X.509 PKI RA schema for Æ-DIR

Note: The RA is the hard part in a PKI!

Disclaimer: Draft concepts ahead...

by Michael Ströder <michael@stroeder.com>
at LDAPcon 2017

RA -- Registration Authority

- PKIX (RFC 5280) defines:
  …an optional system to which a CA delegates certain management functions;
- Does this public key belong to this end entity (EE)?
- In case of service certs (server and client):
  Securely authorize an admin to request cert on behalf of EE
- EE and admin identifiers
- Secure authentication and authorization

Æ-DIR already has...

- Unique constraints for all relevant entity identifiers: uid, host/aeFqdn, etc.
- Paranoid user management
- Administrative relationship of hosts and services
- ACLs for maintaing aeHost, aeService, aeSrvGroup entries
- Two-factor authentication (OATH-LDAP → LDAPcon 2015)
- LDAP server already installed with high availability

Let's Encrypt integration

- HTTP(S) servers might not have DocumentRoot or you don't want to write there
- Prefer config mgmt (no *certbot* on systems)
- Add ACME challenge to aeHost, aeService, aeSrvGroup entry (aeFqdn=foo.example.com) -- Æ-DIR's ACLs in effect!
- Return ACME challenge via proxy (authz by challenge-ID):
  - http://foo.example.com/.well-known/acme-challenge
  - tricky with authorative DNS servers (TXT query type)

Let's Encrypt caveats

- Currently only server certs
- Let's Encrypt limitations:
  - no IDNA DNS names allowed
  - subject DN is only CN=foo.example.com
  - Cert profile not customizable
- All FQDNs published to certificate transparency logs
- Replication latency (two-tier architecture)

Æ-PKI -- basic ideas

- Act as RA for custom X.509 PKI
- Needs more data associated with Æ-DIR entities:
  - CSR queue(s)
  - Cert archive
  - CA (policy)
  - workflow relationships
- Tightly couple cert subject DNs for Æ-DIR entity DNs: Maybe equal or some simple mapping

Æ-PKI -- enrollment

- Well, we're at LDAPcon → let's use LDAP for enrollment
- Admin has to personally bind to Æ-DIR (e.g. with password and yubikey)
- Submitting a CSR is adding an entry to cn=ae-pki
- ACLs and constraints:
  - check whether admin has control over entry with *aeFqdn*
  - if admin does not have control allow *aepkiStatus* requested
- Picking up issued cert with simple search request

Æ-PKI -- EER diagram