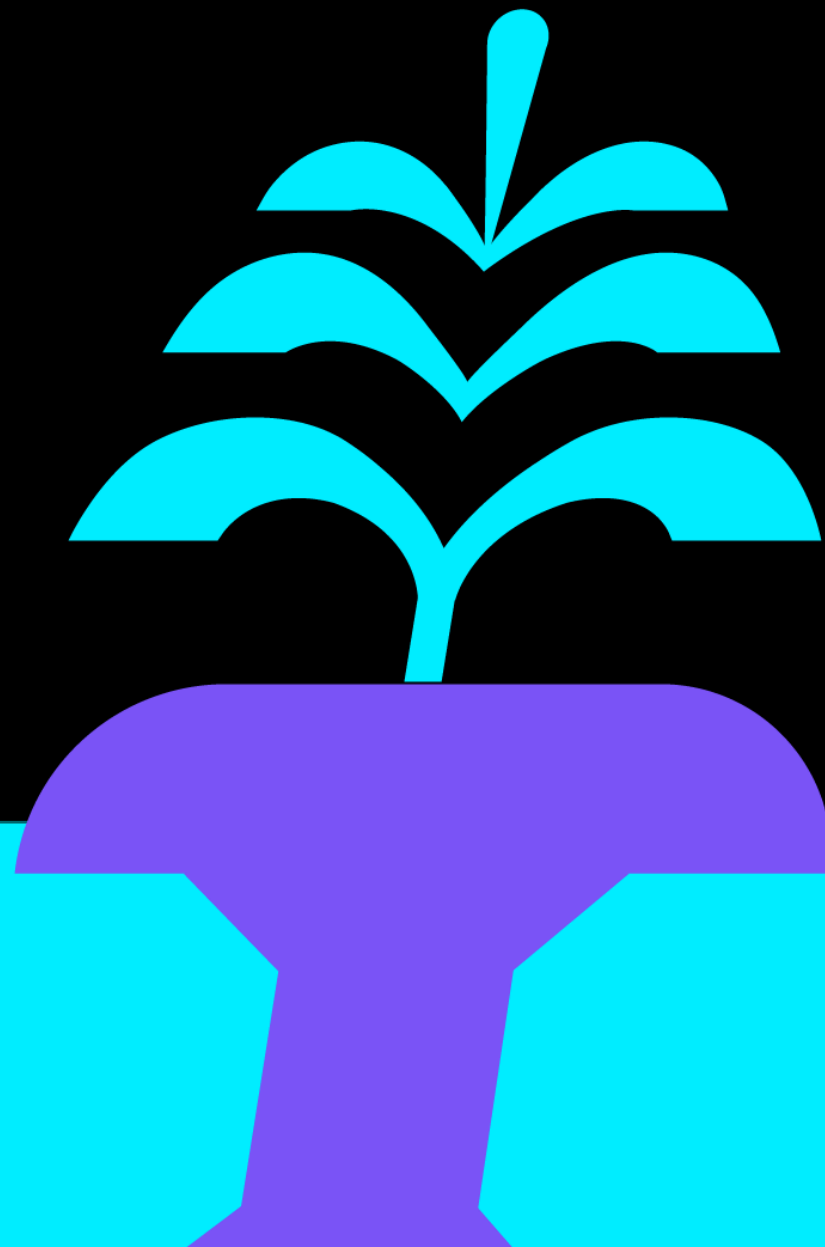




HYBRID
IDENTITY
PROTECTION
conf26

FRANKFURT

**Deep-dive to Entra ID Token
Theft Protection**



Contents

- Token based authentication attacks
- Token Theft attacks
- Conditional Access Policies
- Token Protection
- Continuous Access Evaluation (CAE)

Who am I?

- Dr Nestori Syynimaa (DrAzureAD)
- Principal Identity Security Researcher
- Microsoft Cloud, Application, and Identity Research (CAIR)

nsyynimaa@microsoft.com

@DrAzureAD



@DrAzureAD

NON-U.S. TOUR 2025

Feb 14	Disobey	Helsinki, FIN
Jun 26	TROOPERS	Heidelberg, GER
Sep 4	Cloud Identity Summit	Dortmund, GER
Sep 5	OrangeCon	Amsterdam, NED
Sep 17-19	MCTTP	München, GER
Sep 25-26	BruCon	Mechelen, BEL
Sep 27	RomHack	Rome, ITA
Oct 1-2	SecTor	Toronto, CAN

Sep 17-19 - MCTTP

Feb 14 - Disobey

Sep 27





Working on updates 0% complete.
Don't turn off your PC. This will take a while.

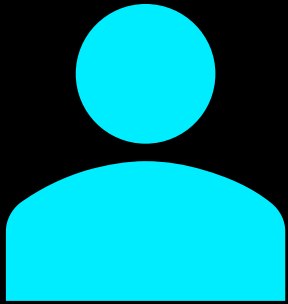
Your PC will restart several times.

Token based authentication attacks



Key concepts of token-based authentication

- Consumes services



User



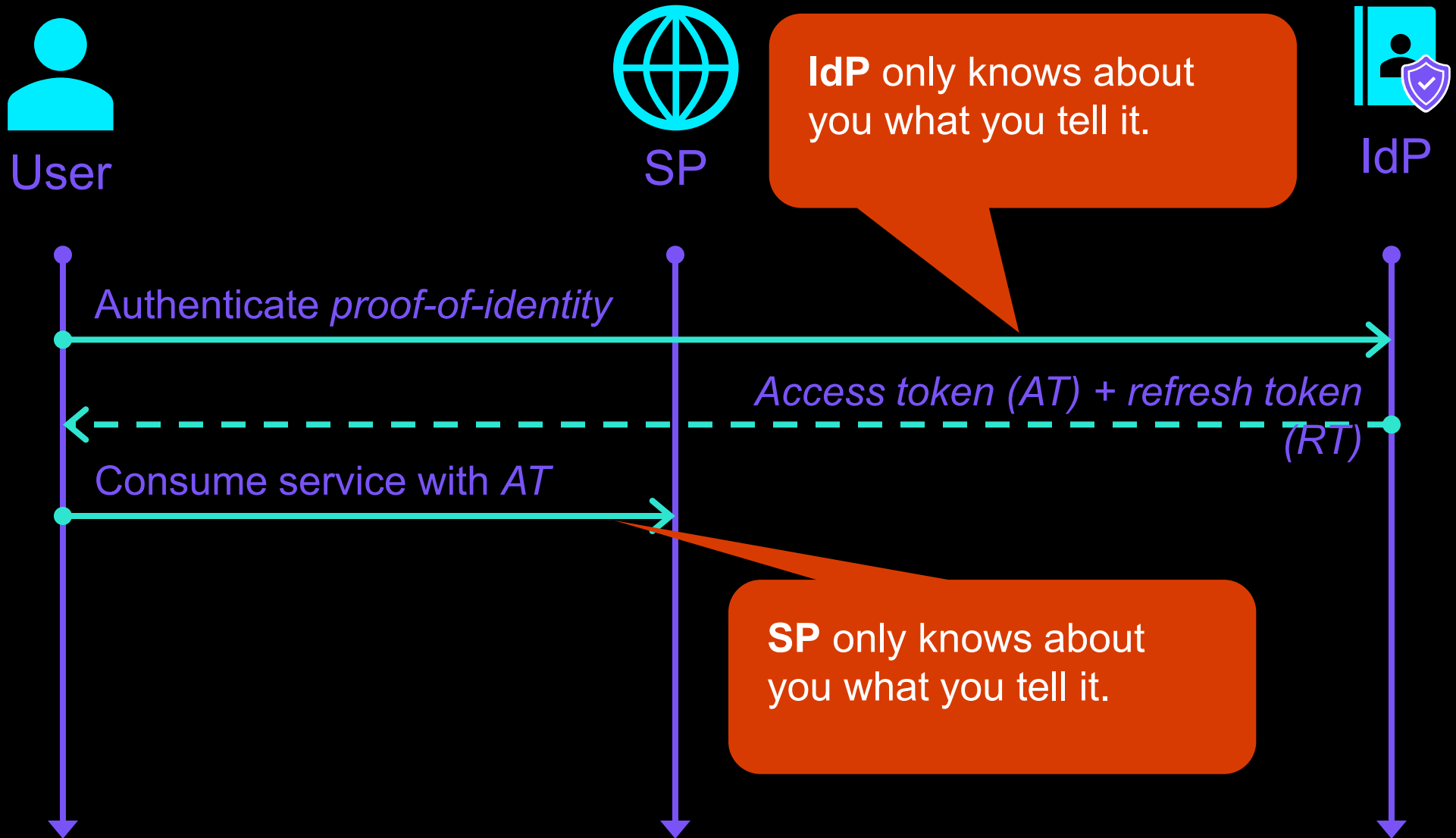
Service Provider
(SP)



Identity Provider
(IdP)

- Provides services
- Provides identity and access management

How the cloud works





Hackers don't break in, they log in

Corey Nachreiner
CSO, WatchGuard

Identity attacks in perspective

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.



<1% of attacks



Less than 1% combined



MFA attacks

- SIM swapping
- MFA fatigue
- AitM

End-run MFA protection by intercepting security codes using stolen phone numbers, barraging users with MFA notifications until they approve, and capturing first and second factor credentials using fake replicas of legitimate websites.



Post-authentication attacks

- Token theft
- Consent phishing

Infiltrate a user's account after they authenticate by stealing a legitimate token created on their device and moving it to a device under the attacker's control, by searching source code repositories for Open Authorization (OAuth) tokens and other non-human credentials, or by tricking the authenticated user into granting permissions to malicious apps.



Infrastructure compromise

Often silently executed by professional groups or nation-state-backed threat actors with sophisticated operations, making them very hard to detect. Threat actors may compromise an on-premises federation server and copy its private signing key to forge tokens, compromise a privileged cloud user and add new federation contracts, or compromise a non-human workload identity and create new credentials with elevated privileges.

Source: Microsoft Threat Intelligence

Identity attacks in perspective

More than **97%**
of identity attacks are
password spray or
brute force attacks

Less than 3%
of attacks are...

(A) Token theft by malware

2.4042%

(B) AiTM

0.2375%

(C) Infrastructure

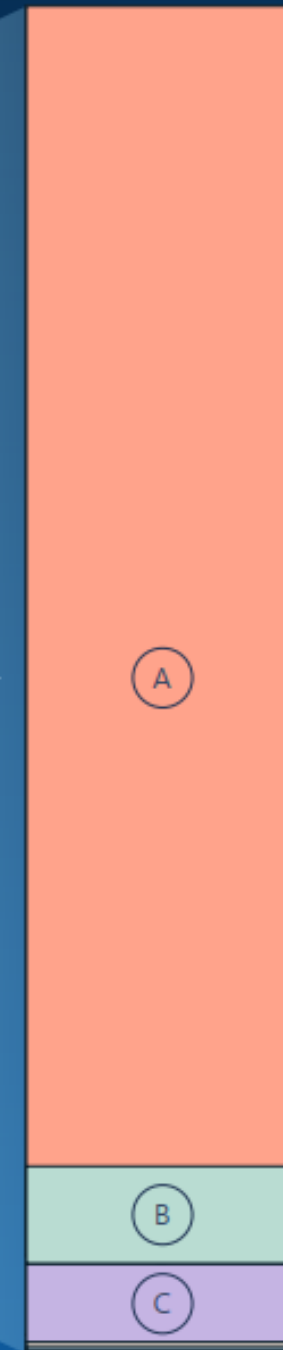
0.1692%

(D) Attacks on MFA

0.0033%

(E) Consent phishing

0.0005%



Source: Microsoft Defender XDR and Entra ID Protection alerts (April-June 2025)

<https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/>



Biggest problem with network defense is that defenders think in lists. Attackers think in graphs.

As long as this is true, attackers win.

John Lambert

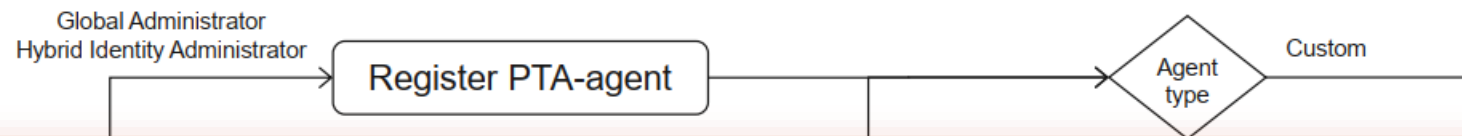
Corporate Vice President, Security Fellow, Microsoft

Exploring Attack Paths Using Graph Theory

Case: Microsoft Entra ID Pass-Through Authentication

Nestori Syynimaa 

Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland



So my first question is: where is there graph theory or attack graphs in this paper?

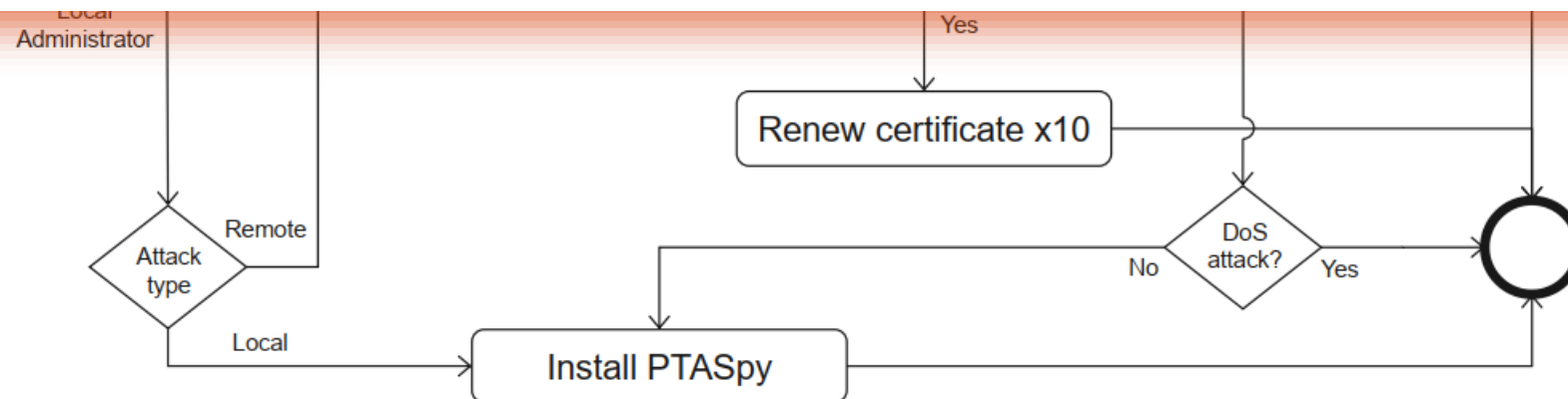


Figure 13. PTA Attack Graph v2

Token-based authentication attack graph

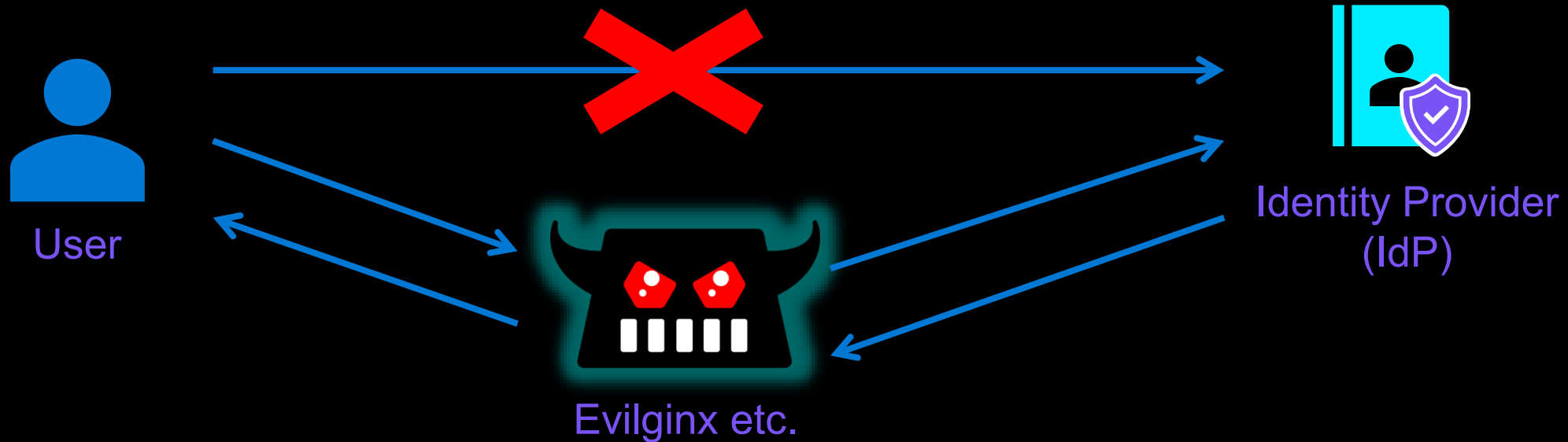


Token Theft



~~Man-in-the-Middle (MitM)~~ Adversary-in-the-Middle (AitM)

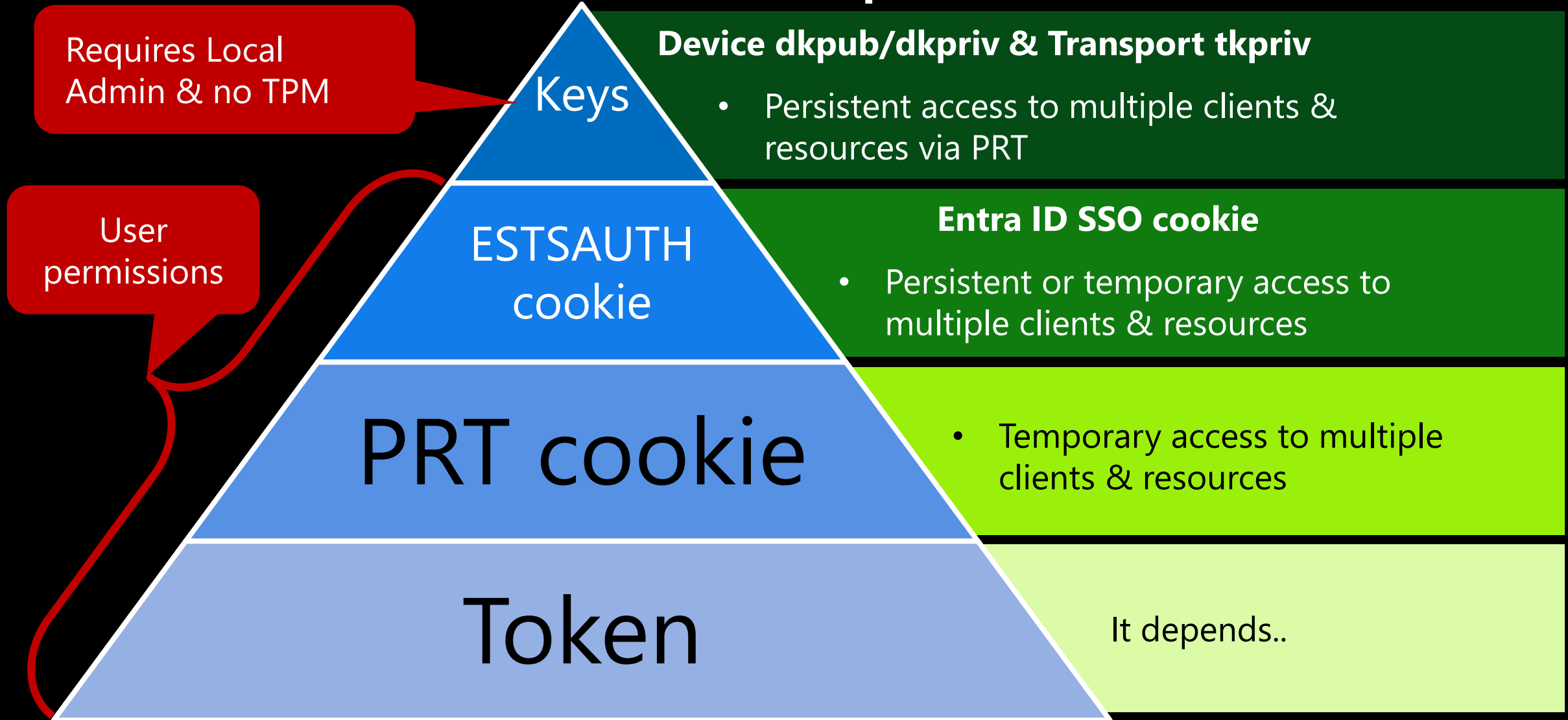
- An attack where the **adversary positions himself in between** the **user** and the **system** so that he can intercept and alter data traveling between them.¹



Demo



What to steal from user's endpoint?



Which token to steal?

Requires Local
Admin & user creds
& no TPM

PRT

Primary Refresh Token (+session key)

90 d

- Persistent access to multiple clients & resources

User
permissions

FRT

Family Of Client IDs (FOCI) Refresh Token **90 d**

- Persistent access to FOCI clients & multiple resources

Refresh Token

90 d

- Persistent access to single client & multiple resources

Access / ID token

1-28 h

- Temporary access to single client & resource

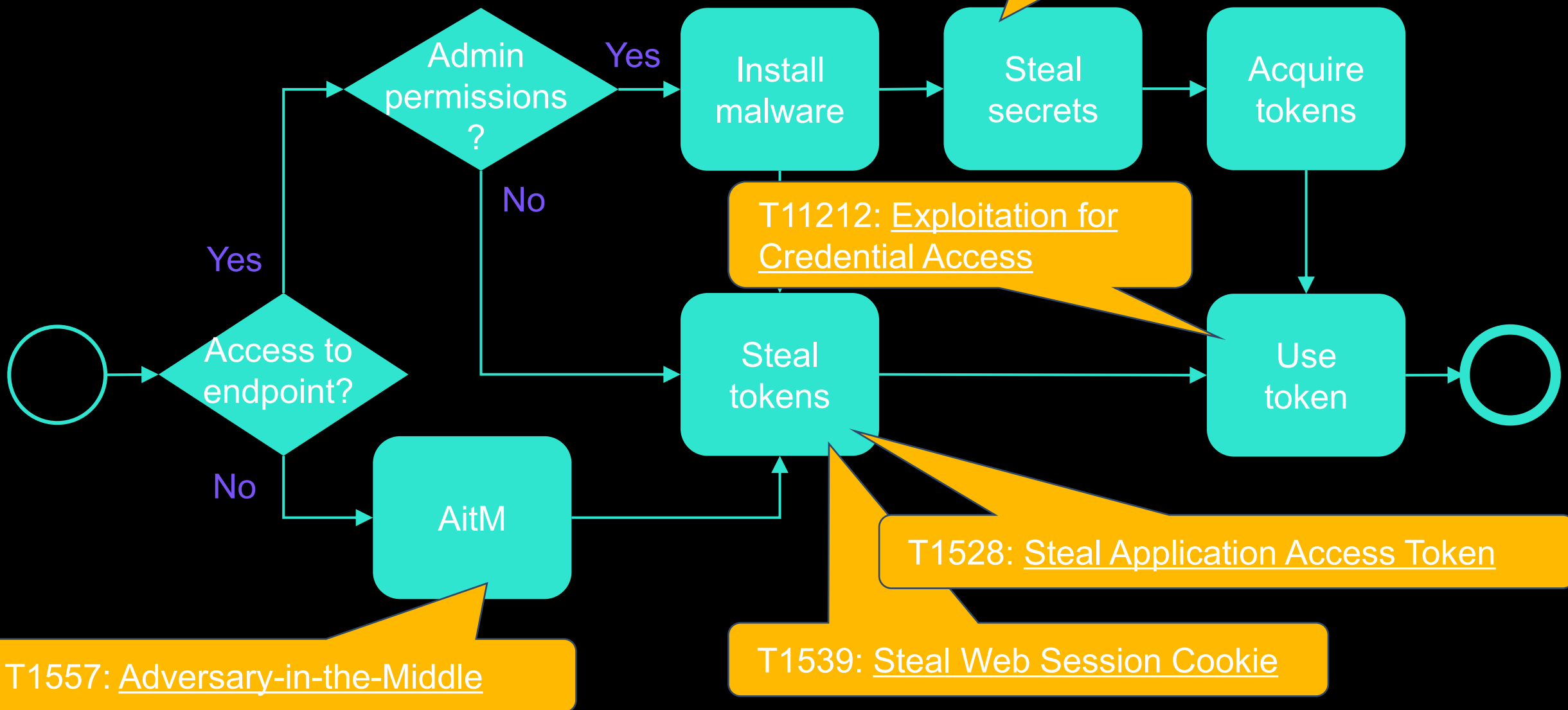
Demo



HYBRID
IDENTITY
PROTECTION
conf26



Token Theft attack graph



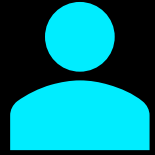
Token security best practices

- **Conditional Access Policies:** Use Conditional Access policies to enforce compliant network checks. **This ensures that tokens are only used from trusted networks and devices.**
- **Token Binding:** Implement Token Protection (formerly known as token binding) to cryptographically tie tokens to client secrets. **This prevents token replay attacks from different devices.**
- **Continuous Access Evaluation (CAE):** Implement CAE to **continuously evaluate the security state of the session**. This helps in detecting and revoking tokens if there are changes in the user's security posture, such as network location changes.

Conditional Access Policies (CAP)



How CAP works?



User

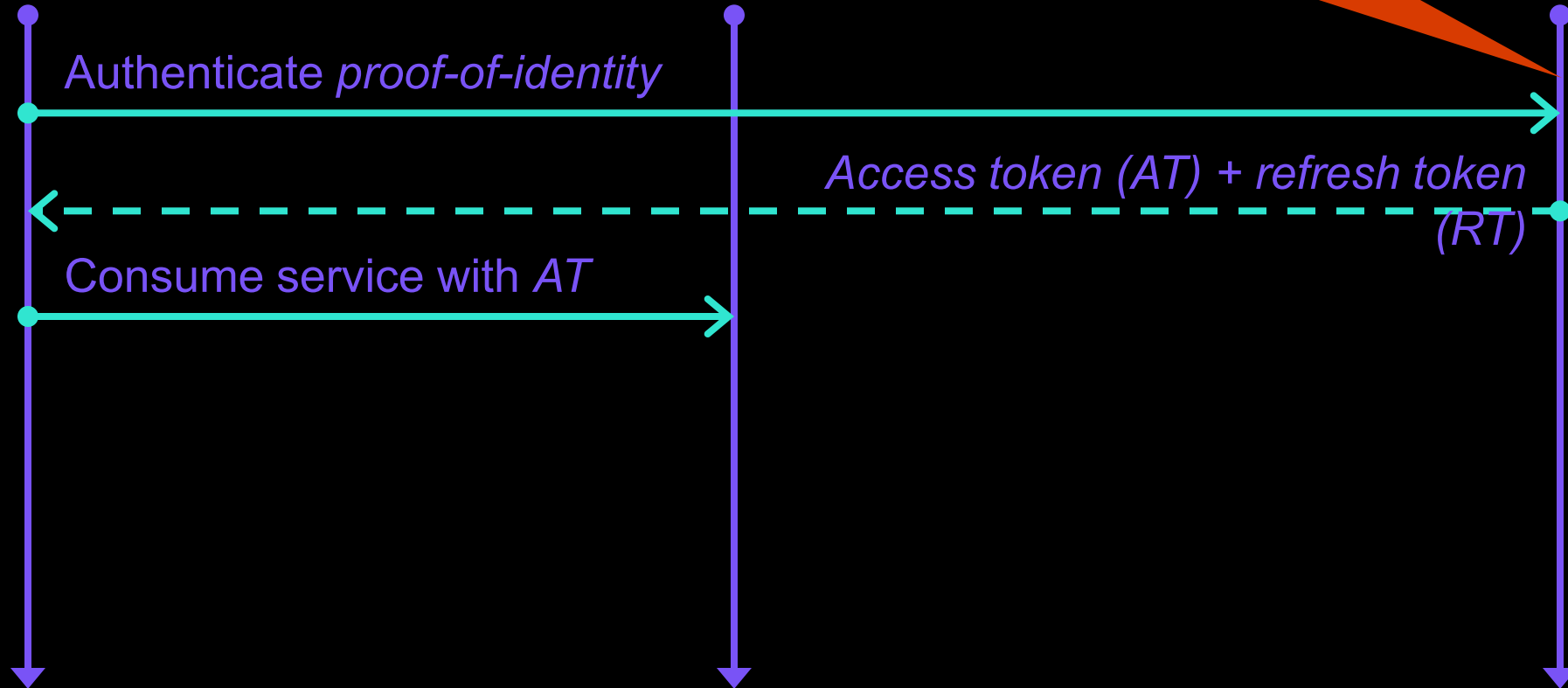


SP

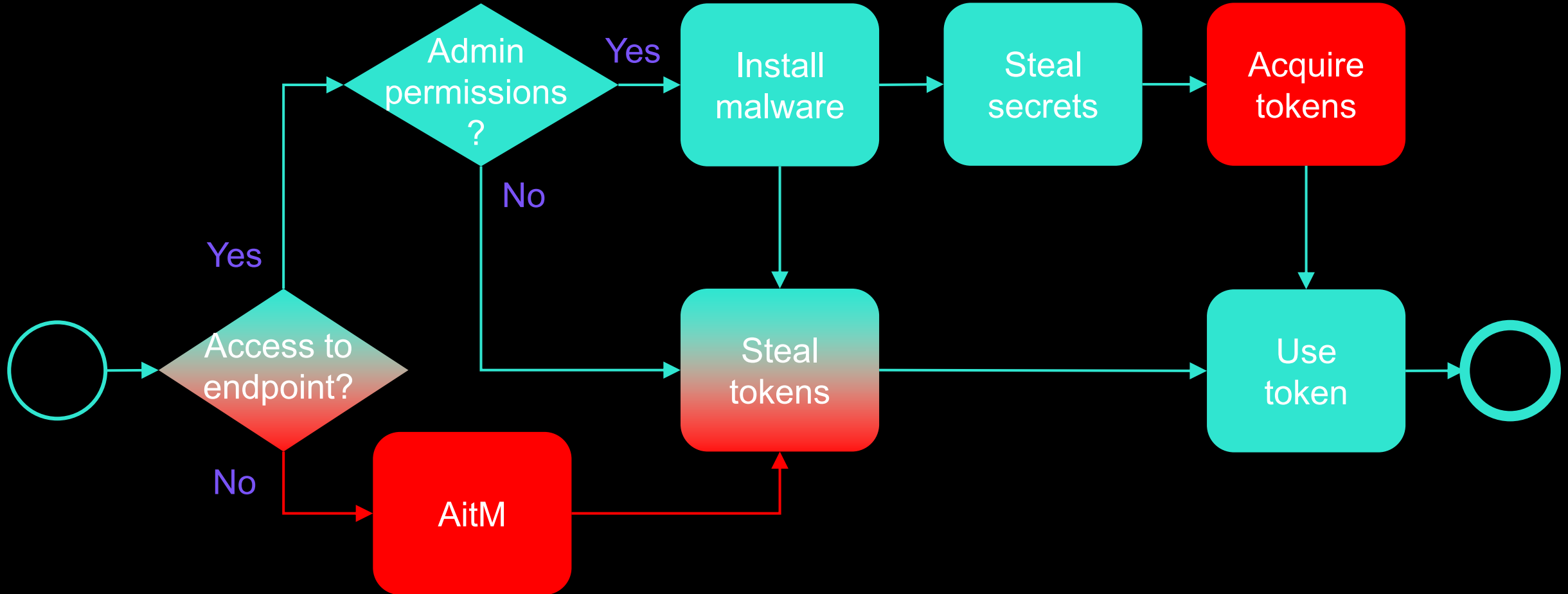


IdP

CAPs evaluated.
Access allowed or
denied. MFA etc. may be
required.



CAP *may* protect against AitM and Acquire token



Demo



Token Protection



Token protection 1/4

- Supports:
 - Office 365 Exchange Online, SharePoint Online, Teams
 - Azure Virtual Desktop
 - Windows 365
- Requirements:
 - Microsoft Entra registered, joined, or hybrid joined Windows 10+ (or hybrid joined WSE 2019+), *preview for MacOS & iOS*
 - Supported native client (OneDrive, Teams, etc.)
 - Entra ID ~~P2~~ P1
- Deployment:
 - Conditional access policy

Token protection 2/4

"Token Protection ensures that tokens can only be used on the intended device. When enforced through Conditional Access policies, tokens authorizing access to resources must come from the device where the user originally signed in. This provides the best available protection for your high-value users and data against breaches involving token theft."

"We're targeting **Refresh Tokens** for protection first as they tend to be longer-lived and more broadly scoped than other types of tokens and are therefore more valuable for an attacker to steal. "

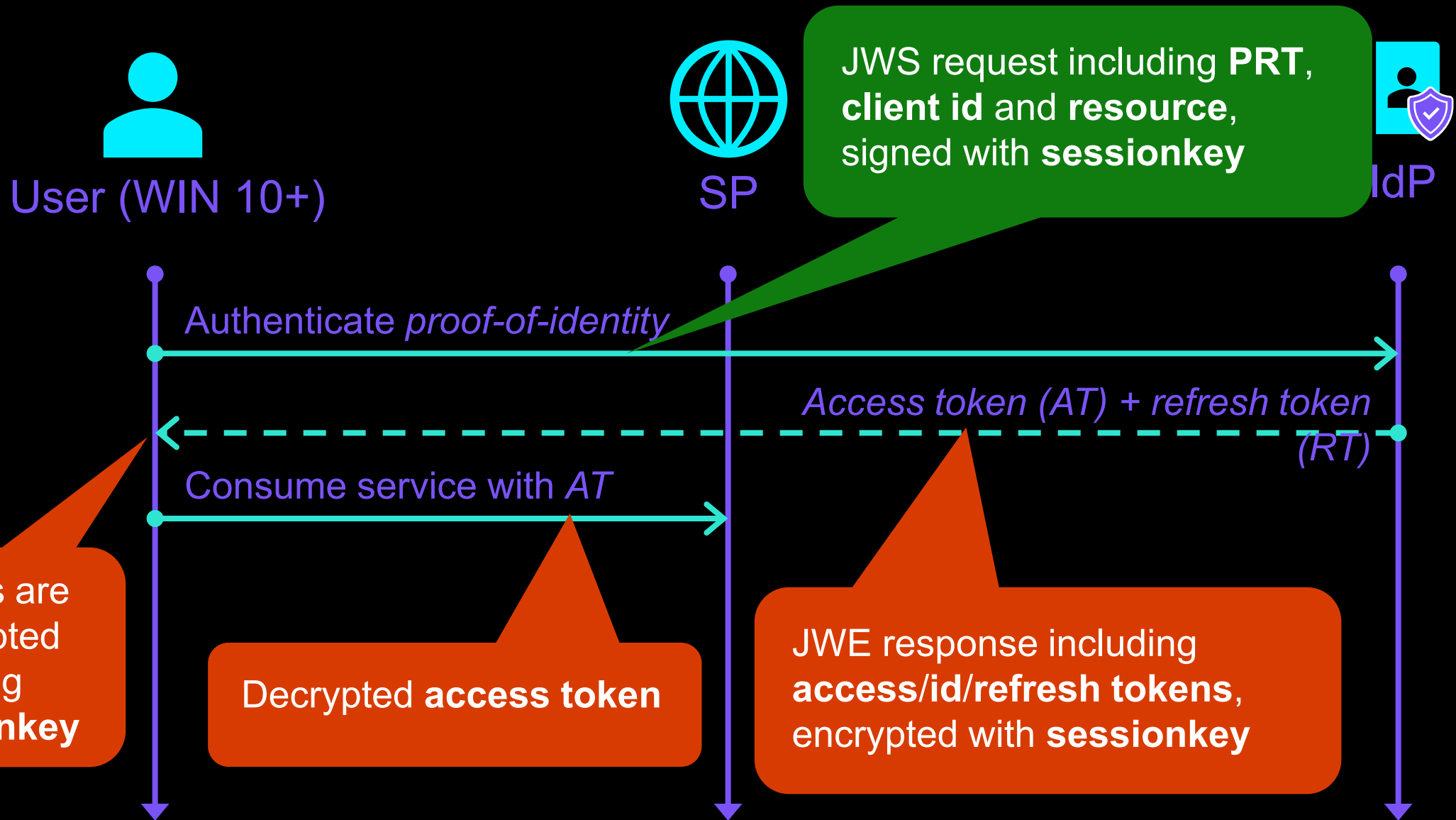
Token Protection 3/4

"A key part of Microsoft's protections against token theft is the use of tokens that are cryptographically tied to the device they own. This is often called **token binding**, but may also be called sender constrained tokens, or token proof of possession. Token protection makes it harder to execute the main types of attacks designed to steal tokens, including network-based attacks and those using malware on the device by restricting use of the stolen token from devices they weren't issued to."

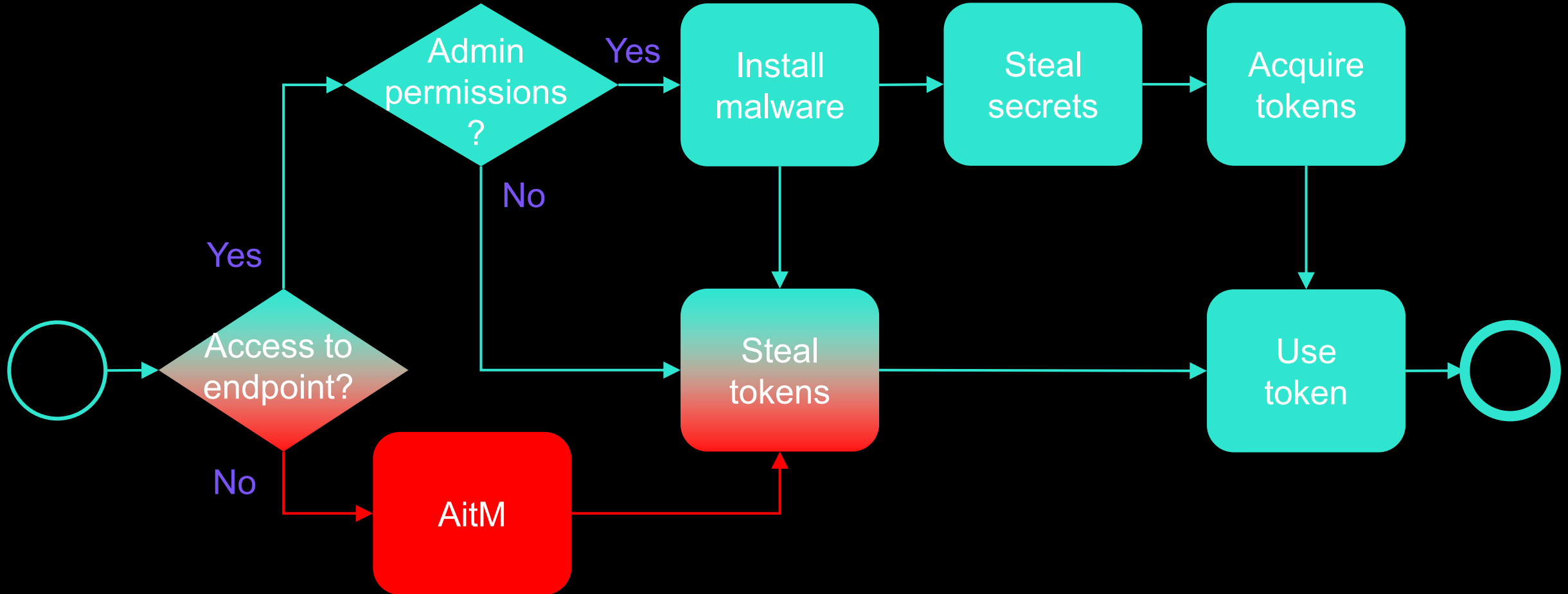
Token Protection 4/4

“Token protection creates a cryptographically secure tie between the token and the device (client secret) it's issued to. Without the client secret, the bound token is useless. When a user registers a Windows 10 or newer device in Microsoft Entra ID, their primary identity is bound to the device. What this means: A policy can ensure that only bound sign-in session (or refresh) tokens, otherwise **known as Primary Refresh Tokens (PRTs)** are used by applications when requesting access to a resource.”

How Token Protection works?



Token Protection prevents AitM attacks



Continuous Access Evaluation (CAE)



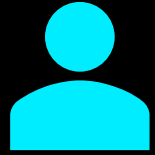
HYBRID
IDENTITY
PROTECTION
conf26



Continuous Access Evaluation

- Supports:
 - Office 365 Exchange Online, SharePoint Online, Teams
- Requirements:
 - Supported client (OneDrive, Teams, custom app etc.)
 - Entra ID P1
- ~~Deployment~~ Customisation:
 - Conditional access policy

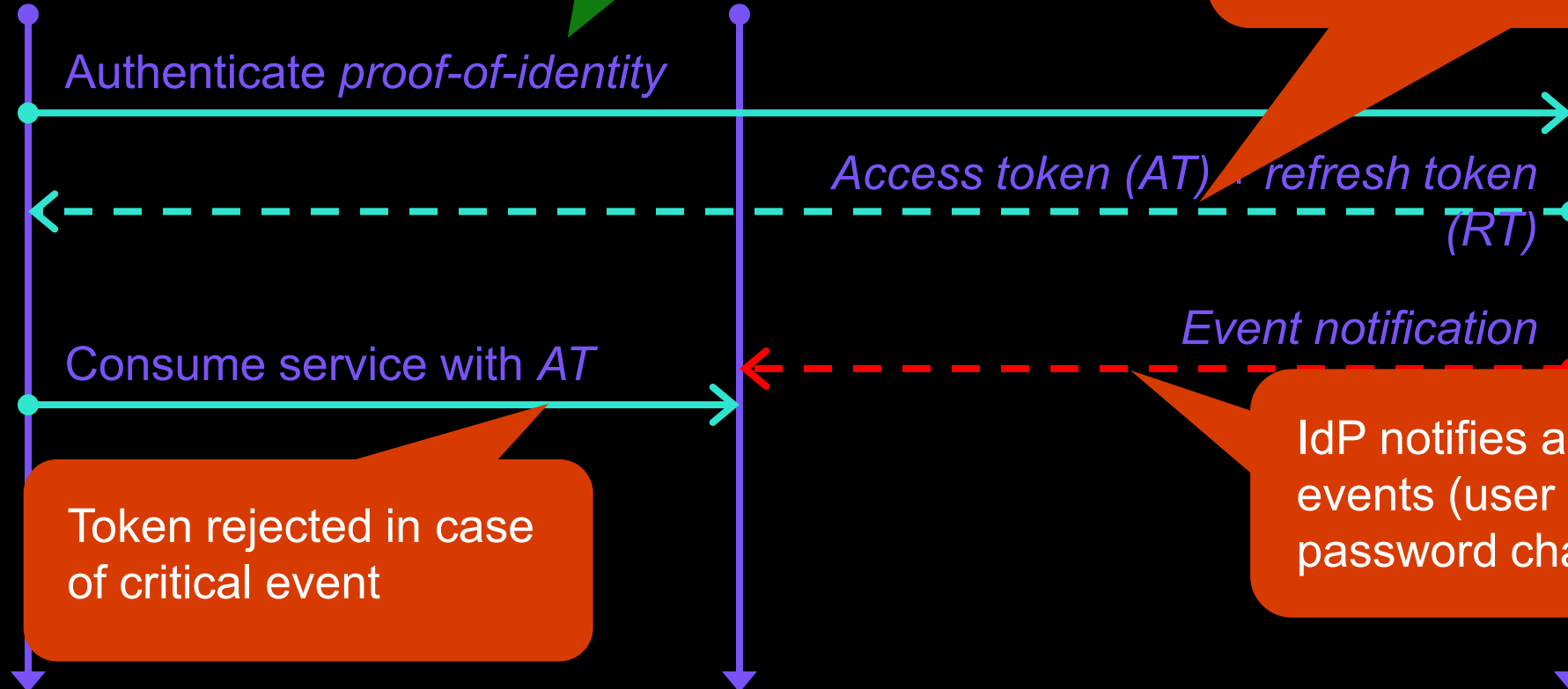
How CAE works?



User

Include **claims** attribute with value **xms_cc={cp1}** *

SP



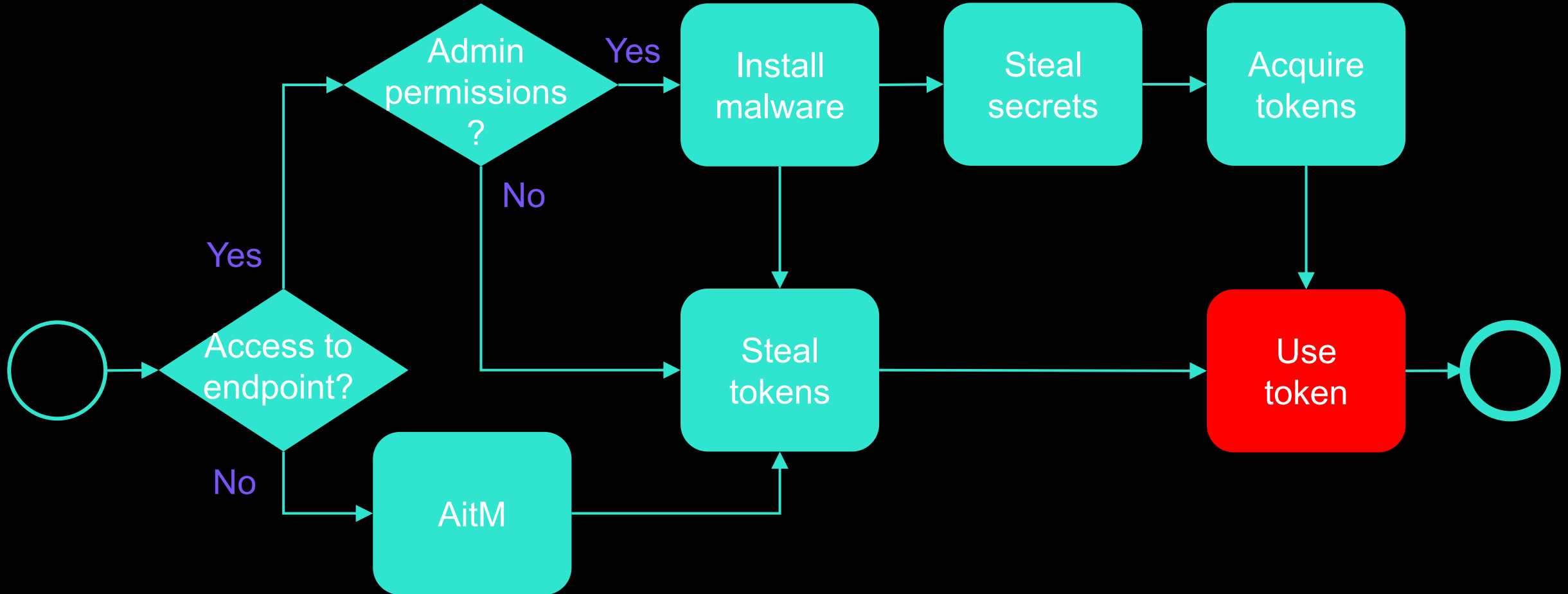
Access token will include **xms_cc={cp1}** claim and lifetime up to 28 hours

Token rejected in case of critical event

IdP notifies about critical events (user disabled, password change, etc.)

* <https://learn.microsoft.com/en-us/entra/identity-platform/claims-challenge?tabs=dotnet#how-to-communicate-client-capabilities-to-microsoft-entra-id>

CAE *may* prevent token replay



* <https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-continuous-access-evaluation#conditional-access-policy-evaluation>

Exploiting CAE

- CAP requires Entra ID P1 license
 - Token Protection is enforced by CAP
 - CAE can be customized using CAP
- You can *request* CAE tokens without P1 license
 - Allows threat actors to get tokens with much longer lifetime (up to 28 hours vs 1 hour)

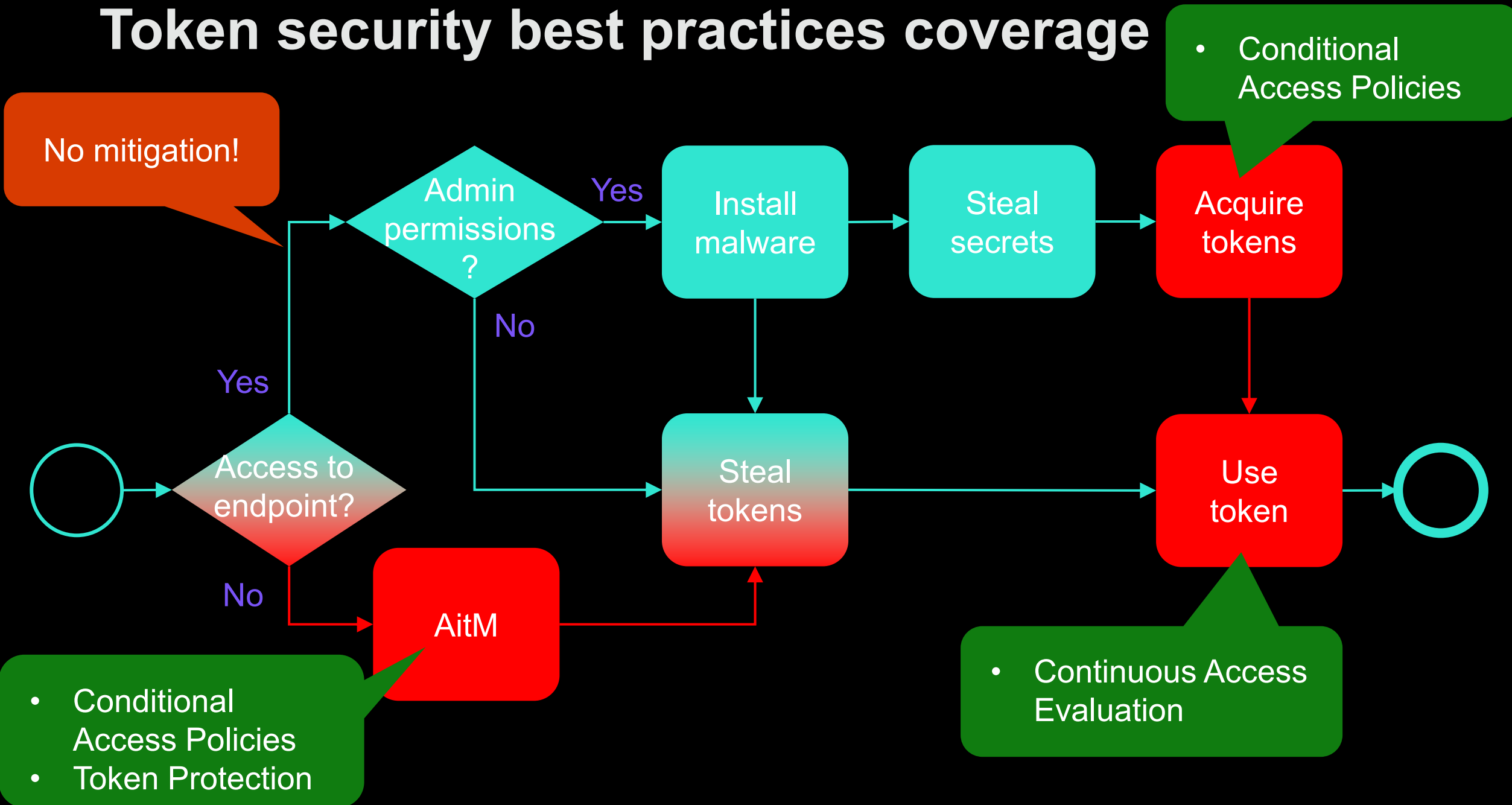
Detecting CAE abuse

```
union isfuzzy=true SigninLogs, AADNonInteractiveUserSignInLogs  
| mv-expand todynamic(AuthenticationProcessingDetails)  
| where AuthenticationProcessingDetails.key has "Is CAE Token"  
| where AuthenticationProcessingDetails.value has "true"  
| project TimeGenerated, AppId, ResourceIdentity, UserPrincipalName
```

Demo



Token security best practices coverage



DANKE SCHÖN!

Questions?

