

Demystify Azure AD workload identities

Thomas Naunheim

Microsoft MVP, Cyber Security Architect
@glueckanja-gab AG



Thomas Naunheim

Cyber Security Architect
@glueckkanja-gab AG

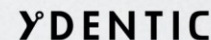
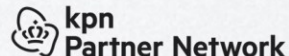
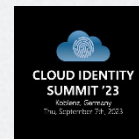
Koblenz, Germany

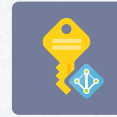


@Thomas_Live



cloud-architekt.net





DIFFERENT TYPES OF
WORKLOAD IDENTITIES



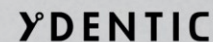
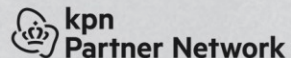
LIFECYCLE MANAGEMENT
AND DELEGATION



DETECTION AND RESPONSE
IN MICROSOFT SECURITY



DIFFERENT TYPES OF WORKLOAD IDENTITIES



Application Identities (Client Secrets)

Workload Identity

Application Instance



Service Principal
(Enterprise App)

Application Definition



Application
(App Registration)



API Permissions



Client Secret



App Roles



Properties

Validation Client Secret

Membership



Azure AD
Roles



Group
Membership

API Access

Admin/User
Consent Permissions

User.Read

Defines Required
Delegated/App Permissions

Exposed API
or App Roles
Permissions



Microsoft
Graph

Microsoft Identity Platform

<https://login.microsoftonline.com/<Tenant>>

/token
Endpoint

Request with
Shared
secret

Token with
API Scope
& Groups

Workload Env.

Shared
Secret



Workload

Authentication
Library

Application Identities (Certificates)

Workload Identity

Application Instance

Service Principal
(Enterprise App)

Application Definition

Application
(App Registration)

API Permissions

Certificate

App Roles

Properties

Validation Public Key

Membership

Azure AD
Roles

Group
Membership

API Access

Granted Admin/User
Consent Permissions

User.Read

Exposed API
or App Roles
Permissions

Microsoft
Graph

Defines Required
Delegated/App Permissions

Microsoft Identity Platform

<https://login.microsoftonline.com/<Tenant>>

/token
Endpoint

Request
with
sign.
JWT
token

Token with
API Scope
& Groups

Workload Env.

Private
/Public Key



Workload

Authentication
Library

Application Identities (Federated Credentials)

Workload Identity

Application Instance

Service Principal
(Enterprise App)

Application Definition

Application
(App Registration)

API Permissions

Federated

App Roles

Properties

Validation ext. Token

Membership

Azure AD
Roles

Group
Membership

API Access

Granted Admin/User
Consent Permissions

User.Read

Exposed API
or App Roles
Permissions

Microsoft
Graph

Microsoft Identity Platform

<https://login.microsoftonline.com/<Tenant>>

/token
Endpoint

Request with
Ext. IdP
token

Token
with
API Scope
& Groups

Workload Env.

Workload

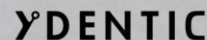
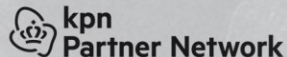
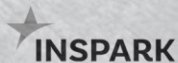
OIDC IdP

Trust relationship



DEMO

Abuse and replay of token from
Federated Workload (GitHub Actions)



System-Assigned Managed Identity

Workload Identity

Application Instance



Service Principal
(Enterprise App)



API
Permissions

Azure Identity Management

Managed Identity Resource Provider
(MSRP)



Certificate

issues certificates
and rolling secrets

Microsoft Identity Platform

<https://login.microsoftonline.com/<Tenant>>

Token with API Scope & Groups

/token
Endpoint

Request with signed JWT token

Membership



Azure AD
Roles



Group
Membership

API Access

Granted Admin/User
Consent Permissions



User.Read

Exposed API
or App Roles
Permissions



Microsoft
Graph

Azure Managed Resource

Assigned 1:1

Managed
Identity
(System)

Workload

Azure Instance
Metadata Service (IMDS)

[http://169.254.169.254/
metadata/identity](http://169.254.169.254/metadata/identity)

Local
Request

/token
Endpoint

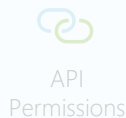
User-Assigned Managed Identity

Workload Identity

Application Instance



Service Principal
(Enterprise App)



Azure Identity Management

Managed Identity Resource Provider
(MSRP)



issues certificates
and rolling secrets
Certificate

Microsoft Identity Platform

<https://login.microsoftonline.com/<Tenant>>

Request with signed JWT token/
Token with API Scope & Groups

/token
Endpoint

Membership



Azure AD
Roles



Group
Membership

API Access

Granted Admin/User
Consent Permissions



User.Read

Exposed API
or App Roles
Permissions

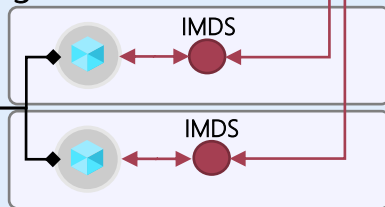


Microsoft
Graph

Azure Managed Resource

Managed
Identity
(User)

Assigned
1:N



Workloads

User-Assigned Managed Identity (Federated)

Workload Identity

Application Instance



Service Principal
(Enterprise App)



Federated

API
Permissions

Validation of ext. Token

Membership



Azure AD
Roles



Group
Membership

API Access

Granted Admin/User
Consent Permissions



User.Read

Exposed API
or App Roles
Permissions



Microsoft
Graph

Microsoft Identity Platform

<https://login.microsoftonline.com/<Tenant>>

/token
Endpoint

Request
with
Ext. IdP
token

Token
with
API Scope
& Groups

Azure



Managed
Identity
(User)

Workload Env.



Workload

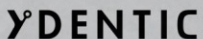
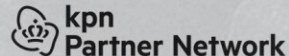
OIDC IdP

Establish Trust
relationship






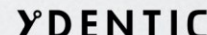
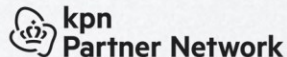
DEMO

Security consideration of Managed Identities,
Cloud Security Explorer and MSIs and
Assignment between resources <> MI object



Comparison of Workload Identity types

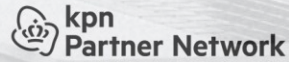
	 Service Principal (Key- or Certificate)	 Service Principal (Federated Credentials)	 Managed Identity (System/User Assign.)
Supported Use Case	No limitation	Limited to supported Workloads (outside of Azure)	Limited to supported Workloads (Azure-managed Resources)
Security Boundary	Single- or multi-tenant	Single- or multi-tenant	Single-tenant*
Relation to Workload	Unassigned	Assigned to Issuer/Entity	Assigned to Resource(s) System (1:1), User (N:1)
Workload Environment	Everywhere	Supported OIDC Federated IdP	Azure- and Azure Arc-enabled resources
Token Lifetime / Cache	1h (Default), 24h (CAE)	less than or equal to 1h	24h (<u>Cache per resource URI</u>)



* access to Azure Resources from onboarded subscriptions via Azure Lighthouse



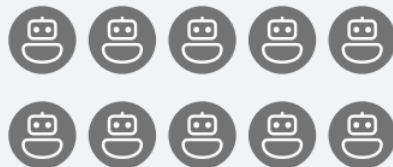
LIFECYCLE MANAGEMENT AND DELEGATION



State of Workload Identity Management

1:10

User identities to
workload identities



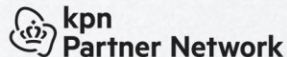
>80%

Of workload identities are
inactive, double the percentage
reported in 2021.



<5%

of permissions are
actually used



Lifecycle Management of Workload Identities

- ❑ Requirements
- ❑ Type of Workload Identity
- ❑ Integration and Auth. Library
- ❑ Definition of Ownership

Planning

- ❑ Create workload identity
- ❑ Assignment of Permissions
- ❑ Delegation and Classification
- ❑ Issuing credentials (if needed)

Provisioning

Deprovision
-ing

- ❑ Remove association
- ❑ Revoke permissions
- ❑ Review ongoing activity
- ❑ Delete workload identity

Monitor and
maintaining

- ❑ Activity and used permissions
- ❑ Suspicious sign-in or changes
- ❑ Delegations and Ownership
- ❑ Change/renewal credentials



Restriction and policies of app management

GET beta https://graph.microsoft.com/beta/policies/appManagementPolicies Run query

Request body Request headers Modify permissions Access token

OK - 200 - 139ms

Response preview Response headers Code snippets Toolkit

```
{
  "@odata.context": "https://graph.microsoft.com/beta/$metadata#policies/appManagementPolicies",
  "value": [
    {
      "id": "943754b8-3000-4fb6-b715-1205becf1d00",
      "deletedDateTime": null,
      "displayName": "Certificates only policy",
      "description": "Disable client secrets and enforce certificate based authentication",
      "isEnabled": true,
      "restrictions": {
        "passwordCredentials": [
          {
            "restrictionType": "passwordAddition",
            "maxLifetime": null,
            "restrictForAppsCreatedAfterDateTime": "2019-01-01T00:00:00.0000000"
          }
        ],
        "keyCredentials": [
          {
            "restrictionType": "asymmetricKeyLifetime",
            "maxLifetime": "P90D",
            "restrictForAppsCreatedAfterDateTime": "2014-01-01T00:00:00.0000000",
            "certificateBasedApplicationConfigurationIds": []
          }
        ]
      }
    }
  ]
}
```

Home > C4A8 Ando | App registrations > aadops-privilegedaccess-sp

aadops-privilegedaccess-sp | Certificates & secrets

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (1) Federated credentials (0)

Client secrets are blocked by a tenant-wide policy. Contact your tenant administrator for more information.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

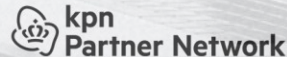
+ New client secret

Description	Expires	Value	Secret ID
identityops-kva	5/29/2023	Cm6*****	b8934654-76c2-41fa-81b0-539025a8e...



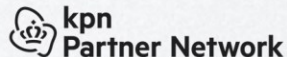
DEMO

Default Permission, AAD Recommendations,
Delegation and Classification



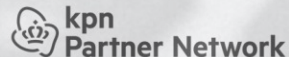
Workload Identities Premium?

Feature	Free (Azure AD License)	Premium (\$3/Month/Service Principal)
Authentication, Authorization, Sign-in and Audit Logs	Yes	Yes
Conditional Access	No	Yes
Access Reviews	No	Yes
Identity Protection	No	Yes
App Management Policies	No	Yes
MDA App Governance	Add-on to MDA, free for E5 customers (starting June 1 st , 2023)	
Entra Permission Management	Standalone product, \$125 per resource, per year	

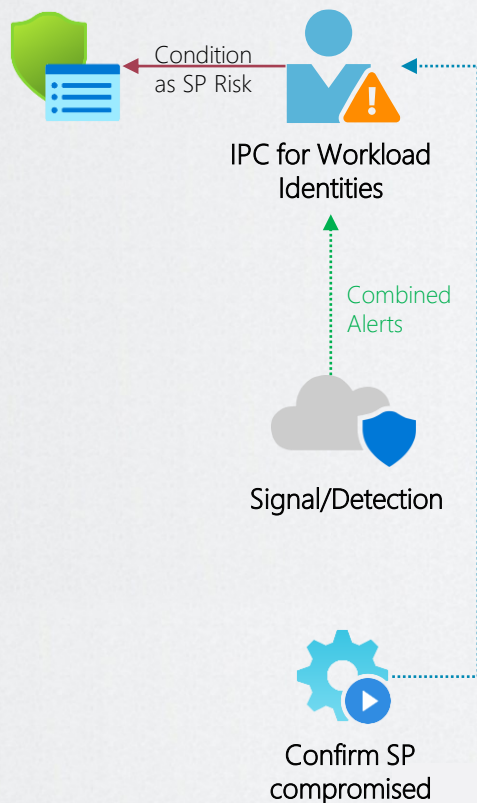




DETECTION AND RESPONSE WITH MICROSOFT SECURITY



Threat Intelligence and CA Integration



Azure AD Identity Protection (IPC)

- Suspicious Sign-ins
- Leaked Credentials (from GitHub)
- Anomalous service principal activity
- ...

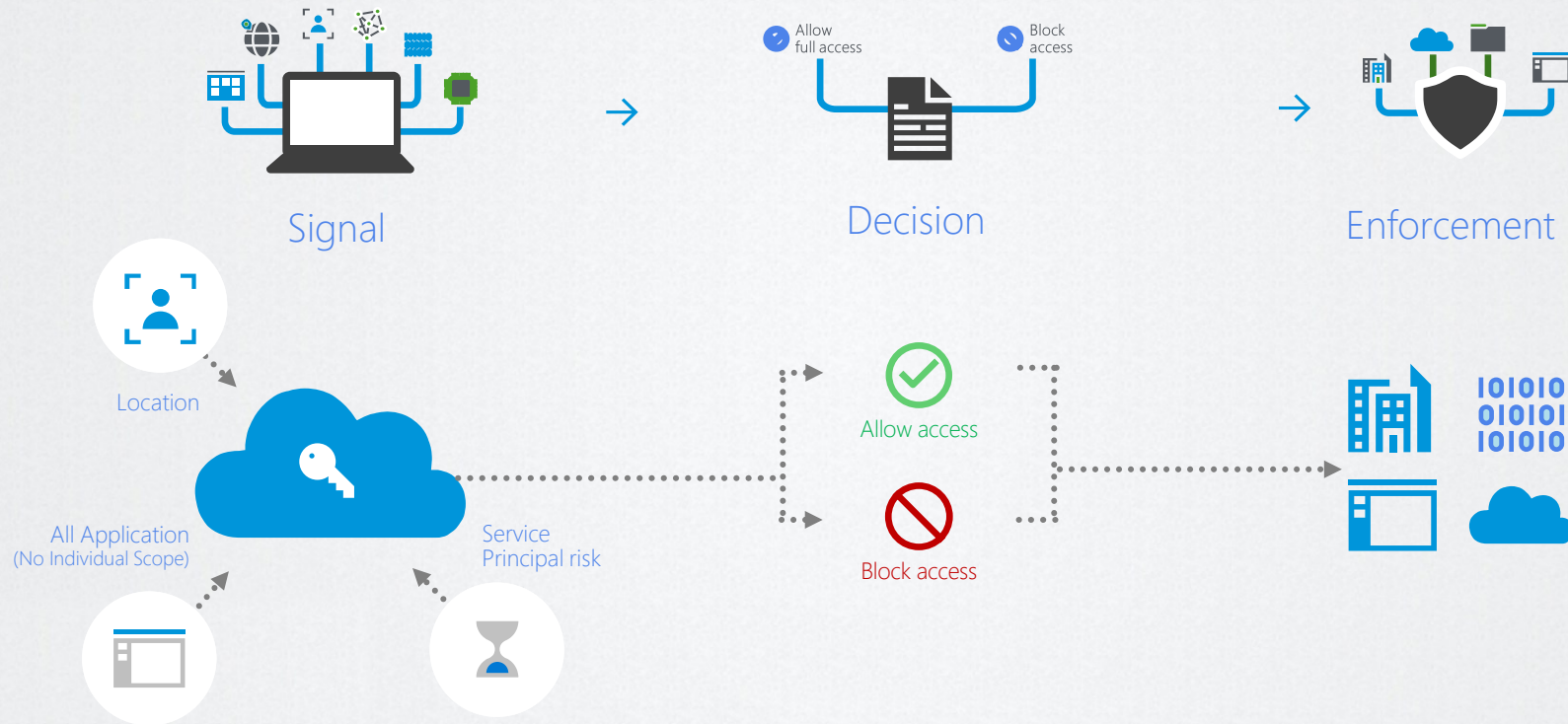
Microsoft Defender for Cloud Apps (MDA)

- Malicious application, Suspicious application
- Unusual addition of credentials to an OAuth app, Unusual ISP for an OAuth app
- ... Azure AD app registration by risky user

Microsoft Sentinel Analytics Rules (Custom Detections)

- Credential added to sensitive Workload Identity by lower-privileged user
- Federated Credential has been created for GitHub entity outside of organization
- ...

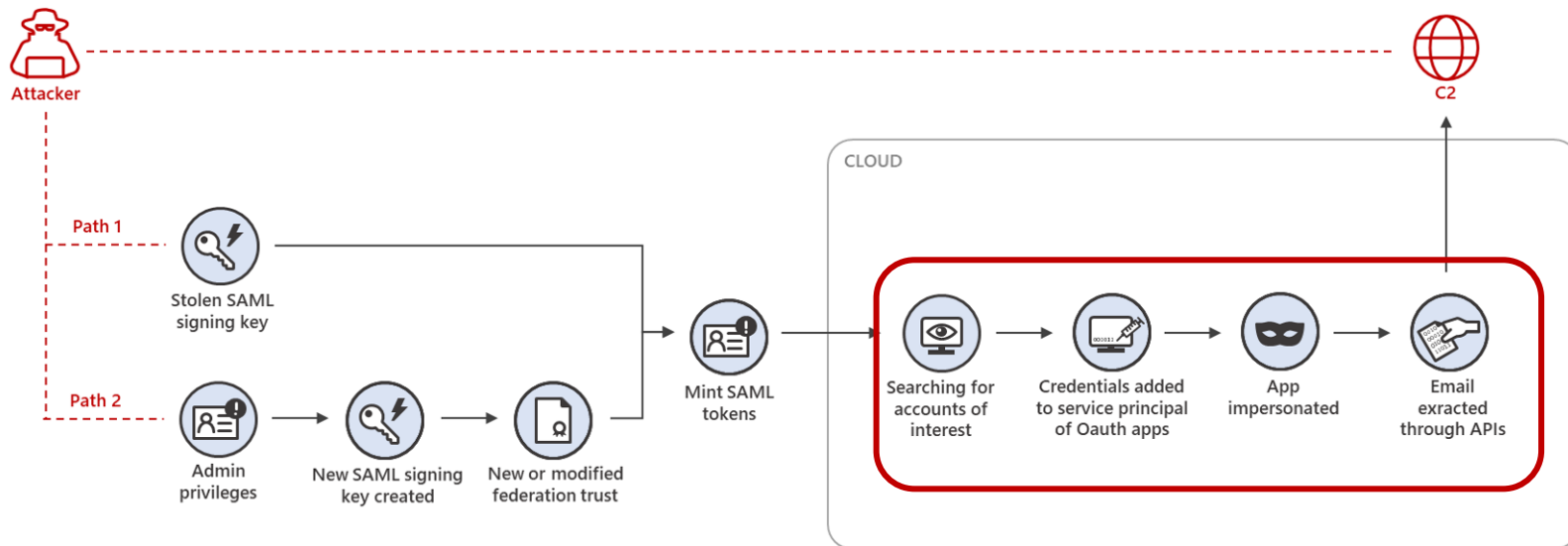
Conditional Access for Workload Identities



Attackers Service Principals

SOLORIGATE ATTACK

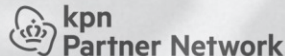
Stage 3: Hands-on-keyboard attack in the cloud





DEMO

Sentinel Analytics Rules,
Workload Identity Premium Features,
MDA App Governance,
Enrichment of Entities and Custom Tables



Summary | Take Aways



Consider secure implementation of authentication library, storing credentials and token caching
Avoid long-term credentials and verify security of trusted entities for Workload Identity Federation
Implement application management policy to govern credential issuing



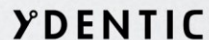
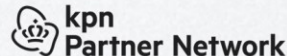
Implement an application and lifecycle management
Consider Azure AD roles and ownership with permissions on application/service principal objects
Classify your application to detect privilege escalation paths and sensitivity of workload identity



Apply Conditional Access Policies for Service Principals and monitor risk detection
Monitor used/unused permissions and activity (IP address and type of access) after AuthN/AuthZ
Implement playbooks to automate response on suspicious sign-in or activity of service principals



Deploy rule templates and integrate MDA App Governance
Build detection to build correlation and enrichment by classification data
Monitor trusted entities/IdP (for Federated Credentials) and resources with assigned MSI particularly
Review and integrate enriched data ([AzADServicePrincipalInsights](#) by Julian Hayward)





Thanks for your attention!

Feedback & Questions



@Thomas_Live



Cloud-Architekt.net





Please rate my session in
the Yellenge app!

