Stream:	Internet Engineering Task Force (IETF)		
RFC:	9733		
Category:	Standards Track		
Published:	February 2025		
ISSN:	2070-1721		
Authors:	D. von Oheimb, Ed. *Siemens*	S. Fries *Siemens*	H. Brockhaus *Siemens*

RFC 9733
BRSKI with Alternative Enrollment (BRSKI-AE)

Abstract

This document defines enhancements to the Bootstrapping Remote Secure Key Infrastructure (BRSKI) protocol, known as BRSKI with Alternative Enrollment (BRSKI-AE). BRSKI-AE extends BRSKI to support certificate enrollment mechanisms instead of the originally specified use of Enrollment over Secure Transport (EST). It supports certificate enrollment protocols such as the Certificate Management Protocol (CMP) that use authenticated self-contained signed objects for certification messages, allowing for flexibility in network device onboarding scenarios. The enhancements address use cases where the existing enrollment mechanism may not be feasible or optimal, providing a framework for integrating suitable alternative enrollment protocols. This document also updates the BRSKI reference architecture to accommodate these alternative methods, ensuring secure and scalable deployment across a range of network environments.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9733.

Copyright Notice

Table of Contents

1. Introduction

Bootstrapping Remote Secure Key Infrastructure (BRSKI) [RFC8995] is typically used with Enrollment over Secure Transport (EST) [RFC7030] as the enrollment protocol for operator-specific device certificates, employing HTTP over TLS for secure message transfer. BRSKI-AE is a variant using alternative enrollment protocols with authenticated self-contained objects for the device certificate enrollment.

This approach offers several distinct advantages. It allows for the authentication of the origin of requests and responses independently of message transfer mechanisms. This capability facilitates end-to-end authentication (i.e., end-to-end proof of origin) across multiple transport hops and supports the asynchronous operation of certificate enrollment. Consequently, this provides architectural flexibility in determining the location and timing for the ultimate authentication and authorization of certification requests while ensuring that the integrity and authenticity of the enrollment messages are maintained with full cryptographic strength.

This specification carries over the main characteristics of BRSKI, namely:

- The pledge is assumed to have received its Initial Device IDentifier (IDevID) [IEEE_802.1AR-2018] credentials during its manufacturing. It uses them to authenticate itself to the Manufacturer Authorized Signing Authority (MASA) [RFC8995], to the registrar (which is the access point of the target domain), and to possibly further components of the domain where it will be operated.
- The pledge first obtains via the voucher [RFC8366] exchange a trust anchor for authenticating entities in the domain such as the domain registrar.

- The pledge then obtains its Locally Significant Device IDentifier (LDevID) [IEEE_802.1AR-2018]. To this end, the pledge generates a private key, called an "LDevID secret". Then, it requests via the domain registrar from the PKI of its new domain a domain-specific device certificate, called an "LDevID certificate". On success, it receives the LDevID certificate along with its certificate chain.

The objectives of BRSKI-AE are to enhance BRSKI by enabling LDevID certificate enrollment through the use of an alternative protocol to EST that:

- supports end-to-end authentication over multiple transport hops and
- facilitates secure message exchanges over any type of transfer mechanism, including asynchronous delivery.

It may be observed that the BRSKI voucher exchange between the pledge, registrar, and MASA involves the use of authenticated self-contained objects, which inherently possess these properties.

The existing well-known URI structure used for BRSKI and EST messages is extended by introducing an additional path element that specifies the enrollment protocol being employed.

This specification allows the registrar to offer multiple enrollment protocols, enabling pledges and their developers to select the most appropriate one based on the defined overall approach and specific endpoints.

It may be important to note that [RFC8995] specifies the use of HTTP over TLS, but variations such as Constrained BRSKI [cBRSKI], which uses the Constrained Application Protocol (CoAP) over DTLS, are possible as well. In this context, "HTTP" and "TLS" are used as references to the most common implementation, though variants using CoAP and/or DTLS are implied where applicable, as the distinctions are not pertinent here.

This specification, together with its referenced documents, is sufficient to support BRSKI with the Certificate Management Protocol (CMP) [RFC9480] as profiled in the Lightweight CMP Profile (LCMPP) [RFC9483]. Integrating BRSKI with an enrollment protocol or profile other than the LCMPP will necessitate additional IANA registrations, as detailed in this document. Furthermore, additional specifications may be required for the details of the protocol or profile, which fall outside the scope of this document.

1.1. Supported Scenarios

BRSKI-AE is designed for use in scenarios such as the following:

- When pledges and/or the target domain leverage an existing certificate enrollment protocol other than EST, such as CMP.
- When the application context precludes the use of EST for certificate enrollment due to factors such as when:
  - The Registration Authority (RA) is not co-located with the registrar and requires end-to-end authentication of requesters, which EST does not support over multiple transport hops.

- The RA or Certification Authority (CA) operator mandates auditable proof of origin for Certificate Signing Requests (CSRs), which cannot be provided by TLS as it only offers transient source authentication.
- Certificates are requested for key types, such as Key Encapsulation Mechanism (KEM) keys, that do not support signing or other single-shot proof-of-possession methods as those described in [RFC6955]. EST, which relies on CSRs in PKCS #10 format [RFC2986], does not accommodate these key types because it necessitates proof-of-possession methods that operate within a single message, whereas proof of possession for KEM keys requires prior receipt of a fresh challenge value.
- The pledge implementation employs security libraries that do not support EST or uses a TLS library lacking support for the "tls-unique" value [RFC5929], which EST requires for the strong binding of source authentication.

- When full RA functionality is not available on-site within the target domain, and connectivity to an off-site RA may be intermittent or entirely offline.
- When authoritative actions by a local RA at the registrar are insufficient for fully and reliably authorizing pledge certification requests, potentially due to a lack of access to necessary data or inadequate security measures, such as the local storage of private keys.

Bootstrapping may be managed in various ways depending on the application domain. Appendix A provides illustrative examples from different industrial control system environments and operational contexts that motivate the support of alternative enrollment protocols.

2. Terminology and Abbreviations

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document relies on the terminology defined in [RFC8995], [RFC5280], and [IEEE_802.1AR-2018], which is partly repeated here. Several further terms are also described here.

To be independent of the terminology of a specific enrollment protocol, this document utilizes generic terminology regarding PKI management operations.

The following terminology is used in this document:

asynchronous: the time-wise interrupted delivery of messages, here, between a pledge and some backend system (e.g., an RA).

attribute request: a message requesting content to be included in the certification request.

attribute response: a message providing the answer to the attribute request.

authenticated self-contained object: a data structure that is cryptographically bound to the identity of its originator by an attached digital signature on the actual object, using a private key of the originator such as the IDevID secret.

backend: the placement of a domain component separately from the domain registrar; it may be on-site or off-site.

CA certs request: a message requesting CA certificates.

CA certs response: a message providing the answer to a CA certs request.

certificate confirm: a message stating to the backend PKI that the requester of a certificate received the new certificate and accepted it.

certification request: a message requesting a certificate with proof of identity.

certification response: a message providing the answer to a certification request.

local RA: the same as LRA.

off-site: the locality of a component, service, or functionality (such as RA or CA) that is not at the site of the registrar. This may be a central site or a cloud service, to which connection may be intermittent.

on-site: the locality of a component, service, or functionality at the site of the registrar.

PKI/registrar confirm: an acknowledgment of the PKI on the certificate confirm.

pledge: a device that is to be bootstrapped into a target domain. It requests an LDevID using IDevID credentials installed by its manufacturer.

registrar: short for domain registrar.

site: the locality where an entity such as a pledge, registrar, or PKI component is deployed. The target domain may have multiple sites.

synchronous: the time-wise uninterrupted delivery of messages, here, between a pledge and a registrar or backend system (e.g., the MASA).

target domain: the domain that a pledge is going to be bootstrapped into.

The following abbreviations are used in this document:

BRSKI: Bootstrapping Remote Secure Key Infrastructure [RFC8995]

BRSKI-AE: BRSKI with Alternative Enrollment. Refers to a variation of BRSKI [RFC8995] in which BRSKI-EST, the enrollment protocol between the pledge and the registrar, is replaced by enrollment protocols that support end-to-end authentication of the pledge to the RA, such as CMP.

CA: Certification Authority

CMC: Certificate Management over CMS

CMP: Certificate Management Protocol [RFC4210] [RFC9480]

CMS: Cryptographic Message Syntax

CRMF: Certificate Request Message Format

CSR: Certificate Signing Request

EST: Enrollment over Secure Transport [RFC7030]

IDevID: Initial Device IDentifier (of a pledge, provided by the manufacturer and comprising of a private key and the related X.509 certificate with its chain).

LCMPP: Lightweight CMP Profile [RFC9483]

LDevID: Locally Significant Device IDentifier (of a pledge, provided by its target domain and comprising of a private key and the related X.509 certificate with its chain).

LRA: Local Registration Authority. A subordinate RA that is close to entities being enrolled and separate from a subsequent RA. In BRSKI-AE, it is needed if a backend RA is used; in this case, the LRA is co-located with the registrar.

MASA: Manufacturer Authorized Signing Authority. Provides vouchers.

RA: Registration Authority. The PKI component to which a CA typically delegates certificate management functions such as authenticating pledges and performing authorization checks on certification requests.

SCEP: Simple Certificate Enrolment Protocol

3. Basic Requirements and Mapping to Solutions

Based on the intended target scenarios described in Section 1.1 and the application examples described in Appendix A, the following requirements are derived to support authenticated self-contained objects as containers carrying certification requests.

The following properties are required for a certification request:

- Proof of possession: demonstrates access to the private key corresponding to the public key contained in a certification request. This is typically achieved by a self-signature using the corresponding private key but can also be achieved indirectly; see [RFC4210], Section 4.3.
- Proof of identity (also called "proof of origin"): provides data origin authentication of the certification request. Typically, this is achieved by a signature using the pledge IDevID secret over some data, which needs to include a sufficiently strong identifier of the pledge, such as the device serial number typically included in the subject of the IDevID certificate.

The remainder of this section gives a non-exhaustive list of solution examples, based on existing technology described in IETF documents.

3.1. Solution Options for Proof of Possession

Certificate Signing Request (CSR) objects are data structures protecting only the integrity of the contained data and providing proof of possession for a (locally generated) private key. Important types of CSR data structures are:

- PKCS #10 [RFC2986]: This very common form of CSR is self-signed to protect its integrity and to prove possession of the private key that corresponds to the public key included in the request.
- Certificate Request Message Format (CRMF) [RFC4211]: This less common but more general CSR format supports several ways of integrity protection and proof of possession. Typically a self-signature is used, which is generated over (part of) the structure with the private key corresponding to the included public key. CRMF also supports further proof-of-possession methods for types of keys that do not have signing capability. For details, see [RFC4211], Section 4.

It should be noted that the integrity protection of CSRs includes the public key because it is part of the data signed by the corresponding private key. Yet, this signature does not provide data origin authentication, (i.e., proof of identity of the requester) because the key pair involved is new and therefore does not yet have a confirmed identity associated with it.

3.2. Solution Options for Proof of Identity

Binding a Certificate Signing Request (CSR) to an existing authenticated credential (which in the BRSKI context is the IDevID certificate) enables proof of origin, which in turn supports an authorization decision on the CSR.

The binding of data origin authentication to the CSR is typically delegated to the protocol used for certificate management. This binding may be achieved through security options in an underlying transport protocol such as TLS if the authorization of the certification request is (sufficiently) done at the next communication hop. Depending on the key type, the binding can also be done in a stronger, transport-independent way by wrapping the CSR with a signature.

This requirement is addressed by existing enrollment protocols in various ways, such as:

- EST [RFC7030] and its variant EST-coaps [RFC9148] utilize PKCS #10 to encode CSRs. While such a CSR has not been designed to include proof of origin, there is a limited, indirect way of binding it to the source authentication of the underlying TLS session. This is achieved by including in the CSR the "tls-unique" value [RFC5929] resulting from the TLS handshake. As this is optionally supported by the EST `"/simpleenroll"` endpoint used in BRSKI, and the TLS handshake employed in BRSKI includes certificate-based client authentication of the pledge with its IDevID credentials, the proof of pledge identity being an authenticated TLS client can be bound to the CSR.

  Yet, this binding is only valid in the context of the TLS session established with the registrar acting as the EST server and typically also as an RA. So even such a cryptographic binding of the authenticated pledge identity to the CSR is not visible nor verifiable to authorization

points outside the registrar, such as a (second) RA in the backend. What the registrar needs to do is authenticate and pre-authorize the pledge and indicate this to the (second) RA. This is done by signing the forwarded certification request with its private key and a related certificate that has the id-kp-cmcRA extended key usage attribute.

[RFC7030], Section 2.5 sketches wrapping CSRs formatted per PKCS #10 with a Full PKI Request message sent to the `"/fullcmc"` endpoint. This would allow for source authentication at the message level, such that the registrar could forward it to external RAs in a meaningful way. This approach is so far not sufficiently described and likely has not been implemented.

- The Simple Certificate Enrolment Protocol (SCEP) [RFC8894] supports using a shared secret (passphrase) or an existing certificate to protect CSRs based on SCEP Secure Message Objects using Cryptographic Message Syntax (CMS) wrapping [RFC5652]. Note that the wrapping using an existing IDevID in SCEP is referred to as "renewal". This way, SCEP does not rely on the security of the underlying message transfer.
- CMP [RFC4210] [RFC9480] supports using a shared secret (passphrase) or an existing certificate, which may be an IDevID credential, to authenticate certification requests via the PKIProtection structure in a PKIMessage. The certification request is typically encoded utilizing CRMF, while PKCS #10 is supported as an alternative. Thus, CMP does not rely on the security of the underlying message transfer.
- Certificate Management over CMS (CMC) [RFC5272] also supports utilizing a shared secret (passphrase) or an existing certificate to protect certification requests, which can be either in a CRMF or PKCS #10 structure. The proof of identity can be provided as part of a Full CMC Request based on CMS [RFC5652] and signed with an existing IDevID secret. Thus, CMC does not rely on the security of the underlying message transfer.

To sum up, EST does not meet the requirements for authenticated self-contained objects, but SCEP, CMP, and CMC do. This document primarily focuses on CMP as it has more industry adoption than CMC and SCEP has issues not detailed here.

4. Adaptations to BRSKI

To enable using alternative certificate enrollment protocols supporting end-to-end authentication, asynchronous enrollment, and more general system architectures, BRSKI-AE provides some generalizations on BRSKI [RFC8995]. This way, authenticated self-contained objects such as those described in Section 3 above can be used for certificate enrollment, and RA functionality can be deployed freely in the target domain. Parts of the RA functionality can even be distributed over several nodes.

The enhancements are kept to a minimum to ensure the reuse of already defined architecture elements and interactions. In general, the communication follows the BRSKI model and utilizes the existing BRSKI architecture elements. In particular, the pledge initiates communication with the domain registrar and interacts with the MASA as usual for voucher request and response processing.

4.1. Architecture

The key element of BRSKI-AE is that the authorization of a certification request **MUST** be performed based on an authenticated self-contained object. The certification request is bound in a self-contained way to a proof of origin based on the IDevID credentials. Consequently, the certification request **MAY** be transferred using any mechanism or protocol. Authentication and authorization of the certification request can be done by the domain registrar and/or by backend domain components. As mentioned in Section 1.1, these components may be offline or off-site. The registrar and other on-site domain components may have no or only temporary (intermittent) connectivity to them.

This leads to generalizations in the placement and enhancements of the logical elements as shown in Figure 1.

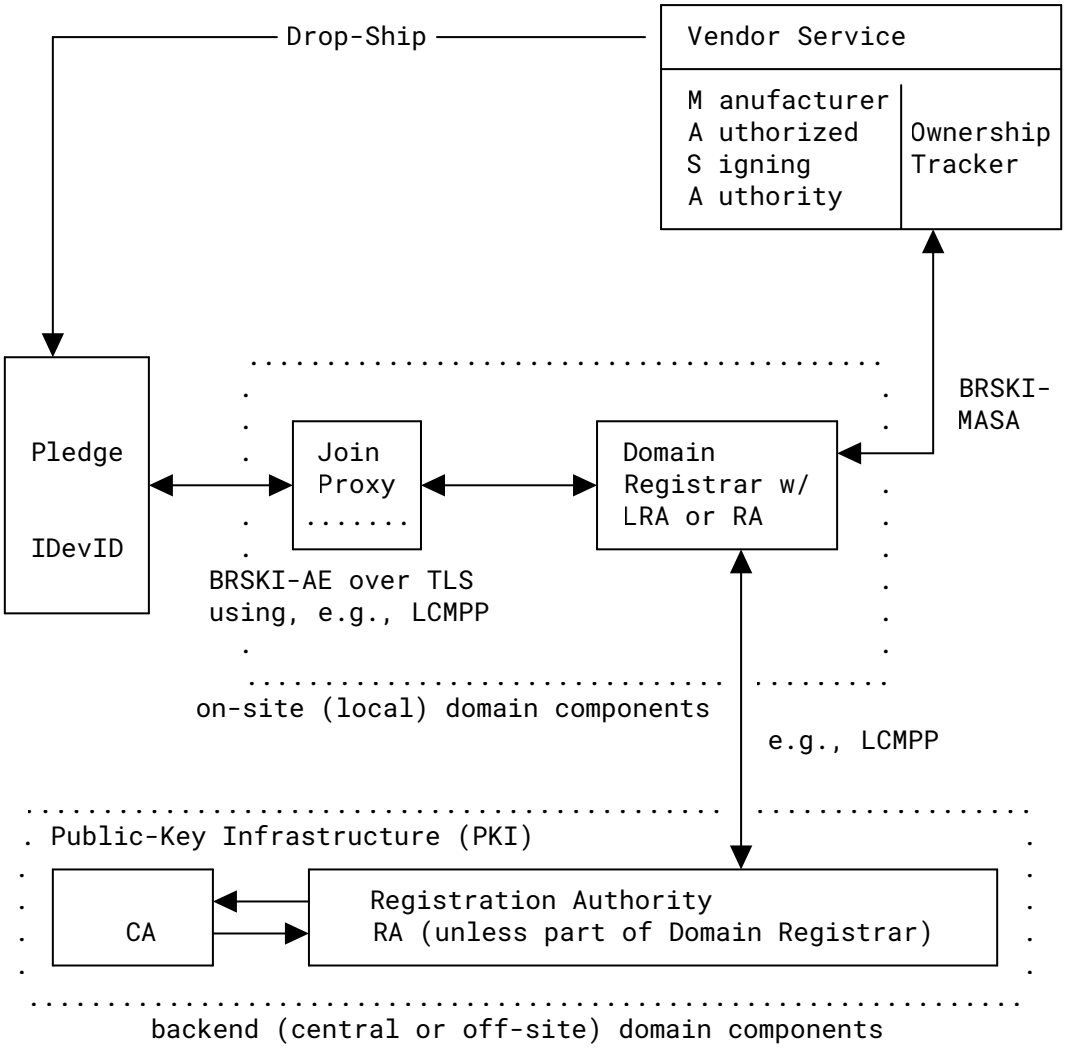

Figure 1: Architecture Overview Using Backend PKI Components

The architecture overview in Figure 1 has the same logical elements as BRSKI but with a more flexible placement of the authentication and authorization checks on certification requests. Depending on the application scenario, the registrar **MAY** still do all of these checks (as is the case in BRSKI) or only do part of them.

The following list describes the on-site components in the target domain of the pledge shown in Figure 1.

- Join Proxy: This has the same requirements as in [RFC8995] (see [RFC8995], Section 4).

- Domain Registrar (including LRA or RA functionality): In BRSKI-AE, the domain registrar has mostly the same functionality as in BRSKI, namely to act as the gatekeeper of the domain for onboarding new devices and to facilitate the communication of pledges with their MASA and the domain PKI. Yet, there are some generalizations and specific requirements:

  1. The registrar **MUST** support at least one certificate enrollment protocol with authenticated self-contained objects for certification requests. To this end, the URI scheme for addressing endpoints at the registrar is generalized (see Section 4.3).
  2. Rather than having full RA functionality, the registrar **MAY** act as a Local Registration Authority (LRA) and delegate part of its involvement in certificate enrollment to a backend RA. In such scenarios, the registrar optionally checks certification requests it receives from pledges and forwards them to the backend RA, which performs the remaining parts of the enrollment request validation and authorization. Note that to this end, the backend RA may need information regarding the authorization of pledges from the registrar or from other sources. On the way back, the registrar forwards responses by the PKI to the pledge on the same channel.

     To support end-to-end authentication of the pledge across the registrar to the backend RA, the certification request signed by the pledge needs to be upheld and forwarded by the registrar. Therefore, for its communication with the PKI, the registrar cannot use an enrollment protocol that is different from the enrollment protocol used between the pledge and the registrar.
  3. The use of a certificate enrollment protocol with authenticated self-contained objects gives freedom with how to transfer enrollment messages between the pledge and an RA. BRSKI demands that the RA accept certification requests for LDevIDs only with the consent of the registrar. BRSKI-AE also guarantees this in the case that the RA is not part of the registrar, even if the message exchange with backend systems is unprotected and involves further transport hops. See Section 7 for details on how this can be achieved.

Despite the above generalizations of the enrollment phase, the final step of BRSKI, namely the enrollment status telemetry, is kept as it is.

The following list describes the components provided by the vendor or manufacturer outside the target domain.

- MASA: This has the functionality as described in [RFC8995]. The voucher exchange with the MASA via the domain registrar is performed as described in [RFC8995].

  > Note: The definition of the interaction with the MASA in Section 5 of [RFC8995] implies that it may be synchronous (using voucher requests with nonces) or asynchronous (using nonceless voucher requests).

- Ownership Tracker: This is as defined in [RFC8995].

The following list describes backend target domain components, which may be located on-site or off-site in the target domain.

- RA: This performs centralized certificate management functions as a PKI for the domain operator. In case these functions are not entirely performed by the domain registrar, it performs the final validation and authorization of certification requests. Otherwise, the RA co-located with the domain registrar directly connects to the CA.
- CA (also called "domain CA"): This generates domain-specific certificates according to certification requests that have been authenticated and authorized by the registrar and/or an extra RA.

Based on the diagram in [RFC8995], Section 2.1 and the architectural changes, the original protocol flow is divided into several phases showing commonalities and differences with the original approach as follows.

- Discover: This is mostly as in step (1) of [RFC8995]. For details, see Section 4.2.1.
- Identify: This is the same as in step (2) of [RFC8995].
- Voucher exchange: This is the same as in steps (3) and (4) of [RFC8995].
- Voucher status telemetry: This is the same as directly after step (4) in [RFC8995].
- Certificate enrollment phase: The use of EST in step (5) is changed to employing a certificate enrollment protocol that uses an authenticated self-contained object for requesting the LDevID certificate.

  It is **REQUIRED** to use the (D)TLS channel established between the pledge and registrar to transport the certificate enrollment request and response messages. To this end, the enrollment protocol, the pledge, and the registrar need to support the use of this existing channel for certificate enrollment. Due to this architecture, the pledge does not need to establish additional connections for certificate enrollment and the registrar retains full control over the certificate enrollment traffic.
- Enrollment status telemetry: This is the final exchange of step (5) of [RFC8995].

4.2. Message Exchange

The behavior of a pledge described in [RFC8995], Section 2.1 is kept, with one major exception. After finishing the Imprint step (4), the Enroll step (5) **MUST** be performed with an enrollment protocol utilizing authenticated self-contained objects, as explained in Section 3. Section 5 discusses selected suitable enrollment protocols and applicable options.

An abstract overview of the BRSKI-AE protocol can be found in the graphics on slide 4 of [BRSKI-AE-overview].

4.2.1. Pledge - Registrar Discovery

Discovery as specified in [RFC8995], Section 4 does not support the discovery of registrars with enhanced feature sets. A pledge cannot find out in this way whether discovered registrars support the certificate enrollment protocol it expects, such as CMP.

As a more general solution, the BRSKI discovery mechanism can be extended to provide up-front information on the capabilities of registrars. For further discussion, see [BRSKI-discovery].

In the absence of such a generally applicable solution, BRSKI-AE deployments may use their particular way of doing discovery. Section 5.1 defines a minimalist approach that **MAY** be used for CMP.

4.2.2. Pledge - Registrar - MASA Voucher Exchange

The voucher exchange is performed as specified in [RFC8995].

4.2.3. Pledge - Registrar - MASA Voucher Status Telemetry

The voucher status telemetry is performed as specified in [RFC8995], Section 5.7.

4.2.4. Pledge - Registrar - RA/CA Certificate Enrollment

The specification in this section replaces the EST integration for PKI bootstrapping described in [RFC8995], Section 5.9 (while [RFC8995], Section 5.9.4 remains as the final phase; see below).

The certificate enrollment phase may involve the transmission of several messages. Details can depend on the application scenario, the employed enrollment protocol, and other factors.

The only message exchange **REQUIRED** is for the actual certification request and response. Further message exchanges **MAY** be performed as needed.

> Note: The message exchanges marked **OPTIONAL** in Figure 2 below cover all those supported by the use of EST in BRSKI. The last **OPTIONAL** one, namely certificate confirmation, is not supported by EST but by CMP and other enrollment protocols.

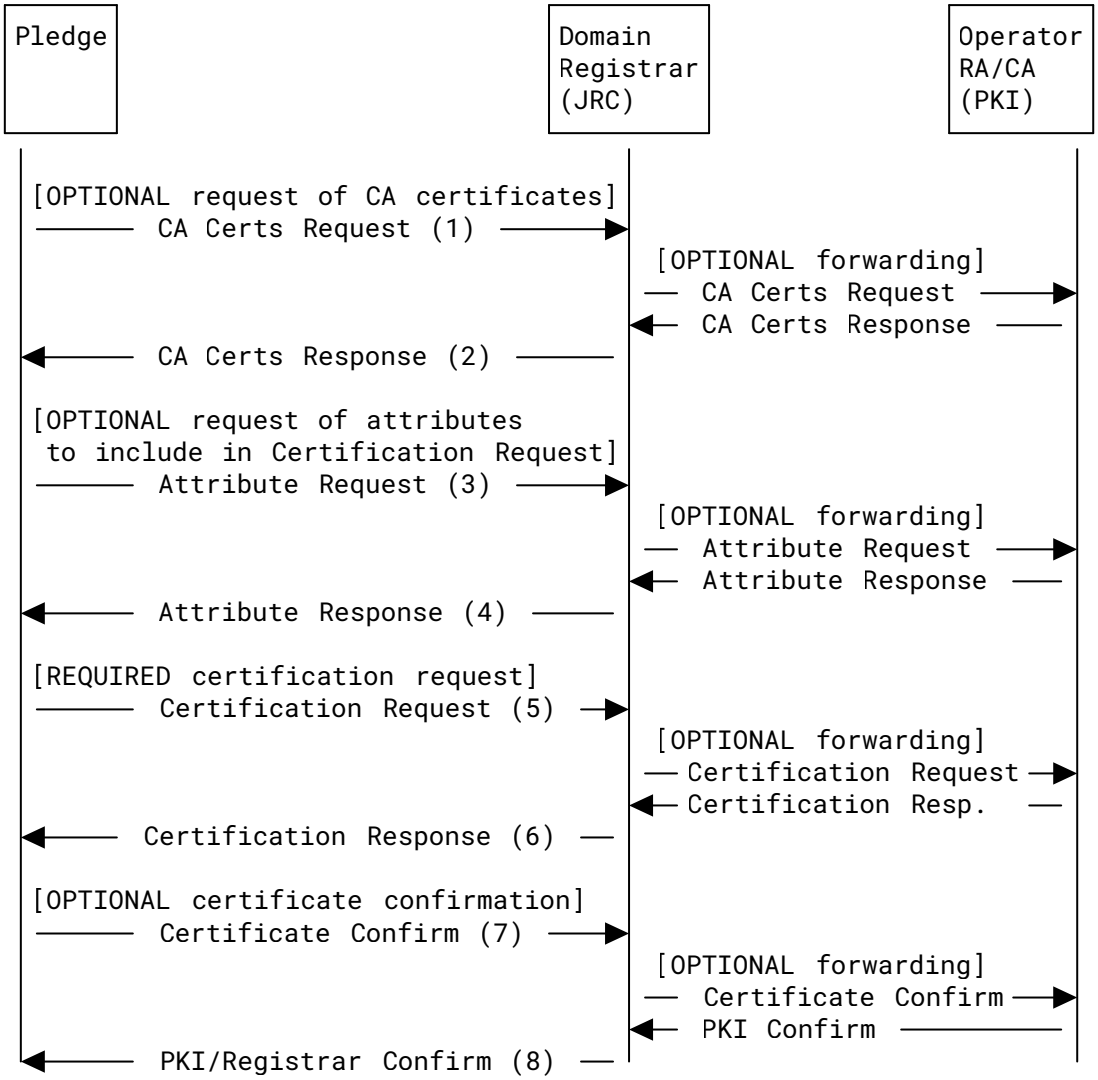

Figure 2: Certificate Enrollment Message Flow

It may be noted that connections between the registrar and the PKI components of the operator (RA, CA, etc.) may be intermittent or offline. Messages should be sent as soon as sufficient transfer capacity is available.

The label '`[OPTIONAL forwarding]`' in Figure 2 means that on receiving a request message of the given type from a pledge, the registrar **MAY** answer the request directly. In this case, it **MUST** authenticate its responses with the same credentials as used for authenticating itself at the TLS level for the voucher exchange. Otherwise, the registrar **MUST** forward the request to the RA and forward any resulting response back to the pledge.

The decision of whether to forward a request or to answer it directly can depend on various static and dynamic factors. They include the application scenario, the capabilities of the registrar, the capabilities of the local RA possibly co-located with the registrar, the enrollment protocol being used, and the specific contents of the request.

Note that there are several options for how the registrar could be able to directly answer requests for CA certificates or for certification request attributes. It could cache responses obtained from the domain PKI and later use their contents for responding to requests asking for the same data. The contents could also be explicitly provisioned at the registrar.

Further note that certification requests typically need to be handled by the backend PKI, but the registrar can answer them directly with an error response in case it determines that such a request should be rejected, for instance, because it is not properly authenticated or authorized. Also, certificate confirmation messages will usually be forwarded to the backend PKI, but if the registrar knows that they are not needed or wanted there, it can acknowledge such messages directly.

The following list provides an abstract description of the flow depicted in Figure 2.

- CA Certs Request (1): The pledge optionally requests the latest relevant CA certificates. This ensures that the pledge has the complete set of current CA certificates beyond the pinned-domain-cert (which is contained in the voucher and which may be just the domain registrar certificate).
- CA Certs Response (2): This **MUST** contain any intermediate CA certificates that the pledge may need to validate certificates and **MAY** contain the LDevID trust anchor.
- Attribute Request (3): Typically, the automated bootstrapping occurs without local administrative configuration of the pledge. Nevertheless, there are cases in which the pledge may also include additional attributes that are specific to the target domain in the Certification Request (5). To get these attributes in advance, the attribute request may be used.
- Attribute Response (4): This **MUST** contain the attributes requested in (3) to be included in the subsequent Certification Request (5).

  For example, [RFC8994], Section 6.11.7.2 specifies how the attribute request is used to signal to the pledge the '`acp-node-name`' field required for enrollment into an Autonomic Control Plane (ACP) domain.
- Certification Request (5): This **MUST** contain the authenticated self-contained object ensuring both the proof of possession of the corresponding private key and the proof of identity of the requester.
- Certification Response (6): On success, this **MUST** contain the requested certificate and **MAY** include further information, like certificates of intermediate CAs and any additional trust anchors.
- Certificate Confirm (7): This is an optional confirmation that is sent after the requested certificate has been received and validated. If sent, it **MUST** contain a positive or negative confirmation by the pledge to the PKI whether the certificate was successfully enrolled and fits its needs.

- PKI/Registrar Confirm (8): This is an acknowledgment by the PKI that **MUST** be sent on reception of the Certificate Confirm.

The generic messages described above may be implemented using any certificate enrollment protocol that supports authenticated self-contained objects for the certification request as described in Section 3. Examples are available in Section 5.

> Note that the optional certificate confirmation by the pledge to the PKI described above is independent of the mandatory enrollment status telemetry done between the pledge and the registrar in the final phase of BRSKI-AE, which is described next.

4.2.5. Pledge - Registrar Enrollment Status Telemetry

The enrollment status telemetry is performed as specified in [RFC8995], Section 5.9.4.

In [RFC8995], this is described as part of the certificate enrollment step, but due to the generalization of the enrollment protocol described in this document, it is regarded as a separate phase here.

4.3. Enhancements to the Endpoint Addressing Scheme of BRSKI

BRSKI-AE extends the addressing scheme outlined in [RFC8995], Section 5 to support alternative enrollment protocols that utilize authenticated, self-contained objects for certification requests (also see Section 5). These extensions are designed to be compatible with existing Registration Authorities (RAs) and Certification Authorities (CAs) that already support such enrollment protocols, enabling their use without requiring any modifications.

The addressing scheme in [RFC8995] for certification requests, related CA certificates, and CSR attributes retrieval functions uses the definition from EST [RFC7030]. An example of simple enrollment is: `"/.well-known/est/simpleenroll"`. This approach is generalized to the following notation: `"/.well-known/<enrollment-protocol>/<request>"` in which "`<enrollment-protocol>`" refers to a certificate enrollment protocol. Note that here, enrollment is considered a message sequence that contains at least a certification request and a certification response. The following conventions are used to provide maximal compatibility with BRSKI:

- "`<enrollment-protocol>`": This **MUST** reference the protocol being used. Existing values include '`est`' [RFC7030] as in [RFC8995] and '`cmp`' as in [RFC9483] and Section 5.1 below. Values for other existing protocols such as CMC and SCEP, as well as newly defined protocols, are outside the scope of this document. For use of the "`<enrollment-protocol>`" and "`<request>`" URI components, they would need to be specified in a suitable RFC and placed into the "Well-Known URIs" registry, just as EST in [RFC7030].
- "`<request>`": If present, this path component **MUST** describe the operation requested depending on the enrollment protocol being used. Enrollment protocols are expected to define their request endpoints, as is done by existing protocols (also see Section 5).

Well-known URIs for various endpoints on the domain registrar are already defined as part of the base BRSKI specification or indirectly by EST. In addition, alternative enrollment endpoints **MAY** be supported by the registrar.

A pledge **SHOULD** use the endpoints defined for the enrollment protocol(s) that it can use. It will recognize whether the protocol it uses and the specific request it wants to perform are understood and supported by the domain registrar. This is done by sending the request to the respective endpoint according to the above addressing scheme and then evaluating the HTTP status code of the response. If the pledge uses endpoints that are not standardized, it risks that the registrar does not recognize a request and thus may reject it even if the registrar supports the intended protocol and operation.

The following list of endpoints provides an illustrative example of a domain registrar supporting several options for EST as well as for CMP to be used in BRSKI-AE. The listing contains the supported endpoints to which the pledge may connect for bootstrapping. This includes the voucher handling as well as the enrollment endpoints. The CMP-related enrollment endpoints are defined as well-known URIs in CMP Updates [RFC9480] and the Lightweight CMP Profile [RFC9483].

- /.well-known/brski/voucherrequest
- /.well-known/brski/voucher_status
- /.well-known/brski/enrollstatus
- /.well-known/est/cacerts
- /.well-known/est/csrattrs
- /.well-known/est/fullcmc
- /.well-known/cmp/getcacerts
- /.well-known/cmp/getcertreqtemplate
- /.well-known/cmp/initialization
- /.well-known/cmp/pkcs10

5. Instantiation with Existing Enrollment Protocols

This section maps the generic requirements to support proof of possession and proof of identity to selected existing certificate enrollment protocols and specifies further aspects of using such enrollment protocols in BRSKI-AE.

5.1. BRSKI-CMP: BRSKI-AE Instantiated with CMP

In this document, references to CMP follow the Lightweight CMP Profile (LCMPP) from [RFC9483] rather than [RFC4210] and [RFC9480], as the subset of CMP defined in the LCMPP sufficiently meets the required functionality.

Adherence to the LCMPP [RFC9483] is **REQUIRED** when using CMP. The following specific requirements apply (refer to Figure 2):

- The validation of server response messages performed by the CMP client within the pledge **MUST** be based on the trust anchor established beforehand via the BRSKI voucher, i.e., on the pinned-domain-cert.

  Note that the integrity and authenticity checks on the RA/CA by the CMP client can be stronger than for EST because they do not need to be performed hop-by-hop but are usually end-to-end.

- CA Certs Request (1) and Response (2): Requesting CA certificates is **OPTIONAL**. If supported, it **SHALL** be implemented as specified in [RFC9483], Section 4.3.1.
- Attribute Request (3) and Response (4): Requesting certification request attributes is **OPTIONAL**. If supported, it **SHALL** be implemented as specified in [RFC9483], Section 4.3.3.

  Alternatively, the registrar **MAY** modify the requested certificate contents as specified in [RFC9483], Section 5.2.3.2.

- Certification Request (5) and Response (6): Certificates **SHALL** be requested and provided as specified in the LCMPP from [RFC9483], Section 4.1.1 (based on CRMF) or [RFC9483], Section 4.1.4 (based on PKCS #10).

  Proof of possession **SHALL** be provided in a manner suitable for the key type. Proof of identity **SHALL** be provided by signature-based protection of the certification request message as outlined in [RFC9483], Section 3.2 using the IDevID secret.

  When the registrar forwards a certification request from the pledge to a backend RA/CA, it is **RECOMMENDED** that the registrar wraps the original certification request in a nested message signed with its own credentials, as described in [RFC9483], Section 5.2.2.1. This approach explicitly conveys the registrar's consent to the RA while retaining the original certification request with the proof of origin provided by the pledge's signature.

  If additional trust anchors beyond the pinned-domain-cert need to be conveyed to the pledge, this **SHOULD** be done in the '`caPubs`' field of the certification response rather than through a CA Certs Response.

- Certificate Confirm (7) and PKI/Registrar Confirm (8): Explicit confirmation of new certificates to the RA/CA **MAY** be used as specified in [RFC9483], Section 4.1.1.

  > Note that independent of the certificate confirmation within CMP, enrollment status telemetry with the registrar at the BRSKI level will be performed as described in [RFC8995], Section 5.9.4.

- If delayed delivery of CMP messages is needed (e.g., to support enrollment over an asynchronous channel), it **SHALL** be performed as specified in Sections 4.4 and 5.1.2 of [RFC9483].

The mechanisms for exchanging messages between the registrar and backend PKI components (i.e., RA and/or CA) are outside the scope of this document. CMP's independence from the message transfer mechanism allows for flexibility in choosing the appropriate exchange method based on the application scenario. For the applicable security and privacy considerations, refer to Sections 7 and 8. Further guidance can be found in [RFC9483], Section 6.

BRSKI-AE with CMP can also be combined with Constrained BRSKI [cBRSKI], using CoAP for enrollment message transport as described by CoAP Transfer for CMP [RFC9482]. In such scenarios, the EST-specific parts of [cBRSKI] do not apply.

For BRSKI-AE scenarios where a general solution for discovering registrars with CMP support is not available (cf. Section 4.2.1), the following minimalist approach **MAY** be used: Perform discovery as defined in [RFC8995], Appendix B, but use the service name `"brski-reg-cmp"` (as defined in Section 6) instead of `"brski-registrar"` (as defined in [RFC8995], Section 8.6). Note that this approach does not support join proxies.

5.2. Support of Other Enrollment Protocols

Further instantiations of BRSKI-AE can be done. They are left for future work.

In particular, CMC [RFC5272] (using its in-band source authentication options) and SCEP [RFC8894] (using its 'renewal' option) could be used.

The fullCMC variant of EST sketched in [RFC7030], Section 2.5 might also be used here. For EST-fullCMC, further specification is necessary.

6. IANA Considerations

IANA has registered the following service name in the "Service Name and Transport Protocol Port Number Registry".

Service Name: brski-reg-cmp
Transport Protocol(s): tcp
Description: Bootstrapping Remote Secure Key Infrastructure registrar with CMP capabilities according to the Lightweight CMP Profile (LCMPP) [RFC9483]
Assignee: IESG <iesg@ietf.org>
Contact: IETF <chair@ietf.org>
Reference: RFC 9733

> Note: We chose the suffix "cmp" here rather than some other abbreviation like "lcmpp" mainly because this document defines the normative CMP instantiation of BRSKI-AE, which implies adherence to the LCMPP is necessary and sufficient.

7. Security Considerations

The security considerations laid out in [RFC8995], Section 11 apply to the discovery and voucher exchange as well as for the status exchange information.

In particular, even if the registrar delegates part or all of its RA role during certificate enrollment to a separate system, it still must be made sure that the registrar takes part in the decision on accepting or declining a request to join the domain, as required in [RFC8995], Section 5.3. As this also pertains to obtaining a valid domain-specific certificate, it must be made sure that a pledge cannot circumvent the registrar in the decision of whether it is granted an LDevID certificate by the CA. There are various ways to fulfill this, including:

- implicit consent;
- the registrar signaling its consent to the RA out-of-band before or during the enrollment phase, for instance, by entering the pledge identity in a database;
- the registrar providing its consent using an extra message that is transferred on the same channel as the enrollment messages, possibly in a TLS tunnel; and
- the registrar explicitly stating its consent by signing the authenticated self-contained certificate enrollment request message in addition to the pledge.

> Note: If EST was used, the registrar could give implicit consent on a certification request by forwarding the request to a PKI entity using a connection authenticated with a certificate containing an id-kp-cmcRA extension.

When CMP is used, the security considerations laid out in the LCMPP from [RFC9483] apply.

8. Privacy Considerations

The privacy considerations laid out in [RFC8995], Section 10 apply as well.

Note that CMP messages themselves are not encrypted. This may give eavesdroppers insight into which devices are bootstrapped into the domain. In turn, this might also be used to selectively block the enrollment of certain devices.

To prevent such issues, the underlying message transport channel can be encrypted. This is already provided by TLS between the pledge and the registrar, and for the onward exchange with backend systems, encryption may need to be added.

9. References

9.1. Normative References

[IEEE_802.1AR-2018]

IEEE, "IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity", IEEE 802.1AR-2018, DOI 10.1109/IEEESTD.2018.8423794, August 2018, <https://ieeexplore.ieee.org/document/8423794>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <https://www.rfc-editor.org/info/rfc8995>.

[RFC9483] Brockhaus, H., von Oheimb, D., and S. Fries, "Lightweight Certificate Management Protocol (CMP) Profile", RFC 9483, DOI 10.17487/RFC9483, November 2023, <https://www.rfc-editor.org/info/rfc9483>.

9.2. Informative References

[BRSKI-AE-overview] von Oheimb, D., Ed., Fries, S., and H. Brockhaus, "Update on BRSKI-AE: Alternative Enrollment Protocols in BRSKI", IETF 116 - ANIMA Working Group Presentation, March 2023, <https://datatracker.ietf.org/meeting/116/materials/slides-116-anima-update-on-brski-ae-alternative-enrollment-protocols-in-brski-00>.

[BRSKI-discovery] Eckert, T., Ed. and E. Dijk, "BRSKI discovery and variations", Work in Progress, Internet-Draft, draft-ietf-anima-brski-discovery-05, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-anima-brski-discovery-05>.

[cBRSKI] Richardson, M., Van der Stok, P., Kampanakis, P., and E. Dijk, "Constrained Bootstrapping Remote Secure Key Infrastructure (cBRSKI)", Work in Progress, Internet-Draft, draft-ietf-anima-constrained-voucher-26, 8 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-anima-constrained-voucher-26>.

[IEC-62351-9] International Electrotechnical Commission, "Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment", IEC 62351-9:2023, June 2023, <https://webstore.iec.ch/en/publication/66864>.

[ISO-IEC-15118-2] International Organization for Standardization, "Road vehicles - Vehicle-to-Grid Communication Interface - Part 2: Network and application protocol requirements", ISO 15118-2:2014, April 2014, <https://www.iso.org/standard/55366.html>.

[NERC-CIP-005-5] North American Electric Reliability Council, "Cyber Security - Electronic Security Perimeter", CIP 005-5, December 2013.

[OCPP] Open Charge Alliance, "Open Charge Point Protocol 2.0.1 (Draft)", December 2019.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, DOI 10.17487/RFC2986, November 2000, <https://www.rfc-editor.org/info/rfc2986>.

[RFC4210] Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, DOI 10.17487/RFC4210, September 2005, <https://www.rfc-editor.org/info/rfc4210>.

[RFC4211] Schaad, J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", RFC 4211, DOI 10.17487/RFC4211, September 2005, <https://www.rfc-editor.org/info/rfc4211>.

[RFC5272] Schaad, J. and M. Myers, "Certificate Management over CMS (CMC)", RFC 5272, DOI 10.17487/RFC5272, June 2008, <https://www.rfc-editor.org/info/rfc5272>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

[RFC5929] Altman, J., Williams, N., and L. Zhu, "Channel Bindings for TLS", RFC 5929, DOI 10.17487/RFC5929, July 2010, <https://www.rfc-editor.org/info/rfc5929>.

[RFC6955] Schaad, J. and H. Prafullchandra, "Diffie-Hellman Proof-of-Possession Algorithms", RFC 6955, DOI 10.17487/RFC6955, May 2013, <https://www.rfc-editor.org/info/rfc6955>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/info/rfc7030>.

[RFC8366] Watsen, K., Richardson, M., Pritikin, M., and T. Eckert, "A Voucher Artifact for Bootstrapping Protocols", RFC 8366, DOI 10.17487/RFC8366, May 2018, <https://www.rfc-editor.org/info/rfc8366>.

[RFC8894] Gutmann, P., "Simple Certificate Enrolment Protocol", RFC 8894, DOI 10.17487/RFC8894, September 2020, <https://www.rfc-editor.org/info/rfc8894>.

[RFC8994] Eckert, T., Ed., Behringer, M., Ed., and S. Bjarnason, "An Autonomic Control Plane (ACP)", RFC 8994, DOI 10.17487/RFC8994, May 2021, <https://www.rfc-editor.org/info/rfc8994>.

[RFC9148] van der Stok, P., Kampanakis, P., Richardson, M., and S. Raza, "EST-coaps: Enrollment over Secure Transport with the Secure Constrained Application Protocol", RFC 9148, DOI 10.17487/RFC9148, April 2022, <https://www.rfc-editor.org/info/rfc9148>.

[RFC9480] Brockhaus, H., von Oheimb, D., and J. Gray, "Certificate Management Protocol (CMP) Updates", RFC 9480, DOI 10.17487/RFC9480, November 2023, <https://www.rfc-editor.org/info/rfc9480>.

[RFC9482] Sahni, M., Ed. and S. Tripathi, Ed., "Constrained Application Protocol (CoAP) Transfer for the Certificate Management Protocol", RFC 9482, DOI 10.17487/RFC9482, November 2023, <https://www.rfc-editor.org/info/rfc9482>.

[UNISIG-Subset-137] UNISIG, "ERTMS/ETCS On-line Key Management FFFIS", Subset-137, Version 1.0.0, December 2015, <https://www.era.europa.eu/system/files/2023-01/sos3_index083_-_subset-137_v100.pdf>.

Appendix A. Application Examples

This informative annex provides some details about application examples.

A.1. Rolling Stock

Rolling stock or railroad cars contain a variety of sensors, actuators, and controllers. These communicate within the railroad car but also exchange information with other railroad cars of the same train and with track-side equipment and/or possibly with backend systems. These devices are typically unaware of backend system connectivity. Enrolling certificates may be done during maintenance cycles of the railroad car but can already be prepared during operation. Such asynchronous enrollment will include generating certification requests, which are collected and later forwarded for processing whenever the railroad car gets connectivity with the backend PKI of the operator. The authorization of the certification request is then done based on the operator's asset/inventory information in the backend.

UNISIG has included a CMP profile for the enrollment of TLS client and server X.509 certificates of on-board and track-side components in the Subset-137, which specifies the ETRAM/ETCS online key management for train control systems [UNISIG-Subset-137].

A.2. Building Automation

In building automation scenarios, a detached building or the basement of a building may be equipped with sensors, actuators, and controllers that are connected to each other in a local network but with only limited or no connectivity to a central building management system. This problem may occur during installation time but also during operation. In such a situation, a service technician collects the necessary data and transfers it between the local network and the central building management system, e.g., using a laptop or a mobile phone. This data may

comprise parameters and settings required in the operational phase of the sensors/actuators, like a component certificate issued by the operator to authenticate against other components and services.

The collected data may be provided by a domain registrar already existing in the local network. In this case, connectivity to the backend PKI may be facilitated by the service technician's laptop. Alternatively, the data can also be collected from the pledges directly and provided to a domain registrar deployed in a different network in preparation for the operational phase. In this case, connectivity to the domain registrar may also be facilitated by the service technician's laptop.

A.3. Substation Automation

In electrical substation automation scenarios, a control center typically hosts PKI services to issue certificates for Intelligent Electronic Devices (IEDs) operated in a substation. Communication between the substation and control center is performed through a proxy/gateway/DMZ, which terminates protocol flows. Note that [NERC-CIP-005-5] requires inspection of protocols at the boundary of a security perimeter (in this case, the substation). In addition, security management in substation automation assumes central support of several enrollment protocols to support the various capabilities of IEDs from different vendors. The IEC standard IEC62351-9 [IEC-62351-9] specifies mandatory support of two enrollment protocols for the infrastructure side, SCEP [RFC8894] and EST [RFC7030], while an IED may support only one of them.

A.4. Electric Vehicle Charging Infrastructure

For electric vehicle charging infrastructure, protocols have been defined for the interaction between the electric vehicle and the charging point (e.g., ISO 15118-2 [ISO-IEC-15118-2]) as well as between the charging point and the charging point operator (e.g., OCPP [OCPP]). Depending on the authentication model, unilateral or mutual authentication is required. In both cases, the charging point uses an X.509 certificate to authenticate itself in TLS channels between the electric vehicle and the charging point. The management of this certificate depends, among other things, on the selected backend connectivity protocol. In the case of OCPP, this protocol is meant to be the only communication protocol between the charging point and the backend, carrying all information to control the charging operations and maintain the charging point itself. This means that the certificate management needs to be handled in-band of OCPP. This requires the ability to encapsulate the certificate management messages in a transport-independent way. Authenticated self-containment will support this by allowing the transport without a separate enrollment protocol, binding the messages to the identity of the communicating endpoints.

A.5. Infrastructure Isolation Policy

The approach described in this section refers to any case in which network infrastructure is normally isolated from the Internet as a matter of policy, most likely for security reasons. In such a case, limited access to external PKI services will be allowed in carefully controlled short periods of time (for example, when a batch of new devices is deployed) and forbidden or prevented at other times.

A.6. Sites with Insufficient Levels of Operational Security

The RA performing (at least part of) the authorization of a certification request is a critical PKI component and therefore requires higher operational security than components utilizing the issued certificates for their security features. CAs may also demand higher security in the registration procedures from RAs, which domain registrars with co-located RAs may not be able to fulfill. In particular, the CA/Browser forum currently increases the security requirements in the certificate issuance procedures for publicly trusted certificates, i.e., those placed in trust stores of browsers, which may be used to connect with devices in the domain. In case the on-site components of the target domain cannot be operated securely enough for the needs of an RA, this service should be transferred to an off-site backend component that has a sufficient level of security.

Acknowledgments

We thank Eliot Lear for his contributions as a co-author at an earlier draft stage.

We thank Brian E. Carpenter, Michael Richardson, and Giorgio Romanenghi for their input and discussion on use cases and call flows.

Moreover, we thank Toerless Eckert (document shepherd); Barry Leiba (SECdir review); Mahesh Jethanandani (IETF area director); Meral Shirazipour (Gen-ART reviewer); Reshad Rahman (YANGDOCTORS reviewer); Deb Cooley, Gunter Van de Velde, John Scudder, Murray Kucherawy, Roman Danyliw, and Éric Vyncke (IESG reviewers); Michael Richardson (ANIMA design team member); and Rajeev Ranjan, Rufus Buschart, Andreas Reiter, and Szofia Fazekas-Zisch (Siemens colleagues) for their reviews with suggestions for improvements.

Contributors

Eliot Lear
Cisco Systems
Richtistrasse 7
CH-8304 Wallisellen
Switzerland
Phone: +41 44 878 9200
Email: lear@cisco.com

Authors' Addresses

David von Oheimb (EDITOR)
Siemens AG
Otto-Hahn-Ring 6
81739 Munich
Germany
Email: david.von.oheimb@siemens.com
URI: https://www.siemens.com/

Steffen Fries
Siemens AG
Otto-Hahn-Ring 6
81739 Munich
Germany
Email: steffen.fries@siemens.com
URI: https://www.siemens.com/

Hendrik Brockhaus
Siemens AG
Otto-Hahn-Ring 6
81739 Munich
Germany
Email: hendrik.brockhaus@siemens.com
URI: https://www.siemens.com/