



Digital Certificate Management Service



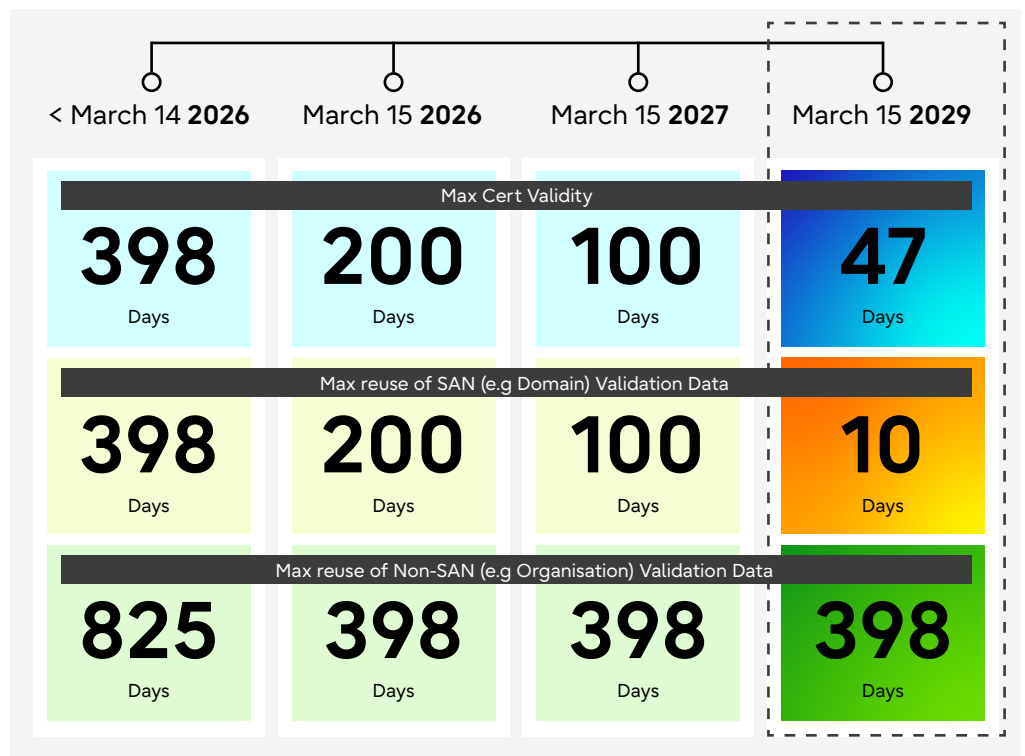
How will you keep up as certificate lifetimes shrink?

TLS certificate lifetimes are rapidly shrinking driving a significant increase in renewal frequency and operational complexity. from 398 days today to as little as 47 days by 2029 - forcing organisations to renew certificates up to eight times per year.

Manual certificate tracking and renewal will become increasingly difficult as renewal frequency increases.

Without automation and centralised control, the risk of outages, misconfigurations and compliance gaps increase.

Siloed management, legacy PKI tools and reactive processes result in limited visibility, reduced control and a higher likelihood of business disruption.



Organisations need to move toward automated certificate discovery, renewal, deployment and governance.



Fujitsu, in partnership with DigiCert, help organisations respond to this change by:



Modernising certificate lifecycle management



Automating processes



Improving visibility



Reducing operational risk



Improving audit readiness and compliance posture

Take control of your certificate lifecycle

Built on DigiCert's Trust Lifecycle Manager and enhanced by Fujitsu's integration and managed service expertise, our joint solution delivers end-to-end control across certificate discovery, issuance, deployment and renewal.

It enables organisations to gain full visibility of certificates across hybrid and multi-cloud environments, enforce consistent governance policies, and integrate certificate management seamlessly into existing enterprise systems and DevOps workflows. By automating lifecycle processes and simplifying operations, Fujitsu helps organisations reduce risk, improve efficiency and scale securely as certificate volumes and renewal demands increase.

Why act now: While the key milestones may seem distant, certificate-related outages and compliance gaps are already a risk, and shorter lifecycles will only increase their likelihood. Modernising takes time. Acting now allows organisations to stay ahead of the change, rather than reacting under pressure.

Our experience suggests that ...

2025 > 2026 =

2x

operational effort

2026 > 2027 =

4x

operational effort

2029 =

8x

operational effort

Prevent outages and reduce risk

Automated certificate and PKI lifecycle management to eliminate expired or misconfigured certificates.

Simplify operations at scale

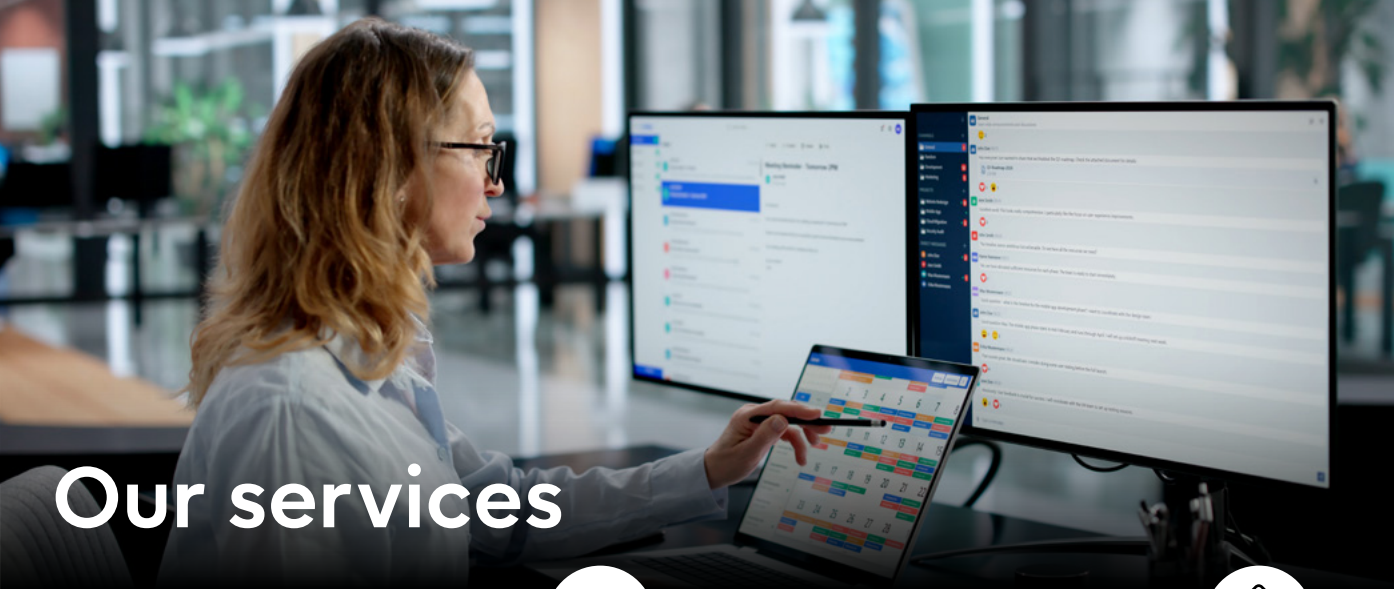
Centralised management and automation reduce manual effort, eliminate inefficiencies and enable teams to manage certificates consistently.

Enable agility and compliance

Tailored deployment and managed services that support hybrid and multi-cloud environments while meeting regulatory requirements.



DigiCert provides the technology platform. Fujitsu provides the services layer to help your organisation design, implement, integrate and operate effectively.



Our services



Digital certificate health check

A point-in-time consultation to map your current processes, define a target automated state, identify key blockers, and provide feasibility-led solution approaches, along with expert support for any DigiCert-related technical queries.

Typically: 10-20 days

Suitable for organisations looking to validate their approach or plan their next step.



Digital certificate lifecycle management as a service

Provides organisations continuous monitoring, automation, and optimisation of your certificate environment, ensuring visibility, compliance, and reduced operational risk.

Ideal for organisations seeking to centralise control and remove the burden of manual certificate management.



Why choose us

Fujitsu supports organisations across the full certificate lifecycle, including current-state assessment, operating model design, platform implementation, integration with enterprise systems, automation enablement, managed operations and ongoing reporting.

Contact us today.

Stay ahead of evolving compliance and cyber threats.

