Proposta per una soluzione di web federation

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
1.0	Febbraio 2008	Prima emissione

INFORMAZIONI		
Data di Emissione	Febbraio 2008	
Versione	1.0	
Tipologia Documento	Allegato Tecnico	
Numero di Protocollo		
Numero Pagine	13	
Numero Allegati		
Descrizione Allegati	1	
	2	
Redatto da	Costantino Imbrauglio	
Approvato da	Gianluca Vadruccio	

INDICE

1 Introduzione

Il 28 febbraio 1974 é la data ufficiale di nascita di Cassa Centrale, l'Istituto centrale provinciale che le 133 Casse Rurali allora operanti in Trentino avevano visto come necessario per sostenere la propria attività.

La decisione di dare vita ad un organismo che svolgesse attività di coordinamento del credito cooperativo trentino si è dimostrata nei fatti determinante per la valorizzazione del sistema provinciale, come testimoniano i dati storici di sviluppo delle Casse Rurali, la cui quota di mercato nella raccolta è passata dal 38,4% del 1976 al 65,59% del 2006 e nel campo degli impieghi dal 35,08% del 1976 al 55,38% del 2006.

Nel dicembre 2002, in occasione dell'allargamento della base sociale alle BCC del Veneto e del Friuli - Venezia Giulia e dell'aumento del capitale sociale, la denominazione "Cassa Centrale delle Casse Rurali Trentine" è stata modificata in "Cassa Centrale delle Casse Rurali Trentine e delle Banche di Credito Cooperativo del Nord Est SpA".

L'attuale denominazione "Cassa Centrale Banca - Credito Cooperativo del Nord Est SpA", in sigla "Cassa Centrale Banca", è entrata in vigore con delibera dell'Assemblea straordinaria del 13 giugno 2007.

Queste modifiche statutarie, come la costituzione di Centrale Finanziaria del Nord Est, sono state funzionali all'entrata di DZ BANK (DZ BANK AG di Francoforte è uno fra i primi gruppi bancari della Germania) quale nuovo socio di Cassa Centrale Banca.

Già da diversi anni il sistema bancario italiano ha inteso cogliere le opportunità offerte dall'avvento di Internet. Cassa Centrale Banca non fa eccezione. A tal proposito sono stati sviluppati due portali web distinti:

- www.cassacentrale.it
- www.buonconsiglio.com/servizi

Il primo è il portale web istituzionale di Cassa Centrale Banca ed è gestito e sviluppato direttamente da Cassa Centrale Banca.

Il secondo è un portale per l'accesso a svariati servizi ed è gestito e sviluppato dalla società PHOENIX Informatica Bancaria S.p.A.

2 Il portale www.cassacentrale.it

Il portale www.cassacentrale.it è gestito e sviluppato direttamenta da Cassa Centrale Banca. La figura seguente presenta la pagina web di accesso al portale.

Figura 1 - Pagina di accesso al portale www.cassacentrale.it

Il portale www.cassacentrale.it offre una serie di servizi parte dei quali prevede l'accesso a funzioni dispositive. In particolare è possibile raggruppare i servizi con funzioni dispositive offerti dal portale nelle seguenti categorie:

- Mercato dei cambi e pronti contro termine (servizi offerti da Reuters)
- Polizze di previdenza integrativa (servizi offerti da ITAS)
- Fondi e SICAV
- Gestione patrimoniale e retail

L'interfaccia web per l'accesso ai suddetti servizi è realizzata attraverso un front-end sviluppato in ambiente Java/Tomcat.

Le utenze regolarmente censite sono in numero di 5.000 circa. Lo user store contenente i profili e gli account degli utenti è rappresentato da un database MySQL.

Come testè evidenziato, una parte dei servizi offerti dal portale www.cassacentrale.it è in realtà erogato attraverso fornitori esterni (Reuters, ITAS, ecc.). A tal proposito sono stati introdotti opportuni meccanismi di SSO (Single Sign On) per il controllo degli accessi. I suddetti meccanismi di SSO sono implementati grazie all'impiego di opportune librerie rese disponibili dai fornitori medesimi.

3 Il portale www.buonconsiglio.com/servizi

Come anticipato nella precedente sezione si tratta di un portale gestito e sviluppato dalla società di servizi PHOENIX Informatica Bancaria S.p.A. La figura seguente presenta la pagina web di accesso al portale.

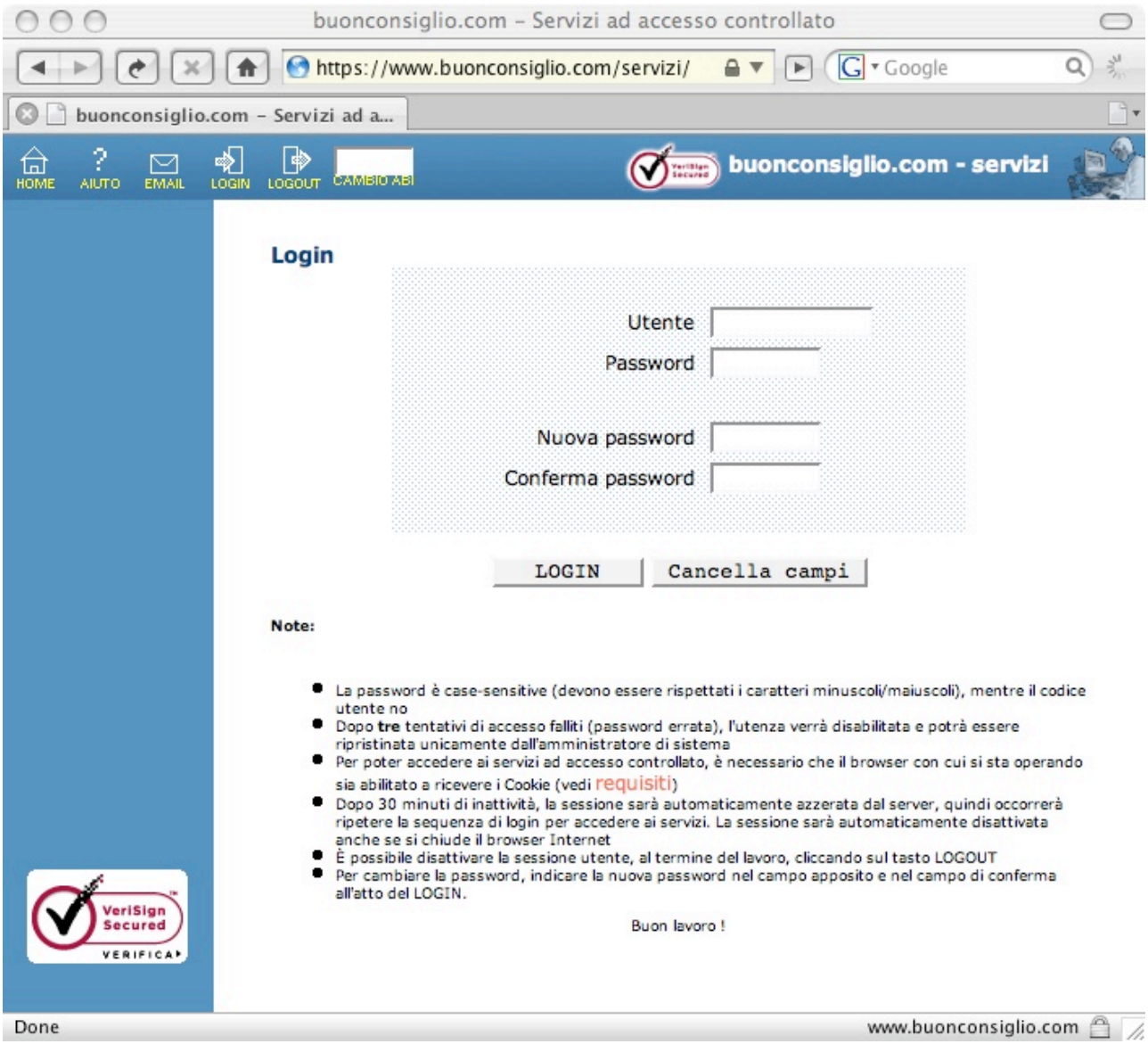

Figura 2 - Pagina di accesso al portale www.buonconsiglio.com/servizi

Il portale www.buonconsiglio.com/servizi offre una serie di servizi molti dei quali richiedono accesso a funzioni dispositive. I servizi in questione sono implementati direttamente a livello di host IBM 3090. L'interfaccia web per l'accesso ai suddetti servizi è invece realizzata attraverso un front-end sviluppato in ambiente IBM WebSphere (l'ambiente operativo è IBM AIX).

Le utenze regolarmente censite sono in numero di 20.000 circa. Lo user store contenente i profili e gli account degli utenti è rappresentato da un database IBM DB2 istanziato sull'host IBM 3090.

Il meccanismo di autenticazione e autorizzazione per il controllo degli accessi e delle transazioni è basato sulla tecnologia IBM RAS/RACF.

4 Il problema dell'autenticazione multipla

L'esistenza di due distinti portali pone un problema di autenticazione multipla. In particolare le utenze censite sul portale www.cassacentrale.it possono essere suddivise in due distinte categorie:

- Utenti che accedono esclusivamente a funzionalità offerte dal portale www.cassacentrale.it
- Utenti che accedono anche a funzionalità del portale www.buonconsiglio.com/servizi

Per quest'ultimo categoria di utenti l'accesso ai servizi è caratterizzato da unidirezionalità nella misura in cui il punto di accesso primario è sempre rappresentato dal portale www.cassacentrale.it (l'accesso ai servizi offerti dal portale www.buonconsiglio.com/servizi avviene per mezzo di opportuni link presenti sulle pagine web del portale istituzionale).

Attualmente i due portali non implementano un meccanismo di SSO (Single Sign On) tra di loro e dunque per accedere ai servizi offerti dal portale www.buonconsiglio.com/servizi è necessario procedere a una seconda autenticazione.

Cassa Centrale Banca sta valutando la possibilità di eliminare il vincolo rappresentato dalla doppia autenticazione. Obiettivo del presente documento è quello di presentare una proposta in questo senso.

Cassa Centrale Banca desidera garantire anche una migliore integrazione dei due portali da un punto di vista grafico e di comunicazione (quest'ultimo tema non è invece oggetto del presente documento).

5 Single Sign On e Web Federation

Il Single Sign On (SSO) è un meccanismo che consente ad un utente di autenticarsi una sola volta e di accedere a tutte le risorse informatiche alle quali è abilitato.

Gli obiettivi sono molteplici:

- Semplificare la gestione delle password
- Semplificare la gestione degli accessi ai servizi
- Semplificare la definizione e la gestione delle politiche di sicurezza
- Migliorare l'esperienza di navigazione dell'utente

Vi sono essenzialmente due approcci per la creazione di un sistema di SSO:

- **Approccio centralizzato** – Prevede l'esistenza di un unico user store globale e centralizzato di tutti gli utenti. Al contempo è prevista una gestione centralizzata della sicurezza. Questo approccio è destinato principalmente a servizi dipendenti dalla stessa entità (per esempio all'interno di una stessa azienda).
- **Approccio federativo** – Questo approccio prevede che differenti gestori ("federati" tra loro) gestiscano dati di uno stesso utente. L'accesso ad uno dei sistemi federati permette automaticamente l'accesso a tutti gli altri sistemi.

  Ad esempio un viaggiatore potrebbe essere sia passeggero di un aereo che ospite di un albergo. Se la compagnia aerea e l'albergo usassero un approccio federativo avrebbero un accordo reciproco sull'autenticazione dell'utente. Il viaggiatore potrebbe ad esempio autenticarsi per prenotare il volo ed essere autorizzato, in forza di quella sola autenticazione, ad effettuare la prenotazione della camera d'albergo.

  Questo approccio è stato sviluppato per rispondere ad un bisogno di gestione decentralizzata degli utenti: ogni gestore federato mantiene il controllo della propria politica di sicurezza.

6 Gestione delle identità federate

Una federazione è definita come un raggruppamento di due o più partner legati tra loro da un rapporto di fiducia nonché da accordi legali e di business. La partecipazione in una federazione consente a un generico utente di uno dei partner di accedere alle risorse e ai servizi offerti da uno qualsiasi degli altri partner in maniera diretta e trasparente.

Le funzionalità offerte da un sistema di gestione delle identità federate (Federated Identity Management – FIM) garantiscono ai partner della federazione i seguenti vantaggi:

- Ridurre i costi di gestione delle identità digitali
- Migliorare l'esperienza dell'utente nella fruizione dei servizi
- Ridurre i rischi connessi alle transazioni

Quando si parla di Federated Identity Management, si fa in realtà riferimento a tre aree distinte:

- Web-based Single-Sign-On e/o Federated Single-Sign-On
- Application based web services security
- Identity life cycle

Le federazioni vengono definite essenzialmente per facilitare il perseguimento di due obiettivi:

- Possibilità per un utente di interagire con i servizi distinti offerti dai vari partner della federazione in modalità sicura e trasparente (federated single-sign-on)
- Possibilità di far interagire applicativi distinti in maniera sicura e trasparente

In entrambi i casi è richiesta l'implementazione di una cosidetta infrastruttura di trust. La figura seguente ne illustra il modello.

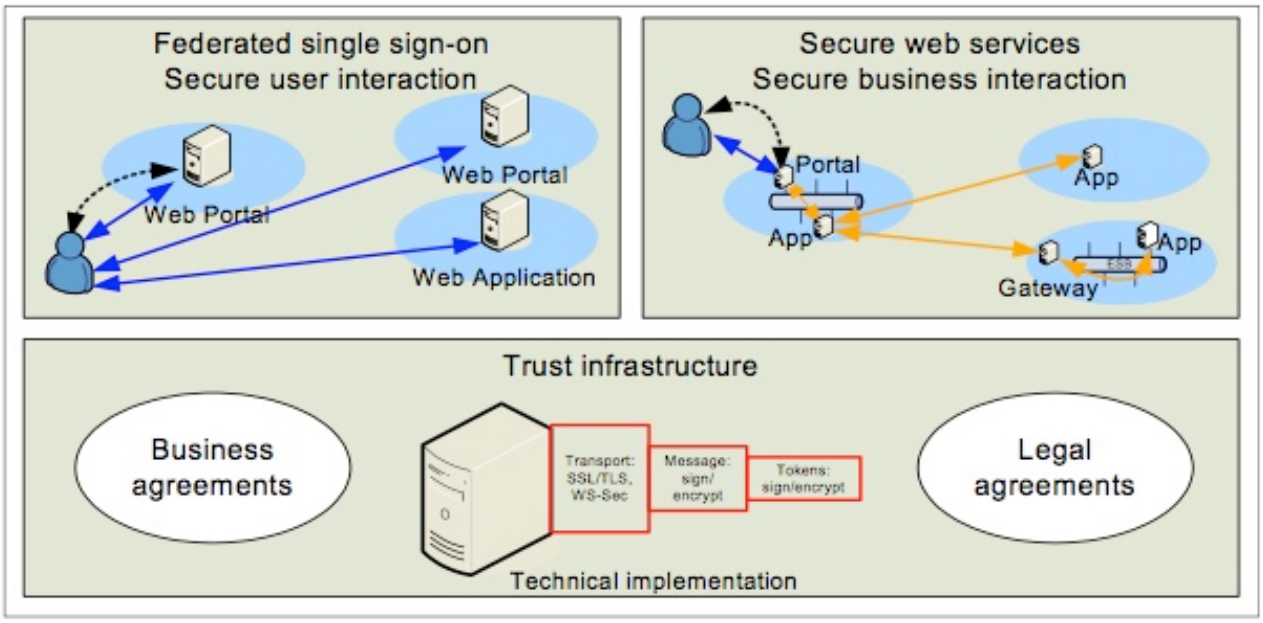

Figura 3 - Infrastruttura di trust

Con l'espressione *federated identity management* si fa spesso riferimento all'interazione tra diversi servizi a livello di web browser. In questo senso sono stati definiti diversi standard (SAML, Liberty Alliance, ecc.) che regolano anche tutti gli aspetti legati alla gestione delle sessioni e dunque non solo gli aspetti legati ai processi di autenticazione.

La realizzazione di una soluzione di federated identy management richiede una piena comprensione delle seguenti aree tematiche:

- Ruoli in seno agli identity provider e ai service provider (ovvero la definizione della sorgente autoritativa per quanto attiene ai profili e alle identità digitali)
- Mappatura delle identità e degli attributi (ovvero la definzione degli attributi condivisi e la mappatura dei medesimi sui vari sistemi federati)
- Gestione e provisioning degli account utente (ovvero le procedure per la gestione delle identità digitali e l'assegnazione delle risorse condivise)
- Account linking (ovvero il processo di mappatura degli account)

- Trust (ovvero la definizione dei processi volti a garantire sicurezza nelle connessioni e nei canali di comunicazione, nonché nei messaggi e nei token)