venéco

Moving you *forward*

WORKPLACEDUDES

Meetup

WORKPLACEDUDES

🗣️ HTTPS://SESSIONIZE.COM/WORKPLACEDUDES

AGENDA

16:00 - 16:30	INLOOP
16:30 – 17:20	JEROEN BURGERHOUT – HOUSTON. WE HAVE A SOLUTION: MICROSOFT CLOUD PKI
17:20 – 18:30	ETEN / DRINKEN / NETWERKEN
18:30 – 19:20	RALPH ECKHARD - UNBOXING TEAMS PREMIUM
19:40 – 20:30	GUUS VAN BERGE - SECURE AND GOVERN ACCESS TO YOUR APPLICATIONS WITH MICROSOFT ENTRA ID
20:30 – 21:30	WRAP UP. LOTERIJ EN BORREL

Houston, We Have a Solution: Microsoft Cloud PKI

Jeroen Burgerhout

26-09-2024

WORKPLACEDUDES

Wateringen, We Have a Solution: Microsoft Cloud PKI

Jeroen Burgerhout

26-09-2024

WORKPLACEDUDES

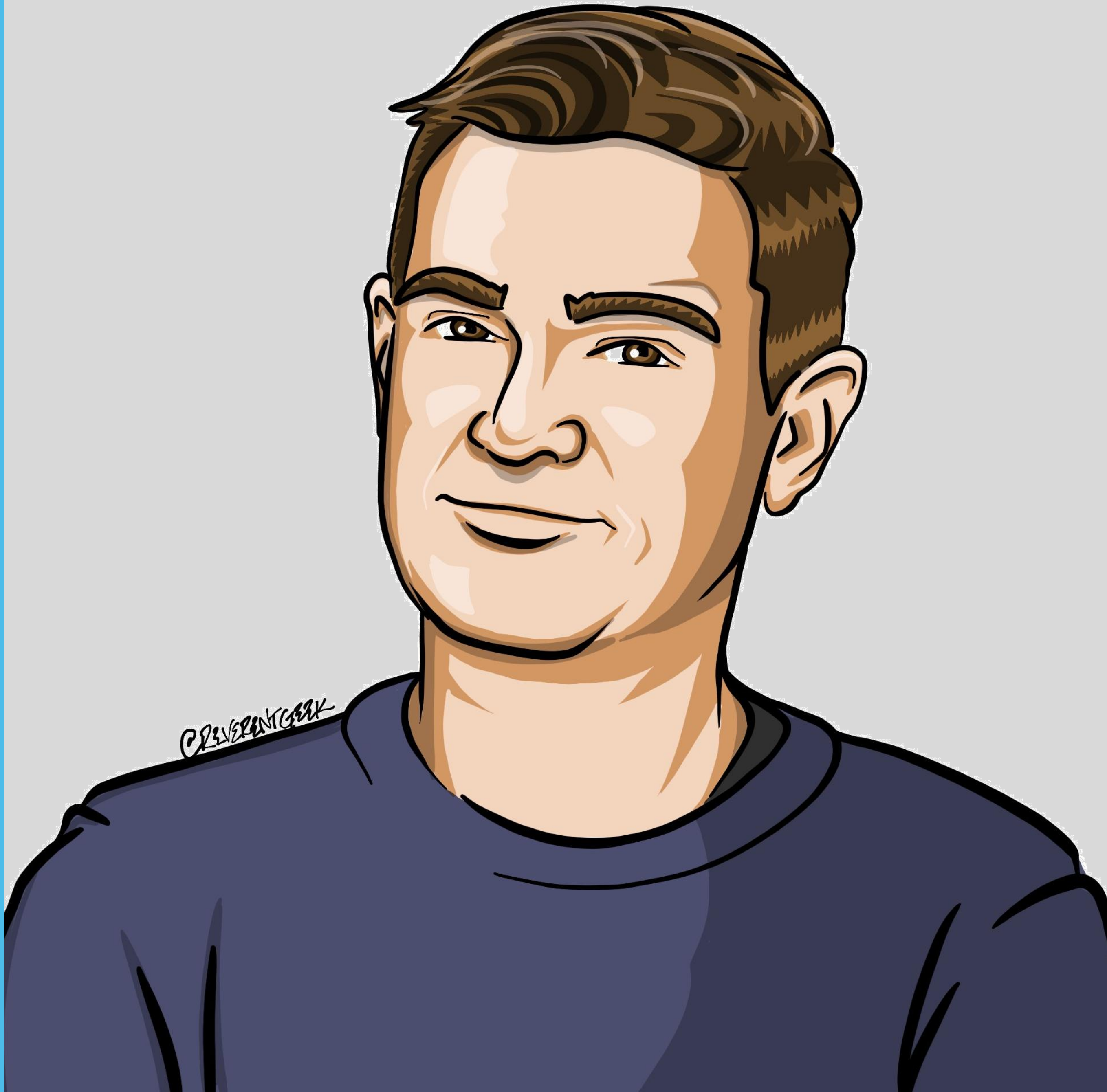
32
02
48

Jeroen Burgerhout

- 🍺 Modern Workplace Brewer
- 📰 burgerhout.org
- 🔗 burgerhou.tj/connect

MVP

Microsoft MCT



What is PKI

A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

What is Cloud PKI?

WORKPLACEDUDES

What is Cloud PKI?

Microsofts solution for PKI
in the Cloud!

Questions?

Microsoft Cloud PKI

General Available since 1st of March 2024

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

Microsoft Cloud PKI

RSA 2048/3072/4096

SHA 256/384/512

Licensed CA -> HSM

Trial CA -> Software keys

2-Tier PKI

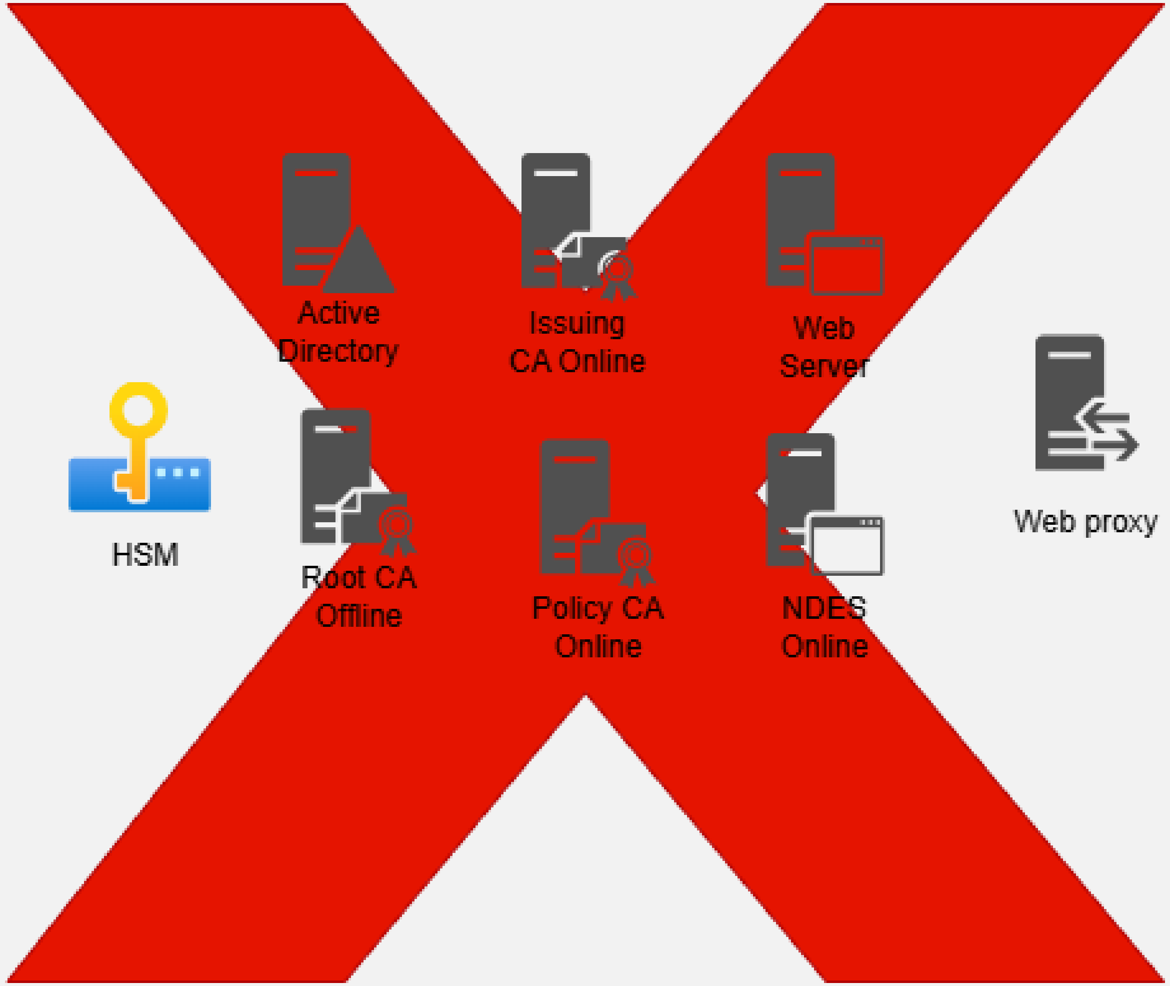
BYOCA

No need for on-prem PKI

Don’t need on-prem servers, like:

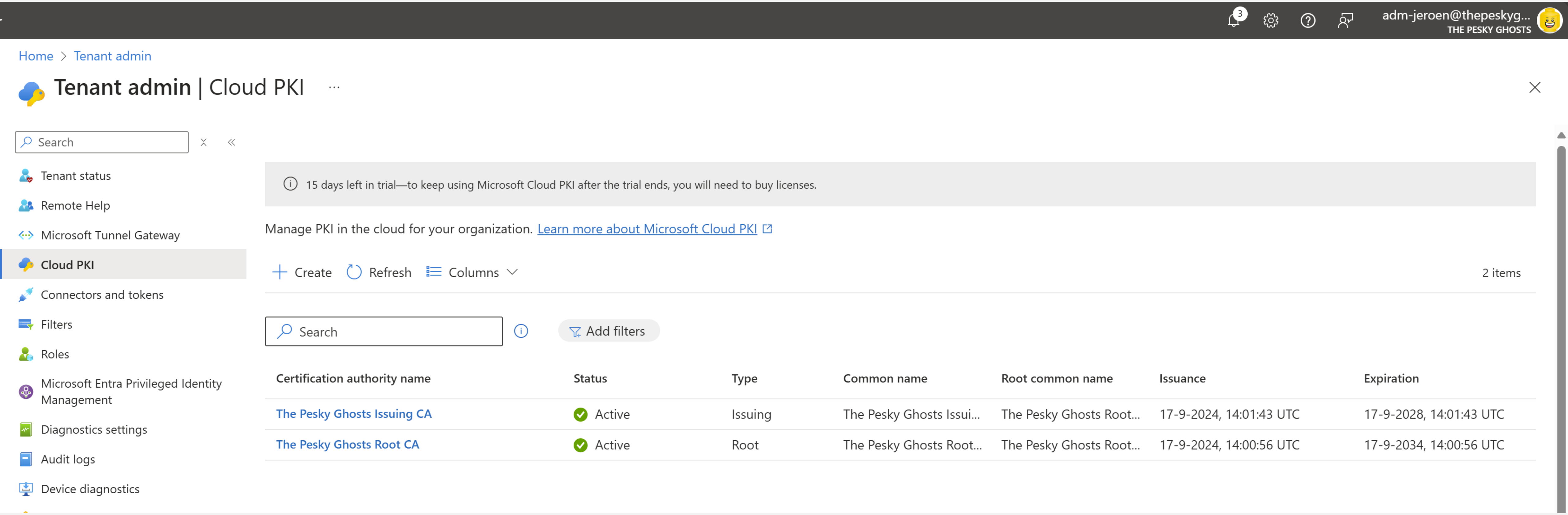
- Root CA
- Issuing CA
- Web
- NDES
- Web proxy
- Policy CA

Also
- a dedicated HSM
- No firewall/port maintenance



WORKPLACEDUDES

Demo setup



Tenant admin | Cloud PKI

15 days left in trial—to keep using Microsoft Cloud PKI after the trial ends, you will need to buy licenses.

Manage PKI in the cloud for your organization. Learn more about Microsoft Cloud PKI

Certification authority name	Status	Type	Common name	Root common name	Issuance	Expiration
The Pesky Ghosts Issuing CA	✓ Active	Issuing	The Pesky Ghosts Issui...	The Pesky Ghosts Root...	17-9-2024, 14:01:43 UTC	17-9-2028, 14:01:43 UTC
The Pesky Ghosts Root CA	✓ Active	Root	The Pesky Ghosts Root...	The Pesky Ghosts Root...	17-9-2024, 14:00:56 UTC	17-9-2034, 14:00:56 UTC

WORKPLACEDUDES

PKI Services

- CRL
  - For each CA
  - Validity period is 7 days. Publishing and refresh happens every 3,5 days. After every revocation, the CRL is updated

- AIA
  - For each Issuing CA
  - Endpoint can be used by relying parties to retrieve parent certificates

- SCEP (PKCS#7)
  - Intune only enrolled devices
  - https://{{CloudPKIFQDN}}/TrafficGateway/PassThroughRoutingService/CloudPki/CloudPkiService/Scep/9028deb3-4647-40fe-b92a-31c3d95459d7/eeefafda-cb0c-4bf1-98f9-16fce4ca6529

Planning

Validity Period (Root CA)

- 5 Year Minimum
- 25 Year Maximum

Validity Period (Issuing CA)

- 2 Year Minimum
- 10 Year Maximum

Best Practice

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

Planning

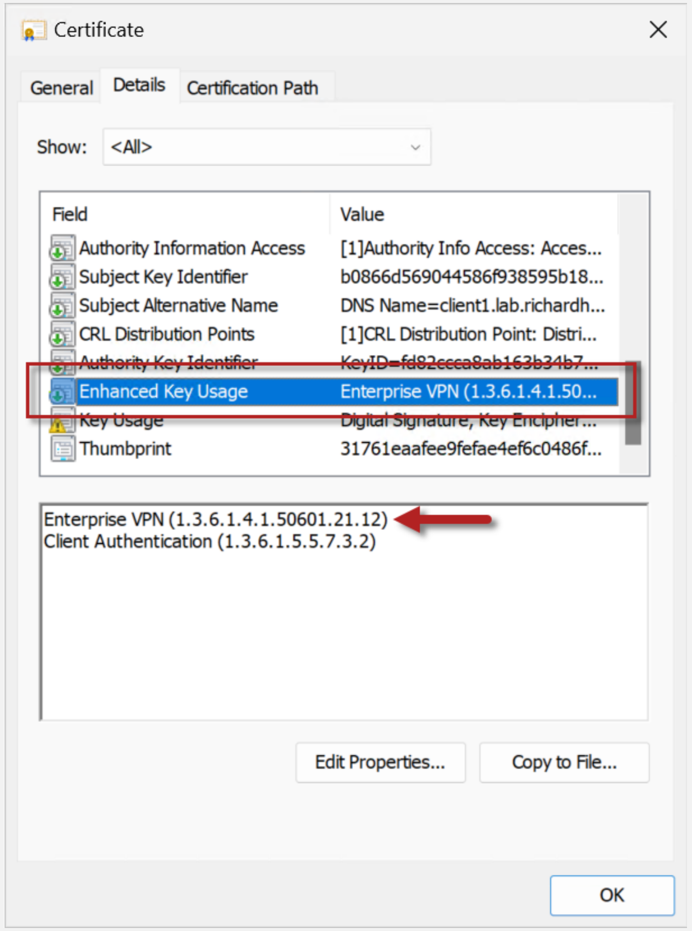
Extended Key Usages (OIDs)

- Client Authentication (1.3.6.1.5.5.7.3.2)
- Server Authentication (1.3.6.1.5.5.7.3.1)
- Smartcard logon (1.3.6.1.4.1.311.20.2.2)
- Code Signing (1.3.6.1.5.5.7.3.3)
- Email Protection (1.3.6.1.5.5.7.3.4)
- And more…

Issuing CA

- Limited to EKUs of Root CA

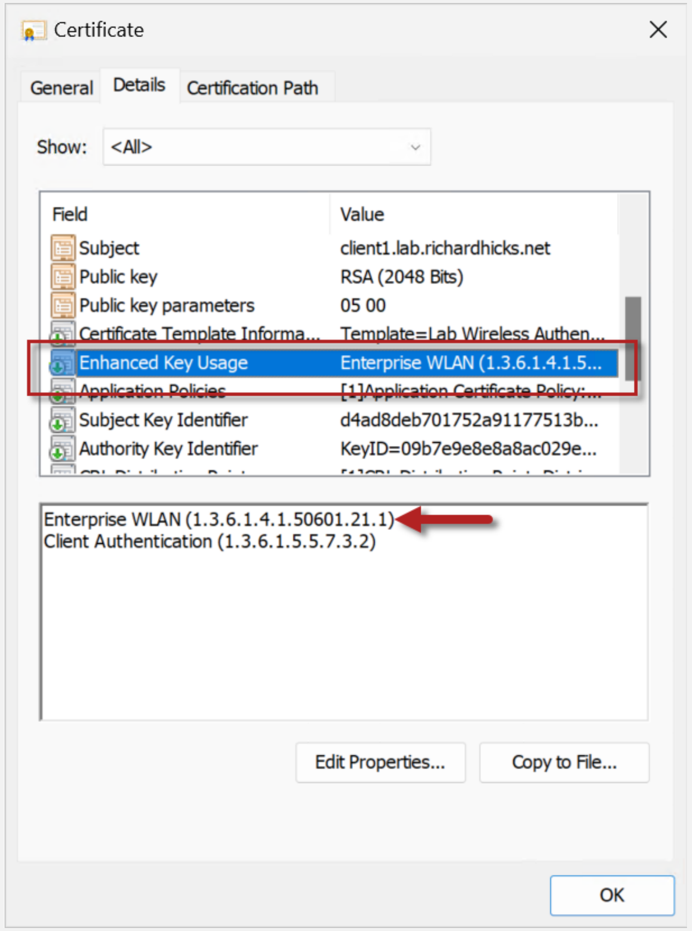
Private Enterprise Number



Show: <All>

Field	Value
Authority Information Access	[1]Authority Info Access: Acces...
Subject Key Identifier	b0866d569044586f938595b18...
Subject Alternative Name	DNS Name=client1.lab.richardh...
CRL Distribution Points	[1]CRL Distribution Point: Distri...
Authority Key Identifier	KeyID=fd82ecca8ab163b34b7...
Enhanced Key Usage	Enterprise VPN (1.3.6.1.4.1.50...
Key Usage	Digital Signature, Key Encipher...
Thumbprint	31761eaafee9fefae4ef6c0486f...

Enterprise VPN (1.3.6.1.4.1.50601.21.12)
Client Authentication (1.3.6.1.5.5.7.3.2)



Show: <All>

Field	Value
Subject	client1.lab.richardhicks.net
Public key	RSA (2048 Bits)
Public key parameters	05 00
Certificate Template Informa...	Template=Lab Wireless Authen...
Enhanced Key Usage	Enterprise WLAN (1.3.6.1.4.1.5...
Application Policies	[1]Application Certificate Policy:...
Subject Key Identifier	d4ad8deb701752a91177513b...
Authority Key Identifier	KeyID=09b7e9e8e8a8ac029e...

Enterprise WLAN (1.3.6.1.4.1.50601.21.1)
Client Authentication (1.3.6.1.5.5.7.3.2)

http://burgerhou.tj/pen

WORKPLACEDUDES

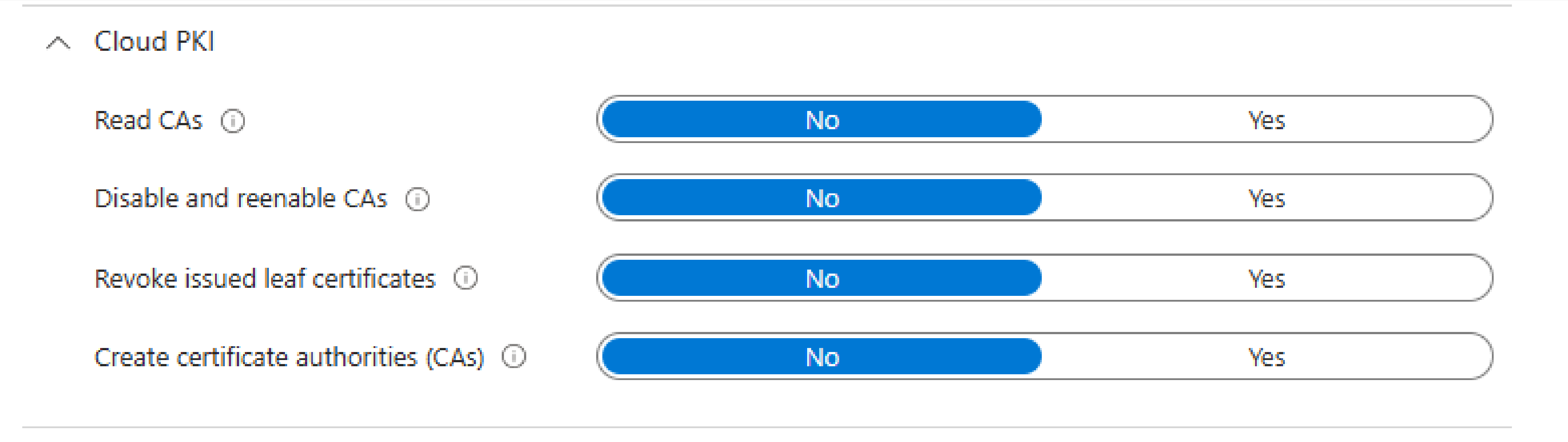
Settings Cannot Be Changed After Deployment!

Limit access

Global Administrator

Intune Administrator

Custom Intune role



Cloud PKI

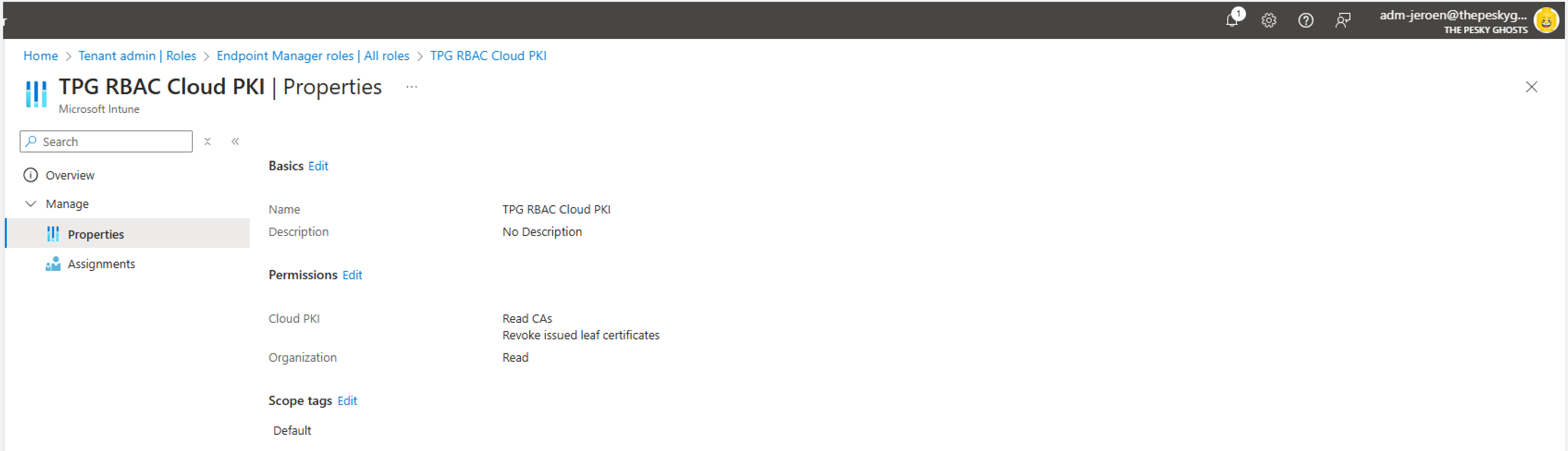
Read CAs ⓘ [✓ No] Yes

Disable and reenable CAs ⓘ [✓ No] Yes

Revoke issued leaf certificates ⓘ [✓ No] Yes

Create certificate authorities (CAs) ⓘ [✓ No] Yes

Demo RBAC



Home > Tenant admin | Roles > Endpoint Manager roles | All roles > TPG RBAC Cloud PKI

TPG RBAC Cloud PKI | Properties

Microsoft Intune

Basics Edit

Name	TPG RBAC Cloud PKI
Description	No Description

Permissions Edit

Cloud PKI	Read CAs Revoke issued leaf certificates
Organization	Read

Scope tags Edit

Default

WORKPLACEDUDES

Use cases

- VPN
- Wi-Fi
- Sensitive Data/Application Access
- Code Signing Scripts/powershell

Certificate Deployment

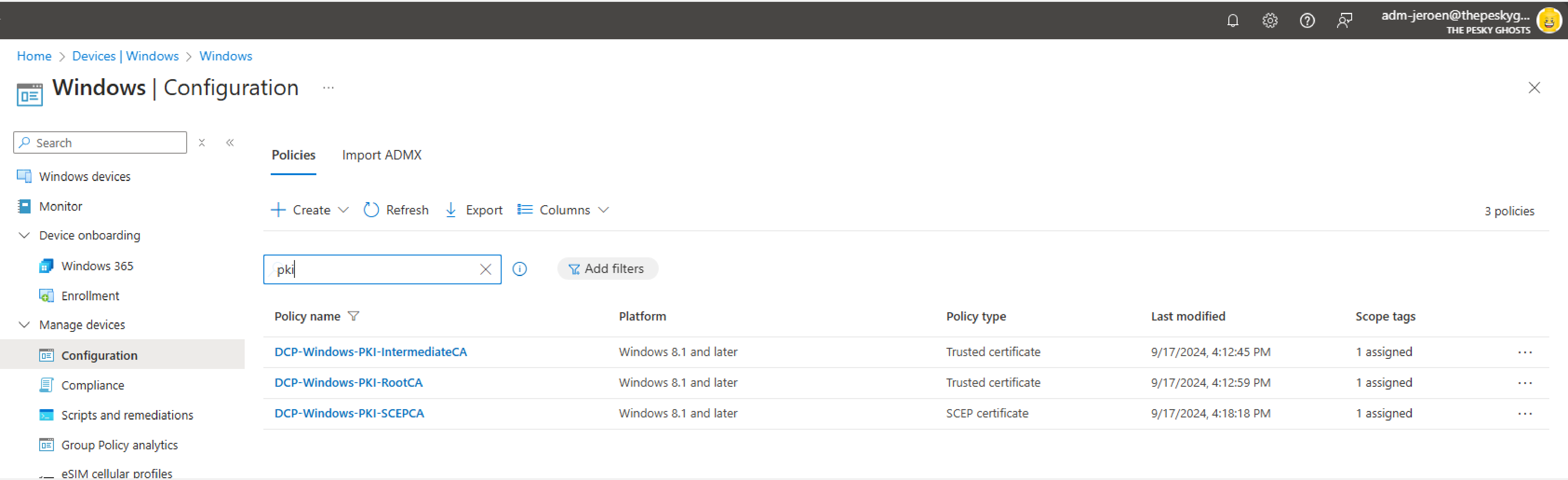
Device Configuration Policies

- Trusted certificate
  - Deploy Root CA Certificate
  - Deploy Issuing CA Certificate

SCEP Certificate

- Entity certificate
  - User
  - Device

Demo deployment



3 policies

pki

Policy name	Platform	Policy type	Last modified	Scope tags
DCP-Windows-PKI-IntermediateCA	Windows 8.1 and later	Trusted certificate	9/17/2024, 4:12:45 PM	1 assigned
DCP-Windows-PKI-RootCA	Windows 8.1 and later	Trusted certificate	9/17/2024, 4:12:59 PM	1 assigned
DCP-Windows-PKI-SCEPCA	Windows 8.1 and later	SCEP certificate	9/17/2024, 4:18:18 PM	1 assigned

Known issues

- ~~Cannot delete CA~~

- EKU
  - Must be set at Root and Issuing CA
  - EKU **Any Purpose** is blocked
  - Issuing CA can only contain EKU from Root CA
  - Once created, cannot be changed

Known issues

- A maximum of 6 CAs in an Intune tenant
  - Licensed: Azure mHSM keys can used for 6 CAs
  - Trial: Up to 6 CAs can be created

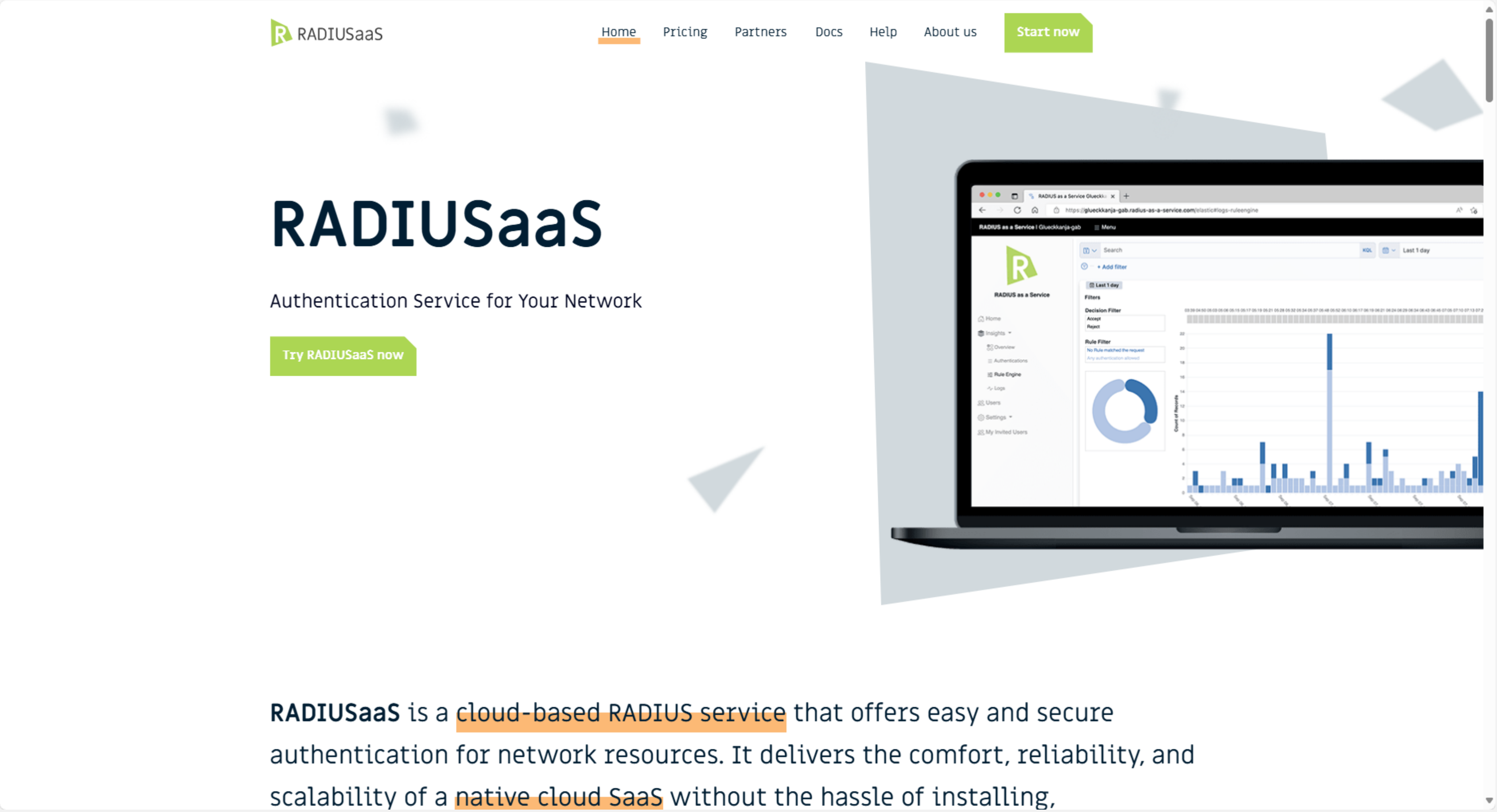
- CA types count towards the capacity:
  - Cloud PKI Root CA
  - Cloud PKI Issuing CA
  - BYOCA Issuing CA

- In the Intune admin center, only the first 1000 issued certificates are shown. As a workaround, go to **Devices** > **Monitor**. To view all issued certificates, select **Certifications**

What about radius?

What about radius?

What about radius?



RADIUSaaS

Authentication Service for Your Network

RADIUSaaS is a cloud-based RADIUS service that offers easy and secure authentication for network resources. It delivers the comfort, reliability, and scalability of a native cloud SaaS without the hassle of installing,

Bring your own CA

Extending Your Existing On-Premises AD CS Infrastructure to Cloud PKI for Intune

Bring your own CA

Cloud PKI Issuing CA

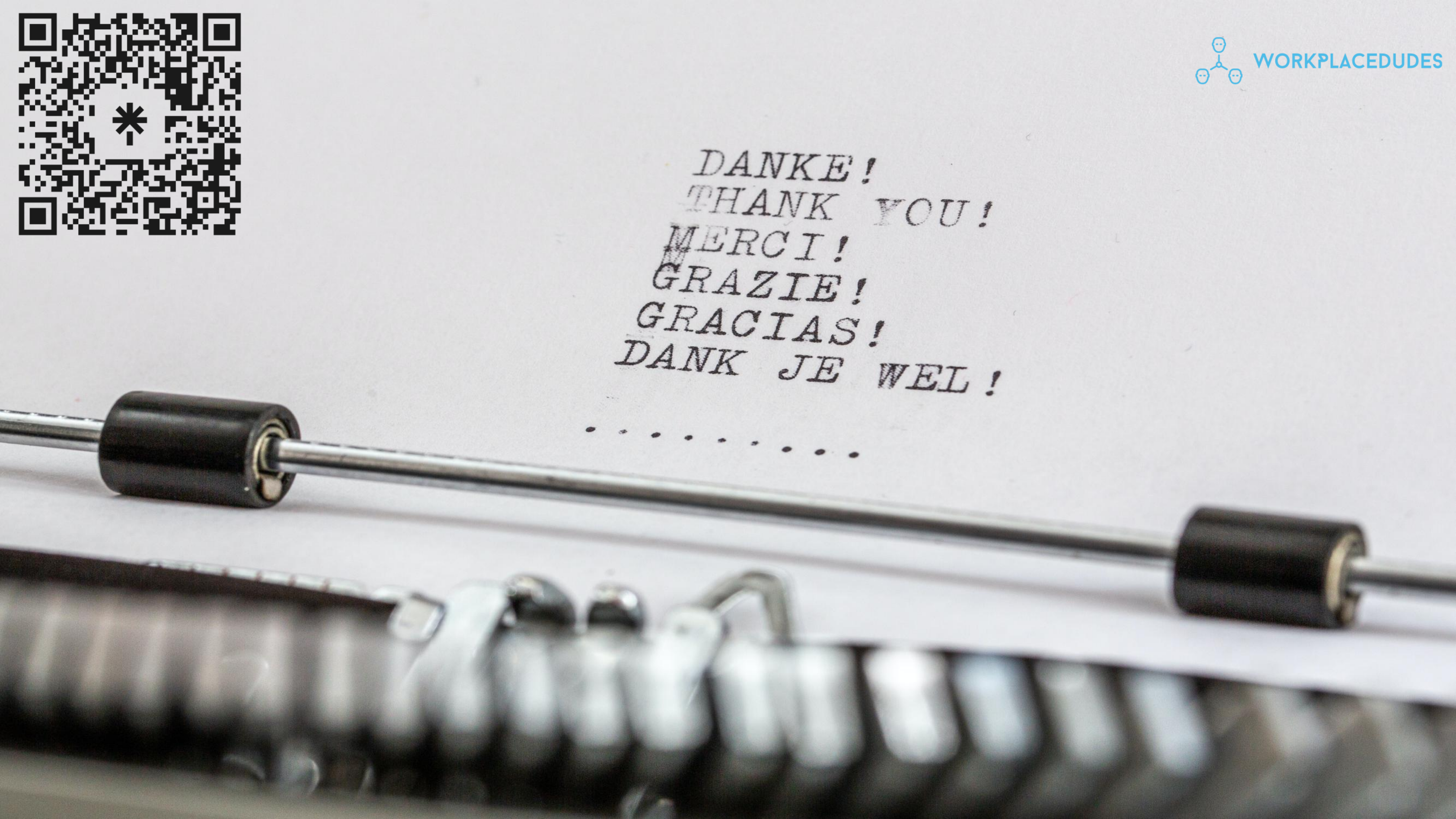
Chained to On-Premises Root CA

Benefits

- Control Root of Trust
- Extend AD CS to Cloud
- Eliminate Need for Intune Certificate Connector
    - No PKCS
    - No NDES/SCEP

Questions?

WORKPLACEDUDES



DANKE!
THANK YOU!
MERCI!
GRAZIE!
GRACIAS!
DANK JE WEL!

....