



**CONSORZIO CBI**  
customer to business interaction

# **L'Infrastruttura CBI tra sicurezza ed efficienza**

**Liliana Fratini Passi**

*Direttore Generale*

**Consorzio CBI**

*Roma, 6 giugno 2013*

# Agenda

**1.**

**Il Consorzio CBI**

**2.**

**Il Consorzio CBI e la sicurezza: una gestione che va oltre il concetto di «tutela»**

## La nostra mission

**Lo sviluppo e la manutenzione dell'infrastruttura tecnica** destinata a consentire il collegamento ed il colloquio tra i consorziati e la propria clientela **per l'erogazione del Servizio CBI**, nonché la definizione delle regole e degli standard tecnici e normativi del Servizio, su base sia nazionale che internazionale.

### Infrastruttura di rete

- Soluzione telematica per la gestione di **più conti presso diverse banche**
- **Colloquio End to End** tra i diversi attori
- **Nodo CBI**



### Comunità estesa

#### • Conсорziati



- Istituti finanziarie : **615**
- Poste e IMEL CartaLis
- Nuovi PSP

**Posteitaliane**

#### • Clienti

- Imprese: **890.000**
- PA



- Disponibilità di oltre **40 funzioni** (Servizio CBI) innovative in area:
  - **Incasso/ pagamento,**
  - **Gestione documentale**
  - **Informativa**
- **~4,4 mld** di transazioni/anno

- **Servizio di Nodo CBI** tra Pubblica Administration Centrale e Sistema Bancario

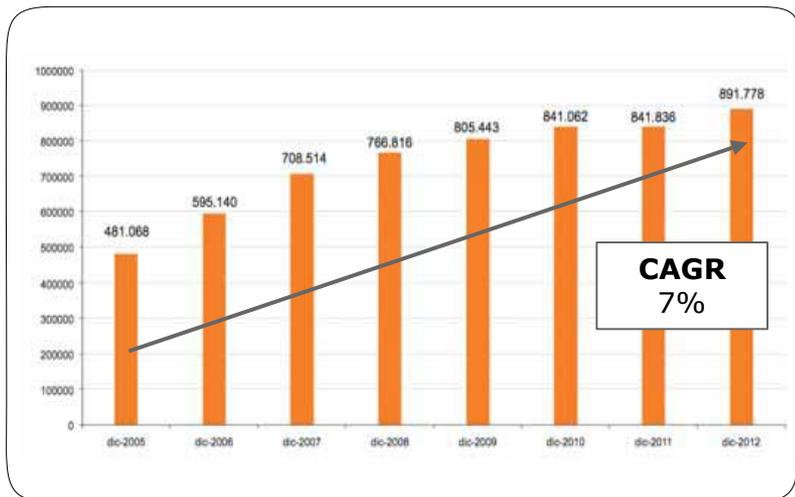
- **3 Pubbliche Amministrazioni Centrali**

**Organismo di standardizzazione**

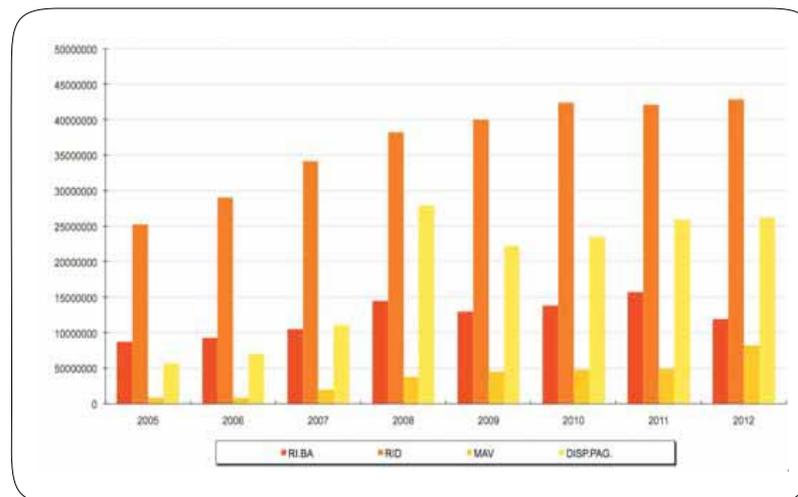
**Nodo CBI per le Pubbliche Amministrazioni**

# Trend di crescita del Consorzio CBI

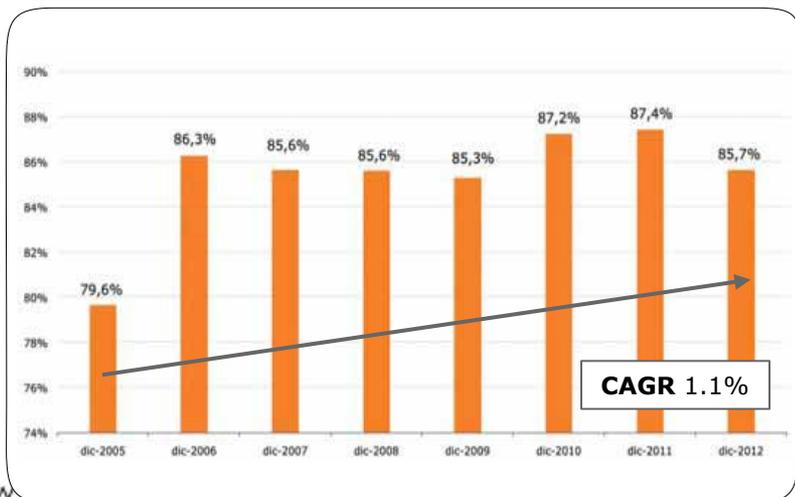
## Utenti Corporate



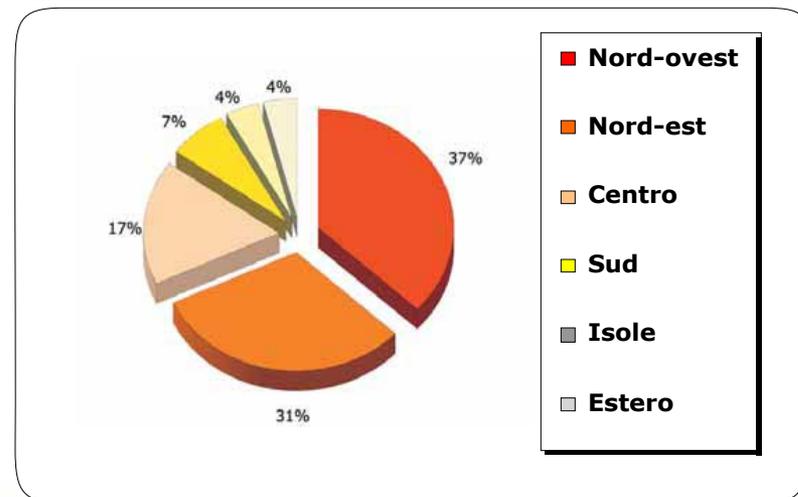
## Ordini di incasso/Ordini di pagamento



## Consoziati (% dell'intero sistema bancario)



## Distribuzione geografica Consoziati



# L'infrastruttura tecnologica del Consorzio CBI, la Governance e la gestione della Sicurezza



## Gestione della Sicurezza

- 1.**

  - Riservatezza ed **integrità dei flussi** di dati tramite lo standard di interconnessione sicuri
  - **Protezione** da tutti gli accessi indesiderati e tracciabilità dei tentativi di intromissione
  - Controllo costante sull'**integrità degli apparati** utilizzati
  - Autenticazione mutua delle componenti architeturali
- 2.**

  - **Autenticazione** mutua tra le componenti **hardware e software** di interfaccia
  - Utilizzo di **componenti di sicurezza** per separare la rete interna della Banca/STD dalla Rete della Nuova Architettura
  - Accesso alle componenti locali di amministrazione tramite **protocolli sicuri** (es. HTTPS)
- 3.**

  - **Firma digitale** sulla base dello standard XMLSignature (W3C)
  - Istituzione dell'albo delle CA accreditate presso il CBI
  - **Crittografia** sulla base dello standard XMLEncryption (W3C)

**La Rete CBI garantisce autenticità, riservatezza ed integrità delle informazioni**

# I servizi del Consorzio CBI

## 1 Servizio CBI

- Servizio CBI consente a ciascun utente mono/multibanca di **interfacciarsi** con uno solo tra i propri Istituti finanziari per effettuare operazioni di **tesoreria complesse** con tutti gli altri Istituti finanziari con cui intrattiene rapporti di conto corrente



## 2 Servizio Nodo CBI

- Servizio di **gateway che permette l'accesso diretto delle PA Centrali alla rete CBI** per lo scambio di flussi con il sistema finanziario/Poste

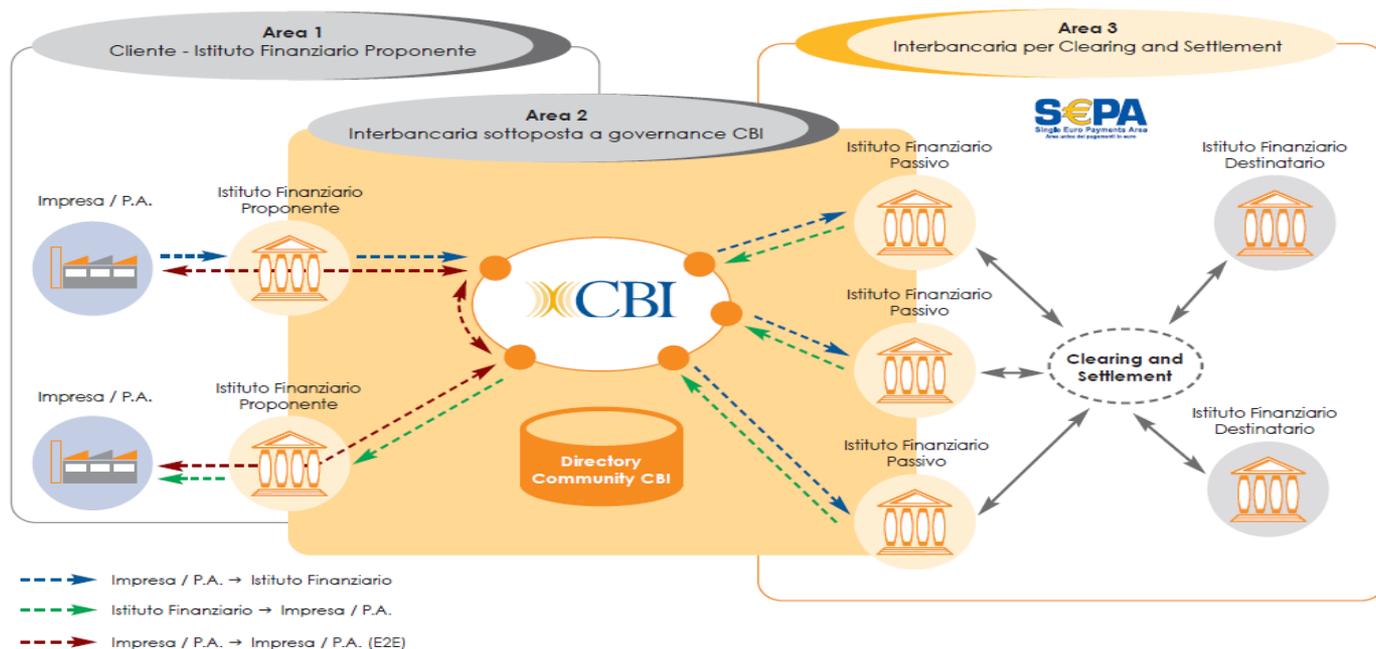
## 3 Servizio CBILL

- Servizio di **e-billing** che consente la **consultazione** e il **pagamento di «bollette»** rivolto a tutti i clienti retail e ai clienti corporate, nel ruolo di Biller



NEW

## L'architettura del Servizio CBI



## Principali evidenze

**Affidabilità e  
sicurezza della  
Rete**

- **Controllo degli accessi** realizzato secondo una politica di tipo RBAC (Role Based Access Control), pertanto l'accesso è selettivamente stabilito secondo delle politiche che attribuiscono ruoli e responsabilità in modo ben definito
- **Meccanismi di crittografia IPSec** garantiscono anche la salvaguardia dell'integrità dei dati trasferiti in rete end-to-end
- Gli apparati centrali e periferici installati presso gli Istituti implementano funzionalità sia di **controllo del traffico** (firewall) sia di **cifratura dei dati**

Per ottemperare alle richieste delle PA Centrali, le **Banche** aderenti al Consorzio CBI hanno **investito** nella creazione del **Nodo Diretto di accesso CBI**, al fine di **supportare il collegamento tra PA Centrali e rete bancaria**

### L'architettura del Servizio Nodo CBI



### Principali evidenze

**Affidabilità e sicurezza del Nodo a supporto della PA**

- **Meccanismi di crittografia IPSec** garantiscono anche la salvaguardia dell'integrità dei dati trasferiti in rete attraverso il Nodo CBI
- Attivazione di un programma periodico di **Security Assessment** (cfr slide succ)
- Applicazione di **standard di sicurezza interbancari internazionali**



Il servizio CBILL consente:

- **Consultazione delle bollette** dei Biller CBI da parte dei clienti debitori delle Banche CBI
- **Pagamento** delle bollette tramite i **multi-canali bancari** (Home Banking, Corporate Banking, ATM, Mobile,...)
- Ricezione del parte del Biller di un **esito di pagamento** con collegamento alla bolletta inviata

## Principali evidenze

**Affidabilità e sicurezza**

- Basato su **business model internazionali**
- Realizzato in **cooperazione** con tutta l'industria finanziaria
- La **Rete CBI** è l'asset di veicolazione interbancaria su cui sono veicolate **milioni di transazioni finanziarie**
- **Nodo CBI** nel ruolo strategico di interconnessione con le PA per erogare servizi e-billing alle stesse PA
- **Standard di sicurezza** interbancari internazionali

**Garanzia di paradigmi EBPP consolidati a livello internazionale**

**Utilizzo di asset CBI (Rete e Nodo) ed interni dei consorziati**

\*I Consorziati potranno proporre il servizio dal **01/02/2013**. Al fine di garantire la **circularità** del servizio le Banche aderiranno nel ruolo di Intermediario dell'Utente in modalità **obbligatoria** entro il **II quarter del 2014**. Le banche del Consiglio CBI, (90% della quota di mercato) aderiranno nel ruolo di Intermediario dell'Utente il modalità obbligatoria entro il **IV quarter del 2013**

# Agenda

**1.**

**Il Consorzio CBI**

**2.**

**Il Consorzio CBI e la Sicurezza: una gestione che va oltre il concetto di «tutela»**

# Oltre alle attività "core" di tutela dei Consorziati, il CBI è impegnato in un programma di Security Assessment...

## Razionali

- La **Rete CBI** rispetta i più alti requisiti tecnologici di **sicurezza**.
- Per garantire la non vulnerabilità della rete occorre agire sui **Nodi di Accesso**
- Consorzio CBI, in qualità di soggetto erogatore di un punto d'accesso alla propria rete, ormai da due anni pianifica un attività di **Security Assessment** attuata sul Nodo CBI

## Programma di Security Assessment

### Obiettivo

- **Analizzare annualmente** i processi per verificare il **livello di sicurezza** delle applicazioni bancarie, del middleware e delle interfacce software (es. front-end web) realizzate dal fornitore dei **servizi di Nodo**, attraverso le quali il Consorzio CBI consente l'accesso alle PPAA.

### Tipologia di test eseguiti

#### Network Penetration Test

- Verifica della **sicurezza** dei servizi di rete che il **Nodo CBI** espone su Internet

#### Web Application Penetration Test

- Identificazione di possibile **vulnerabilità** dell'**applicazione** web messa a disposizione delle Pubbliche Amministrazioni Centrali

## Scenario di riferimento

Recenti analisi\* sul fenomeno delle **frodi informatiche** hanno evidenziato:

- un consistente **aumento** dei **tentativi di frode** sul canale Internet Banking
- il segmento di clientela **Corporate è maggiormente «attaccato»** a causa di una scarsa attenzione al fenomeno da parte delle PMI

## Iniziativa Consorzio ABI Lab e Consorzio CBI

### Obiettivo dell'iniziativa

- Elaborare un **documento di raccomandazioni** per le **Banche** che interagiscono direttamente con la **clientela Corporate per promuovere azioni di contrasto e di prevenzione delle frodi su Servizi di Internet Banking**

### Documentazione

a  
**Elementi di attenzione per le Banche**

### Obiettivo

- Suggestire le azioni di rafforzamento delle attività di **presidio, contrasto e prevenzione delle frodi**
- Promuovere la consapevolezza di un **utilizzo sicuro** dei servizi di **Internet Banking** all'interno della azienda sul tema del cybercrime

La documentazione è stata inviata ai Consorziati ed è disponibile sui portali CBI e ABI Lab nelle relative Aree riservate

\* Report dell'Osservatorio Sicurezza e Frodi Informatiche ABI Lab, edizioni 2012 e 2013

\*\* In collaborazione con la Polizia Postale e delle Comunicazioni

**Obiettivo del documento**

- Suggestire le azioni di rafforzamento delle attività di **presidio, contrasto e prevenzione delle frodi**

**Destinatari**

- **Banche che interagiscono direttamente con la clientela Corporate** e che offrono loro servizi attraverso le proprie piattaforme\*

**Principali contenuti**

**Infrastruttura**

- Adozione di un **secondo fattore di autenticazione**
- Introduzione di un **secondo canale di comunicazione** in fase di notifica delle operazioni
- **Profilazione utenti** del portale di Internet Banking
- **Vulnerability assesment e Penetration Test**

**Processi**

- Attivazione di **monitoraggio / controllo degli accessi** e operazioni
- Adozione di tecnologie e processi a **protezione dei PC Cliente**
- Attivazione di «**Info Sharing**» intra e intersettoriali, in particolare con le Forze dell'Ordine

**Orientamento al cliente**

- **Sensibilizzazione della Clientela Corporate** sul tema della sicurezza dei pagamenti online
- Ulteriori misure di sicurezza (es. condividere con le imprese clienti le policy adottate dalle aziende stesse in materia di sicurezza informatica)

\* **Non sono interessate le tratte c.d. "multibanca"**, in cui l'esecuzione dei servizi telematici si avvale di infrastrutture interbancarie, quali la rete CBI, e/o soggetti intermedi che fungono da gateway di accesso, per cui sono già applicati elevati standard di sicurezza.

## b Azioni di sensibilizzazione per Clientela Corporate

### Obiettivo del documento

- Promuovere la consapevolezza di un **utilizzo sicuro** dei servizi di **Internet Banking** all'interno della azienda sul tema del **cybercrime**

### Destinatari

- **Banche che interagiscono direttamente con la clientela Corporate.** Ciascuna Banca può utilizzare la documentazione predisposta a supporto della propria attività di comunicazione verso la clientela Corporate

### Principali contenuti

#### Policy aziendale

- Suggestire la **definizione di policy aziendali** e attività di controllo che si ritiene utile implementare all'interno dei diversi contesti aziendali, in fase di:
  - accesso ai siti di Internet Banking
  - esecuzione delle operazioni informative e dispositive

#### Protezione delle postazioni

- Suggestire utili indicazioni per la **protezione delle postazioni dalle quali viene svolta l'attività di Internet Banking** (PC utente) ai fini della protezione delle credenziali di autenticazione e dei dati bancari sensibili

#### Buone pratiche di comportamento

- Suggestire **buone pratiche di comportamento per l'utilizzatore dei servizi di Internet Banking**» per conto delle aziende da porre in essere, in modo da incrementarne ulteriormente i livelli di sicurezza

# Grazie dell'attenzione



CONSORZIO CBI  
customer to business interaction

**Consorzio CBI**  
**P.zza del Gesù 49**  
**00186 Roma**  
**[www.cbi-org.eu](http://www.cbi-org.eu)**