

SECURE PASS™

Protecting Identities.

La sfida tecnologica nel creare un
Secure Identity Service Provider

Giuseppe Paternò
CTO, GARL Sagl
19 Ottobre 2011

L'hacking "silenzioso": i furti di identità



10

milioni di vittime di furti di identità solamente negli USA nel 2008 (Javelin Strategy and Research, 2009)

221

miliardi di dollari all'anno la perdita economica mondiale relativa al furto di identità (Aberdeen Group)

5840

ore di lavoro per correggere i problemi relativi ai furti di identità, ovvero l'equivalente di due anni di lavoro di una persona (ITRC Aftermath Study, 2004).

35

milioni di dati compromessi tra le aziende e agenzie governative nel solo 2008 (ITRC)

2

miliardi di euro di danni alle aziende nella sola Italia nel 2009 (Ricerca ABI)

Un esempio concreto



Durante un nostro security assessment di una emittente radiotelevisiva, il furto di identità ha causato:

- Compromissione dell'accesso remoto e accesso a tutti i sistemi
- Accesso alla mail aziendale di tutti i dipendenti
- Accesso alle informazioni estremamente riservate: stipendi, budget dell'azienda, bilanci, ecc...
- Accesso completo al sistema di messa in onda: teletext, messa in onda radio, messa in onda video con la possibilità di cambiare i contenuti in qualsiasi momento
- Accesso ai sistemi elettrici dell'azienda, con la possibilità di spegnere completamente l'azienda e le trasmissioni televisive/radiofoniche

Le identità e la vita reale: “Vorrei ma”



Non
abbiamo
tempo



Non
abbiamo
budget



Le identità e la vita reale

- La tematica delle identità digitali non e' semplice anche per i più esperti. Ci vogliono:
 - personale dedicato, spesso una squadra di persone, con conoscenze tecniche molto elevate
 - infrastrutture dedicate, con ridondanza geografica e alta banda/velocità tra le sedi
 - licenze e canoni di manutenzione di differenti software e sistemi operativi (identity management, strong authentication, data replication, CAL, ...)
 - consulenti estremamente competenti dedicati al set-up dell'infrastruttura
- Non tutte le aziende, anche tra le più grandi, possono permettersi di avere una elevata protezione delle identità
- **Con il cloud computing, i problemi diventano sempre più complicati e costosi** (alta disponibilita', ecc..)

L'idea: SecurePass

Creare una

“Banca Svizzera delle Identità”

che fosse alla portata di tutti e che implementasse alti standard di sicurezza, con particolare focus all'ambito cloud





Cosa fa SecurePass

La “**banca SecurePass**” è un servizio on-line erogato in modalità cloud “Software-as-a-Service” (SaaS) che offre alle aziende una gestione e una protezione a 360 gradi delle identità.

Garantisce l’azienda che chi accede al dato, all’applicazione o al sistema sia veramente chi dice di essere; di essere in linea con i requisiti minimi di legge.

Sollewa l’azienda dai costi fissi e nascosti di gestione.

Garantisce l’utente che la sua identità digitale non venga compromessa.

Sollewa l’utente dal ricordare password complesse, previste dalla legge

I valori di SecurePass

- Garantire la **protezione delle identità** digitali implementando la massima sicurezza possibile
- **Neutralità**: non vogliamo essere influenzati ne' da vendor, da fondi di investimento o da specifiche nazioni.
- **Facilità di gestione**: le identità non devono essere un peso per l'IT Manager, che deve concentrarsi sul sostenere il business principale dell'azienda
- **Facilità di integrazione** negli applicativi e nei sistemi esistenti
- **Trasparenza**: nessun costo nascosto, il cliente paga per quello che usa
- L'uso di **standard Internet**: non vogliamo legare il cliente con protocolli proprietari





Gli ambiti di SecurePass

- **Cloud**

- Applicazioni e sistemi sensibili ospitati in un cloud/hosting provider
- Accesso sicuro ad infrastrutture cloud per cloud providers (es: VMWare, Citrix,)

- **Extranet/DMZ**

- Portali web disponibili dall'esterno a persone selezionate
- Accesso a sistemi e applicazioni esposti su Internet

- **Compatibilità verso VPN e SSL VPN** per avere il massimo ritorno degli investimenti e minor gestione da parte dell'IT

- **Micro/Piccole imprese** che decidono di spostare tutto sulla cloud.

Esempio pratico: Emergency



EMERGENCY

- Agenzia non-governativa che offre cure gratuite e di qualità alle vittime della guerra e della povertà
- Presente in 7 paesi nel mondo, alcuni considerati “zone di guerra”, ha curato più di 4 milioni di persone
- Accessi del personale volontario internazionale da ogni angolo del pianeta via Internet
- **Obiettivo:** proteggere le identità di tutto personale e le cartelle cliniche di tutti i pazienti curati.

Let's get technical now ... :-)

Protezione delle identità

- SecurePass e' un sistema di directory con sistemi di partizionamento sicuro dei dati e crittografia ad alto standard
- La protezione dell'identità dell'utente e' basata su sistemi multipli e indipendenti di autenticazione forte:
 - Il “mattoncino base” e' un sistema One Time Password (OTP) basata su algoritmi standard e riconosciuti dalla comunità internazionale come “robusti”
 - Stiamo lavorando ad altri meccanismi di strong authentication facili da usare
- Client disponibile per:
 - Smartphones (iPhone e Android; BlackBerry in fase di lavorazione), gratuito e indipendente dalla copertura GSM
 - Software token per Windows, Mac e Linux (Ubuntu) gratuito
 - Hardware token
- Secondo livello di password (PIN) alfanumerico

Protezione degli accessi

- SecurePass deve essere facile da integrare in applicazioni, sistemi e apparati presenti sul mercato
- La soluzione e' l'adozione di standard Internet, in particolare:
 - **RADIUS**: presente in gran parte degli apparati di rete, VPN e sistemi operativi
 - **LDAP**: presente in gran parte i sistemi operativi, degli applicativi tradizionali e web-based
 - **CAS**: standard di Web Single Sign-On che vi permette di autenticarvi una volta sola a tutti i vostri applicativi Web
- Se implementate uno di questi standard, siete già compatibili con SecurePass (gran parte del software commerciale e Open Source lo e' già)
- Implementare questi standard e' di poca fatica grazie al gran numero di framework disponibili ed esempi per tutti i linguaggi di programmazione

Esempi: Networking

- Virtual Private Networks
 - SSL VPN e VPN tradizionali
- Network Access Control
 - Accesso alla rete Wireless, incluso gli HotSpots
 - Accesso alla rete “wired”
- Accesso amministrativo agli apparati esposti, es: router ISP con IP pubblico

ADITO VPN



Welcome to **Adito!** A secure gateway to your network.

Username

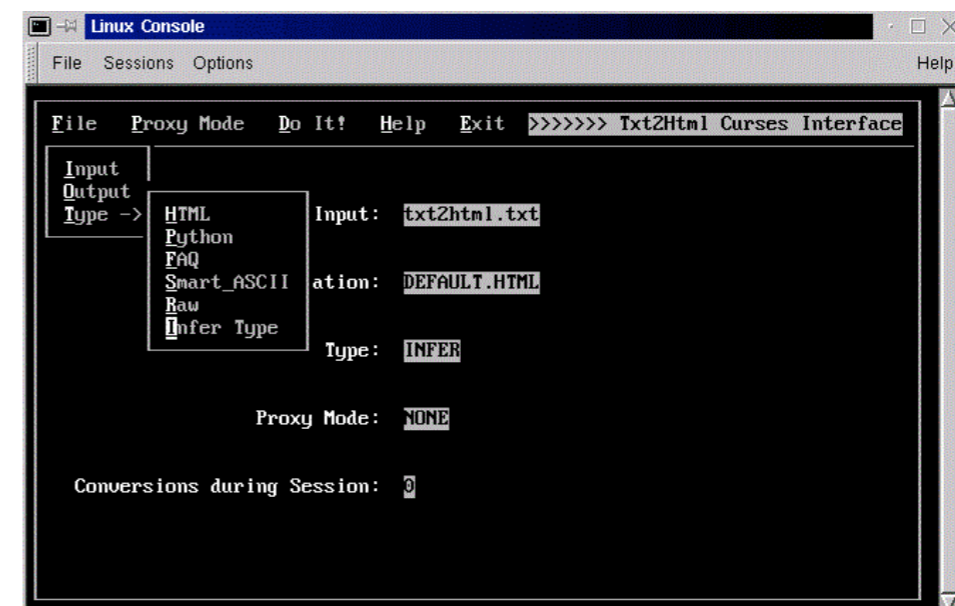
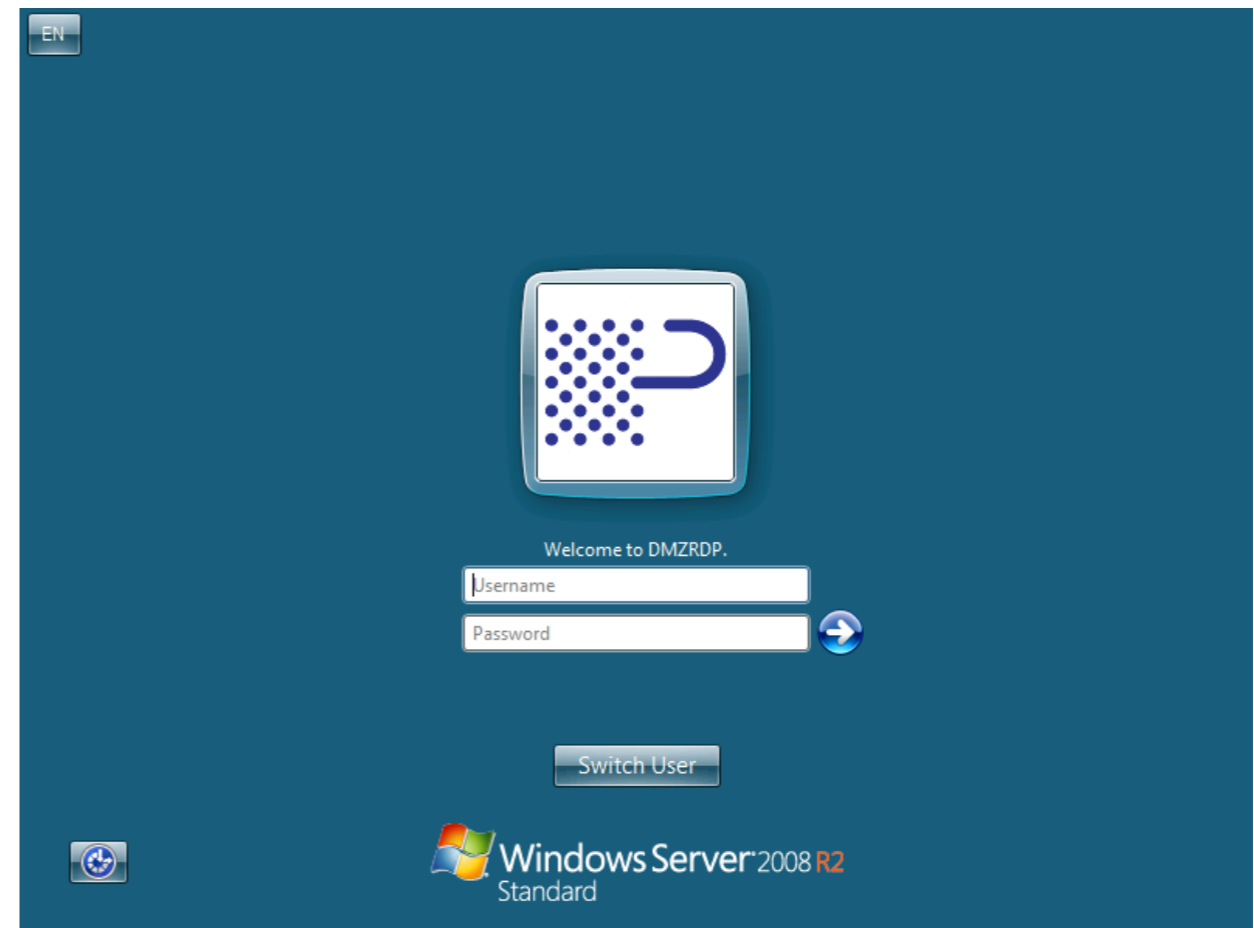


Login



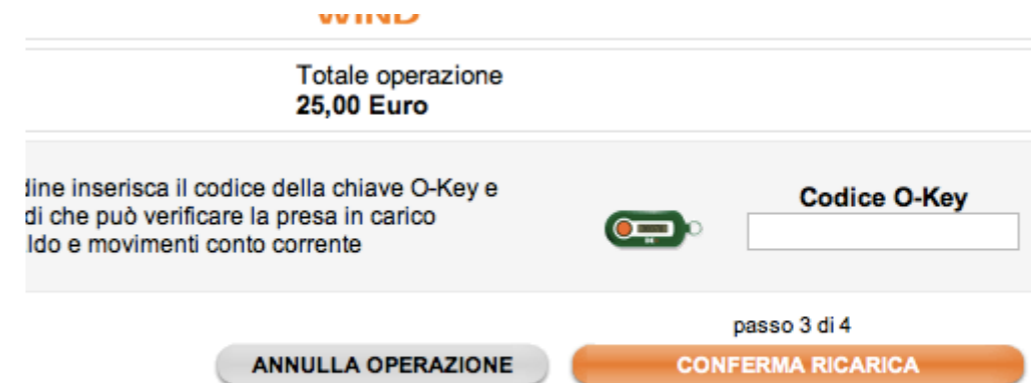
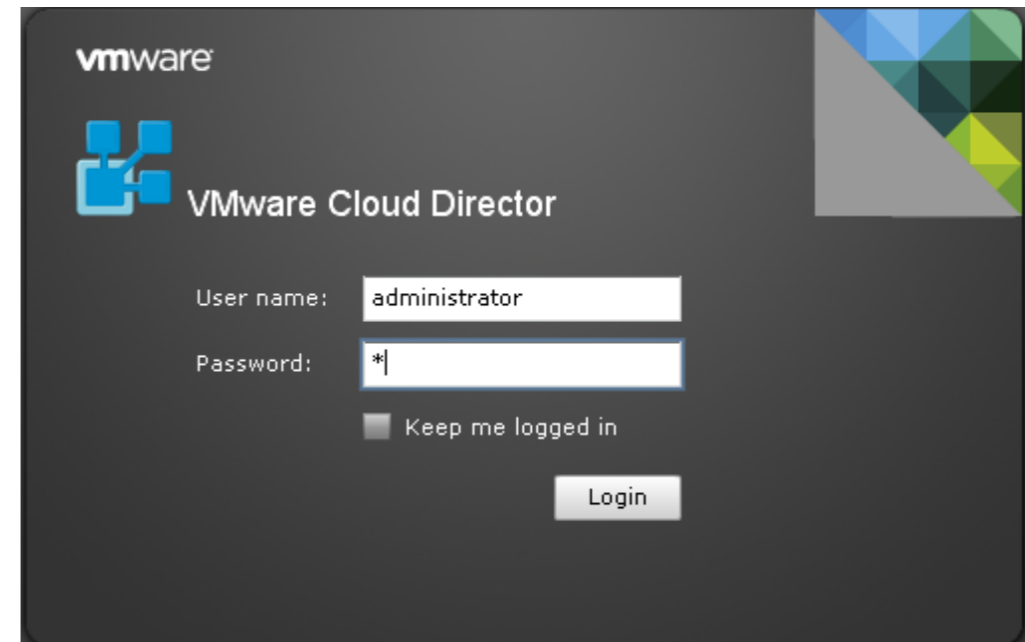
Esempi: Applicazioni tradizionali

- Accesso sicuro a server ed applicazioni che:
 - Sono pubblicati su Internet o Extranet
 - Contengono dati riservati
- Ad esempio accedendo all'applicativo via:
 - Windows Terminal services via RDP
 - SSH ad un host Unix
- Secure File Transfers (SFTP/SCP)



Esempi: Infrastrutture Cloud e applicativi speciali

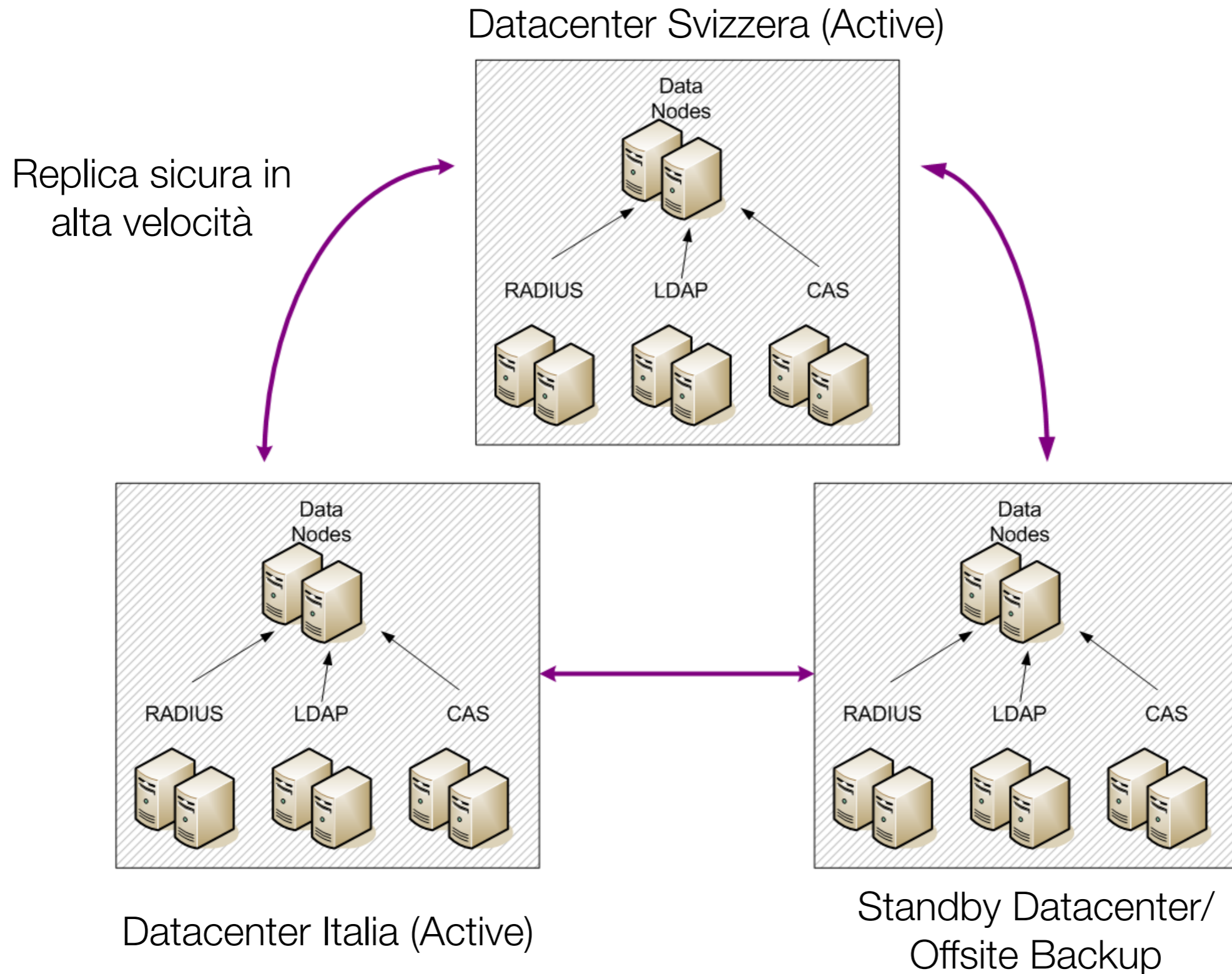
- VMWare Cloud Director
- Qualsiasi sistema di cloud management (es: XenServer) compatibile con:
 - RADIUS
 - LDAP
- Sistemi autorizzativi
 - es: banche e istituti finanziari, istituti governativi, ecc



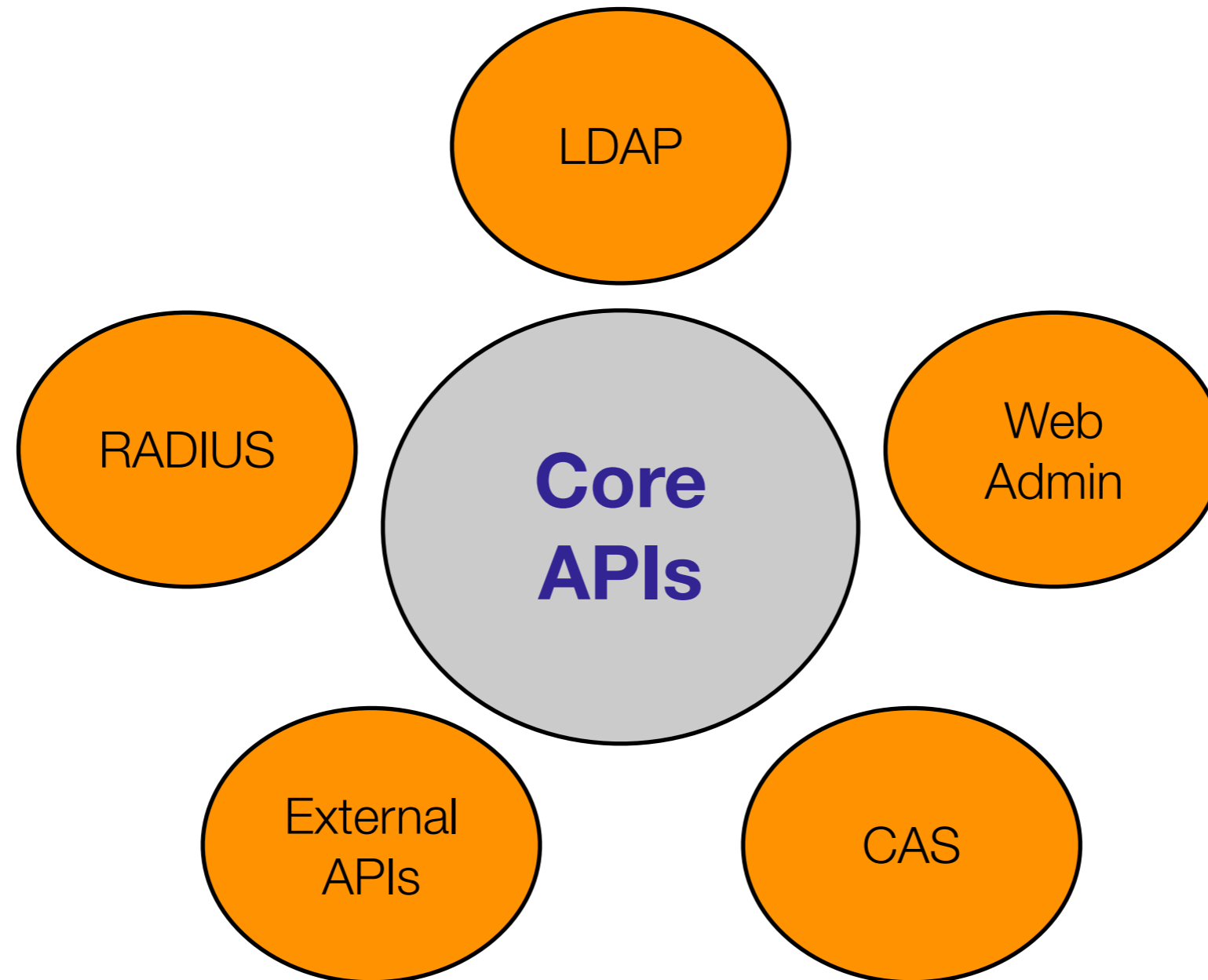
L'approccio “alla Google”

- Una “banca delle identità” deve essere scalabile e resiliente
 - **deve poter scalare** e posizionare i dati il “più vicino possibile” al cliente
 - **deve sopravvivere a multiple failures**, da quelli locali (rottura dei server e degli apparati) a down di un interno datacenter e/o di dorsali Internet di una o più nazioni
- I software “tradizionali” non sono pronti ad un sistema scalabile a piacere: durante i test abbiamo trovato limitazioni sui databases SQL e su LDAP con più di 3-4 datacenters
- Il software e' stato scritto da zero interamente in-house, incluse le interfacce RADIUS e LDAP
- Si e' usato un approccio de-strutturato come quello adottato da Google

SecurePass in architettura Multi-Datacenter



SecurePass: l'architettura software



I meccanismi di protezione di SecurePass

- Macchine fisiche presidiate e in ambiente ad accesso riservato
- Sicurezza dei dati su tutti i livelli dello stack ISO/OSI
- Accesso ai servers soltanto da parte del personale consentito
- Accesso dei clienti alla sola porzione dei dati a loro riservata
- Autorizzazione di accesso multi-livello
- Protezione anti-DoS nativa
- Network Protection & Isolation

Network Protection & Isolation



Acme Inc
valid user



Acme Inc



FooBar Inc

La nostra tecnologia esclusiva di **Network Protection & Isolation** limita l'accesso di un utente al solo apparato o applicazione a cui ha diritto di accedere. SecurePass e' in grado di riconoscere da quale apparato o applicazione proviene la richiesta di autenticazione, se l'apparato o l'applicazione e' valido/a e se l'utente e' abilitato ad accedere da quella risorsa.

Presenza

- SecurePass è un servizio di GARL Sagl
- Sede principale in Svizzera e ufficio a Londra
- Partner presenti sul territorio: Svizzera, Italia, Turchia e UK
- La lista dei partner su www.secure-pass.net



SECURE  **PASS**™
Protecting Identities.

**The Swiss Identity Bank
you trust**

Registrati su:
www.secure-pass.net

ed usa il promo code **smau2011**

