

# BKA OAM Multi-Faktor- Authentifizierung mit Oracle Advanced Authentication (OAA)

---

Konzept und Anwendungsbereiche

Version 1.0

Copyright ©2023, Oracle and/or its affiliates

# Inhaltsverzeichnis

---

<b>Zielbild</b>	<b>3</b>
<b>Multi-Faktor-Authentifizierung</b>	<b>4</b>
<b>MFA-Faktoren</b>	<b>5</b>
<b>OAM &amp; OAA</b>	<b>6</b>
E-Mail mit TOTP	7
SMS mit TOTP	7
Wissensbasierte Authentifizierung (Sicherheitsfragen)	8
Passwortlose Authentifizierung: Push-Benachrichtigung	8
Mobile Authentifizierungs-App mit TOTP	9
YubiKey Token	9
FIDO2	10
<b>MFA-Technologie richtig auswählen</b>	<b>11</b>
Was ist zu betrachten bei Auswahl von MFA-Technologie?	11
Auswahl Matrix	11
<b>Best Practices und Zukunftstrends</b>	<b>16</b>
Do's & Don't's:	16
Passwortlose FIDO2 Trends im öffentlichen Sektor	17
Oracle Security Consulting Team's Empfehlungen:	17
<b>Dokumentation</b>	<b>18</b>
<b>Versionierung</b>	<b>18</b>

---

## Abbildungen

Bild 1: Oracle RADIUS Agent mit einem LDAP-Server und Oracle Advanced Authentication (OAA)	3
Bild 2: High-Level Oracle Advanced Authentication (OAA) Workflow Architektur	3
Bild 3: OAA-Optionsübersicht für den Endanwender	6

---

## Tabellarische Darstellungen

Tabelle 1: MFA-Technologie Vergleichsmatrix	11
Tabelle 2: Referenzen und Produkt Dokumentation	18

## Zielbild

Aktuell sieht sich das BKA als Betreiber des F-IAM vermehrt Rückfragen zum Thema Multi-Faktor-Authentifizierung (MFA) ausgesetzt. Neben der zusätzlichen Absicherung der eigenen administrativen Zugriffe auf das System, wird MFA von angebundenen Anwendungen nachgefragt. Konkret möchte das Verfahren N.SIS die Zugriffe auf das Verfahren sowie den IDM-Selfservice zusätzlich mit einem MFA-Ansatz schützen. Ziel des Dokuments ist es die möglichen Verfahren in dem Oracle Access Management (OAM) mit dem Oracle Advanced Authentication (OAA) Service zu erläutern. Ein wesentlicher Aspekt ist auch die Fragestellung der nachgelagerten Aufwände sowohl auf seitens F-IAM als auch des MFA-Endanwenders.

Zusammenfassend lässt sich sagen, dass die Implementierung von MFA für angebundene Anwendungen eine zusätzliche Sicherheitsebene darstellt, die das Engagement der Organisation für den Schutz sensibler Daten und die Gewährleistung einer sicheren Umgebung für alle Beteiligten durchsetzt. Die Herausforderung für das BKA besteht in diesem Zusammenhang darin, einen Beschluss darüber zu fassen, welche MFA-Technologie für welche Anwendung und für welche Endanwender eingesetzt werden soll. Hintergrund sind die unterschiedlichen Datenverarbeitungen und Aktivitäten in den verschiedenen angebundenen Anwendungen, die eine individuelle Anforderung an das Sicherheitsniveau mit sich bringen. Die MFA-Authentifizierung wird aus exakt diesen Gründen bevorzugt, da sie flexibel anpassbar ist.

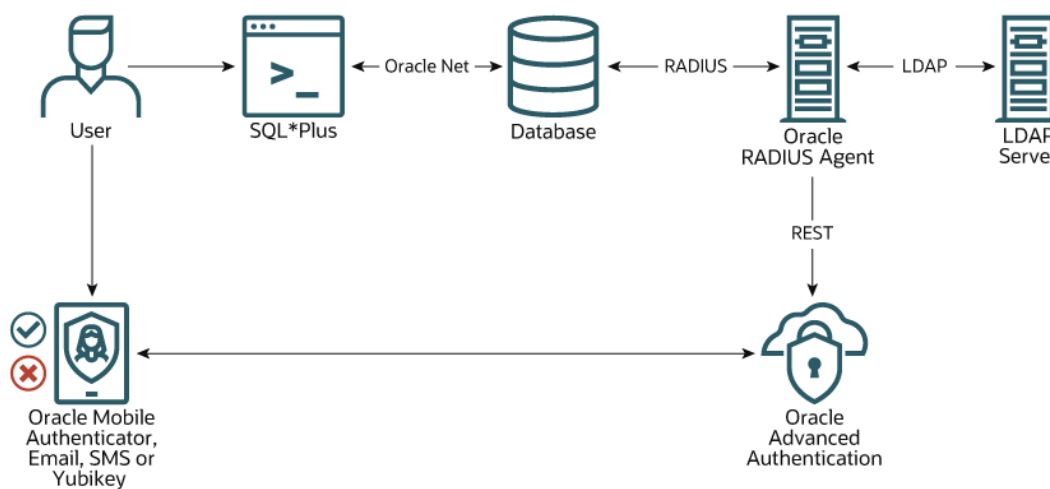


Bild 1: Oracle RADIUS Agent mit einem LDAP-Server und Oracle Advanced Authentication (OAA)

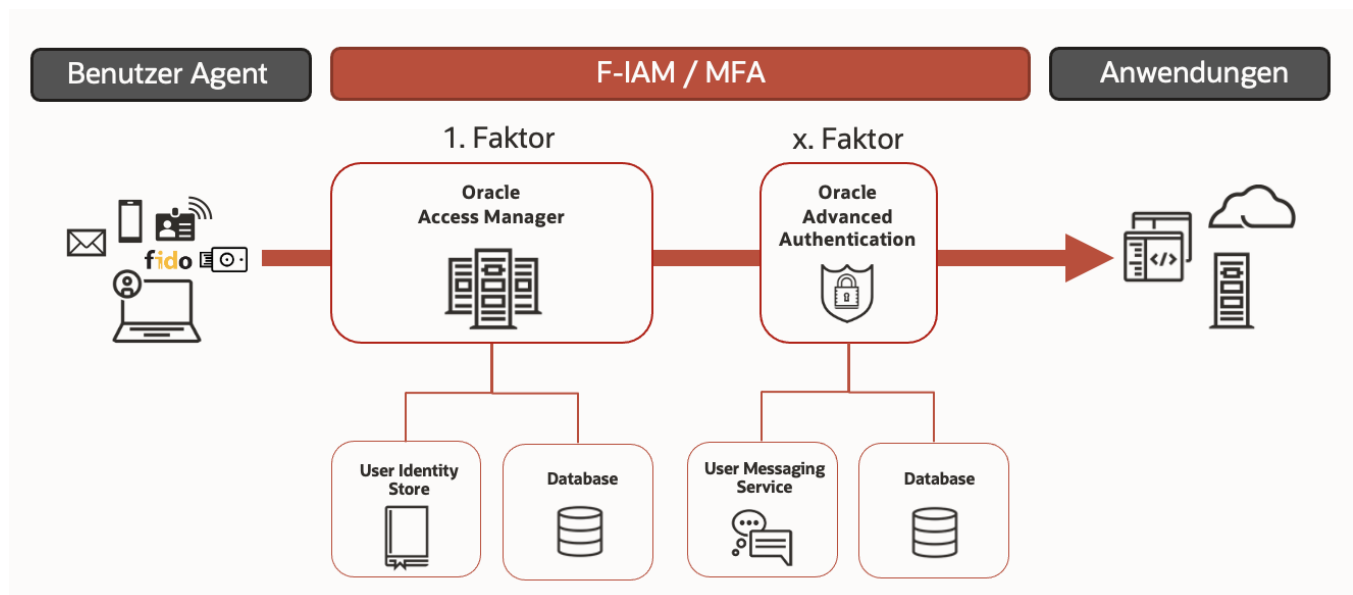


Bild 2: High-Level Oracle Advanced Authentication (OAA) Workflow Architektur

## Multi-Faktor-Authentifizierung

### Warum gibt es MFA?

Die Erfindung der Multi-Faktor-Authentifizierung (MFA) wurde durch die Notwendigkeit stärkerer Sicherheitsmaßnahmen zum Schutz sensibler Informationen und Systeme vor unbefugtem Zugriff vorangetrieben. Die herkömmliche Authentifizierung mit Benutzernamen und Passwort wurde zunehmend unzureichend, da Passwörter leicht erraten oder durch Phishing-Angriffe gestohlen werden konnten. Infolgedessen wurde MFA als Möglichkeit geschaffen, eine zusätzliche Sicherheitsebene zu schaffen, indem sich die Benutzer vor dem Zugriff auf ein System mehrfach identifizieren müssen.

Die Geschichte von MFA lässt sich bis in die späten 1980er Jahre zurückverfolgen, als die ersten Sicherheits-Tokens entwickelt wurden. Diese Tokens generierten einen eindeutigen Code, den die Benutzer zusätzlich zu ihrem Benutzernamen und Passwort eingeben mussten. Dieser zusätzliche Schritt bot eine zusätzliche Sicherheitsebene, da der Code nur einmal verwendet werden konnte und für einen Hacker schwer zu replizieren war. Im Laufe der Zeit wurden weitere Formen der MFA entwickelt, darunter die Authentifizierung per Textnachricht, die biometrische Authentifizierung und die Authentifizierung über mobile Anwendungen.

MFA wurde immer wichtiger, da die Menge an sensiblen Informationen, die von Organisationen gespeichert und verarbeitet werden, zunahm. Da immer mehr Informationen online verfügbar sind, ist auch das Risiko von Datenschutzverletzungen und unbefugtem Zugriff gestiegen, was MFA zu einem wichtigen Instrument zum Schutz sensibler Informationen macht.

In der internationalen Norm für das Informationssicherheitsmanagement, ISO/IEC 27001, die einen umfassenden Rahmen für die Verwaltung und den Schutz sensibler Informationen, einschließlich personenbezogener Daten, geistigen Eigentums und Finanzinformationen, bietet, sind auch Richtlinien für die Implementierung von MFA als Mittel zur Verbesserung der Sicherheit und zum Schutz vor unbefugtem Zugriff enthalten. Insbesondere fordert ISO/IEC 27001 von Organisationen, mehrere Sicherheitsebenen zu implementieren, einschließlich der Verwendung von MFA, um eine starke Verteidigung gegen Sicherheitsbedrohungen zu gewährleisten.

### Wie kann MFA umgesetzt werden?

Die MFA bietet eine zusätzliche Sicherheitsebene für die sensiblen Informationen und Ressourcen einer Organisation. Durch die Forderung nach mehreren Formen der Authentifizierung, z. B. einem Passwort und einem Sicherheits-Token, trägt MFA dazu bei, den unbefugten Zugriff auf Konten zu verhindern und das Risiko von Datenschutzverletzungen zu verringern. Dieser Prozess bietet eine weitere Sicherheitsebene, die über die herkömmliche Authentifizierung mit Benutzernamen und Passwort hinausgeht. Bei der herkömmlichen Authentifizierung kann ein Angreifer auf das System zugreifen, wenn er Zugang zum Kennwort des Benutzers erhält. Bei der MFA muss ein Angreifer jedoch auch Zugriff auf die zweite Form der Identifizierung haben, was den Zugriff auf das System erheblich erschwert.

Organisationen setzen MFA aufgrund der zunehmenden Zahl von Cyber-Angriffen und Datenschutzverletzungen ein. Diese Angriffe können zum Verlust oder Diebstahl von sensiblen Informationen führen, z. B. von Finanzdaten, persönlichen Daten und vertraulichen Geschäftsinformationen. Durch die Implementierung von MFA können Organisationen das Risiko solcher Angriffe verringern und sicherstellen, dass ihre Systeme und Daten geschützt sind.

Es gibt mehrere Optionen für MFA, darunter E-Mail mit einmaligem Time-Based-Passcode (TOTP), SMS mit TOTP, mobile App mit TOTP, Token-basierte, wissensbasierte, passwortlose und FIDO2-Authentifizierung. Jede Methode hat ihre eigenen spezifischen Merkmale, die im vorliegenden Dokument näher erläutert werden.

Die Herausforderung für das Amt besteht darin, sich über die vorgeschlagenen MFA-Optionen zu informieren, jede Option und ihre Merkmale im Detail zu prüfen und eine fundierte Entscheidung über die Wahl der einzuführenden Technologie zu treffen. Ein weiterer wichtiger Punkt ist die Entscheidung, welche Technologie von welchen Nutzern verwendet werden soll, indem Prioritäten gesetzt werden.

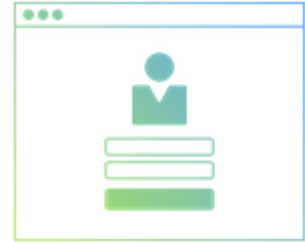
## MFA-Faktoren

Ein Authentifizierungsfaktor ist eine Form von Berechtigungsnachweis, der zur Identitätsprüfung verwendet wird. Jeder Authentifizierungsfaktor bei der MFA fügt dem Authentifizierungsprozess eine weitere Sicherheitsebene hinzu.

### 1FA – Wissensfaktor:

**Die 1-Faktor-Authentifizierung (1FA) ist eine grundlegende Authentifizierungsstufe, bei der nur eine einzige Information zur Überprüfung der Identität eines Benutzers erforderlich ist.** Diese Informationen können ein Passwort, eine Sicherheitsfrage oder eine persönliche Identifikationsnummer (PIN) sein. Die 1FA gilt als die schwächste Form der Authentifizierung, da sie anfällig für Hackerangriffe, das Knacken von Passwörtern und andere Sicherheitsverletzungen ist.

*Beispiel: Anmeldung bei einer Website nur mit einem Nickname und einem Passwort*



### 2FA – Besitzfaktor:

**Die 2-Faktor-Authentifizierung (2FA) ist eine stärkere Authentifizierungsstufe, bei der zwei Informationen zur Überprüfung der Identität eines Benutzers erforderlich sind.** Einer dieser Faktoren ist in der Regel **etwas, das der Benutzer kennt**, z. B. ein Kennwort oder eine PIN, und der andere ist **etwas, das der Benutzer besitzt**, z. B. ein Sicherheits-Token oder ein Mobilgerät. Diese zusätzliche Sicherheitsebene erschwert Unbefugten den Zugang zu vertraulichen Informationen, da sie sowohl das Passwort als auch den zweiten Faktor benötigen, um Zugang zu erhalten. Obwohl die 2FA sicherer ist als die 1FA, kann sie dennoch anfällig für Sicherheitsverletzungen sein, wenn der zweite Faktor verloren geht oder gestohlen wird.

*Beispiel: Bei dem Online-Banking anmelden und einen Code per Textnachricht oder über eine Authentifizierungs-App erhalten und diesen Code eingeben, um auf das Konto zuzugreifen.*



### 3FA – Inhärenzfaktor:

**Die 3-Faktor-Authentifizierung (3FA) ist die stärkste Authentifizierungsstufe und erfordert drei Informationen, um die Identität eines Benutzers zu überprüfen.** Dazu gehören **etwas, das der Benutzer weiß**, **etwas, das der Benutzer hat**, und **etwas, das der Benutzer ist**. Etwas, das der Benutzer weiß, könnte ein Passwort oder eine PIN sein, etwas, das der Benutzer hat, könnte ein Sicherheits-Token oder ein mobiles Gerät sein, und etwas, das der Benutzer ist, könnten biometrische Daten wie ein Fingerabdruck oder eine Gesichtserkennung sein. Diese zusätzliche Sicherheitsebene macht es für Unbefugte noch schwieriger, auf sensible Informationen zuzugreifen. Bei 3FA müsste ein Angreifer sowohl Zugriff auf das Passwort und das physische Gerät haben als auch die biometrischen Daten kennen, um Zugang zu erhalten.

*Beispiel: Verwendung eines Fingerabdrucks oder einer Gesichtserkennung und anschließende Eingabe eines Passworts für den Zugriff auf ein Gerät wie einen Laptop oder ein Telefon.*



Zusammenfassend lässt sich sagen, dass jeder zusätzliche Authentifizierungsfaktor dem Authentifizierungsprozess eine zusätzliche Sicherheitsebene hinzufügt und es Unbefugten erschwert, Zugang zu sensiblen Informationen zu erhalten. Je mehr Faktoren verwendet werden, desto höher ist die Sicherheitsstufe und desto geringer ist das Risiko einer Gefährdung. Zudem ist es sehr wichtig hervorzuheben, dass mit der zunehmenden Anzahl von angewendeten MFA-Faktoren auch der Bedarf an der Verwaltung dieser Technologien sowohl für Organisationen als auch für den Endbenutzer steigt. Künftig wird MFA voraussichtlich zunehmend in den Alltag integriert werden, mit dem Fokus darauf, den Authentifizierungsprozess so nahtlos und benutzerfreundlich wie möglich zu gestalten.

## OAM & OAA

Oracle Advanced Authentication (OAA) ist ein Microservice für Oracle Access Manager (OAM) 12c, der Multi-Faktor-Authentifizierungsfunktionen bietet. Er wurde entwickelt, um die Sicherheit von Online-Anwendungen und -Diensten zu erhöhen, indem Benutzer aufgefordert werden, zusätzliche Formen der Authentifizierung neben dem traditionellen Benutzernamen und Passwort anzugeben.

OAA lässt sich mit OAM integrieren, um eine zentralisierte und skalierbare MFA-Lösung für Organisationen bereitzustellen. Sie unterstützt mehrere MFA-Methoden, darunter von Token oder mobilen Anwendungen generierte Einmalpasswörter (OTP), Sicherheitsfragen und biometrische Authentifizierung. Der OAA-Microservice lässt sich auch mit externen Authentifizierungssystemen wie Smartcards oder biometrischen Lesegeräten integrieren, um eine umfassende MFA-Lösung zu bieten.

OAA bietet eine Reihe von Funktionen, die Organisationen bei der Verwaltung und Sicherung ihrer MFA-Implementierungen unterstützen, darunter:

- **Benutzerverwaltung:** OAA bietet ein zentrales Benutzerverwaltungssystem zur Verwaltung der Benutzer und ihrer MFA-Einstellungen. Dadurch werden die Verwaltung und Sicherung des Zugriffs auf Anwendungen und Dienste erleichtert.
- **Token-Verwaltung:** OAA unterstützt mehrere Token-Typen, einschließlich Hardware- und Software-Token, und bietet ein zentrales Verwaltungssystem für Token und deren Verwendung.
- **Ereignis-Verwaltung:** OAA bietet Ereignisverwaltungsfunktionen zur Protokollierung und Nachverfolgung von MFA-Ereignissen, wie z. B. Benutzerauthentifizierung und Token-Bereitstellung, für Auditing- und Compliance-Zwecke.
- **Anpassbare Authentifizierungsrichtlinien:** OAA bietet eine flexible Richtlinien-Engine, die es Organisationen ermöglicht, benutzerdefinierte Authentifizierungsrichtlinien zu definieren und durchzusetzen, z. B. die Anforderung von MFA für bestimmte Anwendungen oder Dienste.

Die folgende Abbildung zeigt ein Beispiel für einen Endbenutzer, für den alle MFA-Optionen aktiviert sind und der wählen kann, welche er für die Authentifizierung verwenden möchte. Dazu muss lediglich ein Klick darauf erfolgen, und die Anfrage wird gestellt. In den folgenden Unterkapiteln wird jede Option einzeln behandeln und beschreiben.

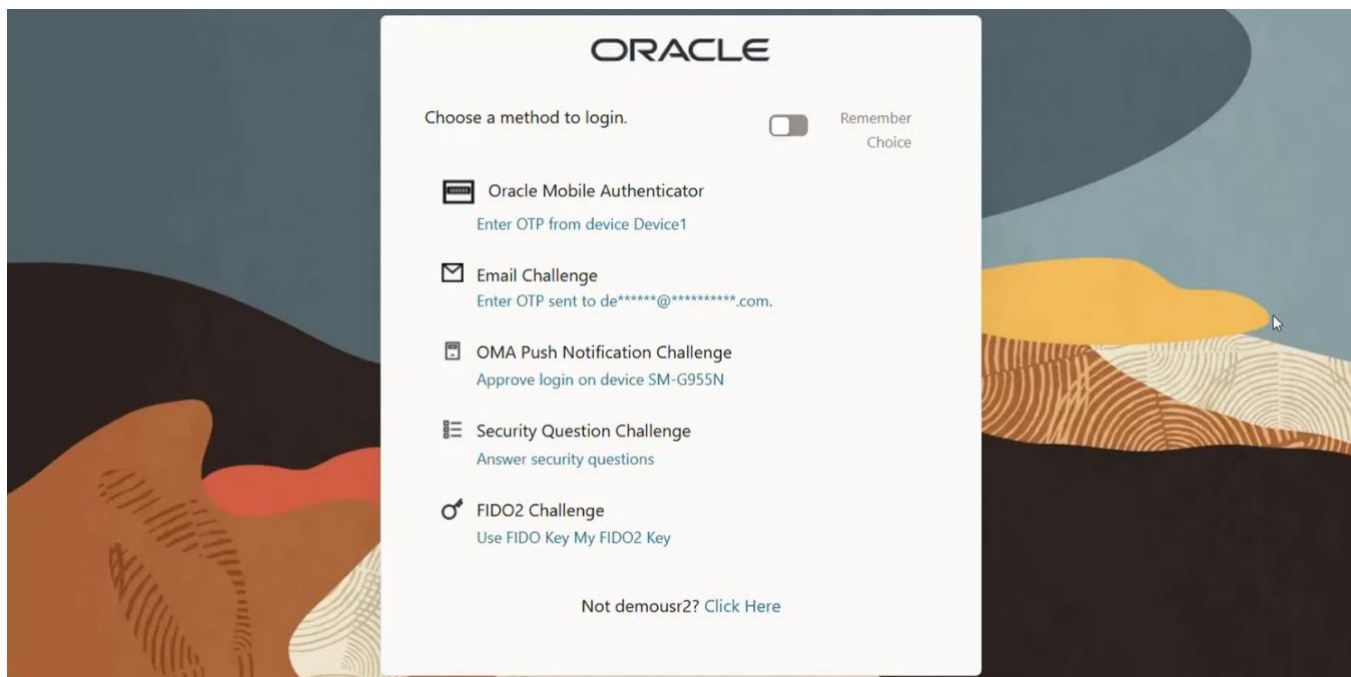


Bild 3: OAA-Optionsübersicht für den Endanwender

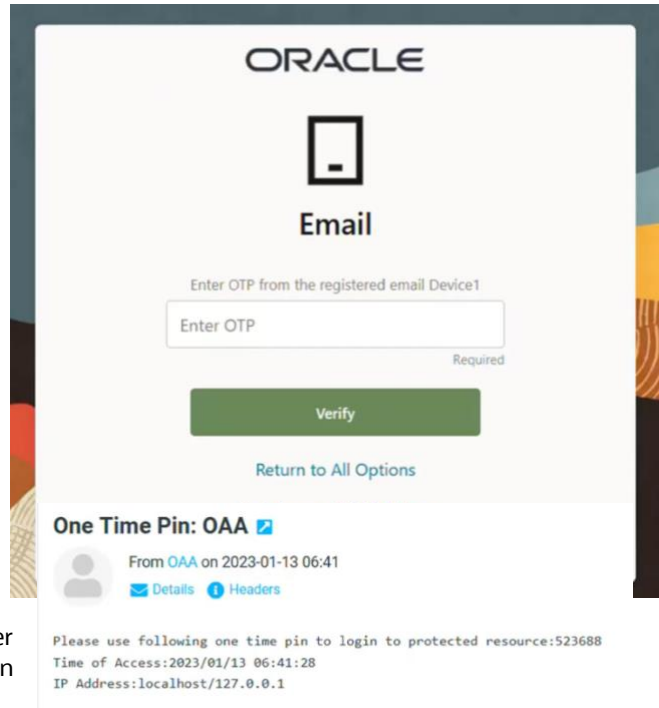
## E-Mail mit TOTP

Diese Option bietet eine zusätzliche Sicherheitsebene zur herkömmlichen Authentifizierung auf der Basis von Benutzernamen und Kennwort, indem sie den Benutzer auffordert, seine Identität nach Erhalt einer E-Mail-Nachricht mit einem TOTP (Time-based-One-Time-Pin) zu bestätigen.

Der E-Mail-TOTP-Dienst funktioniert wie folgt:

- Der Benutzer meldet sich mit seinem Benutzernamen und Kennwort an.
- Das System sendet eine E-Mail-Nachricht an die registrierte E-Mail-Adresse des Benutzers, die ein TOTP enthält.
- Der Benutzer erhält die E-Mail und gibt das Einmalpasswort bei der Anmeldeaufforderung ein.
- Wenn das Einmalpasswort gültig ist und mit dem vom System generierten Passwort übereinstimmt, wird der Benutzer authentifiziert und erhält Zugang zu seinem Konto.

Ein böswilliger Akteur müsste Zugang zum E-Mail-Konto des Benutzers haben, um das Einmalpasswort abzurufen und Zugang zum Benutzerkonto zu erhalten. Es ist wichtig zu beachten, dass die Sicherheit dieser Methode von der Sicherheit des E-Mail-Kontos des Benutzers abhängt. Die Nutzer sollten Maßnahmen ergreifen, um ihr E-Mail-Konto zu schützen und es auf verdächtige Aktivitäten zu überwachen.



## SMS mit TOTP

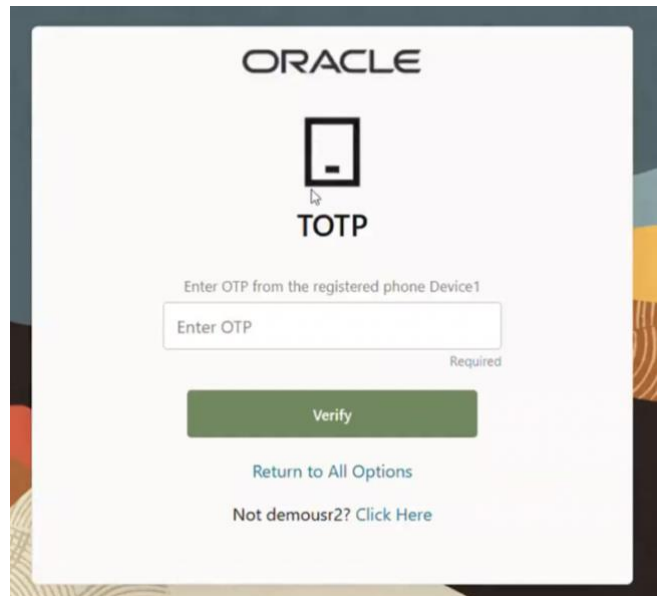
Ähnlich dem E-Mail-basierten TOTP-Verfahren, bietet die SMS TOTP Option eine weitere Sicherungsstufe, indem sie den Benutzer auffordert, seine Identität zu bestätigen, indem er eine Textnachricht mit TOTP auf seiner Handynummer erhält.

Der SMS-TOTP-Dienst funktioniert wie folgt:

- Der Benutzer meldet sich mit seinem Benutzernamen und Passwort an.
- Das System sendet eine Textnachricht an die registrierte Mobiltelefonnummer des Benutzers, die ein TOTP enthält.
- Der Benutzer erhält die Textnachricht und gibt das Einmalpasswort bei der Anmeldeaufforderung ein.
- Wenn das Einmalpasswort gültig ist und mit dem vom System generierten Passwort übereinstimmt, wird der Benutzer authentifiziert und erhält Zugang zu seinem Konto.

Um das Einmalpasswort abzurufen und Zugang zum Benutzerkonto zu erhalten, muss ein Angreifer Zugriff auf das Mobiltelefon des Benutzers haben.

Es ist wichtig zu beachten, dass die Sicherheit dieser Methode anfällig für Abfangen und Manipulation sein kann. Benutzer sollten eine sicherere Form der MFA in Betracht ziehen, wie z. B. eine Push-Benachrichtigung oder Token TOTP, falls verfügbar.





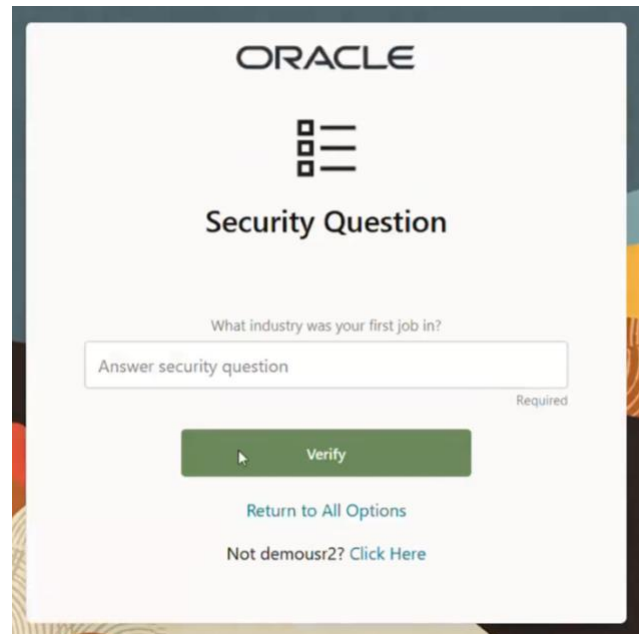
## Wissensbasierte Authentifizierung (Sicherheitsfragen)

Bei dieser Option müssen Benutzer zusätzlich zu ihrem Benutzernamen und Kennwort Antworten auf eine Reihe vordefinierter Sicherheitsfragen geben, um ihre Identität zu überprüfen.

Die Sicherheitsfragen-MFA-Option funktioniert wie folgt:

- Der Benutzer meldet sich mit seinem Benutzernamen und Kennwort an.
- Das System präsentiert dem Benutzer eine Reihe von Sicherheitsfragen, die er richtig beantworten muss.
- Die vom Benutzer gegebenen Antworten werden mit den im System gespeicherten Antworten verglichen.
- Wenn die Antworten übereinstimmen, wird der Benutzer authentifiziert und erhält Zugang zu seinem Konto.

Diese Option bietet eine zusätzliche Sicherheitsebene zur herkömmlichen Authentifizierung mit Benutzernamen und Kennwort und hilft, unbefugten Zugriff auf Benutzerkonten zu verhindern. Es ist jedoch zu beachten, dass die Sicherheit dieser Methode von der Sicherheit der vom Benutzer gegebenen Antworten abhängt, weshalb die Benutzer Antworten wählen sollten, die für andere schwer zu erraten oder zu entdecken sind.

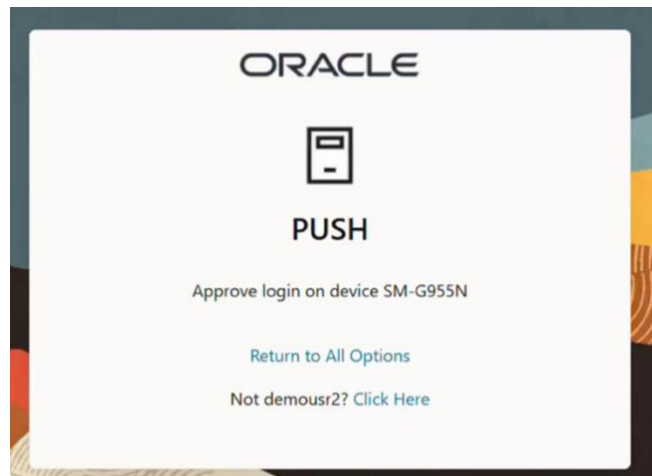


## Passwortlose Authentifizierung: Push-Benachrichtigung

Diese Option bietet eine sicherere und bequemere Methode zur Überprüfung der Identität eines Benutzers im Vergleich zu herkömmlichen Methoden wie Sicherheitsfragen oder SMS-basierten Einmalpasswörtern.

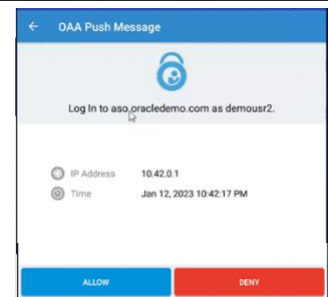
Die MFA-Option mit Push-Benachrichtigung funktioniert wie folgt:

- Der Benutzer meldet sich mit seinem Benutzernamen und Passwort an.
- Das System sendet eine Push-Benachrichtigung an das registrierte Mobilgerät des Benutzers oder ein anderes zugelassenes Gerät.
- Der Benutzer erhält die Push-Benachrichtigung und muss die Anmeldeanfrage genehmigen oder ablehnen.
- Wenn der Benutzer die Anfrage genehmigt, authentifiziert das System den Benutzer und gewährt ihm Zugang zu seinem Konto.



Diese Option bietet eine zusätzliche Sicherheitsebene, da der Benutzer sein Gerät bei sich haben muss, um die Anmeldeanforderung zu genehmigen. Auf diese Weise wird der unbefugte Zugriff auf Benutzerkonten verhindert, selbst wenn ein böswilliger Akteur den Benutzernamen und das Kennwort des Benutzers erlangt hat.

Die Option der Push-Benachrichtigung ist in der Regel schneller und bequemer als andere MFA-Methoden, da keine zusätzlichen Codes eingegeben oder Sicherheitsfragen beantwortet werden müssen. Außerdem bietet sie eine sicherere Authentifizierungsmethode im Vergleich zu SMS-basierten Einmalpasswörtern, die anfällig für Abfangen und Manipulation sein können.





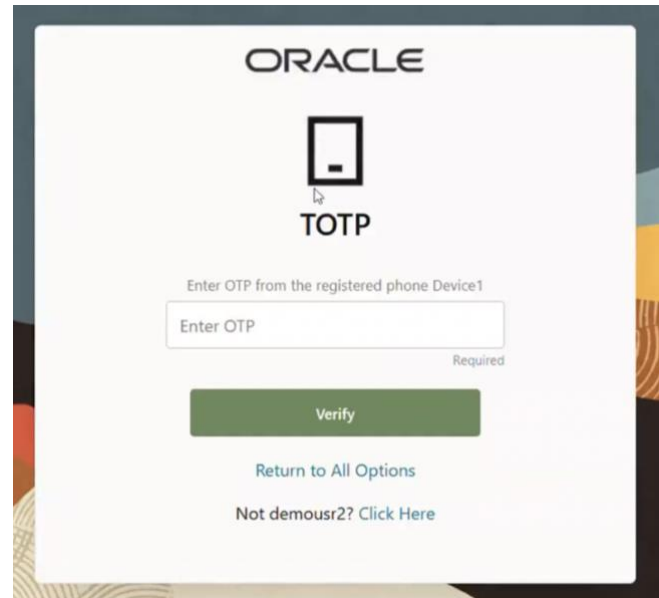
## Mobile Authentifizierungs-App mit TOTP

Das mobile Authentifizierungs-App Verfahren basiert auf zeitlich begrenzten TOTP's, indem es den Nutzer auffordert, seine Identität über sein Mobilgerät zu verifizieren.

Die Mobile App MFA-Option funktioniert wie folgt:

- Der Benutzer meldet sich mit seinem Benutzernamen und Passwort an.
- Das TOTP wird von der App generiert, und ist zwischen 30-60 Sekunden lang gültig.
- Sobald der Benutzer das OTP eingegeben hat, wird es verifiziert und das System gewährt ihm Zugriff auf sein Konto.

Der zusätzliche Schutz ergibt sich daraus, dass der Nutzer sein Gerät bei sich haben muss, um den Code zu empfangen und einzugeben. Deshalb muss das Gerät, auf dem die App installiert wird, registriert werden, da sowohl Authenticator als auch der Server einen eindeutigen Schlüssel teilen. Dies verhindert den unbefugten Zugriff auf Benutzerkonten, selbst wenn ein böswilliger Akteur den Benutzernamen und das Kennwort des Benutzers erhalten hat.

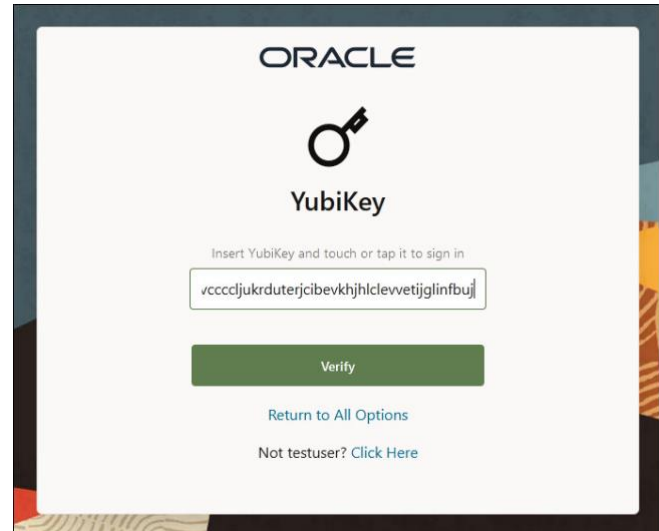


## YubiKey Token

Die Option YubiKey Token TOTP bietet eine zusätzliche Sicherheitsebene zur herkömmlichen Authentifizierung auf der Basis von Benutzernamen und Kennwort, indem sie den Benutzer auffordert, einen eindeutigen, einmaligen Code einzugeben, der von einem physischen Token generiert wird. YubiKey ist ein Sicherheits-Token der Firma [Yubico](https://www.yubico.com/).

Die YubiKey-Token-TOTP-MFA-Option funktioniert wie folgt:

- Der Benutzer meldet sich mit seinem Benutzernamen und Passwort an.
- Der Benutzer wird zum YubiKey-Bildschirm weitergeleitet, klickt in das Feld TOTP und berührt den YubiKey an seinem USB-Anschluss (lange Berührung).
- Der TOTP wird angezeigt Der Benutzer gibt das Einmalpasswort bei der Anmeldeaufforderung ein.
- Wenn das Einmalpasswort gültig ist und mit dem vom System generierten Passwort übereinstimmt, wird der Benutzer authentifiziert und erhält Zugang zu seinem Konto.



Diese Option bietet eine zusätzliche Sicherheitsebene, denn selbst wenn ein böswilliger Akteur den Benutzernamen und das Kennwort des Benutzers in Erfahrung gebracht hat, müsste er immer noch physischen Zugriff auf den Token des Benutzers haben, um das Einmalpasswort zu generieren und Zugriff auf das Benutzerkonto zu erhalten.

## FIDO2

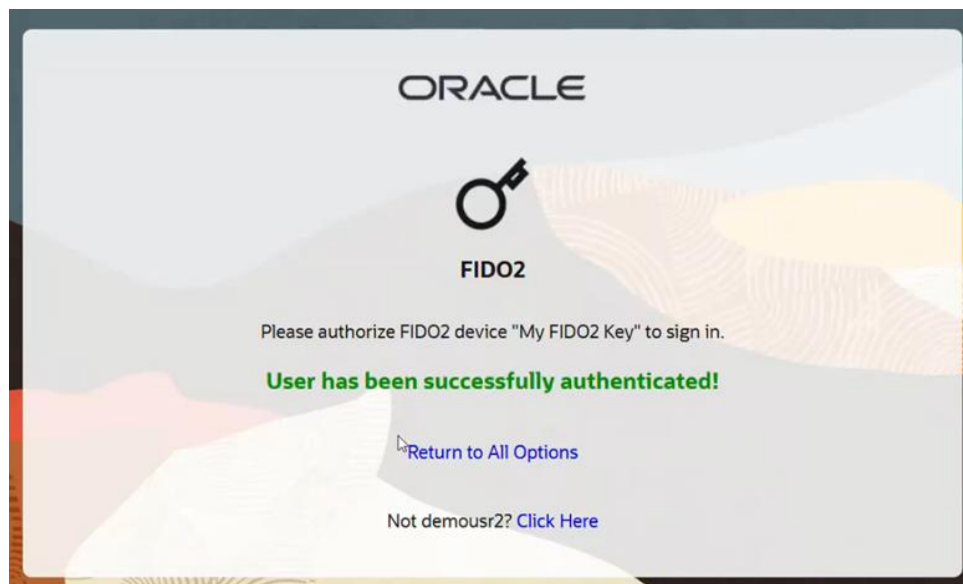
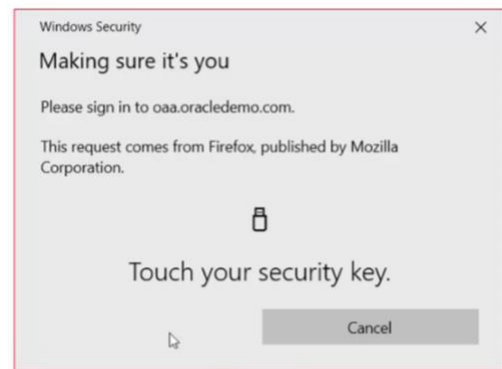
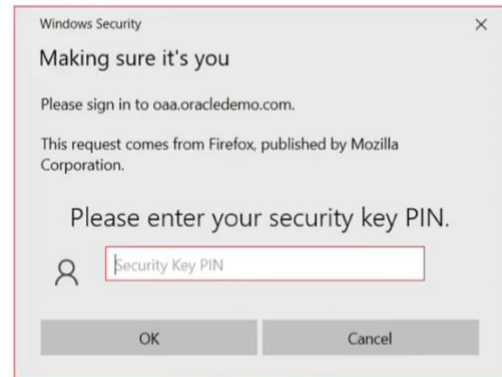
FIDO2 (Fast IDentity Online) ist eine Reihe offener, skalierbarer und interoperabler Spezifikationen für die sichere Authentifizierung, die Passwörter überflüssig machen. Die FIDO2-Authentifizierung verwendet eine Kombination aus Hardware und Software, um Benutzerdaten sicher zu speichern und eindeutige Authentifizierungssignale zu erzeugen, wie z. B. biometrische Daten oder kryptografische Schlüssel. Dies bietet eine sichere und private Authentifizierungsmethode, die gegen Hackerangriffe, Phishing und andere Arten von Cyberattacken resistent ist. FIDO2 wird von einer breiten Palette von Geräten und Plattformen unterstützt und wird bereits von vielen führenden Unternehmen und Organisationen weltweit eingesetzt.

Die FIDO2-Option funktioniert wie folgt:

- Der Benutzer meldet sich mit seinem Benutzernamen und Passwort an.
- Der Benutzer gibt die von ihm vordefinierte Sicherheits-PIN für den FIDO2-Sicherheitsschlüssel ein.
- Der Benutzer steckt seinen FIDO2-Sicherheitsschlüssel in sein Gerät oder berührt den Schlüssel, wenn es sich um einen berührungsbasierten Schlüssel handelt.
- Der Schlüssel sendet eine kryptografische Signatur an das System, um die Identität des Benutzers zu bestätigen.
- Wenn die Signatur gültig ist und mit dem Schlüssel übereinstimmt, der im Konto des Nutzers registriert ist, wird der Nutzer authentifiziert und erhält Zugang zu seinem Konto.

Diese Option bietet eine hochsichere Form der MFA, da die Identität des Benutzers über ein sicheres Gerät überprüft wird, das von seinem Computer oder mobilen Gerät getrennt ist. Sie macht Einmalpasswörter oder Sicherheitsfragen überflüssig und **gilt als eine der sichersten derzeit verfügbaren Formen der MFA.**

Es ist wichtig zu beachten, dass die FIDO2-Option einen FIDO2-kompatiblen Sicherheitsschlüssel erfordert, der möglicherweise nicht für alle Benutzer erworben werden kann. **Für Benutzer, die Zugang zu dieser Technologie haben, bietet die FIDO2-Option jedoch eine äußerst sichere und bequeme Methode der MFA.**



# MFA-Technologie richtig auswählen

## Was ist zu betrachten bei Auswahl von MFA-Technologie?

Bei der Auswahl einer MFA-Technologie sollten die folgenden Faktoren berücksichtigt werden:

- **Benutzerfreundlichkeit:** Die Technologie sollte einfach zu bedienen sein und den Benutzer nicht mit übermäßigen Schritten zur Authentifizierung belasten.
- **Sicherheit:** Die Technologie sollte ein hohes Maß an Sicherheit bieten und vor Phishing und anderen Formen von Cyber-Kriminellen und anderen böswilligen Akteuren standzuhalten und zu widerstehen.
- **Kosten:** Berücksichtigen Sie die Kosten für die Technologie und alle laufenden Wartungskosten.
- **Standort der Benutzer:** Die Technologie sollte für alle Benutzer zugänglich sein, unabhängig von ihrem Standort.
- **Geräteunabhängigkeit:** Berücksichtigen Sie die Rolle der Hardware in jeder Technologie und das Ausmaß, in dem eine MFA von der Hardware abhängt. Je mehr eine Technologie von Hardware abhängt, desto mehr müssen Sicherheitskonzepte vorbereitet werden, um Probleme im Zusammenhang mit verlorenen oder beschädigten Geräten zu verwalten und zu lösen.
- **Zeitaufwand für die Implementierung:** Der Zeitaufwand für die Implementierung und Bereitstellung der MFA-Technologie in einer Organisation, einschließlich der erforderlichen Schulungen und des Supports für die Benutzer.

Auf der Grundlage dieser Faktoren sollte eine fundierte Entscheidung getroffen werden, welche MFA-Technologie verwendet wird.

**Wichtig:** Bei allen MFA-Verfahren sollte das Amt oder die entsprechende Behörde die MFA für den Endnutzer einrichten. Die Selbstbedienung durch den Endnutzer bei der Einrichtung und Konfiguration von MFA-Faktoren wird bei der Größe des Projekts nicht empfohlen, da sie schwer zu kontrollieren und zu überwachen ist, was einen zusätzlichen Aufwand für das Amt und die entsprechende Behörde bedeutet.

*Beispiel: Die Einrichtung von MFA-Verfahren für den Enduser und die Eingabe der dafür benötigten Informationen wie E-Mail-Adresse oder die Registrierung des verwendeten Mobilgeräts.*

## Auswahl Matrix

Die in Tabelle 1. dargestellte Vergleichsmatrix enthält alle zu erwähnten Faktoren und bewertet sie für jede MFA-Technologie. Eine detaillierte Aufschlüsselung der Bewertung folgt in den folgenden Unterabschnitten. Der Zweck dieser Vergleichsmatrix besteht darin, den Organisationen eine allgemeine Übersicht darüber zu geben, welche Faktoren bei welcher Technologie am vorteilhaftesten sind. **Es ist empfehlenswert, die Faktoren nach ihrer Wichtigkeit zu priorisieren und nicht in ihrer Gesamtheit zu betrachten, da verschiedene Faktoren für unterschiedliche Anwendungsszenarien eine andere Bedeutung haben.**

Tabelle 1: MFA-Technologie Vergleichsmatrix

Funktion	E-Mail	SMS	Wissens-basiert	Passwort-los	Mobile Auth App	Yubikey Token	FIDO2 Token
Benutzerfreundlichkeit	gering	medium	hoch	hoch	hoch	medium	medium
Sicherheit	gering	gering	gering	mittelhoch	hoch	hoch	hoch
Kosten	gering	gering	gering	gering-medium	medium	hoch	hoch
Benutzerstandort	hoch	hoch	hoch	hoch	hoch	hoch	medium
Geräteunabhängigkeit	hoch	medium	hoch	gering	gering	gering	gering
Zeitaufwand für die Implementierung	gering	gering	gering	gering-medium	medium	medium-lang	medium

## E-Mail MFA Aufschlüsselung

- **Benutzerfreundlichkeit:** E-Mail-MFA wird als **wenig benutzerfreundlich** angesehen, da die Benutzer auf ihren E-Mail-Client zugreifen müssen, um den Code abzurufen und ihn manuell einzugeben.
- **Sicherheit:** Das Sicherheitsniveau von E-Mail-MFA wird als **niedrig** eingestuft, da E-Mails leicht gehackt oder umgeleitet werden können, was sie anfällig für Phishing-Angriffe macht.
- **Kosten:** Die Kosten für E-Mail-MFA sind **gering**, da keine zusätzliche Hardware oder Software erforderlich ist.
- **Benutzerstandort:** Der Benutzerstandort für E-Mail-MFA ist **hoch**, da die Benutzer von jedem Ort mit einer Internetverbindung auf ihre E-Mails zugreifen können.
- **Geräteunabhängigkeit:** E-Mail-basierte MFA beruht auf dem Zugriff auf ein E-Mail-Konto, das bei Verlust oder Beschädigung eines Geräts gefährdet ist. Die Geräteunabhängigkeit ist **hoch**, da eine Anmeldung über verschiedene Geräte erfolgen kann.
- **Zeit für die Implementierung:** Der Zeitaufwand für die Implementierung von E-Mail-MFA ist **gering**, da lediglich ein E-Mail-basierter Authentifizierungsprozess implementiert werden muss.

### Voraussetzungen für die erfolgreiche Implementierung:

- Das Amt sollte einen E-Mail-Server bereitstellen.
- Das Amt oder die Behörde sollte eine gültige und gemappte E-Mail-Adresse für den Endbenutzer bereitstellen.
- Der Endbenutzer sollte in der Lage sein, E-Mail-Nachrichten zu empfangen.

**Zusammengefasst:** E-Mail-basierte MFA ist bequem und kostengünstig für Organisationen, die den Zugang zu E-Mail-Konten und anderen Online-Diensten sichern müssen. Der Hauptvorteil von MFA per E-Mail sind die geringe Umsetzungskosten und schnelle Integration. Die Sicherheit der E-Mail-basierten MFA ist jedoch relativ gering, da E-Mail-Konten anfällig für Hacker- und Phishing-Angriffe sind.

## SMS MFA Aufschlüsselung

- **Benutzerfreundlichkeit:** SMS MFA hat einen **mittleren Grad** an Benutzerfreundlichkeit, da die Benutzer auf ihr Mobiltelefon zugreifen müssen, um den Code abzurufen und ihn manuell einzugeben.
- **Sicherheit:** Das Sicherheitsniveau von SMS MFA ist **niedrig**, da Telefonnummern leicht entwendet werden können, was es anfällig für SIM-Swapping-Angriffe macht.
- **Kosten:** Die Kosten für SMS MFA sind **gering**, da keine zusätzliche Hardware oder Software erforderlich ist.
- **Benutzerstandort:** Der Benutzerstandort für SMS MFA ist **hoch**, da die Benutzer von überall aus, wo eine Mobilfunkverbindung besteht, auf ihr Mobiltelefon zugreifen können.
- **Geräteunabhängigkeit:** SMS-basierte MFA setzt den Zugang zu einem Mobiltelefon mit einer bestimmten Telefonnummer voraus, das bei Verlust oder Beschädigung des Geräts gefährdet ist. Die Geräteunabhängigkeit ist **medium**, da die Gefahr besteht, dass die Telefonnummer entwendet wird oder die SIM-Karte verloren wird.
- **Zeit für die Implementierung:** Der Zeitaufwand für die Implementierung von SMS MFA ist **gering**, da nur die Implementierung eines SMS-basierten Authentifizierungsprozesses erforderlich ist.

### Voraussetzungen für die erfolgreiche Implementierung:

- Das Amt sollte ein SMS-Gateway bereitstellen.
- Das Amt oder die Behörde sollte eine gültige und gemappte Mobilfunknummer für den Endanwender bereitstellen, die von einem angemeldeten Empfang-fähigen Gerät aktiv verwendet werden kann.
- Der Endbenutzer sollte in der Lage sein, eine SMS-Nachricht zu empfangen.

**Zusammengefasst:** SMS-basierte MFA ist eine weitere kostengünstige Möglichkeit, den Zugang zu Online-Diensten zu sichern, da sie nur eine Mobiltelefonnummer erfordert. Der Hauptvorteil von SMS-MFA ist ihre weite Verbreitung, da die meisten Menschen ein Mobiltelefon besitzen. Allerdings ist SMS-MFA nicht sehr sicher, da Handynummern anfällig für Hijacking sind und SMS-Nachrichten abgefangen oder umgeleitet werden können.

## Wissensbasierte Authentifizierung Aufschlüsselung

- **Benutzerfreundlichkeit:** Wissensbasierte Authentifizierung ist **sehr (hoch)** benutzerfreundlich, da die Benutzer lediglich eine Reihe von vordefinierten Sicherheitsfragen beantworten müssen, um sich zu authentifizieren.
- **Sicherheit:** Diese Methode ist **wenig sicher**, da die Antworten auf die Sicherheitsfragen leicht erraten oder durch Social Engineering-Techniken erlangt werden können. Außerdem beziehen sich die Sicherheitsfragen oft auf öffentlich zugängliche Informationen, was es Angreifern erleichtert, diese Authentifizierungsmethode zu umgehen.
- **Kosten:** Die Kosten sind **niedrig**, da es sich um eine einfache Methode handelt, die keine spezielle Hardware oder zusätzliche Software erfordert und somit eine kostengünstige Option darstellt.
- **Benutzerstandort:** Benutzerstandort wird als **hoch** eingestuft, da die Option von überall aus verwendet werden kann, solange der Benutzer Zugang zu einem Gerät hat, das auf das Authentifizierungssystem zugreifen kann.
- **Geräteunabhängigkeit:** Diese Authentifizierungsmethode benötigt kein Gerät zur Authentifizierung - **hohe** Geräteunabhängigkeit.
- **Zeit für die Implementierung:** Wissensbasierte Authentifizierung wird schnell und einfach in bestehende Systeme integriert und ist somit eine schnelle Option für Organisationen – Zeit für die Implementierung ist **gering**.

### Voraussetzungen für die erfolgreiche Implementierung:

- Das Amt oder die Behörde sollte eine Reihe von Fragen definieren und Regeln festlegen, wie die wissensbasierte Authentifizierung durchgeführt werden soll. Zum Beispiel: Anzahl der gestellten Fragen, zulässige Länge der Antworten, keine Wiederholung von Antworten, usw. ...
- Der Benutzer sollte eine vordefinierte Anzahl von Fragen von dem Fragenkatalog auswählen und beantworten, damit diese zu seinem Account gemappt werden.
- Der Benutzer sollte in der Lage sein, die von ihm ausgewählten Sicherheitsfragen zu beantworten.  
**Wichtig:** Bei wiederholter fehlerhafter Eingabe von Antworten oder bei Vergesslichkeit ist eine erneute Registrierung erforderlich. An diesem Prozess sind sowohl die Behörde als auch der Endnutzer beteiligt.

**Zusammengefasst:** Die Option ist einfach zu handhabende und kostengünstig. Vorteilhaft ist, dass für die Authentifizierung kein physisches Gerät benötigt wird, so dass keine Geräteverwaltung erforderlich ist. Ihr schlechtestes Merkmal ist die geringe Sicherheit, da die Antworten auf die Sicherheitsfragen leicht erraten oder durch Social-Engineering-Techniken erlangt werden können. Außerdem beziehen sich die Sicherheitsfragen oft auf öffentlich zugängliche Informationen, so dass es für Angreifer einfacher ist, diese MFA zu umgehen. Organisationen, die sich für diese Methode entscheiden, müssen sich ihrer Grenzen bewusst sein und sollten andere Optionen wie die FIDO2-Option in Betracht ziehen, wenn sie ein höheres Maß an Sicherheit benötigen.

## Passwortlose Authentifizierung (Push-Benachrichtigungen) Aufschlüsselung

- **Benutzerfreundlichkeit:** Push-Benachrichtigungen sind **sehr benutzerfreundlich**, da sie keine zusätzlichen Schritte zur Authentifizierung des Benutzers erfordern, abgesehen von der Annahme der Push-Benachrichtigung auf seinem mobilen Gerät.
- **Sicherheit:** Push-Benachrichtigungen sind möglicherweise nicht so sicher, wie andere MFA-Optionen wie FIDO2 und anfällig für die Kompromittierung von Mobilgeräten und Konten, wodurch ihre Sicherheit **mittel bis hoch ist**.
- **Kosten:** Die Kosten für die Implementierung sind **gering bis mittel**, da sie in der Regel einmalige Kosten für die Entwicklung und Bereitstellung der erforderlichen Software und Infrastruktur erfordern.
- **Standort des Benutzers:** Push-Benachrichtigungen sind **höchst zugänglich**, da sie überall mit einer Internetverbindung und einem mobilen Gerät empfangen werden können.
- **Geräteunabhängigkeit:** Obwohl Push-Benachrichtigungen auf einer Vielzahl von Geräten, einschließlich Smartphones und Tablets, verwendet werden können, ist die Methode **sehr von dem ausgewählten Gerät abhängig** und kann bei Verlust/Beschädigung des Geräts nicht erneut durchgeführt werden.
- **Zeitbedarf für die Implementierung:** Die Implementierung erfordert in der Regel einen **geringen bis mittleren Zeitaufwand**, abhängig von der Komplexität der bestehenden Systeme und Infrastruktur der Organisation.



## Voraussetzungen für die erfolgreiche Implementierung:

- Das Amt oder die Behörde sollte das Pairing zwischen dem Endgerät und dem Server (Key-Tausch) für den Benutzer abwickeln.
- Das Amt sollte entscheiden, welche mobilen Endgeräten verwendet werden dürfen. Abhängig davon sollte ein Container auf das Gerät installiert werden, um auf das Amt-Netzwerk zugreifen zu können. Möglicherweise kann auch eine BYOD-Strategie in Betracht gezogen werden.
- Der Endanwender sollte über ein mobiles Endgerät mit mobilen Daten verfügen, das angemeldet ist
- Die Behörde sollte eine Anleitung zu Geräteanmeldung bereitstellen.
- Der Endbenutzer sollte die Mobile Auth App auf dem ausgewählten Gerät selbst installieren, die Geräteanmeldung durchführen und in der Lage sein, MFA-Anfragen auf dem Gerät zu genehmigen oder abzulehnen.

**Unterstützte Apps:** Oracle Mobile Authenticator (OMA), Google, and Microsoft

**Wichtig:** Pro Benutzer kann nur 1 Gerät angemeldet werden. Mehrfache Geräteanmeldungen sind nicht zulässig

**Zusammengefasst:** Hauptmerkmale sind die Benutzerfreundlichkeit, die erhöhte Sicherheit und das verringerte Risiko passwortbezogener Sicherheitsbedrohungen wie die Wiederverwendung und das Knacken von Passwörtern. Bei diesem Verfahren müssen jedoch die Implementierungskosten und die Benutzerakzeptanz berücksichtigt werden.

## App MFA Aufschlüsselung

- **Benutzerfreundlichkeit:** App MFA bietet einen **hohen Grad an Benutzerfreundlichkeit**, da die Benutzer einfach eine Authentifizierungs-App auf ihren mobilen Geräten installieren und damit einen Code generieren können.
- **Sicherheit:** Das Sicherheitsniveau von App MFA **ist hoch**, da es eine spezielle Authentifizierungs-App verwendet, die für jede Authentifizierungssitzung einen eindeutigen Code generiert.
- **Kosten:** Die Kosten für App MFA sind **mittelhoch**, da sie den Kauf einer speziellen Authentifizierungs-App oder eine Lizenz für ihre Verwendung erfordern kann.
- **Standort des Benutzers:** Der Benutzerstandort für App MFA ist **hoch**, da die Benutzer von überall aus, wo eine mobile Netzwerkverbindung besteht, auf ihre mobilen Geräte zugreifen können.
- **Geräteunabhängigkeit:** Mobile App MFA erfordert ein Gerät mit einer installierten mobilen App, das anfällig für Verlust oder Beschädigung ist. Da die Mobile App MFA Anmeldung nur auf einem Gerät erlaubt ist, ist die Technologie **stark vom Gerät abhängig** und kann bei Verlust/Beschädigung des Geräts nicht erneut ausgeführt werden.
- **Zeit für die Implementierung:** Der Zeitaufwand für die Implementierung von App MFA ist **mittel**, da für jeden Benutzer eine eigene Authentifizierungs-App installiert werden muss.

## Voraussetzungen für die erfolgreiche Implementierung:

- Das Amt oder die Behörde sollte das Pairing zwischen dem Endgerät und dem Server (Key-Tausch) für den Benutzer abwickeln.
- Das Amt oder die Behörde sollte entscheiden, welche mobilen Endgeräten verwendet werden dürfen. Abhängig davon sollte ein Container auf das Gerät installiert werden, um auf das Amt-Netzwerk zugreifen zu können. Möglicherweise kann auch eine BYOD-Strategie in Betracht gezogen werden.
- Der Endanwender sollte über ein mobiles Endgerät mit mobilen Daten verfügen, das angemeldet ist
- Das Amt oder die Behörde sollte eine Anleitung zu Geräteanmeldung bereitstellen.
- Der Endbenutzer sollte die Mobile Auth App auf dem ausgewählten Endgerät selbst installieren und die Geräteanmeldung durchführen.

**Unterstützte Apps:** Oracle Mobile Authenticator (OMA), Google, and Microsoft

**Wichtig:** Pro Benutzer kann nur 1 Gerät angemeldet werden. Mehrfache Geräteanmeldungen sind nicht zulässig

- Der Endbenutzer sollte in der Lage sein, das TOTP in der App zu empfangen.

**Zusammengefasst:** Mobile App MFA ist eine sicherere Option im Vergleich zu E-Mail- oder SMS-basierter MFA, da sie eine sichere App verwendet, um TOTPs auf dem Gerät des Nutzers zu generieren. Der Hauptvorteil ist die erhöhte Sicherheit sowie die einfache Nutzung, da die App auf den meisten Smartphones und anderen mobilen Geräten installiert werden kann. Allerdings ist dafür ein Gerät erforderlich, auf dem die App installiert wird, und wenn das Gerät verloren geht oder beschädigt wird, kann der Nutzer möglicherweise nicht auf die TOTPs zugreifen.



## Yubikey Token MFA Aufschlüsselung

- **Benutzerfreundlichkeit:** Token-MFA bietet ein **mittleres Maß** an Benutzerfreundlichkeit, da die Benutzer physisch auf das Token zugreifen müssen, um den Code abzurufen und ihn manuell einzugeben.
- **Sicherheit:** Das Sicherheitsniveau von Token MFA ist **hoch**, da der physische Token für jede Authentifizierungssitzung einen eindeutigen Code generiert, was es für Angreifer schwierig macht, Codes vorherzusagen oder wiederzuverwenden.
- **Kosten:** Die Kosten für Token MFA sind **hoch**, da für jeden Benutzer ein physisches Token gekauft werden muss.
- **Standort des Benutzers:** Der Benutzerstandort für Token MFA ist **mittelmäßig**, da die Benutzer physisch auf den Token zugreifen müssen, um den Code abzurufen.
- **Geräteunabhängigkeit:** Obwohl die Hardware-Token basierenden MFA ein physisches Token verwendet, das im Vergleich zu einer gerätebasierten Lösung weniger wahrscheinlich verloren geht oder beschädigt wird, ist die Technologie **stark vom Token abhängig**. Einige Sicherheits-Token-Lösungen bieten auch Backup-Methoden für den Zugriff auf die MFA im Falle eines Verlusts oder einer Beschädigung, was ihre Widerstandsfähigkeit gegenüber gerätebezogenen Problemen weiter erhöht.
- **Zeit für die Implementierung:** Der Zeitaufwand für die Implementierung von Token MFA ist **mittelgroß**, da es die Verteilung von physischen Token an jeden Benutzer und die Integration der Token in andere Systeme erfordert.

### Voraussetzungen für die erfolgreiche Implementierung:

- Das Amt oder die Behörde sollte die Yubikey-Tokens beschaffen, diese an Endbenutzer zuweisen, aktivieren und verteilen.
- Das Amt oder die Behörde sollte eine Anleitung zu Geräteanmeldung und -bedienung bereitstellen.
- Der Endanwender sollte ein kompatibles Gerät, welches Sicherheitsschlüssel auslesen kann besitzen.
- Der Endanwender sollte die Yubico Authenticator-Anwendung für YubiKey auf sein Mobilgerät oder seinen Desktop herunterladen und installieren.
- Der Endanwender sollte das Device mit sich tragen und bedienen können.

**Zusammengefasst:** Die Yubikey-Token MFA ist sehr sicher, da sie einen physischen Token verwendet, um einen einmaligen Code für den Zugriff auf Online-Dienste zu generieren. Der Hauptvorteil ist die erhöhte Sicherheit sowie die Widerstandsfähigkeit gegenüber gerätebezogenen Problemen. Allerdings ist die Yubikey-Token MFA teurer als andere Optionen und erfordert mehr Ressourcen für die Bereitstellung und Wartung.

## FIDO2 Aufschlüsselung

- **Benutzerfreundlichkeit:** Benutzerfreundlichkeit wird als **mittel** eingestuft, da der Benutzer einen FIDO2-kompatiblen Sicherheitsschlüssel besitzen und diesen physisch in sein Gerät einführen oder den Schlüssel berühren muss, wenn er berührungsbasiert ist. Dies kann den Prozess für einige Benutzer weniger intuitiv machen.
- **Sicherheit:** Sicherheit wird als **hoch** eingestuft, da das Verfahren ein sicheres Gerät (den FIDO2-konformen Sicherheitsschlüssel) verwendet, um die Identität des Benutzers zu überprüfen. Der Schlüssel verwendet eine kryptografische Signatur, um die Identität des Benutzers zu bestätigen, wodurch es für Angreifer sehr viel schwieriger ist, diese Authentifizierungsmethode zu umgehen.
- **Kosten:** Die Kosten für FIDO2 sind **hoch**, da die Option den Einsatz spezieller Hardware (den FIDO2-konformen Sicherheitsschlüssel) erfordert, was zusätzliche Kosten für Organisationen verursachen kann. Außerdem können Kosten für den Kauf, die Bereitstellung und die Wartung der Schlüssel anfallen.
- **Standort des Benutzers:** Der Benutzerstandort-Faktor für FIDO2-MFA ist **mittelmäßig**, da vorausgesetzt wird, dass der Benutzer Zugriff auf seinen FIDO2-kompatiblen Sicherheitsschlüssel hat, was unter Umständen nicht möglich ist, wenn sich der Benutzer an einem Ort befindet, an dem er keinen Zugriff auf den Schlüssel hat.
- **Geräteunabhängigkeit:** FIDO2 MFA erfordert die Verwendung eines FIDO2-kompatiblen Sicherheitsschlüssels, was bedeutet, dass bei Verlust oder Beschädigung des Schlüssels eine Geräteverwaltung erforderlich sein kann, da die Methode **stark vom Gerät abhängig ist**. Wenn der Schlüssel eines Benutzers verloren geht oder beschädigt wird, muss ein Ersatzschlüssel beschafft und für den Benutzer eingerichtet werden, was Zeit und Ressourcen in Anspruch

nehmen kann. Wenn der Schlüssel beschädigt ist, muss er repariert oder ersetzt werden, was ebenfalls Zeit und Ressourcen in Anspruch nimmt.

- **Zeit für die Implementierung:** Der Zeitaufwand für die Implementierung wird als **mittel** eingestuft, da der Einsatz spezieller Hardware (den FIDO2-kompatiblen Sicherheitsschlüssel) erfordert wird und im Vergleich zu den anderen Methoden zusätzliche Konfigurations- und Einrichtungsarbeiten erforderlich sein können.

### Voraussetzungen für die erfolgreiche Implementierung:

- Das Amt/die Behörde sollte die FIDO2-Tokens beschaffen, diese an Endbenutzer zuweisen, aktivieren und verteilen.
- Das Amt/die Behörde sollte eine Anleitung zu Geräteanmeldung und -bedienung bereitstellen.
- Der Endanwender sollte ein PIN für sein Token definieren und die Behörde sollte diese seinem Account mappen.
- Der Endanwender sollte das Device mit sich tragen und bedienen können.

**Zusammengefasst:** Die FIDO2-Option ist sicher und äußerst widerstandsfähig. Ihre beste Eigenschaft ist das hohe Sicherheitsniveau, da sie den FIDO2-konformen Sicherheitsschlüssel verwendet, um die Identität des Nutzers zu überprüfen, und es Angreifern sehr viel schwerer macht, diese Authentifizierungsmethode zu umgehen. Der größte Nachteil ist die Notwendigkeit der Geräteverwaltung. Wenn der Schlüssel verloren geht oder beschädigt wird, muss ein Ersatzschlüssel beschafft und für den Benutzer eingerichtet werden, was Zeit und Ressourcen in Anspruch nehmen kann. Außerdem kann die Bereitstellung der FIDO2-Option im Vergleich zur Sicherheitsfrage-Methode länger dauern und mehr Ressourcen erfordern. Wenn ein hohes Maß an Sicherheit erforderlich ist, ist die FIDO2-Option eine gute Wahl, aber Organisationen müssen darauf vorbereitet sein, die Geräte zu verwalten.

## Best Practices und Zukunftstrends

### Do's & Don't's:

#### Do's:

- Informieren Sie sich über die auf dem Markt verfügbaren MFA-Optionen und wählen Sie diejenige aus, die den spezifischen Bedürfnissen und Anforderungen Ihrer Organisation entspricht.
- Wählen Sie eine MFA-Option, die sich gut in Ihre bestehenden Systeme und Infrastrukturen integrieren lässt.
- Investieren Sie in eine MFA-Option, die ein hohes Maß an Sicherheit bietet, wie z. B. die FIDO2-Option.
- Informieren Sie Ihre Mitarbeiter über die Bedeutung von MFA und die richtige Anwendung.
- Halten Sie Ihre MFA-Systeme und -Infrastruktur mit den neuesten Sicherheitsupdates und Patches auf dem neuesten Stand.

#### Don't's:

- Verwenden Sie keinen einzigen Authentifizierungsfaktor (1FA), wie z. B. ein Passwort, da dieser nicht sicher genug ist, um die sensiblen Daten Ihres Unternehmens zu schützen.
- Verwenden Sie keine leicht zu erratenden Sicherheitsfragen, wie z. B. den Mädchennamen Ihrer Mutter, als Authentifizierungsmethode.
- Vernachlässigen Sie nicht, Ihre Mitarbeiter über die Gefahren von Phishing-Angriffen aufzuklären und darüber, wie sie diese vermeiden können.
- Verwenden Sie keine MFA-Option, die ein Gerät erfordert, das nicht leicht zugänglich oder tragbar ist, da dies dazu führen kann, dass sich Mitarbeiter bei Bedarf nicht authentifizieren können.

## Passwortlose FIDO2 Trends im öffentlichen Sektor

In Zukunft ist mit einer zunehmenden Verbreitung von passwortlosen Authentifizierungsmethoden wie Biometrie und FIDO2 zu rechnen, da sie ein höheres Maß an Sicherheit bieten und im Vergleich zu herkömmlichen MFA-Methoden benutzerfreundlicher sind. Darüber hinaus wird der Einsatz von künstlicher Intelligenz und maschinellem Lernen eine größere Rolle bei der MFA spielen und genauere und effizientere Authentifizierungsprozesse ermöglichen.

Dazu veröffentlichte im Dezember 2022 die FIDO Alliance ein White Paper über die Nutzung von FIDO für E-Government-Zwecke. Das Dokument dient als umfassender Leitfaden für die Verwendung einer sicheren Authentifizierung auf der Grundlage des FIDO-Standards für verschiedene Behördendienste.

Das White Paper beleuchtet den dringenden Bedarf an sicherer und starker Authentifizierung im öffentlichen Sektor sowie die Vorteile der Verwendung von FIDO für eine sichere passwortlose Authentifizierung. Die Abhandlung erörtert die verschiedenen Arten von Authentifizierungsmethoden und erläutert die Vorteile der passwortlosen FIDO-Authentifizierung und die damit verbundene erhöhte Sicherheit sowie die Kostenreduzierung, Verbesserung der Benutzerfreundlichkeit und Effizienzsteigerung. Abschließend wird kurz über die Bedeutung der Einführung sicherer Authentifizierungsstandards in der Verwaltung und die Vorteile berichtet, die durch eine koordinierte Umsetzung dieser Standards im öffentlichen Sektor erzielt werden können.

## Oracle Security Consulting Team's Empfehlungen:

- **Sicherheit als Faktor Nummer 1 bei der Auswahl berücksichtigen.** Die Investition in eine MFA-Technologie ist viel kostengünstiger als die Bewältigung einer Sicherheitsverletzung, sowohl in finanzieller Hinsicht als auch in Bezug auf den Ruf der Organisation und potenzielle Haftungsrisiken.
- **Verschiedene Authentifizierungsfaktoren sollten nicht über das gleiche Übertragungsmedium laufen!** Die beste Sicherheit wird gewährleistet, wenn beispielsweise zwei verschiedene Übertragungskanäle für eine 2FA verwendet werden – die Eingabe eines Benutzernamens und eines Passworts auf einem PC und die Bestätigung durch den Erhalt eines TOTP in einer mobilen Authentifizierungs-App auf einem Mobilgerät. Aus diesem Grund raten wir von E-Mail-MFA ab, da die beiden Faktoren bei diesem Verfahren über denselben Übertragungskanal laufen. Wenn der Benutzer seine Anmeldedaten irgendwo auf einem Stück Papier an seinem Arbeitsplatz hat, kann sich jeder an seinem PC anmelden und hat sofort Zugriff auch auf das E-Mail-Konto des Benutzers, da es normalerweise immer angemeldet ist. Die E-Mail-MFA gewährleistet in diesem Fall nicht wirklich einen zusätzlichen Schutz.
- **Fehlende Weiterentwicklung ist ein erster Ausgangspunkt zu Sicherheitsproblemen.** Aus diesem Grund ist es wichtig, mit den Trends Schritt zu halten und in die modernste und sicherste verfügbare Technologie, wie z.B. FIDO2, zu investieren.
- **Für den Fall, dass das Budget begrenzt ist:** Priorisierung der Benutzer in Benutzergruppen je nach der Sicherheit der von ihnen genutzten Informationen und vorgenommenen Aktivitäten. Zu Beginn sollte die FIDO2-Option für eine ausgewählte Anzahl von Benutzern implementiert werden, um dann mit der Zeit soll diese Benutzergruppe erweitert werden.

## Dokumentation

Tabelle 2: Referenzen und Produkt Dokumentation

THEMA	URL
Introducing Oracle Advanced Authentication OAA	<a href="https://docs.oracle.com/en/middleware/idm/advanced-authentication/oaarm/introducing-oaa.html">https://docs.oracle.com/en/middleware/idm/advanced-authentication/oaarm/introducing-oaa.html</a>
FIDO Alliance White Paper: FIDO for e-Government Services	<a href="https://media.fidoalliance.org/wp-content/uploads/2022/12/FIDO-e-Government-White-Paper.pdf">https://media.fidoalliance.org/wp-content/uploads/2022/12/FIDO-e-Government-White-Paper.pdf</a>

## Versionierung

VERSION	AUTOR	ÄNDERUNG	DATUM
1.0	Teodora Kazakova GenO Security Consultant		15.02.2023