Attesting the Trustworthiness of a Credential Issuer

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

***Abstract*—In some industrial environments, authentication credentials as device certificates may be issued locally. However, a locally issued credential may not be as trustworthy as credentials issued by a highly protected centralized security infrastructure. An attestation of the credential issuer can confirm evidence of its trustworthiness. Including such an attestation of the credential issuer within an issued authentication credential allows a relying party to check this information as part of credential validation. This paper proposes to embed such a cryptographically verifiable integrity attestation of a certificate issuer into issued authentication certificates.**

Keywords–cybersecurity; attestation; credential; digital certificate; device authentication, industrial security.

I. INTRODUCTION

Authentication credentials, e.g., digital certificates or authentication tokens, allow a user to authenticate, i.e., to prove a claimed identity. Credentials are conventionally issued by a highly protected issuer like a Certification Authority (CA) of a Public Key Infrastructure (PKI) following well-defined operational processes, or by an Identity and Access Management (IAM) service like for instance an Open Authorization (OAuth) [1] authorization server. However, other deployment options providing local independence and increased flexibility are used in Operation Technology (OT) as well. Digital certificates or authentication tokens may, e.g., be created by engineering tools, or locally on industrial devices implementing an embedded CA (also called Alias CA), or by an edge service. The execution environments that create such credentials may therefore have different technical protections, leading to different levels of trustworthiness. Some of the used execution environments might be manipulated, e.g., if a vulnerability in the implementation can be exploited.

This paper describes how to include within an issued digital certificate a cryptographically protected attestation that confirms the integrity of the issuer's execution environment at the point in time when the digital certificate was issued. The cryptographically protected attestation confirms the actual integrity evidence of the used execution environment. Including the attestation within issued authenticators allows verifying the integrity of the execution environment in which a credential has been created. The trustworthiness of a digital certificate can therefore be determined depending on the included issuer's integrity attestation.

This approach is specifically promising if a centralized, implicitly trusted PKI is not or at least not permanently available in an operational environment. The integrity attestation of the issuing device can provide an increased level of trustworthiness for device- generated credentials, as the attestation functionality that creates the attestation can be protected at a higher level than the functionality to which the attestation relates, in particular if a hardware-based attestation implementation is used.

The remainder of the paper is structured as follows: Section II provides an overview on boundary conditions given by industrial security requirements and on technical considerations when issuing credentials. Section III introduces the concept of providing a statement of the security of the credential issuer execution environment, allowing a relying party to determine trustworthiness in the issued certificates. Section IV concludes the paper and gives an outlook towards future work.

II. RELATED WORK

This section provides an overview of relevant related work.

A. Industrial Security

Protecting Industrial Automation and Control Systems (IACS) against intentional attacks is demanded by operators to ensure a reliable operation, by industrial security standards as IEC 62443 [2], and also by regulation [3][4]. Security requirements defined by the industrial security standard IEC 62443 range from security processes during development and operation of devices and systems, personal and physical security, device security, network security, and application security, addressing the device manufacturer, the integrator, as well as the operator of the IACS. IEC 62443 specifically describes in technical requirements on system and component level, targeting four different security levels, which relate to the strength of a considered attacker. Moreover, this framework also contains specific requirements regarding authentication methods and credentials, as well as the use of cryptographic algorithms including their strength.

Industrial security is also called OT security, to distinguish it from general Information Technology (IT) security. In OT systems, actions in the digital world typically have a direct

impact on the physical world. Therefore, industrial systems have different security priorities and requirements compared to common IT systems. Typically, availability and integrity of an automation system have higher priority than confidentiality. Specific requirements and side conditions of industrial automation systems like high availability, planned configuration (engineering info), scheduled maintenance windows, long life cycles, unattended operation, real-time operation, and communication, as well as safety requirements have to be considered when designing an OT security solution.

B. Considerations for Authentication Credentials

Authentication credentials are used to confirm the identity of a user (human, software process, or device) towards a relying party. Examples are, besides passwords, authentication tokens, but also digital certificates. A digital certificate binds the public key of a user to the user's identity. A digital certificate can include also a certificate practice statement that provides information on the trustworthiness of the issuing process as specified in [5]. A widely used certificate format in IT and also OT applications is X.509 defined by the International Telecommunication Union (ITU-T) [6].

A digital certificate is typically issued by a CA which may be part of an engineering tool, a device management tool, a local security server, on a device, an external PKI. Alternatively, self-signed certificates directly generated on the device may be used. Standards like Trusted Computing Group's TCG specification "Device Identifier Composition Engine" (DICE) [7] and Desktop Management Task Force (DMTF) specification "Security Protocols and Data Models" (SPDM) [8] define that a device can include an internal CA for issuing device certificates, called "embedded CA" or "alias CA". It allows a device to issue a device certificate that includes information on changeable device information as its firmware version.

Certificate transparency, specified by RFC9162 [9], allows to include issued Transport Layer Security (TLS) server certificates in a public log. A digital certificate can comprise an inclusion proof to confirm that the issued certificate has in fact been included in a certificate transparency log. This supports audit of issuing CAs to detect if a CA issued certificates that were not intended by the operating organization.

C. Remote Attestation

A remote attestation is a cryptographically protected data structure that can confirm security-relevant information called evidence about a device (platform attestation) or of a cryptographic key (key attestation). The Remote ATtestation procedureS (RATS) architecture [10] gives an overview on remote attestation use cases.

Meanwhile, standardization has started to adopt remote attestation also in the process of requesting certificates using different formats [11], which can be directly used in typical enrollment protocols. The defined extension allows to convey evidence and attestation results in certification requests. This in turn enhances the verification options of the issuing CA beyond the typical verification of proof-of-possession of the private key corresponding to the public key in the certification request and the proof-of-identity of the requestor to a statement about the platform properties that generated the request.

Once provided as part of a certification request, the attestation statement for the requestor may also be included in the issued certificate for later verification by the relying party.

Note that the focus of this paper is not the integrity attestation of the requestor of a certificate, but of the issuer. Both attestations can be combined, allowing to attest properties of the requester (e.g., a key attestation as statement how a keypair was generated), as well as security-relevant properties of the issuer's execution environment.

III. Issuing Credentials Including an Issuer Attestation

A digital certificate can include a cryptographically protected attestation that confirms the issuer's integrity at the point in time when the digital certificate was issued. The cryptographically protected attestation confirms the actual integrity evidence of the execution environment of the issuer. Including the attestation within issued digital certificate allows to verify the integrity of the execution environment in which the certificate has been created. The trustworthiness of a digital certificate can therefore be determined depending on the included issuer's integrity attestation.

A. Digital Certificate Including Issuer Attestation

A digital certificate binds a public key to the identifier of a subject (e.g., human user, device, process). It is signed by the issuer, e.g., a CA. It is proposed to include in addition an attestation that confirms the integrity of the issuer. For X.509 certificates, this can be easily realized by using the extension capability of certificates, allowing to include additional information by the issuer within an additional certificate extension field. This can be beneficial if it has to be assumed that the issuer itself could be manipulated, as it allows a peer validating the certificate to check the issuer's integrity status at the point in time when the digital certificate was issued.

Figure 1. Digital certificate including an integrity attestation of the issuer.

Figure 1 shows the main conceptual elements of a digital certificate that includes the issuer's attestation in addition to the subject's identity and public key. This is seen as specifically useful if the issuer is a so-called embedded CA

included on a device. The attestation included can be a platform attestation that allows verifying the integrity of the embedded CA issuing the digital certificate, as well as a key attestation confirming the key store type, e.g., a secure-element-based key store, of the issuer's key store, i.e., of the private key used to sign the issued digital certificate.

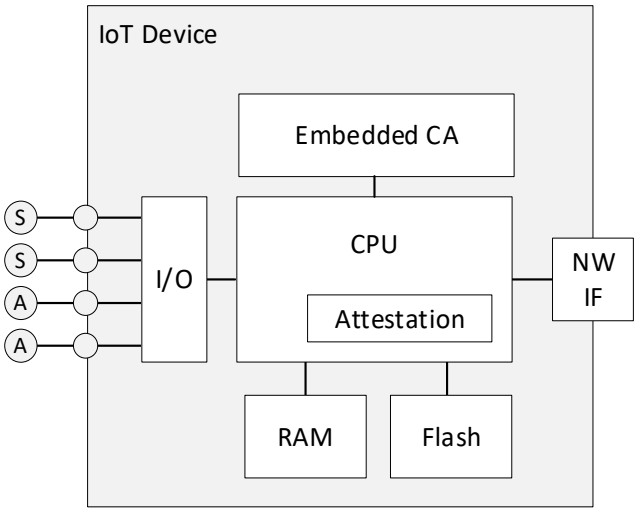

Figure 2. IoT device including an embedded CA.

Figure 2 shows an Internet of Things (IoT) device, e.g., an industrial control device, that includes an embedded CA for issuing digital device certificates. They may include identifying information, such as the device type and serial number, as well as the currently installed firmware version. The attestation included in the device certificate allows verification of the integrity status of the device, in particular of its embedded CA component.

The embedded CA on a device can be realized, e.g., by a dedicated secure element, a logically isolated enclave, or just a software component / app running on the device. This realization information may also be part of the attestation statement, which allows a relying party to make a more fine-grained decision about the issuer's trustworthiness. The device would include furthermore an Attestation Unit (AU), involving a measurement component to determine evidence in a trustworthy way (root of trust for measurements), and a component for issuing the attestation based on the determined evidence. Such attestation functionality is supported on common compute platforms, e.g., using a secure element that can be integrated in the CPU, as shown in Figure 2, or be a dedicated hardware component.

B. Issuing Process Adding Attestation Information

When a digital certificate including an issuer's attestation is to be issued, an attestation concerning the certificate issuer has to be determined and included on the digital certificate. So, the determined attestation can be added to the issued certificate as part of the certificate issuing process.

The Certification Unit (CU) comprises the Registration Authority (RA) and Certification Authority (CA). It includes also the Attestation Unit (AU) with its Attestation measurement Unit (AMU) and the Attestation Signing Unit (ASU). The CU may be an internal component of a device featuring an embedded CA, as well as an external CA (e.g., in an engineering tool or standalone). The CA uses a Hardware Security Module (HSM), e.g., a crypto controller, to create the digital signature of the certificate (Cert) that is then provided to the requesting device.

In the example message sequence shown in Figure 3, the RA extends the Certificate Signing Request (CSR) received form the device with the attestation determined by AU to create the "to-be-signed certificate" data structure (tbsCert) and sends it to the CA for signing, resulting in the signed certificate including the CU's attestation. First, the device generates its key pair and the corresponding certificate signing request (CSR) and sends it to the CU's RA. The RA obtains the CU's attestation (AttCu), from the AU, and extends the received CSR accordingly by adding the CU's attestation (AttCu) as extension to the "to be signed certificate" (tbsCert). The attestation includes evidence depending on the measurements that have been obtained by the AMU. The measurements are usually collected before the attestation is built (as shown in Figure 3). However, it is also possible to determine some measurements on demand, i.e., after the attestation has been requested. The measurements may cover information on the CU's components (RA, CA), e.g., the software version and integrity information of the compute platform on which they are executed. Examples are information on whether secure boot has been active during start-up, and integrity information of the loaded and executed operating system and its components. It is also possible to attest that certain software components, as here RA and CA, are in fact executed in a isolated, protected execution environment, in particular in a specific confidential computing environment. Validating such information allows to determine whether the CU can in fact by trusted by an *external* party. Such information is complementary to manual audits that are performed for centralized PKIs, e.g., on a yearly basis. Including such information in issued certificates allows even the parties validating the certificate to check whether the CA that issued this certificate was in fact in a trustworthy state at the time when this specific certificate was issued.

Besides the included information about the platform itself, the attestation may also contain freshness information. This allows the relying party to verify that the attestation was in fact provided as part of the issuing process, i.e., that it is not stale information that has been residing on the CA for a longer time period. Freshness may be provided in different ways like:

- Application of a nonce provided by the certificate requestor. This nonce may be provided as part of the certification request as outlined in [10] and [11].
- Usage of timestamps if a real-time clock is available
- Furthermore, a hash value created deterministically from certificate content may be used, binding the attestation to the issued certificate.

Which freshness approach is best suited depends on the specific deployment scenario and the available infrastructure. In industrial automation systems, often, no (reliable) real-time clock is available.

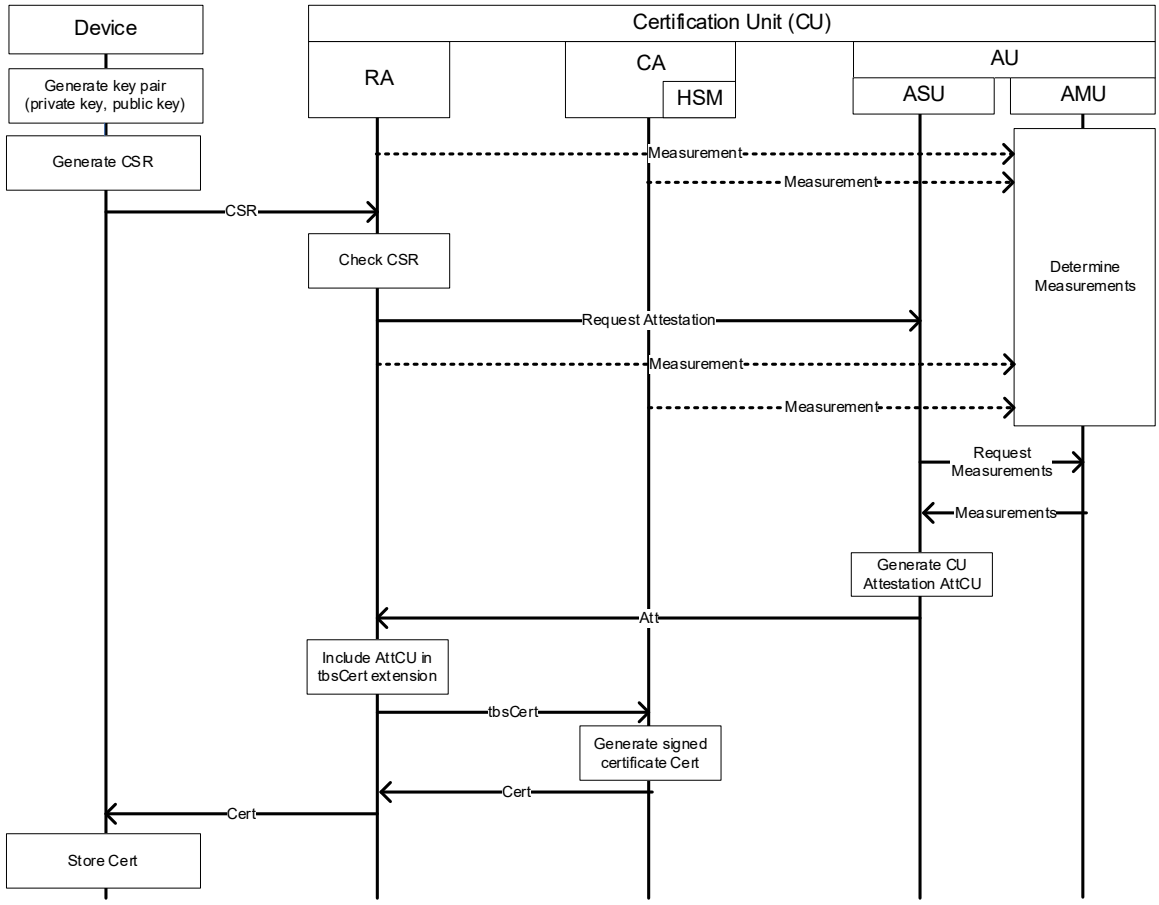

Figure 3. Including an attestation during credential issuing.

C. *Validation a Certificate Including an Issuer Integrity Attestation*

A device can provide its digital certificate including the additional attribute (extension) including the issuer's attestation when authenticating towards a communication peer, e.g., as part of

- Transport Layer Security (TLS) authentication and key agreement.
- Network attachment to provide the device certificate as data element, e.g., towards a device/network management system.
- Application-level protocols or data exchanges utilizing digital certificates.

The relying party validates the received digital certificate following the validation rules specified in X.509 [6], which include, e.g., the verification of the subject name, validity period, certificate revocation status, but also the integrity of the digital certificate itself. Besides the digital certificate itself, also the certification path is validated. This involves the certificate of the issuing CA. For acceptance, the results have to comply with an organization's security policy. The inclusion about an attestation statement of the issuing CA in the device certificate additionally allows to match the trustworthiness of the issuing CA to an expected state necessary for processing certain data. As indicated before, this is specifically interesting for embedded CAs. Depending on the trust evaluation based on the attestation statement, a relying party may decide to, e.g.,

- limit the authoritative actions the certificate holder may perform,
- perform additional plausibility checks on data received from the device,
- provide only uncritical or non-sensitive information to the device, or
- reject interaction completely if the certificate based on the issuer information does not match the expected trustworthiness.

The attestation statement included in a digital certificate enables a more specific interaction with a device depending on its own state but also depending on the state of the issuing CA at the time of issuing the certificate.

IV. Conclusion and Future Work

The concept described in this paper enhances authentication credentials with a statement confirming the credential issuer's platform security state. During validation, it can be matched with an operator's expectations regarding the trustworthiness of the certificate issuer. The approach allows a more fine-grained reaction based upon the attestation statement. It is planned to further evaluate the approach from a theoretical and practical perspective, including how it contributes to enhanced cyber-resilience in cyber-physical systems [12]. As part of the conceptual analysis is to analyze the expected overhead, and to evaluate relevant attack scenarios and the limitations. Further work is needed to determine how to deal with different attestation validation results. Besides rejecting a certificate, more specific reactions could be triggered, e.g., limiting associated access permissions, or planning a maintenance action as, e.g., replacement of the affected device. A prototypical implementation can support the evaluation of the performance overhead (e.g., increased size of certificates including attestation, added latency both for issuing and for validating such a certificate). Furthermore, specific scenarios of a compromised issuer can be evaluated, in particular for an issuer which security configuration is not compliant with an expected policy, and for a compromised issuer. It allows evaluating practically which scenarios can be detected based on the certificate issuer's attestation included in the certificate. The proposed approach relies on the property that the attestation functionality that creates the attestation is protected at a higher level than the credential issuing functionality to which the attestation relates. It can be evaluated in future work which attack scenarios would lead to a compromise of the attestation functionality, making the limitations of a particular attestation technology transparent. Such evaluations are the basis for deciding how well it fits a specific target environment. Which approach fits for protecting freshness of the attestation depends on the specific deployment scenario and the available infrastructure. As in industrial automation systems, often, no, or at least no reliable, real-time clock is available, other options, as outlined in Section III are alternative candidates.

Adding an issuer attestation to a certificate may be done in addition to certificate transparency [9], i.e., both approaches can be combined in a single solution. Monitoring issued certificates and the included issuer's attestation allows third parties furthermore to detect, independently of the actual usage of an issued certificate, if an issuer is not compliant anymore or if it becomes compromised. The comparison of such approaches and also of their combined usage is a further area for deeper investigation.

References

[1] D. Hardt, "The OAuth 2.0 Authorization Framework", IETF RFC 6749, October 2012. [Online]. Available from https://datatracker.ietf.org/doc/html/rfc6749 2025.08.06

[2] IEC 62443, "Industrial Automation and Control System Security" (formerly ISA99). [Online]. Available from: http://isa99.isa.org/Documents/Forms/AllItems.aspx 2025.08.06

[3] "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, November 2024. [Online]. Available from: http://data.europa.eu/eli/reg/2024/2847/oj 2025.08.06

[4] "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 2025.08.06

[5] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", IETF RFC 3467, November 2003. [Online]. Available from https://datatracker.ietf.org/doc/html/rfc3647 2025.08.06

[6] 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. 2020 [Online]. Available from: https://www.itu.int/rec/T-REC-X.509-201910-I/en 2025.08.06

[7] TCG, "DICE Layering Architecture Specification". Online]. Available from: https://trustedcomputinggroup.org/resource/dice-layering-architecture/ 2025.08.06

[8] DMTF, "Security Protocols and Data Models (SPDM)", DSP0274 Version V1.3.1. [Online]. Available from: https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_1.3.1.pdf 2025.08.06

[9] B. Laurie, E. Messeri, and R. Stradling, "Certificate Transparency Version 2.0", IETF RFC9162, December 2021. [Online]. Available from: https://datatracker.ietf.org/doc/rfc9162/ 2025.08.06

[10] H. Birkholz, D. Thaler, M. Richardson, N. Smith, and W. Pan, "Remote ATtestation procedureS (RATS) Architecture", RFC9334, December 2023. [Online]. Available from: https://datatracker.ietf.org/doc/rfc9334/ 2025.08.06

[11] M. Ounsworth, H. Tschofenig, H. Birkholz, M. Wiseman, and N. Smith, "Use of Remote Attestation with Certification Signing Requests", IETF Draft, March 2025. [Online], Available from https://datatracker.ietf.org/doc/draft-ietf-lamps-csr-attestation/ 2025.08.06

[12] R. Falk and S. Fries, "Enhanced Attack Resilience within Cyber Physical Systems", Journal on Advances in Security, vol. 16, no. 1&2, pp. 1-11, 2023. [Online]. Available from: https://www.iariajournals.org/security/sec_v16_n12_2023_paged.pdf 2025.08.06