
# Information Systems Security Architecture Professional (ISSAP)

## Notes by Al Nafi

## Domain 3 - Cryptography

**Author:**

**Osama Anwer Qazi**

# Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is a security framework that enables **secure digital communication, identity verification, and encryption** through public-key cryptography. It provides a structured way to issue, manage, store, distribute, and revoke digital certificates, ensuring that entities communicating over networks can trust each other. PKI is widely used in securing **web transactions (HTTPS), VPN authentication, digital signatures, and identity management systems**. It operates on a hierarchical model, where **Certificate Authorities (CAs) issue, validate, and revoke digital certificates** to establish trust in an ecosystem.

---

## Key Distribution

Key distribution in PKI ensures that cryptographic keys are securely exchanged between entities to enable encryption and authentication. The **public key** in asymmetric cryptography can be freely shared, while the **private key** must remain confidential and secure. PKI facilitates secure key distribution through digital certificates, which contain the public key and other identifying details of an entity. **Key exchange mechanisms**, such as Diffie-Hellman and RSA-based encryption, help securely distribute symmetric session keys used in encrypted communications. Secure protocols, including **TLS (Transport Layer Security) and IPsec**, rely on PKI for distributing encryption keys and establishing trusted connections.

---

## Certificate and Key Storage

Digital certificates and cryptographic keys must be stored securely to prevent unauthorized access or tampering. **Private keys** should never be stored in plaintext and must be protected using **hardware security modules (HSMs), secure enclaves, or encrypted key vaults**. Cloud providers offer managed key storage solutions such as **AWS Key Management Service (KMS) and Azure Key Vault**, which provide secure storage and controlled access to cryptographic keys. Organizations also use **smart cards, USB tokens, and Trusted Platform Modules (TPMs)** to protect and store private keys for user authentication and secure transactions. Ensuring that keys are **encrypted, access-controlled, and regularly backed up** is critical for maintaining the integrity of PKI-based security systems.

---

# PKI Registration

PKI registration is the process of **verifying the identity of an entity before issuing a digital certificate**. The **Registration Authority (RA)** is responsible for authenticating the entity requesting a certificate before forwarding the request to the **Certificate Authority (CA)** for approval. The registration process includes collecting identity information, validating ownership of domains or email addresses, and confirming organizational affiliations. Once the entity's credentials are verified, the CA issues a digital certificate linking the public key to the authenticated entity. This ensures that only **legitimate users, organizations, or devices** receive trusted certificates.

---

# How the Subject Proves Its Organizational Entity

When an organization requests a digital certificate, it must prove its legitimacy to the CA. This is typically done by submitting **legal documents, business registrations, and domain ownership records**. The CA performs **domain validation (DV), organization validation (OV), or extended validation (EV)** to verify the authenticity of the organization.

- **Domain Validation (DV):** The CA confirms control over a domain by requiring DNS record modifications or email verification.
- **Organization Validation (OV):** The CA verifies business registration details and contacts the organization for confirmation.
- **Extended Validation (EV):** A more rigorous verification process that includes detailed legal checks, requiring the organization to meet strict authentication requirements.

These validation methods ensure that certificates are issued only to verified entities, reducing the risk of fraudulent or malicious use.

---

# How a Person, Acting on Behalf of the Subject, Authenticates to Request a Certificate

When an individual requests a certificate on behalf of an organization, **identity authentication and authorization are required** to prevent unauthorized issuance. The requesting individual must provide verifiable credentials, such as:

- **Company email and job role verification** to confirm authority.
- **Two-factor authentication (2FA) or smart card authentication** to validate the requester's identity.
- **Legal authorization documents** confirming the individual's right to obtain the certificate.



 

### Case Study: Digital Certificate Request in a Financial Institution

A financial institution required **email encryption certificates** for all employees handling sensitive transactions. The IT security team assigned a **designated certificate officer** to request certificates from the CA. The officer authenticated their request using a **corporate email, a digitally signed request, and an HR authorization letter**. The CA verified the organization's details and issued certificates to authorized employees, ensuring that only approved personnel could encrypt and sign sensitive financial communications.

---

## Certificate Issuance

Once identity verification is complete, the CA generates and issues a **digital certificate** that binds the entity's public key to its identity. The certificate follows the **X.509 standard** and includes details such as:

- The subject's identity (organization name, domain, or individual name).
- The public key associated with the entity.
- The issuing CA's digital signature.
- The certificate's validity period and expiration date.

The issued certificate can then be used for **TLS encryption, digital signatures, and secure authentication** in various applications.

---

## Trust Models

PKI operates on different trust models that determine how certificates are issued, validated, and relied upon. The three primary trust models include:

- **Hierarchical Model (Single CA or Subordinate CA):** A single **root CA** issues certificates, and subordinate CAs manage specific domains or departments. This model is **highly scalable and commonly used in enterprises**.
- **Cross-Certified Model (Mesh Network):** Multiple CAs establish **mutual trust** through cross-certification agreements, enabling entities to accept certificates from multiple trusted CAs.
- **Bridge CA Model:** A central **bridge CA** acts as an intermediary, linking separate PKI infrastructures to establish **trust between independent organizations**. This is useful in **government and multinational business environments**.

---



 

## Subordinate Hierarchy

A subordinate hierarchy consists of a **root CA** and one or more **intermediate/subordinate CAs** that issue certificates on behalf of the root CA. This model enhances security by **isolating the root CA from direct exposure**, ensuring that even if an intermediate CA is compromised, the root CA remains protected. **Organizations use this model to manage different types of certificates for internal systems and external communication securely**.

---

## Cross-Certified Mesh

A cross-certified mesh model enables multiple CAs to **recognize and trust each other's certificates**. This allows organizations operating under different PKI systems to interoperate securely without relying on a single root CA. Cross-certification is commonly used in **federal agencies, multinational corporations, and industry consortiums** where mutual trust must be established between different entities.

---

## Certificate Chains

A certificate chain, also known as a **chain of trust**, links an end-user certificate to a trusted root CA through **intermediate CAs**. When a browser or system encounters a certificate, it verifies the **entire chain** to ensure it originates from a trusted CA. If any certificate in the chain is invalid or revoked, the verification process fails, warning users that the connection is untrusted.

---

## Certificate Revocation

Certificates must be revoked if they are compromised, expired, or no longer required. Revocation prevents malicious actors from misusing a valid certificate.

## Traditional CRL Model

The **Certificate Revocation List (CRL)** is a periodically updated list of revoked certificates, published by the CA. Systems must download and check CRLs to verify certificate validity, but this method can be slow and inefficient.



 

## Modified CRL-Based Models

The **Online Certificate Status Protocol (OCSP)** is a more efficient alternative that allows real-time certificate status verification. OCSP responders provide instant confirmation of a certificate's validity, improving performance and security.

---

# Cross-Certification

Cross-certification establishes trust between independent PKI infrastructures, enabling secure communication across different organizations.

- **How Applications Use Cross-Certification:** Secure email, document signing, and federated authentication systems rely on cross-certified certificates to recognize external entities.
- **How Cross-Certification Is Set Up:** Organizations negotiate trust agreements, exchange root CA certificates, and configure validation rules to recognize external certificates.
- **How Cross-Certification with a Bridge CA Is Implemented in Practice:** A **bridge CA** acts as a central trust entity, connecting multiple PKIs and enabling seamless interoperability. This approach is widely used in **government agencies and large enterprises** to facilitate secure cross-organization authentication.

# How Applications Use Cross-Certification

Cross-certification is widely used in various applications where organizations, government entities, or different IT ecosystems need to establish mutual trust for secure communication and authentication. One of the most common use cases is **federated identity management**, where users from one organization can access resources in another organization without needing separate credentials. This is often seen in **government agencies, multinational corporations, and industry consortiums**, where employees need access to external systems securely.

Another critical application of cross-certification is **secure email communication**. Organizations using different Certificate Authorities (CAs) must trust each other's digital certificates for **S/MIME (Secure/Multipurpose Internet Mail Extensions)** encryption and signing. Without cross-certification, email security would be fragmented, requiring each user to manually validate certificates, which is impractical in large-scale environments.

In e-commerce and financial transactions, cross-certification allows businesses operating in different jurisdictions to **validate digital signatures on contracts and financial documents**, ensuring legal compliance across borders. **Electronic health record (EHR) systems** also benefit from cross-certification, where hospitals and healthcare providers in different networks can securely exchange patient information while maintaining compliance with regulations such as **HIPAA**.



 

## How Cross-Certification Is Set Up

Setting up cross-certification involves establishing **mutual trust** between different Certificate Authorities (CAs) so that certificates issued by one CA are accepted as valid by another. The process includes the following key steps:

1. **Negotiating Trust Agreements:** Organizations must define the terms and policies governing cross-certification. This includes setting security standards, certificate validity requirements, and conditions under which trust can be revoked.

2. **Exchanging Root CA Certificates:** Each participating CA must obtain and validate the root certificate of the other CA. This involves verifying the authenticity, validity, and compliance of the external CA's policies with internal security standards.

3. **Issuing Cross-Certification Certificates:** Each CA generates a **cross-certification certificate**, which essentially states that the issuing CA trusts the external CA's certificates for specified purposes. This certificate is signed by the root CA of each party to establish mutual recognition.

4. **Defining Certificate Policies and Constraints:** To prevent abuse and misconfiguration, organizations implement policy constraints that specify how far trust extends within the external CA's certificate hierarchy. **Name constraints** and **policy mappings** ensure that only approved entities can participate in the trust network.

5. **Deploying Cross-Certification Certificates in Applications:** Once the cross-certification certificates are issued, they must be integrated into **directory services (LDAP, Active Directory Certificate Services), authentication systems, and security applications** to enforce trust automatically.

6. **Continuous Monitoring and Audit:** Regular audits and revocation checks are necessary to ensure that trust is maintained securely. If a participating CA is compromised or fails to meet security standards, its cross-certification can be revoked to prevent unauthorized access.

Cross-certification is particularly useful in **multi-cloud environments**, where enterprises rely on **PKI-based authentication between AWS, Azure, and Google Cloud services**. This setup ensures that encrypted communications, API requests, and identity management functions work seamlessly across platforms.



 

# How Cross-Certification with a Bridge CA Is Implemented in Practice

A **Bridge Certificate Authority (Bridge CA)** serves as an intermediary entity that facilitates trust between multiple CAs without requiring direct cross-certification agreements between each pair. This model is particularly useful when multiple organizations, government agencies, or industries need to establish a **centralized trust hub** while maintaining their independent PKI structures.

## Implementation Process of a Bridge CA

1. **Establishing the Bridge CA:** A central authority is designated to act as the **Bridge CA**, which will facilitate trust relationships between multiple independent PKIs. This Bridge CA does not issue end-user certificates but rather cross-certifies each participating CA.

2. **Cross-Certification with the Bridge CA:** Each participating CA undergoes a cross-certification process with the Bridge CA. The Bridge CA issues a cross-certification certificate to each member CA, establishing a chain of trust through itself.

3. **Defining Trust Relationships:** The Bridge CA defines **certificate policies, name constraints, and security levels** to ensure consistent validation across all connected PKIs. Policy mapping ensures that trust requirements are met uniformly.

4. **Deploying Certificate Trust Lists (CTLs):** Applications, authentication services, and directory servers use Certificate Trust Lists to recognize and validate cross-certified certificates issued within the Bridge CA's trust network.

5. **Ensuring Secure Communication:** Organizations relying on the Bridge CA can now securely communicate, validate digital signatures, and authenticate users or systems without needing one-to-one cross-certification agreements.

6. **Monitoring and Revocation Management:** The Bridge CA regularly audits trust relationships, ensuring that compromised or non-compliant CAs are removed from the trust network to maintain security. The Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) help applications verify certificate validity in real time.



 

### Real-World Example: Federal Bridge Certification Authority (FBCA)

A well-known implementation of the Bridge CA model is the Federal Bridge Certification Authority (FBCA) in the United States. The FBCA allows various federal agencies, state governments, and private organizations to establish mutual trust in digital transactions and secure communications. Agencies like the Department of Defense (DoD), Department of Homeland Security (DHS), and General Services Administration (GSA) rely on the FBCA to ensure secure authentication and encrypted document exchange across different government bodies.

### Enterprise and Cloud Use Cases

In enterprise environments, a Bridge CA enables interoperability between different corporate PKI infrastructures. For example, a multinational corporation with multiple subsidiaries using separate PKI systems can leverage a Bridge CA to unify authentication and encryption standards across all divisions. In cloud security, organizations use Bridge CA architectures to facilitate secure API authentication and identity federation between cloud service providers like AWS, Microsoft Azure, and Google Cloud.

---

## Conclusion

Cross-certification and Bridge CA models play a crucial role in enabling trust and secure communication across different PKI environments. While direct cross-certification agreements are effective for one-to-one trust relationships, a Bridge CA simplifies trust management for large-scale, multi-entity environments. Organizations implementing cross-certification must ensure strict security policies, policy mappings, certificate constraints, and real-time revocation mechanisms to maintain a trusted ecosystem. As cybersecurity threats evolve, organizations must regularly audit and update their PKI architectures to ensure compliance and prevent unauthorized access.