

# Exploiting Token Based Authentication: Attacking and Defending Identities in the 2020s

Dr Nestori Syynimaa (MSTIC)



#### Who am I?

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



#### **Contents**

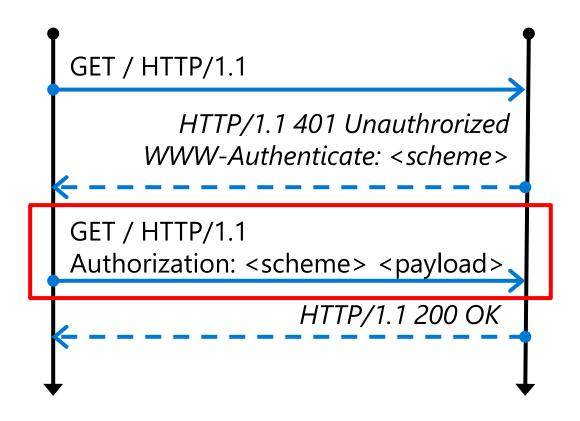
- Introduction
- Federated authentication methods
- Token based authentication attacks
- Detecting & preventing

# Introduction

#### General HTTP Authentication framework <u>RFC 7235</u>







- After the authentication, usually session cookies are used
- · Some schemes:

• Basic <u>RFC 7617</u>

• Bearer <u>RFC 6750</u>

Negotiate / NTLM RFC 4599

## **Key concepts**



Consumes services

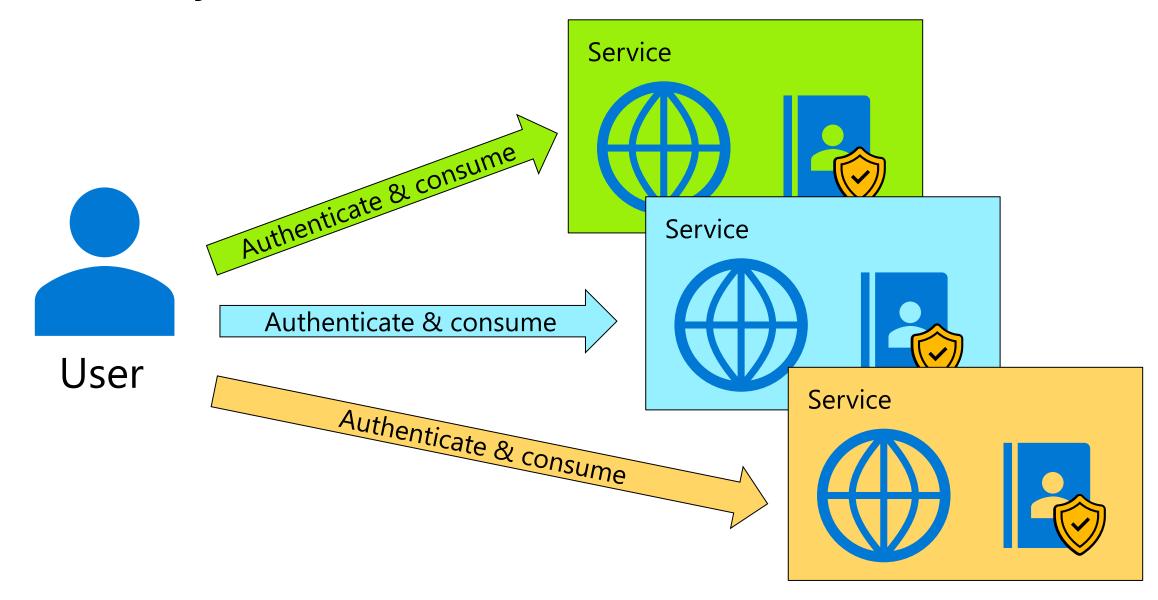




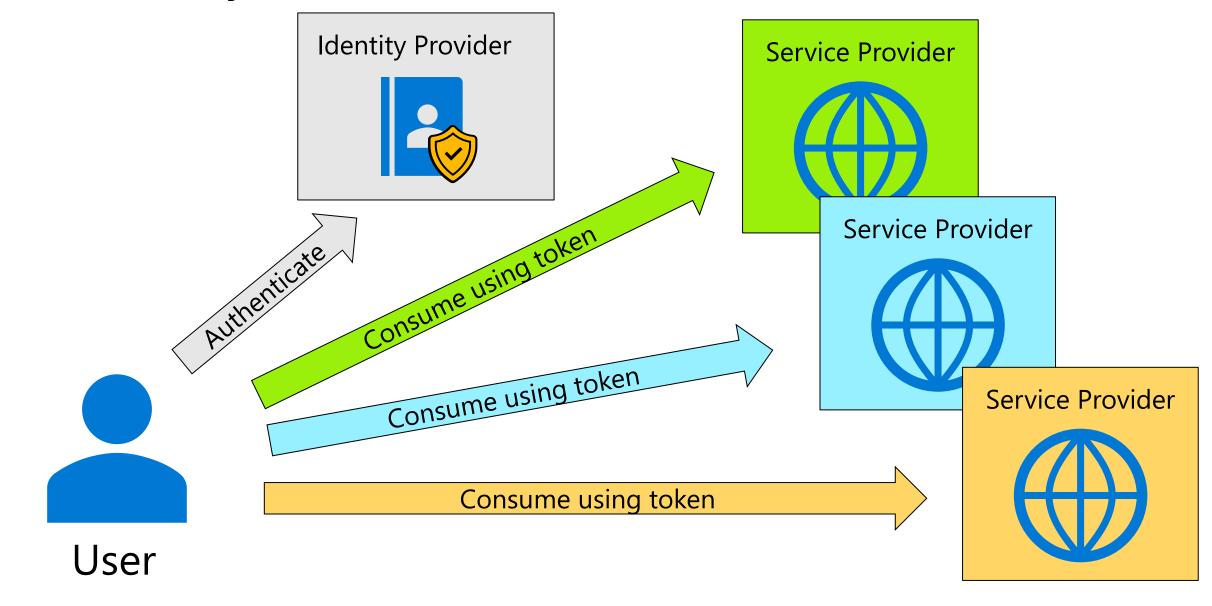


 Provides identity and access management

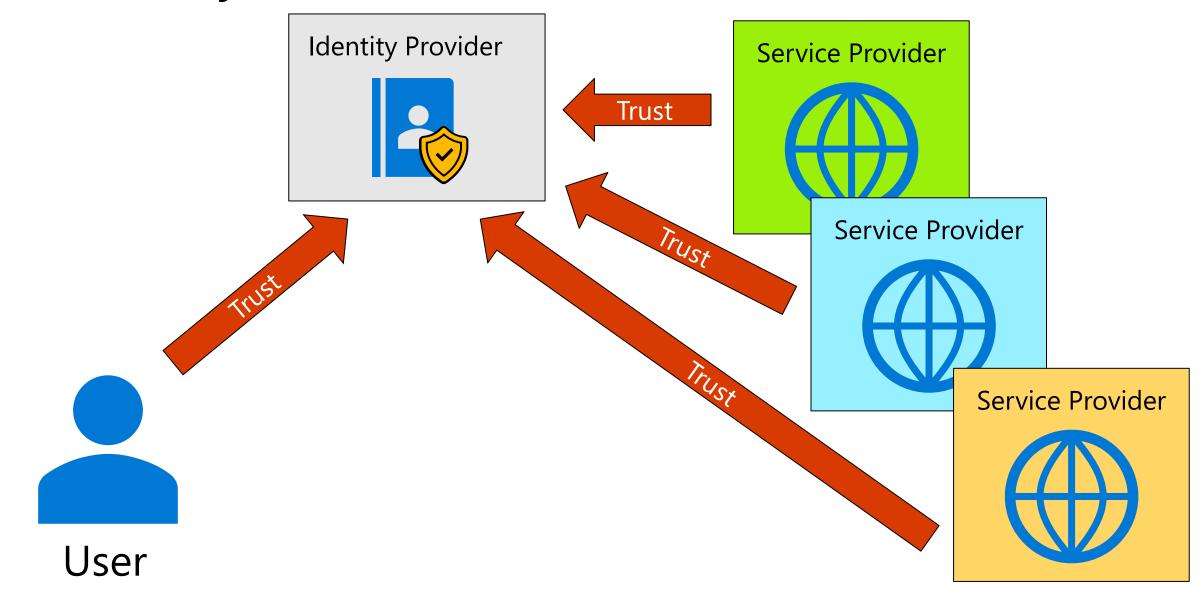
# Brief history of authentication: Silo model



# Brief history of authentication: Federated model (SSO)

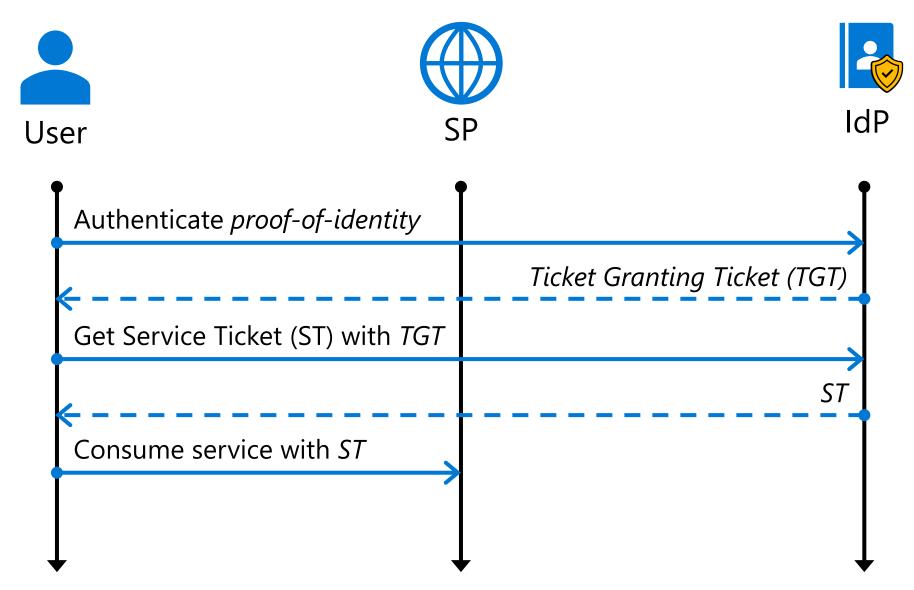


# Brief history of authentication: Federated model (SSO)

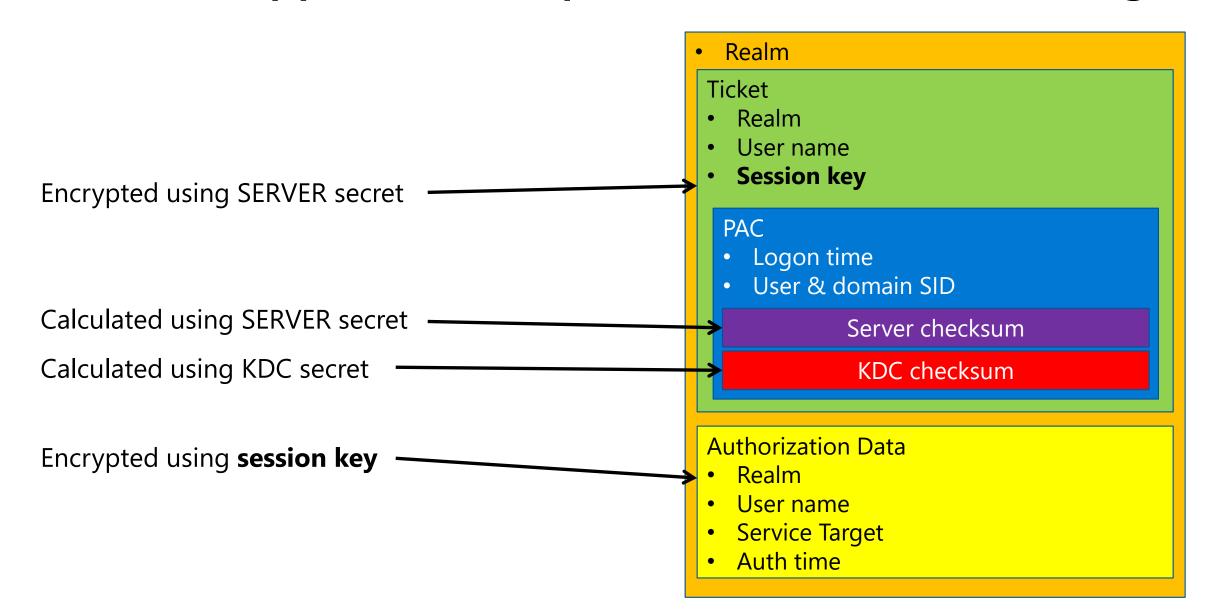


#### Federated authentication methods

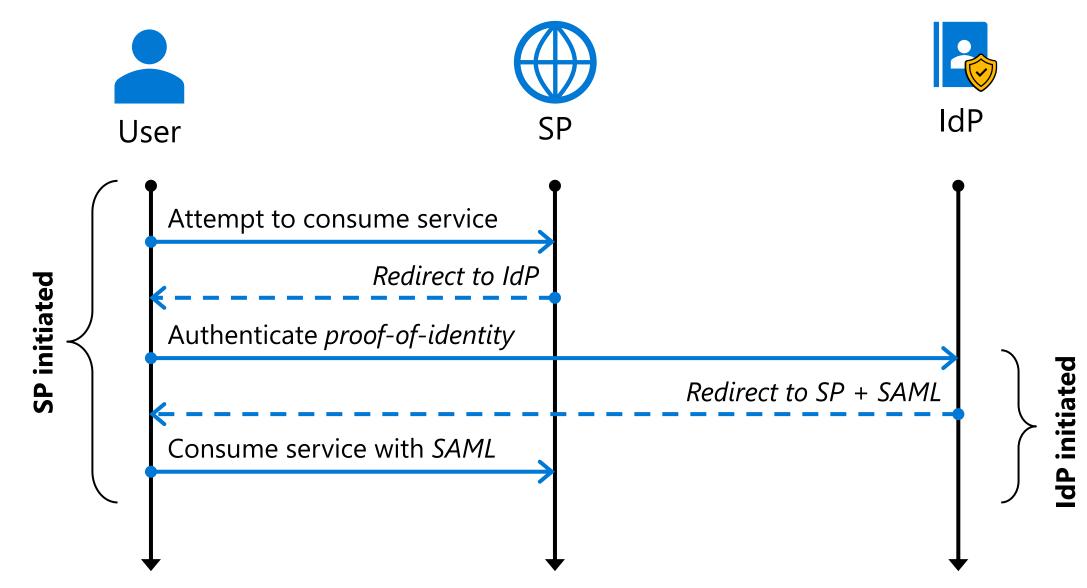
#### **Kerberos authentication flow**



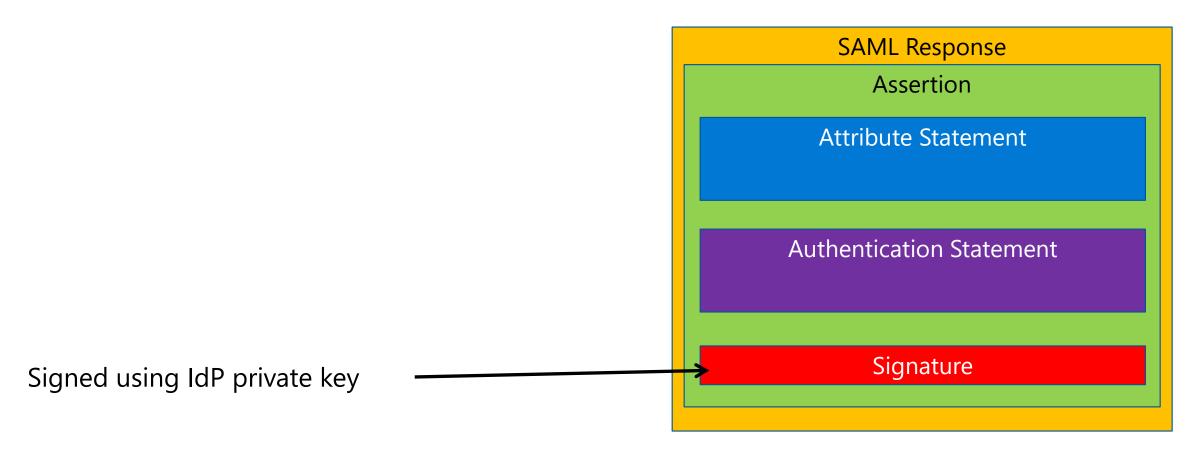
## Kerberos Application Request (KRB\_AP\_REQ) message



#### SAML authentication flows



# SAML response message

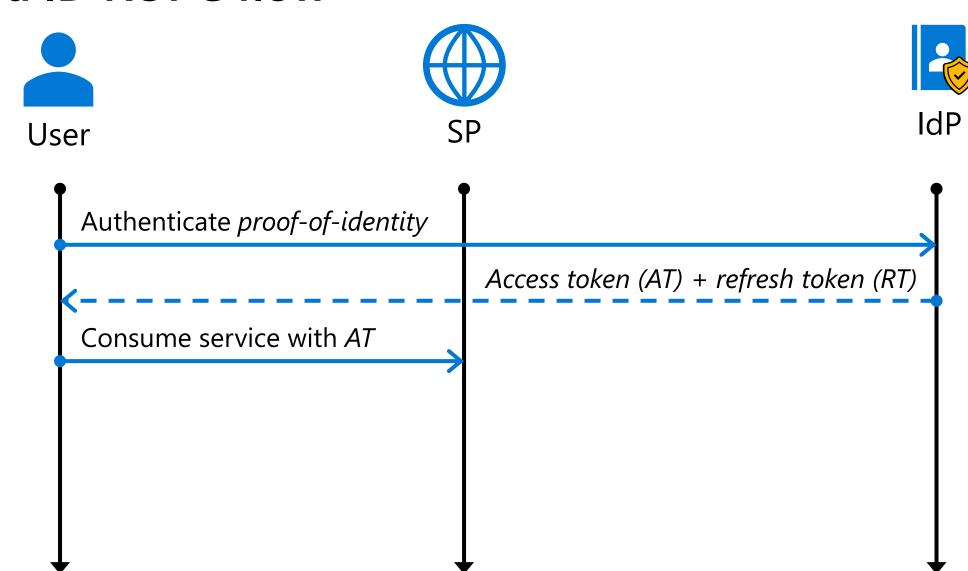


## JSON Web Signature (JWS)

- 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)

#### **Entra ID ROPC flow**



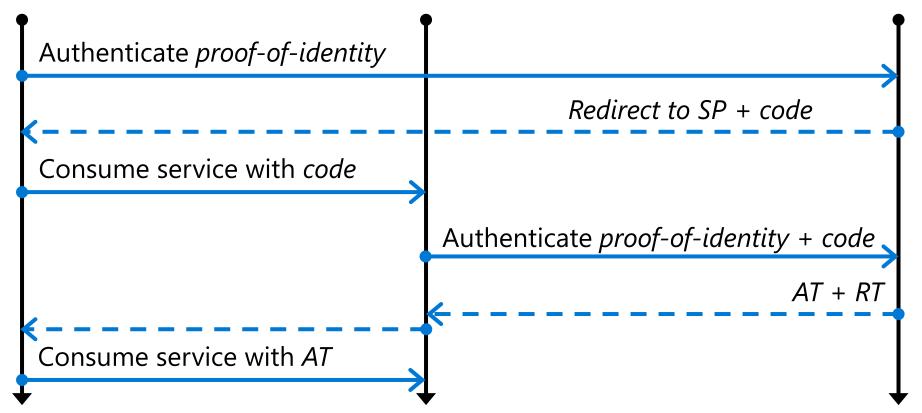
#### Entra ID authorization code flow







IdP

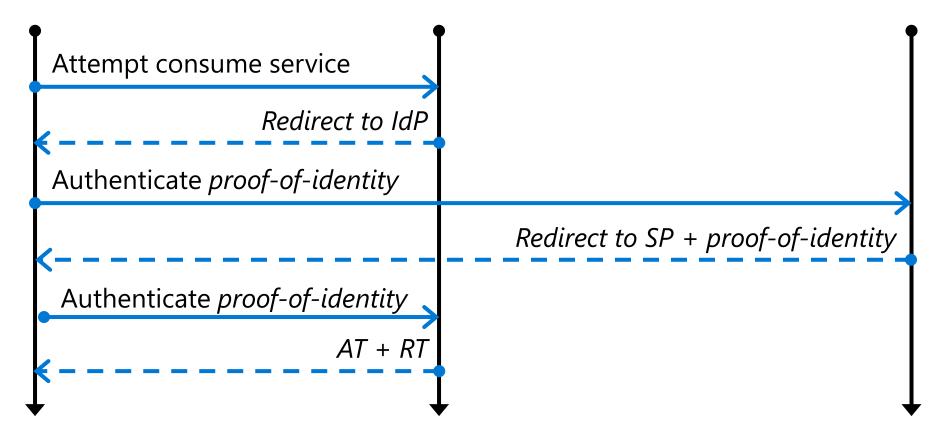


# Entra ID Hybrid authentication flow









# **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

<sup>\*</sup> SAMLp or WS-FED

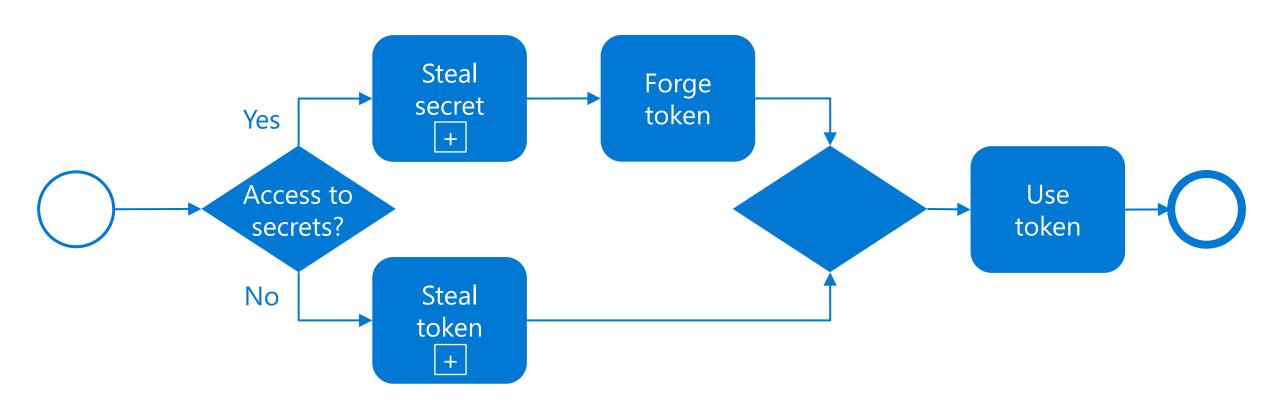
#### Token-based authentication attacks

#### Token based authentication

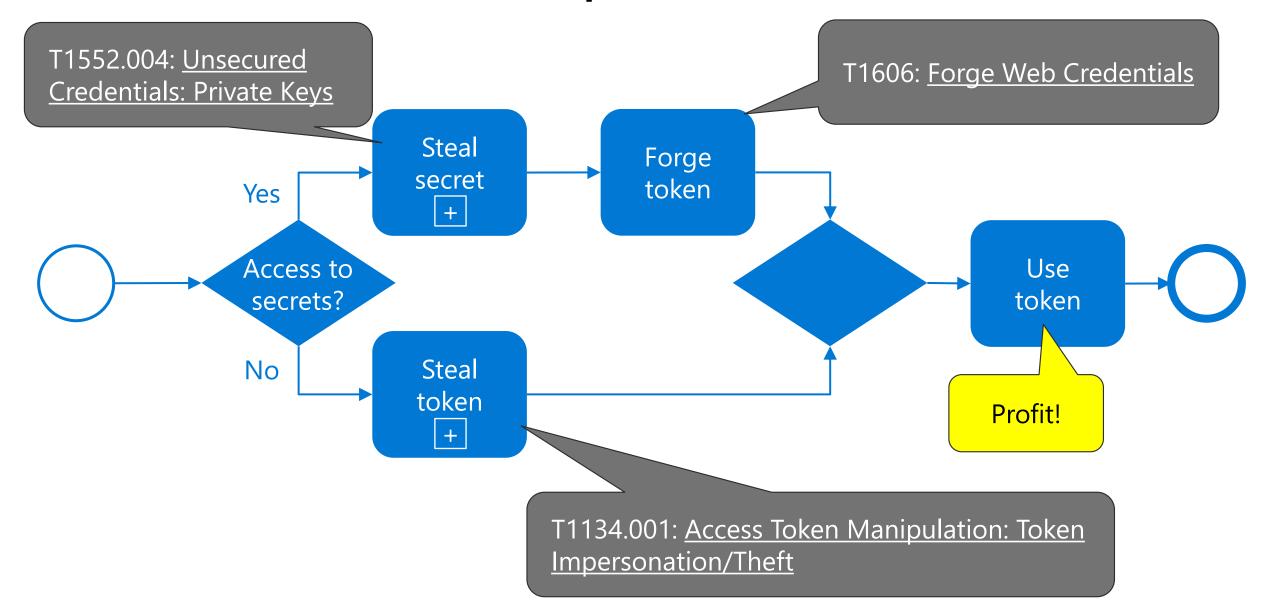
 Any party in possession of a bearer token (a "bearer") can use it to get access to the associated resources (without demonstrating possession of a cryptographic key). To prevent misuse, bearer tokens need to be protected from disclosure in storage and in transport.



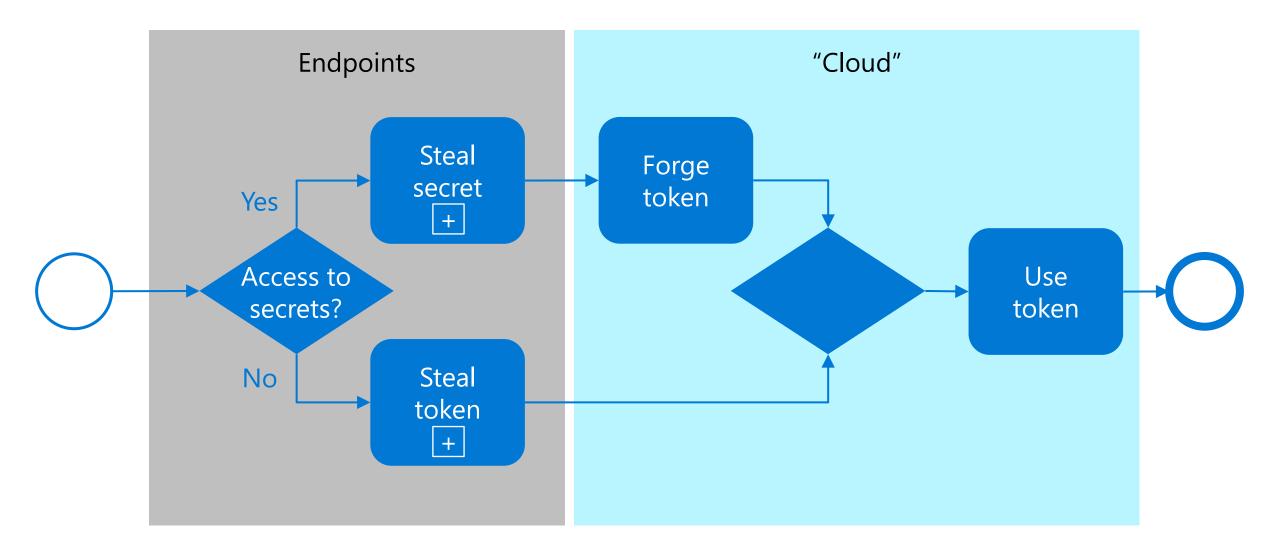
## Token-based authentication attack graph



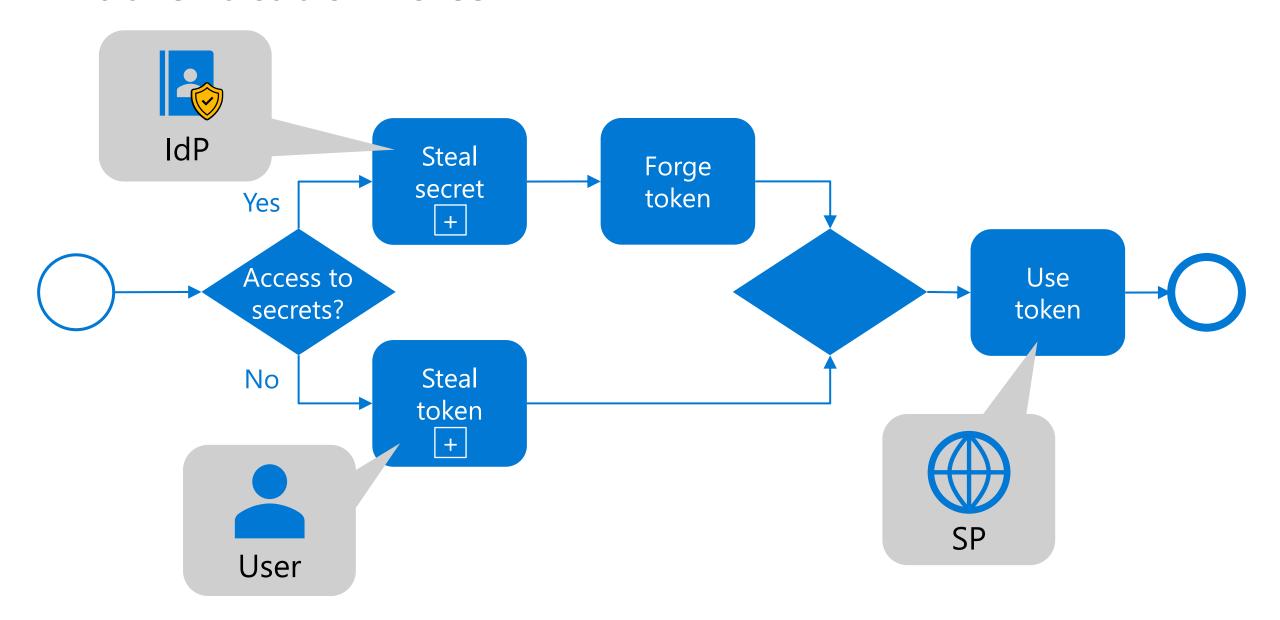
# MITRE ATT&CK® techniques



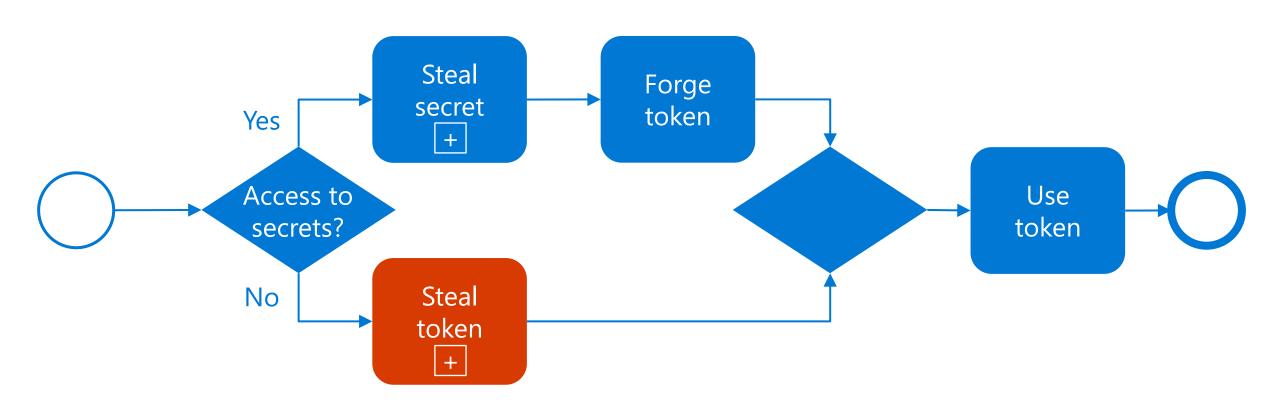
#### Realms



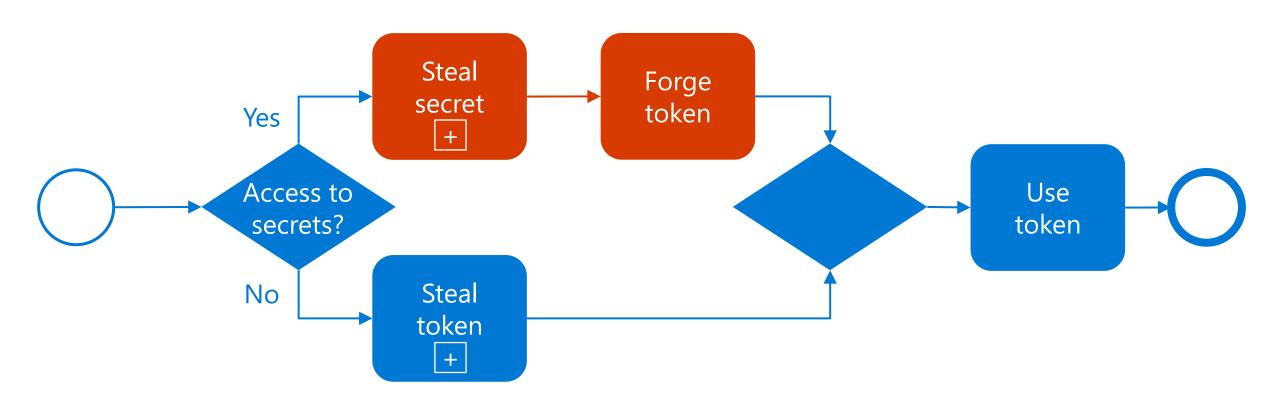
#### **Authentication roles**



# **Demo: Stealing tokens**

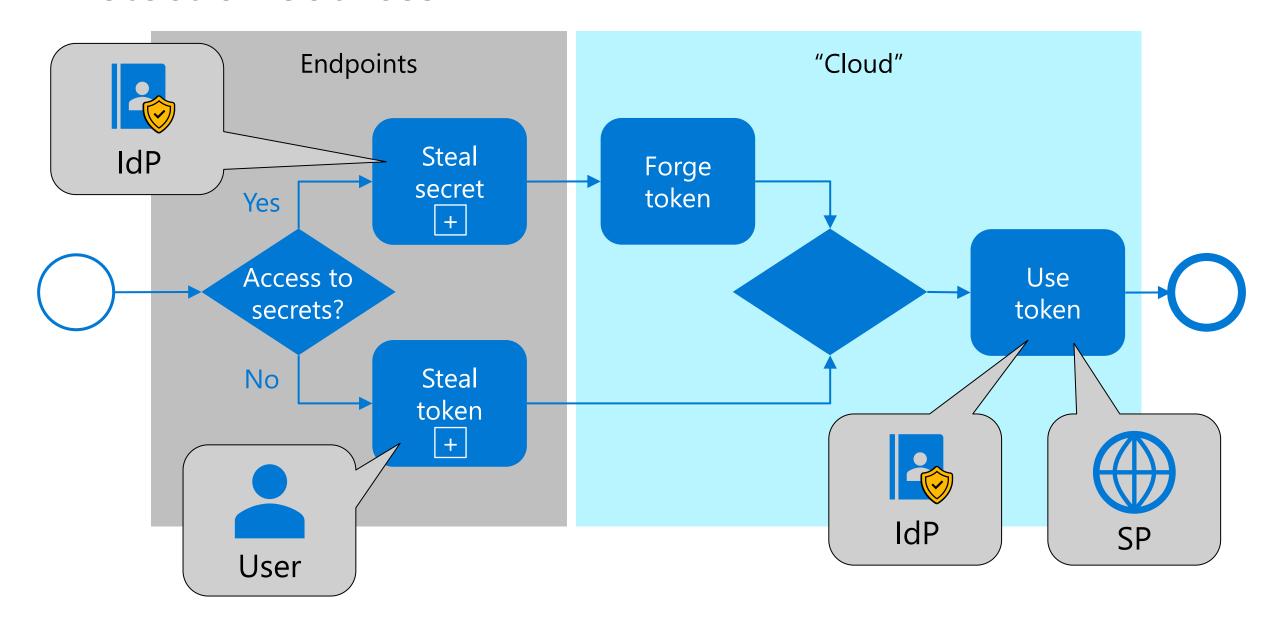


## Demo: Stealing secrets and forging tokens

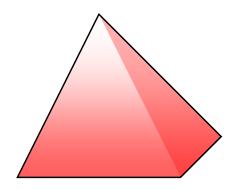


# **Detecting & preventing**

#### **Detection sources**



## Scenario 1: On-prem identity



On-prem Active Directory

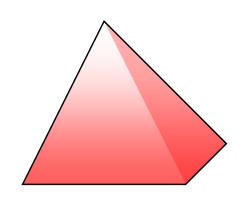




On-prem web server



# Scenario 2: Hybrid identity



On-prem Active Directory





On-prem AD FS



AD FS audit events



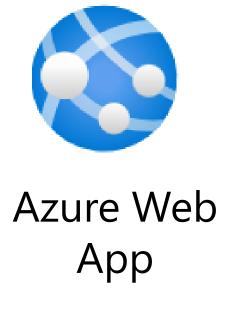
Entra ID



Sign-in logs

# Scenario 3: Cloud-only identity 1









## Scenario 4: Cloud-only identity 2



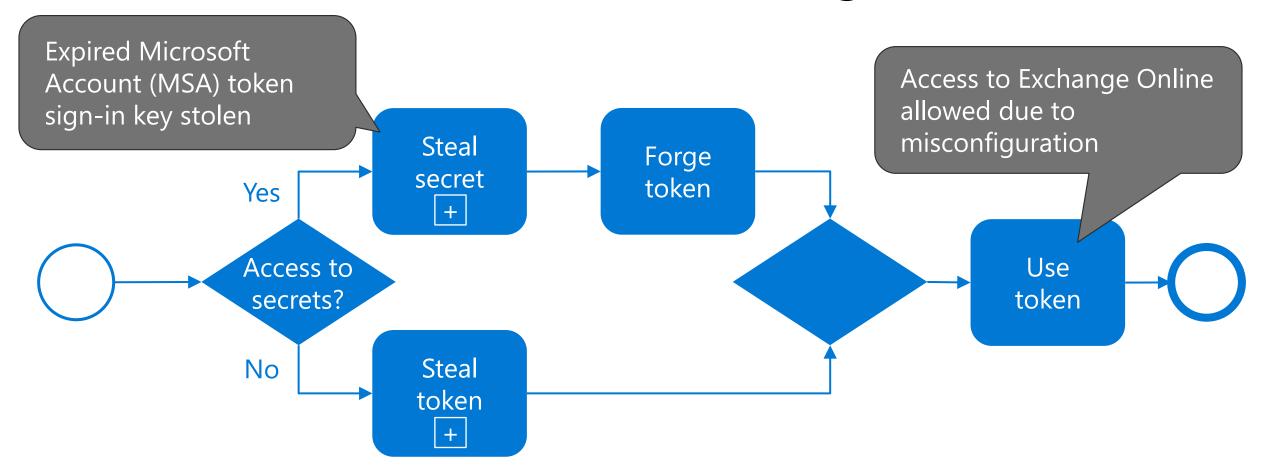








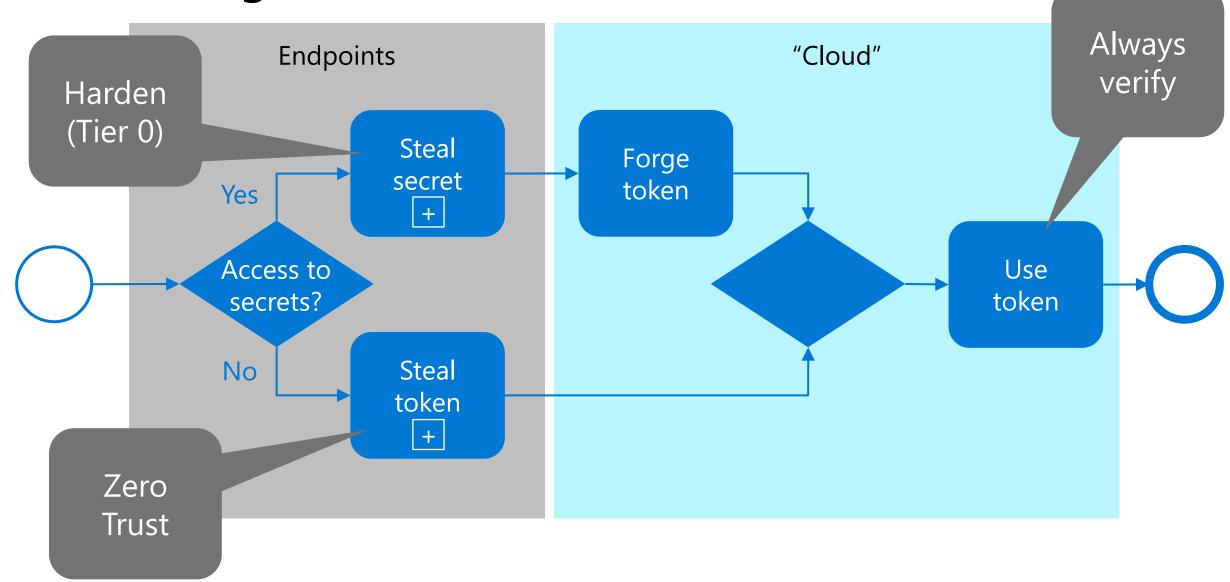
# Storm-0558 accessed emails of 25 organisations



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

