REEP Policy

REEP Policy

The REEP Policy will be determined by 2 key documents: the REEP Key Management Practice Statement and the REEP Metadata Registration Practice Statement. Draft of these can be found below.

REEP Key Management Practice Statement

Abstract

The REEP service is a public registry of SAML metadata which offers a domain validation (DV) trust model for registered SAML metadata. Technical trust in SAML metadata downloaded from the registry relies on XML digtal signatures. This document describes the key management practice for the the private keys used to create those signatures.

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 http://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 April 21, 2014.

Copyright Notice Copyright (c) 2013 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 (http://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.

1. Introduction and Scope

This document describes the Key Management Practice Statement (KMPS) for the REEP Metadata Signing Key (MSK).

2. Applicability

This KMPS applies only to the REEP MSK - the key that is used to sign SAML metadata that result from queries to the REEP metadata endpoint, including the full aggregate of domain validated SAML metadata registered in the REEP service. This is denoted "REEP metadata" below. The trust inferred from validating the REEP MSK signature does not extend to any 3rd party metadata aggregate which may include metadata derived from or dependent on REEP metadata.

3. Roles and Responsibilities

3.1. REFEDS

The REFEDS community is the ultimate authority over the REEP Service. The REEP Steering Group will make decisions reflecting the consensus of the REFEDS community by appointing the roles and executing the processes described below.

3.2. REEP Policy Management Authority

The REEP Policy Management Authority (REEP PMA) is a function appointed by the REFEDS Steering Group in accordance with and reflecting REFEDS consensus. The REEP PMA owns this specification and is responsible for policy and process oversight. The REEP PMA main duty is to oversee the REEP MSK Generation Ceremony and to ensure that the REEP Service Operator and REEP Crypto Officers perform their duties as set down in this and other specifications.

3.3. REEP Service Operator

The REEP Service Operator is the organization tasked by the REFEDS Steering Group to operate the technical infrastructure of the REEP Service including servers, physical facilities and operations of key containers (HSMs) and other technical and procedural controls.

3.4. REEP Crypto Officer

The REEP Crypto Officers is a a group of at least 5 and no more than 7 individuals chosen from the REFEDS community tasked with each carrying a key which, when at least 3 of the Crypto Officers are present can be used to (re)generate the REEP MSK.

4. Changes to this Specification

Changes to this specification is subject to REFEDS consensus. The REEP PMA reserves the right to amend the REEP KMPS without notification for changes that are not material. Such changes may include correcting spelling and other language errors that do not materially impact the KMPS.

5. Publication and Repositories

The public part of the REEP MSK and the REEP Metadata Registration Practice Statement [MRPS] is published on the REEP website: http://refeds.org/reep . The public part of the REEP MSK is published in the form of a self-signed X.509 certificate along with a SHA1 and SHA256 fingerprint of that certificate. In addition the REEP MSK may be published in the following ways:

- in a TLSA record of md.reep.refeds.org.

- as a PKCS#10 certificate signing request

The REEP PMA invites any Certification Authority to indicate trust in the REEP MSK by signing the MSK certificate signing request and publishing the resulting X.509 certificate in its own repository. Relying parties may choose to include the TLSA record and/or any signed versions of the MSK in the validation process for the MSK.

6. Metadata Processing

6.1. Metadata Registration

Registration of REEP metadata is covered by the REEP Metadata Registration Practice Statement [MRPS] which should be considered a normative part of this document.

6.2. Metadata Format

REEP metadata will be annotated with a rpi:RegistrationInfo element containing a reference to the REEP Metadata Registration Practice Statement [MRPS]. The following is a non-normative example:

```
<mdrpi:RegistrationInfo
       registrationAuthority="http://refeds.org/reep"
       registrationInstant="2016-11-29T13:39:41Z">
   <mdrpi:RegistrationPolicy xml:lang="en">
      http://refeds.org/reep/mrps
   </mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

The REEP Metadata Registration Practice Statement may be provided in multiple languages for convenience but the English language version is the only normative version.

6.3. Metadata Validation

An accurate assesment of trust in, and use of REEP metadata requires explicit validation of the XML-dsig signature done using the REEP MSK. Validation of the signature involves the following steps:

1. Identify the XML Signature element in REEP Metadata. If this step fails the metadata is not signed and MUST NOT be trusted.
2. Identify the X509Data element corresponding to the published REEP metadata public key. If this step fails the metadata is not properly signed and MUST NOT be trusted.
3. Process the XML Signature element according to [REC-xmldsig-core-20020212] to confirm that the private key used to sign the REEP metadata corresponds to the identified REEP metadata public key.

Step (2) can be accomplished by comparing certificate fingerprints. Unless this process yields a positive result, the metadata MUST NOT be trusted. Several tools exist that accurately perform this validation given the REEP metadata public key and URL as input.

7. Operational Requirements

7.1. System Description

The REEP system consists of two parts: a web application where users can login, perform domain validation to claim ownership of domains and register SAML metadata for endpoints associated with domains they are able to validate. The second part is an endpoint implementing [I-D.draft-young-md-query-00] which returns parts of, or all of the available REEP metadata signed with the REEP metadata private key.

7.2. Facilities and Physical Controls

The REEP Operator will host all servers and related equipment in secure hosting facilities protected by at least 3 layers of physical security (locked doors, cages, locked racks etc) where at least the inner layer is only accessible to the REEP Operator or the duly appointed representative of the REEP Operator. The hosting facilities will be equipped with redundant power, cooling and will have fire-detection and fire-suppression equipment. The facilities will be operated according to industry best practice and monitored 24x7. Access to the hosting facility will be restricted to authorized personnel and will be subjected to regular inspections to ensure their proper operations.

7.3. Technical Controls

The REEP Operator will implement and maintain logical access control to all components of the REEP service to ensure that access to resources (SAML metadata and domains) in the REEP service is restricted to authorized users only. The access restrictions will be implemented in such a way as to ensure the integrity of the domain-validation assurance defined in the REEP Metadata Registration Practice Statement [MRPS]. The REEP Operator will implement and maintain logical access controls to the cryptographic equipment used to store the private REEP MSK to ensure that only the REEP Crypto Officers are able to access it and then only when at least 3 are present.

The REEP Operator will implement and maintain an Audit log of all events related to the REEP MSK including:

- key generation, backup, recovery and destruction
- key container (HSM) activation and de-activation
- all successful or unsuccessful signing operations

In addition, the REEP Service Operator will maintain an audit log related to the REEP Service including:

- registration and modification of users
- successful and unsuccessful domain validation event
- any operation performed by trusted system operators
- inner physical security layer access

7.4. Procedural Controls

7.4.1. REEP MSK Generation

TBD - in part this depends on the HSM solution.

7.4.2. Crypto Officer Selection and Identification

Crypto Officers will be selected by the REEP PMA and the REFEDS Steering Group to represent the REFEDS community at large. The individuals selected will be persons of good standing in the community and have a proven reliable professional track record. Before credentialing the Crypto Officers they will be asked to provide a government issued identity document (a passport or similar document) attesting to their identity.

7.4.3. Crypto Officer Credentialing

TBD - also depends on the HSM solution

7.4.4. Incident Response

TODO

7.4.5. MSK Rollover

The REEP PMA may decide to perform a MSK rollover process in order to generate new private key material, respond to an incident or to introduce a new signature mechanism. In either case the following process must be followed:

1. Notify the REFEDS community and all registered users no later than 3 months before a planned MSK rollover and no later than 72 hours before an emergency MSK rollover.
2. Assemble at least 3 REEP Crypto Officers and perform the REEP MSK Generation process. For planned MSK rollover this should if at all possible take place in proximity to a REFEDS meeting. For emergency MSK rollover any available time and location can be used.
3. Generate the new MSK self-signed X.509 certificate and associated fingerprints.
4. Sign the new MSK with the old MSK if the old MSK key is still available and deemed trustworthy.
5. Publish the new MSK self-signed X.509 and related artifacts on https://refeds.org/reep.
6. Notify any known signers of the MSK and invite them to re-sign the new MSK and publish the result.

8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997. [MRPS] Harris, N., "REEP Metadata Registration Practice Statement", 2013. [I-D.young-md-query] Young, I., "Metadata Query Protocol", draft-young-md-query-00 (work in progress), August 2013. [W3C.REC-xmldsig-core-20020212]Solo, D., Eastlake, D., and J. Reagle, "XML-Signature Syntax and Processing", World Wide Web Consortium FirstEdition REC-xmldsig-core-20020212, February 2002, <http://www.w3.org/TR/2002/REC-xmldsig-core-20020212>.

REEP Metadata Registration Practice Statement

Abstract

The REEP service is a public registry of SAML metadata which offers a domain validation (DV) trust model for registered SAML metadata. This document specifies the metadata registration practices used by the REEP service in its role as metadata registrar. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

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 http://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 [DATE].

Copyright Notice

Copyright (c) 2013 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 (http://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.

1. Introduction and Applicability

This document describes the Metadata Registration Practice Statement [MRPS] for REEP with effect from the publication date of this document. All new entity registrations performed on or after that date SHALL be processed as described here until this document is superseded by a later edition. The MRPS SHALL be published on the REFEDS website at the following url: http://refeds.org/reep along with archived copies of earlier documents.

2. Metadata Format

Metadata for all entities registered by REEP SHALL make use of the [SAML-Metadata-RPI-V1.0] metadata extension to indicate that the REEP MRPS applies to the entities. The following is a non-normative example:

```
<mdrpi:RegistrationInfo
       registrationAuthority="http://refeds.org/reep"
       registrationInstant="2016-11-29T13:39:41Z">
   <mdrpi:RegistrationPolicy xml:lang="en">
      http://refeds.org/reep/mrps
   </mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

If a metadata relying party requires assurance of an entity's compliance with a documented MRPS, a request MAY be made via the REEP Operator for the registrar to perform a MRPS re-evaluation for the entity. Such a re-evaluation MAY be performed when an entity's metadata is changed by the entity's registrant or when a new MRPS edition is published. The expected result of an PRPS re-evaluation is to verify the entity's registration against the then-current MRPS, witgh the metadata published for the entity being updated to reflect this.

3. Eligibility and Validation

Any organisation can register a SAML Service Provider entity with REEP. REEP SHALL NOT guarantee that this metadata will subsequently be retrieved and published by any metadata relying party.

In order to register an entity, an organisation MUST prove that they own the domain for the entity they wish to register. REEP SHALL carry out domain validation in one of the following ways:

- HTTP validation: with this option the organisation is asked to create a resource in the root of the HTTP service for the domain with a specific string given by the REEP verification service. REEP will then send an HTTP GET request to http://<the new domain>/<the verification string>. If a 200 OK response code is received, REEP considers the domain (and marks it as) verified.
- DNS validation: with this option the organisation is asked to create a DNS TXT record in the domain with a specific string given by the REEP verification service. Once created, REEP checks that such record exists and only if it exits is the domain marked as verified.

Values of the entityID attribute for entities registered with REEP MUST be an absolute URI using the https scheme. The DNS domain used in the URI MUST match the domain validated by REEP.

Validation by REEP only proves that the organisation has some form of ownership for a given domain. No other guarantees about the accuracy or provenance of entity metadata are given.

4. Entity Management

Once a domain has been validated, any number of entities MAY be added by the organisation. Each entity consists of a name, an associated domain, and the XML that describe its metadata. The name is a non empty string that SHALL NOT contain the following characters: !, \, :, & or |. The metadata MUST be valid XML. REEP asks for the following information to be added per entity:

- Entity ID
- Endpoints
- Contact information
- Organization information
- Certificates

All of these fields MUST be completed, leaving one of them empty will trigger a validation error and a prompt to fill in the missing value.

5. Key Management

Key Management for the REEP service is covered by the REEP Key Management Practice Statement which should be considered a normative part of this document.

6. Metadata Retrieval and Publication

TO DO: agree any limitations on federations permitted to fetch metadata from REEP.

7. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[KMPS] Johansson, L., "REEP Key Management Practice Statement", 2013.

[I-D.young-md-query] Young, I., "Metadata Query Protocol", draft-young-md-query-00 (work in progress), August 2013.

[SAML-Metadata-RPI-V1.0] SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0. 03 April 2012. OASIS Committee Specification 01. http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html.