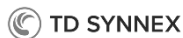




Jeroen Burgerhout
Okta Sari

Demystifying Cloud Security: Unlocking Certificate-Based Authentication and PKI Best Practices

Start 07:45







IT'S LIKE 7 AM



Sprekers



Jeroen Burgerhout

Tech Lead Modern Workplace



<https://burgerhou.tj/connect>

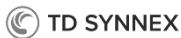


Oktay Sari

Freelance Modern Workplace Consultant



<https://allthingscloud.blog>





What are we going to discuss?

7 points

1. Why use Cloud PKI?
2. Cloud PKI like a Pro!
3. Demo Cloud PKI
4. Why CBA

5. CBA like a pro!
6. Demo CBA
7. Going Passwordless!
8. Questions

1. Why use Cloud PKI



Simplify
certificate
delivery to
Intune clients



Set up a PKI
in minutes
instead of
weeks



Improve
security more
easily than ever



Part of Intune Suite
or
Single license

No need for on-prem PKI

No need for on-prem servers, like:

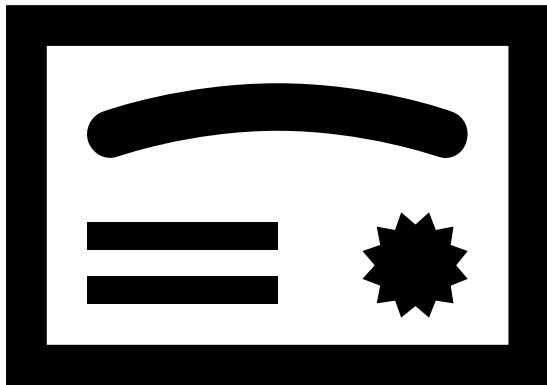
- Root CA
- Issuing CA
- Web
- NDES
- Web proxy
- Policy CA

Also

- a dedicated HSM
- No firewall/port maintenance

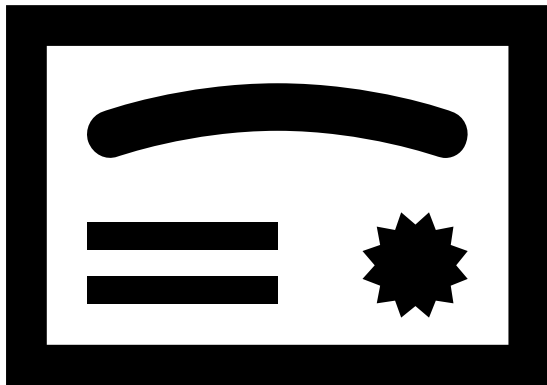


2. Cloud PKI like a Pro



- ❖ AIA (Authority Information Access)
 - ❖ For each Issuing CA
 - ❖ Endpoint can be used by relying parties to retrieve parent certificates
- ❖ CRL (Certificate Revocation List)
 - ❖ For each CA Validity period is 7 days.
 - ❖ Publishing and refresh happens every 3,5 days. After every revocation, the CRL is updated

2. Cloud PKI like a Pro



❖ SCEP (PKCS#7)

- ❖ Intune only enrolled devices
- ❖ <https://{{CloudPKIFQDN}}/TrafficGateway/PassThroughRoutingService/CloudPki/CloudPkiService/Scep/9028deb3-.....>



Planning

Validity Period (Root CA)

- 5 Year Minimum
- 25 Year Maximum

Best Practice

- Issuing CA Half Lifetime of Root CA
- Example: 20 Year Root > 10 Year Issuing

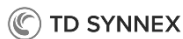
Validity Period (Issuing CA)

- 2 Year Minimum
- 10 Year Maximum



Pro Tips!

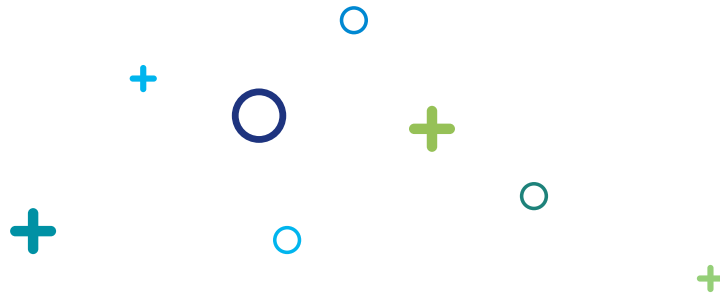
Here are some Pro-tips to take home...





WHAT DID I DO?

NETFLIX



Warning

**Settings Cannot Be Changed After
Deployment!**



Limit access / RBAC

- Global Administrator
- Intune Administrator
- Custom Intune role

^ Cloud PKI

Read CAs ⓘ

No

Yes

Disable and reenable CAs ⓘ

No

Yes

Revoke issued leaf certificates ⓘ

No

Yes

Create certificate authorities (CAs) ⓘ

No

Yes



Demo Time..

- Cloud PKI Setup
- RBAC

1. Why use CBA?



Passwordless
login using X.509
certificates
instead of
passwords



Phishing-resistant:
Private keys can't
be phished or
guessed



Strong security:
Meets high
requirements
mandated in
government etc.



**Simplified user
experience:**
no passwords to
remember or
reset



Integrates with
Cloud PKI

Go for the best!

Bad: Password

Good: Password
and...

Better: Password
and...

Best: Passwordless

123456

qwerty

password

iloveyou

Password1



SMS



Voice



Authenticator
(Push Notifications)



Software
Tokens OTP



Hardware Tokens OTP
(Preview)



Authenticator
(Phone Sign-in)



Window
Hello



FIDO2 security key



Certificates

Passkeys !!!

Password facts...



Password facts...

Forgetting a password brings to light those negative emotions to even more people with 62% feeling stressed or annoyed as a result of forgetting their password. This was highest in the UK (69%) compared with France (65%) and the Netherlands (53%).

Even in organizations that explicitly instruct users on how to select strong passwords, many do not comply, and use weak passwords.

Password fatigue, the stress that users experience due to requirements to create, re-enter, remember and change a large number of passwords can lead to extreme stress.

The potential impact from forgetting a password can cause extreme levels of stress, and over time that can lead to breakdown or burnout.

5. CBA like a Pro

❖ Prerequisites PKI;

- ❖ Didn't we talk about Cloud PKI?
- ❖ Configure at least one certificate authority (CA) and any intermediate CAs in Microsoft Entra ID.
- ❖ User certificates are issued from the PKI
- ❖ An internet accessible Certificate Revocation List (CRL) for each CA



Microsoft



TD SYNEX

Capgemini

infor

DELL
Technologies

nerdio

Professional
Development
Systems BV

INTERSTELLAR



kpn
Partner Network

INS PARK



cegeka

Security | Public key infrastructure (Preview) ...

Search

Getting started

Diagnose and solve problems

Protect

- Conditional Access
- Identity Protection
- Security Center
- Verified ID

Manage

- Identity Secure Score
- Named locations
- Authentication methods
- Multifactor authentication
- Certificate authorities (classic)
- Public key infrastructure (Preview)**

PKIs Deleted PKIs

Create PKI Edit Delete Refresh

Search Add filter

0 PKIs found

Authentication methods | Policies MSFT - Microsoft Entra ID Security

Search Add external method (Preview) Refre

Manage

- Policies**
- Password protection
- Registration campaign
- Authentication strengths
- Settings
- Monitoring

Authentication method policies

Use authentication methods policies to configure the scope for a method, they may use it to authentic scenarios). [Learn more](#)

Method

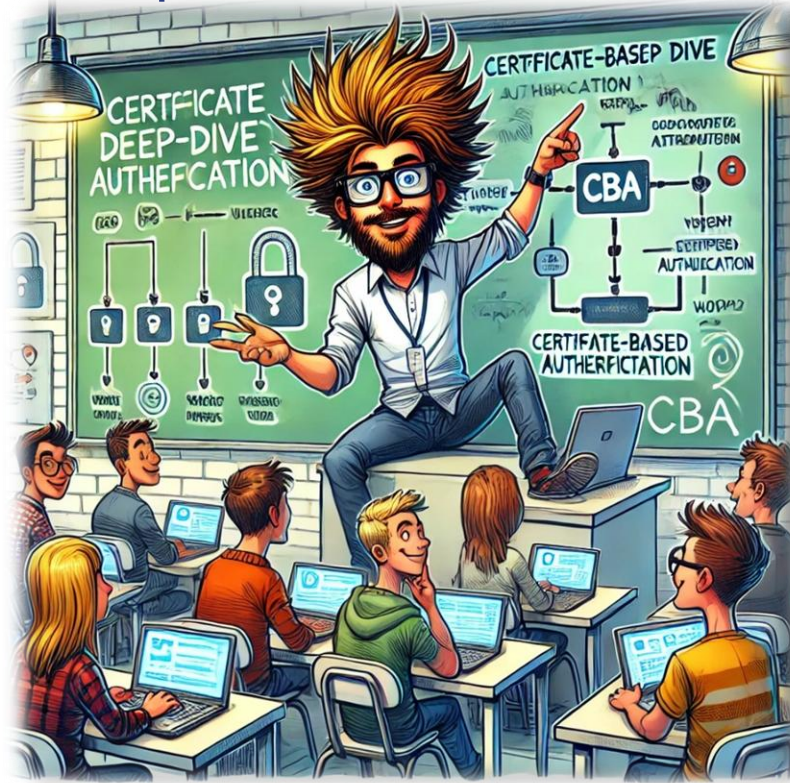
- Built-in**
- Passkey (FIDO2)
- Microsoft Authenticator
- SMS
- Temporary Access Pass
- Hardware OATH tokens (Preview)
- Third-party software OATH tokens
- Voice call
- Email OTP
- Certificate-based authentication**
- QR code (Preview)

5. CBA like a Pro

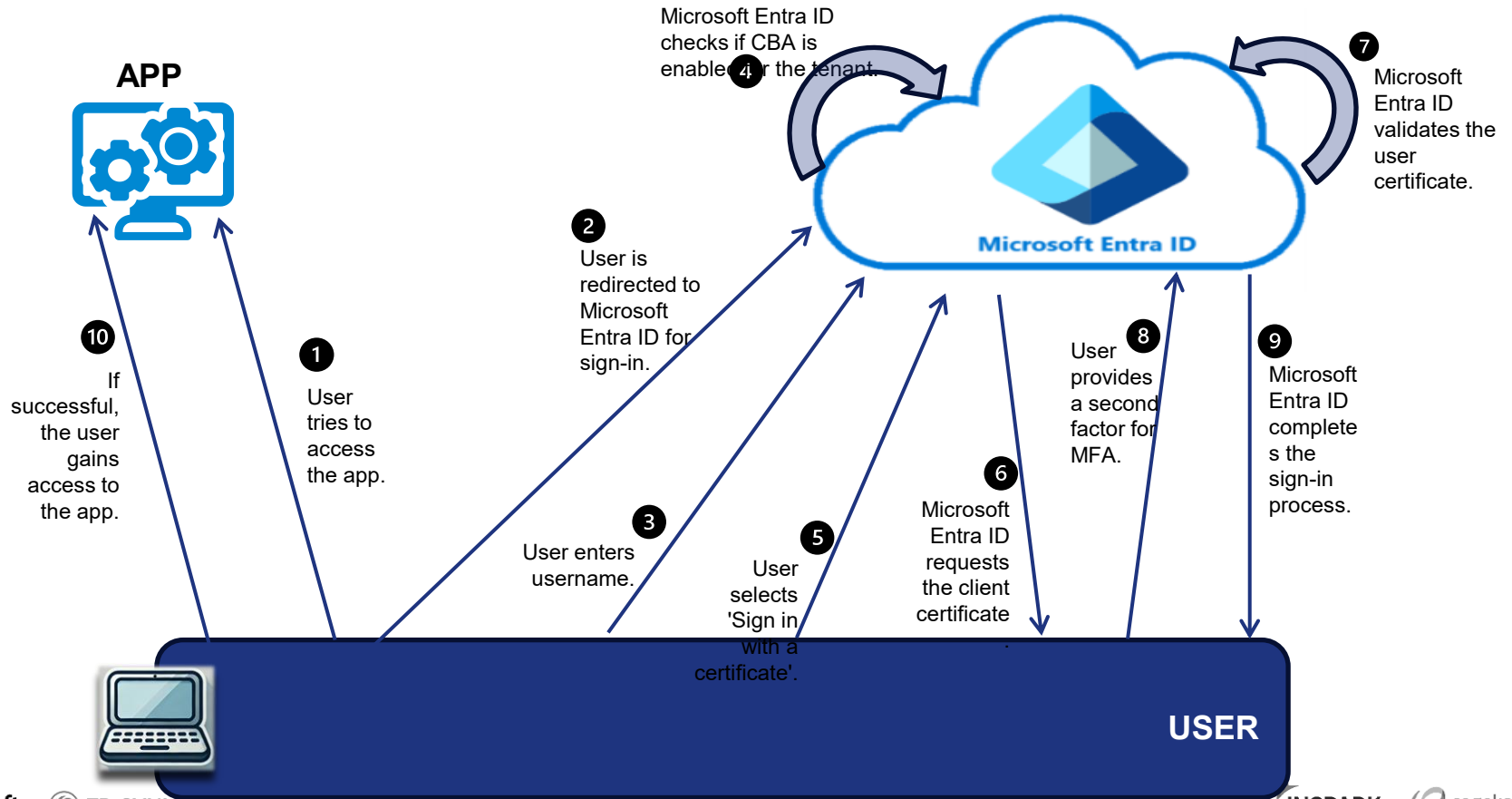
❖ Prerequisites Entra ID;

- ❖ Authentication Methods: Enable Certificate-based Authentication
- ❖ Configure Public key Infrastructure (Preview)

Technical Deep-Dive



How Microsoft CBA works





Demo Time..

- User Experience: iOS
- User Experience: macOS
- User Experience: Windows



Demo Time..

- User Experience: iOS





Sign-in logs

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	...
Device ID						
Browser		Mobile Safari 18.1.1				
Operating System		ios 18.1.1				
Compliant		No				
Managed		No				
Join Type						

Activity Details: Sign-ins

×

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	...
Session Lifetime Policies Applied						
Remember multifactor authentication						
Date	Authentication met...		Authentication met...	Succeeded	Result detail	Requirem...
12/12/2024, 3:07:31 AM	X.509 Certificate			true		



Sign-in logs

Activity Details: Sign-ins

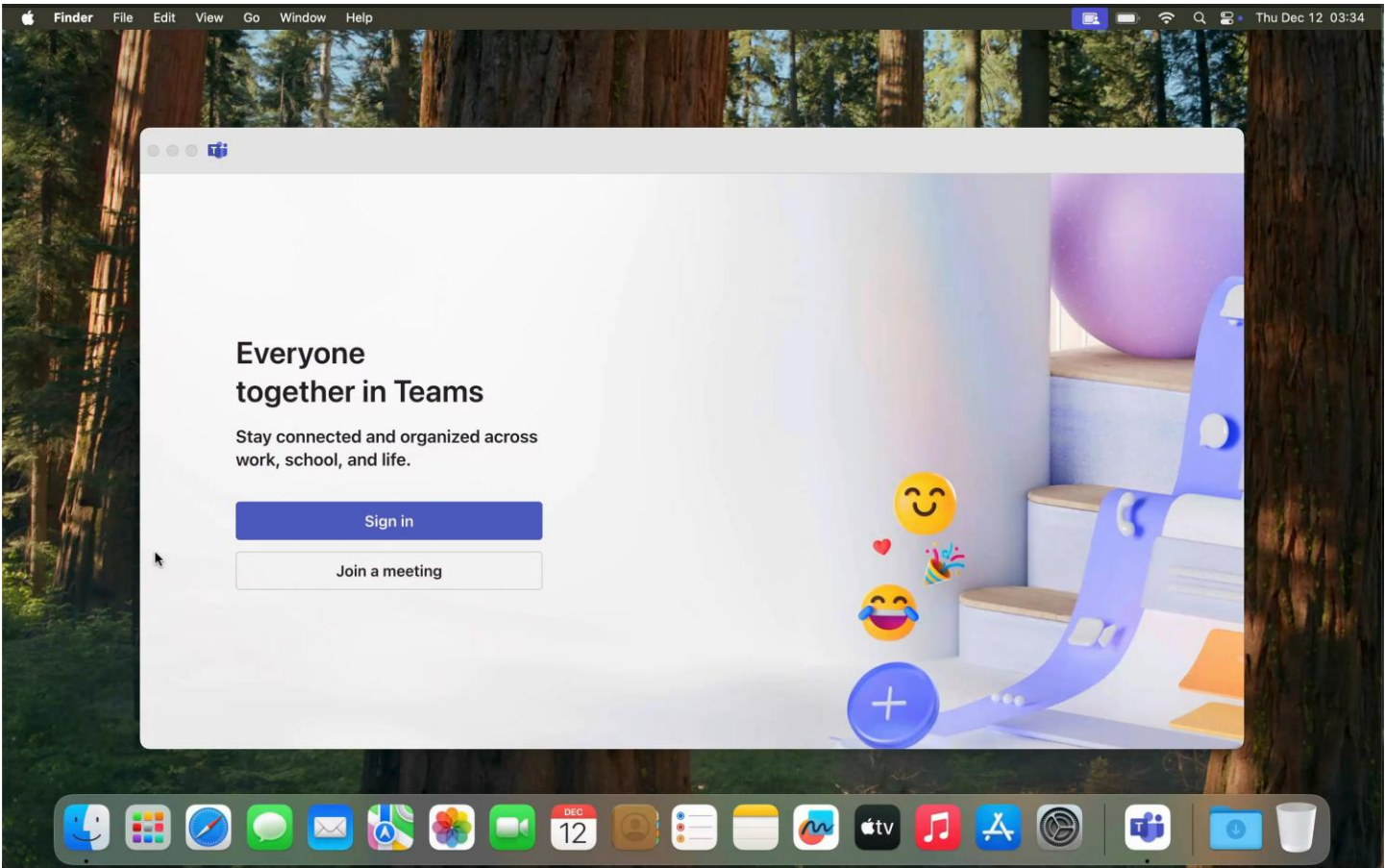


Authentication Details	Conditional Access	Report-only	Authentication Events	Additional Details	...
Domain hint present	True				
Login hint present	True				
User certificate subject	CN=ninja.raccoon, E=ninja.raccoon@allthingscloud.nl				
User certificate issuer	CN=allthingscloud.nl, O=AllThingsCloud, C=NL				
User certificate serial number	00FD58F2B5035E7FCC7687E415392E77DA				
User certificate thumbprint	D03DBDFCA462BC1F62E09BCF961E78220AD50B37				
User certificate valid from	12/12/2024 1:36:03AM				
User certificate expiration	12/12/2025 1:46:03AM				
User certificate binding identifier	ninja.raccoon@allthingscloud.nl				
User certificate binding	Certificate: RFC822Name; User Attribute: userPrincipalName; Rank: 2				
User certificate authentication level	multiFactorAuthentication				
User certificate authentication level type	Issuer				
User certificate authentication level identifier	CN=allthingscloud.nl, O=AllThingsCloud, C=NL				
Issuer Hints set to filter certificates	Enabled				
User certificate affinity mode	Low Affinity				



Demo Time..

- User Experience: macOS



Sign-in logs: PSSO registration

Refresh | Columns | Go to

is 07067013-7236-4566-9508-9d96a8

Application

Microsoft Account Controls V2

Microsoft Account Controls V2

Microsoft Account Controls V2

My Apps

My Apps

Microsoft Authentication Broker

OfficeHome

Microsoft Authentication Broker

Microsoft Intune Web Company P...

Microsoft Intune Web Company P...

Activity Details: Sign-ins

Authentication Details | Conditional Access | Report-only | Authentication Events | Additional Details | ...

Domain hint present	True
User certificate subject	CN=ninja.raccoon, E=ninja.raccoon@allthingscloud.nl
User certificate issuer	CN=allthingscloud.nl, O=AllThingsCloud, C=NL
User certificate serial number	00A890D5075208BC6216012012E0EB37B7
User certificate thumbprint	A4EF11C50E1C2FF7CF0A7A732845D5F684B59BAD
User certificate valid from	12/12/2024 1:29:02AM
User certificate expiration	12/12/2025 1:39:02AM
User certificate binding identifier	ninja.raccoon@allthingscloud.nl
User certificate binding	Certificate: RFC822Name; User Attribute: userPrincipalName; Rank: 2
User certificate authentication level	multiFactorAuthentication
User certificate authentication level type	Issuer
User certificate authentication level identifier	CN=allthingscloud.nl, O=AllThingsCloud, C=NL
Issuer Hints set to filter certificates	Enabled
User certificate affinity mode	Low Affinity

Sign-in logs: myapps with Safari

Activity Details: Sign-ins

Basic info	Location	<u>Device info</u>	Authentication Details	Conditional Access	Report-only
Device ID	5158bdc1-8df1-4010-93b6-c9f1de868bf4				
Browser	Safari 18.1				
Operating System	MacOs				

Activity Details: Sign-ins

Basic info	Location	Device info	<u>Authentication Details</u>	Conditional Access	Report-only	...
Authentication Policies Applied		Session Lifetime Policies Applied				
Conditional Access		Remember multifactor authentication				
Date	Authentication met...	Authentication met...	Succeeded	Result detail	Requirem	
12/12/2024, 3:39:56 AM	Previously satisfied	Azure AD SSO plug-in	true	First factor requiremen...		
12/12/2024, 3:39:56 AM	Previously satisfied		true	MFA requirement satis...		

Authentication Details	Conditional Access	Report-only	Authentication Events	<u>Additional Details</u>	...
Microsoft Entra ID SSO extension version 3.3.19					

Sign-in logs: myapps with Edge

Activity Details: Sign-ins



Basic info

Location

Device info

Authentication Details

Conditional Access

Report-only



Device ID

Browser

Edge 131.0.0

Operating System

MacOs

Basic info

Location

Device info

Authentication Details

Conditional Access

Report-only



Authentication Policies Applied

Conditional Access

Session Lifetime Policies Applied

Remember multifactor authentication

Date	Authentication met...	Authentication met...	Succeeded	Result detail	Requirem...
12/12/2024, 3:41:17 AM	X.509 Certificate		true		
12/12/2024, 3:41:17 AM			true	MFA requirement satis...	

Sign-in logs: myapps with Edge

Activity Details: Sign-ins

Refresh | Columns | Got

ns 07067013-7236-4566-9508-9d96a8

Application ↑↓ Status

Microsoft Account C... Success

Microsoft Account C... Success

Microsoft Account C... Success

My Apps Success

My Apps Success

Microsoft Authentica... Success

OfficeHome Success

Microsoft Authentica... Success

Microsoft Intune We... Success

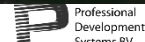
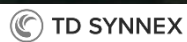
Authentication Details Conditional Access Report-only Authentication Events Additional Details ...

User certificate subject	CN=ninja.raccoon, E=ninja.raccoon@allthingscloud.nl
User certificate issuer	CN=allthingscloud.nl, O=AllThingsCloud, C=NL
User certificate serial number	00A890D5075208BC6216012012E0EB37B7
User certificate thumbprint	A4EF11C50E1C2FF7CF0A7A732845D5F684B59BAD
User certificate valid from	12/12/2024 1:29:02AM
User certificate expiration	12/12/2025 1:39:02AM
User certificate binding identifier	ninja.raccoon@allthingscloud.nl
User certificate binding	Certificate: RFC822Name; User Attribute: userPrincipalName; Rank: 2
User certificate authentication level	multiFactorAuthentication
User certificate authentication level type	Issuer
User certificate authentication level identifier	CN=allthingscloud.nl, O=AllThingsCloud, C=NL
Issuer Hints set to filter certificates	Enabled
User certificate affinity mode	Low Affinity



Demo Time..

- User Experience: Windows





Notes from the field

- Microsoft Entra CBA is a free feature. Play with it in a test tenant
- Other licensing requirements might be in place (Cloud PKI, MFA, M365, Intune)
- Password as an authentication method can't be disabled
- You need to setup a PKI for creating client certificates.
- Sign-in to device is only supported on Windows (using smartcard/fido)
- If CBA is enabled on the tenant, all users see the link to Use a certificate or smart card on the password page.
- Play with Conditional Access and Authentication strength.
- Play with certificates on FIDO2 keys (PIV capable=smartcard)

What's next: Windows Smartcard login





Next sessions 09:00 – 09:45

Security Keynote in Event Hall I & II

AI Keynote in Grand Hall





Next session 10:10 – 11:00

Multi-Tenant Organization (MTO) in Microsoft 365





Please evaluate this session in the App.

THANK YOU

Are there any questions?

