Intune Suite – Cloud PKI

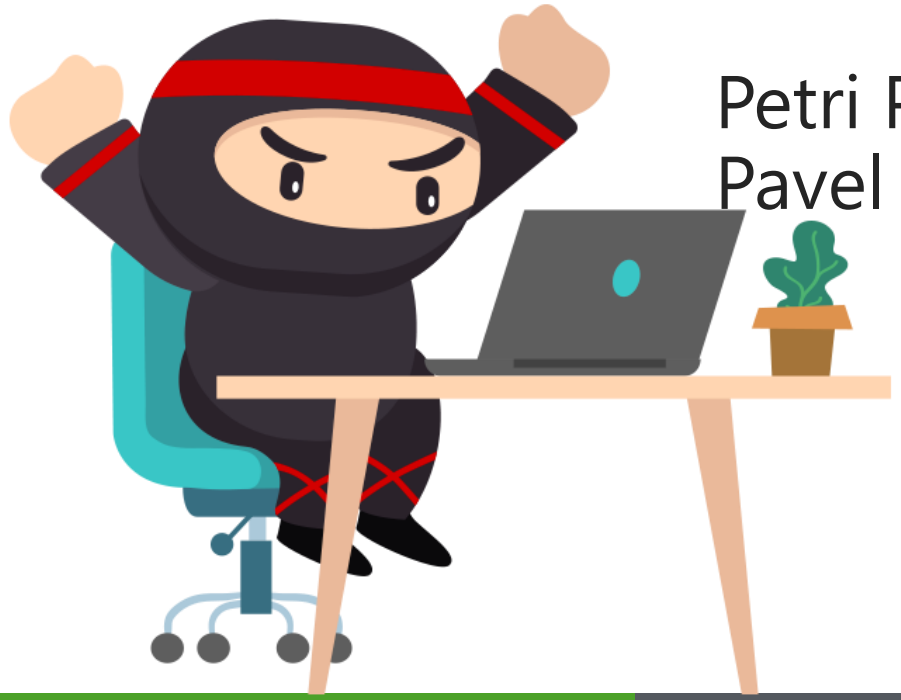
2.10.2025

Etätapaaminen

Workplace Ninja

User Group Finland

Intune Suite – Cloud PKI



Petri Paavola – Ninja MVP
Pavel Mirochnitchenko – Ninja MVP

Petri Paavola

Microsoft MVP – Windows and Intune

Senior Modern Management Principal

Petri.Paavola@yodamiitti.fi

@petripaavola

@intune.ninja

https://github.com/petripaavola

Intune.ninja

Powershell.ninja

Skills

- **Powershell / Graph API**
- **AI**
- **Windows Autopilot + Intune + Intune for Education**
- **Windows 10&11 Deployment and Management**
- **Traditional on-prem deployment and management**
- **Consulting &Training**

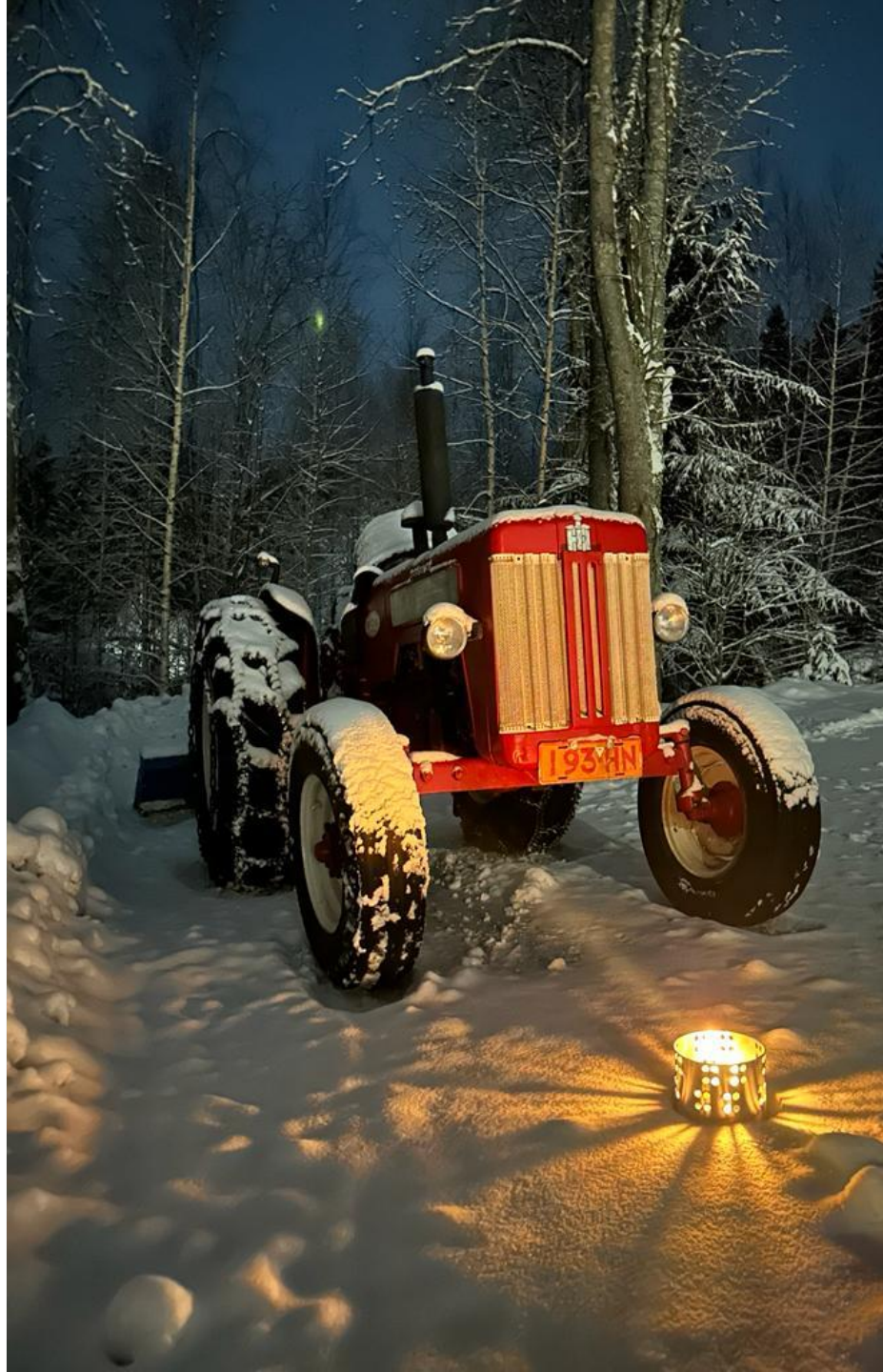
Over 25 years of work experience

Current (10+ years):

- **Yodamiitti Oy / Owner**
  Consulting / Training

Past:

- **Aalto university / IT-services**
  Responsible for Workstation service



Cloud PKI

- **Kaunein esimerkki minkälainen pilvipalvelun pitäisi olla**
  - Helppo ja nopea käyttöönotto
  - Ei palvelimia
  - **Konffaa vartti Intunea ja homma on tuotannossa!**
- **Cloud PKI on Intune Suiten osa**
  - Joko hankitaan koko Intune Suite
  - Tai pelkkä Cloud PKI Add-On
  - Education-hinnoittelu ~5x halvempi kuin normaali Business-listahinta (~10e/käyttäjä/kk)

- https://learn.microsoft.com/en-us/intune/intune-service/protect/microsoft-cloud-pki-overview
- https://learn.microsoft.com/en-us/mem/intune/protect/microsoft-cloud-pki-overview
- https://learn.microsoft.com/en-us/mem/intune/protect/certificates-profile-scep

Cloud PKI

- **2-Tier PKI –malli**
  - Root CA
  - Issuing CA
- **Voidaan hyödyntää myös omaa olemassa olevaa CA:ta**
  - Bring Your Own CA (BYOCA)
  - Intune Cloud PKI jakaa olemassa olevan (on-premise) CA-infran/varmenneketjun varmenteita
  - Ei tarvita NDES/SCEP –konnektoria Intunen kylkeen
- **Salaisuudet tallennetaan fyysiseen HSM (Hardware Security Module)**
  - Kunhan on ostettu lisenssi (ei trial)
  - Eli jos testaatte yhtään tuotanto mielessä, niin haluatte ostaa vähintään yhden lisenssin
- **Kaikki pilvessä, ei omia palvelimia/palveluita**
  - Esim. Certificate Revocation List (CRL) julkaisusta ei tarvitse itse huolehtia

Varmenteiden ikä

- **Root CA**
  - 5-25 vuotta
- **Issuing CA**
  - 2-10 vuotta
- **Suositus**
  - Issuing on puolet Root CA:n pituudesta
  - Esim. 20 vuotta Root CA -> 10 vuotta Issuing CA

Extended Key Usages - EKU

- **"Any Purpose" EKU (eli *) ei ole sallittu**
- **EKU OIDs**
  - Server auth (1.3.6.1.5.5.7.3.1)
  - Client auth (1.3.6.1.5.5.7.3.2)
  - Smartcard logon (1.3.6.1.4.1.311.20.2.2)
  - Code signing (1.3.6.1.5.5.7.3.3)
  - Time stamping (1.3.6.1.5.5.7.3.8)
  - Email Protection (1.3.6.1.5.5.7.3.4)
  - …
- **Private Enterprise Number (PEN)**
  - Onko teidän organisaatiolla oma OID ?

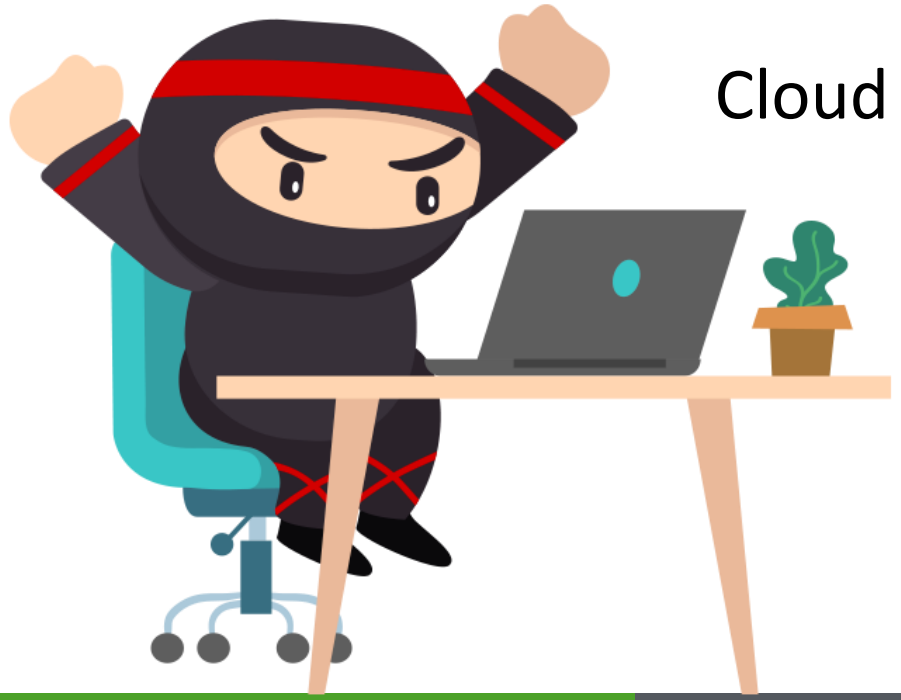
- **Huom! Issuing CA on rajoitettu niihin käyttötarkoituksiin, jotka valitaan Root CA:ssa**
- **Näitä ei voi muokata jälkikäteen!**

Käyttöskenaariot

- **Käyttöskenaariot**
  - Wi-Fi / 802.1x
  - VPN
  - Sovelluksessa käytettävä varmenne
- **Mitä muita käyttötarpeita on pilvihallituissa laitteissa?**

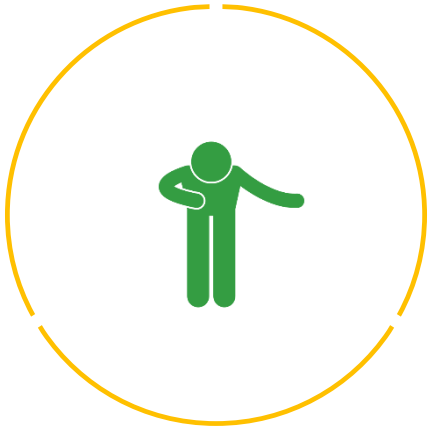
DEMO

Cloud PKI:n konfigurointi



Luettavaa

- **Oliverin blogi on loistava**
  - **How to configure Cloud PKI certificate-based WiFi with Intune**
  - https://oliverkieselbach.com/2024/03/04/how-to-configure-cloud-pki-certificate-based-wifi-with-intune/



Kiitos

Workplace Ninja
User Group Finland