DATENBLATT

PingID

PingID® ist eine IDaaS-basierte, adaptive Multifaktor-Authentifizierungs(MFA)-Lösung, die eine perfekte Balance zwischen hoher Benutzerfreundlichkeit für den Endbenutzer und einem sicheren Zugriff auf Anwendungen bietet. Unternehmen können mit PingID effiziente Authentifizierungsregeln definieren und durchsetzen, die speziell auf ihre Anforderungen zugeschnitten sind.

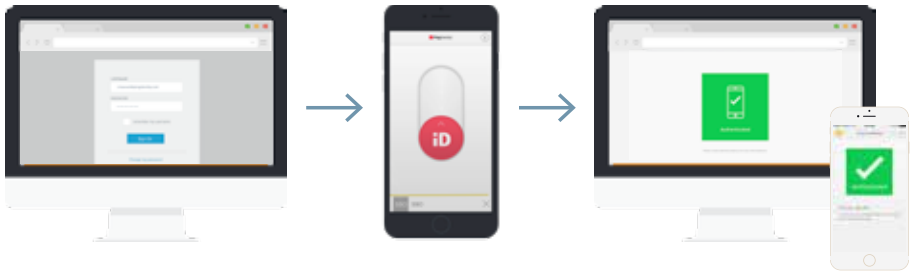
„Eine starke Multifaktor-Authentifizierung gehört zu den wichtigsten Elementen einer Enterprise-IAM-Strategie."

– Forrester

IMPLEMENTIERUNGSOPTIONEN FÜR DIE MFA

Ping bietet zwei Implementierungsoptionen für die MFA: die PingID-App und das PingID-SDK. Bei der PingID-App handelt es sich um eine eigenständige mobile Anwendung für Apple- und Android-Geräte. Meistens kommt sie für Anwendungsfälle mit Mitarbeitern und Partnern zum Einsatz und wird vollständig durch Ping Identity verwaltet. Mit dem PingID-SDK können Sie Multifaktor-Authentifizierungsfunktionen direkt in Ihre eigene mobile Anwendung einbetten. Primär für Kundenszenarien gedacht, unterstützt es mobile Apple- und Android-Apps.

PingID-App für Mitarbeiter und Partner



Funktionsweise

Wenn der Administrator die PingID-App aktiviert, erhält der Benutzer eine Schritt-für-Schritt-Anleitung, um sein Gerät selbstständig zu registrieren. Zunächst muss der Benutzer die PingID-App auf seinem Apple- oder Android-Smartphone oder -Tablet installieren. Als Nächstes scannt er einen QR-Code ein, um sein Gerät zu verbinden. Sobald die Registrierung abgeschlossen ist, kann die PingID-App verwendet werden. Besitzt der User kein Apple- oder Android-Gerät, kann er auch eine Authentifizierung mittels Einmalpasswort wählen, das per SMS, Anruf oder E-Mail kommuniziert wird. Alternativ kann er einen YubiKey-Hard-Token oder die Windows- oder Mac-Desktopanwendungen nutzen. Der PingID-Service erweitert PingOne®, PingFederate®, PingAccess®, Drittanbieteranwendungen, Secure Shell(SSH)-Anwendungen, Windows Login-/RDP- bzw. beliebige RADIUS-konforme VPN-Server oder Remote-Access-Systeme um die adaptive Multifaktor-Authentifizierung.

Die perfekte Balance zwischen Sicherheit und Komfort

Ist eine starke Authentifizierung erforderlich, sendet der PingID-Service über die PingID-App eine Benachrichtigung an das Smartphone des Benutzers. Bei iOS- und Android-Geräten wird diese über den Apple- oder Android-Benachrichtigungsdienst gesendet. Auf diese Weise sind keine SMS oder Anrufe erforderlich. In der Benachrichtigung wird der Benutzer aufgefordert, die PingID-App zu öffnen und über den Bildschirm zu wischen, um sich zu authentifizieren. Die PingID-App bietet auch native Unterstützung für die Apple Watch. Sollte der User kein Signal auf sein Mobiltelefon erhalten können, steht auch ein Offline-Modus zur Verfügung. Hier generiert die PingID-App ein Einmalpasswort. Alternativ kann das Einmalpasswort auch per SMS, Anruf, E-Mail oder Desktopanwendung übertragen werden. In sensiblen Umgebungen oder für Benutzer, die keinen Zugriff auf Smartphones oder andere Geräte haben, ist auch der Einsatz eines YubiKey-Hard-Tokens möglich. Der Registrierungs- und Authentifizierungsprozess ist lokalisiert und dem entsprechenden Branding angepasst. Die Benutzer können ihre vertrauenswürdigen Authentifizierungsgeräte auch selbstständig verwalten.

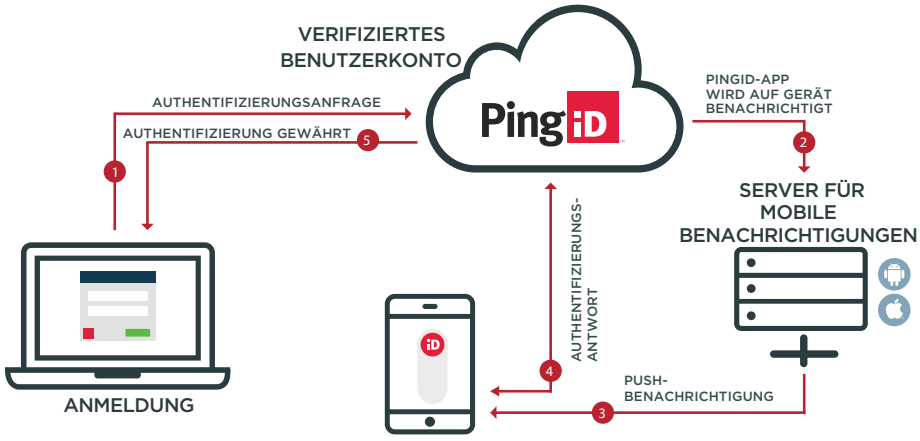
Fingerabdruck als zweiter Faktor

Für eine besonders hohe Benutzerfreundlichkeit können Sie die PingID-App auch so konfigurieren, dass Sie den Fingerabdruckleser auf dem registrierten Gerät nutzen können. Nachdem die Benachrichtigung über die PingID-App an das Smartphone gesendet wird, muss der Benutzer einfach nur den Fingerabdruckleser für die Authentifizierung berühren. Hierbei handelt es sich um ein optionales Feature, das mit dem Apple-Fingerabdrucksensor Touch ID und ausgewählten Android-Geräten funktioniert.

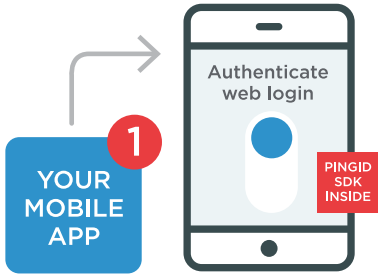
Unterstützung für die adaptive Authentifizierung

Administratoren können erweiterte Regeln für Authentifizierung, Kopplung und Gerätezustand definieren. Hier ein paar Beispiele:

- Beschränkung der MFA auf bestimmte Gruppen, IP-Adressen oder Anwendungen
- Einsatz von Geofencing, um die Aufforderung zur MFA zu vermeiden, wenn sich das Gerät innerhalb einer sicheren Zone befindet.
- Einschränkungen für Geräte, die gerootet oder per Jailbreaking verändert wurden, mittels Root-Erkennung
- Definition von Sitzungen, mit denen Benutzer eine Aufforderung zur MFA vermeiden können, wenn sie innerhalb einer vordefinierten Zeitspanne authentifiziert wurden (Minuten, Stunden, Tage etc.)



PingID-SDK FÜR KUNDEN



FUNKTIONSWEISE

PingID bietet ein mobiles SDK für Apple und Android, mit dem Sie Multifaktor-Authentifizierungsfunktionen nativ in Ihre eigene mobile Anwendung einbetten können. So können Sie Ihren Kunden eine komfortable und sichere MFA ermöglichen, ohne dass sie eine separate Anwendung herunterladen müssen.

VERBESSERUNG BESTEHENDER AUTHENTIFIZIERUNGS-WORKFLOWS

Das PingID-SDK kann Push-Benachrichtigungen senden, um bei Web-, mobilen Web-, Callcenter-, persönlichen sowie hochwertigen Transaktionen oder beliebigen anderen Kundeninteraktionen einen zweiten Authentifizierungsfaktor anzufordern. Auch eine zusätzliche gerätebasierte Autorisierung kann die Sicherheit während der Authentifizierung mit einer mobilen App erhöhen. Das PingID-SDK erhöht die Sicherheit über Ihre native mobile App – ein wichtiger Vorteil, der die Akzeptanz der mobilen App fördert. Das PingID-SDK erweitert Ihren bestehenden Authentifizierungs-Workflow. Kunden, die über Ihre App verfügen, profitieren von zusätzlicher MFA-Sicherheit. Kunden, die diese App nicht haben, müssen sie nicht herunterladen und können stattdessen Ihren bestehenden Authentifizierungsprozess nutzen.

OUT-OF-BAND-WEB-AUTHENTIFIZIERUNG

Mit dem PingID-SDK können Sie die Genehmigung von einem kundendefinierten vertrauenswürdigen Gerät anfordern, wenn ein Kunde versucht, sich in einer Webanwendung anzumelden. Außerdem haben Sie auch die Option einer passwortlosen Authentifizierung: Ihre Kunden müssen dazu nur ihren Benutzernamen eingeben – ihr Passwort wird durch die MFA-Funktionen des PingID-SDK ersetzt.

GENEHMIGUNG VON TRANSAKTIONEN

Für hochwertige Transaktionen können Sie eine starke Out-of-Band-Authentifizierung anfordern. Solche Transaktionen sind zum Beispiel die Überweisung von Geldbeträgen, die Tätigung eines Einkaufs, die Aktualisierung von Kontoinformationen usw. Die Transaktionsinformationen können auch an das vertrauenswürdige Gerät des Kunden gesendet werden, sodass er genau weiß, wofür seine Zustimmung benötigt wird. Die MFA zur Genehmigung hochwertiger Transaktionen kann selektiv, also nur in ausgewählten Fällen, eingesetzt werden. Auf diese Weise können Sie das Sicherheitsrisiko ohne große Auswirkungen auf die Kundenerfahrung erheblich reduzieren.

AUTHENTIFIZIERUNG ÜBER EIN VERTRAUENSWÜRDIGES GERÄT

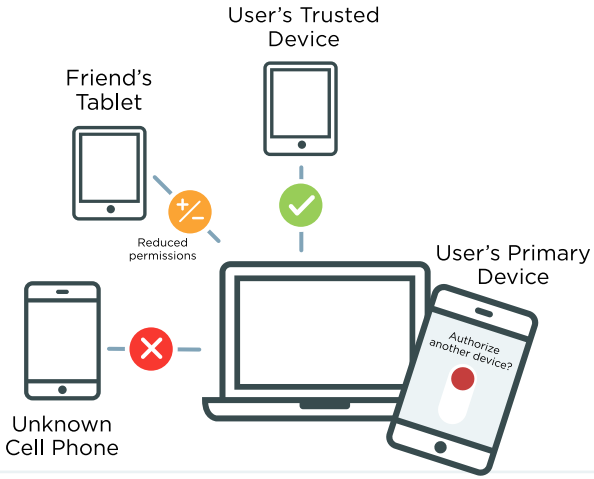
Die Authentifizierung über eine mobile App lässt sich optimieren, wenn Kunden sich von einem vertrauenswürdigen Gerät aus authentifizieren. So profitieren Kunden von einer benutzerfreundlichen, sicheren Mobile-App-Login-Erfahrung, während Hacker daran gehindert werden, sich mittels gestohlener Anmeldedaten von Apps auf nicht vertrauenswürdigen Geräten zu authentifizieren.

NETZWERK VERTRAUENSWÜRDIGER GERÄTE, DAS VOM KUNDEN EIGENSTÄNDIG VERWALTET WIRD

Mit dem PingID-SDK können Ihre Kunden ihr eigenes Netzwerk vertrauenswürdiger Geräte selbstständig verwalten. Zunächst können Kunden ein primäres vertrauenswürdiges Gerät hinzufügen, indem sie sich einfach über Ihre mobile Anwendung authentifizieren. Das Gerät wird ohne weiteres Zutun des Benutzers verbunden. Alternativ können sie ein vertrauenswürdiges Gerät manuell hinzufügen. Dazu brauchen sie nur einen Autorisierungscode, der über einen sicheren, von Ihnen definierten Prozess vermittelt wird. Von ihrem primären Gerät aus können Kunden andere vertrauenswürdige Geräte hinzufügen, ihr primäres Gerät ändern und Geräte mit eingeschränkten Berechtigungen hinzufügen. Mit den APIs des PingID-SDK können Sie Oberflächen in Web- oder mobile Anwendungen einbauen, mit denen Ihre Kunden ihr Netzwerk vertrauenswürdiger Geräte eigenständig verwalten können.

BENUTZERFREUNDLICHES ADMINISTRATIONSPORTAL

Über eine einzige benutzerfreundliche Oberfläche können Sie neue Anwendungen einrichten und verwalten, die das mobile SDK von PingID nutzen, User verwalten sowie Transaktionen und Benutzerberichte ausführen. Ein einziger PingID-SDK-Mandant lässt sich für mehrere mobile Anwendungen nutzen und über ein benutzerfreundliches Administrationsportal verwalten.



DIE PINGID-APP UND DAS PINGID-SDK **IM VERGLEICH**

	PingID-App	PingID-SDK
Primäre Anwendungsfälle	Mitarbeiter und Partner	Kunden
Implementierung	Standalone Ping Identity MFA Mobile App	Benutzerdefiniertes iPhone-/ Android-SDK, das in Ihre eigene mobile Anwendung eingebettet ist
Netzwerk vertrauenswürdiger Geräte, das vom Kunden eigenständig verwaltet wird	Ja	Ja
Genehmigung von Transaktionen	Nein	Ja
Branding/Personalisierung	Personalisierungsoptionen	Umfassende Personalisierung
Authentifizierung über ein vertrauenswürdiges Gerät	Ja	Ja
Geräte mit eingeschränkten Berechtigungen	Nein	Ja
Service-APIs	Öffentliche Web-APIs	Server: öffentliche REST-APIs Mobil: mobile SDK-APIs
SMS, Anruf, E-Mail, Desktop und YubiKey als Alternativen zur Authentifizierung über eine mobile App	Ja	Nein
Integration von Unternehmensanwendungen	Ja	Nein
Out-of-the-Box-Flows für die Registrierung und Authentifizierung	Ja	Beispiel-App

Weitere Informationen zu PingID erhalten Sie unter pingidentity.com.