Workgroup:	ANIMA WG
Internet-Draft:	draft-ietf-anima-brski-async-enroll-04
Published:	8 November 2021
Intended Status:	Standards Track
Expires:	12 May 2022
Authors:	S. Fries	H. Brockhaus	D. von Oheimb	E. Lear
---	---	---	---	---
	Siemens	*Siemens*	*Siemens*	*Cisco Systems*

Support of Asynchronous Enrollment in BRSKI (BRSKI-AE)

Abstract

This document describes enhancements of bootstrapping a remote secure key infrastructure (BRSKI, [RFC8995]) to also operate in domains featuring no or only timely limited connectivity between involved components. To support such use cases, BRSKI-AE relies on the exchange of authenticated self-contained objects (signature-wrapped objects) also for requesting and distributing of domain specific device certificates. The defined approach is agnostic regarding the utilized enrollment protocol allowing the application of existing and potentially new certificate management protocols.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 12 May 2022.

Copyright Notice

Table of Contents

1. Introduction

BRSKI as defined in [RFC8995] specifies a solution for secure zero-touch (automated) bootstrapping of devices (pledges) in a (customer) site domain. This includes the discovery of network elements in the target domain, time synchronization, and the exchange of security information necessary to establish trust between a pledge and the domain. Security information about the target domain, specifically the target domain certificate, is exchanged utilizing voucher objects as defined in [RFC8366]. These vouchers are authenticated self-contained (signed) objects, which may be provided online (synchronous) or offline (asynchronous) via the domain registrar to the pledge and originate from a Manufacturer's Authorized Signing Authority (MASA).

For the enrollment of devices BRSKI relies on EST [RFC7030] to request and distribute target domain specific device certificates. EST in turn relies on a binding of the certification request to an underlying TLS connection between the EST client and the EST server. According to BRSKI the domain registrar acts as EST server and is also acting as registration authority (RA) or local registration authority (LRA). The binding to TLS is used to protect the exchange of a certification request (for a LDevID EE certificate) and to provide data origin authentication (client identity information), to support the authorization decision for processing the certification request. The TLS connection is mutually authenticated and the client-side authentication utilizes the pledge's manufacturer issued device certificate (IDevID certificate). This approach requires an on-site availability of a local asset or inventory management system performing the authorization decision based on tuple of the certification request and the pledge authentication using the IDevID certificate, to issue a domain specific certificate to the pledge. The EST server (the domain registrar) terminates the security association with the pledge and thus the binding between the certification request and the authentication of the pledge via TLS. This type of enrollment utilizing an online connection to the PKI is considered as synchronous enrollment.

For certain use cases on-site support of a RA/CA component and/or an asset management is not available and rather provided by an operator's backend and may be provided timely limited or completely through offline interactions. This may be due to higher security requirements for operating the certification authority or for optimization of operation for smaller deployments to avoid the always on-site operation. The authorization of a certification request based on an asset management in this case will not / can not be performed on-site at enrollment time. Enrollment, which cannot be performed in a (timely) consistent fashion is considered as asynchronous enrollment in this document. It requires the support of a store and forward functionality of

certification request together with the requester authentication (and identity) information. This enables processing of the request at a later point in time. A similar situation may occur through network segmentation, which is utilized in industrial systems to separate domains with different security needs. Here, a similar requirement arises if the communication channel carrying the requester authentication is terminated before the RA/CA authorization handling of the certification request. If a second communication channel is opened to forward the certification request to the issuing RA/ CA, the requester authentication information needs to be retained and ideally bound to the certification request. This uses case is independent from timely limitations of the first use case. For both cases, it is assumed that the requester authentication information is utilized in the process of authorization of a certification request. There are different options to perform store and forward of certification requests including the requester authentication information:

- Providing a trusted component (e.g., an LRA) in the target domain, which stores the certification request combined with the requester authentication information (based on the IDevID) and potentially the information about a successful proof of possession (of the corresponding private key) in a way prohibiting changes to the combined information. Note that the assumption is that the information elements may not be cryptographically bound together. Once connectivity to the backend is available, the trusted component forwards the certification request together with the requester information (authentication and proof of possession) to the off-site PKI for further processing. It is assumed that the off-site PKI in this case relies on the local pledge authentication result and thus performs the authorization and issues the requested certificate. In BRSKI the trusted component may be the EST server residing co-located with the registrar in the target domain.
- Utilization of authenticated self-contained objects for the enrollment, binding the certification request and the requester authentication in a cryptographic way. This approach reduces the necessary trust in a domain component to storage and delivery. Unauthorized modifications of the requester information (request and authentication) can be detected during the verification of the authenticated self-contained object.

Focus of this document the support of handling authenticated self-contained objects for bootstrapping. As it is intended to enhance BRSKI it is named BRSKI-AE, where AE stands for asynchronous enrollment. As BRSKI, BRSKI-AE results in the pledge storing an X.509 domain certificate and sufficient information for verifying the domain registrar / proxy identity (LDevID CA Certificate) as well as domain specific X.509 device certificates (LDevID EE certificate).

The goal is to enhance BRSKI to be applicable to the additional use cases. This is addressed by

- enhancing the well-known URI approach with an additional path for the utilized enrollment protocol.
- defining a certificate waiting indication and handling, if the certifying component is (temporarily) not available.

Note that in contrast to BRSKI, BRSKI-AE assumes support of multiple enrollment protocols on the infrastructure side, allowing the pledge manufacturer to select the most appropriate. Thus, BRSKI-AE can be applied for both, asynchronous and synchronous enrollment.

2. Terminology

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]. The following terms are defined additionally:

CA: Certification authority, issues certificates.

RA: Registration authority, an optional system component to which a CA delegates certificate management functions such as authorization checks.

LRA: Local registration authority, an optional RA system component with proximity to end entities.

IED: Intelligent Electronic Device (in essence a pledge).

on-site: Describes a component or service or functionality available in the target deployment domain.

off-site: Describes a component or service or functionality available in an operator domain different from the target deployment domain. This may be a central site or a cloud service, to which only a temporary connection is available, or which is in a different administrative domain.

asynchronous communication: Describes a timely interrupted communication between an end entity and a PKI component.

synchronous communication: Describes a timely uninterrupted communication between an end entity and a PKI component.

authenticated self-contained object: Describes an object, which is cryptographically bound to the EE certificate (IDevID certificate or LDEVID certificate) of a pledge. The binding is assumed to be provided through a digital signature of the actual object using the corresponding private key of the EE certificate.

3. Scope of solution

3.1. Supported environment

This solution is intended to be used in domains with limited support of on-site PKI services and comprises use cases in which:

- there is no registration authority available in the target domain. The connectivity to an off-site RA in an operator's network may only be available temporarily. A local store and forward device is used for the communication with the off-site services.
- authoritative actions of a LRA are limited and may not comprise authorization of certification requests of pledges. Final authorization is done at the RA residing in the operator domain.
- the target deployment domain already has an established certificate management approach that shall be reused to (e.g., in brownfield installations).

3.2. Application Examples

The following examples are intended to motivate the support of different enrollment approaches in general and asynchronous enrollment specifically, by introducing industrial applications cases, which could leverage BRSKI as such but also require support of asynchronous operation as intended with BRSKI-AE.

3.2.1. 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 building a train, or with a backend. These devices are typically unaware of backend connectivity. Managing certificates may be done during maintenance cycles of the railroad car, but can already be prepared during operation. The preparation may comprise the generation of certification requests by the components which are collected and forwarded for processing, once the railroad car is connected to the operator backend. The authorization of the certification request is then done based on the operator's asset/inventory information in the backend.

3.2.2. Building automation

In building automation, a use case can be described by a detached building or the basement of a building equipped with sensor, actuators, and controllers connected, but with only limited or no connection to the centralized building management system. This limited connectivity may be during the installation time but also during operation time. During the installation in the basement, a service technician collects the necessary information from the basement network and provides them to the central building management system, e.g., using a laptop or even a mobile phone to transport the information. This information may comprise parameters and settings required in the operational phase of the sensors/actuators, like a certificate issued by the operator to authenticate against other components and services.

The collected information may be provided by a domain registrar already existing in the installation network. In this case connectivity to the backend PKI may be facilitated by the service technician's laptop. Contrary, the information can also be collected from the pledges directly and provided to a domain registrar deployed in a different network. In this cases connectivity to the domain registrar may be facilitated by the service technician's laptop.

3.2.3. Substation automation

In electrical substation automation a control center typically hosts PKI services to issue certificates for Intelligent Electronic Devices (IED)s operated in a substation. Communication between the substation and control center is done 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 different enrollment protocols to facilitate the capabilities of IEDs from different vendors. The IEC standard IEC62351-9 [IEC-62351-9] specifies the mandatory support of two enrollment protocols, SCEP [RFC8894] and EST [RFC7030] for the infrastructure side, while the IED must only support one of the two.

3.2.4. Electric vehicle charging infrastructure

For the electric vehicle charging infrastructure protocols have been defined for the interaction between the electric vehicle (EV) 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 the context of a TLS connection between the EV and the charging point. The management of this certificate depends (beyond others) on the selected backend connectivity protocol. Specifically, in case of OCPP it is intended as single 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 is intended to be handled in-band of OCPP. This requires to be able to encapsulate the certificate management exchanges in a transport independent way. Authenticated self-containment will ease this by allowing the transport without a separate enrollment protocol. This provides a binding of the exchanges to the identity of the communicating endpoints.

3.2.5. 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 resources will be allowed in carefully controlled short periods of time, for example when a batch of new devices are deployed, but impossible at other times.

3.2.6. Less operational security in the target domain

The registration point performing the authorization of a certificate request is a critical PKI component and therefore implicates higher operational security than other components utilizing the issued certificates for their security features. CAs may also demand higher security in the registration procedures. Especially the CA/Browser forum currently increases the security requirements in the certificate issuance procedures for publicly trusted certificates. There may be

the situation that the target domain does not offer enough security to operate a registration point and therefore wants to transfer this service to a backend that offers a higher level of operational security.

4. Requirement discussion and mapping to solution elements

For the requirements discussion it is assumed that the domain registrar receiving a certification request as authenticated self-contained object is not the authorization point for this certification request. If the domain registrar is the authorization point and the pledge has a direct connection to the registrar, BRSKI can be used directly. Note that BRSKI-AE could also be used in this case.

Based on the intended target environment described in Section 3.1 and the motivated application examples described in Section 3.2 the following base requirements are derived to support authenticated self-contained objects as container carrying the certification request and further information to support asynchronous operation.

At least the following properties are required:

- Proof of Possession: proves to possess and control the private key corresponding to the public key contained in the certification request, typically by adding a signature using the private key.
- Proof of Identity: provides data-origin authentication of a data object, e.g., a certificate request, utilizing an existing IDevID. Certificate updates may utilize the certificate that is to be updated.

Solution examples (not complete) based on existing technology are provided with the focus on existing IETF documents:

- Certification request objects: Certification requests are structures protecting only the integrity of the contained data providing a proof-of-private-key-possession for locally generated key pairs. Examples for certification requests are:
  - PKCS#10 [RFC2986]: Defines a structure for a certification request. The structure is signed to ensure integrity protection and proof of possession of the private key of the requester that corresponds to the contained public key.
  - CRMF [RFC4211]: Defines a structure for the certification request message. The structure supports integrity protection and proof of possession, through a signature generated over parts of the structure by using the private key corresponding to the contained public key. CRMF also supports further proof-of-possession methods for key pairs not capable to be used for signing.

  Note that the integrity of the certification request is bound to the public key contained in the certification request by performing the signature operation with the corresponding private key. In the considered application examples, this is not sufficient to provide data origin authentication and needs to be bound to the existing credential of the pledge (IDevID)

additionally. This binding supports the authorization decision for the certification request through the provisioning of a proof of identity. The binding of data origin authentication to the certification request may be delegated to the protocol used for certificate management.

- Proof of Identity options: The certification request should be bound to an existing credential (here IDevID) to enable a proof of identity and based on it an authorization of the certification request. The binding may be realized through security options in an underlying transport protocol if the authorization of the certification request is done at the next communication hop. Alternatively, this binding can be done by a wrapping signature employing an existing credential (initial: IDevID, renewal: LDevID). This requirement is addressed by existing enrollment protocols in different ways, for instance:
  - EST [RFC7030]: Utilizes PKCS#10 to encode the certification request. The Certificate Signing Request (CSR) may contain a binding to the underlying TLS by including the tls-unique value in the self-signed CSR structure. The tls-unique value is one result of the TLS handshake. As the TLS handshake is performed mutually authenticated and the pledge utilized its IDevID for it, the proof of identity can be provided by the binding to the TLS session. This is supported in EST using the simpleenroll endpoint. To avoid the binding to the underlying authentication in the transport layer, EST offers the support of a wrapping the CSR with an existing certificate by using Full PKI Request messages.
  - SCEP [RFC8894]: Provides the option to utilize either an existing secret (password) or an existing certificate to protect the CSR based on SCEP Secure Message Objects using CMS wrapping ([RFC5652]). Note that the wrapping using an existing IDevID credential in SCEP is referred to as renewal. SCEP therefore does not rely on the security of an underlying transport.
  - CMP [RFC4210] Provides the option to utilize either an existing secret (password) or an existing certificate to protect the PKIMessage containing the certification request. The certification request is encoded utilizing CRMF. PKCS#10 is optionally supported. The proof of identity of the PKIMessage containing the certification request can be achieved by using IDevID credentials to a PKIProtection carrying the actual signature value. CMP therefore does not rely on the security of an underlying transport protocol.
  - CMC [RFC5272] Provides the option to utilize either an existing secret (password) or an existing certificate to protect the certification request (either in CRMF or PKCS#10) based on CMS [RFC5652]). Here a FullCMCRequest can be used, which allows signing with an existing IDevID credential to provide a proof of identity. CMC therefore does not rely on the security of an underlying transport.

Note that besides the already existing enrollment protocols there is ongoing work in the ACE WG to define an encapsulation of EST messages in OSCORE to result in a TLS independent way of protecting EST. This approach [I-D.selander-ace-coap-est-oscore] may be considered as further variant.

5. Architectural Overview and Communication Exchanges

To support asynchronous enrollment, the base system architecture defined in BRSKI [RFC8995] is enhanced to facilitate support of alternative enrollment protocols. In general, the communication follows the BRSKI model and utilizes the existing BRSKI architecture elements.

The pledge initiates the communication with the domain registrar. Necessary enhancements to support authenticated self-contained objects for certificate enrollment are kept on a minimum to ensure reuse of already defined architecture elements and interactions.

For the authenticated self-contained objects used for the certification request, BRSKI-AE relies on the defined message wrapping mechanisms of the enrollment protocols stated in Section 4 above.

5.1. Support of off-site PKI service

One assumption of BRSKI-AE is that the authorization of a certification request is performed based on an authenticated self-contained object, binding the certification request to the authentication using the IDevID. This supports interaction with off-site or off-line PKI (RA/CA) components. In addition, the authorization of the certification request may not be done by the domain registrar but by a PKI residing in the backend of the domain operator (off-site) as described in Section 3.1. Also, the certification request may be piggybacked by another protocol. This leads to changes in the placement or enhancements of the logical elements as shown in Figure 1.

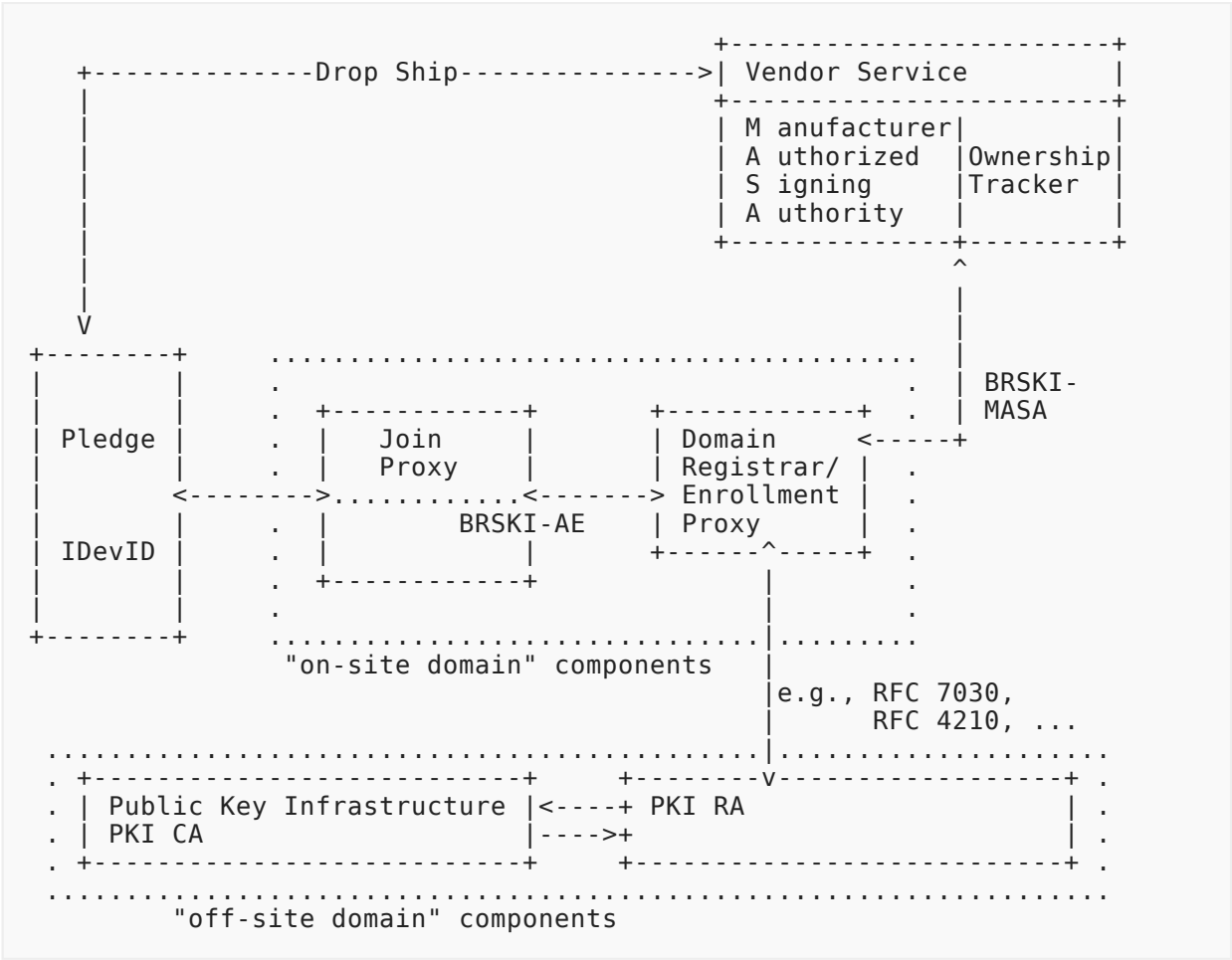

Figure 1: Architecture overview using off-site PKI components

The architecture overview in Figure 1 utilizes the same logical elements as BRSKI but with a different placement in the deployment architecture for some of the elements. The main difference is the placement of the PKI RA/CA component, which is performing the authorization decision for the certification request message. It is placed in the off-site domain of the operator (not the deployment site directly), which may have no or only temporary connectivity to the deployment or on-site domain of the pledge. This is to underline the authorization decision for the certification request in the backend rather than on-site. The following list describes the components in the target domain:

- Join Proxy: same functionality as described in BRSKI.
- Domain Registrar / Enrollment Proxy: In general the domain registrar proxy has a similar functionality regarding the imprinting of the pledge in the deployment domain to facilitate the communication of the pledge with the MASA and the PKI. Different is the authorization of the certification request. BRSKI-AE allows to perform this in the operator's backend (off-site), and not directly at the domain registrar.
  - Voucher exchange: The voucher exchange with the MASA via the domain registrar is performed as described in BRSKI [RFC8995].

- Certificate enrollment: For the pledge enrollment the domain registrar in the deployment domain supports the adoption of the pledge in the domain based on the voucher request. Nevertheless, it may not have sufficient information for authorizing the certification request. If the authorization of the certification request is done in the off-site domain, the domain registrar forwards the certification request to the RA to perform the authorization. Note that this requires, that the certification request object is enhanced with a proof-of-identity to allow the authorization based on the bound identity information of the pledge. As stated above, this can be done by an additional signature using the IDevID. The domain registrar here acts as an enrollment proxy or local registration authority. It is also able to handle the case having no connection temporarily to an off-site PKI, by storing the authenticated certification request and forwarding it to the RA upon reestablished connectivity. As authenticated self-contained objects are used, it requires an enhancement of the domain registrar. This is done by supporting alternative enrollment approaches (protocol options, protocols, encoding) by enhancing the addressing scheme to communicate with the domain registrar (see Section 5.1.5).

The following list describes the vendor related components/service outside the deployment domain:

- MASA: general functionality as described in [RFC8995]. Assumption is that the interaction with the MASA may be synchronous (voucher request with nonce) or asynchronous (voucher request without nonce).
- Ownership tracker: as defined in [RFC8995].

The following list describes the operator related components/service operated in the backend:

- PKI RA: Performs certificate management functions (validation of certification requests, interaction with inventory/asset management for authorization of certification requests, etc.) for issuing, updating, and revoking certificates for a domain as a centralized infrastructure for the domain operator. The inventory (asset) management may be a separate component or integrated into the RA directly.
- PKI CA: Performs certificate generation by signing the certificate structure provided in the certification request.

Based on BRSKI and the architectural changes the original protocol flow is divided into three phases showing commonalities and differences to the original approach as depicted in the following.

- Discovery phase (same as BRSKI)
- Voucher exchange with deployment domain registrar (same as BRSKI).
- Enrollment phase (changed to support the application of authenticated self-contained objects).

5.1.1. Behavior of a pledge

The behavior of a pledge as described in [RFC8995] is kept with one exception. After finishing the imprinting phase (4) the enrollment phase (5) is performed with a method supporting authenticated self-contained objects. Using EST with simple-enroll cannot be applied here, as it binds the pledge authentication with the existing IDevID to the transport channel (TLS) rather than to the certification request object directly. This authentication in the transport layer is not visible / verifiable at the authorization point in the off-site domain. Section 6 discusses potential enrollment protocols and options applicable.

5.1.2. Pledge - Registrar discovery and voucher exchange

The discovery phase is applied as specified in [RFC8995].

5.1.3. Registrar - MASA voucher exchange

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

5.1.4. Pledge - Registrar - RA/CA certificate enrollment

As stated in Section 4 the enrollment shall be performed using an authenticated self-contained object providing proof of possession and proof of identity.

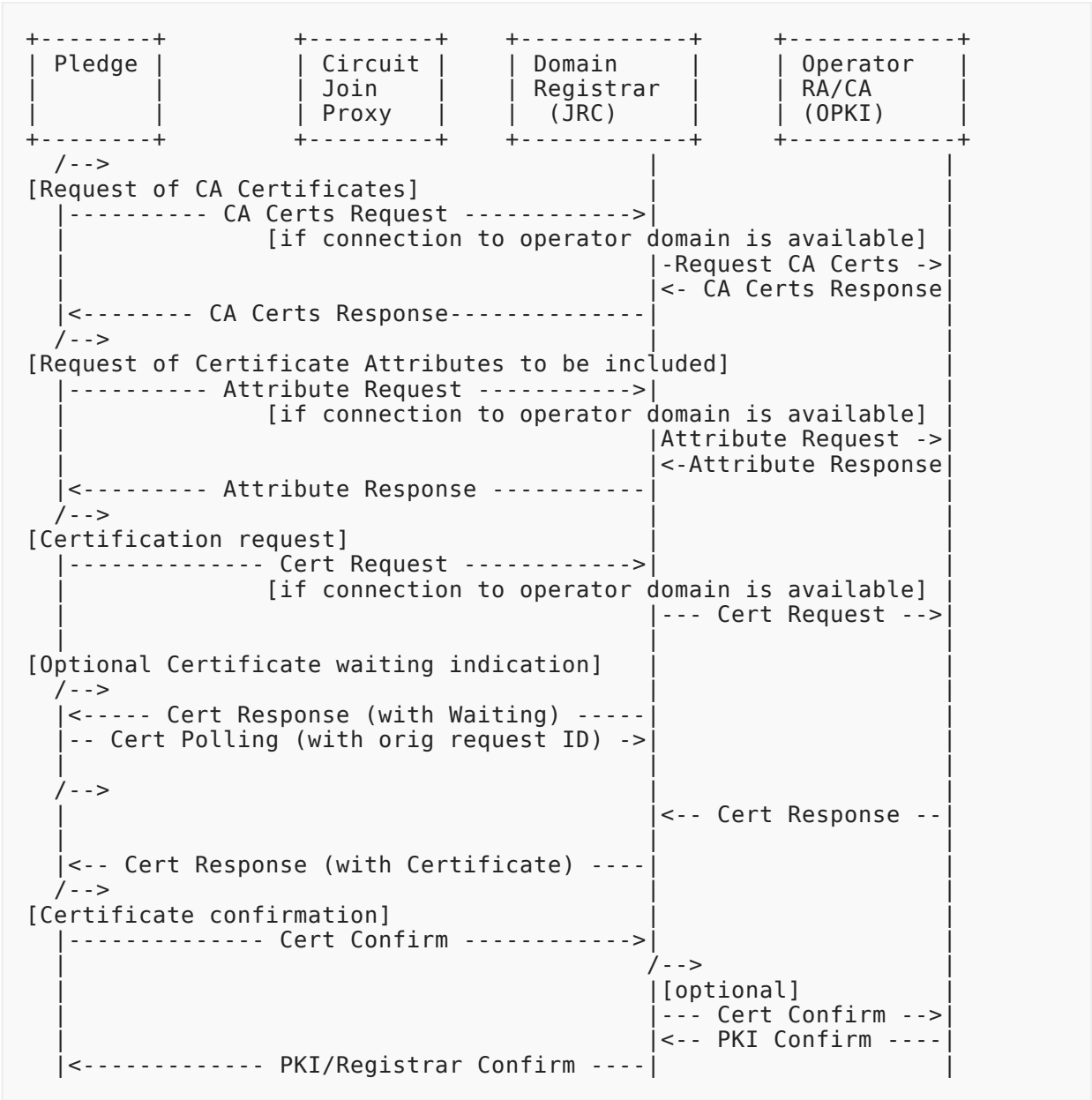

Figure 2: Certificate enrollment

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

- CA Cert Request: The pledge **SHOULD** request the full distribution of CA Certificates. This ensures that the pledge has the complete set of current CA certificates beyond the pinned-domain-cert (which may be the domain registrar certificate contained in the voucher).
- CA Cert Response: Contains at least one CA certificate of the issuing CA.
- Attribute Request: 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 specific to the deployment domain into the certification request. To get these attributes in advance, the attribute request **SHOULD** be used.

- Attribute Response: Contains the attributes to be included in the certification request message.
- Cert Request: Depending on the utilized enrollment protocol, this certification request contains the authenticated self-contained object ensuring both, proof-of-possession of the corresponding private key and proof-of-identity of the requester.
- Cert Response: certification response message containing the requested certificate and potentially further information like certificates of intermediary CAs on the certification path.
- Cert Waiting: waiting indication for the pledge to retry after a given time. For this a request identifier is necessary. This request identifier may be either part of the enrollment protocol or build based on the certification request.
- Cert Polling: querying the registrar, if the certificate request was already processed; can be answered either with another Cert Waiting, or a Cert Response.
- Cert Confirm: confirmation message from pledge after receiving and verifying the certificate.
- PKI/Registrar Confirm: confirmation message from PKI/registrar about reception of the pledge's certificate confirmation.

The generic messages described above can implemented using various protocols implementing authenticated self-contained objects, as described in Section 4. Examples are available in Section 6.

5.1.5. Addressing Scheme Enhancements

BRSKI-AE provides enhancements to the addressing scheme defined in [RFC8995] to accommodate the additional handling of authenticated self-contained objects for the certification request. As this is supported by different enrollment protocols, they can be directly employed (see also Section 6).

The addressing scheme in BRSKI for client certificate request and CA certificate distribution function during the enrollment uses the definition from EST [RFC7030], here on the example on simple enroll: "/.well-known/est/simpleenroll" This approach is generalized to the following notation: "/.well-known/enrollment-protocol/request" in which enrollment-protocol may be an already existing protocol or a newly defined approach. Note that enrollment is considered here as a sequence of at least a certification request and a certification response. In case of existing enrollment protocols the following notation is used proving compatibility to BRSKI:

- enrollment-protocol: references either EST [RFC7030] as in BRSKI or CMP, CMC, SCEP, or newly defined approaches as alternatives. Note: additional endpoints (well-known URI) at the registrar may need to be defined by the utilized enrollment protocol.
- request: depending on the utilized enrollment protocol, the request describes the required operation at the registrar side. Enrollment protocols are expected to define the request endpoints as done by existing protocols (see also Section 6).

5.2. Domain registrar support of different enrollment options

Well-known URIs for different endpoints on the domain registrar are already defined as part of the base BRSKI specification. In addition, alternative enrollment endpoints may be supported at the domain registrar. The pledge will recognize if its supported enrollment option is supported by the domain registrar by sending a request to its preferred enrollment endpoint.

The following provides an illustrative example for a domain registrar supporting different options for EST as well as CMP to be used in BRSKI-AE. The listing contains the supported endpoints for the bootstrapping, to which the pledge may connect. This includes the voucher handling as well as the enrollment endpoints. The CMP related enrollment endpoints are defined as well-known URI in CMP Updates [I-D.ietf-lamps-cmp-updates] and the Lightweight CMP profile [I-D.ietf-lamps-lightweight-cmp-profile].

```
</brski/voucherrequest>,ct=voucher-cms+json
</brski/voucher_status>,ct=json
</brski/enrollstatus>,ct=json
</est/cacerts>;ct=pkcs7-mime
</est/simpleenroll>;ct=pkcs7-mime
</est/simplereenroll>;ct=pkcs7-mime
</est/fullcmc>;ct=pkcs7-mime
</est/serverkeygen>;ct= pkcs7-mime
</est/csrattrs>;ct=pkcs7-mime
</cmp/initialization>;ct=pkixcmp
</cmp/certification>;ct=pkixcmp
</cmp/keyupdate>;ct=pkixcmp
</cmp/p10>;ct=pkixcmp
</cmp/getCAcert>;ct=pkixcmp
</cmp/getCSRparam>;ct=pkixcmp
```

TBD RFC Editor: please delete /*

Open Issues:

- In addition to the current content types, we may specify that the response provide information about different content types as multiple values. This would allow to further adopt the encoding of the objects exchanges (ASN.1, JSON, CBOR, ...). -> dependent on the utilized protocol. */

6. Example for signature-wrapping using existing enrollment protocols

This section map the requirements to support proof of possession and proof of identity to selected existing enrollment protocols. Note that that the work in the ACE WG described in [I-D.selander-ace-coap-est-oscore] may be considered here as well, as it also addresses the encapsulation of EST in a way to make it independent from the underlying TLS using OSCORE resulting in an authenticated self-contained object.

6.1. EST Handling

When using EST [RFC7030], the following constraints should be considered:

- Proof of possession is provided by using the specified PKCS#10 structure in the request.
- Proof of identity is achieved by signing the certification request object, which is only supported when Full PKI Request (the /fullcmc endpoint) is used. This contains sufficient information for the RA to make an authorization decision on the received certification request. Note: EST references CMC [RFC5272] for the definition of the Full PKI Request. For proof of identity, the signature of the SignedData of the Full PKI Request would be calculated using the IDevID credential of the pledge.
- TBD RFC Editor: please delete /* TBD: in this case the binding to the underlying TLS connection is not be necessary. */
- When the RA is not available, as per [RFC7030] Section 4.2.3, a 202 return code should be returned by the Registrar. The pledge in this case would retry a simpleenroll with a PKCS#10 request. Note that if the TLS connection is teared down for the waiting time, the PKCS#10 request would need to be rebuilt if it contains the unique identifier (tls_unique) from the underlying TLS connection for the binding.
- TBD RFC Editor: please delete /* TBD: clarification of retry for fullcmc is necessary as not specified in the context of EST */

6.2. CMP Handling

Instead of using general CMP [RFC4210], this specification refers to the Lightweight CMP Profile [I-D.ietf-lamps-lightweight-cmp-profile], as it restricts the full featured CMP to the functionality needed here. For this, the following constrains should be observed:

- For proof of possession, the defined approach in Lightweight CMP Profile [I-D.ietf-lamps-lightweight-cmp-profile] section 4.1.1 (based on CRMF) and 4.1.4 (based on PCKS#10) should be supported.
- Proof of identity can be provided by using the signatures to protect the certificate request message as outlined in section 3.2. of [I-D.ietf-lamps-lightweight-cmp-profile].
- When the RA/CA is not available, a waiting indication should be returned in the PKIStatus by the Registrar as specified in sections 4.4 and 5.1.2 of [I-D.ietf-lamps-lightweight-cmp-profile] for delayed delivery.
- Requesting CA certificates and certificate request attributes should be implemented a specified in Lightweight CMP Profile sections 4.3.1 and 4.3.3 [I-D.ietf-lamps-lightweight-cmp-profile].

7. IANA Considerations

This document does not require IANA actions.

8. Security Considerations

The security considerations as laid out in Lightweight CMP Profile [I-D.ietf-lamps-lightweight-cmp-profile] apply.

9. Acknowledgments

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

10. References

10.1. Normative References

[I-D.ietf-lamps-cmp-updates] Brockhaus, H., Oheimb, D. V., and J. Gray, "Certificate Management Protocol (CMP) Updates", Work in Progress, Internet-Draft, draft-ietf-lamps-cmp-updates-13, 25 October 2021, <https://www.ietf.org/archive/id/draft-ietf-lamps-cmp-updates-13.txt>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

10.2. Informative References

[I-D.ietf-lamps-lightweight-cmp-profile] Brockhaus, H., Fries, S., and D. V. Oheimb, "Lightweight Certificate Management Protocol (CMP) Profile", Work in Progress, Internet-Draft, draft-ietf-lamps-lightweight-cmp-profile-07, 25 October 2021, <https://www.ietf.org/archive/id/draft-ietf-lamps-lightweight-cmp-profile-07.txt>.

[I-D.selander-ace-coap-est-oscore] Selander, G., Raza, S., Furuhed, M., Vucinic, M., and T. Claeys, "Protecting EST Payloads with OSCORE", Work in Progress, Internet-Draft, draft-selander-ace-coap-est-oscore-05, 5 May 2021, <https://www.ietf.org/archive/id/draft-selander-ace-coap-est-oscore-05.txt>.

[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.

[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>.

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

Appendix A. History of changes TBD RFC Editor: please delete

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.

- 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 3.1 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 5.2 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 5.2 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 6 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 4. 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 5.1 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 offsite 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 5.1.5.

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 5.1.5. 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 5.

- Enhanced consideration of existing enrollment protocols in the context of mapping the requirements to existing solutions in Section 4 and in Section 6.

From individual version 00 -> 01:

- Update of examples, specifically for building automation as well as two new application use cases in Section 3.2.
- 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 5.
- Enhancement of description of architecture elements and changes to BRSKI in Section 5.
- Consideration of existing enrollment protocols in the context of mapping the requirements to existing solutions in Section 4.
- New section starting Section 6 with the mapping to existing enrollment protocols by collecting boundary conditions.

Authors' Addresses

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/

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

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