Entrust Datacard®
sms|passcode

Aufbruch in neue Dimensionen jenseits von Cloud-Adoption

– machen Sie sich startklar für die 4. Generation der Benutzerauthentifizierung

SMS PASSCODE 2020

Für eine passwortfreie Zukunft, mit Smart-Login für nahtlosen Zugriff auf Windows, macOS und alle Ihre Anwendungen

BEWÄHRT Mit mehr als 25 Jahren Erfahrung in der identitätsbasierten Sicherheit

VISIONÄR führen wir Sie über MFA hinaus zu Identitätssicherung

MÜHELOS und ermöglichen Ihnen, alle Ihre Benutzer, Anwendungen und Umgebungen mit einer einzigen flexiblen Plattform mühelos zu sichern

SMS PASSCODE Authentifizierung

Die SMS PASSCODE MFA-Lösung ist seit mehr als 15 Jahren eine führende Technologie in der adaptiven Multi-Faktor-Authentifizierung (MFA). Nun ist sie Vorreiter bei der nächsten Generation einer Authentifizierung, die noch intelligenter und benutzeroptimierter ist und mit der Sie Remote-Zugriffe noch sicherer machen, ohne dass die Benutzerfreundlichkeit darunter leidet.

Mit einer Erfolgsgeschichte von Tausenden von Installationen weltweit und vier Jahren im Gartner Magic Quadrant wissen wir, was zum Schutz Ihrer Systeme und Cloud-Anwendungen erforderlich ist. Dabei ist es egal, ob sich Ihre Benutzer von Aarhus, New York, Berlin oder Bangalore aus anmelden. Durch die dynamische Authentifizierung von Benutzern anhand von Ortung und Mustern beim Anmeldeverhalten helfen wir IT-Managern, mit Cloud-Anwendungen und mobiler Sicherheit auf sich ändernde Geschäftsanforderungen zu reagieren.

Die 4. Generation der Benutzerauthentifizierung ist da!

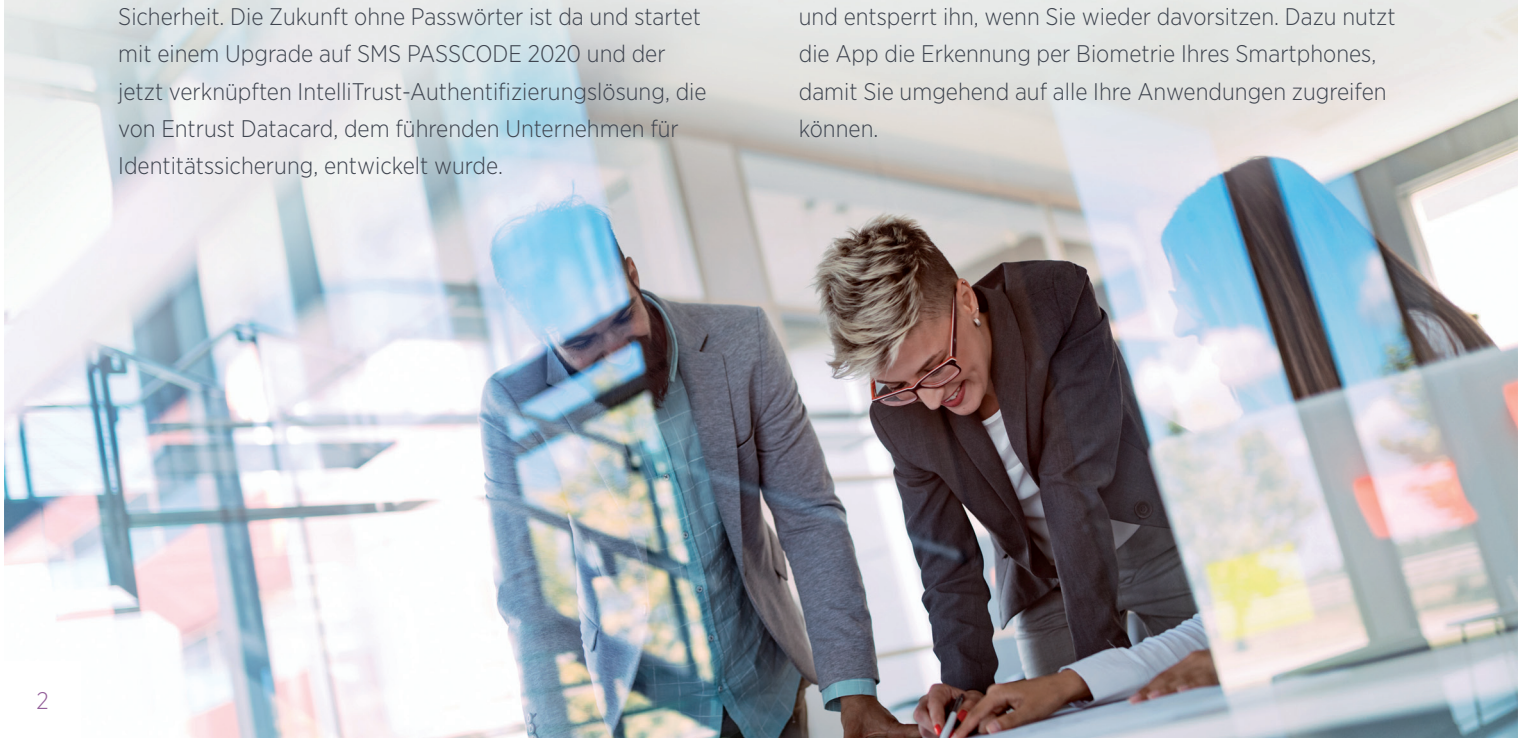
Niemand gibt gerne sein Passwort 50 Mal am Tag ein und immer daran denken zu müssen, den Computer zu sperren, wenn man seinen Schreibtisch verlässt, ist ebenfalls lästig. Stellen Sie sich vor, wie es Ihren Arbeitstag beeinflussen würde, wenn eine App auf Ihrem Smartphone Ihnen diese beiden täglichen Lästigkeiten nähme.

Entrust Datacard hat die IntelliTrust Smart-Login-App entwickelt, die diese beiden Ärgernisse beseitigt. Mit dieser zertifikatsbasierten App müssen Sie Ihr Passwort nie wieder eingeben. Trotzdem stärkt diese deutliche Verbesserung der Benutzerfreundlichkeit auch Ihre digitale Sicherheit. Die Zukunft ohne Passwörter ist da und startet mit einem Upgrade auf SMS PASSCODE 2020 und der jetzt verknüpften IntelliTrust-Authentifizierungslösung, die von Entrust Datacard, dem führenden Unternehmen für Identitätssicherung, entwickelt wurde.

Innovation angetrieben durch **weltweit führende Unternehmen**

Entrust Datacard hat den Raketenantrieb seines Authentifizierungsangebots mit einer sicheren und mühelosen Alternative entzündet, die über die herkömmliche Multi-Faktor-Authentifizierung hinausgeht: Entrust Datacard hat eine App-basierte Lösung entwickelt, die die Benutzeranmeldung jenseits der Cloud bringt. Die IntelliTrust Smart-Login-Lösung bietet eine mühelose und sichere Anmeldung von einem Smartphone aus.

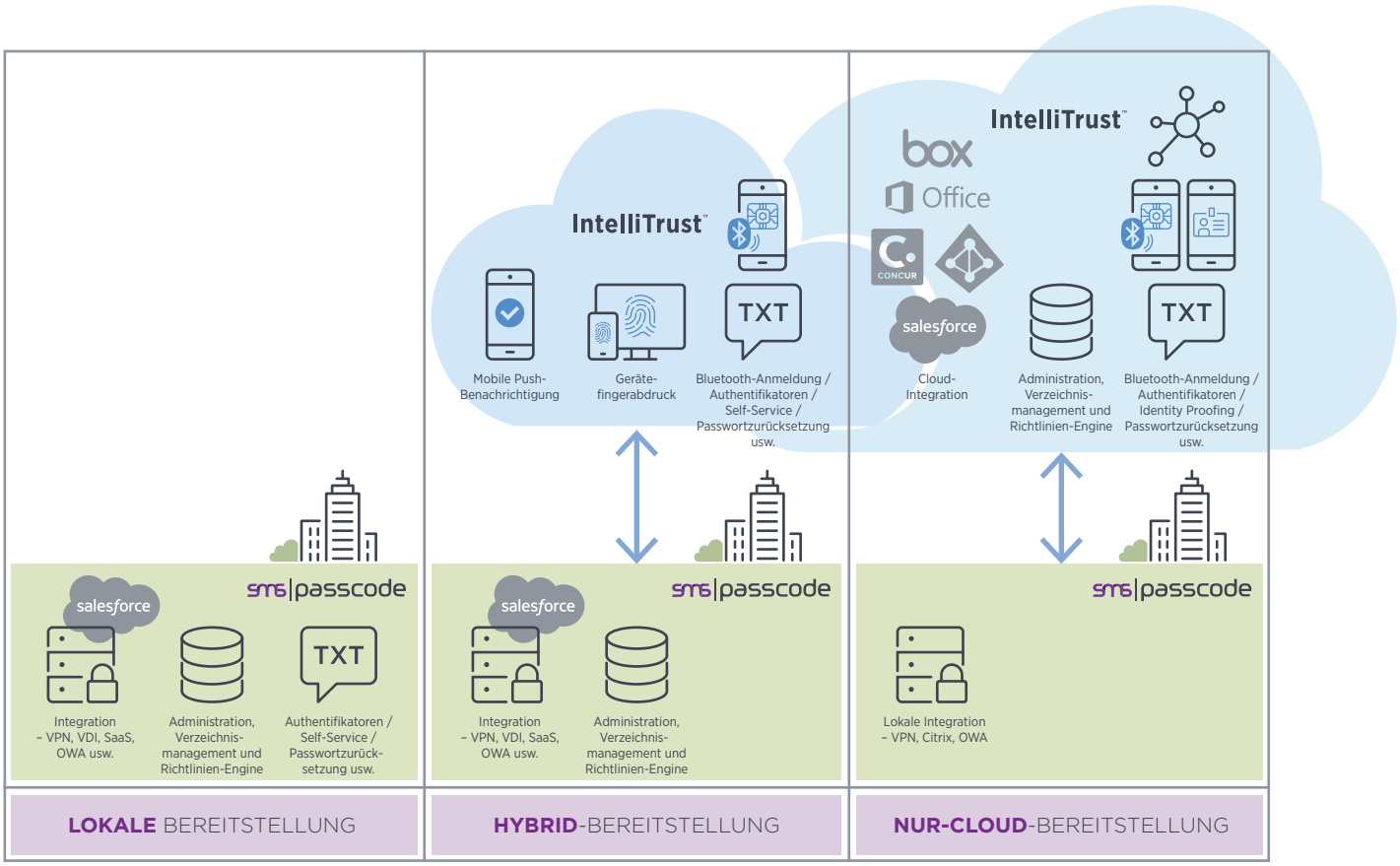
Bei Verwenden der zertifikatsbasierten App sperrt das Telefon den Computer automatisch, wenn Sie ihn verlassen, und entsperrt ihn, wenn Sie wieder davorsitzen. Dazu nutzt die App die Erkennung per Biometrie Ihres Smartphones, damit Sie umgehend auf alle Ihre Anwendungen zugreifen können.



Gerät ein Hacker an das Passwort eines Mitarbeiters, steht ihm praktisch alles offen, worauf der Mitarbeiter Zugriff hat – in der Cloud und lokal. Und da die meisten Unternehmen mehr Cloud-Dienste für Dateisysteme, Intranet oder auch zur Zusammenarbeit nutzen, liegen jetzt noch mehr Daten offen.

Glücklicherweise ist eine starke Benutzerauthentifizierung für Benutzer und Administratoren heute mit weniger Aufwand verbunden als früher. Und mit dieser 11. Hauptversion von SMS PASSCODE können Sie Ihre Cloud nach Belieben nutzen – ohne Passwort und mit einem Smart-Login für Windows 7, 8, 10 und macOS. Die Zukunft ist da – jenseits der Cloud!

SMS PASSCODE 2020 ermöglicht Ihnen, Ihre Cloud nach Belieben zu nutzen – mit der nahtlosen Integration unserer IntelliTrust Cloud Authentication™



Lokale Authentifizierung, Hybrid- oder Full-Cloud-Adoption

Seit der Übernahme von SMS PASSCODE durch Entrust Datacard im Juli 2018 wachsen wir weiter und fügen neue Funktionen hinzu. Mit SMS PASSCODE 2018 haben wir eine hybride Authentifizierungslösung eingeführt, die die lokale Authentifizierung mit unseren Cloud-Services für SMS, Voice und App kombiniert.

In diesem Jahr stellen wir die Integration von IntelliTrust vor. Die preisgekrönte Cloud-Authentifizierungslösung von Entrust Datacard macht bereits Tausende von Authentifizierungen täglich möglich: Cloud-zu-Cloud mit OpenID Connect, passwortfrei und damit benutzerfreundlich, mit einer leicht konfigurierbaren Risiko-Engine für intelligente Authentifizierung und schließlich Bluetooth Unlock/Lock für die beste Arbeitsplatzsicherheit, die es je gab – das ist Identitätssicherung für Anmeldungen der Zukunft, im Büro und in der Cloud.

Lizenzoptionen – was ist enthalten?

Mit SMS PASSCODE 2018 führten wir ein Abonnementpaket ein, das unter anderem Dienste für die OTP-Zustellung per SMS, Voice Call und App sowie Support beinhaltet. Mit SMS PASSCODE 2020 gibt es noch mehr Gründe, sich für das Abonnement zu entscheiden – die Lizenz des Cloud- und Servicezeitalters.

Im Rahmen einer SMS PASSCODE-Abonnementlizenz erhalten Sie sichere und benutzerfreundliche IntelliTrust-Authentifizierungsfunktionen – entweder in einer Hybridlösung oder als vollständige Cloud-Lösung.

	Software Assurance	Abonnement-paket
SMS PASSCODE-Erweiterungen	●	●
Unterstützung von Windows Server 2019	●	●
Gerätefingerabdruck mit AD FS (IntelliTrust)	●	●
Push-Authentifizierung (IntelliTrust)	●	●
IntelliTrust „One Enterprise“, einschließlich Risiko-Engine, Cloud-zu-Cloud-Authentifizierung usw.		●
ActiveSync-Gerätebereitstellung für Office365 und On-Premise Exchange	●	●
Weltweite OTP-Zustellung per SMS App und Voice Call		●
IntelliTrust Single-Sign-Portal für alle Cloud-Services an einem geschützten Ort		●
SMS PASSCODE-Support während der Geschäftszeiten (kann ausgeweitet werden)		●
Smart-Login mit Bluetooth und zertifikatsbasierter Authentifizierung*		●

** Bis 31. März 2020 ist Smart-Login für neue Kunden im SMS PASSCODE-Abonnement enthalten.*

Eine Liste mit Funktionen von SMS PASSCODE 2020 finden Sie auf der Rückseite dieser Broschüre.
Weitere Informationen über IntelliTrust finden Sie im Internet unter intellitrust.entrustdatacard.com.

Drei neue sichere und einfache Möglichkeiten der Authentifizierung

Neben der Unterstützung von Windows 2019 und anderen Verbesserungen der Plattform enthält SMS PASSCODE 2020 zwei neue Authentifizierungsoptionen für Software-Assurance-Kunden und eine zusätzliche Option für die Kunden, die auf unser Abonnementmodell umgestellt haben oder umstellen werden. Nähere Informationen finden Sie im Kasten auf der vorigen Seite.

Durch die drei neuen Funktionen, die alle von IntelliTrust™ stammen, können Mitarbeiter sicher auf Workstations, Netzwerke und Anwendungen zugreifen, ohne bei jeder Sitzung wieder und wieder ihr Passwort eingeben oder sich mit den üblichen Zwei-Faktor-Methoden authentifizieren zu müssen.. Identitätssicherung per Bluetooth-Anmeldung, Gerätefingerabdruck-Authentifizierung und mobile Push-Authentifizierung bieten Benutzern ein reibungsloses und sicheres Anmelde-Erlebnis ohne Passwort.

AUTHENTIFIKATOREN

SMS	FLASH-SMS	Sichere E-mail	Voice-Call	SMS PASSCODE APP (verschlüsseltes OTP)	Google Authenticator	YubiKey-Unterstützung	OATH OTP Token-Unterstützung

DIE DREI NEUEN INTELLITRUST-AUTHENTIFIZIERUNGSFUNKTIONEN
FÜR SMS PASSCODE-KUNDEN:

Gerätefingerabdruck
für einen sicheren, nahtlosen Zugriff auf Cloud-Anwendungen

Mobile Push-Benachrichtigung
App-Authentifizierung, mit Unternehmens-Branding

Zertifikatsbasierte
Authentifizierung über Bluetooth-Verbindung mit Ihrem Desktop

Gerätefingerabdruck als zusätzliche Sicherheitsschicht – oder als Alternative zu OTP
Beim Zugriff auf Cloud-Anwendungen über AD FS ist eine neue Gerätefingerabdruckoption verfügbar. Diese Option ermöglicht die automatische Erkennung eines zuvor verwendeten Geräts, sodass One-Time-Passcodes (OTPs) umgangen werden können. Bei der Verwendung der IntelliTrust Risiko-Engine kann diese Option auch als ein zu berücksichtigender Faktor angesehen werden. Andere Faktoren können u. a. Ortung, IP-Adresse, Anmeldezeitpunkt oder Reisegeschwindigkeit sein.

Mobile Push-Authentifizierung
SMS PASSCODE 2020 unterstützt jetzt auch Push-Authentifizierung mit einer Entrust-App, die Unternehmen mit eigenem Branding versehen können. Diese bietet biometrische Sicherheit mithilfe der biometrischen Erkennung auf dem eigenen Smartphone, um unbefugten Zugriff zu verhindern (oder um zu verhindern, dass Ihre Kinder dem Hacker versehentlich Zugriff gewähren ...). Außerdem müssen Benutzer über Schaltflächen wie „Bestätigen“, „Ablehnen“ und „Problem“ zusätzlich agieren. Probleme werden erfasst und ein Bericht an einen Administrator gesendet.

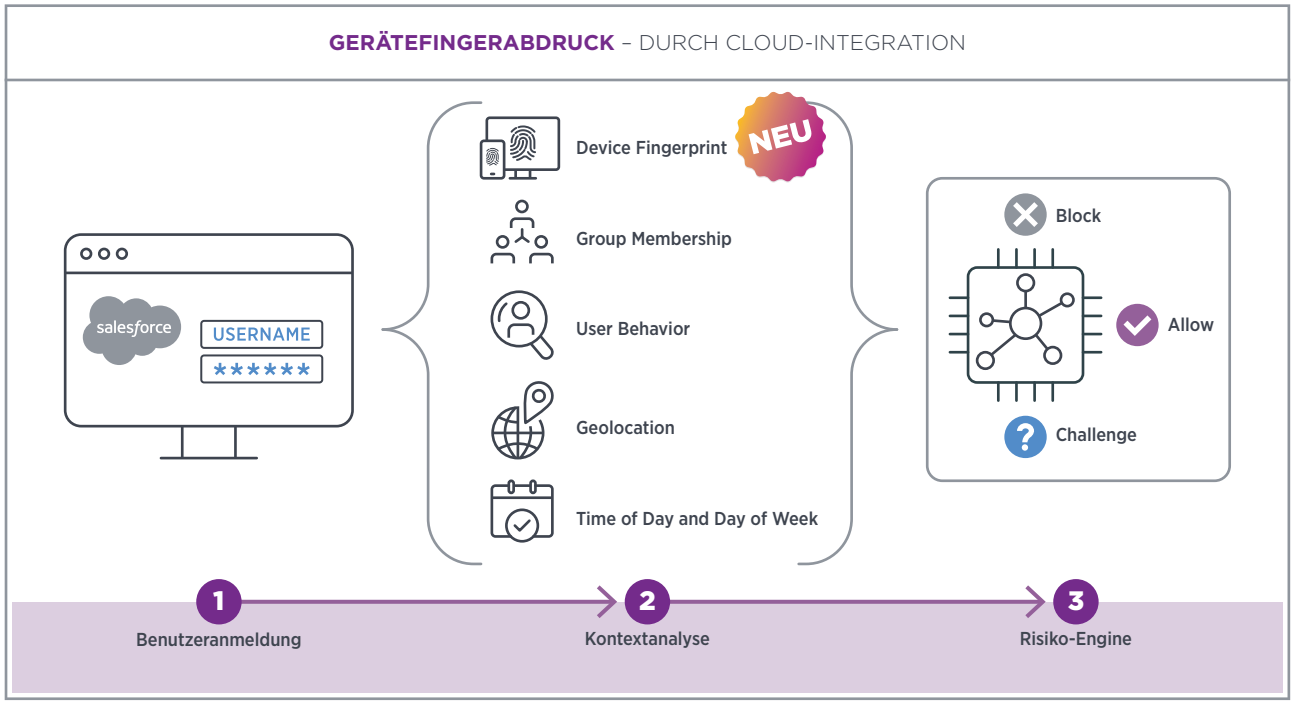
Bluetooth-Desktop-Smart-Login mit Microsoft- oder Entrust-PKI-Zertifikaten
Bei Verwenden von Smart-Login kann das Smartphone den Computer automatisch sperren, wenn Sie ihn verlassen, und entsperren, wenn Sie zurückkehren – verwenden Sie einfach FaceID/TouchID oder ein Android-Äquivalent. Das Microsoft- oder Entrust-Zertifikat bietet Identitätssicherheit auch über die Desktop-Anmeldung hinaus. Schon beim einfachen Öffnen einer Cloud-Lösung sind Sie authentifiziert – Passwörter gehören der Vergangenheit an und wir sorgen gleichzeitig für mehr Sicherheit und Benutzerfreundlichkeit.

Sichere, aber leichtere Anmeldung
mit verbesserten Kontextinformationen

Mehr als 80 % aller unbefugten Netzwerkzugriffe gehen auf die Rechnung von Hackern, die schwache oder gestohlene Benutzerdaten nutzen. Wenn Sie Ihre Dienste mit MFA ausstatten, erhöhen Sie die Sicherheit erheblich, denn damit entledigen Sie Hackern ihrer bevorzugten Waffe.

Um eventuelle Bedenken Ihrer Benutzer zu zerstreuen, sollten Sie sich unsere Funktionen für adaptive bzw. Authentifizierung auf Basis von Kontextinformationen ansehen – Tausende Unternehmen konnten damit bereits den Bedienkomfort für ihre Anwender verbessern SMS PASSCODE war Wegbereiter der adaptiven Authentifizierung, bei der die Anmeldung kontextabhängig erfolgt, egal ob der Benutzer beispielsweise über VPN, Citrix, RDP oder Cloud-Services angemeldet ist.

Der Gerätefingerabdruck ist das neueste Feature. Dieses liefert bei der Validierung des Geräts mehr Sicherheit als die früher bei der Anmeldung verwendeten Authentifizierungscookies.



Sowohl mit SMS PASSCODE als auch mit IntelliTrust bleiben Ihnen wiederholte und frustrierende Anmeldungen erspart. Unsere einfach zu konfigurierende Engine erkennt anhand von Kontextdaten und Benutzerverhalten Risiken in Echtzeit.

ActiveSync-Schutz – ohne Mobile-Device-Management

ActiveSync – das Protokoll zur einfachen Synchronisation von E-Mails, Kontakten usw. stellt ein oft übersehenes Sicherheitsrisiko dar. Wenn ein Benutzer den Zugriff auf wichtige Informationen mit nur einer E-Mail-Adresse und einem Passwort einfach einrichten kann, dann kann das auch der Hacker … Und wenn Sie OWA/Office365 mit MFA schützen, sollten Sie ActiveSync nicht vergessen.

ES GIBT **VORNEHMLICH DREI MÖGLICHKEITEN,** UM AUF OFFICE 365/OWA-INHALTE ZUZUGREIFEN

Der Outlook-Client auf dem PC/Mac 50 % der Zeit für E-Mails aufgewendet	**ActiveSync** über iPhone/Android/Tablet 40 % der Zeit für E-Mails aufgewendet	**Browser** Office.com oder OWA 10 % der Zeit für E-Mails aufgewendet

SMS PASSCODE führte 2014 die ActiveSync-Gerätebereitstellung für On-Premise Exchange ein. Inzwischen wurde es für Exchange Online/Office365 zur Verfügung gestellt.

Diese Funktion bietet keine vollständige MDM-Lösung, wenn Sie ein Tool zum Rollout von Apps und zur Verwaltung von Unternehmensgeräten benötigen. Es bietet jedoch die entscheidende Sicherheitsfunktion, um das Onboarding auf neuen mobilen Geräten zu schützen und die E-Mail-Synchronisierung zu ermöglichen.

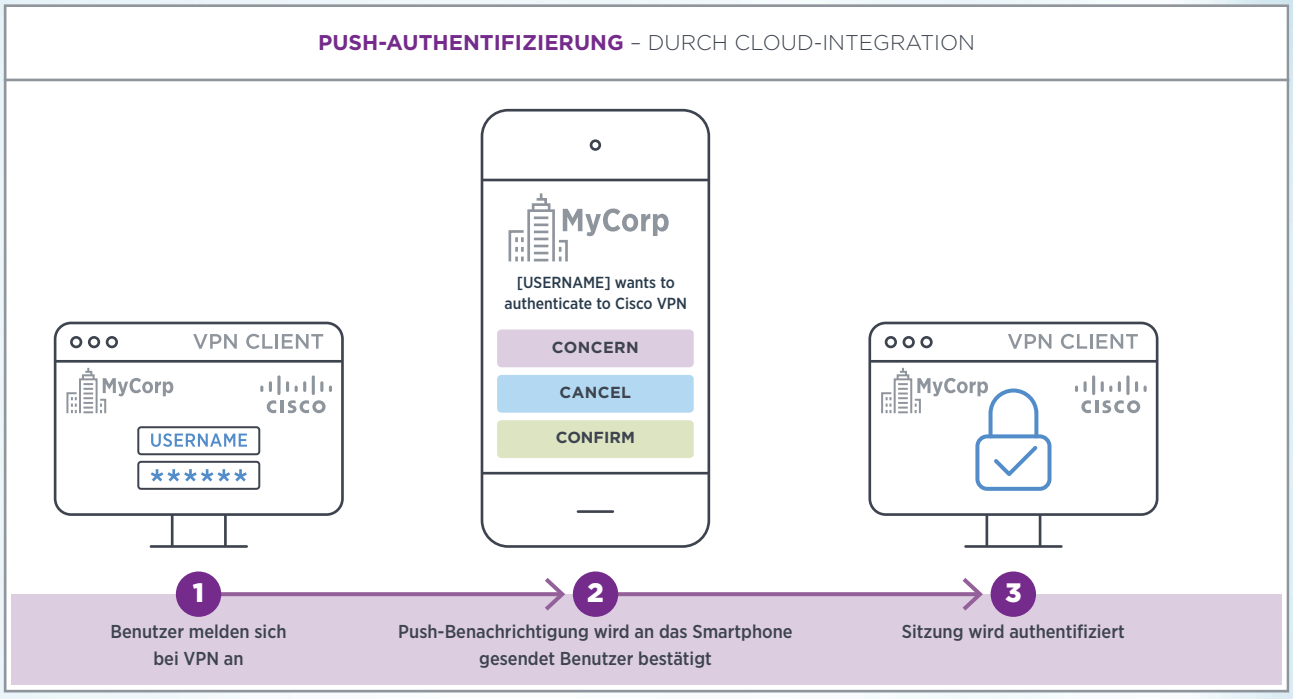
Mit dieser Funktion können Benutzer ihre neuen (privaten) Smartphones einbinden und nutzen und mobile E-Mails so nutzen, wie sie es möchten. Eine einfache, sichere und dennoch leistungsstarke Self-Service-Option, die funktioniert!

Mobile Push-Authentifizierung

SMS PASSCODE 2020 beinhaltet Push-Authentifizierung für den Zugriff über VPN/Citrix (Radius) und AD FS. Ist die Funktion aktiviert, müssen Benutzer auf die auf dem mobilen Bildschirm angezeigte Meldung aktiv reagieren und eine Auswahl treffen: „Problem“, „Abbrechen“ oder „Bestätigen“.

Durch Drücken der Taste „Problem“ wird der Zugriff gesperrt, der Benutzer aber auch im System angemeldet, damit der Administrator die Angelegenheit prüfen kann.

Um die unbefugte Nutzung der mobilen App zu unterbinden oder um zu verhindern, dass ein Benutzer selbst versehentlich einem Hacker Zugriff gewährt, können eine biometrische Validierung hinzugefügt (z. B. Touch/FaceID) und auch Kontextinformationen in der App angezeigt werden (z. B. Anmeldeversuch vom Hilton Hotel in Bangkok, Thailand).



Die App funktioniert sowohl für Android als auch für iOS und ist in zwei Versionen erhältlich – mit und ohne Zertifikatsfunktionen.

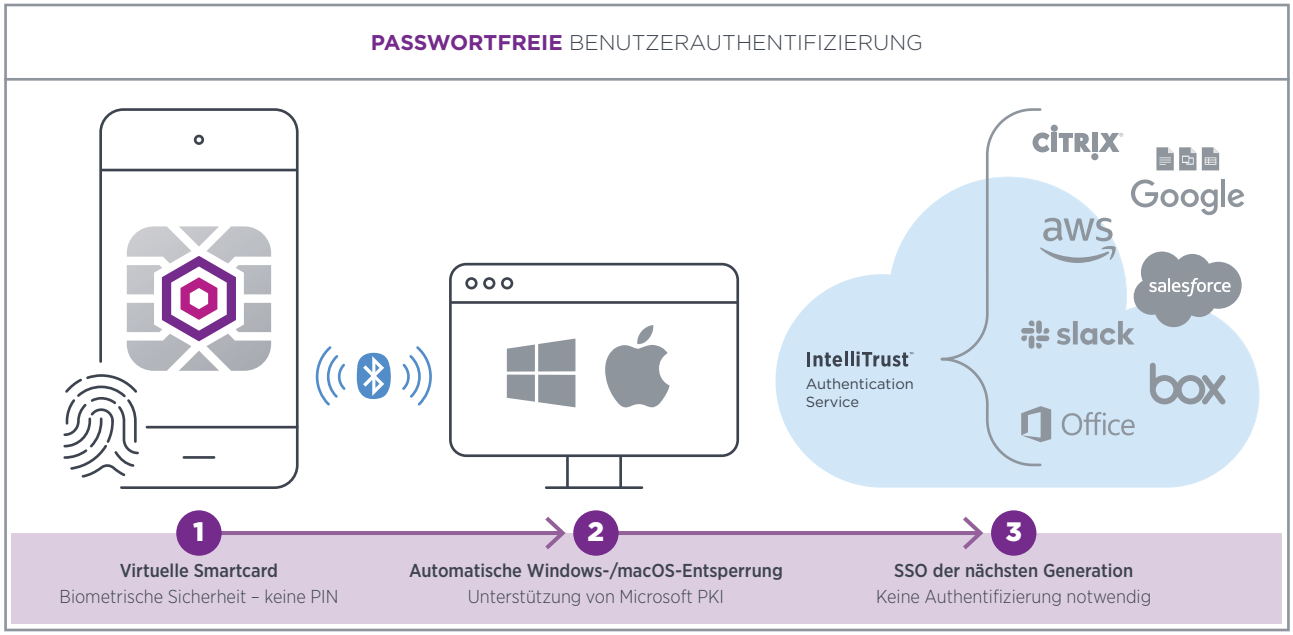
„Push to Authenticate“ ist eine großartige Funktion für IT-affine Benutzer. Optionen wie SMS/Text oder Voice-Call, die keine Installation und Einrichtung auf dem Smartphone erfordern, stellen aber immer noch eine effektive Lösung für viele mobile Mitarbeiter und eine weniger technisch versierte Zielgruppe.

Die 4. Generation der Benutzerauthentifizierung ist Smart-Login – passwortfreier Zugriff auf Desktop- und Cloud-Anwendungen

Die Multi-Faktor-Authentifizierung bietet seit vielen Jahren zusätzlich zu Passwörtern eine notwendige Sicherheitsschicht. Unsere Welt hat sich jedoch sowohl in technologischer Hinsicht als auch in puncto Cyberbedrohung weiterentwickelt. Das führt bei der traditionellen MFA zu Problemen. Erstens erwarten wir als Benutzer mittlerweile, dass wir umgehend Zugriff auf Daten und Anwendungen haben, und MFA sorgt da für mehr „Reibung“ und Frust. Durch die Eingabe von OTP-Codes oder das Mitführen von USB-Schlüsseln verringert MFA nicht nur die Produktivität. Wenn Sie Ihren USB-Schlüssel verlieren oder der Akku Ihres Hardware-Tokens leer ist, können Sie nicht mehr arbeiten. Zweitens finden Hacker immer öfter Wege, um bestimmte MFA-Methoden zu umgehen und verursachen so kostspielige Schäden.

Der Smart-Login von Entrust Datacard löst die größten MFA-Probleme mit einem Ansatz, der die Sicherheit maximiert und für Benutzer mühelose Bedienung bringt. Die Sicherheitsleistung digitaler Zertifikate und der Komfort des Mobiltelefons machen es möglich. Wir bieten fortschrittliche Lösungen, die für Endanwender einfach sind.

Dank Smart-Login können sich Mitarbeiter ganz einfach mit Ihrem Smartphone an ihrem Arbeitsplatz und bei ihren Anwendungen anmelden. Keine Passwörter mehr und keine Zwei-Faktor-Authentifizierung (2FA) mehr mit Wissensfragen, Einmalpasscodes (OTPs) oder Grid-Karten usw. So können Benutzer schnell und einfach auf ihren Computer und ihre Anwendungen zugreifen und mit mehr Produktivität und weniger Sicherheitshürden und Frust arbeiten. Außerdem müssen Mitarbeiter nicht mehr daran denken, ihre Arbeitsplätze zu sperren, da die Funktion sie beim Weggehen automatisch abmeldet.



Lösungshighlights

Nahtlose Integration: Die SMS PASSCODE MFA-Plattform lässt sich nahtlos in Anmeldesysteme und Cloud-Lösungen integrieren und ermöglicht so einen intuitiven und benutzerfreundlichen Remote-Zugriff.

Adaptive Authentifizierung: Kombinieren Sie hohe Sicherheit und Benutzerfreundlichkeit mit einer Lösung, die den Authentifizierungsgrad automatisch an die aktuelle Situation des Benutzers anpasst.

Automatischer Failover: Es ist möglich, hochflexible Failover-Mechanismen einzurichten, um sicherzustellen, dass die OTPs immer ankommen. Die Lösung kann sogar zwischen den Übertragungsarten wechseln, je nach aktuellem Anmeldekontext des Benutzers.

Umfassende Verzeichnisunterstützung: Benutzer können aus Active Directory und allgemeinen LDAP-Verzeichnissen wie OpenLDAP oder AD LDS synchronisiert werden. Benutzer können durch Auswahl einer bestimmten Benutzergruppe oder mithilfe eines LDAP-Filters importiert werden.

Echtzeitschutz: Alle OTP-Codes werden zum Zeitpunkt der Anmeldung in Echtzeit generiert. Es gibt keine vorab ausgegebenen Passcodes oder Seed-Dateien, die gehackt werden könnten. Gleichzeitig ist Echtzeit eine Voraussetzung für die Bereitstellung sitzungsspezifischer OTPs.

PowerShell: SMS PASSCODE MFA unterstützt PowerShell. Administratoren können PowerShell-Skripting verwenden, um rollenbasierten Zugriff zu erstellen, in andere Systeme zu integrieren oder tägliche Aufgaben wie die Überprüfung der Lizenzverfügbarkeit oder länderspezifische Anmeldungen zu automatisieren.

Statusrückmeldung: SMS PASSCODE MFA bietet eine konkurrenzlose Statusrückmeldung, die es dem Benutzer ermöglicht, den Fortschritt der Anmeldung zu verfolgen. Statusrückmeldungen schaffen Vertrauen und reduzieren die Anzahl von Helpdesk-Anfragen.

Kenntnisse über Standort und Verhalten: SMS PASSCODE MFA nutzt die Vorteile von kontextbezogenen Informationen wie Muster beim Anmeldeverhalten und Ortungsdaten, um den Benutzerzugriff einfacher und effizienter zu gewähren oder zu verweigern. Geofencing ermöglicht Administratoren die Erstellung von White- und Blacklists basierend auf Systemen und Standorten. Dazu zählt beispielsweise der eingeschränkte Zugriff über Citrix NetScaler aus bestimmten Ländern.

Secure Device Provisioning: Mit dieser Funktion können Benutzer schnell und einfach neue ActiveSync-Geräte selbst registrieren, ohne die Sicherheit zu gefährden und ohne sich für Unterstützung an den Helpdesk wenden zu müssen.

OTP-Bereitstellungsmethoden: Mit Plug-ins und standardmäßigen OTP-Bereitstellungsmethoden wie Apps, SMS, Voice-Call, sicheren E-Mails, Cloud-Schlüsseln und Hard-/Soft-Token kann SMS PASSCODE MFA Ihre Geschäftsanforderungen jetzt und in Zukunft unterstützen.

Erweitertes Datenbank-Auditing: SMS PASSCODE MFA verfügt über erweiterte Auditfunktionen, die Kunden dabei unterstützen, strenge Branchenvorschriften einzuhalten und Anforderungen der Auditkontrolle zu erfüllen.

Mobile Push-Authentifizierungs-App mit Ihrem eigenen Branding: Fügen Sie ein benutzerfreundliches Sicherheitsniveau hinzu, wenn sich Mitarbeiter zu einem ungewöhnlichen Zeitpunkt oder an einem ungewöhnlichen Ort anmelden möchten. Sofern dem Benutzer der Zugriff erlaubt ist, wird vor der Zugriffserteilung eine Benachrichtigung auf dem Mobiltelefon angezeigt, mit der der Benutzer zur Bestätigung aufgefordert wird (Biometrieoption).

Gerätefingerabdruck: Nach erfolgreicher Anmeldung bei einem Cloud-Dienst über AD FS kann ein Gerätefingerabdruck erfasst und für zukünftige Bewertungen der Anmeldesicherheit verwendet werden. Auf diese Weise wird in der Regel eine einfachere Anmeldung ermöglicht.

Bluetooth-Anmeldung für Windows und macOS + zertifikatsbasierte Authentifizierung: Die App sperrt den Computer automatisch, wenn Mitarbeiter ihn verlassen, und entsperrt ihn, wenn sie zurückkehren. Darüber hinaus kann das Zertifikat für die Cloud-Authentifizierung verwendet werden, sodass keine Passwörter für Desktop und Cloud mehr erforderlich sind.

Schützen Sie Ihre Systeme und Anwendungen

Nachfolgend finden Sie eine Liste mit den von uns unterstützten Systemen.

Barracuda

Check Point SOFTWARE TECHNOLOGIES LTD.

cisco

CITRIX ShareFile

CITRIX

Cyberoam A SOPHOS Company

f5

Google apps

JUNIPER NETWORKS

Microsoft

Office 365

OPENVPN

Outlook Web Access

paloalto NETWORKS

salesforce

SharePoint Online

Teldat

vmware

Unterstützte Systems

SMS PASSCODE unterstützt eine Vielzahl von Anmeldesystemen für den Remote-Zugriff. Die Plattform ist so konzipiert, dass sie sich nahtlos in Hunderte von VPNs integrieren lässt und einen sicheren und intuitiven Anmeldeprozess ermöglicht.

Nachfolgend finden Sie eine Liste mit Beispielen für unterstützte Remote-Zugriffssysteme.

RADIUS VPN/SSL VPN Clients

- Check Point
- Cisco ASA
- Citrix Netscaler (Citrix ADC/Citrix Gateway)
- Juniper
- Pulse Secure
- Barracuda SSL VPN und NG firewalls
- VMware Horizon View
- Netop Remote Control
- Palo Alto
- F5 BIG-IP
- NCP VPN
- Weitere RADIUS clients (Challenge/Response)

Windows Logon, Remote Desktop Services

Unterstützung der folgenden Server und Dienste:

- Remote Desktop Services (RDP-Verbindungen)
- Windows Servers 2008 R2 / 2012 / 2012 R2 / 2016 / 2019
- Windows 7, Windows 8, Windows 8.1 und Windows 10
- VMware Virtual Desktop Portal & Client Access

Microsoft AD FS Schutz

- AD FS 2.0 plug-in for Multi-Factor-Authentifizierung
- AD FS 3.0/4.0/5.0 Adapter for Multi-Factor-Authentifizierung

Multi-factor-Authentifizierung für:

- Zugriff auf Cloud-Anwendungen wie Salesforce.com, Microsoft Office 365, Google Apps usw. (AD FS 3.0/4.0/5.0)
- Zugriff auf Websites, die über Microsoft Web Application Proxy (AD FS 3.0/4.0/5.0) veröffentlicht werden, z. B. Outlook Web Access
- Zulassung von Geräten in Verbindung mit Arbeitsplatzverknüpfungen (AD FS 3.0/4.0/5.0)

Internet Information Services (IIS) Websites

Unterstützung folgender Arten von Websites:

- Outlook Web Access 2010 / 2013 / 2016 / 2019
- Remote Desktop Web Access (Windows Server 2008 R2 / 2012 R2 / 2016 / 2019)
- Websites mit einfacher oder integrierter Windows-Authentifizierung

Secure Device Provisioning

Schutz für ActiveSync-Geräte und die folgenden Systeme:

- Exchange 2010
- Exchange 2013
- Exchange 2016
- Exchange 2019
- Exchange Online

(1) Der Schutz von SharePoint mithilfe von RADIUS wird nur unterstützt, wenn der SharePoint Portal-Server über ein Application Gateway veröffentlicht wird. So wird sichergestellt, dass sich der Benutzer bei erstmaliger Anmeldung nur einmal authentifizieren muss. Zum Beispiel mit dem Citrix Netscaler, der für die Verwendung von permanenten Cookies konfiguriert ist.

Entrust Datacard A/S
Park Allé 350 D, DK-2605 Brøndby

Phone: +45 70 22 55 33

www.entrustdatacard.com

Entrust Datacard®