]HackingTeam[| Cassa Centrale Banca Credito Cooperativo del Nord Est

Cassa Centrale

Progetto Strong Authentication

Allegato tecnico relativo alla strong authentication

Milano

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
0.1	11 Giugno 2008	Emissione
//	//	//
//	//	//

INFORMAZIONI		
Data di Emissione	11 Giugno 2008	
Versione	0.1	
Tipologia Documento	Allegato Tecnico	
Numero di Protocollo	//	
Numero Pagine	7	
Numero Allegati	0	
Descrizione Allegati	1	//
	2	//
Redatto da	Danilo Cordoni	
Approvato da	Banfi Roberto	

INDICE

1 Obiettivo

Lo scopo del presente documento consiste nel descrivere la soluzione di strong authentication nella infrastruttura di rete di Cassa Centrale. La delivery di questa soluzione permetterà al cliente di implementare un sistema di autenticazione centralizzato tramite l'utilizzo di token USB con i quali gli utenti potranno accedere al dominio e autenticarsi a diverse applicazioni web.

2 Analisi dei requisiti

Requisiti necessari per l'implementazione della soluzione:

- Modulo HSM (Hardware Security Module), utilizzato per memorizzare in modo sicuro le chiavi utilizzate per l'autenticazione.
- Database di back-end, MS SQL Server o Oracle.
- Certification Authority e Directory Service.
- Key Management System (KMS), applicazione stand-alone che permette la gestione del modulo HSM.

3 Ambiente di riferimento

E' possibile implementare la soluzione proposta senza dover modificare in modo significativo l'ambiente esistente, grazie all'integrazione con i sistemi già presenti nell'infrastruttura di Cassa Centrale, come i Directory Service LDAP la Certification Authority.

4 La soluzione proposta

4.1 La tecnologia

La soluzione di strong authentication proposta è basata sul software ActivID Card Management System di ActivIdentity. Questo sistema prevede un'architettura suddivisa logicamente in 3 sistemi con funzioni specifiche:

1. **CMS:** Card Management System è l'interfaccia di gestione del sistema, permette la gestione degli utenti, delle smartcard o dei token, la definizione delle policy per il deployment delle card.
2. **Hardware Security Module (HSM):** permette di generare e memorizzare le chiavi in modo sicuro.
3. **KSM (Key Management System):** sistema di gestione, manutenzione, backup e aggiornamento del Hardware Security Module.

La soluzione può essere implementata in modi differenti. Per ognuno di essi riportiamo le modalità di implementazione e i relativi vantaggi-svantaggi:

- **Senza HSM:** è possibile implementare la soluzione di strong authentication di ActivIdentity senza l'utilizzo del HSM.

  Vantaggi : maggior semplicità d'implementazione;

  Svantaggi: la soluzione proposta senza l'utilizzo di HSM non è certificata da ActivIdentity per cui non vi è alcun supporto da parte di ActivIdentity.

- **HSM PCI:** questa soluzione prevede l'utilizzo dell'HSM nella versione scheda PCI che deve essere installata su un server, sul quale deve risiedere anche il KSM ed eventualmente il CMS.

  Vantaggi: supporto ActivIdentity e maggiore sicurezza complessiva.

  Svantaggi:

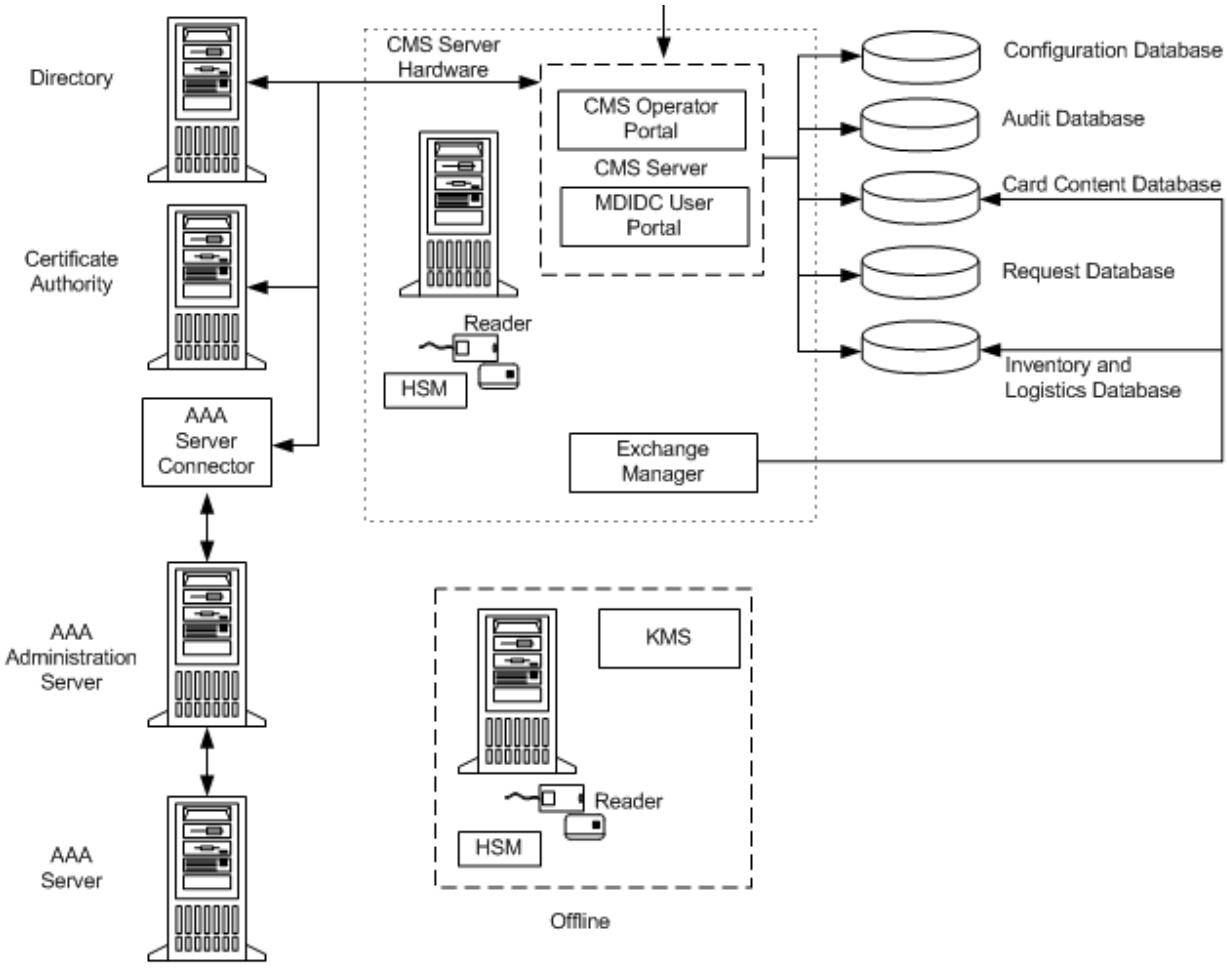
  - utilizzo di un server dedicato all'HSM e KSM, che eventualmente possono essere accorpati sul server CMS;
  - la gestione può avvenire solo localmente (tramite autenticazione con smartcard ad hoc).

- **HSM appliance:** questa soluzione prevede l'utilizzo dell'HSM in versione appliance.

  Vantaggi:

  - l'appliance può essere raggiungibile a livello rete;
  - possibilità di espansione del progetto ad un numero di utenti molto elevato.

4.2 Schema logico



5 Vantaggi della soluzione proposta

La soluzione proposta permette di implementare una soluzione completa volta ad centralizzare il sistema di autenticazione degli utenti aziendali, semplificando la gestione degli utenti stessi e delle relative policy di gestione delle password. Infatti tramite l'utilizzo dei token USB gli utenti possono effettuare il login al dominio aziendale e autenticarsi a diverse applicazioni web, che come unico requisito, devono essere compatibili all'autenticazione tramite smart card e tramite certificati.
Alcuni esempi di applicazioni compatibili che si possono integrare con la soluzione proposta sono:

- Citrix;
  http://www.citrix.com/english/ps2/citrixready/product.asp?ContentID=594873
- Microsoft Terminal Services;
  http://www.actividentity.com/solutions/partner/microsoft__overview.php
- Microsoft Office;
  http://www.actividentity.com/solutions/partner/microsoft__overview.php

Inoltre, per quanto riguarda il login tramite USB token, è possibile effettuarlo anche in assenza di connessione alla rete locale, infatti la soluzione implementa un sistema di caching che permette l'autenticazione ad un utente di dominio anche in mancanza di una connessione al dominio stesso (ad esempio un utente che utilizza il proprio notebook aziendale da casa).

6 Considerazioni

La soluzione standard proposta da ActivIdentity prevede l'utilizzo del modulo HSM (al fine di avere a disposizione il servizio di supporto) e prevede anche che i componenti HSM e KSM risiedano sullo stesso server ma preferibilmente non sulla stessa macchina dove è installato il CMS. La soluzione da noi proposta invece prevede l'utilizzo di un unico server in cui vengono installati tutti i tre componenti e come HSM nella versione PCI. Tale proposta è giustificata dalle dimensioni del progetto richiesto, infatti il numero di utenti per cui è stato pensato il progetto non è elevato, quindi l'implementazione di una soluzione standard come quella proposta da ActivIdentity risulterebbe troppo onerosa sia in termini economici che di effort necessario.