Nick Sullivan

IETF 97 TLS WG

Friday, November 18, 2016

Delegated Credentials

New Draft, Old Idea

Delegated Credentials for TLS

draft-rescorla-tls-subcerts-00

E. Rescorla, Mozilla

R. Barnes, Mozilla

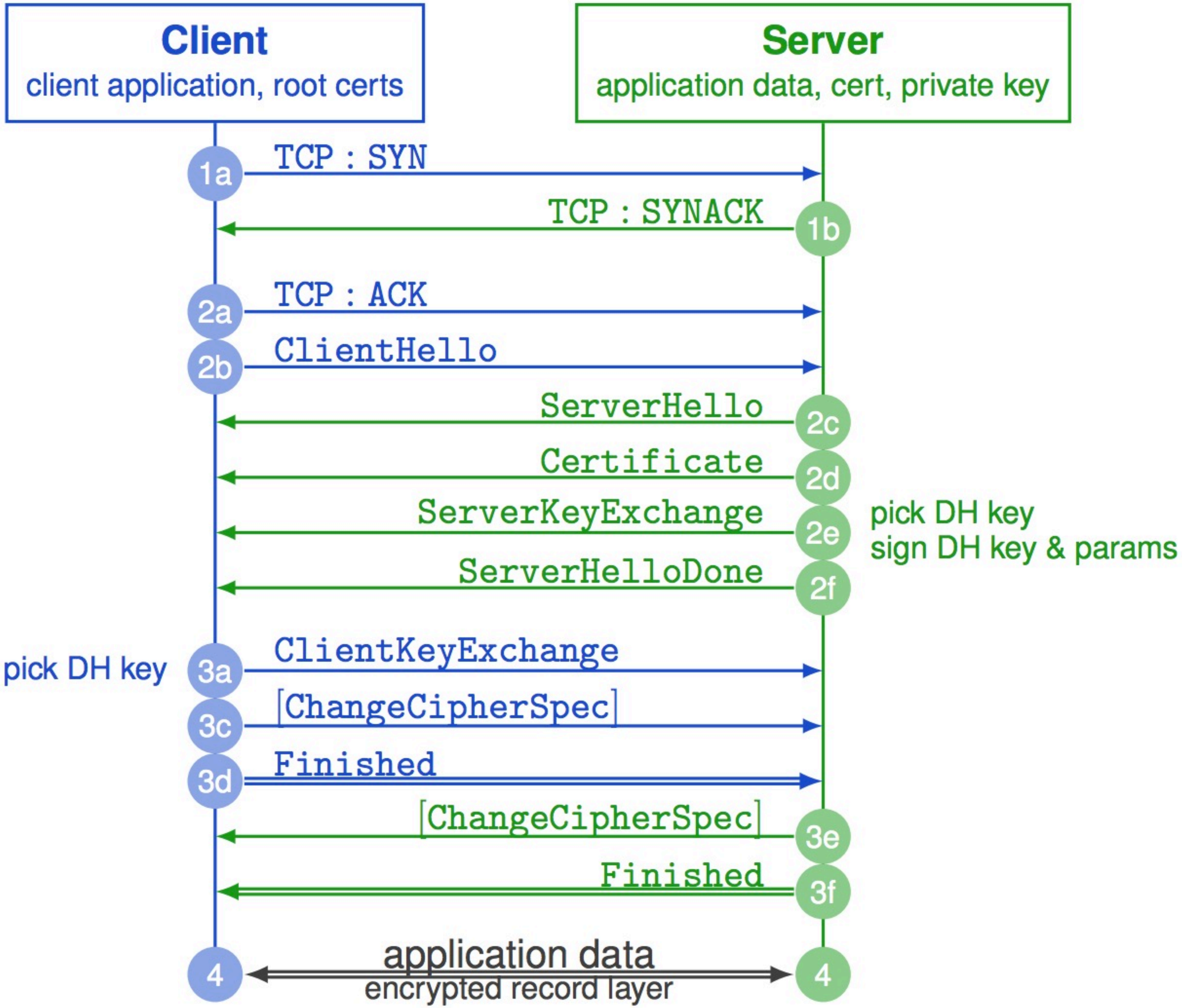
S. Iyengar, Facebook

N. Sullivan, Cloudflare

Motivation

- Internet-facing applications have long term keys in memory

- Reduce the exposure of certificate private keys without compromising performance



Client
client application, root certs

Server
application data, cert, private key

1a TCP : SYN

1b TCP : SYNACK

2a TCP : ACK

2b ClientHello

2c ServerHello

2d Certificate

2e ServerKeyExchange

pick DH key
sign DH key & params

2f ServerHelloDone

pick DH key

3a ClientKeyExchange

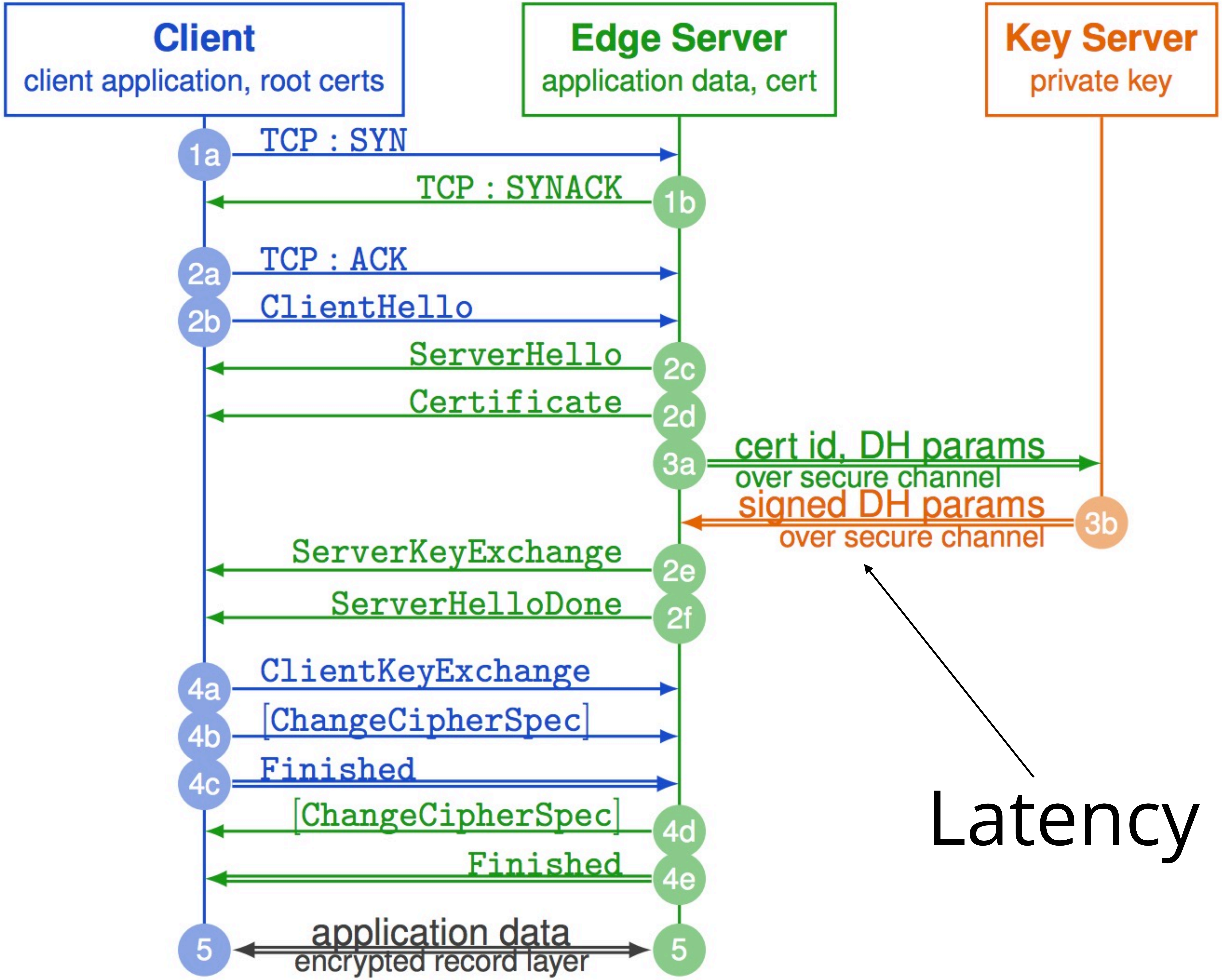
3c [ChangeCipherSpec]

3d Finished

3e [ChangeCipherSpec]

3f Finished

4 application data 4
encrypted record layer


Client
client application, root certs
Edge Server
application data, cert
Key Server
private key
1a
TCP : SYN
TCP : SYNACK
1b
2a
TCP : ACK
2b
ClientHello
ServerHello
2c
Certificate
2d
3a
cert id, DH params
over secure channel
signed DH params
over secure channel
3b
ServerKeyExchange
2e
ServerHelloDone
2f
4a
ClientKeyExchange
4b
[ChangeCipherSpec]
4c
Finished
[ChangeCipherSpec]
4d
Finished
4e
5
application data
encrypted record layer
5

Latency

1
2
4
5
Origin server
Key server
Client
Edge server
3

Delegated credentials

- Time-bounded key swap
- Optional extension advertised by the client
- Server replies with an extension containing a “Delegated Credential”
  - Public key
  - Validity Period (currently max 7 days == max session ticket validity)
  - Additional constraints (maybe)
  - Signed by delegator’s private key
- CertificateVerify uses key from Delegated Credential instead of Certificate

Validating credentials

- Certificate constraints still apply
- Revocation and certificate transparency apply to delegator
- Credential signature validated against delegator public key

Benefits

- Signing key for TLS connection has short validity period (7 days)
- Centralized control of private key (can use HSM)
- Can split edge operations from key management

Implementation options

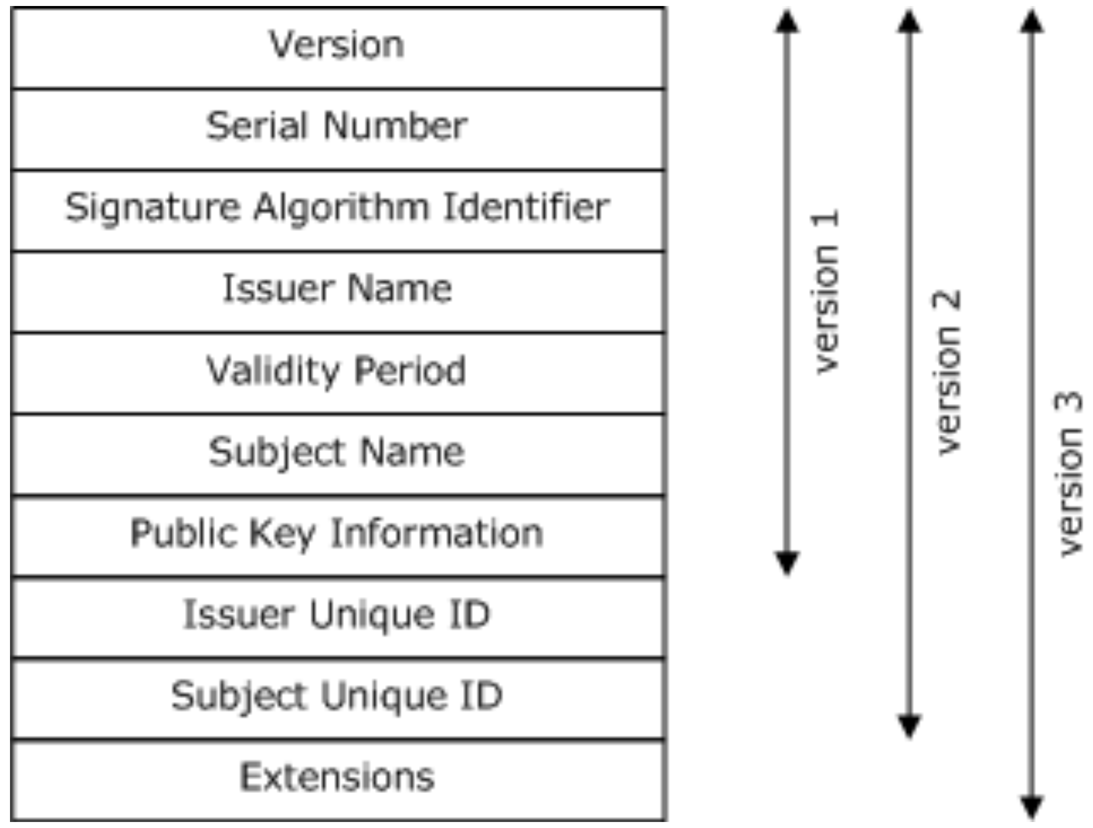
1. Constrained sub-CAs

   - Requires changes to CA business practices
   - Constrained sub-CA may be larger than standard EE cert
   - Requires clients support for critical name constraints
   - More degrees of freedom when validating chain

Implementation options

2. X.509 signed by EE certificate

   - Violates traditional PKI semantics (CA bit)
   - Less risk of unexpected consequences of PKI logic
   - RFC 3820 Proxy Certificates?
   - X.509 is overkill
   - Can be part of certificate chain, or in extension



Version
Serial Number
Signature Algorithm Identifier
Issuer Name
Validity Period
Subject Name
Public Key Information
Issuer Unique ID
Subject Unique ID
Extensions

Implementation options

3.Custom structure

- Smaller message
- New parsing code
- No reuse of PKIX code for validation
- Like a certificate but not: feature creep
- Additional constraints adds complexity (server name)

```
digitally-signed struct {
   uint64 notBefore;
   uint64 notAfter;
   SignatureScheme algorithm;
   ServerName serverName;
   opaque publicKey<0..2^24-1>
 } DelegatedCredential;
```

Security Considerations

- Allows more secure storage of delegator private key
- Allows use of new signatures unavailable in CAs (ed25519, etc.)

- Compromising a delegator private key becomes more dangerous
- Single signature means one delegated credential
  - Seven days (max lifetime) of active compromise + resumption

CLOUDFLARE®

IETF®

Nick Sullivan

IETF 97 TLS WG

Friday, November 18, 2016

Delegated Credentials