XEP-0416: E2E Authentication in XMPP

Evgeny Khramtsov
mailto:ekhramtsov@process-one.net
xmpp:xram@zinid.ru

2019-03-06
Version 0.1.0

Status	Type	Short Name
Deferred	Standards Track	NOT_YET_ASSIGNED

This specification describes how X.509 certificates can be used for end-to-end authentication in XMPP.

Legal

Copyright

Permissions

Warranty

Liability

Conformance

This XMPP Extension Protocol has been contributed in full conformance with the XSF’s Intellectual Property Rights Policy (a copy of which can be found at <https://xmpp.org/about/xsf/ipr-policy> or obtained by writing to XMPP Standards Foundation, P.O. Box 787, Parker, CO 80134 USA).

Contents

1 Introduction

X.509 version 3 certificates can be used to provide a strong cryptographic identity of an XMPP entity, i.e. an association of an XMPP address (RFC 7622 [1]) with its cryptographic key (formally defined under Section 13.7.1.4 of RFC 6120 [2]). They were initially intended for the use in SASL EXTERNAL for c2s and mutual s2s authentication (see Best Practices for Use of SASL EXTERNAL (XEP-0178) [3]). This document extends their usage for end-to-end (e2e) authentication of any entities attached to the XMPP network. A separate document also defines how Certificate Signing Request (CSR) of an XMPP account can be issued and signed using the XMPP protocol (XEP-EAX-SIGN).
Example usages:

E2E encryption For end-to-end encryption, XMPP clients may use certificates to mutually identify each other, i.e. check that the cryptographic key belongs to this exact XMPP address.

External services An XMPP server may authenticate users of other servers at its local services, such as an HTTP Upload component (HTTP File Upload (XEP-0363) XEP-0363: HTTP File Upload <https://xmpp.org/extensions/xep-0363.html>.), e.g. for granting file uploads, or a TURN server (RFC 5766 RFC 5766: Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN) <http://tools.ietf.org/html/rfc5766>.).

XMPP Usage of RELOAD XMPP entities attached to the XOR overlay (XEP-0415) are supposed to use certificates for mutual authentication.

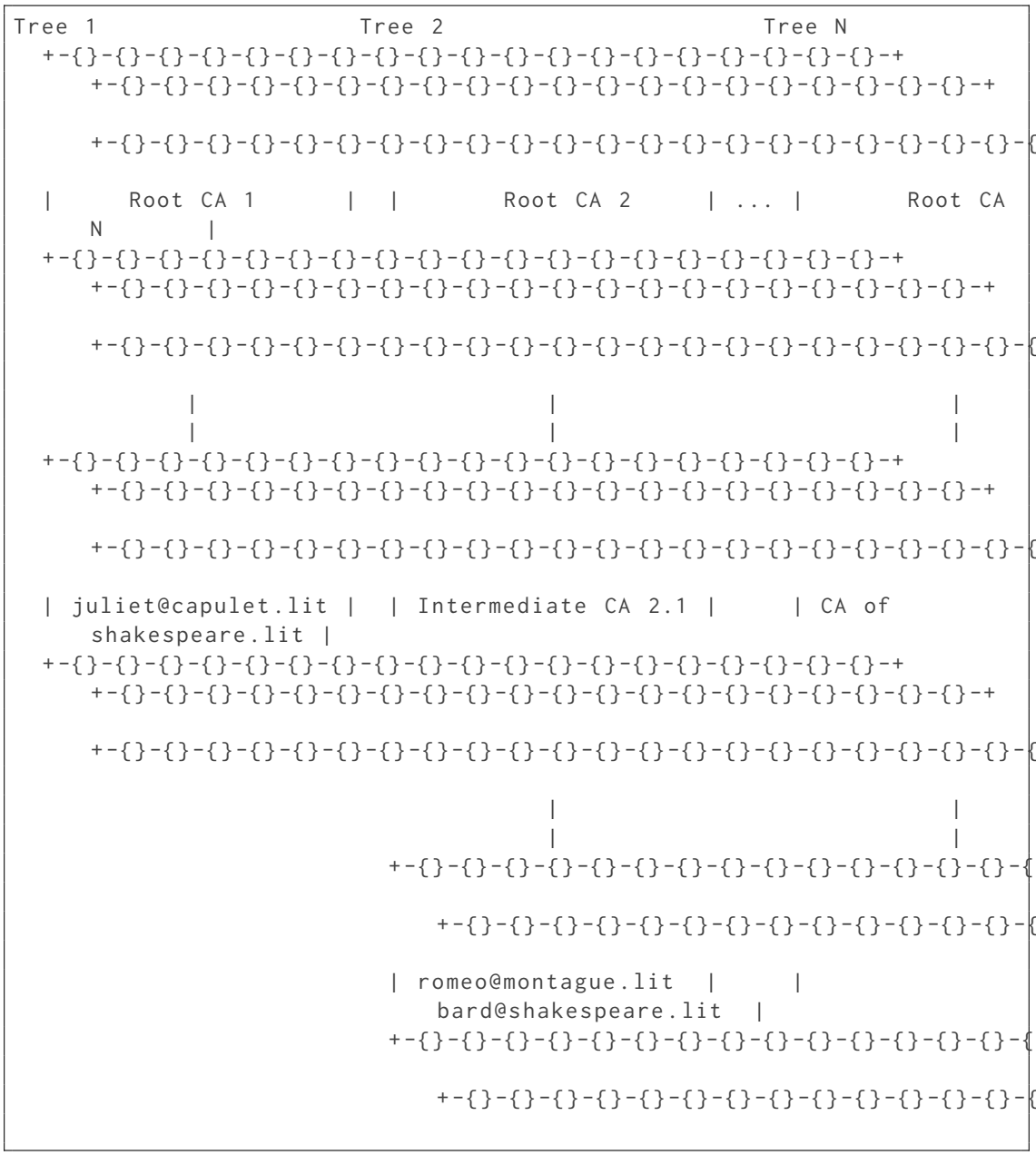
SPAM protection Since certificate authorities are required to be Sybil resistant (XEP-EAX-CAR), a spammer is limited in ability to create accounts massively. Thus it is expected that SPAM dissemination will fall to negligible levels.

Registration delegation XMPP accounts registration typically creates a huge burden for operators of public servers. An operator may want to delegate a registration of accounts of its own server to a trusted CA. The CA will validate the users' identities and will issue certificates for them. The users can use these certificates in c2s SASL EXTERNAL authentication at the operator's server as well as for e2e authentication with other entities.

Note that an XMPP client may use the same certificate for different kinds of e2e authentication.
Conceptually, the idea is to build PKIX trees where in each tree a node corresponds to a certificate of a CA signing certificates of its successors. A leaf in the tree represents a certificate assigned to an XMPP account, a "leaf certificate". The leaf certificates are supposed to be used

[1] RFC 7622: Extensible Messaging and Presence Protocol (XMPP): Address Format <http://tools.ietf.org/html/rfc7622>.
[2] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[3] XEP-0178: Best Practices for Use of SASL EXTERNAL <https://xmpp.org/extensions/xep-0178.html>.

for (but not limited to) e2e authentication.



In the example above, XMPP servers of domains ”capulet.lit” and ”montague.lit” do not have associated certificate authorities, so Root CA 1 and Intermediate CA 2.1 sign certificates of ”juliet@capulet.lit” and ”romeo@montague.lit” directly. An XMPP server of domain ”shakespeare.lit” has an associated CA (whose certificate is signed by Root CA N) and thus is able to sign certificates for users of ”shakespeare.lit” (and only for them). As long as all root CAs are trusted by all parties, ”juliet@capulet.lit”, ”romeo@montague.lit” and

”bard@shakespeare.lit” may mutually authenticate each other using their certificates (for sharing resources, exchanging messages, etc).

2 Glossary

CA Certificate authority - an entity that issues X.509 certificates.

CSR Certificate signing request - a message sent from an applicant to a certificate authority in order to apply for an X.509 certificate.

Leaf certificate A certificate assigned to an XMPP account.

Domain-associated certificate An intermediate certificate assigned for a particular XMPP domain. Such certificates can be used to sign leaf certificates associated with the same XMPP domain only.

Intermediate certificate A non-root certificate used for signing any other certificates.

Root certificate A self-signed certificate used for signing any other certificates.

3 Requirements

3.1 General Requirements

1. The leaf certificate MUST be compliant with c2s SASL EXTERNAL authentication (RFC 6120 [4], Best Practices for Use of SASL EXTERNAL (XEP-0178) [5]).
2. The leaf certificate MUST be compliant with RELOAD authentication (RFC 6940 [6]).

3.2 Certificate Requirements

The following rules apply to any certificate:

1. The certificate MUST conform to RFC 5280 [7].
2. The subject field MUST NOT be null.
3. The certificate MUST contain a keyUsage extension with the digitalSignature bit set.
4. The certificate SHOULD use Elliptic Curve Cryptography. FIXME: correctly define this statement.

[4] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[5] XEP-0178: Best Practices for Use of SASL EXTERNAL <https://xmpp.org/extensions/xep-0178.html>.
[6] RFC 6940: REsource LOcation And Discovery (RELOAD) Base Protocol <http://tools.ietf.org/html/rfc6940>.
[7] RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile <http://tools.ietf.org/html/rfc5280>.

The following rules apply to leaf certificates:

1. The certificate MUST NOT contain a basicConstraints extension with the cA boolean set to TRUE.
2. The certificate MUST include a CRL Distribution Points extension that specifies an URI of a Certificate Revocation List.
3. The certificate MUST possess a single XMPP address represented as an XmppAddr as specified under Section 13.7.1.4 of RFC 6120 [8].
4. The SubjectAltName field in the certificate MUST contain a single RELOAD URI as specified under Section 14.15 of RFC 6940 [9] encoded as uniformResourceIdentifier type. The "destination" part of the URI MUST be a RELOAD Node-ID. The Node-ID MAY be hexadecimal-encoded. The "overlay" part of the URI MUST be "xmpp.org". The "specifier" part of the URI MUST be empty.
5. If the XMPP address doesn't contain non-ASCII characters, it MUST be encoded in the SubjectAltName field as rfc822Name type.

Note that the rules for leaf certificates comply with the rules defined for client certificates under Sections 13.7.1.1 and 13.7.1.4 of RFC 6120 [10]. Thus they can be used for c2s SASL EXTERNAL authentication.
The requirement to possess a RELOAD URI and an rfc822Name address makes it possible to use the certificate for RELOAD authentication. Even if XOR extension (XEP-0415) is unused, the RELOAD URI uniquely identifies a user device: a user MAY have several certificates assigned to their XMPP address but with different RELOAD URIs.
The following rules apply to domain-associated certificates:

1. The certificate MUST contain a keyUsage extension with the keyCertSign bit set.
2. The certificate MUST contain a basicConstraints extension with the cA boolean set to TRUE and pathLenConstraint set to 0 (zero).
3. The certificate MUST include a CRL Distribution Points extension that specifies an URI of a Certificate Revocation List.
4. The certificate MUST possess the associated domain name encoded as DNS-ID identifier type. The domain name MUST NOT contain the wildcard character '*'.

The following rules apply to intermediate certificates, excluding domain-associated certificates:

[8] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[9] RFC 6940: REsource LOcation And Discovery (RELOAD) Base Protocol <http://tools.ietf.org/html/rfc6940>.
[10] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.

1. The certificate MUST contain a keyUsage extension with the keyCertSign bit set.
2. The certificate MUST contain a basicConstraints extension with the cA boolean set to TRUE.
3. The certificate MUST include a CRL Distribution Points extension that specifies an URI of a Certificate Revocation List.

The following rules apply to root certificates:

1. The certificate MUST contain a keyUsage extension with the keyCertSign bit set.
2. The certificate MUST contain a basicConstraints extension with the cA boolean set to TRUE.

3.3 CA Requirements

CA Requirements are outlined in XEP-EAX-CAR.

4 Certificate Validation

The certificate is considered valid if it follows the rules specified in Certificate Requirements and, in the case when it is signed by a domain-associated certificate, it is a leaf certificate and the domain from the domain-associated certificate matches the domain part of the XmppAddr of the certificate. Otherwise, the certificate MUST be considered invalid.
In the case of a certificate chain, the rules for certification path validation are applied (RFC 5280 [11]).

5 Root Certificates Discovery

An XMPP entity MAY maintain its own list of root certificates. However, in practice it's convenient to retrieve this list from a trusted source. For example, several organizations in the Internet maintain and provide such lists for certificates verification in the Web. This section specifies how the list of root certificates can be retrieved for the purpose of e2e authentication in XMPP.
Since the authentication is intended to be compliant with RELOAD and creating new document formats or DNS TXT records without exigency are in general discouraged, the Overlay Configuration document is reused to provide the list of root certificates (see Section 11.1

[11] RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile <http://tools.ietf.org/html/rfc5280>.

of RFC 6940 [12]). The root certificates are PEM-encoded (RFC 7468 [13]) with encapsulation boundaries removed and are included in <root-cert/> elements of the Overlay Configuration. In order to retrieve the Overlay Configuration, an HTTP GET request is performed to "https://xmpp.org/.well-known/reload-config". The requesting UA MUST be prepared to process HTTP redirects. In the case of a failure, the UA MAY repeat the request. In this case exponential backoff MUST be applied. Since the list of root certifcates is not a subject for frequent updates, under normal conditions, the UA SHOULD NOT request the Overlay Configuration more often than once per day. Usage of 'If-Modified-Since' is RECOMMENDED (RFC 7232 [14]).
Further versions of this specification MAY extend the Overlay Configuration with new XML elements.

6 Leaf Certificates Discovery

An XMPP entity MAY want to publish its certificate so other XMPP entities MAY retrieve it. The method to accomplish this depends on the usage:

- In the case of an ordinary XMPP usage (RFC 6120 [15]) a special PEP node (Personal Eventing Protocol (XEP-0163) [16]) is used as specified in XEP-EAX-SIGN.
- In the case of XMPP Usage of RELOAD (XEP-0415) a peer is REQUIRED to store its certificate in the RELOAD overlay (see Section 8 of RFC 6940 [17]).

7 Accessibility Considerations

None required.

8 Internationalization Considerations

None required.

[12] RFC 6940: REsource LOcation And Discovery (RELOAD) Base Protocol <http://tools.ietf.org/html/rfc6940>.
[13] RFC 7468: Textual Encodings of PKIX, PKCS, and CMS Structures <http://tools.ietf.org/html/rfc7468>.
[14] RFC 7232: Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests <http://tools.ietf.org/html/rfc7232>.
[15] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[16] XEP-0163: Personal Eventing Protocol <https://xmpp.org/extensions/xep-0163.html>.
[17] RFC 6940: REsource LOcation And Discovery (RELOAD) Base Protocol <http://tools.ietf.org/html/rfc6940>.

9 Security Considerations

TBD.

10 IANA Considerations

None required.

11 XMPP Registrar Considerations

None required.

12 XML Schema

None required.