



Certilgent

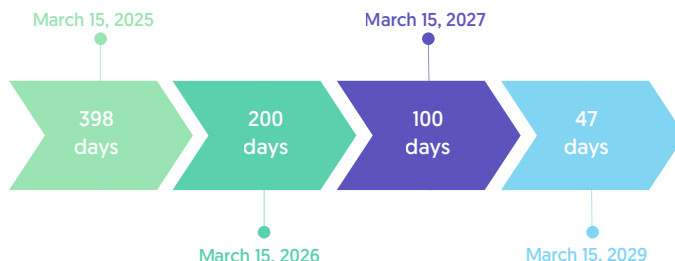
Automated TLS Certificate Renewal

Security without manual work



Why is Certificate Automation no Longer Optional?

Digital certificates are a core part of how all systems should establish trust. However, the way they are issued and maintained has fundamentally changed. The **CA/Browser Forum (CA/B Forum)**, supported by all major browser vendors (Apple Google, Microsoft, Mozilla), has defined a **mandatory, accelerated reduction of public TLS certificate lifetimes**. What was once an annual operational task is becoming a **monthly, continuous process**.



This increases renewal frequency by **8-12x** compared to traditional yearly cycles. Manual processes, scripts, and fragmented tools do not scale under these conditions and significantly increase the risk of outages, security gaps, and audit findings.

Automation is no longer an optimization. It is a prerequisite for compliance, availability, and security.

Certilgent is designed specifically to address this new reality.

The Concept

Certilgent is a platform for **centralized, automated management of TLS digital certificates** across heterogeneous IT environments. It enables organizations to issue, renew, revoke, and monitor certificates through their entire lifecycle, while aligning operations with the accelerating requirements dictated by the CA/B Forum and modern security practices.

Certilgent is designed for **financial institutions, regulated enterprises, and large organizations** that require strict security controls, auditability, scalability, and flexibility in deployment.



Certilgent Agent

Certilgent Agent is a component installed on the customer's infrastructure to automatically discover TLS certificates already present on their servers. Once approved, the Agent automates certificate renewal and required post-renewal actions, eliminating the need to manually issue certificates through a separate ACME client.

Key Features

Complete Certificate Visibility

Automatically discovers TLS certificates across the infrastructure and maps them to the servers, applications, and services using them.

Centralized Management

Enables centralized Agent configuration and management without requiring a restart.

Automated Renewal and Management

Once approved, certificates are automatically renewed on time, with all required post-renewal actions, such as restarting services or containers, handled automatically.

Security by Design

Operates with minimal server privileges, requires no inbound ports, and is distributed with a digital signature.

Wildcard Certificate Distribution

Automatically distributes renewed wildcard certificates to all servers using them.

Simple Installation

Installs on a server within minutes, with the option to review planned actions before they are executed.



Solution Architecture

Certilgent: Solution Capabilities

Automated Renewal

Automates certificate renewals to reduce manual work, ad hoc scripting, and human error while ensuring certificates are renewed on time.

Outage Prevention & Proactive

Monitoring

Automatically renews certificates and alerts administrators about upcoming expirations or failed renewals, helping prevent service disruptions.

Centralized Visibility & Management

Provides a single, authoritative view of certificates, including their status, issuance history, and renewal workflows, through an intuitive management dashboard.

CA Independence & Flexible Integration

Integrates with multiple public and private Certification Authorities through ACME and REST APIs, supporting CAs such as DigiCert, Sectigo, EJBCA, GoDaddy, Let's Encrypt, and ZeroSSL.

Enterprise-Scale Performance

Designed to reliably manage thousands of certificates while maintaining high performance, availability, and operational reliability.

Multi-Tenant Architecture

Enables secure segregation of certificates, configurations, and operations across multiple tenants, making it suitable for organizations managing certificates for multiple customers or business units.

Built for High-Frequency Renewals

Supports short-lived certificate policies and frequent renewals without increasing operational overhead, making it suitable for modern automated certificate environments.

Enterprise Security & Auditability

Provides the security controls, traceability, and auditability required for enterprise and regulated environments.

Use Cases by Industry



Banking & Financial Services

Automate certificate renewals for online banking portals, APIs, mobile apps, open banking / PSD2 interfaces, payment gateways (POS backend, card payment systems), and critical internal systems such as core banking platforms and VPNs to ensure regulatory compliance and prevent service outages.



Regulated organizations

Manage certificates across highly controlled and audit-sensitive environments, including internal applications, external services, and secure network components, with full traceability, policy enforcement, and centralized governance.



Large Enterprises

Manage thousands of certificates across web applications, email servers, VPNs, microservices with centralized visibility, automation, and operational control.