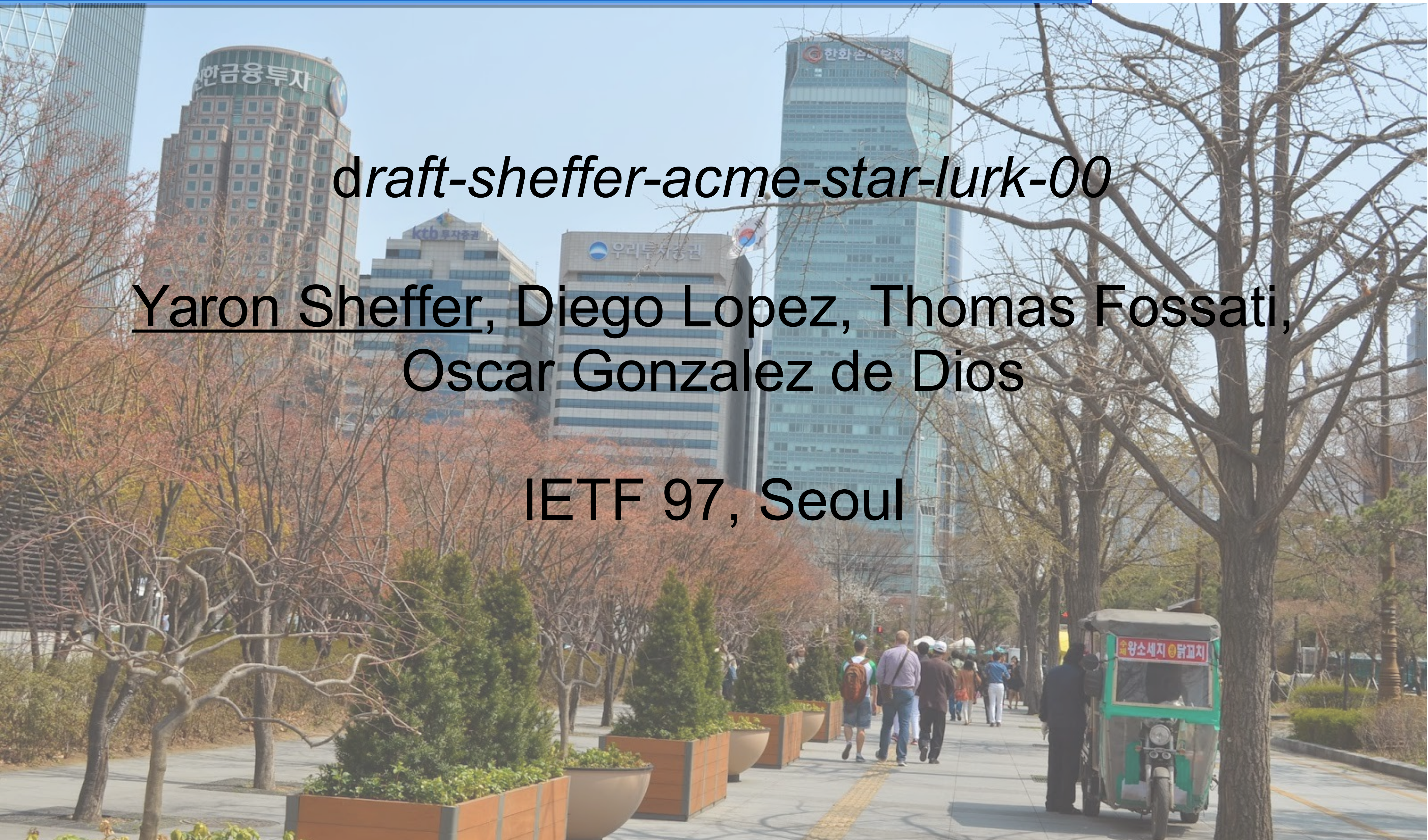
Short Term Certificates



d*raft-sheffer-acme-star-lurk-00*

Yaron Sheffer, Diego Lopez, Thomas Fossati,
Oscar Gonzalez de Dios

IETF 97, Seoul

Motivation

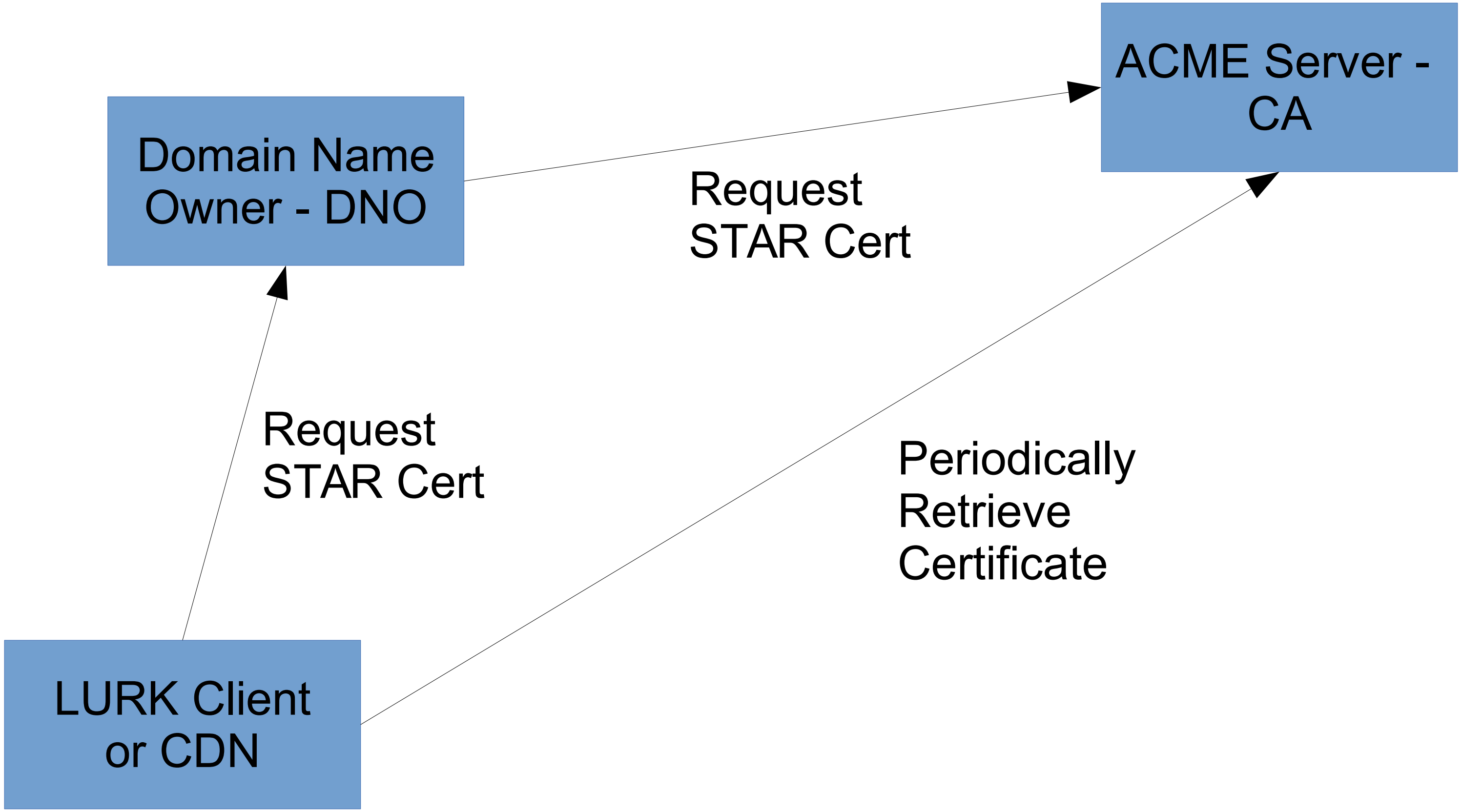
- Delegate the authorization to publish a web site
- Securely: owner can revoke the authorization at any time
- And with no change to the client side (browser)

- Initial use case: CDN
  - Today, sites typically share their private key with the CDN

Background

- The problem space was explored in the LURK BoF
- An alternative: each TLS handshake is forwarded to a “box” that holds the private key and signs responses
  - Obvious engineering issues: performance and availability
- An earlier short-term certs protocol was proposed: draft-sheffer-lurk-cert-delegation
  - The current proposal is significantly different

Overview


ACME Server - CA
Domain Name Owner - DNO
Request STAR Cert
Request STAR Cert
Periodically Retrieve Certificate
LURK Client or CDN

Initial Setup

- Domain Name Owner (DNO) and CDN establish a mutually-authenticated channel
- DNO and CDN agree on a CSR template
  - This is the DNO's policy: what domain names, cert validity period
- DNO registers with the ACME server

Bootstrap

- CDN generates a CSR based on the CSR template, sends it to DNO
- DNO validates that the CSR is in line with the template
- DNO sends the CSR to ACME server, requesting a **Short-Term, Automatically Renewed** (**STAR**) certificate
- ACME performs the usual checks, issues the certificate, sends back a STAR ID and a certificate URL
  - It is the DNO’s responsibility to respond to the issuance checks
- DNO responds to the CDN with the certificate URL
- CDN retrieves the (initial) short-term certificate

Certificate Refresh

- The ACME server periodically renews the certificate
  - E.g. every 3 days
- The ACME server posts the certificate and the CDN retrieves it

Revocation

- The DNO requests the ACME server to stop the automatic renewal process
  - Identified by the STAR ID
- ACME server stops issuing certificates
- No explicit X.509-style revocation

Security Considerations

- How do we prevent the CDN (or a rogue CDN employee) from passing the ACME checks?
  - E.g. https-01, when it can easily set up a web page
- A combination of security measures
  - Ensure the CDN does not own the relevant DNS zone
  - ACME servers MUST respect CAA records
  - Including draft-landau-acme-caa-01, to restrict ACME checks to DNS authorization only

Thank You!