MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

CRYPTO-AGILITY:

RESPONDING QUICKLY TO SECURITY EVENTS

Paul Turner

CTO Products, Venafi

Two Actors on a Network

People
Usernames & Passwords

Machines
Keys & Certificates

Secure and protect identities – people and machines

$7 Billion Annually
on Identity and Access Management

We spend billions protecting usernames and passwords.

But almost nothing protecting **machine identities** which secure our critical systems and data.

Source: MarketsandMarkets.com. Identity and Access Management Market by Component, by Organization Size, by Deployment, by Vertical, and by Region - Global Forecast to 2020. March 2016.

InfoSecWorld Conference & Expo 2018

Key and Certificate Growth in the Enterprise

Certificate Authorities

thawte · GeoTrust · VeriSign · COMODO · Entrust · Microsoft · RSA · cybertrust · redhat · IBM

Symmetric Key Vendors & Products

IBM · Sun microsystems · RSA · THALES · SafeNet · ORACLE · hp · Microsoft · VORMETRIC · NetApp · Townsend SECURITY

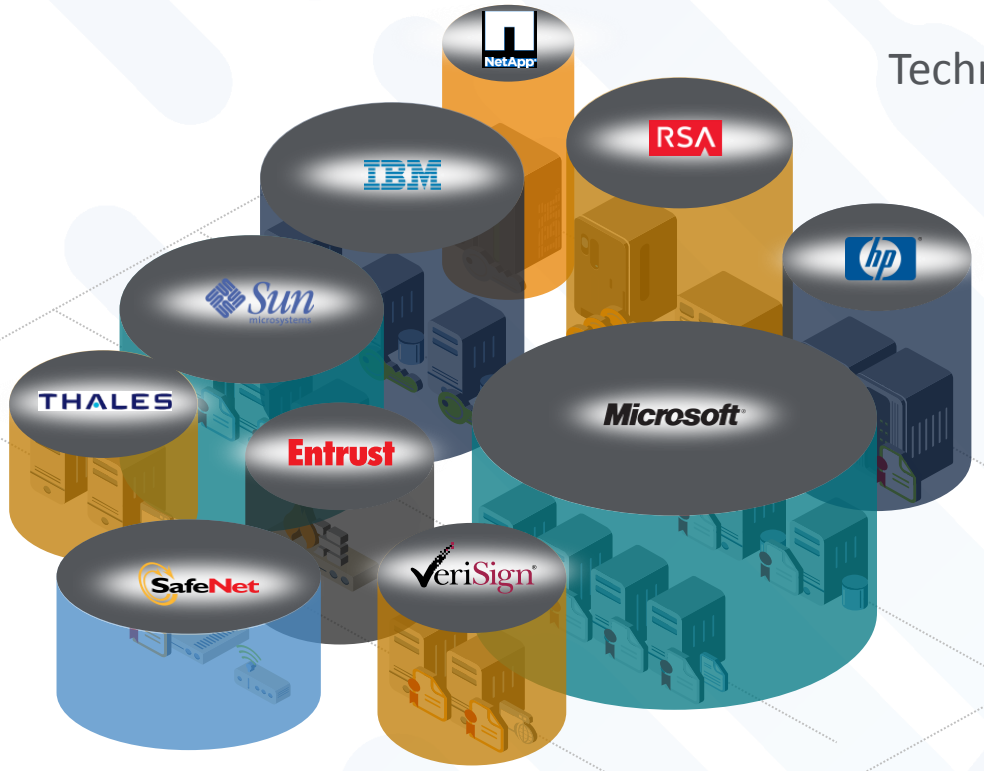
SSH Technologies

OpenSSH · TECTIA · MICRO FOCUS

InfoSecWorld Conference & Expo 2018

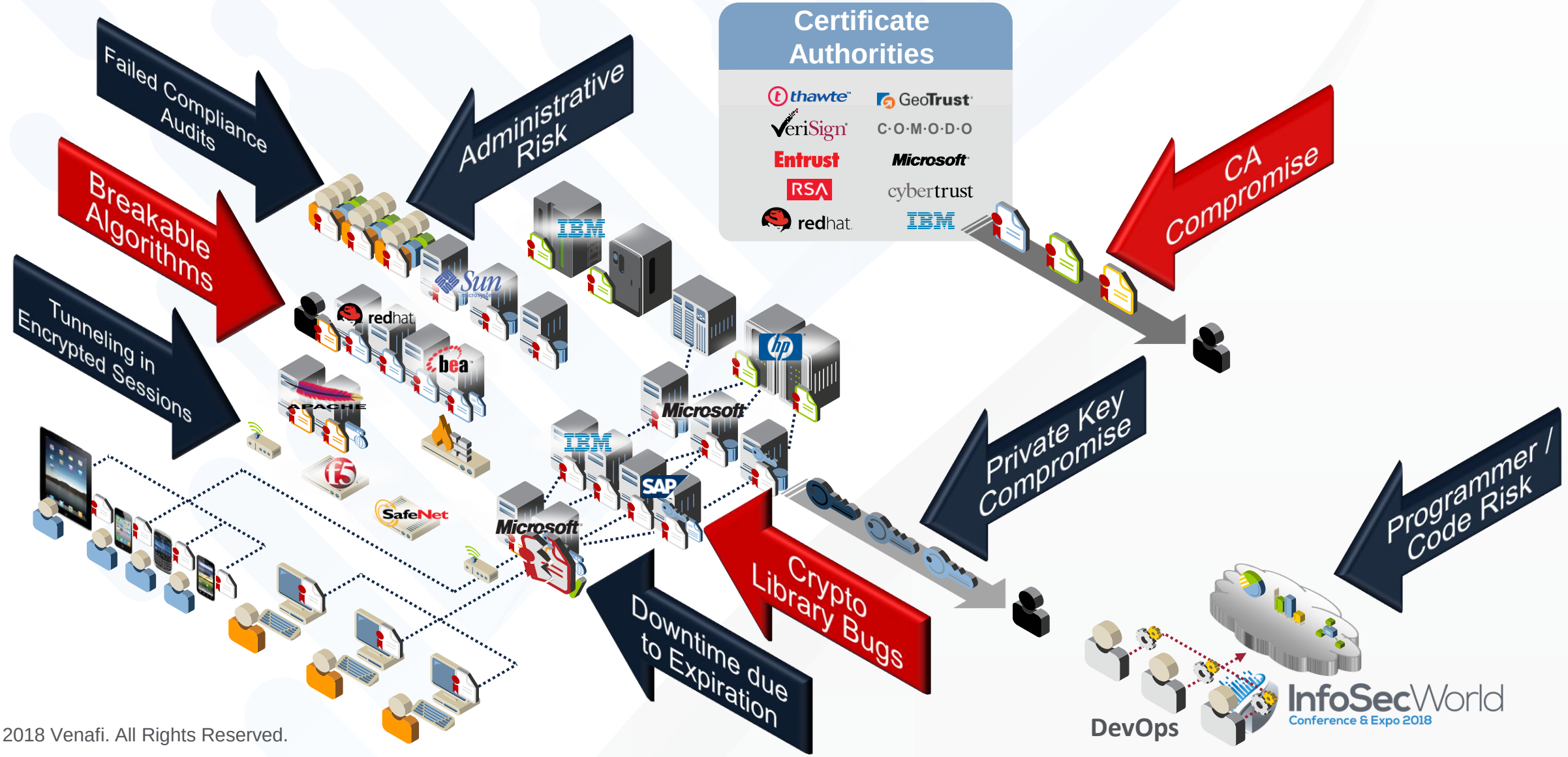
Certificate and Key Management Silos

Technology silos

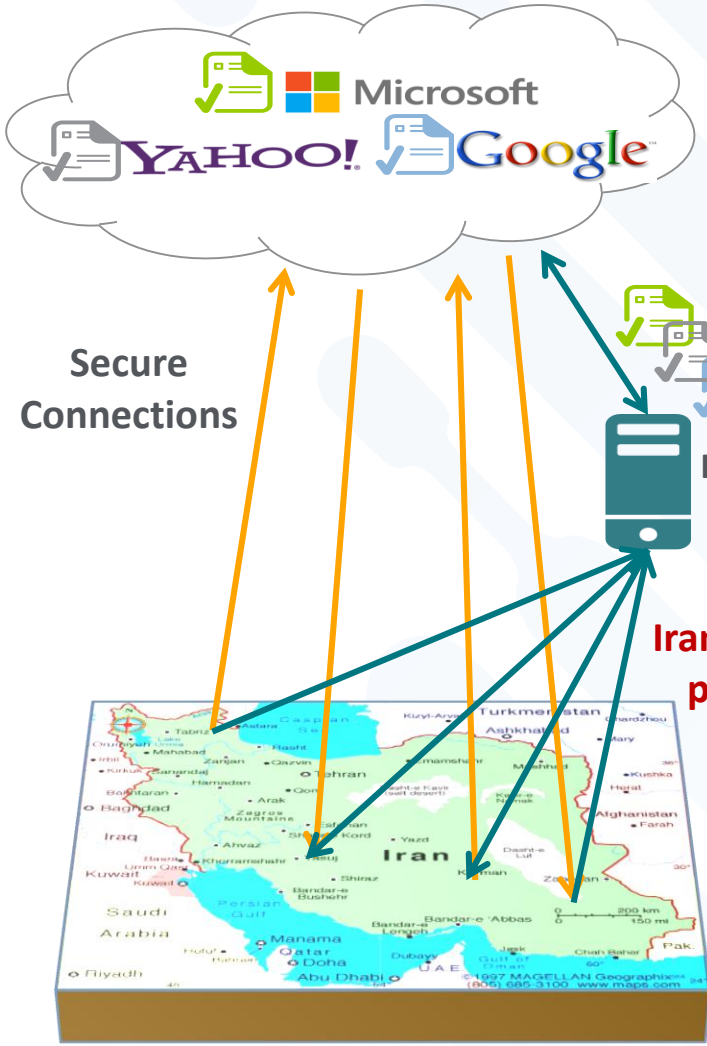


Departmental silos

Certificate and Key Management Risks



DigiNotar CA Compromise Impact

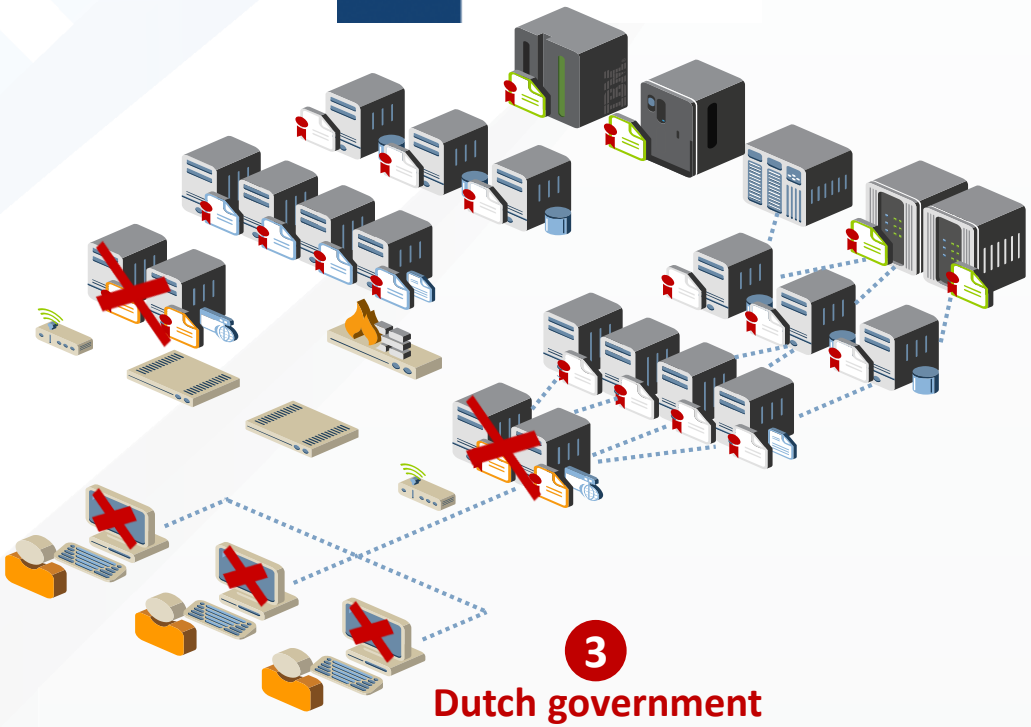


DigiNotar
Internet Trust Services

1
Iranian government performs MITM

2
Major browsers blacklist DigiNotar

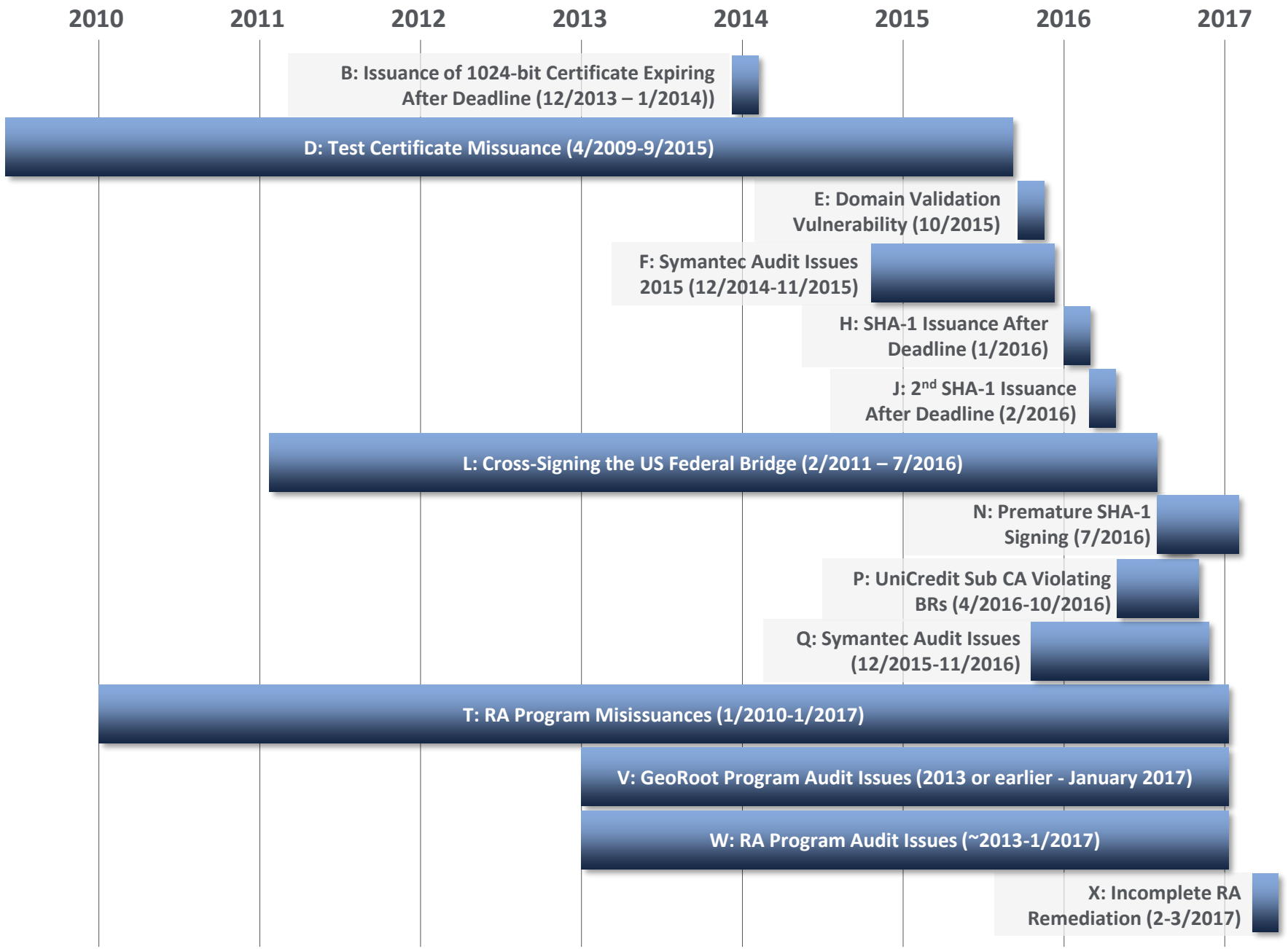
Government of the Netherlands



3
Dutch government goes offline

InfoSecWorld
Conference & Expo 2018

Google and Mozilla distrust Symantec certificates

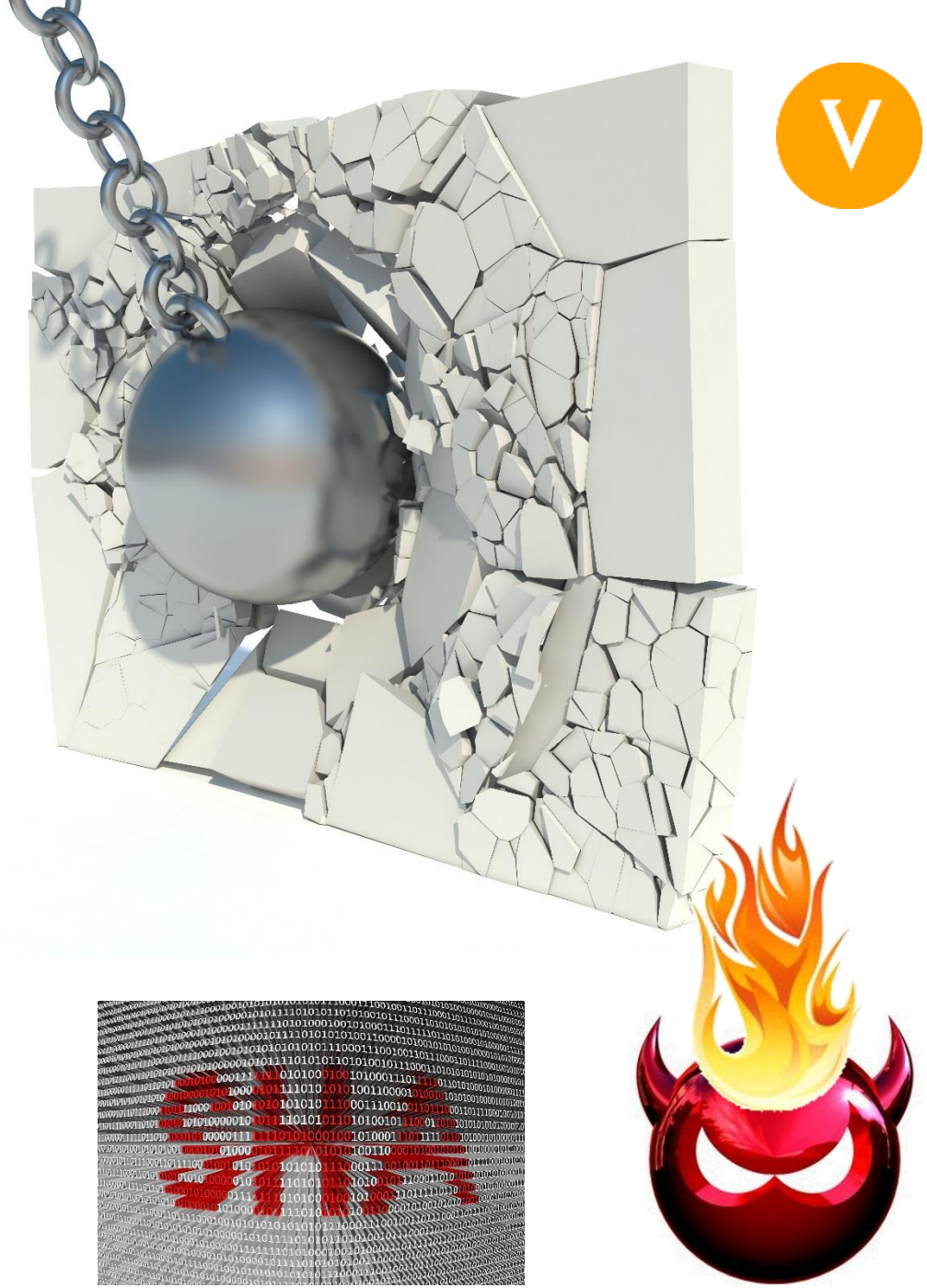


Vulnerable Algorithm

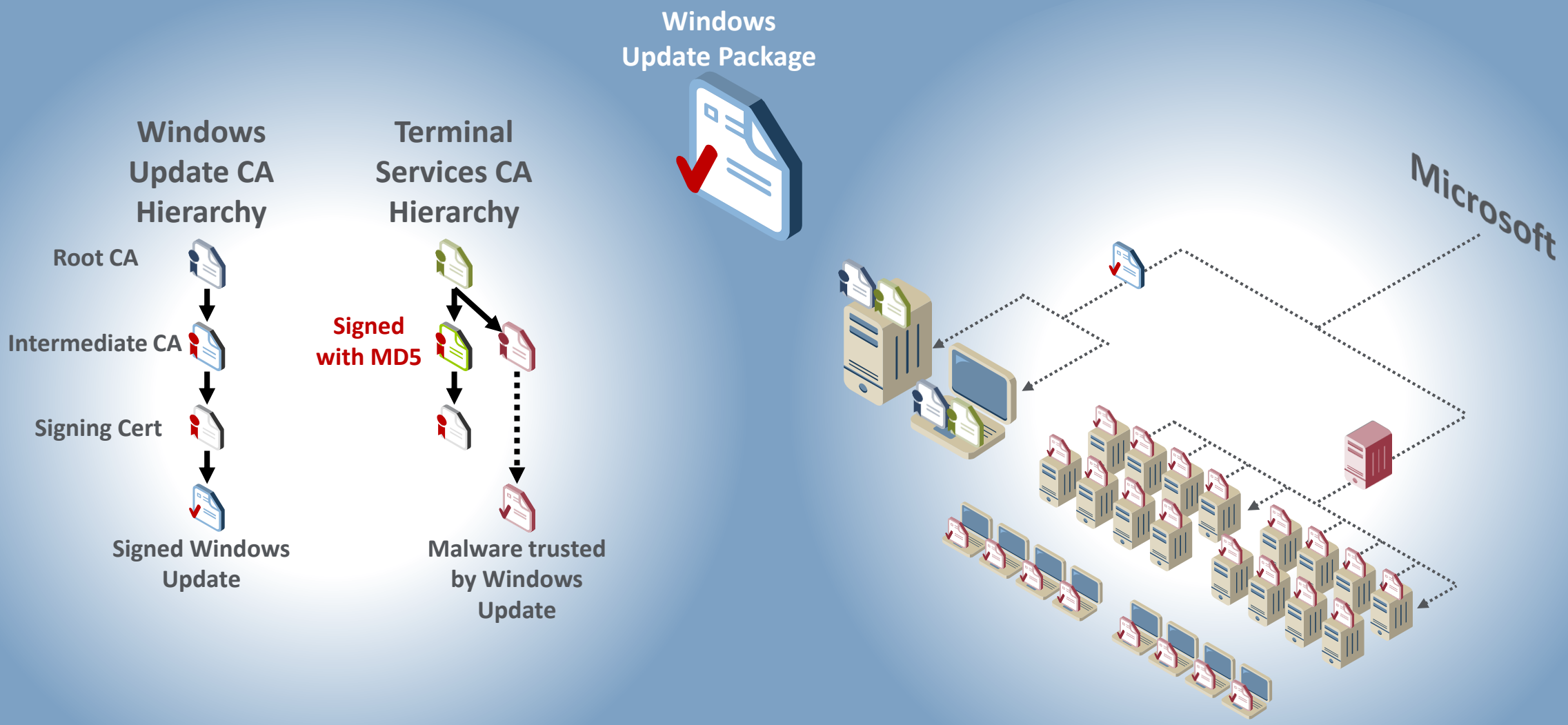
Algorithms become breakable over time

- Increased computing capabilities
- Improved breaking techniques

Weaknesses in signing algorithms allow attackers to forge rogue certificates



FLAME Malware – Exploiting MD5 for Rapid Distribution



SHA-1 SHATTERED

SHA-1 replacement deadline

- Known insecure for years
- Still missed early 2017 deprecation deadlines

In early 2017 more than
1 in 5 certificates for unique
IP addresses were still using SHA-1

Crypto Bugs

Bugs in cryptographic libraries can make keys easier to break

Bugs in programs that use keys and certificates may expose keys to compromise

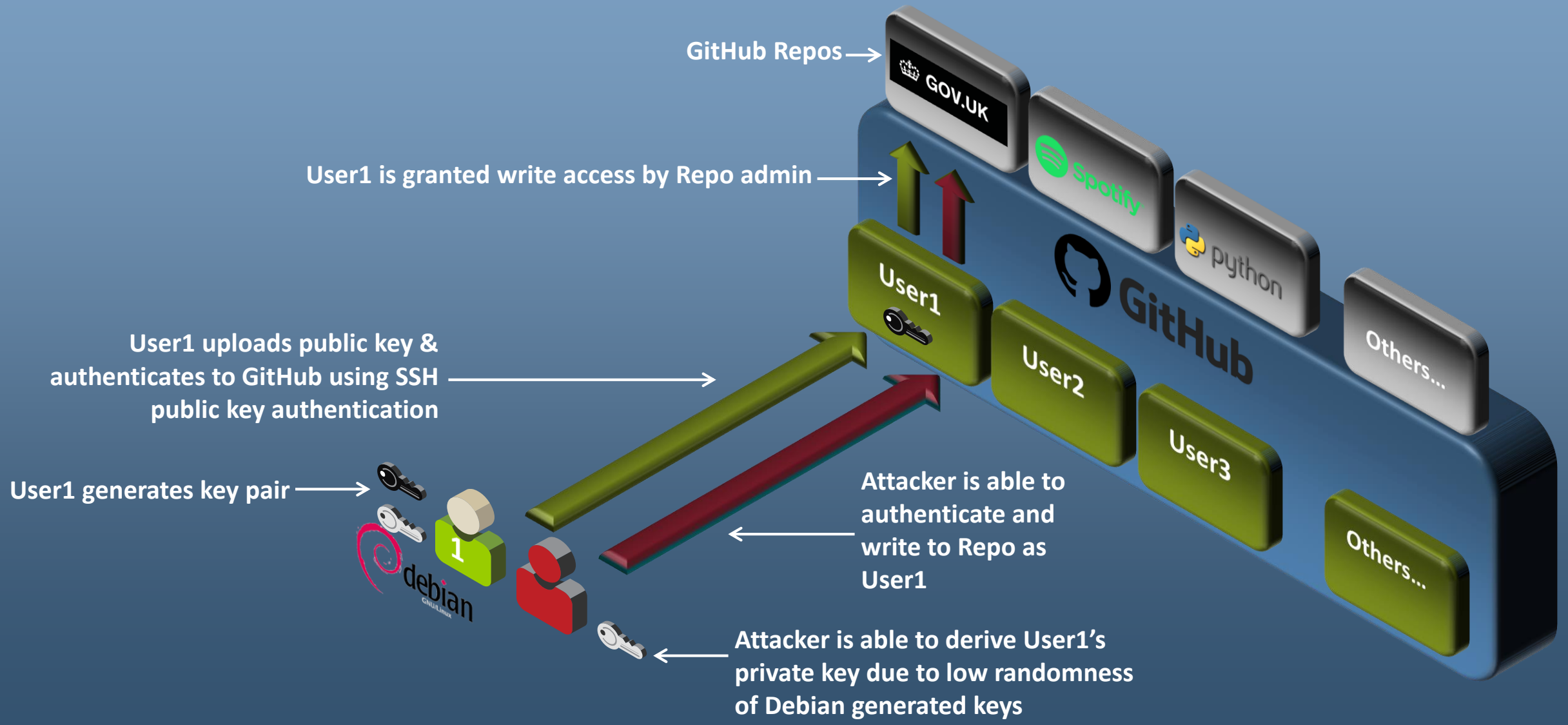
© 2018 Venafi

InfoSecWorld
Conference & Expo 2018

Crypto Bugs

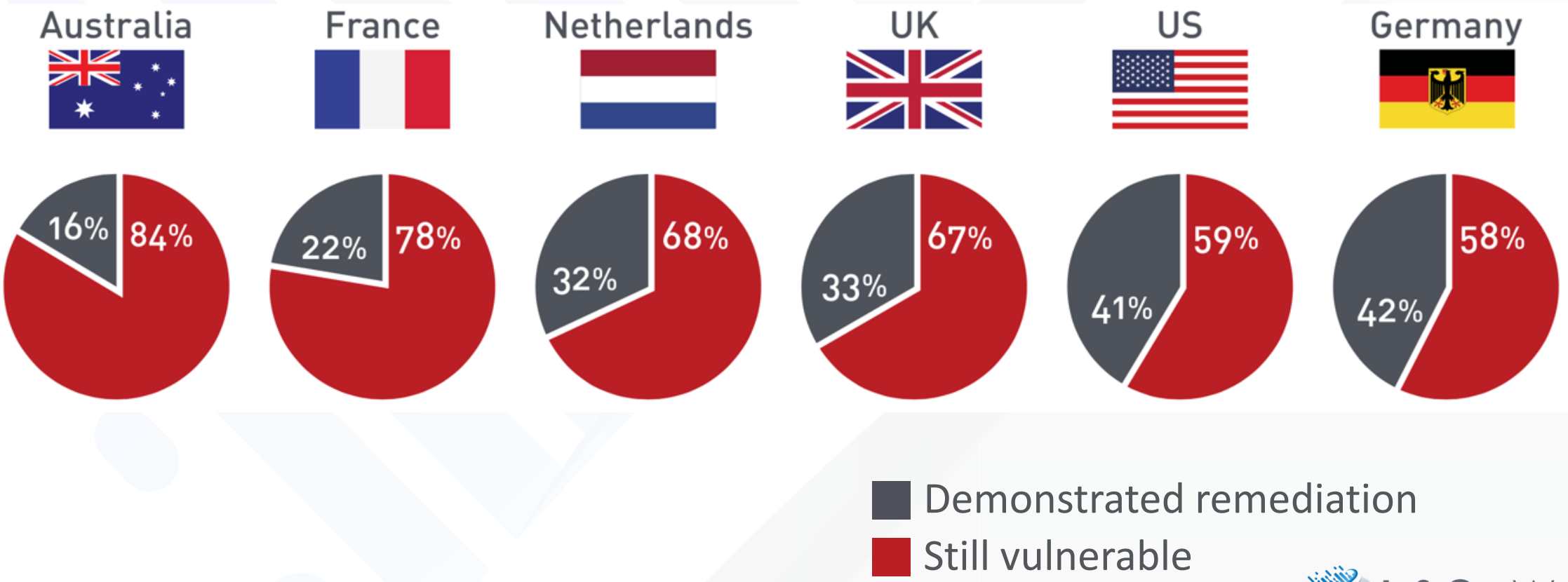
- Debian
- Heartbleed
- Infineon
- …

Weak SSH Keys - GitHub Example



Global 2000: Heartbleed Remediation

Remediation 1 year later – April 2015

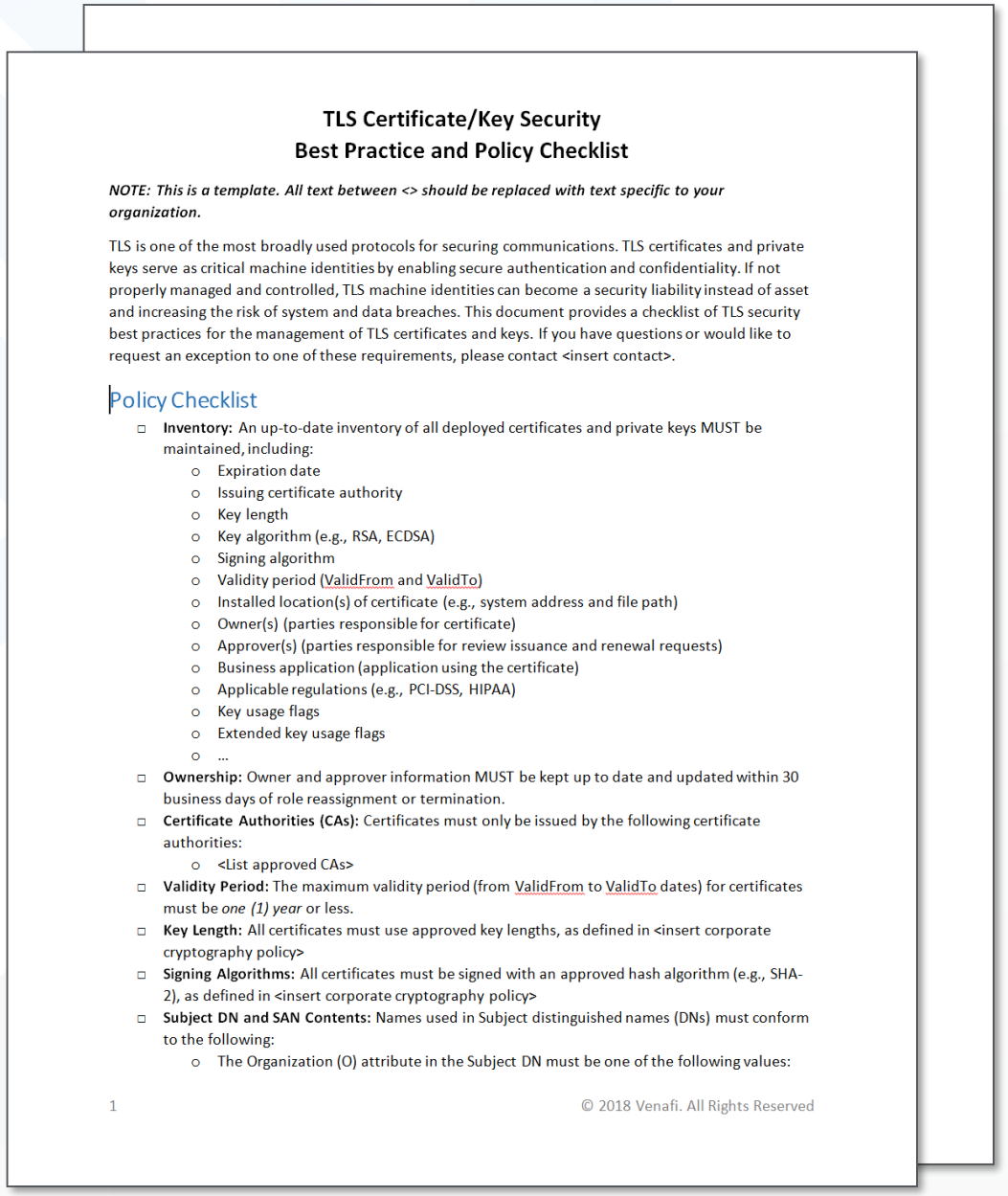


Establishing Crypto-Agility

- Establish and communicate clear policies
- Inventory all crypto assets
- Replace vulnerable keys and certs
- Maintain ownership information
- Automate management
- Automate replacement tracking

Establishing & Communicating Clear Policies

- Distributed nature of cryptography makes policies a requirement
- Must include:
  - Cert/key attributes (key length, algorithm, etc.)
  - Inventory
  - Ownership management
  - Crypto-agility (maximum time to replace all crypto assets)
  - Private key security
  - Dual control
  - CA trust
  - Roles and responsibilities



TLS Certificate/Key Security
Best Practice and Policy Checklist

NOTE: This is a template. All text between <> should be replaced with text specific to your organization.

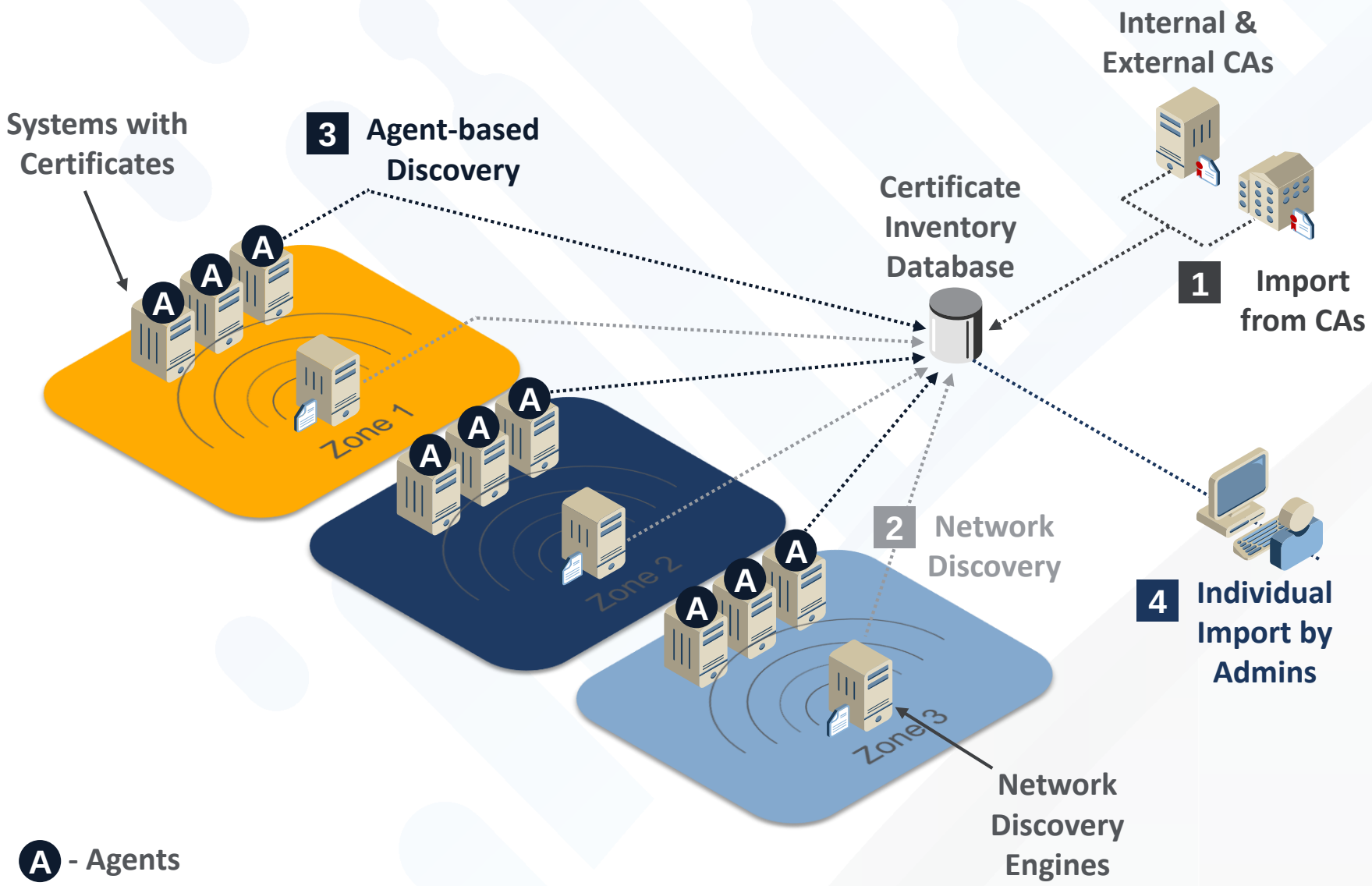
TLS is one of the most broadly used protocols for securing communications. TLS certificates and private keys serve as critical machine identities by enabling secure authentication and confidentiality. If not properly managed and controlled, TLS machine identities can become a security liability instead of asset and increasing the risk of system and data breaches. This document provides a checklist of TLS security best practices for the management of TLS certificates and keys. If you have questions or would like to request an exception to one of these requirements, please contact <insert contact>.

Policy Checklist

- ☐ **Inventory:** An up-to-date inventory of all deployed certificates and private keys MUST be maintained, including:
  - Expiration date
  - Issuing certificate authority
  - Key length
  - Key algorithm (e.g., RSA, ECDSA)
  - Signing algorithm
  - Validity period (ValidFrom and ValidTo)
  - Installed location(s) of certificate (e.g., system address and file path)
  - Owner(s) (parties responsible for certificate)
  - Approver(s) (parties responsible for review issuance and renewal requests)
  - Business application (application using the certificate)
  - Applicable regulations (e.g., PCI-DSS, HIPAA)
  - Key usage flags
  - Extended key usage flags
  - …
- ☐ **Ownership:** Owner and approver information MUST be kept up to date and updated within 30 business days of role reassignment or termination.
- ☐ **Certificate Authorities (CAs):** Certificates must only be issued by the following certificate authorities:
  - <List approved CAs>
- ☐ **Validity Period:** The maximum validity period (from ValidFrom to ValidTo dates) for certificates must be *one (1) year* or less.
- ☐ **Key Length:** All certificates must use approved key lengths, as defined in <insert corporate cryptography policy>
- ☐ **Signing Algorithms:** All certificates must be signed with an approved hash algorithm (e.g., SHA-2), as defined in <insert corporate cryptography policy>
- ☐ **Subject DN and SAN Contents:** Names used in Subject distinguished names (DNs) must conform to the following:
  - The Organization (O) attribute in the Subject DN must be one of the following values:

1 © 2018 Venafi. All Rights Reserved

Establishing a Comprehensive Inventory



Include:

- Certificates
  - Server
  - Client
  - User
  - CA (root)
- SSH
  - Authorized keys
  - Host and user private keys
  - Known host
- DNSSEC
- Symmetric
- …

Default Root CA Certs Trusted in Windows

- AAA Certificate Services
- ABA.ECOM Root CA
- AC Raiz Certicamara S.A.
- AC Raiz DNIE
- AC RAIS FNMT –RCM
- ACEDICOMRoot
- A-CERT ADVANCED
- ACNLB
- Actalis Authentication CA G1
- AddTrust External CA Root
- AdminCA-CD-T01
- Admin-Root-CA
- AffirmTrust Comercial
- AffirmTrust Networking
- AffirmTrust Premium
- AffirmTrust Premium ECC
- Agence Nationale de Certification Electronique
- Agence Nationale de Certification Electronique
- America Online Root Certification Authority 1
- America Online Root Certification Authority 2
- ANCERT Certificados CGN
- ANCERT Certificados Notariales
- ANCERT Corporaciones de Derecho Publico
- ANF Server CA
- Application CA G2
- Application CA
- Arge Daten Oesterreichische Gesellschaft fuer Datenschutz
- A-Trust-nQual-01
- A-Trust-nQual-03
- A-Trust-Qual-01
- A-Trust-Qual-02
- A-Trust-Qual-03
- Autoridad Certificadora Raiz de la Secretaria de Economia
- Autoridad Certificadora Raiz de la Secretaria de Economia
- Autoridad de Certificacion de la Abogacia
- Autoridad de Certificacion Firmaprofesional CIF A6263468
- Autoridad de Certificacion Firmaprofesional CIF A6263468
- Autoridad de Certificacion Raiz delEstado Venezolano
- Autoridad Certificadora Raiz Brasileira
- Autoridad Certificadora Raiz Brasileira v 1
- Baltimore CyberTrust Root
- Baltimore EZ by DST
- Buypass Class 2 CA 1
- Buypass Class 3 CA 1
- CA Disig
- CCA India 2007
- Certeurope Root CA 2
- CERTICAMARA S.A.
- Certificado de la Clave Principal
- Certificado Empresarial Clase-A
- Certigna
- Certinomis – Authorite Racine
- Certipost E-Trust Primary Normalized CA
- Certipost E-Trust Primary Qualified CA
- Certipost E-Trust TOP Root CA
- Certisign – Autoridad Certificadora – AC2
- Certisign – Autoridad Certificadora – AC4
- Certisign Autoridad Certificadora AC1S
- Certisign Autoridad Certificadora AC3S
- CertRSA01
- certSIGN ROOT CA
- Certum CA
- Certum Trust Network CA
- CESAM
- Chambers of Commerce Root
- Chambers of Commerce Root – 2008
- China Internet Information Center EV Certificates Root
- Cisco Root CA 2048
- Class 1 Primary CA
- Class 1 Public Primary Certification Authority
- Class 1 Public Primary Certification Authority
- Class 1 Public Primary Certification Authority
- Class 2 Primary CA
- Class 2 Public Primary Certification Authority
- Class 2 Public Primary Certification Authority
- Class 3 Primary CA
- Class 3 Public Primary Certification Authority
- Class 3 Public Primary Certification Authority
- Class 3P Primary CA
- Class 3TS Primary CA
- CNNIC ROOT
- Common Policy
- COMODO ECC Certification Authority
- COMODO RSA Certification Authority
- ComSign Advanced Security CA
- ComSign CA
- ComSign Secured CA
- Copyright © 1997 Microsoft Corp.
- Correo Uruguayo – Root CA
- Deutsche Telekom Root CA 2
- DigiCert Assured ID Root CA
- DigiCert Global Root CA
- DigiCert High Assurance EV Root CA
- DST (ANX Network) CA
- DST (NRF) RootCA
- DST (UPS) RootCA
- DST ACES CA X6
- DST Root CA X3
- DST RootCA X1
- DST RootCA X2
- DSTCA E1
- DSTCA E2
- DST-Entrust GTI
- D-TRUST Qualified Root CA 1 2007:PN
- D-TRUST Root Class 2 CA 2007
- D-TRUST Root Class 3 CA 2007
- EBG Elektronik Sertifika Hizmet Saglayicisi
- EC-ACC
- E-CERT ROOT CA
- Echoworx Root CA2
- ECRaizEstado
- e-Guven Kok Elektronik Sertifika Hizmet SaglayiCISI
- E-ME SSI (RCA)
- Entrust Root Certification Authority
- Entrust Root Certification Authority – G2
- Entrust.net Certification Authority (2048)
- Entrust.net Secure Server Certification Authority
- ePKI Root Certification Authority
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure eBusiness CA-2
- Equifax Secure Global eBusiness CA-1
- eSign Imperito Primary Root CA
- FNMT Clase 2 CA
- Gatekeeper Root CA
- GeoTrust Global CA
- GeoTrust Global CA 2
- GeoTrust Primary Certification Authority
- GeoTrust Primary Certification Authority – G2
- GeoTrust Primary Certification Authority – G3
- GeoTrust Universal CA
- GeoTrust Universal CA 2
- Global Chambersign Root
- Global Chambersign Root – 2008
- GlobalSign
- GlobalSign
- GlobalSign Root CA
- GLOBAL TRUST
- Go Daddy Class 2 Certification Authority
- Go Daddy Root Certificate Authority – G2
- Government Root Certificate Authority
- GPKIRootCA
- GTE CyberTrust Global Root
- GTE CyberTrust Root
- GTE CyberTrust Root
- Halcom CA FO
- Halcom CA PO 2
- Hongkong Post Root CA
- Hongkong Post Root CA 1
- http://www.valicert.com
- http://www.valicert.com
- http://www.valicert.com
- I.CA – Qualified Certification Authority, 09/2009
- I.CA – Qualified root certificate
- I.CA – Standard Certification Authority, 09/2009
- I.CA – Standard root certificate
- IGC/A
- InfoNotary CSP Root
- IPS SERVIDORES
- ipsCA Global CA Root
- ipsCA Main CA Root
- Izenpe.com
- Izenpe.com
- Juur-SK
- KEYNECTIS ROOT CA
- KISA RootCA 1
- KISA RootCA 3
- Macao Post eSignTrust Root Certification Authority
- Microsec e-Szigno root CA
- Microsec e-Szigno root CA 2009
- Microsoft Authenticode(tm) Root authority
- Microsoft Root Authority
- Microsoft Root Certificate Authority
- Microsoft Root Certificate Authority 2010
- Microsoft Root Certificate Authority 2011
- NetLock Arany (Class Gold) Fotanusitvany
- NetLock Expressz (Class C) Tanusitvanykiado
- NetLock Kozjegyzoi (Class A) Tanusitvanykiado
- NetLock Minositett Kozjegyzoi (Class AA) Tanusitvanykiado
- NetLock Platina (Class Platinum) Fotaniusitvany
- NetLock Uzleti (Class B) Tanusitvanykiado
- Netrust CA1
- NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.
- OISTE WISeKey Global Root GA CA
- Post.Trust Root CA
- Post.Trust Root CA
- Posta CA Root
- POSTArCA
- PostSignum Root QCA 2
- Primary Utility Root CA
- Public Notary root
- QuoVadis Root CA 2
- QuoVadis Root CA 3
- QuoVadis Root Certification Authority
- Registradores de Espana – CA Raiz
- Root CA Generalitat Valenciana
- RSA Security 2048 V3
- Secure Global CA
- Secure Server Certification Authority
- SecureNet CA Class B
- SecureSign RootCA1
- SecureSign RootCA11
- SecureSign RootCA2
- SecureSign RootCA3
- SecureTrust CA
- Security Communication EV RootCA1
- Security Communication RootCA1
- Security Communication EV RootCA2
- Serasa Certificate Authority I
- Serasa Certificate Authority II
- Serasa Certificate Authority III
- SERVICIOS DE CERTIFICACION – A.N.C.
- sigen-ca
- sigov-ca
- SITHS CA v3
- Sonera Class1 CA
- Sonera Class2 CA
- SSC Root CA A
- SSC Root CA B
- SSC Root CA C
- Staat der Nederlanden Root CA
- Staat der Nederlanden Root CA – G2
- Starfield Class 2 Certification Authority
- Starfield Root Certificate Authority – G2
- Starfield Service Root Certificate Authority
- Starfield Service Root Certificate Authority – G2
- StartCom Certification Authority
- S-TRUST Authentication and Encryption Root CA 2005:PN
- Swisscom Root CA 1
- SwissSign Gold CA – G2
- SwissSign Gold Root CA – G3
- SwissSign Platinum CA – G2
- SwissSign Platinum Root CA – G3
- SwissSign Silver CA – G2
- SwissSign Silver Root CA – G3
- TC TrustCenter Class 1 CA
- TC TrustCenter Class 2 CA
- TC TrustCenter Class 2 CA II
- TC TrustCenter Class 3 CA
- TC TrustCenter Class 3 CA II
- TC TrustCenter Class 4 CA
- TC TrustCenter Class 4 CA II
- TC TrustCenter Time Stamping CA
- TC TrustCenter Universal CA
- TC TrustCenter Universal CA II
- TC TrustCenter Universal CA III
- TDC Internet Root CA
- TDC OCES CA
- Telekom-Control-Kommission Top 1
- TeliaSonera ROOT CA v1
- Thawte Personal Basic CA
- Thawte Personal Freemail
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Premium Server CA
- thawte Primary Root CA
- thawte Primary Root CA – G2
- thawte Primary Root CA – G3
- Thawte Server CA
- Thawte Server CA
- Thawte Timestamping CA
- Thawte Timestamping CA
- Trustis EVS Root CA
- Trustis FPS Root CA
- TUBITAK UEKAE Kok Sertifika Hizmet SaglayICISI – Surum 3
- TURKTRUST Elektronik Islem Hizmetleri
- TURKTRUST Elektronik Islem Hizmetleri
- TURKTRUST Elektronik Sertifika Hizmet SaglayICISI
- TURKTRUST Elektronik Sertifika Hizmet SaglayICISI
- TURKTRUST Elektronik Sertifika Hizmet SaglayICISI
- TWCA Root Certification Authority
- TWCA Root Certification Authority
- UCA Global Root
- UCA Root
- USERTrust ECC Certification Authority
- USERTrust RSA Certification Authority
- UTN – DATACorp SGC
- UTN-USERFirst-Client Authentication and Email
- UTN-USERFirst-Hardware
- UTN-USERFirst-Network Applications
- UTN-USERFirst-Object
- VAS Latvijas Pasts SSI(RCA)
- VEN-ROOTCA01-CA
- VeriSign Class 1 Public Primary Certification Authority – G3
- VeriSign Class 2 Public Primary Certification Authority – G3
- VeriSign Class 3 Public Primary Certification Authority – G3
- VeriSign Class 3 Public Primary Certification Authority – G4
- VeriSign Class 3 Public Primary Certification Authority – G5
- VeriSign Class 4 Public Primary Certification Authority – G3
- VeriSign Commercial Software Publishers CA
- VeriSign Commercial Software Publishers CA
- VeriSign Individual Software Publishers CA
- VeriSign Individual Software Publishers CA
- VeriSign Trust Network
- VeriSign Trust Network
- VeriSign Trust Network
- VeriSign Trust Network
- VeriSign Trust Network
- VeriSign Trust Network
- VeriSign Trust Network
- VeriSign Trust Network
- VeriSign Universal Root Certification Authority
- Verizon Global Root CA
- VI Registru Centras RCSC (RootCA)
- Visa eCommerce Root
- Visa Information Delivery Root CA
- VRK Gov. Root CA
- Wells Fargo Root Certificate Authority
- WellsSecure Public Root Certificate Authority
- Xcert EZ by DST
- XRamp Global Certification Authority

Information to Inventory for Crypto-Agility

- Key Length
- Key Algorithm
- Signing Algorithm
- Issuing Certificate Authority
- Location(s)
- Owner(s)
- Management processes
- Applicable regulations

Tracking Certificate and Key Owners is Crucial

Establish a baseline of all certificate and key owners

Ensure groups are tracked instead of individuals – to insulate against job changes

Ensure business units maintain up to date ownership information

Key and Certificate Growth in the Enterprise

- Key and certificate volumes are rapidly increasing into the 1000s
- Must be able to replace certificates in days, not weeks or months
- Mass replacement using manual processes is impossible

Replacement Tracking

- Tracking which certs & keys have been replacement, and which haven't, is critical
- You must know where you're still vulnerable
- Execs and business unit leaders will be asking for status
- Establish a centralized tracking and monitoring of all certificate & keys

Summary

- Machine identities—certificates and keys—impact all critical systems
- Historic crypto issues, like SHA1 replacement, were too hard and took too long
- More events are coming, and we have to do a better job
- You must have plans and systems for responding to mass key and certificate replacement events
- Imperative: Plan and establish crypto-agility

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Paul Turner

CTO Products, Venafi