26th EUGridPMA SHA-2 statements

Sept 10-12, 2011
Lyon, FR

SHA-2 conclusions from Lyon

- The recommendation is that CAs will not issue general availability SHA-2 certs before **1 August 2013** [RP datum point]
- If SHA-1 is broken, revocation and transition will be immediate as inspired by the categorization in the HASHRAT document (seconds to few months).
- The scheduled end of life for SHA-1 EECs is 1 September 2014, meaning that SHA-1 EECs SHOULD have a validUntil date no later than that date.
  If there are CAs with EECs having a later date, the primary mitigation of the risk in case SHA-1 is broken will be removal of said CA from the IGTF distribution.
- CAs SHOULD have SHA-2 issuing capability by October 1st 2012
- No need to move any existing CA self-signed root certs to SHA-2 if we rely only on the distributed metadata.
- Since intermediate CAs are distributed but the distribution may be superseded by dynamic CA chains (subject to the namespace constraints) … SHOULD be SHA-2 after 31 March 2014, and if SHA-1 it MUST be revoked and re-issued if and when SHA-1 is broken (like for EECs).
  Once broken, the new intermediates will be distributed or both the intermediates and root removed from the distribution.
- New CA certs generated after April 2014 SHOULD be SHA-512 from, noting that existing (self-signed) CA certs MAY be SHA-1

- Only SHA-256 and SHA-512, and not 224 nor 384. Each CA MAY pick its own variant.
- CRLs on the default CDP SHOULD be SHA-1 until at least 1 September 2014. CAs MAY start distributing SHA-2 based CRLs after that date, and MAY have SHA-2 based CRLs available on alternate CDPs after 1 October 2012.
- If same subject is signed twice (once SHA-1 once SHA-2) must use different cert serial numbers. Same is true of CRLs with same data. Must be different sequence number.
- Breakage of the SHA-1 algorithm in a way that allows trivial generation of plaintexts with a specific hash necessitates removal of SHA-1 algo support. This is a software vulnerability issue outside of our scope and SHOULD be dealt with using regular vulnerability mechanisms of the RPs. It then WILL necessitate SHA-2 based root certs as well.
- The 'end-of-life' SHA-2 migration recommendation does not apply to certificates with a short life time (for SLCS CAs) until at least 1 September 2014.

- This recommendation does not address attribute authorities
- OCSP will continue to use SHA-1