Securing Digital Ecosystems with Public Key Infrastructure (PKI)

This slide introduces the concept of Public Key Infrastructure (PKI) and its role in securing digital ecosystems.

Introduction to PKI

Security Framework

PKI is a security framework that uses public-key cryptography to establish trust in digital communications.

Secure Transactions

PKI enables secure transactions, such as online banking and e-commerce, through the use of digital certificates.

Identity Verification

PKI provides a reliable way to verify the identity of entities communicating over networks, ensuring trust in digital interactions.

Encryption

PKI facilitates the use of encryption to protect sensitive data during transmission, ensuring confidentiality in digital communications.

PKI is a comprehensive security solution that leverages public-key cryptography to establish trust, enable secure transactions, verify identities, and protect sensitive data in digital communications.

Key Distribution in PKI

Public Key Distribution

Public keys are securely distributed through digital certificates, which contain the public key and identity information of an entity. This enables safe exchange of public keys without the need for direct communication.

Private Key Storage

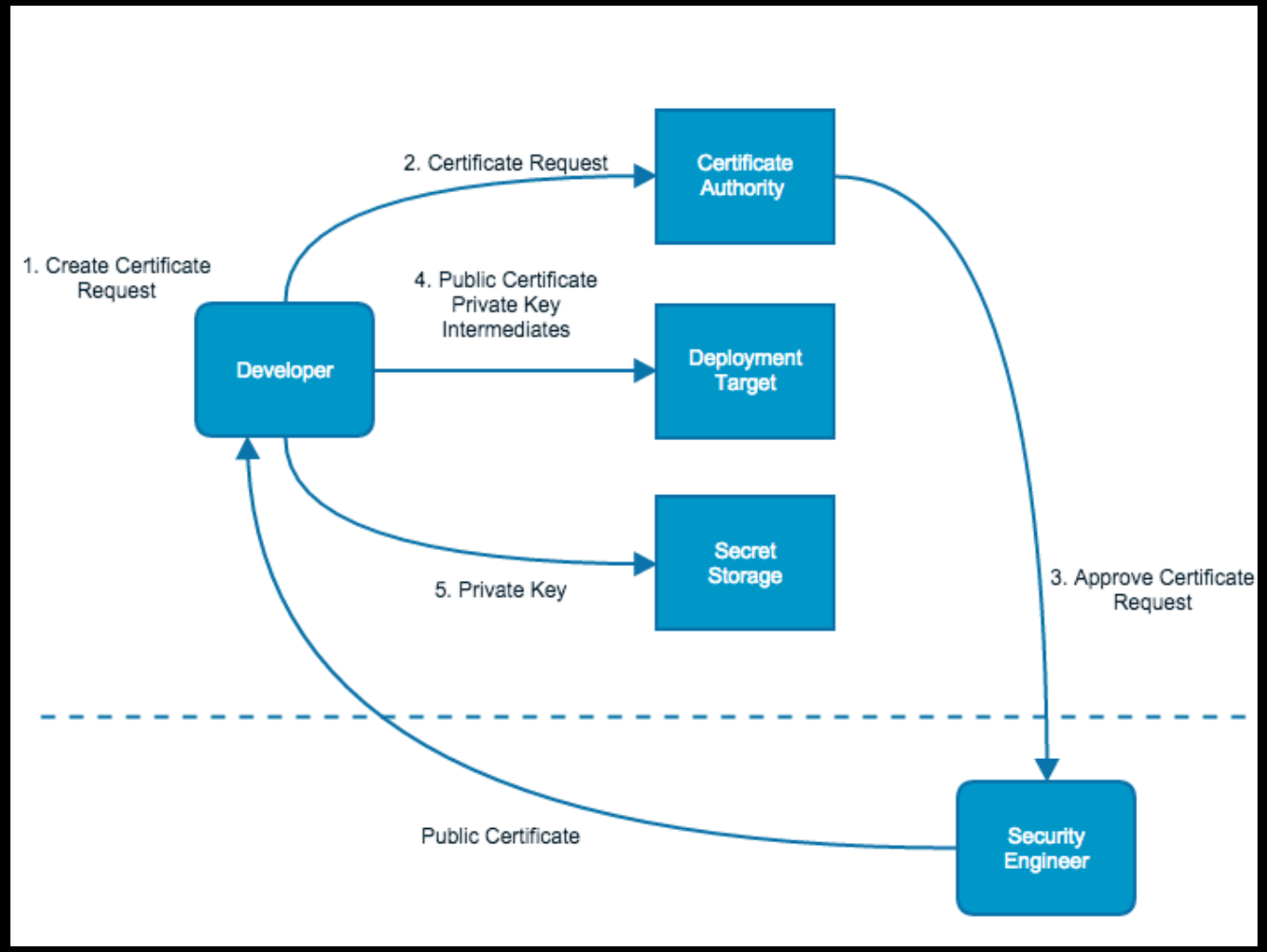
Private keys must be kept confidential and secure, never stored in plaintext. Organizations use hardware security modules (HSMs), encrypted key vaults, and secure hardware like smart cards and USB tokens to protect private keys.

Key Exchange Protocols

Protocols like Diffie-Hellman and RSA-based encryption enable the secure exchange of symmetric session keys used for encrypted communication. PKI provides the necessary trust and identity verification for these key exchange mechanisms.

Secure Communication Protocols

PKI-based protocols like TLS (Transport Layer Security) and IPsec rely on digital certificates to distribute encryption keys and establish trusted connections between communicating entities.



Certificate and Key Storage

Digital certificates and cryptographic keys must be stored securely to prevent unauthorized access or tampering. Private keys are protected using hardware security modules (HSMs), secure enclaves, and encrypted key vaults to ensure the integrity and confidentiality of sensitive cryptographic material.

PKI Registration Process

- ## Entity Requests Certificate
  An individual or organization requests a digital certificate from the PKI system.
- ## RA Authenticates Entity
  The Registration Authority (RA) verifies the identity of the requesting entity by collecting and validating credentials, such as legal documents, business registrations, and domain ownership records.
- ## RA Forwards Request to CA
  Once the entity's identity is confirmed, the RA forwards the certificate request to the Certificate Authority (CA) for processing.
- ## CA Issues Certificate
  The CA generates and issues a digital certificate that binds the entity's public key to its verified identity, following the X.509 standard.

Organizational Authentication for Certificates

Domain Validation (DV)

The CA confirms the organization's control over a domain by requiring DNS record modifications or email verification.

Organization Validation (OV)

The CA verifies the organization's 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.

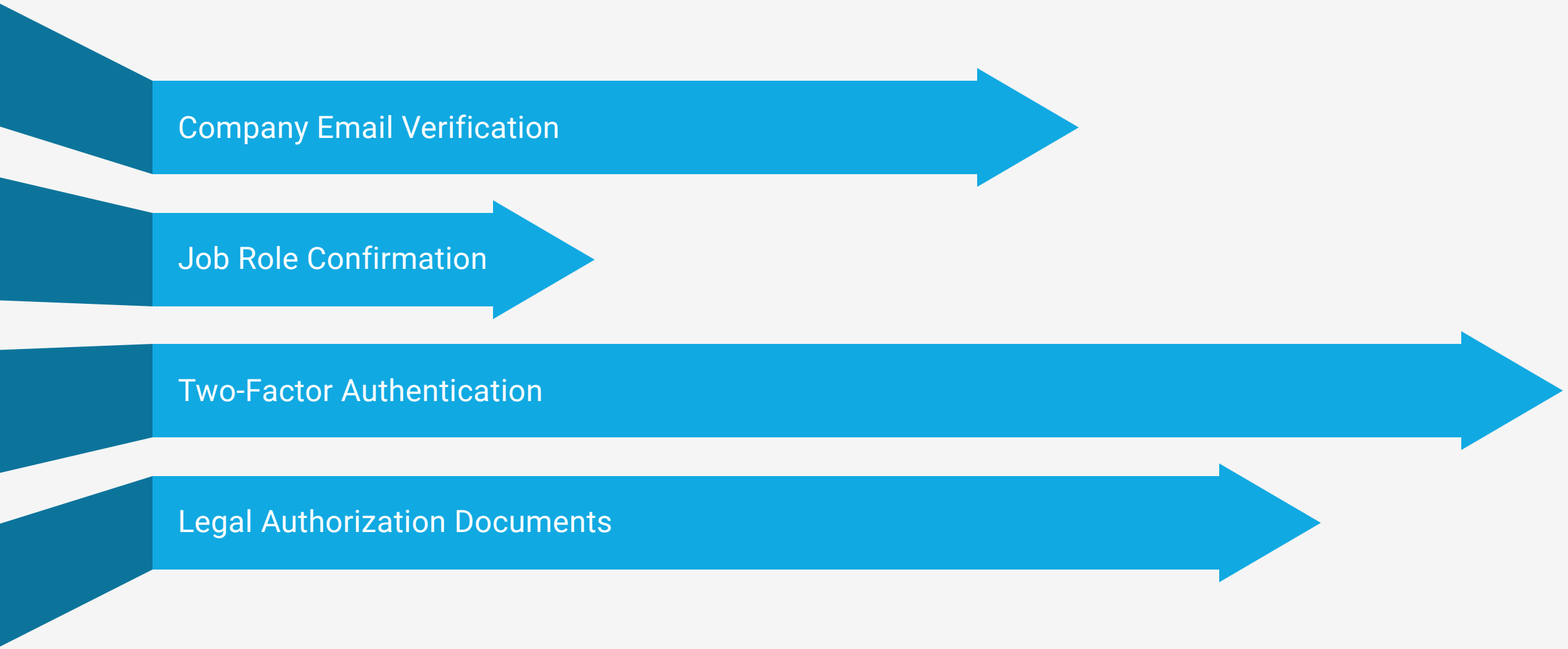
Verifying Organizational Legitimacy

The organization must submit legal documents, business registrations, and domain ownership records to prove its legitimacy to the CA.

Preventing Fraudulent Certificates

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

Individual Authentication for Certificate Requests



Certificate Issuance

- ## X.509 Standard
  The digital certificate follows the X.509 standard, which defines the format and fields for a certificate.

- ## Public Key Binding
  The certificate binds the entity's public key to its identity, enabling secure encryption and authentication.

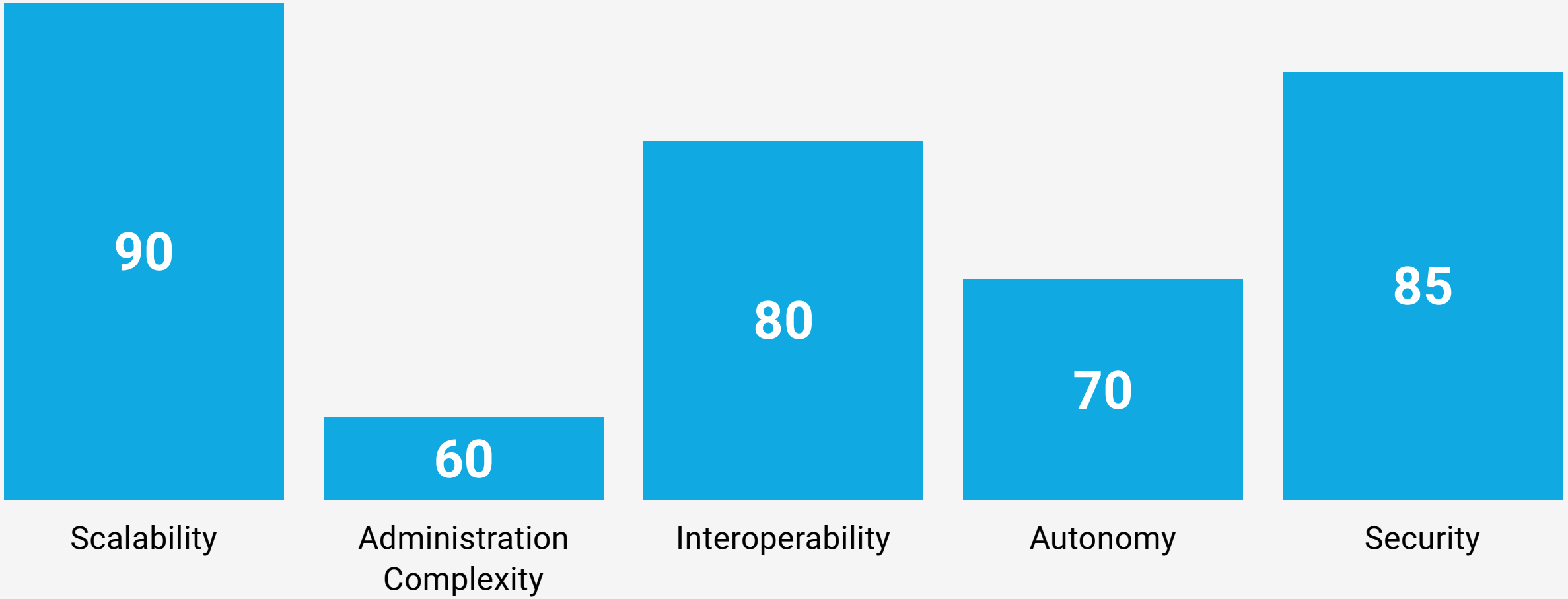
- ## Identity Details
  The certificate includes the subject's identity, such as organization name, domain, or individual name.

- ## Validity Period
  The certificate specifies the validity period, including the expiration date, ensuring it is only used within the intended timeframe.

- ## CA Digital Signature
  The issuing Certificate Authority (CA) digitally signs the certificate, ensuring its authenticity and integrity.

PKI Trust Models

Comparison of key characteristics of PKI trust models (0-100 scale)



Subordinate Hierarchy and Cross-Certified Mesh

Subordinate Hierarchy

Root CA issues certificates to subordinate/intermediate CAs, isolating root from direct exposure

Intermediate CAs

Manage specific domains, departments, or use cases under the overall PKI hierarchy

Security Benefit

Even if an intermediate CA is compromised, the root CA remains protected

Cross-Certified Mesh

Multiple CAs establish mutual trust through cross-certification agreements

Interoperability

Enables organizations with different PKI systems to securely interoperate

Use Cases

Commonly used in federal agencies, multinational corporations, and industry consortiums

Certificate Chains and Revocation

Certificate Chains

Certificate chains link an end-user certificate to a trusted root Certificate Authority (CA) through a hierarchy of intermediate CAs. This chain of trust ensures the validity and integrity of the certificate.

Verifying Certificate Chains

When a system or browser encounters a certificate, it verifies the entire certificate chain to ensure the certificate originates from a trusted root CA. If any certificate in the chain is invalid or revoked, the verification process fails, and the connection is marked as untrusted.

Certificate Revocation

Certificate revocation is the process of invalidating a certificate that has been compromised, expired, or is no longer required. Revoking a certificate prevents its misuse by malicious actors, ensuring the security of the PKI system.

Certificate Revocation Lists (CRLs)

The traditional Certificate Revocation List (CRL) model involves the CA periodically publishing a list of revoked certificates. Systems must download and check the CRLs to verify the validity of a certificate, but this method can be slow and inefficient for large-scale PKI deployments.