Again, sorry for having to cut the demos and walk through the presentation a little faster than I had planned.

I will make videos of my demos as soon as I am able to.

I will also make a blogpost soon about Cond.Access hardening (you guys and girls were the first people I showed this too, but I forgot to mention that little fun-fact). 😱

“Soon” I will also make a follow up blogpost on passkeys, and the Powershell script for MFA adoption (slide 20)

I will try to get this done during August, but no promises 😉

All of this will be available (for free ofc) on my collab-blog: agderinthe.cloud and I will post on LinkedIn when it’s available.

Please check out agderinthe.cloud and subscribe if you will, there are many posts there already on Passkeys, Copilot for M365 and much, much more. Some posts are in “Viking-language” but any browser can translate that for you.

Thank you again! ❤️

Experts Live Kenya

EXPERTS LIVE KENYA

26TH JULY 2024
NAIROBI, KENYA

Experts Live Kenya

No more identity theft!
Harden your identity security today!

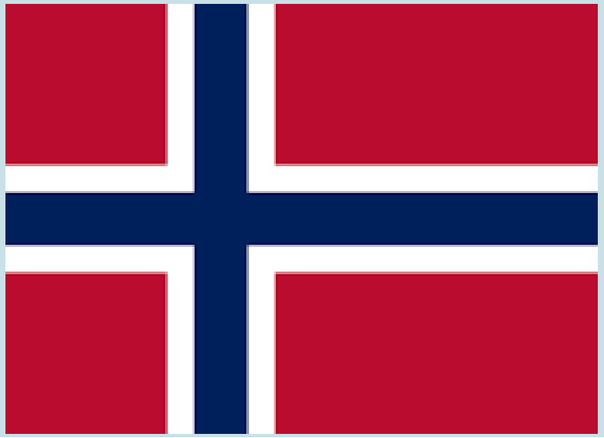
Per-Torben Sørensen
Technical architect @ Crayon

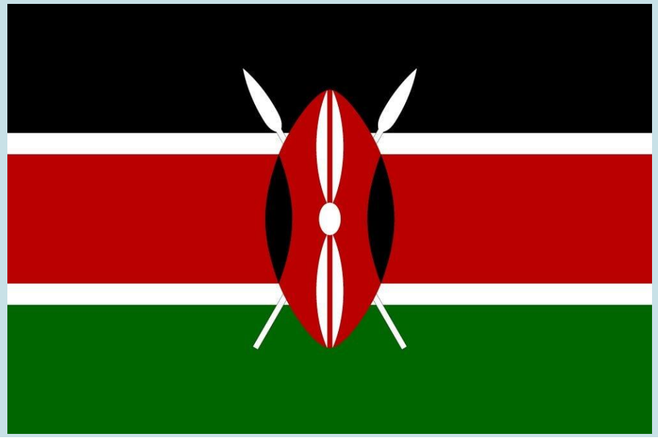
Hi there, hello!

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

Experts Live Kenya

Norway and Kenya ~6500 km apart





	Norway	Kenya
Population	~5,7 million	~60 million
Area	385k km2	582k km2
Capital	Oslo ~1,1 million	Nairobi ~5,5 million
Government	Monarchy	Republic
Length	From ~58° North to ~71° North (mainland)	From ~ 4,5° South to ~4,5° North

Where is Norway?

This is Norway

Norwegian summer

Norwegian summer

Norwegian winter

Norwegian winter

Agenda

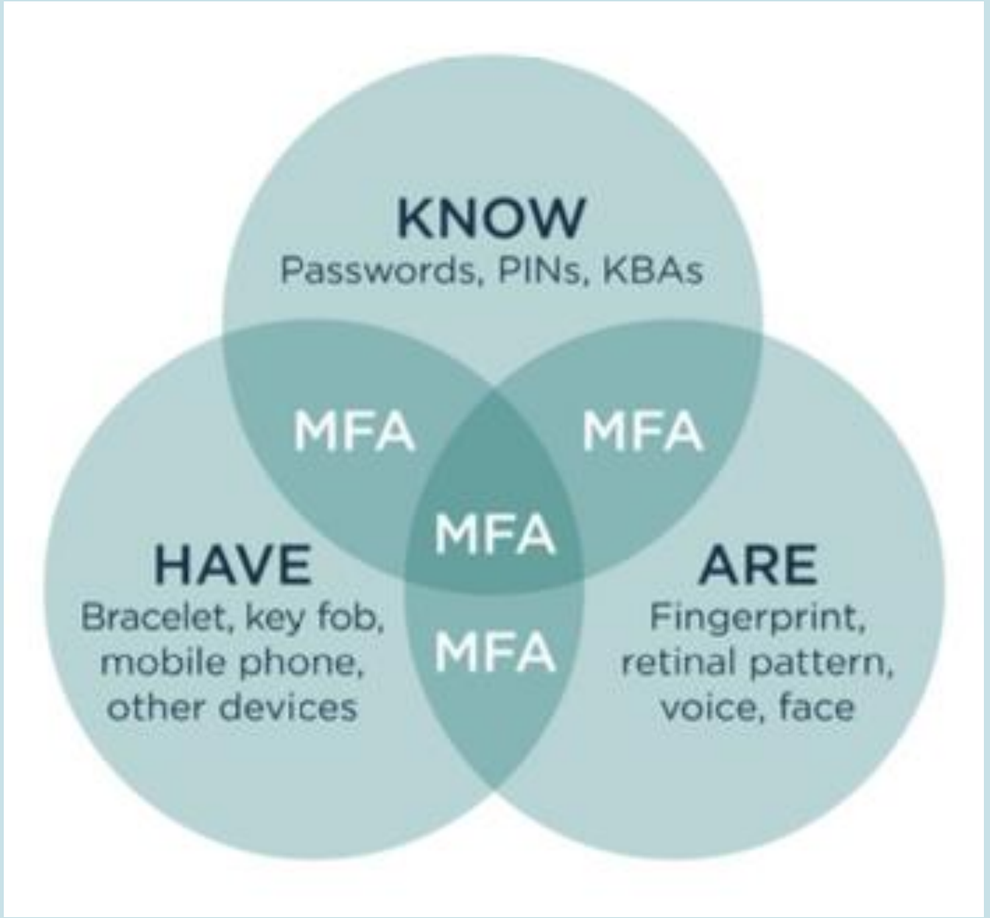
- ✓ Introduction 😊
- ❑ What the fuzz is about 📣 (MY experiences)
- ❑ Conditional Access hardening 🧱
- ❑ Passkeys 😍

What the fuzz is about

It’s about MFA (fatigue)

What is MFA (2FA)?

- Multifactor authentication, 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%

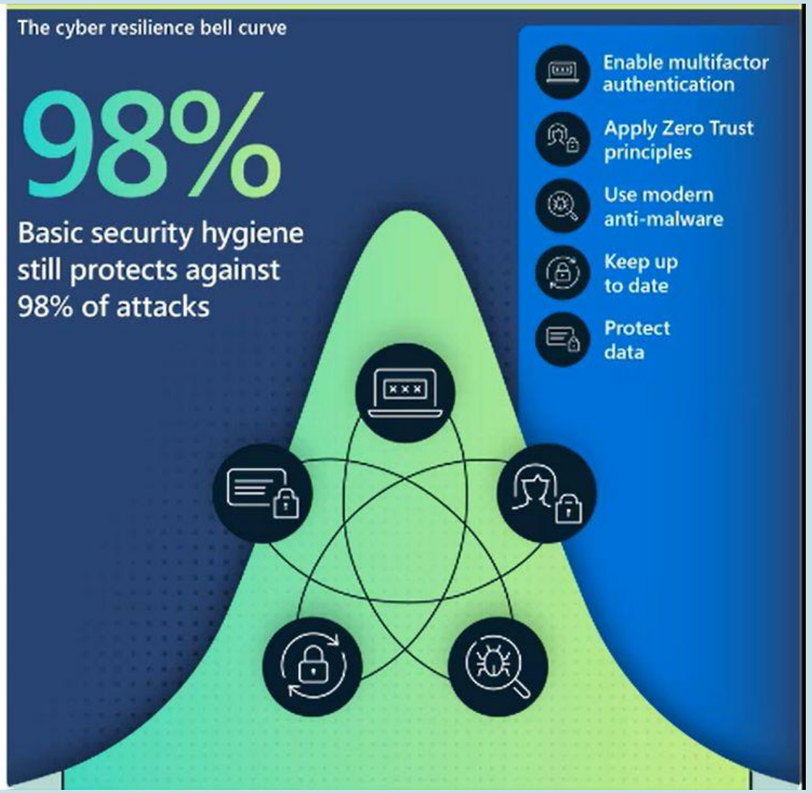
of Password Spray attacks use legacy auth

>97%

of Replay attacks use legacy auth

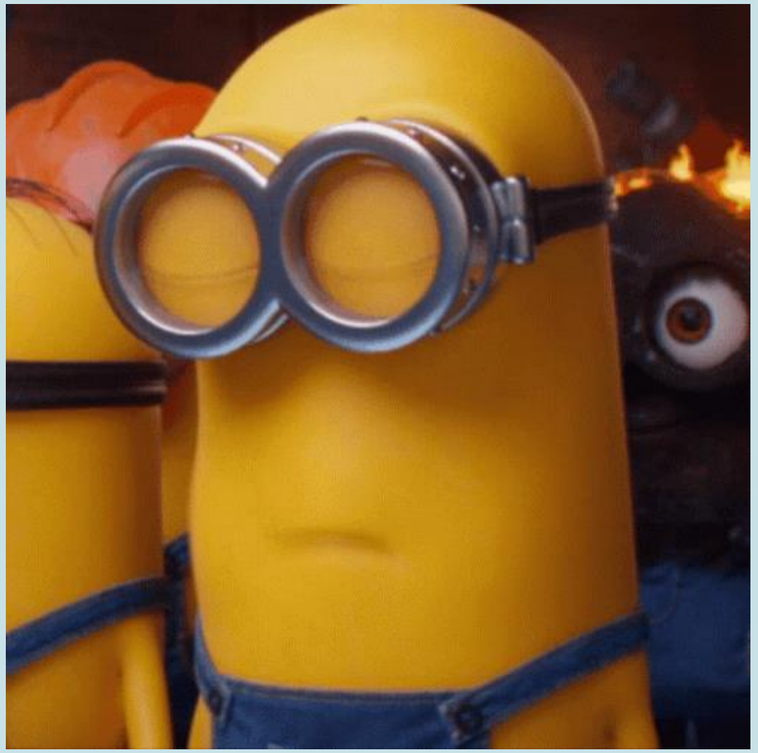
Cyber Resilience

Resilience success factors every organization should adopt



MFA fatigue, my experience

- You've all heard this before… again and again and again and again….
- But when I meet a new customer, their MFA coverage is always bad!
- Identity security is the **foundation** of all security measures for SaaS solutions like M365
- Many customers enable MFA through Conditional Access, but they don't verify all accounts are protected.
- Users are not asked to register MFA, until they log in AND is hit by an MFA requirement



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).
- 2 MFA methods can be deployed with scripts:
  - SMS (But please don’t use it)
  - TAP (Temporary Access Pass)

No need, we have complex passwords

2022

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
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years

2023

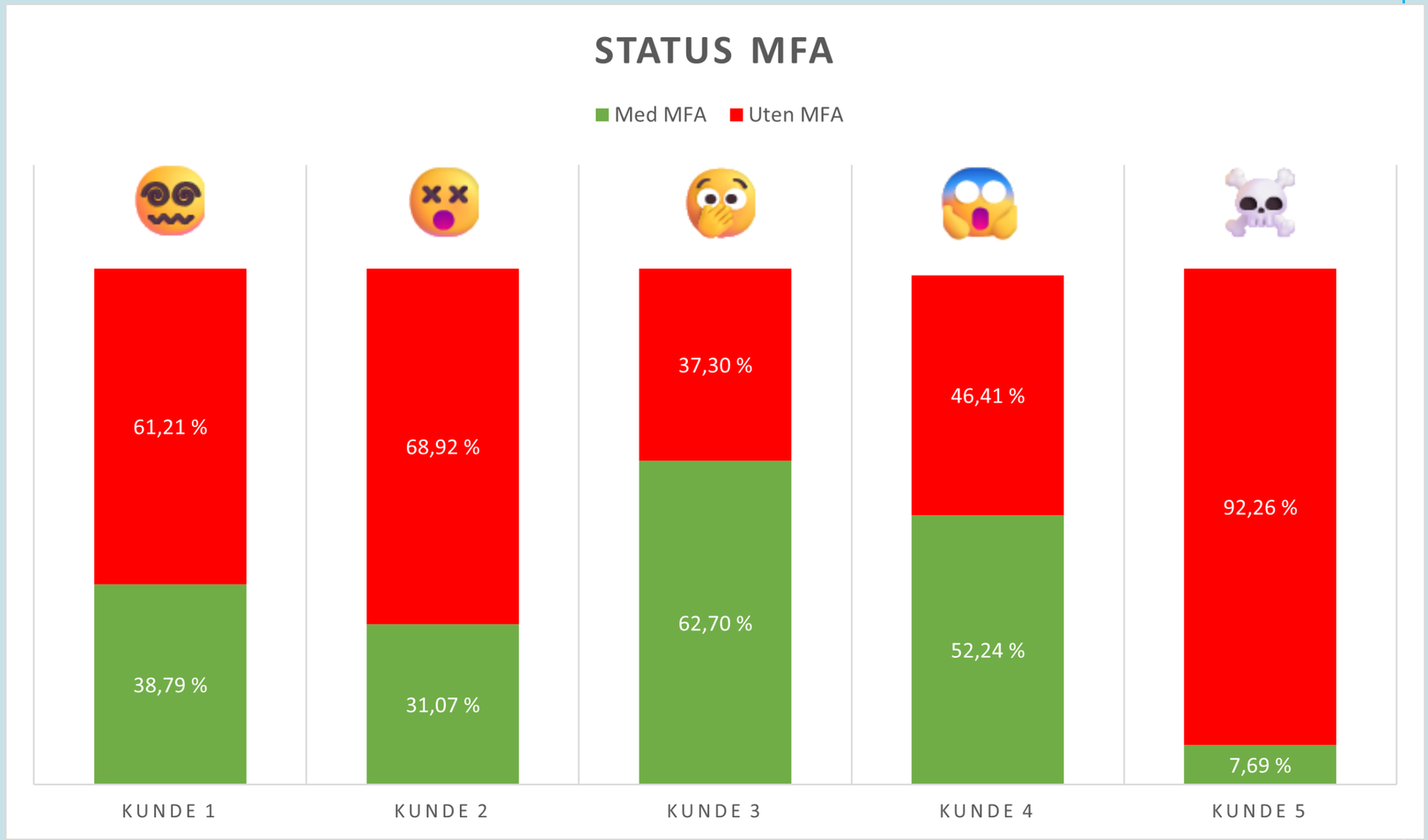
99,978%

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

MFA adoption status

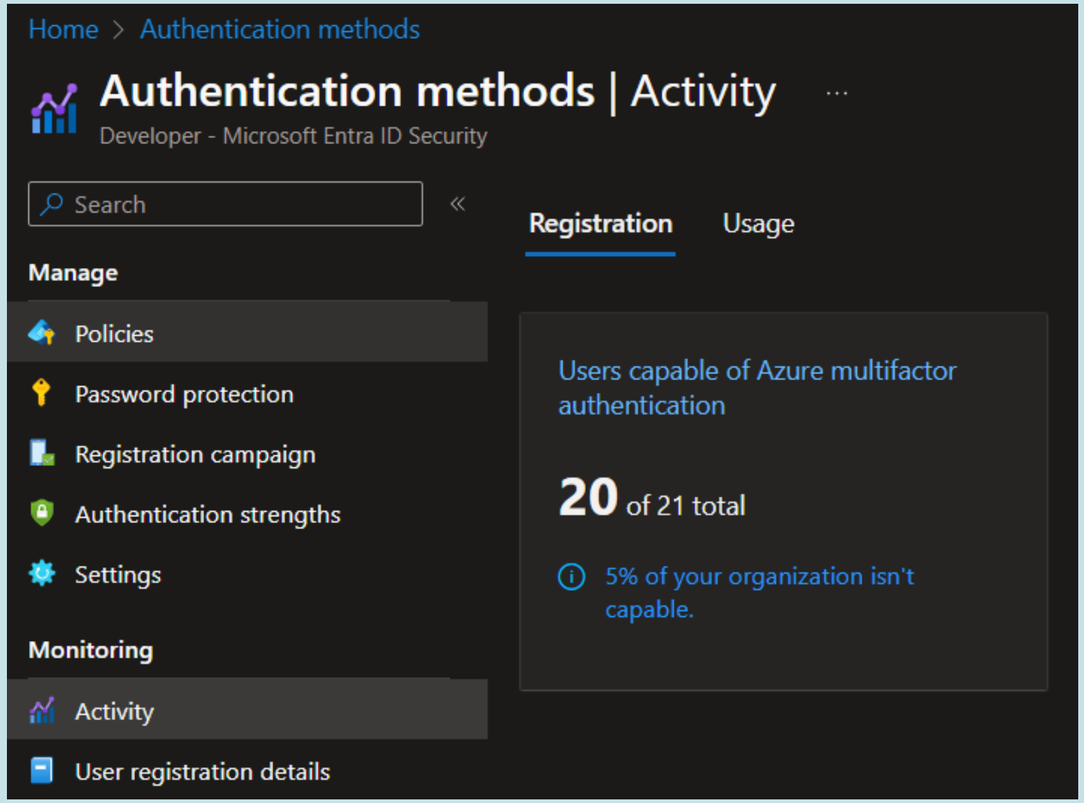
- Random sample of 5 customers over 2 years.
- Smallest ~700 accounts
- Largest ~20000 accounts
- Several reasons:
  - Poor scoping
  - “We don’t have critical data”
  - “It’s only for admins”
  - “Not in the office”



Experts Live Kenya

MFA adoption

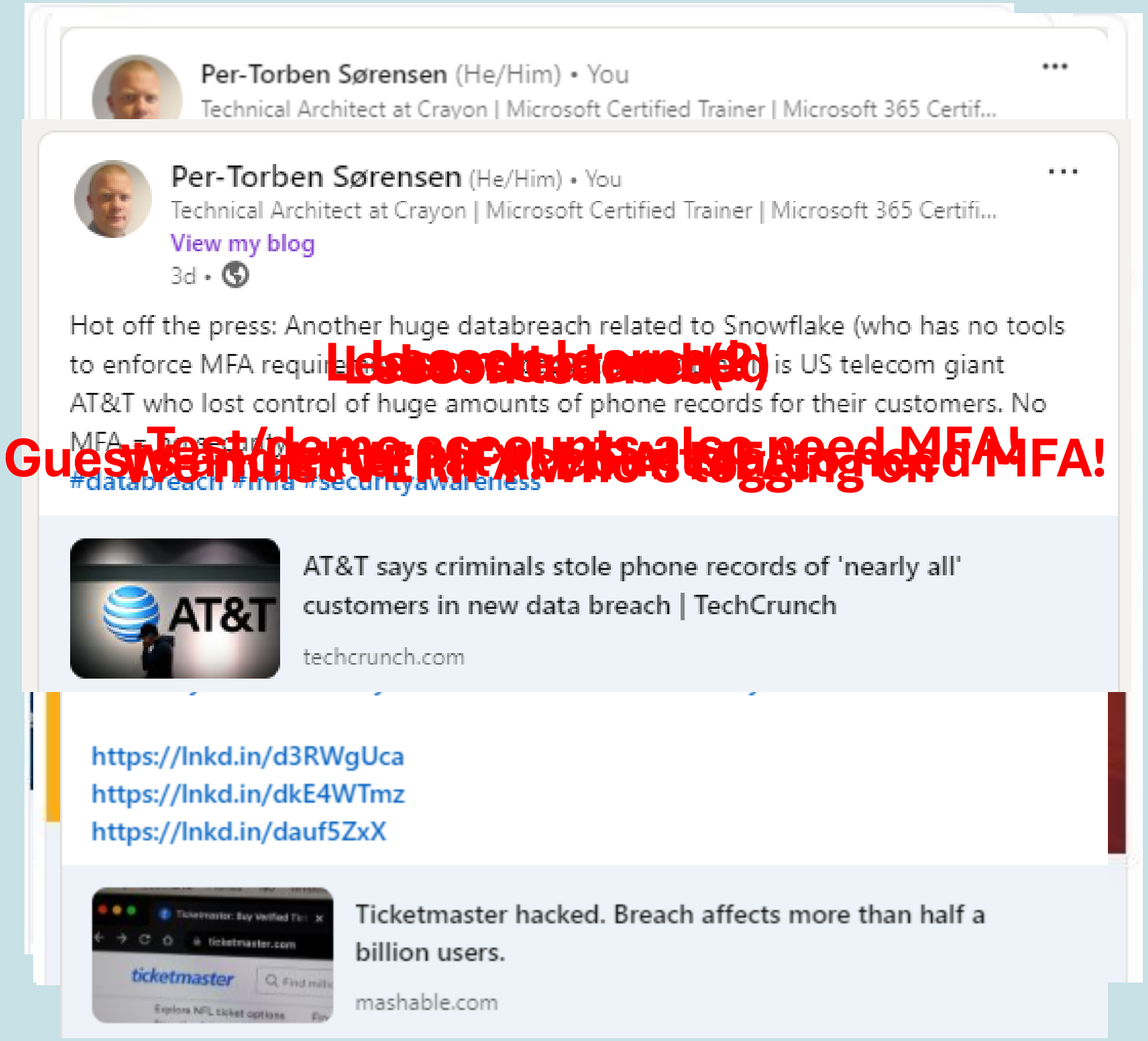
Built-in report in Entra ID



Good old Powershell ❤️

```
user                : Per-Torben Sørensen
upn                 : per-torben@dev.sorensen.ws
usertype            : Member
accountEnabled      : True
MFAstatus           : enabled
authApp             : True
authDevice          : Pixel 8 Pro
phoneSMS            : False
phoneSMSNr          : False
fido                : True
fidotype            : Passkey on Pixel 8 Pro
fidoDetails         : Microsoft Authenticator - Android
helloForBusiness    : False
helloClient         : False
emailAuth           : False
tempPass            : True
tempPassDuration    : 480
tempPassIsUsableOnce : False
passwordLess        : False
softwareAuth        : False
SSPREmail           : False
```

No MFA in 2024



Section conclusion

Identity security is the foundation of SaaS security

MFA must be enforced on ALL accounts

NO MFA = NO SECURITY

The bad actors only need 1 unprotected account…..

Agenda

✓ Introduction 😊

✓ What the fuzz is about 📣 (MY experiences)

❑ Conditional Access hardening 🧱

❑ Passkeys 😍

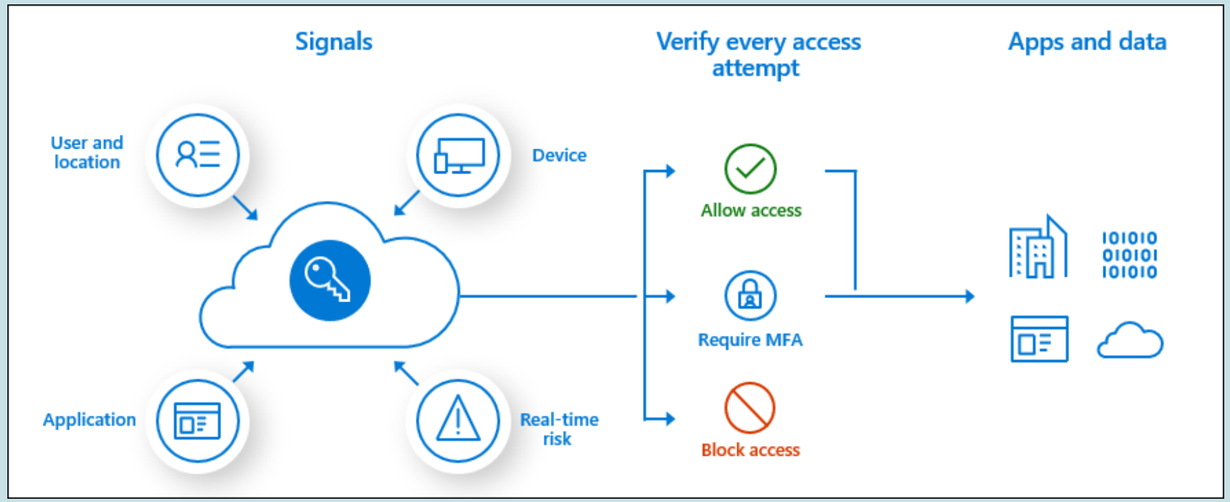
Raise your hands please

Is anyone in the audience unfamiliar with:

The fundamental features and principles of **Entra ID Conditional Access**?

Conditional Access Policy (CAP)

- **Primary** tool for Identity security in Entra ID
- Evaluates every login based on a ruleset
- Very flexible
- Continuously improved and expanded
- Requires Entra ID P1
  - P2 for additional features



DO:

- Use CAP to enforce MFA on all accounts.
- Establish a break-glass account
- Explore and learn all capabilities in CAP to improve your security posture
- Add additional security for privileged accounts
- Use a naming standard
- Use “Authentication Strength”, to block less secure methods

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

Experts Live Kenya

The major flaw: 😱

Conditional access default behavior:

Log in allowed without any MFA

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

Unless anything else is specified, you are blocked from logging in at all!

Conditional access hardening

- Based on Microsoft's framework for Cond.access (Microsoft Learn)
- Scaled down/adjusted to better fit companies who are not in the Enterprise-segment
- It’s NOT a final solution
  - Always adapt to your evorinment/needs
  - Never just copy-paste

GOALS:

👍 Better naming standard

👍 Block login by default

👍 Systematically assign CAP for each persona

👍 Control which accounts can log in

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)

University example:

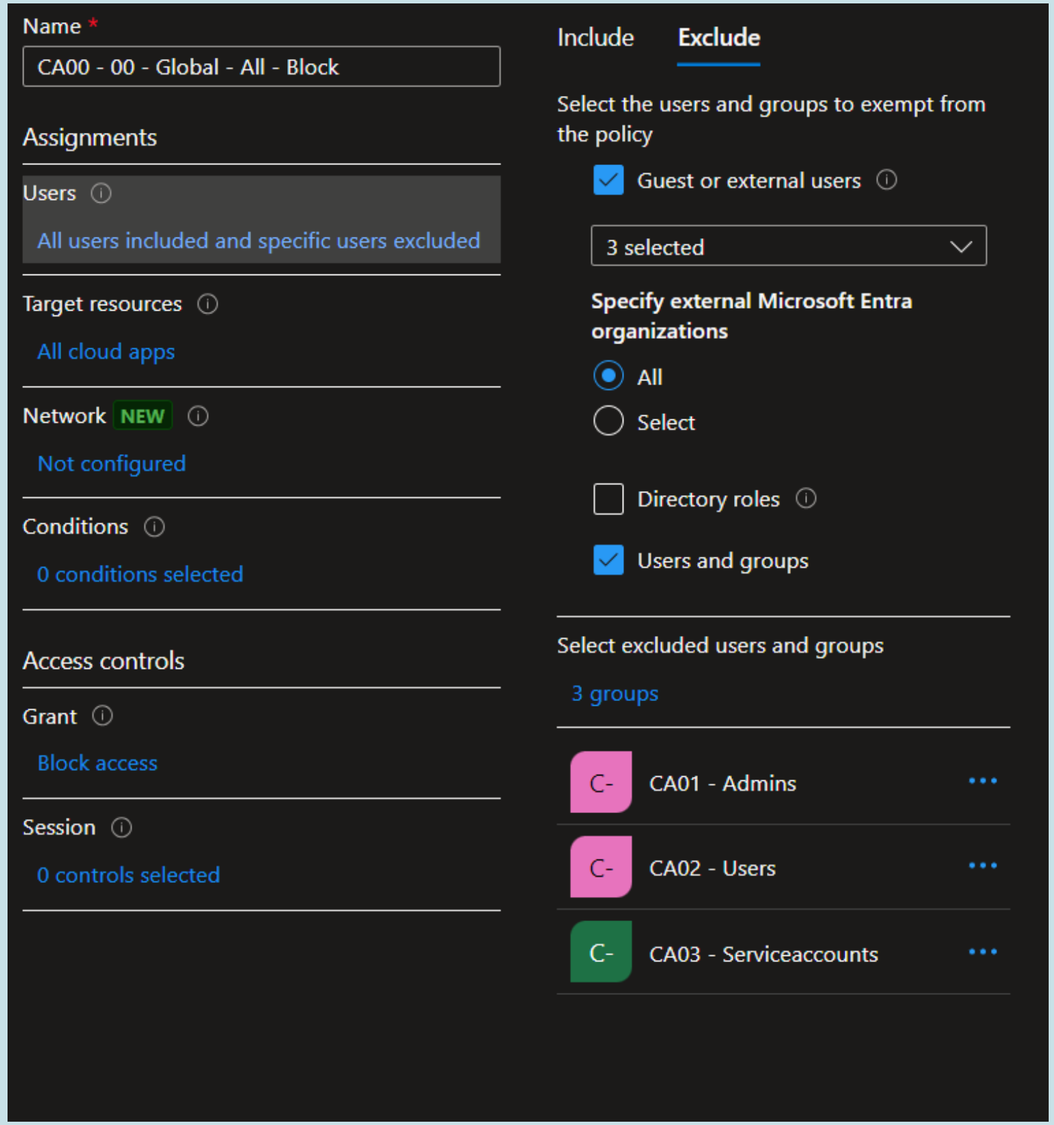
- 00 = Global (all accounts)
- 01 = Admins (privileged accounts)
- 02 = Users (user accounts)
- 03 = Faculty (faculty accounts)
- 04 = Students (student accounts)
- 05 = Research (research accounts)
- 06 = Guests (guest accounts)
- 07 = Svc (service accounts)

- Naming standard:
- CA(Personanr.) – (Seq.nr) – (Persona) – (Target) – (Requirement)

- Examples:
- “CA01 – 00 – Admins – Baseline – Req.MFA”
- “CA02 – 03 – Users – Visma – Req.CompliantDevice”

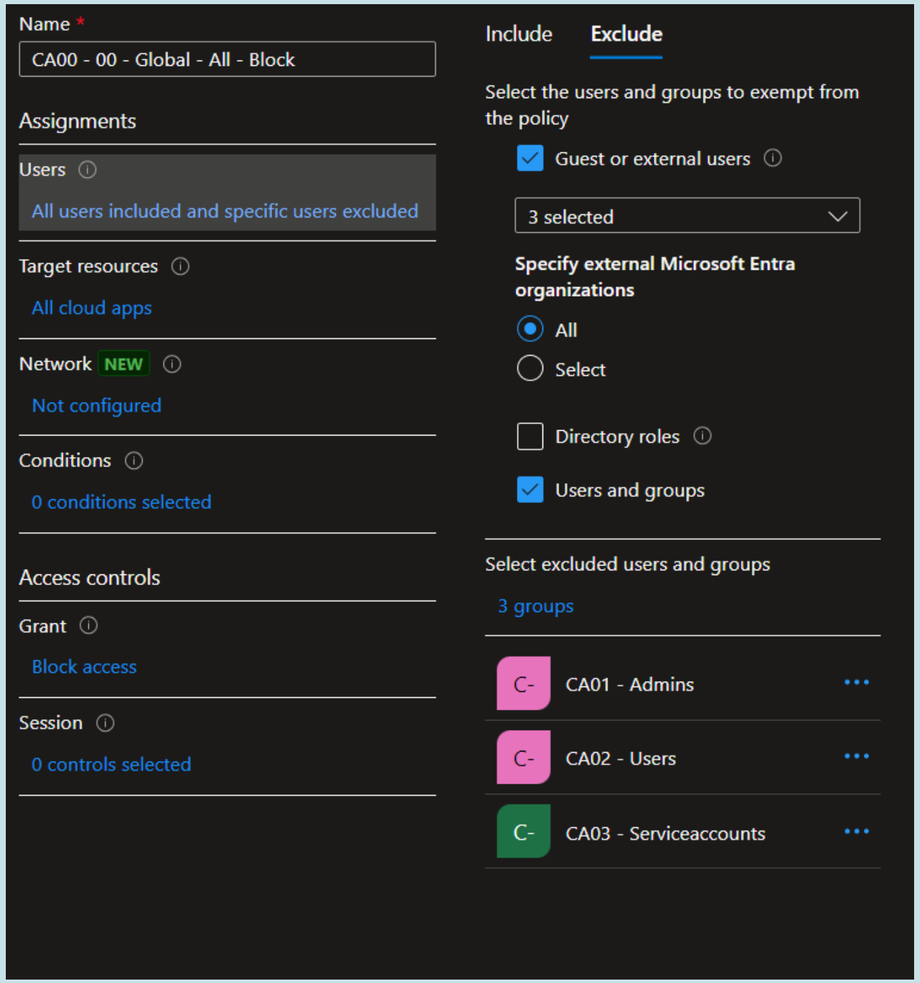
Block login by default

- “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



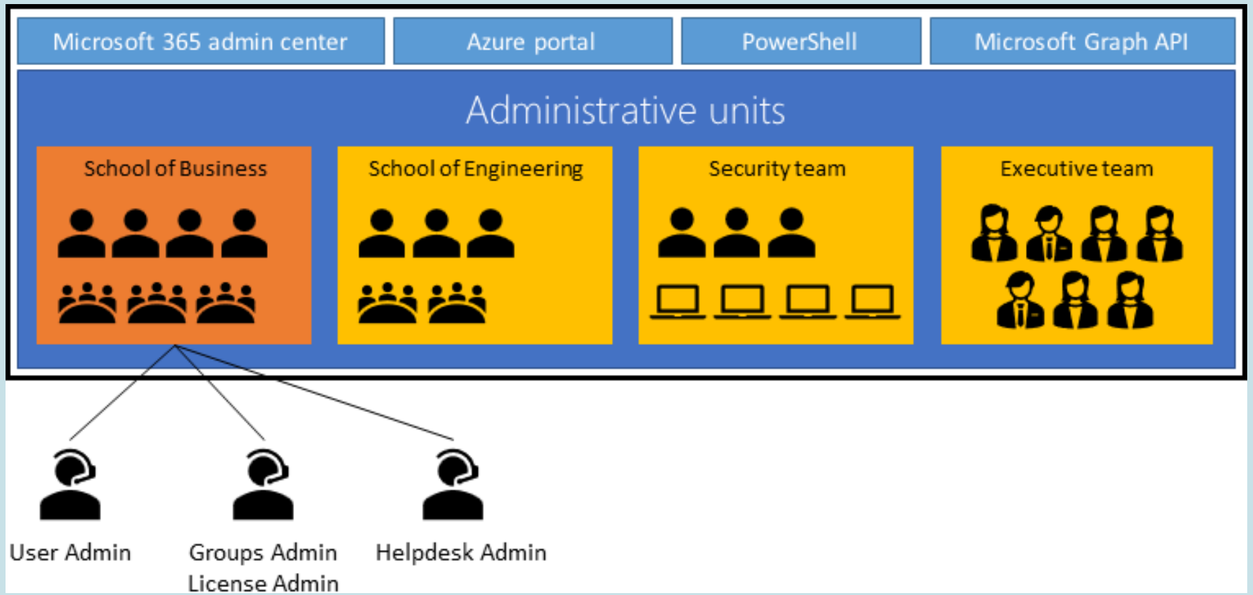
Systematically assign CAP

- 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”
- “Baseline” = Minimum protection
- Use additional rules to add/customize protection
- This setup prevents logins without CAP applied



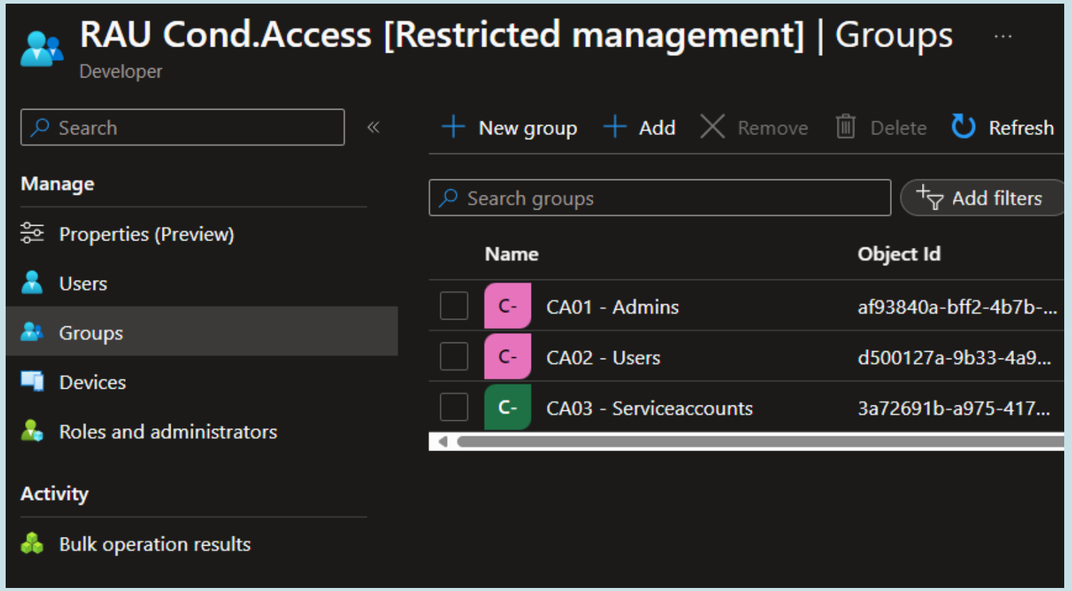
Control which accounts can log in

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



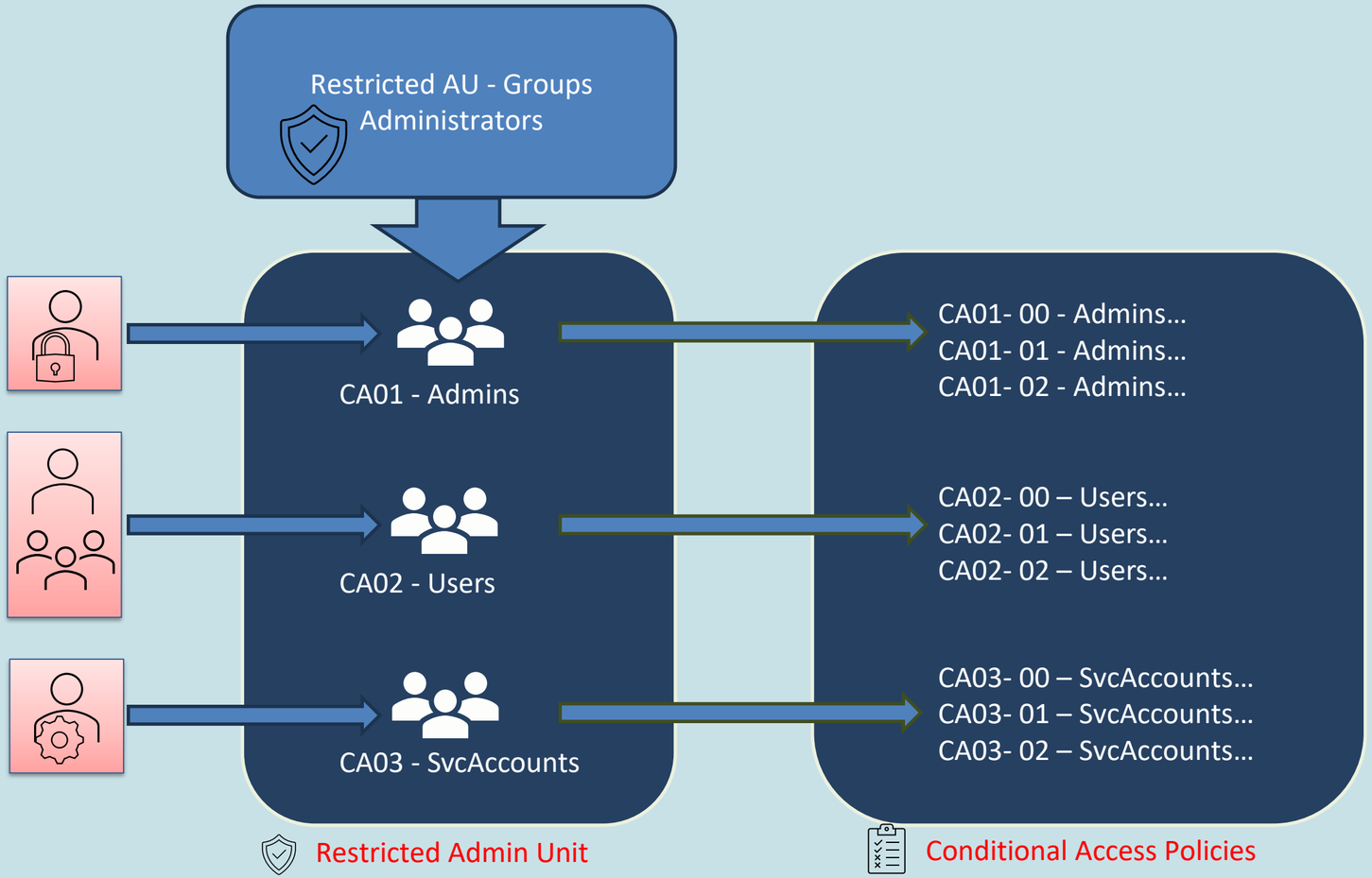
Control which accounts can log in

- Entra ID **Restricted management** AU
- A restricted AU blocks privileged access from other admins in the tenant
  - Only the AU-delegates has privileged access
- We will:
  1. Add the CA-groups into the Restricted AU
  2. Delegate “Groups administrator” role to specific users
- No one else can change group membership, prevents lateral movement
- This effectively locks down the ability to grant log on rights, to specific people in your tenant.



Experts Live Kenya

An overview


Restricted AU - Groups
Administrators
CA01 - Admins
CA02 - Users
CA03 - SvcAccounts
CA01- 00 - Admins…
CA01- 01 - Admins…
CA01- 02 - Admins…
CA02- 00 – Users…
CA02- 01 – Users…
CA02- 02 – Users…
CA03- 00 – SvcAccounts…
CA03- 01 – SvcAccounts…
CA03- 02 – SvcAccounts…
Restricted Admin Unit
Conditional Access Policies

DEMO!
Cond.Access hardening!

Delegate with care!

- Can change Conditional Access settings:
  - Conditional Access Administrator
  - Security Administrator
  - Global Administrator
- Can change or delete Restricted AU:
  - Privileged Role Administrator
  - Global Administrator
- Can change/reset password and MFA on all accounts (including Global Admins):
  - Privileged Authentication Administrator
  - Global Administrator
- Back up your Cond.Access rules!
- Monitor and set up alerts for changes in:
  - Cond.Access rules
  - Restricted AU

Section conclusion

Change Conditional Access to block-by-default

Adapt CAP to your organization and its needs

A good naming standard is important

Back up your CA policies

Monitoring and alert is vital!

Agenda

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

Winter in Kenya

Experts Live Kenya

6 months ago..

Experts Live Kenya

6 months ago..

Experts Live Kenya

6 months ago..

6 months ago..

Experts Live Kenya

Raise your hands please

Is anyone in the audience unfamiliar with:

The fundamental features and principles of
Asymmetric keys (private/public keys)

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

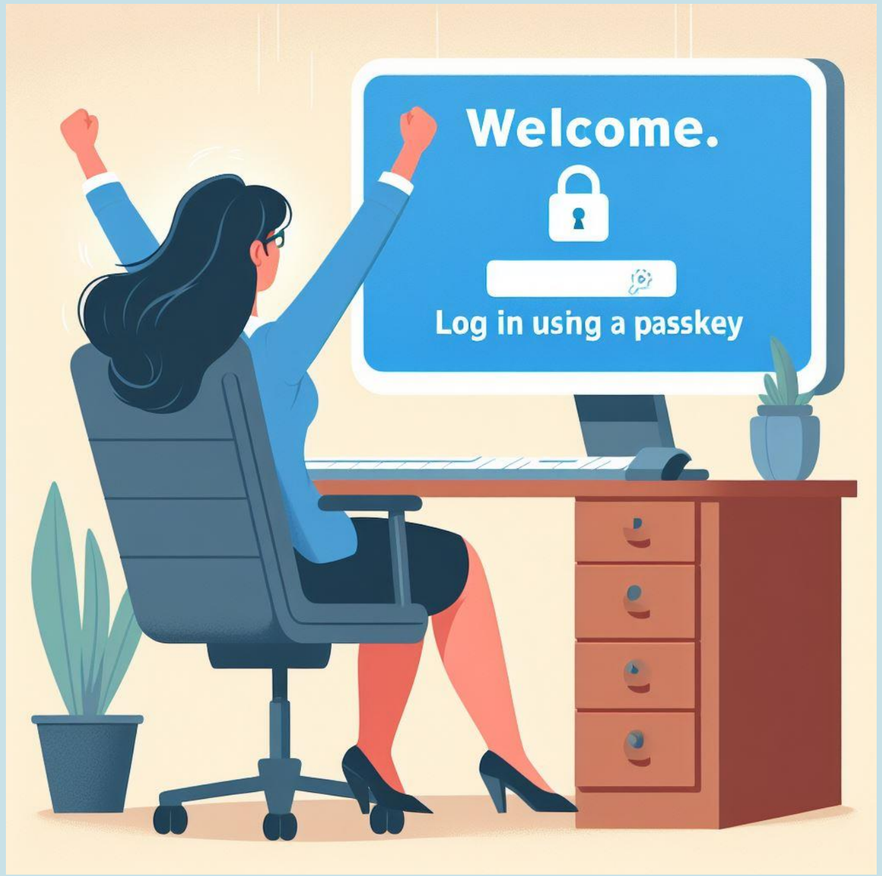
- **Public** key is shared – **Private** key stays with owner, always hidden

- 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 authentication 🥳
- From the FIDO2 alliance
- Built from the ground-up
  - Easier than passwords
  - More secure than passwords
- Based on PKI (Asymmetrical keypairs)
  - Activated by PIN or biometrics
- Communicates over “webauthn”
- First: Generic passkeys

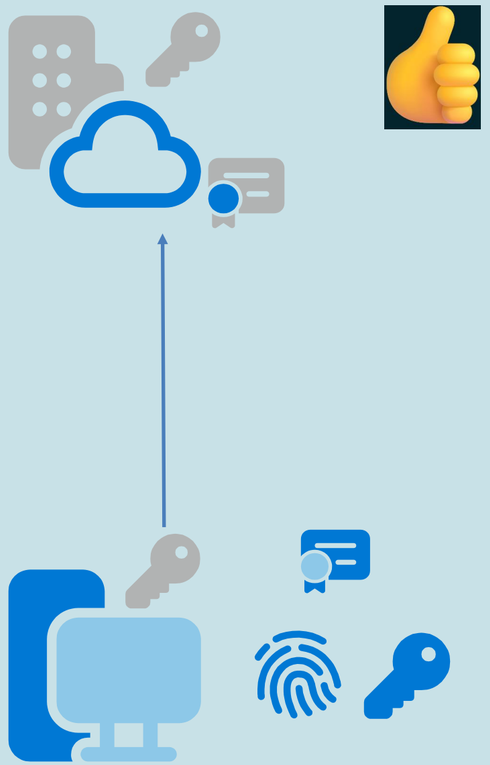


Passkey creation

- 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

Passkey login

1. User wants to log in:
   - Client sends an authentication request
   - Includes public key
2. The cloudservice:
   - Check the public key
   - Generates a random challenge
   - Signs it with the **public** key
   - Transmits it to the client with a credential ID
3. The user:
   - verifies his/her identity locally with PIN/biometric
   - Activates the private key
4. The client:
   - Verifies the signature using the **private** key
   - Signs the challenge with the **private** key
   - Returns it with username and cred.ID
   - Only valid once
5. The cloudservice:
   - Verifies the signature
   - Checks cred.ID
   - provides session token



DEMO!
Passkeys
(Github)

Why are passkeys better?

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

Passkeys in Entra ID (preview)

👍 Public preview since April 2024

👍 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

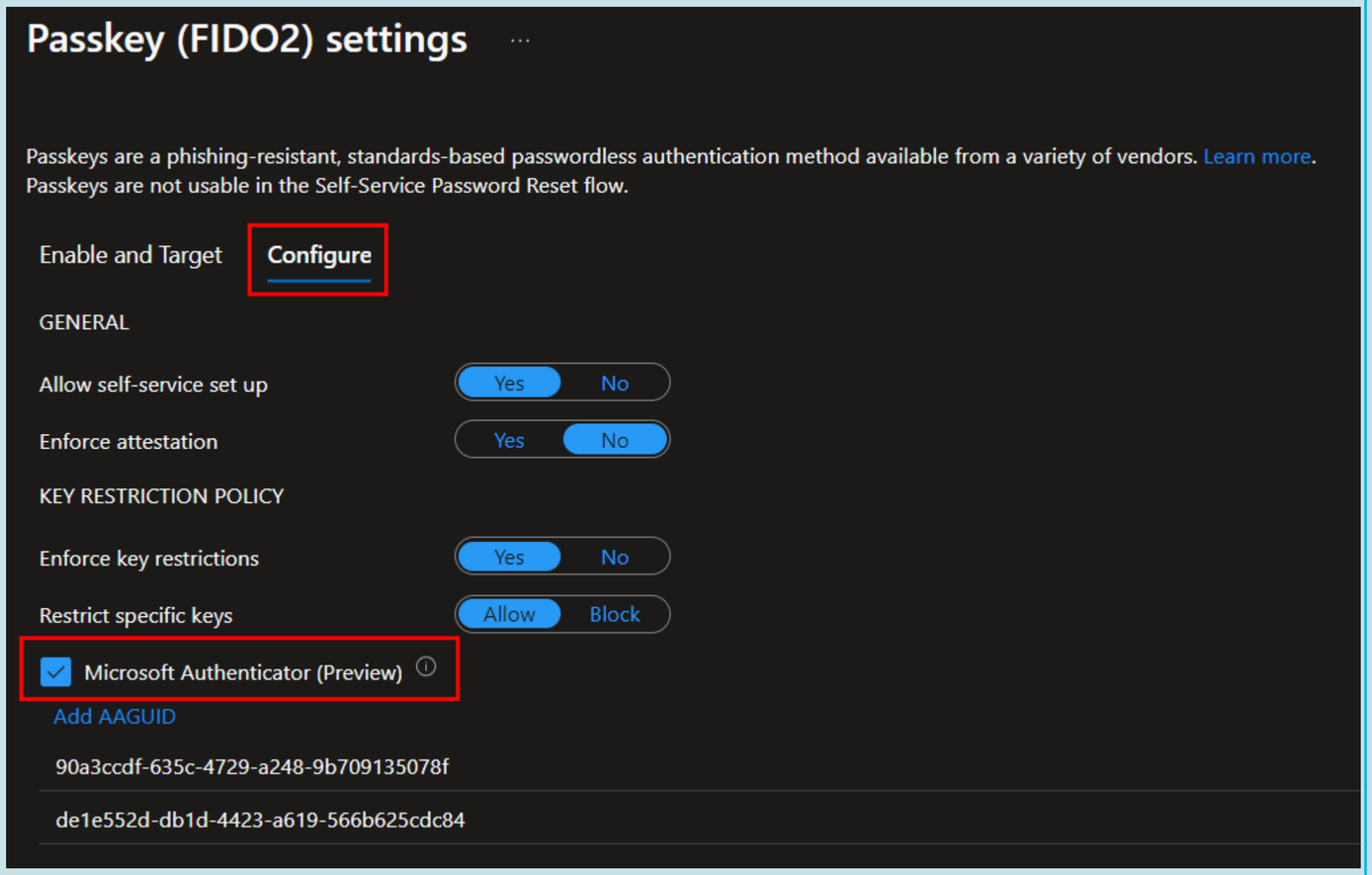
Passkeys in Entra ID (preview)

Admins:
Enable passkeys in the tenant:

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

Remember:

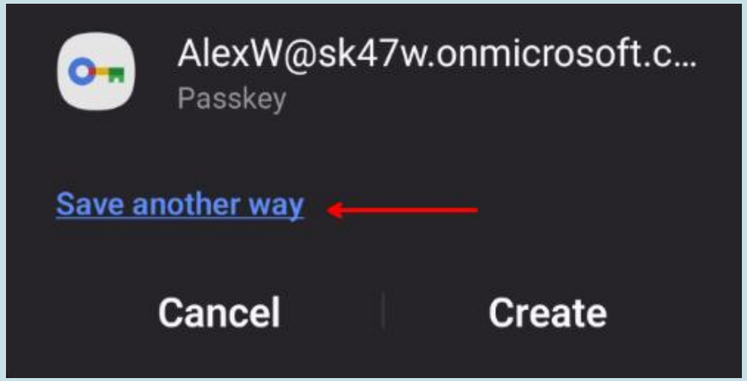
The end-user needs at least one MFA method to register a passkey

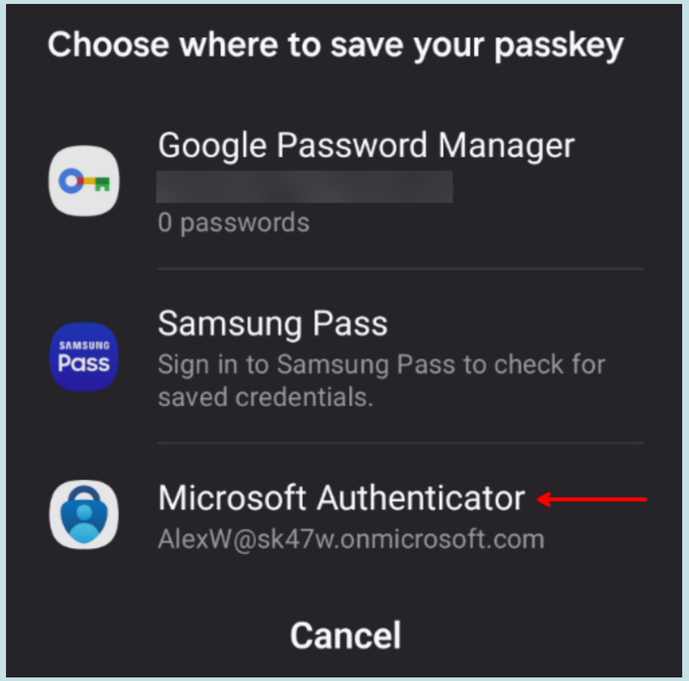


Passkeys in Entra ID (preview)

End-user:

1. Sign in to https://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)

Section conclusion

Passkeys are low-cost and highly secure

Very user friendly

Passkeys in Entra ID requires Authenticator app

Start testing today! This a MAJOR feature!

Asante, Afrika ❤️

If you want to go fast, go alone.

If you want to go far, go together!

Experts Live Kenya

Session Feedback

Session Track:

Security

Session Name:

No more identity theft!

Harden your identity security today

Experts Live Kenya

Experts Live Kenya

THANK YOU

Per-Torben Sørensen
Technical architect @ Crayon
Linkedin:

Experts Live Kenya

THANK YOU TO OUR SPONSORS!

NTT DATA

gebeya

Microsoft

FEITIAN
WE BUILD SECURITY

ADC AFRICA DEVELOPMENT CENTER

USIU AFRICA
United States International University-Africa
Education to take you places

2LINKIT

Computer Revolution Africa Group
Technology redefined

NiCE
IT Management Solutions