QuoVadis Trustlink Schweiz AG

QuoVadis – The Swiss solution for digital certificates with worldwide distribution

QuoVadis Trustlink Schweiz AG
Teufenerstrasse 11, 9000 St. Gallen
www.quovadis.ch

Overview

- Check list for Root signing or managed PKI
  - Basics
  - Certificate policies
  - Certificate pratices
  - Infrastructure
  - Operation and support
  - Internal and QuoVadis audits

Basics

- Motivation and reasons to do a subordination or to use managed PKI
- Expectation for a subordination or a managed PKI
- Certificate Policy (CP) and Certificate practice statement (CPS)
  - ETSI TS 102 042

Basics

- QuoVadis Root CA 2 (SSL und EV/SSL) and
  QuoVadis Root CA 3 (Root signing or managed PKI)
  - 4096 bit key length
  - Support issues of earlier software releases
    - e.g. Java 1.4.x, IBM Lotus Notes < v.8.0
  - Trustworthiness of QuoVadis root certificates
    - Operating systems, browsers, mobile devices
      - e.g. Windows 2008, 7
        - Distribution through group policies if an automated update is not allowed or disabled.
  - Compatibility of encryption algorithms
    - 3DES, AES, etc.

Certificate policy (What)

- What should the certificate be used for? Limitations?
- Who or what systems should use the certificates?
- What services based on certificates should be offered
- Obligations and liability
- Terms and conditions
- Certificate types
  - Personal, device, functional certificates
  - Signature, encryption, authentication

Certificate policy (What)

- Accuracy and completeness of certificate information
- Handling of private key
  - Generation, backup, archiving, recovery, history
- Certificate properties
  - Naming conventions, validity, key length, algorithms, key usage, extension, special OIDs
- Preconditions
  - Issuing, enrollment/delivery, renewal, revocation, restore
- CP and CPS
    - ETSI TS 102 042

Certificate practice (How)

- Certificate
  - Naming (principal)
- Usage of secure certificate stores
  - HSM, USB tokens, smart cards
    - Certification of devices
    - Difference between root, issuing and end certificates
- Detailed process description
  - Lifecycle management
    - Application, identification, issuance, enrollment/delivery, renewal, revocation, restore
  - Requirements for traceability, transparency
    - Logging, monitoring, dual-control, auditing
  - Quantities and periodicity
  - Information storage/archiving

Certificate practice (How)

- Roles
  - Definition, assignment of persons, substitution
- Clarification
  - Rights, obligations and responsibilities
  - Sanctions for misuse
- Training
  - Handling of certificates and corresponding private keys
  - Role execution
  - Carrying out of duties and responsibilities
  - Delinquency, reputation

Infrastructure

- Dedicated hardware (separate virtual server)
- Protection and security of the servers (Root and CAs)
  - Firewalls or combined routers
  - Physical separation of networks
  - Virus protection and protection against malware
  - Regular updates, patches
  - Backups (also for root und CA keys)
- Availability
  - Load Balancing, Fail-Over, Clustering
- System components
  - Operating systems, databases, directory services, web servers, etc.

Infrastructure

- Physical safety precautions
  - Access, authentication, logging
  - Measures against water and fire
  - Storage of backups (internal, external)
  - Information management
    - Storage, controlled destruction

Operation/ Maintenance

- Organization and responsibilities
  - Compliance & Risk, Security, System Administration, IT Revision
- Support organization
  - Accessibility, Emergency scenarios
- Storage locations
  - Certificate database
  - Logs und audit trails
  - Root- and CA certificates
  - Certificate revocation list (CRL) and/or Online certificate status protocol (OCSP)
  - CP and CPS

Internal and QuoVadis Audits

- Periodic Review
    - Process definitions
    - Role assignments and separation of duties
    - Implementation and compliance with requirements
    - Traceability

Further information…

info.ch@quovadisglobal.com

QuoVadis Trustlink Schweiz AG

Teufenerstrasse 11, 9000 St. Gallen
www.quovadis.ch