**Environment Support Guidelines for Modifying or Updating Active Certificates**

**Purpose**

This document defines the standard procedure for managing **modifications or updates to active TLS certificates**. It ensures all environment support requests are properly scoped, risk-assessed, and executed with minimal impact to live systems.  
These requests typically cover **core certificate lifecycle changes** such as SAN additions, malcode updates, or crypto-related configuration support.

**1. Understanding the Request and Requirements**

Environment support tickets must be clearly distinguished from standard certificate issuance or renewal requests. They are intended **only** for controlled updates to existing, active certificates as part of ongoing lifecycle management.

**Scope of Support:**

* **Core Changes:**
  + Addition or modification of SAN values.
  + Updates to malcode or environment-specific identifiers.
  + Crypto-related configuration assistance (e.g., key usage clarifications, cipher compatibility).
* **Out-of-Scope Requests:**
  + Requests that replace standard certificate renewals, re-issuances, or new deployments.

**Key Intake Requirements:**

* Provide a **complete and precise description** of the required change.
* Confirm if **specific approvals or discussions** are needed prior to implementation — especially for **malcode-related changes**.
* Recognize that each change to a live certificate (particularly **PROD**) carries potential **operational risk** and must be handled with **extreme caution**.
* Review and understand the **application stack**, **dependency chain**, and **deployment path** associated with the certificate before initiating any modification.
* For **non-crypto related certificates**, consider processing through a **renewal request** initiated by the deployment group rather than an environment support ticket.

**2. Effective Due Diligence**

Every environment modification must undergo strict due diligence to ensure technical correctness, environment consistency, and compliance with security policies.

**Due Diligence Checklist:**

* **SAN Validation:**
  + Ensure all new SAN values belong to the **same environment tier** (e.g., all SIT or all PROD).
  + Do **not** include SANs that are part of a migration or cross-environment effort.
* **Malcode Changes:**
  + Must be **approved by the Technical Authority Office (TAO)** for both the old and new malcodes.
* **Common Name (CN) Changes:**
  + **Not permitted** for existing active certificates.
  + *Exception:* If the certificate was recently issued, never deployed, and approval is granted, limited CN changes may be considered.
* **Template Considerations:**
  + Verify **Root CA trust** and correct **template alignment**, especially for **internal certificates** and **X9-issued vendor certificates**.
  + Changing a certificate template can affect chain trust and should be approached with caution.

**3. Delivery and Commitments**

After verification and approvals, the certificate update must be executed and delivered in a controlled, documented, and auditable manner.

**Delivery Guidelines:**

* **Accuracy:**
  + Ensure the updated certificate reflects the requested and approved changes exactly.
* **Password Handling:**
  + Use the **existing password** associated with the original certificate issuance.
* **SLA Adherence:**
  + Maintain SLA timelines to prevent escalation or service impact.
* **Traceability:**
  + Ensure both the **certificate renewal request** and **support ticket** reference each other through shared metadata:
    - Request numbers
    - SAN values
    - Malcode references
    - Template information
* **Deployment Coordination:**
  + Coordinate with the application or infrastructure team to **redeploy the application** if necessary (e.g., LTM or server-side redeployments to ensure the new certificate is loaded).

**4. Common Mistakes to Avoid**

The following errors are frequently observed during certificate modification activities. Each should be carefully checked to prevent incidents or rework.

| **Category** | **Common Error** | **Impact / Note** |
| --- | --- | --- |
| **SAN Entries** | Wrong SAN values (e.g., dash “-” vs dot “.” interchanged) | Causes certificate mismatch and application failure |
| **Environment Scope** | Including higher-environment SANs (e.g., PROD) in lower-environment certificates (e.g., SIT) or vice versa | Violates environment isolation and increases risk |
| **Template Selection** | Incorrect template used, especially for iOS or device-specific certificates | May break device authentication or MDM integrations |
| **Wide SAN Scope** | Overly broad SAN entries introducing a single point of failure | Reduces security posture and may affect renewal scope |
| **Missing Tickets** | Installation or redeployment tickets not created | Causes incomplete delivery or audit gaps |
| **OU Details** | Missing Organizational Unit (OU) field during renewal | May break certificate-based authentication or policy mapping |