Ch12:**Security implementation**

12.1 System design and normalization

- Security is a property of systems; to address security, we must speak of the system as a whole:
  - • Identify what assets we are trying to protect.
  - • Evaluate the main sources of risk and where trust is placed.
  - • Work out possible counter-measures to attacks.
- Counter-measures can be both preventative and reactive. They consist of:
- • Rules (Rules can include access control policies, password complexity requirements, network segmentation rules, and other security measures.)
- • Codified responses. (incident response plans, disaster recovery plans, and playbooks for different types of incidents.)

12.1 System design and normalization

- The foundation of security is policy.
- A system consists of an assembly of parts that exhibit three main activities:
- • Input
- • Rules
- • Output.
- By establishing clear policies, defining input handling rules, and ensuring appropriate output generation, organizations can establish a secure and reliable system.
- The framework can protect sensitive information, maintain system functionality, and prevent unauthorized access or malicious activities.

12.1 System design and normalization

- Protecting ourselves against threat also involves a limited number of themes:
- • Applying safeguards (shields)
- • Access control (selective shields)
- • Protocols (specification of and limitation to safe behavior)
- • Feedback regulation (continuous assessment)
- • Redundancy (parallelism instead of serialism) detection and correction
- • Monitoring the system
- • Regulation.

Normalization

- *Normalization* of a system is a concept from the theory of databases.
- • Avoid unnecessary dependencies and inconsistencies.
- • Validate assumptions.
- Why do we need to apply normalization in security implementation?
- Normalization is essential in security implementation to ensure data integrity, support access control mechanisms, maintain data consistency, and enable efficient data management.

12.3 Data integrity and protection

- Although backup copies will not protect us against loss, they do provide minimal insurance against accidents, intentional damage and natural disasters, and make the business of *recovery* less painful.
- There are several general strategies:

Encryption	Prevention of access on theft or tampering
Integrity checksums	Detection of error or tampering
Redundancy	Recovery from loss

12.3.1 Preventing error, tampering and loss

- Data must be protected both when standing still (in storage) and when passing from place to place (in transport).
- Encryption is a strategy for prevention of theft and tampering, particularly in the transmission of data over networks, though it can also be used to protect disk data from theft and backups from tampering.
- Loss against physical disk failure can be mitigated by using RAID solutions which offer real redundancy. RAID stands for Redundant Array of Inexpensive Disks.
- Search on RAID?

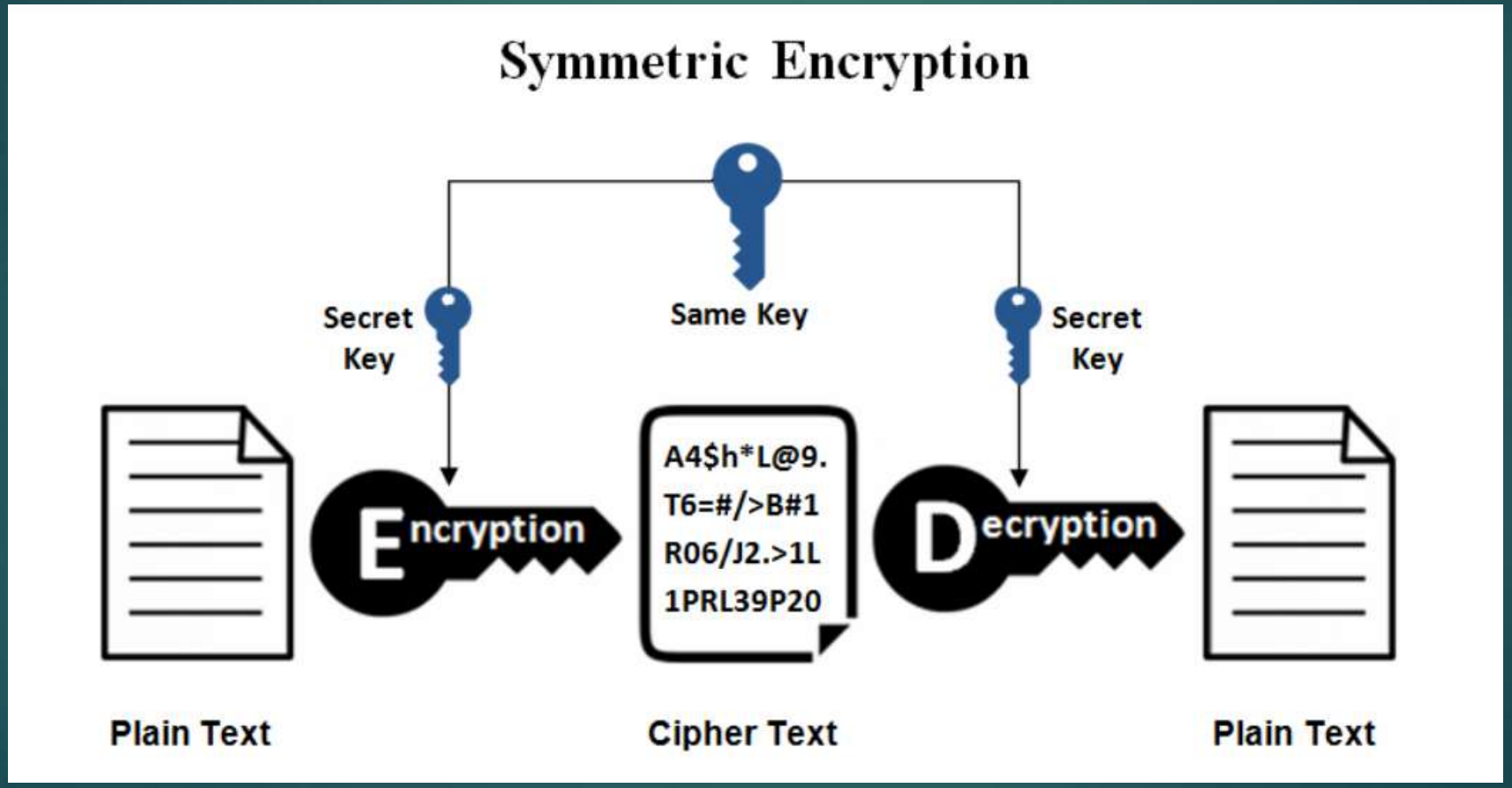
12.3.2 Backup schemes

- Backups are one of the favorite topics of the system administration community.
- The basics of backup are these:
- *Physical location:* A backup should be kept at a different physical location than the original.
- *How often?:* How often do the data change significantly, i.e. how often do we need to make a backup? Every day? Do you need to archive several different versions of files, or just the latest version? The cost of making a backup is a relevant factor here.
- *Relevant and irrelevant files:* There is no longer much point in making a backup of parts of the operating system distribution itself.
- *Backup policy:* Some sites might have rules for defining what is regarded as valid information, i.e. what it is worth making a backup of.

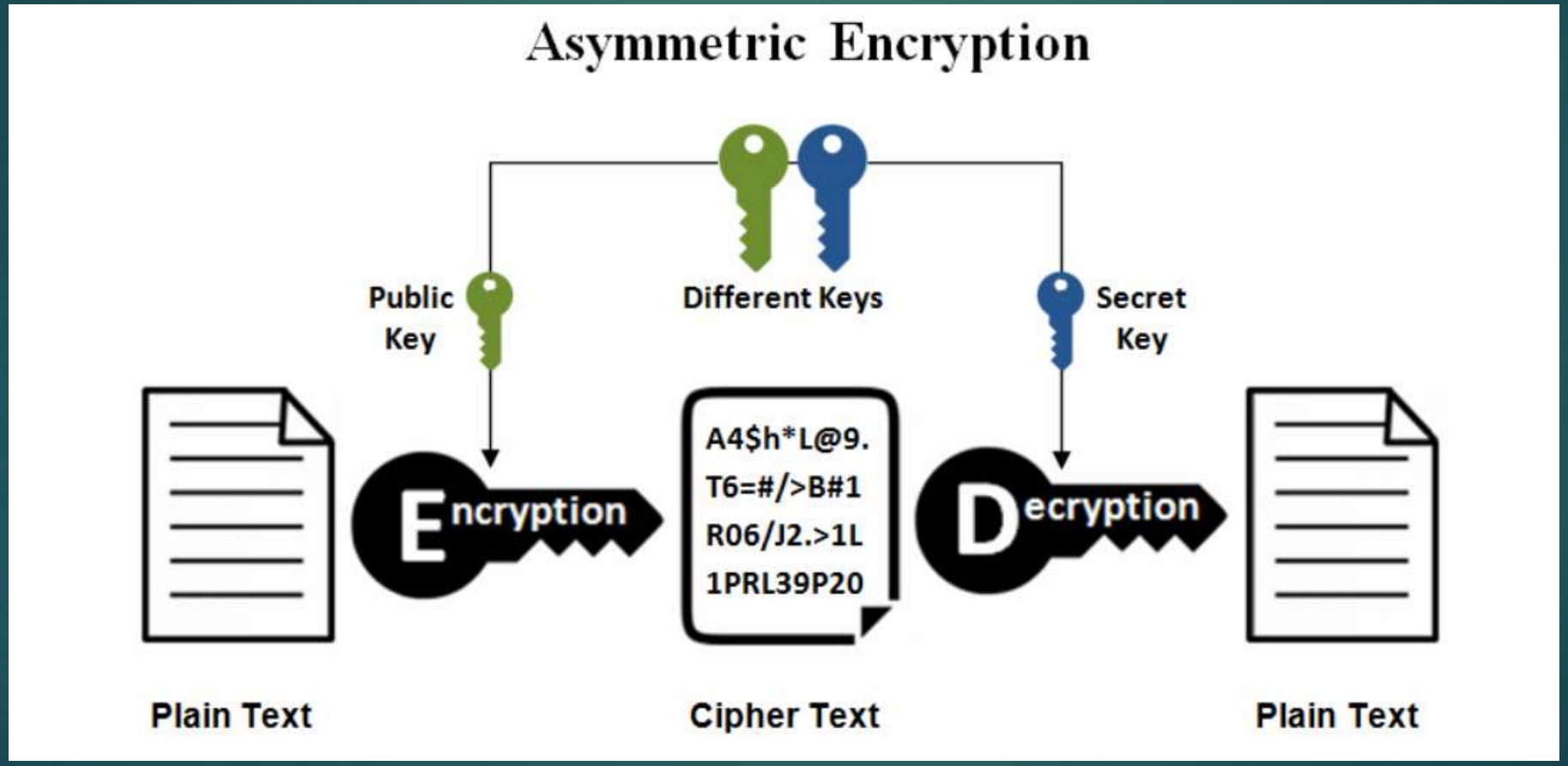
12.4 Authentication methods

- Authentication methods are techniques for re-identifying users.
- They are based on matching attributes that uniquely identify individuals.
- Traditionally authentication has been based on shared secrets used in conjunction with cryptographic algorithms.
- There are two main approaches to the use of encryption: the use of symmetric encryption algorithms and the use of public key algorithms.
- Smart cards (used in mobile phones) and biometrics (fingerprints and iris scans).

12.4.1 Symmetric and asymmetric key methods



12.4.1 Symmetric and asymmetric key methods



Difference Between Symmetric and Asymmetric Encryption

- Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetric encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.
- Symmetric encryption is an old technique while asymmetric encryption is relatively new.
- Asymmetric encryption was introduced to complement the inherent problem of the need to share the key in symmetric encryption model, eliminating the need to share the key by using a pair of public-private keys.
- Asymmetric encryption takes relatively more time than the symmetric encryption.

Key Differences	Symmetric Encryption	Asymmetric Encryption
Size of cipher text	Smaller cipher text compares to original plain text file.	Larger cipher text compares to original plain text file.
Data size	Used to transmit big data.	Used to transmit small data.
Resource Utilization	Symmetric key encryption works on low usage of resources.	Asymmetric encryption requires high consumption of resources.
Key Lengths	128 or 256-bit key size.	RSA 2048-bit or higher key size.
Security	Less secured due to use a single key for encryption.	Much safer as two keys are involved in encryption and decryption.
Number of keys	Symmetric Encryption uses a single key for encryption and decryption.	Asymmetric Encryption uses two keys for encryption and decryption
Techniques	It is an old technique.	It is a modern encryption technique.
Confidentiality	A single key for encryption and decryption has chances of key compromised.	Two keys separately made for encryption and decryption that removes the need to share a key.
Speed	Symmetric encryption is fast technique	Asymmetric encryption is slower in terms of speed.
Algorithms	RC4, AES, DES, 3DES, and QUAD.	RSA, Diffie-Hellman, ECC algorithms.

Trust Model implementation by PKI

- A Trust Model is the collection of rules that inform application on how to solve the legitimacy of a Digital Certificate.
- "Generally an entity can 'trust' the second entity if the first entity makes the assumption that the second entity will behave exactly as the first entity expects."
- Trust is defined as a binary relationship or set of compounded binary relationships, based on individual identity or unique characteristic validation.

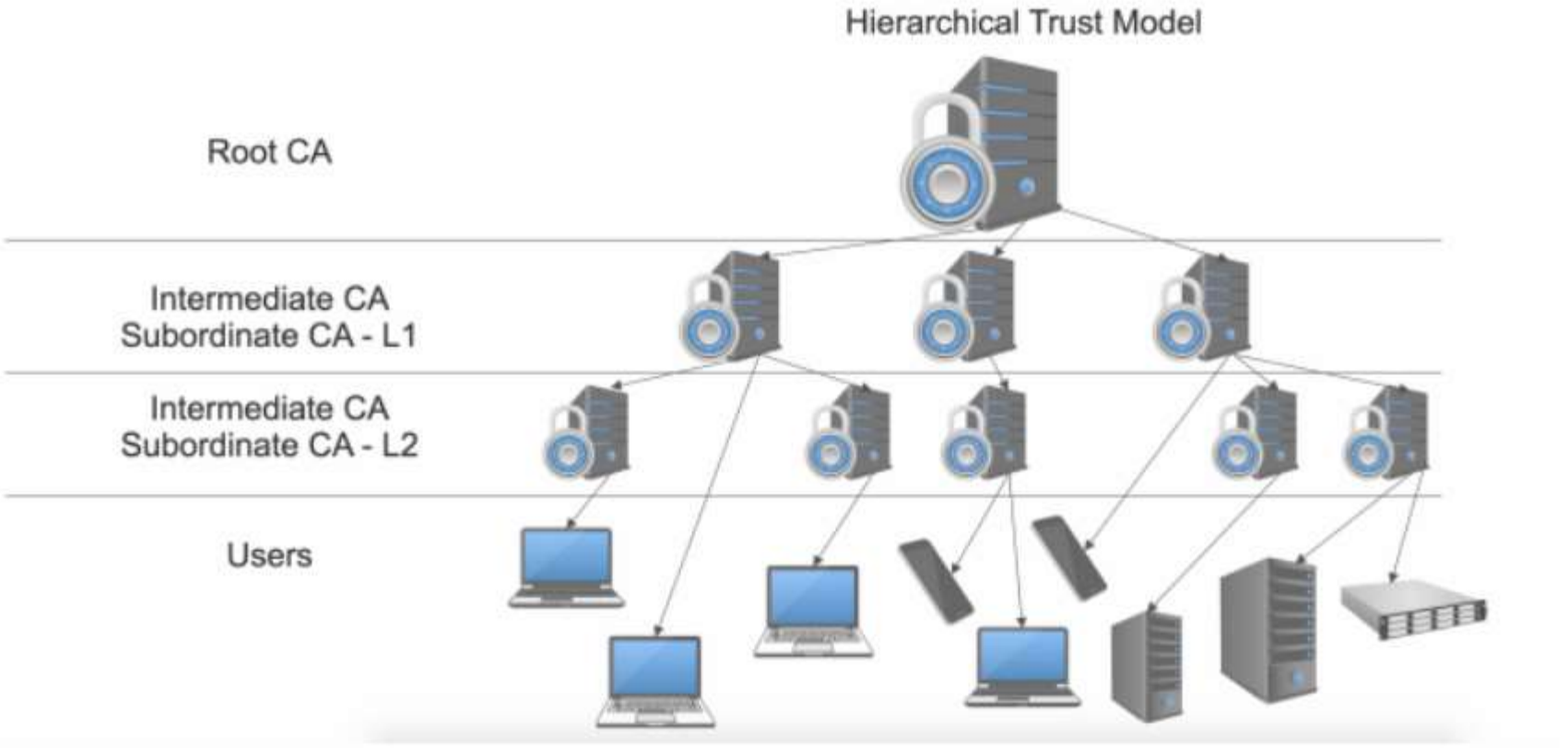
Trust Model implementation by PKI

- One of the best ways is Public Key Infrastructure (PKI) and there are four types that are used to implement the trust model with PKI.
- **A. Hierarchical Trust Model:**
- **B. Bridge Trust Model:**
- **C. Hybrid Trust Model:**
- **D. Mesh Trust Model:**

A. Hierarchical Trust Model:

- The hierarchical model or tree model is the most common model to implement the PKI. A root CA at the top provides all the information and the intermediate CAs are next in the hierarchy, and they only trust the information provided by the root. The root CA also trusts intermediate CAs that are in their level in the hierarchy.

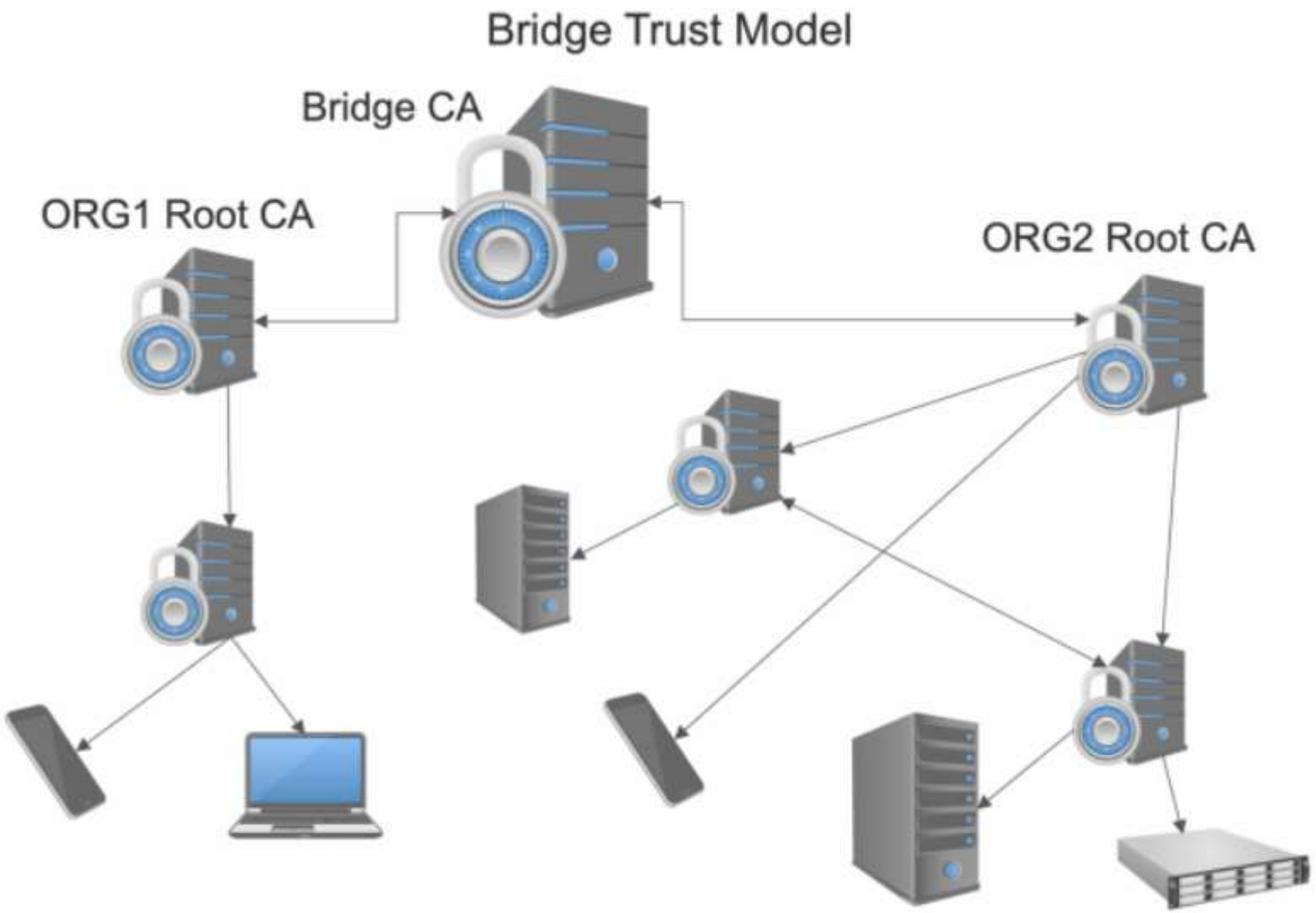
- This arrangement allows a high level of control at all levels of the hierarchical tree this might be the most common implementation in a large organization that wants to extend its certificate-processing capabilities. Hierarchical models allow tight control over certificate-based activities.



Hierarchical Trust Model

B. Bridge Trust Model:

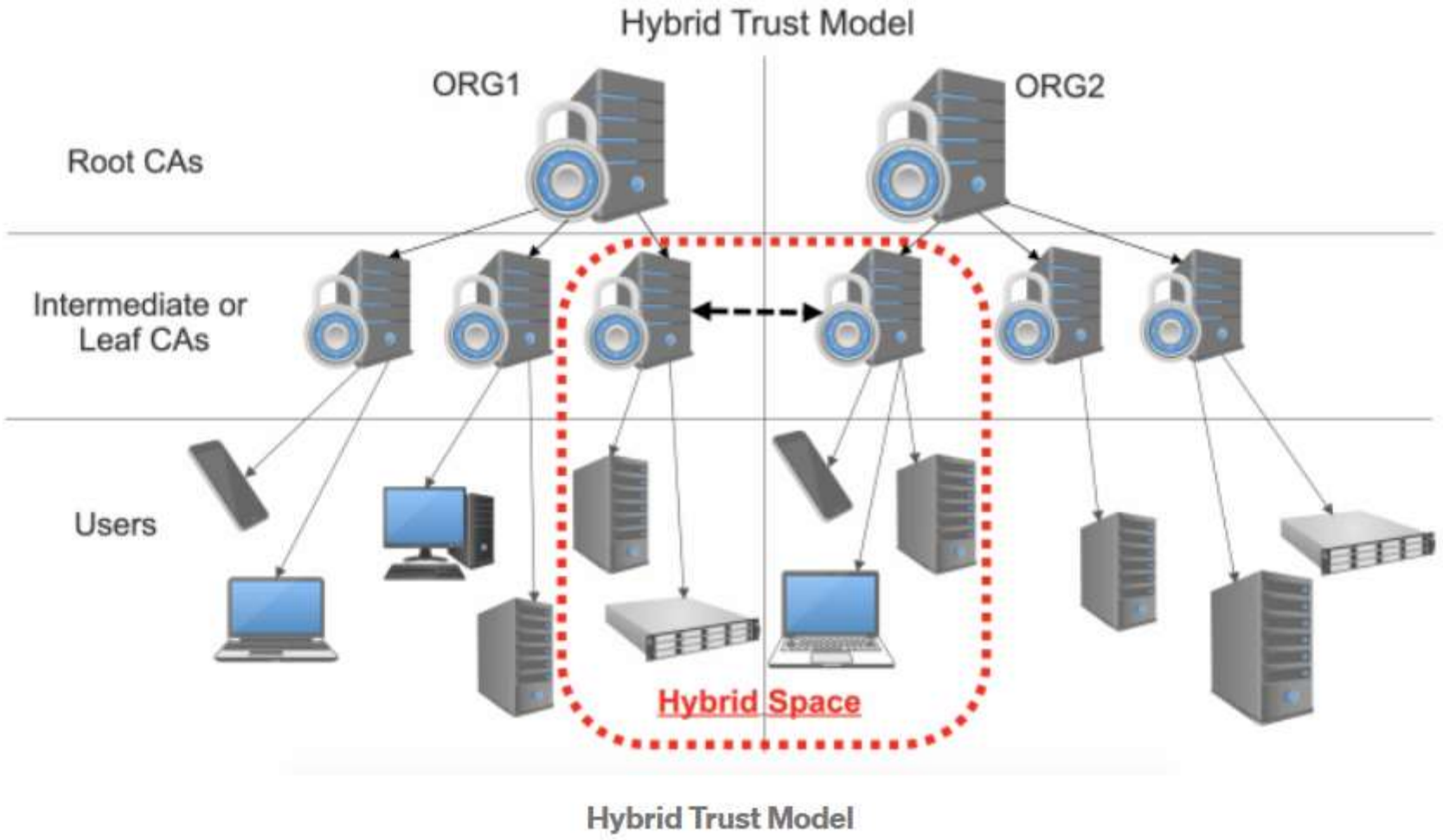
- In Bridge Trust Model we have many P2P relations between RootCAs that the Root CAs can communicate with each other and allow cross-certificates. This implementation model allows a certification process to be established between Organizations (or departments).
- In this model, each intermediate CA trusts only the CAs above and below it but the CA structure can be expanded without creating additional layers of CAs. Additional flexibility and interoperability between organizations are the primary advantages of a bridge model.



Bridge Trust Model

C. Hybrid Trust Model:

- Sometimes you need to link two or more organizations or departments in some part and separate other segments. When you need to make trust in some parts of two organization but you don`t want to be this trust in other segments of your organization. In these times the Hybrid Trust Model can be the best model for you. You can be extremely flexible when you build a hybrid trust structure and the flexibility of this model also allows you to create hybrid environments.
- Notice that in this structure, the intermediate CAs which are out of the hybrid environment can trust only to direct Root CA and Intermediate CAs in the hybrid environment, trust to all Root CAs that connect to any intermediate CA in the hybrid environment.

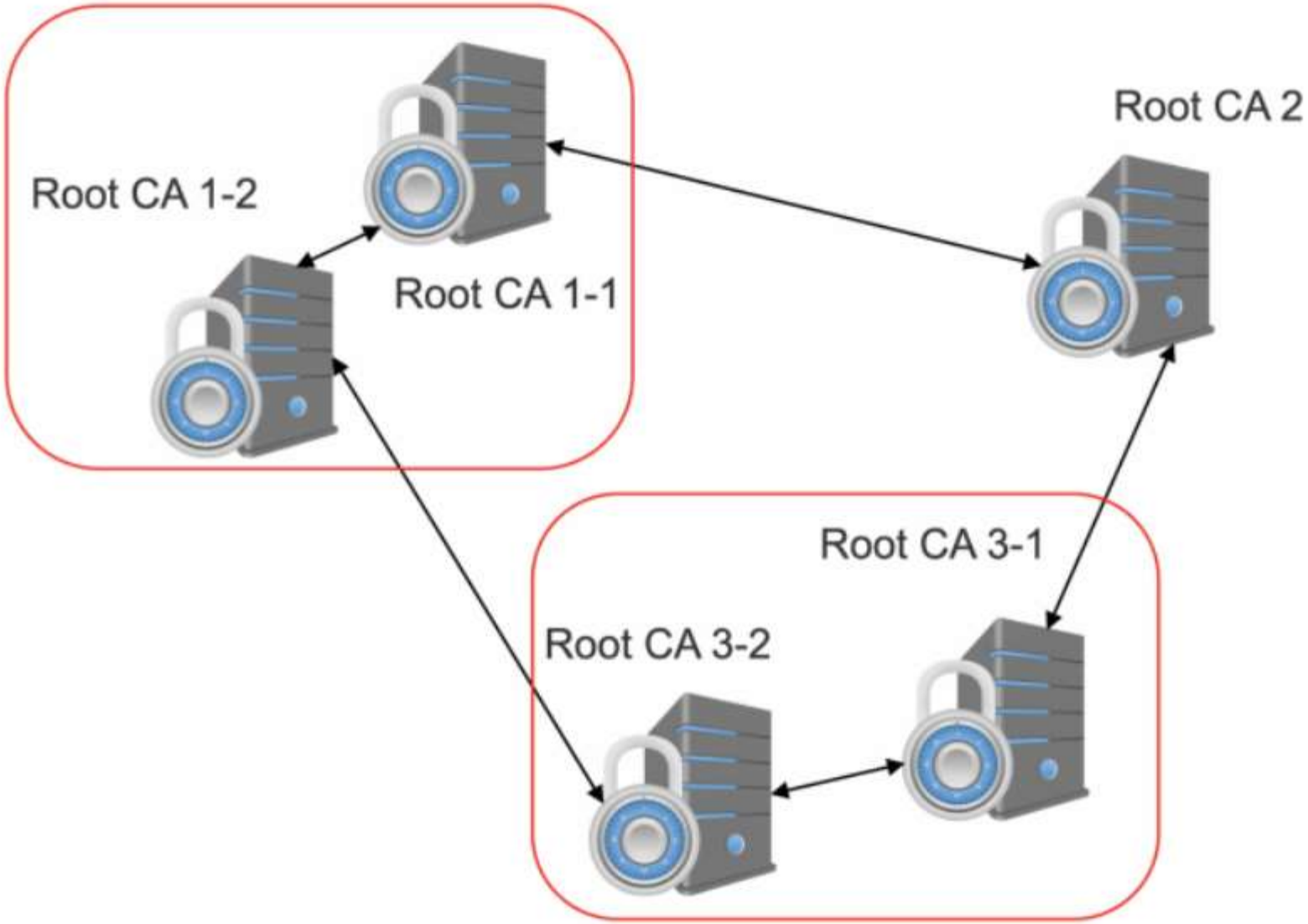


Hybrid Trust Model

D. Mesh Trust Model:

- When you want to Implement a Hierarchical Trust Model with cross-certification checking or a web of Root CAs, the mesh trust model is your best choice. In the other sights, the mesh model migrates the concepts of bridge structure with multi-paths and multi Root CAs.
- Certifications in each one of Root CAs are authorized in all of Root, Intermediate, and leaf CAs and all end-users that connected to each one of CA chains.

Mesh Trust Model



Mesh Trust Model

Zero Trust Model

- Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. **Zero Trust assumes that there is no traditional network edge**; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.
- Zero Trust is a framework for securing infrastructure and data for today's modern digital transformation. It uniquely addresses the modern challenges of today's business, including securing remote workers, hybrid cloud environments, and ransomware threats. While many vendors have tried to create their own definitions of Zero Trust, there are a number of standards from recognized organizations that can help you align Zero Trust with your organizatio

Zero Trust Model

- **Zero Trust is a significant departure from traditional network security which followed the "trust but verify" method.** The traditional approach automatically trusted users and endpoints within the organization's perimeter, putting the organization at risk from malicious internal actors and legitimate credentials taken over by malicious actors, allowing unauthorized and compromised accounts wide-reaching access once inside. This model became obsolete with the cloud migration of business transformation initiatives and the acceleration of a distributed work environment due to the pandemic that started in 2020.