Intunen tehokäyttö Graph API:lla

Matias Haapaniemi

Consigliere & Partner

Matias Haapaniemi

CONSIGLIERE & PARTNER @ Above IT

matias.haapaniemi@aboveit.fi | Seinäjoki | +358505171685

Microsoft 365

Intune, Autopilot, Exchange, Teams

Hybridi-ID, Tietoturva, Power Platform

Azure

IaaS, SaaS, Sentinel

Automation, Logic Apps

18 SERTIFIKAATTIA

- **Microsoft Cybersecurity Architect**
- **Enterprise Administrator Expert**
- Security Administrator Associate
- Security Operations Analyst Associate
- Identity and Access Administrator
- Information Protection Administrator
- Teams Administrator Associate
- Messaging Administrator Associate
- Modern Desktop Administrator Associate
- Azure Administrator Associate
- Azure Security Engineer Associate
- Azure Database Administrator Associate
- **AWS Certified Cloud Practitioner**
- M365 Fundamentals
- Azure Fundamentals
- Security, Compliance, and Identity Fundamentals
- Power Platform Fundamentals
- Azure AI Fundamentals

18 Sertifikaattia

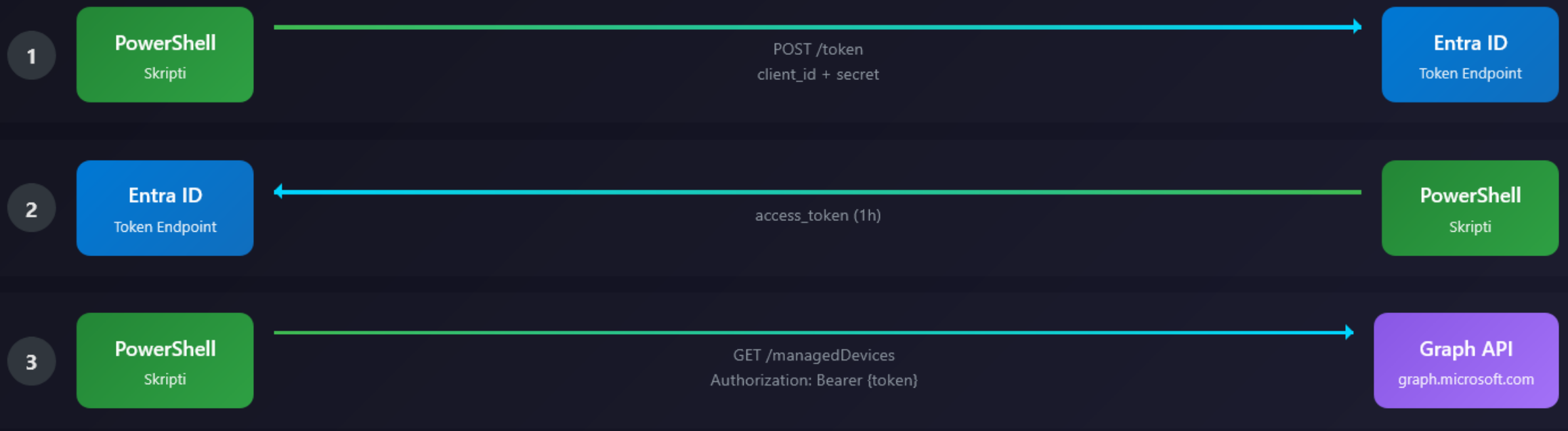
2 Expert

#pilvinatiivi #pilvenreunalla

Client Credentials Flow

Daemon / Backend

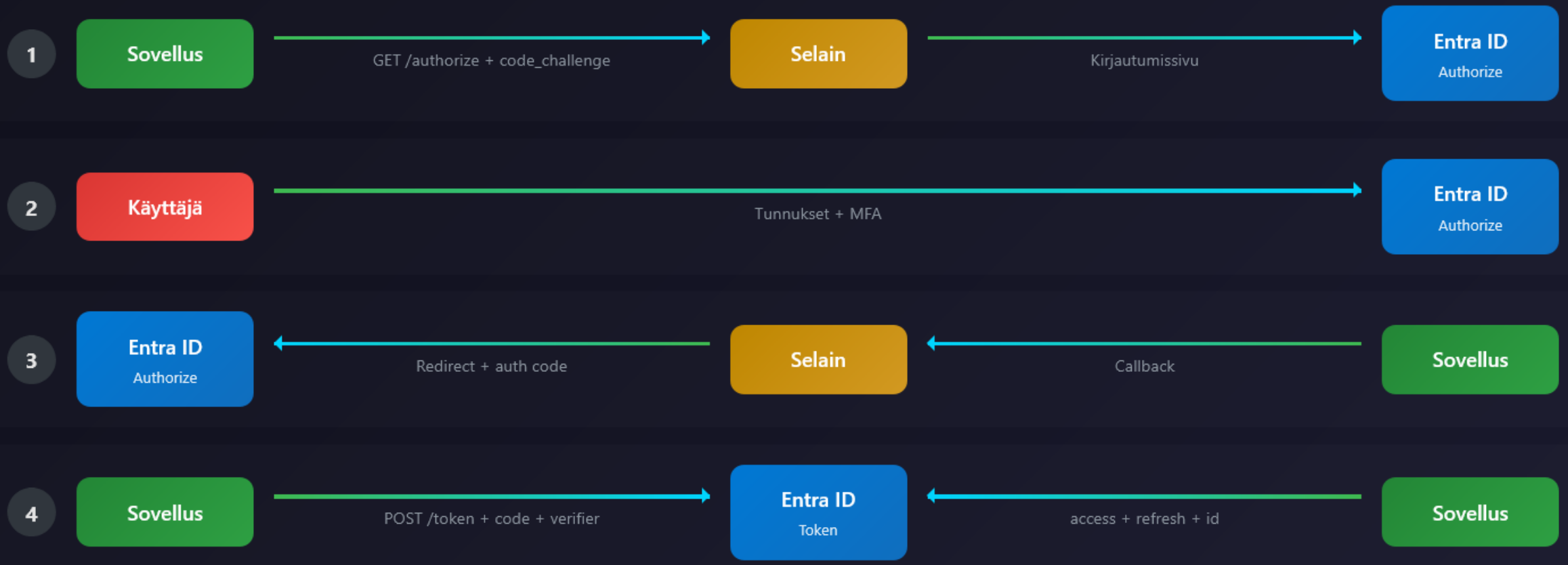
Sovellus toimii omana itsenään ilman käyttäjäkontekstia. Käytetään automaatioissa.



Authorization Code Flow + PKCE

Käyttäjän puolesta

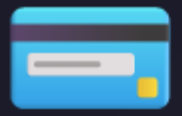
Käyttäjä kirjautuu interaktiivisesti. Tässä flowssa saadaan Refresh Token.



Access Token

= Päivälippu huvipuistoon

Pääset sisään ja nautit laitteista, mutta vain tänään. Huomenna tarvitset uuden lipun.



Refresh Token

= Kausikortti

Et pääse sillä suoraan laitteisiin, mutta voit hakea sillä uuden päivälipun.

Sliding Token vs Absolute Token

Sliding Expiration

Token "liukuu" eteenpäin joka käytöllä. Aktiivinen käyttö pitää tokenin elossa.

- → 90 päivän inaktiivisuusraja
- → Käyttö nollaa laskurin
- → Aktiivisella käytöllä = ikuinen
- → Entra ID:n oletusmalli

Absolute Expiration

Token vanhenee kiinteän ajan jälkeen riippumatta käytöstä.

- → Kiinteä vanhenemispäivä
- → Käyttö ei pidennä elinikää
- → Pakottaa uudelleenkirjautumisen
- → Ei oletuksena Entra ID:ssä

PowerShell Graph API -autentikointi

🔑 REST + Client Secret

Manuaalinen token-haku. Täysi kontrolli, ei riippuvuuksia.

```powershell
$body = @{
    client_id     = "app-id"
    client_secret = "secret"
    scope         = "https://
graph.microsoft.com/.default"
    grant_type    = "client_credentials"
}
$url = "https://login.microsoftonline.com/
tenant/oauth2/v2.0/token"
$token = (Invoke-RestMethod -Uri $url -Method
POST -Body $body).access_token
$headers = @{ Authorization = "Bearer $token"
}
$users = Invoke-RestMethod -Uri "https://
graph.microsoft.com/v1.0/users" -Headers
$headers
```

+ Ei moduuleja
- Manuaalinen refresh

Legacy-ympäristöt, yksinkertaiset skriptit

📦 Connect-MgGraph (SDK)

Microsoft Graph PowerShell SDK. Automaattinen token-hallinta.

```powershell
Connect-MgGraph
$users = Get-MgUser -All
$users | Select-Object DisplayName, Mail
```

+ Auto refresh
- Vaatii moduulin

Päivittäinen hallinta, monimutkaiset skriptit

☁️ Managed Identity

Azuren hallittu identiteetti. Ei salaisuuksia koodissa.

```powershell
Connect-MgGraph -Identity
$users = Get-MgUser -All
$users | Select-Object DisplayName, Mail
```

+ Ei salaisuuksia
- Vain Azuressa

Azure Automation, Functions, Runbooks

Livedemoja

Graph API -automaatioideoita

Helppo

Yksinkertaiset yksinkertaiset kyselyt, ei tarvetta virhehallinnalle

- Laitteiden synkronointi massana
- Ownership-tyypin muutos massana
- Salausavainten vaihtaminen
- Sertifikaattien ja konnektorien valvonta
- Laitteiden massauudelleennimeys
- Verkkokorttien MAC-osoitteiden keräys
- Palautusavaimien olemassaolon varmistus
- Autopilot-laitteiden Userless Enrollment salliminen

Keskivaikea

Useita API-kutsuja, virheenhallinta, dataa pitää manipuloida

- Primary userin automaattinen päivitys kirjautumistietojen perusteella
- Assigmenttien muokkaus API:lla
- Autopilot-laitteiden massatuonti
- Bitlocker & Filevault palautusavaimien varmuuskopiointi
- Laiteajureiden massavapautus
- Autopilot-laitteiden poisto massana
- Laitteiden poisto Entrasta, Intunesta ja Autopilotista sarjanumerolla

Vaikea

Monimutkaiset työnkulut

- Intune-konfiguraatioiden varmuuskopiointi
- Ajuripäivitysten hallinta laitemallikohtaisesti
- Sovellusten automatisoitu tuonti
- Configuraatioiden massatuonti
- Käyttäjäryhmästä laiteryhmäksi synkronointi
- Windows-päivityksien seuranta

Kiitos ja kumarrus