Securing Industry 4.0 with Digital Identities for Embedded Components

Florian Handke
Campus Schwarzwald gGmbH
Freudenstadt, Germany
florian.handke@campus-schwarzwald.de

Jan Pelzl
Hamm-Lippstadt University of Applied Sciences
Hamm, Germany
jan.pelzl@hshl.de

Alexander Harig
Campus Schwarzwald gGmbH
Freudenstadt, Germany
alexander.harig@campus-schwarzwald.de

Christian Schwinne
Hamm-Lippstadt University of Applied Sciences
Hamm, Germany
christian.schwinne@hshl.de

Rohit Bohara
asvin GmbH
Stuttgart, Germany
r.bohara@asvin.io

***Abstract*—The paper "Securing Industry 4.0 with Digital Identities for Embedded Components" addresses the increasing security challenges in industrial environments arising from digitization and interconnected systems. It emphasizes the pivotal role of digital identities in enabling secure authentication, communication, and traceability across manufacturers, integrators, service providers, and operators. The paper introduces a reference approach to certificate lifecycle management as a fundamental building block for secure identity management in Industry 4.0. Developed within the context of the Trustpoint project—an open-source initiative—the approach supports the management of digital identities across diverse industrial systems, including both embedded devices and larger operational technology (OT) systems. Key processes such as certificate generation, renewal, revocation, and deletion are described, with a focus on automation and standardization, leveraging protocols and standards such as BRSKI, CMP, EST, OPC UA, and IEC 62443. By addressing sector-specific challenges, including network segmentation, resource constraints, and interoperability issues, this paper provides a conceptual framework to support manufacturers and operators in establishing secure, scalable, and standards-compliant identity management processes in industrial networks.**

***Keywords*—Industry 4.0 Security, Digital Identities, Certificate Lifecycle Management**

I. INTRODUCTION

The increasing digitization and networking of machines and systems in Industry 4.0 environments place increasingly complex demands on OT/IT security. Digital identities play a critical role in establishing trust between manufacturers, integrators, service provider and operators, enabling secure communication, authentication, and traceability. However, deploying and managing digital identities in industrial environments is challenging due to segmented networks, resource constraints, and lack of interoperability between manufacturers. In addition, many stakeholders lack the expertise and resources to implement comprehensive security and identity solutions, leading to vulnerabilities and operational risks.

This paper explores the theoretical background and describes a reference implementation of certificate lifecycle management as a cornerstone of secure digital identity management for embedded industrial systems. We highlight key processes, including certificate generation, onboarding, renewal, revocation, and deletion, with an emphasis on automated and standardized approaches such as zero-touch onboarding via BRSKI [1], and protocols such as certificate management protocol (CMP) [2] and Enrollment over Secure Transport (EST) [3] for secure certificate renewal. By abstracting complex mechanisms, we show how to enable manufacturers and operators to securely integrate devices into their networks while ensuring compliance with standards such as OPC UA [4] and IEC 62443 [5].

Using real-world examples, this paper demonstrates how certificate lifecycle management supports the scalability, security, and sustainability of industrial applications, paving the way for a safer and more connected Industry 4.0.

A. Proof-of-concept: Architecture and Features

A proof-of-concept has been implemented within the Trustpoint research project, a collaborative initiative funded under the KMU-innovativ program [6], provides a practical open-source framework to address these challenges.

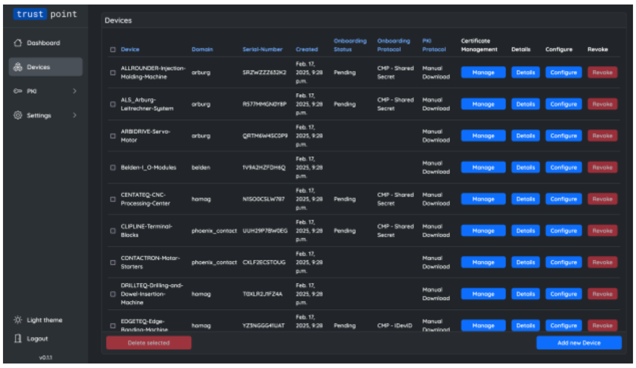
Trustpoint is an open-source platform developed to address the challenges of managing digital identities in industrial environments. With increasing digitization and networking in Industry 4.0, ensuring the security and scalability of connected systems has become critical. Trustpoint serves as a central trust anchor, enabling the efficient management of certificates and cryptographic operations throughout their lifecycle. Its architecture and features are designed to accommodate the unique constraints of industrial settings, such as segmented networks, resource-constrained devices, and diverse manufacturer ecosystems.

At the core of Trustpoint's capabilities is its Certificate Lifecycle Management, which streamlines the processes of generating, issuing, renewing, revoking, and deleting digital certificates. This ensures the secure operation of devices and systems over their entire lifecycle, aligning with industry standards such as OPC UA and IEC 62443. Trustpoint provides two primary deployment modes: it can operate as a Registration Authority (RA) to manage certificate requests in collaboration with an external Public Key Infrastructure (PKI) or function independently as a Certificate Authority (CA) to issue certificates directly.

A key component of Trustpoint is its Protocol Orchestration, which supports a variety of secure protocols such as Certificate Management Protocol (CMP), Enrollment over Secure Transport (EST), and RESTful APIs. Trustpoint is compatible across the broadest range of devices and applications, making it easy to integrate into an industrial network. For example, automated onboarding processes, such as zero-touch onboarding, leverage these protocols to securely integrate devices into networks with minimal manual intervention.

Trustpoint also includes advanced cryptographic support to ensure the robustness and security of its operations. It supports the management of symmetric keys for secure communication, integration with Hardware Security Modules (HSMs) for secure key storage, and adherence to cryptographic standards such as Certificate Management Protocol (defined in [2] and [8]), Enrollment over Secure Transport (defined in [3]), and PKCS#10 Certificate Signing Requests (CSR) (defined in [12]) that provide long-term resilience. Additionally, Truststore Management centralizes the storage and maintenance of trusted certificates and anchors, creating a reliable foundation for authentication and secure communication.

To facilitate scalability and ease of use, Trustpoint incorporates several features tailored to industrial requirements. Certificate Templates simplify the generation of certificates for diverse applications by providing pre-configured settings. Domain Management allows the separation and independent administration of certificate issuance processes for different operational domains, enhancing flexibility for large-scale deployments. The platform also supports comprehensive audit logging, which records certificate-related activities to aid in compliance, troubleshooting, and operational transparency.



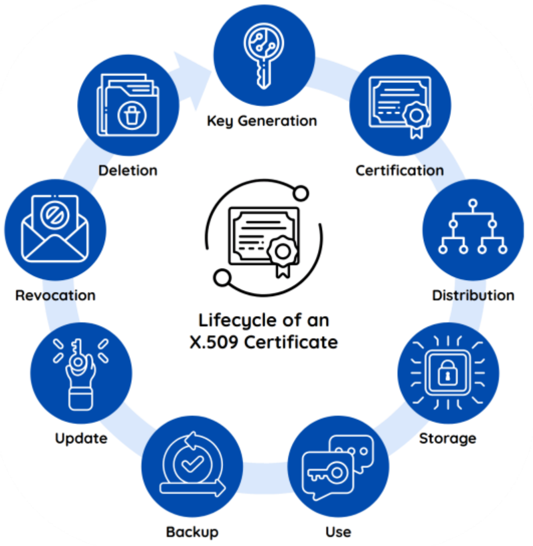
□	Device	Domain	Serial-Number	Created	Onboarding Status	Onboarding Protocol	PKI Protocol	Certificate Management	Details	Configure	Revoke
□	ALLROUNDER-Injection-Molding-Machine	arburg	SRZWZZZ632K2	Feb. 17, 2025, 9:28 p.m.	Pending	CMP - Shared Secret	Manual Download	Manage	Details	Configure	Revoke
□	ALS_Arburg-Leitrechner-System	arburg	R577MMGN0Y8P	Feb. 17, 2025, 9:28 p.m.	Pending	CMP - Shared Secret	Manual Download	Manage	Details	Configure	Revoke
□	ARBIDRIVE-Servo-Motor	arburg	QRTM6W4SC0P9	Feb. 17, 2025, 9:28 p.m.			Manual Download	Manage	Details	Configure	Revoke
□	Belden-I_O-Modules	belden	1V9A2HZFDH6Q	Feb. 17, 2025, 9:28 p.m.			Manual Download	Manage	Details	Configure	Revoke
□	CENTATEQ-CNC-Processing-Center	homag	NISO0CSLW787	Feb. 17, 2025, 9:28 p.m.	Pending	CMP - Shared Secret	Manual Download	Manage	Details	Configure	Revoke
□	CLIPLINE-Terminal-Blocks	phoenix_contact	UUH29P7BWDEG	Feb. 17, 2025, 9:28 p.m.	Pending	CMP - Shared Secret	Manual Download	Manage	Details	Configure	Revoke
□	CONTACTRON-Motor-Starters	phoenix_contact	CXLF2ECSTOUG	Feb. 17, 2025, 9:28 p.m.			Manual Download	Manage	Details	Configure	Revoke
□	DRILLTEQ-Drilling-and-Dowel-Insertion-Machine	homag	T0XLR2J1FZ4A	Feb. 17, 2025, 9:28 p.m.			Manual Download	Manage	Details	Configure	Revoke
□	EDGETEQ-Edge-Banding-Machine	homag	YZ3NGGG4IUAT	Feb. 17, 2025, 9:28	Pending	CMP - IDevID	Manual Download	Manage	Details	Configure	Revoke

II. THE CERTIFICATE LIFECYCLE AND ITS MANAGEMENT WITHIN TRUSTPOINT

Just as industrial devices and machines move through distinct phases of their lifecycle, from manufacturing and installation to operation, maintenance, and eventual decommissioning, digital certificates that represent their identities follow a similar lifecycle. Certificates are the foundation of trust in industrial networks, enabling devices to authenticate themselves, establish secure communication channels, and ensure data integrity. Without properly managed certificates, the risk of unauthorized access, data manipulation, and operational disruption increases significantly.

The certificate lifecycle consists of several key stages: key generation, certificate issuance, renewal, revocation, and deletion. Each stage plays a critical role in ensuring that devices maintain a secure digital identity throughout their operational lifetime. For example, generating cryptographic keys securely is vital to prevent compromise, while timely renewal ensures continued trust and compliance with evolving security standards. Revoking certificates when devices are retired, compromised, or reconfigured prevents unauthorized use and protects the integrity of the system.

The following sections describe each stage of the certificate lifecycle in detail, illustrating how Trustpoint supports and automates the management of digital identities in industrial environments.



A. *Key generation*

To generate a digital certificate, the creation of an asymmetric key pair - consisting of a public and a private key - is required. This can be done in different ways:

On the device itself: The device generates a key pair and constructs a request message containing information about its identity and the public key. This could be a PKCS#10 Certificate Signing Request (CSR), a Certificate Management Protocol (CMP) message or some similar protocol message. This message is then transmitted securely to a Certificate Authority (CA) which in turn will issue the certificate for the device. Generally, this method is preferred due to the private key not leaving the device, which reduces the risk of it being compromised or stolen. This is especially true if the device has a special hardware available like a Hardware Security Module (HSM) or a Trusted Platform Module (TPM). The key can then be generated within this hardware module and even be flagged as non-exportable.

Key generation by CA/Trustpoint: The keys are generated by a trusted entity, often the CA, such as Trustpoint, and then transferred to the device. This method can be useful if the device is very constraint or does not have enough entropy available and thus lacks the capability to generate sufficiently secure random numbers (TRNG / CSPRNG). Furthermore, generating keys can take a long time on constrained devices, which may be mitigated by requesting an externally generated key.

Trustpoint supports both approaches depending on the device capabilities and the selected onboarding process. Protocols such as CMP and EST allow devices to securely request certificates regardless of whether the key is generated locally or externally. CMP, in particular, supports end-to-end message protection and enables devices to request key generation by a CA if necessary. EST is often used when devices generate their keys locally and submit a PKCS#10 CSR containing the public key.

Trustpoint defaults to expecting a public key in certificate request messages, as this follows best practices. However, when external key generation is required, Trustpoint can generate the key itself or - in RA mode - delegate this task to another CA.

B. *Certificate Issuance*

There are several standardized PKI protocols to request, renew and revoke certificates.

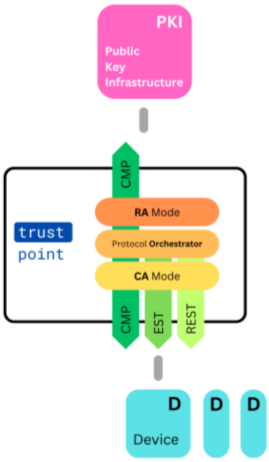
Enrollment over Secure Transport - EST (RFC 7030): EST is a simple and widely used PKI protocol which uses PKCS#10 certificate signing requests and relies on the security of the communication channel, i.e. Transport Layer Security (TLS) [2]. The simplicity of the protocol itself and the wide support of both PKCS#10 objects and TLS by devices, make it one of the most supported and used protocols. One of the disadvantages is, that it is not secured on message level, and may thus be problematic if the request must pass through multiple servers, which are able to manipulate the request.

Simple Certificate Enrollment Protocol (SCEP) (RFC8894 b): SCEP evolved from an enrollment protocol developed by Cisco System [7]. Both old and new versions are still widely used especially in Microsoft Windows environments. The older versions of SCEP are very limited in both functionality and supported key types. It is generally recommended to switch to newer protocols like EST and CMP.

Certificate Management Protocol - CMP (RFC 4210 & RFC 9483): CMP is the most sophisticated protocol. It offers more features than both EST and SCEP and is protected on the message level. While there are some freely available implementations, e.g. OpenSSL offers a CMP client, it is not yet widely used, and the protocol itself is rather complex. It is however the most promising protocol, especially in industrial environments, since multi-hop scenarios are common [2] and [8].

Automatic Certificate Management Environment (ACME) (RFC 8555): The ACME protocol, defined in [9], is mainly used for TLS server certificate issuance. It has several methods of proving that a domain for which the certificate is requested is actually in possession of the requester. This protocol is very common for use in the public internet. However, it may also be used in private LANs for local DNS servers providing private domain names.

Trustpoint aims to support as many of those commonly used protocols as possible such that it can be applied in many different environments including scenarios where different devices only support different subsets of these protocols. It also includes a custom REST API so that devices can request certificates as long as they are able to make HTTP(S) requests.

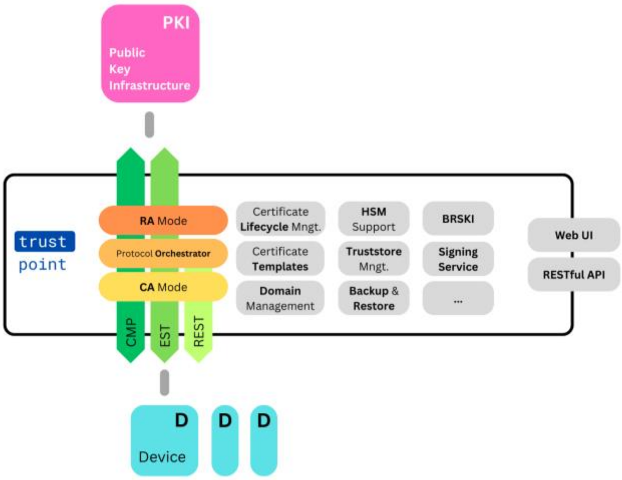


There may be cases in which an already existing PKI shall be integrated and used. There are generally two ways in which this can be accomplished.

1. The external PKI provides an issuing CA credential such that certificates can be locally issued. The advantage is that the connection to the PKI does not need to be persistent or reliable.
2. Certificates are only issued by the existing PKI. The local entity acts as a RA which can do validations and checks on incoming requests and then forward the requests to the actual external PKI.

Trustpoint is designed to support both integration scenarios when working with an existing PKI infrastructure. It can import an issuing CA certificate and key, allowing it to locally issue certificates on behalf of the external PKI. Alternatively, Trustpoint can function as a Registration Authority, validating certificate requests and forwarding them to the external PKI for issuance.

To ensure compatibility with diverse devices and environments, Trustpoint includes a PKI protocol adapter capable of translating incoming certificate requests from one protocol to another. This allows devices that only support protocols like EST or SCEP to interact seamlessly with an external PKI using, for example, CMP. While certain technical limitations exist depending on the external PKI's capabilities, using CMP as the upstream protocol generally enables Trustpoint to offer broad multi-protocol support to devices.



C. *Methods for certificate distribution*

Particularly industrial networks are often comprised of very different kinds of devices. There can be several limiting factors in regards to how certificates can be requested and acquired, the three most common issues are

- No support of onboarding protocols
- No support for any kind of PKI protocol
- Not directly connected to a PKI endpoint such that certificates cannot be requested via network
- Limited set of cryptographic algorithms are supported.

Trustpoint offers several onboarding and certificate distribution methods to mitigate these issues and allow a multitude of different devices to be onboarded with a domain credential or be directly be supplied with application certificates. The following onboarding methods are supported by the Trustpoint:

The highest level distinction is whether the device is onboarded to the network or merely provided with individual application credentials. In this context, onboarding refers to the distribution and installation of a domain credential - an Locally Significant Device Identifier (LDevID) certificate and associated keypair that allow the device to request and manage additional application certificates.

In case onboarding with a domain credential is chosen, multiple onboarding methods are offered:

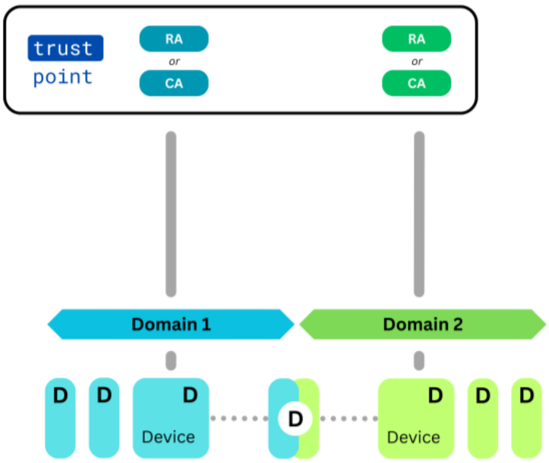
- The most user friendly method is using the **Trustpoint Client**, available at [10], which internally uses CMP and requires no further configuration.
- It is also possible to configure a device to use PKI protocols like CMP and EST directly.
- Zero-touch onboarding is possible by e.g. configuring a set of allowed Initial Device Identifiers (IDevIDs) for devices that may onboard themselves automatically.

If instead no domain credential is issued, application certificates may be issued on an individual basis. This can also be accomplished through different methods:

- The application credential can be generated on Trustpoint and downloaded either via the admin interface, or - using a one-time passcode - via a remote browser client, usually on the target device
- Retrieving an application certificate via EST and CMP using a single-use shared secret is also possible.

If possible, it is always beneficial to issue a domain credential in a production system, as it allows for far greater flexibility in certificate management - for instance, automatic renewals.

Furthermore, devices can be organized into groups, representing sets of devices that are not necessarily disjoint but are intended to primarily communicate within their respective group. Communication across groups is typically restricted, with exceptions for certain devices such as gateways, which facilitate controlled data exchange between groups. In a PKI context, these groups are often referred to as domains, with each domain representing a distinct trust hierarchy. Devices within the same domain trust certificates issued by the same Issuing CA or a common root of trust.



This allows a distinct partitioning of the network into separate secured communication networks and thus reduces the risk of a system wide compromise. To gain access to the whole of the system an attacker would require to breach all of those separate networks, not just one. Consequently, in a case of a compromise, this will also reduce the required work to setup a new domain and trust hierarchy, since only a fraction of devices are affected. Additionally, it adds a layer of data privacy protection in that sensitive data is only shared between devices in the same domain and may not directly be send to devices outside that domain such that a gateway may aggregate and inspect data before passing it on to the desired destination.

The Trustpoint allows to create arbitrary many domains, each using either a distinct trust hierarchy or at least a distinct issuing CA, depending on the actual use-case. For the purpose of gateways, an arbitrary amount of domains can be associated with a single device, such that it can onboard into multiple domains simultaneously, and act as an intermediary between the different domains.

D. Certificate and key storage

Both the public key certificate and the associated private key are stored on the device. As outlined above, the private key is preferably generated on the device itself within a secure cryptographic module, as this approach allows the private key to be used for cryptographic operations such as encryption and digital signatures while protecting against extraction and subsequent misuse of the private key itself.

Given the optional Trustpoint Client is utilized on the device, after successful onboarding, the device obtains domain credentials, which are stored in trustpoint-devid-module. It is a python based storage and integrity utility. In future, it will be extended to use TPMs, HSMs and standard database to securely store credentials [13].

Trustpoint aims to offer **PKCS#11** support for easy integration with hardware security and other cryptographic modules. A **HSM** is a dedicated physical device designed to securely store cryptographic keys and other sensitive cryptographic materials. HSMs provide a highly secure environment that safeguards credentials against unauthorized access, theft, or tampering. They are tamper-resistant and often certified to stringent security standards, such as FIPS 140-2 or Common Criteria. HSMs play a vital role in ensuring the integrity and confidentiality of sensitive operations like encryption, decryption, digital signing, and authentication. In Trustpoint, we plan to support software emulated HSM (SoftHSM) to store the domain and application credentials for devices that have no dedicated cryptographic key storage hardware. In parallel, we build interfaces on Trustpoint Client to interact with a HSM to manage credentials.

E. Usage of certificates

Certificates have a wide range of applications. One of the most common uses in general IT is TLS certificates within the Web PKI framework to secure website transport. In industrial environments, they are used for:

DevIDs according to 802.1 AR: These device identification certificates are used to uniquely and securely identify devices. The *IDevID* uniquely and permanently identifies the device and is issued by the manufacturer. The operator issues the device a *LDevID* to identify it within their domain.

Application-specific certificates: These certificates are issued for specific applications or services within the industrial environment to ensure that only authorized devices and users can access APIs or other resources, and to guarantee the integrity of communication between applications running on the device.

Truststores or trust anchors: These are collections of trusted (CA) certificates used to verify other certificates issued by these CAs. Truststores are essential for the security and integrity of communication channels. Operating systems and browsers usually come with truststores containing well-known and generally trusted CAs, but these can be highly configurable by the user. In industrial environments, it is advisable to trust only those CAs whose certificates are essential for the given application.

TLS client and server certificates: These certificates are used to establish secure communication channels via TLS. TLS is utilized by various application protocols, including HTTPs for secure web transport.

- *Server certificates* authenticate the server to the clients, while
- *Client certificates* authenticate the clients to the server.

Trustpoint supports all aforementioned certificates for different purposes. An LDevID called the *Domain Credential* is used to authenticate a device against the Trustpoint server for PKI operations, such as requesting application credentials. A domain credential contains the initial LDevID certificate resulting from a successful device onboarding process. Domain credentials tie a device to specific domain on trustpoint. A domain is an abstraction on top of the Issuing CAs. Each domain contains only one issuing CA and all credentials in domain have same signature suite. Domain credentials are used to authenticate the device on Trustpoint during the application credential request.

F. *Certificate backup*

In a PKI for use in industrial applications, not only the cryptographic strength of the system needs to be considered, but also the availability of the infrastructure. If certificate issuance, verification, or renewal fail due to unavailability of the PKI, this could lead to prolonged and costly operational interruptions. Therefore, it must be ensured that in the case of unavailability, systems can easily and rapidly be restored, ideally automatically - e.g. via redundant instances with fail-over capability.

This requirement conflicts in some aspects with an essential requirement - the secure storage of private (CA) keys. While proprietary solutions may be available to mirror key material between two instances, such solutions may introduce additional weaknesses and lack interoperability. To ensure reliable and continuous certificate management services even in the case of CA unavailability, Trustpoint is designed in a way to allow take-over of PKI services by a different Trustpoint instance in the same hierarchy to facilitate uninterrupted service.

A notable exception to certificate availability concerns revocation services. If a CA becomes unavailable, it cannot issue updated Certificate Revocation Lists (CRLs), and expired CRLs may cause certificates to be rejected, depending on the verifier policy. Online Certificate Status Protocol (OCSP) responders can face similar availability issues, disrupting operations [14].

To reduce this dependency, modern PKI best practices favor automated short-lived certificates that expire quickly and are not renewed if a key is compromised or other issue occurs. This eliminates the need for CRLs and OCSP checks, reducing complexity and improving system resilience.

G. *Update of certificates*

Certificates are usually only valid for a previously specified time, such that if a certificate is compromised or its algorithm may have been broken in the meantime, it will eventually lose its validity even if it was not revoked. In practice, it is also regularly the case that revocation information is not actually distributed, and hence, even if revoked, entities will still trust the certificate. This is the reason why short-lived certificates are seen as the best practice, that is issuing certificates with a validity duration that is as short as technically feasible and sensible.

In this context, we must make a clear distinction between updating so called End-Entity Certificates, e.g. application certificates like TLS server certificates, and CA certificates, whose purpose is to issue further certificates.

When renewing certificates, it is possible to generate a new key pair as an additional security measure. While not always required, updating the key during renewal can help mitigate risks associated with long-term key usage, particularly in environments with high-security requirements. Frequent key changes reduce the impact of a potential key compromise and align with cryptographic best practices, but they must be balanced with operational constraints**.**

Renewing application certificates is generally straightforward, as it does not affect other certificates in the trust chain. Common PKI protocols provide mechanisms to automate this renewal process, typically involving the generation of a new key pair, followed by a certificate request for a replacement certificate. EST simplifies this process with its simple *Reenroll* mechanism, allowing a device to request a renewed certificate using an existing valid certificate for authentication. CMP offers a Key Update Request (KUR) operation, which supports renewal along with the generation of a new key pair, enabling secure and efficient certificate updates.

Both Trustpoint and Trustpoint-Client offer the renewal of application certificates both manually and fully automated using the Trustpoint-Client. If the Trustpoint-Client is not used, the user can implement the automation of certificate renewal themselves by utilizing the common PKI protocols like EST and CMP.

Renewing CA certificates however can be more complicated. If a CA certificate is renewed without using the same old key but a new one, all issued certificates will also need to be renewed and issued by the new CA.

Trustpoint aims to offer the user a streamlined issuing CA roll-over process which can be initialized such that for a period of time both, the new and old issuing CAs are valid simultaneously until all devices have been onboarded to the new issuing CA and / or all application certificates have been renewed by using the new issuing CA.

H. *Revocation of certificates*

Certificates are intended to be valid only for a specific period, but circumstances may arise that require a certificate to be revoked before its planned expiration date. Revocation is necessary when the trust in a certificate is compromised, as continuing to rely on it could expose systems to security breaches or unauthorized access. Understanding the common reasons for revocation is crucial for maintaining the integrity and security of an industrial PKI system. The most frequent scenarios requiring revocation include the following:

- **Key compromise:** If the private key of a certificate has been compromised, the certificate must be revoked immediately to prevent misuse.

- **CA compromise:** If the CA is compromised, all certificates issued by it must be revoked by a higher authority, such as the Root CA, and replaced with new certificates from a trusted CA.
- **Superseded:** When a certificate is replaced by a newer one, the old certificate can be revoked to minimize attack vectors. Often, certificates are renewed shortly before their expiration date, making revocation unnecessary.
- **Privilege withdrawn:** If the privileges granted by a certificate are withdrawn, the certificate must be revoked to restrict access.
- **Cessation of operation:** When a device is taken out of service, its certificates should be revoked to ensure they cannot be misused.
- **Temporary revocation (certificate hold) due to suspected compromise:** If there is suspicion of compromise, a certificate can be temporarily revoked to allow further investigation. If the certificate is later deemed secure, it may be reactivated.

Trustpoint supports certificate revocation through both manual and automated processes. Operators can revoke certificates manually using the Trustpoint Web UI, which provides an intuitive interface to view certificate details and trigger revocation actions. This method is suitable for individual cases or smaller deployments. For automated and large-scale environments, Trustpoint integrates with the CMP, which allows devices or administrators to submit revocation requests programmatically using the Revocation Request (RR) message. This enables swift responses to key compromise or other security incidents without requiring human intervention.

I. *Deletion of cryptographic material*

The final step in the lifecycle of a certificate is the deletion of its components, particularly the associated private key. Depending on security requirements, securely deleting the private key and any backups may be necessary to prevent unauthorized recovery and misuse. In other cases, simply letting the certificate expire may suffice, especially if the private key remains protected on a secure device.

As outlined earlier, private keys should preferably be generated on the device itself. In this case, deletion is handled locally on the device, often as part of decommissioning or reconfiguration processes. When key pairs are generated by the Trustpoint CA—for example, for constrained devices—Trustpoint irreversibly deletes the private key after successful credential delivery to ensure it is not retained beyond distribution.

Trustpoint retains issued certificates in its database, including expired and inactive ones, to support auditing and traceability. However, particularly in environments using short-lived certificates, the volume of expired records can accumulate quickly. To prevent resource exhaustion, Trustpoint allows the deletion of outdated certificates from its database when their retention is no longer necessary.

Operators are encouraged to periodically review and purge expired certificates, especially in environments with frequent certificate renewals, to maintain system efficiency and ensure that storage is not unnecessarily consumed.

III. Summary and Outlook

The advancing digitization in the industrial sector has significantly increased automation and interconnectivity, consequently elevating the risk of cyber threats. In this context, digital identities for embedded OT systems and machinery are paramount in establishing trust. Nonetheless, the integration and administration of these digital identities are restrained by challenges inherent to industrial systems, including limited hardware and software capabilities and a lack of standardization across different manufacturers. A notable obstacle is the deficiency of expertise and resources among manufacturers and operators for devising and enforcing sophisticated security and identity frameworks, leading to potential vulnerabilities and operational risks.

Addressing these issues, we showed how to establish trust and interoperability within industrial networks and components with a well-defined lifecycle management of digital identities. A reference implementation was demonstrated within the Trustpoint project. The project aims to overcome obstacles such as network segmentation, hardware limitations, and security knowledge gaps by introducing a user-friendly, open-source platform for digital identity management. Trustpoint supports both manual and automated zero-touch device onboarding processes, establishing a foundation of trust across the industrial value chain. We outline a methodology and an implementation, highlighting the adherence and contributions to existing standards like OPC UA Part 21, BRSKI, FIDO FDO, and their implications for stakeholders across the product lifecycle.

Moreover, potential future enhancements for practical deployment to elevate security measures are being discussed. The Trustpoint project demonstrates the practical application of the concept, showcasing the interaction with trust services, such as Public Key Infrastructure, and end devices, illustrating the potential to support secure and reliable communication within industrial settings.

Trustpoint was launched in September 2023 as a joint project between the Campus Schwarzwald, medium-sized companies (PrimeKey Labs GmbH / Keyfactor, asvin GmbH, achelos GmbH), and Hamm-Lippstadt University of Applied Sciences. It is supported by well-known companies such as ARBURG GmbH + Co KG, Belden Inc, Diebold Nixdorf, HOMAG GmbH, FANUC Deutschland GmbH, J. Schmalz GmbH, PHOENIX CONTACT GmbH & Co. KG, and Siemens AG as associated partners. This cooperation is made possible by the Federal Ministry of Education and Research as part of the KMU-innovativ initiative with funding of 1.41 million euros.

[1] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, “Bootstrapping Remote Secure Key Infrastructure (BRSKI)” RFC 8995, DOI 10.17487/RFC8995,

May 2021. [Online]. Available: Information on RFC 8995 » RFC Editor

[2] Adams, C., Farrell, S., Kause, T., and T. Mononen, *“Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)”* RFC 4210, DOI 10.17487/RFC4210, IETF, Sep. 2005. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4210

[3] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., *“Enrollment over Secure Transport”* RFC 7030, DOI 10.17487/RFC7030, IETF, Oct. 2013. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7030

[4] OPC Foundation, “OPC Unified Architecture (OPC UA)” IEC 62541. [Online]. Available: https://www.vde-verlag.de/iec-normen/suchen/?publikationsnummer=62541

[5] ISA Global Cybersecurity Alliance, “Security for industrial automation and control systems” ISA/IEC 62443. [Online]. Available: https://isagca.org/isa-iec-62443-standards

[6] Bundesministerium für Bildung und Forschung (BMBF), “KMU-innovativ”. [Online]. Available: https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/kmu-innovativ

[7] Gutmann, P., *“Simple Certificate Enrolment Protocol”* RFC 8894, DOI 10.17487/RFC8894, IETF, Sep. 2020. [Online]. Available: https://www.rfc-editor.org/info/rfc8894

[8] Hendrik Brockhaus and David von Oheimb and Steffen Fries, *“Lightweight Certificate Management Protocol (CMP) Profile”* RFC 9483, DOI 10.17487/RFC9483, November 2023. [Online]. Available: https://www.rfc-editor.org/info/rfc9483

[9] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, *“Automatic Certificate Management Environment (ACME)”* RFC 8555, DOI 10.17487/RFC8555, IETF, Mar. 2019. [Online]. Available: https://www.rfc-editor.org/info/rfc8555

[10] Trustpoint-Project., *“Trustpoint-Client”* GitHub, Okt. 2024. [Online]. Available: https://github.com/TrustPoint-Project/trustpoint-client

[11] Trustpoint-Project., *“Trustpoint”* GitHub, Mar. 2019. [Online]. Available: https://github.com/TrustPoint-Project/trustpoint

[12] Nystrom, M. and B. Kaliski, *“PKCS #10: Certification Request Syntax Specification Version 1.7”* RFC 2986, DOI 10.17487/RFC2986, November 2000. [Online]. Available: https://www.rfc-editor.org/info/rfc2986

[13] Trustpoint-Project., *“Trustpoint Devid Module”* GitHub, Okt. 2024. [Online]. Available: https://github.com/TrustPoint-Project/trustpoint-devid-module

[14] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, *“.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”* RFC 6960, DOI 10.17487/RFC6960, June 2013. [Online]. Available: https://www.rfc-editor.org/info/rfc6960

Attribution: Figure x contains the icons “Speech Bubble“, “Security System“, “Cyber Security“, “Keyword Research“, “Algorithm“, “Structure“, “Private Key“, “Acceptance“, “Certification“, “Error“, and “Folder“ by Flowicon via Noun Project - Free Icons by Flowicon - Noun Project (licensed under

CC BY 3.0 - Deed - Attribution 3.0 Unported - Creative Commons). The icons were modified.