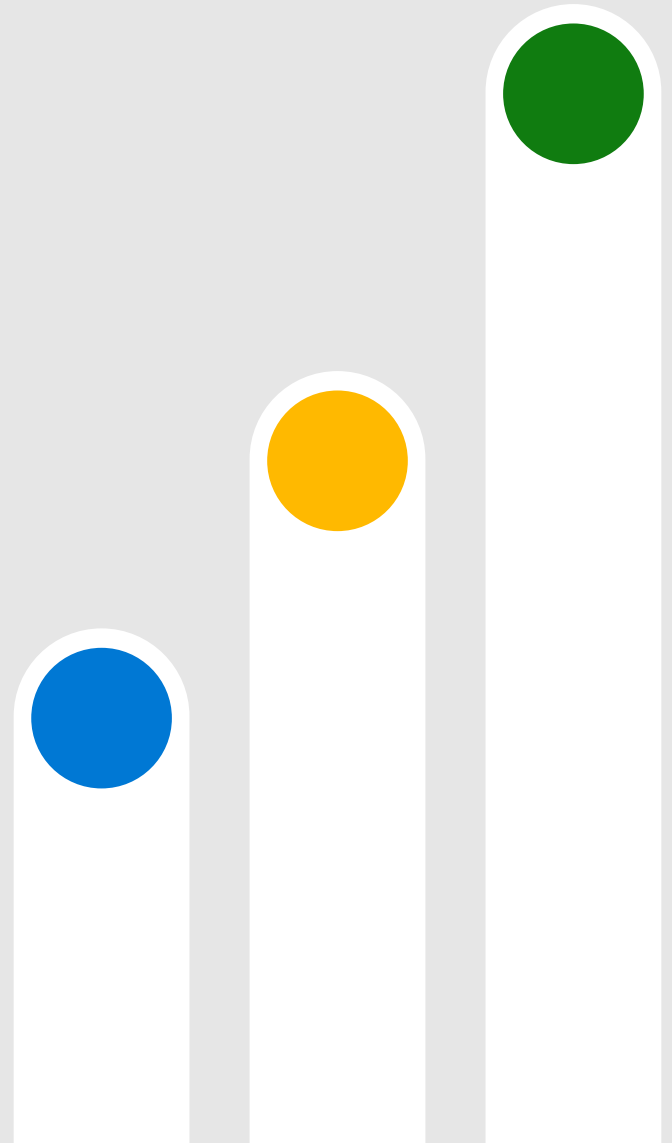**Microsoft Security**

Who am I?

- Dr Nestori Syynimaa (@DrAzureAD)
- Principal Identity Security Researcher
- Microsoft Threat Intelligence Center (MSTIC RnD)

Contents

- Introduction

- Federated authentication methods

- Token based authentication attacks

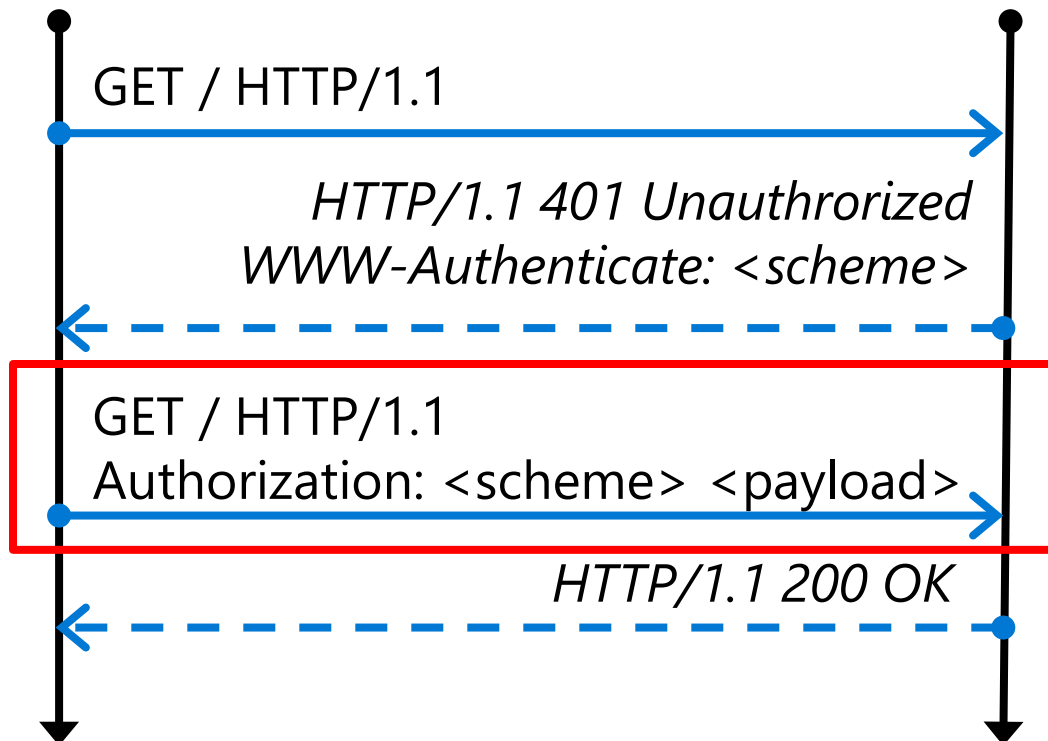- Detecting & preventing

Introduction

General HTTP Authentication framework [RFC 7235](#)

Client — Server

GET / HTTP/1.1

HTTP/1.1 401 Unauthrorized
WWW-Authenticate: <scheme>

GET / HTTP/1.1
Authorization: <scheme> <payload>

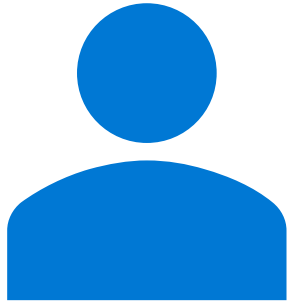*HTTP/1.1 200 OK*

- After the authentication, usually *session* cookies are used
- Some schemes:
  - Basic   [RFC 7617](#)
  - Bearer   [RFC 6750](#)
  - Negotiate / NTLM   [RFC 4599](#)

Key concepts

User

· Consumes services
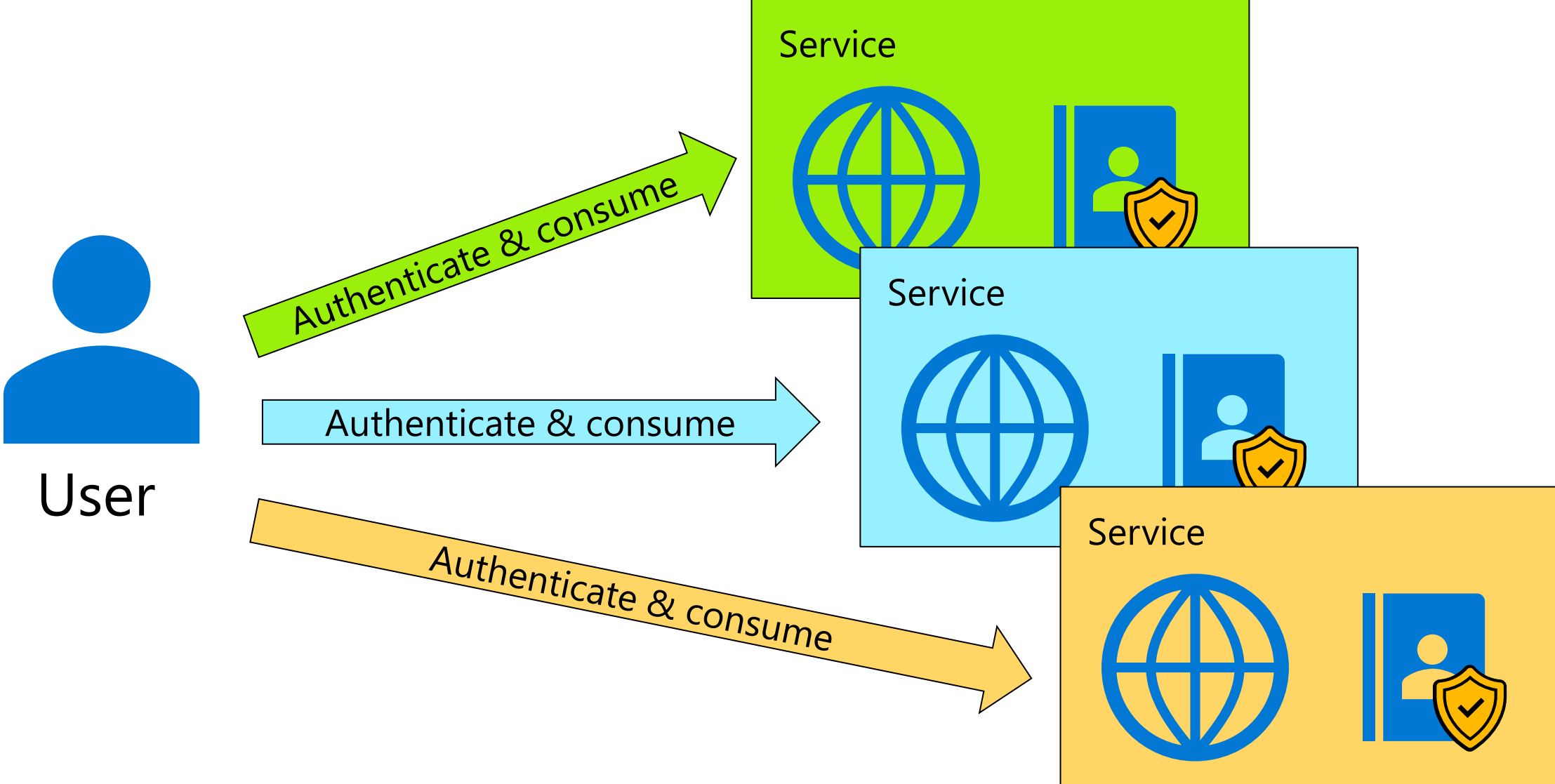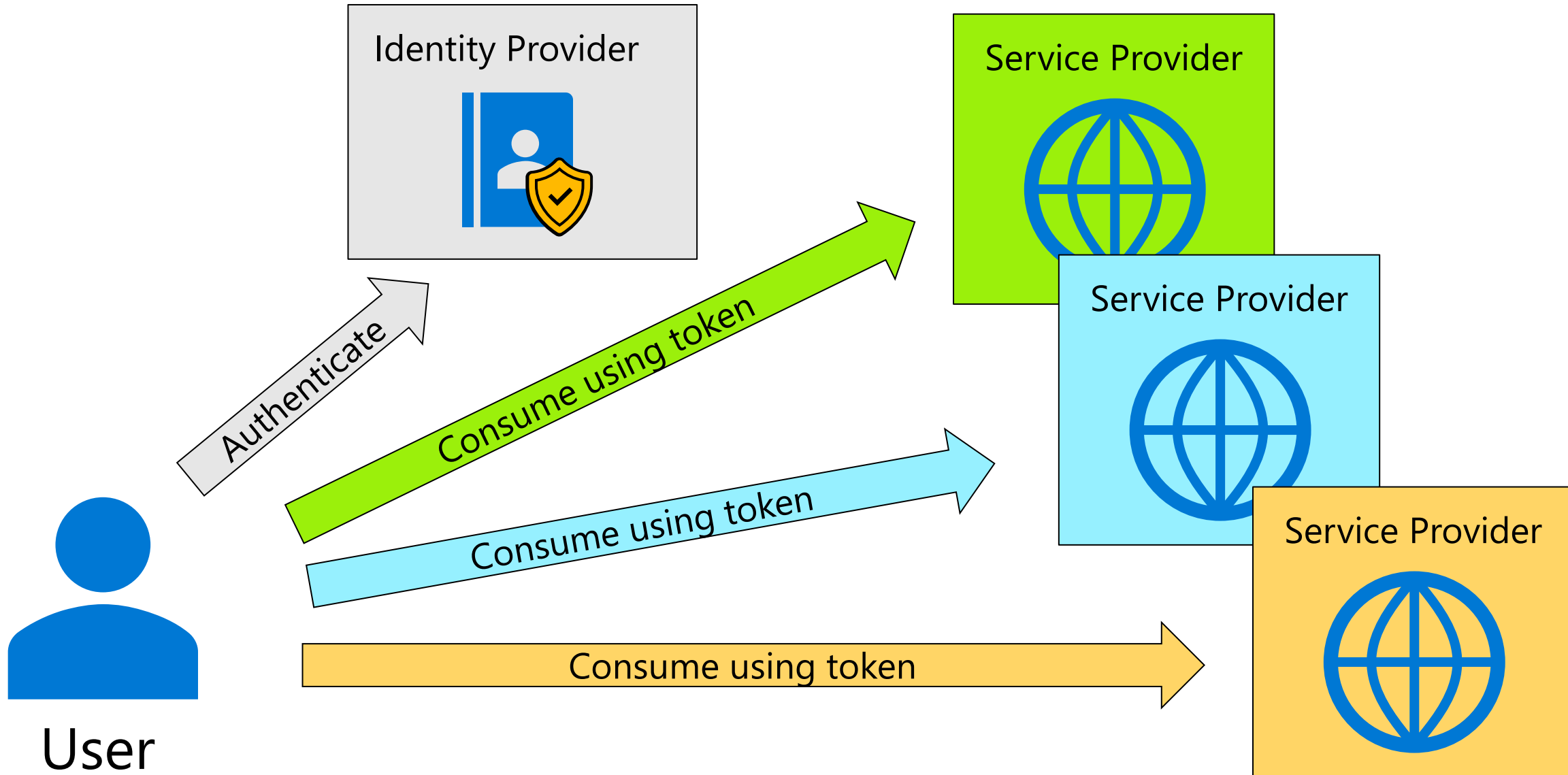
Service Provider (SP)

· Provides services

Identity Provider (IdP)
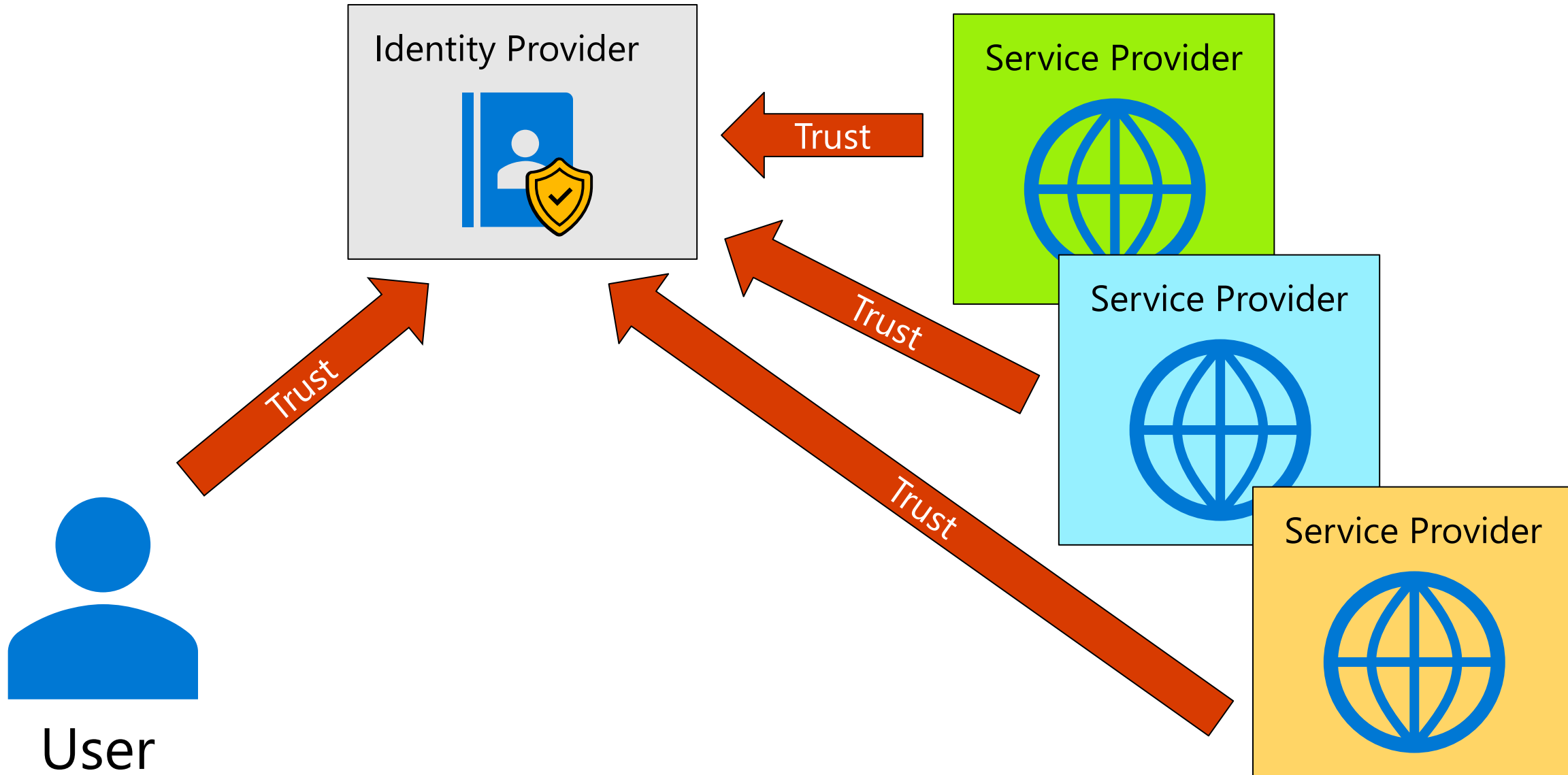
· Provides identity and access management

Brief history of authentication: Silo model

Brief history of authentication: Federated model (SSO)

Identity Provider

Service Provider

Service Provider

Service Provider

Authenticate

Consume using token

Consume using token

Consume using token

User

Brief history of authentication: Federated model (SSO)

Federated authentication methods

Kerberos authentication flow

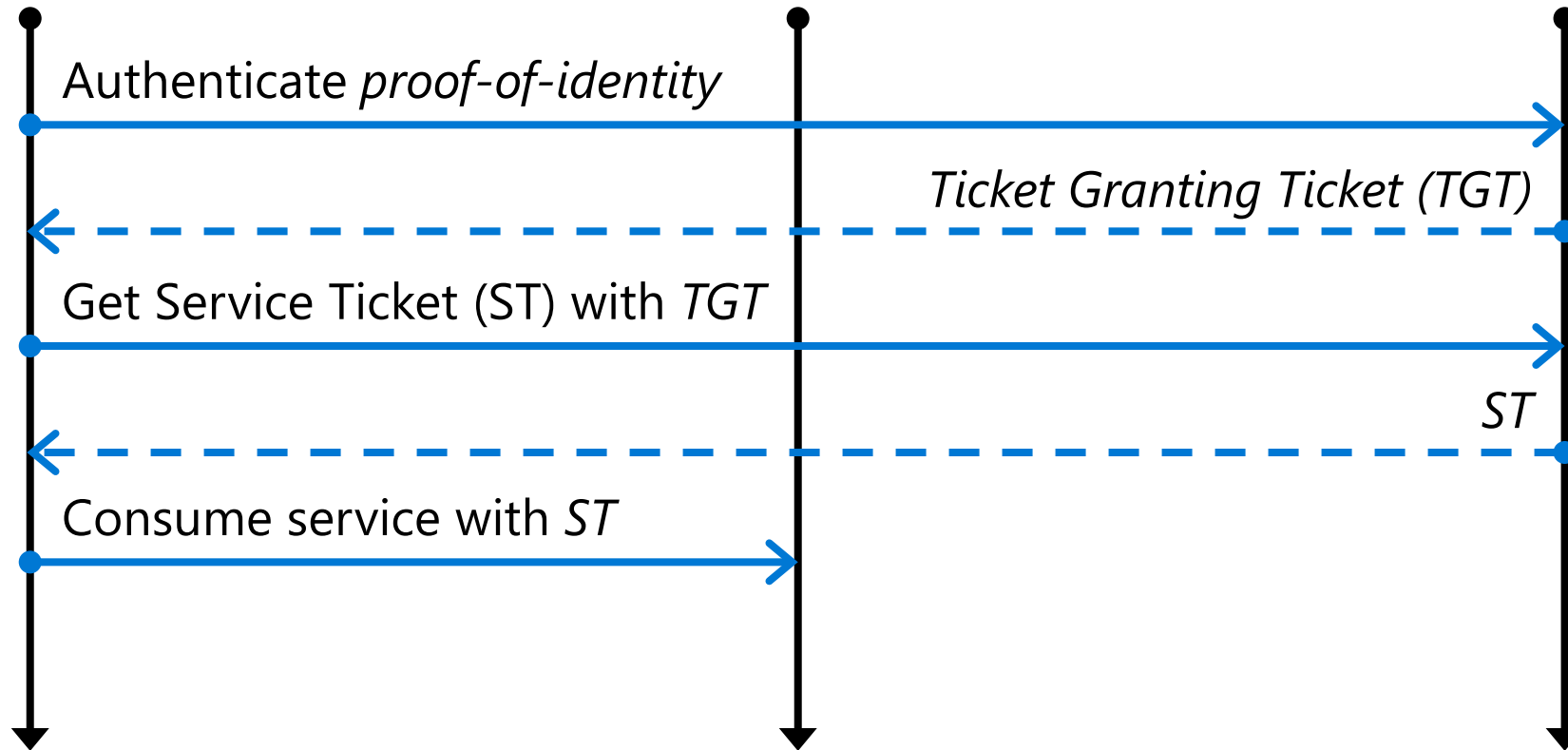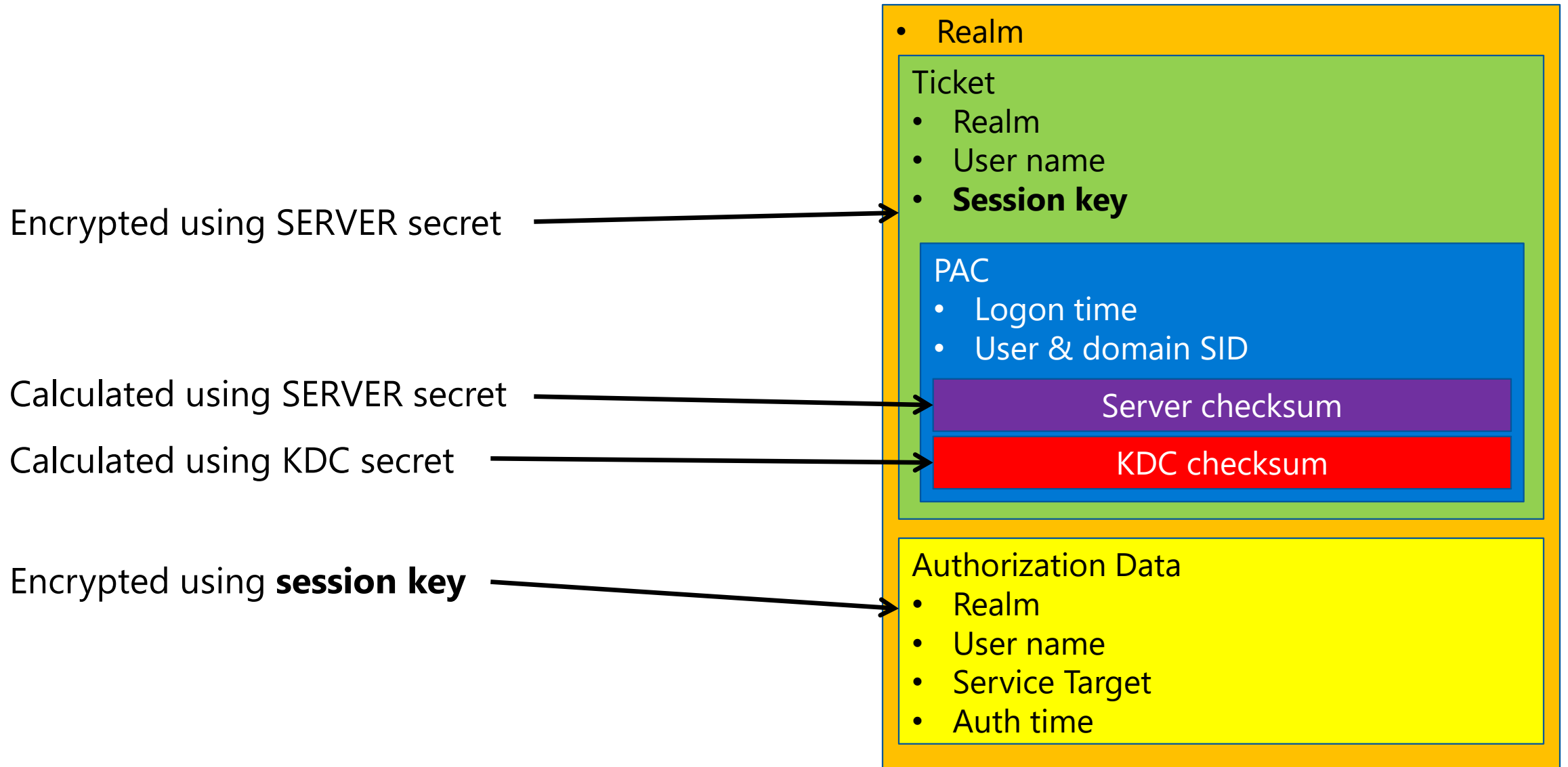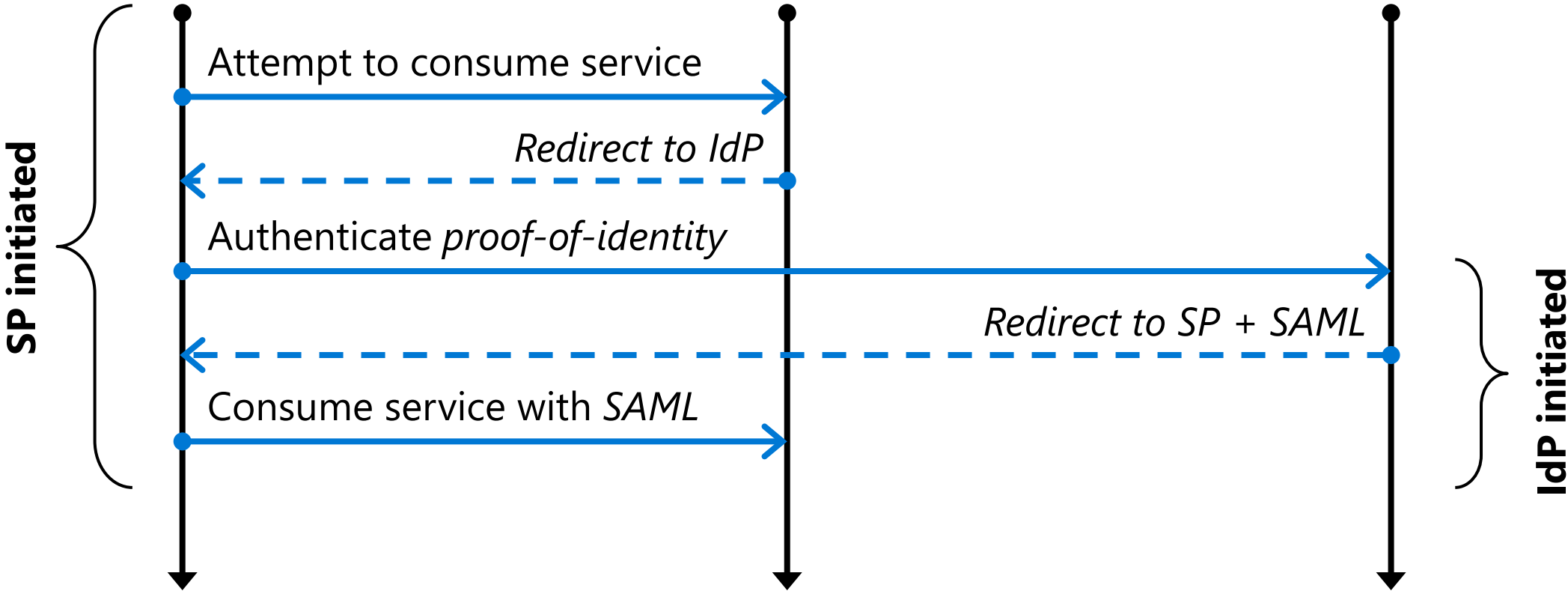# Kerberos Application Request (KRB_AP_REQ) message

Encrypted using SERVER secret

Calculated using SERVER secret

Calculated using KDC secret

Encrypted using **session key**

- Realm
  - Ticket
    - Realm
    - User name
    - **Session key**
  - PAC
    - Logon time
    - User & domain SID
    - Server checksum
    - KDC checksum
- Authorization Data
  - Realm
  - User name
  - Service Target
  - Auth time

SAML authentication flows
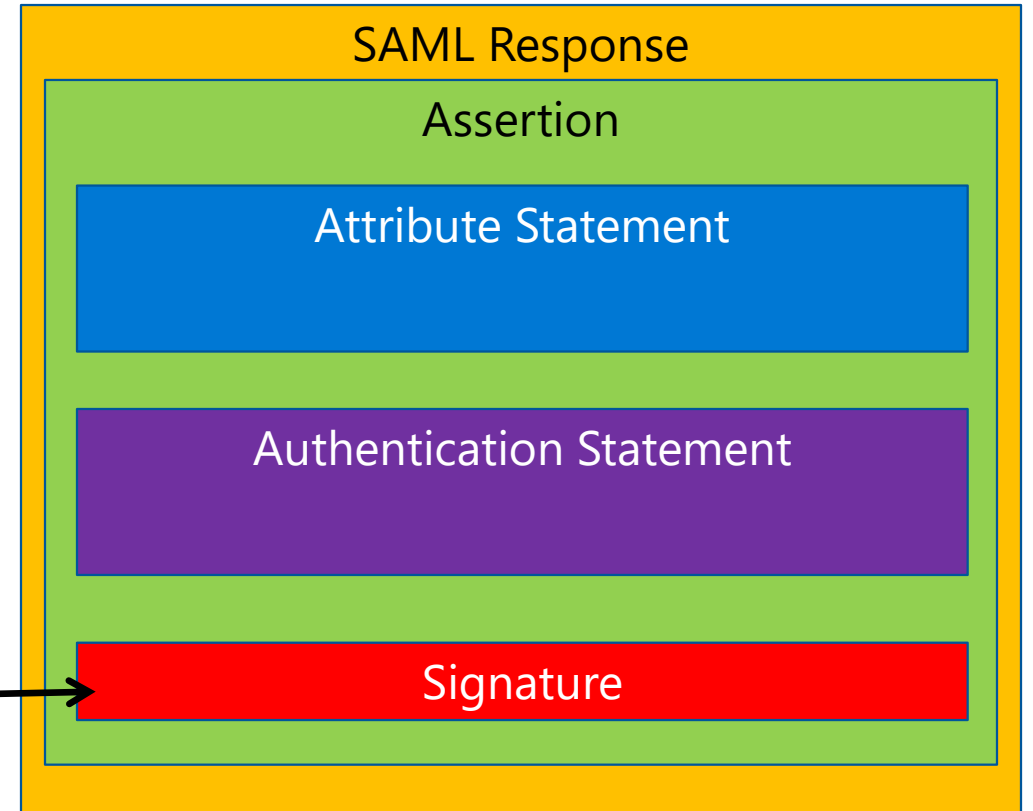
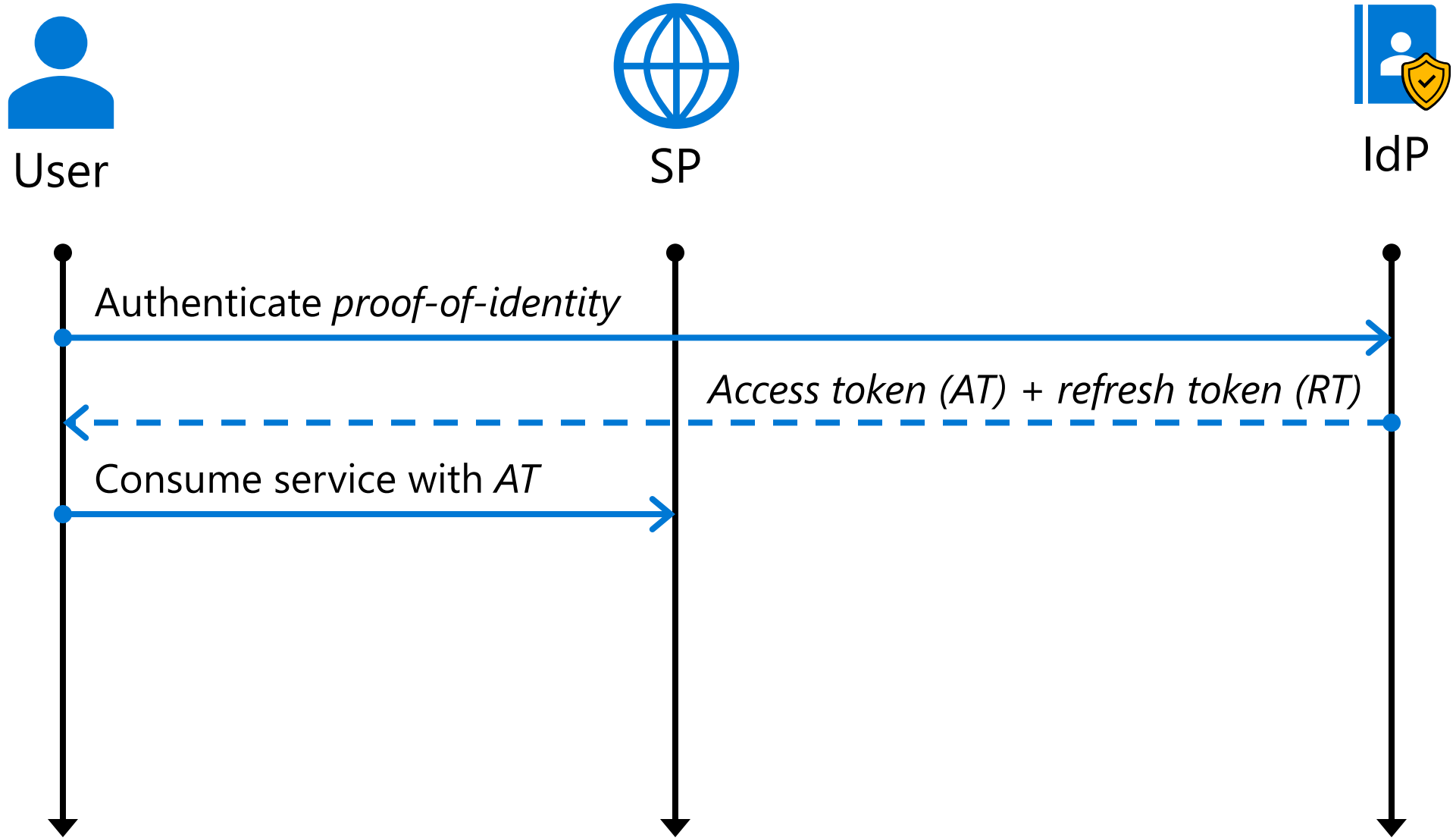# SAML response message

JSON Web Signature (JWS)

· Used in Entra ID for Access & Id tokens

· Three parts

  · JOSE (Javascript Object Signing and Encryption) Header

  · Payload (usually a claims set as JSON)
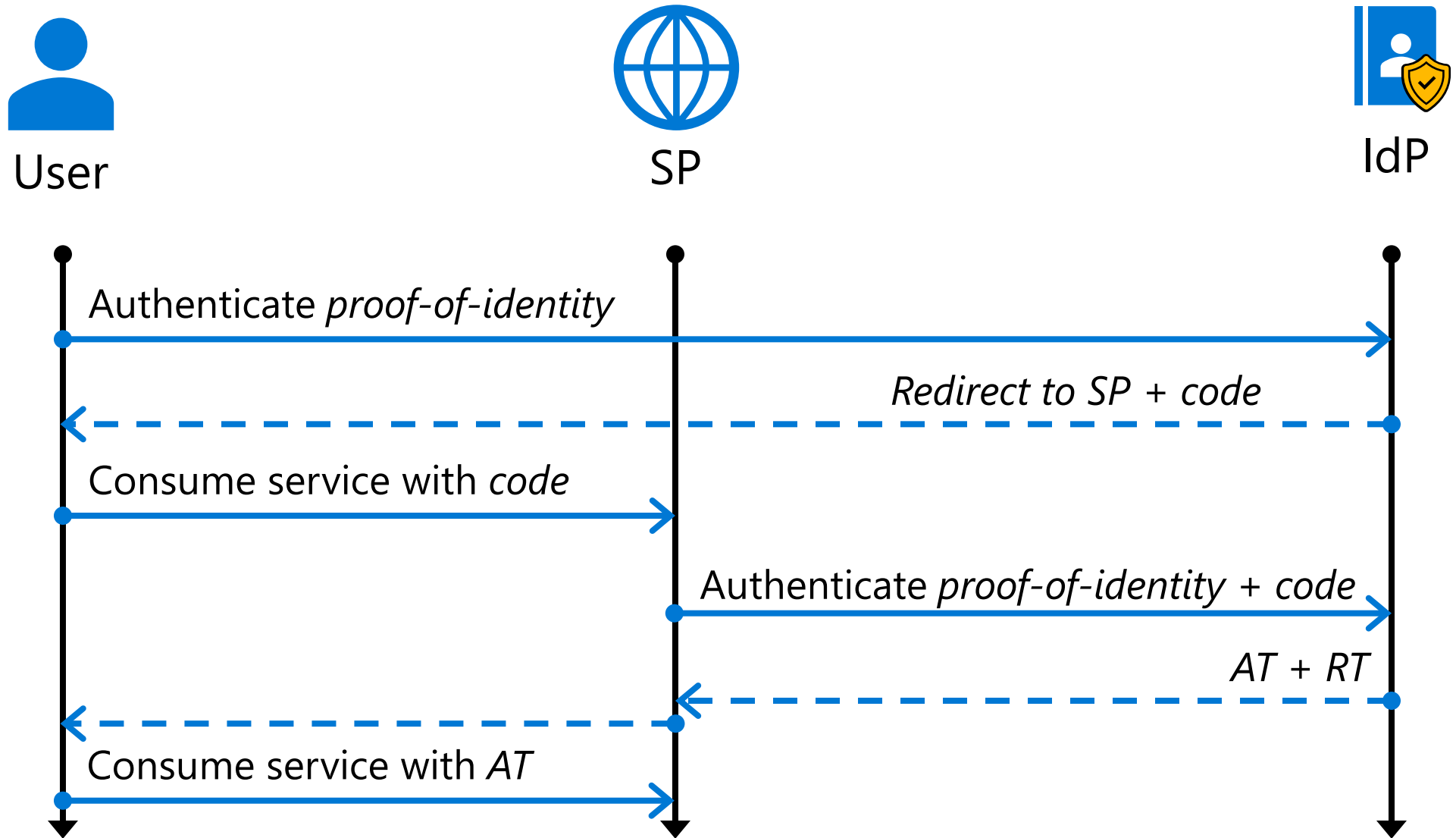
  · Signature (IdP secret key)

B64(UTF8(JOSE Header)) . **B64(Payload)** . **B64(Signature)**

https://www.rfc-editor.org/rfc/rfc7515.html

Entra ID ROPC flow

Entra ID authorization code flow

Entra ID Hybrid authentication flow
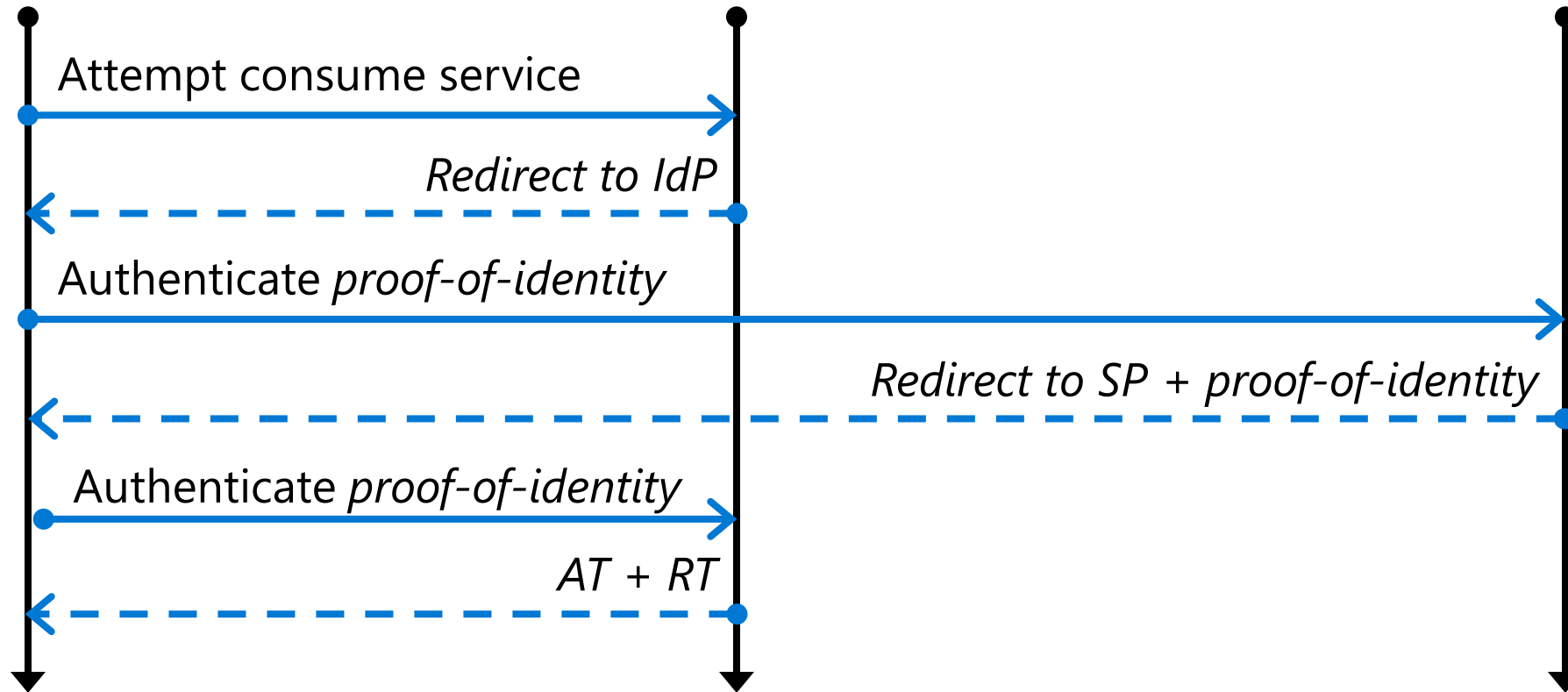
Entra ID Token types

Token	Standard	Purpose	Lifetime	Can be revoked?
id_token	OpenID Connect	User identification	1 h	No
access_token	OAuth2	User (identification and) authorization	1 h	No
refresh_token	OAuth2	For requesting new access_token	90 days	Yes

Summary of federated methods

Protocol	Since	Format	Trust based on
Kerberos	1989	ASN.1	Passwords
SAML*	2002	XML	Certificates
OAuth	2007	JWT (JWS)	Certificates

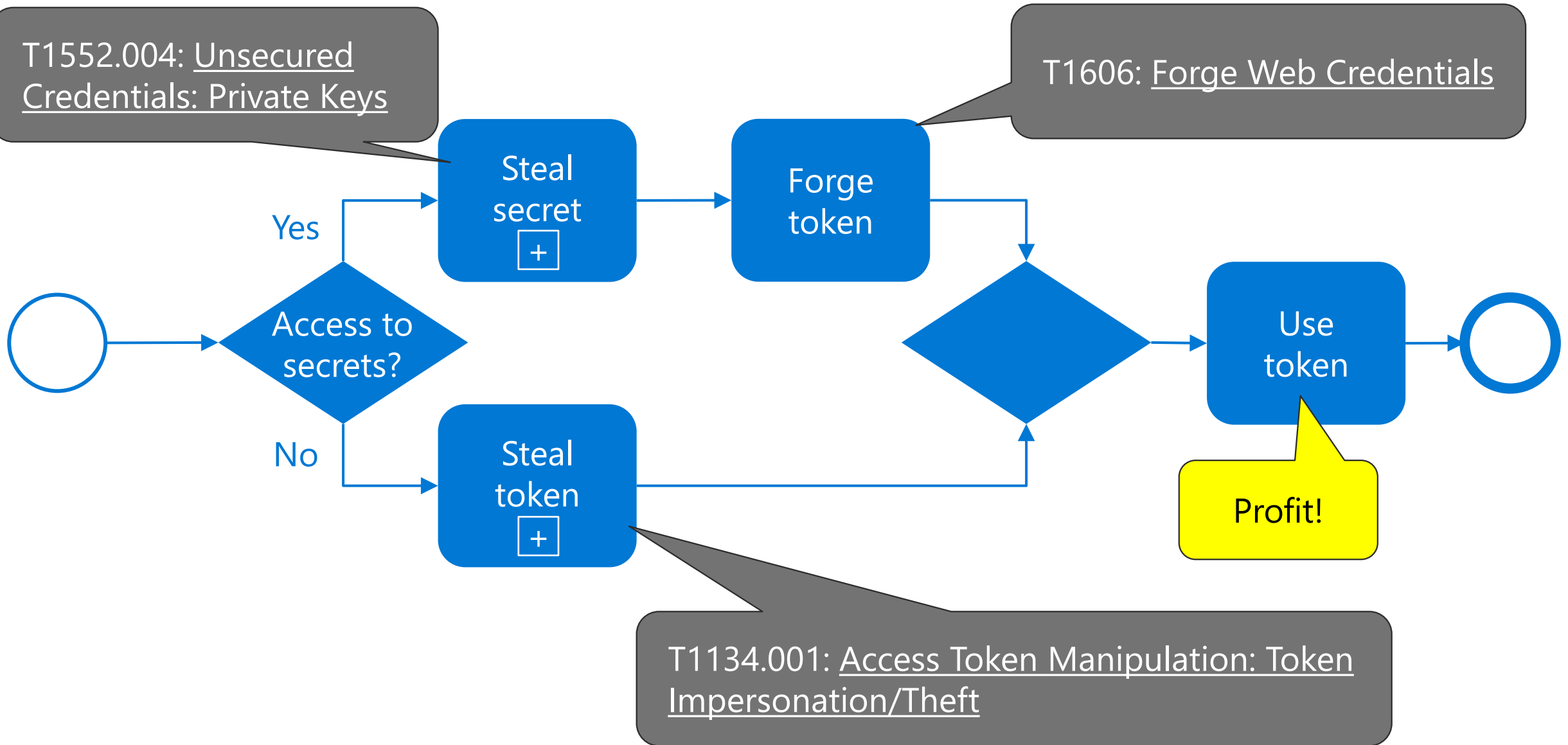* SAMLp or WS-FED

Token-based authentication attacks

Token based authentication

- **Any** party in **possession of a bearer token** (a "bearer") can use it to get access to the associated resources (without demonstrating possession of a cryptographic key). To prevent misuse, **bearer tokens need to be protected** from disclosure in storage and in transport.
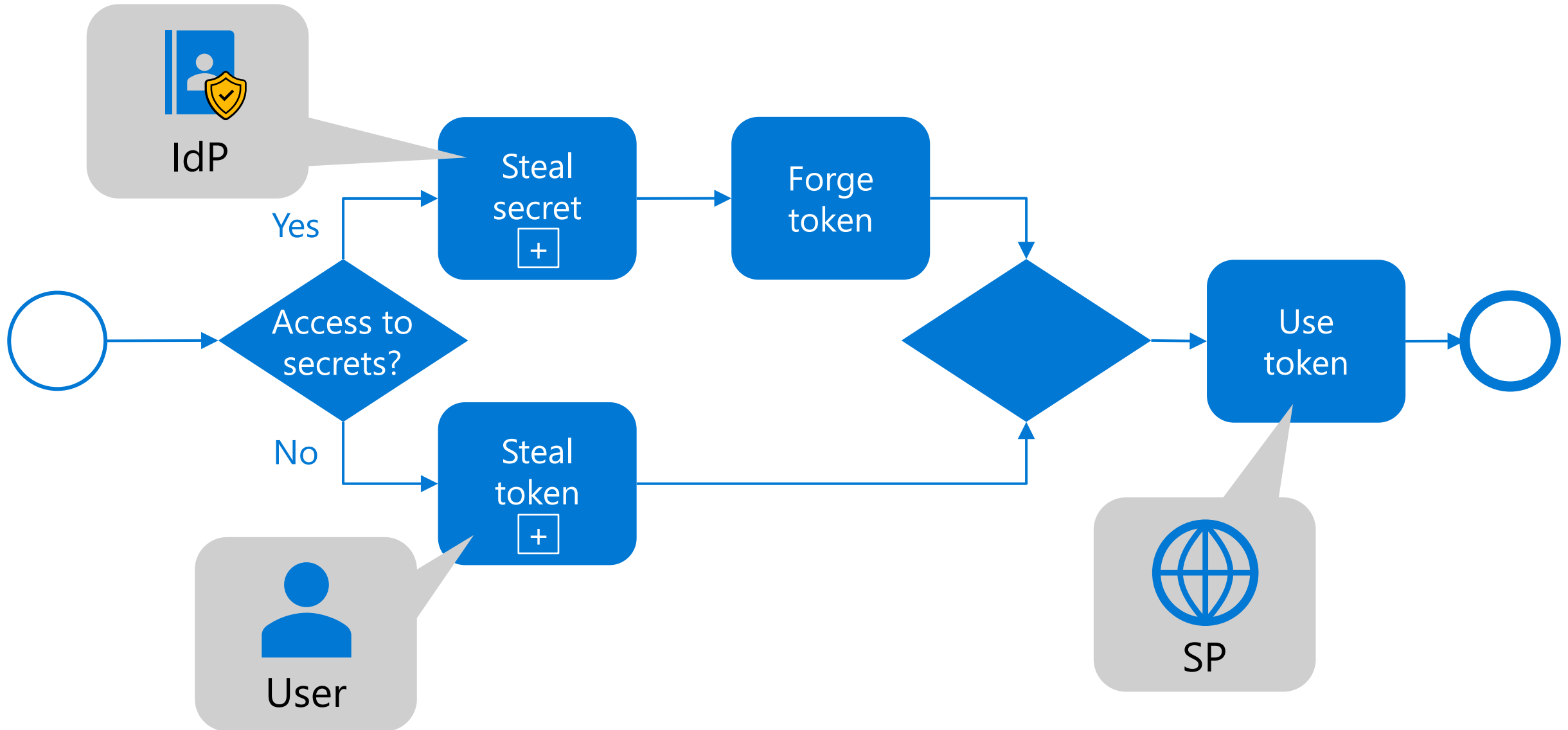
https://datatracker.ietf.org/doc/html/rfc6750

Token-based authentication attack graph

MITRE ATT&CK® techniques

T1552.004: Unsecured Credentials: Private Keys

T1606: Forge Web Credentials

Yes

Steal secret +

Forge token

Access to secrets?

Use token

No

Steal token +

Profit!

T1134.001: Access Token Manipulation: Token Impersonation/Theft
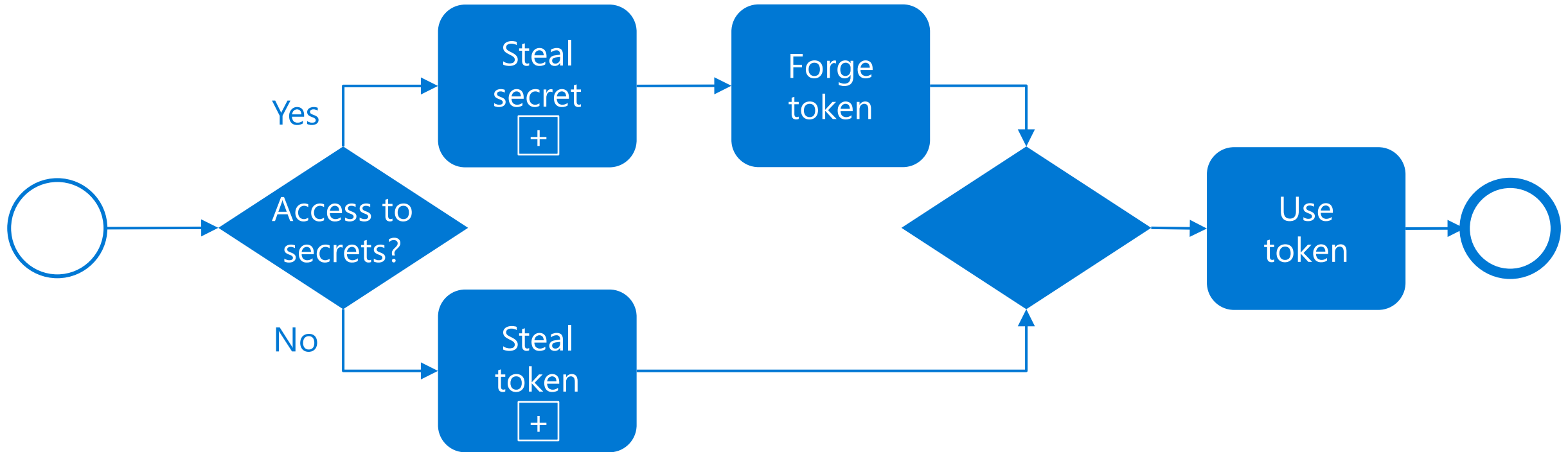
Realms
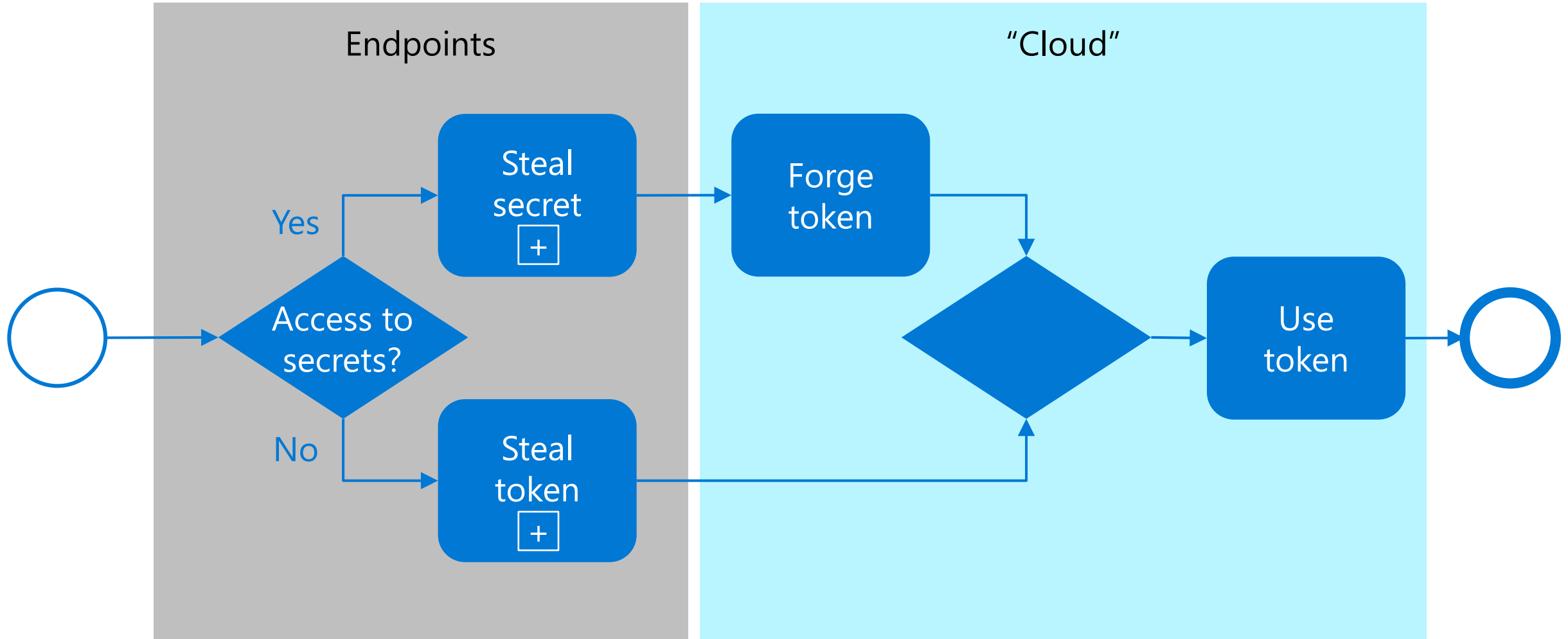
Authentication roles

Demo: Stealing tokens
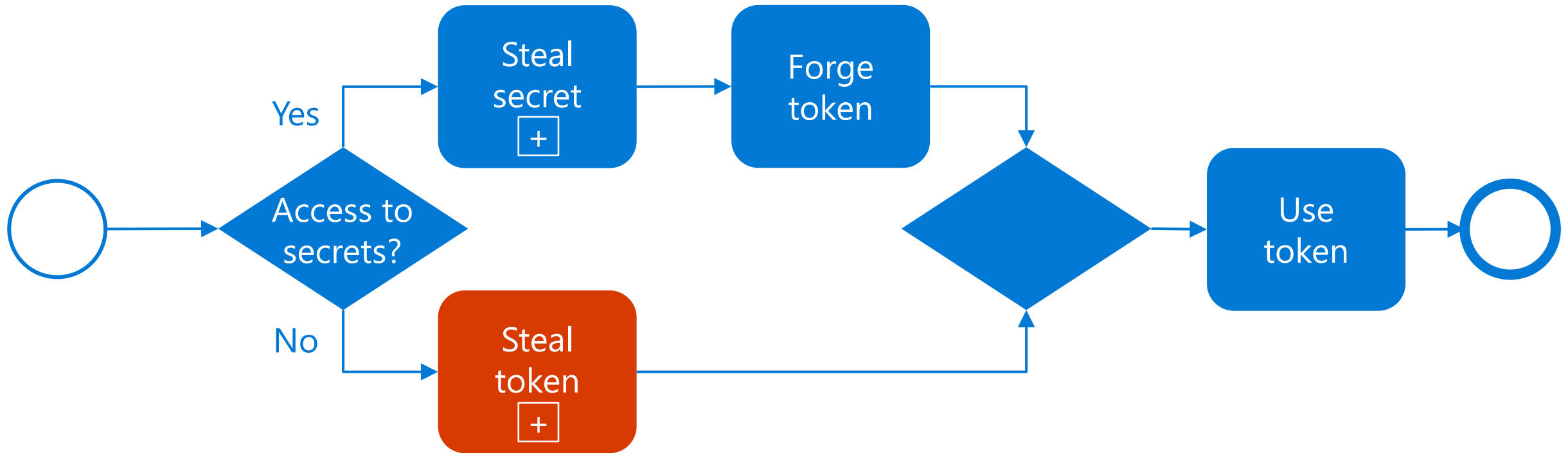
Demo: Stealing secrets and forging tokens
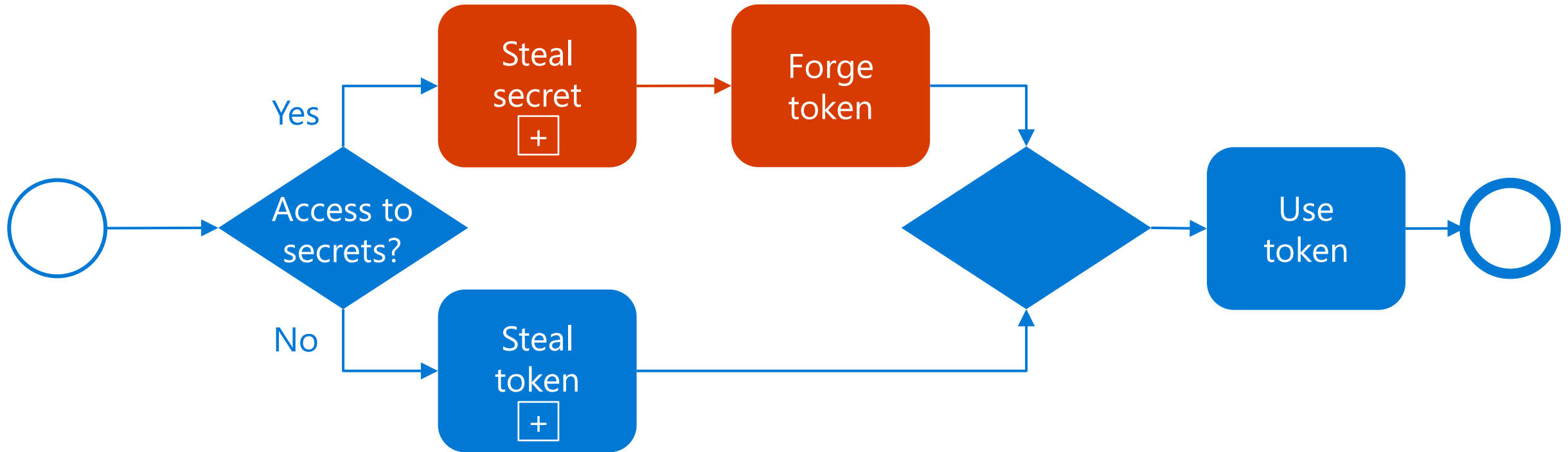
Detecting & preventing

Detection sources
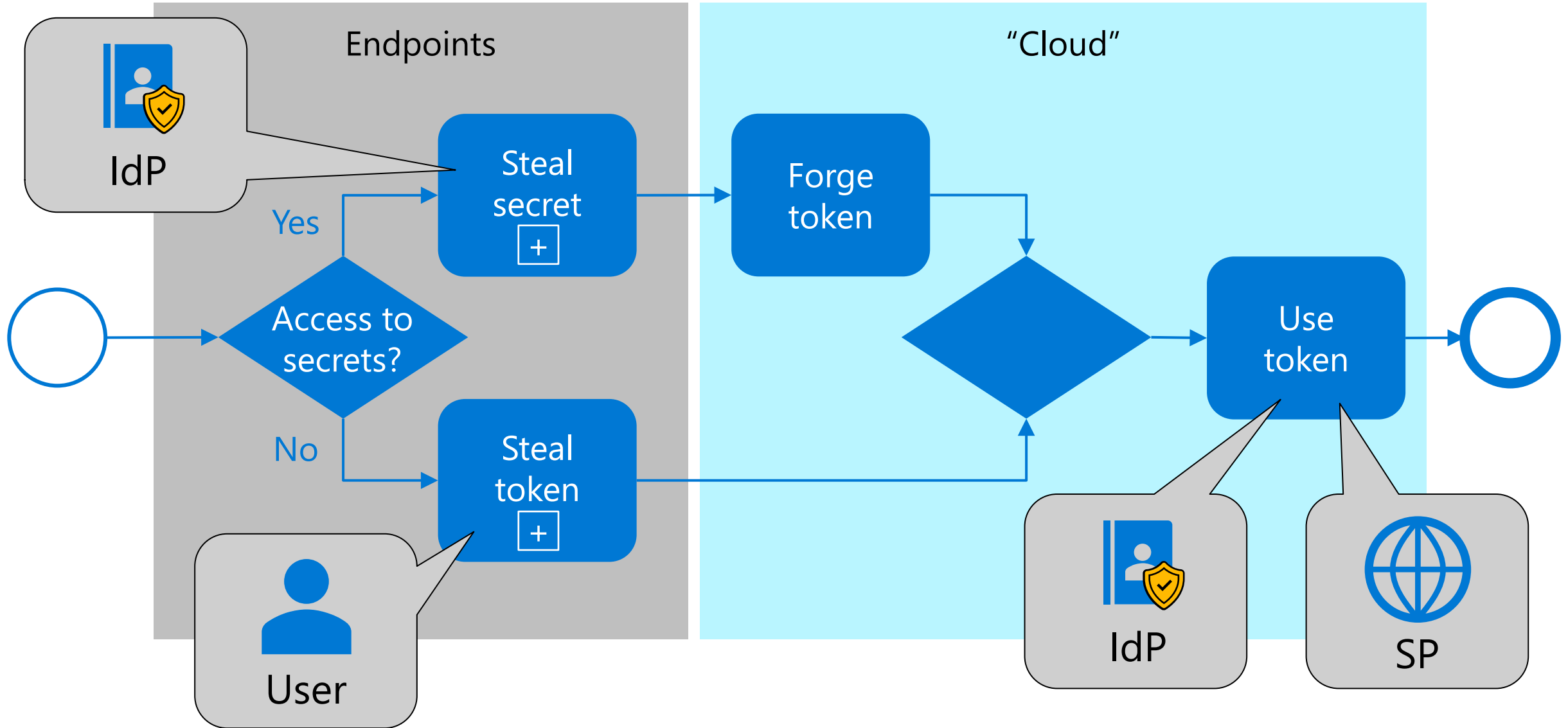
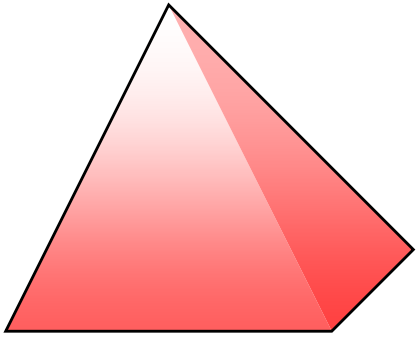# Scenario 1: On-prem identity
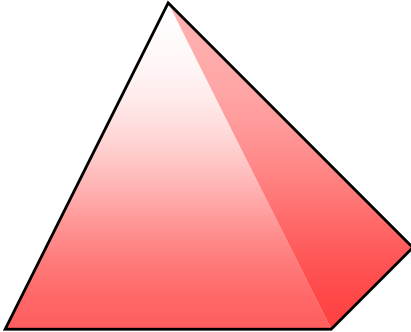
On-prem
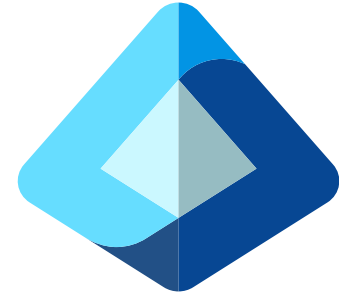Active Directory

On-prem
web server

Logon events

Usage logs

Scenario 3: Cloud-only identity 1
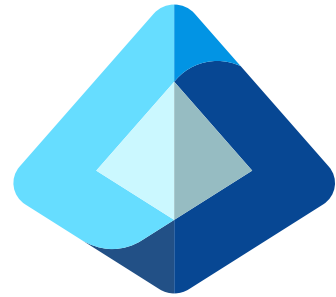
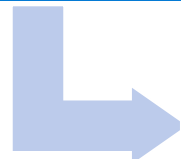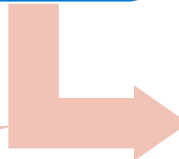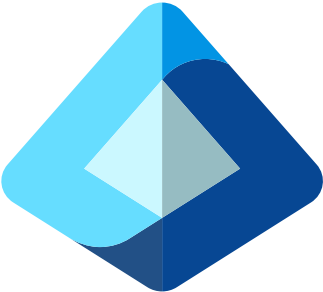Entra ID

Azure Web App

Sign-in logs

Usage logs

Demo 1/2
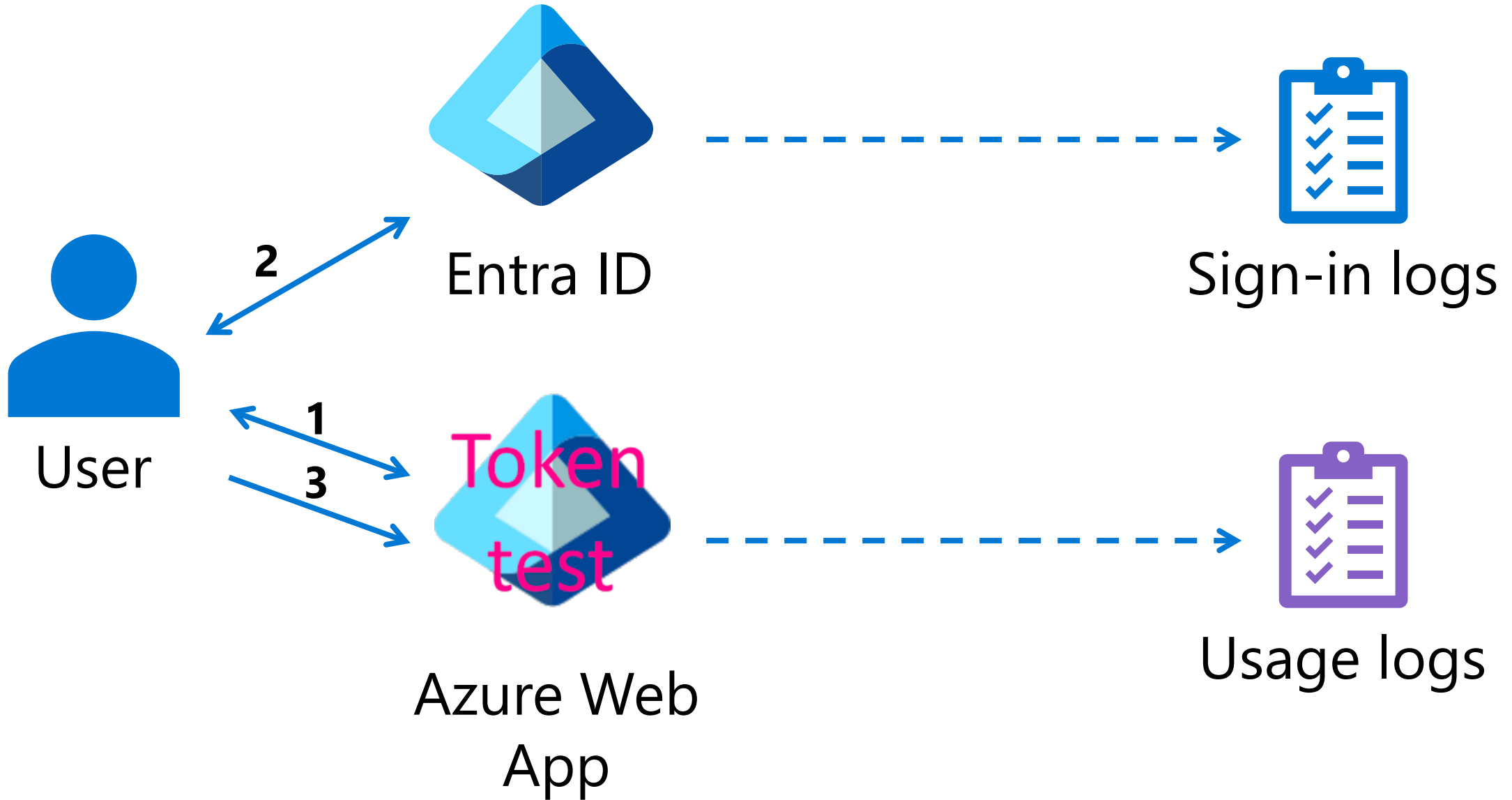
Scenario 4: Cloud-only identity 2

Entra ID

Microsoft 365

Sign-in logs

MS Graph
Activity Logs

Unified audit
log

Storm-0558 accessed emails of 25 organisations

https://aka.ms/storm-0558
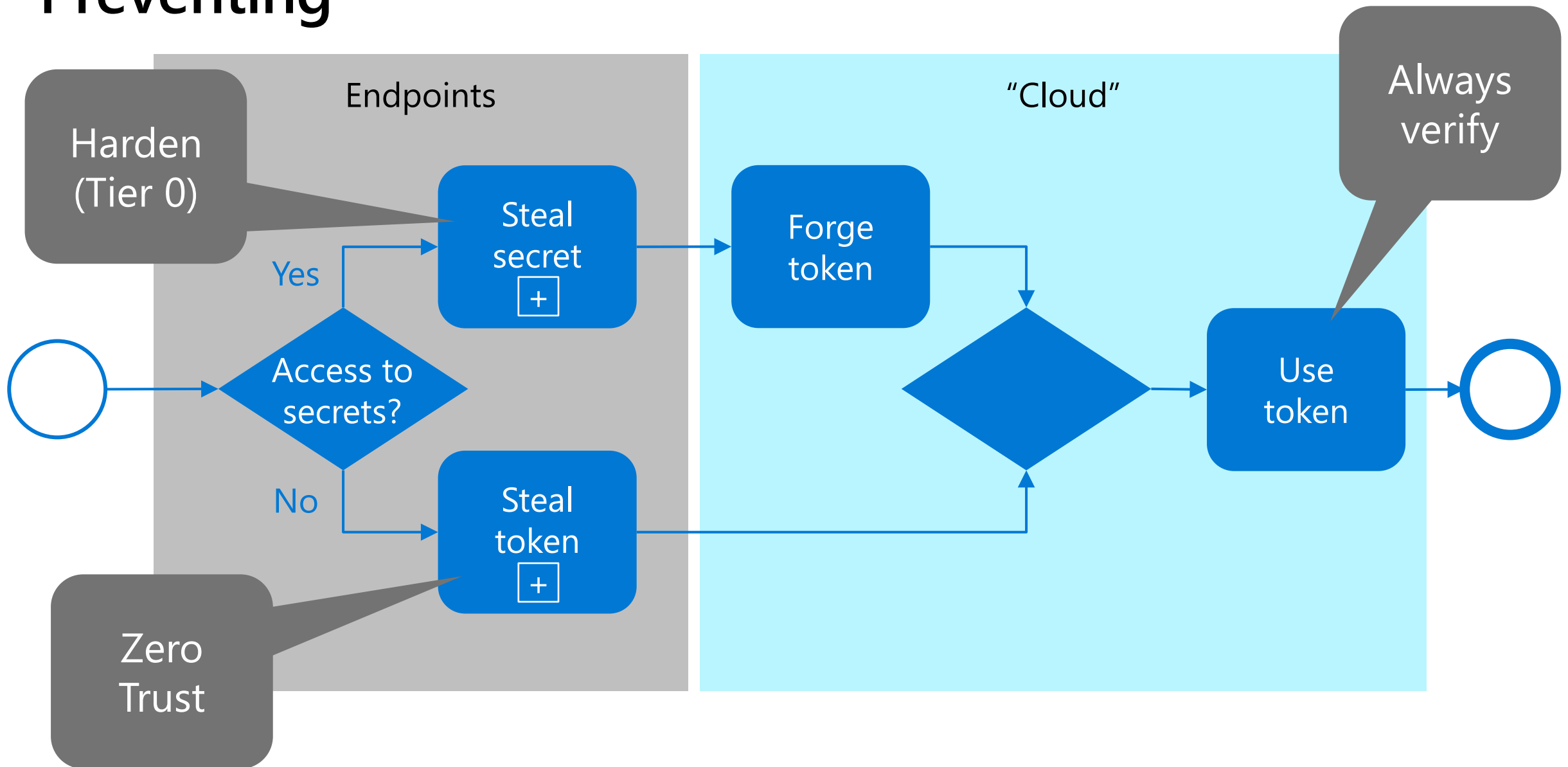https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
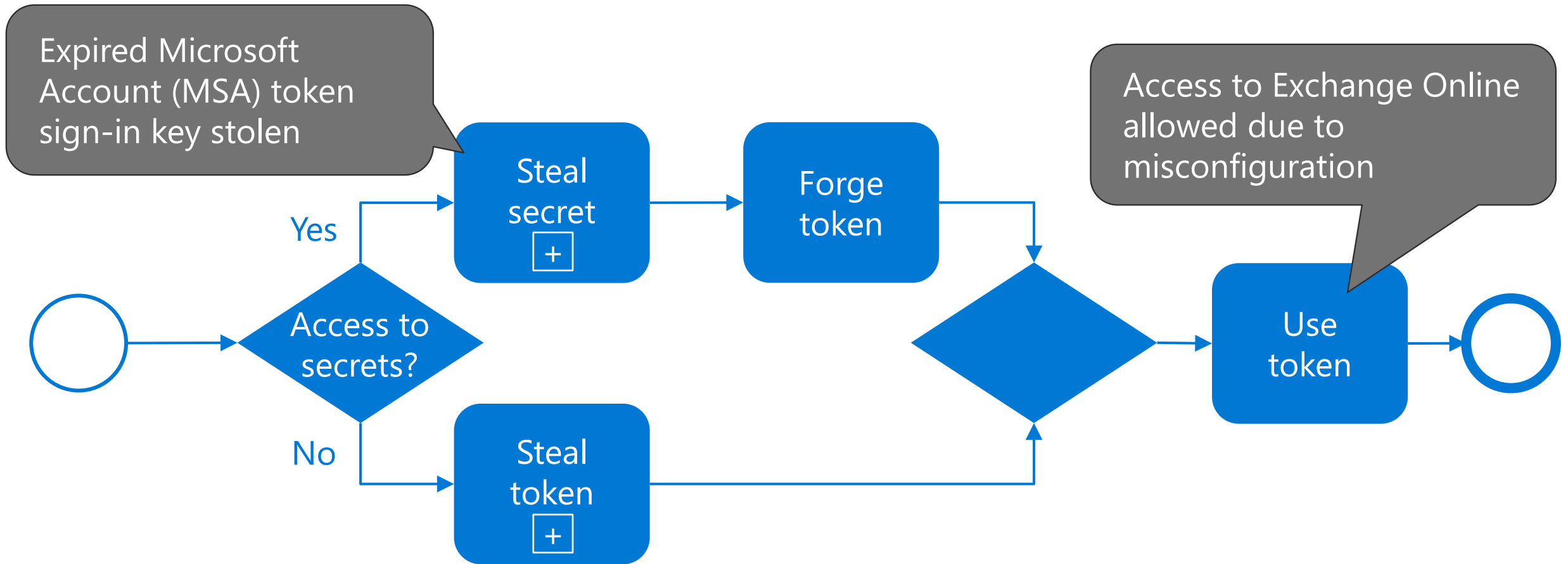
Preventing

Summary

Summary

- Stealing **tokens** gives temporary access as one person
- Stealing token sign-in **secrets** gives persistent access as any person
- Detecting and preventing token-theft is team sport
- Detection requires access to **IdP *and* SP** logs

Microsoft Security