Workgroup:	ANIMA WG
Internet-Draft:	draft-ietf-anima-brski-ae-13
Published:	12 September 2024
Intended Status:	Standards Track
Expires:	16 March 2025

Authors: D. von Oheimb, Ed. *Siemens* S. Fries *Siemens* H. Brockhaus *Siemens*

BRSKI-AE: Alternative Enrollment Protocols in BRSKI

Abstract

This document defines enhancements to the Bootstrapping Remote Secure Key Infrastructure (BRSKI) protocol, known as BRSKI-AE (Alternative Enrollment). BRSKI-AE extends BRSKI to support certificate enrollment mechanisms instead of the originally specified use of EST. It supports certificate enrollment protocols, such as 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.

The RFC Editor will remove this note

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-anima-brski-ae/.

Discussion of this document takes place on the anima Working Group mailing list (mailto:anima@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/anima/. Subscribe at https://www.ietf.org/mailman/listinfo/anima/.

Source for this draft and an issue tracker can be found at https://github.com/anima-wg/anima-brski-ae.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

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 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 is 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]), and 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 (IDevID, [IEEE_802.1AR-2018]). To this end, the pledge generates a private key, called LDevID secret, and requests via the domain registrar from the PKI of its new domain a domain-specific device certificate, called 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 hops.
- Facilitates secure message exchange 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 BRSKI (RFC 8995) specifies the use of HTTP over TLS, but variations such as Constrained BRSKI [I-D.ietf-anima-constrained-voucher] which uses 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 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:

- Pledges and/or the target domain leverage an existing certificate enrollment protocol other than EST, such as CMP.
- The application context precludes the use of EST for certificate enrollment due to factors such as:
  - 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 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 [RFC2986] format, 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.
- 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.
- 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], partly repeated here. Also several further terms are described here.

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

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

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

attribute response: 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: placement of a domain component separately from the domain registrar; may be on-site or off-site

BRSKI: Bootstrapping Remote Secure Key Infrastructure [RFC8995]

BRSKI-AE: BRSKI with **A**lternative **E**nrollment, a variation of BRSKI [RFC8995] in which BRSKI-EST, the enrollment protocol between pledge and the registrar, is replaced by enrollment protocols that support end-to-end authentication of the pledge to the RA, such as Lightweight CMP (see LCMPP).

CA certs request: message requesting CA certificates

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

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

certification request: message requesting a certificate with proof of identity

certification response: message providing the answer to a certification request

CMP: Certificate Management Protocol [RFC9480]

CSR: Certificate Signing Request

EST: Enrollment over Secure Transport [RFC7030]

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

local RA (LRA): 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, and in this case, the LRA is co-located with the registrar.

MASA: Manufacturer Authorized Signing Authority, provides vouchers off-site: locality of component or service or functionality, such as RA or CA, 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: locality of a component or service or functionality at the site of the registrar

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

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

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

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: 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

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: CSRs 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 (the BRSKI context, 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], also its variant EST-coaps [RFC9148], utilizes PKCS #10 to encode Certificate Signing Requests (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 to authenticate and pre-authorize the pledge and to indicate this to the (second) RA 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 PKCS #10-formatted CSRs 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.

- SCEP [RFC8894] supports using a shared secret (passphrase) or an existing certificate to protect CSRs based on SCEP Secure Message Objects using 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.
- CMC [RFC5272] also supports utilizing a shared secret (passphrase) or an existing certificate to protect certification requests, which can be either in CRMF or PKCS #10 structure. The proof of identity can be provided as part of a FullCMCRequest, 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.

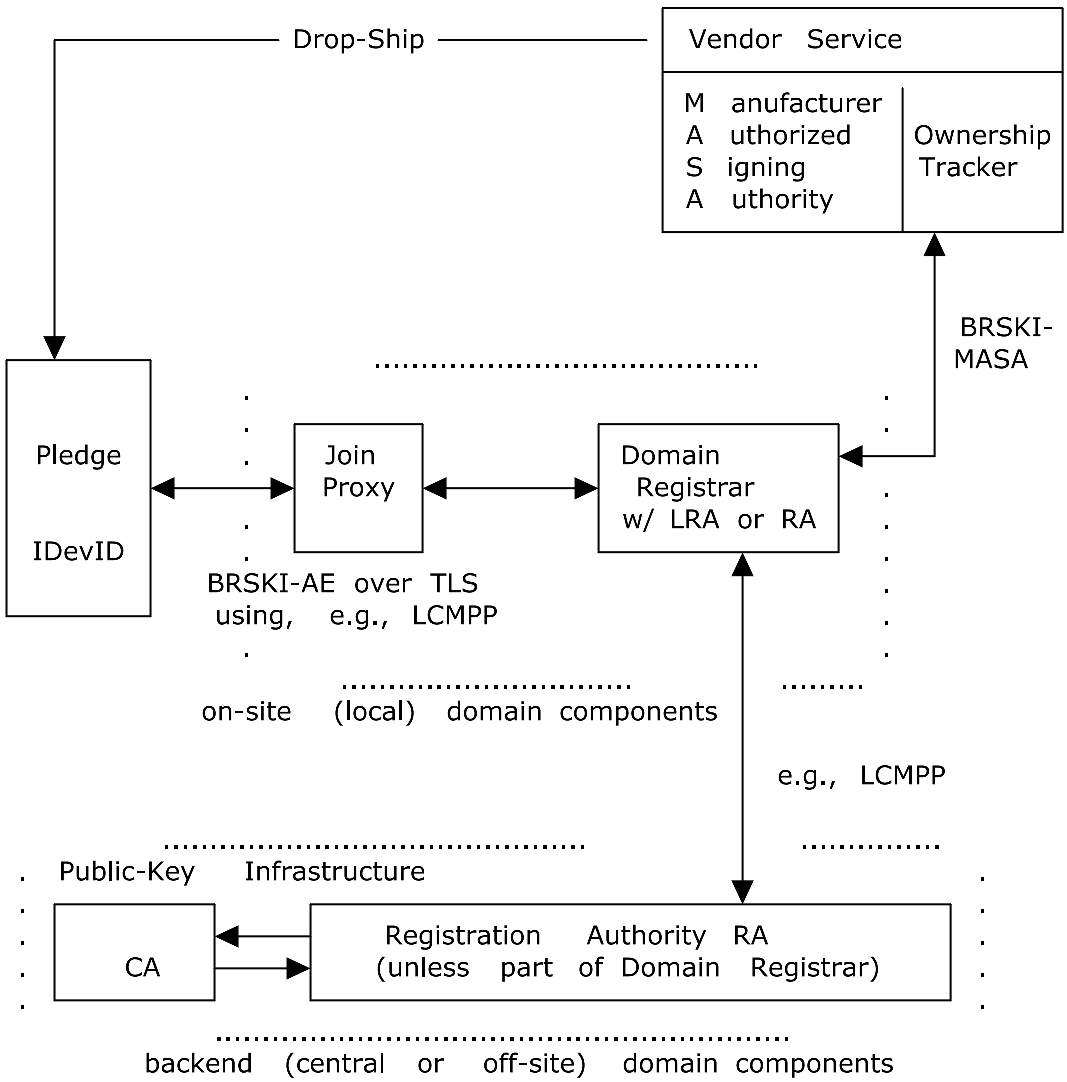

Figure 1: Architecture Overview Using Backend PKI Components

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 part of them.

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

- Join Proxy: same requirements as in BRSKI, 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, the registrar cannot use for its communication with the PKI 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 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 guarantees this also in 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 to 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: functionality as described in BRSKI [RFC8995]. The voucher exchange with the MASA via the domain registrar is performed as described in BRSKI.

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

* Ownership tracker: as defined in BRSKI.

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

* RA: performs centralized certificate management functions as a public-key infrastructure for the domain operator. As far as not already done 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: 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 BRSKI [RFC8995], Section 2.1 and the architectural changes, the original protocol flow is divided into several phases showing commonalities and differences to the original approach as follows.

* Discovery phase: mostly as in BRSKI step (1). For details see Section 4.2.1.
* Identification phase: same as in BRSKI step (2).
* Voucher exchange phase: same as in BRSKI steps (3) and (4).
* Voucher status telemetry: same as in BRSKI directly after step (4).
* 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.

  For transporting the certificate enrollment request and response messages, the (D)TLS channel established between pledge and registrar is **REQUIRED** to use. 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: the final exchange of BRSKI step (5).

4.2. Message Exchange

The behavior of a pledge described in BRSKI [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 options applicable.

An abstract overview of the BRSKI-AE protocol can be found at [BRSKI-AE-overview].

4.2.1. Pledge - Registrar Discovery

Discovery as specified in BRSKI [RFC8995], Section 4 does not support the discovery of registrars with enhanced feature sets. A pledge can not 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. Future work such as [draft-ietf-anima-brski-discovery] may provide this.

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

This 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 the below Figure 2 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.

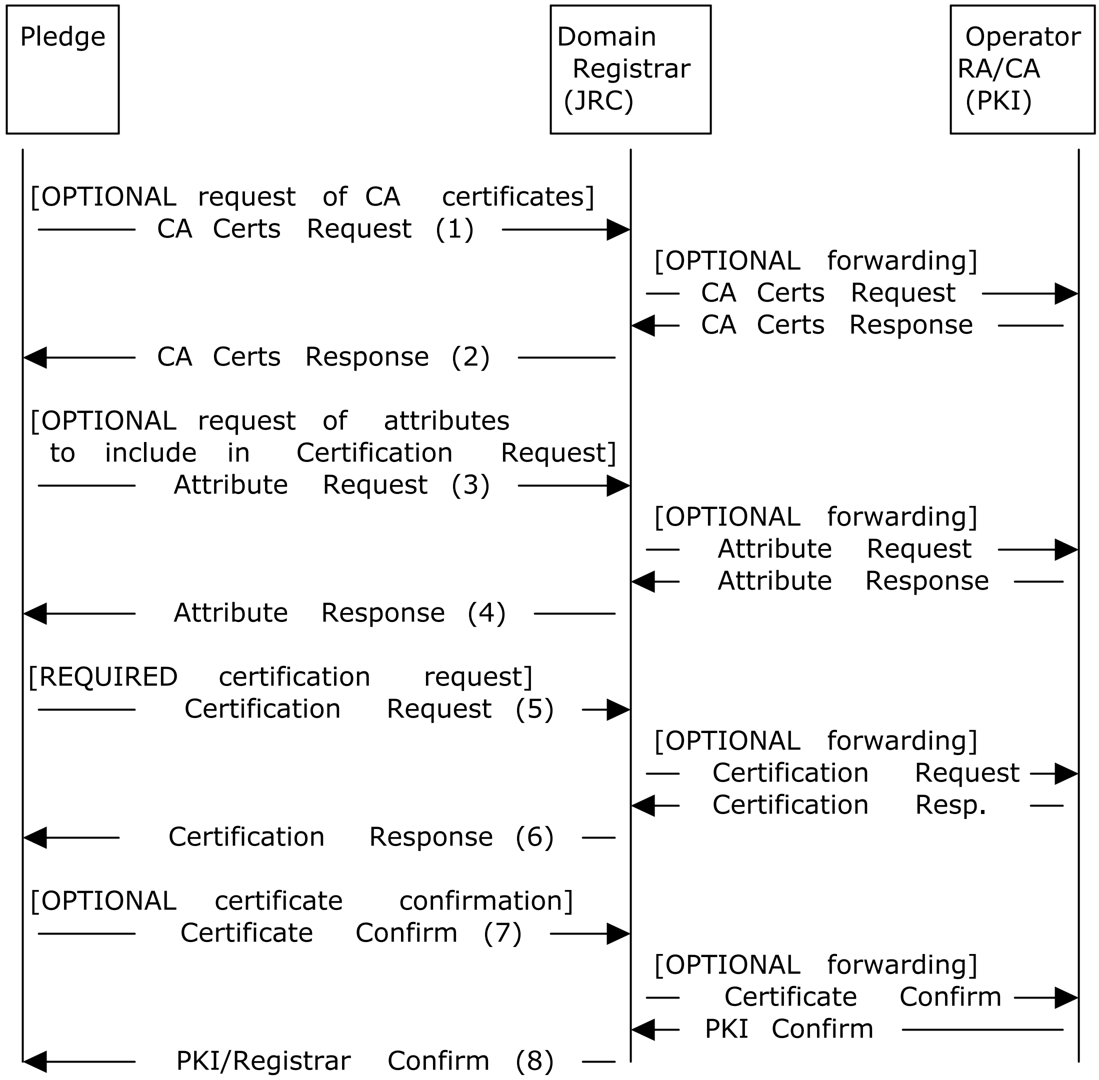

Figure 2: Certificate Enrollment Message Flow

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

The label [OPTIONAL forwarding] in Figure 2 means that on receiving from a pledge a request message of the given type, 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 and 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 is not properly authenticated or not 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 in the Certification Request (5) additional attributes that are specific to the target domain. 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 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): This **MUST** contain on success the requested certificate and **MAY** include further information, like certificates of intermediate CAs and any additional trust anchors.
- Certificate Confirm (7): An optional confirmation 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): 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, 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 BRSKI this is described as part of the certificate enrollment step, but due to the generalization on 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 -- see also 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 BRSKI for certification requests and the related CA certificates and CSR attributes retrieval functions uses the definition from EST [RFC7030]. Here is the example of simple enrollment: `"/.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 enrollment is considered here 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>`: **MUST** reference the protocol being used. Existing values include 'est' [RFC7030] as in BRSKI and 'cmp' as in [RFC9483] and Section 5.1 below. Values for other existing protocols such as CMC and SCEP, as well as for 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, depending on the enrollment protocol being used, the operation requested. Enrollment protocols are expected to define their request endpoints, as done by existing protocols (see also 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 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) [RFC9483] rather than [RFC4210] and [RFC9480], as the subset of CMP defined in 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 LCMPP [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 Section 4.4 and Section 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 Section 7 and Section 8. Further guidance can be found in [RFC9483], Section 6.

BRSKI-AE with CMP can also be combined with Constrained BRSKI [I-D.ietf-anima-constrained-voucher], using CoAP for enrollment message transport as described by CoAP Transport for CMP [RFC9482]. In such scenarios, the EST-specific parts of [I-D.ietf-anima-constrained-voucher] 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 BRSKI [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

This document requires one IANA action: register in the Service Name and Transport Protocol Port Number Registry the following service name.

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

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

7. Security Considerations

The security considerations laid out in BRSKI [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 pertains also to obtaining a valid domain-specific certificate, it must be made sure that a pledge can not circumvent the registrar in the decision of whether it is granted an LDevID certificate by the CA. There are various ways how to fulfill this, including:

- implicit consent
- the registrar signals 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 provides its consent using an extra message that is transferred on the same channel as the enrollment messages, possibly in a TLS tunnel.
- the registrar explicitly states its consent by signing, in addition to the pledge, the authenticated self-contained certificate enrollment request message.

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 [RFC9483] apply.

8. Privacy Considerations

The privacy considerations laid out in BRSKI [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. This in turn 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. 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), as well as Rajeev Ranjan, Rufus Buschart, Andreas Reiter, and Szofia Fazekas-Zisch (Siemens colleagues) for their reviews with suggestions for improvements.

10. References

10.1. 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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/rfc9483>.

10.2. Informative References

[BRSKI-AE-overview] S. Fries and D. von Oheimb, "BRSKI-AE Protocol Overview", March 2023, <https://datatracker.ietf.org/meeting/116/materials/slides-116-anima-update-on-brski-ae-alternative-enrollment-protocols-in-brski-00>. Graphics on slide 4 of the status update on the BRSKI-AE draft 04 at IETF 116.

[draft-ietf-anima-brski-discovery] Eckert, T. and E. Dijk, "Discovery for BRSKI variations", Work in Progress, Internet-Draft, draft-ietf-anima-brski-discovery-04 , July 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-anima-brski-discovery-04>.

[I-D.ietf-anima-constrained-voucher] 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-25, 8 July 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-anima-constrained-voucher-25>.

[IEC-62351-9] International Electrotechnical Commission, "IEC 62351 - Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment", IEC 62351-9, May 2017.

[ISO-IEC-15118-2] International Standardization Organization / International Electrotechnical Commission, "ISO/IEC 15118-2 Road vehicles - Vehicle-to-Grid Communication Interface - Part 2: Network and application protocol requirements", ISO/IEC 15118-2, April 2014.

[NERC-CIP-005-5] North American 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/rfc/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/rfc/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/rfc/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/rfc/rfc5272>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/rfc/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/rfc/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/rfc/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/rfc/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/rfc/rfc8366>.

[RFC8894] Gutmann, P., "Simple Certificate Enrolment Protocol", RFC 8894, DOI 10.17487/RFC8894, September 2020, <https://www.rfc-editor.org/rfc/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/rfc/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/rfc/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/rfc/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/rfc/rfc9482>.

[UNISIG-Subset-137] UNISIG, "Subset-137; ERTMS/ETCS On-line Key Management FFFIS; V1.0.0", December 2015, <https://www.era.europa.eu/sites/default/files/filesystem/ertms/ccs_tsi_annex_a_-

_mandatory_specifications/set_of_specifications_3_etcs_b3_r2_gsm-r_b1/index083_-_subset-137_v100.pdf>. http://www.kmc-subset137.eu/index.php/download/

Appendix A. Application Examples

This informative annex provides some detail about application examples.

A.1. Rolling Stock

Rolling stock or railroad cars contain a variety of sensors, actuators, and controllers, which communicate within the railroad car but also exchange information between railroad cars forming a train, 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 specifying 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 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 (the substation in this case). 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 for the infrastructure side mandatory support of two enrollment protocols: SCEP [RFC8894] and EST [RFC7030], while an Intelligent Electronic Device 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 others, 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

This 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 Level 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. Especially 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 can not 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.

Appendix B. History of Changes TBD RFC Editor: please delete

List of reviewers:

- Toerless Eckert (document shepherd)
- Barry Leiba (SECdir)

* Mahesh Jethanandani (IETF area director)
* Meral Shirazipour (Gen-ART reviewer)
* Deb Cooley, Gunter Van de Velde, John Scudder, Murray Kucherawy, Roman Danyliw, and Éric Vyncke (IESG reviewers)
* Michael Richardson (ANIMA design team)
* Rajeev Ranjan, Rufus Buschart, Szofia Fazekas-Zisch, etc. (Siemens)
* Reshad Rahman (YANGDOCTORS reviewer). Note that YANGDOCTORS Early review of 2021-08-15 referred to the PRM aspect of draft-ietf-anima-brski-async-enroll-03. This has been carved out of the draft to a different one and thus is no more applicable here.

IETF draft ae-12 -> ae-13:

* Due to IANA requirement, shorten service name `"brski-registrar-cmp"` to `"brski-reg-cmp"` and change contact for service name registration from IESG to IETF
* Address Deb Cooley's DISCUSS by adding an item to the requirements list Section 5.1 making the source of the initial trust anchor explicit.
  Including the vouchers in Figure 2 would not fit because the figure has a different scope (namely, certificate enrollment) and would get overloaded.
* Address Gunter Van de Velde's comments by taking over essentially all his rewrites of text to help the structure and simplify reading the content, while keeping the original message, as it helps improve document quality
* Address John Scudder's comments by tweaking Section 2, fully alphabetizing terms
* Address Murray Kucherawy's comment by adapting terminology entries, leaving out 'communication' from 'asynchronous communication' and 'synchronous communication'
* Address Roman Danyliw's comments by updating reference I-D.eckert-anima-brski-discovery to draft-ietf-anima-brski-discovery and adding Section 8, which refers to the BRSKI privacy considerations.
* Address Éric Vyncke's comment by replacing 'production' by 'manufacturing'

IETF draft ae-11 -> ae-12:

* Fix minor issues introduced during authors' response to the AD review, including nits spotted in the Gen-ART review by Meral Shirazipour

IETF draft ae-10 -> ae-11:

* In response to AD review by Mahesh Jethanandani,
  * replace most occurrences of 'Note:' by 'Note that' or the like
  * move 2nd paragraph of abstract to the introduction
  * remove section 1.2 and merge its first paragraph with the preceding section
  * reconsider normative language, replacing one 'may' by '**MAY**' in section 4.1
  * fix several ambiguities and hard-to-read sentences by re-phrasing them
  * make wording more consistent, in particular: 'certification request'
  * fix a number of (mostly grammar) nits
* Improve item on limitations of PKCS#10 regarding keys that cannot sign

IETF draft ae-09 -> ae-10:

* Add reference to RFC 8633 at first occurrence of 'voucher' (fixes #37)
* Update reference of CoAP Transfer for CMP from I-D to RFC 9482
* Move RFC 4210 and RFC 9480 references from normative to informative
* Fix `p10` vs. `pkcs10` entry in list of example endpoints in Section 4.3
* Minor fix in Figure 1 and few text tweaks due to Siemens-internal review
* Extend the list of reviewers and acknowledgments by two Siemens colleagues

IETF draft ae-08 -> ae-09:

* In response to review by Toerless,
  - tweak abstract to make meaning of 'alternative enrollment' more clear
  - expand on first use not "well-known" abbreviations, such as 'EST', adding also a references on their first use
  - add summary and reason for choosing CMP at end of Section 3.2
  - remove paragraph on optimistic discovery in controlled environments
  - mention role of reviewers also in acknowledgments section
* A couple of grammar and spelling fixes

IETF draft ae-07 -> ae-08:

* Update references to service names in Section 5.1

IETF draft ae-06 -> ae-07:

* Update subsections on discovery according to discussion in the design team
* In Section 5.1, replace 'mandatory' by '**REQUIRED**' regarding adherence to LCMPP, in response to SECDIR Last Call Review of ae-06 by Barry Leiba

IETF draft ae-05 -> ae-06:

* Extend section on discovery according to discussion in the design team
* Make explicit that MASA voucher status telemetry is as in BRSKI
* Add note that on delegation, RA may need info on pledge authorization

IETF draft ae-04 -> ae-05:

* Remove entries from the terminology section that should be clear from BRSKI
* Tweak use of the terms IDevID and LDevID and replace PKI RA/CA by RA/CA
* Add the abbreviation 'LCMPP' for Lightweight CMP Profile to the terminology section
* State clearly in Section 5.1 that LCMPP is mandatory when using CMP
* Change URL of BRSKI-AE-overview graphics to slide on IETF 116 meeting material

IETF draft ae-03 -> ae-04:

* In response to SECDIR Early Review of ae-03 by Barry Leiba,
  - replace 'end-to-end security' by the more clear 'end-to-end authentication'

  - restrict the meaning of the abbreviation 'AE' to 'Alternative Enrollment'
  - replace '**MAY**' by 'may' in requirement on delegated registrar actions
  - re-phrase requirement on certification request exchange, avoiding MANDATORY
  - mention that further protocol names need be put in Well-Known URIs registry
  - explain consequence of using non-standard endpoints, not following **SHOULD**
  - remove requirement that 'caPubs' field in CMP responses **SHOULD NOT** be used
  - add paragraph in security considerations on additional use of TLS for CMP

- In response to further internal reviews and suggestions for generalization,
  - significantly cut down the introduction because the original motivations and most explanations are no more needed and would just make it lengthy to read
  - sort out asynchronous vs. offline transfer, off-site vs. backend components
  - improve description of CSRs and proof of possession vs. proof of origin
  - clarify that the channel between pledge and registrar is not restricted to TLS, but in connection with constrained BRSKI may also be DTLS. Also move the references to Constrained BRSKI and CoAPS to better contexts.
  - clarify that the registrar must not be circumvented in the decision to grant and LDevID, and give hints and recommendations how to make sure this
  - clarify that the cert enrollment phase may involve additional messages and that BRSKI-AE replaces [RFC8995], Section 5.9 (except Section 5.9.4)
  - the certificate enrollment protocol needs to support transport over (D)TLS only as far as its messages are transported between pledge and registrar.
  - the certificate enrollment protocol chosen between pledge and registrar needs to be used also for the upstream enrollment exchange with the PKI only if end-to-end authentication shall be achieved across the registrar to the PKI.
  - add that with CMP, further trust anchors **SHOULD** be transported via `caPubs`
  - remove the former Appendix A: "Using EST for Certificate Enrollment", moving relevant points to the list of scenarios in Section 1.1: "Supported Scenarios",
  - streamline the item on EST in Section 3.2: "Solution Options for Proof of Identity",
  - various minor editorial improvements like making the wording more consistent

IETF draft ae-02 -> ae-03:

- In response to review by Toerless Eckert,
  - many editorial improvements and clarifications as suggested, such as the comparison to plain BRSKI, the description of offline vs. synchronous message transfer and enrollment, and better differentiation of RA flavors.
  - clarify that for transporting certificate enrollment messages between pledge and registrar, the TLS channel established between these two (via the join proxy) is used and the enrollment protocol **MUST** support this.
  - clarify that the enrollment protocol chosen between pledge and registrar **MUST** also be used for the upstream enrollment exchange with the PKI.
  - extend the description and requirements on how during the certificate enrollment phase the registrar **MAY** handle requests by the pledge itself and otherwise **MUST** forward them to the PKI and forward responses to the pledge.

- Change "The registrar **MAY** offer different enrollment protocols" to "The registrar **MUST** support at least one certificate enrollment protocol ..."
- In response to review by Michael Richardson,
  - slightly improve the structuring of the Message Exchange Section 4.2 and add some detail on the request/response exchanges for the enrollment phase
  - merge the 'Enhancements to the Addressing Scheme' Section 4.3 with the subsequent one: 'Domain Registrar Support of Alternative Enrollment Protocols'
  - add reference to SZTP (RFC 8572)
  - extend venue information
  - convert output of ASCII-art figures to SVG format
  - various small other text improvements as suggested/provided
- Remove the tentative informative application to EST-fullCMC
- Move Eliot Lear from co-author to contributor, add Eliot to the acknowledgments
- Add explanations for terms such as 'target domain' and 'caPubs'
- Fix minor editorial issues and update some external references

IETF draft ae-01 -> ae-02:

- Architecture: clarify registrar role including RA/LRA/enrollment proxy
- CMP: add reference to CoAP Transport for CMPV2 and Constrained BRSKI
- Include venue information

From IETF draft 05 -> IETF draft ae-01:

- Renamed the repo and files from 'anima-brski-async-enroll' to 'anima-brski-ae'
- Added graphics for abstract protocol overview as suggested by Toerless Eckert
- Balanced (sub-)sections and their headers
- Added details on CMP instance, now called BRSKI-CMP

From IETF draft 04 -> IETF draft 05:

- David von Oheimb became the editor.
- Streamline wording, consolidate terminology, improve grammar, etc.
- Shift the emphasis towards supporting alternative enrollment protocols.
- Update the title accordingly - preliminary change to be approved.
- Move comments on EST and detailed application examples to informative annex.
- Move the remaining text of section 3 as two new sub-sections of section 1.

From IETF draft 03 -> IETF draft 04:

- Moved UC2-related parts defining the pledge in responder mode to a separate document. This required changes and adaptations in several sections. Main changes concerned the removal of the subsection for UC2 as well as the removal of the YANG model related text as it is not applicable in UC1.
- Updated references to the Lightweight CMP Profile (LCMPP).
- Added David von Oheimb as co-author.

From IETF draft 02 -> IETF draft 03:

* Housekeeping, deleted open issue regarding YANG voucher-request in UC2 as voucher-request was enhanced with additional leaf.
* Included open issues in YANG model in UC2 regarding assertion value agent-proximity and CSR encapsulation using SZTP sub module).

From IETF draft 01 -> IETF draft 02:

* Defined call flow and objects for interactions in UC2. Object format based on draft for JOSE signed voucher artifacts and aligned the remaining objects with this approach in UC2 .
* Terminology change: issue #2 pledge-agent -> registrar-agent to better underline agent relation.
* Terminology change: issue #3 PULL/PUSH -> pledge-initiator-mode and pledge-responder-mode to better address the pledge operation.
* Communication approach between pledge and registrar-agent changed by removing TLS-PSK (former section TLS establishment) and associated references to other drafts in favor of relying on higher layer exchange of signed data objects. These data objects are included also in the pledge-voucher-request and lead to an extension of the YANG module for the voucher-request (issue #12).
* Details on trust relationship between registrar-agent and registrar (issue #4, #5, #9) included in UC2.
* Recommendation regarding short-lived certificates for registrar-agent authentication towards registrar (issue #7) in the security considerations.
* Introduction of reference to agent signing certificate using SKID in agent signed data (issue #11).
* Enhanced objects in exchanges between pledge and registrar-agent to allow the registrar to verify agent-proximity to the pledge (issue #1) in UC2.
* Details on trust relationship between registrar-agent and pledge (issue #5) included in UC2.
* Split of use case 2 call flow into sub sections in UC2.

From IETF draft 00 -> IETF draft 01:

* Update of scope in Section 1.1 to include in which the pledge acts as a server. This is one main motivation for use case 2.
* Rework of use case 2 to consider the transport between the pledge and the pledge-agent. Addressed is the TLS channel establishment between the pledge-agent and the pledge as well as the endpoint definition on the pledge.
* First description of exchanged object types (needs more work)
* Clarification in discovery options for enrollment endpoints at the domain registrar based on well-known endpoints in Section 4.3 do not result in additional /.well-known URIs. Update of the illustrative example. Note that the change to /brski for the voucher-related endpoints has been taken over in the BRSKI main document.
* Updated references.
* Included Thomas Werner as additional author for the document.

From individual version 03 -> IETF draft 00:

* Inclusion of discovery options of enrollment endpoints at the domain registrar based on well-known endpoints in Section 4.3 as replacement of section 5.1.3 in the individual draft. This is intended to support both use cases in the document. An illustrative example is provided.
* Missing details provided for the description and call flow in pledge-agent use case UC2, e.g. to accommodate distribution of CA certificates.
* Updated CMP example in Section 5 to use Lightweight CMP instead of CMP, as the draft already provides the necessary /.well-known endpoints.
* Requirements discussion moved to separate section in Section 3. Shortened description of proof-of-identity binding and mapping to existing protocols.
* Removal of copied call flows for voucher exchange and registrar discovery flow from [RFC8995] in Section 4 to avoid doubling or text or inconsistencies.
* Reworked abstract and introduction to be more crisp regarding the targeted solution. Several structural changes in the document to have a better distinction between requirements, use case description, and solution description as separate sections. History moved to appendix.

From individual version 02 -> 03:

* Update of terminology from self-contained to authenticated self-contained object to be consistent in the wording and to underline the protection of the object with an existing credential. Note that the naming of this object may be discussed. An alternative name may be attestation object.
* Simplification of the architecture approach for the initial use case having an off-site PKI.
* Introduction of a new use case utilizing authenticated self-contain objects to onboard a pledge using a commissioning tool containing a pledge-agent. This requires additional changes in the BRSKI call flow sequence and led to changes in the introduction, the application example,and also in the related BRSKI-AE call flow.
* Update of provided examples of the addressing approach used in BRSKI to allow for support of multiple enrollment protocols in Section 4.3.

From individual version 01 -> 02:

* Update of introduction text to clearly relate to the usage of IDevID and LDevID.
* Definition of the addressing approach used in BRSKI to allow for support of multiple enrollment protocols in Section 4.3. This section also contains a first discussion of an optional discovery mechanism to address situations in which the registrar supports more than one enrollment approach. Discovery should avoid that the pledge performs a trial and error of enrollment protocols.
* Update of description of architecture elements and changes to BRSKI in Section 4.1.
* Enhanced consideration of existing enrollment protocols in the context of mapping the requirements to existing solutions in Section 3 and in Section 5.

From individual version 00 -> 01:

* Update of examples, specifically for building automation as well as two new application use cases in Appendix A.

* Deletion of asynchronous interaction with MASA to not complicate the use case. Note that the voucher exchange can already be handled in an asynchronous manner and is therefore not considered further. This resulted in removal of the alternative path the MASA in Figure 1 and the associated description in Section 4.1.
* Enhancement of description of architecture elements and changes to BRSKI in Section 4.1.
* Consideration of existing enrollment protocols in the context of mapping the requirements to existing solutions in Section 3.
* New section starting Section 5 with the mapping to existing enrollment protocols by collecting boundary conditions.

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/