PKI Establishment

Wen-Cheng Wang, Ph.D., PMP,
Chief PKI Product Manager
Information and Communication Security Dept.,
Data Communications Business Group,
Chunghwa Telecom Co., Ltd.

April 16-17, 2015

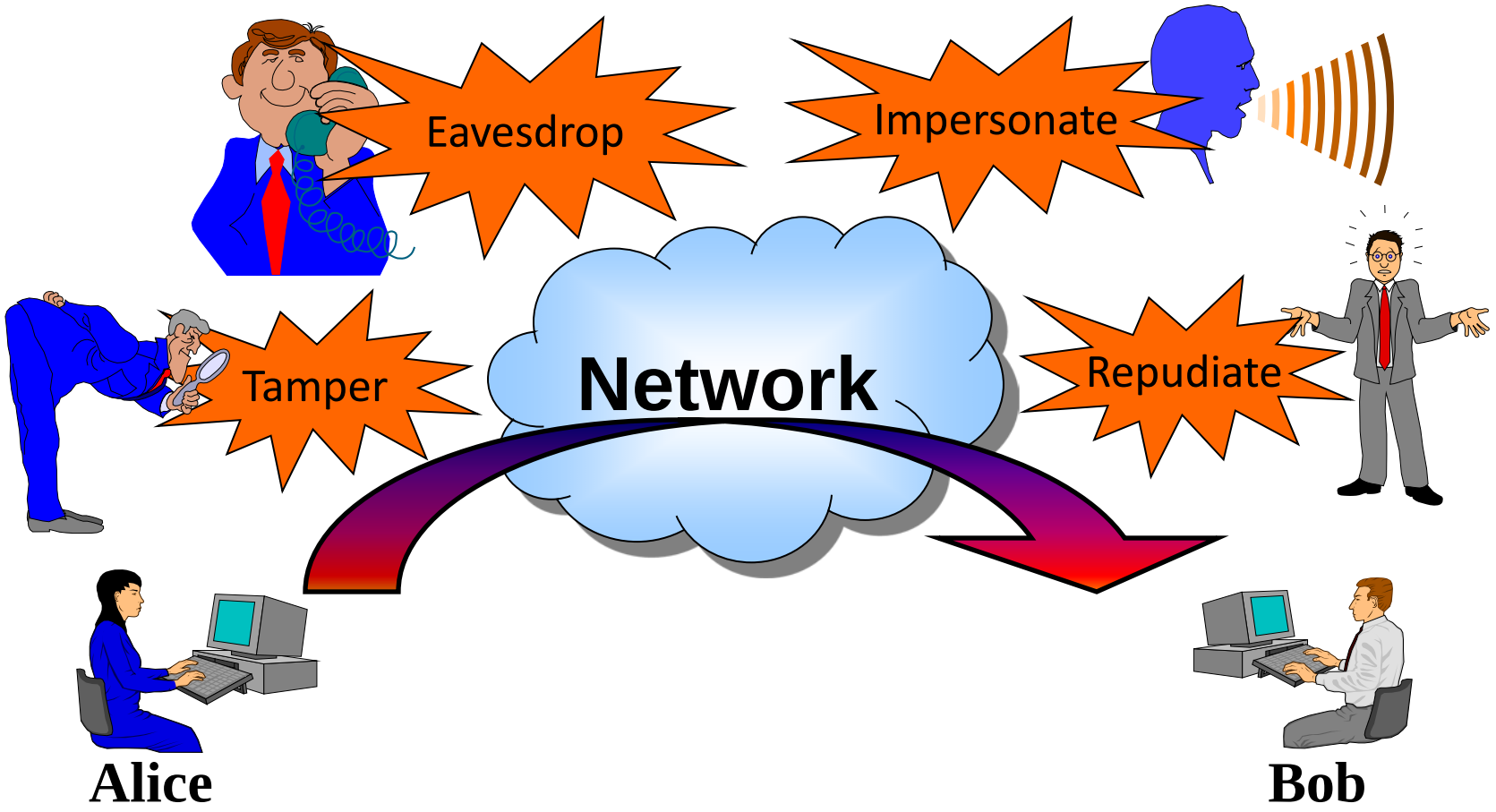
Outline

- PKI Definition
- PKI Trust Model
- PKI Establishment: Step by Step
  - Step 1: Legislation for PKI
  - Step 2: Choose PKI Trust Model
  - Step 3: Establish CA Accreditation Scheme
  - Step 4: Define Certificate Profiles
  - Step 5: Stipulate CP and CPS
  - Step 6: Establish the Root CA
  - Step 7: Establish the Subordinate CA
  - Step 8: Conduct CA Audit
  - Step 9: Consolidate Your Infrastructure
- Homework

Part 1

PKI DEFINITION

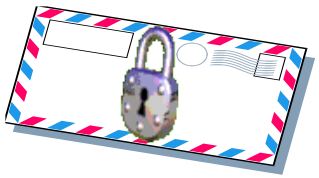
Network Security Threats



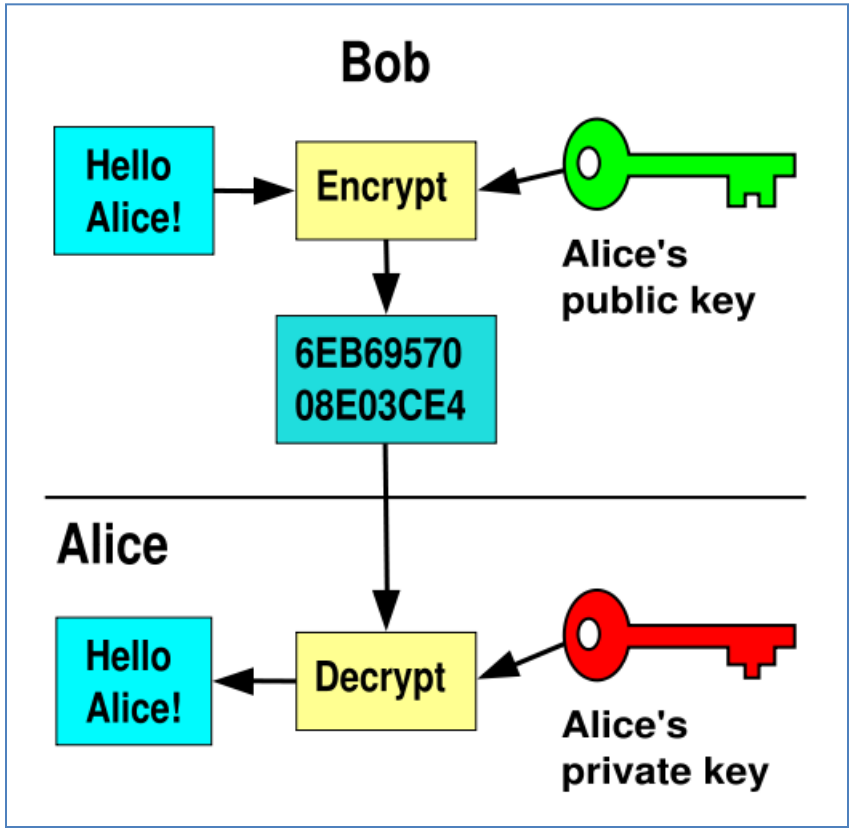
Public Key Cryptography

- Public key cryptographic techniques as countermeasures against network security threats:
  - Digital Signature:
    - Ensure integrity, authenticity, non-repudiation.
    - As a countermeasure against tampering, impersonation, repudiation.

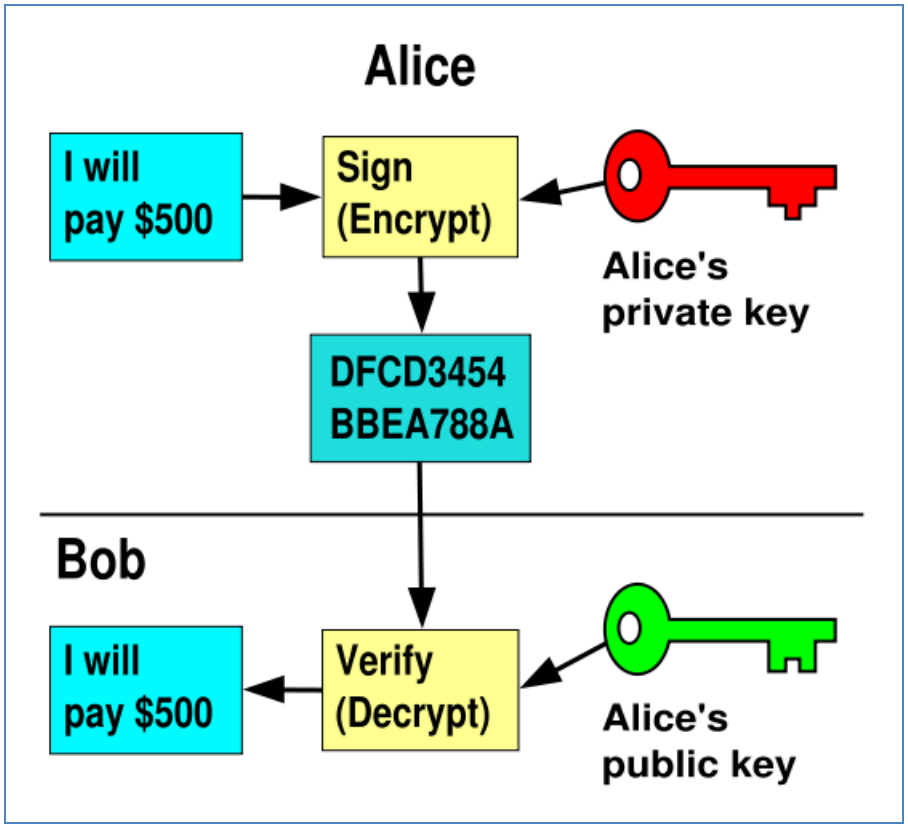
  - Digital Envelope (a.k.a. Public Key Encryption):
    - Ensure confidentiality.
    - As a countermeasure against eavesdropping.



A quick review of public key cryptography



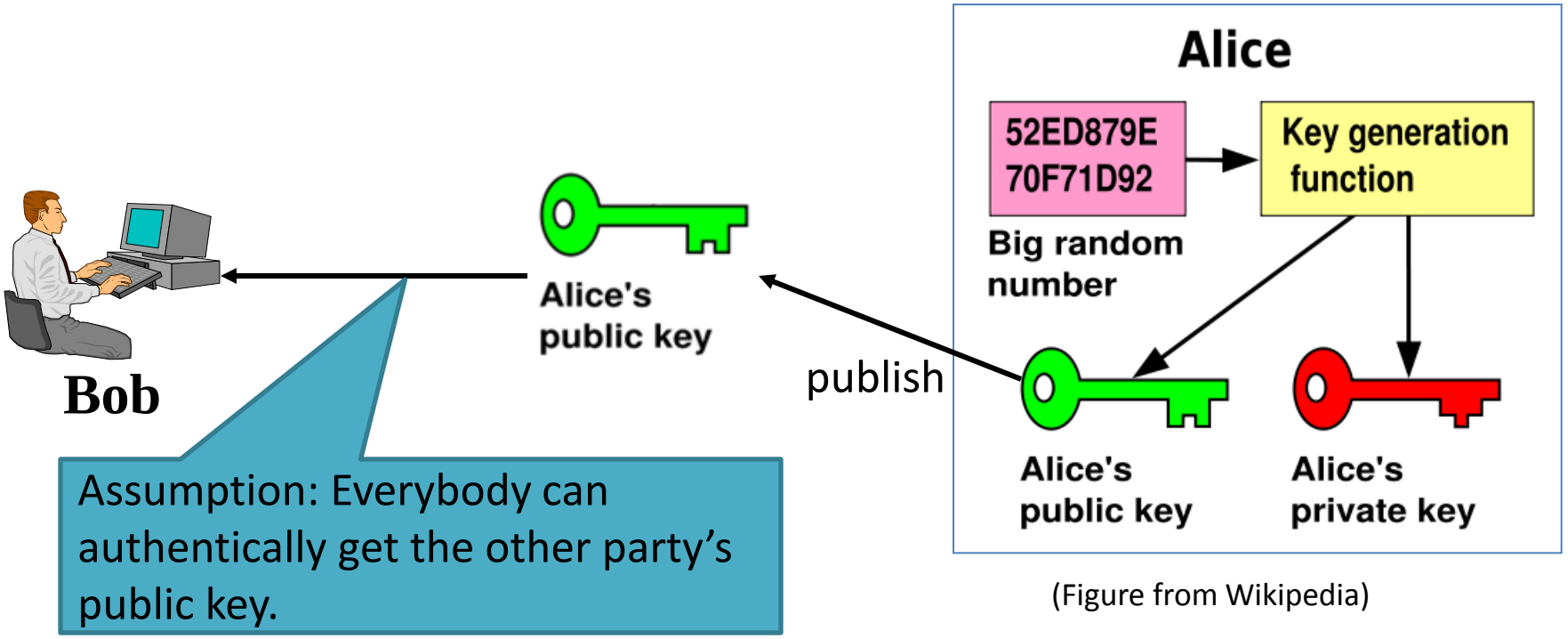
Encryption Scheme



Signature Scheme

(Figures from Wikipedia)

Assumption of public key cryptography



(Figure from Wikipedia)

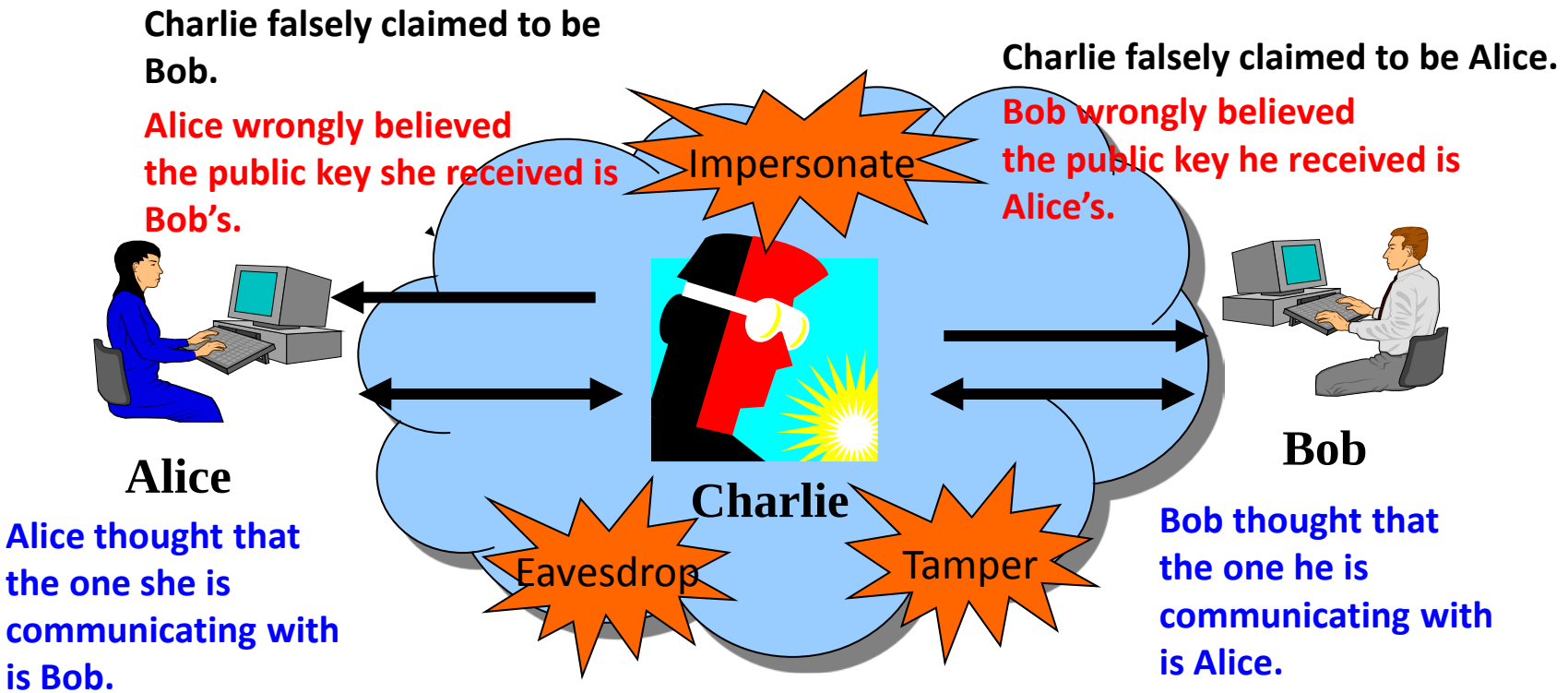
Theory vs. Practice: The one who publishes the public key may be not the one (s)he claims to be.

On the internet, nobody knows you're a dog.

"On the Internet, nobody knows you're a dog."

By Peter Steiner on page 61 of July 5, 1993 issue of the New Yorker

Man-in-the-middle (MITM) Attack



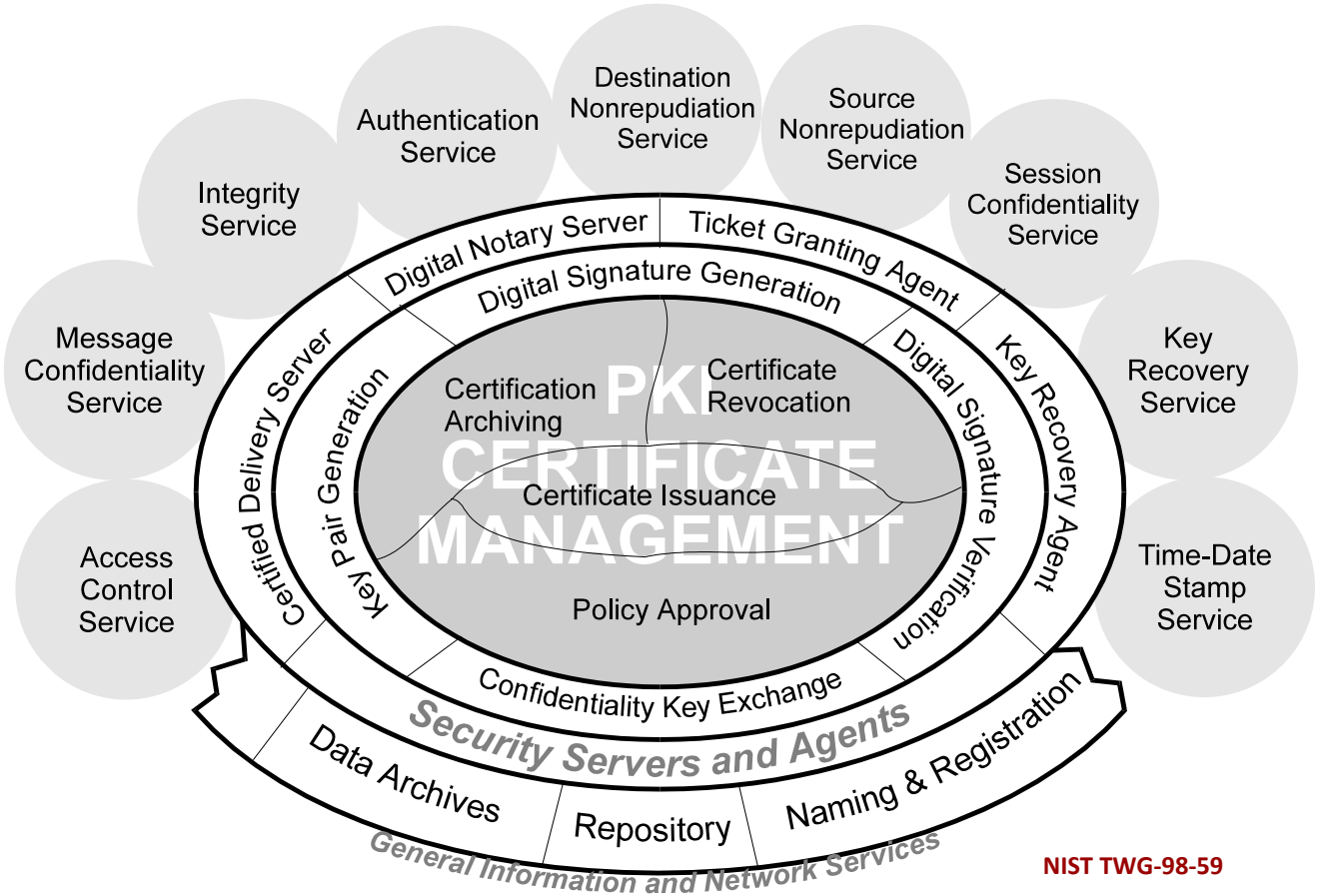
- The assumption made by cryptologists : Everybody can authentically get the other party's public key.
- What cryptologists did not tell you is that it not that easy to make the assumption come true.

What is PKI?

- Public Key Infrastructure(PKI):
  - Personnel, laws, policies, procedures, components and facilities to make public key cryptosystems work.
    - To support participants authentically get the other party's public key.
    - PKI is a countermeasure to MITM attacks.
  - Provides various services to facilitate utilization of Public Key Cryptographic Technologies.
- The foundation of a PKI is the certification authority (CA).

PKI≠CA, but PKI ⊃ CA

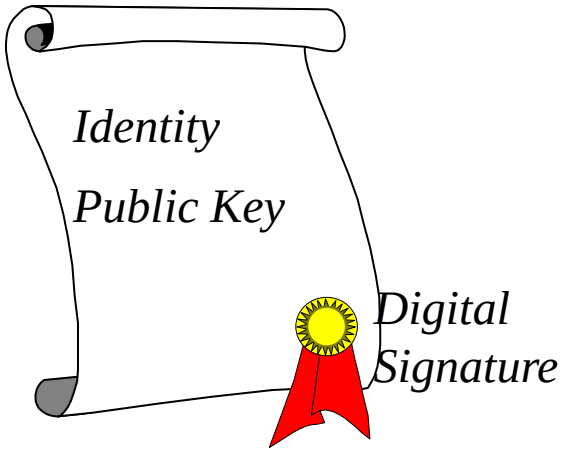
Various Services of PKI

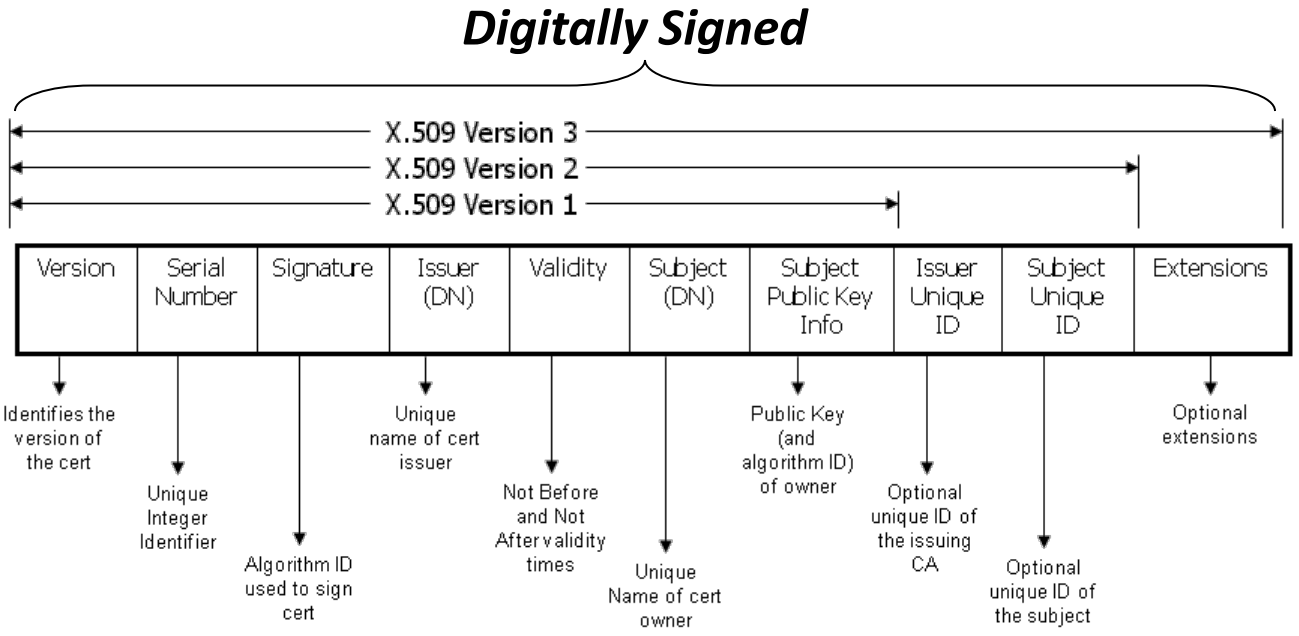


NIST TWG-98-59

PKI Terminology

- Public Key Certificate: (Certificate)
  - A digitized piece of information that binds an identity to a public key, in a manner that is not forgeable.



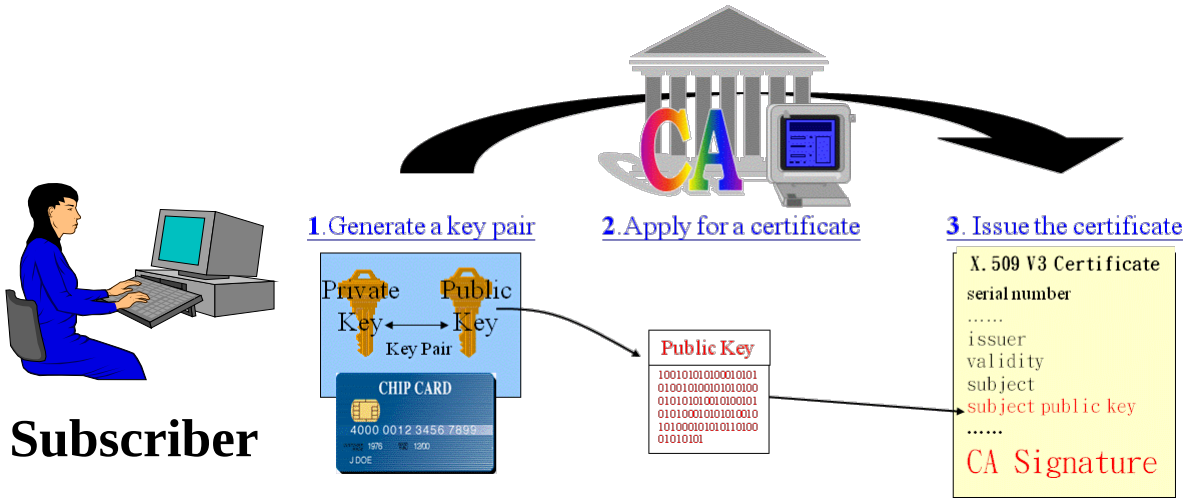


PKI Terminology

- Certification Authority (CA):
  - An entity who issues certificates – that is, who certifies the binding of an identity to a public key.
  - An entity who manages certificate lifecycle, including enrollment, issuance, renewal, revocation, suspension, resumption, etc.
- Certificate Management System:
  - A computer system that enables a CA to support certificate management functions as required.

PKI Terminology

- Subscriber:
  - That person or entity defined as the subject of the certificate.
  - Authorized holder of the private key.
  - The person or entity that is bound to the private/public key pair.

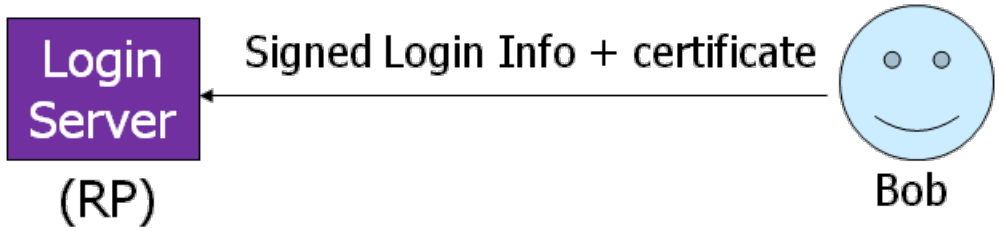


PKI Terminology

- Registration Authority (RA):
  - An optional entity appointed by the CA to support the registration and authentication process of subscribers.
- End-Entity (EE):
  - An entity who will not issues certificates.
  - Anyone other than CA is an EE.

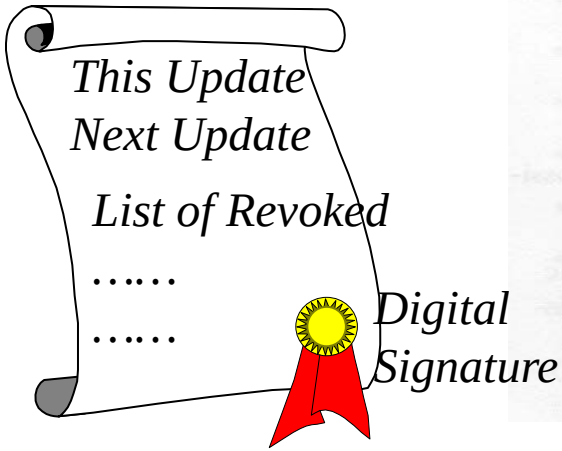
PKI Terminology

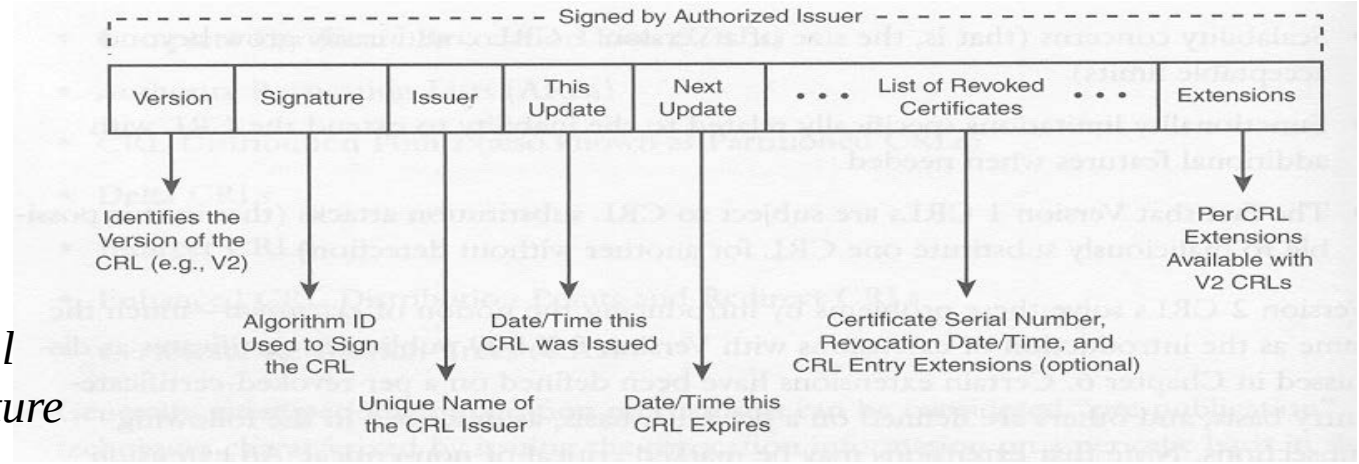
- Relying Party (RP):
  - Anyone who relies on the use of a certificate. (relies on the bindings)
  - A.k.a. Certificate User
  - A.k.a. Certificate-Using System



PKI Terminology

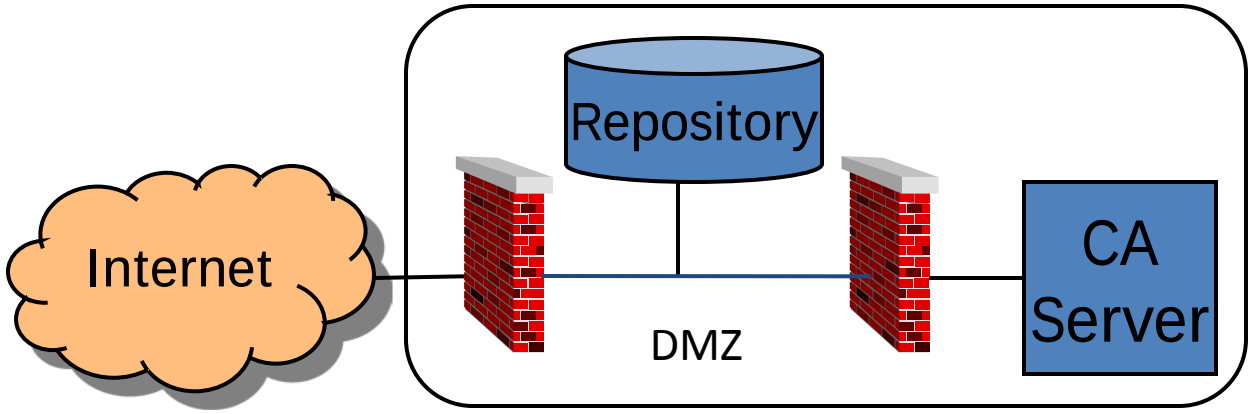
- Certificate Revocation List (CRL):
  - An digitized list that asserts certain previously-issued X.509 certificates have been revoked or have been placed on hold.





PKI Terminology

- Repository:
  - A system for storing and distributing digital certificates and related information (including CRLs, CPSs, and certificate policies) to certificate users (i.e., relying parties).

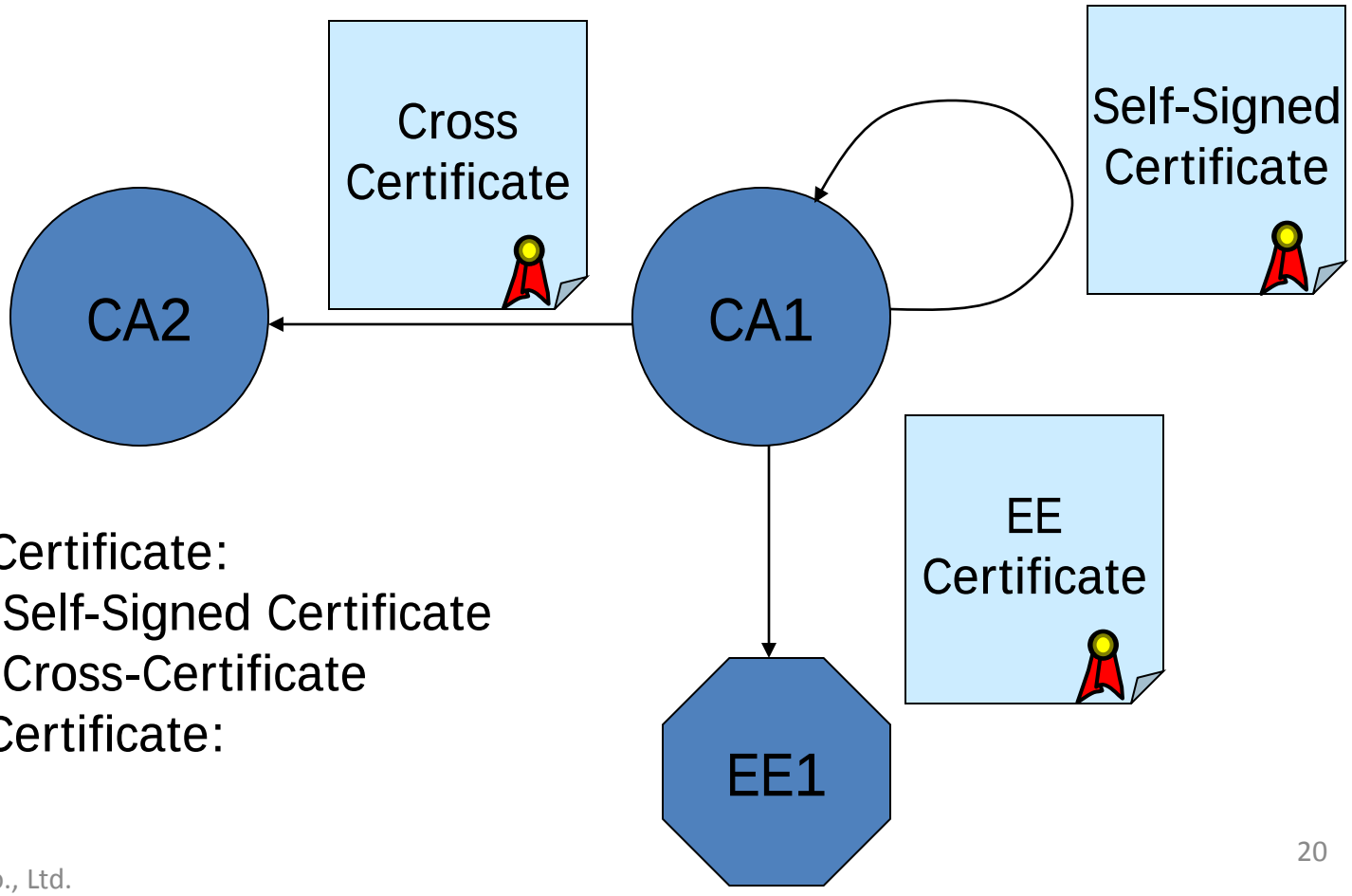


Part 2

PKI TRUST MODEL

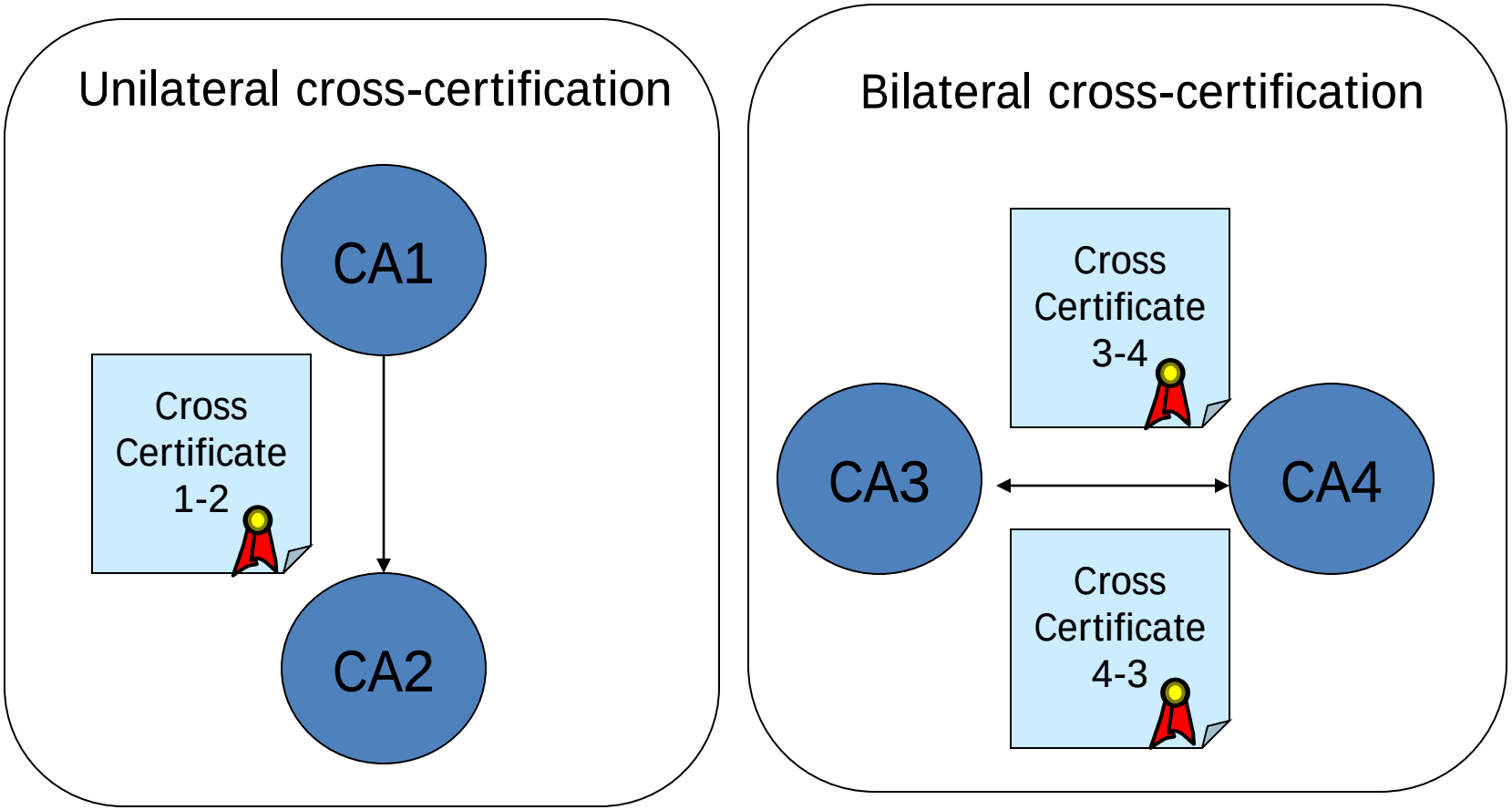
Certificate represents trust

- Type of certificates

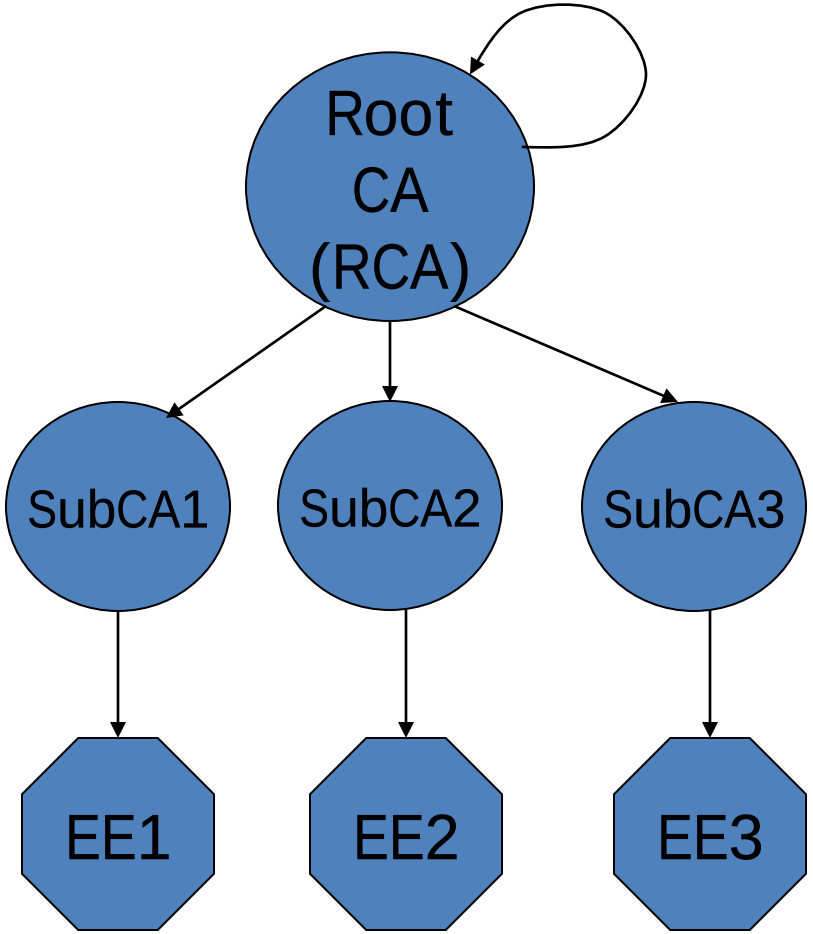


1. CA Certificate:
   - Self-Signed Certificate
   - Cross-Certificate
2. EE Certificate:

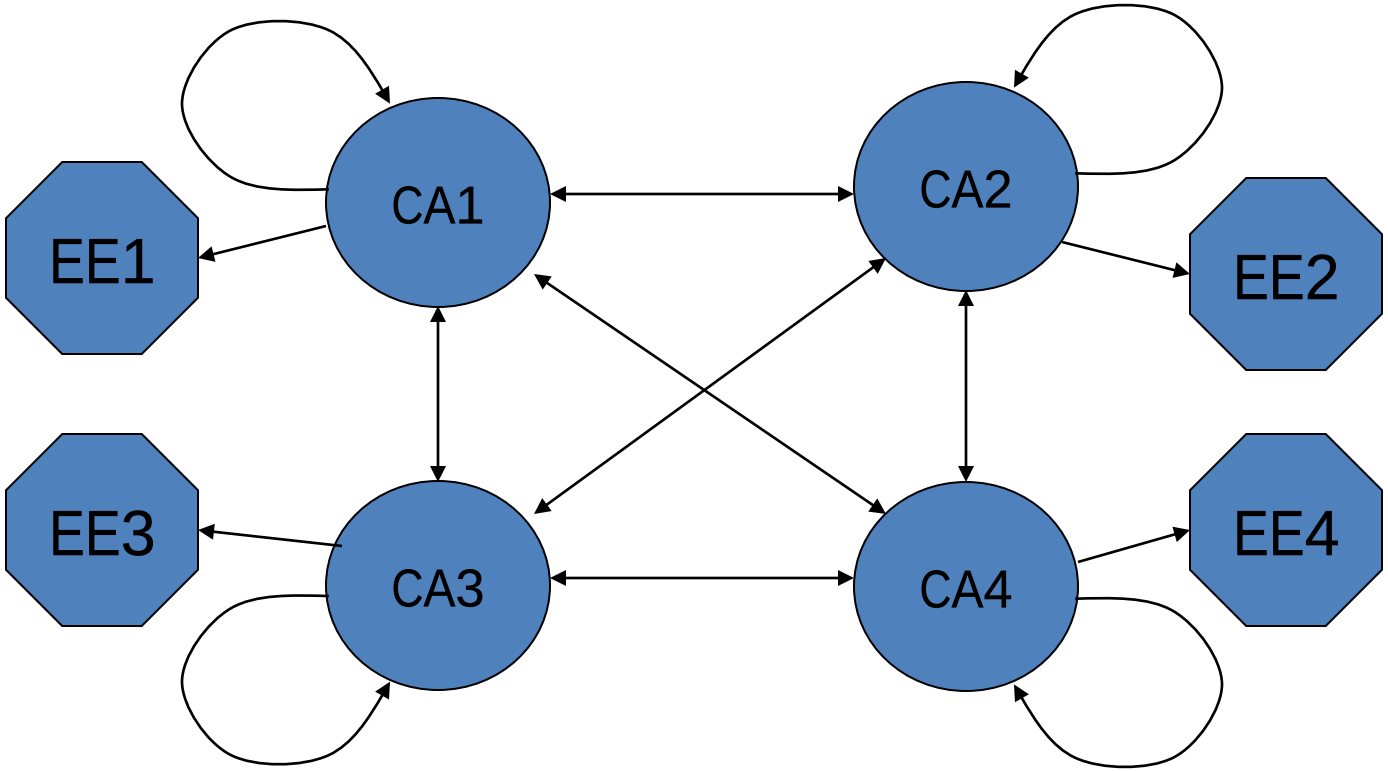
CA-CA Trust Relationship



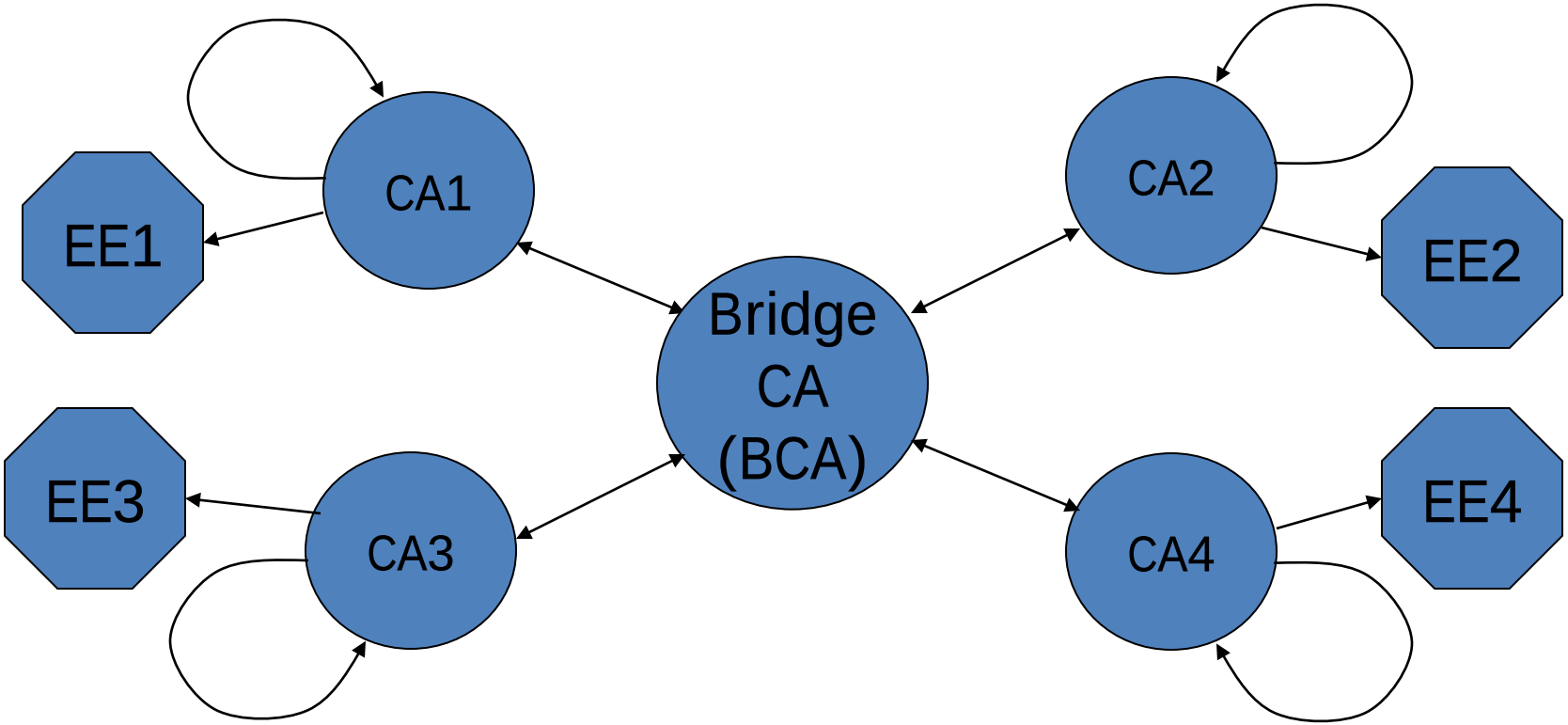
PKI Trust Model: Hierarchy



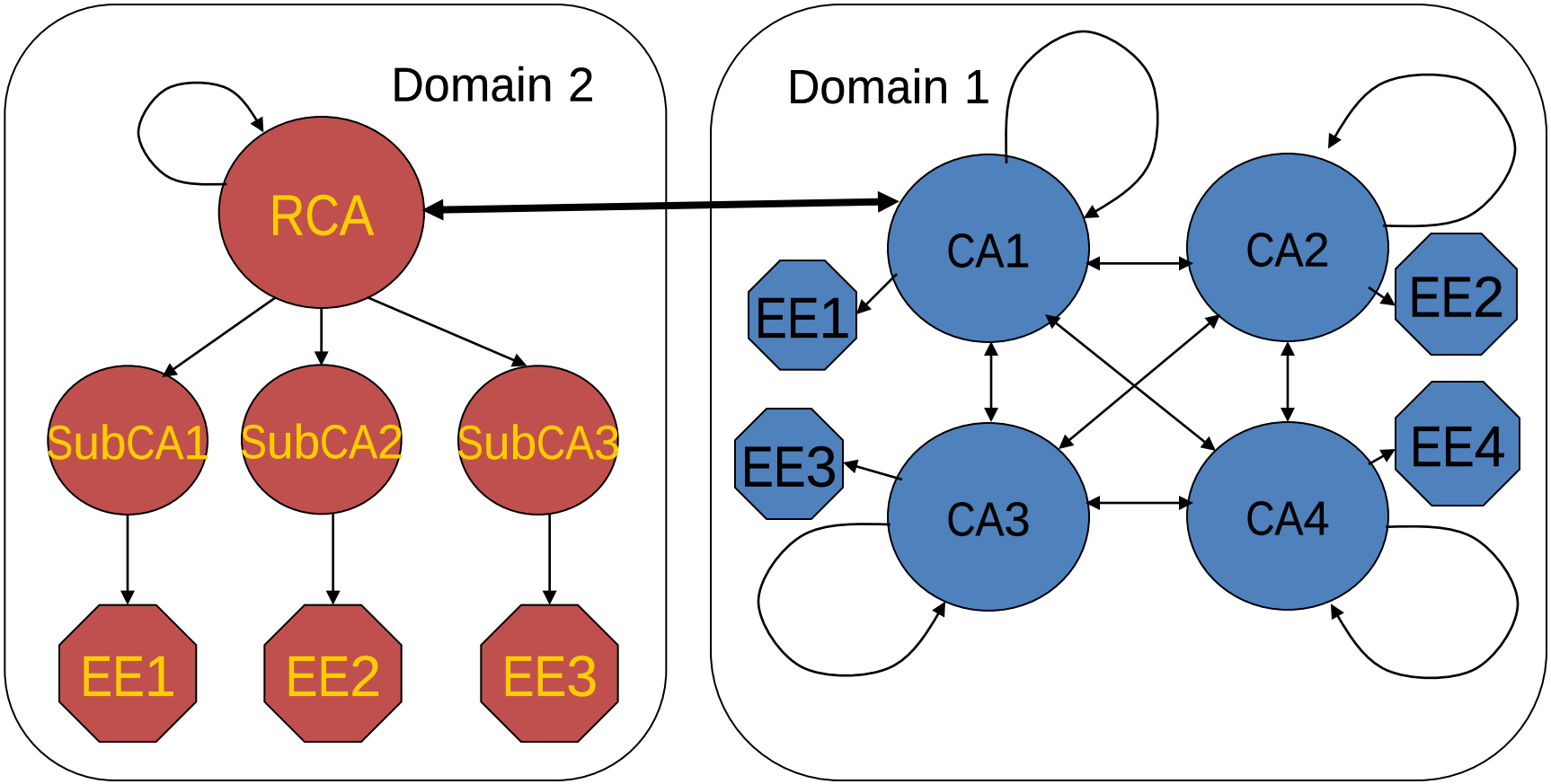
PKI Trust Model: Mesh



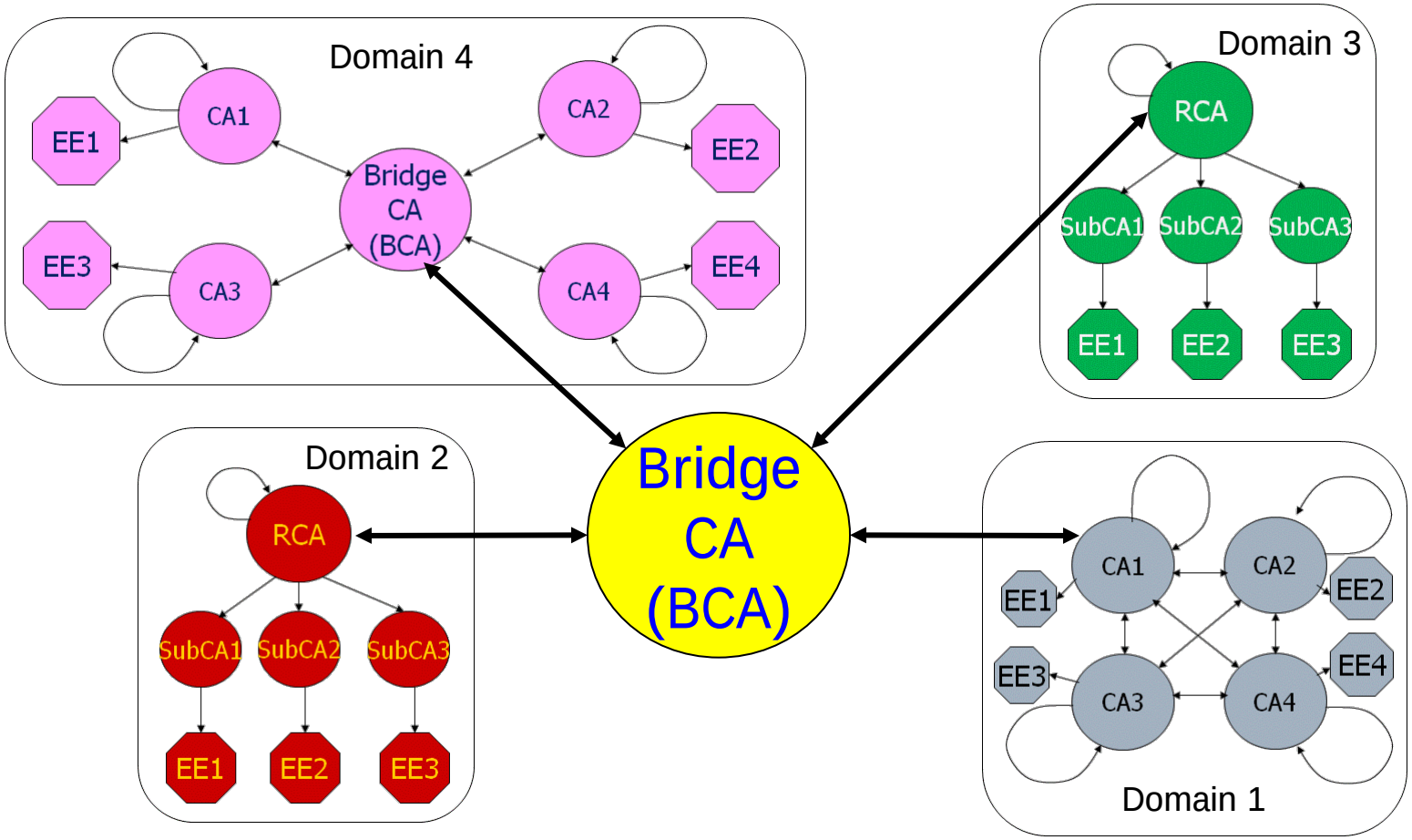
PKI Trust Model: Bridge



PKI Trust Model: Inter-Domain

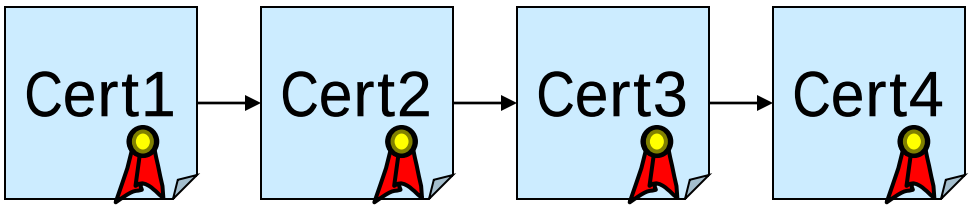


PKI Trust Model: Inter-Domain with Bridge

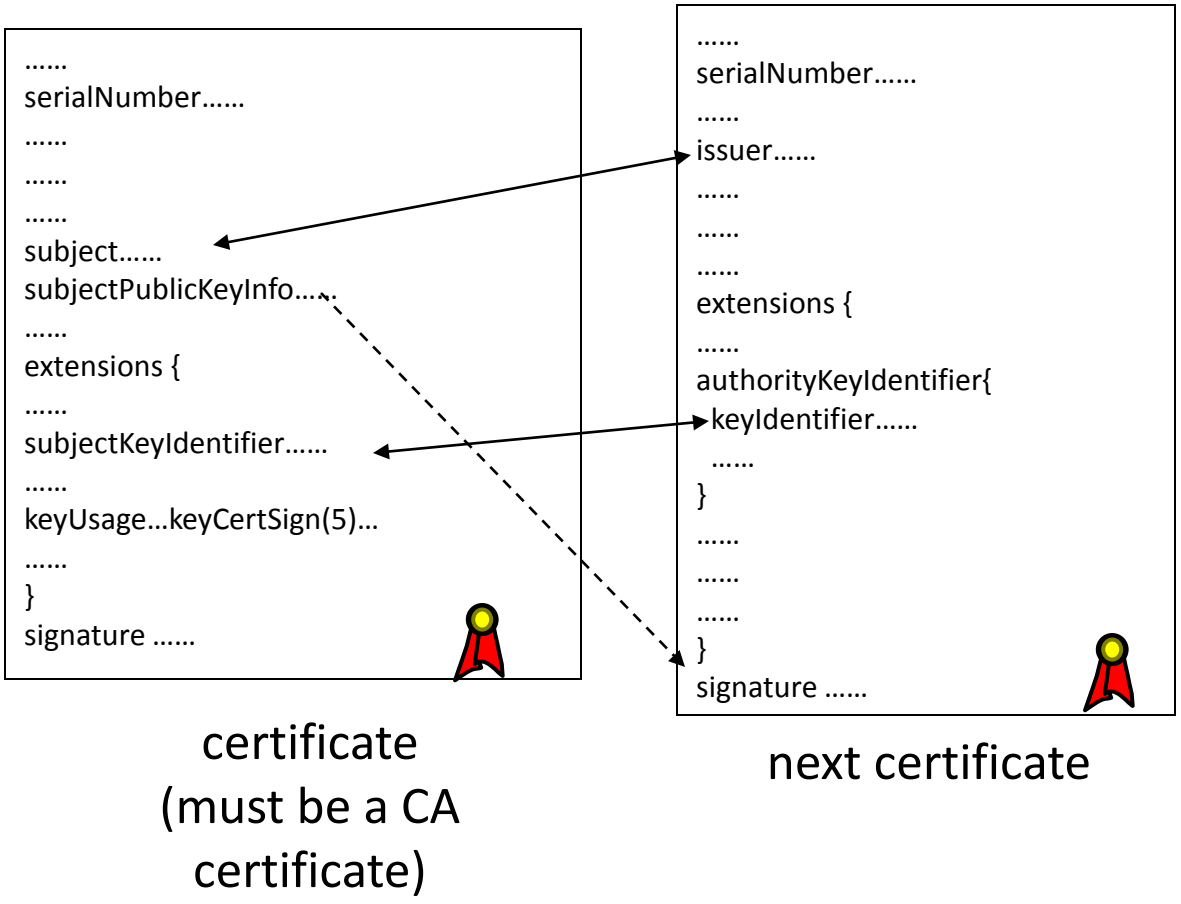


Certification Path

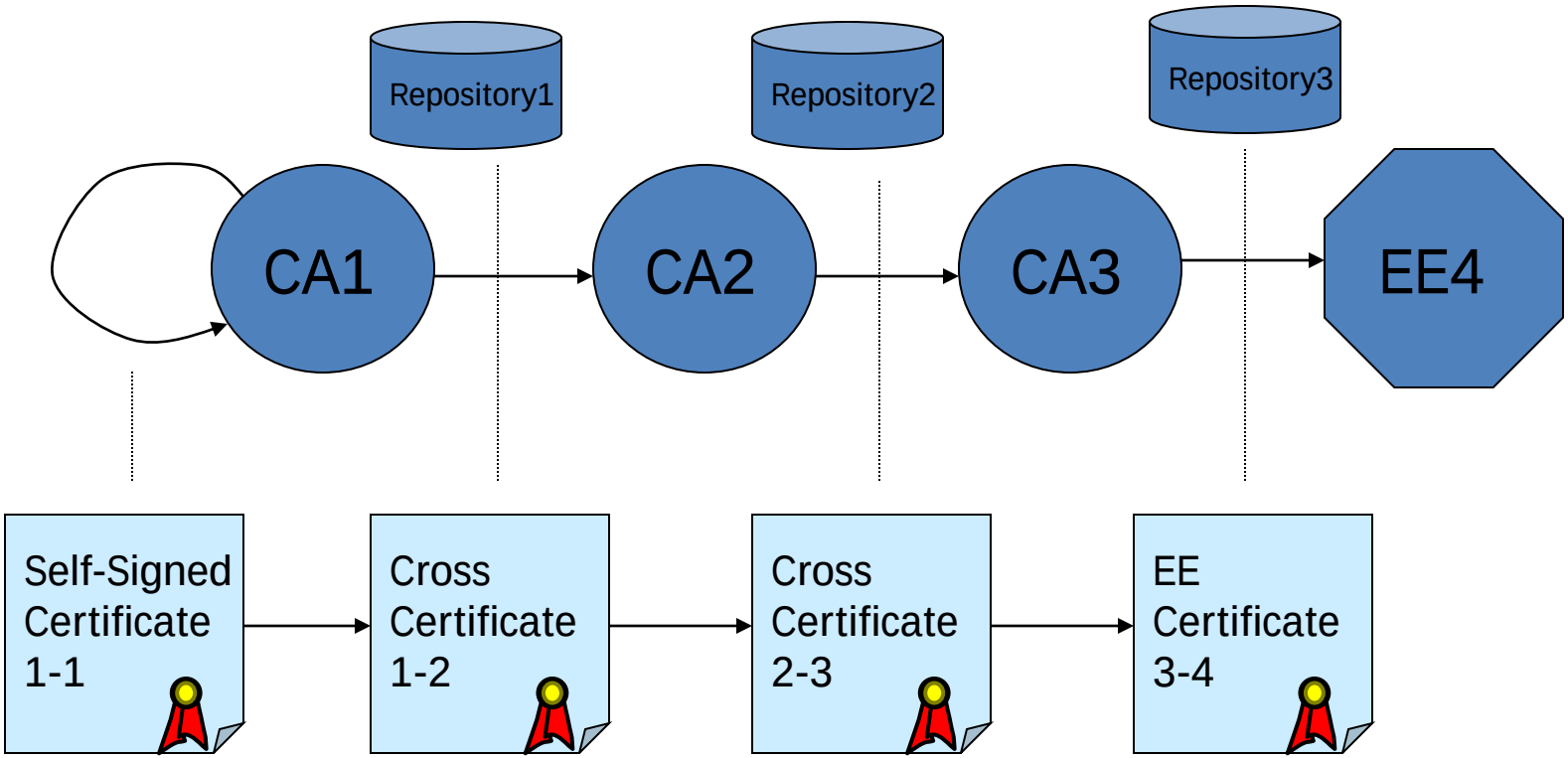
- A.k.a. Certificate Chain
  - An ordered sequence of public-key certificates with the following relationship between a certificate ($Cert_n$) and its next certificate ($Cert_{n+1}$)
    - ✓ Subject Name of $Cert_n$= Issuer Name of $Cert_{n+1}$
    - ✓ Subject Key Identifier of $Cert_n$=Authority Key Identifier $Cert_{n+1}$ (Optional)
    - ✓ The signature of $Cert_{n+1}$ is verifiable by the subject public key of $Cert_n$.



Close-up of Certification Path

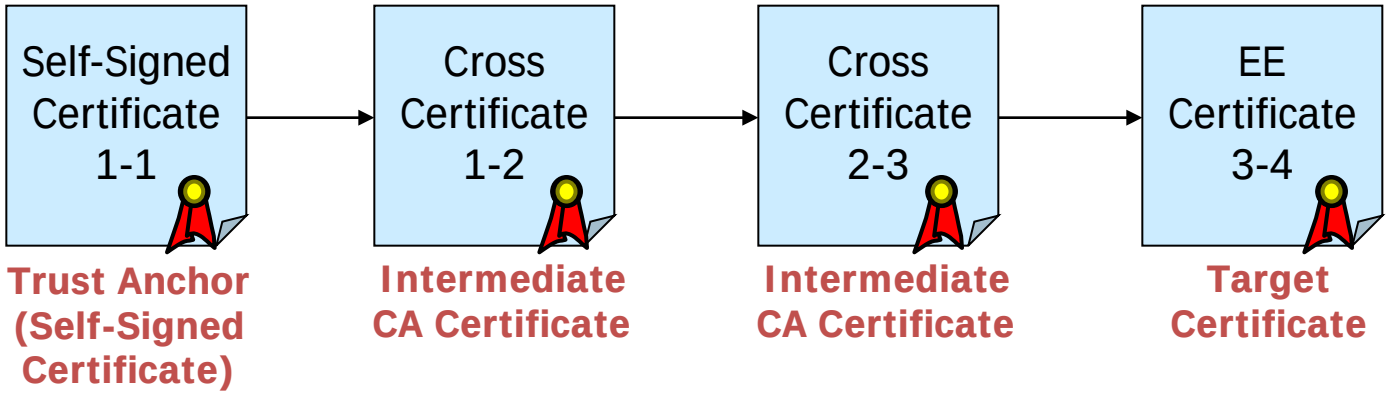


Certification Path represents chain of trust



Trust Anchor, Intermediate CA, Target Certificates

- Trust Anchor：The CA directly trusted by the relying party. (Normally be the Root CA.)
- Intermediate CA certificate: any cross-certificate between the trust anchor and the target certificate.
- Target certificate: the certificate that the relying party intends to use (to trust).



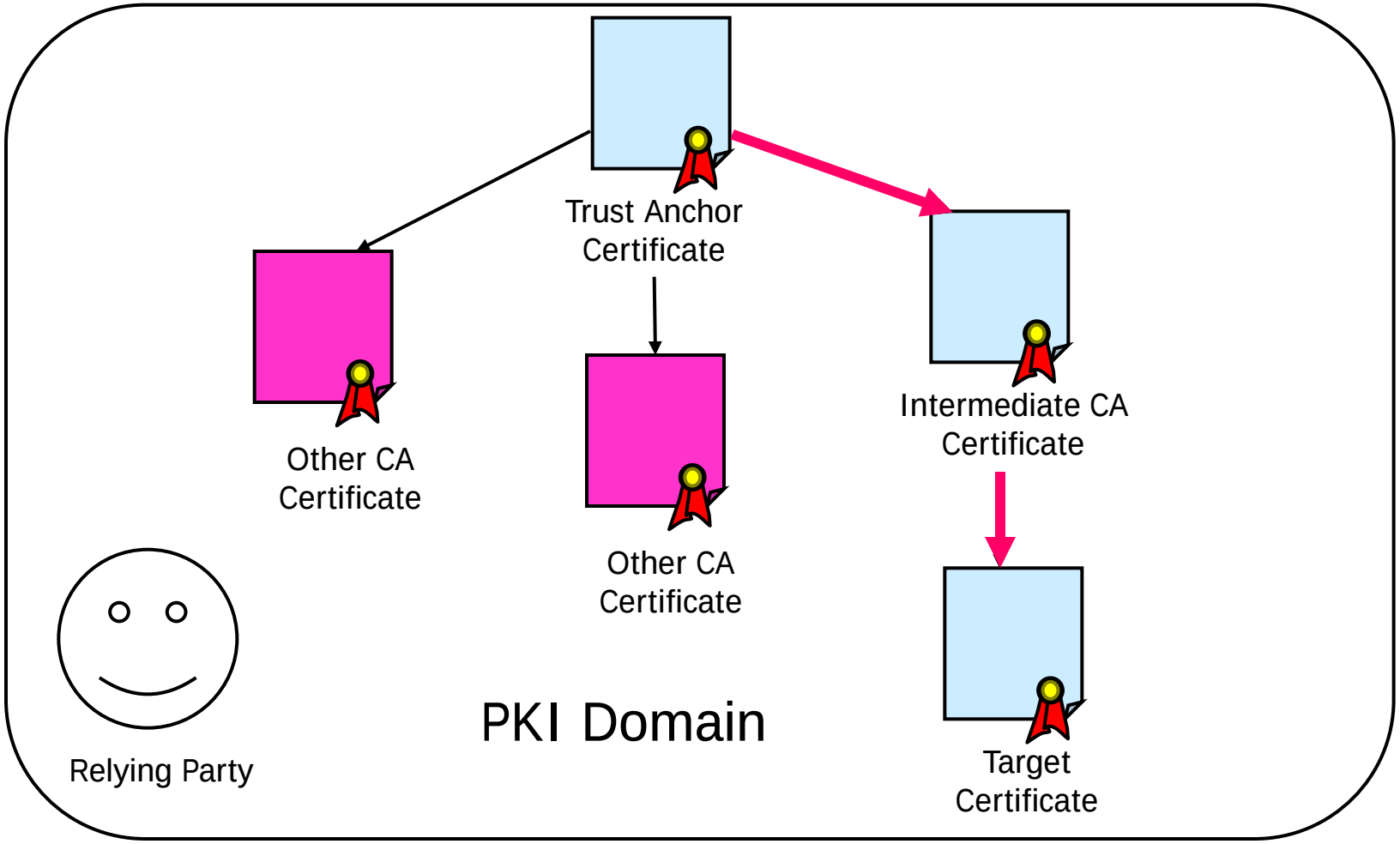
The way to make sure a certificate is trustworthy

- Certification Path Processing is the way a RP make sure a target certificate is trustworthy:
- Includes two phases:
  - Certification Path Construction
  - Certification Path Validation

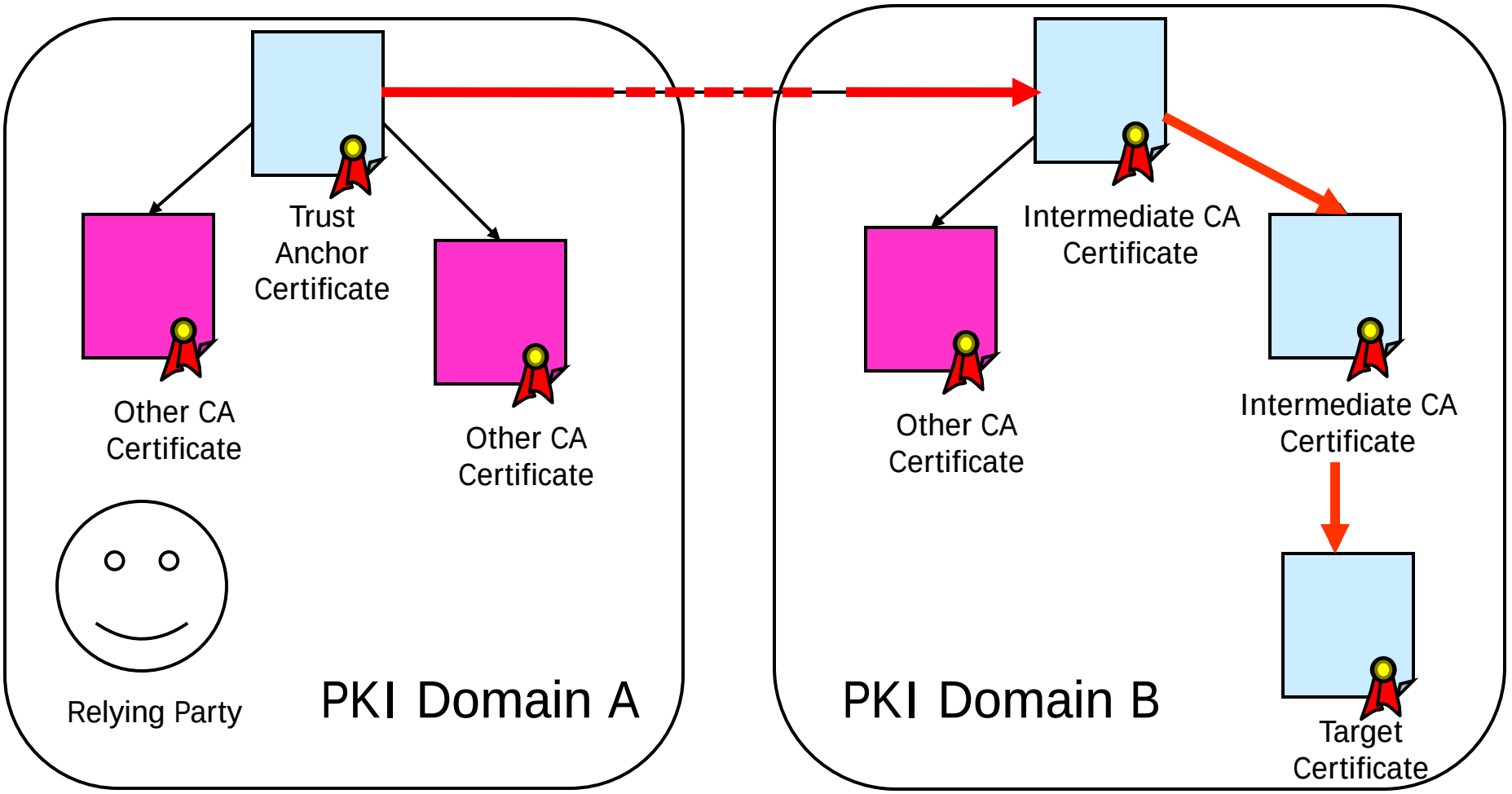
Certification Path Processing

- Certification Path Construction
  - A.k.a. Path Building, Path Finding, or Path Discovery.
  - The process of finding one or more certification paths between trust anchors to the target certificate.
- Certification Path Validation
  - The process of validating (a) the signatures and status of all certificates in a certification path and (b) the required relationships (such as Policy Mappings, Policy Constraints, Name Constraints, etc.) between those certificates, thus validating the contents of the last certificate on the path.

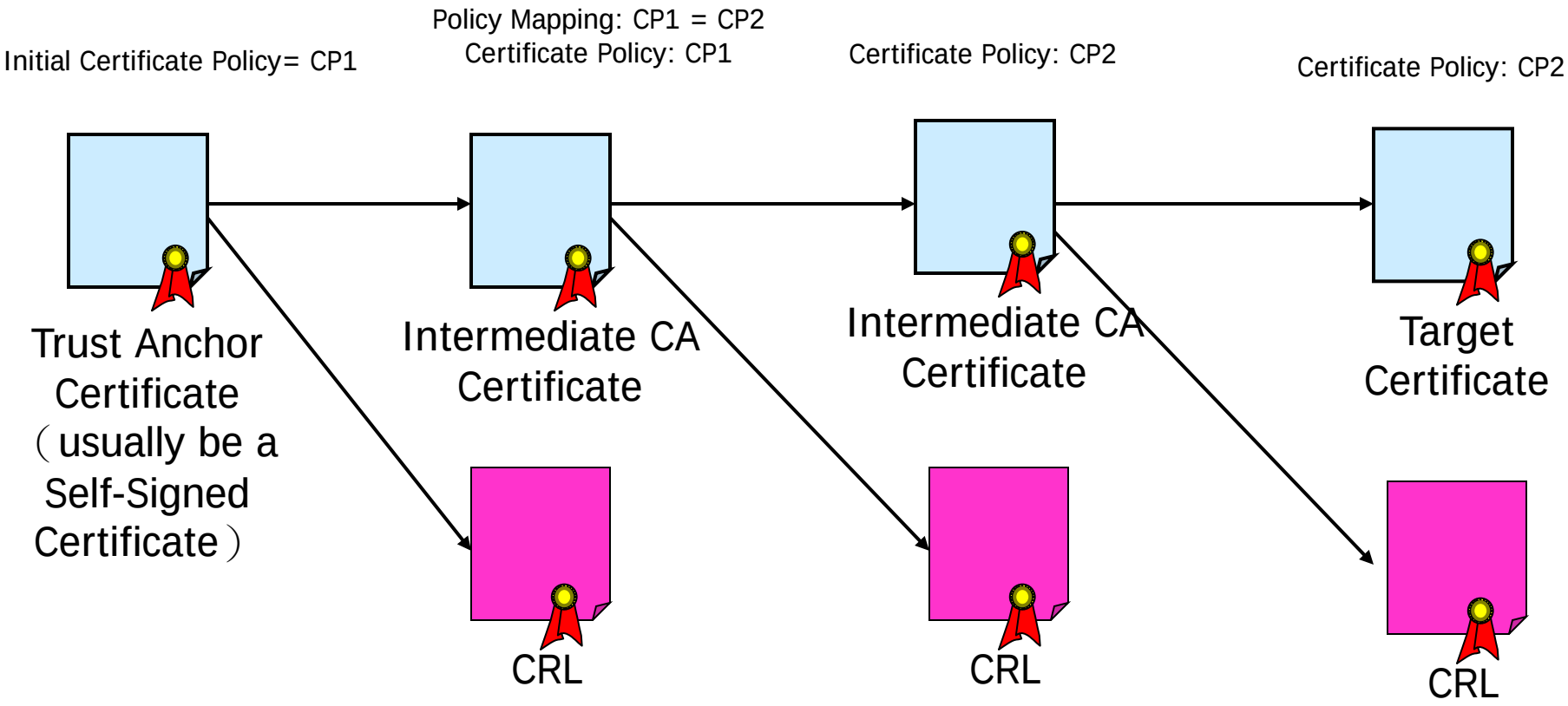
Certification Path Construction – intra-domain



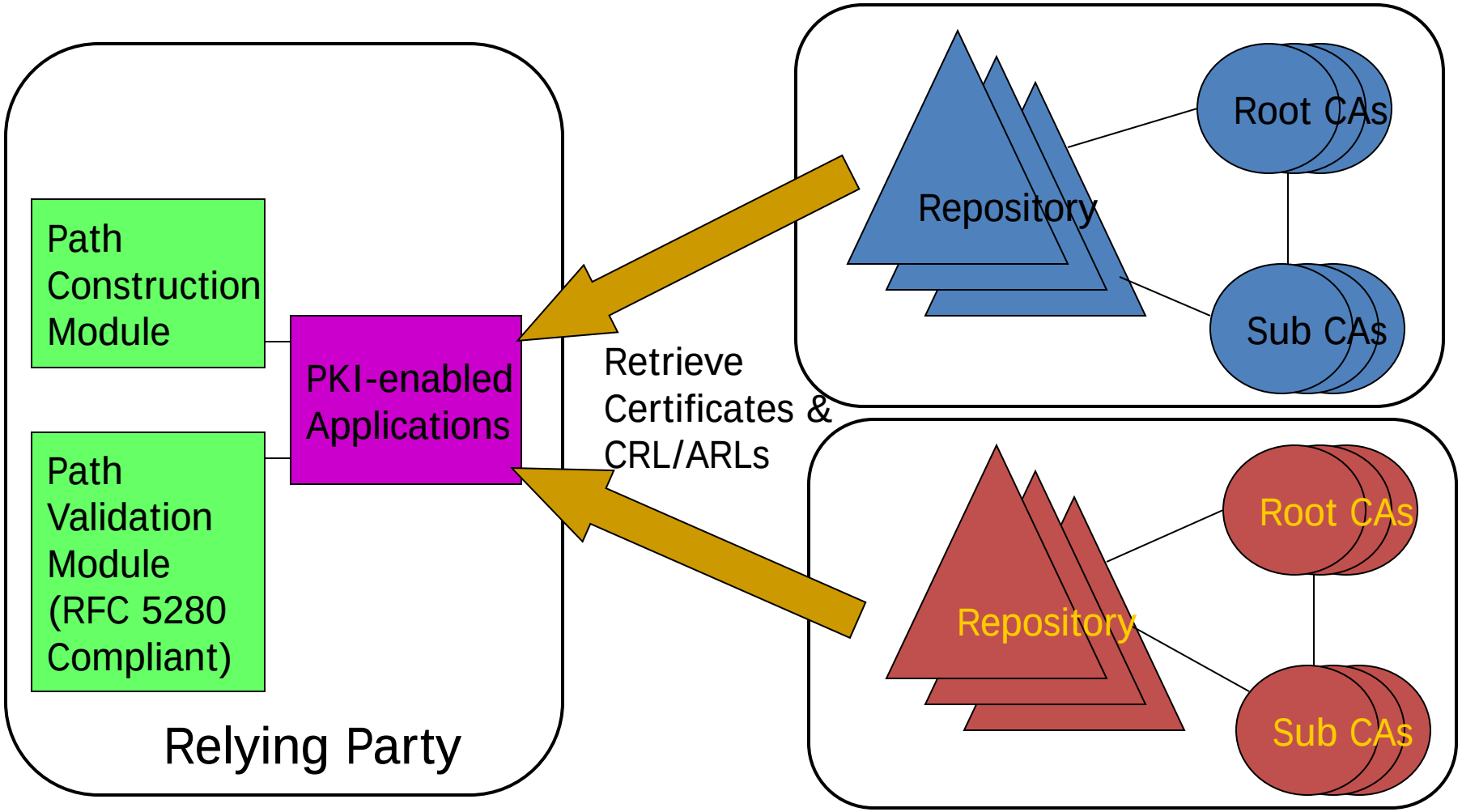
Certification Path Construction – inter-domain



Certification Path Validation



How a RP performs certification path processing



Part 3

PKI ESTABLISHMENT: STEP BY STEP

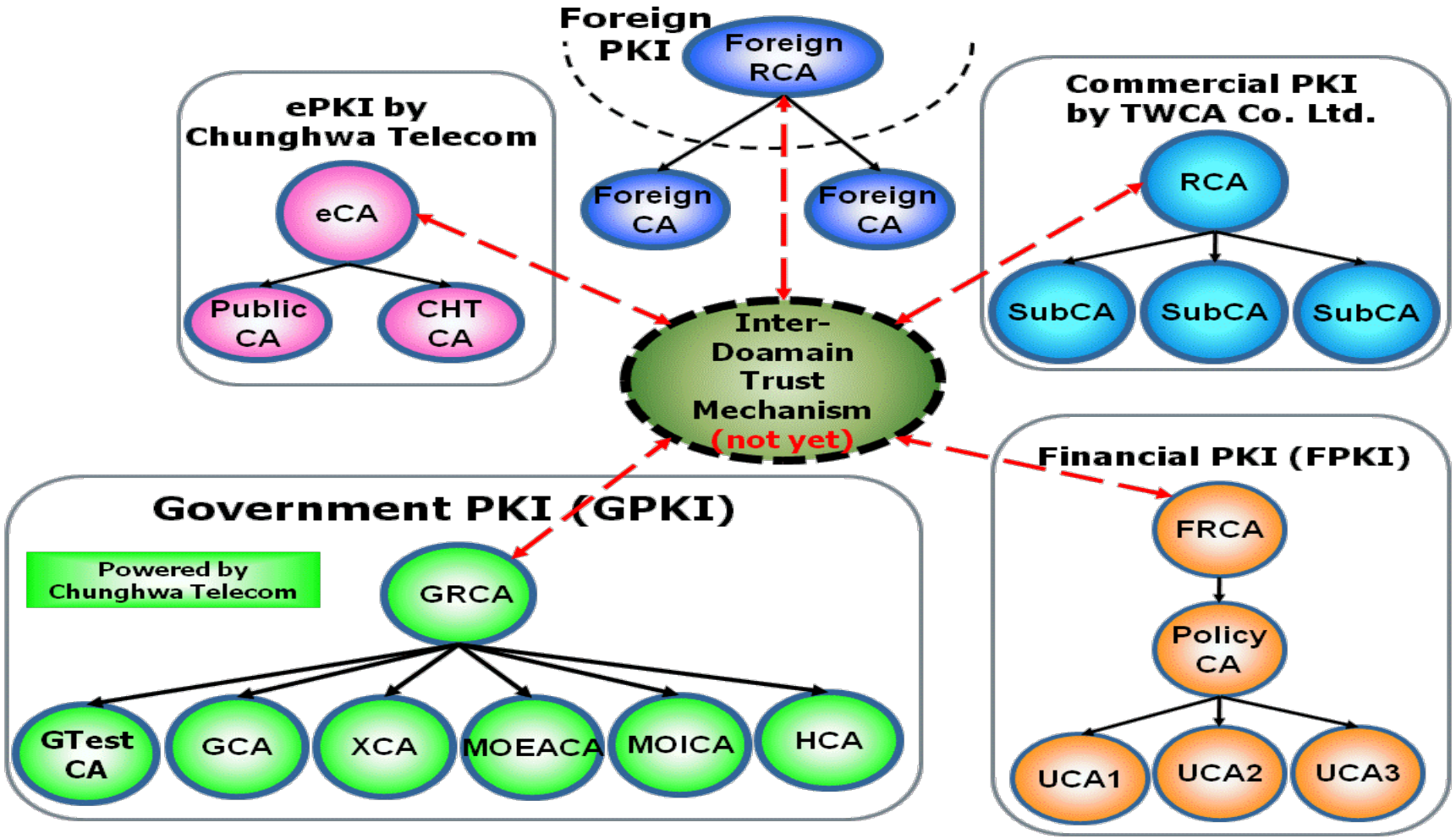
Step 1: Legislation for PKI

- What laws need to be legislated or amended?
  - Electronic Signature Act
  - Digital Signature Act
  - Electronic Transactions Act
  - Electronic Commerce Act
  - Electronic Government Act
- Will the law regulate the establishment, operations, liability of CA?
- What about Encryption Certificates?

Step 2: Choose PKI Trust Model

- What is the most suitable PKI Trust Model for your country/organization?
  - Hierarchy
    - Single Root CA for the whole nation?
  - Mesh
  - Bridge
  - Multiple PKI Domain with Bridge
  - Multiple Independent PKI Domain (a.k.a. Trust List, Multiple Trust Anchors)
    - Trust List is usually application-specific (or RP-specific).

Architecture of Taiwan PKI



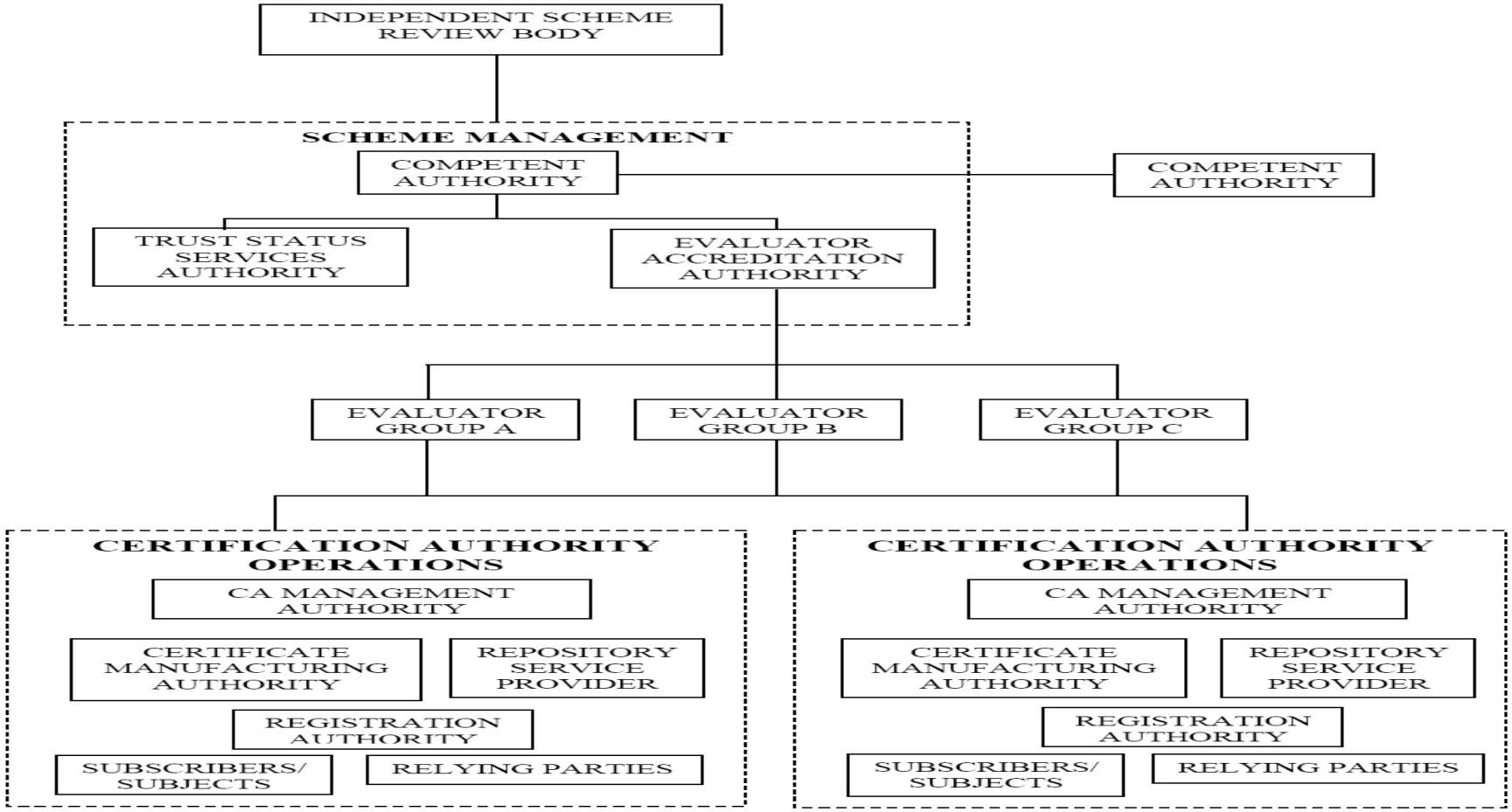
Step 3: Establish CA Accreditation Scheme

- What are the criteria for an entity to be approved (licensed) for establishing a CA?
  - Must be incorporated or be a government agency
  - Has enough capital
  - Conforms to CP/CPS
  - Passes CA audit (such as WebTrust for CA)
- Will the CA Accreditation be voluntary or mandatory (enforced by the law)?

Accreditation vs. Certification

- Accreditation Body - An organization (usually a recognized national authority) that checks certification bodies and, provided their certification assessment processes pass muster, accredits them *i.e.* grants them the authority to issue recognized certificates.
- Certification Body - An organization or individual that assesses the subject (may be an organization or individual) and, provided that it conforms to the requirements specified in the standard, issues a certificate to it.

APEC Model of CA Accreditation Scheme



Step 4: Define Certificate Profiles

- What kinds of entities needs certificates?
  - Individuals (citizens, resident foreigners, professionals, government employees)
  - Organization (certification authorities themselves, government agencies, businesses, not-for-profit organizations)
  - Applications (SSL servers, timestamp servers, OCSP servers, …)
  - Devices (VPN gateways, IPsec devices, …)
- To improve interoperability, you should document formats of all certificates in your PKI in detail. That is certificate profiles.

What is a “profile”?

- In standardization, a profile consists of an agreed-upon subset and interpretation of a specification.
- Many complex technical specifications have many optional features, such that two conforming implementations may not inter-operate due to choosing different sets of optional features to support.
- Even when no formal optional features exist within a standard, vendors will often fail to implement (or fail to implement correctly) functionality from the standard which they view as unimportant.

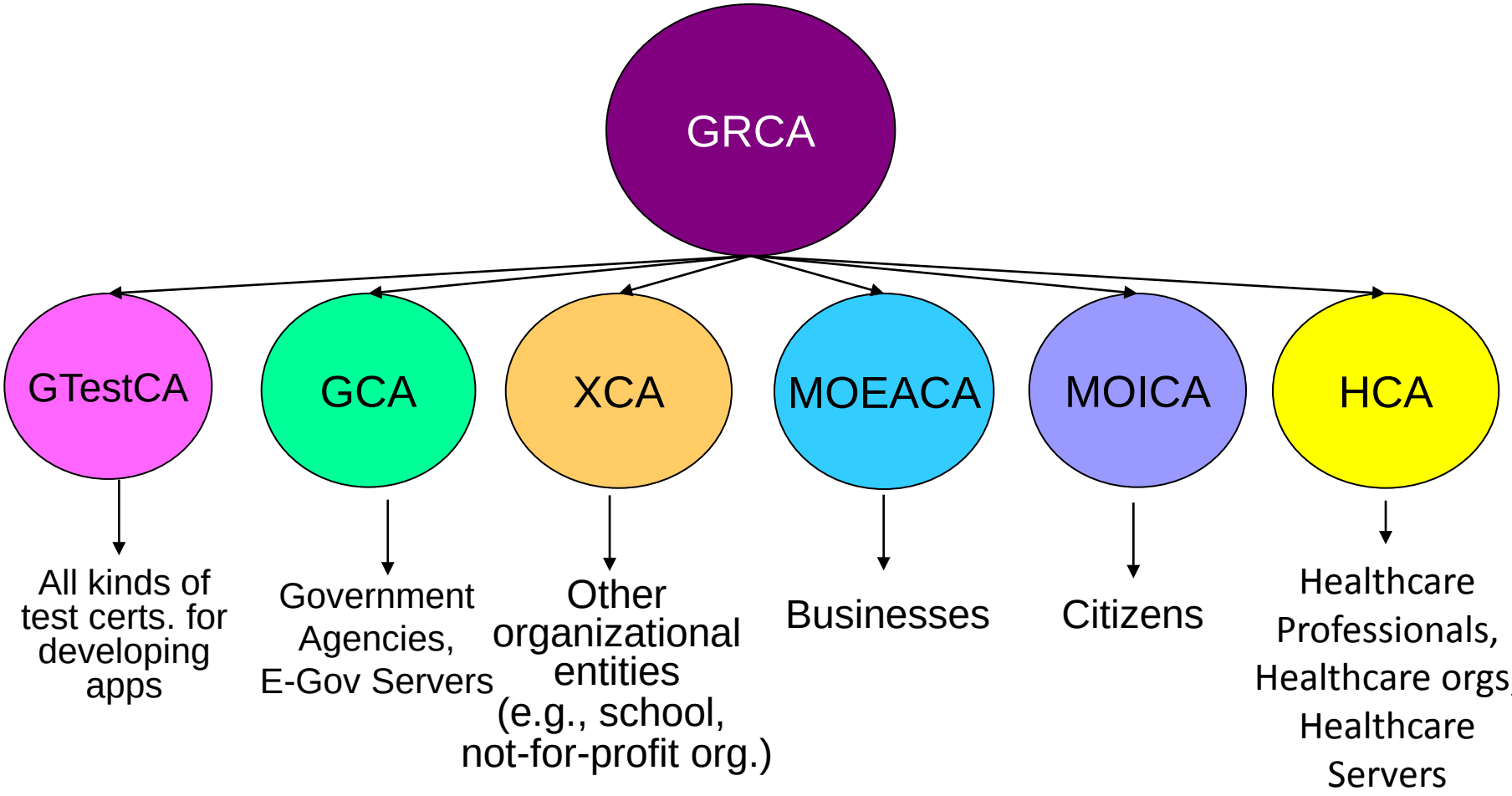
(from Wikipedia)

What is a “profile”? (cont)

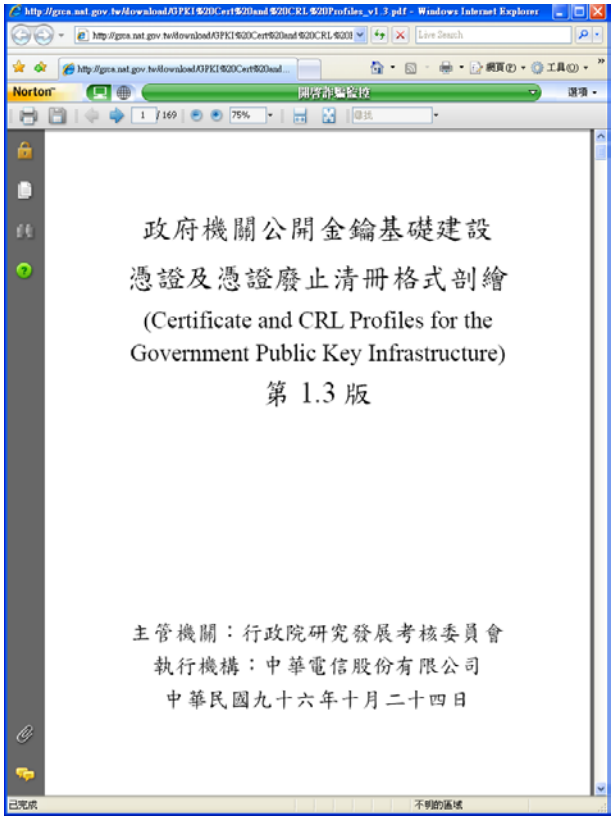
- Also, some writers of standards sometimes produce vague or ambiguous specifications, often unintentionally, but sometimes by intention. The use of profiles can enforce one possible interpretation.
- Users can utilize profiles to ensure interoperability, and in procurement.
- In some cases, profiles themselves can become standardized.

(from Wikipedia)

Types of End-Entities in Taiwan GPKI



Example of Certificate Profiles



政府機關公開金鑰基礎建設

憑證及憑證廢止清冊格式剖繪

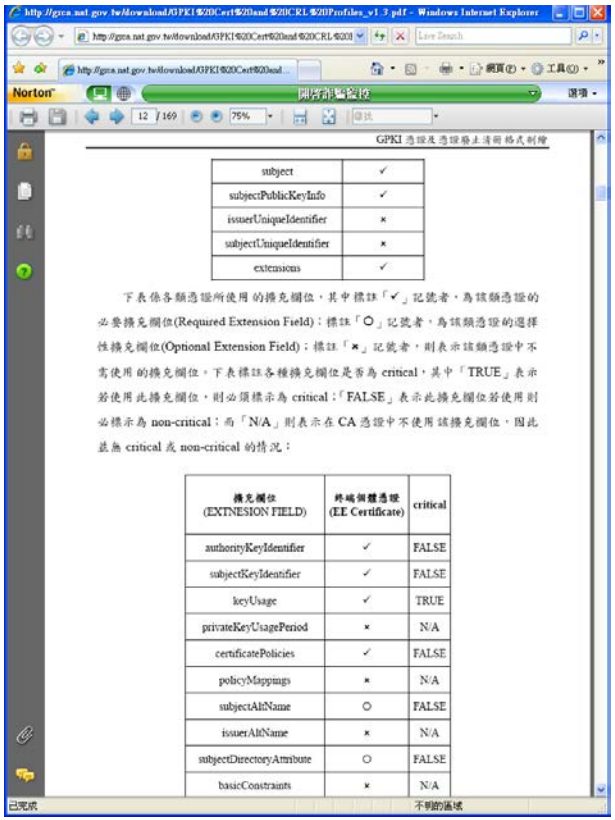
(Certificate and CRL Profiles for the Government Public Key Infrastructure)

第 1.3 版

主管機關：行政院研究發展考核委員會

執行機構：中華電信股份有限公司

中華民國九十六年十月二十四日

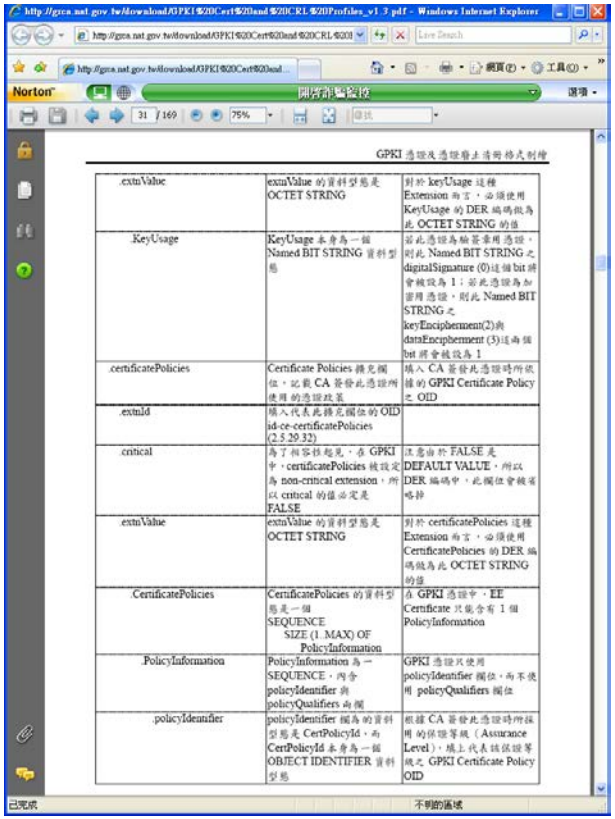


GPKI 憑證及憑證廢止清冊格式剖繪

subject	✓
subjectPublicKeyInfo	✓
issuerUniqueIdentifier	×
subjectUniqueIdentifier	×
extensions	✓

下表係各類憑證所使用的擴充欄位，其中標註「✓」記號者，為該類憑證的必要擴充欄位(Required Extension Field)；標註「○」記號者，為該類憑證的選擇性擴充欄位(Optional Extension Field)；標註「×」記號者，則表示該類憑證中不需使用的擴充欄位。下表標註各種擴充欄位是否為 critical，其中「TRUE」表示若使用此擴充欄位，則必須標示為 critical；「FALSE」表示此擴充欄位若使用則必標示為 non-critical；而「N/A」則表示在 CA 憑證中不使用該擴充欄位，因此並無 critical 或 non-critical 的情況：

擴充欄位 (EXTNESION FIELD)	終端個體憑證 (EE Certificate)	critical
authorityKeyIdentifier	✓	FALSE
subjectKeyIdentifier	✓	FALSE
keyUsage	✓	TRUE
privateKeyUsagePeriod	×	N/A
certificatePolicies	✓	FALSE
policyMappings	×	N/A
subjectAltName	○	FALSE
issuerAltName	×	N/A
subjectDirectoryAttributes	○	FALSE
basicConstraints	×	N/A



GPKI 憑證及憑證廢止清冊格式剖繪

.extnValue	extnValue 的資料型態是 OCTET STRING	對於 keyUsage 這種 Extension 而言，必須使用 KeyUsage 的 DER 編碼後為此 OCTET STRING 的值
.KeyUsage	KeyUsage 本身為一個 Named BIT STRING 資料型態	若此憑證為驗簽專用憑證，則此 Named BIT STRING 之 digitalSignature (0)這個 bit 將會被設為 1；若此憑證為加密用憑證，則此 Named BIT STRING 之 keyEncipherment(2)與 dataEncipherment (3)這兩個 bit 將會被設為 1
.certificatePolicies	Certificate Policies 擴充欄位，記載 CA 簽發此憑證所使用的憑證政策	填入 CA 簽發此憑證時所依據的 GPKI Certificate Policy 之 OID
.extnId	填入代表此擴充欄位的 OID id-ce-certificatePolicies (2.5.29.32)	
.critical	為了相容性起見，在 GPKI 中，certificatePolicies 被設定為 non-critical extension，所以 critical 的值必定是 FALSE	注意由於 FALSE 是 DEFAULT VALUE，所以 DER 編碼中，此欄位會被省略掉
.extnValue	extnValue 的資料型態是 OCTET STRING	對於 certificatePolicies 這種 Extension 而言，必須使用 CertificatePolicies 的 DER 編碼後為此 OCTET STRING 的值
.CertificatePolicies	CertificatePolicies 的資料型態是一個 SEQUENCE SIZE (1..MAX) OF PolicyInformation	在 GPKI 憑證中，EE Certificate 只能含有 1 個 PolicyInformation
.PolicyInformation	PolicyInformation 為一 SEQUENCE，內含 policyIdentifier 與 policyQualifiers 兩欄	GPKI 憑證只使用 policyIdentifier 欄位，而不使用 policyQualifiers 欄位
.policyIdentifier	policyIdentifier 欄為的資料型態是 CertPolicyId，而 CertPolicyId 本身為一個 OBJECT IDENTIFIER 資料型態	根據 CA 簽發此憑證時所採用的保證等級 (Assurance Level)，填上代表該保證等級之 GPKI Certificate Policy OID

(in Chinese)

Step 5: Stipulate CP and CPS

- Certificate Policy (CP)
  - 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. [X.509, RFC 3647]
  - Roughly speaking - a “certificate policy” describes the “level of assurance” one can ascribe to a certificate asserting the policy, and the community and applications the certificates are intended to be used for.
- One CP per PKI Domain
- Each CP is assigned an unique identifier (ASN.1 OID) to be asserted in certificates and the CPS to represent the assurance level.

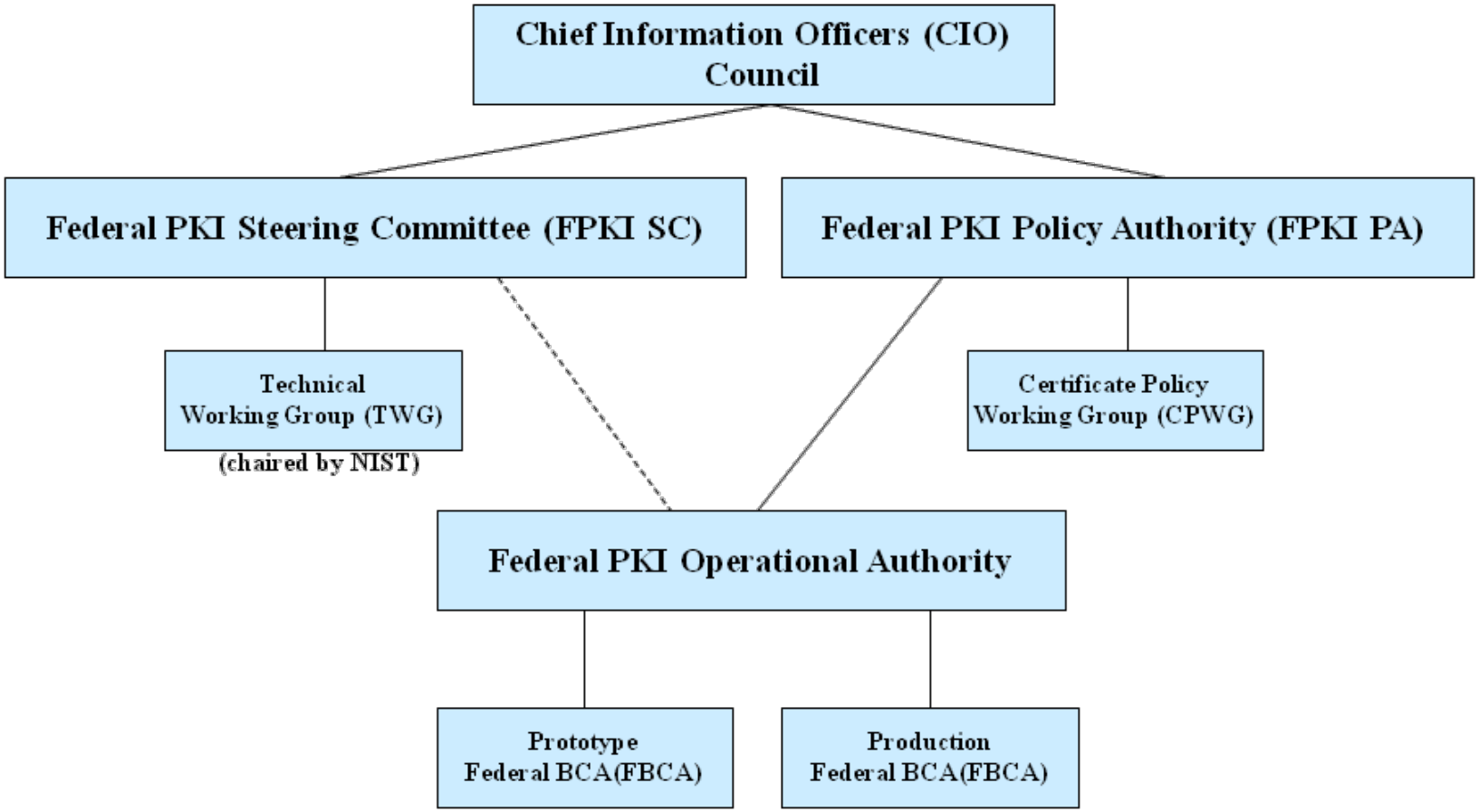
Step 5: Stipulate CP and CPS (cont)

- Certification Practice Statement(CPS)
  - A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates. [RFC 3647, ABA PAG]
  - explain how a CA meets the requirements appearing in the CP
- A CA with a single CPS may support multiple certificate policies.
- Multiple CAs, each with a different CPS, may support the same certificate policy.

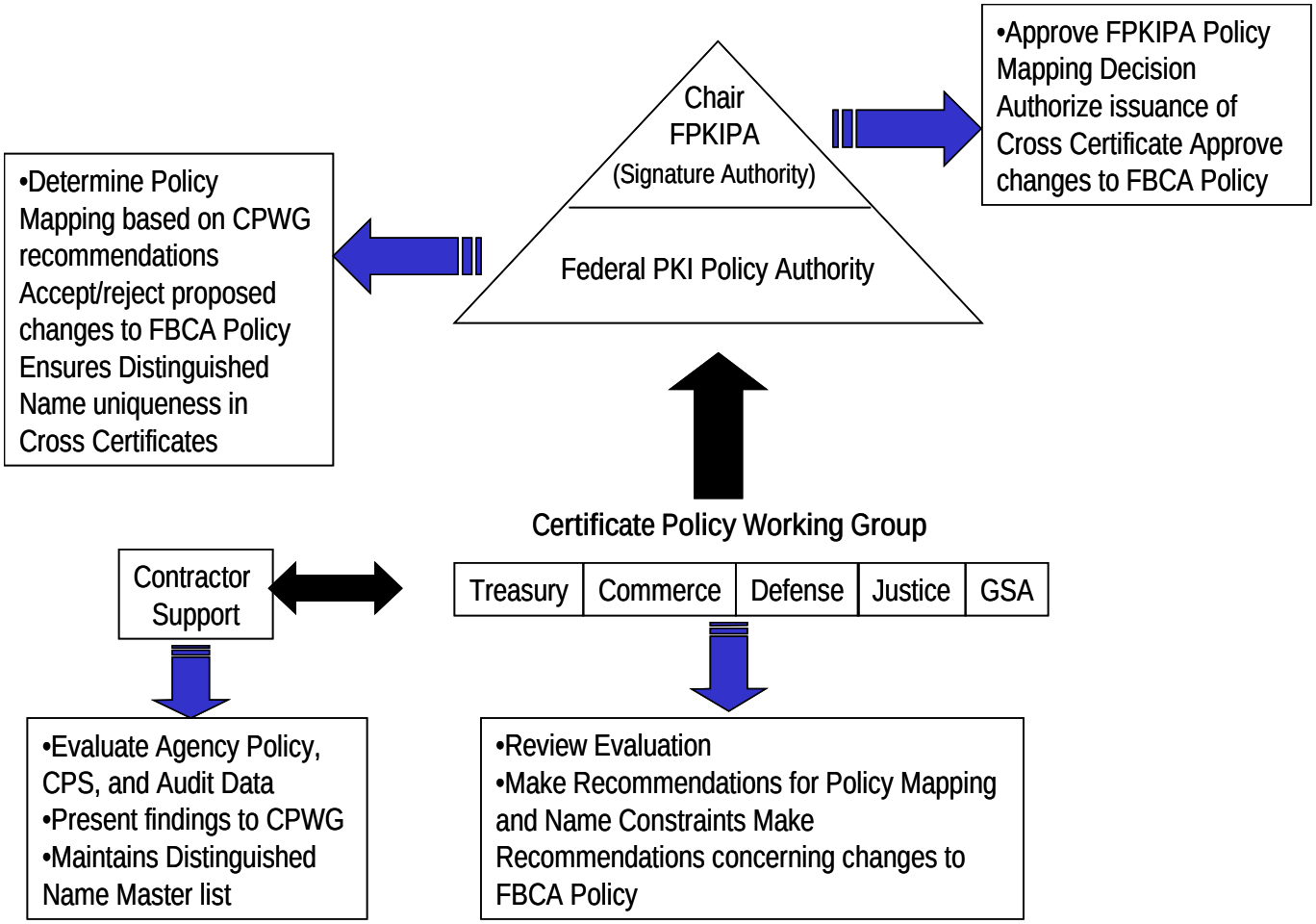
Policy Management Authority(PMA)

- The PMA is responsible for
  - Stipulating or approving the provisions of the CP
  - Stipulating the CPS of the root CA and ensuring its conformance to the CP
  - Accepting applications from other CA desired to become a subordinate CA
  - Ensuring the conformance of the applicant CA's CPS to the CP
  - Ensuring the conformance of the applicant CA's operation to its CPS
  - Negotiating the policy mapping with the PMA of other PKI domain

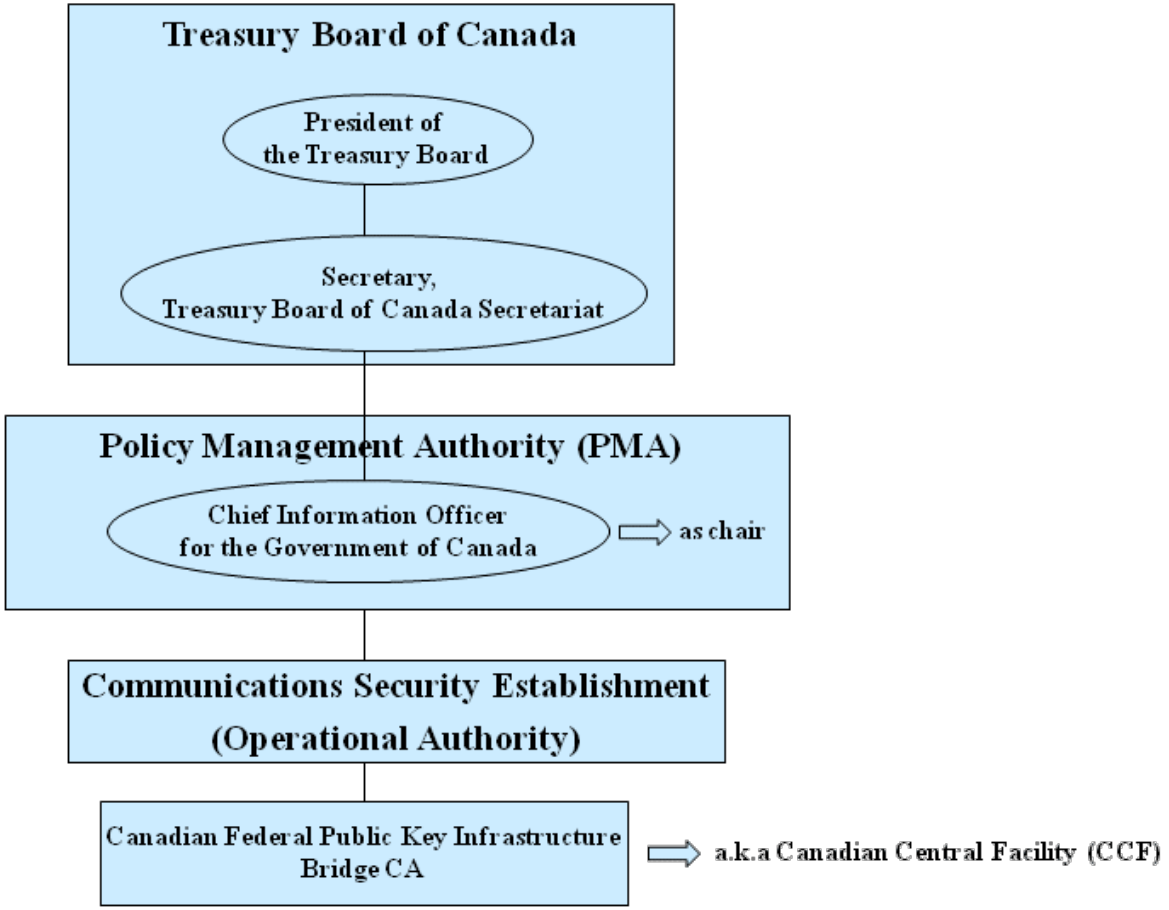
Authorities of US Federal PKI



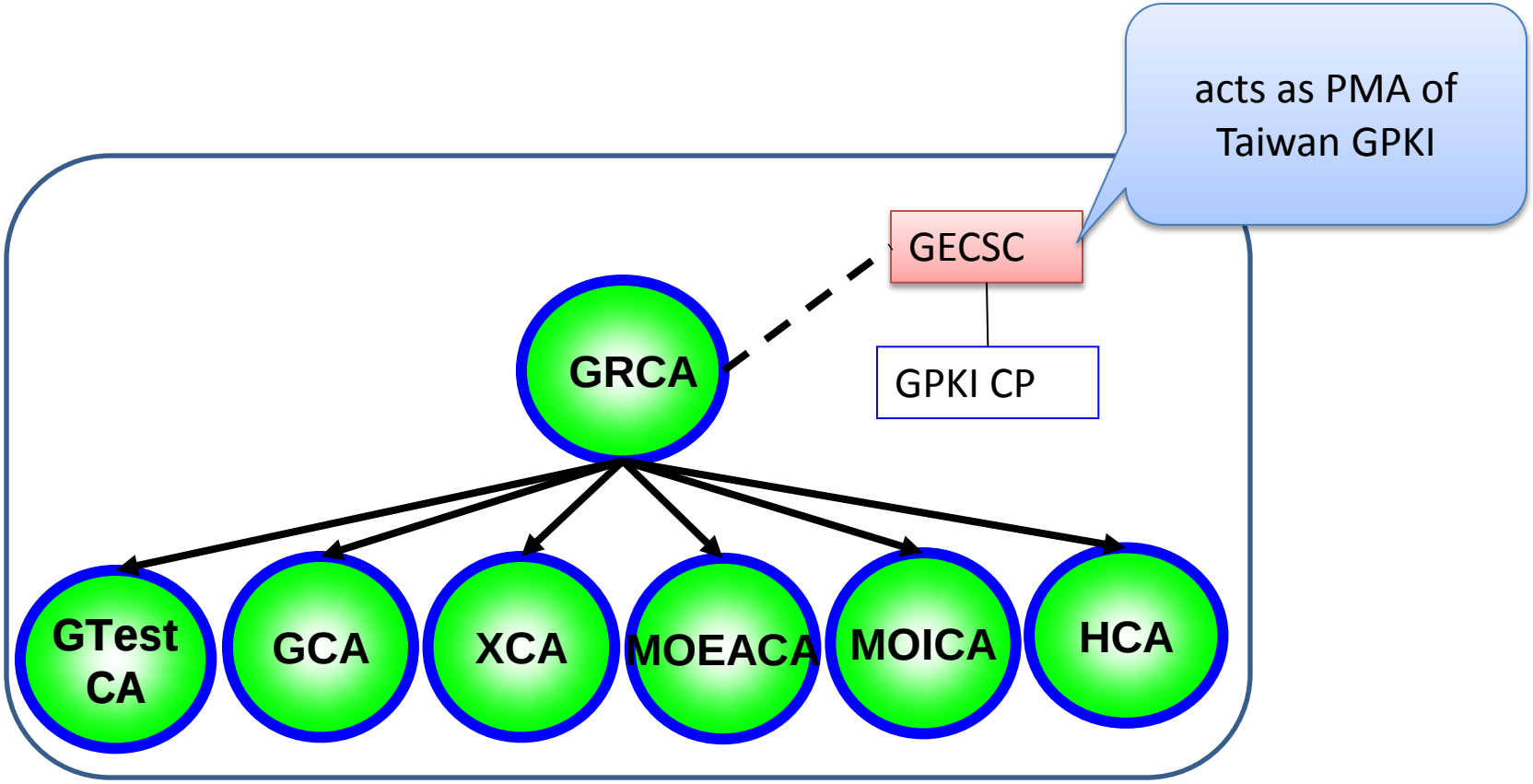
Authorities of US Federal PKI



Authorities of Canada Government PKI



PMA of Taiwan GPKI



GECSC: Government Electronic Certification Steering Commitee

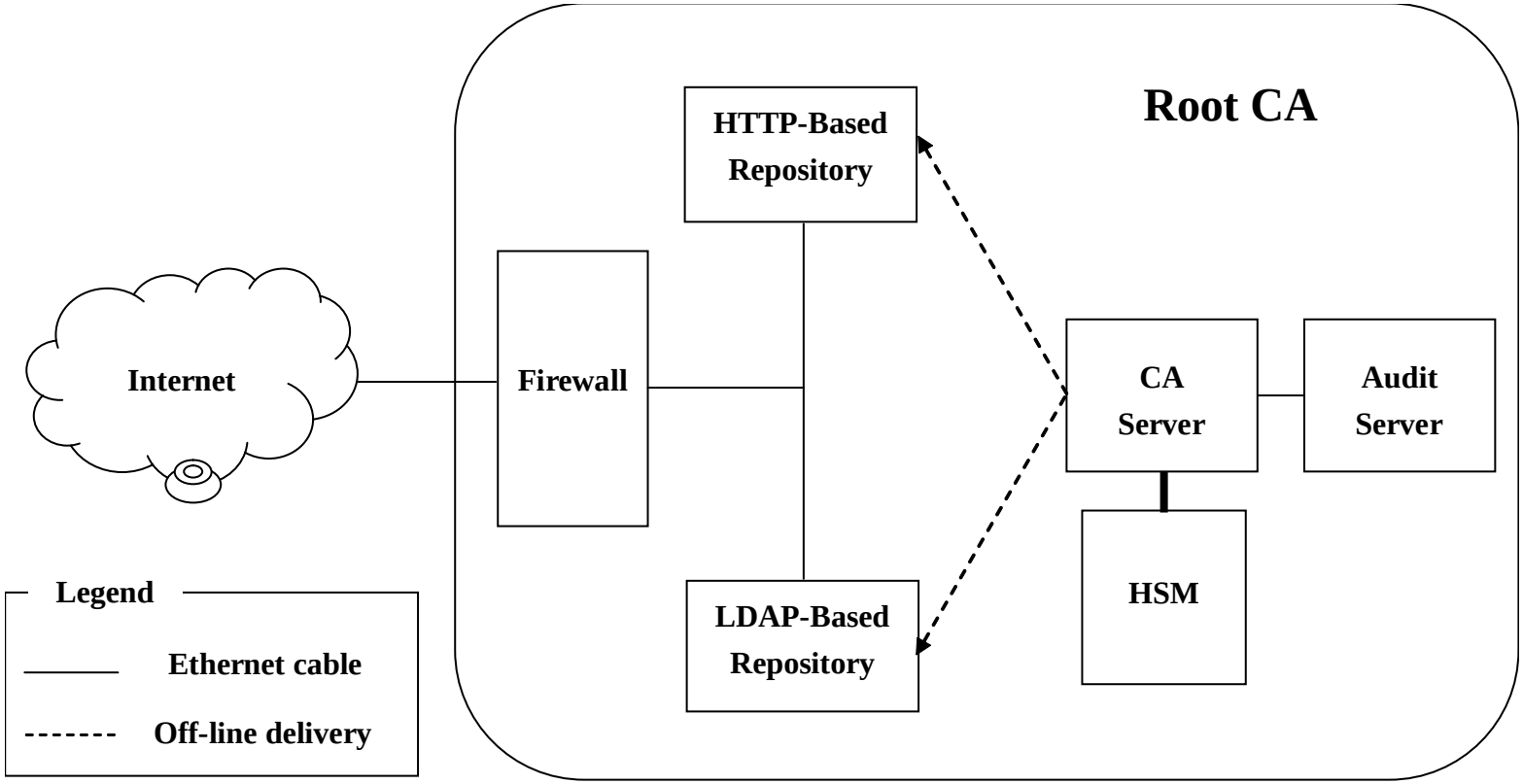
Certificate Policy and Certification Practices Framework

- RFC 3647: Certificate Policy and Certification Practices Framework
  - Define by IETF PKIX WG
  - Obsoletes RFC 2527
  - Aims to explain the concepts of a CP and a CPS, describe the differences between these two concepts, and describe their relationship to subscriber and relying party agreements.
  - Presents a framework to assist the writers and users of certificate policies or CPSs in drafting and understanding these documents.
  - Now, a de facto standard of the document structure of CP and CPS.

Step 6: Establish the Root CA

- The root CA is the trust anchor of the PKI domain if the hierarchical PKI trust model is adopted.
- The characteristics of the root CA is that it only issues a few certificates.
  - Because it only responsible for issuing certificate to the approved subordinate CAs or interoperable CA from other domain.
- It is better to keep the root CA off-line.
  - Therefore, to provide a very high level of assurance.

Certificate Management System for Root CA

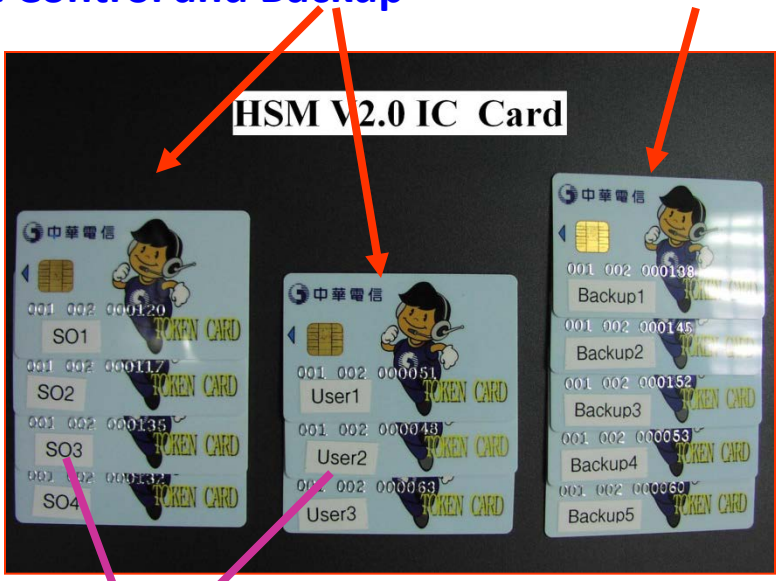


HSM: Hardware Security Module

Adopt Certified HSM

- A Hardware Security Module (HSM) with m-out-of-n control is useful to enforce “separation of duties” to prevent insider attack.

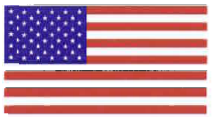
❑**Secret Sharing (m-out-of n): Multiple Control and Backup**



❑**Identity Based Strong Authentication**

Example: FIPS 140-2 Certified HSM

FIPS 140-2 Validation Certificate



The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. **448**

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

SafGuard 200 HSM *by* Chunghwa Telecom Co., Ltd. Telecommunication Labs

(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, *Security Requirements for Cryptographic Modules*. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Designated Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

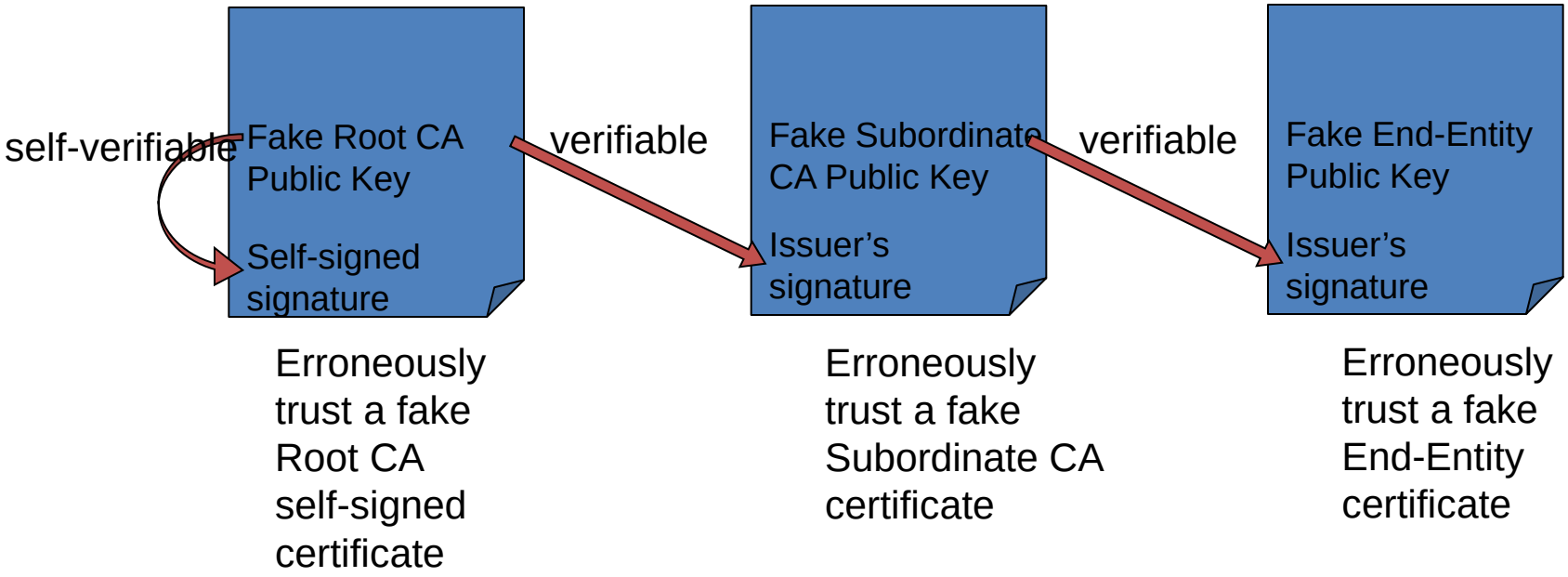
TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments.

Warning: Self-Signed Certificate could be forged

- Self-Signed Certificate:
  - The issuer name and the subject name is the same.
  - The signature of the certificate can be verified by the subject public key contained in the certificate.
- Don’t rely on the signature of the self-signed certificate because it is not endorsed by others.
  - Anyone with ordinary PKI tools can forge a signature-verifiable self-signed certificate with the same issuer/subject name as you root CA.
- The sefl-signed certificate should only be treat as a container to convey root public key, and it needs to be distributred via an out-of-band secure channel.

What if you erroneously trust a fake self-signed certificate

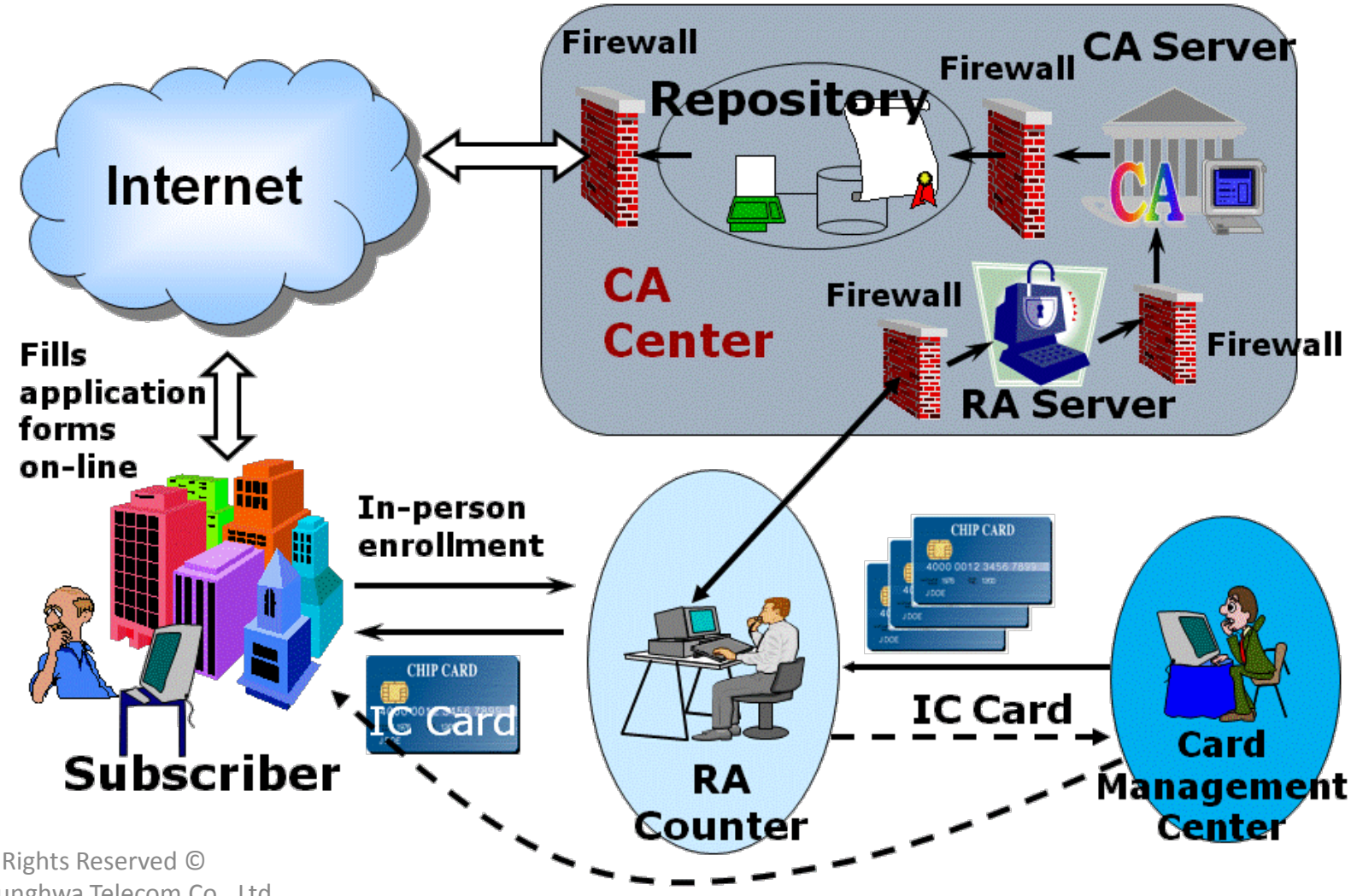
- The attacker could forge the whole certification path!



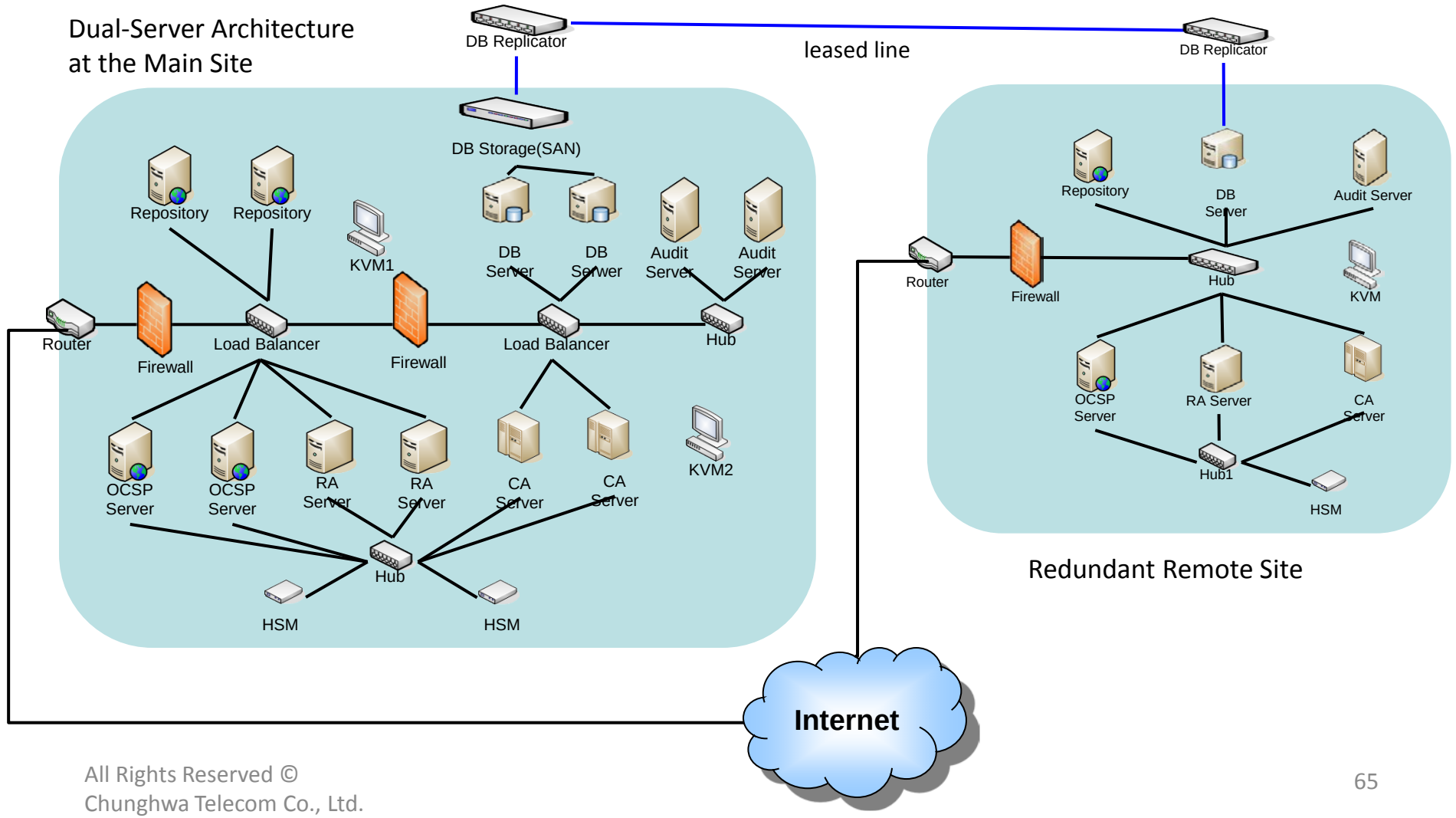
Step 7: Establish the Subordinate CA

- Usually, a subordinate CA needs to issue and manage a large quantity fo certificate, therefore it is not feasible to put it off-line.
- As the same reason with the case of the Root CA, it is a good practice to adopt certified HSMs for used to manage CA keys.
  - m-out-of-n control is useful to enforce “separation of duties” to prevent insider attack.

Certificate Management System of Subordinate CA



Fault-tolerant Certificate Management System



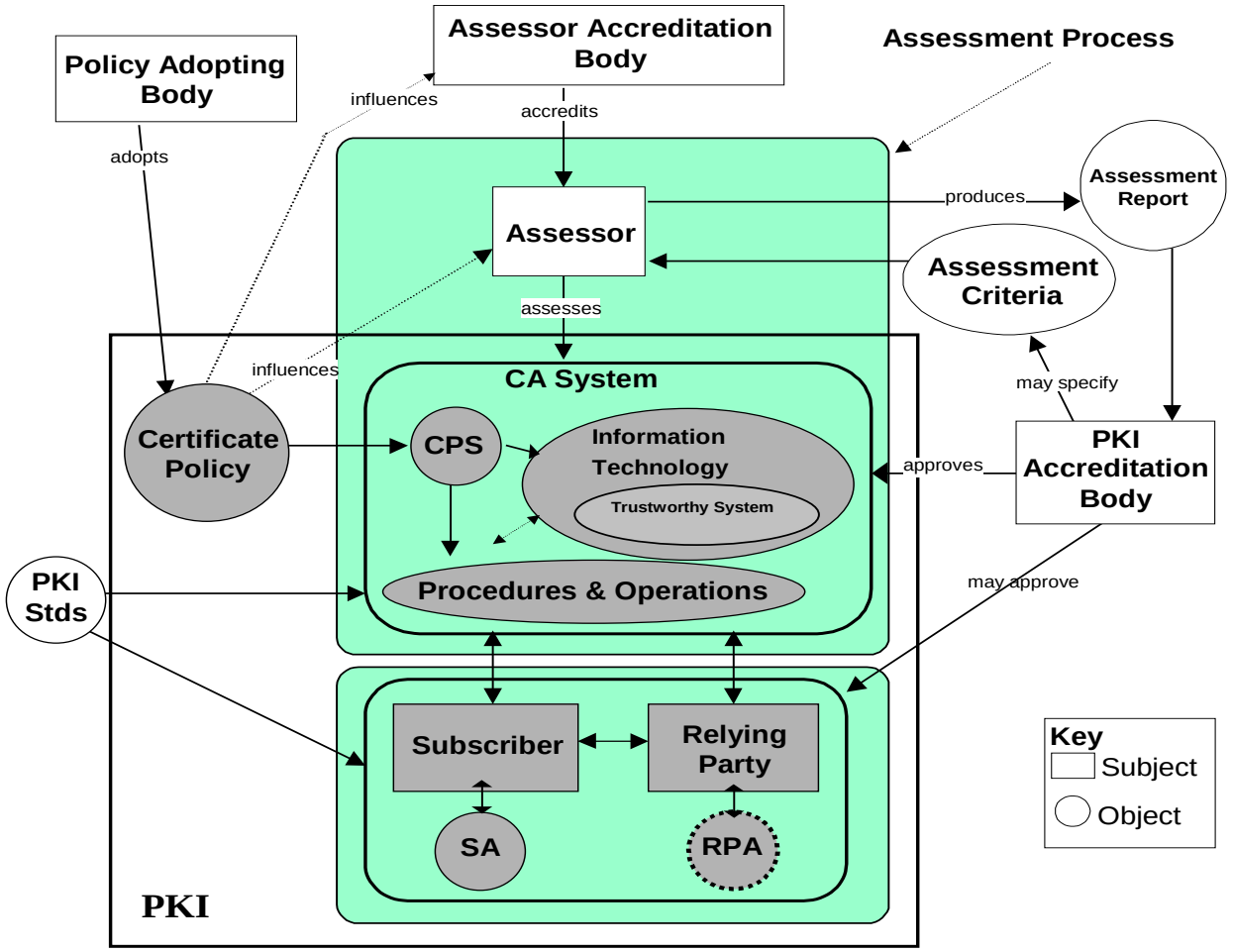
Considering Stronger Keys for End-Entities

- More and more evaluations of the strength of crypto key size by different research group commonly suggest that the current main stream of 1024 bits symmetric key length will be no longer strong enough in the near future.
- For example, US NIST SP800 recommends that
  - Note that 1024 bit RSA is permitted to leverage current products and promote efficient adoption of FIPS 201, but must be phased out by 2010 for authentication keys and 2008 for digital signatures and key management.
- If possible, you should adopt 2048 bits smart cards for end-entities.

Step 8: Conduct CA Audit

- CA audit needs to be conducted by an independent, objective and knowledgeable external auditor.
- The CA accreditation scheme might mandate that CA audit needs to be periodically (e.g., annually) performed.
- Even the CA accreditation scheme might not mandate it, chances are your CP, PMA, or Root CA might still require you to submit external CA audit.
- If by any chance no one mandate it, you should periodically conduct external CA audit by voluntary.
- External CA audit might be the only way that your CA can earn public trust.

PKI Assessment Model



(Figure from Randy V. Sabett, 2001)

WebTrust Program for Certification Authorities

- Often called “WebTrust for CA(s)” for short
- An international program developed by American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Charted Accountants (CICA)
- Might be the most globally recognized CA audit standards today
- Framework to assess adequacy and effectiveness of controls employed by CAs
- Designed specifically for the examinations of CA business activities

WebTrust Program for Certification Authorities

- CA control objectives are based on the following standards:
  - RFC 2527: Certificate Policy and Certification Practices Framework
    - Which is now superseded by RFC 3647
    - Developed by IETF PKIX WG
  - PKI Assessment Guideline (ABA PAG)
    - Developed by American Bar Association(ABA)
  - X9.79: PKI Practices and Policy Framework
    - Developed by ANSI
    - Become an ISO standard in 2006 (ISO 21188)

WebTrust for CA Principles and Criteria

- Principle 1: CA Business Practices Disclosure
  - The Certification Authority discloses its key and certificate life cycle management business and information privacy practices and provides its services in accordance with its disclosed practices.
  - Totally 45 criteria to be assessed

WebTrust for CA Principles and Criteria

- Principle 2: Service Integrity
  - The Certification Authority maintains effective controls to provide reasonable assurance that:
    - Subscriber information was properly authenticated (for the registration activities performed by ABC-CA) and
    - The integrity of keys and certificates it manages is established and protected throughout their life cycles.
  - Totally 188 criteria to be assessed

WebTrust for CA Principles and Criteria

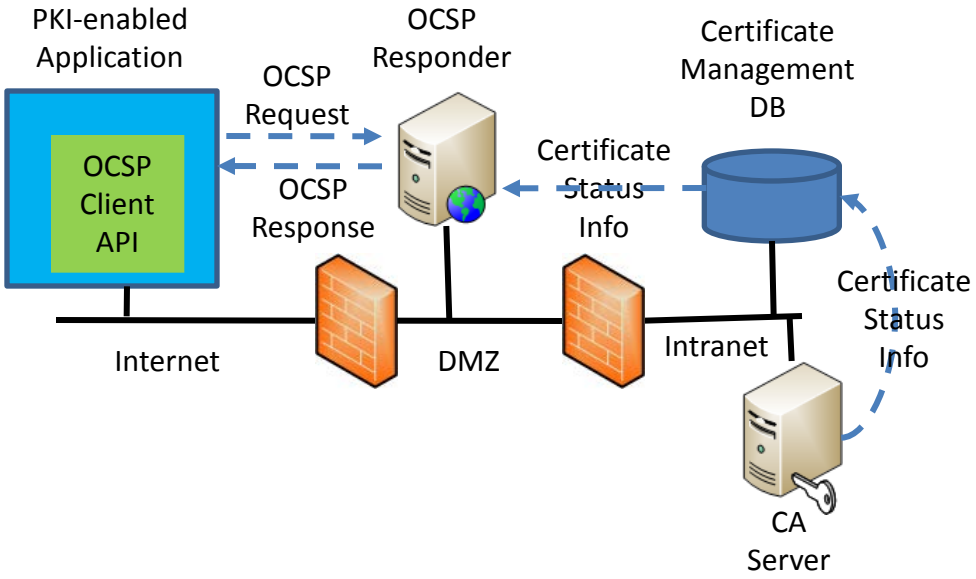
- Principle 3: CA Environmental Controls
  - The Certification Authority maintains effective controls to provide reasonable assurance that:
    - Subscriber and relying party information is restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
    - The continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance and operation are properly authorized and performed to maintain CA systems integrity.
  - Totally 151 criteria to be assessed

Step 9: Consolidate Your Infrastructure

- Remember that CAs are merely the foundation of your PKI, you still need to establish additional services to smooth the utilization of public key technologies in your infrastructure.
- Some useful additional facilities:
  - OCSP Responder
  - SCVP Service
  - PKI Toolkit
  - Timestamp Service

OCSP Responder

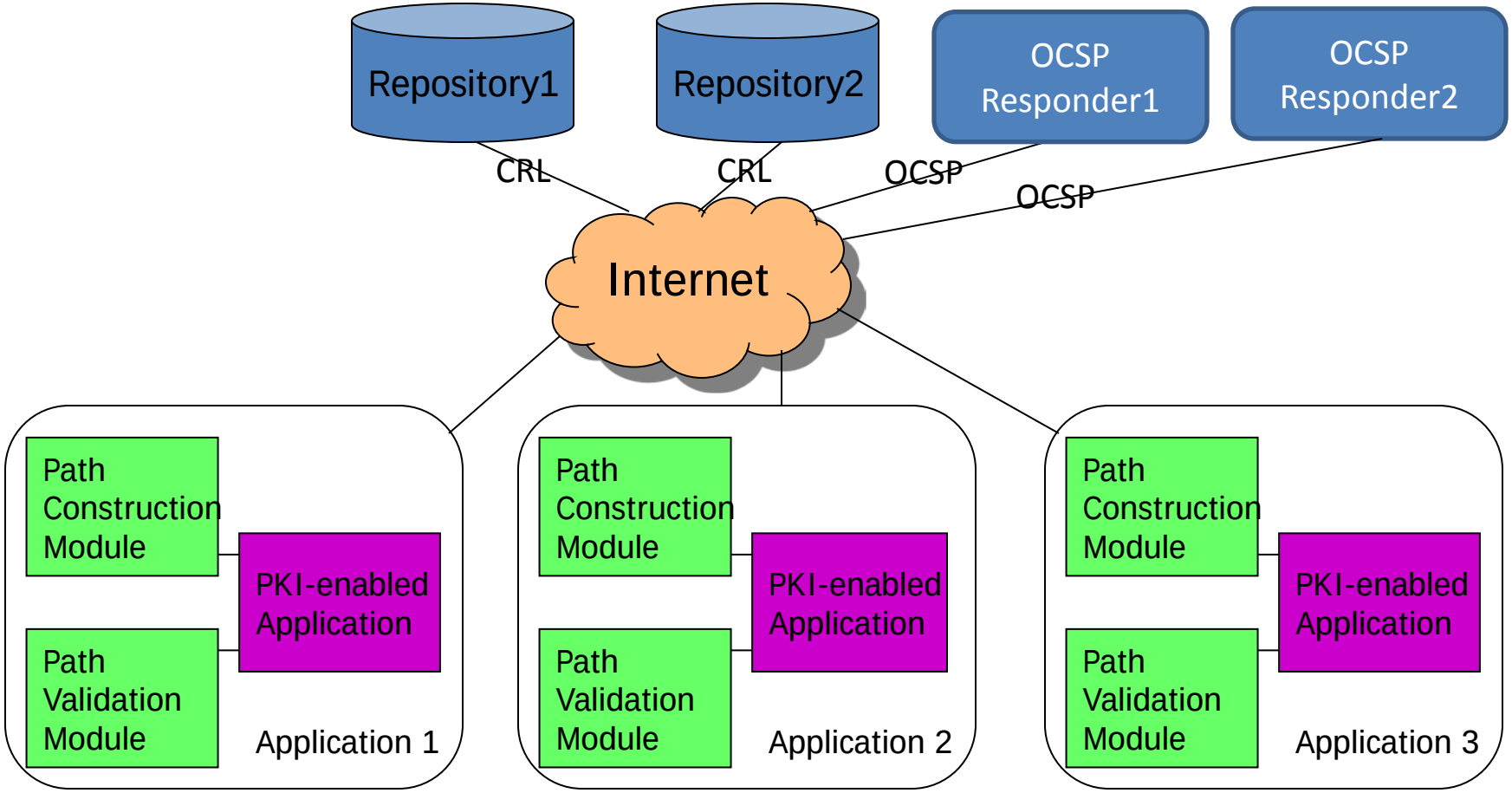
- Online Certificate Status Protocol (OCSP)
  - RFC 2560
  - An alternative to CRL
  - Provide timely information regarding the revocation status of a certificate
  - Almost become a must-have service nowadays



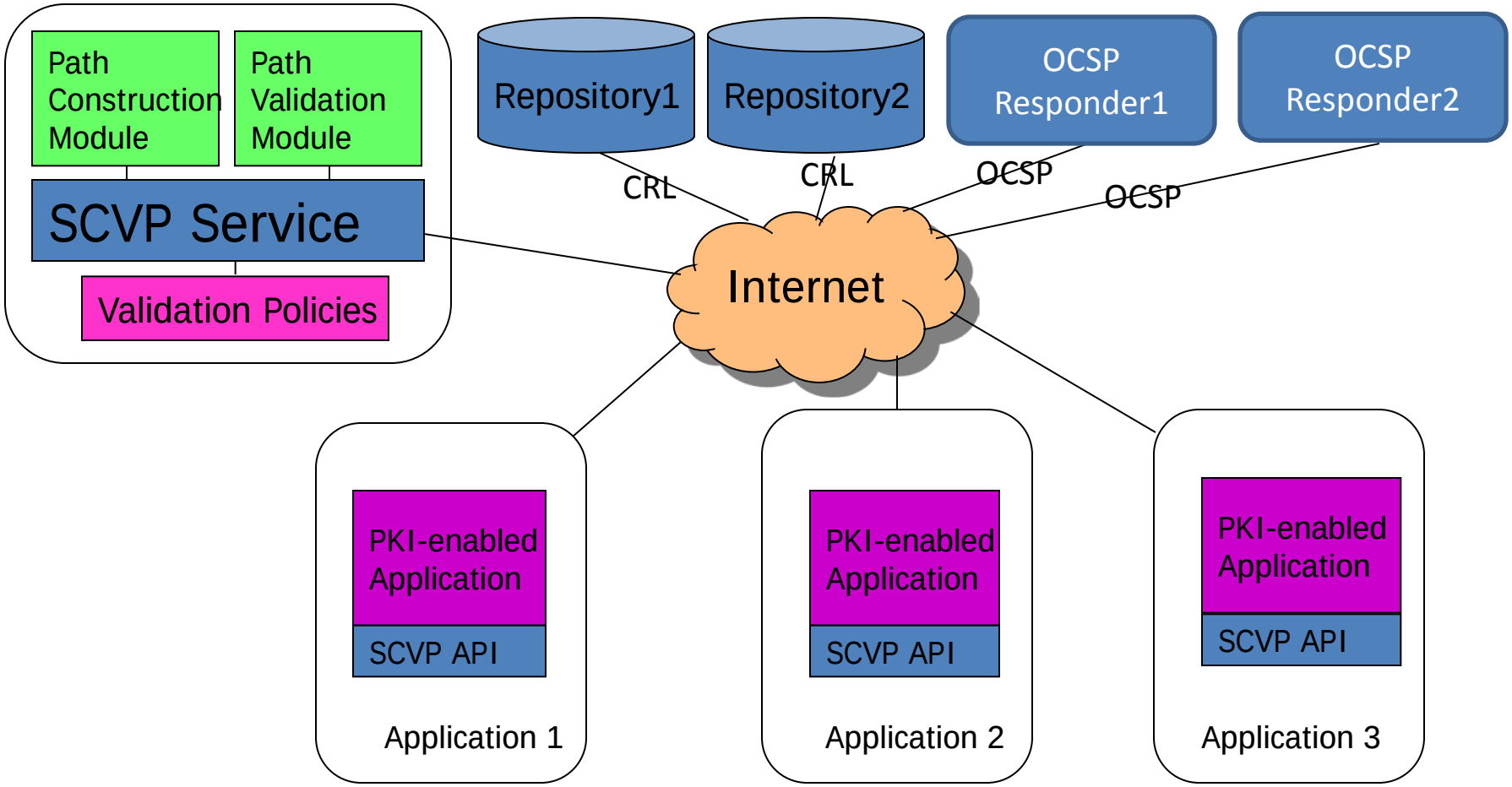
SCVP Service

- RFC 5055
- Provides Delegated Path Discovery (DSD) and Delegated Path Validation (DPD)
- The certification path validation algorithm is too complex for a application developer to implement it.
- Reliefs the burden that developer of PKI-enabled applications.
- A. k. a. Validation Authority (VA)
  - But be careful that sometimes vendors might call their OCSP responder as a VA.
- Could be used to enfcorce centralized validation policy

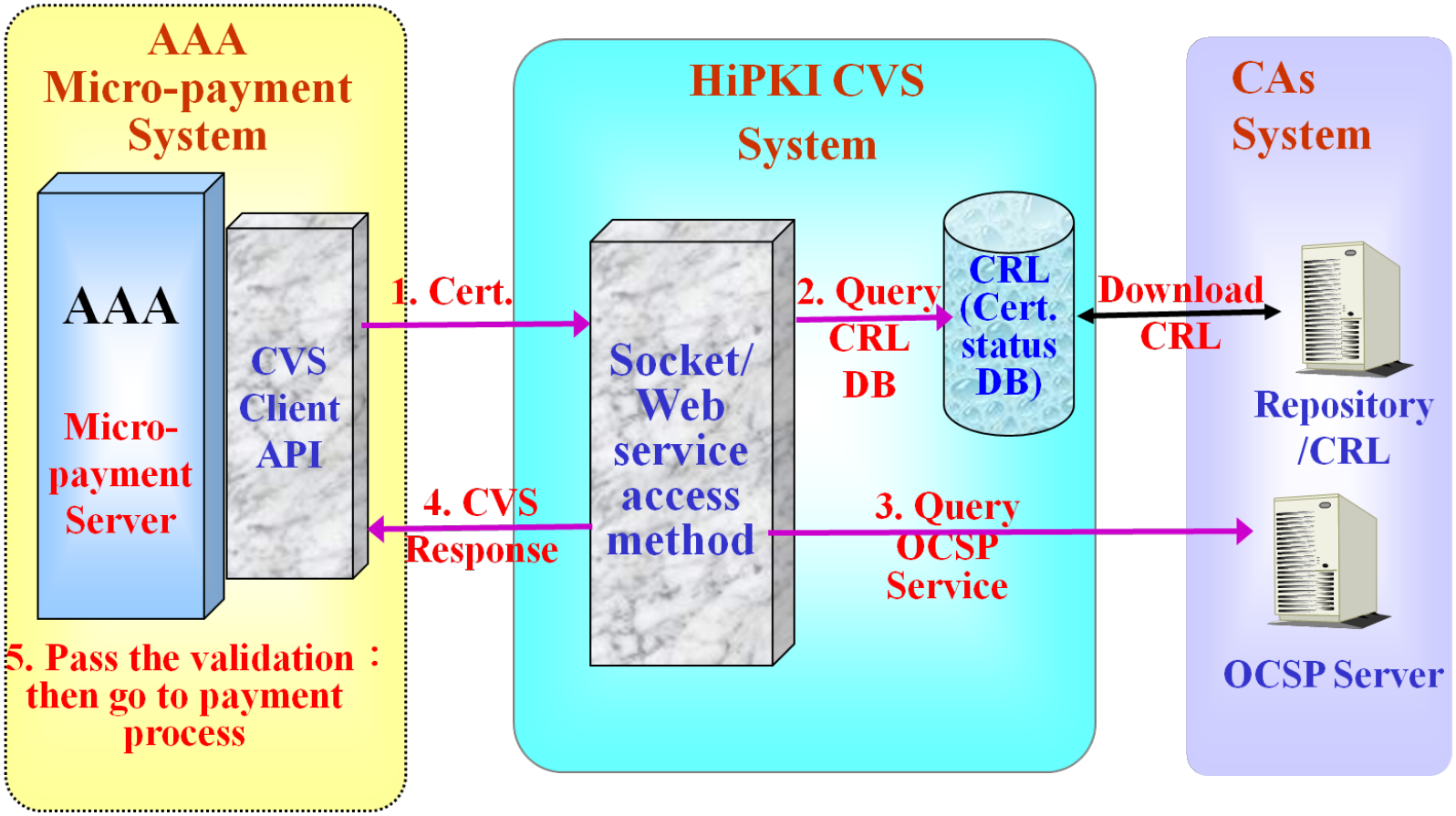
Without SCVP Service



With SCVP Service



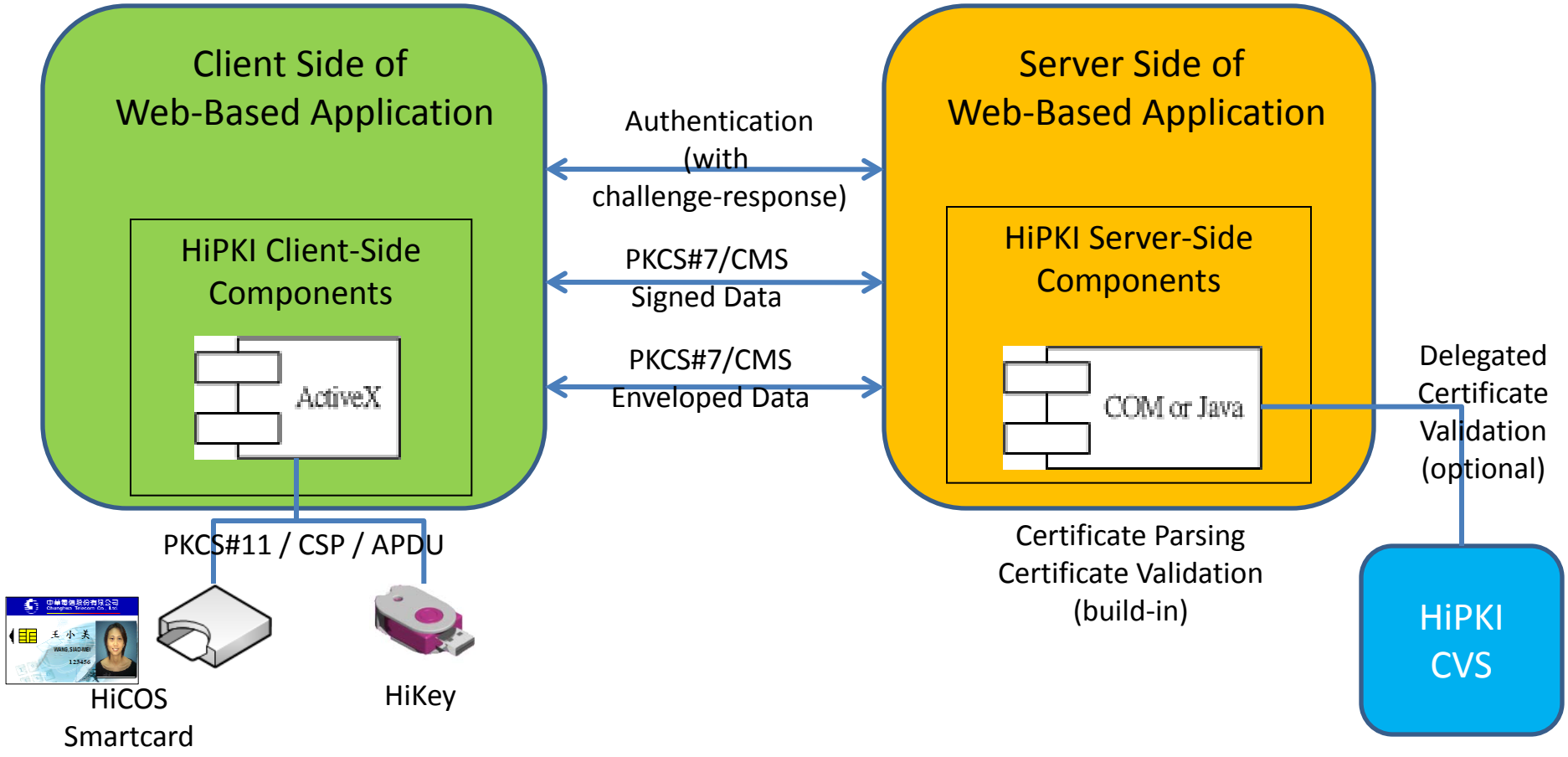
Example: HiPKI Certificate Validation Service (HiPKI CVS)



PKI Toolkit

- A toolkit providing full-featured but easy-to-use PKI programming components, covering
  - IC card/USB token access,
  - PKI-based authentication,
  - digital signature signing/verification,
  - encryption/decryption,
  - certificate/CRL parsing
- Let your applications instantly become PKI-enabled and thus substantially lower the barrier for the applications to adopt PKI.

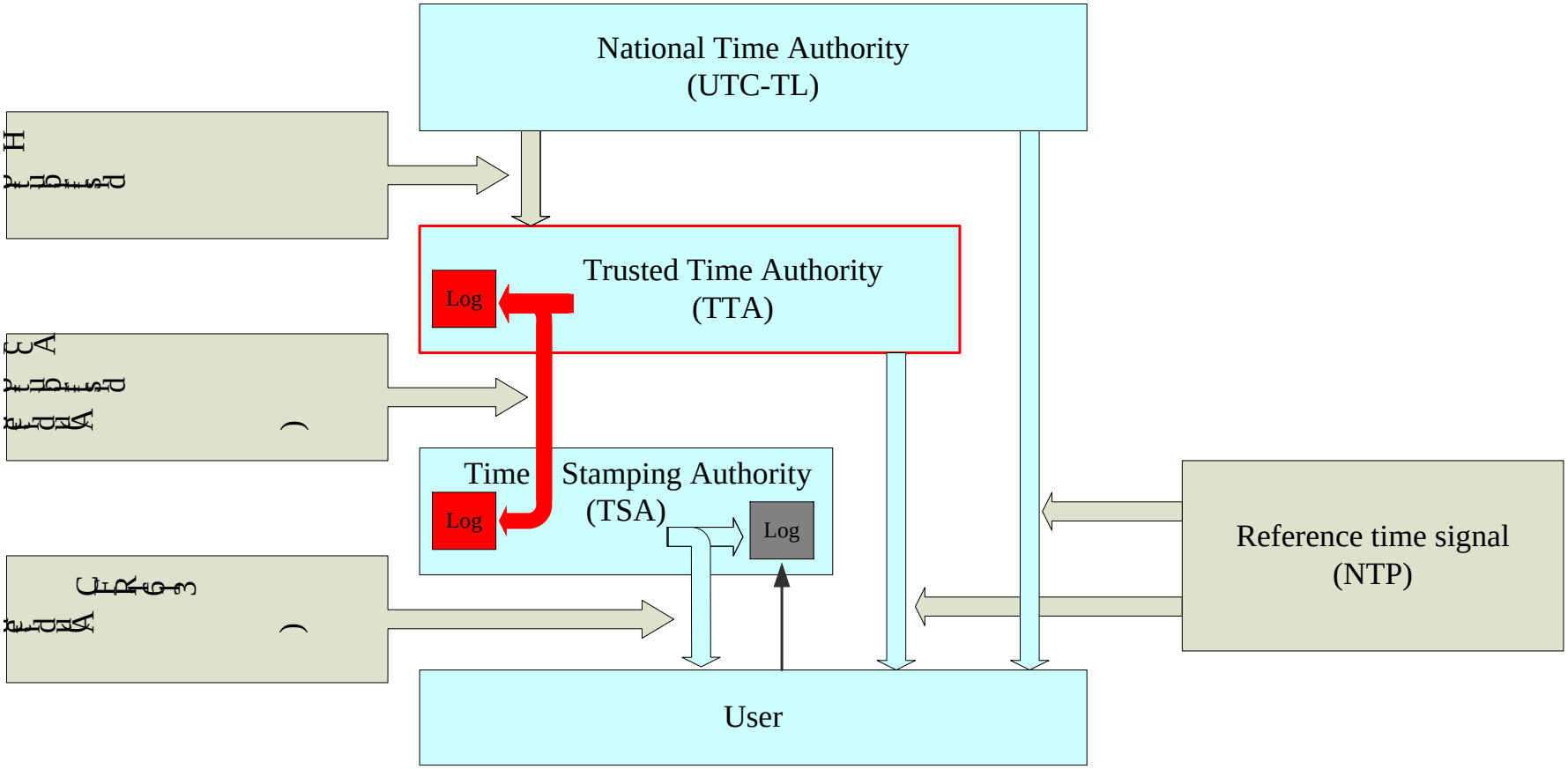
Example: HiPKI Toolkit



Timestamp Service

- RFC 3161
- Supports assertions of proof that a datum existed before a particular time
- If the datum is a digital signature, the timestamp can be used to proof that the signature was created before a particular time
  - e.g., before the signer's certificate was revoked

Architecture of Trusted Timestamping Service



Long-Term Electronic Signature

- **Is the electronic signature enough for the preservation of electronic records ?**

The structure of current electronic records with electronic signature

- **More secure, reliable, long-term, and effective electronic signature.**
  - Advanced Electronic Signature Standards
  - Providing more secure, valid, and verifiable relevant data.
  - Providing more effective content protection for high-value information assets.
  - Accomplishing the purpose of paperless technology with security mechanisms.

The structure of advanced electronic records with electronic signature

Part 4

HOME WORK

Homework

1. How could the off-lined Root CA periodically (e.g., daily) publishes its CRL to the repository?
2. Find a way to securely distribute the self-signed certificate of the Root CA to all relying parties in the PKI domain.

Thank you for your attention!

Email: wcwang@cht.com.tw