

# Houston, We Have a Solution: Microsoft Cloud PKI



Jeroen Burgerhout

# Harelbeke, We Have a Solution: Microsoft Cloud PKI



Jeroen Burgerhout

# About Jeroen Burgerhout

## Focus

Microsoft Intune

## From

Nederland

## My Blog

<https://burgerhout.org>

## Certifications

A lot. MVP & MCT

## Hobbies

Craft beer

## Contact

<https://burgerhou.tj/connect>

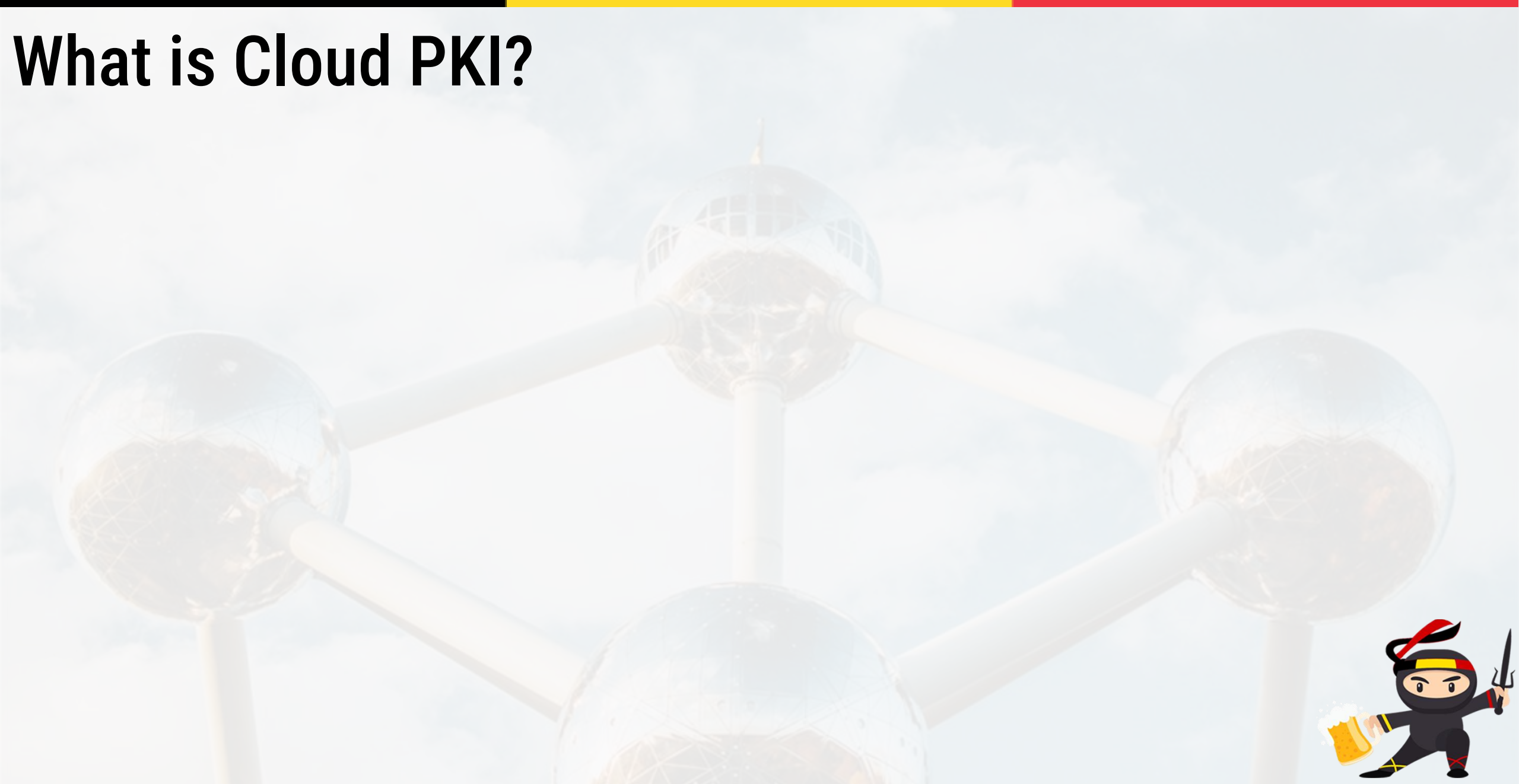








# What is Cloud PKI?



# What is Cloud PKI?

Microsoft's solution for certificate management  
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

No need for on-prem servers, like:

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

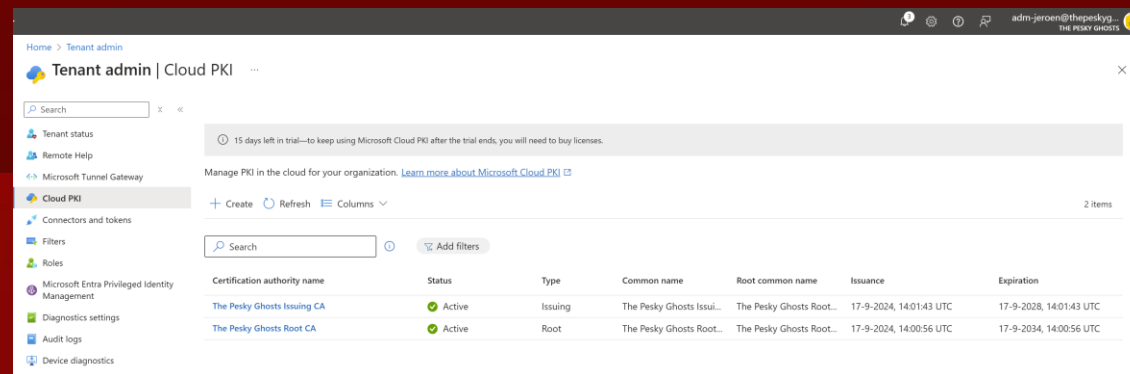
Also

- a dedicated HSM
- No firewall/port maintenance



# DEMO

## Setting it up





# PKI Services

- ❖ 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
- ❖ AIA (Authority Information Access)
  - ❖ 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...

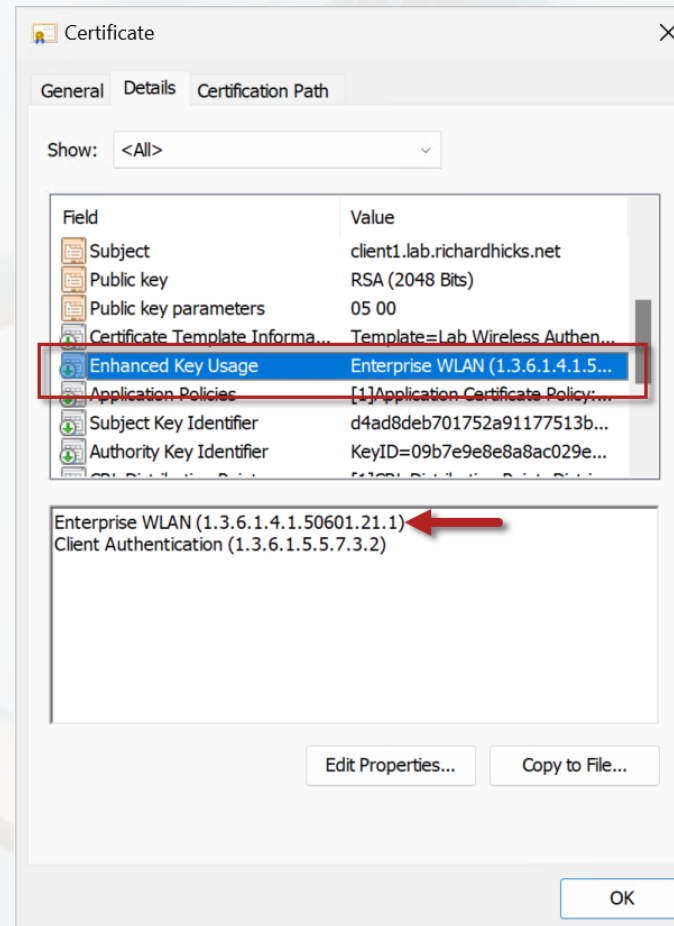
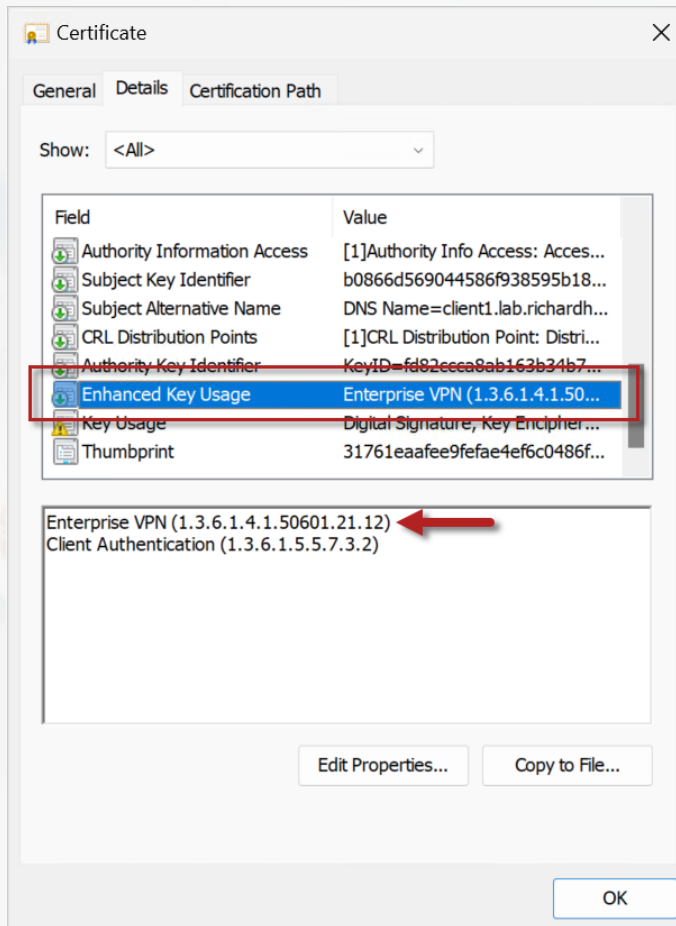
## Issuing CA

- Limited to EKUs of Root CA





# Private Enterprise Number



<https://burgerhou.tj/pen>



# WARNING



**Settings Cannot Be  
Changed After  
Deployment!**



# Limit access

Global Administrator

Intune Administrator

Custom Intune role

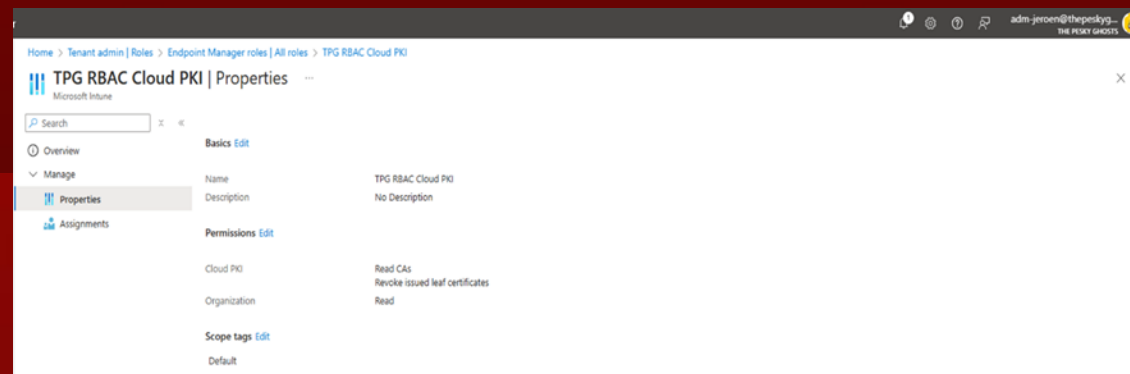


| Cloud PKI                              |   |
|--|---|
| Read CAs ⓘ                             | <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes |
| Disable and reenable CAs ⓘ             | <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes |
| Revoke issued leaf certificates ⓘ      | <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes |
| Create certificate authorities (CAs) ⓘ | <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes |





# DEMO RBAC



# Use cases

- VPN
- Wi-Fi
- Certificate Based Authentication (CBA)
- 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

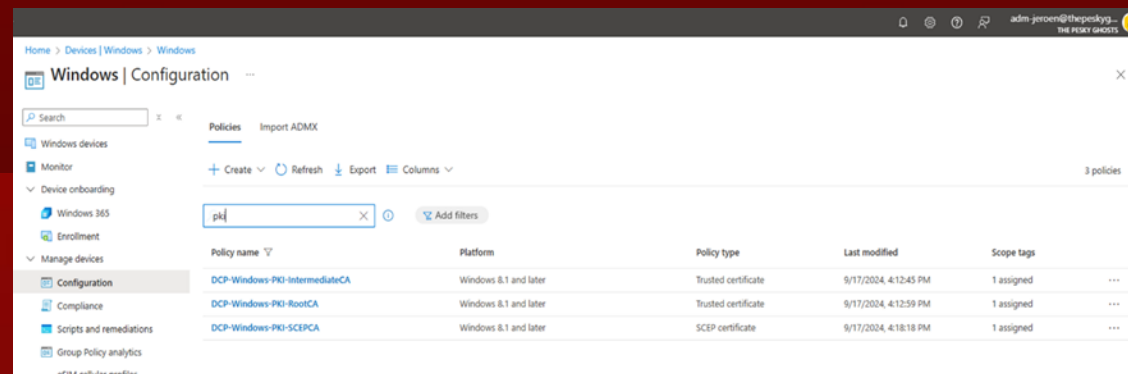
- Entity certificate
  - User
  - Device





# DEMO

## Deploying certificates



# Known issues

## ❖ ECU

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

## ❖ A maximum of 6 CAs in an Intune tenant

- ❖ Licensed: Azure mHSM keys can be used for 6 CAs
- ❖ Trial: Up to 6 CAs can be created



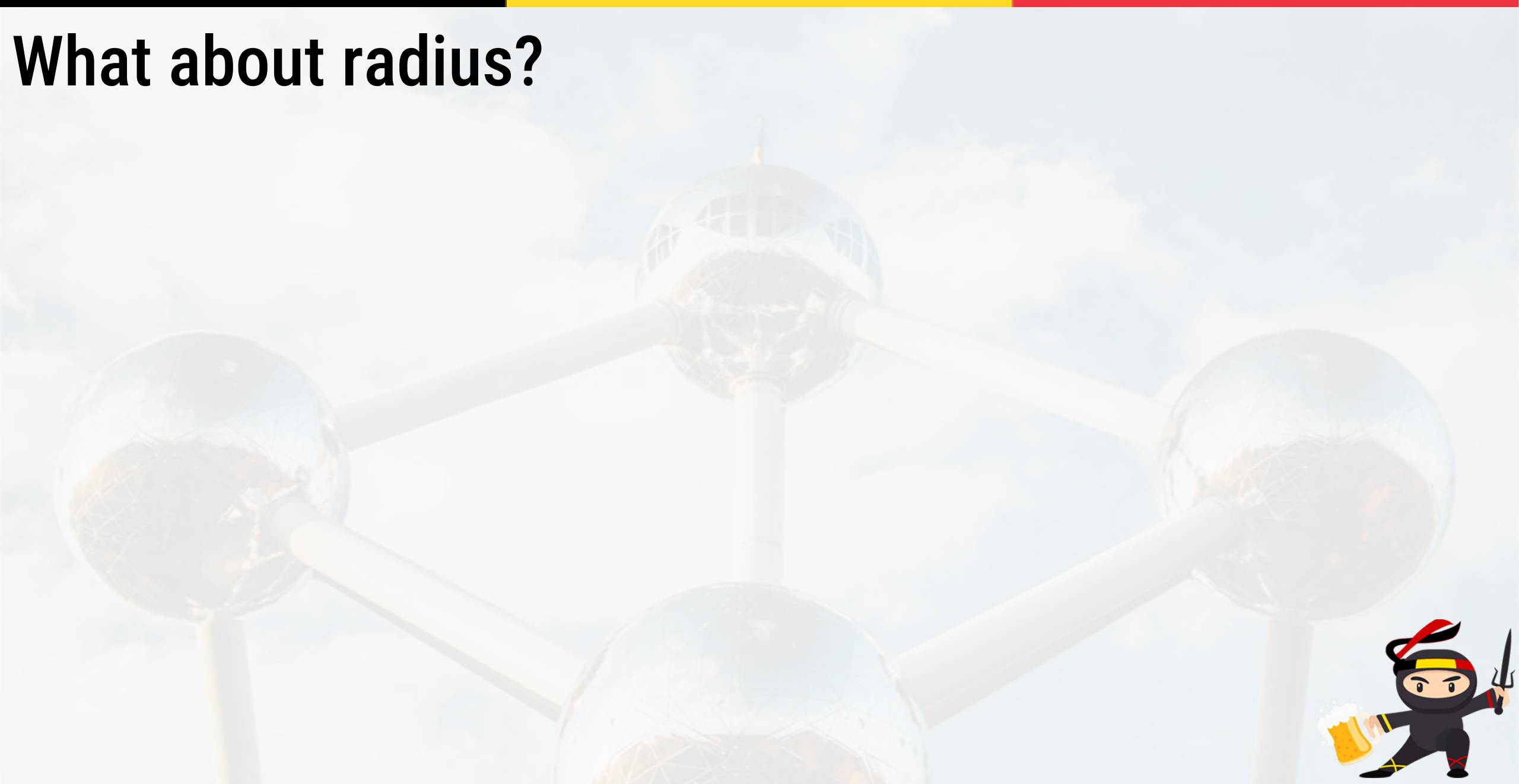
# Known issues

- ❖ 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**





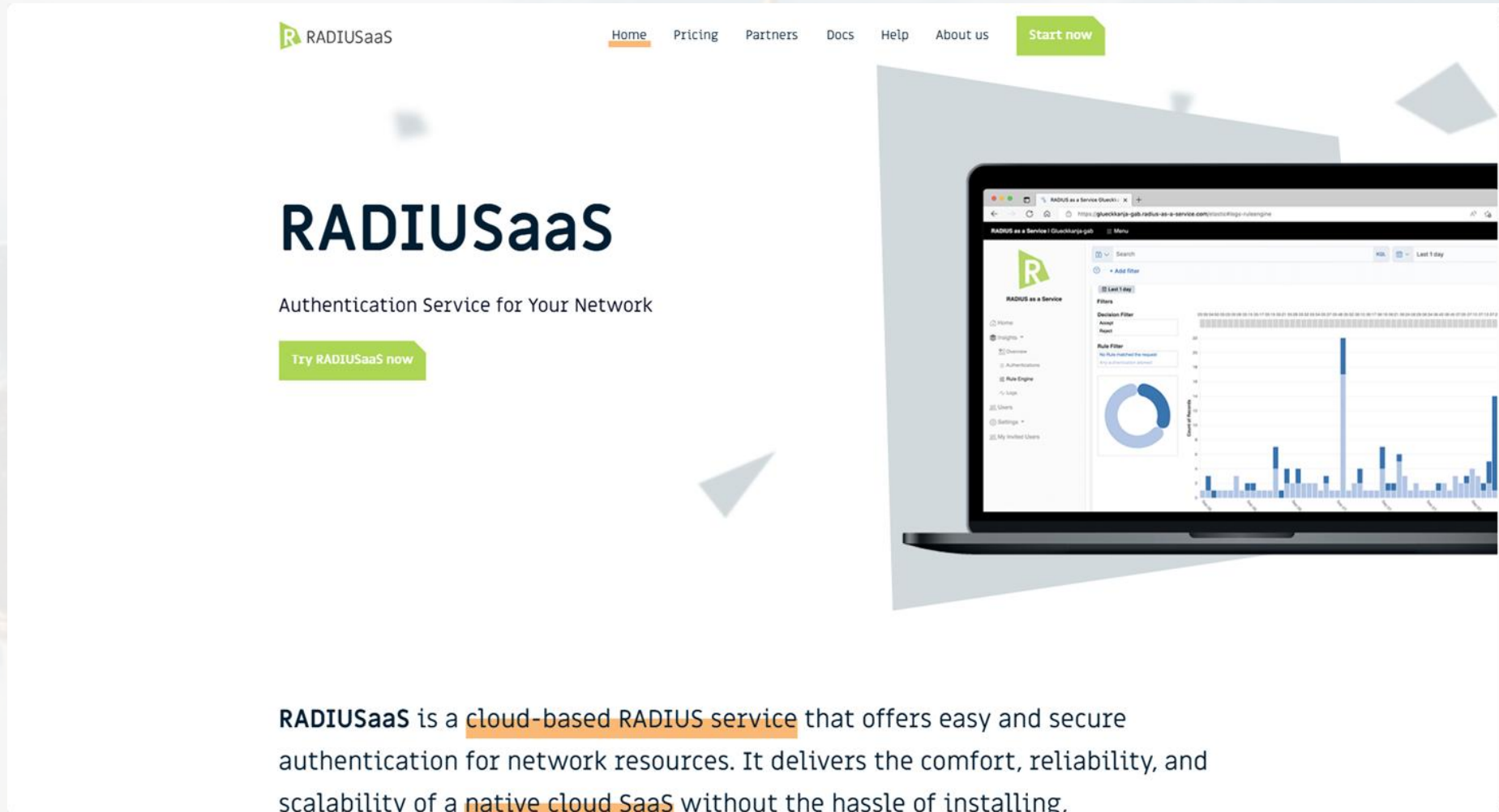
# What about radius?



# What about radius?



# What about radius?



The screenshot displays the RADIUSaaS website and its dashboard. The website header includes the RADIUSaaS logo, navigation links (Home, Pricing, Partners, Docs, Help, About us), and a 'Start now' button. The main heading is 'RADIUSaaS' with the subtitle 'Authentication Service for Your Network' and a 'Try RADIUSaaS now' button. The dashboard, shown on a laptop, features a sidebar with navigation options (Home, Insights, Overview, Authentication, Rule Engine, Users, Settings, My Invited Users) and a main content area with a search bar, filters, a decision filter, a rule filter, a donut chart, and a bar chart showing usage over time.

**RADIUSaaS**  
Authentication Service for Your Network

Try RADIUSaaS now

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

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?



Thank you