Whitepaper

Technisches Whitepaper zu Okta FastPass

Inhalt

Was ist Okta FastPass?

Okta FastPass ist eine Zero-Trust-Authentifizierungslösung, die umfassenden Schutz bietet. In Verbindung mit einem FIPS 140-3 Level 2-kompatiblen Gerät erfüllt FastPass die Anforderungen der Revision 4 der NIST Special Publication 800-63 Digital Identity Guidelines für Authentication Assurance Level 3 (AAL3). Damit bietet unsere Lösung die höchstmögliche Authentifizierungssicherheit.

FastPass sichert den ersten Authentifizierungspunkt und die weitere Dauer aktiver SSO-Sessions (Single Sign-On). Dadurch kann die Auswirkung von Phishing-Angriffen, Session-Diebstahl und nicht autorisierten lokalen Aktivitäten minimiert werden. Ermöglicht wird das durch passwortlosen und kryptografisch abgesicherten Zugriff – ausschließlich auf vertrauenswürdige Anwendungen – mit einer intuitiven User Experience, die für alle gängigen verwalteten und unverwalteten Plattformen und Geräte einheitlich ist. FastPass stärkt die Zero-Trust-Sicherheit Ihres Unternehmens, indem bei jeder Anmeldung bei einer Anwendung Kontextbewertungen von Browsern und Geräten durchgeführt (sofern aktiviert) und Indikatoren aus Ihrem Sicherheitsökosystem (auch von Drittanbietern) ausgewertet werden.

Damit Endbenutzer FastPass nutzen können, müssen sie auf ihren Desktops, Laptops oder Mobilgeräten die aktuelle Version der Authentifikator-App Okta Verify installieren. Okta Verify mit FastPass-Unterstützung ist für iOS, Android, Windows und macOS verfügbar. Endbenutzer können sich damit bei OIDC-, SAML- oder Web Federation-Anwendungen anmelden, die von Okta geschützt werden.

Okta Verify und FastPass stellen gemeinsam eine der sichersten Login-Möglichkeiten für Endbenutzer bereit. Okta Verify ist die App, während FastPass einer der drei Authentifikatoren ist, die von Okta Verify unterstützt werden. Die anderen beiden sind Push-Benachrichtigungen und Einmal-Passwörter (One-Time Passwords, OTPs). Diese werden nur von den Mobilversionen von Okta Verify (Android und iOS) unterstützt und in diesem Whitepaper nicht weiter erläutert. Administratoren können festlegen, dass FastPass nicht nur als Phishing-resistenter Authentifikator dient, sondern im Rahmen des Authentifizierungsprozesses auch die Gerätesicherheit analysiert und bewertet. Als Anwendung für FastPass müssen Kunden einen Service erwerben, der den Okta Verify-Service enthält, und die Benutzer müssen sich in Okta Verify registrieren, um FastPass nutzen zu können.

Vorteile von Okta FastPass

Vorteile für Administratoren

Phishing-resistente Authentifizierung

FastPass kann die gängigsten Phishing-Angriffe auf verwaltete und unverwaltete Geräte auf allen unterstützten Plattformen abwehren, wenn das durch Richtlinien definiert ist. Bei der Anmeldung bei einer Anwendung mit FastPass wird überprüft, ob der Ursprungs-Header der Authentifizierungsanfrage (die von einer potenziell schädlichen Webseite stammen kann), mit der vom Benutzer kontaktierten Website übereinstimmt. Dadurch wird sichergestellt, dass Benutzer nicht zum Angeben ihrer Anmeldedaten bei einer schädlichen Website verleitet werden, die sich als legitim ausgibt. Administratoren können in den Authentifizierungsregeln für zu schützende Anwendungen Phishing-resistente Einschränkungen festlegen. Der Phishing-resistente Authentifikator FastPass hält die Vorschriften NIST 800-63-3 AAL2 und AAL3 sowie die Empfehlungen für NIST 800-63-4 ein.

Stärkere Gesamtsicherheit

Für die Authentifizierung der Benutzer nutzt FastPass Verschlüsselung mit öffentlichem Schlüssel. Dadurch werden Passwörter (und die damit verbundenen Angriffspunkte) vermieden. Wenn ein Benutzer sich bei FastPass registriert, werden auf dem Gerät öffentliche und private Schlüssel generiert. Die privaten Schlüssel werden sicher im Gerät gespeichert (z. B. in einem Hardware-Modul, sofern verfügbar), während die öffentlichen Schlüssel an den Okta-Cloud-Service gesendet werden. Wenn der private Schlüssel vom Okta-Cloud-Service abgefragt wird, wird damit ein einmaliges Nonce signiert und an Okta zurückgesendet. Anschließend validiert der Okta-Cloud-Service die digitale Signatur und gewährt bei Erfolg Zugriff.

Umfangreicher Gerätekontext

FastPass verifiziert während der Authentifizierung das Gerät sowie den genutzten Browser und erfasst Indikatoren von First-Party- und Third-Party-Quellen, um fundierte Entscheidungen zu Authentifizierung und Autorisierung zu treffen. Der Gerätekontext wird bewertet, sobald sich ein Benutzer zum ersten Mal anmeldet. Anschließend erfolgt die Bewertung jedes Mal im Hintergrund, wenn der Benutzer eine neue Anwendung öffnet. Dadurch wird zusätzlich gewährleistet, dass das Gerät und seine Sicherheitseinstellungen nicht verändert wurden. Erst wenn diese Bewertung abgeschlossen ist, wird der Zugriff auf das nachgelagerte System gewährt. Falls das genutzte Gerät die in der Richtlinie festgelegten Bedingungen nicht erfüllt, erhalten Benutzer Self-Service-Anleitungen dazu, welche Korrekturen erforderlich sind, um die Geräte- oder Browser-Sicherheitsprüfungen zu bestehen.

Die Indikatoren können aus mehreren Quellen stammen, z. B. aus Device Assurance-Richtlinien zur Bewertung des Gerätestatus oder aus Device-Management-Lösungen, die überprüfen, ob das Gerät ordnungsgemäß verwaltet wird. Der Gerätekontext kann auch Indikatoren von Endpoint-Sicherheitsintegrationen umfassen. FastPass kann Informationen zur Gerätesicherheit (z. B. Risiko-Score) von Lösungen für Unified Endpoint Management (UEM) und Endpoint Detection and Response (EDR) nutzen.

Interoperabilität

FastPass führt die Authentifizierung bei allen von Okta geschützten OIDC-, SAML- und WS-Federation-Anwendungen inline durch. Okta agiert hier als Identity-Anbieter und übernimmt die FastPass-Authentifizierung am Endbenutzergerät, ohne dass der Service Provider bei sich Änderungen vornehmen muss. FastPass kann sich auch mit den geräteinternen Authentifikatoren wie Windows Hello, Touch ID oder Face ID integrieren, um biometrische Authentifizierung und vollständige Multi-Faktor-Authentifizierung (MFA) zu ermöglichen.

FastPass ist sowohl ein Authentifikator als auch eine Lösung zur Bewertung der Gerätesicherheit und kann mit einem weiteren Authentifikator kombiniert werden, um MFA-Anforderungen zu erfüllen. Falls ein Administrator einen anderen Authentifikator nutzen möchte (z. B. einen FIDO2-Sicherheitsschlüssel), kann FastPass dennoch in Verbindung mit dem anderen Authentifikator genutzt werden, um umfassende Geräteindikatoren für den Authentifizierungsprozess bereitzustellen.

Lebenszyklusverwaltung für Geräte

Sobald ein Gerät in Okta Verify registriert wurde, werden in Universal Directory auf der Seite „Devices“ (Geräte) grundlegende Informationen zu diesem Gerät bereitgestellt. Dazu gehören Sicherheitsindikatoren, der Gerätemanagement-Status und Geräteidentifikatoren. In der Okta Admin-Konsole können Administratoren den Lebenszyklus von Geräten verwalten. Hier haben sie die Möglichkeit, Geräte nach Bedarf remote zu sperren/entsperren sowie zu aktivieren/deaktivieren. Diese Aktionen werden auch per APIs unterstützt, was individuelle Workflows erlaubt, z. B. die temporäre Sperrung des Zugriffs nicht richtlinienkonformer Geräte.

Vorteile für Endbenutzer

Passwortlose Logins für höhere Produktivität

Endbenutzer profitieren von passwortloser Authentifizierung bei allen von FastPass geschützten Ressourcen. Dies verbessert die User Experience erheblich, da die Reibungspunkte durch Passwörter (und Passwortrücksetzungen) sowie Out-of-Band-Faktoren wie Push-Benachrichtigungen, TOTPs (Time-based One-Time Passwords) und SMS beseitigt werden. Dank der nahtlosen Unterstützung der Plattform-Authentifikatoren zur biometrischen Authentifizierung können Benutzer bei minimalen zusätzlichen Reibungspunkten höhere Sicherheitsanforderungen erfüllen.

Einheitliche plattformübergreifende User Experience

FastPass stellt benutzerfreundliche und einheitliche Authentifizierungsabläufe bereit – unabhängig davon, ob Benutzer sich mit verwalteten oder unverwalteten Geräte mit iOS, Android, Windows oder macOS anmelden. Unter Windows werden die VDI-Umgebungen (Virtual Desktop Infrastructure) Windows 365, Citrix und AWS WorkSpaces unterstützt. Dadurch profitieren Endbenutzer auf allen Geräten von der gleichen sicheren und passwortlosen User Experience.

Wichtige Konzepte

Geräteregistrierung und Gerätemanagement im Vergleich

Ein Gerät gilt als „registriert“, wenn es in FastPass registriert ist. Im Gegensatz dazu gilt ein Gerät als „verwaltet“, wenn es von einer MDM-Lösung (Mobile Device Management) oder einer ähnlichen Anwendung kontrolliert oder verwaltet wird. Bei FastPass haben Administratoren keinen Lese- oder Schreibzugriff auf persönliche Daten auf dem Gerät. Sie können das Gerät auch nicht remote löschen oder den genauen Standort abfragen, was bei per MDM verwalteten Geräten möglich ist.

Geräte-Identity und -Registrierung

FastPass ist einer von mehreren Authentifikatoren, die von Okta Verify unterstützt werden, und die Benutzer müssen sich in Okta Verify registrieren, um FastPass nutzen zu können.

Wenn sich ein Benutzer bei Okta Verify registriert, wird in Okta Universal Directory eine individuelle Geräte-Identity erstellt, die Benutzer und Gerät verknüpft. Dem Gerät wird eine Geräte-ID zugewiesen. Universal Directory speichert zusätzliche Kontextdaten über das Gerät, z. B. Anzeigename, Betriebssystem, Modell, Hersteller und Management-Status. Jedes Mal, wenn Benutzer sich erfolgreich bei FastPass authentifizieren, werden die Gerätedetails aktualisiert. Eine vollständige Liste der Gerätedetails finden Sie in der Produkt-Dokumentation. Administratoren können in der Okta Admin-Konsole nach Geräten suchen und sie dort sperren, entsperren, deaktivieren, reaktivieren und löschen. Weitere Informationen zu den verschiedenen Lebenszyklus-Phasen finden Sie hier.

Phishing-resistente Authentifizierung

Das National Institute of Standards and Technology (NIST) stellt technische Richtlinien für Unternehmen zur Implementierung digitaler Identity-Services bereit. In der Special Publication 800-63B definiert das NIST wichtige Attribute für Phishing-Schutz. Dazu gehören:

- **Verifizierer-Namensbindung** zum Aufbau eines vertrauenswürdigen geschützten Kanals mit dem Verifizierer; dabei wird eine Authentifikator-Ausgabe generiert, die kryptografisch an einen Verifizierer-Identifikator (z. B. die Ursprungs-Domain) gebunden ist
- **Replay-Resistenz** durch Authentifikatoren wie OTP-Geräte, kryptografische Authentifikatoren und Look-Up Secrets sowie Protokolle, die Nonces oder Abfragen und Aktualitätsdaten verwenden
- **Schutz vor Verifizierer-Kompromittierung** dank Authentifizierungs-protokollen, die keine dauerhaft gespeicherten Secrets erfordern, z. B. durch die Verwendung eines kryptografischen Authentifikators und Speicherung aller öffentlichen Schlüssel mit kryptografischen Algorithmen
- **Authentifizierungsabsicht**, d. h. dass der Benutzer auf jede Authentifizierungs- oder Neu-Authentifizierungsanfrage explizit reagieren muss

Besitznachweis-Faktor

Dieser Faktortyp erfüllt die Besitzanforderung („etwas, das Sie besitzen“). Wenn sich der Benutzer bei FastPass registriert, generiert Okta ein Schlüsselpaar und legt es als Proof-of-Possession-Schlüsselpaar für FastPass fest. Der private Schlüssel wird im Hardware-Schlüsselspeicher des Geräts (sofern verfügbar) oder in einem nicht-exportierbaren Software-Schlüsselspeicher des jeweiligen Betriebssystems abgelegt. Der öffentliche Schlüssel wird an den Okta-Server gesendet. Während des Authentifizierungsprozesses überprüft der Okta-Server mithilfe dieses öffentlichen Schlüssels, dass die Payload-Signatur mit dem entsprechenden privaten Schlüssel signiert wurde.

Bei erfolgreicher Signaturverifizierung wird davon ausgegangen, dass der Benutzer einen Besitzfaktor verwendet hat. Wenn die Authentifizierungsrichtlinie für die Anwendung zusätzliche Faktoren erfordert, fragt der Okta-Server beim Benutzer einen weiteren Authentifizierungsfaktor ab.

Sie können konfigurieren, ob FastPass als Besitznachweis-Faktor mit oder ohne Überprüfung der Benutzerpräsenz erfasst wird. Wenn die Benutzerpräsenz erforderlich ist, fordert Okta Verify eine Benutzerinteraktion an (z. B. die Abfrage „Ja, das bin ich“), bevor die Verifizierung fortgesetzt wird.

Benutzerverifizierungs-Faktor

Dieser Faktortyp erlaubt die Benutzerverifizierung durch einen Inhärenzfaktor (z. B. Biometrie) oder einen Wissensfaktor (z. B. eine PIN oder einen Passcode) als zweiten Faktor zusätzlich zum Besitznachweis-Faktor, den FastPass bereitstellt.

Während der Okta Verify-Registrierung werden zusätzliche Schlüsselpaare generiert, wenn der Endbenutzer seine biometrischen Daten oder den Geräte-Passcode zur Benutzerverifizierung angibt. Sofern verfügbar, wird der private Schlüssel sicher im Hardware-Schlüsselspeicher des Geräts gespeichert, während der öffentliche Schlüssel an den Okta-Server gesendet wird. Der private Schlüssel kann nur zum Signieren einer Payload verwendet werden, wenn der Endbenutzer seine biometrischen Daten oder den Passcode angegeben hat, um die Anforderungen der Benutzerverifizierung zu erfüllen.

Gerätekontext

Während des Authentifizierungsprozesses erfasst FastPass den Kontext des verwendeten Geräts. Dazu gehören grundlegende Geräteindikatoren wie Plattform-Name, Betriebssystem-Version, Anzeigename des Geräts usw. Abhängig von der Konfiguration der Authentifizierungsrichtlinie durch den Administrator kann FastPass auch Informationen wie Management-Nachweis, Jailbreak-Status und weitere Sicherheitsindikatoren erfassen, die für die Geräte-Compliance erforderlich sind.

Geräte-Analyse (Probing)

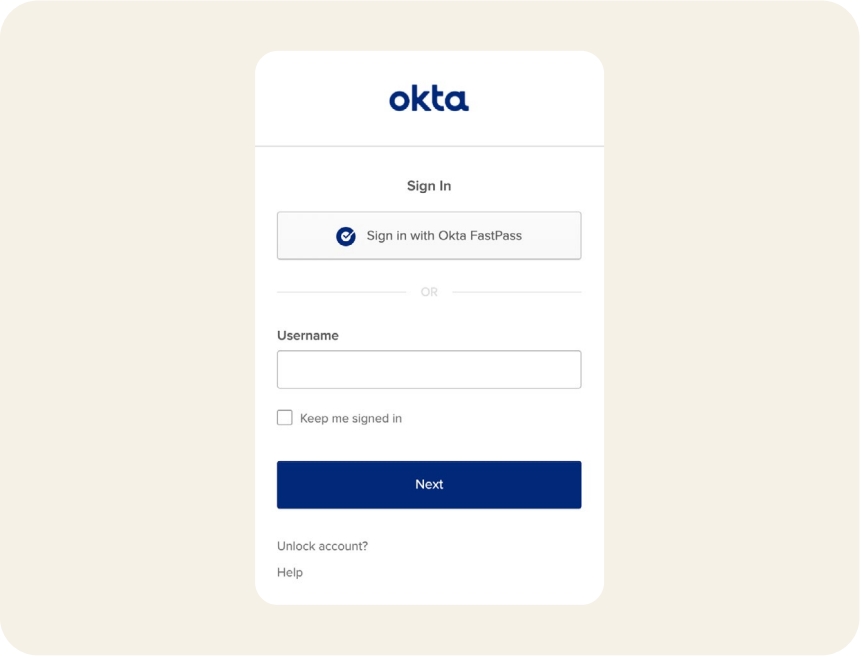
Beim Probing kommuniziert Okta-Widget für die Anmeldung (Okta SIW), das in einer Browser-Registerkarte oder in Webview aufgeführt wird, mit Okta Verify auf dem Gerät. Wenn Okta Verify nicht installiert ist, schlägt der Probing-Mechanismus fehl, und der Benutzer wird zur Nutzung anderer Authentifikatoren aufgefordert.

Interaktives Probing und Probing im Hintergrund im Vergleich

FastPass unterstützt Probing im Hintergrund sowie interaktives Probing in jedem Browser. Das Probing im Hintergrund erfordert keine Benutzerinteraktionen und bietet die beste User Experience. Deshalb versucht FastPass stets zuerst diese Methode.

Methode	Typ	Unterstützte Plattformen
Loopback	Hintergrund, Interaktiv	macOS, Windows, Android und iOS
Credential SSO	Hintergrund, Interaktiv	Managed iOS und macOS
Universal Link	Interaktiv	iOS
App Link	Interaktiv	Android
Custom URI	Interaktiv	Windows und macOS

Wenn das Probing im Hintergrund nicht verfügbar ist (z. B. wenn der Loopback-Server nicht startet), weicht das SIW auf eine interaktive Probing-Methode aus und der Endbenutzer muss Okta Verify mit einer interaktiven Methode starten. In diesem Fall muss der Benutzer im SIW auf den Button „Sign in with Okta FastPass“ (Anmeldung mit Okta FastPass) klicken oder tippen.



Unabhängig von der verwendeten Probing-Methode versucht das SIW, folgende Informationen zu erfassen:

- Nur Besitznachweis-Faktor oder
- Besitznachweis-Faktor und Benutzerverifizierungs-Faktor

Die Entscheidung zum Erfassen von einem oder beiden Faktoren ist abhängig von der Konfiguration in Okta Verify sowie von der Konfiguration der Authentifizierungsrichtlinie.

Wenn der Button „Sign in with Okta FastPass“ (Anmeldung mit Okta FastPass) aktiviert wird, bietet er Benutzern eine einfache Möglichkeit zur Authentifizierung ohne Eingabe von Benutzername oder Passwort. Damit können sich Benutzer auch leichter bei Okta Verify und FastPass registrieren und erhalten Anleitungen zur Einrichtung und Eingabeaufforderungen.

Geräte-Probing-Schemas

Wenn Probing-Schema erfolgreich sind, binden sie das Gerät an die Session. FastPass unterstützt folgende Probing-Schemas:

- **Loopback:** Okta Verify führt einen Server auf einem lokalen Host-Port aus, der auf Probing-Anfragen vom SIW reagieren kann. Wenn der Loopback-Server vom SIW kontaktiert wird, kann er die Sicherheitsabfrage akzeptieren, um ein Nonce digital zu signieren. Dieses Probing-Schema ist Phishing-resistent und für Windows, macOS, Android und iOS verfügbar.

- **Credential SSO:** Benutzer mit verwalteten iOS- und macOS-Geräten können FastPass nahtlos mit einer SSO-Erweiterung nutzen, die auf den Geräten durch eine MDM-Lösung bereitgestellt wird. Dieses Probing-Schema ist Phishing-resistent und für unterstützte Anwendungen und Browser verfügbar.

- **Universal Link:** Auf iOS-Geräten kann das SIW mit Universal Links nach einem Benutzer-Klick die Okta Verify-App starten. Das SIW hängt die Sicherheitsabfrage an den Universal Link an. Wenn der Benutzer auf „Sign in with FastPass“ (Anmeldung mit Okta FastPass) klickt, wird die Abfrage an FastPass weitergegeben. In Kombination mit Loopback sind Universal Links Phishing-resistent, sodass Okta nach Möglichkeit immer die Kombination wählt.

- **App Link:** Auf Android-Geräten kann das SIW mit App Links nach einem Benutzer-Klick die Okta Verify-App starten. Das SIW hängt die Sicherheitsabfrage an den App Link an. Wenn der Benutzer auf „Sign in with FastPass“ (Anmeldung mit Okta FastPass) klickt, wird die Abfrage an FastPass weitergegeben. Wie Tests durch Okta ergeben haben, funktionieren App Links nicht immer in nativen Authentifizierungsabläufen. In Kombination mit Loopback sind App Links Phishing-resistent, sodass Okta nach Möglichkeit immer die Kombination wählt.

- **Custom URI:** Auf Geräten mit macOS und Windows kann das SIW mithilfe der eigenen URI die Okta Verify-App per Benutzer-Klick starten. Ebenso wie beim Universal Link- und App Link-Schema reagiert Okta Verify nach dem Klicken auf das Custom URI-Schema. Das SIW hängt die Sicherheitsabfrage an die Custom URI an. Die Custom URI ist nicht Phishing-resistent, kann jedoch genutzt werden, um den Loopback-Server der Anwendung zu starten.

Sicherheits-modell

Generierung und Schutz des Schlüssels

Bei der Registrierung von Okta Verify auf einem Gerät werden zwei Schlüsselpaar-Typen generiert: für den Besitznachweis (Proof-of-Possession) und für die Benutzerverifizierung. Standardmäßig werden private Schlüssel sicher im Hardware-Schlüsselspeicher eines Geräts gespeichert (sofern verfügbar), z. B. in einem TPM oder einer Secure Enclave (iOS). Die privaten Schlüssel verlassen zu keinem Zeitpunkt den Hardware-Schlüsselspeicher und können nicht in einem Backup gesichert oder zu anderen Geräten exportiert werden. Falls das Gerät nicht über einen Hardware-Schlüsselspeicher verfügt, werden die privaten Schlüssel in einem nicht-exportierbaren Software-Schlüsselspeicher der Plattform oder des Betriebssystems gespeichert.

Während der Faktorerfassung nutzt FastPass den Schlüsselspeicher, um die digital signierte Ausgabe für eine bestimmte Eingabe-Payload zu erhalten. Diese signierte Ausgabe-Payload wird zur Signaturüberprüfung an den Okta-Server gesendet. Dies erfolgt über eine TLS-Pinning-Verbindung, die von intermediären Parteien nicht abgefangen werden kann.

Administratoren können Authentifizierungsrichtlinien erstellen, die Hardware-gebundene Schlüssel erfordern. Weitere Informationen finden Sie unter „Configure an authentication policy“ (Konfigurieren einer Authentifizierungsrichtlinie).

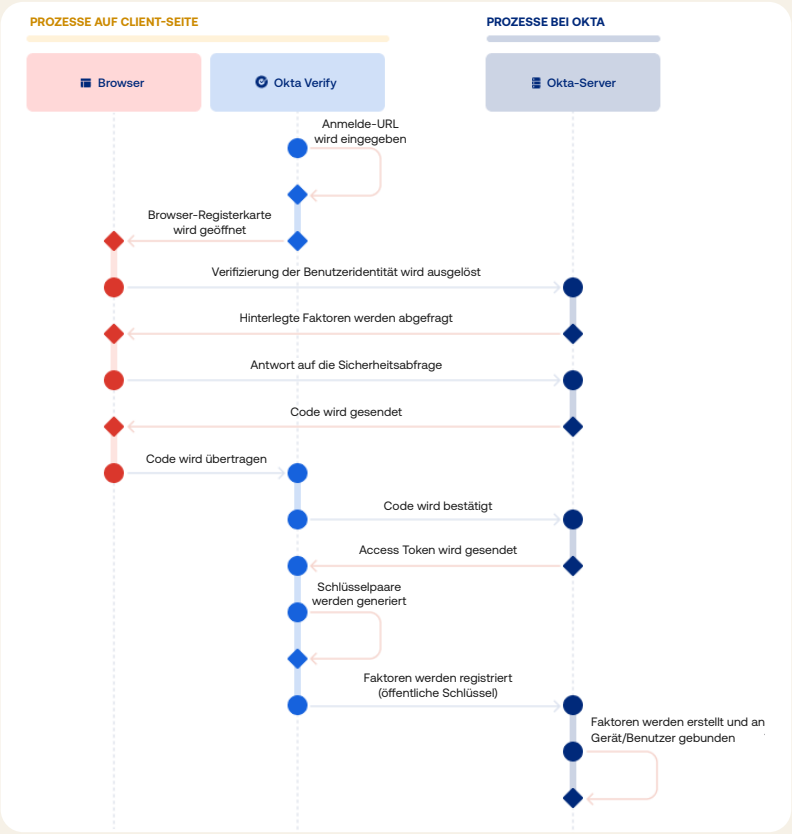
Platform	Verwendeter digitaler Signaturalgorithmus	Schlüsselgröße
macOS	ES256	256 Bit
Windows	RS256	2048 Bit
iOS	ES256	256 Bit
Android	RS256	2048 Bit

Schutz vor Manipulation

Die Okta Verify-App verfügt über Manipulationsschutz, der schädliche Aktivitäten verhindert. Die Manipulationsschutz-Maßnahmen in Okta Verify können erkennen, ob Malware oder ein Angreifer versucht, das beabsichtigte Verhalten der Anwendung zu verändern. In diesem Fall stürzt Okta Verify sofort ab, um alle Prozesse zu deaktivieren.

Okta FastPass im Detail

Registrierung



Wenn der Endbenutzer sich bei FastPass registriert, gewährleistet der Prozess eine starke Bindung zwischen dem Authentifikator, dem Gerät und dem Benutzer. Pro Gerät und User Account ist nur eine einzige FastPass-Registrierung zulässig.

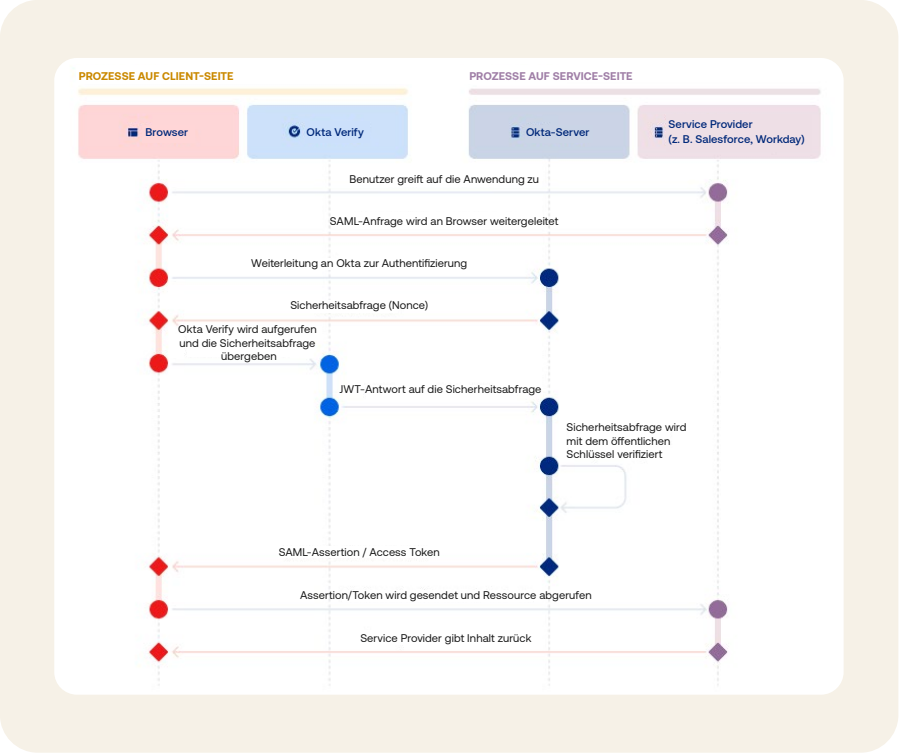
Vor der Registrierung bei FastPass muss der Benutzer zur Identitäts-verifizierung weitere Faktoren angeben, die von der Authentifikator-Registrierungsrichtlinie festgelegt werden. Nachdem die Identität überprüft wurde, fordert Okta Verify den Benutzer auf, die biometrische Authentifizierung (z. B. Touch ID, Face ID, Windows Hello) oder die Verwendung von Geräte-Passcodes zu aktivieren. Wenn die entsprechende Option aktiviert ist, generiert Okta Verify ein Schlüsselpaar zur Benutzerverifizierung.

Um den FastPass-Registrierungsprozess Phishing-resistent zu machen, können Administratoren den Nachweis eines Phishing-resistenten Authentifikators vorschreiben.

Wenn Endbenutzer ein zweites Gerät Phishing-resistent in Okta Verify registrieren möchten, ist dies per Bluetooth (für Android, iOS, macOS oder Windows) oder per YubiKey möglich.

Authentifizierungsvorgang und Probing

Das folgende Diagramm zeigt beispielhaft einen typischen FastPass-Flow für einen SAML-basierten SSO-Prozess (Single Sign-On).



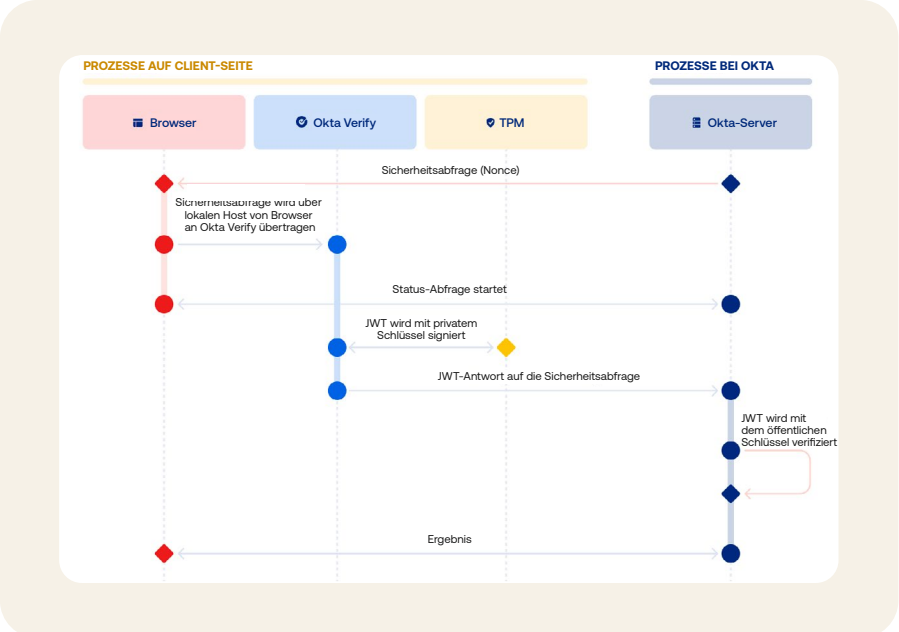
Beispiel: FastPass bei einem typischen SSO-Prozess mit einer SAML-Anfrage

1. Der Endbenutzer greift mit einem Browser auf einen Service wie Salesforce oder Workday zu.
2. Der Service Provider generiert die SAML-Anfrage und leitet die Anfrage zurück an den Browser und anschließend zur Authentifizierung an Okta weiter.
3. Der Okta-Server bewertet die Anfrage und generiert die FastPass-Sicherheitsabfrage, die z. B. zur Benutzerverifizierung auffordern und spezifische Gerätebedingungen verlangen kann, die in der Authentifizierungsrichtlinie der Anwendung festgelegt sind. Der Okta-Server sendet die Abfrage zusammen mit dem SIW an den Browser. Das SIW im Browser ruft FastPass auf.

4. FastPass generiert eine Antwort (mit den entsprechenden Geräteindikatoren) und signiert diese Antwort mit dem privaten Benutzerverifizierungs-Schlüssel (der für den Benutzer clientseitig registriert ist). Der private Benutzerverifizierungs-Schlüssel dient sowohl als Besitznachweis als auch der Benutzerverifizierung.
5. Der Okta-Server identifiziert den Benutzer, indem er die Signatur mit dem öffentlichen Schlüssel überprüft. Die erfassten Geräteinformationen werden anhand der relevanten Authentifizierungsrichtlinie bewertet.
6. Wenn die Bedingungen mit den Zugriffsbedingungen übereinstimmen, generiert der Okta-Server die SAML-Assertion und leitet den Browser zum Service Provider zurück. Andernfalls kann der Okta-Server abhängig von der Richtlinie zur Eingabe eines weiteren Faktors auffordern oder den Zugriff vollständig blockieren.

Faktor-Erfassung mit Loopback

Eine Methode für die Kommunikation des SIW mit der lokalen Okta Verify-Installation verwendet einen lokalen Server, der von Okta Verify gehostet wird und nicht über das allgemeine Internet erreichbar ist. Das ermöglicht eine umfangreiche Kommunikation lokal auf dem Gerät zwischen der Browser-Session und der lokalen Anwendungsinstallation. Dank dieses Servers bleibt Okta Verify während des Authentifizierungsablaufs im Hintergrund und wird nur dann aktiv, wenn der Okta-Server Aktionen wie die Erfassung biometrischer Informationen oder die Einwilligung des Benutzers anstößt.



Faktor-Erfassung mit der Credential SSO-Erweiterung

Die Credential SSO-Erweiterung steht nur unter macOS/iOS zur Verfügung. Okta Verify ist so konfiguriert, dass die Lösung HTTP-Traffic zwischen dem Browser und dem Okta-Server kontrolliert. Wenn der Okta-Server eine Sicherheitsabfrage auslöst, wird diese vom Browser mit einer 401-Antwort über die SSO-Erweiterung an FastPass übergeben. Sobald FastPass einen 401-Status entdeckt, werden die signierte Nonce-Abfrage und der Antwort-Vorgang gestartet.

Faktor-Erfassung mit Custom URI und Universal Link

Wenn Loopback oder Credential SSO fehlschlagen, können Browser per Deep Link Sicherheitsabfragen an FastPass starten und weiterleiten. Bei Windows und macOS nutzen wir das Custom URI-Schema, bei Android die App Link-Methode und bei iOS die Universal Link-Methode. App Links und Universal Links bieten hohe Sicherheit, da sie nur von verifizierten Anwendungen aufgerufen werden können. Sie stehen jedoch nicht auf allen Plattformen zur Verfügung.

Device Assurance-Richtlinien und Kontext-Neubewertung

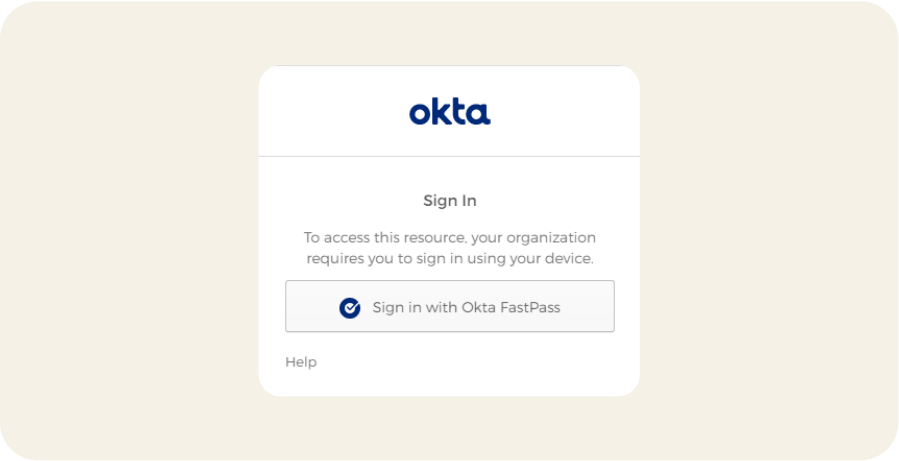
FastPass erfasst First-Party-Signale zum Gerätestatus mithilfe von Device Assurance-Richtlinien. Damit können Administratoren festlegen, dass im Rahmen einer Authentifizierungsrichtlinie verschiedene sicherheitsbezogene Geräteattribute überprüft werden. So kann mithilfe einer Device Assurance-Richtlinie beispielsweise sichergestellt werden, dass eine bestimmte Betriebssystem-Version bzw. ein Sicherheits-Patch installiert ist, bevor das Gerät Zugriff auf Ressourcen erhält, die von Okta geschützt werden. Mit solchen Prüfungen kann festgelegt werden, dass Geräte beim Zugriff auf sensible Systeme und Anwendungen Mindestanforderungen erfüllen. Wenn das Gerät eines Benutzers die Anforderungen bei einem erforderlichen Attribut nicht erfüllt, bietet das Okta SIW Anleitungen zur Problembehebung.

Wenn ein Benutzer sich mit FastPass authentifiziert, werden alle Geräteindikatoren (einschließlich Drittanbieter-Signale aus Integrationen mit Endpoint-Sicherheitslösungen) abgerufen und bewertet. Das erfolgt nicht nur zu Beginn der SSO-Session, sondern jedes Mal, wenn eine neue Anwendung im Okta-Dashboard geöffnet wird bzw. wenn eine erneute Authentifizierung erforderlich ist. Diese Kontextprüfungen im Hintergrund können die kontinuierliche Sicherheit der verwendeten Geräte gewährleisten und das Risiko von Session Hijacking minimieren, da sie potenzielle Angriffe erkennen und in diesem Fall den Zugriff auf nachgelagerte Anwendungen sperren.

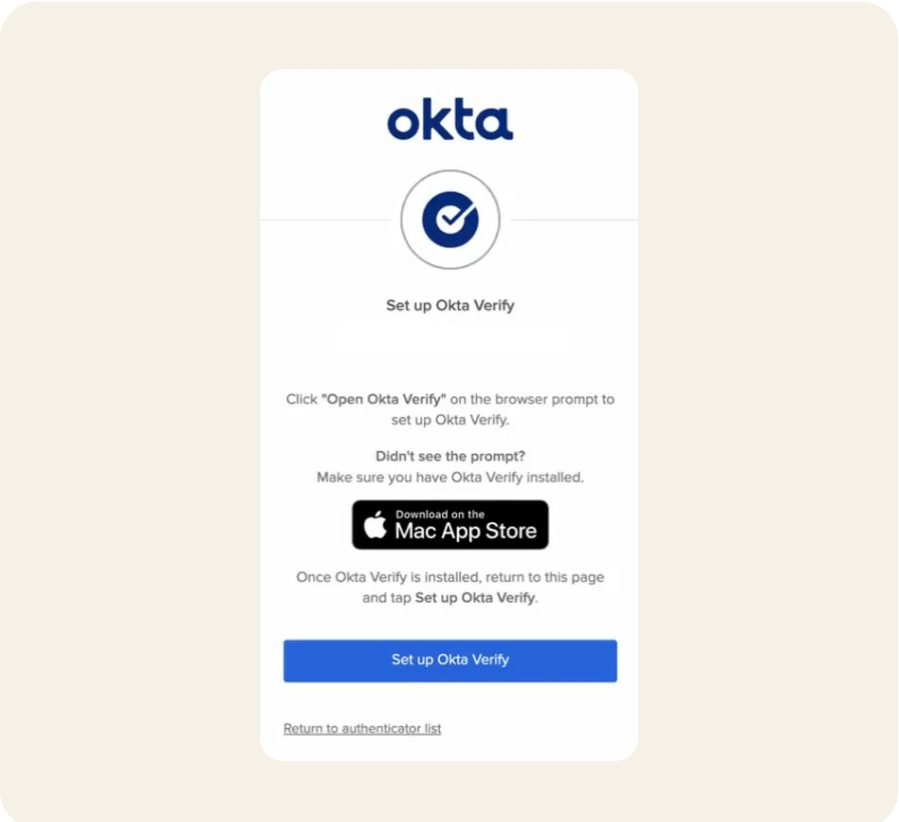
Problembehebung

Wenn Gerätebedingungen nicht erfüllt werden, empfiehlt das SIW den Endbenutzern Behebungsmaßnahmen:

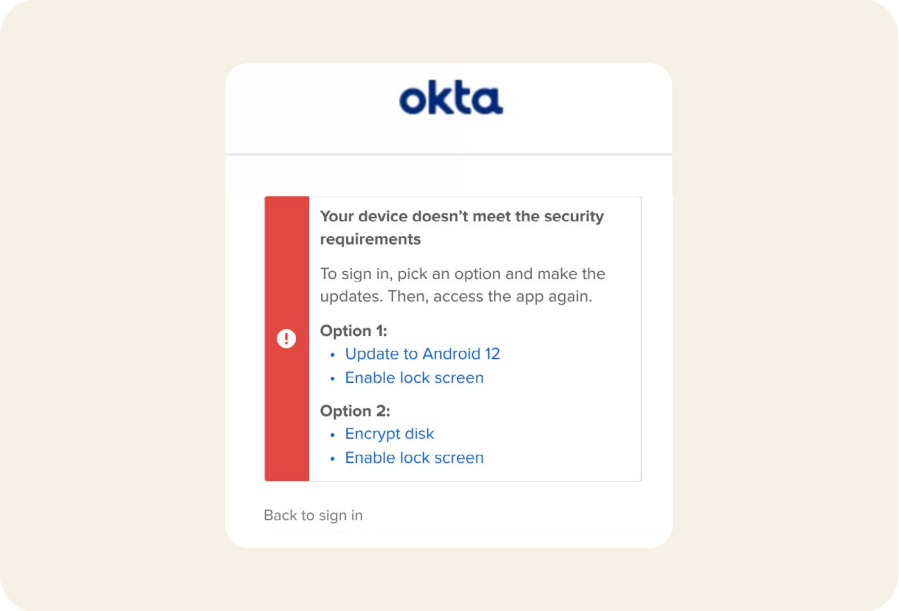
- Beispiel Nr. 1: Wenn FastPass für den Zugriff auf eine Anwendung erforderlich ist



- Beispiel Nr. 2: Wenn für den Zugriff ein registriertes Gerät erforderlich ist und Okta Verify nicht installiert wurde



- Beispiel Nr. 3: Wenn die Bedingung einer Device Assurance-Richtlinie nicht erfüllt wird, z. B. nicht die neueste Betriebssystem-Version installiert ist



Verwaltete Geräte

Okta integriert sich mit Gerätemanagement-Softwareanbietern und gewährleistet so, dass Geräte ordnungsgemäß verwaltet werden, bevor Endbenutzer damit auf Anwendungen zugreifen können. Während des Authentifizierungsablaufs erfasst FastPass Geräteindikatoren, die zur Verifizierung an den Okta-Server übergeben werden. Hier finden Sie die Schritte zum Konfigurieren und Bereitstellen von verwalteten Geräten.

Auf Desktop-Geräten (Windows und macOS) werden mit dem Client-Zertifikat der Okta-Zertifizierungsstelle (Certificate Authority, CA) oder Ihrer eigenen CA die Management-Nachweisinformationen erstellt. Die Okta-CA stellt Client-Zertifikate für verwaltete Desktop-Geräte mithilfe des SCEP-Protokolls bereit. Die Okta-CA bietet statische, dynamische oder delegierte Modi zur Bereitstellung von SCEP-Zertifikaten. Okta empfiehlt Windows-Administratoren, die MDM-SCEP-Richtlinie so zu konfigurieren, dass private Schlüssel in den Geräte-Hardware-Schlüsselspeichern gespeichert werden und Zertifikate nicht exportierbar sind.

Wenn die Authentifizierungsrichtlinie für Anwendungen den Status des verwalteten Geräts abfragt, fordert der Okta-Server per FastPass-Protokoll den Gerätemanagement-Nachweis an. Der Okta Verify-Client unter Windows und macOS identifiziert das richtige Client-Zertifikat auf dem Gerät und signiert damit ein individuelles Nonce in der Anfrage, um einen Management-Nachweis zu erstellen. Der Okta-Server überprüft zuerst, ob das Client-Zertifikat von der bekannten CA ausgestellt wurde, und validiert anschließend die Management-Nachweis-Signatur mit dem öffentlichen Schlüssel des Client-Zertifikats.

In Bereitstellungen mit Drittanbieter-CA überprüft der Okta-Server regelmäßig (aller 6 Stunden) die Zertifikatsperrliste (Certificate Revocation List, CRL) des Drittanbieters und macht inaktive Client-Zertifikate ungültig. Dadurch können zurückgezogene, gesperrte oder suspendierte Client-Zertifikate den Management-Nachweis nicht erbringen.

Der Okta-Server ordnet das Client-Zertifikat dem Geräteobjekt in Universal Directory zu. Wenn der Management-Nachweis in einer Replay-Attacke von einem anderen Gerät wiederholt übermittelt wird, schlägt er fehl. Dadurch wird verhindert, dass Client-Zertifikate von nicht autorisierten Geräten für den Management-Nachweis missbraucht werden können.

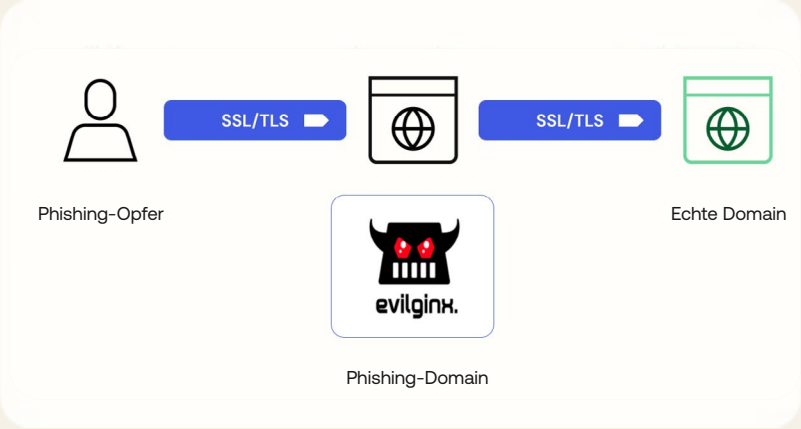
Auf Mobilgeräten (iOS und Android) wird ein Management-Hinweis (Shared Secret) zur verwalteten Anwendung an das Gerät übermittelt. Ebenso wie bei zertifikatbasierten Bereitstellungen antwortet Okta Verify mit dem Shared Secret, wenn vom Okta-Server eine Sicherheitsabfrage über das FastPass-Protokoll erfolgt. Der Okta-Server verifiziert das Secret durch Vergleich mit einem Hash-Wert, der während der Erstkonfiguration gespeichert wurde. Der Okta-Server speichert das eigentliche Secret nicht. Daher sind Sie selbst für dessen sichere Speicherung verantwortlich.

Phishing-resistente Authentifizierung

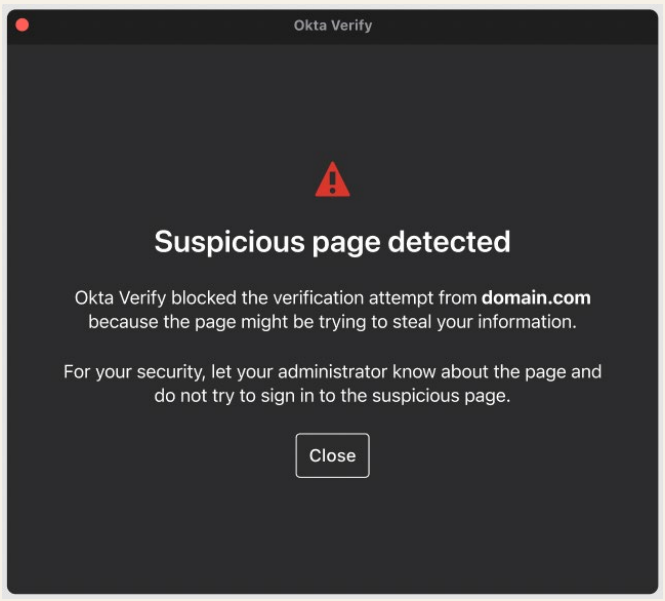
Bei einem Phishing-Angriff werden Benutzeranmeldedaten mit Social-Engineering-Taktiken gestohlen, um anschließend den Benutzer imitieren und seinen Datenzugriff missbrauchen zu können. Das Opfer wird dazu verleitet, einen Link zu einer Fake-Website zu öffnen, die sich als vertrauenswürdige Entität ausgibt, und den Angreifern seine Anmeldedaten zu übermitteln. FastPass ist ein hochentwickelter Phishing-resistenter Authentifikator, der eine der häufigsten Phishing-Taktiken verhindern kann: Adversary-in-the-Middle-Angriffe (AiTM).

AiTM-Angriffs-Framework mit Evilginx

Angriffs-Framework für Adversary-in-the-Middle-Attacken zum Phishing von Login-Anmeldedaten und Sessions



Bei diesen Attacken nutzt der Bedrohungsakteur einen Proxy, um das Okta SIW zu initiieren und sich als vertrauenswürdige Entität auszugeben. Dies erfordert eine Proxy-Anfrage von der schädlichen Website an den Okta-Server. Der Server kann den Ursprungs-Header validieren und Diskrepanzen erkennen. Wenn eine Domain-Diskrepanz entdeckt wird, schlägt die FastPass-Authentifizierung fehl, das Ereignis wird im Okta SysLog protokolliert und dem Benutzer wird eine Warnung wegen verdächtiger Aktivitäten angezeigt.

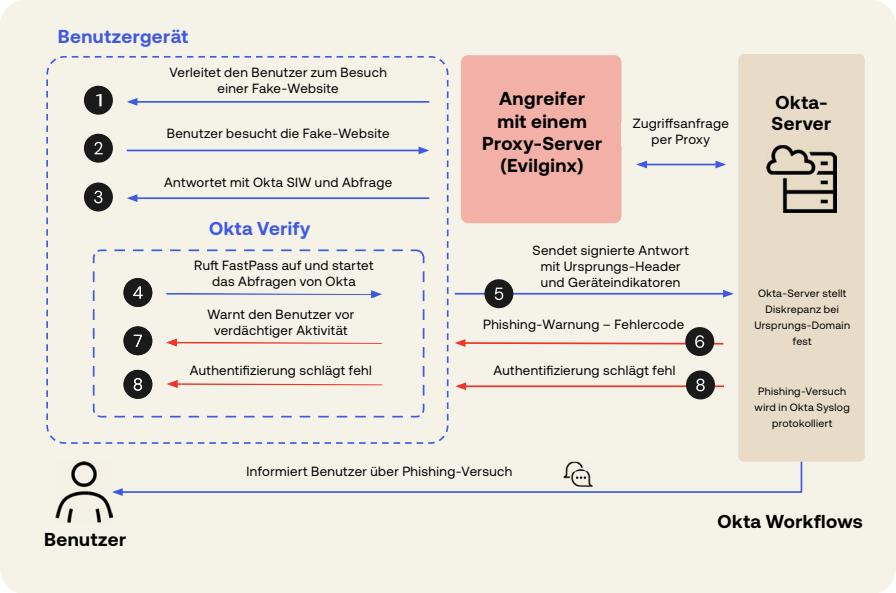


Administratoren können die Endbenutzer mit Okta Workflows über einen Rückkanal wie Slack oder E-Mail warnen und weitere Maßnahmen treffen, z. B. den Traffic zu und von der Phishing-Website blockieren.

Dank dieser Verifizierer-Namensbindung über den Ursprungs-Domain-Header ist FastPass Phishing-resistent. In seltenen Fällen (z. B. wenn native Anwendungen und schädliche Browser-Plugins beteiligt sind) kann ein Angreifer die Ursprungs-Header programmgesteuert in JavaScript ändern. Dieses Problem tritt bei den meisten derzeit erhältlichen Phishing-resistenten Authentifikatoren auf. Auf Desktop-Geräten unterstützt FastPass Filter für vertrauenswürdige Anwendungen und gewährleistet dadurch, dass nur vertrauenswürdige Anwendungen die FastPass-Authentifizierung auslösen können. Administratoren können eine Allow-Liste für Anwendungen erstellen und festlegen, dass nur signierte und verifizierte Anwendungen FastPass aufrufen dürfen. So wird verhindert, dass schädliche oder nicht verifizierte Anwendungen FastPass für unbefugten Zugriff missbrauchen.

User Journey-Beispiele

Szenario 1: Phishing-Versuch

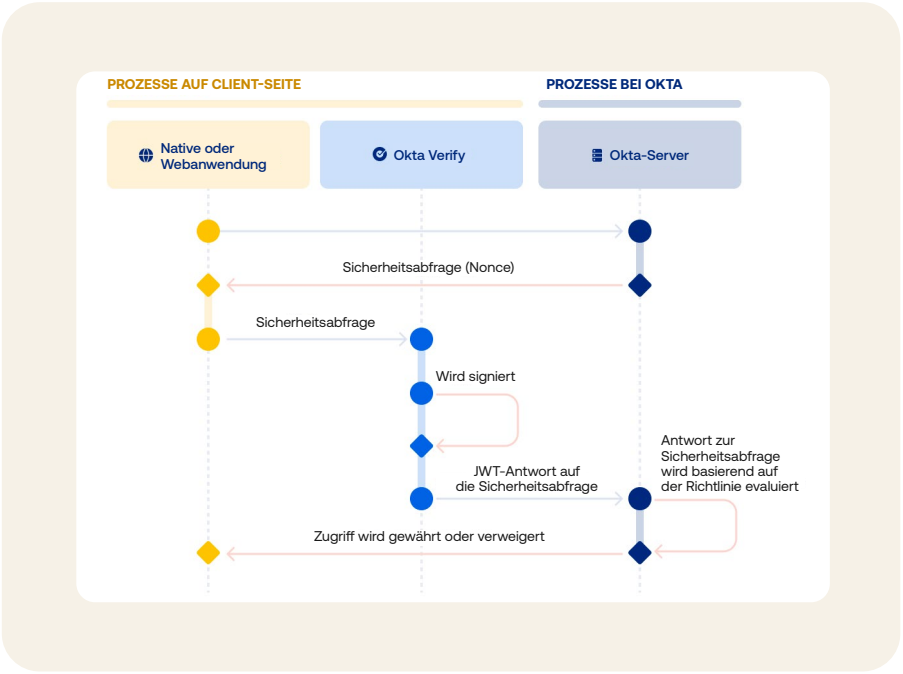


Dies ist ein typischer Ablauf des FastPass-Phishing-Schutzes:

1. Der Bedrohungsakteur lockt das Opfer mit einer Phishing-E-Mail zu einer schädlichen Website.
2. Der Benutzer fällt auf den Phishing-Versuch herein und klickt auf einen Link zur Fake-Website, die wiederum den Authentifizierungsprozess startet. Die schädliche Website sendet eine Proxy-Zugriffsanfrage an den Okta-Server.
3. Die schädliche Website sendet eine Proxy-Antwort einschließlich des Okta SIW mit dem Sicherheitsabfrage-Nonce zurück an den Benutzer.
4. Der Benutzer meldet sich mit FastPass an. Das SIW ruft FastPass über den Loopback-Server auf und startet das Abfragen des Ergebnisses beim Okta-Server.
5. FastPass signiert das Nonce, Geräteindikatoren sowie den Ursprungs-Header und sendet die Antwort zurück an den Okta-Server.
6. Der Okta-Server validiert den Ursprungs-Header und erkennt eine Diskrepanz zwischen dem erwarteten Ursprungs-Header und dem von FastPass gelieferten Ursprung. Der Okta-Server antwortet mit einem Fehlercode.
7. Okta zeigt einen Meldung an, die den Benutzer warnt und auf eine verdächtige Aktivität hinweist.

8. Der Okta-Server protokolliert den Phishing-Versuch im Okta SysLog und verweigert die Authentifizierung.
9. Der Benutzer wird in anderen Kanälen (z. B. per E-Mail oder Textnachricht) über den Phishing-Angriff informiert, sofern die Administratoren Okta Workflows entsprechend konfiguriert haben.

Szenario 2: Authentifizierung im Hintergrund



Wie der Name bereits andeutet, bezeichnet die Authentifizierung im Hintergrund den FastPass-Prozess des Hintergrund-Probings. In diesem Fall greift ein Benutzer mit einem registrierten Gerät auf die Anwendung zu. Dies löst eine Reihe von Validierungsaktionen zwischen dem Okta-Server und der Okta Verify-App auf dem Gerät aus. Wenn Benutzer und Gerät die Sicherheitsanforderungen erfüllen, die zum Anmelden bei der Anwendung erforderlich sind, gibt der Okta-Server den Zugriff frei.

1. Der Benutzer besucht eine von Okta geschützte Ressource und initiiert damit die Authentifizierung.
2. Der Okta-Server erstellt eine individuelle Sicherheitsabfrage für diese Authentifizierungsanfrage.

3. Das SIW im Browser oder in der nativen Anwendung leitet diese Abfrage basierend auf der Gerät-Benutzer-Bindung per Loopback oder Credential SSO an die Okta Verify-App weiter, die auf dem gleichen Gerät installiert ist.
4. FastPass generiert eine Antwort (mit den entsprechenden Geräteindikatoren) und signiert diese Antwort mit dem privaten Besitznachweis-Schlüssel, den der Benutzer zuvor registriert hatte.
5. FastPass sendet die Abfrageantwort an den Server.
6. Der Okta-Server validiert die Signatur und überprüft, ob die Antwort mit der ursprünglichen individuellen Sicherheitsabfrage übereinstimmt.
7. Der erfasste Gerätekontext wird basierend auf der Okta-Richtlinie evaluiert. Sofern das Ergebnis zufriedenstellend ist, wird der Benutzer angemeldet.

Szenario 3: Benutzerpräsenz und Benutzerverifizierung

Ein Okta-Administrator kann Authentifizierungen so konfigurieren, dass sie einen Nachweis der Benutzerpräsenz und Benutzerverifizierung liefern. Bei Authentifizierungen mit Nachweis der Benutzerpräsenz verlangt FastPass von den Benutzern die Bestätigung, dass sie sich bei der angegebenen Anwendung anmelden möchten. Dazu wird eine Popup-Meldung mit einem Bestätigungs-Button angezeigt. Wenn die Antwort mit dem Besitznachweis-Schlüssel signiert wird, ist ein bestimmter Claim in der Antwort enthalten und zeigt an, dass die Einwilligung des Benutzers gegeben wurde.

Bei der Benutzerverifizierung nutzt Okta Verify die biometrischen Funktionen der Geräte-Hardware (z. B. Touch ID). Wenn biometrische Funktionen nicht unterstützt werden oder gewünscht sind, kann die Benutzerverifizierung auch per Geräte-Passcode oder PIN erfolgen. In jedem Fall wird die Abfrage mit dem relevanten privaten Benutzerverifizierungs-Schlüssel signiert, der im Gerät gespeichert ist. Für den Zugriff auf solche privaten Schlüssel ist der biometrische Benutzerpräsenz-Nachweis mit Plattform-Authentifikatoren wie Touch ID, Face ID, Windows Hello u. a. oder die Eingabe des Geräte-Passcodes erforderlich. Als zusätzliche Überprüfung neben FastPass kann der private Benutzerverifizierungs-Schlüssel sowohl als Besitznachweis als auch der Benutzerverifizierung dienen.

In diesem typischen Ablauf wird die Benutzerverifizierung in Form biometrischer Merkmale abgefragt:

1. Der Benutzer besucht eine von Okta geschützte Ressource und initiiert damit die Authentifizierung.
2. Der Okta-Server erstellt eine individuelle Sicherheitsabfrage für diese Authentifizierungsanfrage.
3. Das SIW im Browser oder in der nativen Anwendung leitet diese Abfrage an die Okta Verify-App weiter, die auf dem gleichen Gerät installiert ist.
4. FastPass fordert den Benutzer zur Angabe seiner biometrischen Merkmale auf. Sobald der Benutzer sie angegeben hat, generiert FastPass eine Antwort mit dem privaten Benutzerverifizierungs-Schlüssel, der zuvor vom Benutzer registriert wurde.
5. FastPass sendet die Abfrageantwort an den Server.
6. Der Okta-Server validiert die Signatur und überprüft, ob die Antwort mit der ursprünglichen individuellen Sicherheitsabfrage übereinstimmt.
7. Der erfasste Gerätekontext wird basierend auf der Okta-Richtlinie evaluiert. Sofern das Ergebnis zufriedenstellend ist, wird der Benutzer angemeldet.

Szenario 4: Authentifizierung mit verwalteten Geräten

In der Enterprise-Welt werden die Geräte der Belegschaft per MDM oder mit einer anderen Endpoint-Management-Software verwaltet. Mithilfe dieses Tools verwaltet der Administrator den Lebenszyklus von Geräten, Software-Installationen, die Geräte-Compliance und weitere Faktoren, mit denen die Sicherheit des Unternehmens gestärkt wird.

Mit Okta können Administratoren festlegen, dass der Zugriff auf Anwendungen nur über verwaltete Geräte zulässig ist. Administratoren können auch in einer Authentifizierungsrichtlinie für Anwendungen festlegen, dass für den Zugriff von einem verwalteten Gerät geringere Sicherheitsvoraussetzungen erforderlich sind als von unverwalteten Geräten.

Dies ist ein typischer Management-Nachweisablauf für ein Desktop-Gerät:

1. Der Benutzer initiiert auf einem verwalteten Gerät den FastPass-Login-Prozess über das Okta SIW.
2. Im Rahmen der Richtlinie fordert der Okta-Server den Management-Nachweis und den Gerätekontext an.
3. Das SIW übergibt die Abfrage an Okta Verify.
4. FastPass generiert eine Antwort mit den Geräteindikatoren und dem Management-Nachweis. Zum Generieren von Management-Nachweisen wird das individuelle Nonce mit dem Zertifikat des Desktop-Geräts signiert. Die Antwort wird ebenfalls mit dem privaten Besitznachweis-Schlüssel signiert, den der Benutzer registriert hatte.
5. FastPass sendet die Abfrageantwort an den Server.
6. Der Okta-Server validiert die Signatur und überprüft, ob die Antwort mit der ursprünglichen individuellen Sicherheitsabfrage übereinstimmt.
7. Der erfasste Gerätekontext und der Management-Status werden basierend auf der Okta-Richtlinie evaluiert. Sofern das Ergebnis zufriedenstellend ist, wird der Benutzer angemeldet.

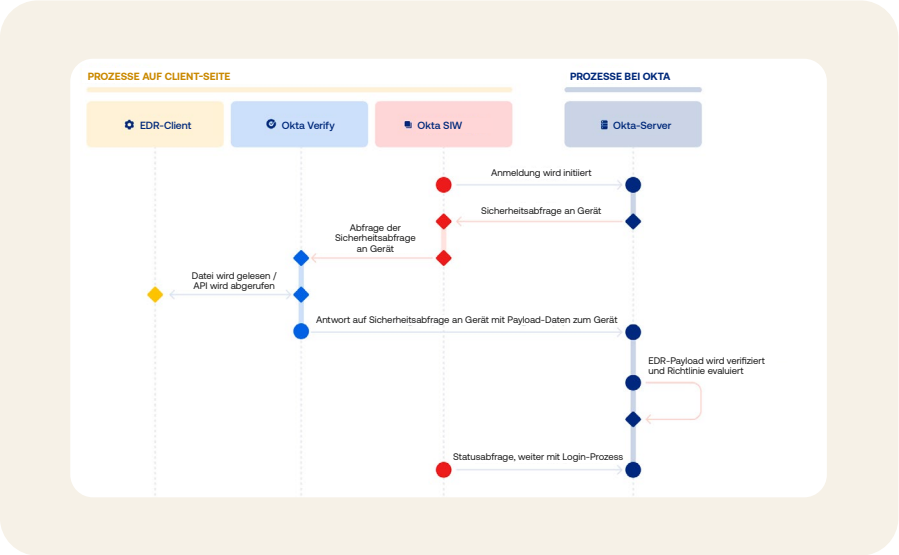
Szenario 5: FastPass-Integrationen

FastPass integriert sich mit Drittanbieter-EDR-Software (Endpoint Detection and Response), um während der Authentifizierung zusätzliche Informationen zur Gerätesicherheit abzurufen. Diese Indikatoren können zum Definieren von Authentifizierungsrichtlinien für Anwendungen herangezogen werden, mit denen der Zugriff auf sensible Ressourcen geschützt wird.

Okta standardisiert mithilfe eines Plugin-Frameworks, wie Endpoint-Sicherheitsintegrationen Indikatoren sicher an Okta übertragen können. Okta unterstützt derzeit Integrationen mit CrowdStrike und Windows Security Center (WSC). Informationen zum Konfigurieren dieser Integrationen finden Sie hier.

Okta unterstützt auch den Chrome Device Trust Connector für sicheren Zugriff auf Okta-geschützte Ressourcen über verwaltete ChromeOS-Geräte und Chrome-Browser unter Windows und macOS. Für diesen Connector ist jedoch weder Okta Verify noch FastPass erforderlich.

Dies ist ein typischer Ablauf, bei dem Endpoint-Sicherheitsindikatoren den Zugriff verhindern:



1. Der Benutzer initiiert den FastPass-Login-Prozess über das Okta SIW.
2. Der Okta-Server antwortet und fragt den Gerätestatus ab.
3. Das SIW übergibt die Abfrage an Okta Verify.
4. Mithilfe der vordefinierten Integrationsmethoden ruft FastPass die erforderlichen Endpoint-Sicherheitsindikatoren von einem EDR-Client ab. FastPass sendet eine Antwort mit den Indikatoren des EDR-Clients und den nativ von FastPass erfassten Indikatoren. Diese werden mit dem privaten Besitznachweis-Schlüssel signiert, den der Benutzer zuvor registriert hatte. Anschließend sendet FastPass die Abfrageantwort zurück an den Server.
5. Der Okta-Server validiert die Signatur und überprüft, ob die Antwort mit der ursprünglichen individuellen Sicherheitsabfrage übereinstimmt. Er überprüft auch die Einzigartigkeit und Authentizität der Endpoint-Sicherheitsindikatoren.
6. Die Endpoint-Sicherheitsindikatoren sowie die weiteren erfassten Gerätekontext-Informationen werden basierend auf der Okta-Richtlinie evaluiert. Sofern das Ergebnis zufriedenstellend ist, wird der Benutzer angemeldet.

Fazit

Okta FastPass ist ein Zero-Trust-Authentifikator, der Benutzern äußerst sichere Login-Optionen bietet. Er bietet umfassenden Schutz mit Phishing-resistenter, passwortloser Authentifizierung, der Zugriffe auch lange nach der ersten Zugriffsanfrage absichert. Durch den Einsatz passwortloser, Phishing-resistenter Authentifizierungsabläufe und Geräteprüfungen gewährleistet FastPass den sicheren Zugriff auf Unternehmensressourcen – bei minimalen Reibungspunkten für Endbenutzer. Mit FastPass können Unternehmen den Gerätekontext nahtlos bewerten, sobald ein Benutzer eine geschützte Ressource öffnet. Das liefert einen zusätzlichen Nachweis der Gerätesicherheit, bevor der Zugriff auf nachgelagerte Systeme gewährt wird. FastPass bietet hohen Benutzerkomfort und eine einheitliche User Experience für alle großen verwalteten und unverwalteten Plattformen oder Geräte.

Dank der umfangreichen Funktionen und der Konzentration auf Sicherheit ist FastPass die ideale Lösung für Unternehmen mit modernen hybriden Belegschaften, die das richtige Gleichgewicht aus Sicherheit und Benutzerkomfort suchen.

Weitere Informationen zu Okta FastPass finden Sie unter www.okta.com/fastpass.

Haftungsausschluss:

Diese Informationen und die darin enthaltenen Empfehlungen stellen keine Rechts-, Datenschutz-, Sicherheits-, Compliance oder Geschäftsberatung dar. Dieses Dokument dient nur zu allgemeinen Informationszwecken und gibt womöglich nicht den aktuellen Stand aller relevanten Fragen wieder. Es liegt in Ihrer Verantwortung, sich mit Blick auf die Rechtslage, den Datenschutz, die Sicherheit, die Compliance und das Business beraten zu lassen. Stützen Sie sich nicht allein auf die enthaltenen Empfehlungen. Okta übernimmt keine Haftung für Verluste oder Schäden, die sich potenziell aus der Umsetzung der Empfehlungen in diesen Materialien ergeben. Okta gibt keine Zusicherungen, Garantien oder sonstigen Zusicherungen in Bezug auf den Inhalt dieser Materialien. Informationen zu den vertraglichen Zusicherungen von Okta an seine Kunden finden Sie unter okta.com/agreements.

Über Okta
Okta ist das weltweit führende Identity-Unternehmen. Als ein führender unabhängiger Identity-Anbieter ermöglichen wir es unseren Partnern und Kunden, jede Technologie sicher zu nutzen – überall, mit jedem Gerät und jeder Anwendung. Die weltweit renommiertesten Marken vertrauen beim Schutz von Zugriff, Authentifizierung und Automatisierung auf Okta. Im Mittelpunkt unserer Okta Workforce Identity Cloud sowie der Okta Customer Identity Cloud stehen Flexibilität und Neutralität. Mit unseren individualisierbaren Lösungen und unseren über 7.000 vorkonfigurierten Integrationen können sich Führungskräfte und Entwickler ganz auf neue Innovationen und eine rasche Digitalisierung konzentrieren. Wir entwickeln eine Welt, in der Ihre Identity ganz Ihnen gehört. Weitere Informationen finden Sie unter okta.com/de.