SSL.COM WHITE PAPER

Improving PKI Resilience with a Backup Certificate Authority



CONTENTS

Table of Contents

01 Build a resilient, flexible, and secure certificate infrastructure 3

02 Understanding the Root Causes of Mass Certificate Revocations 7

03 The Strategic Value of a Backup Certificate Authority 8

04 A 5-Step PKI Administrator's Guide to Navigate Certificate Authority Disruptions 10

05 Key Technical Considerations in a Backup CA 13

06 Reinforcing Trust with a Backup CA 15

SECTION 01

Build a resilient, flexible, and secure certificate infrastructure

Secure and reliable certificate management is the foundation for business resilience. After all, digital certificates are the backbone of secure communications, data protection, identity verification, and regulatory compliance.

A Certificate Authority (CA) is responsible for issuing, managing, and revoking certificates as well as validating the identity bound to a certificate. However, many organizations rely only on a single primary CA. But what happens if certificates from a single CA are revoked or the service is no longer available? Disruptive CA events such as mass revocations and browser distrust can be unforgiving, as we've seen with past major CA incidents:

Symantec Distrust — 2018

The Symantec Distrust (2018) is perhaps the most comprehensive and historically notable example of CA operational failure and its cascading effects. Chrome distrusted the Symantec Certificate Authority after repeated failures by Symantec to comply with the baseline requirements for issuing and managing publicly trusted certificates. The distrust process unfolded in phases, with certificates issued before June 1, 2016, stopping functionality in Chrome 66, and all remaining Symantec SSL/TLS certificates ceasing to work in Chrome 70.

Since Symantec certificates were behind about a third of the TLS-equipped sites on the internet, the impact was massive, forcing millions of websites to obtain replacement certificates or face browser warnings for their users.

Entrust Distrust — 2024

The Entrust Distrust (2024) is likely the most dramatic recent example of a single CA dependency risk. In November 2024, Google Chrome, Apple, and Mozilla distrusted the new issuance of Entrust certificates because they fell short of browser expectations for a publicly trusted Certificate Authority.

The distrust affected several major organizations, posing immediate operational challenges as these high-traffic websites faced potential browser warnings. Organizations that had relied solely on Entrust as their primary CA scrambled to obtain replacement certificates from alternative providers to mitigate service disruptions.

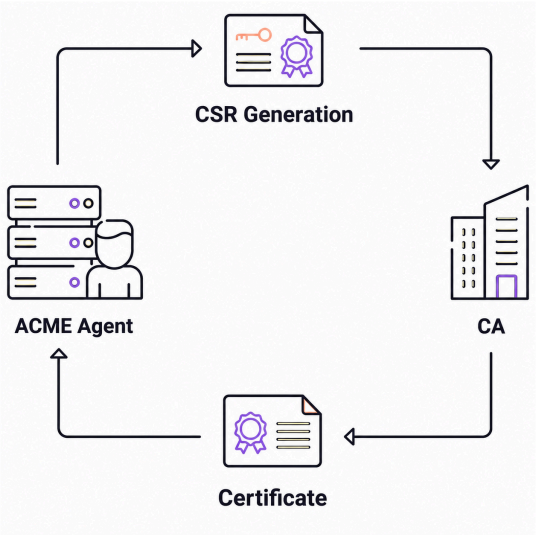
DigiCert Mass Revocation — 2024

The DigiCert mass revocation event (2024) demonstrated that even the most reputable Certificate Authorities can experience critical failures that require immediate action. DigiCert was forced to mass-revoke SSL/TLS certificates due to a bug in its verification process for determining whether a customer owned or operated a domain, which required impacted customers to reissue their certificates within 24 hours. The incident affected over 83,000 SSL certificates across 6,807 customers, with major corporations such as Bloomberg, ABB, Yahoo, and Hitachi among the most impacted organizations, presenting unprecedented pressure on IT teams worldwide.

When a primary CA becomes unavailable, whether caused by regulatory actions, compliance failures, or technological bugs, customer security dependencies can grind to a halt due to the inability to manage certificates effectively. The cost of downtime goes well beyond technical aspects. A lone CA's failure can disrupt operations, resulting in revenue loss, reputational damage, compliance issues, and amplified security exposure.

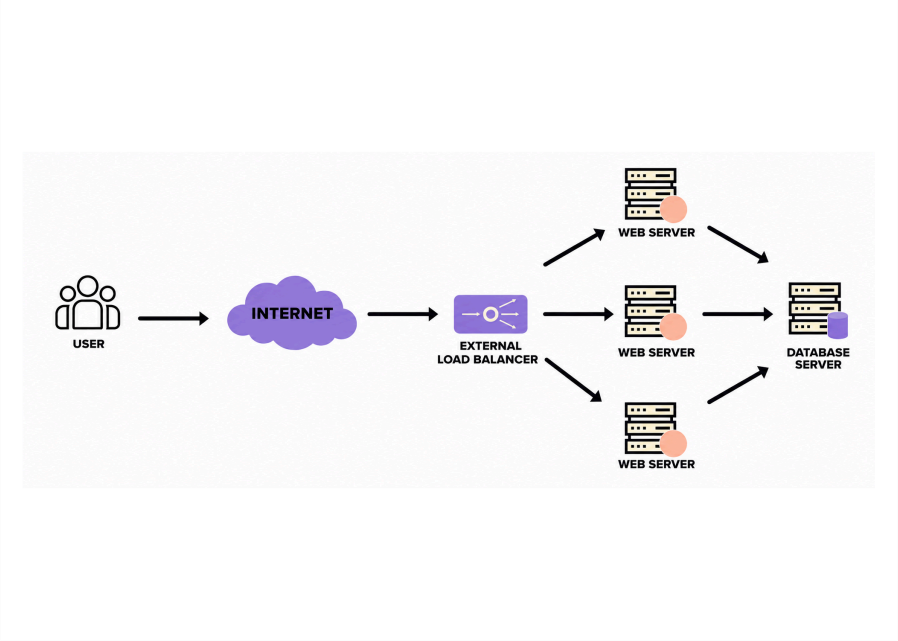
To mitigate risks, forward-thinking organizations can implement several strategies to strengthen their digital resilience against certificate-related disruptions, including:

ACME protocol integration — Reduces human error by enabling automation of the certificate renewal process for SSL/TLS certificates



Certificate transparency monitoring systems — Continuously scan public logs for unauthorized certificates issued against their domains

Load balancing and redundant infrastructure design — Help distribute certificate dependencies across multiple endpoints, reducing the impact of individual certificate failures



Internal Certificate Authorities (for non-public facing communications) — Network segmentation ensures that certificate failures in one domain don't cascade to unrelated systems

Above all, investing in a backup Certificate Authority (backup CA) as part of your digital resilience strategy is the most sophisticated approach to avoid issues from mass revocation or unexpected distrust events. This white paper explores the necessity of a backup CA and key implementation strategies.

SECTION 02

Understanding the Root Causes of Mass Certificate Revocations

Mass certificate revocations occur when Certificate Authorities must comply with stringent industry standards that prioritize the security and integrity of the internet's encryption infrastructure. Every public CA must comply with the Baseline Requirements that the CA/Browser Forum sets and determines by voting members of the CA and browser communities. Revocation becomes mandatory under specific conditions that compromise the certificate's validity or security.

Additionally, violations of the CA's Certificate Policy (CP) or Certification Practice Statement (CPS) can occur due to various factors, including failure to follow the defined processes for issuance, failure to maintain the required security measures, or using digital certificates for unauthorized purposes. These policy violations can manifest in numerous ways that may seem minor but carry significant consequences under industry standards. For instance, CAs may discover that their validation procedures deviated from documented processes, such as inadequate verification of organizational details during Extended Validation (EV) certificate issuance, or failure to properly document and audit certificate requests as required by their CPS.

Security measure violations might include insufficient protection of public key infrastructure, inadequate logging of certificate operations, or failure to meet the physical security requirements for hardware security modules (HSMs). Compliance requirements leave CAs with no choice but to revoke digital certificates when violations are discovered, regardless of the impact on subscribers.

SECTION 03

The Strategic Value of a Backup Certificate Authority

A backup CA is not merely a fail-safe. Without it, even a temporary lapse in certificate issuance capabilities can cascade into broader security and availability issues for your customers. The strategic advantages of a backup CA fall into several critical areas:

Service Disruption Prevention

A functioning CA is crucial for issuing, renewing, and revoking certificates that help keep your applications, websites, internal networks, and communications secure. Consider that if your only CA suddenly becomes unavailable, you could experience numerous problems with services that rely on valid certificates, including trust warnings on your website, application failures, devices no longer accepting new certificates, and failed user authentications. A backup CA acts as a safety net, allowing your certificate operations to run smoothly with minimal, if any, disruption.

Compliance Resilience

Various compliance standards, such as ISO/IEC 27001, NIST SP 800-53, HIPAA, and PCI DSS, all emphasize the importance of system availability and mandate the availability of critical infrastructure components, including certificate services and continuity. For example, the National Institute of Standards and Technology (NIST) cites resilient key management and contingency planning as cybersecurity tenets. A backup CA helps satisfy these requirements and contributes to compliance readiness, providing auditors with evidence of redundant capabilities and proactive risk management.

Business Continuity

Organizations must take a balanced approach to security and continuity. A backup CA helps organizations avoid catastrophes by continuing to issue and validate certificates, maintain secure authentication protocols, and preserve user trust during emergencies.

Enterprises can also avoid bandwidth congestion for IT teams that might require hours or even days to manually restore the CA and trust without automated failover mechanisms. Moreover, if you have a disruption while you're providing a service to another customer and that service is suddenly disrupted because of the CA's inability to issue certificates, you may then inadvertently violate a service-level agreement (SLA) with another entity.

Maintaining your primary Certificate Authority is especially vital for businesses in highly regulated industries or those with continuous, 24/7 operations. With a solid backup in place, your leadership (and customers) can have peace of mind knowing that internal systems stay connected and external services remain accessible, even if the primary CA is offline.

Disaster Recovery Planning

When mass revocations occur, operations can grind to a halt. During critical incidents, organizations without a backup CA will likely experience extended downtime periods, weakened security posture, and operational paralysis. Certificate Authority disruptions represent a critical threat vector that must be integrated into comprehensive disaster recovery planning, alongside traditional concerns such as natural disasters, cyberattacks, and infrastructure failures.

Just as disaster recovery plans include provisions for alternative data processing locations, communication systems, and personnel coordination, they must also address Certificate Authority failover scenarios. A backup CA is a key component of recovery planning, ensuring that encryption, authentication, and secure access remain intact and that disruption is avoided.

SECTION 04

A 5-Step PKI Administrator's Guide to Navigate Certificate Authority Disruptions

1	2	3	4	5
Certificate Inventory & Monitoring	Diversify CA Relationships	Incident Response Procedures	Regular Testing & Validation	Activate Backup CA

1 Establish a Comprehensive Certificate Inventory and Monitoring

To ensure Public Key Infrastructure (PKI) runs smoothly, it's essential to start with detailed inventory management and automated monitoring systems. PKI admins should maintain comprehensive records of all our certificates, including issuing CA tracking, expiration dates, application dependencies, and renewal schedules.

Using automated certificate lifecycle management tools helps you stay proactive with renewals and provides early warnings of potential issues. Moreover, establish clear escalation procedures and ensure that multiple team members are cross-trained on certificate management. This can help to maintain or restore continuity even during challenging times when primary personnel may not be readily available.

2 Diversify Certificate Authority Relationships

By building relationships with several trusted CAs, your organization can eliminate single points of failure. Think about pre-negotiating emergency issuance procedures with alternative providers, keeping domain control verification validated across different CAs, and ensuring that their certificate installation processes are standardized. The entity validation used in the certificate should be completed ahead of time, as validation is typically the longest part of the certificate issuance process (including several items that need review such as a Dun & Bradstreet form, an attorney letter, and contact verification).

Additionally, for internal applications that aren't publicly facing, considering the use of internal Certificate Authorities can be a smart move. This approach can help reduce dependence on publicly trusted external providers for internal communications and lessen the overall risk of disruptions from external CAs.

3 Develop Comprehensive Incident Response Procedures

Create detailed playbooks outlining step-by-step procedures for various Certificate Authority disruption scenarios, from temporary outages to complete provider distrust. These plans should include straightforward, pre-approved emergency procurement processes and templates for communicating with stakeholders. Additionally, a clear decision tree will help determine when it’s time to activate backup providers.

It is recommended that PKI admins document specific procedures for rapid certificate replacement, service restoration priorities, and coordination between technical teams and business stakeholders, especially during certificate-related emergencies.

STEP 3 CONT.

For organizations managing high-volume certificate deployments in the millions, throughput becomes a critical consideration that must be addressed proactively by maintaining backup CA providers. PKI administrators must engage in detailed discussions with their backup CAs to understand daily issuance capacity limitations, as even the largest Certificate Authorities may not be able to process millions of certificate requests within a single day during emergency failover scenarios.

This reality necessitates implementing tiered triage strategies that prioritize critical certificates first, such as public-facing web services, revenue-generating applications, and essential infrastructure components. Additionally, high-volume organizations should consider maintaining a strategic percentage of pre-issued certificates from backup CAs that remain on hand for immediate deployment during emergencies.

4 Implement Regular Testing and Validation

Regularly scheduled or biannual testing of incident response procedures through tabletop exercises and mock outage events can help assess whether teams can execute efficiently under pressure if or when real incidents occur. It is vital to test backup CA integration processes, validate certificate replacement procedures, and verify that monitoring systems correctly identify and alert admins to any system compatibility or certificate-related issues. These exercises can help identify configuration gaps or staff readiness for emergencies.

Schedule periodic reviews of CA relationships, contract terms, and emergency procedures to ensure they remain current with both organizational needs and industry best practices. Additionally, it is recommended to have all technical aspects, such as API integration, set up and ready for deployment, as this is often what can cause the most significant downtime. It can save your technical teams from the pain points of scrambling to complete integrations or automation at the last minute.

5

Activate Backup Certificate Authority Infrastructure

As soon as you know that a distrust event, such as a mass revocation, is going to happen, contact the Certificate Authority that is providing your backup CA service. This is also why it's critical that, before engaging a backup CA, you should have all your integrations in place, all certificate lifecycle automations tested, all your validations completed, and all your due diligence done beforehand.

They also reduce emergency procurement time from days to hours and provide negotiating leverage with primary providers by demonstrating alternatives. Most importantly, established backup CA relationships maintain business continuity by allowing organizations to weather industry-wide depreciation events or other unexpected CA issues with minimal operational impact. It can mean the difference between minor inconveniences and catastrophic service disruptions.

SECTION 05

Key Technical Considerations in a Backup CA

Implementing a backup Certificate Authority should be approached with careful planning and adherence to recommended practices. The foundational elements of an effective technical strategy include:

Infrastructure Separation

The backup CA should be hosted on a separate infrastructure from the primary CA to minimize the risk of simultaneous failure. This includes using separate physical default locations or a virtual server, ideally placing it in an entirely different geographic region. Physical and logical separation provides a safeguard against localized disasters or targeted attacks.

Routine Testing and Drills

Just having a backup CA is not enough. It must work effectively when needed, so periodically testing its ability to issue, renew, and revoke certificates can help ensure system compatibility. Any backup CA engagement should include a designated number of certificates available to you at any given time, ensuring that very short-term issuing is working properly and that your certificate lifecycle is fully operational once you invoke the full backup CA.

> Regular quarterly or biannual testing drills can also help ensure that failover processes work smoothly. Additionally, organizations should schedule and conduct mock outage events. These exercises can help identify gaps in configuration or staff readiness for emergencies.

SECTION 06

Reinforcing Trust with a Backup CA



Backup plans are a benchmark for success in virtually all major industries across various business models. However, many organizations are increasingly relying on encrypted communications. As identity validation and secure device interactions increase, certificate infrastructure becomes a high-value target among malicious actors and a critical operational dependency. A single point of any potential catastrophic failure is not worth the risk.

Implementing a backup Certificate Authority is crucial for ensuring business continuity, meeting regulatory compliance requirements, and maintaining customer trust. Moreover, it enables your enterprise to comply with regulations, recover quickly from disasters and disruptions, and operate securely in an increasingly volatile digital landscape.

Whether you need assistance with reliable high-volume automated SSL/TLS certificate lifecycle management services or custom PKI solutions, we're dedicated to guiding you through every step, from initial consulting and infrastructure planning to ongoing support. Our team understands that every organization's needs are unique, so we deliver customized, scalable solutions tailored to meet your specific business requirements.

Let SSL help you improve your digital resilience today. Contact our team to help your organization design, implement, and maintain a customized backup CA plan to support your enterprise.

SSL | ssl.com @sslcorp · linkedin.com/company/ssl-com

2002

Founded in Houston, Texas

180+

Countries served worldwide

CA/Browser Forum

Full voting member

WebTrust

Audit compliant

© SSL.com 2026. All rights reserved.