



# Epic CA Fails

Not ok

## Prepare Now For The Inevitable

Over the past decade, we've seen a broad spectrum of Certificate Authority (CA) errors.

### Inadequate Internal Controls

Lack of CA policies or processes can result in improper actions.

### Human Error

Even with clear policies, CA staffers can still make mistakes.

### Technology Malfunction

Sometimes automation technology is to blame for CA errors.

### Business Partner Compromise

Reseller partners may misissue intermediate certificates.

### Hacker Compromises

Attackers steal or forge certificates for nefarious purposes.

### Abuse of Trust

Malicious activity violates the trust CAs are supposed to create.

\*\*\*\*\*

## A Long History of Certificate Authority Errors

\*\*\*\*\*

Mar 2018 **Trustico: business partner compromise**  
Reseller triggers immediate revocation by emailing 23,000 private keys

Sept 2017 **PROCERT: inadequate controls**  
CA is responsible for numerous issues centering around the misissuing of SSL certificates

Jan 2017 (Symantec intermediate)  
**CrossCert: business partner compromise**  
Partner overrides Symantec compliance flags to bypass domain validations

Oct 2016 **Comodo: technology malfunction**  
OCR failure results in the issuance of certificates to the wrong entities  
**WoSign & StartCom: abuse of trust**  
CA engages in numerous questionable practices, such as backdating SHA-1 certificates

Aug 2016 **GoDaddy: technology malfunction**  
Faulty upgrade allows certain servers to bypass the authentication process  
**WoSign: abuse of trust**  
CA is caught issuing certificates to non-domain owners

July 2016 **Comodo: technology malfunction**  
Dangling markup injection issues arbitrary wildcard certificates

Feb 2016 **Symantec: technology malfunction**  
Systems incorrectly parse email addresses, leaving them open to abuse

Sept 2015 **Symantec: human error**  
CA misissues test certificates without review by authentication personnel

Mar 2015 **CNNIC: abuse of trust**  
Unconstrained intermediate certificate is used for network interception  
**Comodo: inadequate controls**  
CA issues a certificate to a misconfigured privileged email on Microsoft's live.fi

July 2014 **NIC India: inadequate controls**  
Weak processes misissue several unauthorized Google certificates

Dec 2013 **ANSSI: business partner compromise**  
Subordinate CA misissues intermediate certificate, later abused by user

Sept 2011 **GlobalSign: hacker compromise**  
CA voluntarily suspends operations while investigating breach

Aug 2011 **DigiNota: hacker compromise**  
Hacked systems issue hundreds of fraudulent certificates

June 2011 **StartCom: hacker compromise**  
Breach causes CA to temporarily suspend certificate issuance

Mar 2011 **DecGlobalTrust.it: hacker compromise**  
Hacker counterfeits certificates for seven high-profile domains

Dec 2008 **CertStar: business partner compromise**  
Comodo reseller bypasses security mechanism to misissue Mozilla.com certificate

July 2008 **Thawte: inadequate controls**  
CA misissues certificate for login.live.com via email

\*\*\*\*\*

## Certificate Authorities Aren't Perfect

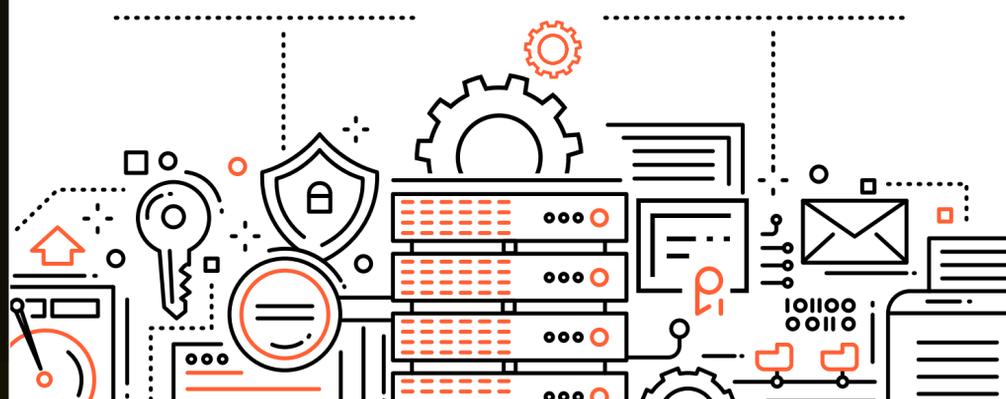
What's the potential impact of a CA error or compromise?

### Forged or fraudulent certificates

Allow attackers to perform Man-in-the-Middle (MiTM) traffic attacks to eavesdrop on private communications

### Misissued intermediate certificates

Allow attackers to act as their own certificate authority to issue fraudulent certificates for virtually any site



## What Can You Do About It?

Choose agile management that allows you to switch CAs quickly and easily

**Automate the rotation,** replacement and revocation of keys and certificates

**Actively manage** all your certificates from a single CA-agnostic platform

**Enforce consistent** security policies across all CAs



Learn more about how Venafi can help you proactively manage all CAs and all keys and certificates.

Visit [venafi.com](http://venafi.com)