Reference Certificate Policy

Andrew Regenscheid

Mathematician

Computer Security Division

NIST

National Institute of
Standards and Technology
U.S. Department of Commerce

Overview

- Purpose and Motivation
- Reference CP Overview
- What Changes Were Made?
- Future Plans

Introduction

- Government and industry interested in “raising the bar” for security at CAs
- The draft is a starting point- we want and need feedback from the wider public and private CA communities
- Motivation
  - Security incidents at publicly-trusted CAs in 2011 highlighted need for stronger security practices
  - Some incidents were the result of weak computer and network security practices at impacted CAs and RAs
  - Current audit programs were not sufficient to identify these weaknesses

Purpose

- Identify a stronger set of security practices to serve as a baseline for publicly-trusted CAs
- Encourage adoption by the CA community and OS/browser community (i.e., trust anchor managers)
- Incorporate baseline security practices into audit programs

Reference Certificate Policy

- Why a Reference CP?
  - – Standard format for expressing requirements of relying parties
  - – Organized in a way that emphasizes where the gaps were filled
  - – Puts the pointers where they point to
  - – CP used as audit checklist

Reference Documents

- Federal PKI Common Policy Framework
- Baseline Security Requirements for Network Security Zones in the Government of Canada
- CAB Forum Baseline Requirements
- Various NIST and PKI industry standards and papers

Common Policy Baseline

- Mature, comprehensive CP
- End-user, end-device oriented
- Up to date, civilian oriented
- Inclusive of user types, PKI topologies

Target Audience

- As recommended security practices:
  - – Focus on publicly-trusted CAs
  - – TLS/Code signing
- As a reference document:
  - – Certificate policy writers
  - – Policy managers
  - – Trust anchor managers
  - – Auditors

How to Use the Reference CP

Three categories of text:

- **Suggested Text**- Intended to be used (nearly) verbatim
- **Fill-in Fields**- Details to be filled in by CP writer
  - e.g., CAs that issue certificates to subscribers or operate on-line must issue CRLs at least once every <18> hours
- **Instructions**- Guidance to the CP writer

Reference CP

- **Common Policy**
  - Basis for many sections
    - Trusted Roles and Procedural controls
    - Key management and certificate lifecycle
    - Audit Logging
    - Physical controls
  - But removed USG-specific language
- **CAB Forum Guidelines**
  - Reference in identity-proofing sections
- Ensured requirements were appropriate and flexible for large and small CAs

Computer/Network Security

- Significant updates in computer, lifecycle and network security control sections
- Major topic areas:
  - Access control
  - System integrity
  - Isolation and boundary protection
  - Communications security
  - Remote access
  - Monitoring

Computer/Network Security

- Identifies well-established best practices based on:
  - SP800-53 controls and NIST publications
  - SANS 20 Critical Security Controls
  - Baseline Security Requirements for Network Security Zones, Government of Canada
- Far more detailed than typical CPs
  - Major gap we identified
  - Details intended to support audit requirements

Next Steps

- NISTIR 7924 released for comment
  - – We want your feedback!
  - – Outreach to industry groups, audit community
- Standardization Efforts
  - – NISTIR a publishing vehicle to get broader feedback
  - – Plan to submit RefCP to an internationally-recognized standards organization
  - – Related efforts being considered/underway in several SDOs

Draft NISTIR 7924

available at csrc.nist.gov

Comment Period Closes
June 7, 2013

Contact Information

Andrew Regenscheid

Andrew.R@nist.gov