VENAFI™

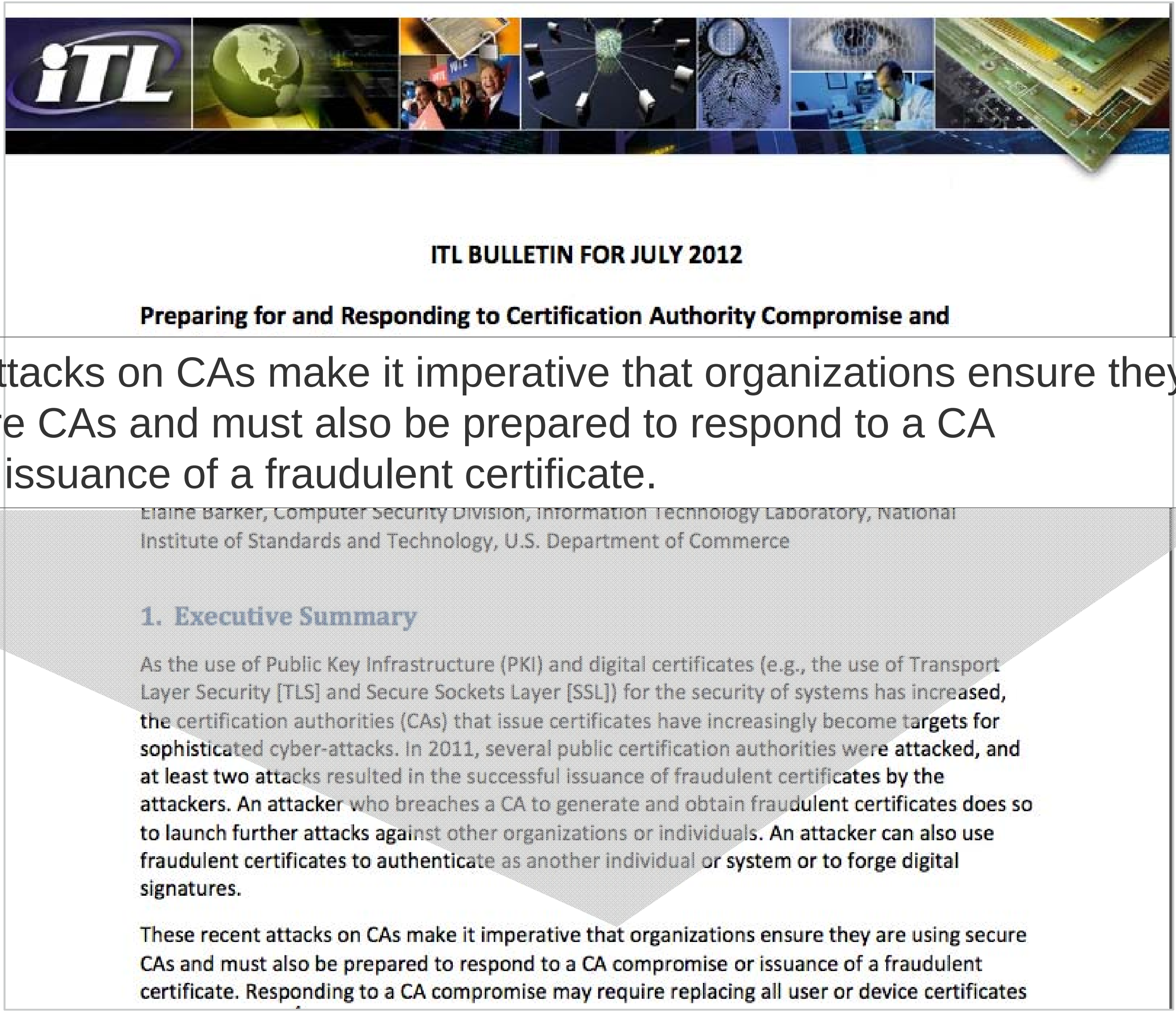
NIST ITL July 2012
CA Compromise

Prepared for: Intelligent People

paul.turner@venafi.com

NIST ITL Bulletin on CA Compromise

http://csrc.nist.gov/publications/nistbul/july-2012_itl-bulletin.pdf



ITL BULLETIN FOR JULY 2012

Preparing for and Responding to Certification Authority Compromise and

These recent attacks on CAs make it imperative that organizations ensure they are using secure CAs and must also be prepared to respond to a CA compromise or issuance of a fraudulent certificate.

Elaine Barker, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce

1. Executive Summary

As the use of Public Key Infrastructure (PKI) and digital certificates (e.g., the use of Transport Layer Security [TLS] and Secure Sockets Layer [SSL]) for the security of systems has increased, the certification authorities (CAs) that issue certificates have increasingly become targets for sophisticated cyber-attacks. In 2011, several public certification authorities were attacked, and at least two attacks resulted in the successful issuance of fraudulent certificates by the attackers. An attacker who breaches a CA to generate and obtain fraudulent certificates does so to launch further attacks against other organizations or individuals. An attacker can also use fraudulent certificates to authenticate as another individual or system or to forge digital signatures.

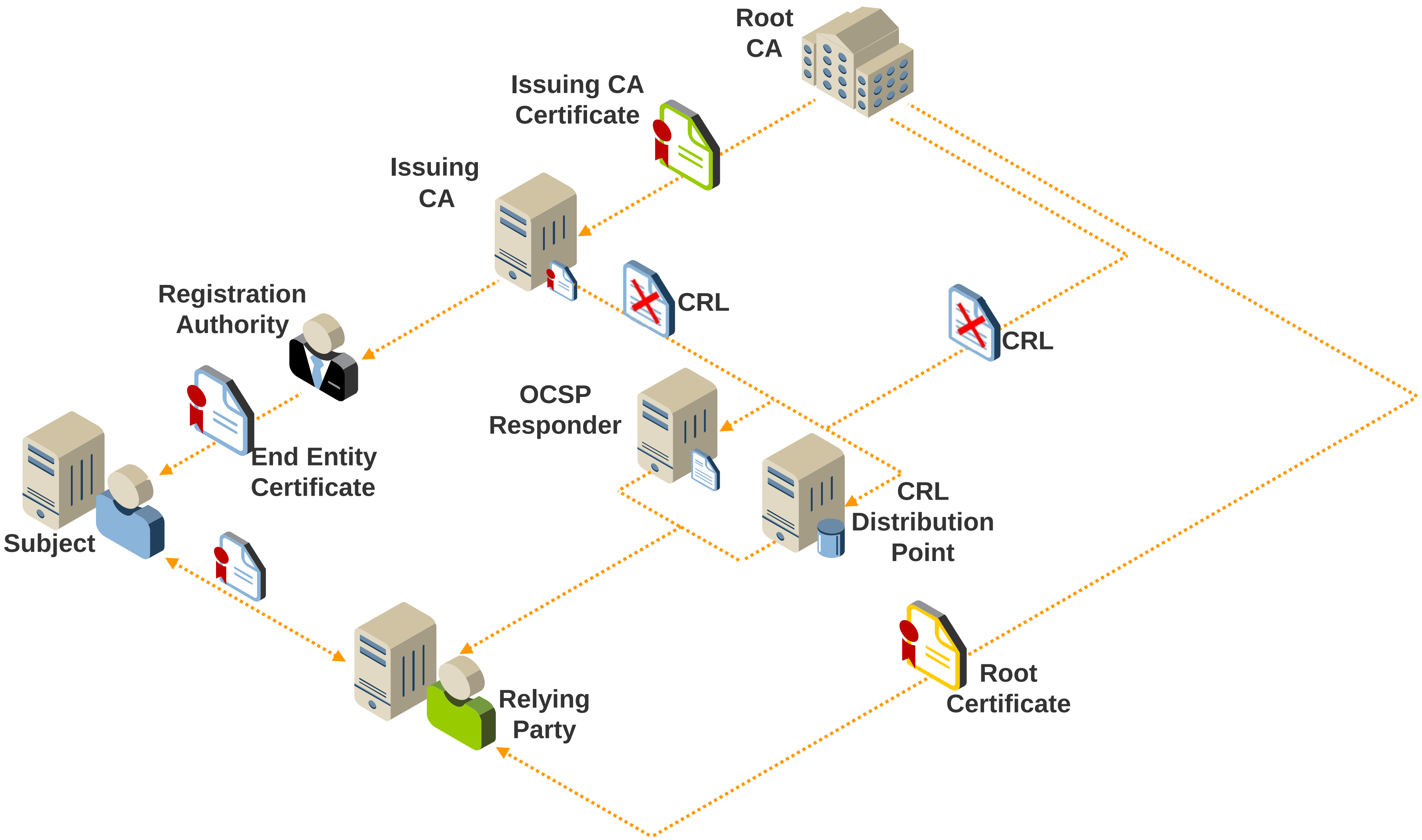
These recent attacks on CAs make it imperative that organizations ensure they are using secure CAs and must also be prepared to respond to a CA compromise or issuance of a fraudulent certificate. Responding to a CA compromise may require replacing all user or device certificates

Recent Public Certificate Authority & Counterfeit Certificate Incidents

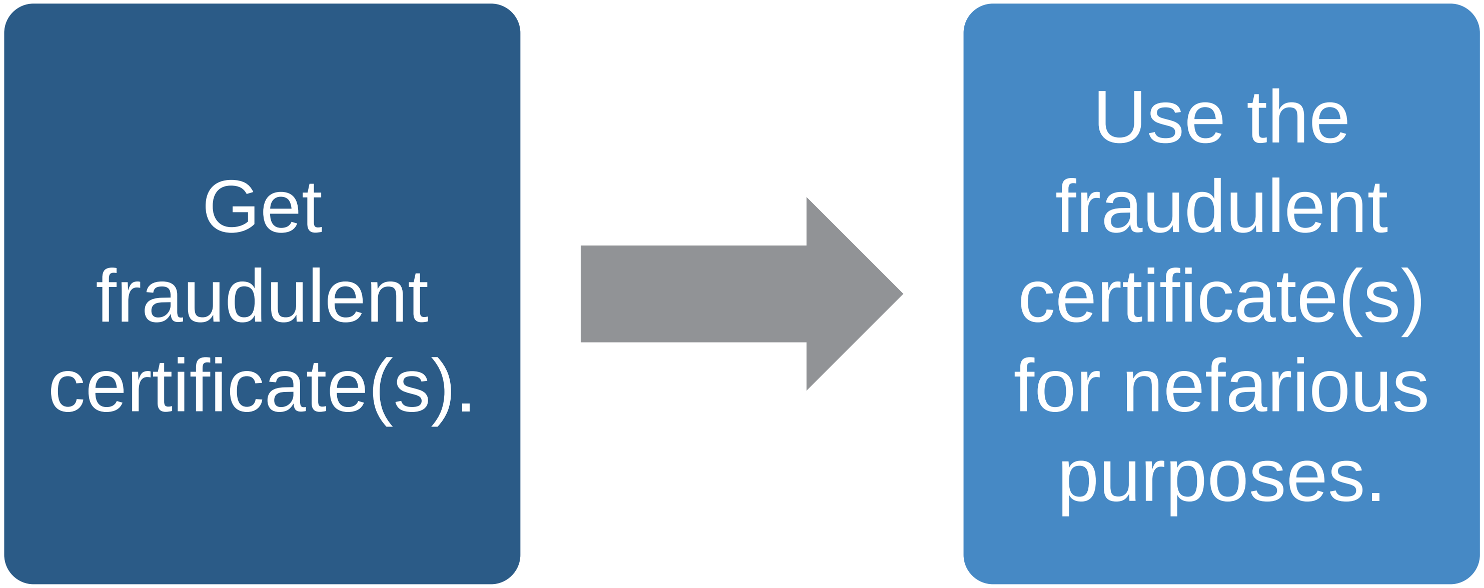
Year	Incidents
2001	- VeriSign issues Microsoft Corporation code signing certificate to a non-Microsoft employee.
2008	- Thawte issues certificate for Live.com to non-Microsoft employee - Comodo issues mozilla.org certificate to Startcom - Organization forges VeriSign RapidSSL certificates
2011	- Comodo issues nine counterfeit certificates (Google, Yahoo, Live, etc.) when registration authority is compromised. - StartSSL CA compromised - DigiNotar compromised. 531 fraudulent certificates issued. Dutch government experiences major service outages. - Boeing CA compromised
2012	- Microsoft CA certificates forged by exploiting MD5 (Flame)

* Electronic Freedom Foundation uncovers many more unpublicized CA incidents by analyzing CRLs from public CAs

Diagram of PKI Ecosystem



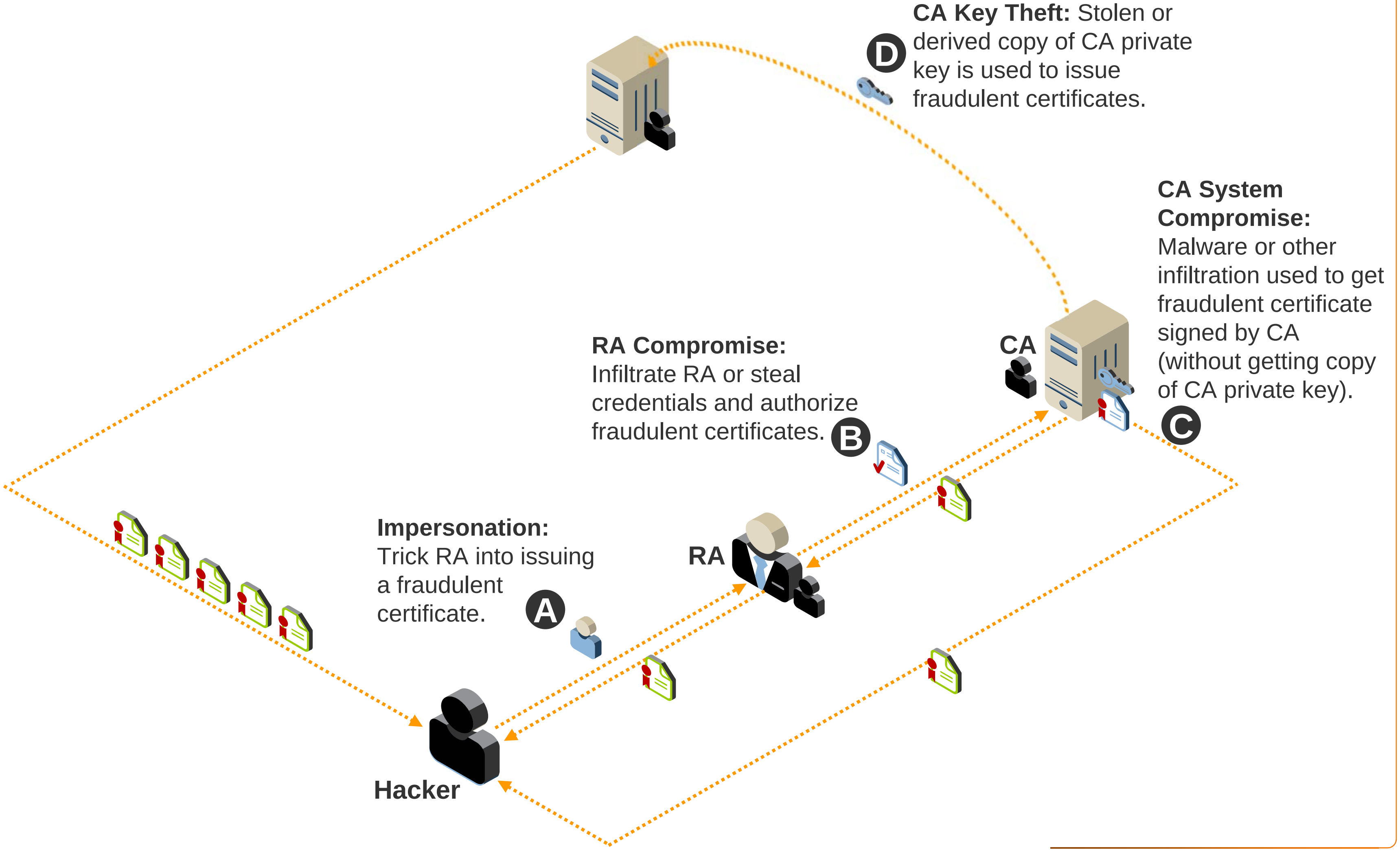
Using Fraudulent Certificates: A Two-Phased Attack



Get fraudulent certificate(s).

Use the fraudulent certificate(s) for nefarious purposes.

CA Compromise and Fraudulent Certificate Scenarios



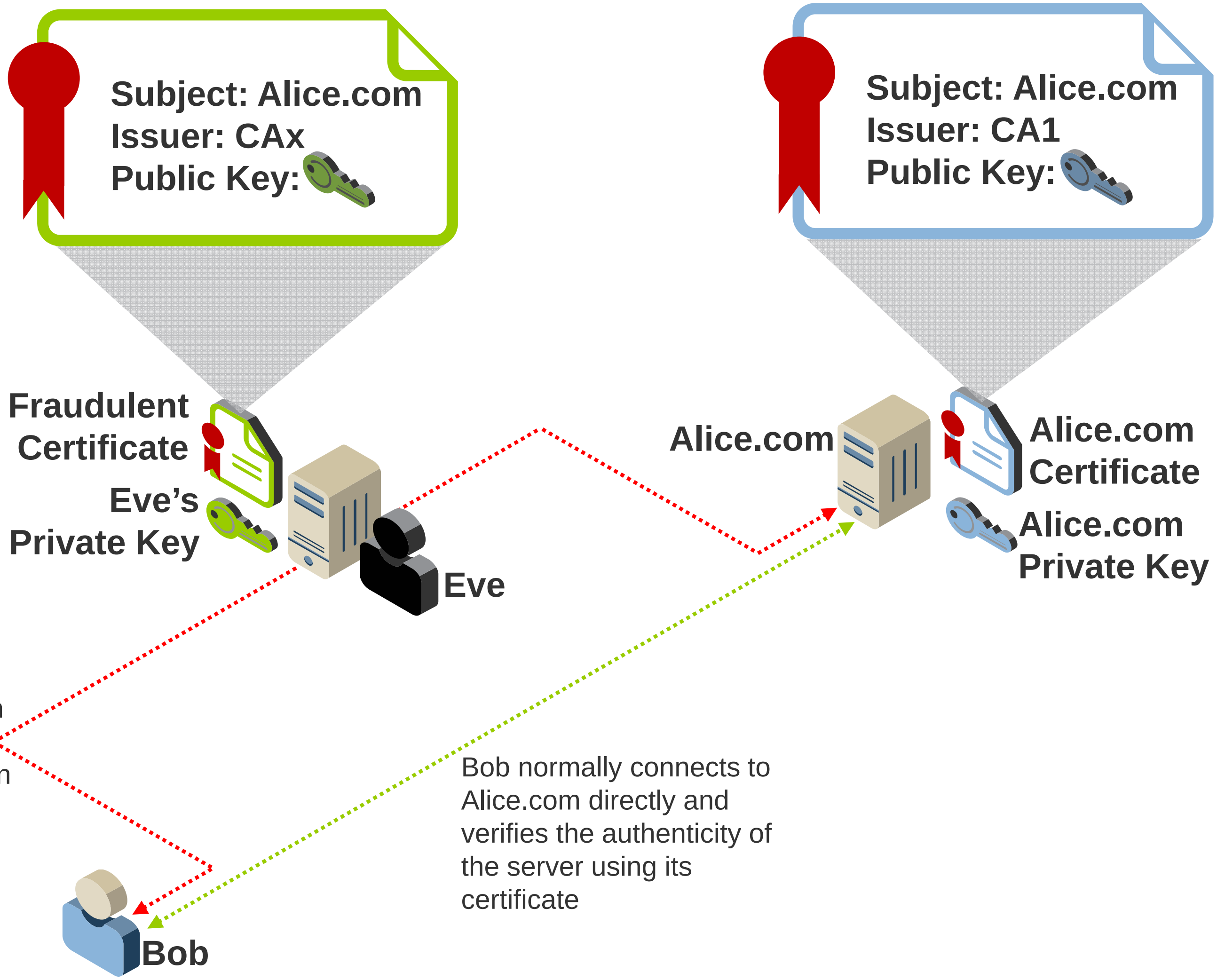
CA Key Theft: Stolen or derived copy of CA private key is used to issue fraudulent certificates.

CA System Compromise: Malware or other infiltration used to get fraudulent certificate signed by CA (without getting copy of CA private key).

RA Compromise: Infiltrate RA or steal credentials and authorize fraudulent certificates.

Impersonation: Trick RA into issuing a fraudulent certificate.

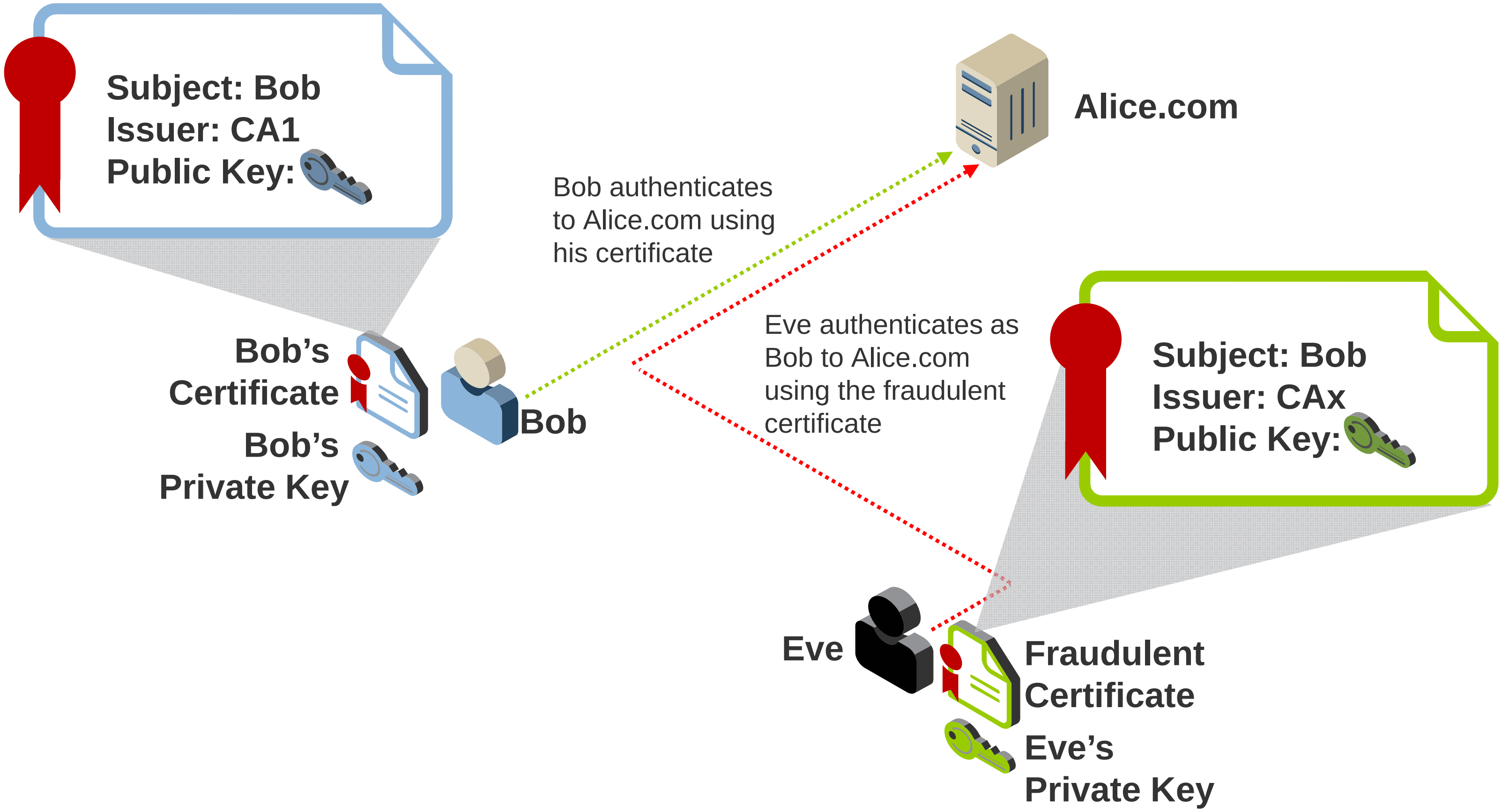
Man-in-the-Middle Eavesdropping



Bob is redirected thru Eve's server and presented with the fraudulent certificate. Eve can view all encrypted data.

Bob normally connects to Alice.com directly and verifies the authenticity of the server using its certificate

Impersonation



Subject: Bob
Issuer: CA1
Public Key:

Bob's Certificate

Bob's Private Key

Bob

Bob authenticates to Alice.com using his certificate

Alice.com

Eve authenticates as Bob to Alice.com using the fraudulent certificate

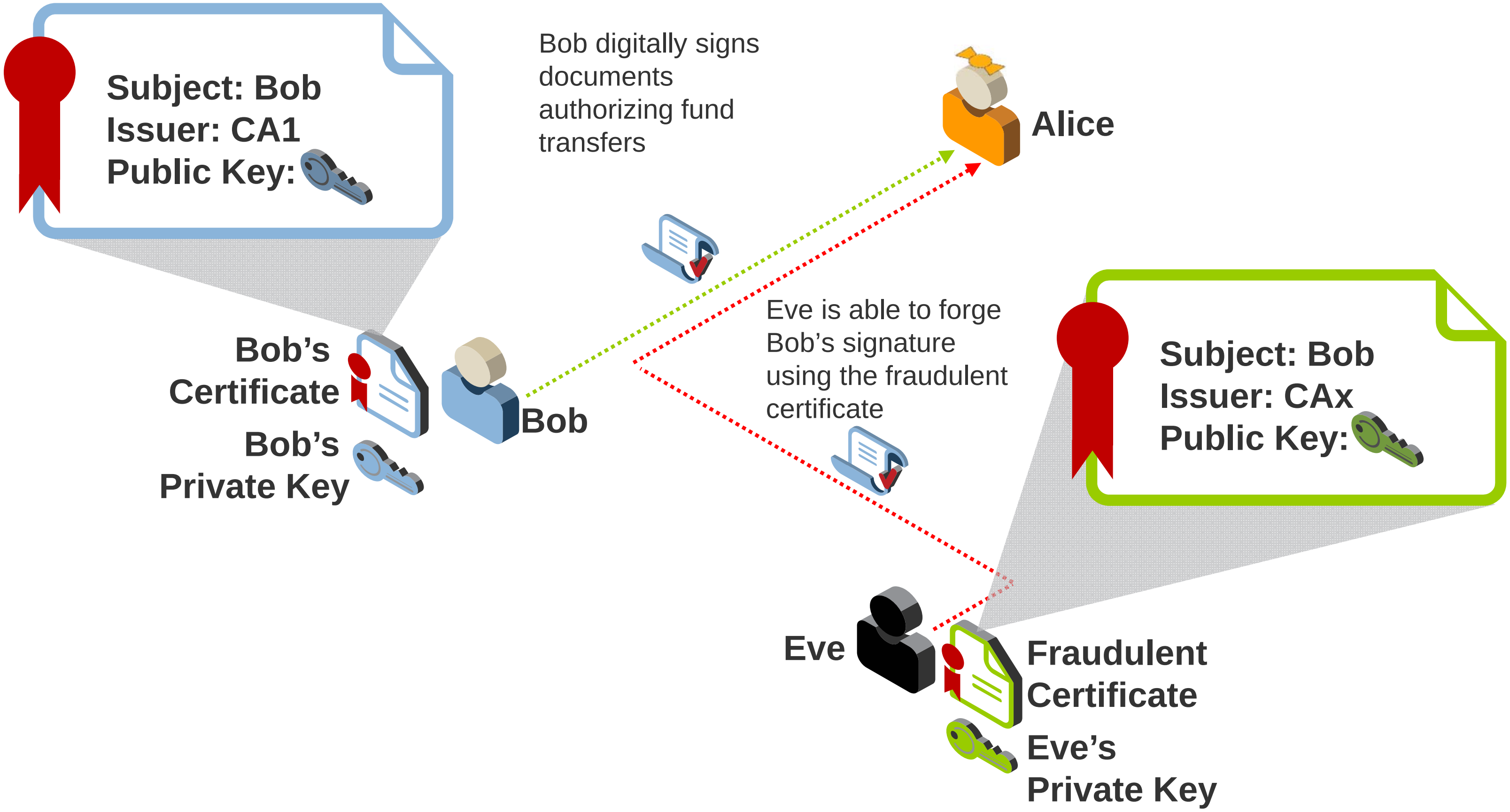
Subject: Bob
Issuer: CAx
Public Key:

Eve

Fraudulent Certificate

Eve's Private Key

Forge Digital Signatures

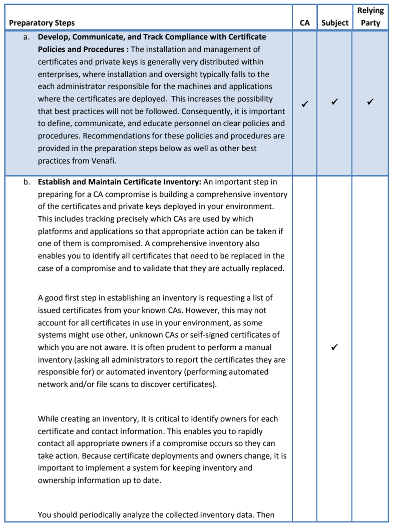


CA Compromise & Counterfeit Certificate and Remediation Matrix

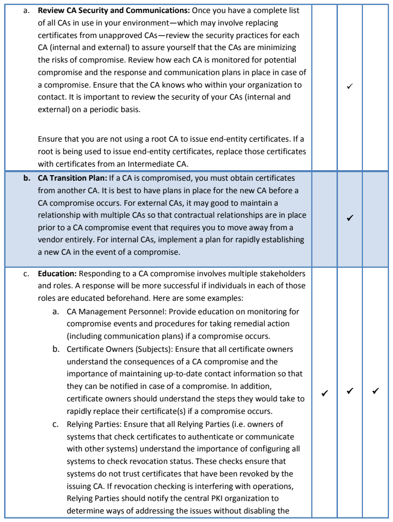
	Revoke Counterfeit Certificates	Revoke CA Cert	Replace **All** Certs from CA	Remove Root Cert from Relying Parties
A. Impersonation	✓			
B. RA Compromise	✓			
C. CA System Compromise		✓	✓	
D. CA Signing Key Compromise		✓	✓	
E. Root CA Compromise			✓	✓

Detailed Steps for Preparing for & Responding in the Best Practices Document

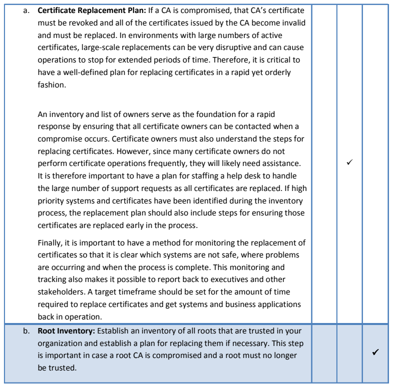
Preparing for a CA Compromise



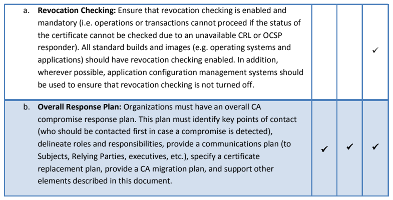
Preparatory Steps	CA	Subject	Relying Party
a. **Develop, Communicate, and Track Compliance with Certificate Policies and Procedures :** The installation and management of certificates and private keys is generally very distributed within enterprises, where installation and oversight typically falls to the each administrator responsible for the machines and applications where the certificates are deployed. This increases the possibility that best practices will not be followed. Consequently, it is important to define, communicate, and educate personnel on clear policies and procedures. Recommendations for these policies and procedures are provided in the preparation steps below as well as other best practices from Venafi.	✓	✓	✓
b. **Establish and Maintain Certificate Inventory:** An important step in preparing for a CA compromise is building a comprehensive inventory of the certificates and private keys deployed in your environment. This includes tracking precisely which CAs are used by which platforms and applications so that appropriate action can be taken if one of them is compromised. A comprehensive inventory also enables you to identify all certificates that need to be replaced in the case of a compromise and to validate that they are actually replaced. A good first step in establishing an inventory is requesting a list of issued certificates from your known CAs. However, this may not account for all certificates in use in your environment, as some systems might use other, unknown CAs or self-signed certificates of which you are not aware. It is often prudent to perform a manual inventory (asking all administrators to report the certificates they are responsible for) or automated inventory (performing automated network and/or file scans to discover certificates). While creating an inventory, it is critical to identify owners for each certificate and contact information. This enables you to rapidly contact all appropriate owners if a compromise occurs so they can take action. Because certificate deployments and owners change, it is important to implement a system for keeping inventory and ownership information up to date. You should periodically analyze the collected inventory data. Then		✓	



a. **Review CA Security and Communications:** Once you have a complete list of all CAs in use in your environment—which may involve replacing certificates from unapproved CAs—review the security practices for each CA (internal and external) to assure yourself that the CAs are minimizing the risks of compromise. Review how each CA is monitored for potential compromise and the response and communication plans in place in case of a compromise. Ensure that the CA knows who within your organization to contact. It is important to review the security of your CAs (internal and external) on a periodic basis. Ensure that you are not using a root CA to issue end-entity certificates. If a root is being used to issue end-entity certificates, replace those certificates with certificates from an Intermediate CA.		✓	
b. **CA Transition Plan:** If a CA is compromised, you must obtain certificates from another CA. It is best to have plans in place for the new CA before a CA compromise occurs. For external CAs, it may good to maintain a relationship with multiple CAs so that contractual relationships are in place prior to a CA compromise event that requires you to move away from a vendor entirely. For internal CAs, implement a plan for rapidly establishing a new CA in the event of a compromise.		✓	
c. **Education:** Responding to a CA compromise involves multiple stakeholders and roles. A response will be more successful if individuals in each of those roles are educated beforehand. Here are some examples: a. CA Management Personnel: Provide education on monitoring for compromise events and procedures for taking remedial action (including communication plans) if a compromise occurs. b. Certificate Owners (Subjects): Ensure that all certificate owners understand the consequences of a CA compromise and the importance of maintaining up-to-date contact information so that they can be notified in case of a compromise. In addition, certificate owners should understand the steps they would take to rapidly replace their certificate(s) if a compromise occurs. c. Relying Parties: Ensure that all Relying Parties (i.e. owners of systems that check certificates to authenticate or communicate with other systems) understand the importance of configuring all systems to check revocation status. These checks ensure that systems do not trust certificates that have been revoked by the issuing CA. If revocation checking is interfering with operations, Relying Parties should notify the central PKI organization to determine ways of addressing the issues without disabling the	✓	✓	✓

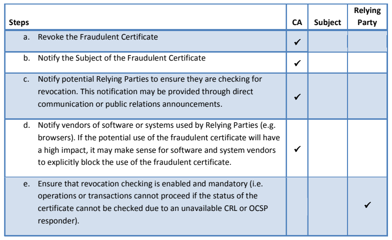


a. **Certificate Replacement Plan:** If a CA is compromised, that CA's certificate must be revoked and all of the certificates issued by the CA become invalid and must be replaced. In environments with large numbers of active certificates, large-scale replacements can be very disruptive and can cause operations to stop for extended periods of time. Therefore, it is critical to have a well-defined plan for replacing certificates in a rapid yet orderly fashion. An inventory and list of owners serve as the foundation for a rapid response by ensuring that all certificate owners can be contacted when a compromise occurs. Certificate owners must also understand the steps for replacing certificates. However, since many certificate owners do not perform certificate operations frequently, they will likely need assistance. It is therefore important to have a plan for staffing a help desk to handle the large number of support requests as all certificates are replaced. If high priority systems and certificates have been identified during the inventory process, the replacement plan should also include steps for ensuring those certificates are replaced early in the process. Finally, it is important to have a method for monitoring the replacement of certificates so that it is clear which systems are not safe, where problems are occurring and when the process is complete. This monitoring and tracking also makes it possible to report back to executives and other stakeholders. A target timeframe should be set for the amount of time required to replace certificates and get systems and business applications back in operation.		✓	
b. **Root Inventory:** Establish an inventory of all roots that are trusted in your organization and establish a plan for replacing them if necessary. This step is important in case a root CA is compromised and a root must no longer be trusted.			✓



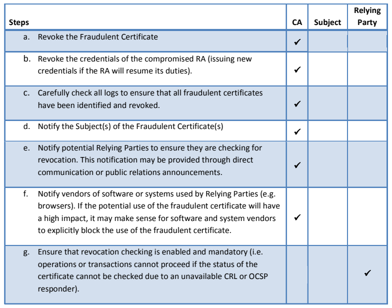
a. **Revocation Checking:** Ensure that revocation checking is enabled and mandatory (i.e. operations or transactions cannot proceed if the status of the certificate cannot be checked due to an unavailable CRL or OCSP responder). All standard builds and images (e.g. operating systems and applications) should have revocation checking enabled. In addition, wherever possible, application configuration management systems should be used to ensure that revocation checking is not turned off.			✓
b. **Overall Response Plan:** Organizations must have an overall CA compromise response plan. This plan must identify key points of contact (who should be contacted first in case a compromise is detected), delineate roles and responsibilities, provide a communications plan (to Subjects, Relying Parties, executives, etc.), specify a certificate replacement plan, provide a CA migration plan, and support other elements described in this document.	✓	✓	✓

Impersonation



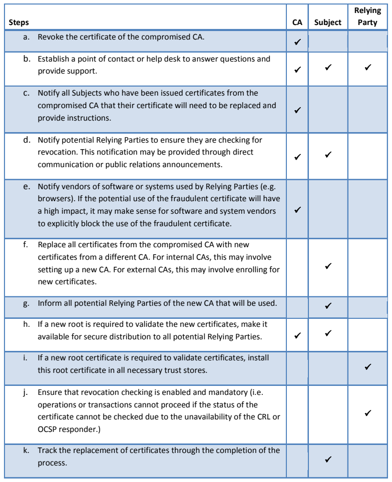
Steps	CA	Subject	Relying Party
a. Revoke the Fraudulent Certificate	✓		
b. Notify the Subject of the Fraudulent Certificate	✓		
c. Notify potential Relying Parties to ensure they are checking for revocation. This notification may be provided through direct communication or public relations announcements.	✓		
d. Notify vendors of software or systems used by Relying Parties (e.g. browsers). If the potential use of the fraudulent certificate will have a high impact, it may make sense for software and system vendors to explicitly block the use of the fraudulent certificate.	✓		
e. Ensure that revocation checking is enabled and mandatory (i.e. operations or transactions cannot proceed if the status of the certificate cannot be checked due to an unavailable CRL or OCSP responder).			✓

RA Compromise



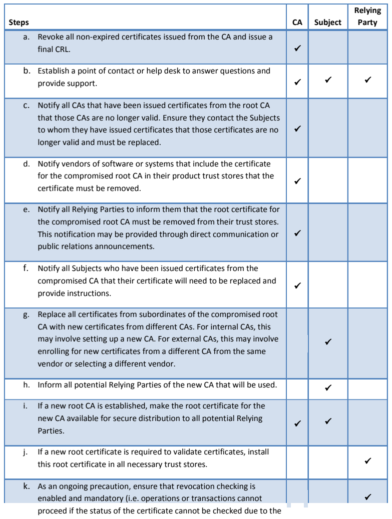
Steps	CA	Subject	Relying Party
a. Revoke the Fraudulent Certificate	✓		
b. Revoke the credentials of the compromised RA (issuing new credentials if the RA will resume its duties).	✓		
c. Carefully check all logs to ensure that all fraudulent certificates have been identified and revoked.	✓		
d. Notify the Subject(s) of the Fraudulent Certificate(s)	✓		
e. Notify potential Relying Parties to ensure they are checking for revocation. This notification may be provided through direct communication or public relations announcements.	✓		
f. Notify vendors of software or systems used by Relying Parties (e.g. browsers). If the potential use of the fraudulent certificate will have a high impact, it may make sense for software and system vendors to explicitly block the use of the fraudulent certificate.	✓		
g. Ensure that revocation checking is enabled and mandatory (i.e. operations or transactions cannot proceed if the status of the certificate cannot be checked due to an unavailable CRL or OCSP responder).			✓

CA Key or System Compromise



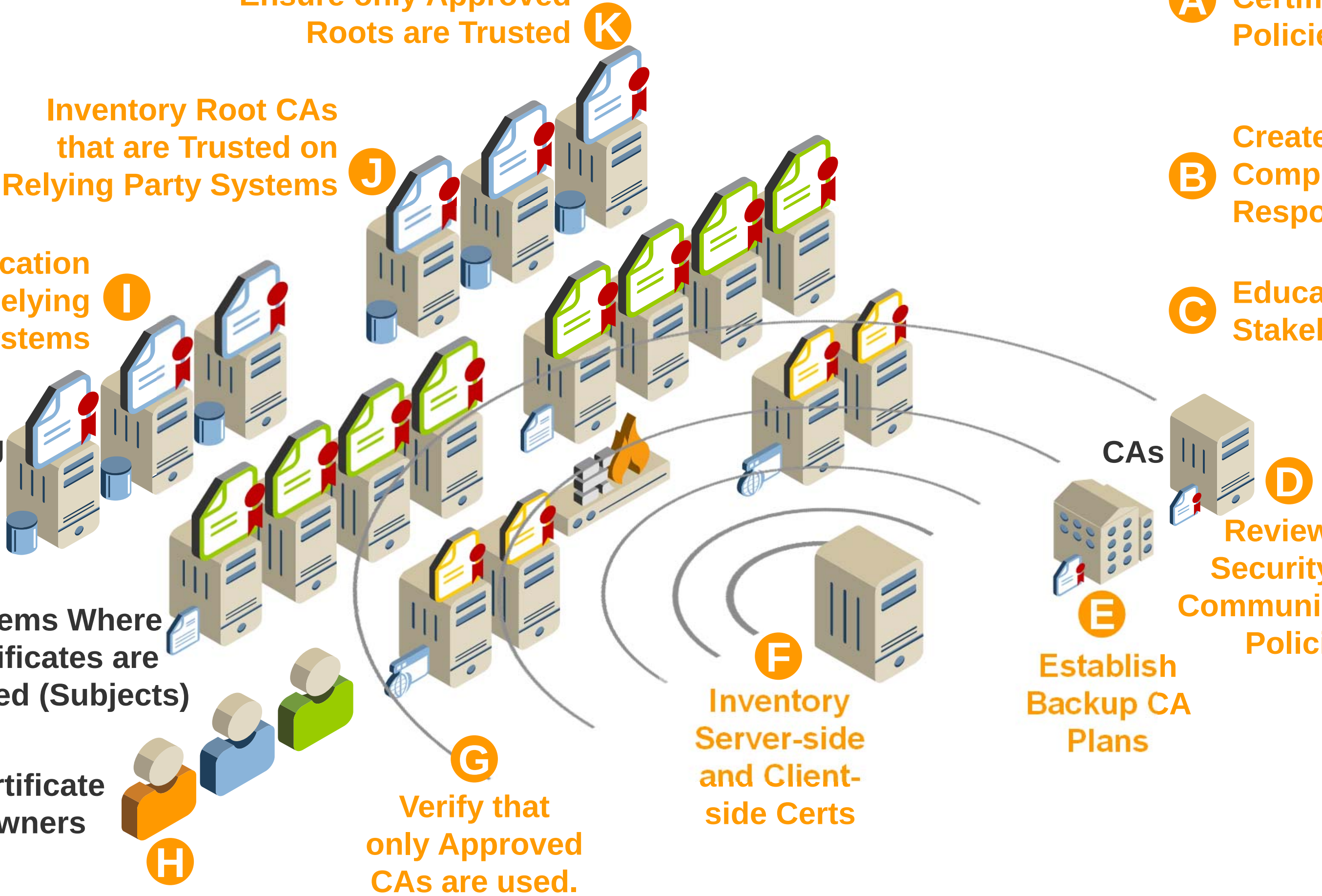
Steps	CA	Subject	Relying Party
a. Revoke the certificate of the compromised CA.	✓		
b. Establish a point of contact or help desk to answer questions and provide support.	✓	✓	✓
c. Notify all Subjects who have been issued certificates from the compromised CA that their certificate will need to be replaced and provide instructions.	✓		
d. Notify potential Relying Parties to ensure they are checking for revocation. This notification may be provided through direct communication or public relations announcements.	✓	✓	
e. Notify vendors of software or systems used by Relying Parties (e.g. browsers). If the potential use of the fraudulent certificate will have a high impact, it may make sense for software and system vendors to explicitly block the use of the fraudulent certificate.	✓		
f. Replace all certificates from the compromised CA with new certificates from a different CA. For internal CAs, this may involve setting up a new CA. For external CAs, this may involve enrolling for new certificates.		✓	
g. Inform all potential Relying Parties of the new CA that will be used.		✓	
h. If a new root is required to validate the new certificates, make it available for secure distribution to all potential Relying Parties.	✓	✓	
i. If a new root certificate is required to validate certificates, install this root certificate in all necessary trust stores.			✓
j. Ensure that revocation checking is enabled and mandatory (i.e. operations or transactions cannot proceed if the status of the certificate cannot be checked due to the unavailability of the CRL or OCSP responder.)			✓
k. Track the replacement of certificates through the completion of the process.		✓	

Root CA Compromise



Steps	CA	Subject	Relying Party
a. Revoke all non-expired certificates issued from the CA and issue a final CRL.	✓		
b. Establish a point of contact or help desk to answer questions and provide support.	✓	✓	✓
c. Notify all CAs that have been issued certificates from the root CA that those CAs are no longer valid. Ensure they contact the Subjects to whom they have issued certificates that those certificates are no longer valid and must be replaced.	✓		
d. Notify vendors of software or systems that include the certificate for the compromised root CA in their product trust stores that the certificate must be removed.	✓		
e. Notify all Relying Parties to inform them that the root certificate for the compromised root CA must be removed from their trust stores. This notification may be provided through direct communication or public relations announcements.	✓		
f. Notify all Subjects who have been issued certificates from the compromised CA that their certificate will need to be replaced and provide instructions.	✓		
g. Replace all certificates from subordinates of the compromised root CA with new certificates from different CAs. For internal CAs, this may involve setting up a new CA. For external CAs, this may involve enrolling for new certificates from a different CA from the same vendor or selecting a different vendor.		✓	
h. Inform all potential Relying Parties of the new CA that will be used.		✓	
i. If a new root CA is established, make the root certificate for the new CA available for secure distribution to all potential Relying Parties.	✓	✓	
j. If a new root certificate is required to validate certificates, install this root certificate in all necessary trust stores.			✓
k. As an ongoing precaution, ensure that revocation checking is enabled and mandatory (i.e. operations or transactions cannot proceed if the status of the certificate cannot be checked due to the			✓

Preparing for a CA Compromise



A Document Clear Certificate Policies

B Create CA Compromise Response Plan

C Educate all Stakeholders

CAs

D Review CA Security and Communications Policies

E Establish Backup CA Plans

F Inventory Server-side and Client-side Certs

G Verify that only Approved CAs are used.

Certificate Owners

H Identify Cert Owners (Subjects) and Relying Parties

Systems Where Certificates are Installed (Subjects)

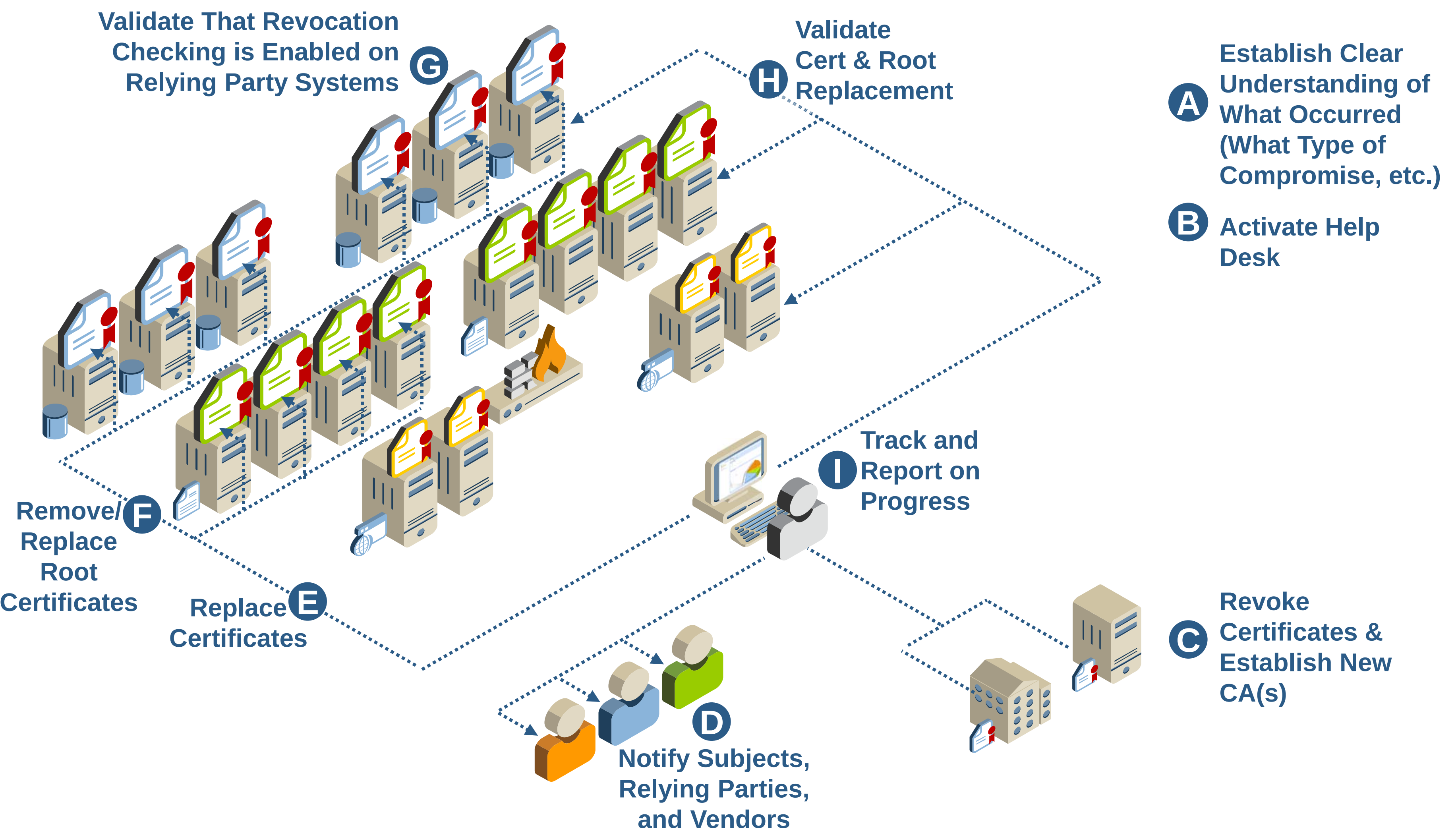
Systems Trusting Certificates (Relying Parties)

I Enforce Revocation Checking on Relying Party Systems

J Inventory Root CAs that are Trusted on Relying Party Systems

K Ensure only Approved Roots are Trusted

Responding to a CA Compromise



Validate That Revocation Checking is Enabled on Relying Party Systems G

H Validate Cert & Root Replacement

A Establish Clear Understanding of What Occurred (What Type of Compromise, etc.)

B Activate Help Desk

I Track and Report on Progress

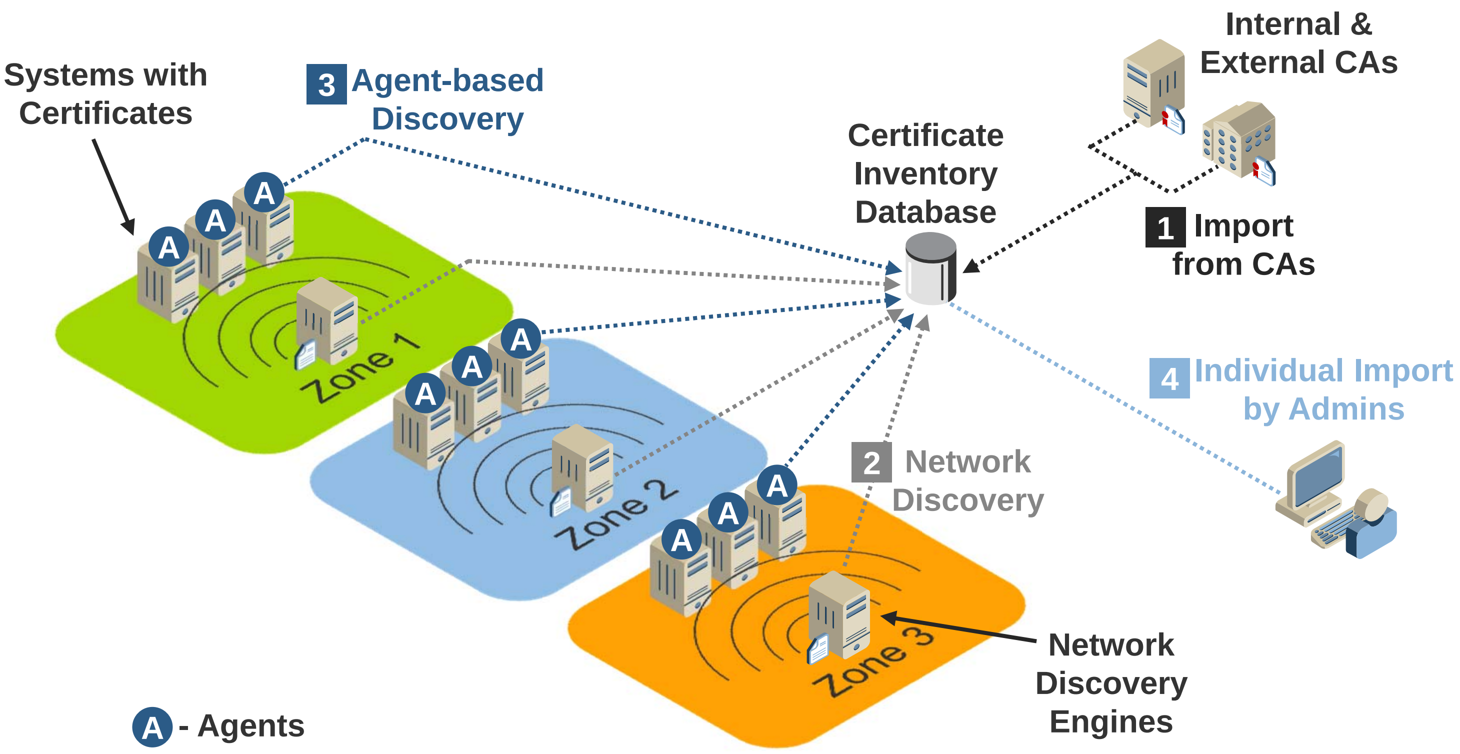
C Revoke Certificates & Establish New CA(s)

D Notify Subjects, Relying Parties, and Vendors

E Replace Certificates

F Remove/ Replace Root Certificates

Establishing a Comprehensive Inventory

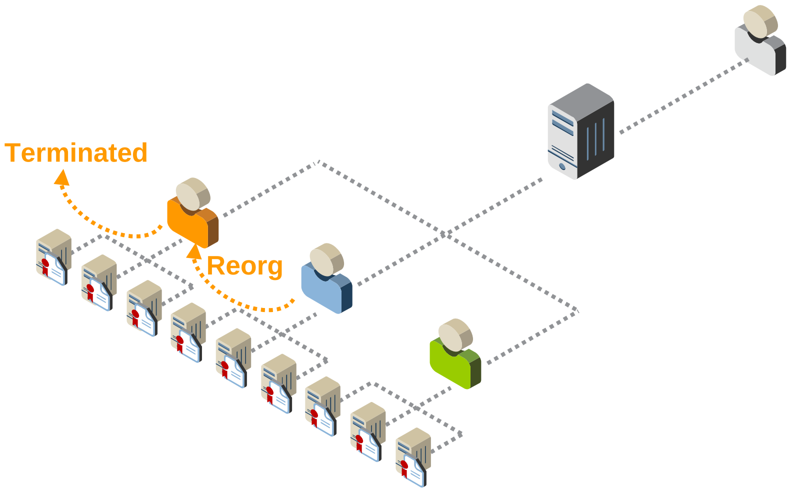


Analyze Inventory and Evaluate Compliance

- Certificate authorities/self-signed certificates
- Key lengths
- Signing hash algorithms (e.g. MD5 or SHA1)
- Validity periods
- Expiration dates
- Locations
- Keystore types
- Owners
- Business applications
- Applicable policies and regulations
- Current management processes

Managing Ownership Information

- It is critical to have up-to-date ownership information
  - Notifications for expirations
  - Notifications in case of compromise
  - Invalid notification is worse than no notification at all
- Best to have owners directly manage the updating of information
- Provide central oversight and support



Summary

Preparing for and Responding to CA Compromise

1. Establish an accurate inventory of certificates
   - Identify Owners
2. Ensure only trusted CAs are in use
3. Review CA security
4. Establish backup CA(s)
5. Inventory trust anchors (root certs)
6. Create strategy for rapid certificate replacement (to minimize business interruptions due to CA compromise)
7. Establish method of tracking replacement of certificates

Discussion

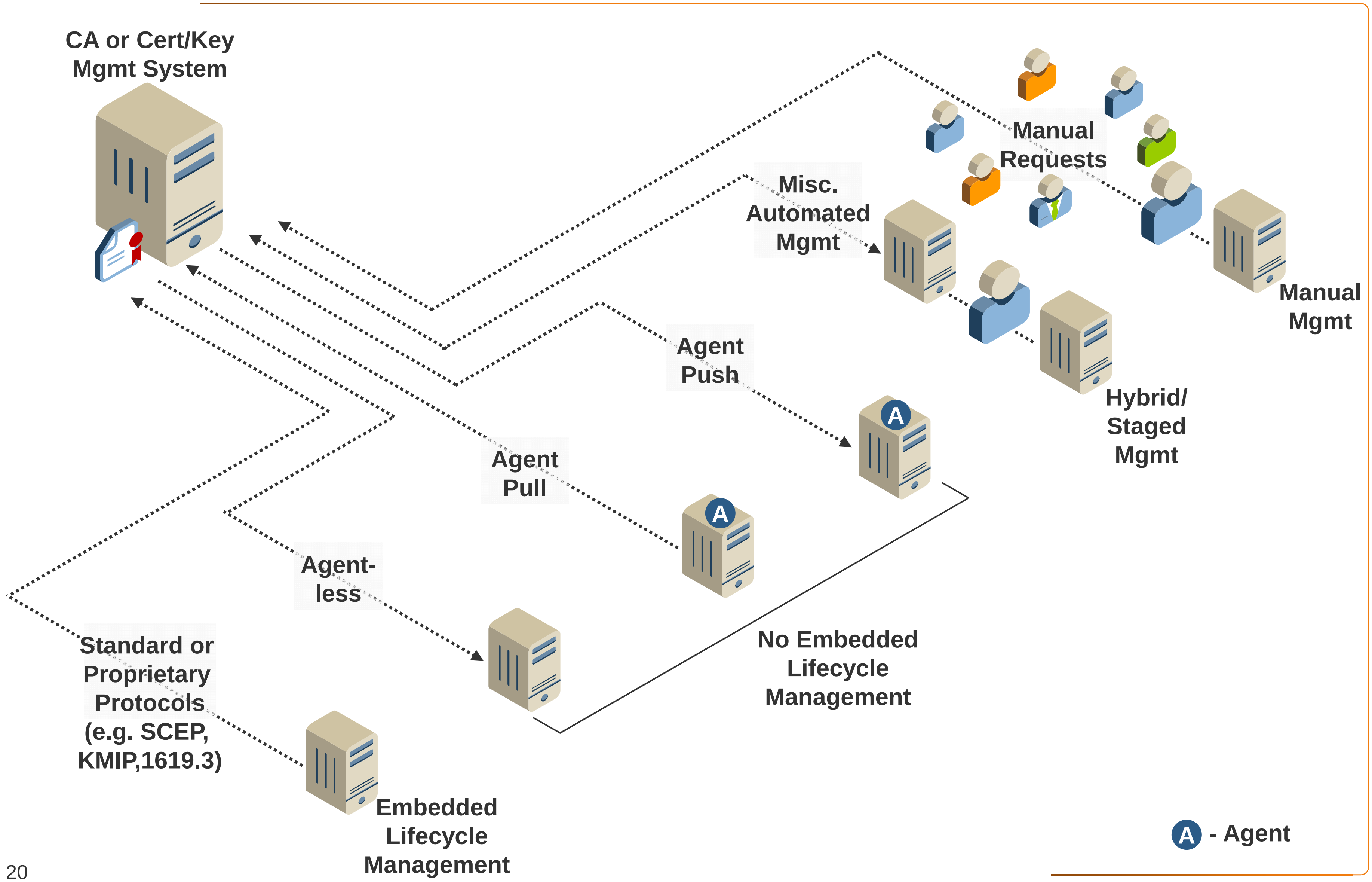
Unpublished Work of Venafi, Inc. All Rights Reserved.

General Disclaimer

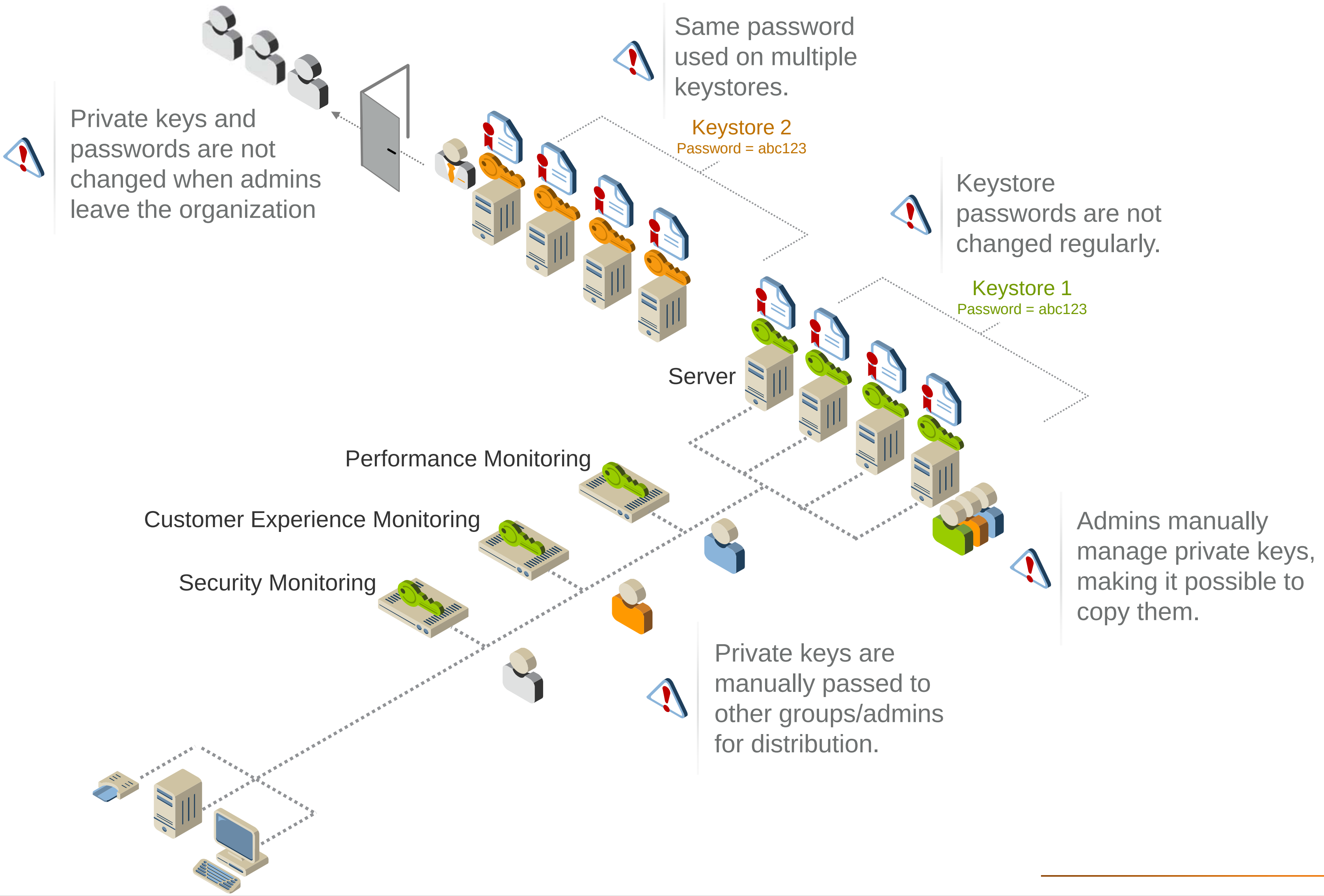
This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. Venafi, Inc. makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Venafi, Inc. reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Venafi marks referenced in this presentation are trademarks or registered trademarks of Venafi, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

VENAFI™

Encryption Management and Distribution Models


CA or Cert/Key Mgmt System
Manual Requests
Misc. Automated Mgmt
Manual Mgmt
Agent Push
Hybrid/ Staged Mgmt
Agent Pull
Agent-less
No Embedded Lifecycle Management
Standard or Proprietary Protocols (e.g. SCEP, KMIP,1619.3)
Embedded Lifecycle Management
A
A
A - Agent

Another Risk:
Private Key Security



Private keys and passwords are not changed when admins leave the organization

Same password used on multiple keystores.

Keystore passwords are not changed regularly.

Admins manually manage private keys, making it possible to copy them.

Private keys are manually passed to other groups/admins for distribution.