Abstract

This document discusses an enhancement of automated bootstrapping of a remote secure key infrastructure (BRSKI) to operate in domains featuring no or only timely limited connectivity to backend services offering enrollment functionality, specifically a Public Key Infrastructure (PKI). In the context of deploying new devices the design of BRSKI allows for online (synchronous object exchange) and offline interactions (asynchronous object exchange) with a manufacturer’s authorization service. For this it utilizes a self-contained voucher to transport the domain credentials as a signed object to establish an initial trust between the pledge and the deployment domain. The currently supported enrollment protocol for request and distribution of deployment domain specific device certificates provides only limited support for asynchronous PKI interactions. This memo motivates the enhancement of supporting self-contained objects for certificate management by using an abstract notation. This allows off-site operation of PKI services outside the deployment domain of the pledge. This addresses specifically scenarios, in which the final authorization of certification request of a pledge cannot be made in the deployment domain and is therefore delegated to a operator backend. The goal is to enable the usage of existing and potentially new PKI protocols supporting self-containment for certificate management.

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."
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 January 9, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ........................................... 3
2. History of changes ..................................... 5
3. Terminology ............................................. 6
4. Scope of solution ....................................... 6
4.1. Supported environment ............................... 6
4.2. Application Examples ................................. 7
4.2.1. Rolling stock .................................... 7
4.2.2. Building automation ............................... 7
4.2.3. Substation automation ............................ 8
4.2.4. Electric vehicle charging infrastructure ......... 8
4.2.5. Infrastructure isolation policy ................. 8
4.2.6. Less operational security in the deployment domain 9
4.3. Requirement discussion and mapping to solution elements 9
5. Architectural Overview ................................. 11
5.1. Behavior of a pledge ................................. 14
5.2. Secure Imprinting using Vouchers .................... 14
5.3. Addressing ........................................... 15
6. Protocol Flows .......................................... 15
6.1. Pledge - Registrar discovery and voucher exchange .... 15
6.2. Registrar - MASA voucher exchange .................. 16
6.3. Pledge - Registrar - RA/CA certificate enrollment .... 17
7. Mapping to existing enrollment protocols ................ 19
7.1. EST Handling ........................................ 19
7.2. CMP Handling ........................................ 20
8. IANA Considerations .................................... 20
9. Privacy Considerations ................................. 20
1. Introduction

BRSKI as defined in [I-D.ietf-anima-bootstrapping-keyinfra] specifies a solution for secure zero-touch (automated) bootstrapping of devices (pledges) in a target deployment domain. This includes the discovery of network elements in the deployment domain, time synchronization, and the exchange of security information necessary to establish trust between a pledge and the domain and to adopt a pledge as new network and application element. Security information about the deployment domain, specifically the deployment domain certificate (domain root certificate), is exchanged utilizing vouchers as defined in [RFC8366]. These vouchers are self-contained objects, which may be provided online (synchronous) or offline (asynchronous) via the domain registrar to the pledge and originate from a manufacturer’s authorization service (MASA). The manufacturer signed voucher contains the target domain certificate and can be verified by the pledge due to the possession of a manufacturer root certificate. It facilitates the enrollment of the pledge in the deployment domain and is used to establish trust.

For the enrollment of devices BRSKI relies on EST [RFC7030] to request and distribute deployment 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 an LDevID certificate) and to provide data origin authentication to support the authorization decision for processing the certification request. The TLS connection is mutually authenticated and the client side authentication bases on the pledge’s manufacturer issued device certificate (IDevID certificate). This approach requires an on-site availability of the RA as PKI component and/or a local asset or inventory management system performing the authorization decision based on the certification request to issue a domain specific certificate to the pledge. This is due to the EST server terminating the security association with the pledge and thus the binding between the certification request and the authentication of the pledge. 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 operators 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. 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 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. If a second communication channel is opened to forward the certification request to the issuing CA, the requester authentication information needs to be bound to the certification request. 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 deployment domain, which stores the certification request combined with the requester authentication information (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 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 deployment domain.

- Utilization of self-contained objects 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 requestor information (request and authentication) can be detected during
the verification of the cryptographic binding of the self-contained object in the off-site PKI.

This document targets environments, in which connectivity to the PKI functionality is only temporary or not directly available by specifying support for handling self-contained objects supporting asynchronous enrollment. 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 a X.509 root certificate sufficient for verifying the domain registrar / proxy identity as well as an domain specific X.509 device certificate (LDevID certificate).

The goal is to enhance BRSKI to either allow other existing certificate management protocols supporting self-contained objects to be applied or to allow other types of encoding for the certificate management information exchange.

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. History of changes

From version 00 -> 01:

- Update of examples, specifically for building automation as well as two new application use cases in Section 4.2.
- 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 4.3.
- New section starting Section 7 with the mapping to existing enrollment protocols by collecting boundary conditions.
3. 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 [RFC2119].

This document relies on the terminology defined in [I-D.ietf-anima-bootstrapping-keyinfra]. 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 side, to which only a temporarily 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.

4. Scope of solution

4.1. 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 deployment domain. The connectivity to the backend RA may only be temporarily available. A local store and forward device is used for the communication with the backend 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 backend operator 
domain.

- the target deployment domain already uses a certificate management 
  approach that shall be reused to be consistent throughout the 
lifecycle.

4.2. 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.

4.2.1. Rolling stock

Rolling stock or railroad cars contain a variety of sensors, 
actuators, and controller, 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 operators asset/inventory information.

4.2.2. 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.
4.2.3. Substation automation

In substation automation a control center typically hosts PKI services to issue certificates for Intelligent Electronic Devices (IED)s 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 [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 [I-D.gutmann-scep] and EST [RFC7030] for the infrastructure side, while the IED must only support one of the two.

4.2.4. 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 authenticates an X.509 certificate to authenticate 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. Self-containment will ease this by allowing the transport without a separate communication protocol. For the purpose of certificate management CMP [RFC4210] is intended to be used.

4.2.5. 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.
4.2.6. Less operational security in the deployment 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 deployment domain does not offer enough security to operate a registration point and therefore wants to transfer this service to a backend.

4.3. Requirement discussion and mapping to solution elements

For the requirements discussion it is assumed that the entity receiving the self-contained object in the deployment domain is not the authorization point for the certification request contained in the object. If the entity is the authorization point, BRSKI can be used directly. Note that BRSKI-AE could address both cases.

Based on the supported deployment environment described in Section 4.1 and the motivated application examples described in Section 4.2 the following base requirements are derived to support self-contained objects as container carrying the certification request and further information to support asynchronous operation. Moreover, potential solution examples (not complete) based on existing technology are provided with the focus on existing IETF standards track documents:

- Certification requests are structures protecting at least integrity of the contained data combined with a proof-of-private-key-possession for locally generated key pairs. Examples for certification requests
  - PKCS#10 [RFC2986]: Defines a structure for a certification request. The structure must be signed to ensure integrity protection and proof-of-private-key-possession. Hence, the signature is performed by using the private key of the requestor (corresponding to the contained public key).
  - CRMF [RFC4211]: Defines a structure for the certification request. The structure also typically contains an integrity protection and a proof of possession, in which a signature value is generated by using the corresponding private key to the contained public key. This self-signature can also be replaced by the RA after verification, if the RA intends to update or alter the request message.
Note that the integrity is bound to the public key contained in the certification request. In the considered application examples, this is not sufficient and needs to be bound to the data origin authentication (IDevID). This binding also supports the authorization decision for the certification request. The binding of data origin authentication to the certification request is delegated to the management protocol.

- The container carrying the certification request should support a binding to an existing credential known to the peer performing the authorization of the certification request as proof of identity. The binding may be transport dependent if the endpoint at the next communication hop is authorizing the certification request. 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) contains 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.

  * SCEP [I-D.gutmann-scep]: 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 ([RFC5652]). Note that the wrapping using an existing IDevID credential is not specified directly in SCEP.

  * 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 calculate a signature over the header and the body of the PKIMessage utilizing the protectionAlg signaled in the PKIMessage header and the PKIProtection carrying the actual signature value.

  * 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 would be used, which allows signing with an existing IDevID credential to provide a proof of identity.
The container carrying the certification request should support transport independent protection using an existing credential of the pledge verifiable at the authorization point of the certification request (typically the RA in conjunction with an inventory). This requirement is addressed by existing enrollment protocols in different ways, for instance:

* EST [RFC7030]: Not supported.
* SCEP [I-D.gutmann-scep]: Not specified in SCEP, could be done using message wrapping with signature (based on CMS).
* CMP [RFC4210]: Message wrapping with signature.
* CMC [RFC5272]: Message wrapping with signature.

5. Architectural Overview

To support asynchronous enrollment, the base system architecture defined in BRSKI [I-D.ietf-anima-bootstrapping-keyinfra] is changed to allow for off-site operation of the PKI components. The assumption for BRSKI-AE is that the authorization for a certification request is performed using an inventory or asset management system residing in the backend of the domain operator as described in Section 4.1. This leads to changes in the placement or enhancements of the logical elements as shown in Figure 1.
Figure 1: Architecture overview of BRSKI-AE

The architecture overview in Figure 1 utilizes the same logical elements as BRSKI but with a different placement in the architecture for some of the elements. The main difference is the placement of the PKI RA/CA component, which is actually performing the authorization decision for the certification request message. Also shown is the connectivity of the RA/CA with an inventory management system, which is expected to be utilized in the authorization process.
decision. Note that this may also be an integrated functionality of
the RA. Both components are 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 domain of the pledge.
This is to underline the authorization decision for the certification
request in the backend rather than in the deployment domain itself.
The following list describes the components in the deployment domain:

- **Join Proxy:** same functionality as described in BRSKI

- **Domain Registrar / 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 operators backend (off-site), even if the deployment domain
  has only temporary or no connectivity to an operator domain.
  
  - **Voucher exchange:** The voucher exchange with the MASA via the
domain registrar is performed as described in BRSKI

  [I-D.ietf-anima-bootstrapping-keyinfra].

  - **Certificate enrollment:** For the pledge enrollment the domain
    registrar in the deployment domain support the authorization of
    the pledge to be part of the domain, but not necessarily to
    authorize the certification request provided during enrollment.
    This may be due to lack of authorization information in the
    deployment domain. If the authorization is done in the
    operator domain, the domain registrar is used to forward the
    certification request to the RA. Thus it basically works as a
    proxy. In the case of no connectivity, the domain registrar
    stores the certification request and forwards it to the RA upon
    connectivity. As this requires the certification request to be
    self-contained, the domain registrar needs functionality
    enhancements with respect to the support of alternative
    enrollment approaches supporting self-containment. To support
    alternative enrollment approaches (protocols, encodings), it is
    necessary to enhance the addressing scheme at the domain
    registrar. The communication channel between the pledge and
    the domain registrar may be similarly described as in BRSKI
    within the same "/.well-known" tree and may result in "/.well-
    known/enrollment-variant/request".

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

- **MASA:** general functionality as described in BRSKI. Assumption
  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 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 operator.

- PKI CA: Performs certificate generation by signing the certificate structure provided in the certification request.

- Inventory (asset) management: contains information about the known devices belonging to the operator. Specifically, the inventory is used to provide the information to authorize issuing a certificate based on the certification request of the pledge. Note: the communication between the inventory (asset) management and the PKI components (RA/CA) are out of scope of this document.

- (Domain) registrar: Optional component if the deployment domain does not feature a domain registrar but only a proxy. In this case it is involved in the certification request processing and is assumed to be co-located with the PKI RA.

5.1. Behavior of a pledge

The behavior of a pledge as described in [I-D.ietf-anima-bootstrapping-keyinfra] is kept with one exception. After finishing the imprinting phase (4) the enrollment phase (5) is performed with a method supporting self-contained objects. Using simpleenroll with EST as taken in BRSKI cannot be applied here, as it binds the pledge authentication with the existing IDevID using the transport channel. This authentication is not visible/verifiable at the authorization point in the off-site domain. /* mapping to existing protocols based on the outcome of the discussion */

5.2. Secure Imprinting using Vouchers

The described approach in [I-D.ietf-anima-bootstrapping-keyinfra] is kept as is.
5.3. Addressing

For the provisioning of different enrollment options at the domain registrar, the addressing approach of BRSKI using a "/.well-known" tree from [RFC5785] is enhanced.

/* to be done: Description of "/.well-known/enrollment-protocol/request" in which enrollment-protocol may be an already existing protocol like "est" or "scep" or "cmp" or "cms" or a newly defined protocol. */

6. Protocol Flows

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 accompany the application of self-contained objects for the enrollment).

6.1. Pledge - Registrar discovery and voucher exchange

The discovery phase is applied as specified in [I-D.ietf-anima-bootstrapping-keyinfra]. /* for discussion: is a reference to BRSKI sufficient here or is it helpful to provide additional information and the figure? */
**Figure 2:** Pledge discovery of domain registrar discovery and voucher exchange

### 6.2. Registrar - MASA voucher exchange

The voucher exchange is performed as specified in [I-D.ietf-anima-bootstrapping-keyinfra]. /* for discussion: is a reference to BRSKI sufficient here or is it helpful to provide additional information and the figure? */
6.3. Pledge - Registrar - RA/CA certificate enrollment

The enrollment for BRSKI-AE will be performed using a self-contained object. According to the abstract requirements from [I-D.ietf-anima-bootstrapping-keyinfra]. This object shall at least contain the following information:

- Proof of Possession: utilizing the private key corresponding to the public key contained in the certification request.
- Proof of Identity: utilizing the existing IDevID credential to generate a signature of the certification request.
- /* further parameter to be specified */.

Figure 3: Domain registrar - MASA voucher exchange
Figure 4: Certificate enrollment

The following list provides an abstract description of the flow depicted in Figure 4.

- **CA Cert Request**: The pledge SHOULD request the full distribution of CA Certificates message. This ensures that the pledge has the complete set of current CA certificates beyond the pinned-domain-cert.
o Attribute Request: Typically, the automated bootstrapping occurs without local administrative configuration of the pledge. Nevertheless, there are cases, in which the pledge should 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.

o Cert Request: certification request message (to be done: reference to PKCS#10 or CRMF, proof of possession, pledge authentication)

o Cert Response: certification response message containing the requested certificate and potentially further information like certificates of intermediary CAs on the certification path.

o 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.

o Cert Poling: querying the registrar, if the certificate request was already processed; can be answered either with another Cert Waiting, or a Cert Response.

o Cert Confirm: confirmation message from pledge after receiving and verifying the certificate.

o PKI/Registrar Confirm: confirmation message from PKI/registrar about reception of the pledge’s certificate confirmation.

/* to be done: - investigation into handling of certificate request retries - message exchange description - confirmation message (necessary? optional? from Registrar and/or PKI?) */

7. Mapping to existing enrollment protocols

This sections maps the requirements and the approach described in Section 6.3 to already existing enrollment protocols.

7.1. EST Handling

When using the EST protocol [RFC7030], the following constrains should be observed:

o Proof of possession is provided by using the specified PKCS #10 structure in the request method.

o For proof of identity only the /fullcmc endpoint should be used with a fullcmc request. This contains sufficient information for
the RA/CA to make an authorization decision on the received certification request. Note that 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: in this case the binding to the underlying TLS connection may not be necessary */

- When the CA/CA is not available, as per [RFC7030] Section 4.2.3, a 202 return code should be returned by the Join Registrar. The pledge in this case would retry with the same PKCS#10 request as in the initial simpleentroll run. Note that if the TLS connection is teared down for the waiting time, the PKCS#10 request would need to be rebuild as it contains the unique identifier (tls_unique) from the underlying TLS connection for the binding.

7.2. CMP Handling

When using the CMP protocol [RFC4210], the following constrains should be observed:

- For proof of possession, the defined approach in CMP [RFC4210] section 4.3 should be supported. This can be achieved by using either CRMF or PKCS#10 to specify the certification request.

- Proof of identity can be provided by using the MSG_SIG_ALG to protect the certificate request message with signatures as outlined in section D.5.

- When the CA/CA is not available, as per [RFC4210] Section 5.2.3, a waiting indication should be returned in the PKIStatus by the Join Registrar. The pledge in this case would retry using the PollReqContent with a request identifier certReqId provided in the initial CertRequest message as specified in section 5.3.22.

8. IANA Considerations

This document requires the following IANA actions:

/* to be done: clarification necessary */

9. Privacy Considerations

/* to be done: clarification necessary */
10. Security Considerations

/* to be done: clarification necessary */

11. Acknowledgements

We would like to thank the various reviewers for their input, in particular Brian E. Carpenter, Giorgio Romanenghi, Oskar Camenzind for their input and discussion on use cases and call flows.

12. References

12.1. Normative References

[I-D.ietf-anima-bootstrapping-keyinfra]


12.2. Informative References


[ISO-IEC-15118-2]

[NERC-CIP-005-5]

[OCPP]
Open Charge Alliance, "Open Charge Point Protocol 2.0", April 2018.


Authors’ Addresses
Steffen Fries  
Siemens AG  
Otto-Hahn-Ring 6  
Munich, Bavaria  81739  
Germany  
Email: steffen.fries@siemens.com  
URI:  http://www.siemens.com/

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

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