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
Latency
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
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)

```c
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
Delegated Credentials