Device Onboarding Transparency – Supporting Initial Trust Establishment

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

***Abstract*—Device onboarding is the process of introducing devices into target systems and target domains, and further on to bring them into operational state. This has a direct relation to cybersecurity, as it establishes trust between the device and the domain based on identities and associated cryptographic parameters. Different technologies for automated device onboarding have been specified. Having information on performed onboarding is important during operation, in which the identities and cryptographic parameters are maintained as part of device lifecycle management. Current onboarding approaches do not explicitly consider binding this information to the device management information used during operation. The binding information may be specifically important if attacks occur, as 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. This paper proposes enhancements to current onboarding approaches that provide this transparency.**

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

I. INTRODUCTION

Device onboarding can be described as introduction of a new device into an operational environment. This introduction typically comprises different exchanges of information about the identity of the onboarding device and its capabilities, as well as the provisioning of the device with operational parameters of the deployment environment to serve the intended purpose. This typically comprises also domain specific security parameters, like a locally assigned device identity and associated credentials.

New devices in a system may have an influence on the security status of the overall operational environment. 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 the system.

Technically, there have already several solutions been specified that support the onboarding of devices in new deployment environments in a secure way. While they differ in their detailed functionality, they can be used to ensure that only known and devices are put into operation as intended. Solutions range from Trust-On-First-Use (TOFU), which focuses on the initial use of a device in its new operational environment implicitly assumed to be trustworthy during onboarding, 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 system, it 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, from the development of the product from an idea to the final product, covering the processes and the technical features of the product. Meanwhile there are regulative requirements for both, system operators and product manufacturers to consider security as integral part of operation and manufacturing. As 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.

This paper is structured in the following way. Section II provides an overview about related work. It concentrates on regulative boundary conditions and standardized system security requirements. 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 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 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 and have a clear relation to being able to monitor the security state of components, as well as 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

Examples from Europe are provided by the NIS2 directive [1] that describes minimum cybersecurity means to be realized by entities operating critical infrastructures in 18 different sectors (application domains). The Radio Equipment Directive (RED) [2] and also the EU Cyberresilience Act [3], which are currently defined, target product manufacturers and pose specific cybersecurity requirements on the products and the related product development process.

An example from US is provided by the executive order EO 14028 [4], requiring operators beyond others to maintain a dedicated security level, obligate incident reporting, and specifically address the security in the supply chain.

B. Requirements Engineering Standards

Various requirement standards for procedural and technical 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.

A holistic cybersecurity framework defining specific requirements for automation system operators, integrators, and manufacturers is provided by IEC 62443 [5]. While it has been developed with the focus on industrial automation and control systems, it has already been adopted in the power system industry, railway industry, and healthcare for cybersecurity requirement specification. Moreover, it is the main base for creating harmonized standards to address the requirements from regulation and to provide means to show conformity. 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 [6] 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 considered as process to introduce devices into a target domain and to bring them into operational state. This process has direct relation to cybersecurity, as it includes the trust establishment of the domain into the device in the first step. There may be situations, in which it is also required to support the trust establishment of the device into the domain to ensure that a device is operated in its intended environment. Approaches, which do not require the device to verify the domain are often called “trust-on-first-use”, while approaches in which an explicit trust establishment is performed may be understood as mutually trusted onboarding.

Key for the trust establishment are identities and corresponding cryptographic key material, which is imprinted into devices during product manufacturing. Identity information of the device is provided, along the supply chain as shown in Figure 1. It is issued by the manufacturer together with cryptographic information, as X.509 certificate [7] and known as IDevID (Initial Device Identity).

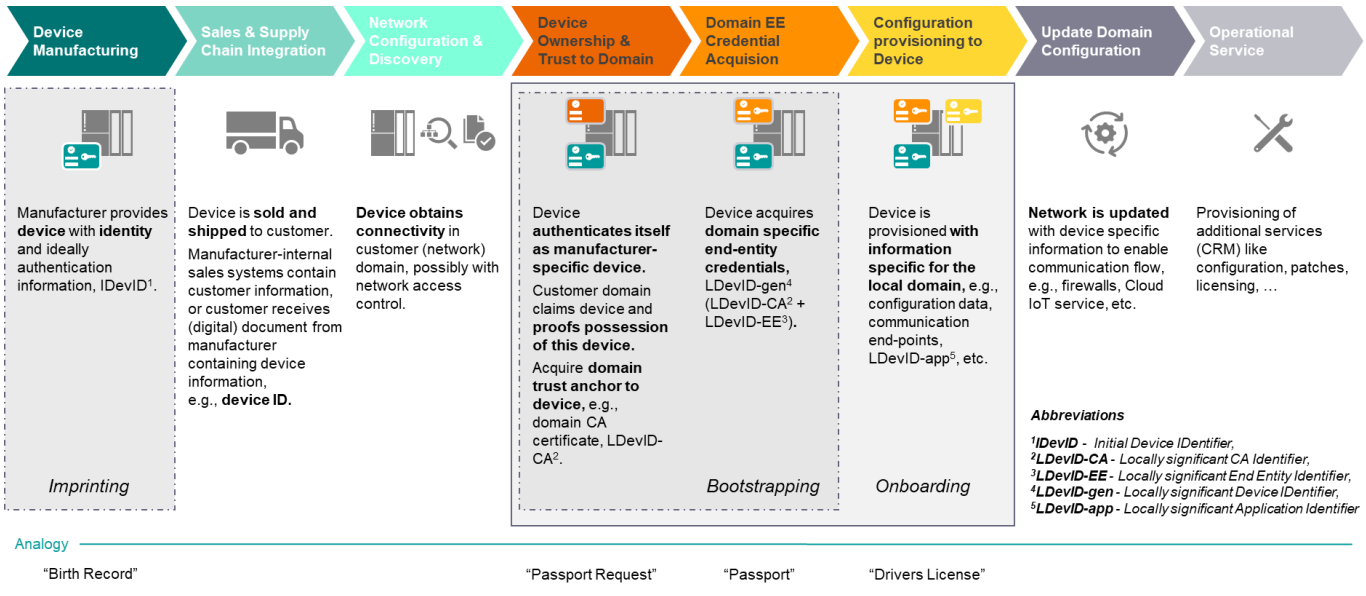

Figure 1. Onboarding Overview: From Imprinting in Factory to Operation.

In the target domain, it can be used to bootstrap mutual trust in an automated way and to support issuing domain-related identities and associated cryptographic keys, known as LDevID (Locally significant Device Identity), as operational credentials.

Based on the established trust relations and credentials, further operational data, like configuration and engineering information including security parameters, can be provided to the device. To achieve this, several technical approaches for onboarding and provisioning already exist. Examples for onboarding are specified as:

- Bootstrapping Remote Secure Key Infrastructure (BRSKI, [8]) provides a standardized way to establish a mutually trusted relation between a device and a new network domain supported by a manufacturer service known as Manufacturing Authorized Signing Authority (MASA) based on a so-called voucher, a signed statement containing the domain certificate. Once trust is established, domain specific security credentials (LDevIDs) can be enrolled be used to secure the further system interaction. The enrollment utilizes Enrollment over Secure Transports (EST, [9]) as main approach. Enhancements to BRSKI exist, supporting alternative enrollment protocols (BRSKI-AE, [10]) using the Certificate Management Protocol (CMP, [11]) or scenarios, in which the joining device acts as server, rather than as client (BRSKI-PRM, [12]).
- Secure Zero Touch Provisioning Protocol (SZTP, [13]) specifies a further approach employing a so-called ownership voucher, which accompanies a device along its lifecycle. It supports the mutual trust establishment and enrollment of domain specific credentials and further operational information.
- FIDO Device Onboarding (FDO, [14]) enables building a trust relation of a device into a new owner, based on the trust into 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 rendezvous server instead of a service of the manufacturer.
- OPC-UA Device Onboarding (Part 21, [15]) provides mechanisms to verify the authenticity of devices to be onboarded, to set up their security and to maintain their configuration. For this it uses so-called tickets, which can be understood as vouchers.

As stated above, part of the onboarding is typically the enrollment of operational certificates. As for onboarding, also for enrollment, there exists a variety of approaches, two of them, EST and CMP, have already been named.

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 [16] is known that provides an extension to PKI services for publicly logging issued certificates. This is intended to identify certificates that have been issued inappropriately.

IV. PROPOSED ONBOARDING ENHANCEMENTS

As discussed in Section II, there are several onboarding approaches known and applied. It is very likely that a device may only support one onboarding approach, while the infrastructure likely supports multiple approaches. This will ensure that in environments utilizing different standards, products from different vendors can be easily integrated. To select the appropriate onboarding approach at the earliest point in time, the supported technical onboarding approach may be contained in the IDevID certificate, which can be analyzed by the first network component during network attachment. As the IDevID certificate is essentially an X.509 certificate, it can be enhanced by so called extensions. An `extension` is added as certificate component similar to other certificate components like the `subject` or the `issuer`.

To provide information about supported onboarding and provisioning approaches, a new extension is defined as shown in Figure 2.

```
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 2. 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 transparency information.

A target network infrastructure may be designed in a way to have different virtual LANs (VLAN) defined for different onboarding approaches, to keep new devices contained within a separate network zone until they have received their LDevID. 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 3 below.

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).

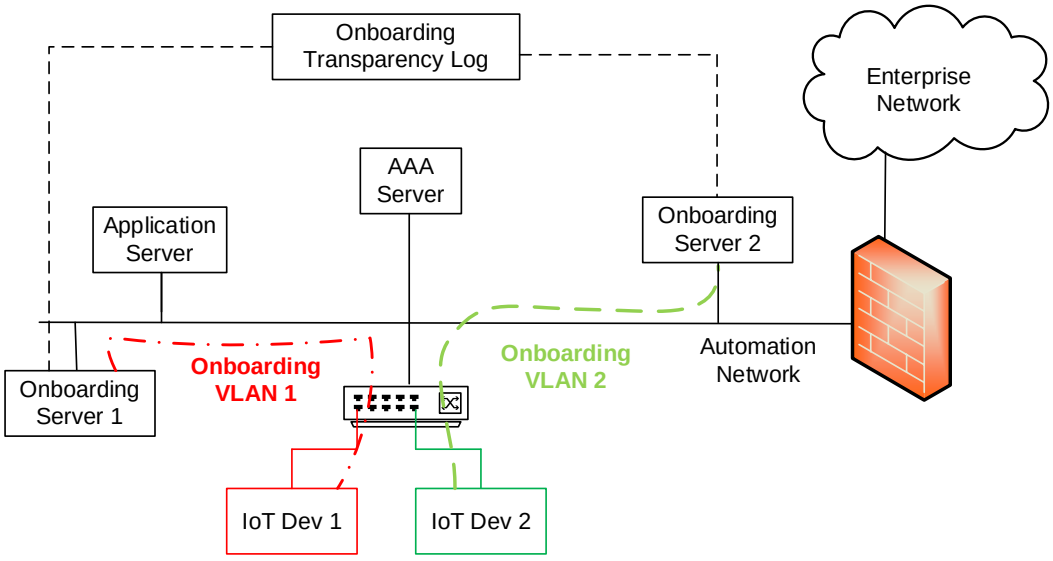

Figure 3. Onboarding Decision Support and Onboarding Transparency.

The check of the supported provisioning methods and the decision is made here by the AAA server to which the IoT device authenticates itself during network access. It is also possible for the AAA server to provide information on the provisioning method to be used by the device if multiple methods are supported. This has the advantage that the device does not have to try several provisioning methods to determine one that is supported by the connected network and that the device can continue to temporarily block other provisioning methods so that they cannot be misused.

While the proposed method eases the automated assignment of devices to the correct onboarding VLANs, the finally chosen onboarding variant may 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. This 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 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 [16].

As stated, the information may be helpful in performing root cause analysis in case of discovered anomalies in an operational network.

V. Conclusion and Outlook

This paper provides an overview on onboarding and provisioning as part of introducing devices into a network and to provide the devices with information to securely communicate with other devices. This is done from a general viewpoint and by investigating different standardized technical approaches. In addition, it proposes enhancements to the currently known approaches and processes to leverage information about supported onboarding and provisioning methods of new devices, as well as the actually chosen onboarding approach during network introduction.

The novel 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 has been compromised. The onboarding information may support the identification 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, it is planned to investigate into a proof of concept to verify effectiveness of the proposed approach. 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.

REFERENCES

[1] "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: September, 2024]

[2] "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", 10/2023, [Online]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053 [retrieved: September, 2024]

[3] "Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/10202", COM/2022/454 final, Document 52022PC0454, Sep. 2022, [Online]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454 [retrieved: September, 2024]

[4] "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: September, 2024]

[5] IEC 62443, "Industrial Automation and Control System Security" (formerly ISA99), [Online]. Available from: http://isa99.isa.org/Documents/Forms/AllItems.aspx [retrieved: September, 2024]

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

[7] 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: September, 2024]

[8] 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: September, 2024]

[9] 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: September, 2024]

[10] 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: September, 2024]

[11] 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: September, 2024]

[12] 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: September, 2024]

[13] 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: September, 2024]

[14] FIDO Device Onboarding, [Online]. Available from https://fidoalliance.org/device-onboarding-overview/, [retrieved: September, 2024]

[15] OPC Foundation, "OPC 10000-21: UA Part 21: Device Onboarding", Nov. 2022, [Online]. Abailable from: https://reference.opcfoundation.org/Onboarding/v105/docs/, [retrieved: September, 2024]

[16] 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: September, 2024]