
ACTIVIDENTITY™

Starke Authentifizierung:
Aktuelle Trends und Neuerungen

Dirk Losse, CISSP
Principal Pre-Sales Consultant – Central Europe
September 24, 2009

ACTIVIDENTITY™

Starke Authentifizierung - Heute

- 52 % der Unternehmen verwenden statische Passworte für den Zugriff auf kritische Daten
- 64 % der Unternehmen verlangen von ihren Mitarbeitern nicht, die Passworte zu ändern
- 45 % der Unternehmen erlauben die Verwendung „lexikalischer Ausdrücke“ (z.B. „Passwort“)
- 29 % der Unternehmen erzwingen keine bestimmte Passwortlänge

(Quelle: „Strong User Authentication“, Aberdeen Group, März 2009)

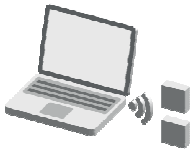
Starke Authentifizierung - Heute

- Anzahl der Implementierung wissensbasierender Authentifizierung, von Einmal-Passwort Verfahren und „out-of-band“ Authentifizierung ist gewachsen.
- OATH als offener OTP Standard hat die Hemmschwelle zur Einführung eines solchen Verfahrens gesenkt.
- Im Unternehmensumfeld dominieren Einmal-Passwort Verfahren bei der Absicherung des Fernzugriffs – mit zunehmender Einbindung von Mobil-Telefonen und „out-of-band“ Methoden, während im lokalen Umfeld verstärkt eine Tendenz zu „Smart Token“ zu erkennen ist.
- Der Bedarf der Unternehmen mehrere, unterschiedliche Authentifizierungsmethoden zu unterstüzen führt zu einem Bedarf von offenen, flexiblen Authentifizierungsinfrastrukturen.

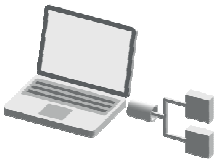
(Quelle: „Market Overview: Authentication“, Gartner, September 2008)

Anwendungsfälle Starker Authentifizierung (1)

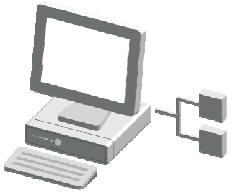
Employer-to-Employee



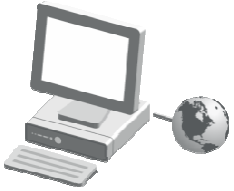
WLAN access



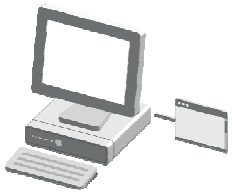
VPN access



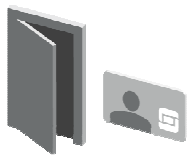
LAN access



web access



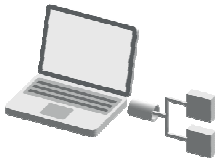
application access



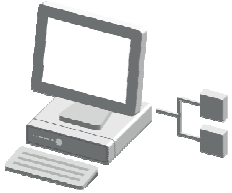
physical access

Business-to-Customer

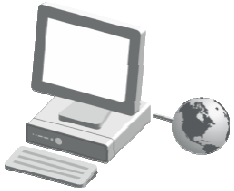
identity proofing



VPN access



LAN access



web access

transaction verification

Government-to-Citizen

e-government

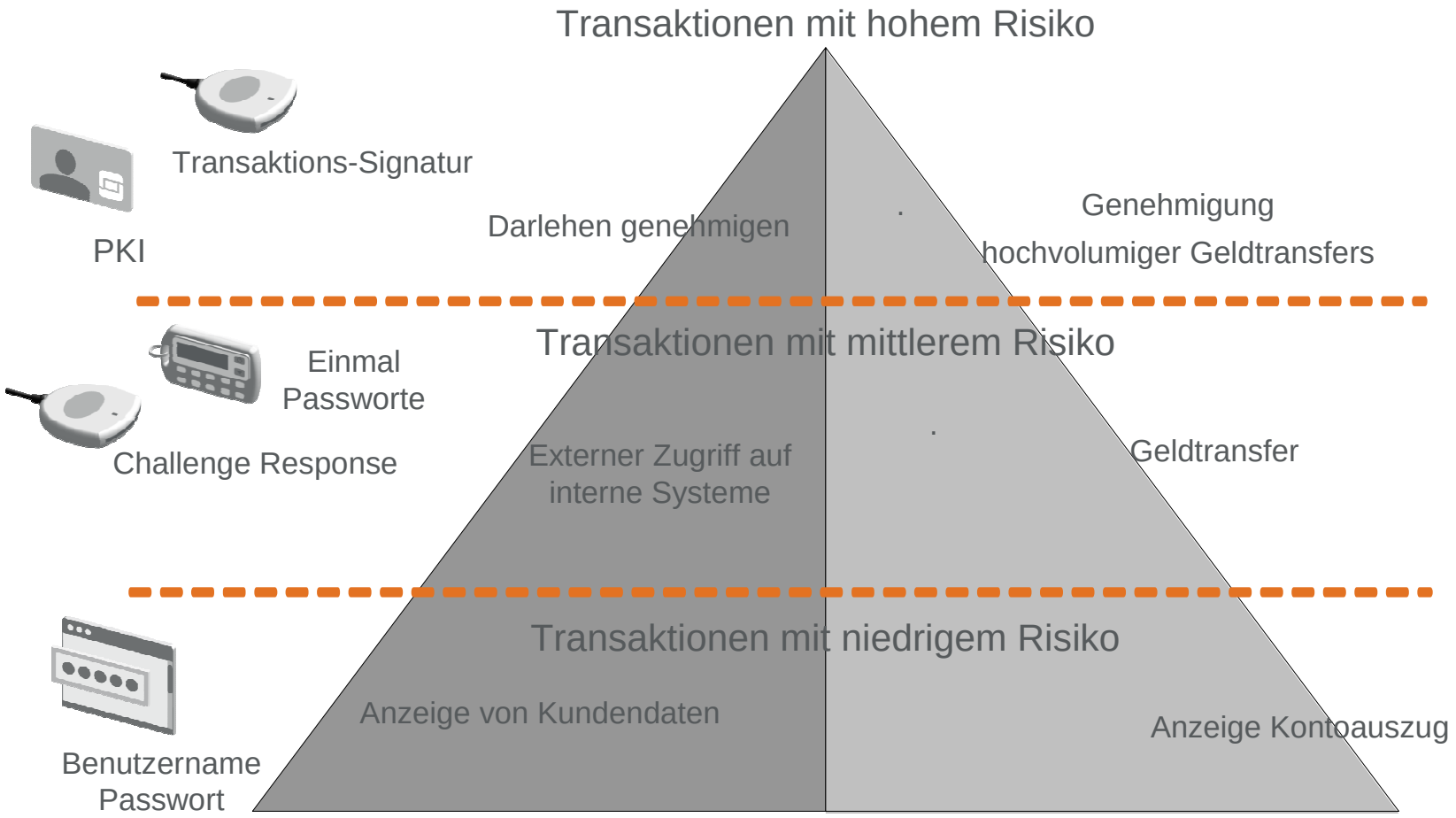
travel

driver's license

healthcare card

ACTIVIDENTITY™

Anwendungsfälle Starker Authentifizierung (2)

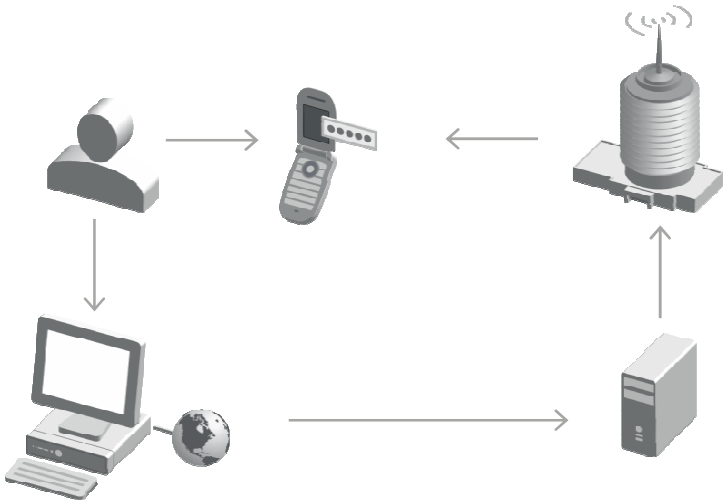


Initiative for Open AuTHentication (OATH)

- Spezifikation einer standardisierten Authentifizierungsinfrastruktur
- Entkopplung von Authentifzierungsserver und Authentifizierungsgeräten
  - Breiteres Angebot an Authentifizierungsgeräten
  - Investitionssicherheit bei Auswahl eines entsprechenden Authentifizierungsservers
- Authentifizierungsmethoden
  - HOTP (HMAC SHA1, RFC 4226): Eventbasierendes Einmal-Passwort
  - OCRA: Challenge- / Response-basierendes Einmal-Passwort
  - TOTP: Zeitbasierendes Einmal-Passwort
- Provisionierung
  - PSKC (Portable Symmetric Key Container)

Out-of-Band Authentifizierung

- Einmal-Passwort Versand per SMS
- Keine zusätzlichen Authentifizierungsgeräte
- Ideal für
  - Anwender mit seltener Einmal-Passwort Nutzung
  - Backup Authentifizierung



ACTIVIDENTITY™

Definition: “Versatile Authentication”

Ein einzelner Server (Software, oder Software / Hardware Appliance) mit Unterstützung für

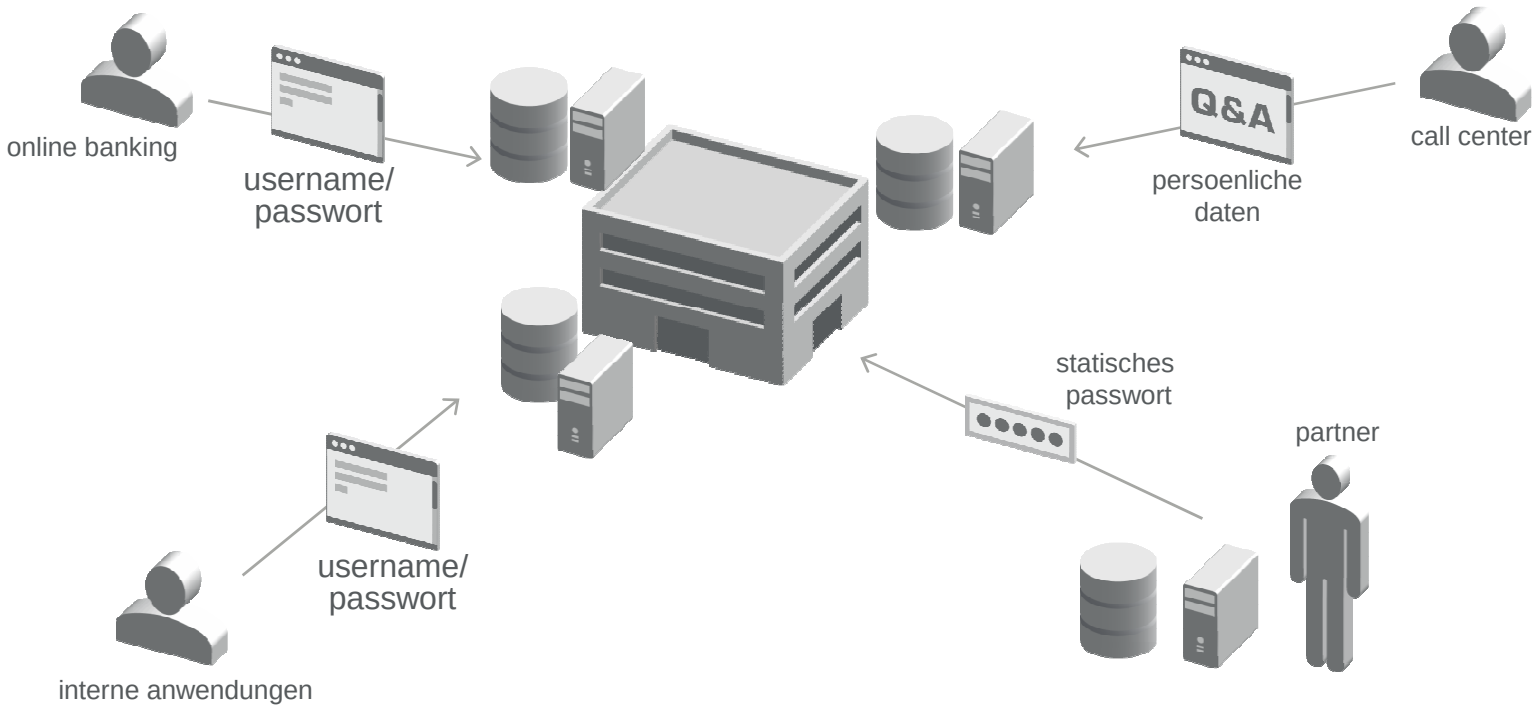
- verschiedene proprietäre Authentifizierungsmethoden, mit der Möglichkeit Methoden von Drittanbietern als “Plug-In” bei Bedarf zu integrieren
- Offene, standardisierte Authentifizierungsverfahren, wie X.509, OATH, EMV CAP
- in einer in-homogenen Landschaft.

Unterstützung für “Adaptive Access Control” Regeln ist wünschenswert (aber wenig verbreitet).

(Quelle: “Market Overview: Authentication”, Gartner, September 2008)

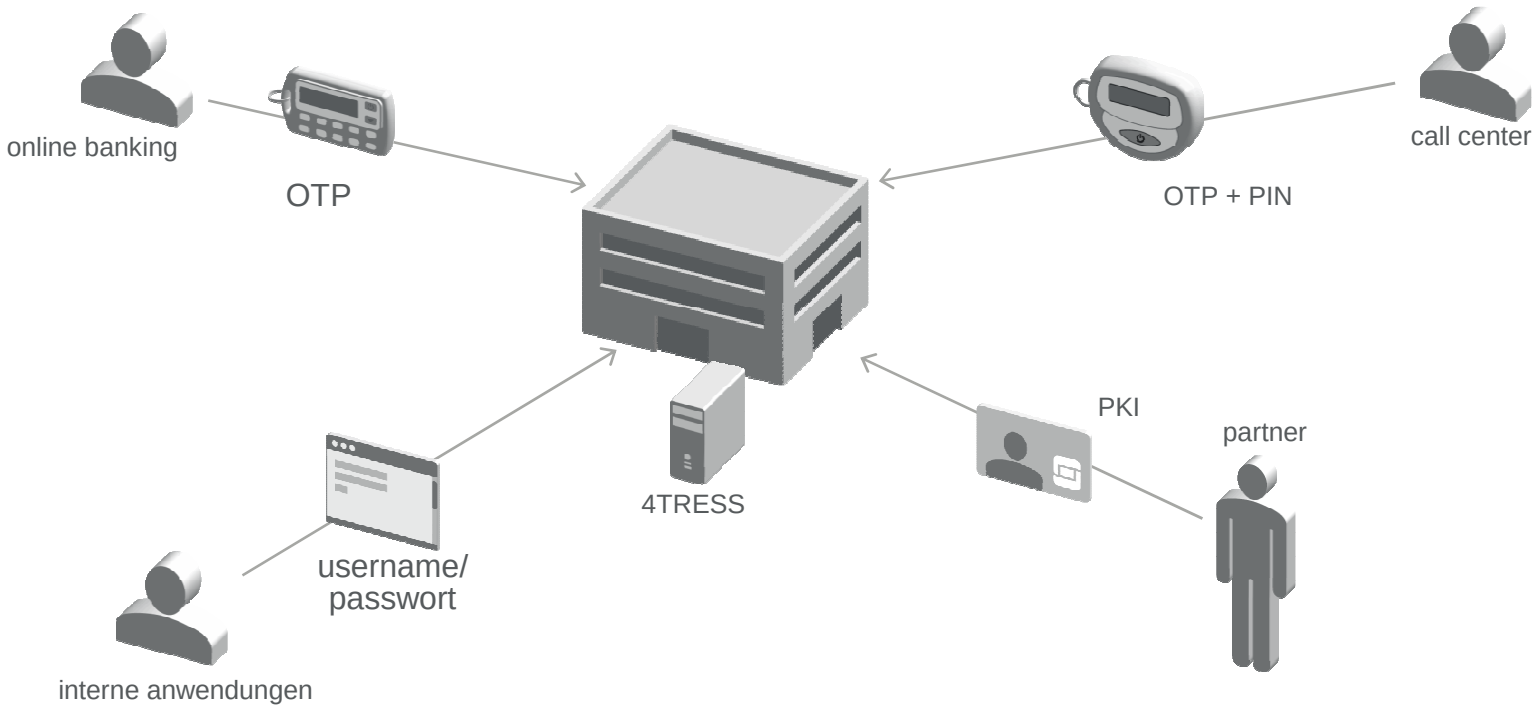
Situation Mit Unterschiedlichen Authentifizierungssystemen

- Teilweise schwache Authentifizierung
- Jede Authentifizierungsmethode benötigt ihren eigenen Server und Datenbank

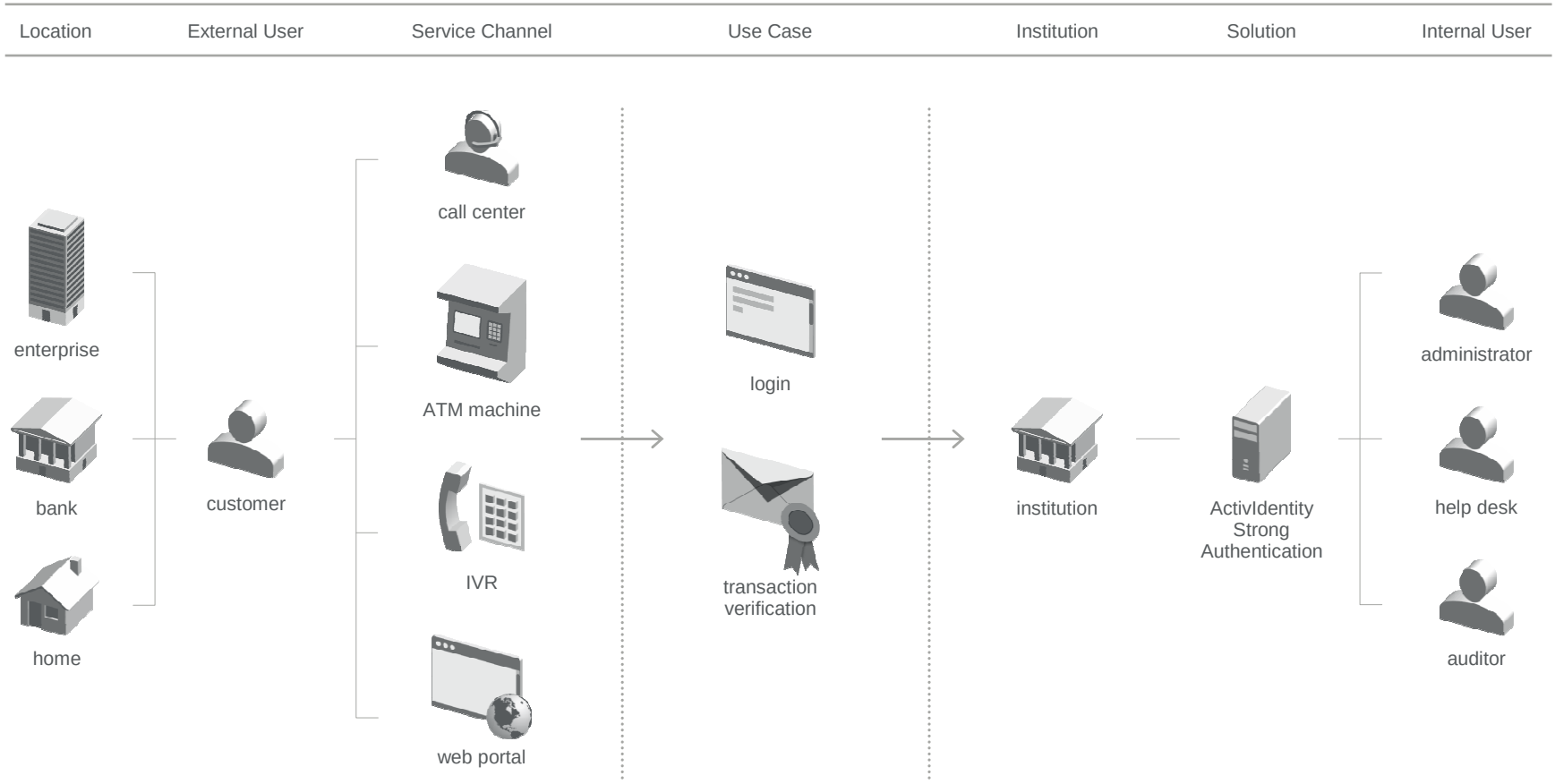


Situation Mit Einem „Versatile“ Authentifizierungsserver

- Durchgängig starke Authentifzierung
- Zentralisierte Administration und Datenhaltung



ActivIdentity 4TRESS Authentication Server (1)



ActivIdentity 4TRESS Authentication Server (2)

- Authentifizierungsmethoden
  - ActivIdentity Einmalpasswortalgorithmen
  - OATH
  - EMV/CAP
  - PKI
  - Statische Passworte
  - Sicherheitsfragen
  - ... Erweiterbar über Plug-In API
- Authentifizierungskanäle
  - Web
  - Radius
  - Beliebige Applikationen (SOAP, RMI, JAAS, C#)
- Offene Plattform
  - IBM Websphere oder JBOSS


ACTIVIDENTITY™