



die das

Authentication Management verändert

Angesichts der immer strengeren Sicherheitsauflagen durch Behörden und in der Industrie suchen immer mehr Unternehmen nach Möglichkeiten, um die wenig sichere Passwortabfrage unter Windows durch eine stärkere Form der Authentifizierung ersetzen zu können. Doch die bisherigen Lösungen waren komplex und teuer.

Hier kommt **imprivata OneSign® Authentication Management** ins Spiel. Für Organisationen, die ihren Benutzerzugriff in Microsoft Windows-Umgebungen sicherer machen wollen, ersetzt OneSign Authentication Management die Netzwerk-Passwörter durch eine effektive Zwei-Faktoren-Authentifizierung, unabhängig davon, ob die Benutzer online sind und eine Verbindung zum Unternehmensnetzwerk besteht oder ob sie offline sind und sich auf ihrem Laptop anmelden.

Für Unternehmen aller Größenordnungen erlaubt OneSign Authentication Management, das Sicherheitsmanagement für den Netzwerkzugriff in stark dezentral ausgelegten Unternehmen kostengünstiger und einfacher zu machen. Es ist damit die leistungsfähigste und innovativste Authentication-Management-Lösung der gesamten Industrie.

Bestechend Einfach

Sofort einsatzbereite Appliance

OneSign wird als redundantes Appliance-Paar vorinstalliert und ist für die schnelle und einfache Inbetriebnahme vorbereitet. Es muss keine zusätzliche Hardware oder Software beschafft, installiert, eingebunden oder gewartet werden. Eine dezentrale Architektur erlaubt den Einsatz als eine verteilte, hochverfügbare Lösung, die für unbegrenzt viele Benutzer ausgelegt werden kann.

Einheitliche Plattform für das Authentication Management

OneSign sorgt für ein einfaches und flexibles Authentication Management, sogar die Verwaltung für One-Time-Password Token ist integriert. Ein sicherer Netzwerkzugang lässt sich innerhalb von

Stunden einrichten, ohne dass die vorhandenen Benutzerverzeichnisse geändert werden müssen. Richtlinien werden zentral gemanagt und können in Minutenschnelle transparent angewandt werden. Dies hat keine negativen Auswirkungen auf die Benutzerproduktivität, erfordert nur einen minimalen täglichen Administrationsaufwand und verändert die Desktop-Benutzeroberfläche nicht.

Einfachere Compliance und Berichterstattung

Integrierte Überwachungs-, Protokollierungs- und Reporting-Funktionen, die dokumentieren, welche Benutzer wann eingeloggt sind, ermöglichen es den Organisationen, ihre Sicherheitsrichtlinien zu verbessern und die Einhaltung der gesetzlichen Vorschriften nachzuweisen.

Einfach Intelligent

Effektive Authentifizierung – online oder offline

Windows-Passwörter sind die Schwachstelle Ihrer Sicherheitslösung. OneSign Authentication Management ist flexibel und für die Unterstützung zahlreicher Authentifizierungsverfahren konfiguriert, u. a. für die einfache Verwaltung von One-Time Password (OTP)-Token, aktiven/passiven Proximity Cards, Smart Cards, USB-Token und biometrische Daten per Fingerabdruck, um erhöhte Sicherheit für den Zugriff zu gewährleisten.

Integriertes VASCO DIGIPASS Token-Management

Mit einem Embedded-RADIUS-Host und einem VACMAN Controller von VASCO Data Security ermöglicht OneSign den Kunden das rasche Einrichten, Einsetzen und Verwalten von DIGIPASS-Token

aller Art – für die dezentrale ebenso wie für die lokale Netzwerk-Authentifizierung.

Nahtloses Upgrade zu Single Sign-On und Integrated IT/ Building Access

Die OneSign Appliance ist eine komplette und umfassende Plattform für das konvergente Identitäts- und Zugangsmanagement. Mit einem einfachen Lizenzschlüssel können die Kunden das OneSign Authentication Management nahtlos um das Single Sign-On zu Enterprise-Applikationen und/oder um konvergente Sicherheitsrichtlinien erweitern, wobei Lösungen führender Security-Anbieter für die ortsbezogene Authentifizierung eingesetzt werden können.

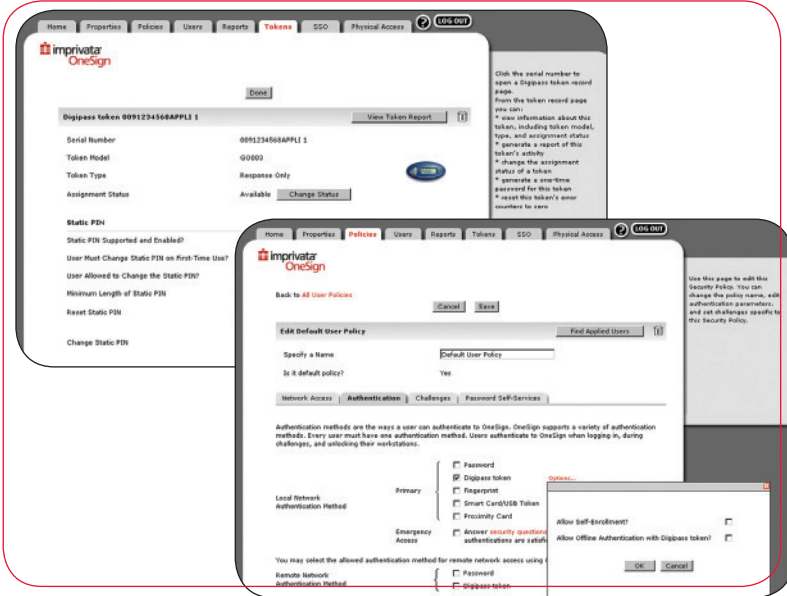
Einzigartiges Preis-Leistungs-Verhältnis

Kostengünstigste Zwei-Faktor-Authentifizierung

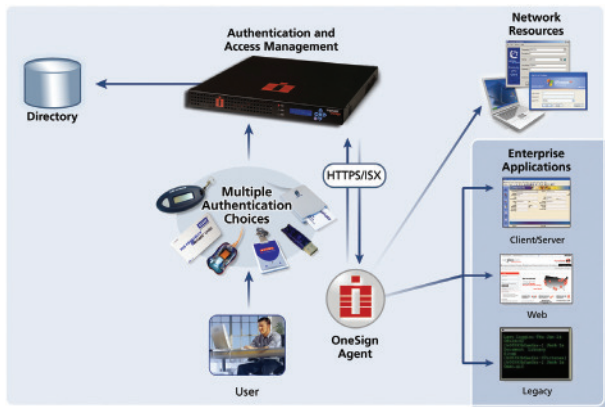
Dieschnelle Implementierung, die hohe Benutzerfreundlichkeit und die eingebaute Unterstützung für mehrere Authentifizierungsmethoden von OneSign führen zu sofortigen Kostenersparnissen. So macht sich die Investition sofort bezahlt. Als eigenständige Appliance bietet

OneSign Authentication Management die gesamte Funktionalität zur effektiven Implementierung und Verwaltung der Netzwerk-Authentifizierung. Es sind weder sonstige Anschaffungen noch eine kostspielige Integration erforderlich.

➔ Einfaches Management des gesamten Authentication Management-Prozesses



➔ Starke Authentifizierung von Applikationen auf der Transaktionsebene



Die ProvelD-Funktion von OneSign ermöglicht einer Applikation die Nutzung der starken Authentifizierungsdienste von OneSign zur eindeutigen Identifizierung eines Benutzers an jedem Punkt des Applikations-Workflows. Was die Anwendungsmöglichkeiten von ProvelD betrifft, kann die Lösung beispielsweise zur eindeutigen Identifizierung von Benutzern einer Banking-Website vor der Durchführung einer Finanztransaktion eingesetzt werden. Eine weitere Möglichkeit wäre der Einsatz im Gesundheitswesen vor der Ausgabe eines Medikaments.



OneSign & DIGIPASS

- OneSign Authentication Management umfasst ein integriertes VASCO Token-Management —es sind keine zusätzlichen Server erforderlich.
- Kunden können BELIEBIGE DIGIPASS-Token zur Netzwerk-Authentifizierung mit OneSign verwenden. Es ist schnell. Es ist einfach. Es sind keine zusätzlichen Anschaffungen erforderlich.



TECHNISCHE SPEZIFIKATIONEN

Anforderungen an die Administrationskonsole

- Internet Explorer 6.0 oder höher unter Windows 2000, Windows XP Professional oder XP Embedded, Windows Server 2000, Windows Server 2003.

Unterstützte Client-Systeme

- Internet Explorer 5.5 oder höher unter Windows 2000 SP3, Windows XP Professional SP1 oder XP Embedded SP1, Windows Server 2003, Windows Vista.

Unterstützte Verzeichnisdienste

- Microsoft Active Directory 2000 / 2003 Server, NT 4.0 Domain, Sun ONE Directory Server 5.0, Oracle Internet Directory (OID) 10g, Novell Netware 5.1 mit NDS 8.0 oder höher, Novell eDirectory 8.0, IBM Tivoli LDAP.

Unterstützte starke Authentifizierungsverfahren

- OTP Token, Proximity Cards, Smart Cards, USB-Token und biometrischer Fingerabdruck.

Appliance

- Betriebsfertiges, redundantes rack-mounted (1U) Serverpaar. Failover inbegriffen. Betriebssystem ist SUSE® LINUX Enterprise 9 von Novell.

Imprivata OneSign Authentication Management ist eine bestechend einfache, intelligente und einzigartig günstige Netzwerk-Authentifizierungslösung, die erhöhte Sicherheit beim Windows-Logon bietet.



www.imprivata.com • sales@imprivata.com • 1-877-OneSign • 1-781-674-2700

Corporate Headquarters

10 Maguire Road
Building 4
Lexington, MA 02421
t 781 674 2700
f 781 674 2760

Imprivata EMEA

Forsyth House, 77 Clarendon Road
Watford, Herts WD17 1LE
United Kingdom
t +44 (0)1923 813 511
f +44 (0)1923 813 501

Imprivata APAC

#01-03 60 Cambridge Road
Singapore 219757
t +65 82 004 840