TLS Certificate Request Intake Process Guidelines

Purpose

This document provides standardized guidelines for TLS Certificate Request Intake Coordinators to ensure all certificate requests are reviewed, validated, and processed with accuracy, consistency, and compliance. The process is divided into three key stages:

1. **Understanding the Request and Requirements**
2. **Effective Due Diligence**
3. **Delivery and Documentation of Commitments**

---

1. Understanding the Request and Requirements

Each TLS certificate request must be evaluated independently — **not based on any prior request** with similar attributes. Intake coordinators must review and validate all information provided before proceeding.

Key Verification Steps:

- **Environment Identification:** Determine whether the request is for **DEV**, **SIT**, **PAT**, or **PROD** environments.
- **Certificate Template Selection:** Verify that the appropriate **certificate template** is used based on the environment type and intended use.
- **Common Name (CN) and Subject Alternative Name (SAN):**
  - Ensure CN and SAN values follow approved **naming conventions**.
  - Confirm that CN and SAN fields accurately represent the intended endpoint(s).
- **Deployment Group & Clarity Code:** Validate correct assignment based on deployment ownership and tracking.
- **Hosting Type:** Identify whether the request is for **Azure** or **Non-Azure** environments.
- **Installation Requirements:** Determine whether installation assistance is required or if it will be self-managed by the requestor.

Note: Each request must be handled on its own merits. Avoid assumptions or replication from previous tickets.

---

2. Effective Due Diligence

Before certificate issuance, the coordinator must conduct thorough due diligence to confirm **accuracy, relevance, and compliance** of the request.

Checklist for Due Diligence:

- **Purpose Identification:**
  - What is the **intended use** of the certificate?
  - Which **application, system, or service** will it secure?
- **Environment Context:**
  - Confirm deployment environment (DEV/SIT/PAT/PROD).
  - Verify if the certificate will be **server-side** or **client-side**.
- **Integration Context:**
  - Identify if the request supports **LTM (Load Traffic Manager)** configurations or **vendor integrations**.
- **Application Stack Awareness:**
  - Document whether the certificate will be deployed on **Windows, Linux, or appliance-based** infrastructure.
- **Certificate Type:**
  - Specify **Internal** or **External** consumption.
  - Identify the required **format** (e.g., `.CER`, `.PFX`, `.PEM`).
- **Project Association:**
  - Determine whether the request is tied to a **specific project or release**.
- **Completeness Validation:**
  - Ensure that the request **satisfies all policy requirements** and **completes the Description field** with:
    - Application name and environment
    - Purpose of the certificate
    - Associated project name (if applicable)
    - Key usage (Server Authentication, Client Authentication, etc.)
    - Any installation or dependency notes

---

3. Delivery and Documentation of Commitments

Once validation is complete, ensure timely and compliant delivery of the issued certificate.

Issuance and Delivery Guidelines:

- **Accuracy and Completeness:**
  - Deliver only fully verified and correctly formatted certificates.
  - Validate correct certificate chain before issuance.
- **Recipient Handling:**
  - Deliver the certificate to the **authorized requester**, **LTM administrator**, or **third-party contact** as appropriate.
- **Password Sharing:**

    - Share private key passwords securely following the **approved key management procedure**.
- **Internal Documentation:**
    - Record certificate details in the internal tracking system, including:
        - Request number and environment
        - CN/SAN and issuance date
        - Expiry date and renewal reminders
        - Owner contact and deployment notes
- **SLA Adherence:**
    - Ensure each request meets defined **Service Level Agreements (SLAs)** to prevent escalation.
- **Follow-up and Closure:**
    - Track pending issues (installation, testing, or dependency resolution).
    - Confirm successful deployment and update internal logs.
- **Archival and Coding:**
    - Categorize each request based on **issuance type** (Internal, External, Renewal, Replacement).
    - Ensure all information is complete for **future audits or renewals**.

Summary

Stage	Focus	Key Actions
1. Understanding the Request	Classification & Initial Validation	Validate environment, CN/SAN, templates, hosting type
2. Effective Due Diligence	Context & Purpose Verification	Verify usage, stack, integration, and compliance
3. Delivery & Commitments	Issuance & Documentation	Deliver securely, maintain SLA, update logs