Clone Service Principal

Azure

Agenda

- Goal Definition
- Requirements
- Problem Statement
- Going Forward Plan Definition
- Risks (Threat Model)

GOAL

Create a Service Principal (SPN) that can create other Service Principals

Goal	Functional Requirement
Automated Azure AD object creation	API • Microsoft Graph Permission • Application.ReadWrite.OwnedBy Admin Consent • True Application resource permissions
Read Azure AD Objects Write Azure AD Objects	API • Microsoft Graph Permission • User.Read • Directory.Read.All • Directory.ReadWrite.All Admin Consent • True Integrate Azure Active Directory with Azure Kubernetes Service
Request Permissions	Application Owner
Grant Permission	Tenant Administrator • Application Administrator * Global Administrator Application Administrator

Requirements

Non-Functional Requirements

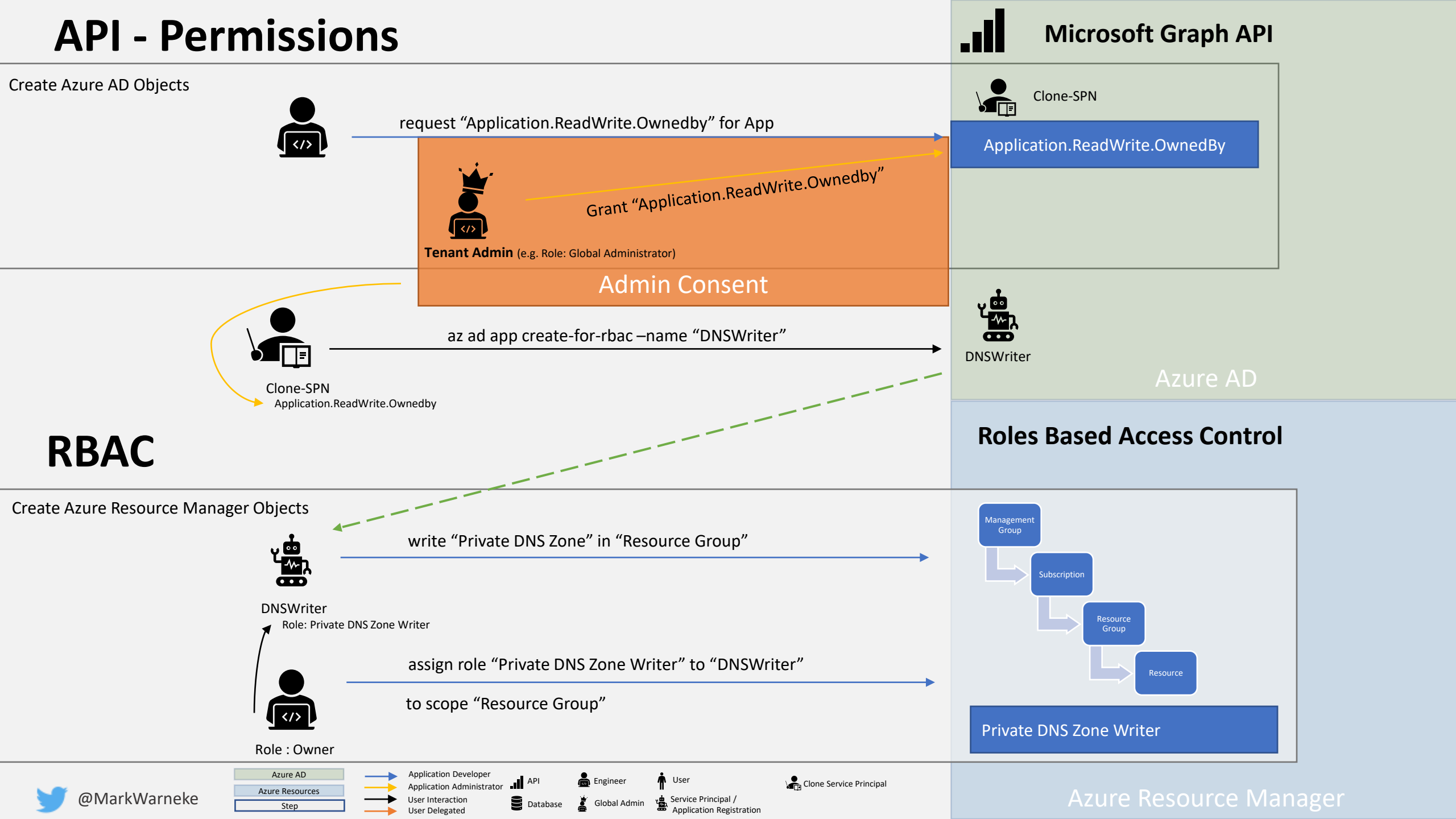
- Governance
  What is Azure AD Identity Governance
  - Tracing
    - Creation
    - Usage (Historization)
    - Archive
  - Monitoring
  - Application assignment
  - Owner
  - Notification (SPOC)
  - App Retirement
- Key Rotation
- Protection
- Azure AD Quota Limits
  Grant permission to create unlimited app registrations
- Azure Policies

* Application Administrator: This role also grants the ability to *consent* to delegated permissions and application permissions, with the exception of permissions on the Microsoft Graph API [1]

Azure AD Permissions & Roles vs Azure Resource Manager Roles

Differences and Comparison

API - Permissions



Problem Statement

01

Create Service Principal automatically

02

Request permissions automatically

03

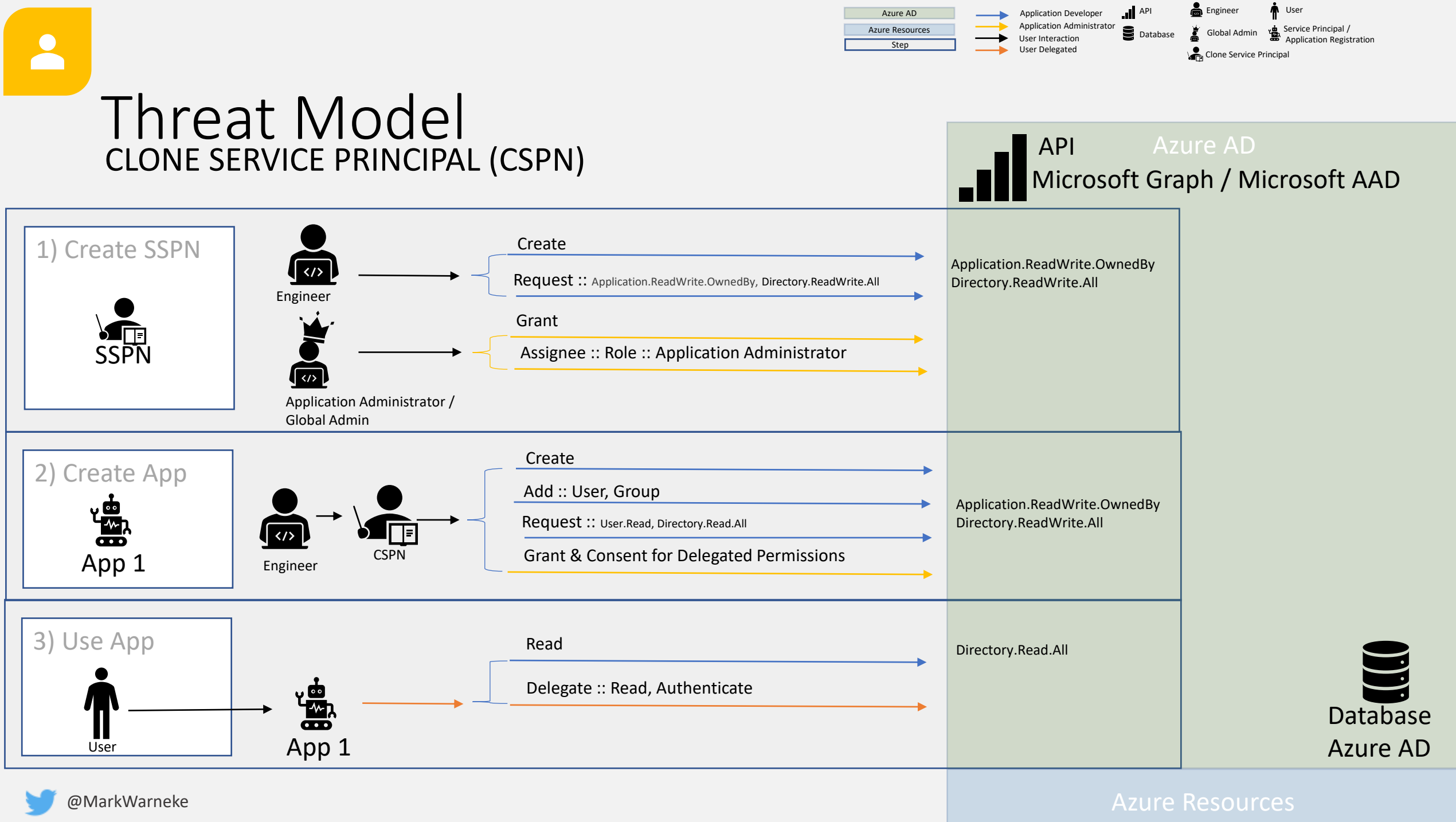
Grant permissions automatically

04

Establish Governance structure

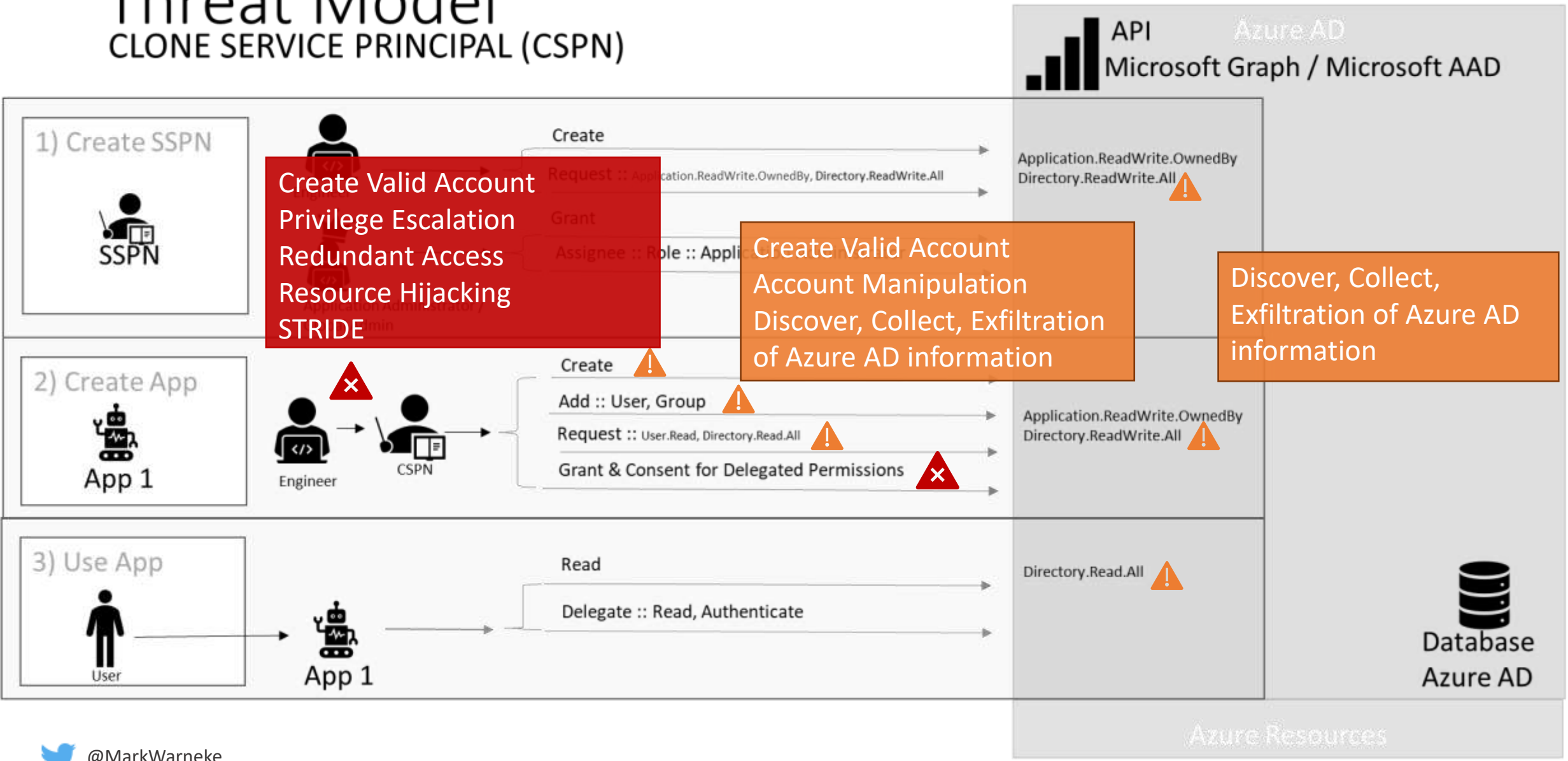
Solutions Inspection

CLONE SERVICE PRINCIPAL


Azure AD
Azure Resources
Step
Application Developer
Application Administrator
User Interaction
User Delegated
API
Database
Engineer
Global Admin
Clone Service Principal
User
Service Principal / Application Registration
Threat Model
CLONE SERVICE PRINCIPAL (CSPN)
API
Azure AD
Microsoft Graph / Microsoft AAD
1) Create SSPN
SSPN
Engineer
Application Administrator / Global Admin
Create
Request :: Application.ReadWrite.OwnedBy, Directory.ReadWrite.All
Grant
Assignee :: Role :: Application Administrator
Application.ReadWrite.OwnedBy
Directory.ReadWrite.All
2) Create App
App 1
Engineer
CSPN
Create
Add :: User, Group
Request :: User.Read, Directory.Read.All
Grant & Consent for Delegated Permissions
Application.ReadWrite.OwnedBy
Directory.ReadWrite.All
3) Use App
User
App 1
Read
Delegate :: Read, Authenticate
Directory.Read.All
Database
Azure AD
@MarkWarneke
Azure Resources

Threat Model

CLONE SERVICE PRINCIPAL (CSPN)



@MarkWarneke

SPECIAL SERVICE PRINCIPAL

Threat (MITRE ATT&CK)

Below are the tactics and technique representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques.

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery / Collection / Exfiltration	Impact
Create Valid Accounts (Rogue) Creation of malicious application associated to the Azure AD tenant. (Rogue)	Use for Account Manipulation (Rogue) Created Redundant Access (Rogue) Create Valid Accounts (Rogue)	Valid Accounts (Rogue)	Redundant Access, Valid Accounts (Rogue)	Account Manipulation (Rogue) Leakage of synced secrets & custom identity properties *	Enumerate Azure AD (Rogue)	Resource Hijacking accidental deletion of Azure AD objects like application registrations. deliberate deletion of Azure AD objects by a rogue admin.

* Due to forest migration secrets are synced to Azure AD

https://attack.mitre.org/matrices/enterprise/cloud/azure/

SPECIAL SERVICE PRINCIPAL

Threat (STRIDE)

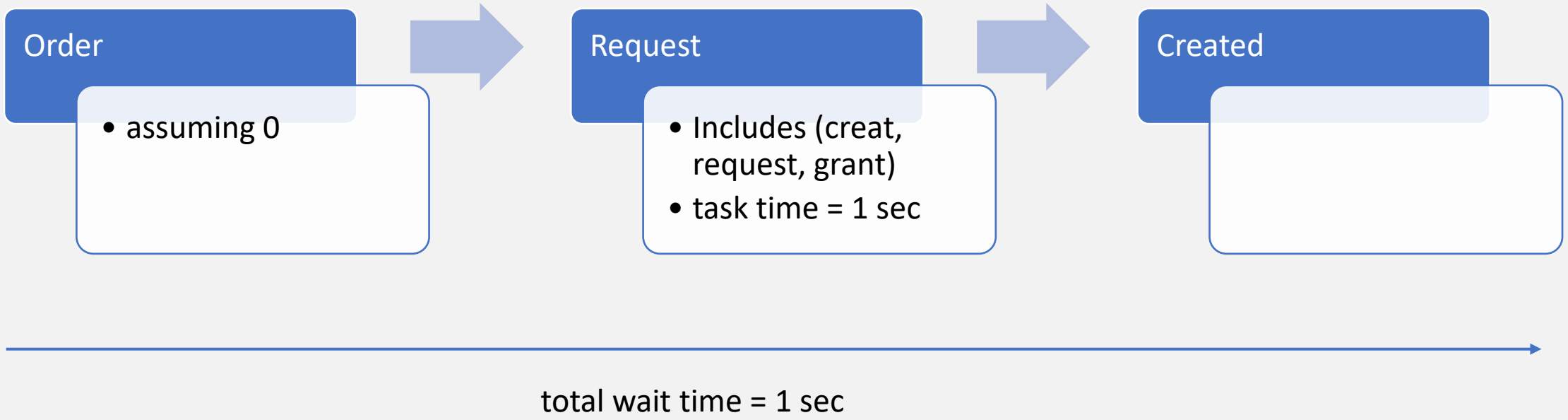
STRIDE categorizes different types of threats and simplifies the overall security conversations.

Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Creation of malicious application associated to the Azure AD tenant	Use for Account Manipulation, grant access to Application Registrations of others	Service Principal not User Principal	Use for Account Manipulation, grant access to Application Registrations of others Gather employee data	accidental & deliberate deletion of Azure AD objects	Use to elevate access of user / service principals

https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats#stride-model

ANALYSIS SPECIAL SERVICE PRINCIPAL

Value Stream Mapping



Touch time = 1/1 = 1 = 100%
0 % lead time

Analysis Special Service Principal

Risk Quantity (applicable/ identified risk)	**20/20**	
Risk Impact	**Severe**	Compromise of Azure AD possible, elevated permissions possible (tenant admin)
Grad of Automation (based on handover)	**High**	No Handover

01

Create Service Principal automatically

02

Request permissions automatically

03

Grant permissions automatically

04

Establish Governance structure

Service Principal Creator/Factory

- Service Principal to create other service principal
- Create and request predefined & limited (least privilege) permissions based on automation process
- Notification of tenant admin

Pool Approval

Administrator approves pools of created service principals based on predefined process and convention given risk acceptance & approval
- “Standard” change

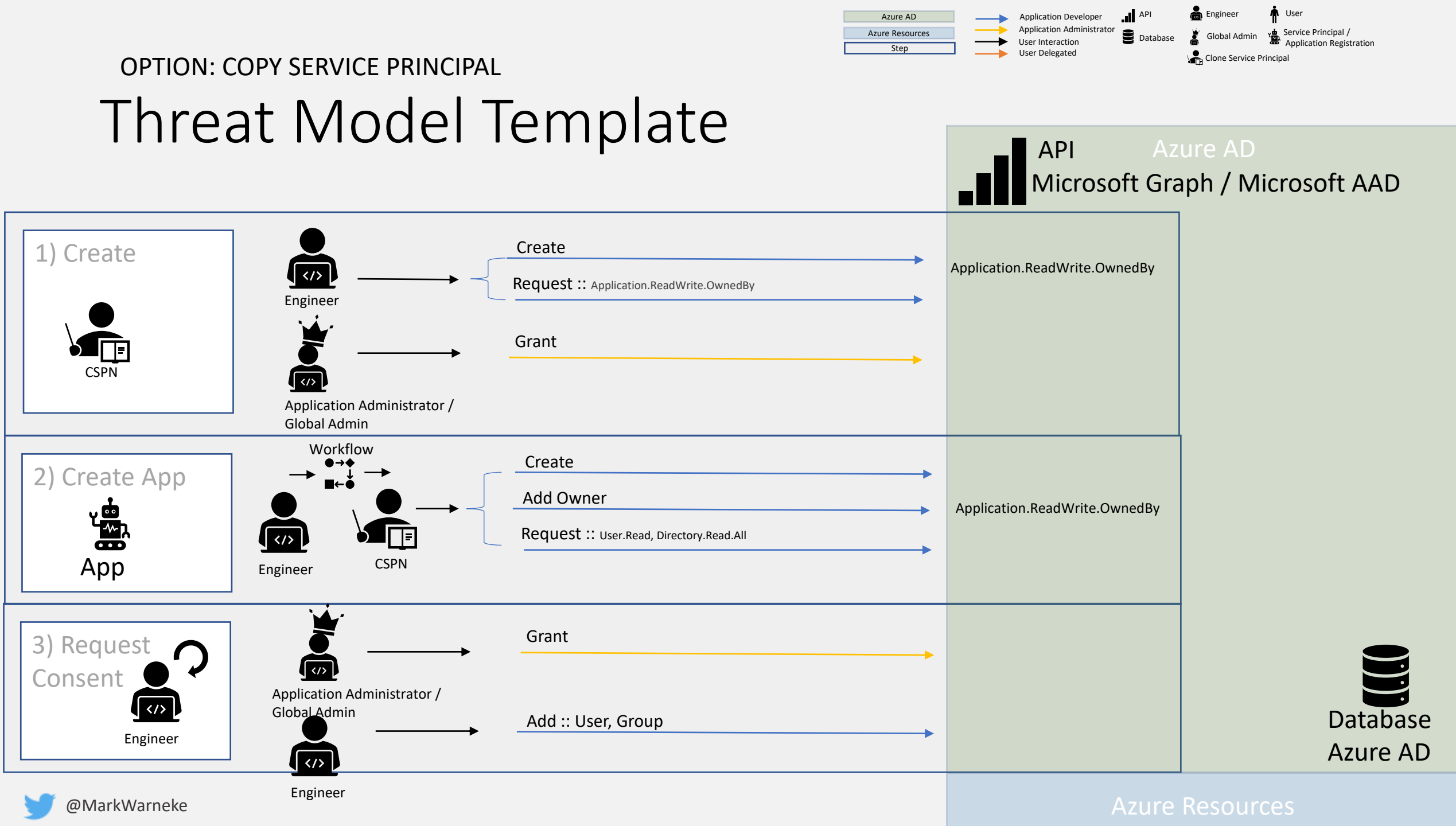
Ownership

assign and manage service principals per customer given approved/granted permissions
(same as before)

Option

OPTION: COPY SERVICE PRINCIPAL

Threat Model Template



@MarkWarneke

CENTRAL SERVICE SERVICE PRINCIPAL

Threat (MITRE ATT&CK)

Below are the tactics and technique representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques.

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery / Collection / Exfiltration	Impact
~~Create Valid Accounts (Rogue)~~ ~~Creation of malicious application associated to the Azure AD tenant. (Rogue)~~	~~Use for Account Manipulation (Rogue)~~ ~~Created Redundant Access (Rogue)~~ ~~Create Valid Accounts (Rogue)~~	~~Valid Accounts (Rogue)~~	~~Redundant Access, Valid Accounts (Rogue)~~	~~Account Manipulation (Rogue)~~ ~~Leakage of synced secrets & custom identity properties *~~	~~Enumerate Azure AD (Rogue)~~	Resource Hijacking accidental deletion of Azure AD objects like application registrations. deliberate deletion of Azure AD objects by a rogue admin.

* Due to forest migration secrets are synced to Azure AD

https://attack.mitre.org/matrices/enterprise/cloud/azure/

CENTRAL SERVICE SERVICE PRINCIPAL

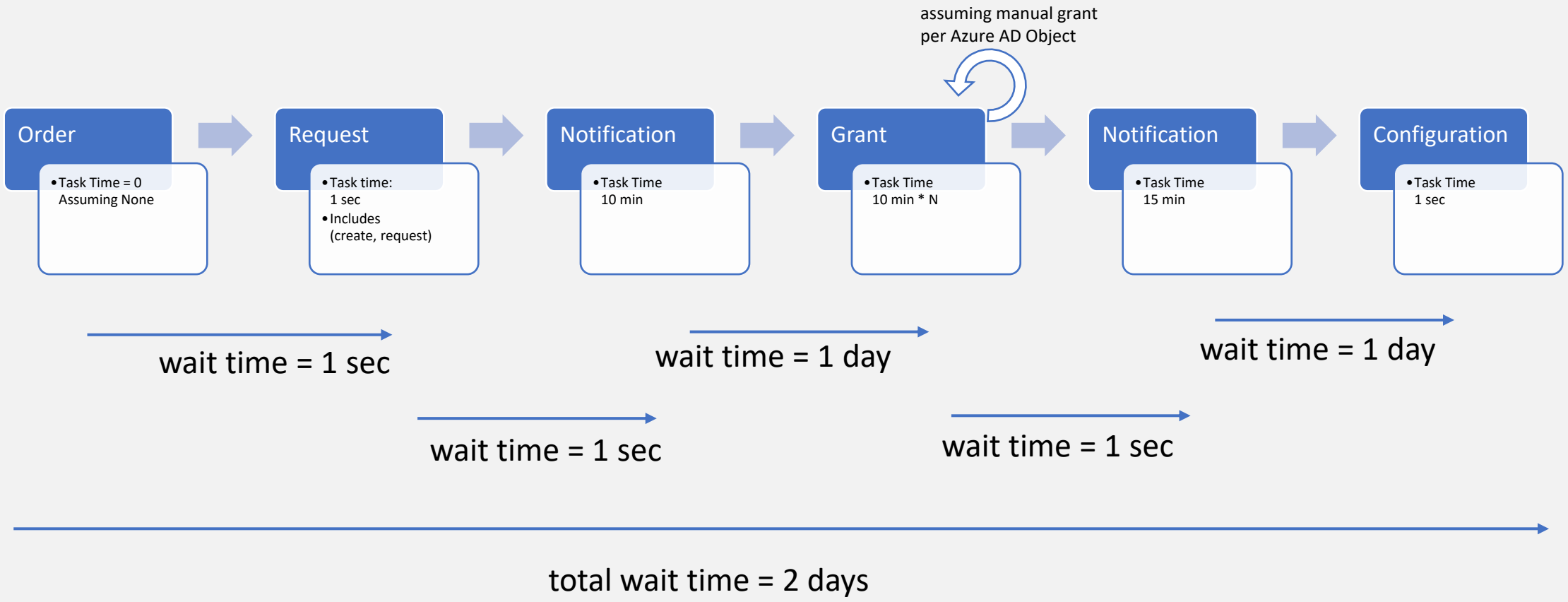
Threat (STRIDE)

STRIDE categorizes different types of threats and simplifies the overall security conversations.

Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
~~Creation of malicious application associated to the Azure AD tenant~~	~~Use for Account Manipulation, grant access to Application Registrations of others~~	~~Service Principal not User Principal~~	~~Use for Account Manipulation, grant access to Application Registrations of others~~ Gather employee data	~~accidental & deliberate deletion of Azure AD objects~~	~~Use to elevate access of user / service principals~~

OPTION: COPY SERVICE PRINCIPAL

Value Stream Mapping



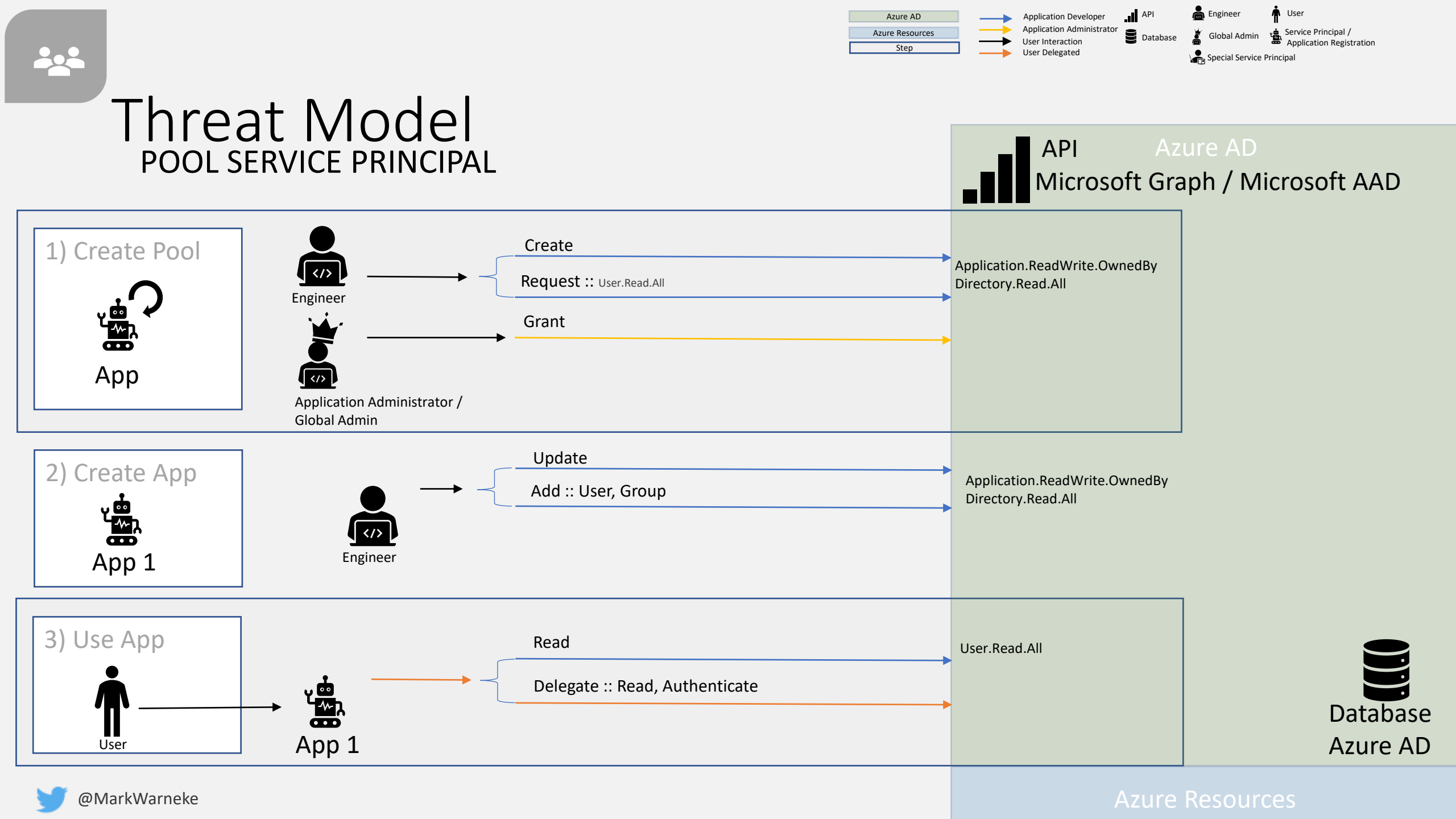
touch time = 10 / 960 = 0.0104 = 1.04 %
98.95% of lead time

@MarkWarneke

Others Solution Inspection

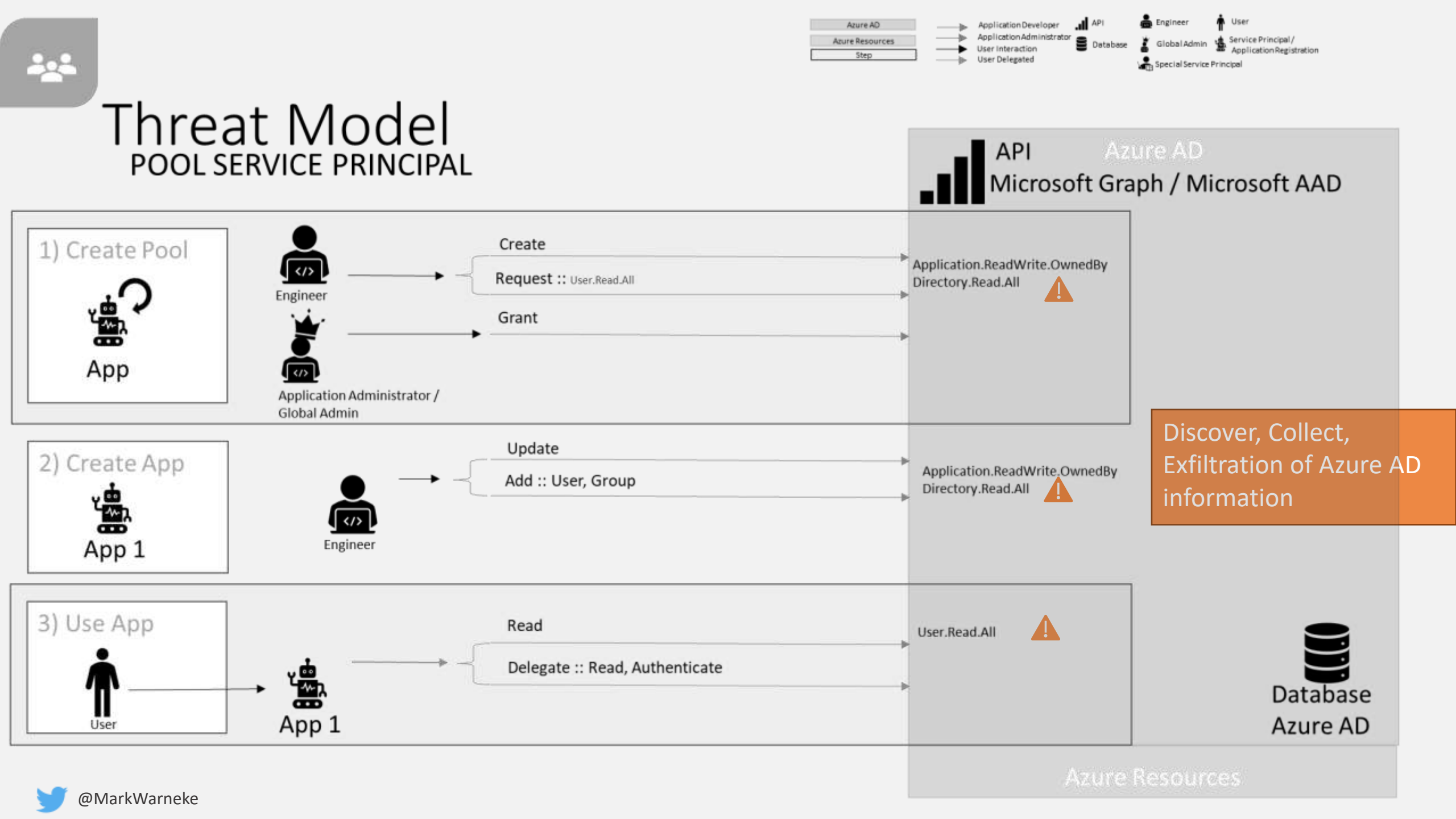
POOL OF SERVICE PRINCIPALS

CENTRAL SERVICE FOR APPROVAL PROCESS


Azure AD
Azure Resources
Step
Application Developer
Application Administrator
User Interaction
User Delegated
API
Database
Engineer
Global Admin
Special Service Principal
User
Service Principal / Application Registration
Threat Model
POOL SERVICE PRINCIPAL
API
Azure AD
Microsoft Graph / Microsoft AAD
1) Create Pool
App
Engineer
Application Administrator / Global Admin
Create
Request :: User.Read.All
Grant
Application.ReadWrite.OwnedBy
Directory.Read.All
2) Create App
App 1
Engineer
Update
Add :: User, Group
Application.ReadWrite.OwnedBy
Directory.Read.All
3) Use App
User
App 1
Read
Delegate :: Read, Authenticate
User.Read.All
Database
Azure AD
@MarkWarneke
Azure Resources

Threat Model

POOL SERVICE PRINCIPAL



@MarkWarneke

POOL SERVICE PRINCIPAL

Threat (MITRE ATT&CK)

Below are the tactics and technique representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques.

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery / Collection / Exfiltration	Impact
~~Create Valid Accounts (Rogue)~~ ~~Creation of malicious application associated to the Azure AD tenant. (Rogue)~~	~~Use for Account Manipulation (Rogue)~~ ~~Created Redundant Access (Rogue)~~ ~~Create Valid Accounts (Rogue)~~	~~Valid Accounts (Rogue)~~	~~Redundant Access, Valid Accounts (Rogue)~~	~~Account Manipulation (Rogue)~~ Leakage of synced secrets & custom identity properties *	Enumerate Azure AD (Rogue)	~~Resource Hijacking~~ ~~accidental deletion of Azure AD objects like application registrations.~~ ~~deliberate deletion of Azure AD objects by a rogue admin.~~

* Due to forest migration secrets are synced to Azure AD

https://attack.mitre.org/matrices/enterprise/cloud/azure/

POOL SERVICE PRINCIPAL

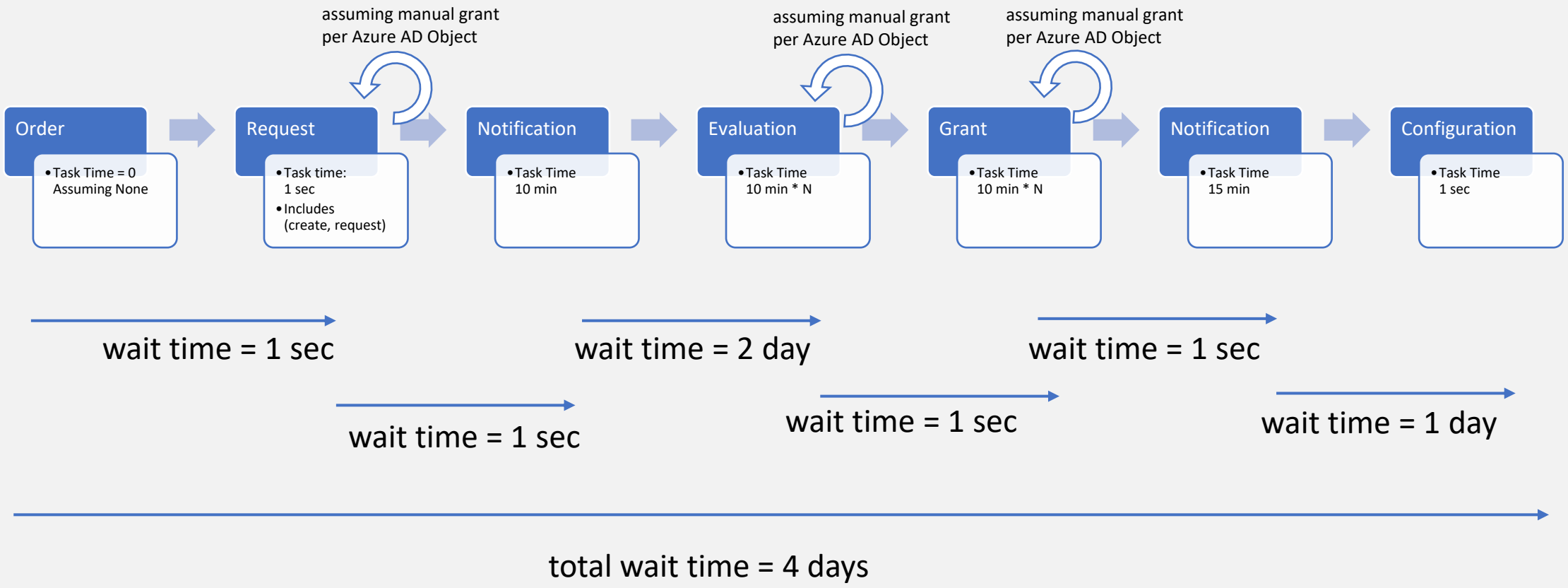
Threat (STRIDE)

STRIDE categorizes different types of threats and simplifies the overall security conversations.

Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
~~Creation of malicious application associated to the Azure AD tenant~~	~~Use for Account Manipulation, grant access to Application Registrations of others~~	~~Service Principal not User Principal~~	~~Use for Account Manipulation, grant access to Application Registrations of others~~ Gather employee data	~~accidental & deliberate deletion of Azure AD objects~~	~~Use to elevate access of user / service principals~~

POOL SERVICE PRINCIPAL

Value Stream Mapping

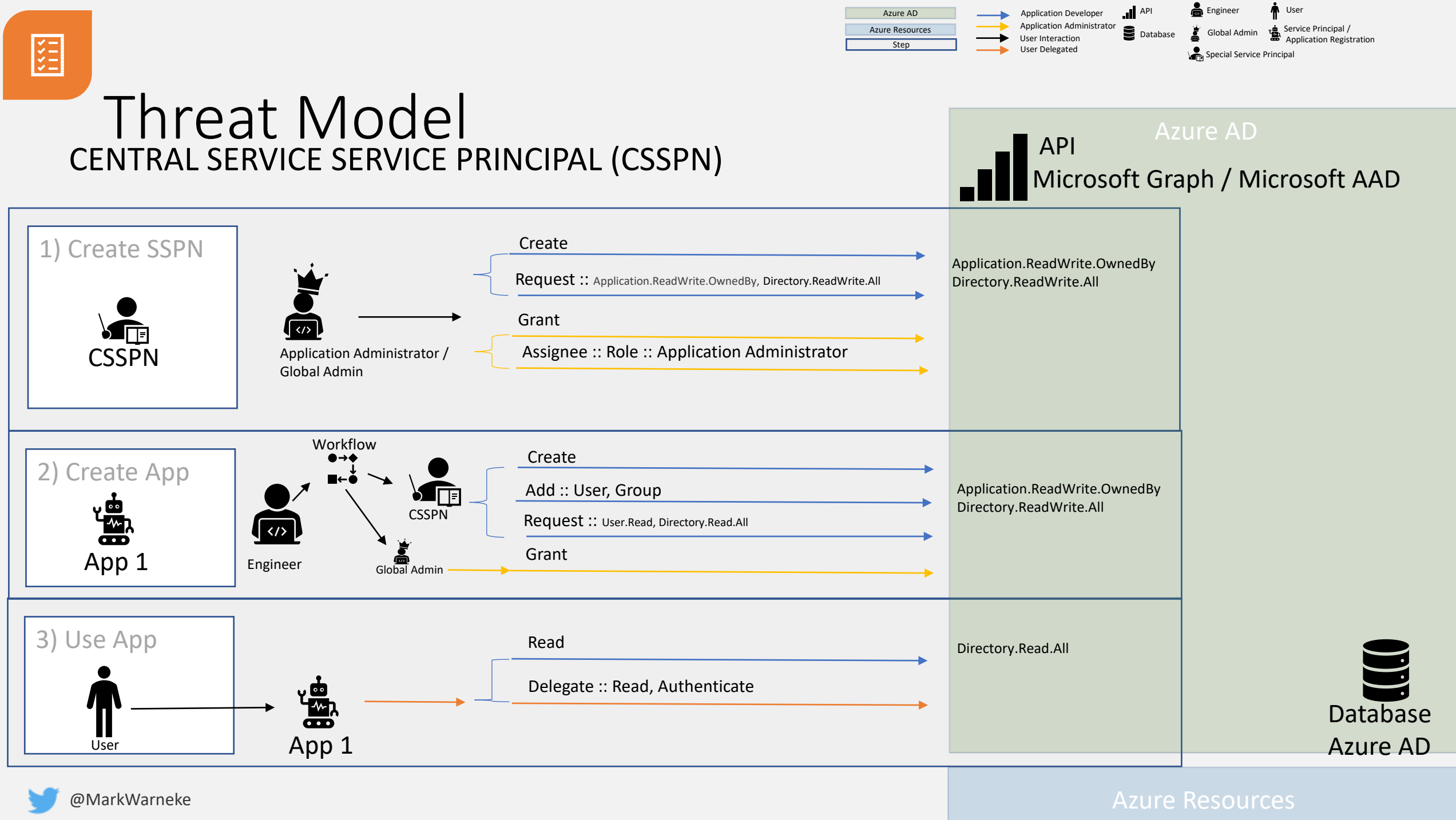


touch time = 10 / 1920 = 0.0052 = 0.52 %
99.5% of lead time

@MarkWarneke

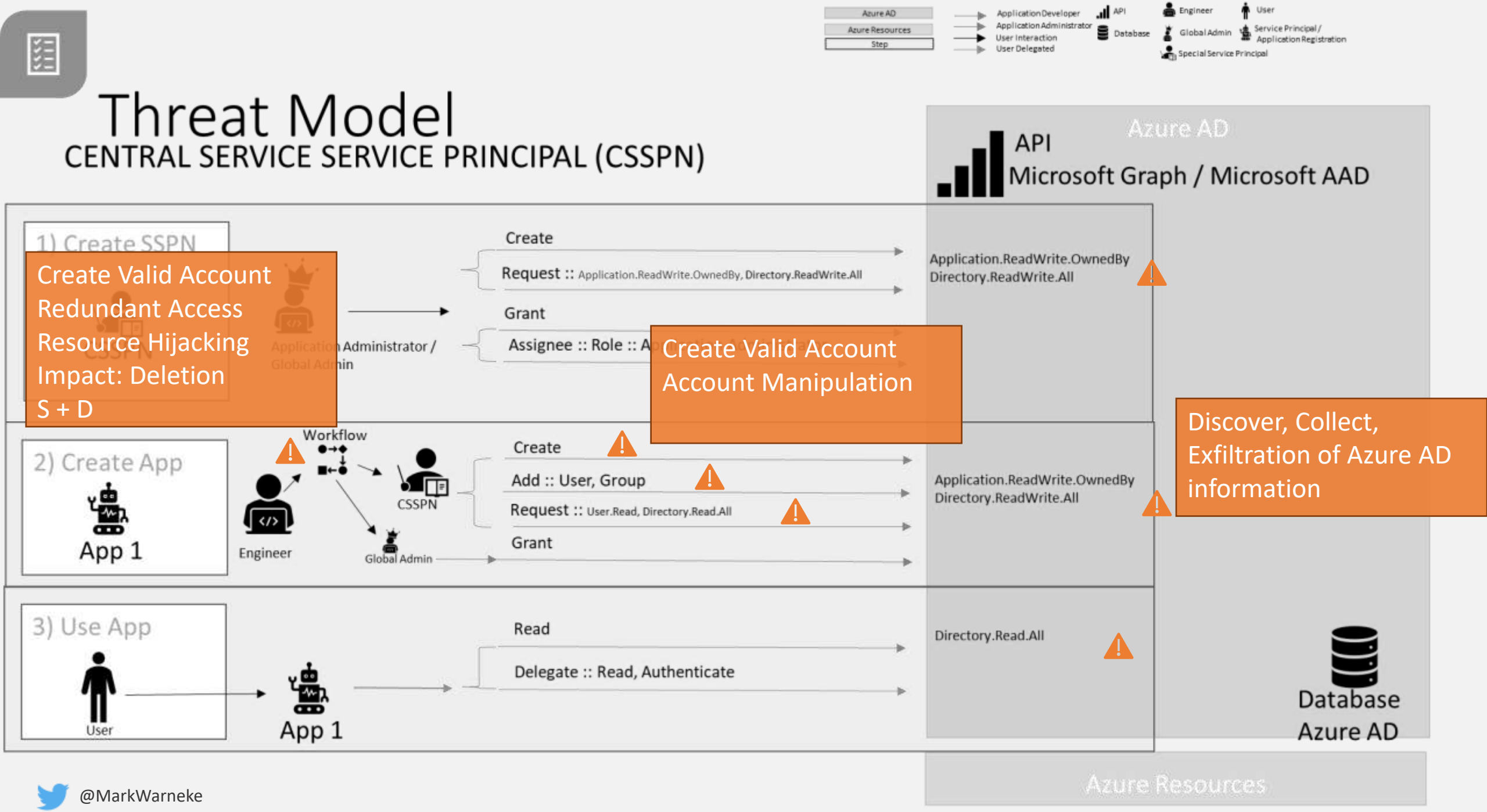
Analysis Pool Service Principal

Risk Quantity (applicable/ identified risk)	**3/20**	
Risk Impact	**Low**	Low, as pool like manual but in batches, can be specified and approved once including definition of permissions etc.
Grad of Automation (based on handover)	**Low**	2 handover per pool


Azure AD
Azure Resources
Step
Application Developer
Application Administrator
User Interaction
User Delegated
API
Database
Engineer
Global Admin
Special Service Principal
User
Service Principal / Application Registration
Threat Model
CENTRAL SERVICE SERVICE PRINCIPAL (CSSPN)
Azure AD
API
Microsoft Graph / Microsoft AAD
1) Create SSPN
CSSPN
Application Administrator / Global Admin
Create
Request :: Application.ReadWrite.OwnedBy, Directory.ReadWrite.All
Grant
Assignee :: Role :: Application Administrator
Application.ReadWrite.OwnedBy
Directory.ReadWrite.All
2) Create App
App 1
Workflow
Engineer
CSSPN
Global Admin
Create
Add :: User, Group
Request :: User.Read, Directory.Read.All
Grant
Application.ReadWrite.OwnedBy
Directory.ReadWrite.All
3) Use App
User
App 1
Read
Delegate :: Read, Authenticate
Directory.Read.All
Database
Azure AD
@MarkWarneke
Azure Resources

Threat Model

CENTRAL SERVICE SERVICE PRINCIPAL (CSSPN)



@MarkWarneke

CENTRAL SERVICE SERVICE PRINCIPAL

Threat (MITRE ATT&CK)

Below are the tactics and technique representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques.

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery / Collection / Exfiltration	Impact
Create Valid Accounts (Rogue) ~~Creation of malicious application associated to the Azure AD tenant. (Rogue)~~	~~Use for Account Manipulation (Rogue)~~ Created Redundant Access (Rogue) Create Valid Accounts (Rogue)	Valid Accounts (Rogue)	Redundant Access, Valid Accounts (Rogue)	~~Account Manipulation (Rogue)~~ Leakage of synced secrets & custom identity properties *	~~Enumerate Azure AD (Rogue)~~	Resource Hijacking accidental deletion of Azure AD objects like application registrations. deliberate deletion of Azure AD objects by a rogue admin.

* Due to forest migration secrets are synced to Azure AD

https://attack.mitre.org/matrices/enterprise/cloud/azure/

CENTRAL SERVICE SERVICE PRINCIPAL

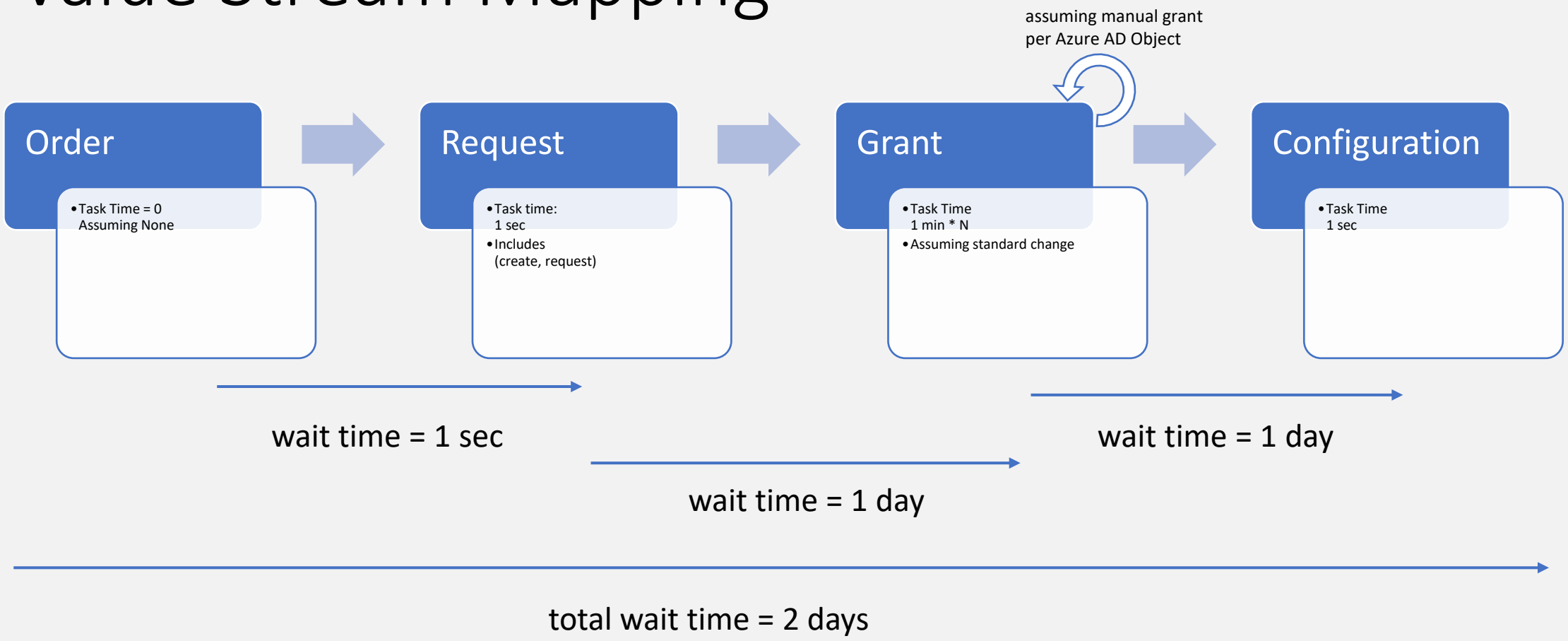
Threat (STRIDE)

STRIDE categorizes different types of threats and simplifies the overall security conversations.

Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Creation of malicious application associated to the Azure AD tenant	~~Use for Account Manipulation, grant access to Application Registrations of others~~	~~Service Principal not User Principal~~	~~Use for Account Manipulation, grant access to Application Registrations of others~~ Gather employee data	accidental & deliberate deletion of Azure AD objects	~~Use to elevate access of user / service principals~~

CENTRAL SERVICE SERVICE PRINCIPAL

Value Stream Mapping



touch time = 1 / 960 = 0.001 = 0.01 %
99.9% of lead time

@MarkWarneke

Analysis Central Service Service Principal

Risk Quantity (applicable/ identified risk)	**12/20**	
Risk Impact	Low - **Medium**	Medium, as workflow **must reduce risk exposure and reduce threat vector** – but needs to be implemented correctly. Could be miss used for escalation of permissions.
Grad of Automation (based on handover)	**Medium** to high	2 handover needed per request, for each SP effort for creating request and granting access needed based on “special service principal”

Analysis Comparison

Solution	CENTRAL SERVICE FOR APPROVAL PROCESS	POOL OF SERVICE PRINCIPALS	CLONE SERVICE PRINCIPAL
Risk Quantity (applicable/ identified risk)	12 / 20	**3 / 20**	20/20
Risk Impact	**Low** - Medium Medium, as workflow can reduce risk exposure and reduce threat vector – but needs to be implemented correctly	**Low** Low, as pool like manual but in batches, can be specified and approved once including definition of permissions etc.	Severe high impact risks, e.g. risk of full tenant compromise
Grad of Automation (based on handover)	Medium (2 Handover) per request	Low (2 Handover) per pool	**High** No Handover

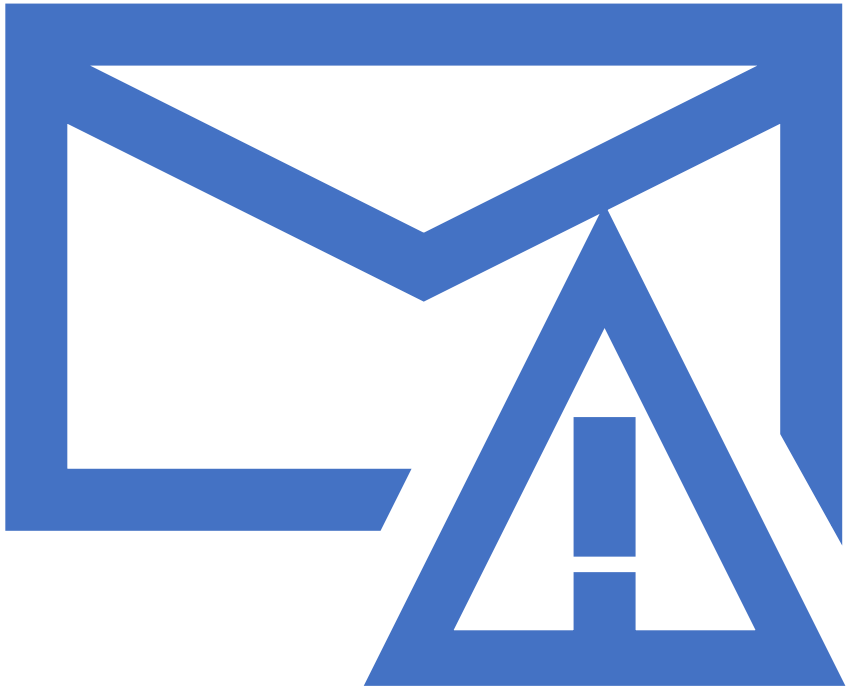
Mitigation

- Monitor the sign-in activity reports in the Azure Active Directory portal of the *Service Principal* or consider creating alerts similar to Role security > emergency accounts for unexpected sign-ins.
- Create Azure AD Identity Governance for the *Service Principals*.
  Make sure the created applications are active and used, recycle unused application periodically.
- Consider the permission granted *Service Principal* as a high privileged account and secure the secrets and access to it accordingly, by improving security by protecting elevated-privilege accounts at Microsoft and securing privileged access for hybrid and cloud deployments in Azure AD.

Thoughts out of the box

- Create own Azure AD tenant -> federation with AAD **(ESAE Administrative Forest Design Approach)**
- Azure AD custom roles and available permissions
- One Service Principal per service with granted permissions -> using multiple secrets (One secret per customer, revoke secret when compromised)
  - can not identify which customer on usage
- Workflow engine that is user principal based with automated decommissioning of special service principal
  - Soft delete
- PIM, PAM for service principal

Limitations



Azure AD Quota

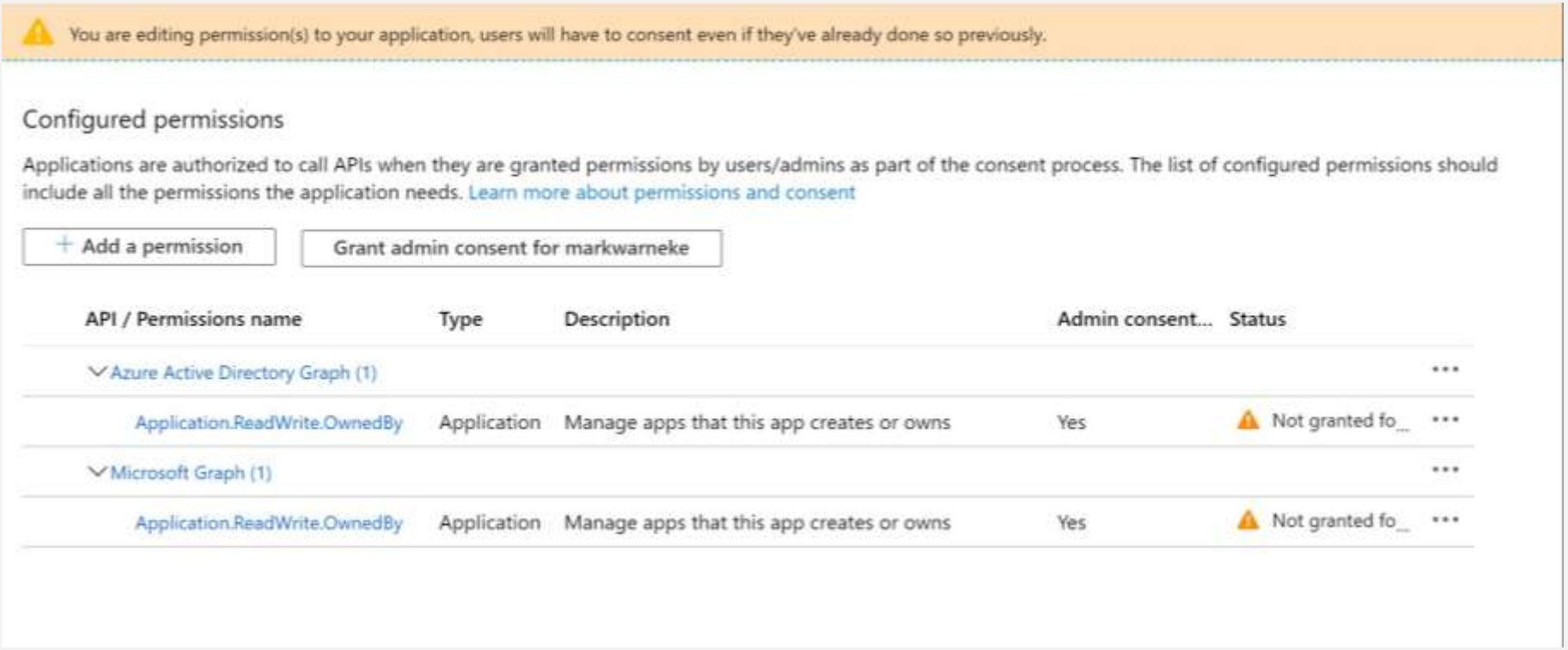
Code: Directory_QuotaExceeded
Message: The directory object quota limit for the Principal has been exceeded. Please ask your administrator to increase the quaote limit or delete objects to reduce the used quota.

The Application Developer role grants the ability, but the total number of created objects is limited to 250 to prevent hitting the directory-wide object quota. Source

Resources

- **Integrate Azure Active Directory with Azure Kubernetes Service** https://docs.microsoft.com/en-Us/azure/aks/azure-ad-integration
- **Integrate Azure Active Directory with Azure Kubernetes Service using the Azure CLI** https://docs.microsoft.com/en-Us/azure/aks/azure-ad-integration-cli
- **Delegated permissions, Application permissions, and effective permissions:** https://developer.microsoft.com/en-us/graph/graph/docs/concepts/permissions_reference#delegated-permissions-application-permissions-and-effective-permissions
- **Azure Active Directory v1.0 App Provisionin:** https://marketplace.visualstudio.com/items?itemName=stephane-eyskens.aadv1appprovisioning

Application permissions (Creator SPN)



Application permission (AKS)

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

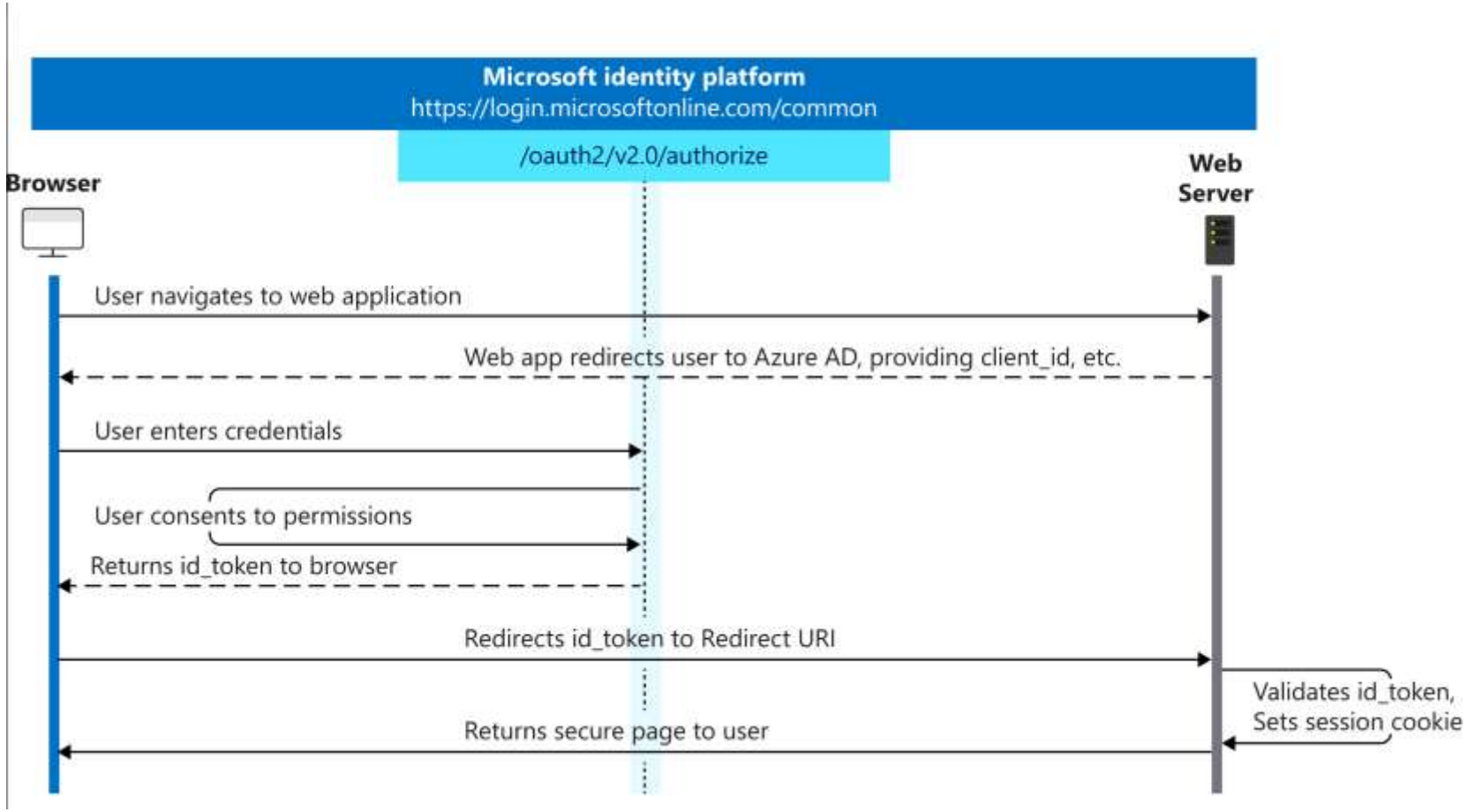
+ Add a permission

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
Microsoft Graph (3)			
Directory.Read.All	Delegated	Read directory data	Yes ⚠ Not granted for Micro...
Directory.Read.All	Application	Read directory data	Yes ⚠ Not granted for Micro...
User.Read	Delegated	Sign in and read user profile	-

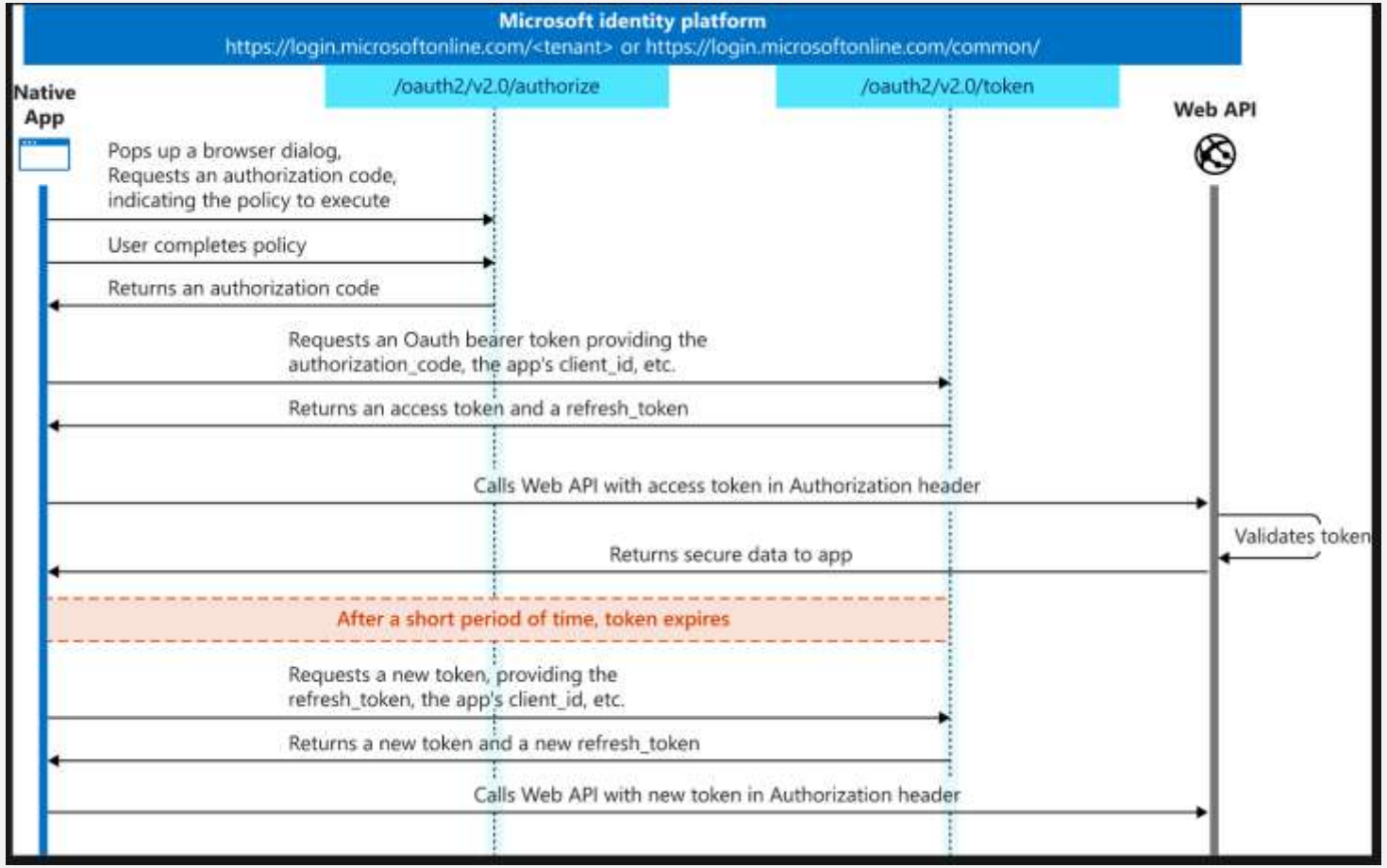
These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions

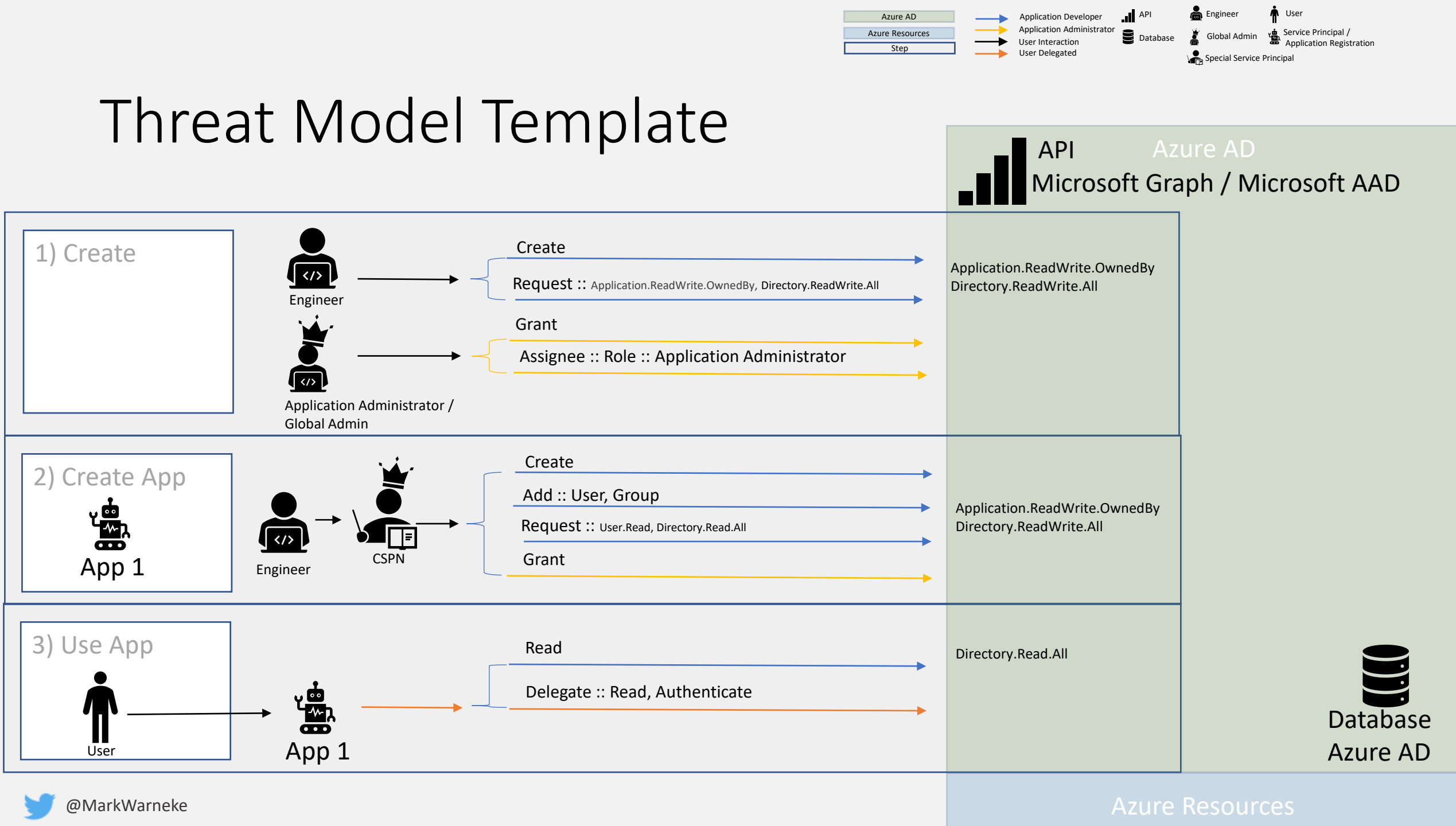
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration#create-the-server-application

Protocol diagram: sign-in



Microsoft identity platform and OAuth 2.0 authorization code flow




Azure AD
Azure Resources
Step
Application Developer
Application Administrator
User Interaction
User Delegated
API
Database
Engineer
Global Admin
Special Service Principal
User
Service Principal / Application Registration
Threat Model Template
API
Azure AD
Microsoft Graph / Microsoft AAD
1) Create
Engineer
Create
Request :: Application.ReadWrite.OwnedBy, Directory.ReadWrite.All
Application.ReadWrite.OwnedBy
Directory.ReadWrite.All
Grant
Assignee :: Role :: Application Administrator
Application Administrator / Global Admin
2) Create App
App 1
Engineer
CSPN
Create
Add :: User, Group
Request :: User.Read, Directory.Read.All
Grant
Application.ReadWrite.OwnedBy
Directory.ReadWrite.All
3) Use App
User
App 1
Read
Delegate :: Read, Authenticate
Directory.Read.All
Database
Azure AD
@MarkWarneke
Azure Resources