Delegated Credentials for TLS
draft-ietf-tls-subcerts-05

Abstract

The organizational separation between the operator of a TLS endpoint and the certification authority can create limitations. For example, the lifetime of certificates, how they may be used, and the algorithms they support are ultimately determined by the certification authority. This document describes a mechanism by which operators may delegate their own credentials for use in TLS, without breaking compatibility with peers that do not support this specification.

Status of This Memo

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

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

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

This Internet-Draft will expire on May 6, 2020.

Copyright Notice

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

Typically, a TLS server uses a certificate provided by some entity other than the operator of the server (a "Certification Authority" or CA) [RFC8446] [RFC5280]. This organizational separation makes the TLS server operator dependent on the CA for some aspects of its operations, for example:

- Whenever the server operator wants to deploy a new certificate, it has to interact with the CA.
The server operator can only use TLS authentication schemes for which the CA will issue credentials.

These dependencies cause problems in practice. Server operators often want to create short-lived certificates for servers in low-trust zones such as Content Delivery Network (CDNs) or remote data centers. This allows server operators to limit the exposure of keys in cases that they do not realize a compromise has occurred. The risk inherent in cross-organizational transactions makes it operationally infeasible to rely on an external CA for such short-lived credentials. In Online Certificate Status Protocol (OCSP) stapling (i.e., using the Certificate Status extension types ocsp [RFC6066] or ocsp_multi [RFC6961]), if an operator chooses to talk frequently to the CA to obtain stapled responses, then failure to fetch an OCSP stapled response results only in degraded performance. On the other hand, failure to fetch a potentially large number of short lived certificates would result in the service not being available, which creates greater operational risk.

To remove these dependencies, this document proposes a limited delegation mechanism that allows a TLS peer to issue its own credentials within the scope of a certificate issued by an external CA. Because the above problems do not relate to the CA’s inherent function of validating possession of names, it is safe to make such delegations as long as they only enable the recipient of the delegation to speak for names that the CA has authorized. For clarity, we will refer to the certificate issued by the CA as a "certificate", or "delegation certificate", and the one issued by the operator as a "delegated credential" or "DC".

1.1. Change Log

(*) indicates changes to the wire protocol.

draft-05

- Removed support for PKCS 1.5 RSA signature algorithms.
- Additional security considerations.

draft-04

- Add support for client certificates.

draft-03

- Remove protocol version from the Credential structure. (*)
draft-02

- Change public key type. (*)
- Change DelegationUsage extension to be NULL and define its object identifier.
- Drop support for TLS 1.2.
- Add the protocol version and credential signature algorithm to the Credential structure. (*)
- Specify undefined behavior in a few cases: when the client receives a DC without indicated support; when the client indicates the extension in an invalid protocol version; and when DCs are sent as extensions to certificates other than the end-entity certificate.

2. Solution Overview

A delegated credential is a digitally signed data structure with two semantic fields: a validity interval and a public key (along with its associated signature algorithm). The signature on the credential indicates a delegation from the certificate that is issued to the peer. The secret key used to sign a credential corresponds to the public key of the peer’s X.509 end-entity certificate [RFC5280].

A TLS handshake that uses delegated credentials differs from a normal handshake in a few important ways:

- The initiating peer provides an extension in its ClientHello or CertificateRequest that indicates support for this mechanism.
- The peer sending the Certificate message provides both the certificate chain terminating in its certificate as well as the delegated credential.
- The authenticating initiator uses information from the peer’s certificate to verify the delegated credential and that the peer is asserting an expected identity.
- Peers accepting the delegated credential use it as the certificate’s working key for the TLS handshake.

As detailed in Section 3, the delegated credential is cryptographically bound to the end-entity certificate with which the credential may be used. This document specifies the use of delegated
Delegated credentials allow a peer to terminate TLS connections on behalf of the certificate owner. If a credential is stolen, there is no mechanism for revoking it without revoking the certificate itself. To limit exposure in case a delegated credential is compromised, peers may not issue credentials with a validity period longer than 7 days. This mechanism is described in detail in Section 3.1.

It was noted in [XPROT] that certificates in use by servers that support outdated protocols such as SSLv2 can be used to forge signatures for certificates that contain the keyEncipherment KeyUsage ([RFC5280] section 4.2.1.3). In order to prevent this type of cross-protocol attack, we define a new DelegationUsage extension to X.509 that permits use of delegated credentials. (See Section 3.2.)

2.1. Rationale

Delegated credentials present a better alternative than other delegation mechanisms like proxy certificates [RFC3820] for several reasons:

- There is no change needed to certificate validation at the PKI layer.
- X.509 semantics are very rich. This can cause unintended consequences if a service owner creates a proxy certificate where the properties differ from the leaf certificate. For this reason, delegated credentials have very restricted semantics that should not conflict with X.509 semantics.
- Proxy certificates rely on the certificate path building process to establish a binding between the proxy certificate and the server certificate. Since the certificate path building process is not cryptographically protected, it is possible that a proxy certificate could be bound to another certificate with the same public key, with different X.509 parameters. Delegated credentials, which rely on a cryptographic binding between the entire certificate and the delegated credential, cannot.
- Each delegated credential is bound to a specific signature algorithm that may be used to sign the TLS handshake ([RFC8446] section 4.2.3). This prevents them from being used with other, perhaps unintended signature algorithms.
2.2. Related Work

Many of the use cases for delegated credentials can also be addressed using purely server-side mechanisms that do not require changes to client behavior (e.g., a PKCS#11 interface or a remote signing mechanism [KEYLESS]). These mechanisms, however, incur per-transaction latency, since the front-end server has to interact with a back-end server that holds a private key. The mechanism proposed in this document allows the delegation to be done off-line, with no per-transaction latency. The figure below compares the message flows for these two mechanisms with TLS 1.3 [RFC8446].

Remote key signing:

Client            Front-End            Back-End
|----ClientHello--->|                    |
<----ServerHello----|
<----Certificate----|
<----CertVerify-----|
|<---remote sign---->|
|  ...  |

Delegated credentials:

Client            Front-End            Back-End
|----ClientHello--->|<--DC distribution->|
|<----ServerHello----|
<----Certificate----|
<----CertVerify-----|
|  ...  |

These two mechanisms can be complementary. A server could use credentials for clients that support them, while using [KEYLESS] to support legacy clients.

It is possible to address the short-lived certificate concerns above by automating certificate issuance, e.g., with Automated Certificate Management Environment (ACME) [RFC8555]. In addition to requiring frequent operationally-critical interactions with an external party, this makes the server operator dependent on the CA’s willingness to issue certificates with sufficiently short lifetimes. It also fails to address the issues with algorithm support. Nonetheless, existing automated issuance APIs like ACME may be useful for provisioning credentials within an operator network.
3. Delegated Credentials

While X.509 forbids end-entity certificates from being used as issuers for other certificates, it is perfectly fine to use them to issue other signed objects as long as the certificate contains the digitalSignature KeyUsage ([RFC5280] section 4.2.1.3). We define a new signed object format that would encode only the semantics that are needed for this application. The credential has the following structure:

```c
struct {
  uint32 valid_time;
  SignatureScheme expected_cert_verify_algorithm;
  opaque ASN1_subjectPublicKeyInfo<1..2^24-1>;
} Credential;
```

**valid_time:** Relative time in seconds from the beginning of the delegation certificate’s notBefore value after which the delegated credential is no longer valid.

**expected_cert_verify_algorithm:** The signature algorithm of the credential key pair, where the type SignatureScheme is as defined in [RFC8446]. This is expected to be the same as CertificateVerify.algorithm sent by the server. Only signature algorithms allowed for use in CertificateVerify messages are allowed. When using RSA, the public key MUST NOT use the rsaEncryption OID, as a result, the following algorithms are not allowed for use with delegated credentials: rsa_pss_rsae_sha256, rsa_pss_rsae_sha384, rsa_pss_rsa_sha512.

**ASN1_subjectPublicKeyInfo:** The credential’s public key, a DER-encoded [X690] SubjectPublicKeyInfo as defined in [RFC5280].

The delegated credential has the following structure:

```c
struct {
  Credential cred;
  SignatureScheme algorithm;
  opaque signature<0..2^16-1>;
} DelegatedCredential;
```

**algorithm:** The signature algorithm used to verify DelegatedCredential.signature.

**signature:** The delegation, a signature that binds the credential to the end-entity certificate’s public key as specified below. The signature scheme is specified by DelegatedCredential.algorithm.
The signature of the DelegatedCredential is computed over the concatenation of:

1. A string that consists of octet 32 (0x20) repeated 64 times.
2. The context string "TLS, server delegated credentials" for servers and "TLS, client delegated credentials" for clients.
3. A single 0 byte, which serves as the separator.
4. The DER-encoded X.509 end-entity certificate used to sign the DelegatedCredential.
5. DelegatedCredential.cred.
6. DelegatedCredential.algorithm.

The signature effectively binds the credential to the parameters of the handshake in which it is used. In particular, it ensures that credentials are only used with the certificate and signature algorithm chosen by the delegator. Minimizing their semantics in this way is intended to mitigate the risk of cross protocol attacks involving delegated credentials.

The code changes required in order to create and verify delegated credentials, and the implementation complexity this entails, are localized to the TLS stack. This has the advantage of avoiding changes to security-critical and often delicate PKI code.

3.1 Client and Server behavior

This document defines the following TLS extension code point.

```c
enum {
    ...
    delegatedCredential(TBD),
    (65535)
} ExtensionType;
```

3.1.1 Server authentication

A client which supports this specification SHALL send an empty "delegatedCredential" extension in its ClientHello. If the client receives a delegated credential without indicating support, then the client MUST abort with an "unexpected_message" alert.

If the extension is present, the server MAY send a delegated credential; if the extension is not present, the server MUST NOT send
a delegated credential. The server MUST ignore the extension unless
TLS 1.3 or a later version is negotiated.

The server MUST send the delegated credential as an extension in the
CertificateEntry of its end-entity certificate; the client SHOULD
ignore delegated credentials sent as extensions to any other
certificate.

The algorithm and expected_cert_verify_algorithm fields MUST be of a
type advertised by the client in the "signature_algorithms" extension
and are considered invalid otherwise. Clients that receive invalid
delegated credentials MUST terminate the connection with an
"illegal_parameter" alert.

3.1.2. Client authentication

A server which supports this specification SHALL send an empty
"delegated_credential" extension in the CertificateRequest message
when requesting client authentication. If the server receives a
delegated credential without indicating support in its
CertificateRequest, then the server MUST abort with an
"unexpected_message" alert.

If the extension is present, the client MAY send a delegated
credential; if the extension is not present, the client MUST NOT send
a delegated credential. The client MUST ignore the extension unless
TLS 1.3 or a later version is negotiated.

The client MUST send the delegated credential as an extension in the
CertificateEntry of its end-entity certificate; the server SHOULD
ignore delegated credentials sent as extensions to any other
certificate.

The algorithm and expected_cert_verify_algorithm fields MUST be of a
type advertised by the server in the "signature_algorithms" extension
and are considered invalid otherwise. Servers that receive invalid
delegated credentials MUST terminate the connection with an
"illegal_parameter" alert.

3.1.3. Validating a Delegated Credential

On receiving a delegated credential and a certificate chain, the peer
validates the certificate chain and matches the end-entity
certificate to the peer’s expected identity in the usual way. It
also takes the following steps:

1. Verify that the current time is within the validity interval of
   the credential and that the credential’s time to live is no more
than 7 days. This is done by asserting that the current time is no more than the delegation certificate’s notBefore value plus DelegatedCredential.cred.valid_time.

2. Verify that expected_cert_verify_algorithm matches the scheme indicated in the peer’s CertificateVerify message and that the algorithm is allowed for use with delegated credentials.

3. Verify that the end-entity certificate satisfies the conditions in Section 3.2.

4. Use the public key in the peer’s end-entity certificate to verify the signature of the credential using the algorithm indicated by DelegatedCredential.algorithm.

If one or more of these checks fail, then the delegated credential is deemed invalid. Clients and servers that receive invalid delegated credentials MUST terminate the connection with an "illegal parameter" alert. If successful, the participant receiving the Certificate message uses the public key in the credential to verify the signature in the peer’s CertificateVerify message.

3.2. Certificate Requirements

We define a new X.509 extension, DelegationUsage, to be used in the certificate when the certificate permits the usage of delegated credentials. What follows is the ASN.1 \[X680\] for the DelegationUsage certificate extension.

```
ext-delegationUsage EXTENSION ::= {
  SYNTAX DelegationUsage IDENTIFIED BY id-ce-delegationUsage
}
```

DelegationUsage ::= NULL

```
id-ce-delegationUsage OBJECT IDENTIFIER ::= ( 1 3 6 1 4 1 44363 44 )
```

The extension MUST be marked non-critical. (See Section 4.2 of [RFC5280].) The client MUST NOT accept a delegated credential unless the server’s end-entity certificate satisfies the following criteria:

- It has the DelegationUsage extension.
- It has the digitalSignature KeyUsage (see the KeyUsage extension defined in [RFC5280]).
4. IANA Considerations

This document registers the "delegated_credentials" extension in the "TLS ExtensionType Values" registry. The "delegated_credentials" extension has been assigned a code point of TBD. The IANA registry lists this extension as "Recommended" (i.e., "Y") and indicates that it may appear in the ClientHello (CH), CertificateRequest (CR), or Certificate (CT) messages in TLS 1.3 [RFC8446].

This document also defines an ASN.1 module for the DelegationUsage certificate extension in Appendix A. IANA is requested to register an Object Identifier (OID) for the ASN.1 in "SMI Security for PKIX Module Identifier" arc. An OID for the DelegationUsage certificate extension is not needed as it is already assigned to the extension from Cloudflare’s IANA Private Enterprise Number (PEN) arc.

5. Security Considerations

5.1. Security of delegated private key

Delegated credentials limit the exposure of the TLS private key by limiting its validity. An attacker who compromises the private key of a delegated credential can act as a man-in-the-middle until the delegate credential expires, however they cannot create new delegated credentials. Thus, delegated credentials should not be used to send a delegation to an untrusted party, but is meant to be used between parties that have some trust relationship with each other. The secrecy of the delegated private key is thus important and several access control mechanisms SHOULD be used to protect it, including file system controls, physical security, or hardware security modules.

5.2. Re-use of delegated credentials in multiple contexts

It is possible to use the same delegated credential for both client and server authentication if the Certificate allows it. This is safe because the context string used for delegated credentials is distinct in both contexts.

5.3. Revocation of delegated credentials

Delegated credentials do not provide any additional form of early revocation. Since it is short lived, the expiry of the delegated credential would revoke the credential. Revocation of the long term private key that signs the delegated credential also implicitly revokes the delegated credential.
5.4. Interactions with session resumption

If a client decides to cache the certificate chain an re-validate it when resuming a connection, the client SHOULD also cache the associated delegated credential and re-validate it.

5.5. Privacy considerations

Delegated credentials can be valid for 7 days and it is much easier for a service to create delegated credential than a certificate signed by a CA. A service could determine the client time and clock skew by creating several delegated credentials with different expiry timestamps and observing whether the client would accept it. Client time could be unique and thus privacy sensitive clients, such as browsers in incognito mode, who do not trust the service might not want to advertise support for delegated credentials or limit the number of probes that a server can perform.

6. Acknowledgements

Thanks to David Benjamin, Christopher Patton, Kyle Nekritz, Anirudh Ramachandran, Benjamin Kaduk, Kazuho Oku, Daniel Kahn Gillmor, Watson Ladd for their discussions, ideas, and bugs they have found.

7. References

7.1. Normative References


7.2. Informative References


Appendix A. ASN.1 Module

The following ASN.1 module provides the complete definition of the DelegationUsage certificate extension. The ASN.1 module makes imports from [RFC5912].

DelegatedCredentialExtn { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) modules(0) id-mod-delegate-credential-extn(TBD) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

- EXPORT ALL

IMPORTS

EXTENSION FROM PKIX-CommonTypes-2009 - From RFC 5912 { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-pkixCommon-02(57) } ;

- OIDS

id-cloudflare OBJECT IDENTIFIER ::= { 1 3 6 1 4 1 44363 }

- EXTENSION

ext-delegationUsage EXTENSION ::= { SYNTAX DelegationUsage IDENTIFIED BY id-ce-delegationUsage }

id-ce-delegationUsage OBJECT IDENTIFIER ::= { id-cloudflare 44 }

DelegationUsage ::= NULL

END

Authors’ Addresses

Richard Barnes
Cisco
Email: rlb@ipv.sx

Subodh Iyengar
Facebook
Email: subodh@fb.com

Nick Sullivan
Cloudflare
Email: nick@cloudflare.com