit der Kommunikation zwischen Komponenten des Schienennetzes wird angestrebt, ist den vorstehenden Schutzzielen jedoch nachgeordnet.

Da sich die Sicherheitseinschätzung der gängigen Kryptoverfahren im Laufe der kommenden Jahrzehnte zweifellos ändern wird, muss es möglich sein, diese Algorithmen zu aktualisieren oder ganz auszutauschen. Man spricht hierbei von Kryptoagilität. Diese ist auch und gerade für die Umstellung auf Post-Quanten-Verfahren notwendig, die voraussichtlich in den nächsten zehn Jahren stattfinden muss [1]. Hintergrund ist, dass gängige Kryptoalgorithmen wie RSA oder Diffie-Hellman mit einem leistungsfähigen Quantencomputer gebrochen werden können. Zwar wird es noch eine Weile dauern, bis Geräte dieser Art mit entsprechender Rechenstärke verfügbar sind, doch die Umstellung auf quanten-resistente Verfahren (also auf Post-Quanten-Kryptografie) sollte sicherheitshalber bereits jetzt beginnen. Die Standardisierung von Post-Quanten-Verfahren läuft derzeit auf Hochtouren, erste Produkte mit Post-Quanten-Unterstützung sind schon erhältlich.
Allgemein gesprochen wird eine kryptoagile Realisierung der verwendeten Sicherheitslösungen die kommenden Investitionen in Gleisfeldkomponenten schützen. Eventuelle Sicherheitslücken in den genutzten Kryptoverfahren werden nicht dazu führen, dass gänzlich neue Komponenten ins Feld gebracht werden müssen.

3 Kryptoagilität für EULYNX

Die Unternehmen Eviden und Westermo haben in einer Arbeitsgemeinschaft eine Kryptolösung entwickelt, die die Anforderungen der EULYNX-Variante A kryptoagil umsetzt und einen neuen Weg zur langfristig wirtschaftlichen Nutzbarkeit bietet (Bild 1). Diese Lösung kann auch auf Object-Controller übertragen werden, die der EULYNX-Variante B entsprechen und bei vergleichbaren Anwendungsfällen für Komponenten des Rolling Stock, beziehungsweise für OT-Anwendungen in anderen Branchen genutzt werden.
Eviden ist ein weltweit führender Anbieter für Cybersecurity mit einem umfangreichen Portfolio an patentierten Technologien für sichere digitale Identitäten, Vertraulichkeit, Advanced Computing, Künstliche Intelligenz (KI), Cloud und digitale Transformation [2].
Die Westermo Gruppe mit Hauptsitz in Västerås (Schweden) ist ein weltweit agierender Spezialist für industrielle Datenkommunikation [3]. Unter anderem bietet das Unternehmen ein komplettes Sortiment an Netzwerkprodukten für Bahnunternehmen mit den entsprechenden Zulassungen an, wie beispielsweise EN 50121 für die elektromagnetische Verträglichkeit für alle Komponenten im Eisenbahnbereich, und ist für lange Produktlebenszyklen bekannt.
Die Arbeitsgemeinschaft hat die nach EN 62443 entwickelten Switches von Westermo für die Umsetzung der Security Implementierung in der Bauform Cyptobox EULYNX-Variante A ausgewählt. Die-

tions can be implemented as a complement to safety. Particular attention has been paid to ensuring that the security has no repercussions on safety.
The cryptographic protection of digital communication plays a significant role in security and especially in information security. It has the following objectives within this context:

- Authenticity: it must be impossible for an attacker to send any false instructions, as this could result in the setting of a switch or a signal, for example. Authenticity is therefore of immense importance.
- Integrity: an attacker must be unable to manipulate any messages, as this would also allow dangerous interference in rail traffic. Integrity is therefore also of great importance within this context.
- Confidentiality: the confidentiality of the communications between the rail network components is desirable, but subordinate to the aforementioned protection objectives.

Since the security assessment for the common crypto procedures will undoubtedly change over the coming decades, it must also be possible to update or replace these algorithms completely. This is referred to as crypto agility. This is also especially necessary for the conversion to any post-quantum methods, which will probably have to take place in the next ten years [1]. The background to this lies in the fact that common crypto algorithms such as RSA or Diffie-Hellman can be broken using a powerful quantum computer. Although it will still be a while before devices of this type with the appropriate computing power become available, the switch to quantum-resistant methods (i.e. to post-quantum cryptography) should begin now to be on the safe side. The standardisation of post-quantum methods is currently in full swing and the first products with post-quantum support are already available.
Generally speaking, a crypto-agile implementation of the used security solutions will protect any upcoming investments in trackside components. The existence of any security gaps in the applied crypto methods will not lead to the need to introduce completely new components to the field.

3 Crypto agility for EULYNX

A joint venture between the Eviden and Westermo companies has developed a crypto solution that has implemented the requirements of EULYNX variant A in a crypto-agile way and offers a new path to long-term economic use (fig. 1). This solution can also be transferred to object controllers that correspond to EULYNX variant B and are used for rolling stock components or for OT applications in comparable use cases in other industries.
Eviden is a global leader in cybersecurity with an extensive portfolio of patented technologies used for securing digital identities, confidentiality, advanced computing, AI (Artificial Intelligence) and cloud and digital transformation [2].
The Westermo Group, headquartered in Västerås (Sweden), is a global specialist in industrial data communication [3]. Amongst other things, the company offers a complete range of network products for railway companies with the appropriate approvals, such as EN 50121 for the electromagnetic compatibility of all the components in the railway sector, and it is known for its long product lifecycles.
The consortium has opted for Westermo's switches developed according to EN 62443 for the implementation of the security implementation in the Cyptobox EULYNX variant A design.

Bild 1: Das eingesetzte Krypto-Netzwerk-Modul (links) wird mit einem HSM im microSD-Format (rechts) betrieben. Das HSM ist austauschbar, wodurch unter anderem neue Krypto-Algorithmen eingespielt werden können.
Fig. 1: The used crypto network module (left) is operated with an HSM in microSD format (right). The HSM is interchangeable, which means that new crypto algorithms can be imported, amongst other things.
Quelle / *Source*: Westermo (left part) and Eviden (right part)

se Geräte werden bereits heute in verschiedenen Anwendungsszenarien bei elektronischen Stellwerken verwendet.

4 Austauschbare Module

Um die digitale Kommunikation im Gleisfeld absichern zu können, werden die verwendeten Layer-3-Switches um Kryptofunktionen erweitert. Hierzu werden die Geräte mit austauschbaren Hardware Security Modulen (HSM) von Eviden ausgestattet, die in der Bauform von microSD-Karten eingesetzt werden. In ähnlicher Verwendung werden die microSD Karten bereits seit Jahren im deutschen Fiskalmarkt genutzt. Der kryptografische Kern der verwendeten HSM ist gemäß Common Criteria EAL 4+ zertifiziert.
Die Kryptoagilität der Sicherheitsgateways wird durch ein mehrstufiges Konzept gewährleistet, das Nachteile vermeidet, die durch die Obsoleszenz fest verbauter Security-Module entstehen. Die verwendeten microHSM ergänzen Fähigkeiten und Funktionen, die Netzwerkkomponenten bzw. vergleichbare Geräte ohne Kryptofunktionen nicht besitzen oder die zum Zeitpunkt der Herstellung des Gerätes technologisch noch nicht verfügbar waren. Man kann durch die Verwendung von microHSM nun mehrere Lebenszyklen für die Geräte erreichen. Dies gilt sowohl in Bezug auf die zugrundeliegende Software als auch auf deren Hardware. Dies ist ein erheblicher Vorteil, da die Anpassungsfähigkeit der Kryptofunktionen in den Geräten sonst zum limitierenden Faktor ihrer Nutzungsdauer wird.
Das microHSM arbeitet komplementär zu den intrinsischen Security-Funktionen des Netzwerkmoduls – z. B. zu denen, die mithilfe des Trusted Platform Modules (TPM) realisierbar sind. Ein TPM ist ein in zahlreichen PC, Smartphones und anderen Geräten fest eingebauter Hardware-Chip, der etwa die Leistungsfähigkeit einer Chipkarte aufweist. Ein TPM ist bewusst so konstruiert, dass es nicht ohne Weiteres vom zugehörigen Gerät entfernt werden kann. Dies bietet zwar einige Vorteile, steht jedoch dem Wunsch nach Kryptoagilität entgegen.
Das TPM kann jedoch ein HSM in einigen Punkten ergänzen. So lässt sich ein TPM durch die Nutzung von manipulationssicheren Hashwerten (digitaler Fingerabdruck) für den Schutz vor Malware-Angrif-

These devices are already being used in various application scenarios for electronic interlockings.

4 Replaceable modules

In order to be able to secure digital communication in the trackside environment, the Layer 3 switches will be expanded to include crypto functions. For this purpose, the devices will be equipped with interchangeable hardware security modules (HSM) from Eviden, which are used in the form of microSD cards. MicroSD cards have been used in a similar way in the German fiscal market for years. The cryptographic core of the used HSM has been certified according to Common Criteria EAL 4+.
The crypto agility of the security gateways is ensured by a multi-level concept that avoids the disadvantages caused by the obsolescence of any permanently installed security modules. The used microHSM complements the capabilities and functions that network components or comparable devices without crypto functions do not possess or that were not yet technologically available at the time the device was manufactured. The use of microHSM makes it possible to achieve multiple lifecycles for the devices. This applies to both the underlying software and its hardware. This is a significant advantage, as otherwise the adaptability of the crypto functions in the devices becomes a limiting factor for their useful life.
The microHSM works in a complementary way to the intrinsic security functions of the network module – for example, those that can be implemented with the help of the Trusted Platform Module (TPM). A TPM is a hardware chip that is permanently installed in numerous PCs, smartphones and other devices and has the performance of a chip card. A TPM is deliberately designed in such a way that it cannot be easily removed from the associated device. While there are some benefits to this, it runs counter to the desire for crypto agility.
However, a TPM can complement an HSM in a number of ways. For example, a TPM can be used to protect against malware at-

fen einsetzen. Außerdem kann es sichere Firmware-Updates durch digitale Signaturen absichern, wobei es sich empfiehlt, ein hashbasiertes Signaturverfahren (z. B. XMSS) zu nutzen. Hashbasierte Signaturverfahren sind quantensicher und nach Ansicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) so gut verstanden, dass keine anderweitigen Sicherheitslücken zu erwarten sind [4]. Hashbasierte Signaturverfahren sind zwar für den Alltagsgebrauch nicht praktikabel, jedoch für ein Firmware-Update, das nur in größeren Intervallen stattfindet, durchaus geeignet.

5 Aktualisierbarkeit erhöht die Sicherheit

Die Aktualisierbarkeit der im microHSM verwendeten Softwarekomponenten beschränkt sich jedoch nicht auf kryptografische Verfahren. Die Architektur des microHSM ermöglicht es vielmehr auch, eigenständige Software-Upgrades für die Sicherheitsmodule durchzuführen. Die Safety-Funktionen im Host-System bleiben hierbei unverändert, was eine deutliche Senkung des Aufwandes für Test und Evaluierung zur Folge hat.
Ein weiterer Vorteil, den ein austauschbares microHSM bietet: Während die Cryptobox EULYNX A über längere Zeit unverändert in Betrieb bleiben kann, lässt sich das microHSM bei Bedarf auf einfache Weise austauschen. Auf diese Weise kann ein neuer Prozessor, ein neues Security-Modul oder eine neue Firmware eingebracht werden. Ein solches modulares Hardware-Upgrade erfordert deutlich weniger Aufwand als ein kompletter Austausch des jeweiligen Geräts – auch deshalb, weil der Wechsel einer microSD-Karte sehr einfach zu bewerkstelligen ist.
Die von der Arbeitsgemeinschaft entwickelten Geräte unterstützen zur Verschlüsselung und Authentifizierung das IPsec-Protokoll mit IKEv2 für den Schlüsselaustausch. Es wird somit auf eine bewährte und standardisierte Technik gesetzt. Die Verschlüsselungsparameter entsprechen der TR-02102-3 des BSI [5], die Empfehlungen für die Verwendung von kryptografischen Mechanismen in den Protokollen IPsec und IKE gibt und dabei auf die Technische Richtlinie TR-02102-1 (Kryptographische Verfahren: Empfehlungen und Schlüssellängen) verweist [6]. Ziel der Anschlussprojekte ist eine tiefere Integration in die Softwarearchitektur der Object-Controller und die Verschlüsselung auf Basis von TLS 1.3.

tacks by using tamper-proof hash values (digital fingerprints). In addition, it can secure firmware updates with digital signatures, although it is recommended to use a hash-based signature method (for example, XMSS). Hash-based signature methods are quantum-secure and, according to the Federal Office for Information Security (BSI), they are so well understood that no other security vulnerabilities are to be expected [4]. Even though hash-based signature methods are not practical for everyday use, they are quite suitable for firmware updates that only take place at longer intervals.

5 Upgradeability increases security

However, the upgradability of the software components used in the microHSM is not limited to cryptographic methods. The architecture of the microHSM also makes it possible to carry out stand-alone software upgrades to the security modules. The safety functions in the host system remain unchanged, which results in a significant reduction in the costs required for testing and evaluation.
Another advantage of a replaceable microHSM lies in the fact that the microHSM can be easily replaced if necessary, while the Cryptobox EULYNX A can remain in operation unchanged for a longer period. In this way the microHSM can be updated with for example a new processor, a new security module or a new firmware. Such a modular hardware upgrade requires significantly less cost than the complete replacement of the respective device – also because changing a microSD card is very easy to do.
The devices developed by the consortium support the IPsec protocol with IKEv2 for the key exchange with encryption and authentication. Thus, a proven and standardised technology has been used. The encryption parameters correspond to the BSI's TR-02102-3 [5], which provides recommendations for the use of cryptographic mechanisms in the IPsec and IKE protocols and refers to Technical Guideline TR-02102-1 (Cryptographic Methods: Recommendations and Key Lengths) [6]. The follow-up projects aim to achieve deeper integration into the software architecture of the object controllers and encryption based on TLS 1.3.

6 Eine anspruchsvolle Aufgabe

Die Implementierung von Security-Maßnahmen in das System Eisenbahn ist ein äußerst anspruchsvolles Vorhaben. Zu den Herausforderungen gehört nicht nur die große Zahl der Komponenten und deren jahrzehntelanger Einsatz, der Kryptoagilität erfordert. Die zum Einsatz kommenden Lösungen müssen zudem zugleich die notwendige Sicherheit und einen möglichst effektiven Betrieb ohne größeren Wartungsaufwand gewährleisten. Ein wichtiges Ziel ist es, diese Anforderungen mit Standard-Technologien wie der selektiven Anlehnung an die IEC62443 zu erreichen und branchenspezifische Entwicklungen zu vermeiden.

Da eine Eisenbahninfrastruktur stets eine große Zahl an Komponenten umfasst, die geografisch weit verteilt sind, muss es zudem möglich sein, die verwendete Technologie zentral und ganzheitlich zu steuern. Onboarding- und Roll-Out-Mechanismen für das automatisierte Einbinden von neuen (unkonfigurierten) Geräten sind für diesen Zweck ebenso notwendig wie ein vollständiges Lifecycle-Management der Komponenten, das von der Produktion bis zur Entsorgung reicht. Das in RFC 8995 beschriebene BRSKI-Protokoll (Bootstrapping Remote Secure Key Infrastructure) in Verbindung mit dem in RFC 7030 spezifizierten EST (Enrollment over Secure Transport) bietet hierfür eine sichere und komfortable Lösung, die auf der Kombination von Hersteller-Vertrauensankern und PKI (Public Key Infrastructure)-Zertifikaten des Infrastrukturbetreibers basiert. Auch für die notwendigen Update- und Patch-Prozesse sowie für den Tausch defekter Geräte bietet die Integration in die PKI viele Vorteile.

Funktionale Safety-Updates an den Object-Controllern sind heutzutage langfristig geplante Projekte in mehrjährigen Zyklen. Aus Sicht der Security wird es jedoch zukünftig notwendig sein, Update-Intervalle zu verkürzen und kurzfristig durchzuführende Patches bzw. Updates vorzusehen – wenn beispielsweise eine Sicherheitslücke bekannt wird. Es ist wichtig, dass alle Beteiligten die Erhaltung der Security als vitalen Lebensprozess des Gesamtsystems verstehen, ebenso wie Essen oder Trinken tägliche Notwendigkeiten für uns sind.

Die Kombination der Kryptoagilität mit bewährten, langlebigen Komponenten ist ein richtungsweisender Ansatz für die Sicherheit und Managebarkeit von Kommunikationsnetzen im Umfeld Kritischer Infrastrukturen. Insbesondere auch in Hinblick auf die langen Lebenszyklen in diesen Bereichen und auf die damit verbundene Gesamtkostenrechnung bietet das Konzept optimale Möglichkeiten. ■

6 A challenging task

The implementation of security measures in the railway system is an extremely demanding undertaking. The challenges involve more than just the large number of components that require crypto agility and their decades of use. At the same time, the applied solutions must also ensure the necessary safety and the most effective operations possible without any major maintenance costs. An important goal lies in achieving these requirements using standard technologies such as selective alignment with IEC62443 and avoiding any industry-specific developments.

Since a railway infrastructure always includes a large number of components that are geographically widely distributed, it must also be possible to control the used technology both centrally and holistically. Onboarding and roll-out mechanisms for the automated integration of new (unconfigured) devices are just as necessary for this purpose as the complete lifecycle management of the components, ranging from production to disposal. The BRSKI protocol (Bootstrapping Remote Secure Key Infrastructure) described in RFC 8995 in conjunction with EST (Enrolment over Secure Transport) specified in RFC 7030 provides a secure and convenient solution based on the combination of vendor trust anchors and PKI certificates from the infrastructure operator. Integration into PKI also offers many advantages for the necessary update and patch processes as well as for the replacement of defective devices.

Nowadays, functional safety updates on object controllers are long-term projects that take place in multi-year cycles. From a security point of view, however, it will be necessary to shorten the update intervals in the future and to enable patches or updates to be carried out at short notice if, for example, a security vulnerability becomes known. It is important that all the involved parties understand the maintenance of security as a vital life process in the overall system, just as eating or drinking are daily necessities for us.

Combining crypto agility with proven, long service-life components is a game-changing approach to the security and manageability of communications networks around critical infrastructures. The concept offers optimal possibilities, especially with regard to the long lifecycles in these areas and the associated total cost accounting. ■

LITERATUR | LITERATURE

[1] PQC Migration Guide. The essentials. Eviden 2023. https://www.cryptovision.com/en/download-access-2/
[2] Eviden: Sichere und praxistaugliche Speicherung von Transaktionsdaten, konform zu gesetzlichen Vorschriften. https://www.cryptovision.com/de/produkte/security-token-hardware-solutions/cryptovision-tse-v2/ (abgerufen am 05.03.2024)
[3] Westermo: Data network solutions for the rail industry. https://www.westermo.de/industries/rail (abgerufen am 29.1.2024)
[4] Bashiri, K.; Kousidis, S.: Migration zu einer quantensicheren Verwaltungs-PKI. BSI Forum 5/2023
[5] Technische Richtlinie TR-02102-3, Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2). Bundesamt für Sicherheit in der Informationstechnik, 2023
[6] Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Bundesamt für Sicherheit in der Informationstechnik, 2023

AUTOREN | AUTHORS

Gunnar Preissler
Program Manager – Cyber security and mission critical systems
Eviden Digital Security
Anschrift / *Address*: Torgauer Straße 231-233, D-04347 Leipzig
E-Mail: gunnar.preissler@eviden.com

Andreas Hinterschweiger
Market Director Trackside
Westermo Data Communications GmbH
Anschrift / *Address*: Santorastraße 8, A-2482 Münchendorf
E-Mail: andreas.hinterschweiger@westermo.com

Klaus Schmeh
Chief Marketing Editor
Eviden Digital Security
Anschrift / *Address*: Munscheidstraße 14, D-45886 Gelsenkirchen
E-Mail: klaus.schmeh@eviden.com