NIST

Streamlining the CP and CPS Process

Generic Rudimentary Certificate Policy and Practice Statement

June 20, 2002

Streamlining the CP and CPS Process

- Goal:
  - Develop Generic Certificate Policy (CP) and Practice Statment (CPS) templates
  - Enable Agencies to quickly produce CP and CPS documents
- Separate Generic CP and CPS templates cooresponding to FBCA levels:
  - Rudimentary
  - Basic
  - Medium

Generic Rudimentary Certificate Policy

- Generic to fit many possible PKI implementations
- Explanatory text included to help writer tailor specific sections as needed
- Based on FBCA CP to allow for easier cross-certification analysis

Examples of Explanatory Text

- Section 3.1.9 Authentication of Individual Identity - For subscribers, the CA shall ensure that the applicant's identity information is verified and checked in accordance with the CPS. **{Outline the specific process your organization is going to take in authenticating an individual's identity in the CPS.}**

- Section 4.2 Certificate Issuance - **{While the subscriber may do most of the data entry, it is still the responsibility of the CA to verify that the information is correct and accurate. This may be accomplished either through a system approach linking databases containing personnel information or through personal contact with the program's attribute authority (as put forth in the CA's CPS). If databases are used to confirm subscriber attributes, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance specified for the certificates conveying the subscriber attributes.}**

Generic Rudimentary CPS Template

- Corresponds to Generic Rudimentary CP
- Provides the options to identify how policy is met
- Document creation will be automated through the use of CPS development tool

CPS template and automation tool are still under development.