Voucher Profile for Bootstrapping Protocols

draft-ietf-anima-voucher-02

ANIMA WG

IETF 98 (Chicago)

Recap

- At IETF 97 we presented the Voucher document for the first time as an ANIMA draft

- Bootstrapping Design team has met weekly since, about 50% discussion on BRSKI and 50% discussion on Voucher.

Updates Since IETF 97

(Not sorted)

1. Removed support for voucher-revocations.
   - Focus on voucher-renewals instead.

2. Removed single voucher mapping to many pledges.
   - Initially due to not wanting a course-revocation, but became not wanting to unnecessary block a renewal due to being to coarse.

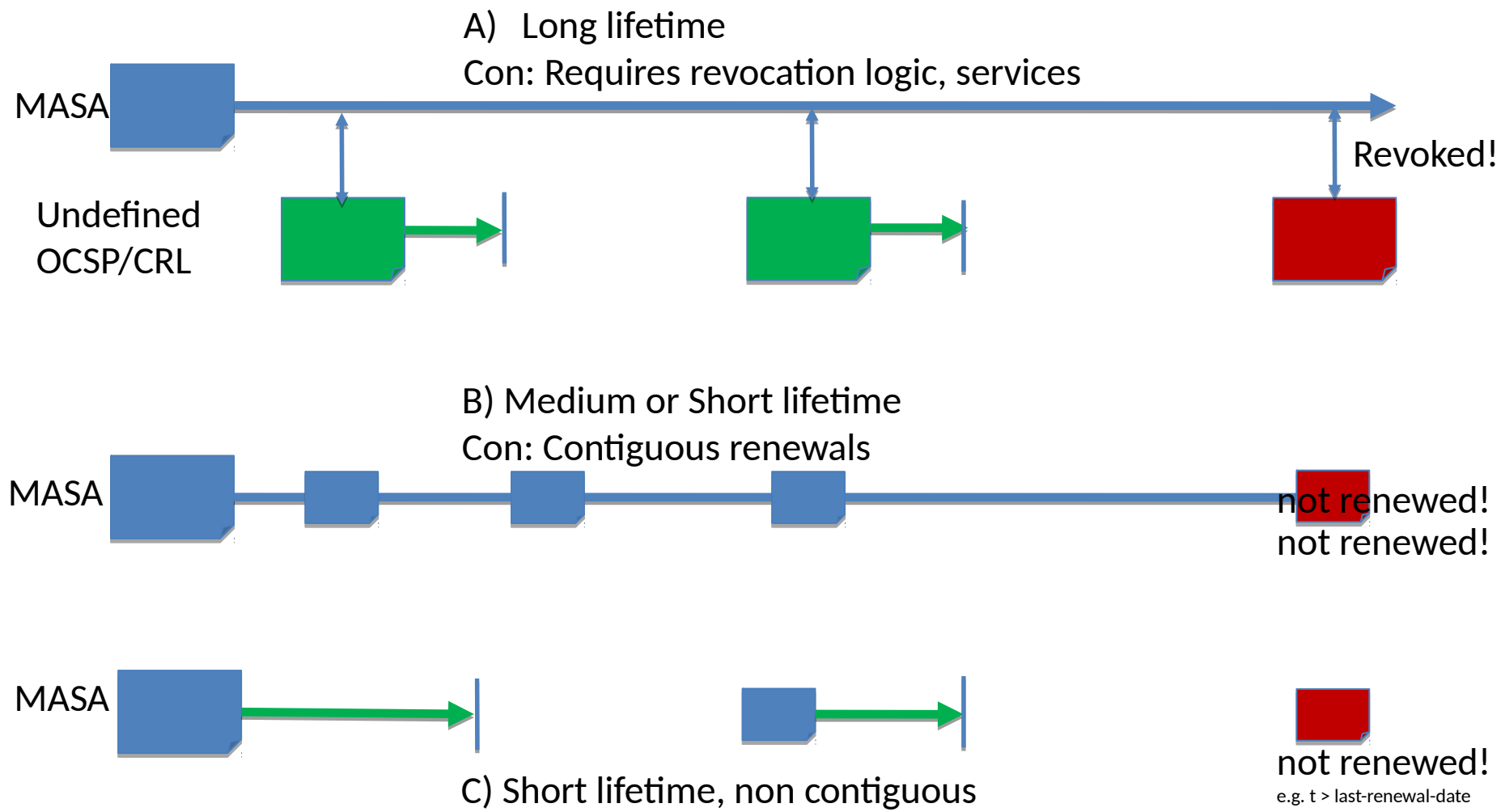
3. Selected PKCS#7 for the signing strategy.

4. Selected JSON for encoding
   - Removed support for XML encoding
   - (setup for future alignment with JWT)

5. Moved terminology from BRSKI into Voucher.

6. Added “Survey of Voucher Types” section.

Renewals > Revocations



Renewals > Revocations

- Design Considerations: Voucher s6.1
  - **Single flow, always exercised**
  - Equivalent to short lifetime revocation statements with simpler operational management
  - No longer need additional revocation status protocols (e.g. RFC6066, section 8 inline certificate status extensions)
  - Threat modeling is simpler
  - Looks like ”Web Tokens”
  - ACME w/ domain validation is effectively the same: a simple method of obtaining a new credential on demand rather than complex renewal
  - Theoretically an (EST) PKI could do this simply by supporting renewal beyond validity period (note: “last-renewal-date” is informative)

Voucher

New parts:

1. authority-key-identifier
   - "The Subject Key Identifier of the MASA's leaf certificate"
   - Intended to identify voucher issuer certificate (may be redundant w/ PKCS7 structures)
2. domain-certificate-identifier/subject
   - Requires the mandatory "trusted-ca-certificate"
   - Allows domain to roll public key during voucher validity period
3. assert-certificate-revocations
   - Flag telling pledge how it should go about validating the domain certificate chain.
4. last-renewal-date
   - An informative field, not processed by pledges, indicating the last date the MASA projects it will renew a voucher on.

Open Issues

1. Does the voucher still need to support indirect issuer?
2. Need to support revocations of domain certificate?
3. PKCS#7 or something else, like CWT?
4. Is there a need for authority-key-identifier?

(Each discussed on upcoming slides)

1. Does the voucher still need to support an indirect issuer?

Specifically the “domain-certificate-identifier” container?

```
+--ro trusted-ca-certificate binary
+--ro domain-certificate-identifier
| +--ro subject? binary
| +--ro cn-id? string
| +--ro dns-id? string
```

Do we need this anymore, if short-lived vouchers are expected, would the domain certificate always be pinned?

This is an issue for NETCONF zerotouch more so than BRSKI, but may affect other bootstrapping protocols as well.

2. Need to support revocations of domain certificate?

Specifically the “assert-certificate-revocations” leaf?

```
+--ro assert-certificate-revocations? boolean
```

The voucher itself is not revocable, but the domain certificate might be.

Event though it’s recommended that vouchers be as short-lived as possible, SHOULD voucher tell device to verify revocation status of the domain’s certificate?

Note: the voucher could also indicate how far out it could determine the revocation status to be good for…

3. PKCS#7 or something else, like CWT?

Right now Voucher uses PKCS#7 for signing

- like SMIME with stapled certificate chain

Some would like to align it with CWT for ultra-small IoT devices

- but CWT is not a good match

Worry about in some future RFC instead?

4. Is there a need for authority-key-identifier?

- PKCS7 includes SignerInfo
- This could be held off until non-PKCS7 signing methods are defined in future work

Final Stretch

We just need to work through these issues.

- Ideally a Last Call in a few weeks…

Questions, Comments, Concerns?