Passwordless Authentication Webinar
26. & 31. Oktober 2023

AVANTEC
Competence. Security. Trust.

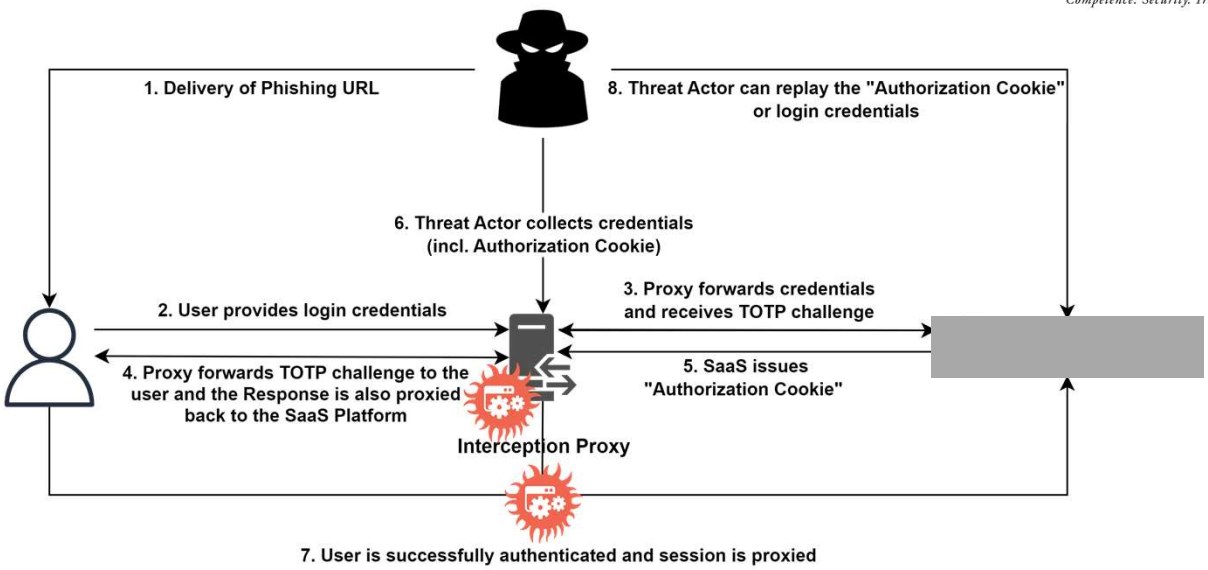
Weil Sicherheit alles ändert.

Michael Scherzinger
Senior Security Engineer | PAM Product Manager
scherzinger@avantec.ch

Robin Helbling
Cyber Defense Specialist
helbling@avantec.ch

Demo: Cyber Defense Team

AVANTEC
Competence. Security. Trust.



AVANTEC
Competence. Security. Trust.

Passwordless Authentication Webinar
26. & 31. Oktober 2023

Awareness

MFA Fatigue Attack

What is an MFA Fatigue Attack?

A multi-factor authentication (MFA) fatigue attack – also known as MFA Bombing or MFA S
second-factor authentication requests to the target victim's email, phone, or registered devi
authenticating the attackers attempt at entering their account or device.

To initiate the MFA push notifications, and attacker must first login in as the target user. Th
such as phishing, to gain credentials. Stolen credentials may also be acquired from the darl

Most modern MFA platforms support push-notification style authentication. After submittir
then receives a push notification asking them to confirm their second factor authentication
allows users to authenticate their identity through a single phone notification, and often a s

The prevalence of this simplified authentication architecture is what's causing MFA fatigue
fatigue attack is the September 2022 **Uber breach by Lapsus$**, a hacking group notorious f
ransomware software, taking corporate resources or sensitive data hostage in exchange fo

Microsoft

We're enabling a stronger form of multifactor authentication beginning September 15, 2023

You're receiving this email because you have a Microsoft Entra ID tenant.

On September 15, 2023, we'll begin prompting your users who authenticate using SMS and voice methods to set up the Microsoft Authenticator app when they sign in to their work or school account. This change will take place on a rolling basis over six weeks as part of ongoing efforts to improve security.

This change will affect Microsoft Entra ID (previously Azure Active Directory) tenants that have the registration campaign feature set to the Microsoft managed state. After we enable the feature, users will be prompted to install the Microsoft Authenticator app, a stronger form of multifactor authentication than SMS and voice methods.

Recommended action

After the registration campaign feature is enabled, everyone in your organization who currently uses SMS or voice authentication will need to set up Microsoft Authenticator. **To avoid any confusion, let your users know what to expect by September 15, 2023:**

- When they sign in to their work or school account, they'll see a prompt to set up the Authenticator app—they can choose to install it or skip the prompt. They can skip up to three times before they're required to install it.
- To install it, they'll need to select *Next* on the prompt, which will take them through the Authenticator app setup.

Noch ne OTP Challenge

AVANTEC
Competence. Security. Trust.

- **Per App zum TOTP-Code**
- Die bekannteste dieser TOTP-Apps dürfte der Google Authenticator sein. Dieser und der Microsoft Authenticator gerieten jedoch 2020 in die Schlagzeilen, weil sie unter Android das Erstellen von Screenshots nicht deaktiviert hatten. Entsprechend hätte eine Schadsoftware einfach einen Screenshot der App erstellen und so an die 2FA-Codes gelangen können.

Passwordless Authentication Webinar
26. & 31. Oktober 2023

What is Passwordless?

AVANTEC
Competence. Security. Trust.

- Was ist nun «Passwordless»?
  - Authentication based on Asymmetric Cryptography (Public Key Algorithm)
    - Smart Card – Certificate-based AuthN
    - FIDO – Key-based
    - WHfB – Key- or Certificate-based
    - Passkey (Google, Apple, Dashlane, NordPass, 1Password)
    - Hypr
    - VeridiumID
    - FUTURAE
    - ZSO

Warum reicht denn nun nicht OTP?

AVANTEC
Competence. Security. Trust.

- Die Methode sollte für Desktop, Classic Application and Web-Services (Cloud) sein.
- Seeds – Shared Secret – symmetrisch
  - Wer hat Zugriff auf die Seeds (Dienstleister, Cloudanbieter …)?
- Screenshots on Mobile Device – Anfang 2020
  - Backup der Codes im Google Account?
  - 2-Step Verification
- PushOTP – MFA Bombing
- Seed im QR-Code versus DSKPP
- And no SMS

AVANTEC
Competence. Security. Trust.

Passwordless Authentication Webinar
26. & 31. Oktober 2023

Differents in Asymmetric vs. Symmetric & Smart Card vs. FIDO

AVANTEC
Competence. Security. Trust.

- What is FIDO compared with a Smart Card (cba)?
- Algorithm
  - Public Private Key
  - Symmetric Key
- Keys on hardware or software protected

Was bringt uns nun dieses Asymmetrische?

AVANTEC
Competence. Security. Trust.

- Den Public Key können wir jedem geben – auch jedem Angreifer.
- Secure Authentication – Non-Repudiation
- Phishing Resistancy
- No man-in-the-middle
- No pwd rotation

AVANTEC
Competence. Security. Trust.

Passwordless Authentication Webinar
26. & 31. Oktober 2023

Mehr Background zu FIDO

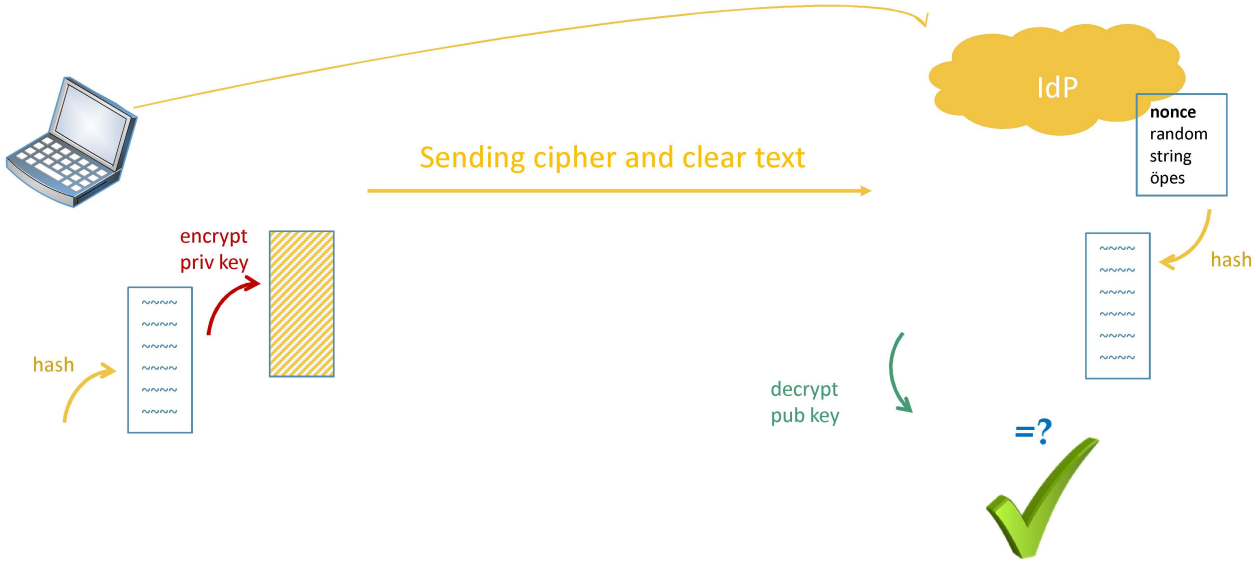
AVANTEC
Competence. Security. Trust.

- Public Key-based AuthN
- No userID
- No trust chain
- Validity
- Revocation

- ➔ We need an IdP

Passwordless – Asymmetric Authentication

AVANTEC
Competence. Security. Trust.



AVANTEC
Competence. Security. Trust.

Passwordless Authentication Webinar
26. & 31. Oktober 2023

Mehr zu Certificate-based Authentication

- Smart Card – Trennung von Using and AuthN Device
- Trust a RootCA Certificate
- Subject in the Certrificate (Subject Alternate Name)
- Validation
- Recovery
- Flexibler mit Algorithmen
- Enhanced Key usage

- Private Keys sicher aufbewahren – Hardware (USB-Token oder Smart Cards [ID-1])

Thales devices – pure FIDO – pure SC or hybrid

SafeNet IDPrime FIDO

SafeNet eToken FIDO

SafeNet eToken FIDO

SafeNet eToken Fusion Series

- https://cpl.thalesgroup.com/access-management/authenticators/fido-devices#IDPrime

Passwordless Authentication Webinar
26. & 31. Oktober 2023

Welche Dienste unterstützen nun «Passwordless»?

AVANTEC
Competence. Security. Trust.

- SSH Private Key AuthN
- The most products VPN GW, Windows Desktop (rdp), encryption products and a lot more Certificate-based AuthN
- Webservices or products supporting FIDO2
- Windows Hello for Business
  - Key-based oder Certificate on TPM
- Passkey: Google and Apple start switching 2022 to Passkey

- Passphrase or PIN, Fingerprint, Face Recognition are used for Private Key Approval

Optimization:
- SAML
- OIDC

Und was schlägst Du nun vor?

AVANTEC
Competence. Security. Trust.

1. Smart Card
   → Hybride Karten mit Gebäudezutritt und Payment, Secure Printing, Digital Signing …

2. Kombinationen
   - IDPrime 3930 mit NFC und FIDO
   - eToken Fusion

- Oder sonstiges
- Windows Hello for Business

- SAML / OIDC

AVANTEC
Competence. Security. Trust.

Passwordless Authentication Webinar
26. & 31. Oktober 2023

Check your Authentication

AVANTEC
Competence. Security. Trust.

- Interne AuthN – Zielsystem
- Externe / Cloud AuthN – Ressourcen / Services
- Password Rotation
- Password-Speicher
- Welche Verfahren werden eingesetzt?
- Welche Daten werden wo gespeichert?
- MFA – UserID in pwd in der Cloud?

- Phishing Resistancy – which authentication is phishing-resistant?
- Azure AD mit FIDO oder SC – geht das?
- Hybride Karten (IDPrime – FIDO – RFID (LEGIC)

Passwordless strategy

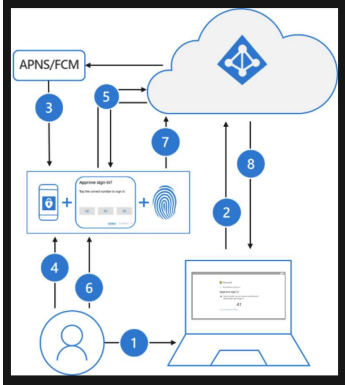
- Der Aufwand muss sich lohnen
  - Phishing Protection
  - No stolen Identities

- Synergien nutzen
- Single Sign-on

- Smart Card / FIDO on Azure

- SAML/OIDC or so

Passwordless authentication using the Authenticator app follows the same basic pattern as Windows Hello for Business. It's a little more complicated as the user needs to be identified so that Azure AD can find the Authenticator app version being used:



1. The user enters their username.
2. Azure AD detects that the user has a strong credential and starts the Strong Credential flow.
3. A notification is sent to the app via Apple Push Notification Service (APNS) on iOS devices, or via Firebase Cloud Messaging (FCM) on Android devices.
4. The user receives the push notification and opens the app.
5. The app calls Azure AD and receives a proof-of-presence challenge and nonce.
6. The user completes the challenge by entering their biometric or PIN to unlock private key.
7. The nonce is signed with the private key and sent back to Azure AD.
8. Azure AD performs public/private key validation and returns a token.

To get started with passwordless sign-in, complete the following how-to:

Enable passwordless sign using the Authenticator app

FIDO2 security keys

The FIDO (Fast IDentity Online) Alliance helps to promote open authentication standards and reduce the use of passwords as a form of authentication. FIDO2 is the latest standard that incorporates the web authentication (WebAuthn) standard.

AVANTEC
Competence. Security. Trust.

Passwordless Authentication Webinar
26. & 31. Oktober 2023

Fragen

AVANTEC
Competence. Security. Trust.

AVANTEC
Competence. Security. Trust.