**Project Name: CertHub**

**Description**:  
**CertHub** is a centralized **Certificate Management System** (CMS) that automates the issuance, revocation, and rotation of digital certificates across your organization. The system is built around the concept of **PKI (Public Key Infrastructure)**, featuring a multi-tier CA (Certificate Authority) structure, with a **Root CA**, **Intermediate CA**, and **Leaf CA** for efficient certificate management. Additionally, it includes **Root and Intermediate CA rotation** to ensure that cryptographic keys are periodically refreshed and infrastructure remains secure.

**System Overview:**

The system operates based on a **multi-tier CA hierarchy**, where:

1. **Root CA (Root Certificate Authority)**:  
   The highest authority in the certificate chain, responsible for signing intermediate CAs and providing the trust anchor for the entire PKI ecosystem. The **Root CA** should remain offline as much as possible to protect it from exposure.
2. **Intermediate CA (Intermediate Certificate Authority)**:  
   Serves as an intermediary between the **Root CA** and **Leaf CA** (end-entity certificates). It signs certificates for **Leaf CAs** or directly issues certificates for servers, services, or users. Intermediate CAs help mitigate the risk of compromising the Root CA.
3. **Leaf CA (Leaf Certificate Authority)**:  
   The certificate issued to individual devices, servers, or services. It is typically signed by an **Intermediate CA**. These are the certificates used in day-to-day operations, ensuring end-to-end encryption, identity verification, and trust.

**Core Features:**

1. **Centralized Certificate Management**:
   * **Issuing** and **revoking** certificates at each level (Root, Intermediate, Leaf).
   * Secure storage of private keys for Root and Intermediate CAs.
   * Full lifecycle management of certificates, including **expiration** and **renewal**.
2. **Automated Root and Intermediate CA Rotation**:
   * **Root CA Rotation**: Periodic generation of new Root CA certificates to replace old ones, ensuring long-term security and compliance with industry standards.
   * **Intermediate CA Rotation**: Rotation of Intermediate CAs to maintain the **trust chain** and improve security without needing to replace the Root CA.
   * Automated signing and replacement of certificates at the **Leaf CA** level upon rotation.
3. **Certificate Issuance Workflow**:
   * **Leaf CA** requests a certificate from the **Intermediate CA**.
   * The **Intermediate CA** signs the certificate request (CSR) and issues the **Leaf Certificate**.
   * Upon **Root CA rotation**, the **Intermediate CA** may also need to renew its certificate (signed by the new Root CA), and subsequently, all **Leaf Certificates** may need to be reissued.
4. **Secure Storage and Access Control**:
   * Private keys for **Root CA** and **Intermediate CA** are stored in **Hardware Security Modules (HSMs)** or **secure vaults** to prevent unauthorized access and ensure key protection.
   * Access to certificate management functions is **role-based**, with tight controls over who can issue, revoke, or rotate keys.
5. **Automated Alerts and Notifications**:
   * Alerts for **certificate expiration**, **Root/Intermediate CA rotation** events, and **rekeying actions**.
   * Notifications about any **security breaches**, **revocation requests**, or **issues with certificate chains**.

**Detailed Architecture:**

1. **Root CA**:
   * **Private Key Management**: The **Root CA private key** is **never exposed online** to minimize the risk of compromise. It is used only to sign **Intermediate CAs** and occasionally for **rekeying** purposes.
   * **Rotation of Root CA**: The **Root CA** certificate needs to be rotated (replaced with a new key) periodically (typically every 10–20 years). When the Root CA is rotated, all **Intermediate CAs** must also be re-signed by the new Root CA. This ensures the trust anchor is updated.
   * **Root CA Certificate Revocation**: In case of a breach or if a new Root CA needs to be generated, the old Root CA certificate should be revoked, and the new certificate should be trusted across the system.
2. **Intermediate CA**:
   * **Intermediate CA Rotation**: The **Intermediate CA** should also be rotated periodically (typically every 5–10 years). When the **Root CA** rotates, new **Intermediate CAs** are generated and signed by the new Root.
   * **Intermediate CA Signatures**: The **Intermediate CA** signs **Leaf CA** certificates. If the **Intermediate CA** is rotated, it will need to re-sign the **Leaf CAs** certificates issued under the old Intermediate.
   * **Intermediate CA Revocation**: If an Intermediate CA is compromised or its lifecycle is complete, it must be revoked, and all **Leaf CA certificates** signed by that Intermediate must also be revoked or reissued.
3. **Leaf CA**:
   * **Leaf Certificates**: These certificates are used for securing communication between servers and clients (e.g., HTTPS, email encryption). They can be issued by the **Intermediate CA**.
   * **Rekeying and Renewal**: Whenever the **Root CA** or **Intermediate CA** is rotated, the **Leaf CA certificates** need to be renewed or reissued to ensure they remain valid under the new trust chain.
   * **Automatic Renewal**: **Leaf CA certificates** can be automatically renewed as they approach expiration, ensuring minimal downtime or disruption.
   * **Revocation**: If a **Leaf certificate** is no longer valid (e.g., the associated private key is compromised), it should be automatically revoked, and a replacement issued.

**Automation of Root and Intermediate CA Rotation:**

1. **Root CA Rotation Process**:
   * **Pre-rotation planning**: Before rotating the Root CA, a new Root certificate is generated and signed by an existing trusted Root (or self-signed).
   * **Intermediate CAs Sign New Root CA**: All **Intermediate CA certificates** must be re-signed by the new Root CA.
   * **Leaf CA Reissue**: Once the **Intermediate CA** is updated, all **Leaf certificates** issued by the old Intermediate CA are reissued with the new Intermediate CA certificate.
   * **Trust Chain Update**: The trust chain in all systems relying on certificates must be updated to include the new **Root and Intermediate CAs**.
2. **Intermediate CA Rotation Process**:
   * **Pre-rotation**: New Intermediate CA certificates are generated and signed by the current Root CA.
   * **Leaf CA Reissue**: Existing **Leaf CA certificates** are reissued with the new **Intermediate CA certificate**.
   * **Automated Rotation**: The entire **rotation** process can be automated to ensure **minimal downtime** and a **seamless transition**.
3. **Reissue and Revocation Workflow**:
   * **Automated Reissue**: Once an Intermediate or Root certificate is rotated, the system automatically generates a new Leaf certificate, ensuring that trust is maintained.
   * **Revocation Management**: Revocation of old certificates happens as part of the rotation process, reducing human intervention.

**Security Considerations:**

* **Key Protection**: Ensure all private keys for Root, Intermediate, and Leaf CAs are stored securely using HSMs or encrypted vaults.
* **Multi-Factor Authentication (MFA)**: Use **MFA** for accessing the certificate management system, especially for administrative tasks like rotation and revocation.
* **Audit Logging**: Every action (certificate issuance, rotation, revocation, etc.) should be logged to ensure accountability and traceability.