digitalscepter

The Decryption Blueprint: Building A Two-Tier CA for SSL Inspection

ZACHRY SUM - DIRECTOR OF TECHNICAL SERVICES, DIGITAL SCEPTER JON ROBINSON - PRESIDENT, DIGITAL SCEPTER

November 19th, 2024



- Firewall migrations
- Firewall operations mass upgrades, backups, change/remove/add
- Firewall Healthchecks
- Panorama design
- Zero Trust Network Access
- Network Segmentation

- MFA
- SSL Decryption
- Inbound SSL Inspection
- Remote Access ("Always on")
- Securing Cloud infrastructure
- Dual ISP redundancy
- Network engineering
- Endpoint Security/EDR/MDR



- CMAS
- NASPO
- SPURR
- OMNIA Partners



- Palo Alto Networks
- Crowdstrike
- SentinelOne
- Okta
- Arista
- Juniper
- HPe/Aruba

- AWS
- Microsoft/Azure
- Proofpoint
- Zscaler
- Gigamon
- Rapid7
- Knowbe4
- Netskope

Agenda

- 1. General PKI Overview
- 2. Disclaimer
- 3. Offline Root CA Buildout
- 4. Issuing CA Buildout
- 5. SSL Inspection With Palo Alto

General PKI Overview





Public Key Infrastructure is a system designed to create, manage, distribute, use, store, and revoke digital certificates and public-private key pairs

- **Purpose:** Manages creation, distribution, and revocation of digital certificates and public-private key pairs
- **Role:** Enables secure, trusted communication across digital platforms (websites, emails, networks)
- **Applications:** Widely used in HTTPS, secure email, enterprise access, and code signing



- **Public and Private Keys:** Each user or device within a PKI system has a unique public and private key pair. The public key is openly distributed, while the private key is kept secure. These keys are mathematically linked and work together for secure data exchange.
- **Digital Certificates:** Digital certificates, often issued by trusted Certificate Authorities (CAs), link a public key to an entity's identity. Certificates provide information about the certificate owner, including name, public key, expiration date, and the CA's digital signature, which certifies its authenticity.



Components of PKI (continued)

- **Certificate Authorities (CA):** CAs are trusted entities responsible for issuing and verifying digital certificates. They validate the identity of certificate applicants before issuing certificates.
- **Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP):** CRLs and OCSPs manage and check the status of certificates, indicating whether a certificate is valid, expired, or revoked.

How It Works - According To ChatGPT

• **Me:** Can you diagram how a client and server negotiate an SSL connection?

• ChatGPT:



digitalscepter

How It Really Works

- Different cipher suites and key exchange algorithms will have different steps in establishing an SSL/TLS session
- The process sees the client and server exchanging supported protocol versions, cypher suites, etc.
- During this process a key is securely exchanged to convert to symmetric encryption for transmitting data for the remainder of the session





Disclaimer



When deploying a private CA it's important to understand the risks involved and how to properly secure and maintain your CA

- **1. Key Management Risks:** Compromise of the CA's private key or improper key storage can undermine the entire system.
- 2. Certificate Management Challenges: Mismanagement of certificate issuance, revocation, or expiration can lead to security vulnerabilities and outages.
- **3. Compliance and Policy Risks:** Failure to adhere to standards or enforce strict policies can result in weak security and exploitation.
- **4. Operational Overhead:** High costs, complexity, and reliance on skilled staff make maintaining a secure CA resource-intensive.
- 5. **Insider Threats:** Malicious or careless insiders with access to the CA can misuse it to issue fraudulent certificates.
- 6. **Reputation Risks:** Compromise of the CA undermines trust in the organization's infrastructure and services.



It is recommended to consider risk avoidance through the below options:

- **1.** Use a Trusted Third-Party CA: Outsource certificate issuance and management to established providers to offload operational and compliance burdens.
- 2. Deploy Hardware Security Modules (HSMs): Securely store private keys to prevent compromise.
- **3.** Automate Certificate Management: Use tools to track, issue, renew, and revoke certificates automatically.
- **4. Enforce Strict Access Controls:** Limit and monitor access to CA infrastructure to prevent insider threats.
- 5. **Implement Strong Policies and Audits:** Regularly review and enforce certificate policies and perform security audits.
- 6. Adopt a Hybrid Approach: Use external CAs for public-facing certificates and an internal CA for specific internal needs.



Offline Root CA Buildout



- 1. Your root CA is the linchpin to your PKI's integrity
- 2. If it's compromised, any device that trusted your root CA is at risk, and any service that leveraged certificate authentication should be reviewed for signs of compromise
- 3. With this in mind, here are some considerations for your root CA:
 - a. It should be kept powered off
 - b. Only powered up to renew CA certs or publish new CRL
 - c. It should not be domain-joined
 - d. It should have no network connection
 - e. Ideally, keys would be stored on a Hardware Security Module (HSM)
- 4. Your root CA should only need to issue one certificate, and that is to your Issuing (Intermediate) CA





- 1. Once the deployment platform is determined, proceed with installing a hardened Windows installation
- 2. Create file C:\Windows\CAPolicy.inf:

[Version] Signature="\$Windows NT\$" [Certsrv_Server] RenewalKeyLength = 4096 RenewalValidityPeriod = Years RenewalValidityPeriodUnits = 10 AlternateSignatureAlgorithm = 0 CRLPeriod = Years CRLPeriodUnits = 10 CRLDeltaPeriod = Days CRLDeltaPeriodUnits = 0

3. In **Server Manager**, install the **Active Directory Certificate Services** Role on the server, selecting only the **Certification Authority** role service during installation



1. Once installation completes, proceed with configuring the Certification Authority role using the settings below:

Setting	Value
Specify credentials to configure role services	A user that is a local administrator
Specify the setup type of the CA	Standalone CA
Specify the type of the CA	Root CA
Specify the type of the private key	Create a new private key
Specify the cryptographic Options	RSA#Microsoft Software Key Storage Provider, 4096, SHA256
Specify the name of the CA	Populate common name of your choice, leave other fields
Specify the Validity Period	<=10 years (think golf, lower is betterand more difficult)



AD CS Configuration			-		×
ole Services			DESTINA	ION SER	WER ki01
Credentials Role Services Confirmation Progress Results	Select Role Services	to configure b Enrollment nt Service b Service cy Web Service			
	More about AD CS Server Rol	es			

digitalscepter



digitalscepter





R

AD CS Configuration	- 🗆 X
Credentials Role Services Setup Type CA Type	DESTINATION SERVER labwpki01 Specify the type of the private key To generate and issue certificates to clients, a certification authority (CA) must have a private key.
Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	 Use this option if you do not have a private key or want to create a new private key. Use existing private key Use this option to ensure continuity with previously issued certificates when reinstalling a CA. Select a certificate and use its associated private key Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key. Select an existing private key on this computer Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.
	More about Private Key



ryptography fo	or CA		DESTINA	labwp	ki01
Credentials Role Services Setup Type CA Type	Specify the cryptographic options Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider	v	Key length:		v
Private Key	Select the hash algorithm for signing certificates issued b	y this CA:			
Cryptography	SHA256	^			
CA Name	SHA384				
Validity Period	SHA512				
Certificate Database	MD5	~			
Confirmation	Allow administrator interaction when the private key i	s accessed i	by the CA		
		5 decesses i	by the Crit		
	More about Cryptography				



AD CS Configuration		-		×
CA Name		DESTINAT	ION SER	VER ki01
Credentials Role Services	Specify the name of the CA			
Setup Type CA Type Private Key	Type a common name to identify this certification authority (CA). This n certificates issued by the CA. Distinguished name suffix values are autor be modified. Common name for this CA:	ame is added t natically gener	o all ated but	can
Cryptography CA Name Validity Period	Digital Scepter Lab Root CA Distinguished name suffix:			
Certificate Database Confirmation	Preview of distinguished name:			
	CN=Digital Scepter Lab Root CA			
	More about CA Name			
	< Previous Next	Configure	Cance	4



AD CS Configuration					-		×
/alidity Period					DESTINAT	TION SER	VER aki01
Credentials Role Services Setup Type	Spec	ify the validity	y period	enerated for this cert	tification authority (C	A):	
CA Type	10	Years	*				
Private Key Cryptography CA Name	CA exp The val certific	iration Date: 11/17/ lidity period configu ates it will issue.	2034 12:26:00 AM	I rtificate should excee	d the validity period	for the	
Validity Period							
Certificate Database							
Confirmation							



- 1. Open Local Security Policy and navigate to Local Policies > Audit Policy
- 2. Open Audit object access and check Success and Failure





1. Open an **Administrative Command Prompt** and enter the following commands, modifying the distinguished name for your domain Configuration partition

certutil.exe -setreg CA\DSConfigDN "CN=Configuration,DC=your,DC=domain,DC=com" certutil.exe -setreg CA\ValidityPeriodUnits 5 certutil.exe -setreg CA\ValidityPeriod "Years" certutil.exe -setreg CA\CRLPeriodUnits 52 certutil.exe -setreg CA\CRLPeriod "Weeks" certutil.exe -setreg CA\CRLOverlapPeriodUnits 12 certutil.exe -setreg CA\CRLOverlapPeriod "Hours" certutil.exe -setreg CA\CRLDeltaPeriodUnits 0 certutil.exe -setreg CA\CRLDeltaPeriodUnits 12 net stop certsvc net start certsvc



- 1. Open Certification Authority right click your CA and select Properties
- 2. Click **Extensions**
- 3. Select the **file://...** location and click **Remove**
- 4. Click **Add** and enter path found in chart below
- 5. Check box Include in CRLs... and Include in the CDP extension...
- 6. Click **Select Extension** dropdown and select **Authority Information Access**
- 7. Select the **file://...** location and click **Remove**
- 8. Click **Add** and enter path found in chart below
- 9. Check box Include in the AIA extension...
- 10. Make sure to update italicized values with your own

Setting	Value
CDP Extension Location	http://pki.your.domain.com/CertData/ <caname><crlnamesuffix><deltacrlallowed>.crl</deltacrlallowed></crlnamesuffix></caname>
AIA Extension Location	http://pki.your.domain.com/CertData/ <serverdnsname>_<caname><certificatename>.crt</certificatename></caname></serverdnsname>



Certification Authority System		Certification Authority
Manage user certificates	>	System
 Credential Manager Manage computer certificates Manage file encryption certificates 	>	 Open Run as administrator Run as different user Open file location Pin to Start Pin to taskbar



General Policy Module Exit Module Extensions Storage Certificate Managers elect extension:	nrollment Agents	Auditing	Recove	ry Agents	Sec	curity
Extensions Storage Certificate Managers elect extension: ::RL Distribution Point (CDP) secfy locations from which users can obtain a certificate revocation list RL). ::WINDOWS\system32\Cert Srv\Cert Enroll\ <caname><crlnamesuffic>CN=CerterShvlCv2. ::WINDOWS\system32\Cert Srv\Cert Enroll<<caname><crlnamesuffic>CN=CerterShvlCv2. ::WINDOWS\system32\Cert Srv\Cert Enroll<<caname><crlnamesuffic>CN=CerterShvlCv2. ::WINDOWS\system32\Cert Enroll<<caname><crlnamesuffic>CN=ServerShvlDisName><certenroll< caname=""><crlnamesuffic>CN=ServerShvlDisName><certenroll< td=""> ::WINDOWS\system32\Cert Enroll<<caname><crlnamesuffic>CN=ServerShvlDisName><certenroll< td=""> ::WINDOWS\system32\Cert Enroll :Caname><crlnamesuffic>CN=ServerShvlDisName><certenroll< td=""> ::WINDOWS\system32\Cert Enroll :Caname><certenroll< td=""> :WINDOWS\system32\Cert Enroll :Caname><certenroll< td=""> :WINDOWS\system32\Cert Enroll :Caname><certenroll< td=""> :WINDOWS\system32\Cert Enroll :Caname><certenroll< td=""> :WINDOWS\system32\Cert Enroll :Caname><certenroll< td=""> :WINDOWS\sy</certenroll<></certenroll<></certenroll<></certenroll<></certenroll<></certenroll<></certenroll<></certenroll<></certenroll<></certenroll<></crlnamesuffic></certenroll<></crlnamesuffic></caname></certenroll<></crlnamesuffic></certenroll<></crlnamesuffic></caname></crlnamesuffic></caname></crlnamesuffic></caname></crlnamesuffic></caname>	General	Policy M	odule	Đ	t Module	
elect extension: IRL Distribution Point (CDP) peofy locations from which users can obtain a certificate revocation list RL). INVINDOWS'system32:/CertSrv\/CertEnroll. <caname><crlnamesuf lap:///CN=<catruncatedname><crlnamesuffic>.CN=CSrverShortl Int//CServerDNSName><certenroll.<caname><crlnamesuffic>.CN= Add Rempe Add Rempe Publish CRLs to this location Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually. Include in CRLs. Clients use this to find Deta CRL locations. Include in CRLs to this location Include in the CDP extension of issued certificates Publish Deta CRLs to this location</crlnamesuffic></certenroll.<caname></crlnamesuffic></catruncatedname></crlnamesuf </caname>	Extensions	Storage		Certificate	Manager	rs
IRL Distribution Point (CDP) Decify locations from which users can obtain a certificate revocation list RL). INUNDOWS'system32'Cert Srv \Cert Enroll. <cename><crlnamesuffice.cn=<crlnamesuffice.cn=<crlnamesuffice.cn=<cerlname><crlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<ce< td=""><td>elect extension:</td><td></td><td></td><td></td><td></td><td></td></crlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<cerlnamesuffice.cn=<ce<></crlnamesuffice.cn=<crlnamesuffice.cn=<crlnamesuffice.cn=<cerlname></cename>	elect extension:					
Publish CRLs to this location Publish CRLs. Clients use this to find Deta CRL locations Include in CRLs. Clients use this to find Deta CRL locations. Include in the CDP extension of issued certificates Publish Deta CRLs to this location	RL Distribution Point	(CDP)				V
Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually. Include in CRLs. Clents use this to find Deta CRL locations. Include in the CDP extension of issued certificates Publish Deta CRLs to this location	RL), \\WINDOWS\aysten lap:///CN= <catrunc ttp://<serverdnsna o///<serverdnsnan< td=""><td>n 32\CertSrv\C atedName><c me>/CertEnrol te>/CertEnrol</c </td><td>ertEnroll\<ca RLNameSul /<caname></caname></ca </td><td>Name><ci fix>.CN=<s <crlname< td=""><td>RLName: ServerSho e Suffix><</td><td>Suffix: ortNar Delta</td></crlname<></s </ci </td></serverdnsnan<></serverdnsna </catrunc 	n 32\CertSrv\C atedName> <c me>/CertEnrol te>/CertEnrol</c 	ertEnroll\ <ca RLNameSul /<caname></caname></ca 	Name> <ci fix>.CN=<s <crlname< td=""><td>RLName: ServerSho e Suffix><</td><td>Suffix: ortNar Delta</td></crlname<></s </ci 	RLName: ServerSho e Suffix><	Suffix: ortNar Delta
when publishing manually. Include in CRLs. Clients use this to find Deta CRL locations. Include in the CDP extension of issued certificates Publish Deta CRLs to this location	Publish CRLs to this		Ac	ld	Reme	ye s
Include in CRLs. Clients use this to find Deta CRL locations. Include in the CDP extension of issued certificates) Publish Deta CRLs to this location	Publish CRLs to this	location	Ac	id	Reme	ye a
holude in the CDP extension of issued certificates) Publish Delta CRLs to this location	Publish CRLs to this Include in all CRLs, when publishing ma	location Specifies when mully.	Action Publish	id	Rem P	ye Sny
Publish Delta CRLs to this location) Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cli	location Specifies when nually. ents use this to	Ad re to publish	id	Reme re Directo	ye a ory
	Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Ok Include in the CDP	location Specifies when nually. ents use this to extension of iss	Ad the to publish find Deta C sued certifica	id (in the Activ RL location stes	Rempo	ye any
) Include in the IDP extension of issued CRLs	Publish CRLs to this Include in all CRLs, when publishing ma Include in CRLs, CR Include in the CDP Publish Delta CRLs	location Specifies when mually. ents use this to extension of iss to this location	Ac re to publish find Deta C sued certifica	id (in the Activ IRL location ites	Reme re Directo	ye any





Enrollment Agents	Auditing	Reco	very Agents	Sec	urity
General	Policy M	lodule	E	xt Module	1
Extensions	Storage		Certificate	Manager	5
elect extension:					
Authority Information	Access (AIA)				v
C:\WINDOWS\ayste Idap:///CN= <catrun http://<serverdnsn< td=""><td>m32\CertSrv\C catedName>,C ame>/CertEnro</td><td>ertEnroll\< N=AIA,CN I/<server1< td=""><td>ServerDNSN =Public Key DNSName></td><td>lame>_<c Services.(<caname< td=""><td>aNa N=S</td></caname<></c </td></server1<></td></serverdnsn<></catrun 	m32\CertSrv\C catedName>,C ame>/CertEnro	ertEnroll\< N=AIA,CN I/ <server1< td=""><td>ServerDNSN =Public Key DNSName></td><td>lame>_<c Services.(<caname< td=""><td>aNa N=S</td></caname<></c </td></server1<>	ServerDNSN =Public Key DNSName>	lame>_ <c Services.(<caname< td=""><td>aNa N=S</td></caname<></c 	aNa N=S
tie // «ServerDINSINa	me>/CertEnroll	/ <serverd< td=""><td>NSName>_<</td><td>CaName></td><td>Cer</td></serverd<>	NSName>_<	CaName>	Cer
ile // <serverdinsna< td=""><td>me>/CetEnroll</td><td>/«ServerD</td><td>NSName>_<</td><td>Region</td><td><car Car</car </td></serverdinsna<>	me>/CetEnroll	/«ServerD	NSName>_<	Region	<car Car</car
Include in the AIA (extension of iss	ued certific	Add	Repor	re



digitalscepter

 Open Certification Authority and expand your CA, right-click Revoked Certificates and click All Tasks > Publish. Select New CRL and click OK

2 🖻 🙆				
Certification Autho	rity (Local) ab Root CA	Request ID	Revocation Date	Effective Revocation Da
Ssued Ce	All Tasks	>	Publisk	
Pending I Failed Rei	View	>	45	
	Refresh Export List			
	Properties			
	Help			





1. We should now have two files in

C:\Windows\System32\CertSrv\CertEnroll

- a. One certificate (the root CA certificate which contains the public key only)
- b. One CRL that we published in the prior step
- 2. These need to be copied to the CertData folder on the Issuing CA
- 3. But wait, you don't have a network connection
- 4. Whether virtualized or physical, USB device is generally your best bet
- 5. For virtual, an existing hard disk is an option
- 6. Can do virtual floppy too depending on hypervisor





Build Root CA (finished?)

- 1. You're DONE!
- 2. Ok, with the root only
- 3. So you're half done!
- 4. Well, a little less than half actually, there's this thing-nevermind, we'll get to it

Issuing CA Buildout



©2022 Digital Scepter. All rights reserved. digitalscepter.com

- 1. Your issuing CA will be domain-joined
- 2. This will simplify cert deployment, renewal, etc.
- 3. Permissions on cert templates are paramount
 - a. If these are too lax, certificates can be provisioned and misused, exposing the organization to significant risk
- 4. CDP, AIA and OCSP provide end users certificate revocation information as well as your CA certificates when they weren't provided as part of the server chain. This is primarily pulled via http/https.
- 5. If users outside of your network will need to access services using internal certificates, then you will likely need to make these services available from outside your network
- 6. In this case a separate server on a DMZ network would be ideal for hosting these files
- 7. If it is purely internal, it is not uncommon to keep this local to the issuing CA
- 8. For purpose of this buildout, we will consolidate these functions to the issuing CA


Prepare Issuing CA

1. In **Server Manager**, install the **Web Server (IIS)** role on the server, leaving all defaults selected





Prepare Issuing CA (continued)

- Open IIS Manager and expand your server > Sites, and right-click Default Web Site then click Add Virtual Directory
 - a. Alias: CertData
 - b. Physical Path: C:\CertData
- 2. Click **CertData** virtual directory and double-click **Directory Browsing**. Click **Enable** in the Actions column
- 3. Enable Double Escaping on Default Web Site (required to host delta CRL's)

C:\Windows\System32> cd %windir%\system32\inetsrv C:\Windows\System32\inetsrv> Appcmd set config "Default Web Site" /section:system.webServer/Security/requestFiltering -allowDoubleEscaping:True C:\Windows\System32\inetsrv> iisreset





1. Create file **C:\Windows\CAPolicy.inf**, replacing italicized values below:

[Version] Signature = "\$Windows NT\$" [PolicyStatementExtension] Policies = AllIssuancePolicy,InternalPolicy [AllIssuancePolicy] OID = 2.5.29.32.0 [InternalPolicy] OID = 1.2.3.4.1455.67.89.5 Notice = "Digital Scepter Lab Certification Authority and any issued certificates are for internal usage only." URL = http://pki.lab.digitalscepter.com/cps.html [Certsrv_Server] RenewalKeyLength = 4096 RenewalValidityPeriod = Years PonowalValidityPeriod = Years
RenewalValidityPeriod = Years
RenewalValidityPeriodUnits = 5 AlternateSignatureAlgorithm = 0
LoadDefaultTemplates = 1

2. Install **Active Directory Certificate Services** Role on the server, selecting the **Certification Authority** and **Certificate Authority Web Enrollment** role services during installation



1. Once installation completes, proceed with configuring the **Certification Authority** and **Certification Authority Web Enrollment** roles using the settings below:

Setting	Value
Specify credentials to configure role services	A user that is both a local administrator and member of Enterprise Admins
Specify the setup type of the CA	Enterprise CA
Specify the type of the CA	Subordinate CA
Specify the type of the private key	Create a new private key
Specify the cryptographic Options	RSA#Microsoft Software Key Storage Provider, 4096, SHA256
Specify the name of the CA	Populate common name of your choice, leave other fields
Request a certificate from parent CA	Save a certificate request to file on the target machine



AD CS Configuration		-		×
ole Services		DESTINA Iabwpki02.lab.digit	TION SER	com
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Select Role Services to configure Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service			
	More about AD CS Server Roles			

digitalscepter

AD CS Configuration	- D X
Setup Type	DESTINATION SERVER labwpki02.lab.digitalscepter.com
Credentials	Specify the setup type of the CA
Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	 Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates. Interprise CA Enterprise CA Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies. Standalone CA Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).
	More about Setup Type







R

AD CS Configuration	- 🗆 X
Private Key	DESTINATION SERVER labwpki02.lab.digitalscepter.com
Credentials Role Services Setup Type CA Type	To generate and issue certificates to clients, a certification authority (CA) must have a private key.
Private Key Cryptography CA Name Certificate Request Certificate Database Confirmation Progress Results	Use this option if you do not have a private key or want to create a new private key. Use existing private key Use this option to ensure continuity with previously issued certificates when reinstalling a CA. Select a certificate and use its associated private key Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key. Select an existing private key on this computer Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.
	More about Private Key

digitalscepter

ryptography fo	rCA	laby	wpki02.lab.digita	lscepter.co
Credentials Role Services Setup Type	Specify the cryptographic options Select a cryptographic provider:		Key length:	
CA Type	RSA#Microsoft Software Key Storage Provider	~	4096	
Private Key	Select the hash algorithm for signing certificates issued to	y this CA:		
Cryptography	SHA256	^		
CA Name	SHA384			
Certificate Request	SHA512			
Certificate Database	SHA1			
Confirmation	LMD5	*		
	Allow administrator interaction when the private key	is accessed b	by the CA.	



DESTINA Iebwpki02.leb.digit of the CA identify this certification authority (CA). This name is added CA. Distinguished name suffix values are automatically gene A:	ation SERVER talscepter.com
e of the CA identify this certification authority (CA). This name is added CA. Distinguished name suffix values are automatically gene A:	i to all erated but can
identify this certification authority (CA). This name is added CA. Distinguished name suffix values are automatically gene A:	l to all erated but can
- cal	
ig CA	
c	
er,DC=com	
name:	
ssuing CA,DC=lab,DC=digitalscepter,DC=cc	
	xc er,DC=com name: Issuing CA,DC=lab,DC=digitalscepter,DC=cc



R

-	
DESTINATIO est labwpki02.lab.digitalso	ON SERVER
Request a certificate from parent CA You require a certificate from a parent certification authority (CA) to allow this subordinal issue certificates. You can request a certificate from an online CA or you can store your ma a file to submit to the parent CA. Send a certificate request to a parent CA: Select Computer name Computer name	te CA to equest to
Parent CA: Save a certificate request to file on the target machine:	sct_
File name: C:\labwpki02.lab.digitalscepter.com_lab-LABWPKJ02-CA.req You must manually get a certificate back from the parent CA to make this CA oper	rational.
	DESTINATION Laborphi02.lab.digitalscepter.com_lab-LABWPK02-CA.req Source a certificate request to file on the target machine: File name: CMabwpki02.lab.digitalscepter.com_lab-LABWPK02-CA.req Source a certificate back from the parent CA to make this CA ope



 Navigate to C:\CertData and double-click the CA certificate file that was copied here earlier. Click Install Certificate

	certifica	te Infor	mation					
Th in: Au	is CA Root ce stall this cert ithorities sto	ertificat ficate i re.	e is not n the Tr	trusted. usted R	To er oot Ce	able tri ertificat	ust, ion	
-	Issued to:	Digital S	Scepter L	ab Root (CA			2
	Issued by:	Digital S	Scepter L	ab Root (CA			
	Valid from	11/17/3	2024 to	11/17/2	034			
-			Instal	Certifical	te]	Issuer 1	Statement	



1. Click Local Machine and then Next

Jertificate Import Wizard	×
Welcome to the Certificate Import Wizard	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
Store Location	
Current User Local Machine	
To continue, dick Next.	
Cancel	



 Click Place all certificates in the following store then Browse and select Trusted Root Certification Authorities

Certificate Store Certificate stores	are system areas whe	re certificates are ke	pt.
Windows can auto the certificate.	omatically select a cert	ificate store, or you	can specify a location fo
O Automatical	ly select the certificat	e store based on the	type of certificate
O Place all cer	tificates in the following	ng store	
Certificate	store:		
Trusted R	oot Certification Auth	orities	Browse



- 1. Copy the certificate request created earlier to the root CA...
- 2. I'm sorry, it's this again, get your virtual 5 ¼" floppy ready to move some files back and forth
- 3. Once you have it on the root, you can open the **Certification Authority** console and right-click your CA name, then click **All Tasks** > **Submit New Request...**
- 4. Browse to your cert request and click **OK.**
- 5. Select **Pending Requests** then right-click the single request in the window and click **All Tasks > Issue**
- 6. Select **Issued Certificates** and double-click the only issued certificate. Go to **Details** tab and click **Copy to File...**
- 7. Select **P7B** format and choose a location to save this. I'd recommend your virtual floppy drive, because guess what. This is going back to your Issuing CA



- With your signed certificate back on the issuing CA, we want to open **Certification** Authority and right-click your CA name, then click All Tasks > Install CA Certificate
- Select the certificate you copied over from the root CA and click **Open**. The cert will be installed and you should now be able to right-click your CA name, click **All Tasks** > **Start Service**

- 1. Open Local Security Policy and navigate to Local Policies > Audit Policy
- 2. Open Audit object access and check Success and Failure





 Open an Administrative Command Prompt and enter the following commands. These will allow your CA to issue certificates with expiration dates up to 3 years out.

certutil.exe -setreg CA\ValidityPeriodUnits 3 certutil.exe -setreg CA\ValidityPeriod "Years" certutil.exe -setreg CA\AuditFilter 127 net stop certsvc net start certsvc

- 1. Open Certification Authority right click your CA and select Properties
- 2. Click **Extensions**
- 3. Click **Add** and enter path found in chart below
- 4. Check box Include in CRLs... and Include in the CDP extension...
- 5. Click Select Extension dropdown and select Authority Information Access
- 6. Click **Add** and enter path found in chart below
- 7. Check box **Include in the AIA extension...**
- 8. Make sure to update italicized values with your own

Setting	Value
CDP Extension Location	http://pki.yourdomain.com/CertEnroll/ <caname><crlnamesuffix><deltacrlallowed>.crl</deltacrlallowed></crlnamesuffix></caname>
AIA Extension Location	http://pki.yourdomain.com/CertEnroll/ <serverdnsname>_<caname><certificatename>.crt</certificatename></caname></serverdnsname>

digitalscepter

- Open IIS Manager and expand your server > Sites, Default Web Site and click CertEnroll
- 2. Double-click **Directory Browsing** and click **Enable** in the Actions column
- 3. We did this earlier with the CertData virtual directory, so this likely feels familiar

 Open Certification Authority and expand your CA, right-click Revoked Certificates and click All Tasks > Publish. Select New CRL and click OK

 	🔋 🗟 🗟 🛐			
Gertificatio ✓ ♂ Digital	on Authority (Local) Scepter Lab Issuing	CA Request II	D Revocation Date	Effective Revocation
	Jec All Tasks	>	Publish	
🧮 Per 🚞 Fai	ndi lec View	>		
🦰 Ce	tif Refresh Export List			
	Properties			
	Help			





- 1. We need to create a certificate for pki.lab.digitalscepter.com so we can enable https on our Certificate Authority Web Enrollment website
- 2. Run **certlm.msc** to open your Local Machine certificate store.
- 3. Right-click **Personal** and click **All Tasks > Advanced Operations > Create Custom Request**
- 4. Under Template select **Web Server** then click **Details** and **Properties** when under the Active Directory Enrollment Policy page
- 5. Populate your **Common Name** and **Alternative Name** and click **OK**



1. Populate your **Common Name** and **Alternative Name** and click **OK**

Subject	General	Extensions	Private Kev	
The subject can enter in can be used	of a certi formatio I in a certi	ficate is the n about the t ificate.	user or computer to types of subject na	o which the certificate is issued. You me and alternative name values that
Subject of c	ertificate			
The user or	compute	r that is rece	iving the certificate	
Subject nan Type:	ne:			CN=pki.lab.digitalscepter.com
Common	name	~	Add >	
Value:			< Remove	
Alternative	name:			
Туре:				DNS pki lab digitalscepter.com
DNS		~		
Value:			Add >	
			< Remove	



Choose a filename and save in Base 64 format

		3 — 3		×
1	Certificate Enrollment			
	Where do you want to save the offline request?			
	If you want to save a copy of your certificate request or want to process the request to your hard disk or removable media. Enter the location and name of your certifica click Finish.	later, save te request	the reque , and then	est I
	File Name: C:\pki.req	E	Browse	
	File format: Base 64 Binary			
		Finish	Can	cel



1. Open an **Administrative Command Prompt** and enter the following command:

certreq -attrib "CertificateTemplate:WebServer" -submit C:\pki.req

- 2. When prompted save the resulting certificate. It can go in the same location as the CSR, but specify the extension of .cer so in this case, it would be pki.cer
- 3. Run the below command to import the certificate, automatically pairing it with the private key created with the CSR:

certreq -accept pki.cer



- Open IIS Manager and right-click Default Web Site and click Edit Bindings
- 2. Click **Add**
- 3. Type: https
- 4. SSL Certificate: *pki.lab.digitalscepter.com*
- 5. Click **OK**, then **Close**,

Туре:	IP address	8		Port:		
https 🚿	All Unass	igned	~	443		
Host name:						
Require Server Na	ame Indicatio	on				
Disable TLS 1.3 o	ver TCP	Disable QUIC				
Disable Legacy T	LS	Disable HTTP/2				
Disable OCSP Sta	pling	Negotiate Client	t Certif	icate		
SSL certificate:						
	r.com	~	Se	elect	View	
pki.lab.digitalscepte						



 Still within the CertSrv virtual directory, double-click Authentication and Disable all options except Windows Authentication which should be enabled.

File View Help			
Connections 🔍 🕶 🔝 1 💋 1 😥 🖓 Start Page	Group by: No Grouping		
 LABWPKI02 (LAB\zsum) Application Pools Sites Sites CertData CertEnroll CertSrv 	Name Anonymous Authentication ASP.NET Impersonation Digest Authentication Windows Authentication	Status Disabled Disabled Disabled Enabled	Response Type HTTP 401 Challenge HTTP 401 Challenge



Build Issuing CA (done!)

1. It has to be lunch time by now



SSL Inspection With Palo Alto



SSL Decryption Punch List

- 1. The Palo Alto Networks firewalls need to be issued a subordinate CA certificate from your newly created Issuing CA
- 2. Microsoft has a Subordinate Certification Authority template we can use
 - a. Generally, I recommend cloning the default MS templates so you can tweak them as needed for your organization, e.g. changing the validity period.
- 3. Punch list should look like this:
 - a. Generate a CSR on the PAN firewalls
 - b. Use the web enrollment site to have cert issued via request file
 - c. Import signed certificate to PAN firewalls
 - d. Apply Forward Trust Certificate role to decrypt certificate
 - e. Generate a self-signed CA on the PAN firewalls and assign it the **Forward Untrust Certificate** role
 - f. Create **Decryption** policies

digitalscepter	DASH	BOARD ACC	C MONITOR F	C Device Groups C POLICIES OBJECTS	N	ETW	– Templates – VORK DI	VIC	3	P/
Panorama 🗸	Ten	nplate labfw01	~	View by Device			ŝ	~	Mo	ode
Setup • Availability Log Forwarding Card	De	evice Certificates	Default Trusted Cer	tificate Authorities			4 iter	ns)	\rightarrow	<
Password Profiles		NAME	SUBJECT	ISSUER	СА	к	EXPIRES	S	A	U.
Authentication Profile		💭 github	CN = github.int.digitals	issuer=DC = com, DC = di		/	Mar 29 05:	e	R	
User Identification		💭 wildcard.int	CN = *.int.digitalscepte	R10			Jan 1 02:11	v	R	
√ 🔏 IoT Security		crt.saml_azu	CN = Microsoft Azure F	CN = Microsoft Azure Fed			Jul 7 23:00:	e	R	
 DHCP Server Log Inges Data Redistribution VM Information Sources 		🗐 gp.digitalscepto	er.com gp.digitalscepter	Eó			Dec 20 18:	v	E	
Certificate Management										
Sectificate Profile •										
SSL/TLS Service Profile	Θ	Delete Revoke	Renew 🛓 Import 튏	Generate 🔓 Export Ce	rtifica	ate	PDF/CSV			
zsum Logout Last Login Time: 11	1/17/2	2024 01:24:47 Si	ession Expire Time: 12/17	//2024 15:01:28 §∃ T	asks	l La	anguage 🥠	pal	oalt	0



Certificate Type	Local O SCEI	P	
Certificate Name	decrypt_lab		Panorama
	Shared		Setup
Common Name	decrypt.lab.digitalscepter.com		
1	or FQDN to appear on the certificat	te	High Availability
Signed By	External Authority (CSR)	~	Log Forwarding Card
[Certificate Authority		Password Profiles
[Block Private Key Export		Administrators
OCSP Responder	are .	~	Admin Roles
Algorithm	RSA		Authentication Profile
Number of Bits	2048		Authentication Seque
Digest	sha256		I liser Identification
Expiration (days)	365		V al IoT Security
Certificate Attributes -			P DHCP Server Low
Түре	VALUE		Data Redistribution
			WM Information Sour
			🗸 🧊 Certificate Managem
			Certificates
+ Add - Delete			Certificate Profile
			OCSP Responder
			A SSI /TI S Service
			C SSL/TES SCIVICE

Ten	nplate labfw01	~	View by Device			~
De	evice Certificates	Default Trusted Certifica	ate Authorities			
Q (
	NAME	SUBJECT	ISSUER	СА	к	EXPIRE
	🗊 github	CN = github.int.digitalsce	issuer=DC = com, DC = digit		2	Mar 29
	💭 wildcard.int.digi	CN = *.int.digitalscepter.c	R10			Jan 1 02
. 🗆	🗊 crt.saml_azure	CN = Microsoft Azure Fe	CN = Microsoft Azure Feder			Jul 7 23
	🗊 gp.digitalscepte	CN = gp.digitalscepter.com	E6			Dec 20
	Jecrypt_lab	decrypt.lab.digitalscepter				
		Template labfw01 Device Certificates NAME Image:	Template labfw01 Device Certificates Default Trusted Certification Q	Template labfw01 ✓ View by Device Device Certificates Default Trusted Certificate Authorities Q ISSUER NAME SUBJECT ISSUER Image: Signature of the structure o	Template labfw01 View by Device Device Certificates Default Trusted Certificate Authorities Image: Subject in the image: Subjec	Template labfw01 View by Device Device Certificates Default Trusted Certificate Authorities Image: Subject in the image: Subject intervention of the image: Subject interven

digitalscepter

File Action View	Help			
Certification Auth Certification Auth Revoked Certification Issued Certification Pending R Failed Rec	nority (Local) r Lab Issuing CA Certificates tificates equests uests	Name Direc Dom Kerb EFS F Basic	ctory Email Replication ain Controller Authentication eros Authentication Recovery Agent - FFS	In D C Fi
Certifici	Manage	Cast Dasa	n Controller	C
	New	>	erver uter	Se
	View	>		E
	Refresh Export List		Jinate Certification Authority listrator	N
	Help			





G.

Sup	erseded To	emplates		Exte	ensions		Security
Com	patibility		General		Issua	nce Re	quirements
emplat	e display r	ame:					
PANSu	bСА						
[emplat PANSu	e name: IbCA						
/alidity	period:		B	enewa	l period:		
2	years	~		c			
			-	0	weeks	~	
] <u>P</u> ubl	ish certific Do not auto Directory	ate in Act	- ive Directo reenroll if	ory a dupli	cate certif	icate e	kists in Active

• 🔿 🖄 🙆 🖄				
 Certification Authority (Local Digital Scepter Lab Issuing Revoked Certificates Issued Certificates Pending Requests Failed Requests 	CA CA CA CA CA CA CA CA CA CA CA CA CA C	Name Directory Em Domain Con Kerberos Aut EFS Recovery Basic EFS	ail Replication troller Authentication thentication Agent	Intended Purpose Directory Service Email Replication Client Authentication, Server Authen Client Authentication, Server Authen File Recovery Encrypting File System
Centificate Tem	Manag New	e >	roller Certificate Template	Client Authentication, Server Authen
	View	>	Certification Authority	Encrypting File System, Secure Email
Ref Exp	Refresh Export I	List		Microsoft Trust List Signing, Encrypti
	Help			

digitalscepter

Enable Certificate Templates

Select one Certificate Template to enable on this Certification Authority. Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers. All of the certificate templates in the organization may not be available to your CA. For more information, see Certificate Template Concepts.

Name	Intended Purpose
Recovery Agent	Key Recovery Agent
Response Signing	OCSP Signing
R PANSubCA	<al></al>
RAS and IAS Server	Client Authentication, Server Authentication
🚇 Router (Offline request)	Client Authentication
🖳 Smartcard Logon	Client Authentication, Smart Card Logon
🖳 Smartcard User	Secure Email, Client Authentication, Smart Card Logon
🚇 Trust List Signing	Microsoft Trust List Signing
🚇 User Signature Only	Secure Email, Client Authentication
Workstation Authentication	Client Authentication

Cancel

OK





Microsoft Active Directory Certificate Services - Digital Scepter Lab Issuing CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC c server) in the Saved Request box.

Saved Request:

ggKt0lAP2+qKJr/iP2sproEAYKcmap q297/vhgaz161xbio69r/MAvHZyb9c sRI= END CERTIFICATE REQUEST	boYnvRJQFoPI + bbCK90HZVhet
	· //
ate:	
PANSubCA 🗸	•
ites:	
	Submit >
	ggKt0lAP2+qKJr/iP2sproEAYKcmap q297/vhgaz161xbio69r/MAvHZyb9c sRI= END CERTIFICATE REQUEST 4 ate: PANSubCA

digitalscepter

Microsoft Active Directory Certificate Services - Digital Scepter Lab Issuing CA

Request a Certificate

Select the certificate type:

User Certificate

Or, submit an advanced certificate request.




digitalscepter

Certificate Type	O Local	⊖ SCEP	◯ Cloud	
Certificate Name	decrypt_lab			
File Format	Base64 Encoded	Certificate (PEM)		~
Certificate File	C:\fakepath\cert	new.cer		Browse.
Key File	Block Private I	Key Export		Browse.
Key File				Browse.
Passphrase				
Confirm Passphrase				
	Charad			

dıgıtalscepter	DASHBOARD	ACC MONITOR	C Device Groups POLICIES OBJECTS	C Templates	PANOI
anorama 🗸	Template labfw01		View by Device	✓ Mode Si	ngle VS
Setup • Availability	Device Certificate	s Default Trusted Ce	rtificate Authorities		
Password Profiles	Q(1			
Administrators		SUE	UECT	ISSUER	
Authentication Profile	🔲 🗊 github	CN	= github.int.digitalscepter.com	issuer=DC = com, DC = digit	talscep
Authentication Sequence	🔲 🗊 wildcard.int.d	igitalscepter.com CN	= *.int.digitalscepter.com	R10	
o IoT Security	Crt.saml_azur	e_gp.shared CN	= Microsoft Azure Federated SSO Cer	tificate CN = Microsoft Azure Federa	ated S
步 DHCP Server Log Inges 品 Data Redistribution	🔲 💭 gp.digitalscep	ter.com CN	= gp.digitalscepter.com	E6	
WM Information Sources	decrypt_lab	CN	= decrypt.lab.digitalscepter.com	Digital Scepter Lab Issuing C	A



ertificate info	rmation	0	digitalscepter	DAS	HBOARD AC	C MONITOR	Device Groups POLICIES OBJECTS	NET	r Templates WORK [DEVICE	
	mation		Panorama 🗸 🗸	- Tr	emplate labfw01		✓ View by Device			~	Mod
Name	decrypt_lab		Setup •	^ [Device Certificate	s Default Trusted (ertificate Authorities				
	✓ Shared		High Availability								
Subject	/CN=decrypt.lab.digitalscepter.com		Password Profiles	C	2(4 it	ems -	×κ
Issuer	/DC=com/DC=digitalscepter/DC=lab/CN=Digital Scepter Lab Issuing CA		Administrators								
Not Valid Before	Nov 17 23:11:19 2024 GMT		Admin Roles		NAME	SUBJECT	ISSUER	CA K.	EXPIRES	S /	A U.
Not Valid After	Nov 17 23:11:19 2026 GMT		Authentication Sequence		github	CN = github.int.digitals	issuer=DC = com, DC = di		Mar 29 05:	e	R
Algorithm	RSA	- I			wildcard.int	CN = *.int.digitalscepte	R10		Jan 1 02:11.	. v I	R
Revoke:	Certificate Authority Forward Trust Certificate Forward Untrust Certificate Trusted Root CA		Did Security DHCP Server Log Inges Data Redistribution Wh Information Sources Certificate Management Certificate Profile OCSP Responder SSL/TLS Service Profile	•	Delete Revoke	Ch = Microsoft Azure ter.com gp.digitalscepter	CN = Microsoft Azure Fed E6	ertificate	 Dec 20 18: Dec 20 18: 	· e	R

Certificate Name decrypt_lab_untrust Common Name UNTRUSTED - DO NOT CONTINUE - IP or FQDN to appear on the certificate Signed By Certificate Authority Discl. Priote Kine Forced	DS LAB
Common Name UNTRUSTED - DO NOT CONTINUE - IP or FQDN to appear on the certificate Signed By Certificate Authority Certificate Authority	DS LAB
Common Name UNTRUSTED - DO NOT CONTINUE - IP or FQDN to appear on the certificate Signed By Certificate Authority	DS LAB
IP or FQDN to appear on the certificate Signed By Certificate Authority Review Director Konstant	
Signed By Certificate Authority Red Direct Kar Forest	
Certificate Authority	
Directo Defension Kerne Comparts	
BIOCK Private Key Export	
OCSP Responder	`
Cryptographic Settings	
Algorithm RSA	~
Number of Bits 2048	~
Digest sha256	~
Expiration (days) 3650	
ertificate Attributes	
TYPE VALUE	
Add (_)Delete	

Certificate info	ormation	?
Name	decrypt_lab_untrust	
	Shared	
Subject	/CN=UNTRUSTED - DO NOT CONTINUE - DS LAB	
Issuer	/CN=UNTRUSTED - DO NOT CONTINUE - DS LAB	
Not Valid Before	Nov 17 23:55:19 2024 GMT	
Not Valid After	Nov 15 23:55:19 2034 GMT	
Algorithm	RSA	
	Certificate Authority	
	Forward Trust Certificate	
	Forward Untrust Certificate	
	Trusted Root CA	
Revoke	Сапсе	



©2022 Digital Scepter. All rights reserved. digitalscepter.com

E	evice Group lab		~										G
Q	(2 items
					Sou	irce			Destination				
	NAME	LOCATION	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	URL CATEGORY	SERVICE	ACTION
1	Protect Confidential	lab	none	any	C INTERNAL_NE	any	any	P2 outside	any	any	custom_no_decrypt financial-services government health-and-medicine	any	no-decrypt
2	Decrypt - Outbound	lab	none	any	Labwpki02	any	any	PP outside	any	any	any	any	decrypt



©2022 Digital Scepter. All rights reserved. digitalscepter.com







digitalscepter



Conclusion

- Thanks for attending!
- Implementing Zero Trust Security Principles Today at 4 pm in Harbor G (2nd floor)
- Falco product demonstration Wednesday at 10 am Tomorrow at 10 am in Expo Hall Lobby Room B



What is Falco?

- A tool to detect configuration issues
- A managed service to assist with fixing them
- Product demonstration
 Wednesday at 11 am







Sample Falco Report

Falco Plus



digitalscepter

sales@digitalscepter.com (888) 299-3718

digitalscepter.com