IETF®

Nick Sullivan
IETF 104 TLS WG
March 26, 2019

Delegated Credentials

Delegated Credentials for TLS

Adopted draft, relatively stable

draft-rescorla-tls-subcerts-03

E. Rescorla, Mozilla

R. Barnes, Cisco

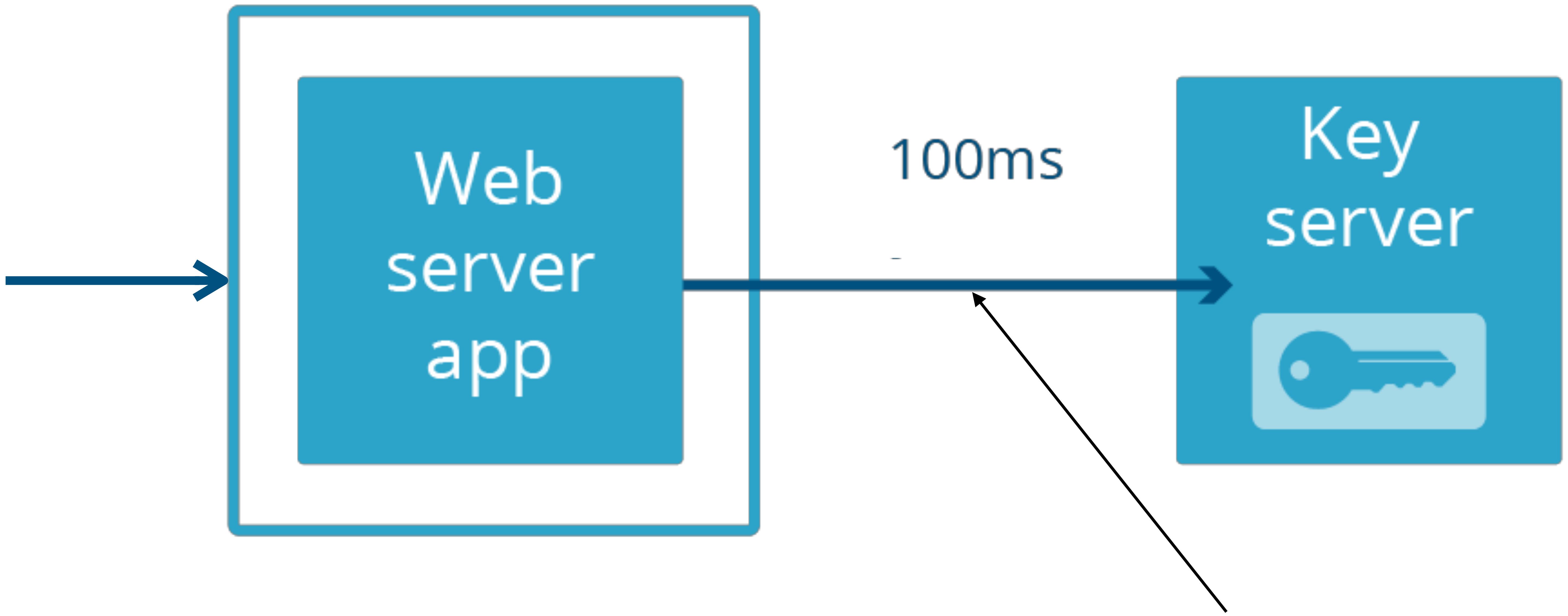
S. Iyengar, Facebook

N. Sullivan, Cloudflare

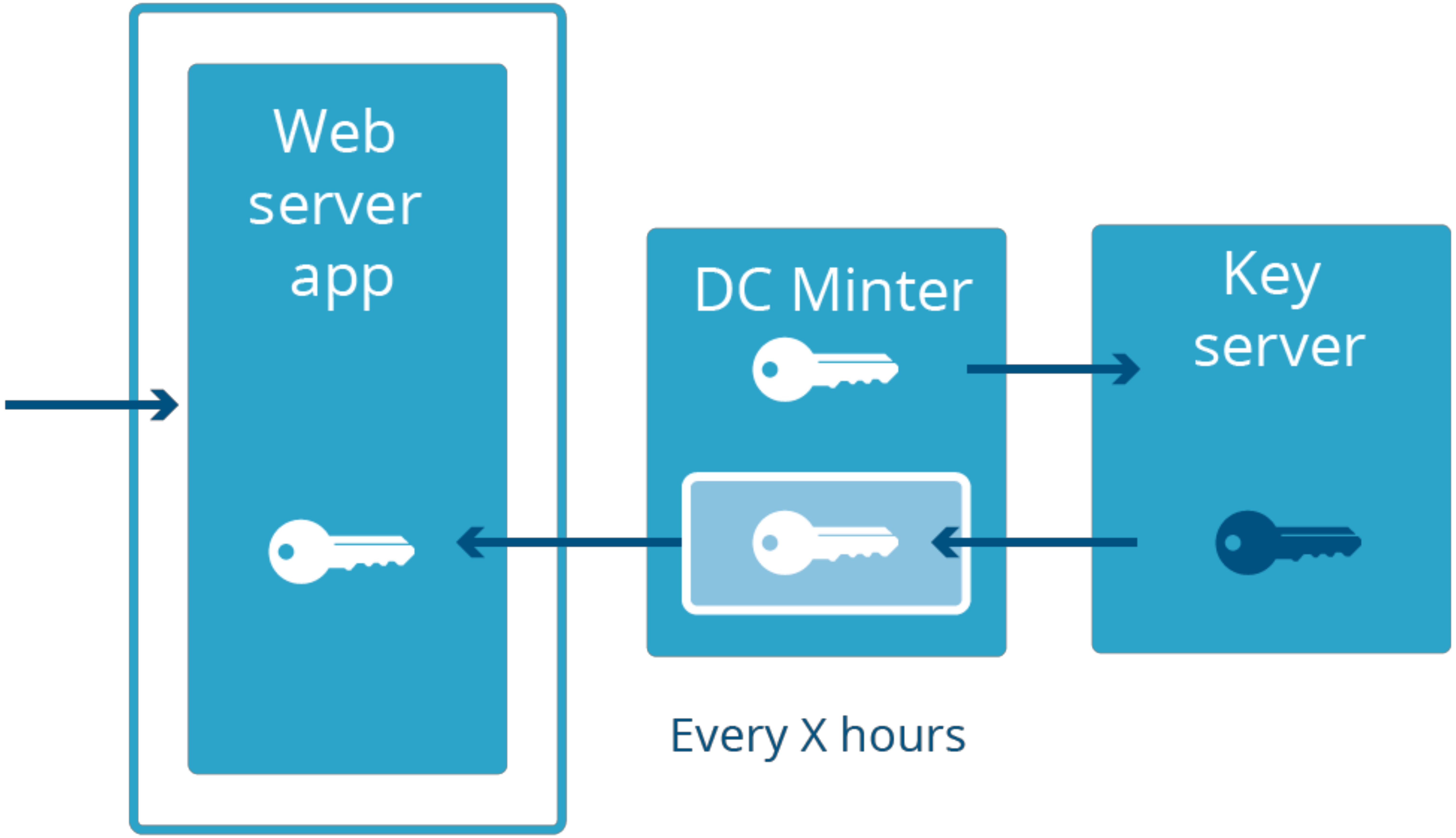
Motivation

- Internet-facing applications have long term keys in memory
- Reduce the exposure of certificate private keys without compromising performance

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



Latency



Every X hours

Delegated credentials

- Time-bounded key swap
- Support advertised through empty extension, delegated_credential
- Server response contains DelegatedCredential struct
- CertificateVerify uses key from Delegated Credential instead of Certificate

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

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

Handshake Validation

- Certificate needs to have OID specifying support
- All certificate constraints still apply
- Revocation and certificate transparency requirements 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
- No risk of expanding scope of certificate
- Compromise of server is limited to lifetime of delegated credential

Updates

- Only minor changes in -03
  - Protocol version removed for more flexibility
- Server implementation in BoringSSL
- Server deployment at kc2kdm.com with proposed OID issued by DigiCert
- Ongoing work to support DCs in NSS, Firefox
- Initial discussion on mozilla.dev.security.policy about interactions with CA/B Forum BRs

Next Steps

- Formal security analysis - J. Hoyland
  - Equivalent to additional certificate
  - Stronger binding to delegator certificate (unlike certificate chain)
- Does the working group think this document is ready for last call?

Nick Sullivan
IETF 104 TLS WG
March 26, 2019

Delegated Credentials