NT KONFERENCA

25. – 27. SEPTEMBER 2023
PORTOROŽ

Paswordless in druge Microsoft Entra avtentikacije

Slavko Kukrika
(Slavko.Kukrika@Outlook.com)
MCT in prijazen fant

Agenda

- Passwords are bad! *(and insecure)*
- Multi-factor authentication is better
- Passwordless authentication *(is the best!)*
- Certificate-based authentication
- Temporary Access Pass

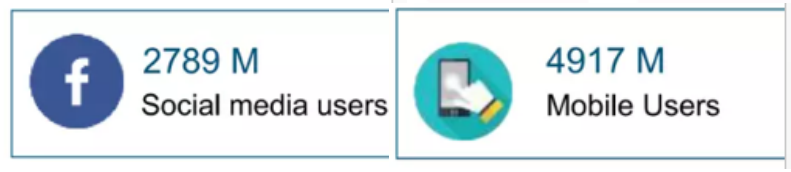
Nobody Likes Passwords

Alpha-numeric passwords are hard for humans to remember and easy for computers to guess

On mobile devices entering passwords is challenging

Credential reuse across multiple services increases attack surface

Even the strongest passwords are easily phishable



Strength of authentication methods

Bad: Password

123456

qwerty

password

iloveyou

Password1

Good: Password
and...

SMS

Voice

Better: Password
and...

Authenticator
(Push Notifications)

Software
Tokens OTP

Hardware Tokens OTP

Best: Passwordless

Authenticator
(Phone Sign-in)

Window
Hello

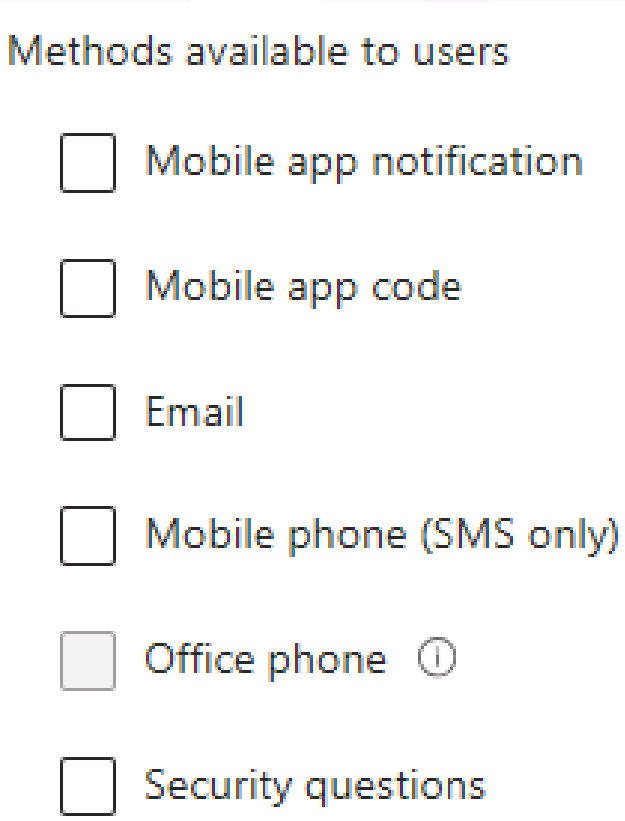
FIDO2 security key

Certificates

Single factor

Two-Factor/Multi-Factor Authentication

Microsoft Entra authentications



- Passwords
- One time password (OTP)
- Temporary Access Pass
- Multi-factor authentication
  - SMS with code
  - OTP code
  - Certificate-based authentication
- Passwordless
  - Microsoft Authenticator
  - FIDO2 security key
  - Windows Hello for Business
  - Certificate-based authentication

Method
FIDO2 security key
Microsoft Authenticator
SMS
Temporary Access Pass
Hardware OATH tokens (Preview)
Third-party software OATH tokens
Voice call
Email OTP
Certificate-based authentication

Microsoft Entra and MFA

Available from the first day, in all Microsoft Entra editions

- Without Microsoft Entra ID P1 you cannot use conditional access policy (only per-user MFA)

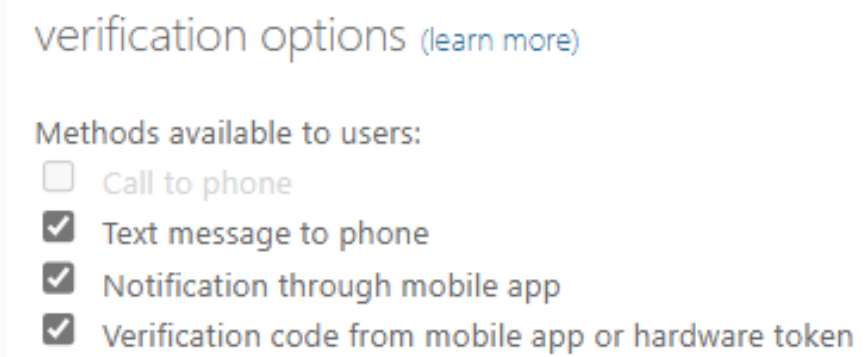
Microsoft Entra Security defaults require MFA

True MFA potential can be achieved by using conditional access

Microsoft Entra ID protection

On September 30th, 2024, the legacy multifactor authentication and self-service password reset policies will be deprecated

- Legacy policies should be migrated to Authentication policies



Demo

Using MFA (SMS, one-time passcode)
SSPR with email, security questions
Conditional access policy

Password replacement technology

Passwordless is a form of MFA authentication that replaces the password with a secure alternative

This type of authentication requires two or more verification factors to sign in that are secured with a cryptographic key pair

Windows Hello

Microsoft Authenticator

FIDO2 Security Keys

Windows Hello for Business

Replaces passwords with strong multi-factor authentication

Windows 10/Windows 11 device required

User credentials are linked to a device

- Biometric or PIN is used to unlock access
- Can sign in with your face, iris scan, fingerprint or PIN

Password is not used and not stored anywhere

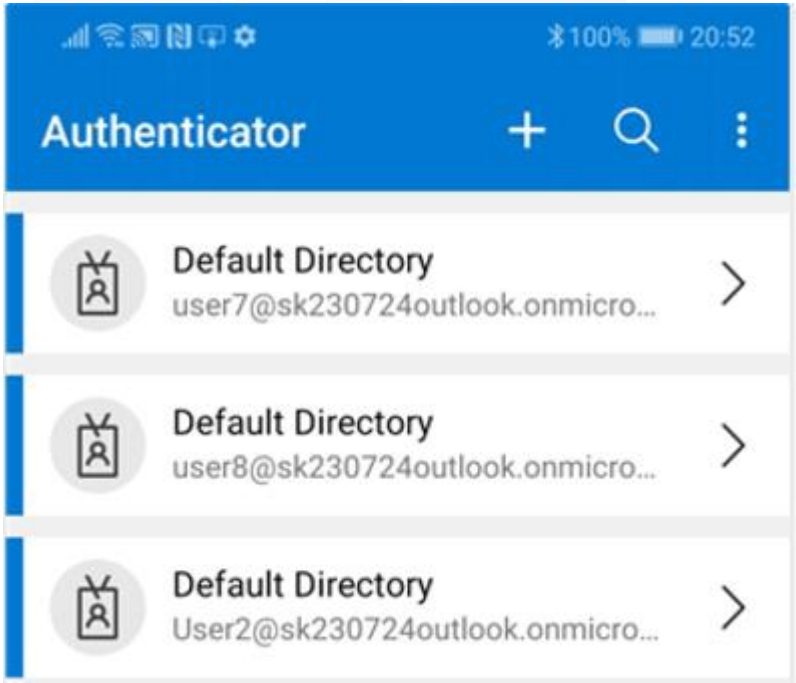
The biometric data is only used locally and never leaves the device

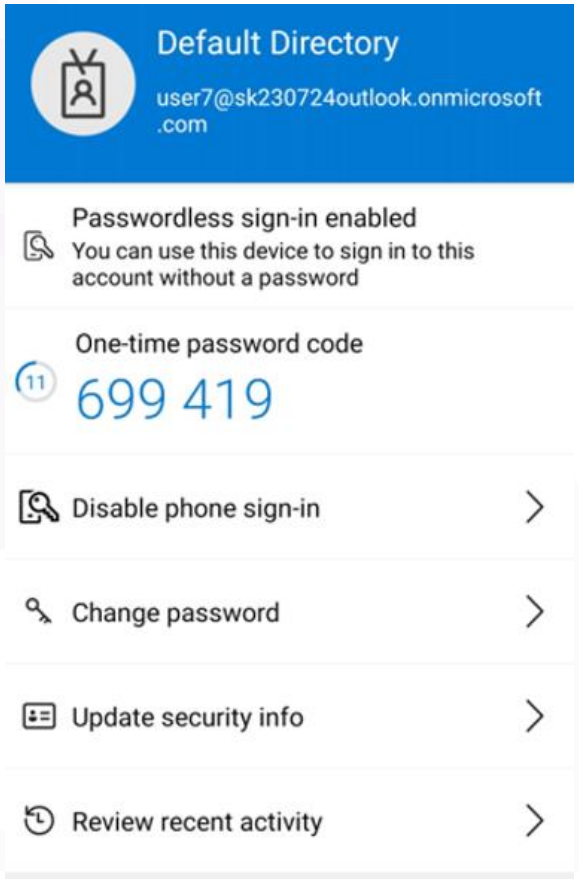
Microsoft Authenticator app

Available for Android and iOS

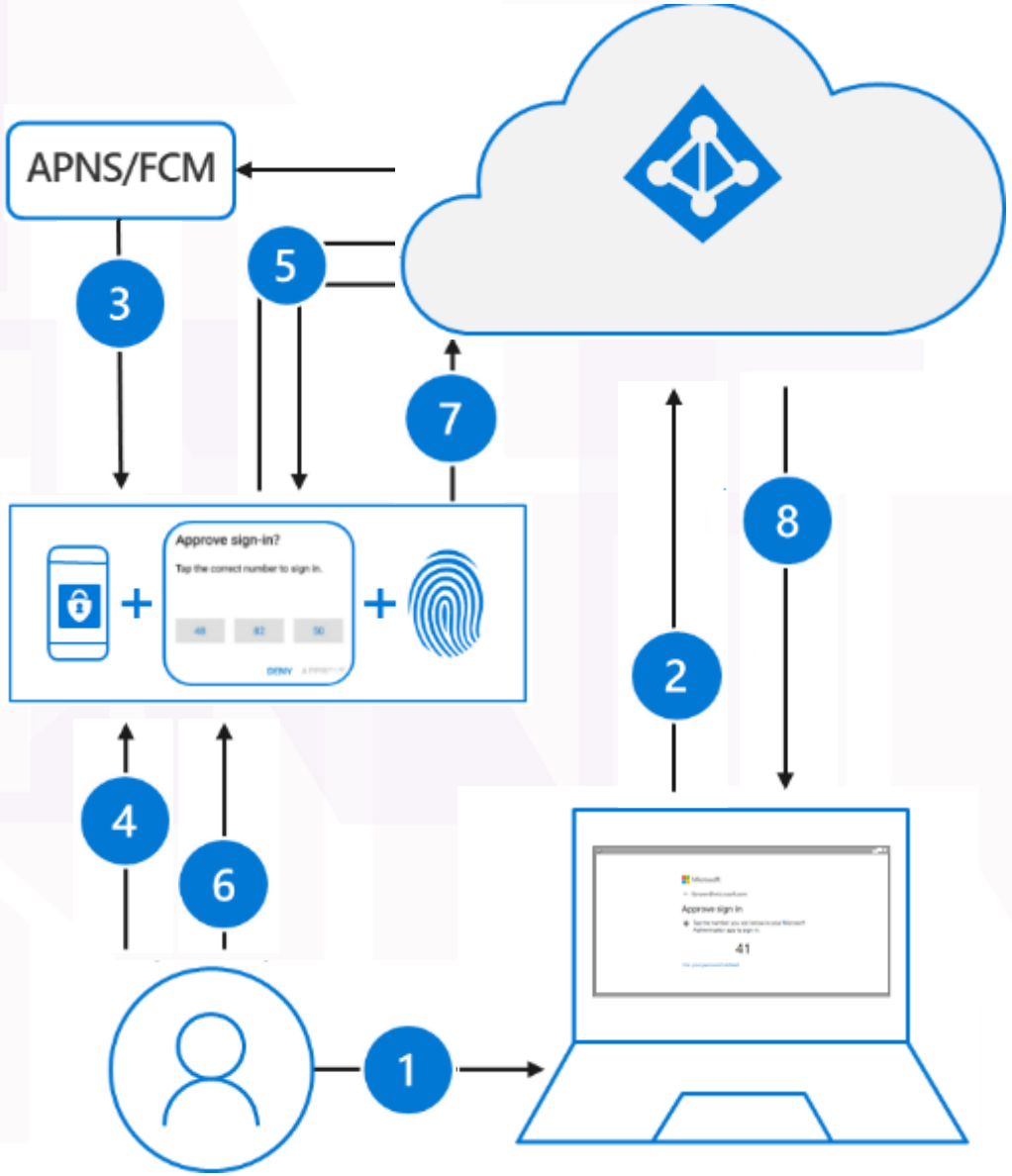
Can augment password with one-time passcode or push notification

Securely store Verified IDs

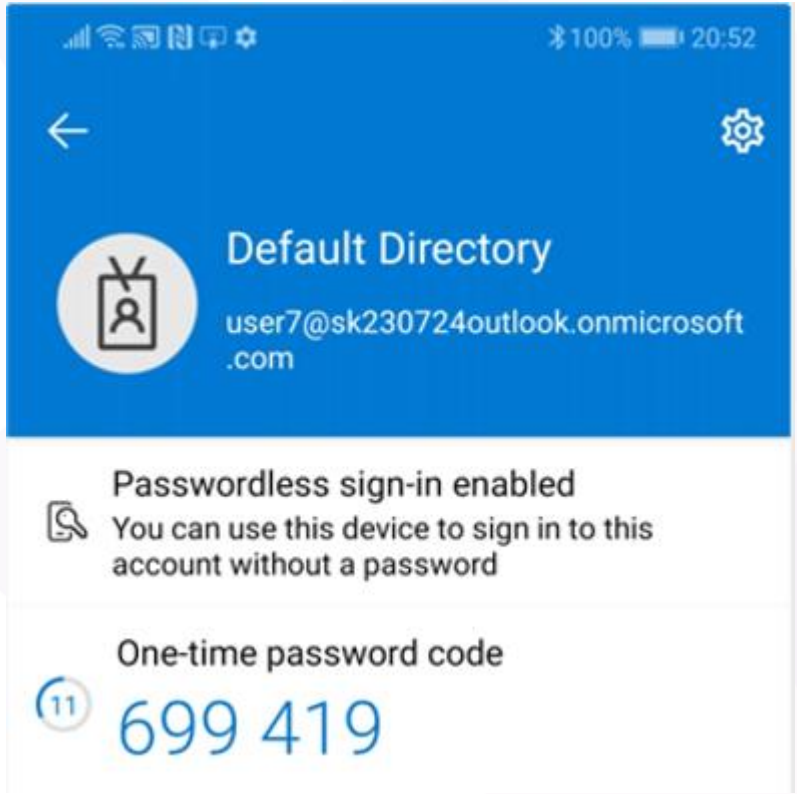


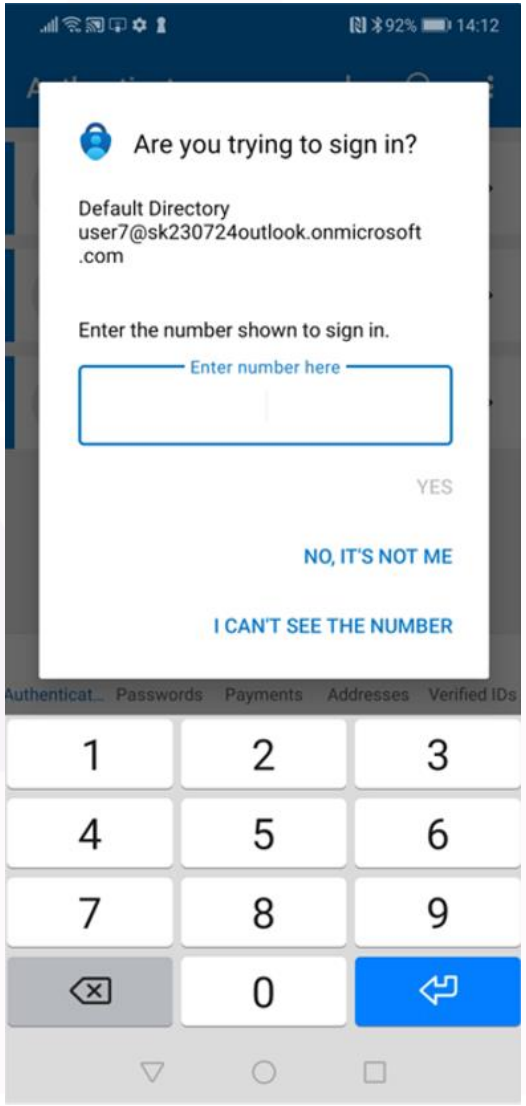


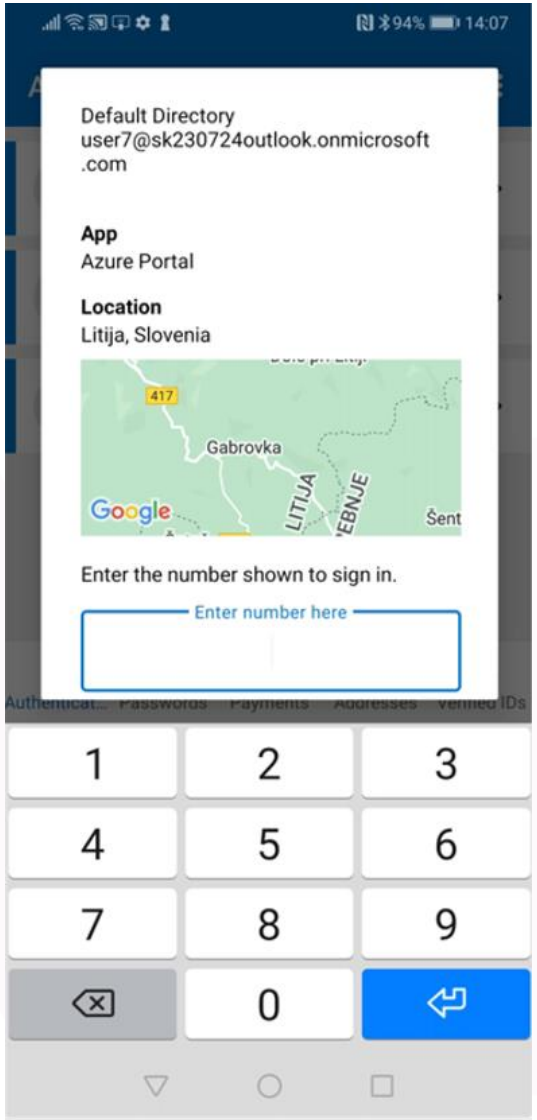
Authentication Flow with Microsoft Authenticator app



Microsoft Authenticator authentication







NT KONF
NT KONFERENCA

#ntk23

Demo

Paswordless sign in
Configuring Microsoft Authenticator method

Certificate-based authentication (CBA)

- Authenticate with X.509 certificates for applications and browser sign-in
  - Available with all Microsoft Entra ID editions
  - Passwords not needed, they don’t need to be synced to the cloud for hybrid users
  - Works with Windows, Android and iOS devices
- PKI for creating client certificates is not part of CBA
- One CRL Distribution Point (CDP) for a trusted CA is supported
  - Must be accessible over HTTP protocol - Online Certificate Status Protocol (OCSP) and Lightweight Directory Access Protocol (LDAP) URLs are not supported
- Password as an authentication method cannot be disabled
- If CBA is enabled on the tenant, all users see link to sign in with certificate
  - Only users in scope for CBA are able to authenticate by using certificate

Configuring CBA

Use your own PKI infrastructure (for example AD Certificate Services)

Certificates must be deployed to users (Microsoft Intune, GP, …)

1. Configure the certification authority (upload CA certificate)
2. Enable CBA on the Microsoft Entra tenant
3. Configure authentication binding policy
4. Ensure that users have certificate on their device
5. Test the configuration

Demo

Signing in by using CBA
Configuring CBA

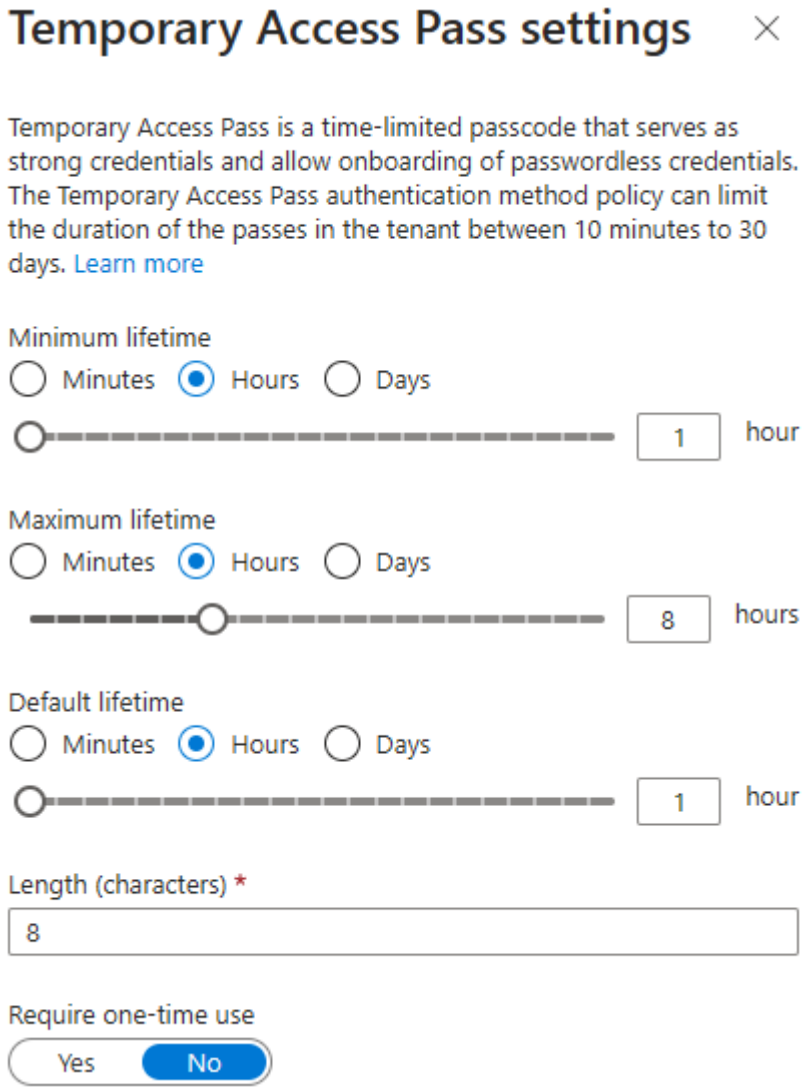
Temporary Access Pass

Time-limited passcode that can be configured for single use or multiple

- Often used to onboard to other authentication method, including passwordless
- Makes recovery easier when a user has lost or forgotten their strong authentication factor

To configure Temporary Access Pass

1. Enable the Temporary Access Pass policy
2. Create a Temporary Access Pass
3. Provide Temporary Access Pass to user



Summary

Passwords are here from the first days …

… but they should be supplemented (MFA) or replaced (Passwordless)

Use conditional access policies to require MFA

Microsoft Entra provides many authentication methods

And they can be used in the same Microsoft Entra tenant

Migrate to authentication method policies

Consider passwordless and CBA

No authentication is perfect …

… but we are getting close!

Additional information

Authentication and verification methods in Microsoft Entra ID

https://learn.microsoft.com/azure/active-directory/authentication/concept-authentication-methods

Migrate MFA and SSPR policy settings to Authentication methods

https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-authentication-methods-manage

Passwordless authentication options for Microsoft Entra ID

https://learn.microsoft.com/azure/active-directory/authentication/concept-authentication-passwordless

Enable passwordless sign-in with Microsoft Authenticator

https://learn.microsoft.com/azure/active-directory/authentication/howto-authentication-passwordless-phone

Overview of Microsoft Entra certificate-based authentication

https://learn.microsoft.com/azure/active-directory/authentication/concept-certificate-based-authentication

Questions?

Slavko.Kukrika@Outlook.com

25. – 27.
SEPTEMBER
2023
PORTOROŽ

This is not school, but we love to get grades.
Please fill out our questoineers and leave us your feedback.
You may even win some cool rewards.