



STRATEGIEPAPIER

Offene Authentifizierung

Eine Vision für die starke Authentifizierung aller Benutzer, Geräte und Anwendungen in allen Netzwerken



Where it all comes together.™



INHALT

+ Proprietäre kontra offene Systeme: Die Entwicklung von Open Networking	3
+ Die Suche nach dem Schlüssel zum Erfolg	4
Reichen Passwörter aus?	5
Was wäre, wenn?	5
+ Die Notwendigkeit einer umfassenden, starken Authentifizierung	7
Zunahme der Identitätsdiebstähle	7
Die Entwicklung föderierter Netzwerke	7
Nutzung der IP-Infrastruktur für Innovationen	7
+ Hindernisse für die umfassende Anwendung starker Authentifizierungslösungen	8
+ Offene Authentifizierung: Eine neue Vision für die starke Authentifizierung von Benutzern, Geräten und Anwendungen	9
Anforderungen für offene Authentifizierung	9
Branchenweite Zusammenarbeit	10
Standardisierte Referenzen	10
Nutzung vorhandener Middleware	10
Weite Verbreitung	11
Ein neuer Internetinfrastrukturdienst	11
+ VeriSign: Wegbereiter für eine umfassende, starke Authentifizierung	12



Obwohl starke Identitätsreferenzen für das kontinuierliche Wachstum und die Leistungsfähigkeit von Online-Unternehmen unerlässlich sind, stehen die Kosten und die Komplexität starker Authentifizierungslösungen häufig ihrer Einführung im Wege. Es beginnt sich jedoch eine neue Vision der starken Authentifizierung durchzusetzen, die dieses Problem angeht. Auf der Grundlage des Leitfadens für offene Authentifizierung, für den sich die Brancheninitiative Open Authentication (OATH) einsetzt, umfasst diese Vision die Einrichtung einer allgemeinen, auf offenen Standards basierenden Authentifizierungsplattform, über die Unternehmen jederzeit sämtliche Benutzer, Geräte und Netzwerke authentifizieren können. VeriSign hat sich dieser Vision verschrieben, um Unternehmen dabei zu unterstützen, neue Geschäftsmöglichkeiten zu erschließen, fortschrittliche Technologien einzusetzen und strategische Prozesse online durchzuführen. Aufbauend auf der dynamischen Stärke von VeriSigns Infrastruktur, Technologie, Daten und Informationsressourcen führt die nächste Generation der VeriSign® Strong Authentication Services die Authentifizierung im Rahmen einer Architektur von Netzwerkdiensten durch, die eine weite Verbreitung der starken Authentifizierung fördert, indem sie die Komplexität und die Total Cost of Ownership (TCO) reduziert.

Proprietäre kontra offene Systeme: Die Entwicklung von Open Networking

Aufgrund der Unzuverlässigkeit der Netzwerktechnologie scheuten große Unternehmen in den siebziger Jahren davor zurück, wichtige Transaktionen zu automatisieren. IBM entwickelte daher eine Reihe von Protokollen und Produkten, um Großrechner mit lokalen Terminals, Druckern und Computern zu verbinden. Diese Lösungen basierten auf proprietären Protokollen wie Systems Network Architecture (SNA) und Token Ring und eröffneten Unternehmen noch nie da gewesene Möglichkeiten. Anstatt Daten mithilfe von Bandmedien weiterzuleiten, was Stunden oder sogar Tage in Anspruch nehmen konnte, wurden dieselben Aufgaben nun innerhalb von Sekunden oder Minuten durchgeführt. Unternehmen begannen, Netzwerke aufzubauen und diese für unternehmenskritische Anwendungen einzusetzen.

Diese frühen Netzwerke basierten auf aufwändigen und dedizierten Vermittlungsprozessoren, die von einem zentralen Großrechner verwaltet wurden. Sie funktionierten gut, solange alle Kommunikationsgeräte von spezialisierten und qualifizierten Mitarbeitern installiert und verwaltet wurden. Der Netzwerkaufbau war ungeheuer komplex und nur IBM verfügte über alle erforderlichen Elemente. Aufgrund des zentralisierten Aufbaus konnte ein Netzwerkfehler das gesamte Unternehmen zum Erliegen bringen. Mit anderen Worten: Die Lösung war kostspielig, kompliziert und unflexibel. Sie beseitigte jedoch schwerwiegende Probleme und die Kunden waren zufrieden, da es keine Alternativen gab.

In den achtziger Jahren zeichnete sich eine Reihe neuer Anforderungen ab. Großrechner wurden durch Minicomputer ersetzt und Terminals durch Personal Computer (PCs). Die verteilte Datenverarbeitung (Distributed Computing), bei der Komponenten verschiedener Händler zur Anwendung kamen, setzte sich immer mehr durch. Eine radikale Umstellung auf offene, dialogfähige und einfache Netzwerkstandards wurde notwendig.

Das Transmission Control Protocol/Internet Protocol (TCP/IP) stellte diesen offenen Rahmen bereit und revolutionierte alle Aspekte der Datenverarbeitung. Die massive, globale Ausbreitung von Netzwerktechnologien in den neunziger Jahren betraf sowohl Unternehmen als auch Privathaushalte. IP-Netzwerke ermöglichten Einsatzszenarien, von denen die frühen Benutzer von SNA- und Token-Ring-Technologien nur träumen konnten.

Die Migration von proprietären auf offene Standards ist ein unvermeidlicher Schritt in der Evolution aller Technologien. Bestehende proprietäre Authentifizierungslösungen beheben zwar einige Probleme der Online-Sicherheit, aber neu entstehende Bedrohungen und Möglichkeiten erfordern einen ausgereifteren Ansatz. Durch Authentifizierung wird die erforderliche Grundlage geschaffen, um das Internet zu einem sicheren Medium für Kommunikation und Handel zu machen. Wie die Vernetzung kann sich die Authentifizierung jedoch nur durchsetzen, wenn die Umstellung von einer proprietären auf eine offene Architektur erfolgt. Ihre Verbreitung wird eine Zukunft ermöglichen, die für heutige Benutzer von proprietären Lösungen kaum vorstellbar ist.

Die Suche nach dem Schlüssel zum Erfolg

Die Kommerzialisierung des Internets hat die Arbeitsweise von Unternehmen von Grund auf verändert. Durch diese Revolution konnten sowohl die Umsatzmöglichkeiten als auch die Produktivität erheblich gesteigert werden. Schätzungen des Congressional Budget Office zufolge werden über 48 % der Produktivitätssteigerungen in den nächsten zehn Jahren auf die Anwendung der Internettechnologie zurückzuführen sein. Trotz der weit verbreiteten Auffassung, dass Online-Geschäftsaktivitäten seit dem Platzen der „Seifenblase“ im März 2000 nachgelassen haben, beschleunigte sich das Wachstum des Internets in Wirklichkeit erheblich. Die Anzahl der täglichen Webinteraktionen schoss um über 500 % in die Höhe und E-Commerce-Transaktionen nahmen um sensationelle 74 % pro Jahr zu.

Erhöhte Nutzung bedeutet jedoch auch erhöhtes Risiko. Online-Identitätsdiebstahl breitet sich immer mehr aus und gestohlene Identitäten werden für eine Vielzahl von schädlichen Aktivitäten eingesetzt, von Spam über betrügerische Kreditkartentransaktionen bis hin zu orchestrierten Sicherheitsangriffen mithilfe der kompromittierten Computer. Analysten schätzen, dass aufgrund von Vertrauensmangel mehr als 15 Milliarden US-Dollar im Bereich Handel und Kommunikation nicht realisiert wurden. Die Unfähigkeit, Benutzer zweifelsfrei zu authentifizieren, verhindert, dass das Internet zu einem wirklich sicheren Medium für Handel und Zusammenarbeit wird.

Darüber hinaus erschweren Sicherheitsprobleme die Einführung neuer Technologien sowie die Migration kritischer Transaktionen ins Internet. Die Kosten und die Komplexität der Authentifizierung hemmen die Verbreitung neuer Technologien wie Voice over IP (VoIP). Sie beschränken zudem die Bewegung von unternehmenskritischen Finanzdaten, Supply-Chain-Managementdiensten und Transaktionen zwischen privaten und öffentlichen Netzwerken und verhindern so, dass die inhärente Offenheit, Interoperabilität und Kosteneffizienz des Internets der Wirtschaft zugute kommt.

Das Problem wird noch verstärkt, indem Informationen über eine Vielzahl von Geräten und Kanälen zugänglich sind, die alle über eigene Sicherheitsmechanismen, Protokolle und proprietäre Technologien verfügen. Ein Benutzer kann seine E-Mails z. B. über seinen Bürocomputer, drahtlosen Laptop, Pager, sein Mobiltelefon oder im Internetcafé abrufen. In dieser Umgebung ist die Implementierung und konsequente Durchsetzung einer übergreifenden Sicherheitsstrategie mit großem Aufwand und hohen Kosten verbunden, so dass Unternehmen häufig unerwünschte Kompromisse machen müssen. Während sie Kosten, Risiken und Chancen gegeneinander abwägen, müssen Unternehmen bedenken, dass sie sich u. U. einem größeren Risiko aussetzen, ihre bestehenden Investitionen nicht voll ausschöpfen, Geschäftsmöglichkeiten nicht nutzen oder wertvolle Mittel von wichtigen Unternehmensprozessen abzweigen müssen.

+ Reichen Passwörter aus?

Von allen Authentifizierungsmethoden ist ein Passwort am einfachsten zu implementieren und zu verwenden. Ist es jedoch ausreichend? Abhängig vom Risikomanagementszenario ist es für zahlreiche Anwendungen geeignet. Ein Passwort kann jedoch leicht mitgeteilt, gestohlen oder erraten werden und deswegen ist der Missbrauch von Passwörtern die häufigste Ursache für Identitätsdiebstahl. Orchestrierte Angriffe wie „Phishing“ können bewirken, dass Benutzer einer Person, die sich als eine rechtmäßige Organisation ausgibt, freiwillig ihr Passwort mitteilen, das von dieser Person dann für kriminelle Zwecke genutzt wird. Schwachstellen und Sicherheitslücken treten in sämtlichen Bereichen der Passwortimplementierung auf, einschließlich Eingabe, Übertragung, Verifizierung und Speicherung.

Darüber hinaus können mit Passwörtern nur Benutzer authentifiziert werden. Heutzutage ist eine starke Authentifizierung jedoch auch für Geräte oder Netzwerkelemente erforderlich. Da Benutzer von jedem Standort aus Zugriff auf Informationen benötigen, müssen Unternehmen zulassen, dass Gastcomputer eine Verbindung zu ihren Netzwerken herstellen und auf ihre Ressourcen zugreifen. Diese Anforderung, die Verbreitung von Wireless-Technologien für PCs und Mobiltelefone sowie der verstärkte Einsatz von IP-Netzwerken – für Sprachübertragungen, Webdienste und das Supply-Chain-Management ebenso wie für kritische Operationen wie Ölbohrungen – erfordern ein Höchstmaß an Netzwerksicherheit. Ein befallenes Netzwerkelement, ob absichtlich oder unabsichtlich beschädigt, kann ein Netzwerk innerhalb von Minuten mit einem Wurm oder einem anderen Virus infizieren und lahm legen. Und obwohl Passwörter für die Authentifizierung von Benutzern ausreichen mögen, stellen sie für Geräte und Anwendungen keine brauchbare Alternative dar.

Eine starke Authentifizierung für öffentliche und private Netzwerke ist zweifellos ein notwendiger Schritt für die Entwicklung der Internetsicherheit und bildet die Grundlage für künftige Innovationen.

+ Was wäre, wenn?

Welche Vorteile hätte es, wenn starke Authentifizierungsreferenzen für weniger als 10 US-Dollar pro Benutzer bereitgestellt werden könnten? Welche Chancen würden sich eröffnen, wenn eine starke Authentifizierung aller Benutzer und Geräte im Internet möglich wäre? Wie sieht die Zukunft aus, die für heutige Benutzer kaum vorstellbar ist?

Wir können zumindest die folgenden Vorteile erwarten:

- erhebliche Reduzierung von Kreditkartenbetrug und somit niedrigere Kosten für Händler, Banken, Kartenunternehmen und letztlich für Kunden
- erhöhter Datenschutz für Benutzer, da eine eindeutige Referenz bereitgestellt wird, die die Identität einer Person verifiziert, ohne personenbezogene Informationen (z. B. den Namen oder die Sozialversicherungsnummer) preiszugeben
- Anbieter von Internet- und Mobildiensten können neue Einnahmequellen erschließen, indem sie Mehrwert-Abonnementdienste anbieten
- Bereitstellung sicherer virtueller Gemeinschaften für Kinder und andere Interessengruppen
- Durchführung wichtiger Offline-„Transaktionen“ (z. B. Wählen)
- Beschleunigung der Migration von Sprachanwendungen, finanziellen Transaktionen und anderen kritischen Diensten auf die bestehende IP-Infrastruktur

Leistungsfähigere Mechanismen für die Identitätsauthentifizierung

Die folgenden Mechanismen bieten ein höheres Maß an Sicherheit als Passwörter, vor allem, wenn eine Kombination dieser Mechanismen eingesetzt wird.

+ Digitale Zertifikate

Digitale Zertifikate basieren auf der Verschlüsselung durch öffentliche Schlüssel und stellen eindeutige, einprägsame Online-Referenzen zur Verfügung, die die Identität eines Geräts oder Gerätebenutzers authentifizieren und Berechtigungen für den autorisierten Zugriff auf private Online-Informationen identifizieren. Abgesehen davon, dass digitale Zertifikate einen effektiveren Mechanismus für die Identitätsauthentifizierung bieten, ermöglichen sie – im Gegensatz zu Passwörtern und persönlichen Identifikationsnummern (PINs) – die digitale Signatur und Verschlüsselung, um Datenschutz, Datenintegrität und Nachweisführung zu gewährleisten.

+ Tokens und Smartcards

In Tokens und Smartcards ist ein Mikrochip eingebaut, der Sicherheitsdaten und -anwendungen speichert. Sie enthalten mehr Informationen als Magnetstreifenkarten und können für verschiedene Anwendungen programmiert werden. Auf einem einzelnen Token können mehrere Anwendungen gespeichert sein; außerdem können Anwendungen hinzugefügt, gelöscht oder aktualisiert werden, ohne dass der Token neu ausgestellt werden muss. Die Abfrage einer PIN für den Zugriff auf Referenzen bietet zusätzlichen Schutz, falls der Token selbst verloren geht oder gestohlen wird. Darüber hinaus können Tokens in Verbindung mit Biometrie, z. B. Handgeometrie, Fingerabdruck oder Netzhautabtastung, eingesetzt werden, um die Sicherheit zu verstärken.

+ Digitale Zertifikate mit Tokens

Die Kombination aus digitalen Zertifikaten und Token bietet mehr Sicherheit, Benutzerfreundlichkeit und Mobilität für die Kommunikation und den Handel im Internet als digitale Zertifikate oder Token allein. Auf einem Token sind die digitalen Zertifikate besser gegen Diebstahl oder Identitätswechsel geschützt als auf der Festplatte des Benutzers. Dadurch wird die Gefahr, dass Netzwerke, Systeme und Anwendungen beschädigt werden, reduziert. Außerdem können auf dem Token ein oder mehrere Identifikationszertifikate gespeichert werden. Benutzer haben damit stets die entsprechenden Referenzen zur Hand, um von Remote-Standorten aus auf Systeme zuzugreifen, und sind nicht mehr an einen bestimmten Arbeitsplatz gebunden.

+ Digitale Zertifikate mit Trusted Platform Modules (TPMs)

TPMs sind isolierte Chips, die sich auf der Hauptplatine des Computers befinden und digitale Signaturen verwenden, um sicherzustellen, dass das Betriebssystem und andere Komponenten der Softwareumgebung nicht beschädigt sind. In Kombination mit digitalen Zertifikaten stellen sie die stärkste Authentifizierung dar.

Die Notwendigkeit einer umfassenden, starken Authentifizierung

Starke Authentifizierung bildet die Grundlage für sicherere Netzwerke, in denen alle Benutzer und Geräte zuverlässig identifiziert werden können. Sie ist eine wichtige Voraussetzung für vertrauenswürdige Netzwerke, in denen Transaktionen bedenkenlos ausgeführt werden können. Eine Reihe von Faktoren unterstreicht die Notwendigkeit einer starken Authentifizierung: die Zunahme der Identitätsdiebstähle, die Entwicklung föderierter Identitätsnetzwerke und vor allem der Wunsch, die IP-Netzwerkinfrastruktur für die neuesten Innovationen zu nutzen.

+ Zunahme der Identitätsdiebstähle

Die Federal Trade Commission (FTC) – stellte in ihrem jährlichen Bericht 2003 - zum vierten Mal in Folge – fest, dass Identitätsdiebstahl der häufigste Grund ist, warum sich jemand an eine Verbraucherschutzbehörde wendet. Da die wichtigsten Verbraucherservices wie Finanz-, Gesundheits- und Versicherungsservices ins Netzwerk verlagert werden, müssen Unternehmen sicherstellen, dass Kreditkartenkonten, E-Mail-Adressen, Sozialversicherungsnummern und andere personenbezogene Informationen nicht gestohlen werden können. Eine starke digitale ID – in Form eines speziellen Geräts oder integriert in traditionelle digitale Assistenten und Mobiltelefone – reduziert die zahllosen Angriffspunkte in einem globalen öffentlichen Netzwerk.

+ Die Entwicklung föderierter Netzwerke

Die Einführung netzwerkbasierter Systeme für die Verwaltung von Unternehmensinhalten, Supply-Chain-Daten und Kundendienst stellt Unternehmen vor die Herausforderung, einer großen und dynamischen Gruppe von Endbenutzern, z. B. Außendienstmitarbeitern, Geschäftspartnern und Kunden, den Zugriff auf Unternehmensressourcen zu ermöglichen. Aufgrund der Komplexität und der Kosten, die mit der Verwaltung von Identitäten in internen und externen Systemen verbunden sind, sowie der Notwendigkeit, den Zugriff auf Daten zu ermöglichen, sind föderierte Netzwerke erforderlich, in denen Identifikation, Referenzen und Attribute von Partnern gemeinsam verwendet werden können. Wenn eine Identität gemeinsam verwendet wird, hängt die Sicherheit der gesamten Access-Control-Chain von der Stärke dieser Identität ab und es entstehen komplexe Abhängigkeiten und Verantwortlichkeiten zwischen mehreren Geschäfts- und juristischen Parteien. Eine starke Authentifizierung ist von entscheidender Bedeutung, um den Zugriff auf föderierte Netzwerke zu sichern und die Datenschutzverordnungen der US-Regierung, z. B. den Health Insurance Portability and Accountability Act (HIPAA), den Gramm-Leach-Bliley Act (GLBA), die Verordnung Food and Drug Administration (FDA) 21 Code of Federal Regulations (CFR) Part 11 und den California State Bill (SB) 1386, einzuhalten.

+ Nutzung der IP-Infrastruktur für Innovationen

Die IP-Infrastruktur ist eine allgemeine, globale Ressource, die einzigartig auf der Welt ist. Sie ist das Ergebnis organischer Investitionen von unzähligen Organisationen. Ihre Offenheit ist Möglichkeit und Hindernis zugleich. IP-Netzwerke stecken noch in den Kinderschuhen und bevor ihr Potenzial voll ausgeschöpft werden kann, muss das Problem der Sicherheit gelöst werden.

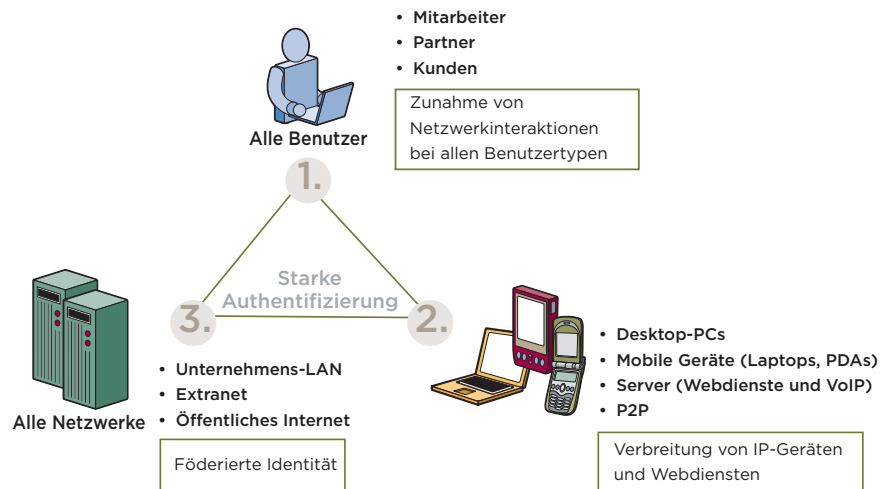
Die Fähigkeit, Benutzer, Geräte und Anwendungen in sämtlichen Netzwerken zu authentifizieren, ist eine wichtige Voraussetzung dafür, dass sich die IP-Netzwerkinfrastruktur über ihre aktuelle Funktionalität hinaus weiterentwickeln kann. Beispielsweise kann die Nutzung von IP-Netzwerken für Sprachverkehr zu einer erheblichen Senkung der Kosten beitragen. Bevor IP-Netzwerke im Hinblick auf ihre Zuverlässigkeit jedoch mit einem öffentlichen Fernsprechwahlnetz vergleichbar sein werden, muss ihre Sicherheit erheblich verbessert werden. Diese Sicherheit kann nur durch eine starke Authentifizierung jedes Netzwerkelements erreicht werden. Ebenso werden wichtige Finanztransaktionen nach wie vor zum Großteil über geschlossene und private Netzwerke vorgenommen. Ähnlich wie bei VoIP führt die Nutzung des Internets für diese Transaktionen zu Kosteneinsparungen, erfordert jedoch ein Höchstmaß an Sicherheit bei der Authentifizierung von Benutzern und Anwendungen.

Hindernisse für die umfassende Anwendung starker Authentifizierungslösungen

Bestehende Lösungen für starke Authentifizierung können zwar die mit dem Netzwerkzugriff verbundenen Probleme lösen, aber ihre Komplexität und die hohen Costs of Ownership stellen Hindernisse für eine umfassende Anwendung dar. Zu diesem Problem tragen in erster Linie die fehlende Interoperabilität, eine mangelnde Skalierbarkeit sowie die Anschaffungs- und laufenden Kosten bei.

- **Fehlende Interoperabilität** – Wie frühere Netzwerkprodukte sind die heutigen Lösungen für starke Authentifizierung proprietär und vertikal integriert. Sie enthalten eigene Verzeichnis-, Bereitstellungs- und Validierungskomponenten sowie Authentifizierungsgeräte, die nur mit diesen Komponenten eingesetzt werden können. Selbst innerhalb eines Unternehmens müssen EDV-Abteilungen häufig mehrere Parallelinstanzen für unterschiedliche Anwendungen oder separate Organisationen verwalten.
- **Mangelnde Skalierbarkeit** – Obwohl die heutigen Lösungen für die Bereitstellung in Unternehmen ausreichen, lassen sie sich nicht für das Internet skalieren. Sie können Tausende von Benutzern mit Millionen von Transaktionen pro Tag unterstützen, aber nicht Millionen von Benutzern mit Milliarden von Transaktionen. Sie unterstützen nicht die horizontale Skalierung oder die verteilten Zugangspunkte, die erforderlich sind, um der Größe des Internets kosteneffizient gerecht zu werden.
- **Hohe Kosten und Komplexität** – Vorhandene Lösungen bestehen aus dedizierten Software- und Hardwarekomponenten, deren Implementierung und Verwaltung erhebliche Investitionen an Zeit und Ressourcen erfordert. Darüber hinaus sind die Authentifizierungsgeräte selbst (z. B. Tokens, Smartcards und Universal Serial Bus [USB]-Tokens) übersteuert und an proprietäre Bereitstellungs- und Validierungssysteme gebunden. Diese Faktoren erhöhen die Kosten und die Komplexität der Integration von Authentifizierungsmechanismen in die vorhandene Netzwerk- und Anwendungsinfrastruktur.

Offene Authentifizierung: Eine neue Vision für die starke Authentifizierung von Benutzern, Geräten und Anwendungen



Um eine umfassende Anwendung der starken Authentifizierung für alle Benutzer, Geräte und Netzwerke zu ermöglichen, muss die Technologie einfach bereitzustellen und zu verwenden, preiswert und dialogfähig sein. Wie bei der Entwicklung anderer Technologien auch, ist die Umstellung auf eine offene, modulare Architektur ein entscheidender Schritt. Indem proprietäre, unternehmensweite Lösungen durch einen offenen Rahmen ersetzt werden, kann sich die Authentifizierung zu einem standardbasierten Netzwerkdienst für das globale Internet entwickeln. Wenn starke Authentifizierung zu einem festen Bestandteil des Netzwerks wird, werden sich neue Möglichkeiten sicherer Interaktionen eröffnen und die gesamte Benutzergemeinschaft wird daraus Nutzen ziehen.

+ Anforderungen für offene Authentifizierung

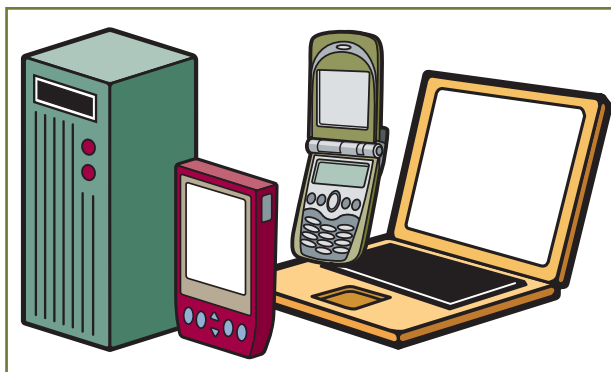
Um das Potenzial der starken Authentifizierung voll auszuschöpfen, müssen Anwender folgende Maßnahmen implementieren:

- **Standardisierung von Authentifizierungsgeräten** – Verwendung offener Standards, um eine flexible Auswahl an eigenständigen und eingebetteten Referenzen zu gewährleisten, die für alle Anwendungen eingesetzt werden können
- **Nutzung bestehender Middleware** – Aufbau auf vorhandenen Anwendungs- und Netzwerkinfrastrukturkomponenten, ohne dass zusätzliche Hardware oder Software erforderlich ist; Nutzung etablierter Protokolle
- **Föderierte und integrierte Identitäten** – Nutzung föderierter Identitätsstandards als leistungsfähige Mechanismen für die Integration der Authentifizierung in interne und externe Anwendungen

+ Branchenweite Zusammenarbeit

Die Authentifizierungstechnologie muss sich weg von proprietären, eng gekoppelten Lösungen und hin zu einem vollständig neuen Ansatz entwickeln, der offene Standards und bestehende Best-of-Breed-Infrastrukturkomponenten umfasst. Die Migration auf offene Standards ist unerlässlich für eine weitläufigere Bereitstellung. Indem sie die Grundlage für Verbreitung, Integration und Interoperabilität schafft, kann eine offene Architektur das Risiko und die Komplexität der Bereitstellung starker Authentifizierungslösungen reduzieren und somit die Übernahme durch Unternehmen, Dienstanbieter und Regierungen auf der ganzen Welt fördern.

OATH – eine von VeriSign ins Leben gerufene Brancheninitiative – hat einen Leitfaden für die gemeinsame Entwicklung einer offenen Spezifikation für starke Authentifizierung entworfen, die branchenweit eingesetzt werden kann. Dieser Leitfaden, bei dem der Einsatz bestehender Technologien und Standards im Vordergrund steht, dient als Ausgangspunkt für den Entwurf einer offenen Architektur. Diese offene Architektur wird die Grundlage für dialogfähige Lösungen bilden, die über zahlreiche Geräte, Plattformen für die Identitätsverwaltung und Netzwerke eingesetzt werden können. Gleichzeitig lässt sie Freiraum für Innovationen, um neue Produkte auf den Markt zu bringen.



+ Standardisierte Referenzen

Die meisten Authentifizierungsgeräte, von USB-Tokens bis hin zu Smartcards, basieren auf proprietären Technologien. Eine bestimmte Art von Token kann nicht mit der Software eines anderen Händlers verwendet werden. Um die Verwendung von Referenzen zu vereinfachen und Flexibilität bei der Auswahl des Geräte- oder Referenztyps zu gewährleisten, sollten Benutzer in der Lage sein, alle Referenzen, die auf OTP (OneTime Password), PKI (Public Key Infrastructure) und SIM (Subscriber Identity Module) basieren, auf einer gemeinsamen Plattform zu speichern und zu verwalten. Außerdem sollte jedes beliebige Gerät verwendet werden können. OATH ist ein Zusammenschluss einschlägiger Unternehmen, die Spezifikationen für die Standardisierung des Bereitstellungsprozesses sowie OTP-Algorithmen entwickeln. Diese Spezifikationen werden Organisationen wie der Internet Engineering Task Force (IETF) und der Smart Card Alliance vorgelegt und von diesen standardisiert. Letzten Endes werden diese Spezifikationen sowohl in eigenständigen Referenzen wie Tokens als auch in eingebetteten Referenzen, z. B. Mobiltelefonen, PDAs und Laptops, eingesetzt.

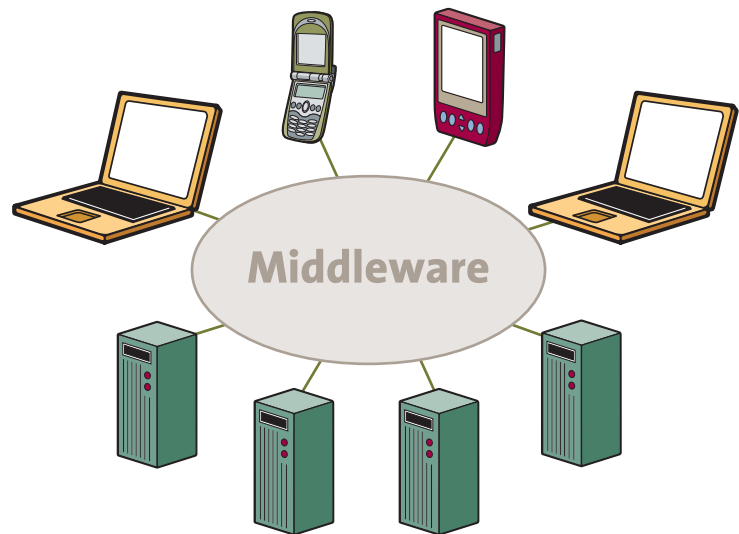
+ Nutzung vorhandener Middleware

Ein weiterer Aspekt der Authentifizierungsintegration ist die Nutzung vorhandener Netzwerk- und Anwendungsinfrastrukturen zur Bereitstellung, Verwaltung und Validierung starker Authentifizierungsgeräte. Auf diese Weise werden Kosten eingespart, da weder parallele Hardware- und Software-Infrastrukturen noch eine kostspielige und komplexe Integration erforderlich sind.

OATH setzt etablierte Protokolle wie Lightweight Directory Access Protocol (LDAP) und Remote Authentication Dial-In User Service (RADIUS) ein, damit OATH-kompatible Referenzen durch vorhandene Netzwerke und Anwendungen bereitgestellt und validiert werden können. Dieser Ansatz ermöglicht Unternehmen die Bereitstellung einer starken Authentifizierung ohne spezielle Software und Hardware, komplexe Integrationsprozesse oder nicht standardmäßige Bereitstellungsverfahren. Ein Unternehmen, das beispielsweise Microsoft®-Server und -PCs einsetzt, kann standardmäßige Microsoft-Bereitstellungs- und -Verzeichnisdienste verwenden, um allen Benutzern starke Referenzen uneingeschränkt zur Verfügung zu stellen. Das Gleiche gilt für Umgebungen mit Java 2 Enterprise Edition (J2EE™) und andere Umgebungen.

+ Weite Verbreitung

Die Implementierung der OATH-Vision wird die Ausbreitung starker Authentifizierungsreferenzen und anderer Authentifizierungskomponenten an zahlreichen Netzwerkendpunkten (z. B. Desktop-Computern, Webdienste-Servern, Wi-Fi-Zugangspunkten und Digitalempfängern) ermöglichen. OATH nutzt vorhandene föderierte Identitätsstandards, um Anwendungen die Validierung von Referenzen zu ermöglichen, die von anderen Organisationen ausgestellt wurden. Da die Referenzen von Dritten vertrauenswürdig und nutzbar sind, werden dialogfähige Transaktionen ermöglicht.



+ Ein neuer Internetinfrastrukturdienst

Wenn starke Authentifizierungslösungen in großer Zahl eingesetzt werden, werden die zur Unterstützung der Identitätsvalidierung und -verifizierung erforderlichen Transaktionsfähigkeiten (und Kosten) über einzelne Unternehmen hinausgehen und das gesamte Internet umfassen müssen. Starke Authentifizierung wird sich folglich von einem Unternehmensdienst zu einem Netzwerkdienst entwickeln. Skalierbarkeit wird in Zukunft noch wichtiger sein als jetzt, da Authentifizierungssysteme sowohl aktuelle als auch abgelaufene Zertifikate verfolgen werden. Diese Entwicklung erfordert eine globale Infrastruktur, die höchste Leistung und Verfügbarkeit bietet.

VeriSign: Wegbereiter für eine umfassende, starke Authentifizierung

In den kommenden Monaten wird VeriSign, zusammen mit einigen Schlüsselpartnern, einen starken Authentifizierungsdienst vorstellen. Dieser Dienst nutzt die in diesem Strategiepapier beschriebenen Kernspezifikationen, um die Authentifizierung im Rahmen einer Architektur für Netzwerkdienste durchzuführen, die eine umfassende Anwendung der starken Authentifizierung fördert, indem sie die Komplexität und die Total Cost of Ownership reduziert. Auf der Grundlage der von OATH entwickelten Leitlinien wird die offene Referenzarchitektur eine gemeinsame Schnittstelle für die Verwaltung aller Arten von Referenzen verschiedener Hersteller zur Verfügung stellen.

Die neue Dienstlösung trägt VeriSigns Vision von einer umfassenden, starken Authentifizierung Rechnung, indem sie die folgenden Anforderungen erfüllt:

- Bereitstellung einer offenen, modularen Lösung, die auf der bestehenden Infrastruktur aufbaut und einfach einzusetzen ist
- Bereitstellung eines hochgradig skalierbaren Dienstprogramms für die Netzwerkauthentifizierung, um die Authentifizierung zu vereinfachen und die Bildung von Identitätsgruppen zu ermöglichen
- Reduzierung der Total Cost of Ownership

Die erste Version der VeriSign Strong Authentication Services wird sich auf die nahtlose Integration mit Microsoft-Servern und Desktop-Anwendungen konzentrieren, um eine Vielzahl von Hardware-Referenzen zu verwalten, z. B. OTPs, Smartcards, PKI-basierte digitale Zertifikate sowie hybride Referenzen. Die Lösung wird ab Sommer 2004 erhältlich sein. J2EE-Versionen, die in Zusammenarbeit mit anderen Partnern angeboten werden, sollen wenig später folgen.

Weitere Informationen finden Sie auf unserer Website www.verisign.de