Standards for Registration Practices Statements

IGTF Considerations

Scott Rea
Sr. PKI Architect, DigiCert Inc.

IGTF RPS Standard

Table of Contents

Policy Structure for PKIs

- RFC 3647 : Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- Published in 2003, as an update to 2527
- CPs and CPSs play a central role in documenting the requirements and practices of a PKI
- This is how a CA conveys to a Relying Party what it does to bind identities to keys and how it protects the infrastructure that facilitates that process

Policy Structure for PKIs

- RFC 3647 : CP definition
  - "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements"
- RFC 3647 : CPS definition
  - "A statement of the practices which a certification authority employs in issuing certificates."
  - “A more detailed description of the practices followed by a CA in issuing and otherwise managing certificates may be contained in a certification practice statement (CPS) published by or referenced by the CA.”

CP vs CPS

- Relationship Between Certificate Policy and Certification Practice Statement
  - A CP and CPS address the same set of topics that are of interest to the relying party in terms of the degree to and purpose for which a public key certificate should be trusted.
  - Their primary difference is in the focus of their provisions.
    - The purpose of the CP is to establish what participants must do
    - The purpose of the CPS is to disclose how the participants perform their functions and implement controls

Framework

- RFC 3647 defines a Framework of 9 areas that a CP/CPS should address:
  - 1. Introduction
  - 2. Publication and Repository
  - 3. Identification and Authentication
  - 4. Certificate Life-Cycle Operational Requirements
  - 5. Facilities, Management, and Operational Controls
  - 6. Technical Security Controls
  - 7. Certificate, CRL, and OCSP Profile
  - 8. Compliance audit
  - 9. Other Business and Legal Matters

Framework

- “PKIs can use this simple framework of nine primary components to write a simple CP or CPS. Moreover, a CA can use this same framework to write a subscriber agreement, relying party agreement, or agreement containing subscriber and relying party terms.”

- “This simple framework may also be useful for agreements other than subscriber agreements and relying party agreements. For instance, a CA wishing to outsource certain services to an RA or certificate manufacturing authority (CMA) may find it useful to use this framework as a checklist to write a registration authority agreement or outsourcing agreement.”

Framework

- “a PKI can establish a set of core documents (with a CP, CPS, subscriber agreement, and relying party agreement) all having the same structure and ordering of topics, thereby facilitating comparisons and mappings among these documents and among the corresponding documents of other PKIs”

- An RPS can be considered as a subordinate document to the CPS

Content Recommendation

- If we consider an RPS as a subordinate document to the CPS
  - NOTE: This is common practice for many PKIs
- An RPS should use the RFC 3647 Framework of 9 defined areas that mirrors the structure of a CP and/or CPS document
  - This allows easy comparisons of the relative policy and practice documents
  - Ensures completeness of the material covered
  - Non-applicable areas of RFC 3647 for an RPS can be designated as such

Content Recommendation

- Recommendation on which sections an RPS should pay most attention to:
  - 1.2. DOCUMENT NAME AND IDENTIFICATION
  - 1.3.2. Registration Authorities
  - 1.3.3. Subscribers
  - 3. IDENTIFICATION AND AUTHENTICATION
  - 3.1 Naming
  - 3.1.1 Types of names
  - 3.1.2 Need for names to be meaningful
  - 3.1.3 Anonymity or pseudonymity of subscribers
  - 3.1.4 Rules for interpreting various name forms
  - 3.1.5 Uniqueness of names
  - 3.1.6 Recognition, authentication, and role of trademarks
  - 3.2 Initial identity validation
  - 3.2.1 Method to prove possession of private key
  - 3.2.2 Authentication of organization identity
  - 3.2.3 Authentication of individual identity
  - 3.2.4 Non-verified subscriber information
  - 3.2.5 Validation of authority
  - 3.2.6 Criteria for interoperation
  - 3.3 Identification and authentication for re-key requests
  - 3.3.1 Identification and authentication for routine re-key
  - 3.3.2 Identification and authentication for re-key after revocation
  - 3.4 Identification and authentication for revocation request

Content Recommendation

- Recommendation on which sections an RPS should pay most attention to:
  - 4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS
  - 4.1 Certificate Application
  - 4.1.1 Who can submit a certificate application
  - 4.1.2 Enrollment process and responsibilities
  - 4.2 Certificate application processing
  - 4.2.1 Performing identification and authentication functions
  - 4.2.2 Approval or rejection of certificate applications
  - 4.2.3 Time to process certificate applications

  - 4.9 Certificate revocation and suspension
  - 4.9.1 Circumstances for revocation
  - 4.9.2 Who can request revocation
  - 4.9.3 Procedure for revocation request
  - 4.9.4 Revocation request grace period
  - 4.9.5 Time within which RA must process the revocation request

  - 5.2 Procedural controls
  - 5.2.1 Trusted roles
  - 5.2.2 Number of persons required per task
  - 5.2.3 Identification and authentication for each role
  - 5.2.4 Roles requiring separation of duties

Content Recommendation

- Recommendation on which sections an RPS should pay most attention to:
  - 5.3 Personnel controls
  - 5.3.1 Qualifications, experience, and clearance requirements
  - 5.3.2 Background check procedures
  - 5.3.3 Training requirements
  - 5.3.4 Retraining frequency and requirements
  - 5.3.5 Job rotation frequency and sequence
  - 5.3.6 Sanctions for unauthorized actions
  - 5.3.7 Independent contractor requirements
  - 5.3.8 Documentation supplied to personnel
  - 5.4 Audit logging procedures
  - 5.4.1 Types of events recorded
  - 5.4.2 Frequency of processing log
  - 5.4.3 Retention period for audit log
  - 5.4.4 Protection of audit log
  - 5.4.5 Audit log backup procedures
  - 5.4.6 Audit collection system (internal vs. external)
  - 5.4.7 Notification to event-causing subject
  - 5.4.8 Vulnerability assessments
  - 5.5 Records archival
  - 5.5.1 Types of records archived
  - 5.5.2 Retention period for archive
  - 5.5.3 Protection of archive
  - 5.5.4 Archive backup procedures
  - 5.5.5 Requirements for time-stamping of records
  - 5.5.6 Archive collection system (internal or external)
  - 5.5.7 Procedures to obtain and verify archive information

Content Recommendation

- Recommendation on which sections an RPS should pay most attention to:
  - 5.7 Compromise and disaster recovery
  - 5.7.1 Incident and compromise handling procedures
  - 5.7.2 Computing resources, software, and/or data are corrupted
  - 5.7.3 Entity private key compromise procedures
  - 5.7.4 Business continuity capabilities after a disaster
  - 5.8 CA or RA termination

  - 6.1.2 Private key delivery to subscriber
  - 6.1.3 Public key delivery to certificate issuer

  - 6.5.1 Specific computer security technical requirements

  - 6.6.1 System development controls
  - 6.6.2 Security management controls
  - 6.6.3 Life cycle security controls
  - 6.7 Network security controls
  - 6.8 Time-stamping

  - 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS
  - 8.1 Frequency or circumstances of assessment
  - 8.2 Identity/qualifications of assessor
  - 8.3 Assessor's relationship to assessed entity
  - 8.4 Topics covered by assessment
  - 8.5 Actions taken as a result of deficiency
  - 8.6 Communication of results

Content Recommendation

- Recommendation on which sections an RPS should pay most attention to:
  - 9. OTHER BUSINESS AND LEGAL MATTERS
  - 9.1 Fees
  - 9.1.1 Certificate issuance or renewal fees
  - 9.1.2 Certificate access fees
  - 9.1.3 Revocation or status information access fees
  - 9.1.4 Fees for other services
  - 9.1.5 Refund policy
  - 9.2 Financial responsibility
  - 9.2.1 Insurance coverage
  - 9.2.2 Other assets
  - 9.2.3 Insurance or warranty coverage for end-entities
  - 9.3 Confidentiality of business information
  - 9.3.1 Scope of confidential information
  - 9.3.2 Information not within the scope of confidential information
  - 9.3.3 Responsibility to protect confidential information
  - 9.4 Privacy of personal information
  - 9.4.1 Privacy plan
  - 9.4.2 Information treated as private
  - 9.4.3 Information not deemed private
  - 9.4.4 Responsibility to protect private information
  - 9.4.5 Notice and consent to use private information
  - 9.4.6 Disclosure pursuant to judicial or administrative process
  - 9.4.7 Other information disclosure circumstances
  - 9.5 Intellectual property rights
  - 9.6 Representations and warranties

Content Recommendation

- Recommendation on which sections an RPS should pay most attention to:
  - 9.6.2 RA representations and warranties
  - 9.6.3 Subscriber representations and warranties
  - 9.6.4 Relying party representations and warranties
  - 9.6.5 Representations and warranties of other participants
  - 9.7 Disclaimers of warranties
  - 9.8 Limitations of liability
  - 9.9 Indemnities
  - 9.10 Term and termination
  - 9.10.1 Term
  - 9.10.2 Termination
  - 9.10.3 Effect of termination and survival
  - 9.11 Individual notices and communications with participants
  - 9.12 Amendments
  - 9.12.1 Procedure for amendment
  - 9.12.2 Notification mechanism and period
  - 9.12.3 Circumstances under which OID must be changed
  - 9.13 Dispute resolution provisions
  - 9.14 Governing law
  - 9.15 Compliance with applicable law
  - 9.16 Miscellaneous provisions
  - 9.16.1 Entire agreement

Process Recommendation

- Update the "***Accreditation and Membership Process Guidelines***"
  - New Category of Membership: Registration Authority
    - A CA Member may have integrated RA functions per the existing functionality and application process;
      - In this case the CA only need publish the standard CP/CPS

    or

    - A CA Member may specify one or more existing accredited RA(s), or a new to-be-accredited RA(s) as part of its membership application
      - When CA & RA functions are separated, the CA must describe how security, integrity, and audit responsibilities are shared between them for each RA
      - Each accredited RA must publish an RPS
      - The CA must demonstrate how the RPS for each accredited RA meets the requirements of its own CPS

Process Recommendation

- Update the "***Accreditation and Membership Process Guidelines***"
  - An RA Member should be accredited under the existing Authority process outlined in the document
    - *The applicant should make a face-to-face presentation discussing each authority at a plenary meeting of the PMA.*
    - *The presentation must discuss all important elements of the authority, including the authentication model, identity vetting model, and naming, as well as physical security measures, record keeping, and auditing.*
  - An RA must publish an RPS
    - A link to the RPS will become part of the CA metadata
    - IGTF will create a new Repository with appropriate metadata for accredited RAs
    - IGTF will create a new RA profile for accreditation against

Process Recommendation

- Update the "***Accreditation and Membership Process Guidelines***"
  - An RA Member should be subject to the same self-audit requirements and schedule as are CAs
  - A CA must reference a current RA self-audit for each accredited RA used when reporting on its own self-audit
  - A new set of audit checklists should be created specific to RPS accreditation

Benefits

- Separating RAs from the CA function has the following benefits:
  - Potential to reduce overall accreditation efforts by not duplicating CA components when new communities join
  - Potential to make it easier for new communities to join by simply choosing an existing CA and focusing on RA functions only
    - Something they typically already know how to do
  - Facilitates easier transitions for existing projects who need to change CA providers
  - Is in keeping with the guidelines for Constituencies and Moderation
    - Potentially reducing the number of CA trust anchors while still facilitating new communities to join
    - Reduces the overall load on the system that needs to process an ever-expanding set of accredited CAs.
  - Will create greater consistency (facilitating greater trust) among RA processes across the community, the same way similar CPS did for CAs
  - Potential to leverage RPS from existing external PKIs communities outside IGTF, lowering entry barriers, increasing interoperability

Summary

- IGTF should create a new membership category: Registration Authority
  - RAs should be defined under the existing Authority definition and accredited based on a published RPS
- An RPS can be considered as a subordinate document to the CPS
  - An RPS should use the RFC 3647 Framework of 9 defined areas that mirrors the structure of a CP and/or CPS document
- A new RA Membership category would allow for more efficient trust processing of the overall system
  - IGTF to create a new Repository of Approved RAs
  - CAs may have integrated RA functions or use an accredited RA
  - This allows the existing accredited CAs or a reduced number to facilitate trust processing for expanded communities without impacting performance of overall community
  - Easier for new communities to join IGTF by just focusing on RA responsibilities & using an existing CA

DigiCert Contacts

Website: http://www.DigiCert.com/

Email: support@DigiCert.com

Scott Rea: (801) 701-9636, Scott@DigiCert.com

digicert