Prevent service outages with ServiceNow® Certificate Inventory and Management

The IT challenge

TLS certificates are the standard for establishing trust in digital environments. By authenticating the identity of websites—and more broadly, digital services—they prevent impersonation by malicious actors, and they also provide the foundation for secure, encrypted communications.

By design, TLS certificates expire and need to be renewed. This is critical for maintaining trust. It ensures that the issuing certificate authority periodically revalidates the certificate owner, and that certificates keep pace with the latest security technology. However, certificate expiration is a two-edged sword. If a certificate expires, it's no longer trusted. Web browsers display warnings that frighten off users, and machine-to-machine communication shuts down. The result? Expired certificates are responsible for a significant number of service outages and security breaches, including many well-publicized, high-impact incidents.

That's why it's so important to renew your certificates before they expire. However, this is no easy task. Typical enterprises have thousands of certificates, and that number continues to increase as businesses digitize and adopt highly distributed, cloud-based microservice architectures. It's not as easy as automatically renewing certificates before they expire with your certificate authority—or more likely, multiple certificate authorities. For example, you may need to upgrade certificates in planned maintenance windows to avoid service downtime.

In fact, there isn't even an easy way to associate certificates with digital services—no service context that helps you to understand the criticality of each certificate, identify the responsible service owner, determine whether a certificate is in a production or development environment, drive renewal approvals and workflows, or even decide whether a certificate needs to be renewed.

It's no wonder that many organizations struggle with the sheer volume of work required and still end up with expired certificates—experiencing devastating outages and breaches as a result.

The ServiceNow solution

ServiceNow® Certificate Inventory and Management creates a centralized inventory of your certificates and drives optimized renewal workflows. It leverages your existing ServiceNow® Visibility mechanisms[1] and configuration—for example, previously configured IP ranges—to identify certificates in your IT environment. This provides a complete record of your certificates with little or no additional effort. Certificate Inventory and Management then associates these certificates with corresponding CIs in your ServiceNow® CMDB, adding the service context needed to drive efficient, accurate renewal processes.

Certificate Inventory and Management then optimizes these renewal processes. This includes getting as raising incidents for expired certificates. This ensures that you assess and renew certificates if required before they expire, and that you quickly remediate expired certificates. This can be managed with customized policies that allow for robust levels of automation You can automatically request, renew, and revoke certificates using the ServiceNow Service Catalog, providing a complete solution for managing the lifecycle of your certificates. The result? You avoid service outages and security breaches while reducing operational costs and time.

approvals and assigning renewal tasks when a certificate is about to expire, as well Certificate Inventory and Management also comes with an intuitive Certificate Management dashboard that shows you the summary status of your certificates at a glance. From here, you can drill into the details to identify and resolve issues. And because Certificate Inventory and Management provides a complete inventory of your certificates, you can now optimize your certificate portfolio across multiple certificate authorities.

1. Certificate Inventory and Management also integrates out of the box with GoDaddy, DigiCert, Entrust, and Sectigo, allowing you to extract certificate information directly from your certificate authorities.

See all of your certificates in on place

Automatically discover your deployed certificates, creating a centralized inventory in your CMDB.

Automate TLS certificate operations

Define and create custom policies that allow zero touch automation for request, renewal, and revoking of TLS certificates.

Avoid service outages and security breaches

Drive optimized certificate renewal processes, including renewing soon-to-be-expired certificates and raising incidents for expired tickets.

Focus on what matters

Prioritize renewal of certificates that support mission-critical services. Eliminate the cost of renewing certificates that are no longer needed.

Reduce operational effort

Improve your certificate management processes with service-aware workflows that automatically assign work to the right application and service owners and track its progress.

Rapid time to value

Leverage your existing ServiceNow CMDB and Visibility investment to manage your TLS certificates with little or no additional effort.

Scale for digitalization

Keep pace with rapidly increasing certificate volumes as your business digitalizes more and more processes and adopts cloud-based microservice architectures.

servicenow.