



CONET Webinar

MFA, Neue Trends & Möglichkeiten

26.10.2023 | Jörg Meuser

Vorstellung des Referenten

Jörg Meuser

**Managing Consultant
Identity & Security Management**



Multifaktor-Authentifizierung

Agenda

- Teil 1** ■ **Der Stand der Dinge**
- Teil 2** ■ **Zukunft und Gegenwart**
- Teil 3** ■ **Ausblick**



Teil 1

Der Stand der Dinge

1

CONET

Multifaktor-Authentifizierung

Passwörter sind Gefahrgut

- Unterliegt besonderen Auflagen (Compliance)
- Schwierig zu transportieren (Rollout)
- Komplexe Handhabung (Passwortmanagement)
- Hoch explosiv (Angriffsvektor)
- Schwer zu lagern (Speicherung)



Multifaktor-Authentifizierung

Akteure

- Diensteanbieter
- IT-Organisation
- Partner
- Anwender
- Software Hersteller
- Hardware Hersteller



Multifaktor-Authentifizierung

Die Faktoren bestimmen...



Multifaktor-Authentifizierung Herausforderungen

- Technische Komplexität
- Variierende Use-Cases
- Compliance Anforderungen
- Fehlende Prozesse
- Legacy-Anwendung & Dienste
- Budget



Multifaktor-Authentifizierung Vorsicht Falle!

- **Schlagwort-Abtausch**
 - 2FA vs. MFA
 - Passwort-Attacken
 - Passwort-Entropie
- **MFA reicht nicht**
 - MFA 2.0
 - Modern MFA
 - Phishing Resistant MFA
- **Authentifizierungsansatz...**
 - zu technisch
 - zu lösungszentriert
 - nicht Use-Case orientiert

Multifaktor-Authentifizierung

Die Lage (unverändert)

- Name & Passwort ist immer noch das häufigste oder einzige Verfahren
- Authentifizierung wird meistens Applikations- oder Dienst-bezogen umgesetzt
- MFA wird nur für bestimmte Dienste genutzt
- Die Auswahl der Faktoren orientiert sich am Angebot der Diensteanbieter
- Konzepte für eine organisationsbezogene Authentifizierung fehlen



Teil 2

Zukunft und Gegenwart

1

CONET



Multifaktor-Authentifizierung Entwicklung



FIDO2 ist etabliert



Breite Unterstützung der Hersteller



Vereinfachte Integration



Sicherheit durch passwortlose Verfahren

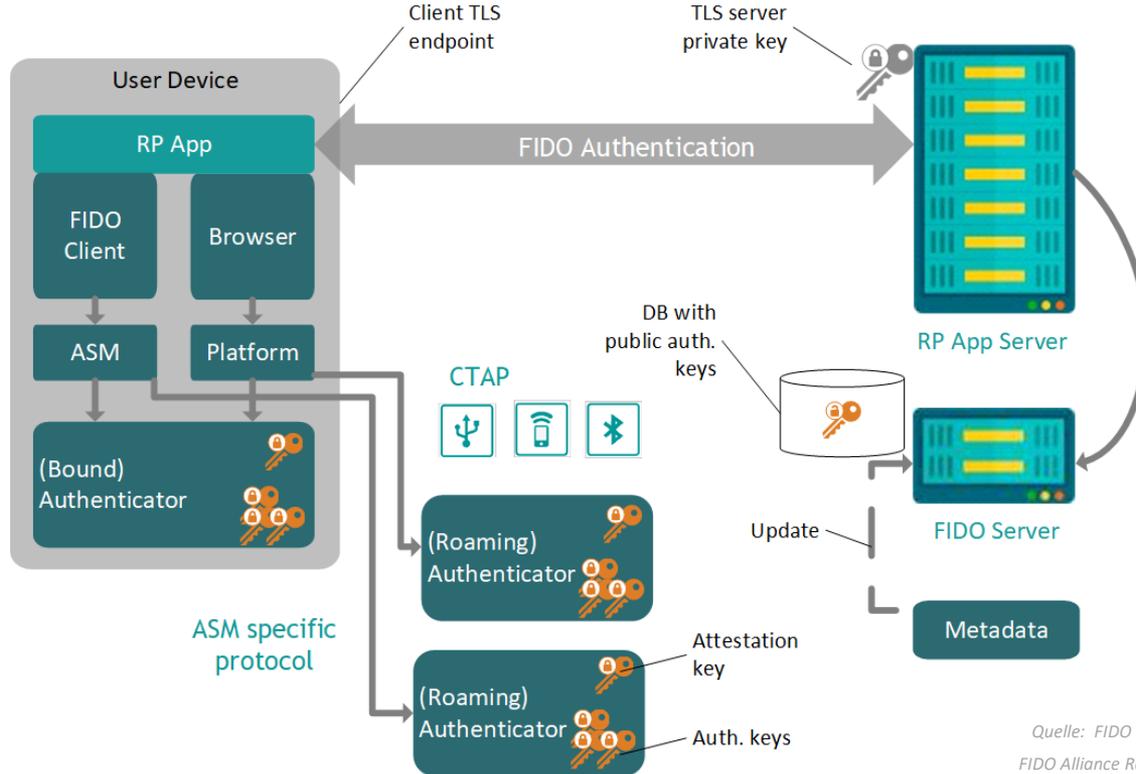


Multifaktor-Authentifizierung Begriffe und Mythen

- **Klarstellung**
 - Passwortlose Verfahren sind keine Technologie
 - FIDO ist kein Produkt
 - Faktoren können beliebig kombiniert werden
- **Nicht verwechseln..**
 - MFA <> Passwortloses Verfahren
 - Passwortlose Verfahren <> FIDO
 - PIN <> Passwort
- **FIDO Alliance bündelt...**
 - Universal Second Factor (U2F)
 - Universal Authentication Framework (UAF)
 - WebAuthn & CTAP (FIDO2)

Multifaktor-Authentifizierung

FIDO Security Reference



Quelle: FIDO Reference Architecture,
FIDO Alliance Review Draft 25 May 2021



Risikobasierte Authentifizierung

- Vorevaluierung des Risikos eines Authentifizierungsversuchs auf Basis vordefinierter Faktoren
- Ausdruck des Risikos in einem Risikowert
- Anbieten verschiedener Authentifizierungsmethoden auf Basis des Risikowerts
- Steuerung von Step-up Authentication auf Basis des Risikowertes / Zugriffs

Teil 3

Ausblick

1

CONET



Multifaktor-Authentifizierung Trends

- Passwortlose Verfahren per default
- Biometrische Systeme
- Verhaltensbasierte Authentifizierung
- Kontinuierliche Authentifizierung

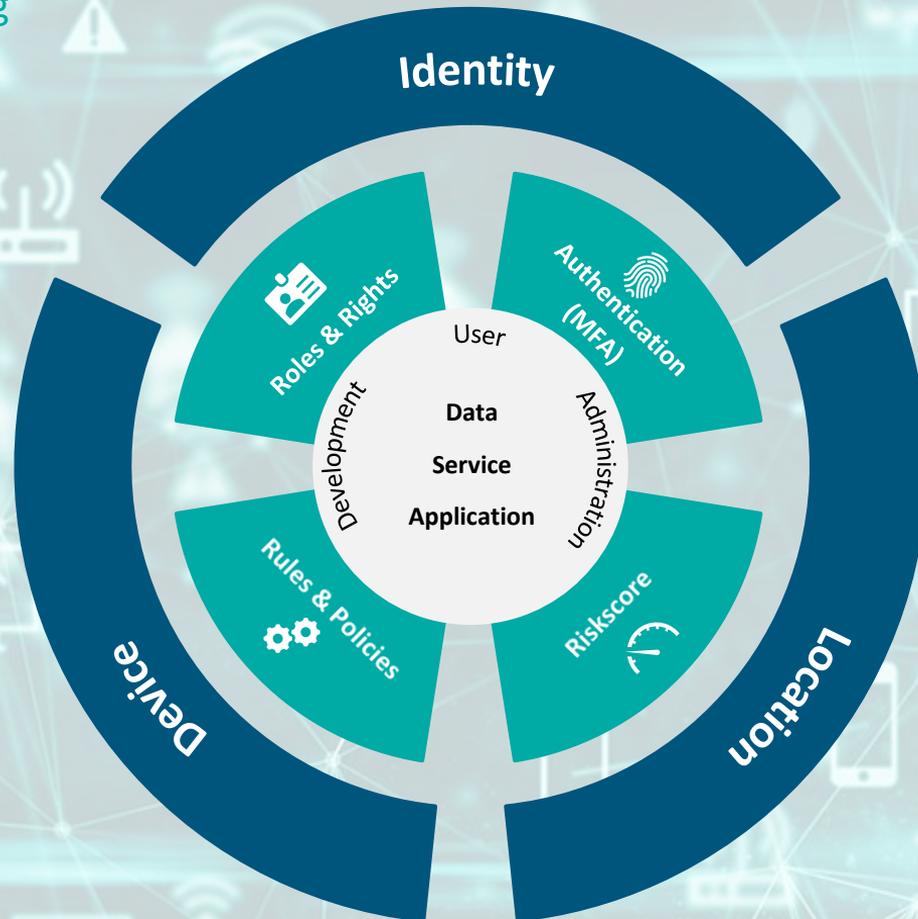


Multifaktor-Authentifizierung

Tipps



- Authentifizierung und Autorisierung trennen
- Authentifizierung ist Teil des Identitätsmanagement
- Authentifizierung kann Teil des Berechtigungsmanagement sein
- Passwörter eliminieren wenn möglich
- SingleSignOn-Optionen prüfen
- Authentifizierung kreativ nutzen



Multifaktor-Authentifizierung

Fazit

- MFA ist Pflicht (nicht Kür)
- Passwortlose-Verfahren sind kein Hype
- Offene Standards helfen und sind praxistauglich
- Authentifizierung ist ein Schlüsselfaktor für die Security Strategie



Vielen Dank für Ihre Aufmerksamkeit!

Noch Fragen?

Multifaktor-Authentifizierung

Nehmen Sie gerne Kontakt mit uns auf!



CONET Solutions GmbH

Jörg Meuser

Managing Consultant

Bundeskanzlerplatz 2

53113 Bonn



www.conet.de



+49 228 9714-219



jmeuser@conet.de



[Aktuelle Stellenangebote](#)

Folgen Sie uns:

