Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 59-25 (2025) 107–112

# Decentralized Industrial Security Architecture for Heterogeneous Automation Systems

**Marwin Madsen** * **Mike Barth** **

* *Karlsruhe Institute of Technology, Karlsruhe, Germany (ORCID: 0009-0006-9953-2382)*

** *Karlsruhe Institute of Technology, Karlsruhe, Germany (ORCID: 0000-0003-2337-063X)*

**Abstract:** Digital X.509 certificates are essential for securing automation systems. In industrial domains, such as automated production systems, there is a notable lack of innovative approaches for managing these certificates, especially when compared to the classical IT domain. This paper proposes an architecture for certificate management that is independent of underlying communication protocols, thereby enabling broader applicability. This approach is particularly beneficial for modular production systems, where the interchange of components is a regular occurrence. By enhancing security across diverse automated production systems, this method leads to increased trustworthiness and efficiency.



*Keywords:* IT/OT-Security, Certificate Management, Decentralized PKI, Production Gray Box

## 1. INTRODUCTION

A number of innovations are currently emerging in industry that focus on functional aspects and, in particular, the modularization and flexibilization of production environments such as the Module Type Package (VDI/VDE NAMUR 2658, 2022) or Namur Open Architecture (NE 175, 2020). These new concepts vary in their approach to security, with some explicitly addressing it and others not considering it at all. Predominantly, security mechanisms beyond anomaly detection and logging rely heavily on the implementation of signatures and encryption, which necessitate the use of X.509 certificates (Walz et al., 2022; OPC Foundation, 2024a; PNO, 2019). While some industrial communication protocols, such as OPC UA (OPC Foundation, 2024b) and PROFINET (PNO, 2019) have defined concepts for certificate management (CM), a generic zero-touch approach remains absent (Madsen et al., 2024). In particular, the underlying concept of public key infrastructure (PKI) has seen little innovation at its core in an industrial context, i.e. in operational technology (OT). In contrast, experts in information technology (IT) have extensively researched PKI (Khan et al., 2023; Vaziry et al., 2025). To emphasize the difference, the term IT-PKI and industrial PKI are used in the following to distinguish between PKI concepts in the different domains. IT-PKI innovations may offer fitting solutions for industrial PKI challenges, despite differing requirements and challenges. This paper explores potential approaches for applying IT-PKI innovations within the context of modularization. The goal is to enable the seamless integration of modules into systems with minimal configuration, regardless of the manufacturer, adhering to a plug-and-play paradigm through standardized interface descriptions. Encompassing security mechanisms to achieve the desired objectives is fundamental for this approach. However, there are currently no comprehensive solutions for certain security mechanisms, particularly for CM.

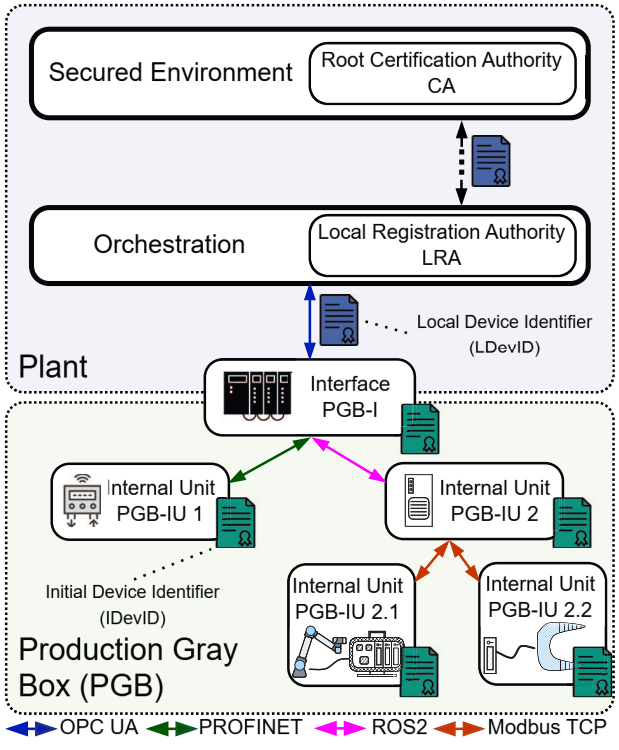


Fig. 1. Example of an industrial PKI in a modularized context with the generic PGB architecture

Figure 1 illustrates the fundamental components of an industrial PKI in the context of modularization, consisting of the production gray box (PGB) (Madsen et al., 2024)

2405-8963 
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2025.11.933

and the plant operator's PKI. The following paragraphs first provide an example based on certificate revocation to demonstrate the potential of IT-PKI innovations for the industrial PKI despite differing domain requirements, before addressing the central challenges of industrial PKI in modularization, illustrated through the PGB architecture in Figure 1.

Currently, the industrial PKI is characterized by a centralized architecture with a single point of failure in the form of the root certification authority (CA), necessitating the root CA to be in a dedicated secure environment (IEC 62443, 2009/2024). Consequently, revocation mechanisms are challenging to implement and often unused. In IT-PKI, several newly proposed architectures and mechanisms have emerged (Khan et al., 2023), including the continuous reduction of certificate validity periods, with an accepted proposal reducing it to 47 days (Zacharopoulos, 2025). In industrial PKI, short certificate validity is impractical to impossible for manufacturer-issued certificates so-called Initial Device Identifiers (IDevIDs), but feasible for certificates issued from the plant operator, known as Local Device Identifiers (LDevIDs) (IEEE 802.1AR, 2018). However, even LDevIDs currently have validity periods of several years.

The heterogeneous nature of OT, with its variety of devices and communication protocols, presents challenges for CM. Solutions tailored to one protocol often require proprietary extensions for protocol mappings, which are often tied to the specific architecture of the automation solution. An example is that protocols expect certain locations for certificates on the storage system, which are not standardized between communication protocols (OPC Foundation, 2024a). Moreover, CM protocols typically depend on direct communication between the end entity (EE) and a PKI management entity, which is not always feasible in modular setups with nested EEs.

Regulations like the Cyber Resilience Act (Chiara, 2022) increasingly mandate integrity and confidentiality in OT. Protection must therefore extend beyond outward communication. NAMUR, for example, promotes field-level integrity measures aligned with a defense-in-depth approach (NE 201, 2025), highlighting the need to address internal attack vectors across all automation layers, not just northbound protection.

The concepts in this paper explicitly refer to the architecture of a PGB as introduced in Madsen et al. (2024) and illustrated in Figure 1. The PGB interface (PGB-I) is integrated into the orchestration layer and, consequently, into the plant operator's PKI. In contrast, the PGB internal unit (PGB-IU), e.g. sensors, lack external communication capabilities and only communicate indirectly with the operator's plant via the PGB-I. The PGB can be found in various forms, such as in the context of industrial robotic systems (Witucki et al., 2025), the Module Type Package, line topologies, or even in the form of a train system. Therefore, it is not domain-specific and can be applied in the process and manufacturing industries as well as in transportation.

The CM of the PGB-I is not the focus of this work, as existing approaches such as OPC UA Part 21 (OPC Foundation, 2024b) are sufficient for this purpose. Instead, the focus is on how the PGB-IUs can request, renew, and revoke certificates while allowing for device exchange or maintenance processes, where a PGB-IU might be accessed via an engineering tool. While CM can be implemented within the PGB, it is either restricted to specific communication protocols used throughout the PGB or requires additional configurations and functionalities for the PGB-IUs. Using the example in Figure 1, PGB-IU 2.1 cannot contact the plant operator's PKI directly, as it only communicates directly with PGB-IU 2. Forwarding requires additional functionality on PGB-IU 2 and PGB-I, as well as configuration of PGB-IU 2.1 to identify the final recipient. However, these possibilities contradict the goal of modularization: low-effort, manufacturer- and architecture-independent integration.

In the following formal requirements for CM solutions in the context of the PGB architecture as defined by the authors are first presented, followed by an evaluation of improvement categories from IT-PKI and the derivation of potentials for industrial PKI. On this basis, a specific, adaptation is proposed.

## 2. REQUIREMENTS

While there is research on industrial PKI, it is mostly tied to dedicated communication protocols. Solutions are developed for individual problems without formalizing holistic requirements for industrial CM, which is crucial given the heterogeneous automation landscape. Such requirements are necessary to evaluate IT-PKI for their applicability or to identify whether sub-concepts can advance industrial PKI. The following requirements were identified in (Madsen and Barth, 2025) for CM in a PGB:

- **R1** Adhere to the zero-trust paradigm (Stafford, 2020)
- **R2** Achieve zero-touch CM of all devices in a PGB architecture for plant operators under the following restrictions:
  - Independent of specific communication protocol
  - Ability to exchange devices and perform maintenance (access via engineering tool)
- **R3** Minimize necessary changes to established security mechanisms of communication protocols
- **R4** Minimize hardware resources and runtime impact under the use of cryptographic capabilities

**R1** is not based on the architecture of the PGB but represents a desirable architectural design paradigm from a security perspective. The principles it contains — "never trust, always verify," "principle of least privilege" and "assume breach" — align with the new regulatory environment and plant operators expectations that the field level, despite access restrictions and compartmentalization, must still be regarded as a point of entry into the system. Therefore, communication in this area must employ security mechanisms to ensure integrity.

**R2** narrows the solution space for industrial PKI. There are various optimization approaches for an industrial PKI but as there are no problems with the current state of the art, such as with the CM of the PGB-I, no optimization approaches are considered in this paper. Instead, the focus is on problems arising through the goals of modularization. CM can be implemented by integrating manual steps. However, this increases the vulnerability of the overall system to human error, especially since security mechanisms

do not provide verbose error messages to avoid giving additional information to potential attackers. Complete automation is also not desirable, as there must be dedicated points at which trust is initialized in the system. Still, it is possible to shift this responsibility from the plant operator to the manufacturer or supplier. The requirement also aligns with the background of modularization, which is why the system should be integrated into the plant through standardized interfaces without requiring specific, complex manual interaction with the module's interior. Since lifecycle events such as device replacement or maintenance must also be enabled, the module is handled as a gray box. Furthermore, the solution should not be tied to a specific communication protocol, i.e. there should be no assumptions about how the actual process-related communication of the PGBs takes place.

**R3** is based on the fact that the actual communication between devices is linked to other factors, such as real-time requirements. Communication protocols have developed corresponding mechanisms to enable security features such as digital signatures, usually based on X.509 certificates, without violating these factors. A new approach to CM should thus minimally influence the security mechanisms of communication protocols applied during runtime, as otherwise functional aspects could be affected.

**R4** excludes protocols and devices that cannot implement security mechanisms. Thus, this paper explicitly does not consider brownfield environments. Instead, it focuses on blue- and greenfield environments, where storage and resources are expected to implement defined security mechanisms. It is desirable to keep additional hardware requirements as low as possible. The same applies to runtime effects. Although CM operations are not required for every communication interaction and do not have to run within a cycle time, the shorter these interactions are, the more capacity can be used for the actual process.

**R1** and **R2** are hard requirements, essential for secure and low-effort integration in modular environments. In contrast, **R3** and **R4** are soft requirements, focused on compatibility and efficiency. Accordingly, **R1** and **R2** carry greater weight in the following evaluation of IT-PKI advancements for industrial applicability.

## 3. EVALUATION OF THE STATE OF THE ART IN IT-PKI

Table 1 summarizes the clusters of IT-PKI innovations identified in (Madsen and Barth, 2025; Khan et al., 2023; Vaziry et al., 2025) and their relationship to the requirements defined in section 2. In the following, each cluster is briefly described and specifically their greatest weakness with regard to the requirements **R1** to **R4** is explained.

The reason for this research and the challenges associated with the *classic hierarchical* PKI stem from the lack of generic solutions and the difficulty in implementing zero-touch mechanisms (**R2**). This cluster also includes architectural modifications that continue to rely on the hierarchical structure, such as cross-certification, mesh, or bridge architectures.

Table 1. Evaluation of IT-PKI innovations against the elaborated requirements

| IT-PKI innovation clusters | R1 | R2 | R3 | R4 |
|---|---|---|---|---|
| Classic hierarchical | ++ | -- | ++ | ++ |
| Log-based | ++ | -- | - | - |
| Reputation-based | -- | + | -- | ++ |
| Revocation | ++ | -- | - | - |
| Decentralized - Blockchain | ++ | - | + | - |
| Decentralized - P2P | ++ | ++ | -/+ | - |

Two clusters of considerations revolve around enhancing the trustworthiness of entities. The first focuses on trustworthiness of the CAs itself through *log-based* approaches. However, the trustworthiness of a CA itself is not a significant issue in industrial PKI, as, in contrast to IT-PKI, the CA is under the control of the plant operator and there is no multitude of third-party CAs involved in the operation phase (**R2**). The second evaluates participating entities based on their actions, in the form of a *reputation-based* approach. While evaluating the behavior of EEs is certainly relevant for industrial PKIs, it can only be assessed retrospectively based on the interaction of EEs. This contradicts the zero-trust paradigm and actions executed individually can impact safety or damage underlying hardware (**R1**). Furthermore, the *reputation-based* concepts would introduce completely new trust models and thus mechanisms (**R3**).

Another cluster is the improvement of *revocation* mechanisms. Although this is fundamentally important for industrial PKIs, it is limited to a part of the certificate lifecycle and does not address challenges like the automated initial registration (**R2**).

The last two clusters involve *decentralization* approaches. First, recent research in this area predominantly utilizes *blockchain* concepts. However, these approaches require EEs to access the *blockchain* and the consensus algorithms involved are typically computationally and resource-intensive as well as preventing delegation. Push mechanisms for low-resource devices are thus ineffective. Second, earlier research on *decentralization* focused on *peer-to-peer (P2P)* concepts. These concepts necessitate communication between all participants, either through direct cross-communication or a logical overlay network. The latter also increases resource requirements and necessitates modifications to certificate validation (**R3, R4**). It should be noted that the underlying trust model is reputation-based (a certain number must confirm an EE), as is the case with most others (e.g., in classic hierarchical models, instances confirm trust on behalf of the central CA). However, in *decentralized P2P*, initial trust is generated via an initial configuration (bootstrapping) and is not evaluated retrospectively based on the concrete interaction of the EE, as would be the case in approaches from the *reputation-based* cluster.

Although the *P2P* approach aligns best with the requirements, no single IT-PKI approach fully satisfies all criteria. Direct adoption of these mechanisms may not be feasible, but they offer valuable insights and a solid foundation. The following section will develop approaches for industrial PKI based on these IT-PKI considerations.

## 4. DERIVING APPROACHES FOR INDUSTRIAL PKI

The primary challenge of implementing zero-touch industrial PKI in the field lies in enabling EE to identify and communicate with PKI Management Entities without necessitating additional configurations or communication elements specific to the plant operator's architecture or

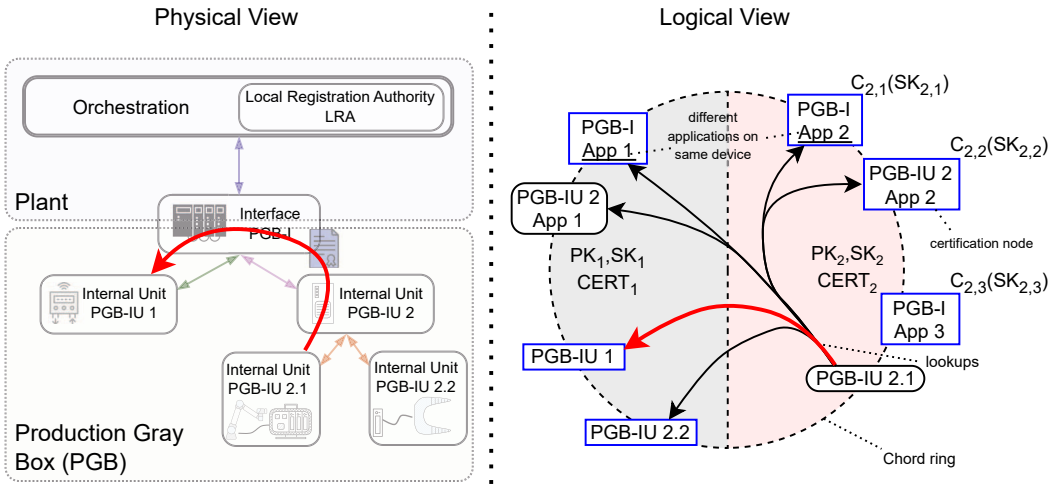


Fig. 2. Mapping the PGB architecture to the Chord-PKI approach

intermediate devices. Discovery mechanisms, such as those employed by OPC UA, offer a potential solution. However, these mechanisms are protocol-specific and cannot be universally applied across a heterogeneous automation architecture. Additionally, they do not eliminate the need for supplementary forwarding mechanisms. Integrating PGB-IUs into the plant operator's PKI contradicts the goals of modularization, as no standardized architecture-independent solutions currently exist. Thus, this work proposes the following hypothesis:

**H1** Integrating PGB-IUs in the plant operator's PKI is not required to fulfill the identified requirements **R1** to **R4**.

Based on this hypothesis and the identified IT-PKIs, adaption approaches for industrial PKI with the highest potential to meet these requirements are summarized in Table 2. In this section, each adaptation is succinctly outlined, highlighting only their most significant drawback concerning requirements **R1** to **R4**.

Table 2. Evaluation of industrial PKI approaches for PGB against the requirements

| Architectures | R1 | R2 | R3 | R4 |
|---|---|---|---|---|
| Self-signed | - | -- | ++ | ++ |
| Symmetric keys | - | -- | - | ++ |
| Proximity CA | (-) | + | ++ | ++ |
| P2P | ++ | ++ | ++ | + |

A common industrial PKI approach involves using *self-signed* certificates instead of establishing a PKI. While self-signed certificates simplify implementation, in dynamic contexts, certificates must be stored as trusted by the respective communication partners. In this form, certificates offer limited advantages and could effectively be replaced by *symmetric keys*. Both approaches imply decoupling from a PKI, but due to the desired zero-trust and zero-touch paradigms, they do not meet the requirements **R1** and **R2**.
Another approach, the so-called *proximity CA*, involves integrating the CA into the PGB and authenticating only the PGB-I using existing methods as a representative, providing it with an LDevID of the plant operator. Since the machine builder controls the architecture and communication, they can configure it so that the plant operator does not need to interact with the PGB, thus fulfilling **R2** by outsourcing interaction. However, a CA should be particularly secured as a single point of failure. Integrating it in the field and transporting it with the PGB would necessitate a threat analysis, which could indicate a risk-based contraindication for this approach (**R1**).
A *P2P*-PKI approach would also bring certification into the field. However, this would no longer depend on a single instance but would be distributed among all involved entities. The corruption of a single instance would not enable the takeover of other devices. By distributing cryptographic mechanisms via threshold cryptosystems (Desmedt, 1992) across multiple entities, the resource load would also be reduced. However, direct physical or logical communication between all involved entities would need to be enabled, impacting the hardware resources and runtime. Nevertheless, adaptations of the *P2P*-PKI approaches from IT for the special architecture of the PGB offer possibilities to mitigate these effects.
The evaluated IT approaches and adaptation proposals for industrial PKI do not offer a complete solution but can improve the current situation. The following section will offer an adaption proposal of a *P2P*-PKI approach in detail to illustrate its advantages, disadvantages, and feasibility.

## 5. CONCEPT OF THE DECENTRALIZED P2P-PKI ARCHITECTURE FOR THE PGB

To elaborate on the advantages and disadvantages of a P2P-PKI, the communication protocol and overlay network Chord is utilized with the Chord-PKI concept as described by (Avramidis et al., 2012). Figure 2 illustrates the core idea of how the PGB architecture would be realized within the specific IT-PKI framework. The core element of overlay networks is the abstraction of the physical communication structure at a logical level, enabling

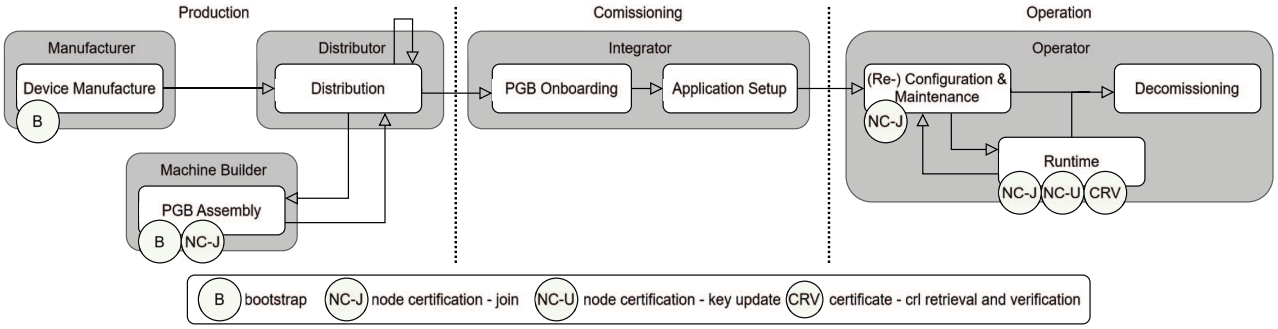


Fig. 3. Mapping of Chord-PKI procedures to PGB lifecycle according to OPC UA Part 21

cross-communication between each participating entity as illustrated with the red lookup arrow and the dotted circle in the logical view representing the Chord ring. In the IT domain, decoupling addressing from the physical layer is common practice. However, in OT, there is a strong dependency on the physical layer due to the emphasis on efficient and real-time communication. While an overlay network is conceptually and technologically feasible in an industrial context, it introduces additional requirements and restrictions, thereby impacting **R3**.

The core concept of the Chord-PKI is to use threshold cryptography with a proactive update of key shares. All entities participate in the generation of a shared secret in such a way that no one knows the secret key to be shared, not even during the key generation phase. Furthermore, a set of $n$ entities can share the secret key $SK$ of a public/secret key pair $(PK, SK)$ such that any set of more than $t$ entities can use their shares of $SK$ to jointly generate a digital signature that can be verified with the public key $PK$. In addition, the Chord ring is divided into $s$ segments to support larger networks and higher tolerances of the system against malicious nodes. Each segment $SEG_i, 1 \leq i \leq s$, i.e. a set of nodes, thus has the public/secret segment key pair $(PK_i, SK_i)$ and a certificate $CERT_i = SIG_{SK_i}(i, PK_i)$. Within each segment, there are certification nodes $C_{i,j} \in SEG_i, 1 \leq j \leq n$ which each have a key share $SK_{i,j}$ of the key $SK_i$. With the proactive update of key shares, the entities update their shares without changing the secret key itself, limiting the time period a potential adversary has to compromise the secret key. Essentially, instead of relying on a single CA, a configurable number of entities $t$ within the PGB, namely PGB-Is and PGB-IUs, must form an attestation to determine the trustworthiness of an instance by creating a signature on a certificate, thereby adhering to the zero-trust paradigm and **R1**. The Chord-PKI outlines several operational procedures tailored to various use cases of CM on top of the Chord ring. Among these, the following procedures are defined:

- Bootstrapping
- Node certification
- Certificate — CRL retrieval and verification

The mapping of these procedures to the lifecycle of a PGB, based on OPC UA, is illustrated in Figure 3. During the production phase, the bootstrapping procedure must occur as the onboarding of the PGB should be automated for the plant operator. In a traditional hierarchical PKI, bootstrapping would imprint the IDevIDs. In contrast, the Chord-PKI approach divides the Chord ring into segments and selects $n \geq 2t + 1$ certification nodes per segment. Threshold cryptosystems should be selected to allow the threshold to be relaxed to $n \geq t + 1$ in the PGB setting. Otherwise, there could be insufficient certification nodes in small PGBs. These nodes collaboratively generate the public/secret key pair $(PK, SK)$, establishing an initial trust relationship. The IT-PKI concept envisions an open system with numerous nodes, functioning correctly as long as fewer than $t$ nodes are corrupt or faulty, using a $(t, n)$ threshold signature scheme. Specifically, $t + 1$ of the initial certification nodes in a segment must be trusted for bootstrapping. In the OT environment, this phase takes place in a secure manufacturer setting where all nodes are under manufacturer control and only a few entities exist within the PGB. From a risk-based perspective, it is reasonable to assume that at most one node may be corrupt at any given time. Segmentation mitigates the risk of Sybil attacks — where a large number of pseudonymous identities are created to gain disproportionate influence in the P2P network— and reduces the cost associated with certification nodes. However, it increases the number of nodes required for bootstrapping, posing challenges for small PGB networks. Thus, segmentation should often be minimized or omitted. For example, in the PGB scenario from Figure 2, the Chord ring has two segments ($s = 2$) with three certification nodes ($n = 3$) in each segment and a signature threshold of $1 \leq t \leq 2$ as $t \geq 1$ with equality if exactly one node is needed to create a signature. It should be noted, that a PGB can be subdivided into nodes not only by device (i.e. PGB-I or PGB-IU) but also by application, as demonstrated by PGB-I and PGB-IU 2 in Figure 2. Ideally, bootstrapping occurs once the PGB is fully assembled and the next step is the commissioning. In modular contexts, this point of time may be unclear from a manufacturer or machine builder perspective. If additional devices are added post-bootstrapping, there have to be mechanisms enabling these devices to join the PGB and its CM which is handled by the node certification procedure in the Chord-PKI.

After bootstrapping, PGB-Is and PGB-IUs possess cryptographic material for communication fulfilling **R1**. As the PGB-I should handle authentication on behalf of the PGB and integrate into the operator's PKI using an LDevID via state of the art mechanisms no specific CM procedures are required in the commissioning phase for the Chord-PKI in Figure 3. Thus, by outsourcing bootstrapping to the production phase, **R2** is fulfilled.

In the operation phase, except for the join mechanisms

via the node certification during reconfiguration or maintenance, other procedures are only relevant during the runtime. The most frequently executed procedure, which can impact the runtime, is the certificate validation for verifying communication partners. While process-based communication in the PGB uses the physical structure, certificate validation requires the overlay network, introducing higher latency. Symmetric keys should be exchanged post-certificate validation, ensuring subsequent communication does not rely on them. This approach mirrors secure sessions with OPC UA in a classic PKI. Although certificate validation has higher latency, it need not be executed every cycle and can be initiated before the session is deemed untrustworthy. Thus, **R4** is at least satisfiable.

## 6. CONCLUSION

In this work, different IT-PKIs were evaluated for their applicability in OT, based on the requirements for CM in a module known as the production gray box (PGB). The challenge in OT concerning PGB is the hierarchical nature of plant communication, necessitating dedicated forwarding functionalities tailored to the plant or PGB architecture. This ultimately contradicts the goal of modularization. Not a single IT-PKI concept directly addresses this issue. However, adaptations of IT-PKI concepts offer solutions, each with specific advantages and disadvantages, which were briefly presented based on the requirements.
The most promising approach of utilizing P2P concepts dedicated to CM was analyzed in detail. The focus was on the idea of using a Chord ring as an overlay network for the industrial PKI and its transferability to the lifecycle of a PGB in OT. The primary disadvantage of the Chord-PKI approach is the precondition that all entities communicate with each other, leading to increased latency. Additional software functionality for using the overlay network is needed, which can be provided independently of the communication protocol and architecture for each module.
A thorough evaluation of whether and how an overlay network can be implemented in OT while meeting domain-specific requirements must be part of future work. It remains to be determined whether a Chord ring is the most suitable choice for the overlay network. Other structured overlay systems, such as Kademlia, which builds a tree via XOR, may offer further optimization to the required resource and runtime requirements. The PGB typically has few PGB-IUs and is more static, except for device exchanges, differing from the classical design approach of overlay networks and thus providing another optimization approach. A proof of concept is particularly needed in this context. Additionally, low-resource and legacy devices have been explicitly excluded so far. Future research must determine whether these can be integrated into the P2P-PKI through delegation mechanisms or if implementation is limited to blue- and greenfield scenarios.

## REFERENCES

Avramidis, A., Kotzanikolaou, P., Douligeris, C., and Burmester, M. (2012). Chord-pki: A distributed trust infrastructure based on p2p networks. *Computer Networks*, 56(1), 378–398.

Chiara, P.G. (2022). The cyber resilience act: the eu commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction. *International Cybersecurity Law Review*, 3(2), 255–272.

Desmedt, Y. (1992). Threshold cryptosystems. In *International Workshop on the Theory and Application of Cryptographic Techniques*, 1–14. Springer.

IEC 62443 (2009/2024). Industrial communication networks - Network and system security series.

IEEE 802.1AR (2018). IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity. doi:10.1109/IEEESTD.2018.8423794.

Khan, S., Luo, F., Zhang, Z., Ullah, F., Amin, F., Qadri, S.F., Heyat, M.B.B., Ruby, R., Wang, L., Ullah, S., Li, M., Leung, V.C.M., and Wu, K. (2023). A survey on x.509 public-key infrastructure, certificate revocation, and their modern implementation on blockchain and ledger technologies. *IEEE Communications Surveys & Tutorials*, 25(4), 2529–2568. doi:10.1109/COMST.2023.3323640.

Madsen, M. and Barth, M. (2025). Dezentrale ot-security-konzepte für heterogene automatisierungsarchitekturen [decentralized ot security concepts for heterogeneous automation architectures]. In *Conference proceedings of the VDI Congress AUTOMATION 2025. Baden-Baden, Germany, July 1–2, 2025, in german.*

Madsen, M., Geib, B., and Barth, M. (2024). Enabling industrial security via certificate management concepts in the life cycle of a production gray-box. In *IECON 2024-50th Annual Conference of the IEEE Industrial Electronics Society*, 1–8. IEEE.

NE 175 (2020). NAMUR Open Architecture - NOA Concept.

NE 201 (2025). Identitiy and Access Management on Automation Devices.

OPC Foundation (2024a). OPC 10000-2: UA Part 2: Security.

OPC Foundation (2024b). OPC 10000-21: UA Part 21: Device Onboarding.

PNO (2019). PI White Paper: Security Extensions for PROFINET.

Stafford, V. (2020). Zero trust architecture. *NIST special publication*, 800(207), 800–207.

Vaziry, A., Garzon, S.R., Herbke, P., Segat, C., and Küpper, A. (2025). Sok: A taxonomy for distributed-ledger-based identity management. In *2025 Crypto Valley Conference (CVC)*, 56–80. doi:10.1109/CVC65719.2025.00015.

VDI/VDE NAMUR 2658 (2022). Automation engineering of modular systems in the process industry.

Walz, A., Berndt, D., Visoky, J., Koppers, J., Wiberg, J., Armstrong, R., Vincent, S., and Merklin, S. (2022). Faq on industrial ethernet security concepts. Technical report, Industrial Ethernet Security Harmonization Group.

Witucki, L., Madsen, M., Wagemann, E., and Barth, M. (2025). Introduction of a unified robot integration package. *at - Automatisierungstechnik*. doi:doi:10.1515/auto-2025-0007.

Zacharopoulos, D. (2025). Sc-081v3: Introduce schedule of reducing validity and data reuse periods. URL `https://groups.google.com/a/groups.cabforum.org/g/servercert-wg/c/9768xgUUfhQ?pli=1`.