

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
- ...

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

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 NTLM
- Updating certificates before they are expired
- Updating CRLs
- Certificate templates

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

Digitale Zertifikate und PKI Webinar

28. Mai / 04. Juni 2024

Database backup & clean-Up

- Certutil –backupdb
- Certutil –deleterow
- manageability

This PC > Local Disk (C:) > Windows > System32 > CertLog >

Name	Date modified	Type	Size
archive-02-09-22-09-41-55	9/2/2022 9:41 AM	File folder	
archive-18-08-23-14-53-26	8/18/2023 2:53 PM	File folder	
AVALAB-ISSUING01.jfm	8/18/2023 2:20 PM	JFM File	16 KB
AVALAB-IssuingCA.edb	5/26/2024 5:23 AM	EDB File	12,288 KB
AVALAB-IssuingCA.jfm	5/7/2024 2:20 PM	JFM File	16 KB
edb.chk	5/8/2024 1:22 PM	Recovered File Fragments	8 KB
edb.log	5/27/2024 4:23 PM	Text Document	1,024 KB
edb0000A.log	2/12/2024 12:44 PM	Text Document	1,024 KB
edb0000B.log	2/12/2024 10:55 PM	Text Document	1,024 KB
edb0000C.log	2/13/2024 8:56 AM	Text Document	1,024 KB
edb0000D.log	2/13/2024 7:16 PM	Text Document	1,024 KB
edb0000E.log	2/14/2024 5:37 AM	Text Document	1,024 KB
edb0000F.log	2/14/2024 3:42 PM	Text Document	1,024 KB
edb00007.log	8/18/2023 4:17 PM	Text Document	1,024 KB
edb0001A.log	2/19/2024 8:18 AM	Text Document	1,024 KB
edb0001B.log	2/19/2024 6:34 PM	Text Document	1,024 KB
edb0001C.log	2/20/2024 4:49 AM	Text Document	1,024 KB
edb0001D.log	3/4/2024 2:48 PM	Text Document	1,024 KB
edb0001E.log	3/12/2024 3:41 PM	Text Document	1,024 KB
edb0001F.log	3/18/2024 4:02 PM	Text Document	1,024 KB
edb00002.log	8/28/2023 1:17 PM	Text Document	1,024 KB
edb00003.log	10/9/2023 10:42 AM	Text Document	1,024 KB
edb00004.log	11/5/2023 5:43 AM	Text Document	1,024 KB
edb00005.log	12/3/2023 3:48 AM	Text Document	1,024 KB
edb00006.log	12/22/2023 3:48 AM	Text Document	1,024 KB
edb00007.log	1/2/2024 4:30 AM	Text Document	1,024 KB
edb00008.log	1/8/2024 5:02 AM	Text Document	1,024 KB
edb00009.log	1/20/2024 1:23 PM	Text Document	1,024 KB
edb00010.log	2/15/2024 1:48 AM	Text Document	1,024 KB
edb00011.log	2/15/2024 12:18 PM	Text Document	1,024 KB
edb00012.log	2/15/2024 10:34 PM	Text Document	1,024 KB
edb00013.log	2/16/2024 8:44 AM	Text Document	1,024 KB

Subject name supply in request

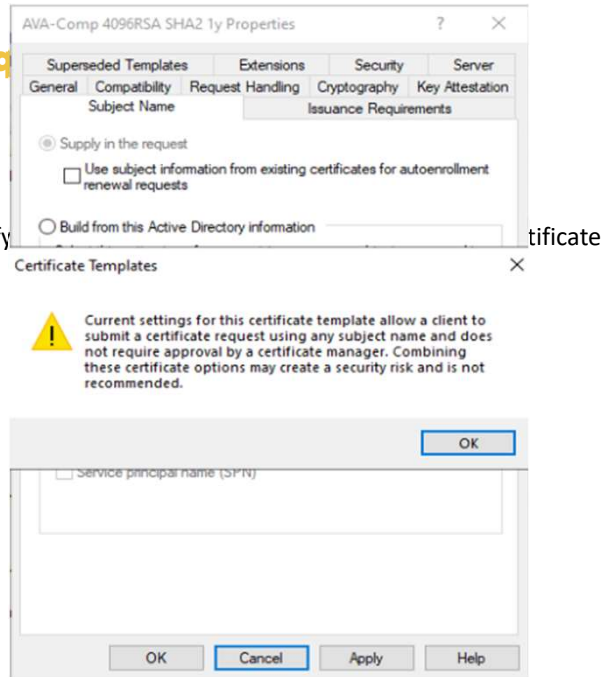
- Subject name or subject alternate name
- Certificate manager is responsible for identifying requester and the content of the issued certificate

Digitale Zertifikate und PKI Webinar

28. Mai / 04. Juni 2024

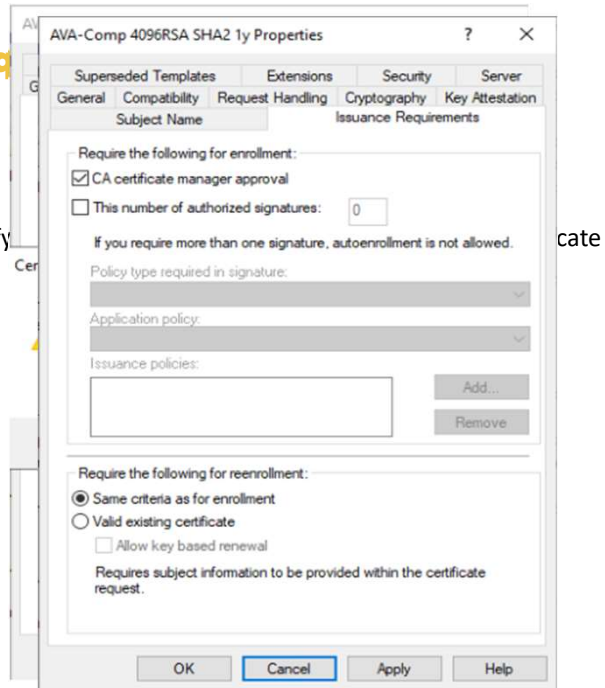
Subject name supply in request

- Subject name or subject alternate name
- Certificate manager is responsible for identifying certificate



Subject name supply in request

- Subject name or subject alternate name
- Certificate manager is responsible for identifying certificate

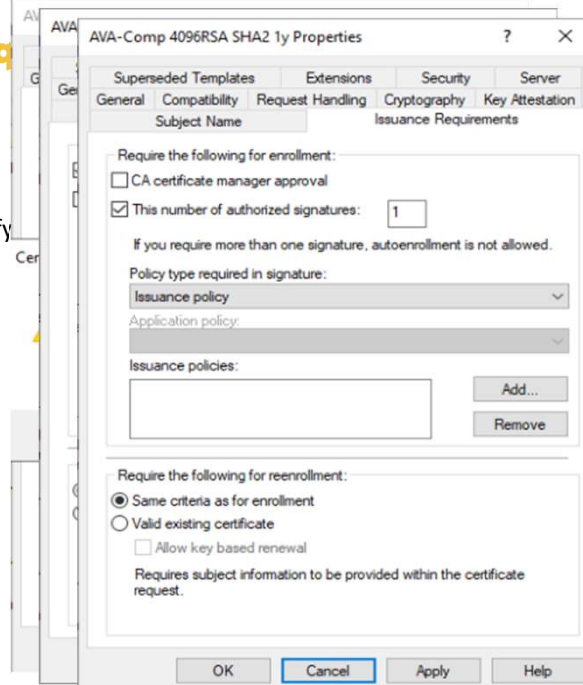


Digitale Zertifikate und PKI Webinar

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

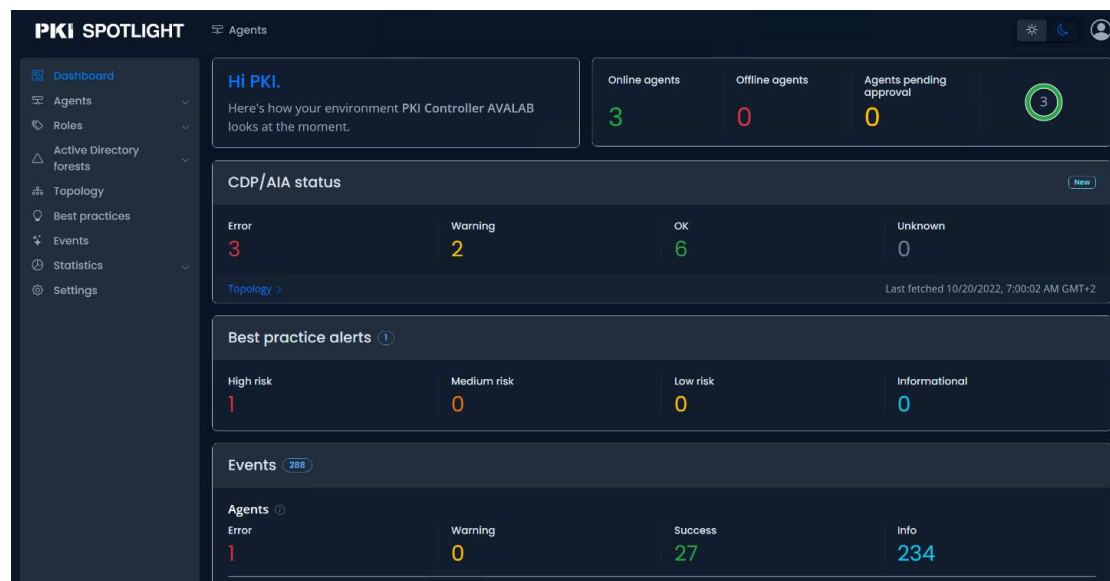
Digitale Zertifikate und PKI Webinar

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



Digitale Zertifikate und PKI Webinar

28. Mai / 04. Juni 2024

Threat

Threats / Detected threats

A template is configured with weak security which could enable a low privilege user to create a fraudulent authentication certificate as any entity in the organization. This has been identified as SpecterOps Certified Pre-Owned ESC1.

Status	Closed
Severity	High risk
Rule	H.1011 (NTDS_SPECTEROPS_OFFLINE_NTAUTH_NO_APPROVAL)
Message	A template is configured with weak security which could enable a low privilege user to create a fraudulent authentication certificate as any entity in the organization. This has been identified as SpecterOps Certified Pre-Owned ESC1.
Forest name	avalab.ch
Forest ID	cc0837ef-0810-4472-a7c0-ac78c2af38e2
Common name	AVA-webserver4096RSASHA2z2y
Detected on	4/23/2024, 10:13:03 AM GMT+2
Detected by	NDES-01.avalab.ch
Closed	4/26/2024, 4:21:46 PM GMT+2 automatically by best practice engine

- Threat has been detected. Detected by agent NDES-01.avalab.ch. 4 weeks ago
- Threat has been closed. Closed automatically by best practice engine. 4 weeks ago

Description
The alerting template has been found to be vulnerability to Security Threat: ESC1 as published in SpecterOps Certified Pre-Owned. This indicates that the template is configured in a way that will enable a low privilege user to potentially request and be issued an authentication certificate that can be used to impersonate any user or computer in the environment. The combination of allowing the subject name to be supplied in the request, application purposes allowed for authentication and with no CA manager approval can cause this issue to occur. The template properties creating this vulnerability are:

- The template is assigned as available to an issuing CA
- The template does not require a CA Manager approval prior to issuance AND
- The template does not require an Enrollment Agent co-signature AND
- The template subject name is set for Supply in Request
- The template Application Policy is Client Authentication, Smartcard Logon, PKINIT Client Authentication (1.3.6.1.5.2.3.4), Any Purpose, or a blank Application Policy

Remediation
On a server with the Certificate Authority role or the Windows Remote Server Administrator Tools (RSAT), run certtmpl.msc and select the alerting template. Select the Subject Name tab and set to Build from this Active Directory information. Alternatively, if Supply in the request is needed, remove any application policies on the Extensions tab that allow client authentication. Click OK to save the template properties.

Security Posture Management

This server is vulnerable to PetitPotam because the Certificate Enrollment Web Service is not configured to Enforce Extended Protection for Authentication in the web.config file and NTLM is enabled.

Status	Active
Severity	High risk
Rule	H.1005 (CES_PETITPOTAM_EPA_POLICY_NOT_ENFORCED)
Message	This server is vulnerable to PetitPotam because the Certificate Enrollment Web Service is not configured to Enforce Extended Protection for Authentication in the web.config file and NTLM is enabled.
Site path	Default Web Site/AVALAB-ISSUING01_CES_UsernamePassword
Detected on	12/22/2023, 7:06:15 PM GMT+1
Detected by	PKI-WEB01.avalab.ch

- Threat has been detected. Detected by agent PKI-WEB01.avalab.ch. 22

Description
This server has been identified as being vulnerable to PetitPotam due to the following condition:

- The Certificate Enrollment Web Service is not configured to Enforce Extended Protection for Authentication in the web.config file.

PetitPotam is a known vulnerability for Microsoft AD CS based PKI servers. PetitPotam is a form of NTLM Relay attack and can enable an adversary to obtain user authentication credentials - which can include escalated and privileged accounts. Adversaries may also be able to obtain authentication credentials both inside and outside of the organization's security perimeter and utilize them to gain inappropriate access to resources. PetitPotam takes advantage of servers where AD CS is not configured with protections for NTLM Relay Attacks. The most effective way to remediate the PetitPotam vulnerability is to disable NTLM in IS or for all Windows processes. If disabling NTLM is not possible, then additional remediation steps are needed. Refer to the PetitPotam AD CS KB article below for details on disabling NTLM. NOTES:

- There may be additional remediation steps necessary if there are other misconfigured items affecting the vulnerability to PetitPotam. Review any other PKI Spotlight Threat Detections to determine which additional items, if any, need to be addressed in addition to this alert.
- If NTLM has been disabled on all your domain controllers, or you have removed NTLM as an authentication provider you may still receive this alert due to detection abilities. If NTLM has been properly disabled in the environment, this alert can be ignored.

ADDITIONAL READING: Refer to [Mitigating NTLM Relay Attacks on AD CS](#) for more information on PetitPotam and AD CS.

If NTLM can not be disabled on the server, configure the web.config file to enforce **Extended Protection for Authentication**. On the alerting server:

- Use File Explorer to navigate to the web.config file for the CES service located in %windir%\systemdata\CES\YOUR_CA_NAME_HERE_CES_Kerberos.
- Use Notepad open the web.config file.
- Locate the <Security mode="Transport"> section.
- Add <extendedProtectionPolicy policyEnforcement="Always" /> to the Transport section such as:

```
<binding name="TransportWithHeaderClientAuth">  
<security mode="Transport">  
<transport clientCredentialType="Windows">  
<extendedProtectionPolicy policyEnforcement="Always" />
```

Digitale Zertifikate und PKI Webinar

28. Mai / 04. Juni 2024

Best Practice Checks & Governance

[Best practices](#) / Best practice alerts

The CA does not appear to be configured to back up any of its configuration or database files.

Status	Active
	<input type="button" value="Suppression"/>
Severity	Medium risk ⓘ
Rule	M.47 (CA_BACKUP_NO_BACKUP)
Message	The CA does not appear to be configured to back up any of its configuration or database files.
Raised on	12/22/2023, 7:02:46 PM GMT+1
Raised by	ISSUING1-AVALAB.avalab.ch

Description	To ensure the CA can be properly restored after a failure, the CA should be backed up on a regular basis. The timing and frequency of the backups will determine how much information may be lost if the CA database is restored. After a recovery, any certificate that was issued after the last backup will remain valid and in use in the environment even though it won't be shown in the CA database, nor will it be revokable. Additionally, the CA is only properly backed up if the Volume Shadow Snapshot service is used to perform a system state backup, or if the CA is directly instructed to back up its data via command line or GUI. The use of 3rd party backup solutions may or may not properly backup the CA service. The use of VM snapshots will also not properly back up the CA database or trigger the commit and clean up for CA database log files. As a result, snapshots should not be used as the primary mechanism of backing up a CA. If a 3rd party backup solution is in place and properly performing backups, this best practice can be safely ignored.
Remediation	Implement a regular backup process that either invokes the Windows Volume Shadow Snapshot service for a system state backup, such as Windows Backup or 3rd party tool. The use of a command line or GUI process that automates the backup is also acceptable. Refer to Backing up ADCS Certificate Authorities (Part 1 of 2) for more details on how the CA database functions and why backups are critical. A sample PowerShell script to perform a backup of the CA can be referenced here: Backing up ADCS Certificate Authorities (Part 2 of 2) .

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/>

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