



The Keys to the Cloud: How Aetna Addresses Certificate and Key Management

Tim Tompkins
Aetna, Inc.

Session ID: TECH-204

Session Classification: Intermediate

RSACONFERENCE**2012**

Session Learning Objectives

- Identify security issues that cloud vendors must address for highly regulated industries
- Recognize the problems associated with encryption chaos
- Become familiar with Aetna's best-practices approach to automating certificate management
- Relate lessons learned from Aetna's implementation to your own organization



Key Issues for Issuing Keys

- Outages due to expiration or deployment error
 - Renewal & implementation lifecycle
- Security of private keys
 - Key storage & access control
- Managing & authorizing certificate requesters
- Validating request attributes

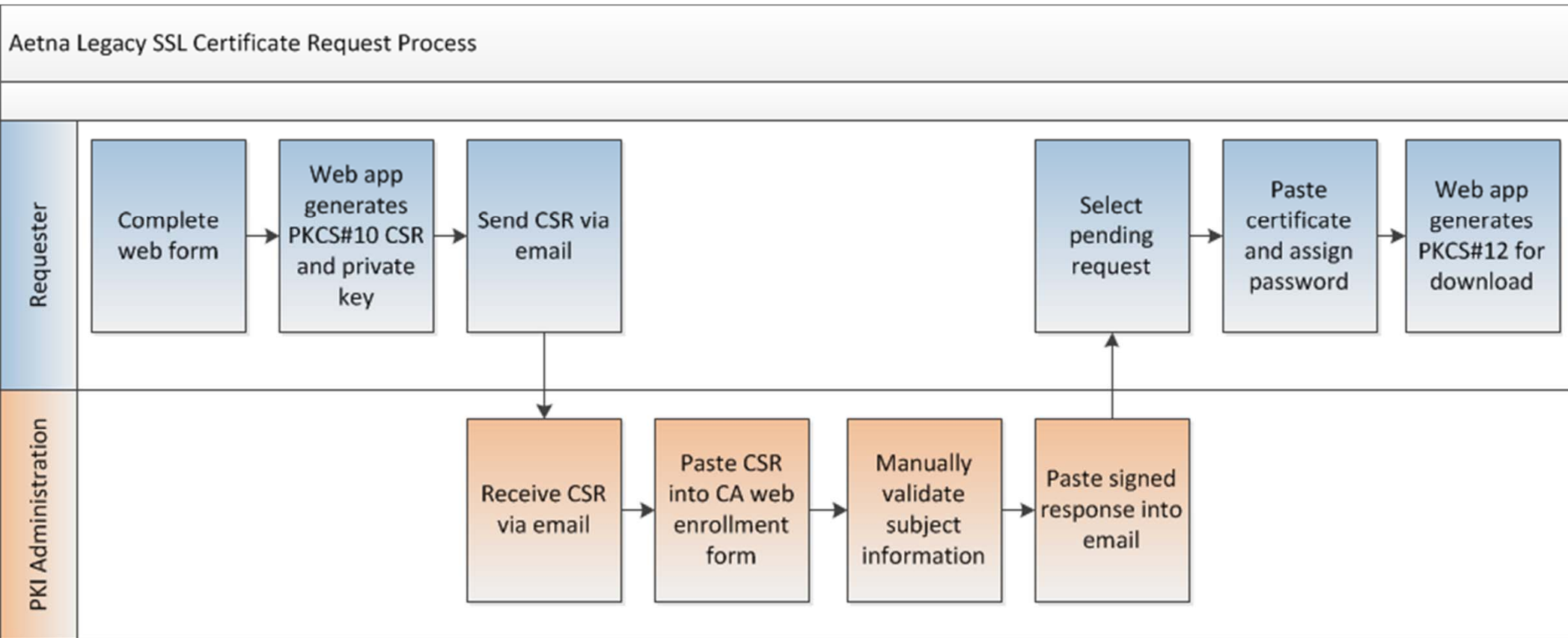


X.509 Key Management Challenges

- Varied locations
 - Internal
 - External
 - Cloud
 - Third party issued
- Everything has a cert
 - Native key management is poor



Previous State at Aetna



- Renewal notifications
- No monitoring
- No formal key escrow (lost passwords)
- 5 day SLA



Requester View



https://certrequest.aetna.com/ - Microsoft Internet Explorer provided by Aetna

https://certrequest.aetna.com/

Create new Certificate Request

Certificate Common Name: Required

Primary Email Address: Required

Secondary Email Address: Required

Certificate Usage: Required

Certificate Type: GeoTrust

PKI Admin View



Microsoft Certificate Services - Microsoft Internet Explorer provided by Aetna

https://sslca.aetna.com/certsrv/certrqxt.asp

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwajELMAkGA1UEBhMCVVMxFDAS
MRMwEQYDVQQHEwpNaWRkbGV0b3duMRMwEQYDVQQK
VQQDExJyc2EtdGVzdC5hZXRUYS5jb20wgZ8wDQYJ
AoGBAOnCOMZ8Gg6EWXiU9iuohfs3vQxH/BCrSDZz
43U967NgIqOIlyY0j9WI+NY17dbWoFuNTdoP1W7D
-----
```

Subject:

CN=rsa-test.aetna.com
O=Aetna Inc.
L=Middletown
S=Connecticut
C=US

Is Subject Correct
Yes ☐ No ☐

Certificate Template: Aetna Web Server

Email Address for CN:

(List each Email Address on a separate line)

Subject Alternative Name:

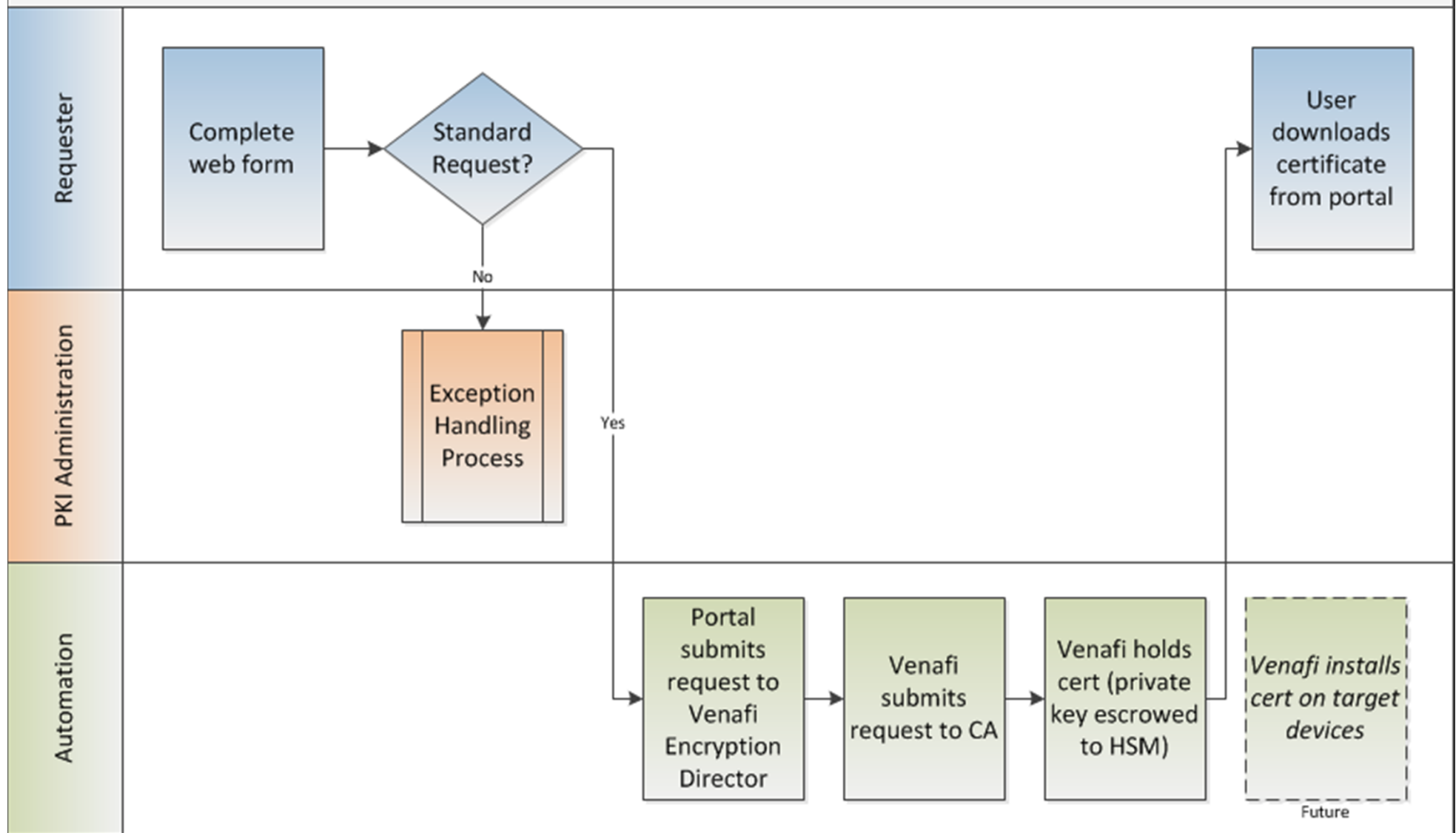
Our Solution

- Completely overhaul process and technology
 - Security objective: Protect the keys
 - Engineering objective: Optimize the workflow
 - Executive objective: Eliminate outages



Current State at Aetna

Aetna Certificate Request Process





[Home](#)

[My Certificates](#)

[New Certificate Request](#)

[Manage Certificate](#)

Main Menu

- [Request A New Certificate](#)

Click here to request a new Certificate. You may upload CSR or generate private key with your request.

- [My Certificates](#)

Click here to see list of certificates you are authorized to manage.

- [Renew An Existing Certificate](#)

Click here to renew a Certificate. You or your AD groups should be contact on the original certificate to perform this operation.

- [Download An Existing Certificate or Private Key](#)

Click here to download an existing Certificate or private key. You or your AD groups should be contact on the original certificate to perform this operation.

- [Update Information On An Existing Certificate](#)

Click here to update Contacts and/or TABoR Id on an existing Certificate. You or your AD groups should be contact on the original certificate to perform this operation.

- [Revoke An Existing Certificate](#)

Click here to revoke an existing Certificate. You or your AD groups should be contact on the original certificate to perform this operation.



Request New Certificate

Certificate Usage: Web Server

Do you have CSR?: ☒ No ☐ Yes

Certificate Name:

Add Certificate Name as a Subject Alternate Name: ☒

Subject Alternate Name(s): [Add](#)

Name: [Delete](#)

Key Size: 2048

Contacts: [Add](#)

Name: Tompkins, Timothy [Delete](#)

TABoR Id:

Will the Certificate be hosted outside Aetna?: ☒ No ☐ Yes

Target Systems: [Add](#)

FQDN of Server: Port: 443 Application: IIS on Windows 2003 [Delete](#)

Cancel

Submit



Project Pitfalls

- Other parties relying on existing interfaces
- Resistance to automation
- Customization scope creep
- Vendor product limitations



Applying to your Organization

- Within the next 3 months
 - Conduct analysis of current PKI operations
 - Key management standards
 - Outages related to certificates
 - Security of private keys
 - Workflows
 - Inventory certificates
- Within the next 6 months
 - Decide on appropriate level of monitoring, centralization, and automation
- Within the next 9 months
 - Design a workflow first, then implement supporting technology



Session Learning Objectives Revisited

- Identify security issues that cloud vendors must address for highly regulated industries
- Recognize the problems associated with encryption chaos
- Become familiar with Aetna's best-practices approach to automating certificate management
- Relate lessons learned from Aetna's implementation to your own organization



Conclusion

- Thanks for attending!
- Questions?
- Feel free to contact me for further discussion or questions:

Tim Tompkins
Aetna, Inc.
tompkinst@aetna.com

