Leveraging Transparency of Initial Trust Establishment for Device Security Management

Steffen Fries, Rainer Falk
Siemens AG
Technology
Munich, Germany
e-mail: {steffen.fries|rainer.falk}@siemens.com

***Abstract*—Device onboarding is the process of bootstrapping new devices into target systems or target domains, and further on to bring them into an operational state. Secure Device Onboarding has a direct relation to cybersecurity of the operation of the device in a system later on, as it establishes trust between the device and the domain based on device identities and associated cryptographic parameters. Moreover, new devices are provisioned with domain-specific security parameters. Different technologies for automated device onboarding have been specified. Having a reliable information on performed onboarding operations is important during operation, in which the identities and cryptographic parameters are maintained as part of device management. Currently available onboarding technologies do not explicitly consider a binding of this information to the device management during operation. The onboarding information may be specifically important to address upcoming vulnerabilities and threats. Specifically in cases of attacks, it can support the root cause analysis to derive immediate measures to further maintain the attacked service. This supports addressing requirements from existing and currently developed regulations and standards. This paper proposes enhancements to current onboarding approaches that provide this transparency of the onboarding process.**

Keywords–communication security; onboarding; trust establishment; industrial automation and control system; cybersecurity; system security management; Internet of Things.

I. INTRODUCTION

Security management comprises the setup and maintenance of security measures to protect the secure operation and service provisioning of a system, e.g., a cyber-physical system or an Internet of Things (IoT) system. Security measures may protect in particular single devices or the interaction of these devices via communication networks, e.g., to protect data exchange. It also considers operational network internal interfaces between components but also external interfaces to offer a service or to connect to further information resources. Security management therefore supports a reliable and trustworthy operation of systems. Security management depends on various information. One of the most important is the oversight of components and networks that form the managed system to enable a system view (inventory). This system view is the base to monitor the security state of the system and its components (devices). This may include information about the operating system, the patch level, potential known vulnerabilities and also the operational security parameters. Device introduction into a system is therefore the first step for a device-specific security state monitoring, contributing to the overall system security management.

Device onboarding as described in [1] is the introduction of a new device into an operational environment. This introduction typically comprises different exchanges of information related to the identity of the onboarding device and its capabilities. Moreover, it contains the provisioning of the device with operational parameters of the deployment environment to serve the intended purpose. This typically also relates to domain specific security parameters, like a locally assigned device identity and associated credentials in the first place to ensure the new device can be identified as part of the operational environment. In a later stage, further operational security parameter are typically provisioned like cipher suites and session parameter for utilized security protocols.

New devices in a system, specifically if they interact with others, likely have an influence on the security status of the overall system. Therefore, the introduction of new devices needs to be performed in a trusted and auditable way, which supports also root cause analysis in case of failures in or attacks to the system.

Several technical solutions have been specified for secure onboarding of devices in new operational deployment environments. While they differ in their detailed functionality, they can be used to ensure that only known and intended devices are put into operation. Solutions range from so called "Trust-On-First-Use" (TOFU), which implicitly assumes a device trustworthy based on the initial use of this device in its new operational environment, up to automated, mutually trusted introduction of devices into the system to ensure that not only the system trusts the new device, but also to ensure the device trusts the operational environments likewise.

As the onboarding of new devices directly relates to the security of the overall operational system, onboarding security is in the interest of the operator of the system to safeguard the continuous and reliable service provisioning during operation. Besides the business continuity requirements of an operator (e.g., an automation service provider), there are also more and

more regulative requirements defined that require the operator of specifically critical systems to operate the system in a resilient and secure way. This obviously affects the processes of the operator to maintain the system and components used in his operational environment. As a precondition, it already requires product manufacturers to support security in a holistic way to provide a secure product. This ranges from the development of the product starting with the idea up to the final product, covering the design and manufacturing processes and the technical features of the product. Meanwhile there exist regulative requirements for both, system operators and product manufacturers, to consider security as integral part of operation and manufacturing. As stated further, onboarding concerns the introduction of devices into an operational domain, it supports asset management and thus also supports keeping track of the security state of devices as part of continuous system security management.

This paper is structured in the following way. Section II provides an overview about related work. It concentrates on regulative boundary conditions to outline the importance of device security starting with its system introduction and standardized system security requirements supporting the definition of various technical solutions and also their conformance evaluation. Section III gives an overview about device onboarding in general, the relation to product lifecycle and the supply chain interaction. Moreover, it provides examples of existing technologies and standards developed to perform onboarding. Section IV outlines potential onboarding enhancements that provide improvements specifically to support the auditing of trust establishment and maintenance started with the introduction of new devices into an operational environment. This in turn contributes to a consistent security view of an operational environment. Section V provides an evaluation of the proposed onboarding transparency and derives necessary functionalities in the devices and the operational environment. Section VI concludes the paper and provides an outlook to potential future work.

II. Related Work

As stated in the introduction, several regulative requirements have been defined that have to be fulfilled by operators of critical infrastructures, by integrators, or by product manufacturers. They relate to the security of the products and systems and also their interaction and operation. They have a clear relation to monitoring of the security state of components, as well as of their operational security parameters. The introduction of devices into operational environments is considered as onboarding and thus constitutes an important point in the ability to monitor system security.

A. Regulative Boundary Conditions

An example of a regulation applicable in Europe is the NIS2 directive [2]. It describes minimum cybersecurity means to be realized by entities operating critical infrastructures in 18 different sectors (application domains). Beyond others, this also relates to the system security management including keeping track of device security states to address disclosed vulnerabilities in time.

The Radio Equipment Directive (RED) Delegated Act [3] is a further example, which is in force since May 2024 and targets product manufacturers. It requires that “radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service”. To address this requirement, oversight of the system security and specifically security handling of the utilized devices may be necessary.

A further European regulation example targeting product manufacturers is the EU Cyber Resilience Act [4], which is in force since December 2024 with a 3-year transition period. It poses specific cybersecurity requirements on the products and the related product development process but doesn’t stop there. It additionally defines reporting obligations for manufacturers regarding potential vulnerabilities in their products and utilized components as well as the provisioning of security patches to address known vulnerabilities.

An example from US is provided by the executive order EO 14028 [5], requiring operators beyond others to maintain a dedicated security level, obligate incident reporting, and specifically address the security within the supply chain.

Figure 1 shows further examples of security regulations also from selected countries, to underline that there is a higher demand in cybersecurity also on country specific level.

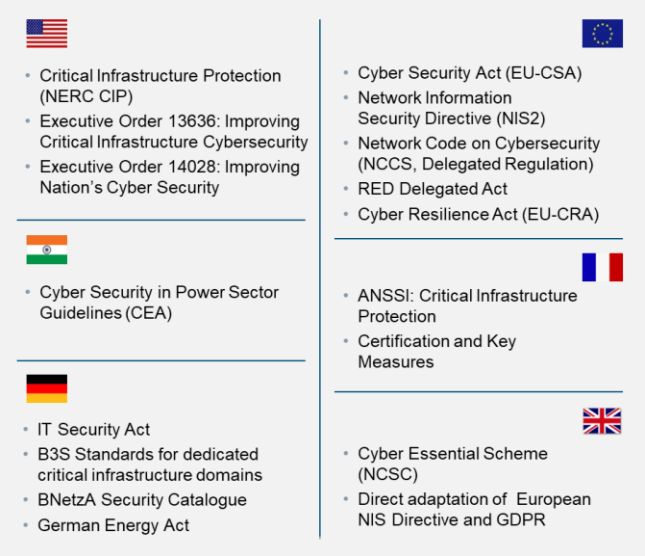

Figure 1. Examples for Security Regulation from different Countries.

B. Requirements Engineering Standards

Various requirement standards for procedural and technical security requirements have been specified. Here, two holistic frameworks are referenced as examples to show how they address device security, as well as credential and trust management throughout the lifecycle of devices. Both frameworks are broadly applied in industry. Moreover, they are consistently further developed to keep pace with the development of advances in security.

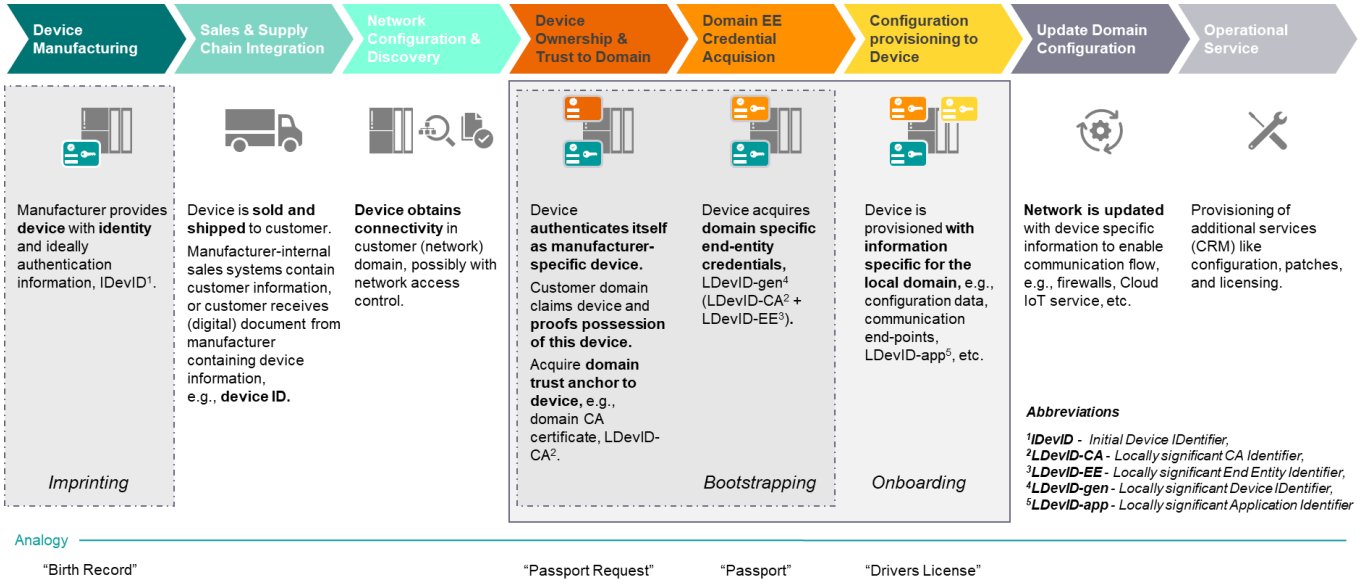

Figure 2. Onboarding Overview: From Imprinting Devices with Initial Security Credentials during Manufacturing to Operation with Domain specific Security Parameters.

A holistic cybersecurity framework defining specific requirements for automation system operators, integrators, and manufacturers is provided by IEC 62443 [6].

While it has been developed with the focus on industrial automation and control systems, it has already been adopted in industries like the power system automation and railway automation. Moreover, IEC 62443 is a main base for creating harmonized standards that address the regulative requirements (specifically for European regulation as outlined in Section II.A), and that provide requirements that can be used to show conformity with regulation. Besides providing requirements to operational and development processes, it specifically describes technical requirements on system and component level, targeting four different security levels, which relate to the strength of a potential attacker. Also, it contains requirements regarding security of devices and the lifecycle management of their security credentials in operative environments.

The NIST Cybersecurity Framework (CSF) 2.0 [7] provides general guidance on managing cybersecurity risk along the operation, including the identification of risks, the detection of potential attacks, but also the recovery to addresses resilience for normal and adverse situations.

III. Onboarding – Overview and Approaches

Device onboarding is the process to introduce devices into a target domain and to bring them into an operational state. This process has direct relation to cybersecurity, as it includes the establishment of trust between the domain and the device in the first step. There may be situations in which it is also required to ensure that a device is operated in fact in its intended target environment. Approaches that do not involve domain verification, are often called "Trust-On-First-Use" (TOFU), as they rely on the identification information of the device only. Other approaches that support explicit trust establishment may be understood as mutually trusted bootstrapping.

Key for the trust establishment are identities and corresponding cryptographic key material and parameters, which are imprinted into devices during product manufacturing. Identity information of a device is provided, along the supply chain as shown in Figure 2 to ensure that the interaction is always done with the intended device. This identity is issued by the manufacturer together with cryptographic information, as X.509 certificate [8] and known as Initial Device Identifier (IDevID). This imprinted identity typically will not change during the device's lifetime. Nevertheless, due to advances in quantum computing, currently used asymmetric cryptographic algorithms like RSA (Rivest, Shamir, Adleman) or ECDSA (Elliptic Curve Digital Signature Algorithm), which are used to bind the identity to a cryptographic credential, i.e., the X.509 certificate, are endangered [9]. This may require that also IDevIDs can be updated in the future to ensure secure identification and authentication during onboarding specifically for long-lived devices.

In the target domain, the IDevID can be used to bootstrap mutual trust in an automated way and to support issuing domain-related identities and associated cryptographic keys, known as Locally significant Device Identifiers (LDevID), which are used as operational credentials. The reason to switch from manufacturer issued IDevIDs to operator issued LDevIDs relates to the maintenance of and complete reliance on operational credentials.

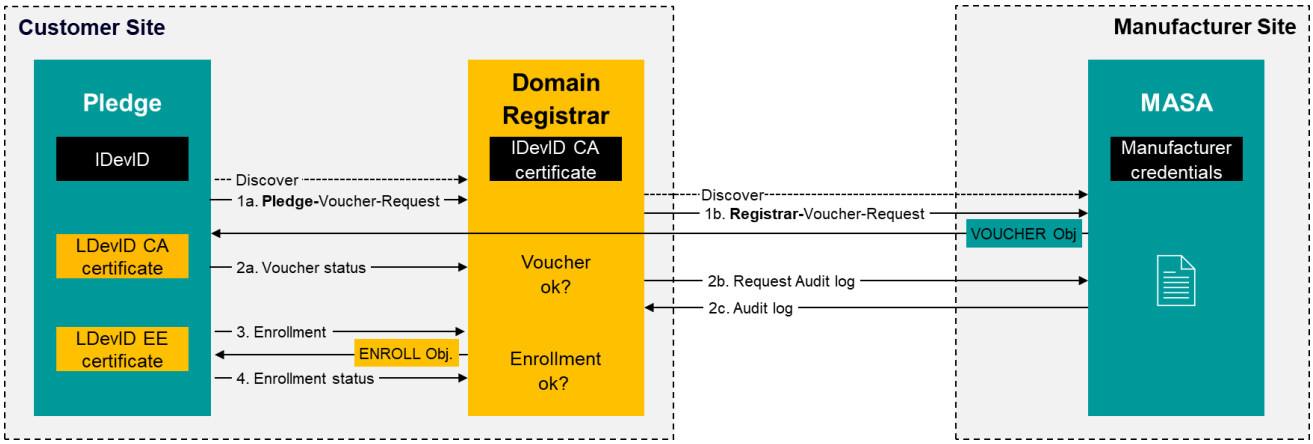

Figure 3. Onboarding Example: - Bootstrapping Remote Secure Key Infrastructure [10]

Manufacturer-issued credentials should not be used beyond bootstrapping. While IDevIDs have a longer, sometimes even undetermined lifetime, LDevIDs are updated more regularly and are under control of the operator, responsible for the security of his operational environment.

Based on the established trust relations and credentials, further operational data, like service-related configuration and engineering information including security parameters, can be provisioned on the device. To perform this comprehensive step, several technical approaches for onboarding have been developed, and furthers are likely to appear.

Several variants and approaches for supporting mutually trusted onboarding have been standardized. They provide similar functionality in terms of onboarding a component into an operational environment but differ in the respective interaction model. This relates specifically to the involvement of different service actors in the onboarding process, like the manufacturer. While some solutions are intended independent from the later application, others are part of an application framework. The following overview provides examples for the different cases:

- Bootstrapping Remote Secure Key Infrastructure (BRSKI, [10]), as shown in Figure 3, provides a standardized way to establish a mutually trusted relation between a new device (also called pledge) and a customer site network. It is supported by a manufacturer service known as Manufacturing Authorized Signing Authority (MASA) based on a voucher object for trust establishment. After discovery of the domain registrar, the pledge requests a voucher from its MASA via the domain registrar. The corresponding MASA is identified using the so-called MASA-URI extension, which is part of the IDevID certificate of the pledge. The voucher is a signed statement containing a trust anchor (as the "pinned-domain-cert") used to allow the pledge to verify the domain registrars certificate. During the onboarding procedure, the pledge voucher request (PVR) undergoes some intermediate processing by the domain registrar, in the target domain. The original voucher request from the pledge (PVR) is wrapped into a new registrar voucher request (RVR), which contains further information about the domain. The requests allow the MASA to verify it is issuing a voucher to a device produced by that manufacturer and that it has a certain trust relation to the target operative domain. Once trust has been established, domain specific security credentials (LDevID) can be enrolled to the new device. The LDevID credentials make the device a member of the domain and can be used to secure the further system interaction. The enrollment utilizes Enrollment over Secure Transport (EST) [11] for certificate management. Enhancements to BRSKI exist, supporting alternative enrollment protocols as BRSKI-AE [12] using the Lightweight Profile LCMPP [13] of the Certificate Management Protocol (CMP) [14]). Further enhancements support scenarios in which the joining device acts as server, rather than as a client (BRSKI-PRM, [15]). It needs to be triggered for interaction rather initiating the discovery of domain components upon boot. Even further variations exist which take more constraint setups into account (cBRSKI, [16]). cBRSKI uses more compact encoding with the Concise Binary Object Representation (CBOR) instead of the JavaScript Object Notation (JSON) encoding and CoAP-over-DTLS instead of HTTP-over-TLS.
- Secure Zero Touch Provisioning Protocol (SZTP) [17] specifies a further onboarding approach employing a so-called ownership voucher, which accompanies a device along its lifecycle. As in BRSKI above, the voucher is issued by a MASA. SZTP supports mutual trust establishment and enrollment of domain specific credentials and further operational information is supported by a bootstrapping server. This SZTP defined component may provide operational information directly to the new device or provide redirect information allowing to incorporate already existing services in the operational environment.
- FIDO Device Onboarding (FDO) [18] enables building a trust relation of a device to a new owner, based on trust in

the previous owner, also supported by an ownership voucher. As the manufacturer is only involved at the beginning, the interaction with the voucher is facilitated by a so-called rendezvous server instead of a service of the manufacturer as in BRSKI and SZTP. This server provides the rendezvous point between the device and the onboarding service in the new owner's domain allowing to perform a mutual authentication between the device and the new owner, based on the ownership voucher and attestation information from the device.

- OPC UA Device Onboarding specified in the OPC UA specification Part 21 [19] provides mechanisms for verifying the authenticity of devices to be onboarded and to set up their security configuration as part of the overall OPC-UA framework. It uses so-called tickets, which are similar to vouchers used in BRSKI. As BRSKI, also OPC-UA includes manufacturer specific information in the IDevID certificate as Product-Instance-URI.

As stated above, part of the onboarding is typically the enrollment of operational certificates to allow for domain-specific identification and authentication of new devices. As for onboarding, a variety of approaches exist also for enrollment. Two of them, EST and CMP, have already been stated above.

In addition to pure onboarding or provisioning standards, further standards support the propagation of security-relevant data. Specifically for the enrollment as part of the onboarding, certificate transparency [20] is known that provides an extension to PKI services for publicly logging issued certificates. As seen in the onboarding examples outlined before, certificates play a crucial role during onboarding but also during operation as they are used to identify and authenticate operational devices. This makes trust in the issuer even more important. Certificate transparency allows to identify certificates that have been issued inappropriately. Based on this information, potential impersonation attacks using unauthorized issued certificates can be detected. This underlines that logging information about issued security relevant parameters and procedures supports the root cause analysis in failure situation. The following section will outline an approach to providing enhanced information, which can be used for decision support and actually used onboarding techniques with the goal to have transparency that in turn can further support root cause analysis.

IV. ONBOARDING TRANSPARENCY ENHANCEMENTS

As discussed in Section III, several onboarding approaches are known. It is very likely that a device may only support a single or some few technical onboarding approaches, while the infrastructure likely supports multiple approaches. This will ensure that devices can be easily integrated in environments even if they originate from different manufacturers and support different onboarding and provisioning standards. To select the appropriate onboarding approach at the earliest point in time, the device-supported technical onboarding approach may be contained in the IDevID certificate, which can be analyzed by the first network component during network attachment. While standards like BRSKI or OPC-UA provide information from which the onboarding approach can be implicitly derived, the proposal here targets explicit information provisioning of the actual supported onboarding technique.

As the IDevID certificate is essentially an X.509 certificate, it can include so called extensions. An `extension` is added as certificate component similar to other certificate components like the `subject` or the `issuer`. If the extension is known to the relying party, it can be verified by the relying party. It is also possible to enforce the verification of such an extension by marking it as `critical`, which enforces the verification. If a relying party would not support the extension, it would not be allowed to further process the certificate. As the intention is here to support the onboarding in operational environments, which want to support transparency, but not to block usage in others, the extension is not marked as `critical`.

To provide information about supported onboarding and provisioning approaches, a new X.509 certificate extension is defined as shown in Figure 4.

```
supportedProvisioningMethods EXTENSION ::= {
  SYNTAX SupportedProvisioningMethods
  IDENTIFIED BY id-ce-SupportedProvisioningMethods }

SupportedProvisioningMethods ::= ProvisioningDescription
{{ ProvisioningMethod }}

ProvisioningMethod::= SEQUENCE {
  provisioningMethod     Name,
  provisiningId          OBJECT IDENTIFIER OPTIONAL,
  provisioningVersion    integer OPTIONAL
}

ProvisioningMethod ::= {CMP, SCEP, EST, CMC, ACME, FDO,
OMA-DM, OPC-UA-P21, BRSKI, SZTP, …}
```

Figure 4. Proposed Provisioning Certificate Extension

Out of the listed `ProvisioningMethod`, a device may support one or multiple options. As an example, a device with an IDevID certificate containing the information `ProvisioningMethod ::= {EST, BRSKI}` provides the information that it supports BRSKI for onboarding and EST for certificate management. The proposed enhancement is independent of the specific chosen onboarding method as it relies only on the X.509 certificate utilized to carry the onboarding transparency information. This onboarding transparency information may then be used as following.

A target network infrastructure may be designed in a way to have different virtual LANs (VLAN) defined for different onboarding mechanisms, to keep new devices contained within a separate network zone until they have received their LDevID. A motivation for this separation can be argued by different security properties of the onboarding mechanisms. As described in Section III, onboarding may be done based on TOFU, unilateral authentication of the device, or based on mutual authentication and trust establishment between the device and the domain. In case of a security breach, it may be desired to verify, how certain devices have been introduced into the operational environment and have established mutual trust to better find the root cause of a security problem.

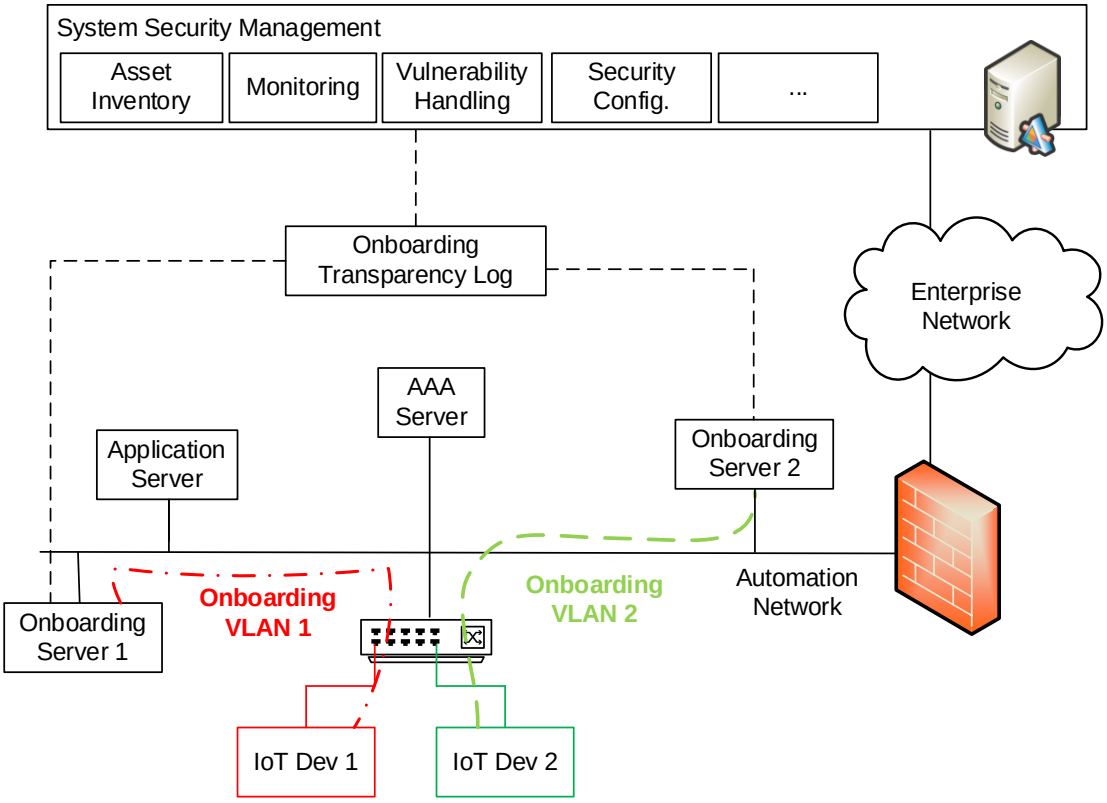

Figure 5. Onboarding Decision Support and Onboarding Transparency.

The proposed extension provides exactly this information, which can be utilized for auditing.

During the onboarding process, if the IDevID carries the extension with the onboarding and provisioning information, the device can be assigned to the appropriate VLAN based on its supported provisioning methods. This is depicted in Figure 5 above.

The figure shows an example with two devices (IoT Dev 1, IoT Dev 2). Depending on the provisioning methods supported by the respective device, they are connected by the network access switch to the onboarding VLAN1 (for local onboarding, e.g., OPC-UA-P21) or to VLAN2 (for infrastructure-based onboarding, e.g., BRSKI).

The evaluation of the supported onboarding and provisioning methods and the decision is made in the example by the AAA server to which the IoT device authenticates itself during network access. This enables the AAA server to select a specific onboarding and provisioning method, if the IoT device supports different approaches. Thus, it is possible for the AAA server to provide information on the provisioning method to be used by the device based on the assigned VLAN. Note that this may require a specific naming of the VLAN to reveal the expected onboarding mechanism to be used. This has the advantage that the device does not have to try several provisioning methods to determine the one supported by the operational network and that the device can continue to temporarily block other provisioning methods so that they cannot be misused. As a sidenote, it is expected that specifically in the case of constraint devices a device will only support a single onboarding and provisioning mechanism, while the operational infrastructure is considered more capable and to support multiple mechanisms.

While the proposed method eases the automated assignment of devices to the correct onboarding VLANs, the finally chosen onboarding variant should be logged in an onboarding transparency service. This is specifically helpful in case of security breaches, as the root cause may be related to the method how the device has been introduced into the network.

The information about onboarding may be provided as data structure encoded in different formats like XML or JSON and is ideally signed by the onboarding server. The onboarding transparency log can then verify the signature either directly or in case of a security breach. The data structure may contain different sets of information like

- Device identification (e.g., product serial number, fingerprint of the IDevID certificate of the device or the IDevID certificate directly)
- Time stamp of the actual onboarding
- Voucher issued during the onboarding. The voucher shows which device from which manufacturer was put into operation in which target (sub-)domain.

- Number of successful onboarding processes: Information on the history of the device can be provided, e.g., how often the device has already been put into operation in other domains.
- Issued LDevID certificate for the device (or a fingerprint of the LDevID certificate). This information can also be linked to the known approach of Certificate Transparency [20].

As stated, the information may be helpful in performing root cause analysis in case of discovered anomalies in an operational network. As shown in Figure 5, this information may be queried by an overall system security management and correlated to further information from monitoring, asset management or vulnerability databases.

V. EVALUATION

This section gives a preliminary evaluation of the presented concept regarding derived duties for the involved parties and components.

Device manufacturer perspective: It is assumed that a manufacturer is able to imprint IDevID certificates to devices during production. Either an own Public Key Infrastructure (PKI) or PKI services of third-party providers can be used. To support the proposed extension, issued IDevID certificates need to be extended to encode the device's onboarding capabilities. This may require an information exchange between the manufacturing site and a device database containing information to prepare for later onboarding operations.

End device implementation perspective: Besides possessing an IDevID certificate including the onboarding extension, a device may need to be configurable with a VLAN identifier to be used for onboarding to support deployments where operators use a dedicated VLAN for onboarding. Alternatively, a default VLAN can be used for the onboarding network as outlined in [21]. Devices supporting multiple onboarding mechanisms may try to perform onboarding using one of the supported approaches by discovering onboarding components in the network as specified in [22] for the different variants of BRSKI.

Domain operator network attachment perspective: The AAA server of the operator's domain (given the example in Figure 5) should be able to inspect and validate the contained certificate extension during network attachment, either directly or via a service for certificate validation, to assign a specific VLAN for device onboarding and provisioning if desired. Alternatively, the AAA server itself may act as provisioning server and signal the onboarding variant.

Domain operator onboarding server perspective: The onboarding and provisioning server may support multiple different onboarding mechanisms. An operator should support a discovery mechanism to allow devices to discover the onboarding server without additional configuration. The onboarding techniques described in Section III support this discovery in their specification already. In addition, as for BRSKI several variants are specified, [22] provides a solution approach to discover the specific BRSKI variants supported by the infrastructure.

Domain operator system security management perspective: If onboarding transparency is supported in the operator's domain, the information of the chosen onboarding and provisioning mechanism needs to be kept in either the onboarding server or directly in the system security management. An operator may also choose to store this information in its asset management database containing further details of the utilized components in his operational network. It allows verifying how and when a certain device has been onboarded within the operator domain, so that this information can be used for device security purposes.

Engineering perspective: Leveraging the onboarding transparency extension may require the setup of different VLANs for the intended onboarding mechanisms (given the example in Figure 5). If different VLANs are used, the naming should be done accordingly to allow a device to utilize this information to select the associated mechanism. Alternatively, devices may use discovery functions to detect if the domain supports an onboarding server matching their technical capabilities.

VI. CONCLUSION AND OUTLOOK

This paper provides an overview on onboarding and provisioning as part of introducing devices into a network and to provision the devices with information to securely communicate with other devices. This is done from a requirements point of view by investigating regulative requirements as well as motivating the functionality from a general viewpoint to support root cause analysis in case of security breaches. Moreover, different standardized technical approaches have been investigated to underline the variety of possible onboarding approaches. In addition, the paper proposes enhancements to currently known approaches and processes to leverage information about supported onboarding and provisioning methods of new devices, as well as the finally chosen onboarding approach during introduction into the operational network.

A main contribution of this paper is the usage of the onboarding method information to perform access decisions as well as in the aftermath of a security event, e.g., if the device or the network was compromised. The onboarding information may support system security management to identify, which network element caused the breach, which in turn can be used to provide a fast remediation.

While the described approach has been investigated from a conceptual point of view, a further evaluation about required support from the devices and also from the operational infrastructure has been included. It is planned to investigate further into a proof of concept to verify effectiveness of the proposed approach. As outlined in the evaluation, such a proof of concept requires enhancements during the issuing of IDevIDs and LDevIDs to include the supported and chosen onboarding method in the extension of the utilized X.509 certificates. Moreover, it also requires enhancements in the evaluation of the additional onboarding information during security decisions in the operational phase and the consideration in potential post-event analysis.

ACKNOWLEDGEMENT

We would like to thank Thomas Werner for his thoughtful review and comments particularly to the discussed onboarding technologies.

REFERENCES

[1] S. Fries and R. Falk, "Device Onboarding Transparency – Supporting Initial Trust Establishment", International Conference on Emerging Security Information, Systems and Technologies, November 3 to 7, 2024, Nice, France, pp. 47-51, 2024. [Online]. Available from: https://www.thinkmind.org/library/SECURWARE/SECURWARE_2024/securware_2024_2_40_30026.html, [retrieved: February, 2025]

[2] "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union", Document 02022L2555-20221227, Dec. 2022, [Online]. Available from: https://eur-lex.europa.eu/eli/dir/2022/2555, [retrieved: February, 2025]

[3] "Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance", Nov. 2023, [Online]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053 [retrieved: February, 2025]

[4] "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)", , Document 32024R2847, Nov. 2024, [Online]. Available from: https://eur-lex.europa.eu/eli/reg/2024/2847/oj [retrieved: February, 2025]

[5] "Executive Order 14028: Improving the Nation's Cybersecurity", May 2017, [Online]. Available from https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity [retrieved: February, 2025]

[6] IEC 62443, "Industrial Automation and Control System Security" (formerly ISA99), [Online]. Available from: http://isa99.isa.org/Documents/Forms/AllItems.aspx [retrieved: February, 2025]

[7] NIST CSF, "The NIST Cybersecurity Framework (CSF) 2.0", Feb. 2024, [Online]. Available from: https://doi.org/10.6028/NIST.CSWP.29 [retrieved: February, 2025]

[8] ITU-T X.509 ISO/IEC 9594-8:2020, Rec. ITU-T X.509 (2019), Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, [Online]. Available from: https://www.itu.int/rec/T-REC-X.509-201910-I/en, [retrieved: February, 2025]

[9] S. Fries and R. Falk, "Supporting Cryptographic Algorithm Agility with Attribute Certificates", International Journal on Advances in Security, Vol 17, No 1&2, 2024, pp. 92-98. [Online]. Available from: https://www.iariajournals.org/security/sec_v17_n12_2024_paged.pdf, [retrieved: February, 2025]

[10] M. Pritikin, M. Richardson, T. Eckert, M. Behringer, and K. Watson, IETF RFC 8995, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", May 2021, [Online]. Available from: https://datatracker.ietf.org/doc/html/rfc8995, [retrieved: February, 2025]

[11] M. Pritikin, P. Yee, and D. Harkins, IETF RFC 7030, "Enrollment over Secure Transport", October 2013, [Online]. Available from https://datatracker.ietf.org/doc/html/rfc7030, [retrieved: February, 2025]

[12] D. von Oheimb, H. Brockhaus, and S. Fries IETF Draft, "Alternative Enrollment Protocols in BRSKI (BRSKI-AE)", Work in Progress, [Online]. Available from: https://datatracker.ietf.org/doc/draft-ietf-anima-brski-ae/, [retrieved: February, 2025]

[13] H. Brockhaus, D. von Oheimb, and S. Fries IETF RFC 9483, "Lightweight Certificate Management Protocol (CMP) Profile", November 2023, [Online]. Available from: https://datatracker.ietf.org/doc/html/rfc9483, [retrieved: February, 2025]

[14] C. Adams, S. Farrell, T. Krause, and T. Mononen, IETF RFC 4210, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", September 2005, [Online]. Available from https://datatracker.ietf.org/doc/html/rfc4210, [retrieved: February, 2025]

[15] S. Fries, T. Werner, E. Lear, and M. Richardson., IETF Draft, "BRSKI with Pledge in Responder Mode (BRSKI-PRM)", Work in Progress, [Online]. Available from: https://datatracker.ietf.org/doc/draft-ietf-anima-brski-prm/, [retrieved: February, 2025]

[16] M. Richardson, P. van der Stok, P. Kampanakis, and E. Dijk, IETF Draft "Constrained Bootstrapping Remote Secure Key Infrastructure (cBRSKI)", Work in Progress, [Online]. Available from: https://datatracker.ietf.org/doc/draft-ietf-anima-constrained-voucher/, [retrieved: February, 2025]

[17] K. Watsen, M. Abrahamsson, and I. Farrer, IETF RFC 8572, "Secure Zero Touch Provisioning (SZTP)", June 2021, [Online]. Available from: https://datatracker.ietf.org/doc/rfc8572, [retrieved: February, 2025]

[18] FIDO Device Onboarding, [Online]. Available from https://fidoalliance.org/device-onboarding-overview/, [retrieved: February, 2025]

[19] OPC Foundation, "OPC 10000-21: UA Part 21: Device Onboarding", Nov. 2022, [Online]. Available from: https://reference.opcfoundation.org/Onboarding/v105/docs/, [retrieved: February, 2025]

[20] B. Laurie, E. Messeri, and R. Stradling, IETF RFC 9162, "Certificate Transparency Version 2.0" Dec. 2021, [Online]. Available from: https://datatracker.ietf.org/doc/html/rfc9162, [retrieved: February, 2025]

[21] A. Dekok and M. Richardson, IETF Draft "EAP defaults for devices that need to onboard", Work in Progress, [Online]. Available from: https://datatracker.ietf.org/doc/draft-richardson-emu-eap-onboarding/, [retrieved: February, 2025]

[22] T. Eckert and E. Dijk, "BRSKI discovery and variations", Work in Progress, [Online]. Available from: https://datatracker.ietf.org/doc/draft-ietf-anima-brski-discovery/, [retrieved: February, 2025]