PKI Disaster Recovery and Key Rollover

<draft-pinkas-pkix-pki-dr-kr-00.txt>

Denis.Pinkas@bull.net

Bull S.A.S.

- The topic was originally proposed at the IETF meeting from July 2001 under the name :
  PKI Disaster Planning and Recovery.
- There was no interest at that time in the PKIX WG, but many individual demands came later for getting the draft, ... even years later.
- The initial document has been fully redrafted with Joel Kazin, as co-editor.
- It is proposed as an INFORMATIONAL RFC.

General topics

- The draft identifies various ways to recover from exceptional situations, like private key-compromise or private key-loss and to quickly restore normal operations: it allows to build a **disaster recovery plan**.

- **Private key-compromise** or a **private key-loss** may happen to :
  - End-entities,
  - Certification Authorities,
  - Revocation Authorities,
  - Attribute Authorities, or
  - Time-Stamping Authorities.

- Denial of service attacks on CRL Repositories is considered.

- Since certificates have finite validity, CA key-rollover is considered so that it can be planned in advance.

End-Entities

- The cases are different whether the keys are used for authentication, message-confidentiality or non repudiation (i.e. content commitment).
- The cases are also different for :
  - keys used to decrypt stored data (Data-at-Rest), and
  - keys used to decrypt communications (Data-in-Transit).

CAs

- Different cases apply to:
  - Root CA key-compromise,
  - Intermediate CA key-compromise.

- If a CA has issued 10 millions certificates in smartcards, and its issuing private key is compromise, the draft describes a solution, to *quickly* recover from that situation without re-issuing 10 millions smartcards.

Revocation Authorities

- Addresses:
  - CRL Issuers, and
  - OCSP Responders.
- Makes the difference between:
  - key-compromise within certificate life-time,
  - key-compromise beyond certificate life-time.

Attribute Authorities

- Addresses:
  - Attribute certificate revocation,
  - Attribute Authority Key compromise,
  - Attribute Authority Key loss.

Time-Stamping Authorities

- Addresses:
  - Time-Stamping Unit Key loss, and
  - Time-Stamping Unit Key compromise.
- Makes the difference between a compromise:
  - during the validity period of the TSU certificate, and
  - after the end of the validity period of the TSU certificate.

CRL Repositories

- Addresses the case of hiding an "emergency CRL" by performing a denial of service attack.
- Suggests to add a rule in the validation policy:

  Whenever a CRL is needed, look for it in a cache :

  - if not present, fetch the CRL as usual and place it in the cache with the time when it was fetched, and use it;

  - if present, look for the time when it was fetched, and only use it if it was fetched earlier than x minutes, otherwise, look for a new CRL, and use it.

Proposed way forward

- The proposal is to progress the document as a WG document rather than an individual contribution, so that it will be referenced on the PKIX web page.
- In order to achieve this goal, it is requested:
  - to consider the acceptance of this work item by PKIX WG,
  - then, to include this work-item in the work plan.
- The benefits will be to be able to improve the draft using the expertise from the WG participants.