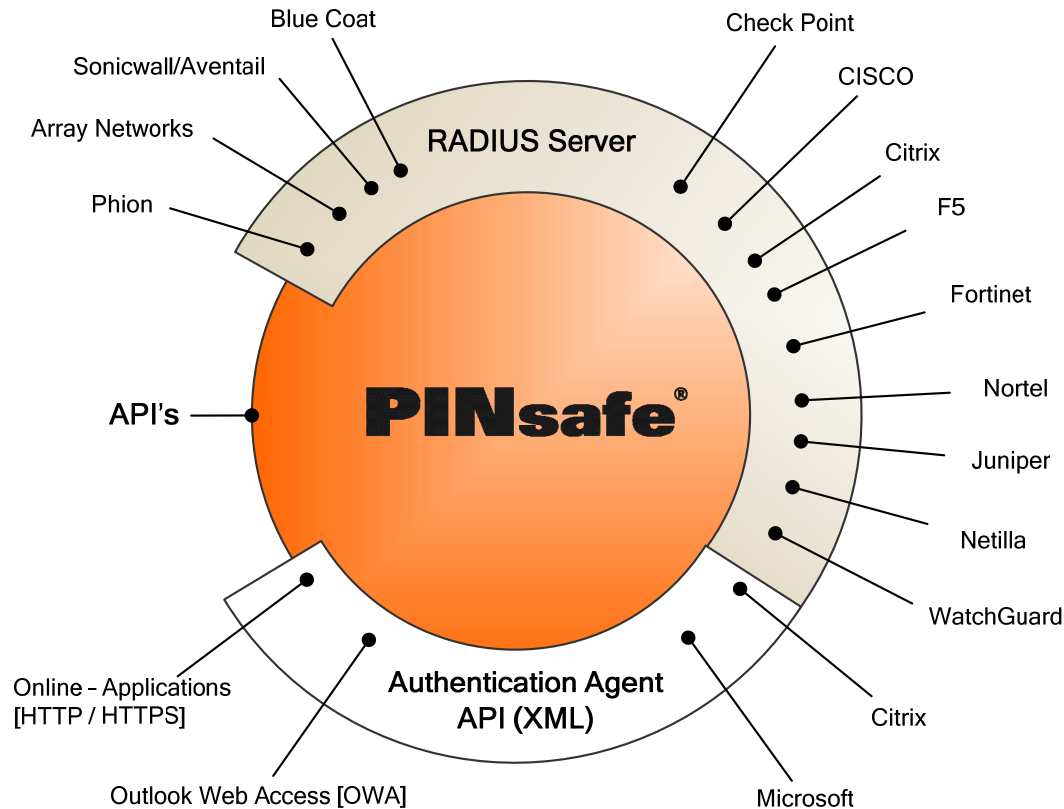


PINsafe — Multi-Faktor-Authentifizierung — Integration

PINsafe bietet mit integrierter Radius Server Technologie einfache Anbindungen zu gängigen VPN und Remote Access Lösungen, zum Beispiel:

- Array Networks
- Bluecoat
- Checkpoint
- Cisco
- Cisco ASA
- Citrix Access Gateway Standard
- Citrix Access Gateway Advanced
- Citrix Access Gateway Enterprise



- Juniper
- F5
- Fortinet
- Microsoft IAG
- Nortel
- Netilla
- Sonicwall/Aventail
- Phion
- WatchGuard

Per XML - Schnittstelle:

- Microsoft IIS
- Microsoft ISA Sever
- Microsoft Outlook Web Access
- Citrix Web Interface
- Microsoft IAG

Über die Entwicklungsschnittstellen [APIs] und die Authentication Agent API mit XML lassen sich weitere Systeme integrieren.



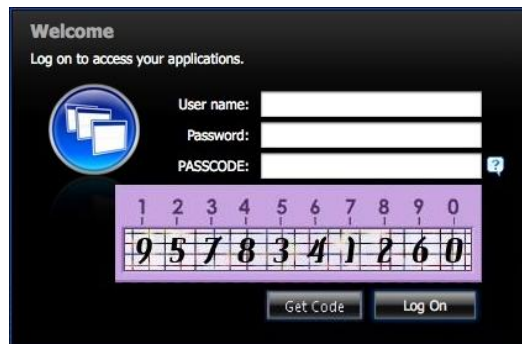
Starke Multi-Faktor-Authentifizierung

Was ist PINsafe?

PINsafe ist ein Authentifizierungssystem, das ohne weitere Hardware (z.B. Token) beim Anwender den sicheren Zugriff auf Netzwerke und Computersysteme ermöglicht. Über gesicherte Netzwerkverbindungen [VPN], über Webseiten, Firmenanwendungen und mobile Geräte kann nach der Authentifizierung durch PINsafe der Zugriff erfolgen.

Warum PINsafe?

PINsafe ermöglicht nur tatsächlich autorisierten Personen Zugang zu den Daten, für den sie innerhalb eines Sicherheitsbereiches auch legitimiert sind. Durch die einzigartige, patentierte OTC Generierung ist PINsafe die sicherste, einfachste, zuverlässigste und kostengünstigste Authentifizierung auf dem Markt.



PINsafe - Total Cost of Ownership (TCO)

Neben einem hohen Sicherheitsanspruch sprechen weitere Faktoren für PINsafe:

- LifeTime Lizenz!
Die User Lizenz läuft nie aus.
- Keine Installation beim Client
- Kein Neukauf alle drei Jahre von teuren neuen Token.
- Keine internen Administrationskosten.
- PINsafe User lassen sich über vorhandene Kontenverwaltungen (z.B. Active Directory von Microsoft) verwalten.
- Schlimmstenfalls kann der User bei PINsafe die PIN Nummer vergessen, welche problemlos neu aufgesetzt werden kann— äusserst schnell.
- Die Kosten für die sonst übliche Hardware (z.B. Smartcards oder Token) und der damit verbundene administrative Aufwand entfallen bei PINsafe.

PINsafe - wie funktioniert das?

A) per SMS (oder App, falls man offline ist)

-> **Handy als Token**

B) per Code beim Login Screen

-> **komplett ohne Token**

C) als PositiveID

-> **PC/Laptop als Token**

Bei dieser Technologie handelt es sich um das Auslesen der PC/Laptop IDs (Prozessor ID, MAC ID, etc.).

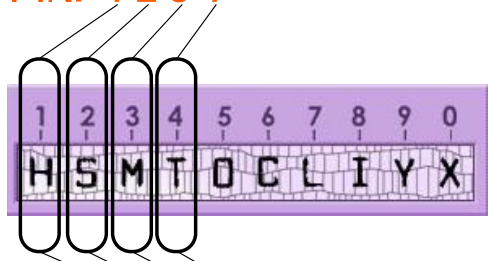
Die originale PIN Nummer wird dabei nie direkt eingegeben, sondern nur das Extrakt.



Patentierte One Time Code (OTC) Generierung

Beispiel 1

PIN: 1 2 3 4



OTC: H S M T

Ein wesentliches Merkmal von PINsafe:

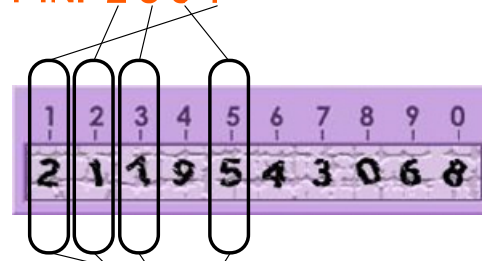
der Benutzer benötigt nur den zufällig erzeugten Security Code und die nur ihm bekannte PIN- Nummer, um sich authentifizieren zu können.

Die One Time Code (OTC) Extraktion ist sehr einfach anzuwenden: die PIN bestimmt, welche Stellen aus dem Security Code in welcher Reihenfolge als OTC eingegeben werden müssen.

Im Beispiel 1 oben ist zu sehen, wie die PIN-Nummer 1 2 3 4 zusammen mit dem Security Code den OTC H S M T ergibt. Die Länge der PIN Nummer kann zwischen 4 bis 10 Stellen variieren. Der Security Code kann aus Buchstaben, Zahlen oder einem Mix aus Buchstaben und Zahlen bestehen.

Beispiel 2

PIN: 2 3 5 1



OTC: 1 7 5 2

Der Vorteil:

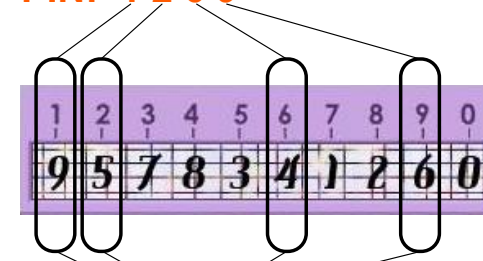
Der OTC, den der Nutzer eingibt, variiert bei jeder Authentifizierung und die PIN Nummer wird nie direkt eingegeben.

Die Authentifizierung erfordert immer zwei Elemente: den Security Code, der über verschiedene Kanäle an den Nutzer gesendet werden kann und die PIN Nummer, die sich der Nutzer selber merkt. Der Benutzer verwendet niemals seine PIN Nummer direkt zur Authentifizierung. Dies schützt z.B. vor Key-Logging oder Man-in-the-Middle Attacken.

Die Zusendung des Security Codes kann auch an einen bestimmten Kanal - z.B. ein

Beispiel 3

PIN: 1 2 6 9

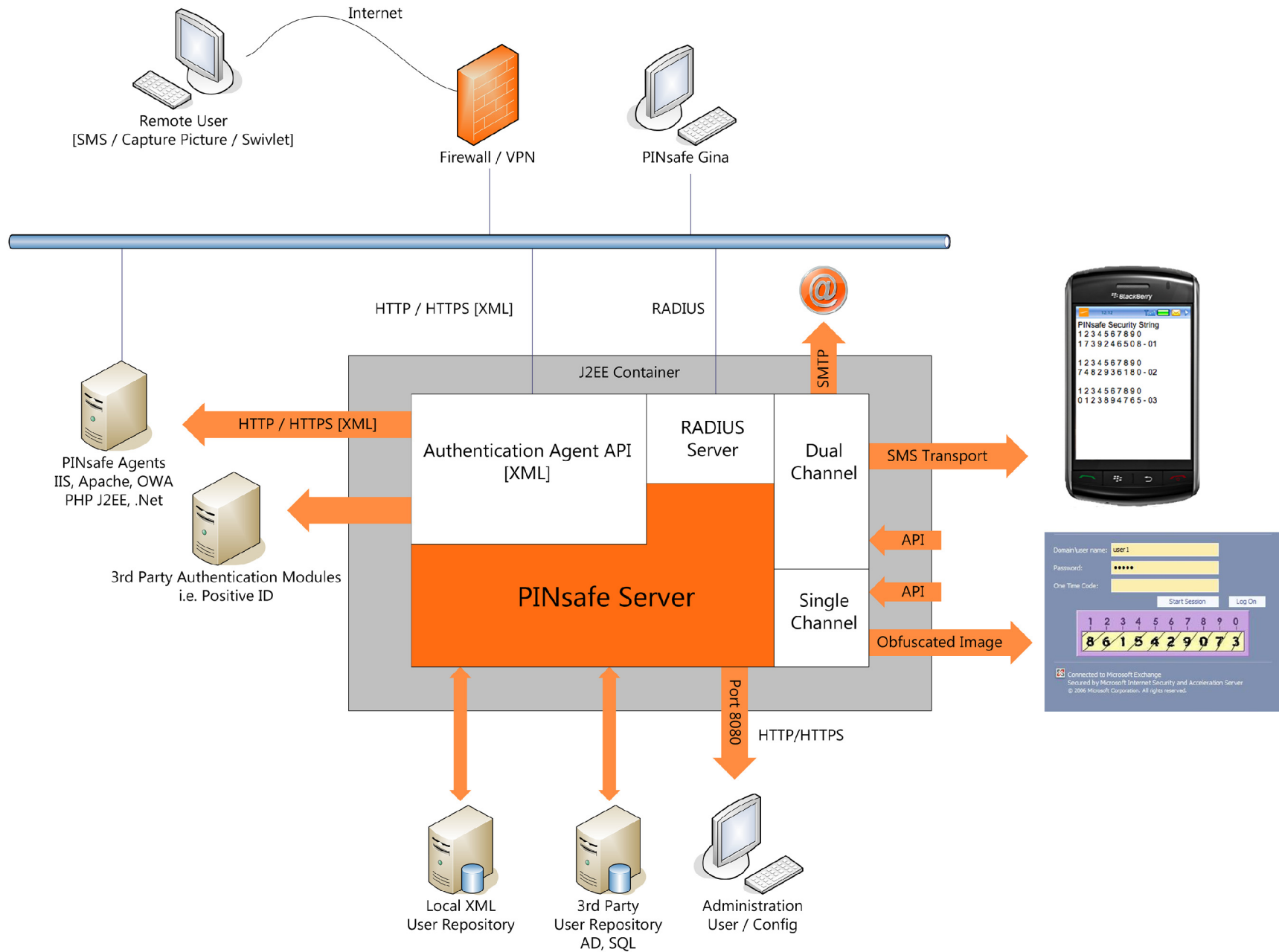


OTC: 9 5 4 6

Mobiltelefon oder PC - gebunden werden.

Somit kann problemlos eine echte 2-Faktor Authentifizierung umgesetzt werden. Der große Vorteil dieses Modells ist, dass es in verschiedensten Umgebungen implementiert werden kann und so verschiedenen Nutzergruppen und der gewünschten Authentifizierungsstärke Rechnung trägt. Der Security Code kann als verschleiertes, nicht Maschinen-lesbares CAPTCHA Bild auf einer VPN Login Seite dargestellt oder als SMS auf das Mobiltelefon eines Nutzers gesendet werden.

PINsafe Security String
Message 1119
[1234567890](#)
[2034567891](#)



Das Unternehmen

Im Jahre 2000 gegründet und mit Sitz in Wetherby, England, hat sich Swivel auf Lösungen zur Netzwerkabsicherung spezialisiert. Hierzu konnte Swivel in den letzten Jahren mehrere internationale Patente anmelden. **PINsafe**, die Multi-Faktor-Authentifizierungstechnologie von Swivel, setzt auf diesen Patenten auf und bietet somit immer mehr Unternehmen die gewünschte Sicherheit.

Swivel Secure Limited ist eine 100%ige Tochter der Unternehmensgruppe Marr T&T mit Sitz in London. Im Jahr 2009 erzielte die Marr Gruppe über 1 Milliarde US \$ Umsatz in 8 verschiedenen Produktgruppen. Zum Bereich Technologie innerhalb der Marr Gruppe gehören

neben Swivel die Schwesterfirmen Wavecrest und Mobix, die im Bereich der Telekommunikation und IP-Netzwerke angesiedelt sind. Über das internationale Vertriebsnetz unterstützt Swivel Kunden aus Industrie, Finanzen, Handel, Recht, sowie Staats- und Gesundheitsbehörden in über 30 Ländern.

Niederlassungen befinden sich in Großbritannien, Spanien, Frankreich, Portugal, USA und Deutschland.

Swivel Secure

Cologne, Germany

+49 221-510 7951

www.swivelsecure.com

ce@swivelsecure.com