

The logo features the word "NIC" in a large, white, sans-serif font. Below it, the word "EMPOWER" is written in a smaller, white, sans-serif font, with wide letter spacing. A horizontal line with a color gradient from purple to yellow passes behind the text.

NIC

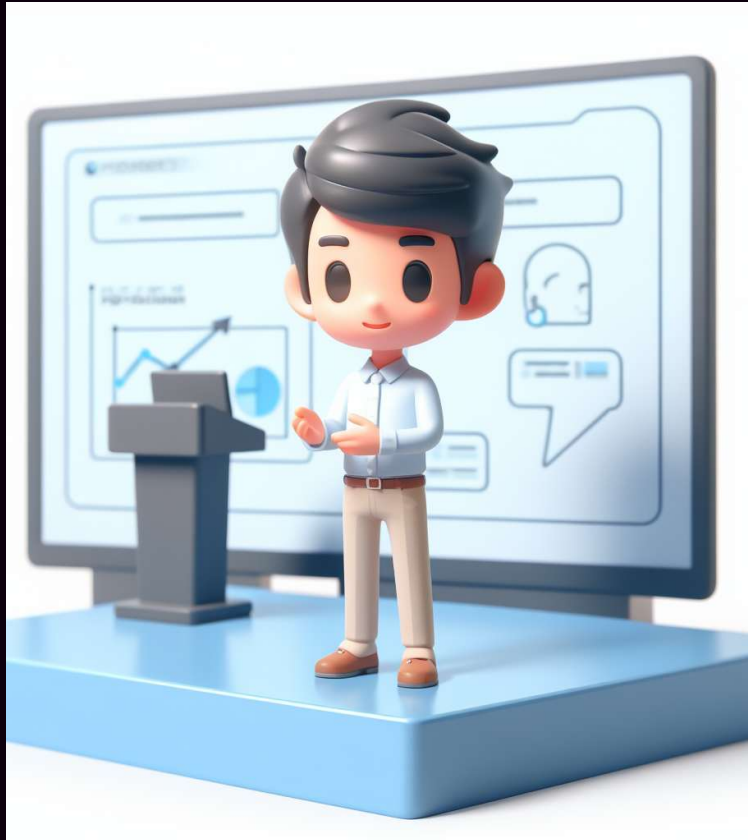
EMPOWER

November 13-15, Oslo Spektrum

Hi there! Hello!



Name	: Per-Torben Sørensen
Age	: 45
Lives	: Kristiansand, Norway
Qualifications	: MCT, MCSE M365
Background	: Norwegian armed forces, Ventelo, EVRY, Advania, rewired
Title	: Technical architect @ Crayon
XP	: 25 years of Micosoft IT
👍	: Microsoft 365, Security, PowerShell and ☀️
👎	: Insecure IT systems, legacy solutions and ❄️
Blog	: agderinthe.cloud
LinkedIn	: https://www.linkedin.com/in/pertorbensorensen



AGENDA

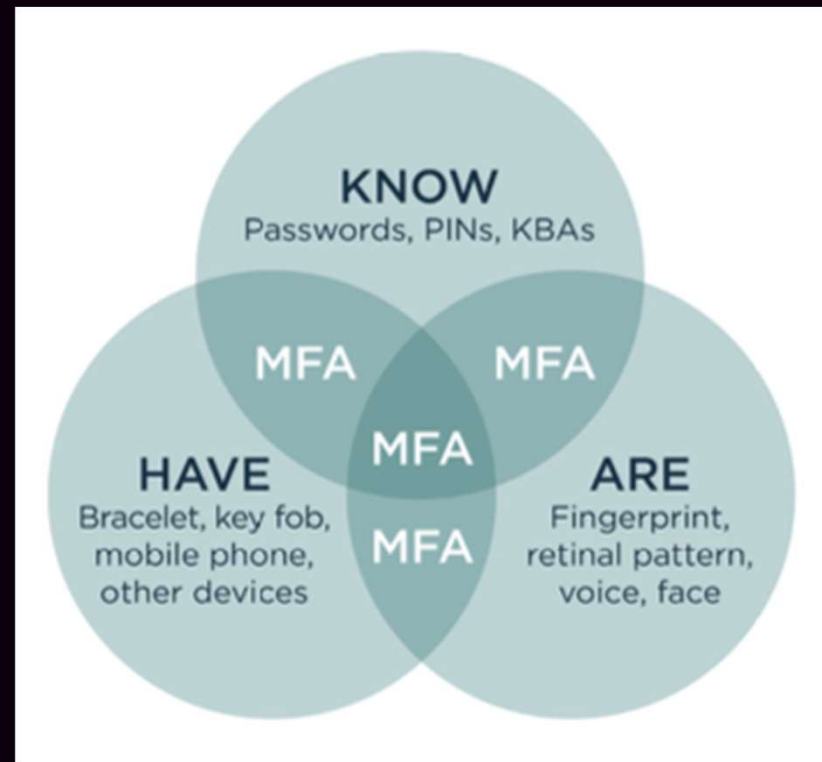
- ✓ 😊 Introduction
- ❑ 🔊 What the fuzz is about (MY experiences)
- ❑ 🧱 Conditional Access hardening
- ❑ 😍 Passkeys

What the fuzz is about

It's about MFA (and MFA fatigue)

What is MFA (2FA)?

- Multi-Factor Authentication
 - Used to VERIFY your account.
- 3 Factors:
 - **Something you KNOW**
 - Password, PIN
 - **Something you HAVE**
 - Phone, USB key
 - **Something you ARE**
 - Fingerprint, retinal scan
- MFA = Use at least 2 of these 3 factors when you log in



The problem: MFA fatigue

>1.2M

compromised accounts in January 2020

>99.9%

compromised accounts did not have MFA

>99%

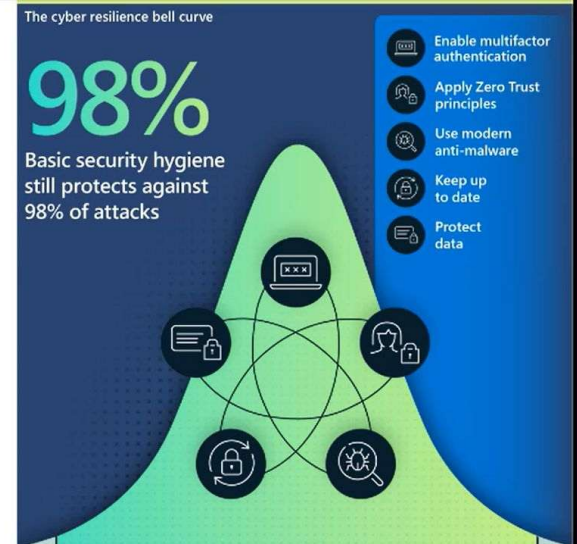
of Password Spray attacks use legacy auth

>97%

of Replay attacks use legacy auth

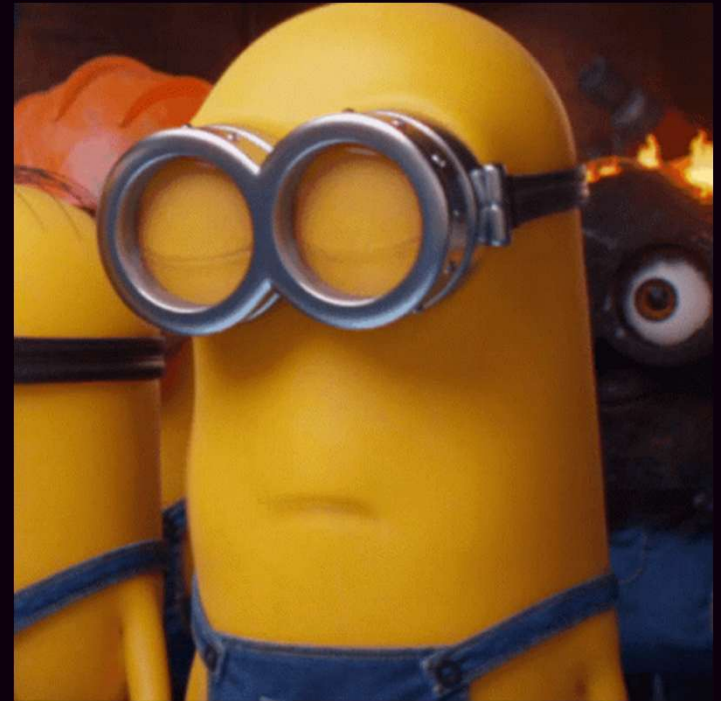
Cyber Resilience

Resilience success factors every organization should adopt



The problem: MFA fatigue

They've all heard this before... again and again and again....



Another approach

- Unlike in IaaS, identity security is the foundation of all security measures for SaaS solutions like M365
- In my experience: Many customers enable MFA through Conditional Access, but they don't verify all accounts are protected.
- Remember, users are not asked to register MFA until:
 1. They log in - AND
 2. They are hit by an MFA requirement!

VERIFY your MFA adoption

- Entra ID → Authentication Methods → Activity
- 2267 users have MFA method(s) registered
- 7101 users don't

Users capable of Azure multifactor authentication

2267 of 9368 total



76% of your organization isn't capable.

🤔 But what does that mean?

- 2267 users (MFA capable)



- 7101 users (MFA incapable)



Account hijacking

- Accounts are particularly vulnerable *before* MFA is configured.
- Don't create or sync stale accounts.
- Immediately secure new accounts when they are created or synced.
- 3 MFA methods can be deployed with scripts:
 - SMS (But PLEASE don't use it)
 - TAP (Temporary Access Pass)
 - And... FIDO2! 🙌🙌



“We don’t need MFA, we have complex passwords”

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
----------------------	--------------	-------------------	-----------------------------	--------------------------------------	---

9	Instantly	10 secs	1 hour	7 hours	2 days
---	-----------	---------	--------	---------	--------

2022

99,978%

202

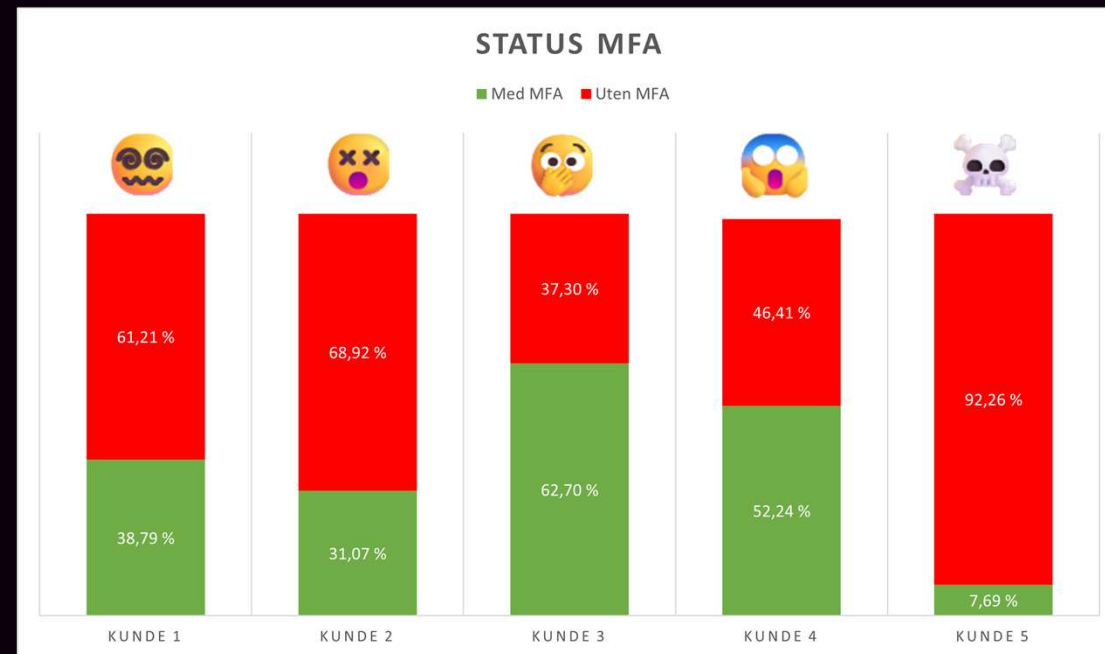
2023

(ChatGPT hardware)

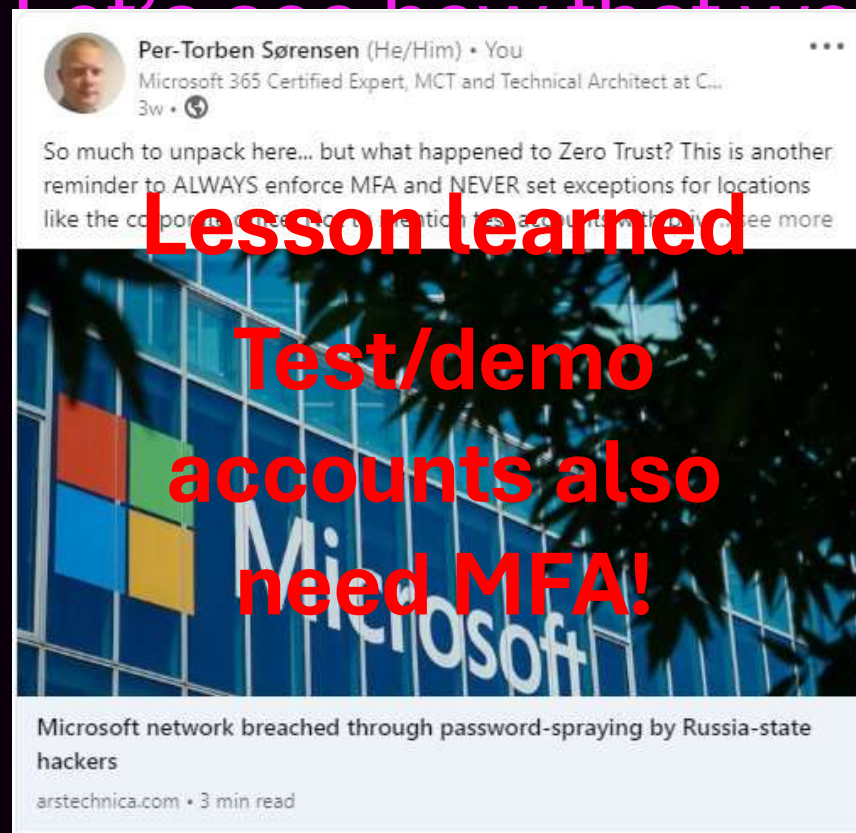
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months

Customer MFA adoption status

- Random sample of 5 customers over 2 years
- Smallest ~700 accounts
- Largest ~20000 accounts
- Several reasons:
 - Poor scoping
 - Assume everyone has MFA
 - “It’s only for admins”
 - “Not while in the office”



No MFA? Let's see how that worked out...



Lesson learned

**Test/demo
accounts also
need MFA!**

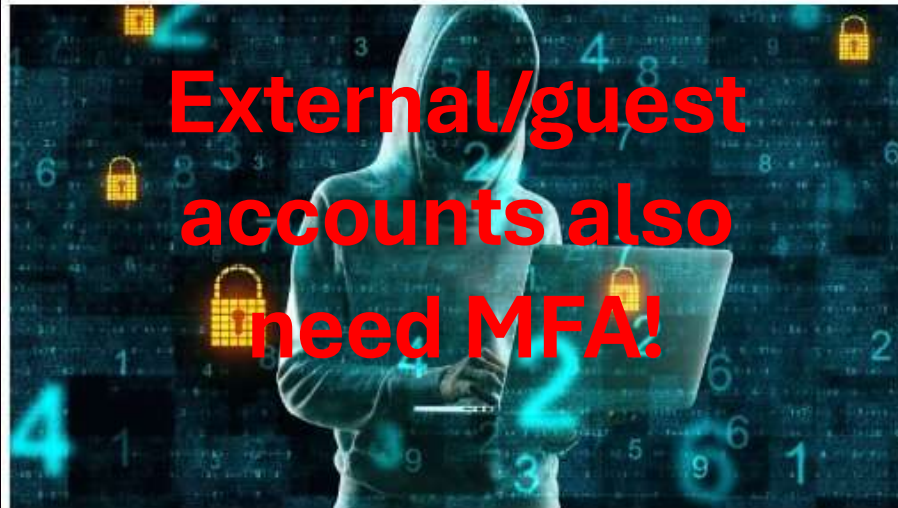


Per-Torben Sørensen (He/Him) • You

Microsoft 365 Certified Expert, MCT and Technical Architect at C...

1w •

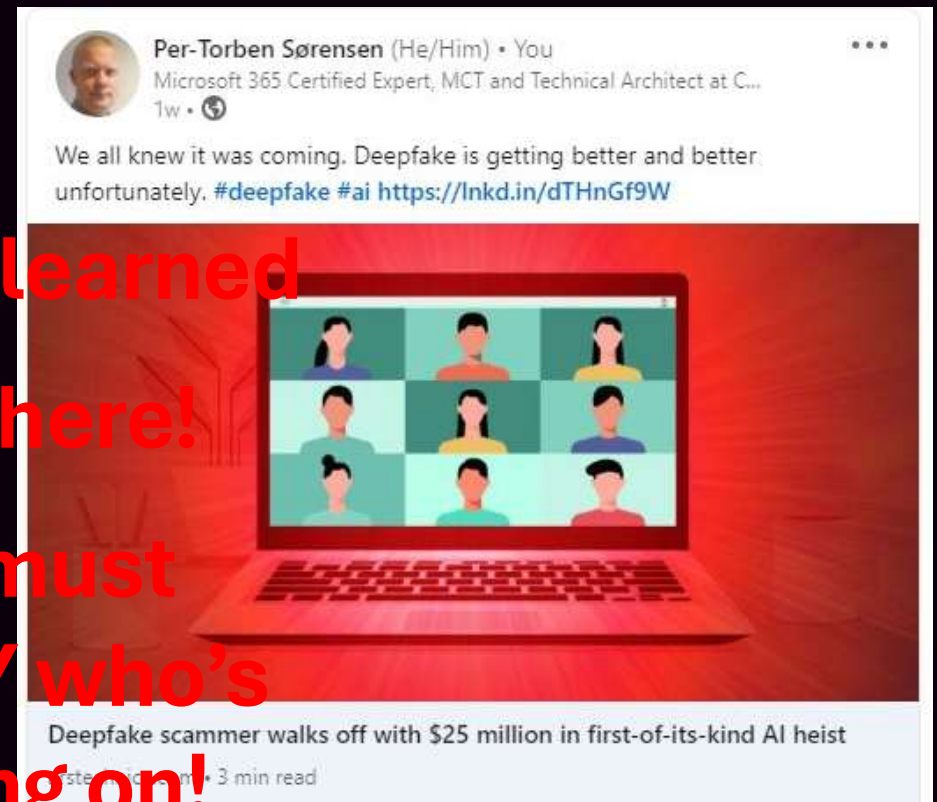
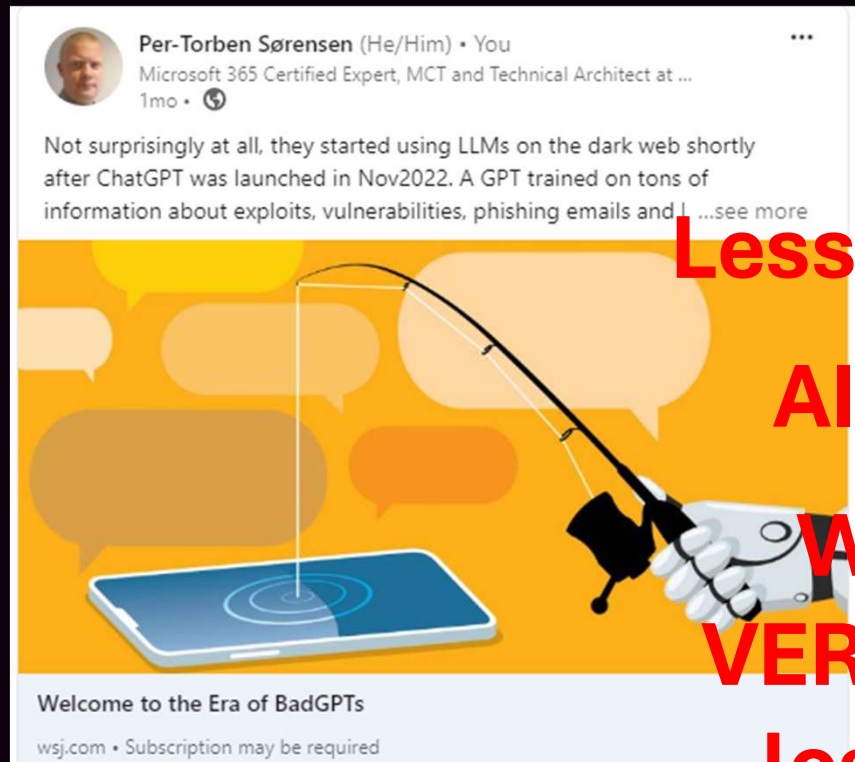
HUGE breach in France! (A 2 week old story which popped up in my feed today). 33 MILLION people in France were affected by the data leak, which included details like "the name" (status disclosure) in the... see more



1 in 2 people in France have data stolen in massive cyberattack

euronews.com • 2 min read

Lesson learned
External/guest
accounts also
need MFA!



Lesson learned
AI is here!
We must
VERIFY who's
logging on!

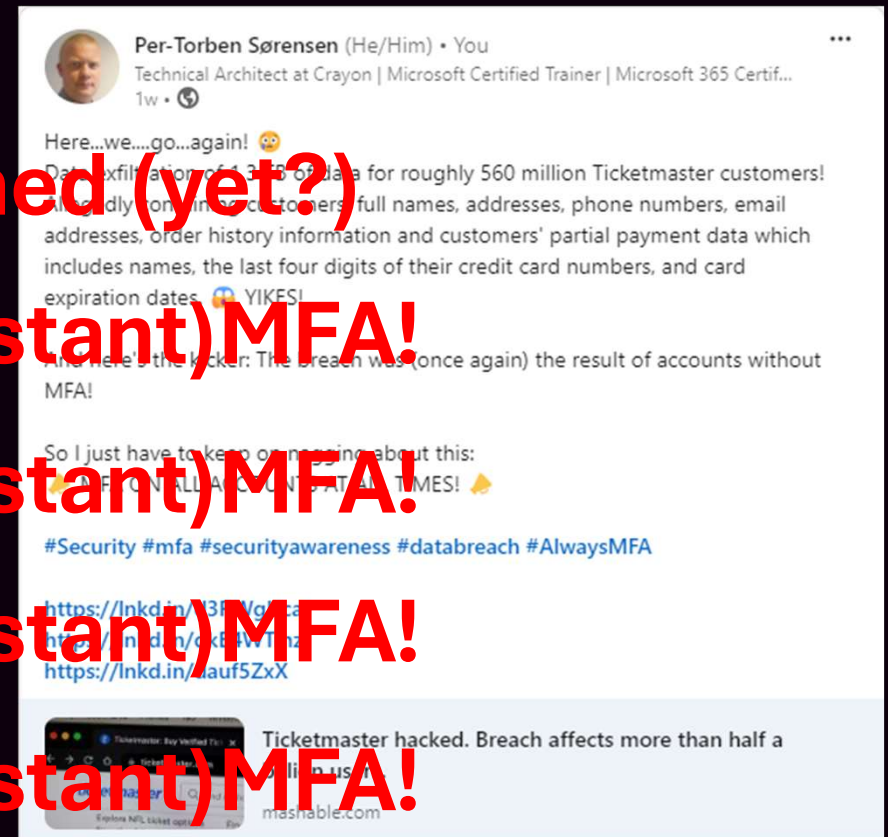
Lesson learned



Anyone can
attack!

Anyone can be
targeted!

We need phishing
resistant MFA!



Lesson learned (yet?)

(Phishing resistant)MFA!

(Phishing resistant)MFA!

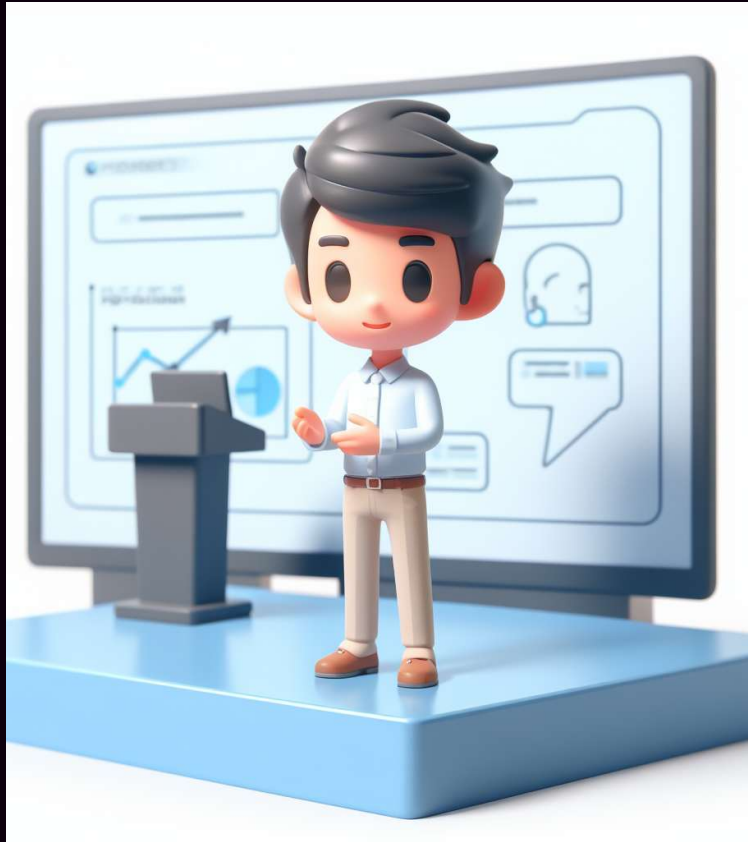
(Phishing resistant)MFA!

(Phishing resistant)MFA!

MFA conclusion:

- Identity security is the foundation of SaaS security
- MFA must be enforced on ALL accounts
 - NO MFA = NO SECURITY
- The MFA method should be phishing resistant
- The bad actors only need 1 unprotected account.....



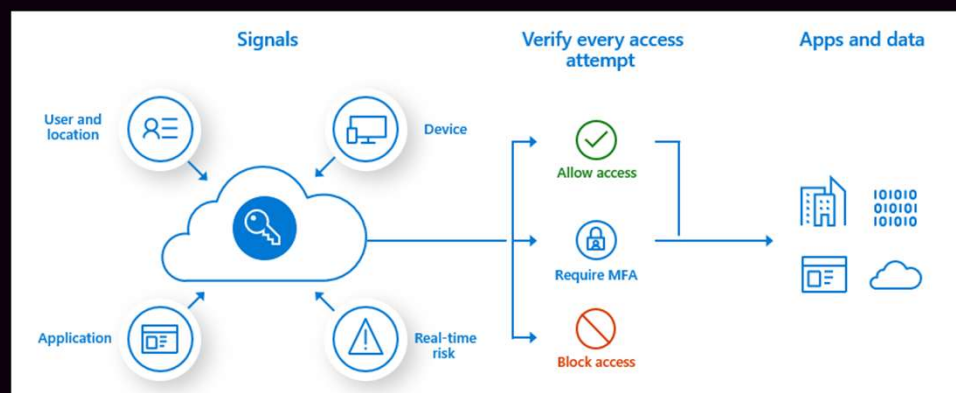


AGENDA

- ✓ 😊 Introduction
- ✓ 🔊 What the fuzz is about (MY experiences)
- ❑ 🧱 Conditional Access hardening
- ❑ 😍 Passkeys

Entra ID Conditional Access

- PRIMARY tool for Identity security in Entra ID
 - The “firewall” in M365
 - This lets you close and lock the door
- Evaluates every login based on a ruleset
 - Conditional Access Policy (CAP)
- Very flexible and continuously improved and expanded
- Requires Entra ID P1
 - P2 for additional features



DO

- Use CAP to enforce MFA on all accounts.
- Explore and learn all capabilities in CAP to improve your security posture
- Add additional security for privileged accounts
- Use a naming standard
- Create a break-glass account with FIDO2, monitoring and alerts
- And test it regularly

DON'T

- Exclude MFA for office networks!
- “Set and forget”
- Lock yourself out of your tenant
- Implement changes without testing
- Skip monitoring and rule backup
- Forget to **verify** MFA adoption

The major flaw: 🤖

Conditional access default behavior:

Log in allowed without any MFA

Unless anything else is specified, you are blocked from logging in at all!
Unless anything else is specified, you can log in from anywhere, on any device, access any app, without any MFA!

Conditional Access hardening – my way

- Based on Microsoft's framework for Cond.access (Microsoft Learn)
- Scaled down and adjusted
 - We are not in the Enterprise-segment
- It's NOT a final solution
 - Always adapt to your environment and needs
 - **Never** just copy-paste from someone else



Conditional access hardening

Only 5 steps!

GOALS:

- 👍 Block login by default
- 👍 Protect all signins with at least one CAP
- 👍 Complete control which accounts can log in
- 👍 Better naming standard

DISCLAIMER



The following settings are for demonstration purposes only.

These should not be implemented or considered as advice.

Step 1 - Persona and naming standard

Numbering and personas example:

- 00 = Global (all accounts)
- 01 = Admins (privileged accounts)
- 02 = Users (user accounts)
- 03 = Svc (service accounts)
- 04 = Guests (guest accounts)
- 99 = Test (test accounts)

University example:

- 00 = Global (all accounts)
- 01 = Admins (privileged accounts)
- 02 = Users (user accounts)
- 03 = Faculty (faculty accounts)
- 04 = Students (student accounts)
- 06 = Guests (guest accounts)
- 07 = Svc (service accounts)
- 99 = Test (test accounts)

Naming standard:

CA(Personanr.) – (Seq.nr) – (Persona) – (Target) – (Requirement)

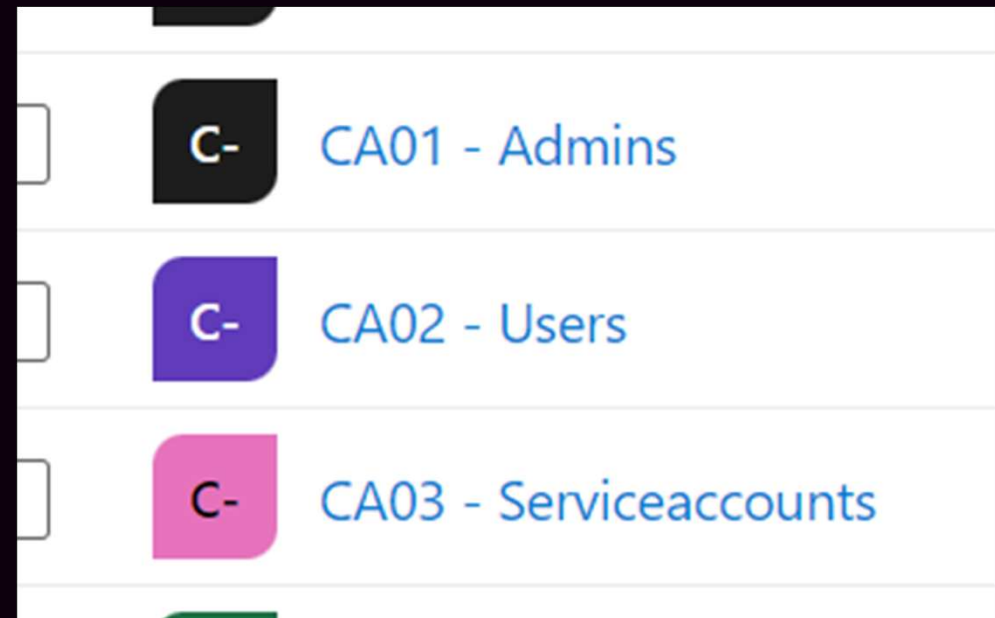
Examples:

“CA01 – 00 – Admins – Baseline – Req.MFA”

“CA02 – 03 – Users – VivaEngage – Req.CompliantDevice”

Step 2 – Corresponding Entra ID groups

- Create corresponding groups in Entra ID
- Use dedicated groups
 - Easy troubleshooting
 - Lock down with Restricted AU
- Group nesting works 👍



Step 3 – Block by default

“CA00 – 00 – Global – All – Block”

Scoped to:

- All users (excluding allowed users)
- All cloud apps
- Block access

Only the exclude list can log in

- Guests
- Members of groups
 - CA01
 - CA02
 - CA03
- Break-glass account

The screenshot shows the configuration for a Conditional Access policy. The policy name is "CA00 - 00 - Global - All - Block". The "Assignments" section shows "Users" with the selection "All users included and specific users excluded". "Target resources" is set to "All cloud apps". "Network" is set to "NEW" with the status "Not configured". "Conditions" shows "0 conditions selected". "Access controls" shows "Grant" with the selection "Block access". "Session" shows "0 controls selected".

The "Include" and "Exclude" tabs are visible. Under the "Exclude" tab, "Guest or external users" is selected. A dropdown shows "3 selected". Under "Specify external Microsoft Entra organizations", "All" is selected. "Directory roles" is not selected. "Users and groups" is selected. Below this, "Select excluded users and groups" shows "1 user, 3 groups". The list of excluded users and groups includes:

- CA01 - Admins
- CA02 - Users
- CA03 - Serviceaccounts
- Emergency Access Account (... BreakGlass@...)

Step 4 – Baseline protection

- Baseline config pr persona
 - “CA01 – 00 – Admins – Baseline – Req.MFA”
 - “CA02 – 00 – Users – Baseline – Req.MFA”
 - “CA03 – 00 – SvcAccounts – Baseline – Req.OfficeNetwork”
 - “CA04 – 00 – Guests – Baseline – Req.MFA”
- All exclusions gets a new CAP
 - This setup prevents logins without any Cond.Access policies applied
- Use additional rules to add/customize protection

Policy name

CA00 - 00 - Global - All - Block

CA01 - 00 - Admins - Baseline - Req.MFA

CA02 - 00 - Users - Baseline - Req.MFA

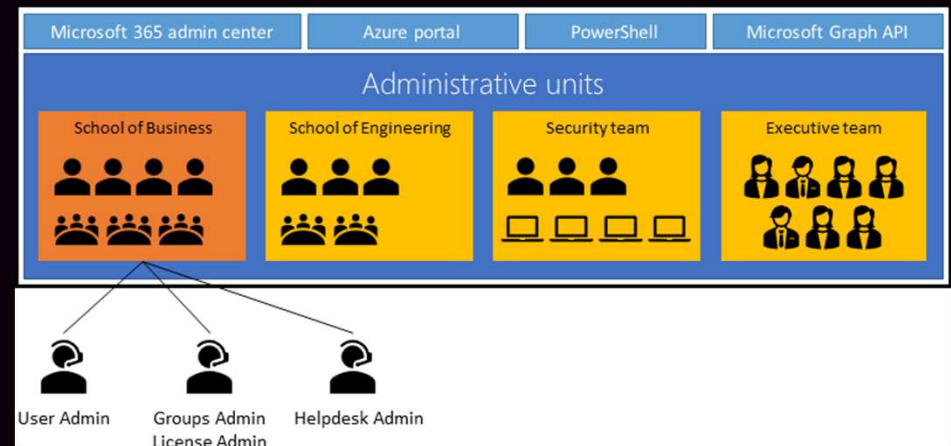
CA03 - 00 - SvcAccounts - Baseline - Req.OfficeNetwork

CA04 - 00 - Guests - Baseline - Req.MFA

CA99 - 00 - Test - Adminportal - MFA

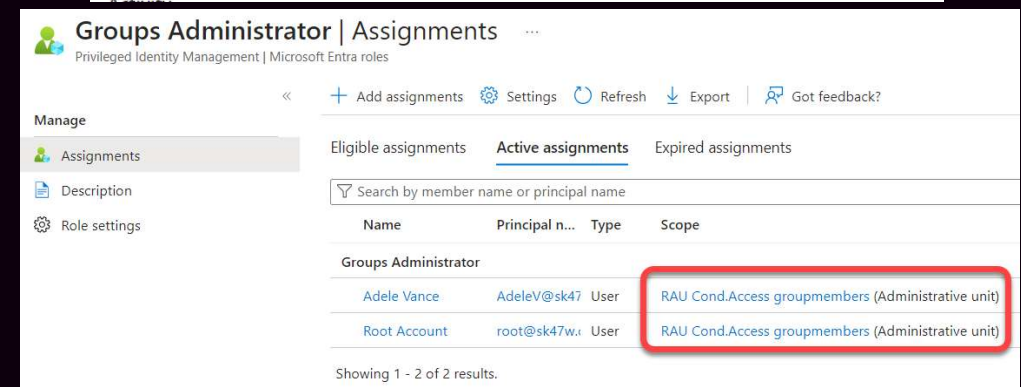
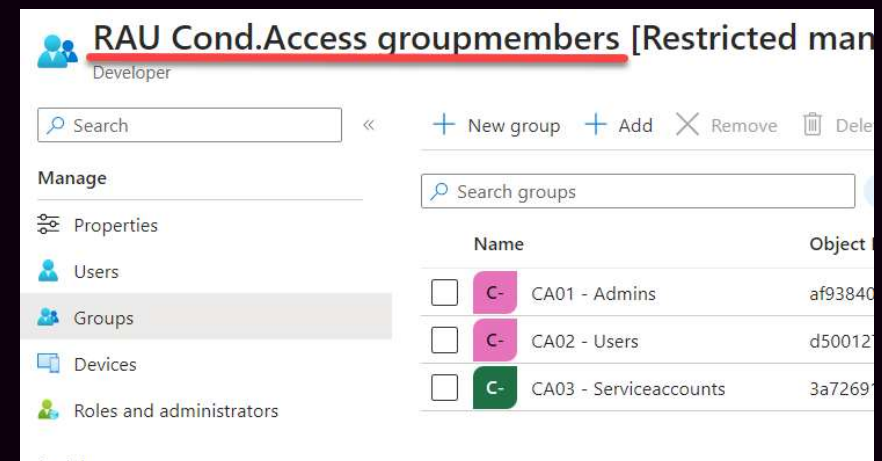
Step 5 (Optional) – Restricted AU

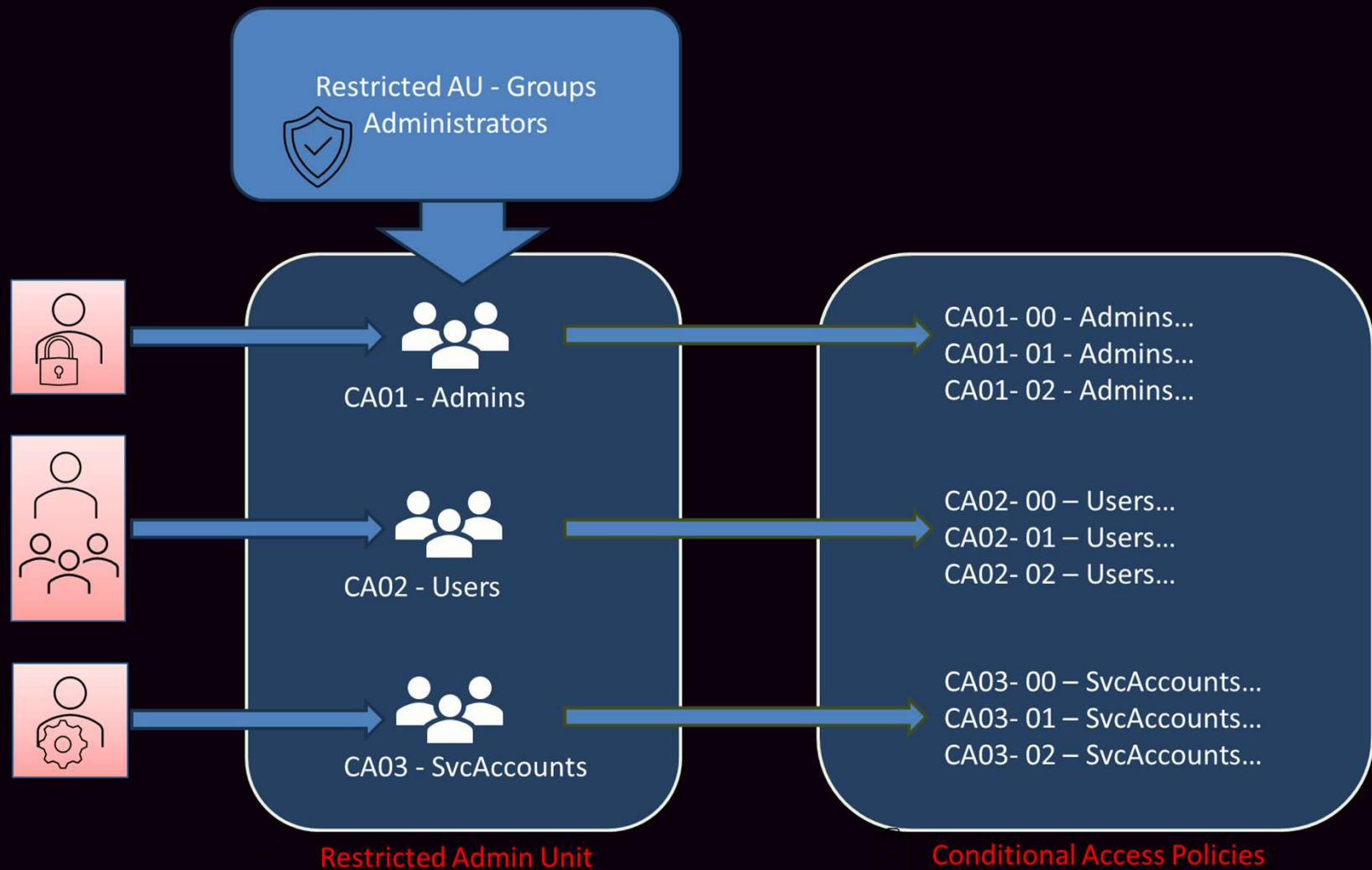
- Entra ID Administrative Unit (AU)
 - Delegation of admin rights in Entra ID
- Delegate certain roles to specific users
 - They only have admin rights within the AU
- Other privileged users have admin access to all AUs
- Target specific (add to AU)
 - Users
 - Groups
 - Devices



Step 5 (Optional) – Restricted AU

- Entra ID Restricted management AU
- Blocks privileged access from other admins
- We will:
 1. Add the CA-groups into the Restricted AU
 2. Delegate “Groups administrator” role to specific users
- This effectively locks down the ability to grant log on rights, to specific people in your tenant.





DEMO! Cond.Access hardening



The following settings are for demonstration purposes only.

These should not be implemented or considered as advice.

Delegate with care

Can change Conditional Access settings:

- Conditional Access Administrator
- Security Administrator
- Global Administrator

Can change/reset password and MFA on all accounts (including GA):

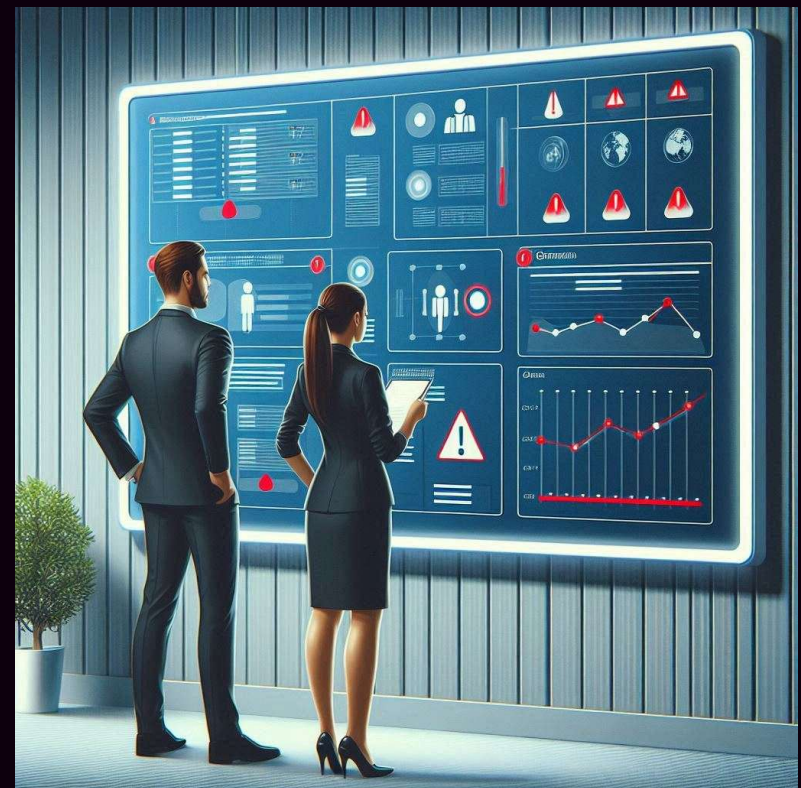
- Privileged Authentication Administrator
- Global Administrator

Can change or delete Restricted AU:

- Privileged Role Administrator
- Global Administrator

And don't forget:

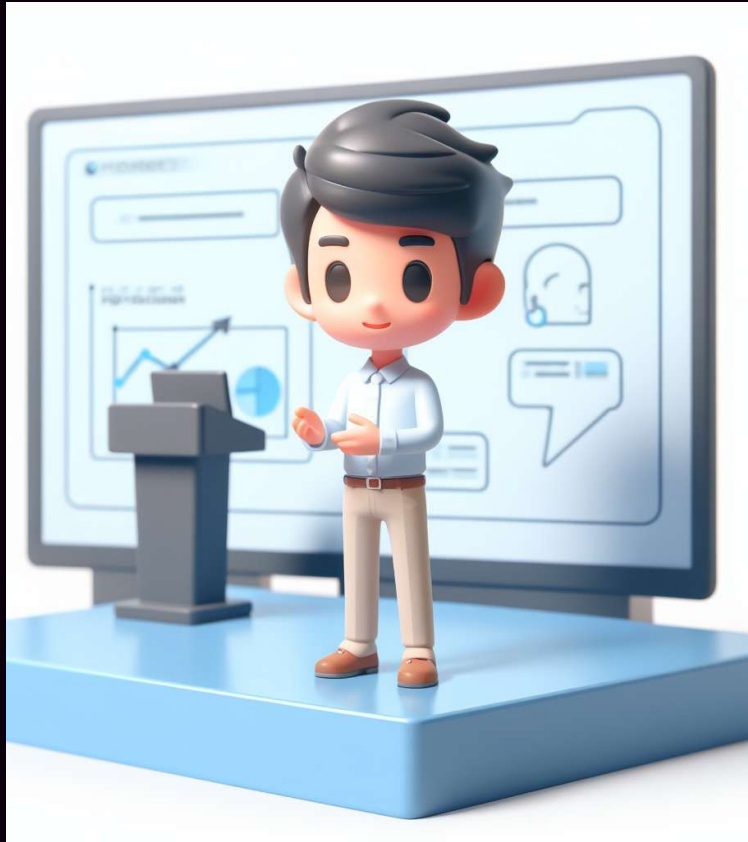
- Treat your Cond.Access policies like you would treat your firewall rules!
- Limit access as much as your can
- Back up all your Cond.Access policies
- Set up monitoring and alerts for:
 - Any changes in Cond.Access rules
 - Any changes with your Restricted AUs



Conditional Access conclusion:

- Change Conditional Access to block-by-default
- Adapt CAP to your organization and its needs
- Establish a good naming policy
- Back up your CA policies
- Monitoring with alerts is vital!





AGENDA

- ✓ 😊 Introduction
- ✓ 🔔 What the fuzz is about (MY experiences)
- ✓ 🧱 Conditional Access hardening
- ☐ 😍 Passkeys

Asymmetric keys, introduction

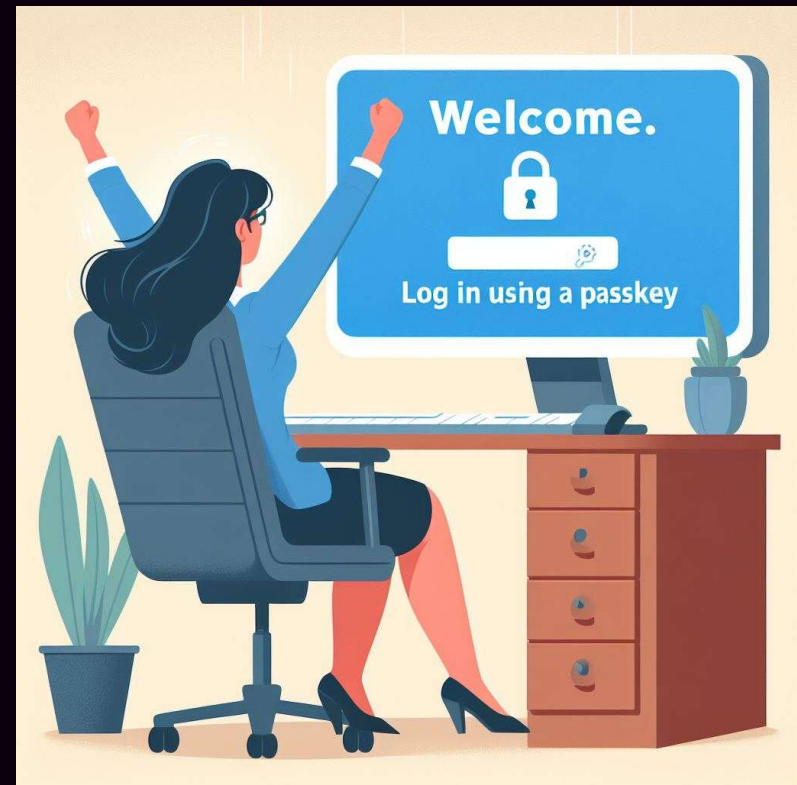
- The problem:
 - How do we encrypt/sign data without any pre-shared knowledge?
- The solution:
 - We use math.
 - The system generates two mathematical “keys” based on very large prime numbers.

Asymmetric keys, introduction

- Asymmetric encryption uses a keypair:
 - A public key and a private key.
 - Globally unique
- Public key is shared – Private key stays with owner, always hidden
- If data is encrypted/signed with **public** key:
 - The same **public** key can NOT decrypt/verify ❌
 - Only **private** key can decrypt/verify ✅
- If data is encrypted/signed with **private** key:
 - The same **private** key can NOT decrypt/verify ❌
 - Only **public** key can decrypt/verify ✅

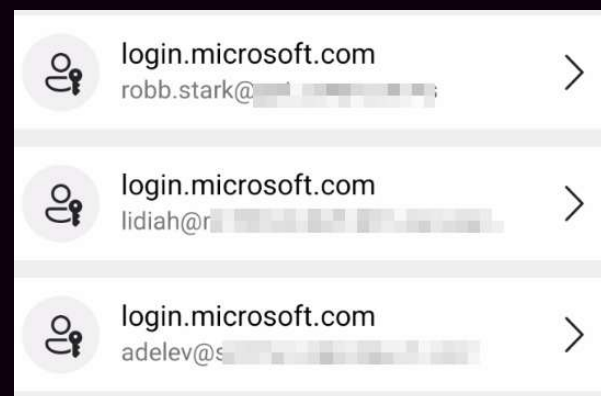
Passkeys

- Passwordless and phishing resistant authentication 🧐
- From the FIDO alliance
 - Built from the ground-up
 - Easier than passwords
 - More secure than passwords
- Based on PKI (Asymmetrical keypairs)
 - Activated by PIN or biometrics
- “Generic” passkeys is not like Microsofts



Is it passkeys? or “FIDO2”? or “security keys”?

- I employ a simple classification:
 - A “**FIDO2 Key**” refers to a tangible device that connects via USB or NFC
 - A “**Passkey**” is a software iteration of the FIDO2 Key, which is integrated within the operating system, web browser, password manager, mobile application etc



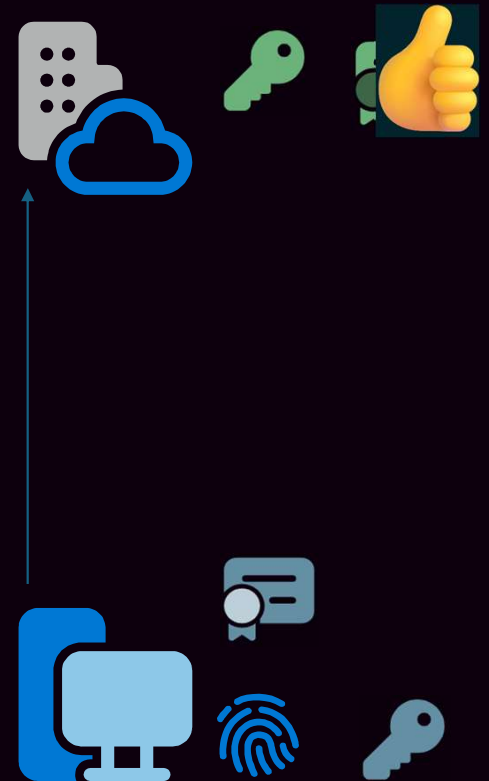
Passkey creation

- Login with MFA
- Public key
 - Created and stored LOCALLY
 - Domain-bound
 - A copy is transmitted to the cloud service
- Private key
 - Created and stored LOCALLY
 - NEVER exposed
 - Inactive state



Passkey login

1. User wants to log in to a cloud service with a passkey
2. The cloud service generates a random challenge
 - signs with its Public key
 - sends it to the client with a credential ID
3. User verifies himself/herself locally with PIN or biometrics
 - This activates the Private key
4. Private key verifies signature, signs challenge and sends it back with username and credential ID
 - Only valid once
5. The cloud service verifies the signature, checks the credential ID and issues the session token



DEMO!

«Generic» passkey (Github)

Why are passkeys better?

- NO PASSWORDS over the network!
- Local authentication
 - Man-in-the-middle resistant
- Cross-platform
 - Works with all major devices and browsers
- Domain-bound public key
 - Phishing site resistant
- Signed response only works once
 - Replay-attack resistant
- Very user friendly

Passkeys in Entra ID

- 👍 Public preview since April 2024, GA January 2025
- 👍 Easier and more secure than traditional password+MFA push
- 👎 Not as user friendly as regular passkeys
- 👎 MS requires you to store the passkeys in Microsoft Authenticator app
 - Android 14 / iOS 17
 - A major disadvantage for users without mobile phones.
 - For example: Elementary school students and healthcare workers

Create a passkey in Entra ID

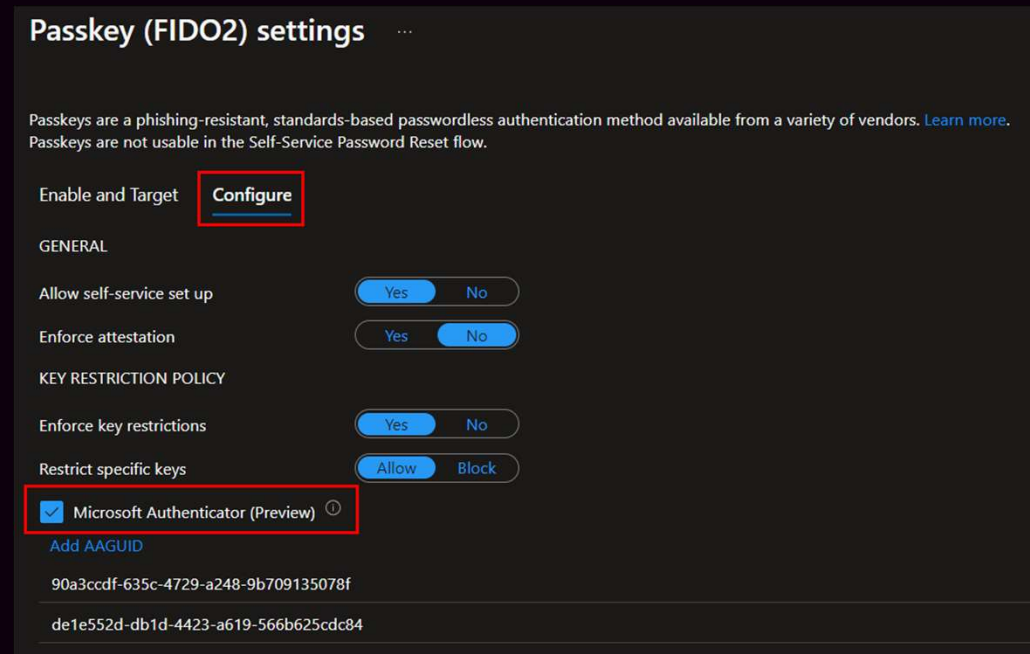
Admins:

Enable passkeys in the tenant:

1. Authentication methods
2. Passkey (FIDO2) settings
3. Configure

Remember:

The end-user needs at least one MFA method to register a passkey



Passkey (FIDO2) settings ...

Passkeys are a phishing-resistant, standards-based passwordless authentication method available from a variety of vendors. [Learn more](#).
Passkeys are not usable in the Self-Service Password Reset flow.

Enable and Target **Configure**

GENERAL

Allow self-service set up Yes No

Enforce attestation Yes No

KEY RESTRICTION POLICY

Enforce key restrictions Yes No

Restrict specific keys Allow Block

☒ Microsoft Authenticator (Preview) ⓘ

[Add AAGUID](#)

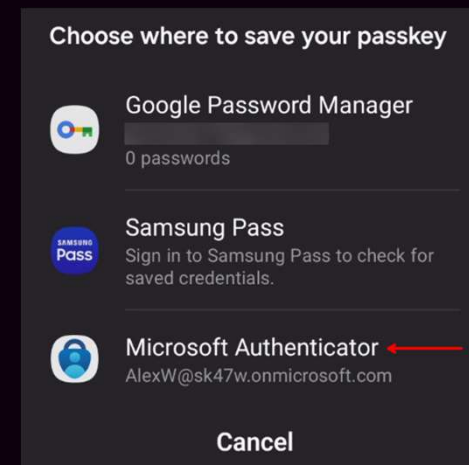
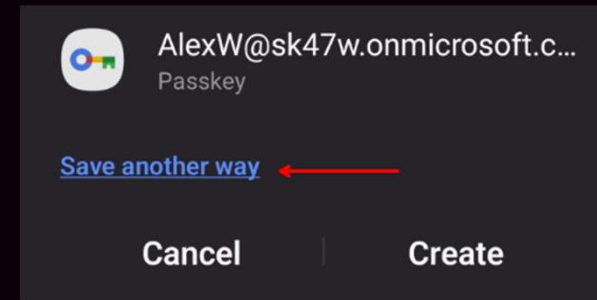
90a3ccdf-635c-4729-a248-9b709135078f

de1e552d-db1d-4423-a619-566b625cdc84

Create a passkey in Entra ID

End-user:

1. Sign in to aka.ms/mfasetup
2. Click “Add sign-in method”
3. Select “Passkey in Microsoft Authenticator (preview)”
4. Follow the wizard
5. Select device
6. Important to select “Microsoft Authenticator” to save the passkey



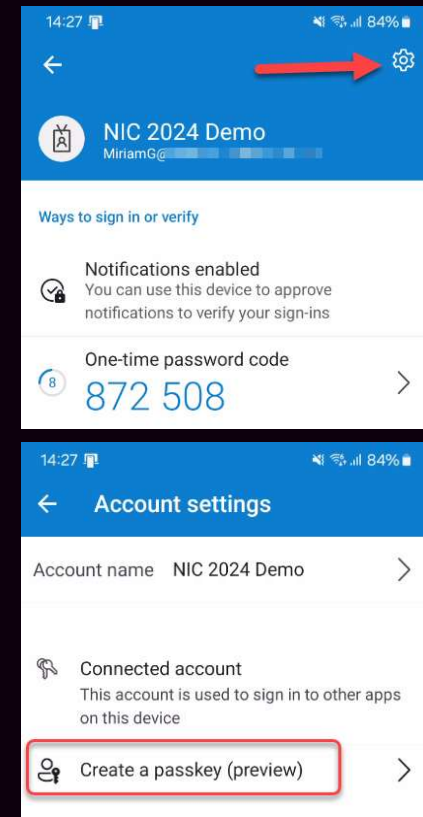
DEMO!

Passkeys (Entra ID)

NEW - Create a passkey in Entra ID

New option!

1. Open Microsoft Authenticator app on your phone.
2. Add account → Sign in 🤖
3. Add a passkey to the signed-in account



DEMO!

Passkeys (Entra ID)

Passkey conclusion

- Passkeys are low-cost and highly secure
- Very user friendly (once they are set up)
- Passkeys in Entra ID requires the Authenticator mobile app 😞
- Start testing today! This a MAJOR feature!



Before I go..

“If you want to go fast, go alone.

If you want to go far, go together!”



See you at the NIC party!! 🥳



Thank you! ❤️



Per-Torben Sørensen

Blog: [AgderInThe.Cloud](https://agderinthecloud.com)

Linkedin: →

