Workgroup: ANIMA WG
Internet-Draft: draft-ietf-anima-brski-async-enroll-04
Published: 8 January 2022
Intended Status: Standards Track
Expires: 12 July 2022

Authors:

S. Fries	H. Brockhaus	D. von Oheimb, Ed.	E. Lear
Siemens	*Siemens*	*Siemens*	*Cisco Systems*

Support of Asynchronous Enrollment in BRSKI (BRSKI-AE)

Abstract

This document makes bootstrapping a remote secure key infrastructure (BRSKI, [RFC8995]) flexible on the certificate enrollment protocol being used. BRSKI-AE allows employing protocols such as CMP, where the origin of certificate requests and responses can be authenticated independently of message transfer. Using self-contained (signature-wrapped) objects for requesting and returning domain-specific device certificates, the origin and authenticity of messages can be verified also in domains that have no (or just limited) online connectivity.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

BRSKI, as defined in [RFC8995], specifies a solution for secure automated zero-touch bootstrapping of devices (aka pledges) in an operational 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 defined in [RFC8366]. These vouchers are authenticated self-contained (signed) objects, which may be provided online (synchronously) or offline (asynchronously) via the domain registrar to the pledge and originate from a Manufacturer Authorized Signing Authority (MASA).

For enrolling devices with LDevID certificates, which are end-entity (EE) certificates that are specific to the target domain, BRSKI typically relies on EST [RFC7030]. In this setting the pledge is the client, interacting via TLS with the domain registrar, which acts both as EST server and as registration authority (RA). The TLS connection is mutually authenticated, where the pledge uses an initial device certificate (aka IDevID certificate) issued by its manufacturer. In order to provide proof of origin of the certificate request, i.e., proof of identity of the requester, EST specifically relies on binding the certification request to the underlying TLS connection. The EST server uses the authenticated pledge identity for checking the authorization of the pledge for the given request before issuing to the pledge a domain-specific certificate (LDevID certificate). This approach requires online or on-site availability of an inventory (or asset management system) for performing the authorization decision based on the certification request and its authentication via the IDevID certificate. 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 can be called *synchronous enrollment*.

For certain use cases, the required RA/CA components and/or asset management may not be available on-site but rather be provided by backend systems, to which site may have no online connection or just intermittent connectivity. This may be due to security requirements for operating the backend systems or due to site deployments where on-site or always-online operation may be not feasible or too costly. The authorization of certification request based on an asset management in this case will not or can not be performed on-site at enrollment time. In this document, enrollment that is not performed in a (time-wise) consistent way is called *asynchronous enrollment* (AE).

Asynchronous enrollment requires a store-and-forward transfer of certification requests along with the information needed for authenticating the requester. This enables off-line processing 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 registrar/RA can authorize the certification request. When a second communication channel is opened to forward the certification request to the RA and issuing CA, the requester authentication information needs to be retained and ideally bound directly to the certification request. This use case is independent of the time-wise limitations of the first use case.

There are several options for performing store-and-forward transfer of certification requests including the requester authentication information:

- Providing a trusted component (e.g., a local RA) 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 preventing changes to the combined information. Note that the assumption is that the information elements may not be bound cryptographically. 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 when performing the authorization and issuing the requested certificate. In BRSKI the trusted component may be the EST server, co-located with the registrar in the target domain.
- Utilizing authenticated self-contained objects for the enrollment, directly binding the certification request and the requester authentication in a cryptographic way. This approach reduces the necessary trust in a domain component for storage and delivery. Unauthorized modification of the requester information (request and authentication) can be detected during the verification of the authenticated self-contained object.

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

The goal is to enhance BRSKI for being applicable to additional use cases. This is addressed by

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

BRSKI-AE can be applied for both synchronous and asynchronous enrollment.

Note that in contrast to BRSKI, BRSKI-AE allows support of multiple enrollment protocols on the infrastructure side, enabling the pledge developer to select one that is most appropriate for the pledge.

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.

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 time-wise interrupted communication between a pledge (end entity) and a registrar or PKI component.

synchronous communication: Describes a time-wise uninterrupted communication between a pledge (end entity) and a registrar or PKI component.

authenticated self-contained object: Describes in this context an object that is cryptographically bound to an 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 private key corresponding to 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 like the following.

- There is no registration authority available in the target domain. Connectivity to an off-site RA is intermittent or entirely offline. A store-and-forward mechanism is used for communicating with the off-site services.
- Authoritative actions of a local RA are limited and may not be sufficient for authorizing certification requests by pledges. Final authorization is done by an 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 protocol approaches in general and asynchronous enrollment specifically. They introduce industrial application scenarios where leveraging BRSKI as-is would be problematic because they need support of asynchronous operation or protocols other than EST, as supported by 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, with track-side equipment, and/or possibly with backend systems. These devices are typically unaware of backend system connectivity. Managing certificates may be done during maintenance cycles of the railroad car, but can already be prepared during operation. Preparation will include generating certification requests, which are collected and later 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.

UNISIG has included a CMP profile for enrollment of TLS certificates of on-board and track-side components in the Subset-137 specifying the ETRAM/ETCS on-line key management for train control systems [UNISIG-Subset-137].

3.2.2. Building automation

In the building automation scenarios, a detached building or the basement of a building may be equipped with sensors, actuators, and controllers that are connected with 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 this case, connectivity to the domain registrar may also be facilitated by the service technician's laptop.

3.2.3. Substation automation

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

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 is deployed, and forbidden or prevented at other times.

3.2.6. Less operational security in the target domain

The registration authority performing the authorization of a certificate request is a critical PKI component and therefore implicates higher operational security than 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 situations where the target domain does not offer a sufficient level of security to operate a registration authority and therefore wants to transfer this service to a backend service that offers a higher security level.

4. Requirement discussion and mapping to solution elements

For the requirements discussion we assume that the domain registrar receiving a certification request as an authenticated object is not the (final) authorization point for this certification request. If the domain registrar is the only authorization point and the pledge has a direct connection to it, BRSKI can be used directly. Note that BRSKI-AE may still be needed in this case, for instance when the pledge prefers a protocol other than EST.

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

At least the following properties are required:

- 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 private key.
- Proof of identity: provides data origin authentication of a data object such as a certificate request. This typically is achieved by a signature using the private key associated with the IDevID certificate of the pledge, or, in case of certificate updates, with the certificate to be updated.

Here is an incomplete list of solution examples, based on existing technology described in IETF documents:

- Certification request objects: Certification requests are data structures protecting only the integrity of the contained data and providing proof of possession for a (locally generated) private key. Examples for certification request data structures are:
  - PKCS#10 [RFC2986]. The structure is self-signed to protect its integrity and prove possession of the private key that corresponds to the included public key of the requester.
  - CRMF [RFC4211]. Also this structure supports integrity protection and proof of possession, typically by a self-signature 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 support any signature algorithm.

  The integrity protection of certification request fields includes the public key because it is part of the data signed by the corresponding private key. Yet note that for the above examples this is not sufficient to provide data origin authentication, i.e., proof of identity. This extra property can be achieved by an additional binding to the IDevID of the pledge. This binding to source authentication supports the authorization decision for the certification request. The binding of data origin authentication to the certification request may be delegated to the protocol used for certificate management.

- Solution options of proof of identity: The certification request should be bound to an existing authenticated credential (here, IDevID) to enable a proof of identity and, based on it, an authorization of the certification request. The binding may be achieved through security options in an underlying transport protocol such as TLS if the authorization of the certification request is (completely) done at the next communication hop. This binding can also be done in a transport-independent way by wrapping the certification request with signature employing an existing credential. In the BRSKI context, this will be the IDevID initially, the LDevID for renewals. This requirement is addressed by existing enrollment protocols in various ways, such as:
  - EST [RFC7030] utilizes PKCS#10 to encode the certification request. The Certificate Signing Request (CSR) may contain a binding to the underlying TLS session by including the tls-unique value in the self-signed CSR structure. The tls-unique value results from the TLS handshake. Since the TLS handshake includes client authentication and the pledge utilizes 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. As an alternative to binding to the underlying authentication in the transport layer, [RFC7030] sketches wrapping the CSR with a Full PKI Request message using an existing certificate.
  - 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 credential in SCEP is referred to as renewal. Thus SCEP does not rely on the security of the underlying transfer.
  - CMP [RFC4210] 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 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 format. The proof of identity can be provided as part of a FullCMCRequest, based on CMS [RFC5652] and signed with an existing IDevID credential. Thus CMC does not rely on the security of the underlying transfer.

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

5. Architectural Overview and Communication Exchanges

To support asynchronous enrollment, BRSKI-AE enhances the system architecture defined in BRSKI [RFC8995] such that authenticated self-contained objects can be used for certificate enrollments. This is achieved by allowing the use of alternative enrollment protocols with their message wrapping mechanisms, such as those described in Section 4 above.

The enhancements needed are kept to a minimum in order to ensure 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 as usual.

5.1. Support of off-site PKI service

The key element 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 enables interaction with off-site or off-line PKI (RA/CA) components. In addition, the authorization of the certification request may be done not only by the domain registrar but by PKI components residing in the backend of the domain operator (off-site) as described in Section 3.1. Also, the certification request may be piggybacked on another protocol. This leads to generalizations in the placement and enhancements of the logical elements as shown in Figure 1.

```
                                           +------------------------+
   +--------------Drop-Ship--------------->| Vendor Service         |
   |                                       +------------------------+
   |                                       | M anufacturer|         |
   |                                       | A uthorized  |Ownership|
   |                                       | S igning     |Tracker  |
   |                                       | A uthority   |         |
   |                                       +--------------+---------+
   |                                                      ^
   |                                                      |
   V                                                      |
+--------+     .........................................  |
|        |     .                                       .  | BRSKI-
|        |     .  +------------+       +------------+  .  | MASA
| Pledge |     .  |   Join     |       | Domain     <-----+
|        |     .  |   Proxy    |       | Registrar/ |  .
|        <-------->............<-------> Enrollment |  .
|        |     .  |        BRSKI-AE    | Proxy      |  .
| IDevID |     .  |            |       +------^-----+  .
|        |     .  +------------+              |        .
|        |     .                              |        .
+--------+     ...............................|.........
                on-site "domain" components   |
                                              | e.g., RFC 7030,
                                              |       RFC 4210, ...
 .............................................|.....................
 . +---------------------------+     +--------v------------------+ .
 . | Public-Key Infrastructure <-----+ Registration Authority    | .
 . | PKI CA                    +-----> PKI RA                    | .
 . +---------------------------+     +---------------------------+ .
 ...................................................................
         off-site or central "domain" components
```

Figure 1: Architecture overview using off-site PKI components

The architecture overview in Figure 1 has the same logical elements as BRSKI, but some or them are placed differently. The main difference is the placement of the PKI RA/CA component, which performs the authorization decision for certification request messages. It is placed in the off-site or central domain of the operator, to which the deployment or on-site domain of the pledge may have no or only temporary (intermittent) connectivity. 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 deployment target domain of the pledge.

- Join Proxy: same functionality as described in BRSKI [RFC8995].
- Domain Registrar / Enrollment Proxy: in BRSKI-AE, the domain registrar has mostly the same functionality as in BRSKI, namely to facilitate the communication of the pledge with the MASA and the PKI. Regarding the enrollment of the pledge to the deployment domain, there is a difference in the authorization of certification requests. BRSKI-AE allows to perform this in the operator's backend (off-site), and not just directly at the domain registrar.
- Voucher exchange: the voucher exchange with the MASA via the domain registrar is performed as described in BRSKI.

- Certificate 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 is done off-site, the domain registrar forwards the certification request to the RA to perform the authorization there. Note that this requires that the certification request object includes a proof of origin such that the authorization to be based on the included pledge identity information. 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 situation that it has only intermittent connection 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) and generalizing 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 BRSKI [RFC8995]. Note that the interaction with the MASA may be synchronous (voucher request with nonce) or asynchronous (voucher request without nonce).
- Ownership tracker: as defined in BRSKI.

The following list describes the operator-related components/service operated in the off-site backend of the domain.

- PKI RA: Performs certificate management functions (validation of requests, interaction with inventory/asset management for final 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 with the RA directly.
- PKI CA: Performs certificate generation by signing the certificate structure provided in already authenticated and authorized certification requests.

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 follows.

- Discovery phase: same as in BRSKI [RFC8995] steps (1) and (2)
- Voucher exchange with deployment domain registrar: same as in BRSKI steps (3) and (4).
- Enrollment phase: step (5) is 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 suitable 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 not only proof of possession but also proof of identity (source authentication).

```
+--------+                        +------------+     +------------+
| Pledge |                        | Domain     |     | Operator   |
|        |                        | Registrar  |     | RA/CA      |
|        |                        |  (JRC)     |     | (OPKI)     |
+--------+                        +------------+     +------------+
  /-->                                      |                    |
[Recommended Request of CA Certificates]    |                    |
  |---------- CA Certs Request ------------>|                    |
  |              [if connection to operator domain is available] |
  |                                         |-Request CA Certs ->|
  |                                         |<-CA Certs Response-|
  |<-------- CA Certs Response--------------|                    |
  /-->                                      |                    |
[Recommended Request of Certificate Attributes to be included]   |
  |---------- Attribute Request ----------->|                    |
  |              [if connection to operator domain is available] |
  |                                         |-Attribute Request->|
  |                                         |<- Attrib Response -|
  |<--------- Attribute Response -----------|                    |
  /-->                                      |                    |
[Certification request]                     |                    |
  |-------------- Cert Request ------------>|                    |
  |            [when connection to off-site domain is available] |
  |                                         |--- Cert Request -->|
[Optional Certificate Waiting indication]   |                    |
  /-->                                      |                    |
  |<----- Cert Waiting Response ------------|                    |
  |                                         |                    |
  |-- Cert Polling (with orig request ID) ->|                    |
  |                                         |                    |
  /-->                                      |                    |
  |                                         |<-- Cert Response --|
  |<-- Cert Response (with Certificate) ----|                    |
  /-->                                      |                    |
[Certificate confirmation]                  |                    |
  |-------------- Cert Confirm ------------>|                    |
  |                                        /-->                  |
  |                                         |[optional]          |
  |                                         |--- Cert Confirm -->|
  |                                         |<-- PKI Confirm ----|
  |<------------- PKI/Registrar Confirm ----|                    |
```

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 latest relevant 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 the 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 subsequent certification request.
- Cert Request: 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: The certification response message contains the requested certificate and potentially further information, like certificates of intermediary CAs on the certification path.
- Cert Waiting: Optional waiting indication for the pledge, which should retry after a given time. For this a request identifier is necessary. This request identifier may be either part of the enrollment protocol or can derived from the certification request.
- Cert Polling: This is used to query the registrar whether the certification request meanwhile has been processed; can be answered either by another Cert Waiting, or a Cert Response.
- Cert Confirm: positive or negative confirmation message by the pledge after receiving and verifying the certificate.
- PKI/Registrar Confirm: An acknowledgment by the PKI or domain registrar on reception of the Cert Confirm.

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

5.1.5. Addressing Scheme Enhancements

BRSKI-AE provides generalizations to the addressing scheme defined in BRSKI [RFC8995] to accommodate the handling of authenticated self-contained objects for certification requests. As this is supported by various 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 enrollment: "/.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 URIs) at the registrar may need to be defined by the utilized enrollment protocol.
- <request>: depending on the utilized enrollment protocol, the <request> path component describes the required operation at the registrar side. Enrollment protocols are expected to define their request endpoints, as done by existing protocols (see also Section 6).

5.2. Domain registrar support of specific enrollment options

Well-known URIs for various 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 whether its preferred enrollment option is supported by the domain registrar by sending a request to its preferred enrollment endpoint and evaluating the HTTP response status code.

The following figure provides an illustrative example for 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 [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/fullcmc>;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/getcacerts>;ct=pkixcmp
  </cmp/getcertreqtemplate>;ct=pkixcmp
```

TBD RFC Editor: please delete /*

Open Issues:

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

6. Examples for signature-wrapping using existing enrollment protocols

This section maps the requirements to support proof of possession and proof of identity to selected existing enrollment protocols. Note 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 of the underlying TLS connection using OSCORE, which results in using authenticated self-contained objects.

6.1. EST Handling

When using EST [RFC7030], the following aspects and 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 would contain 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 performed 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 necessary. */
- When the RA is temporarily not available, as per [RFC7030] section 4.2.3, an HTTP status code 202 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 taken down for the waiting time, the PKCS#10 request needs 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 full-featured CMP to the functionality needed here. When using this variant of CMP, the following requirements should be observed:

- For proof of possession, the approach defined in the 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 applied.
- Proof of identity should be provided by using signature-based protection of 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 the Lightweight CMP Profile [I-D.ietf-lamps-lightweight-cmp-profile] apply as far as CMP is used.

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-16, 22 December 2021, <https://www.ietf.org/archive/id/draft-ietf-lamps-cmp-updates-16.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., Oheimb, D. V., and S. Fries, "Lightweight Certificate Management Protocol (CMP) Profile", Work in Progress, Internet-Draft, draft-ietf-lamps-lightweight-cmp-profile-09, 17 December 2021, <https://www.ietf.org/archive/id/draft-ietf-lamps-lightweight-cmp-profile-09.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>.

[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. History of changes TBD RFC Editor: please delete

From IETF draft 04 -> IETF draft 05:

- David von Oheimb became the editor.
- Streamlined wording and improved grammar throughout the text.

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.

LocalWords: bcp uc prot vexchange enrollfigure req eo selander coap LocalWords: oscore fullcmc simpleenroll tls env brski UC seriesinfo LocalWords: Attrib lt docname ipr toc anima async wg symrefs ann LocalWords: sortrefs iprnotified

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 (EDITOR)
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