The Certificate Policy Framework of Certification Services in China

Jiwu Jing

State Key Laboratory of Information Security , CAS

Data Assurance and Communication Security Center, CAS

17 September, 2012

Certificate Policy - CP

- **CP**
  - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements
  - By IETF PKIX Working Group
- **CPS**
  - Another similar but different definition
  - CPS is a statement of the practices which a certification authority employs in issuing certificates, - by IETF PKIX Working Group

The usage of CP and CPS

- **A simple example**

The CA designs a CP, describing the security requirements that it satisfies

Based on the CP, the CA develops its CPS (a detailed specification), and follows the CPS to issue certificate

A user valuates the CP, and decides whether to accept the certificate

Security requirement in CP

- **The security requirements described in a CP document, - RFC 3647**
  - Identification and Authentication
  - Certificate Life-Cycle Operational Requirements
  - Facilities, Management, and Operational Controls
  - Technical Security Controls
  - Certificate, CRL, and OCSP Profile
  - Compliance audit
  - Other Business and Legal Matters
- **Users decide whether to accept a certification service, according to the CP document**

Different Usage Model of CP/CPS

- **CP and CPS by CA**
- **CP by user, and CPS by CA**
- **CP and CPS by CA, evaluated by authority**

CP and CPS by CA

- **VeriSign**
  - Trust Network Certificate Policies
  - Class 1-2.16.840.1.113733.1.7.23.1
  - Class 2-2.16.840.1.113733.1.7.23.2
  - Class 3-2.16.840.1.113733.1.7.23.3
- **CP and CPS are designed by VeriSign**
- **User choice: to accept or not**
  - After evaluating the policies

CP by user, and CPS by CA

- **USA Federal PKI**
  - Citizen and Commerce Class Common Certificate Policy
  - X.509 Certificate Policy for The Federal PKI Common Policy Framework - 6 policies
  - X.509 Certificate Policy for the E-Governance Certification Authorities - 3 policies
- **Then, based the CP, CA companies develop their CPS to issue certificates**
- **FPKI, who designs the CP, is the user who takes the certification services**

CP and CPS by CA, Evaluated by another authority

- **WebTrust, a typical example**
- **CA companies design CP/CPS by themselves**
- **WebTrust evaluates the CA companies, by its own criteria**
- **The WebTrust seal is a reference for users**

The certificate policy framework in China

- **This work is supported by MIIT and TC260**
  - Ministry of Industry and Information Technology
  - China National Information Security Standardization Committee
- **The CPs will been published as Chinese National Standards**
  - Current status: request for comments

Our Purpose
A different/hybrid usage model

- An independent organization designs CPs
- CA companies follow one of the CPs to develop their own CPS, and issue certificates
- Evaluate whether the CPS match the corresponding CP
  - E.g., by MIIT, available publicly
- Users decide whether to accept a certification service, according to the CP and the evaluation results

The certificate policy framework

3 categories of CPs

Device	• Network communication • The certificate subject is a device • e.g., news website, weibo server, SSL
Commerce	• Commercial activities • The certificate subject is a person or company
Public service	• Public services by Government • The certificate subject is a citizen • Digital ID to access public services

Why 3 different categories?

- **A CP indicates the security requirements of applications**
- **The major security requirement**

Device

- Data origin authentication
- Transmission integrity

Commerce

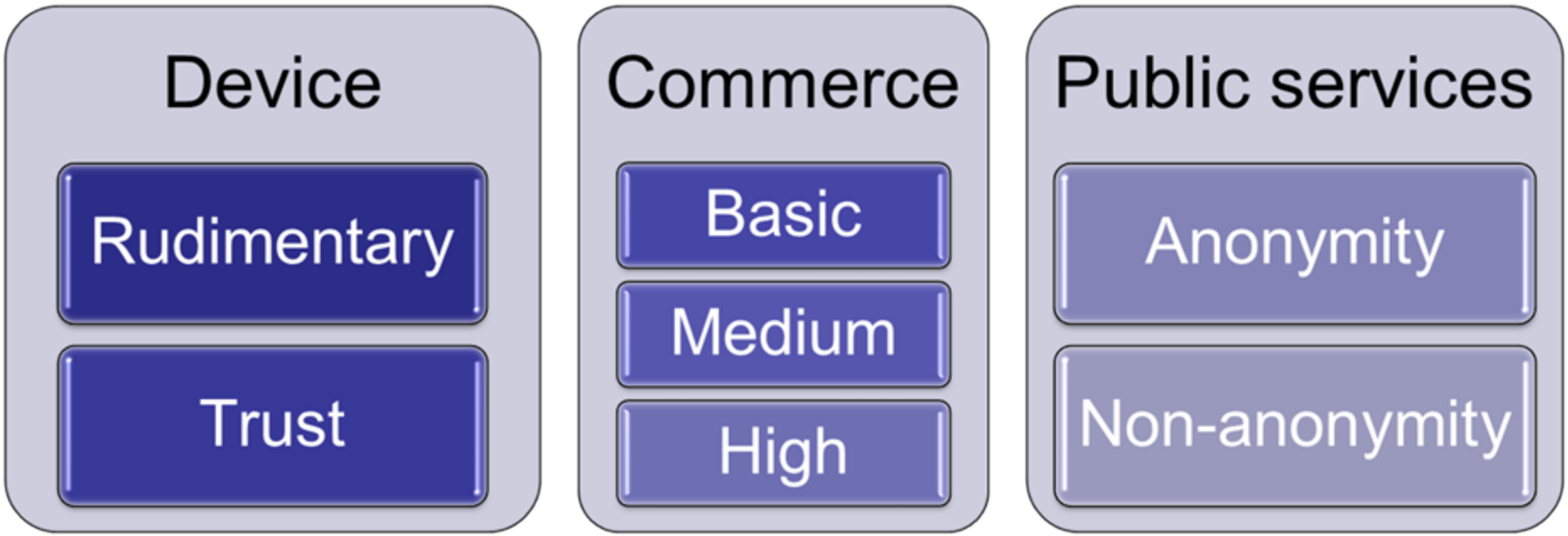
- Non-repudiation
- Credit rating
- (+authentication, integrity)

Public service

- Authentication of citizenship
- (+authentication, integrity)

Certificate Policies

8 Certificate Policies



- Define basic requirements of certification services

The main difference of CP

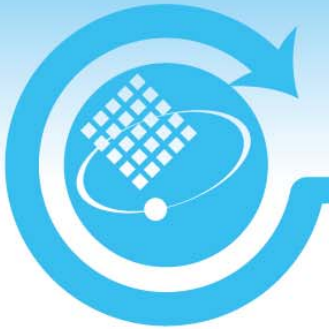
- **Device**
  - Rudimentary
  - Trust
- **The protection level of the device**
  - Environment
  - Security mechanism
  - …

The main difference of CP

- **Commerce**
  - Basic
  - Medium
  - High
- **Two factors are important in online business**
  - The assurance level of identity
  - The certificate holder’s economic capability

Why the Baseline CP?

- **According to China Electronic Signature Law, a CA company shall applied a license from MIIT**
  - before he can issue PKI certificates as the TTP
- **The 7 policies define requirements, comparable to VeriSign, US FPKI, etc.**
- **However, not all network transactions require high assurance certificates**
- **The baseline CP is designed for this purpose, as the basic requirement to obtain the CA license.**



THE END!
THANKS VERY MUCH!

ANY COMMENTS?