#htmdcommunity

@htmdcommunity

HTMD Community Conference - 2024

Thank You Sponsors!

Microsoft

PATCH MY PC

ZERO TOUCH

nerdio

Speaker

Saurabh Sarkar

Microsoft Intune CAT Product Manager

linkedin.com/in/saurabh-sarkar-3ab7758a/

aka.ms/intunevideos

Certificate Deployment Options via Intune:

Understanding On-Prem NDES and Cloud PKI

Speaker

Snehasis Pani

Specialist – Cloud and Infrastructure Services

linkedin.com/in/snehasis-pani-980076201

@SnehasisPani

Certificate Deployment Options via Intune:

Understanding On-Prem NDES and Cloud PKI

AGENDA

- Certificates: Background/Need/Advantages
- Relevant Certificate Types
- Brief of on-prem NDES
- Flow of SCEP cert via on-prem NDES
- Issues with on-prem PKI and Top asks
- Cloud PKI: Background, Advantages and Comparison
- Flow of SCEP certificate via Cloud PKI
- Cloud PKI Architecture
- High level features of Cloud PKI

Certificates: Background/Need/Advantages

For any user to access any application, he must go through 2 phase-Authentication phase and Authorization phase.

Authentication phase- User's authenticity is checked (if the user is, who he claims to be)

Authorization Phase- User is subjected to some conditions and depending on the output we determine whether the user should be given access or not.

Conventionally authentication may that be to an App,Wifi,Vpn etc is done by username/password.

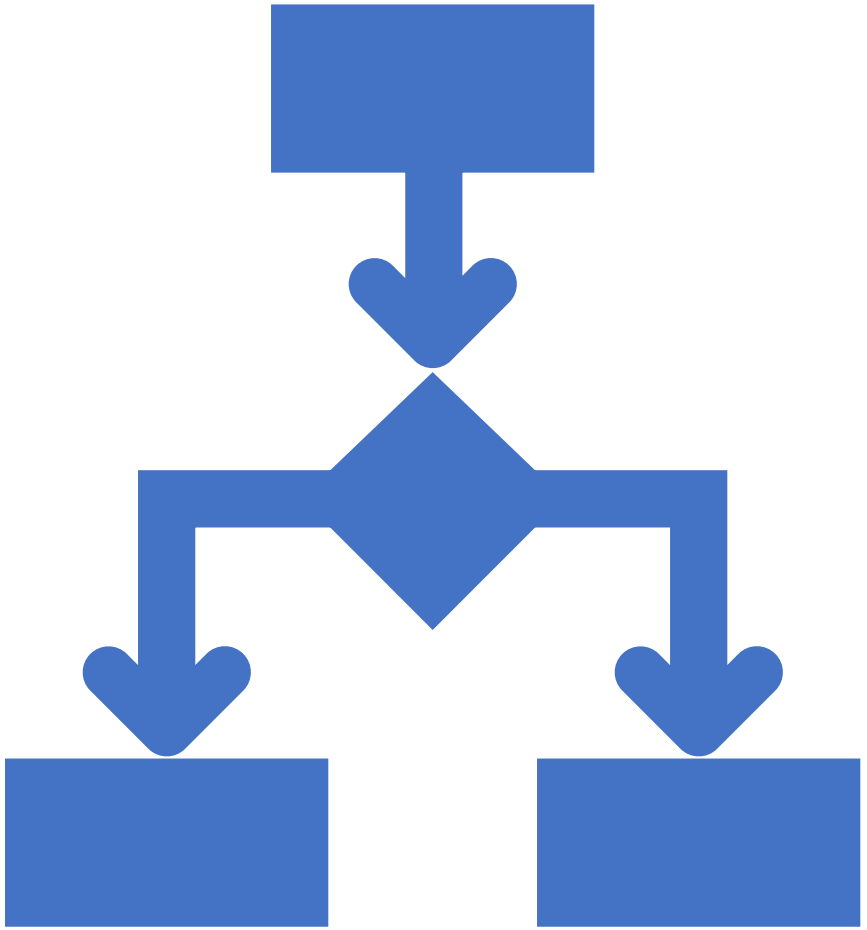
To make this more seamless we introduced the concept of using a certificate for facilitating the authentication. Certificates are the best phishing-resistant credentials that can be used to improve security.

Using a certificates for authentication has the below benefits over using username/password:

Seamless and Automated authentication	Removes the overhead for the user to enter the username/password manually	More secured than passwords which are prone to leakage.

Relevant Certificate Types

- Trusted Root Certs- Self Signed. Topmost in the tree
- Intermediate Certs-> Subordinate CA. Issued by the Root
- Client Certs- Leaf Certificate
  - SCEP and PKCS
- Server Certs- Identify a service



Brief Of On-Prem NDES

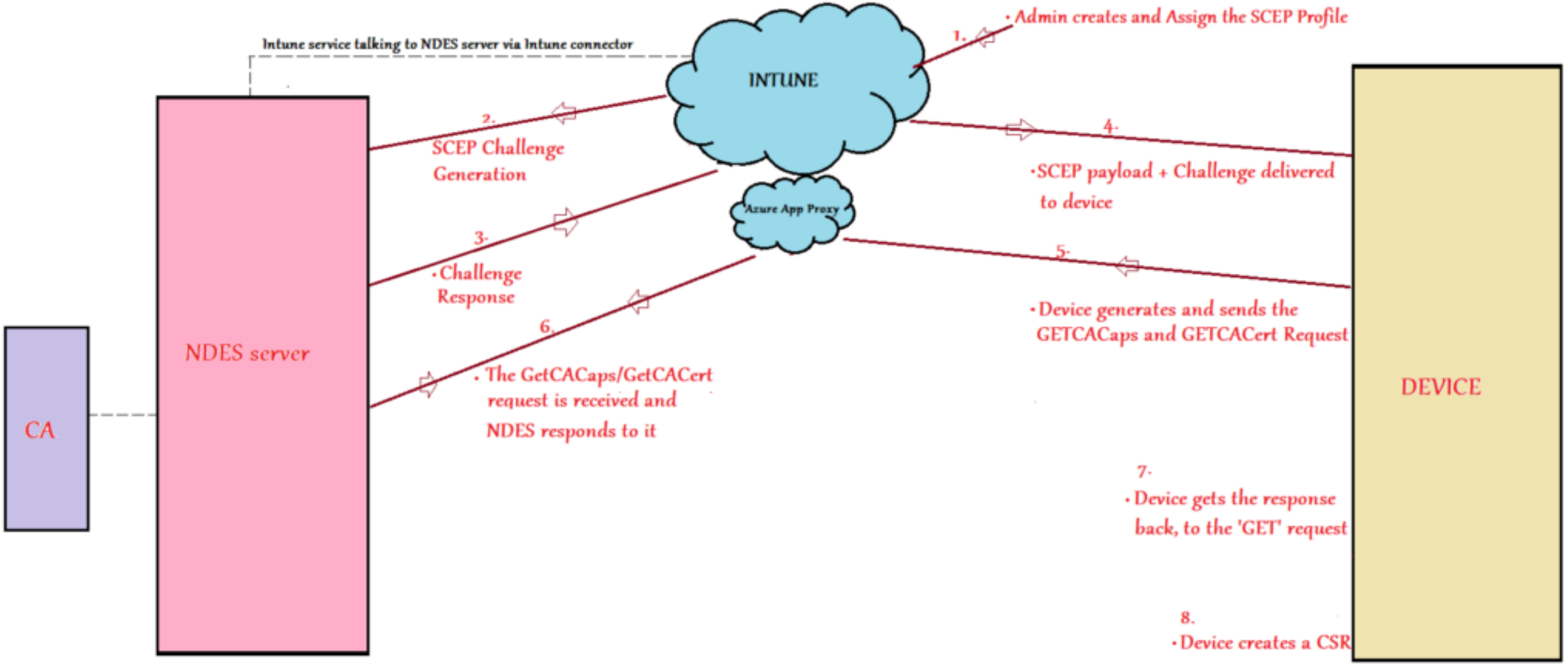
THIS IS A CONVENTIONAL WAY OF DISTRIBUTING SCEP CERTIFICATES TO DEVICES.

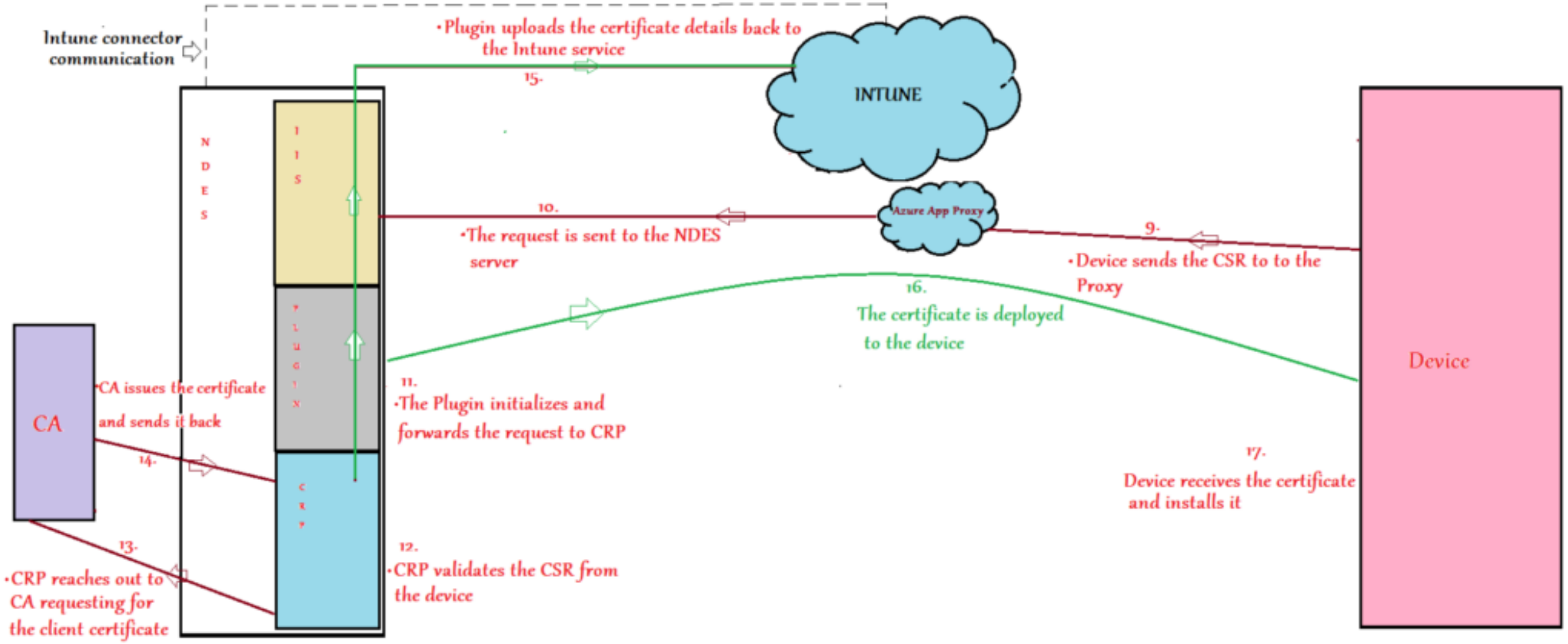
THE DEVICES CAN REACHOUT TO THE NDES SERVER WHICH IN TURN GOES TO THE ISSUING CA AND GRABS THE CERTIFICATE ON USER'S BEHALF.

THE NDES SERVER IS BINDED WITH THE CA HENCE BOTH NEED TO BE IN THE SAME ON-PREM DOMAIN

AS DEVICES REACHOUT TO THE NDES SERVER OVER THE INTERNET, THE NDES NEEDS TO BE PUBLICLY AVAILABLE

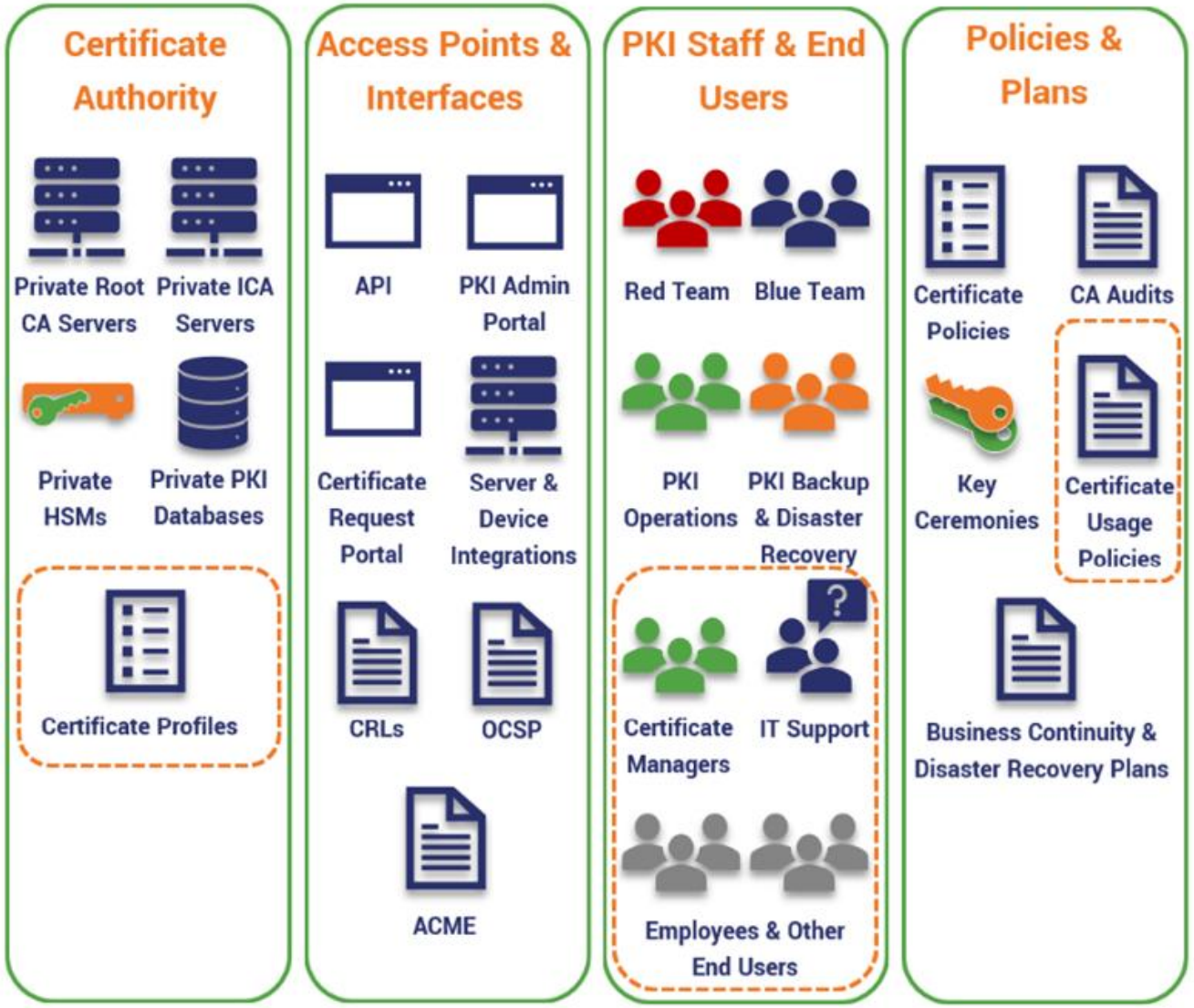
TO ACHIEVE THIS, THE ON-PREM NDES IS FRONT ENDED BY AN APP PROXY WHICH ROUTES THE TRAFFIC FROM INTERNET TO THE NDES


Intune service talking to NDES server via Intune connector
INTUNE
Azure App Proxy
NDES server
CA
DEVICE
1. • Admin creates and Assign the SCEP Profile
2. SCEP Challenge Generation
3. • Challenge Response
4. • SCEP payload + Challenge delivered to device
5. • Device generates and sends the GETCACaps and GETCACert Request
6. • The GetCACaps/GetCACert request is received and NDES responds to it
7. • Device gets the response back, to the 'GET' request
8. • Device creates a CSR


Intune connector communication
•Plugin uploads the certificate details back to the Intune service
15.
INTUNE
NDES
IIS
Plugin
CRP
10.
•The request is sent to the NDES server
Azure App Proxy
9.
•Device sends the CSR to to the Proxy
16.
The certificate is deployed to the device
Device
CA
•CA issues the certificate and sends it back
14.
11.
•The Plugin initializes and forwards the request to CRP
17.
Device receives the certificate and installs it
13.
•CRP reaches out to CA requesting for the client certificate
12.
•CRP validates the CSR from the device

PKIs are complex and costly

- **High OPS cost**
  - ✓ Dedicated servers (HA/DR, CRLs, NDES, HSM)
  - ✓ Ongoing maintenance
  - ✓ Dedicated staff
- **New deployments or additions require…**
  - ✓ Lots of coordination across an organization: Server infrastructure, Identity, networking, security, desktop & mobile teams, engineering and support teams across the board.
- **Requires deep knowledge to set up, secure, maintain**



Top 5 Asks

- Ease of use - reduce complexity (NDES too complex)
- Reduce management and OPS related costs
- Manage the cert lifecycle
  - Validity period, Issue, renewal, expire, revoke
- Monitoring & reporting
  - Issued certs validity period, expired, revoked
  - Warnings / notifications for certs about to expire (lifetime)
- RBAC support

Microsoft Intune Suite

Microsoft integrated value

Remote Help

Tunnel for Mobile App Management

Advanced app management

Endpoint Privilege Management

Cloud-based certificate management

Advanced endpoint analytics

Microsoft Edge

Microsoft Windows

Microsoft Teams

Microsoft 365 Apps

Microsoft Graph

Microsoft Entra

Microsoft Defender for Business

Simplicity | Security | Savings

Intune suite and Cloud PKI

Capability	Standalone add-on	Intune Plan 2	Intune Suite
Endpoint Privilege Management	✔		✔
Enterprise App Management	✔		✔
Advanced Analytics	✔		✔
Remote Help	✔		✔
Microsoft Tunnel for Mobile Application Management		✔	✔
Microsoft Cloud PKI	✔		✔
Firmware-over-the-air update		✔	✔
Specialized devices management		✔	✔

Cloud PKI Background

- Microsoft announced Cloud PKI as an upcoming offering in August 2023.
- In March 2024 Cloud PKI became Generally Available for usage which will let us manages the full lifecycle of issued certificates for Intune managed device.
- Traditionally admins had an option of doing this via on-prem NDES server which was cumbersome to setup and troubleshoot.

Brief of Cloud PKI

01

Using Microsoft Cloud PKI organizations can simplify their certificate management with minimal effort.

02

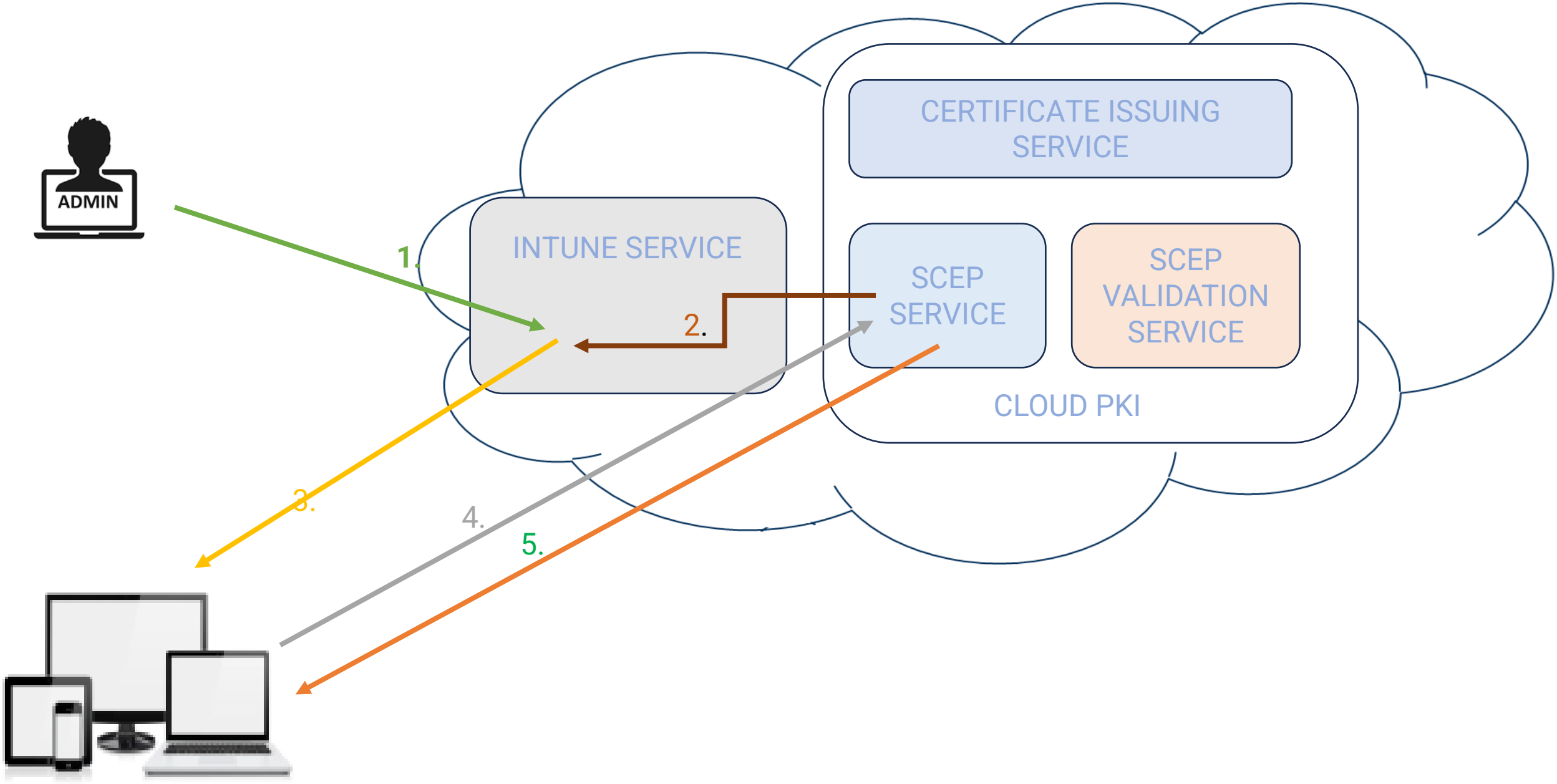
The overhead of managing and maintaining an on-prem CA is removed/reduced using the SaaS based certificate registration authority which is hosted in Azure on behalf of the customer

03

As the service is hosted in Azure, its Highly Available and we don't have to worry about its load balancing

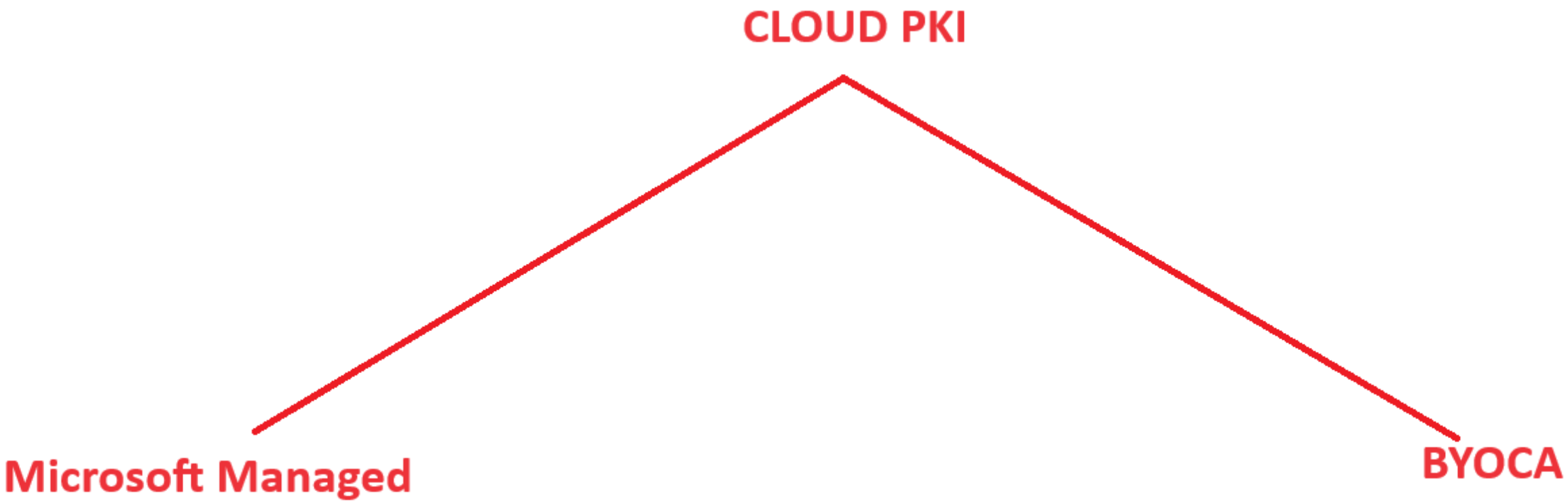
Comparison/Benefits of CPKI

CRITERIA	***On-Prem NDES***	***Microsoft Cloud PKI***
Manageability (Components to be managed)	**Management is difficult– NDES server, Issuing/Root CA, App Proxy, Intune Connector**	**Management is easy– Nothing is needed to be managed on-prem**
Deployment	**Deployment is complex**	**Deployment is straight forward**
Load Balancing/Redundancy	**We need to spin up multiple NDES instances on-prem**	**As its SaaS on Azure, its Highly Available hence LB is not needed**
Supported Devices and Certificates	**Can be used to supply certs to all kinds of devices. Also, we can issue almost all kinds of certs**	**(As of now) can supply certs to Intune Managed devices only. Also, only Client authentication certs can be issued. SSL certs/SMIME cannot be issued as of now.**
Control (over attributes)	**We have more granular control/customization available**	**Less granular control/selection available**
Cost	**No additional licensing cost except cost of managing the NDES server**	**Extra licensing cost – 2$/user/month**
Troubleshooting	**As many components are on-prem, customer can check and troubleshoot them at his end.**	**Not much of troubleshooting can be/(has to be) done at customer's end due to components in SaaS**


ADMIN
1.
INTUNE SERVICE
2.
CERTIFICATE ISSUING SERVICE
SCEP SERVICE
SCEP VALIDATION SERVICE
CLOUD PKI
3.
4.
5.

CPKI Architecture

Note: We can have a maximum of 6 CAs in Cloud PKI



Details

Create 2-tier PKI hierarchy

Root, issuing CA in the cloud

Support Bring Your Own CA (BYOCA)

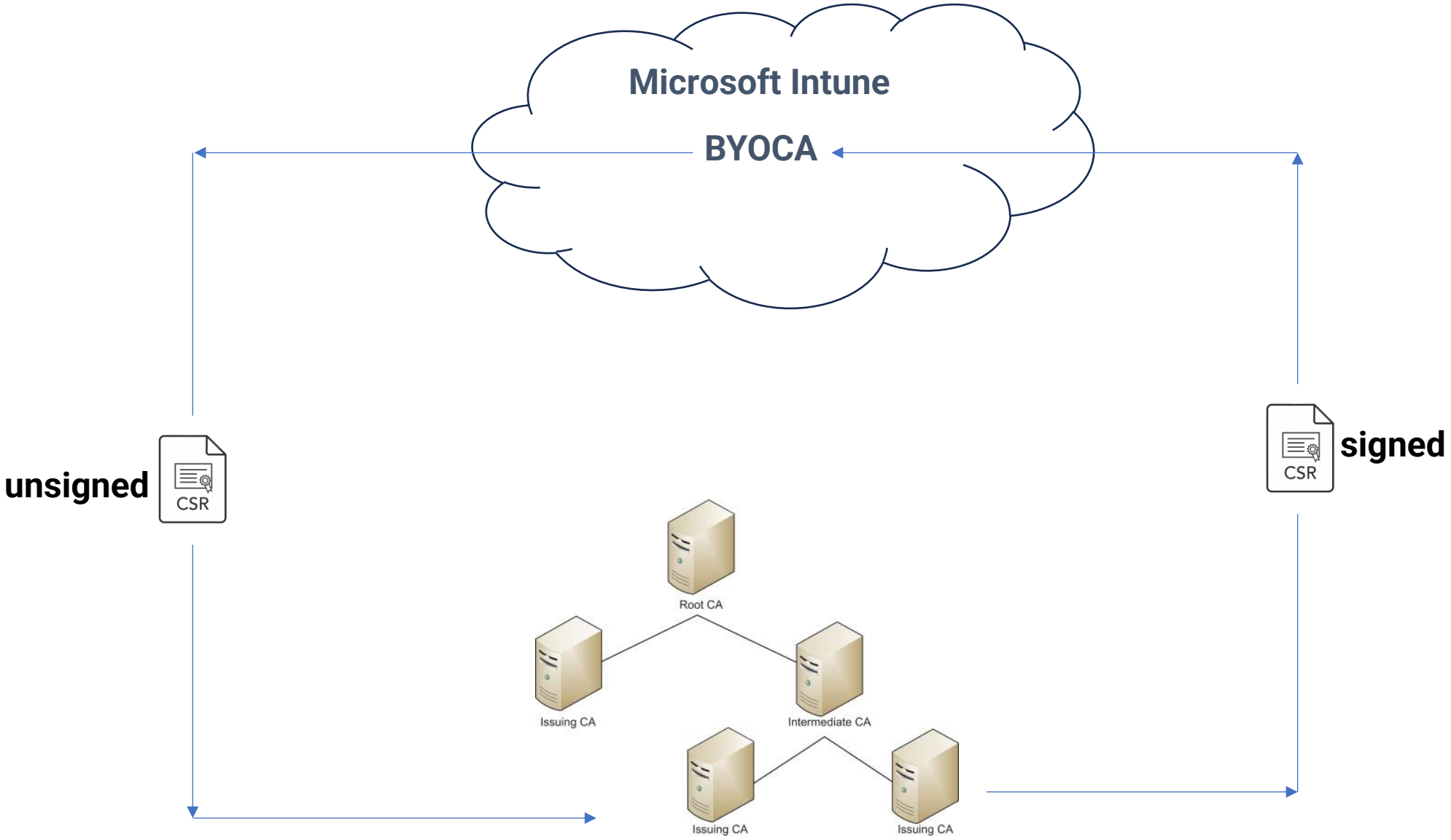
Anchor Intune issuing CA to a private CA

Signing and encryption algorithms | RSA

RSA Key sizes – 2048, 3072, 4096

Hash algorithms – SHA-256, SHA-384, SHA-512

Any Purpose Eku not supported


Microsoft Intune
BYOCA
unsigned
CSR
signed
CSR
Root CA
Issuing CA
Intermediate CA
Issuing CA
Issuing CA

CPKI Feature Summary

Issue certificates for Intune-managed devices

- Platforms: Windows, iOS, macOS, Android
- Provide a certificate registration authority to deploy certificates (SCEP)
- Automatically deploy certificates to Intune-managed devices

Monitor and reporting

- Dashboard metrics (issued, revoked, expired certificates)
- Detailed reports for issued certificates (users, devices, policy)

Manage issued certificates

- Support automatic and manual certificate revocation
- Remove certificates from devices (retire, delete, wipe)

Certificate-Based Authentication (CBA)

- Support current scenarios (Wi-Fi, VPN, applications)

CPKI Feature Details

Create certification authorities per Intune tenant

- Create 2-tier PKI hierarchy
  - Root, issuing CA in the cloud
- Support Bring Your Own CA (BYOCA)
  - Anchor Intune issuing CA to a private CA
- Signing and encryption algorithms | RSA
  - RSA Key sizes – 2048, 3072, 4096
- Hash algorithms – SHA-256, SHA-384, SHA-512
- Providing a Cloud Certificate Registration Authority (SCEP) service per issuing CA
- CRL distribution points

End-entity (leaf) certificate issuance

- Protocol/Cert format – SCEP (PKCS#7)
- Platforms: Intune-enrolled devices on iOS, Android, Mac, and Windows

Certificate life cycle management

- Automatic and manual certificate revocation

Reporting/Dashboard

- Issuing CA summary (issued, expired, revoked) and detailed information about issued certificates

Audit

- Admin actions performed on the CA (i.e., create, disable, delete, renew, revoke)

RBAC permissions and scope tags

EverythingAboutIntune

@everythingaboutintune1713 · 4.85K subscribers · 37 videos

This channel aims to educate everyone on Intune- Microsoft's MDM solution on the Azure ...more

facebook.com/saurav.sarkar.7399

Customize channel | Manage videos

Detailed Video:
aka.ms/intunevideos

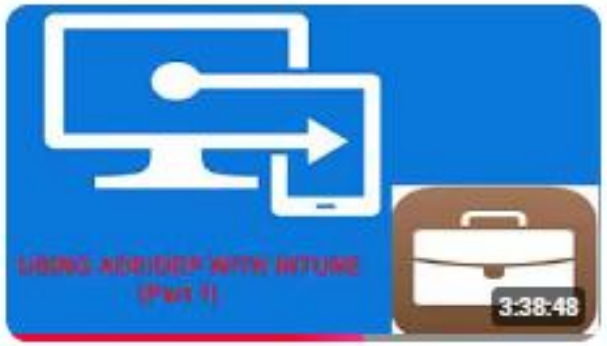
Detailed Blog:
https://everythingaboutintune.com/

Home | Videos | Playlists | Community

Latest | Popular | Oldest

IntuneNugget 40- Microsoft Cloud PKI and SCEP: Understanding Background Flow an...

1.7K views · 7 months ago



#IntuneNugget 39- Using ADE/DEP with Intune (Part 1)

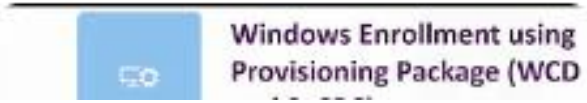
3.4K views · 10 months ago

#IntuneNugget 38- Load Balancing NDES and SCEP via Intune

1.2K views · 1 year ago

#IntuneNugget 37- Using SCEP and NDES with Intune- Demystified and Simplified.

3.4K views · 1 year ago




THANK
YOU