Digitale Zertifikate und PKI Webinar
28. Mai / 04. Juni 2024

Weil Sicherheit alles ändert.

Dirk Gluch
Principal Security Engineer
gluch@avantec.ch

Digital certificates and PKI Assessment

- Public trusted certificates
- Private trusted certificates
- Internal PKI Assessment
- …

AVANTEC
Competence. Security. Trust.

Digitale Zertifikate und PKI Webinar
28. Mai / 04. Juni 2024

Use case

- Securing communication
  - Intern & extern
  - Identification and encryption
  - TLS (SSL), RDP
- Securing OT networks
- Secure Authentication with internal and external IdPs
  - SAML, Oauth
  - MS Entra ID – cba
  - Good old Smart Card
  - Combination with FIDO
- Document signing
- Code signing
- Secure e-Mail

Public trusted certificates

- Usage:
  - TLS/SSL certificate, code or document signing, authentication (azure)
- Requirements for the future
  - More than 3000 Bits
  - One year (90 day)
  - https://www.tec-bite.ch/key-length-versus-life-time/
    - Code signing and document signing trusted for the next 10 years
- Updates via TrustCenter
  - ACME
- Central and comprehensive Certificate Management

AVANTEC
Competence. Security. Trust.

Digitale Zertifikate und PKI Webinar
28. Mai / 04. Juni 2024

Private trusted certificates

- Flexible customizing certificates
  - Validity
  - Enrolment
  - Automation
  - Enhanced Key usages
  - Flexible configuration of certificate parameters

- Securing communication
- Identification of communication partners
- Authentication
- Securing script execution

➔ Establishing and managing your own PKI

Challenges

- Private key protection → HSM
- Certificate where the subject or subject alternate name is not well controlled
  https://posts.specterops.io/certified-pre-owned-d95910965cd2
- NDES (webserver) – PETITPOTAM → disable NTML
- Updating certificates before they are expired
- Updating CRLs
- Certificate templates

AVANTEC
Competence. Security. Trust.

Digitale Zertifikate und PKI Webinar
28. Mai / 04. Juni 2024

PKI Assessment – Microsoft Certificate Services - 1

- https://www.tec-bite.ch/ueberpruefe-die-pki-so-gehts/
- Documentation – Concept – Operating – Disaster Recovery Guides
- Protect the private key
  - Software, Appliances with disc encryption, TPM, HSM – Smart Cards
  - CA, NDES, CES, all enrolment agents certificates
- Permission
  - 4-eyes principals, identification
- Backup

- 2

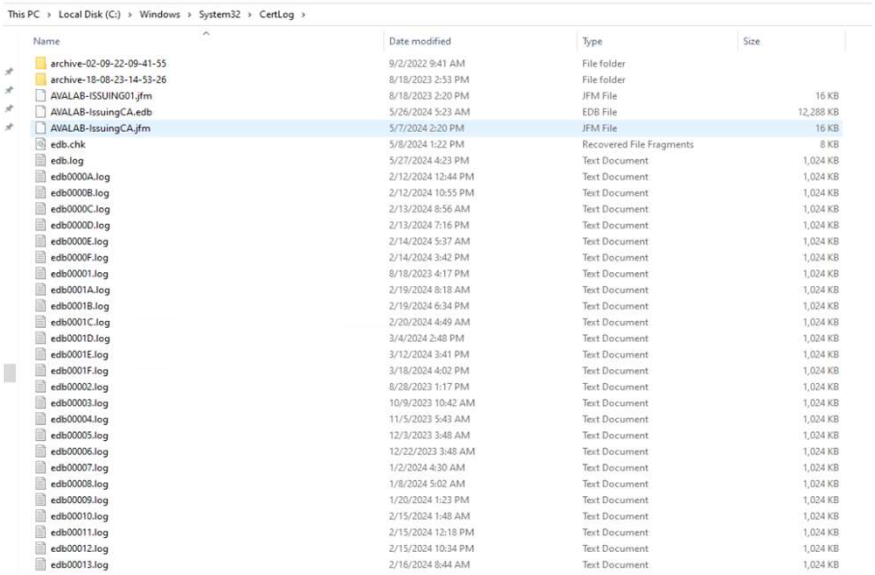
- CA config
  - SHA-1 and 2048 Bit for RSA key length should not be a theme
- CDP & AIA – for external usages, monitoring
  - Example MS Entra ID
- Updates
  - SID in client certificates
  - https://www.pkisolutions.com/adcs-hotfixes/
- SMTP Auditing
  - Recover all certificates between last backup and outage

AVANTEC
Competence. Security. Trust.

Digitale Zertifikate und PKI Webinar
28. Mai / 04. Juni 2024

Database backup & clean-Up

- Certutil –backupdb
- Certutil –deleterow
  - managebility



Subject name supply in request

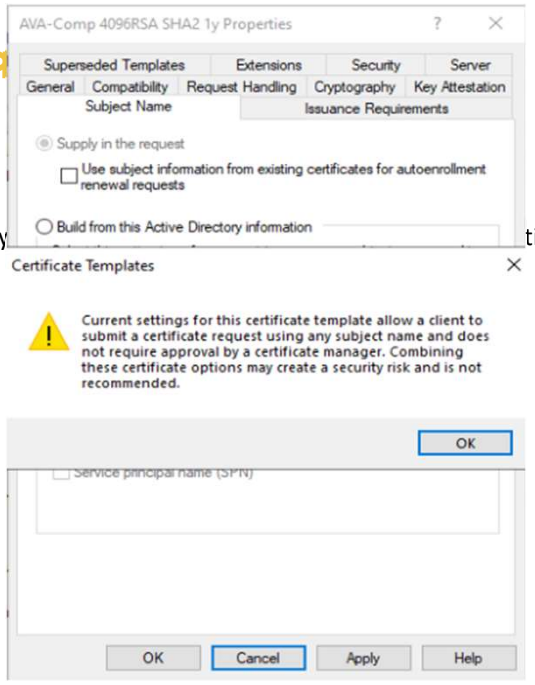
- Subject name or subject alternate name
- Certificate manager is responsible for identifying requester and the content of the issued certificate

AVANTEC
Competence. Security. Trust.

Digitale Zertifikate und PKI Webinar
28. Mai / 04. Juni 2024

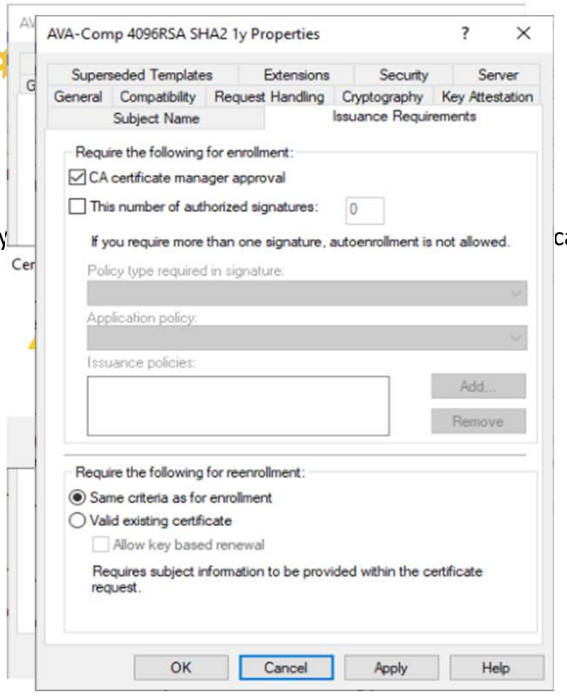
Subject name supply in req

- Subject name or subject alternate name
- Certificate manager is responsible for identify tificate



Subject name supply in req

- Subject name or subject alternate name
- Certificate manager is responsible for identify cate

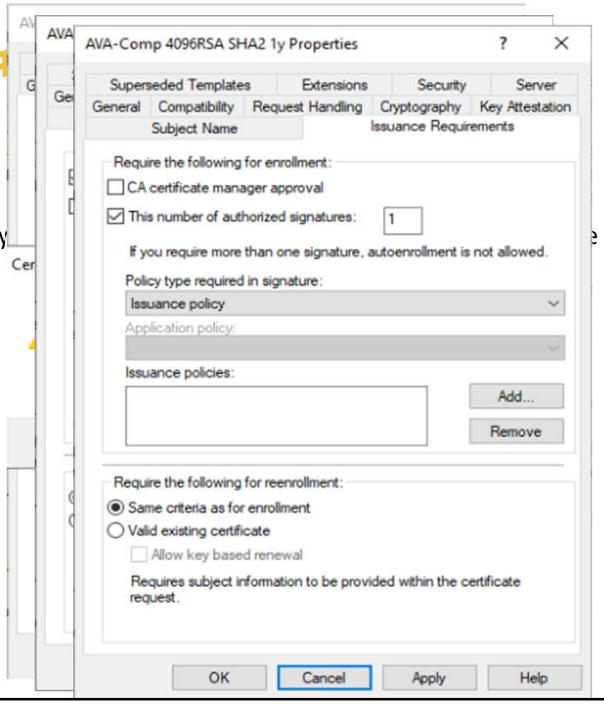


AVANTEC
Competence. Security. Trust.

Digitale Zertifikate und PKI Webinar
28. Mai / 04. Juni 2024

Subject name supply in req

- Subject name or subject alternate name
- Certificate manager is responsible for identify



Gartner Doc – April 2024
"Effectively Manage Your Organization's Certificates"

- In the new Gartner document "Effectively Manage Your Organization's Certificates" Posture Management of PKI gets an separate section.
- Not just managing certificates and CRLs, also managing the Public Key Infrastructure is important for trustworthiness of certificates
  - validity of CRLs and CA certificates → monitoring & auditing
  - threat detection
  - regulary check the security configuration
  - Best Practices Checks will help to improve availability and trust

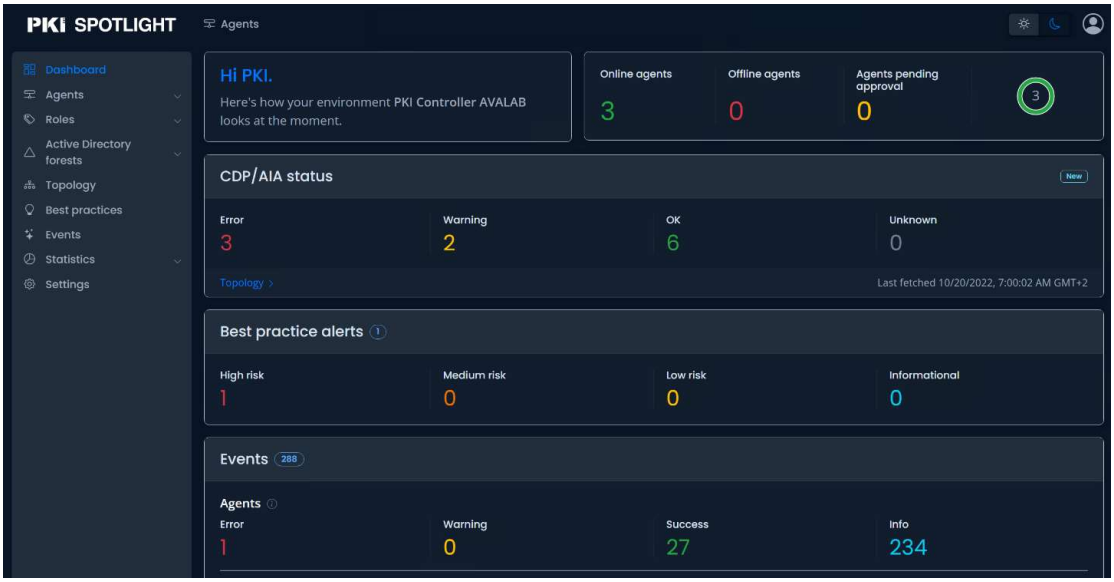
AVANTEC
Competence. Security. Trust.

Digitale Zertifikate und PKI Webinar
28. Mai / 04. Juni 2024

Comprehensive solution

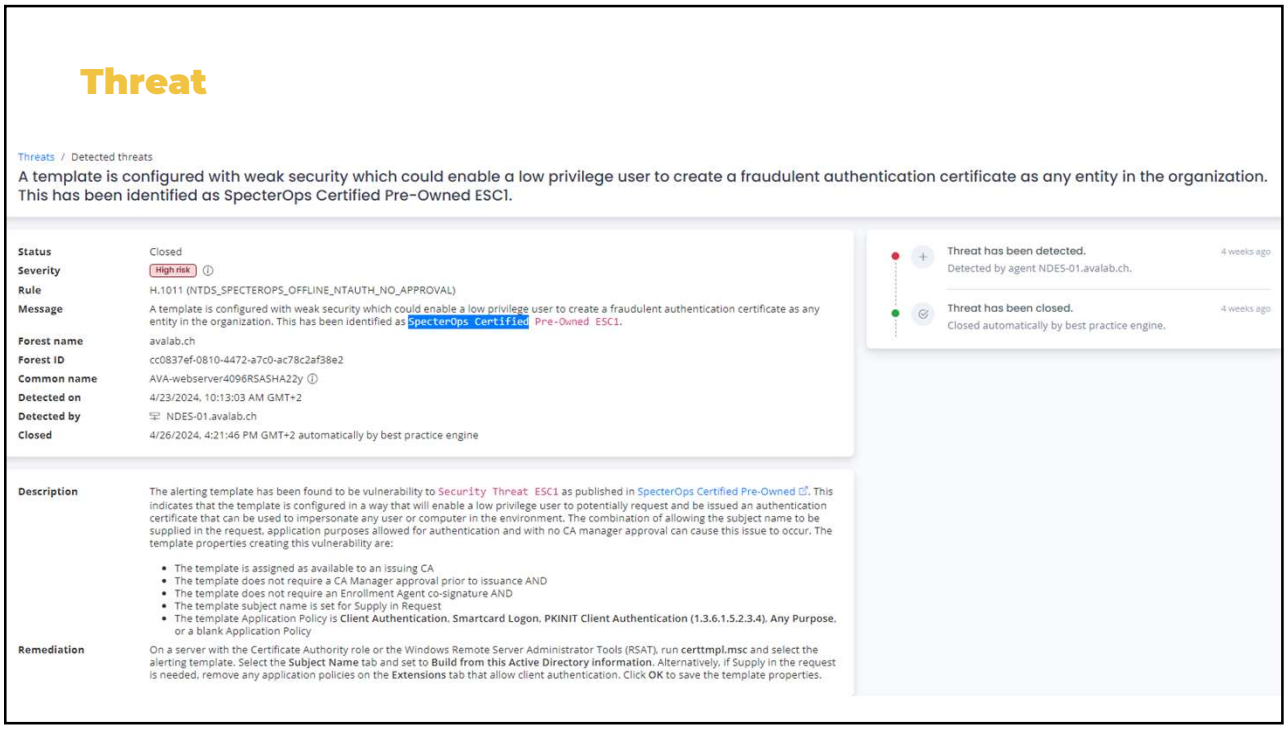
- Auditing and Monitoring your PKI environment for stable operation
  - Really is alive checks of CA components
- Threat detection - stop abnormal activity
- Security Posture Manage - continuously checks of your configuration
- Best Practice Checks & Governance

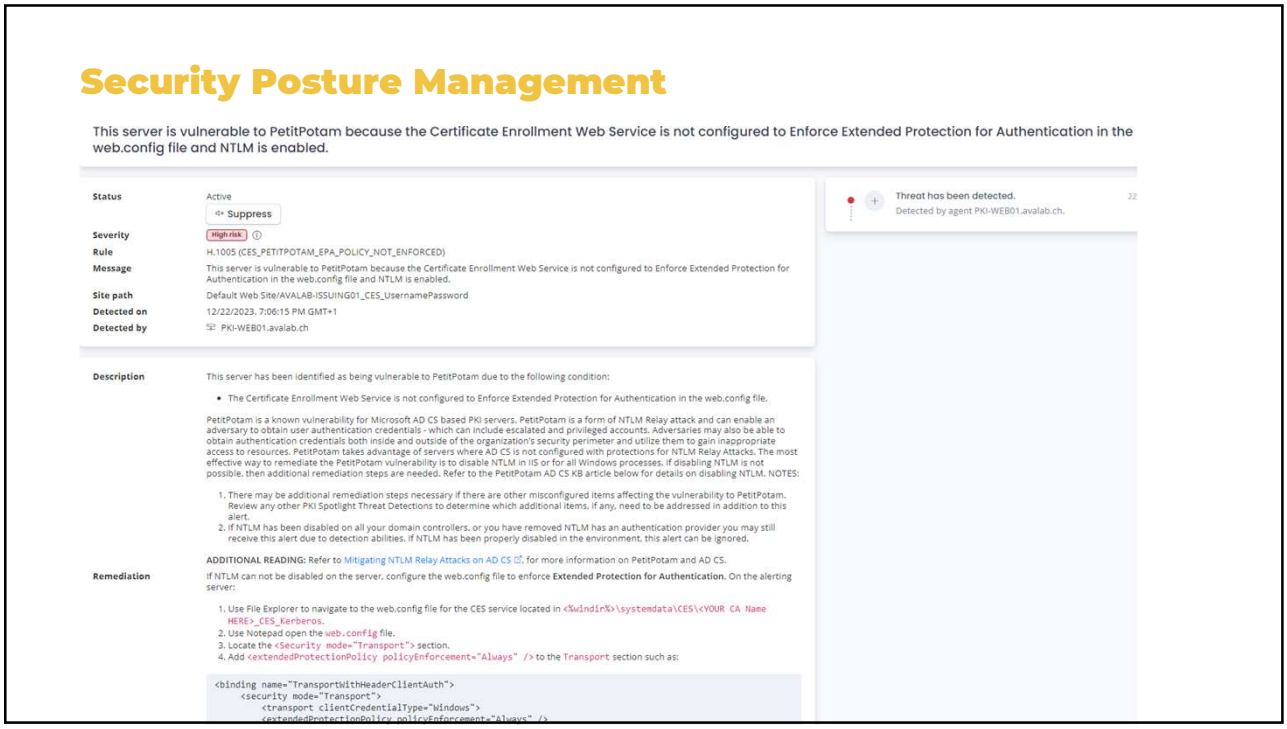
Auditing & Monitoring



AVANTEC
Competence. Security. Trust.

Digitale Zertifikate und PKI Webinar
28. Mai / 04. Juni 2024

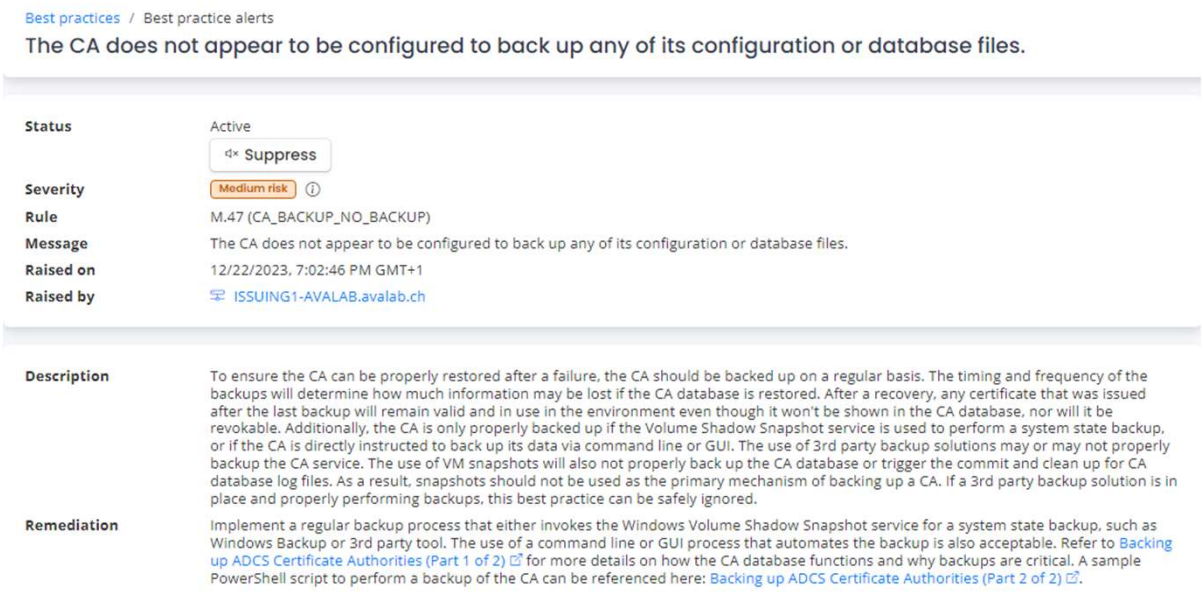




AVANTEC
Competence. Security. Trust.

Digitale Zertifikate und PKI Webinar
28. Mai / 04. Juni 2024

Best Practice Checks & Governance



Offering

PKI Assessment

- AVANTEC PKI Assessment based on CIS Controls – extended with real technical checks
- Review concept and certificate usages – Goals of the PKI
- Checking
  - RootCA config
  - IssuingCA config
    - DB Backup, Clean-Up
  - Monitoring CA certificates, CRLs, AIA
  - Extended Auditing for Disaster Recovery
  - Certificate templates
  - NDES, CEP & CES
  - Network concept & segmentation for CA

  - https://www.avantec.ch/services/public-key-infrastructure/

AVANTEC
Competence. Security. Trust.

Digitale Zertifikate und PKI Webinar
28. Mai / 04. Juni 2024

Further AVANTEC Offering

- https://www.avantec.ch/services/public-key-infrastructure/

- PKI Quick Assessment
- PKI Assessment
- PKI Consulting & Design
- PKI Design & Basic Implementation
- PKI Training

- Smart Card Management

AVANTEC
Competence. Security. Trust.