

**Un approccio integrato  
al furto di identità.**

**L'esperienza CREDEM**

*Lorenzo Grillo – Country Manager VeriSign Italia*

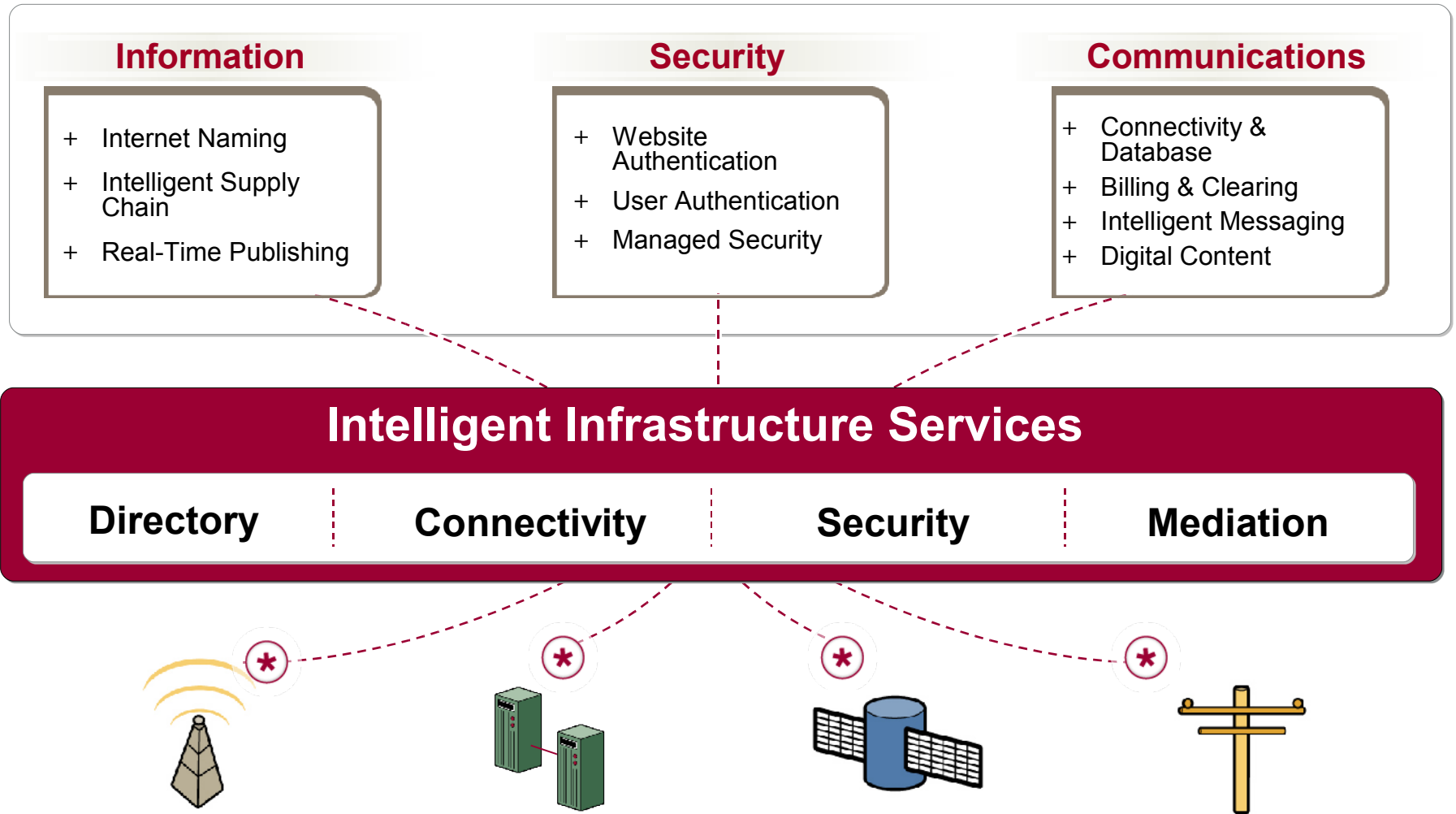


**Where it all comes together.™**

- + **Presente in 75 paesi,**
  - 4600 dipendenti nel mondo
- + **HQ a Mountain View, CA**
  - S&P 500 and Fortune 1000 company
- + **Stato patrimoniale**
  - Più di \$760m in cash, equivalents and investments
- + **Fatturato 2006: \$1.6b**
  - Capitalizzazione \$6b
- + **Fondata 1995**
  - IPO nel 1998



# Servizi VeriSign – Enable and Protect



# VeriSign Security Services, molto più di SSL

## Assicurare la Conformità agli standard

- Compliance assessments and audits
- Compliance through co-managed services
- Host Log monitoring

## Prevenire le Frodi interne

- Vulnerability assessment
- Post incident forensics
- Protecting data across internal networks
- Identity and access management

## Assicurare la “Data Privacy”

- Data across internal & external networks
- Data privacy best practice

## Prevenire le Frodi online

- Anti-phishing and incident response
- Brand protection
- Risk based Authentication
- Consumer Two Factor Authentication
- PCI Assessment and Audit

## Minimizzare le minacce esterne

- Firewall management
- Managed intrusion prevention & detection
- Penetration testing

## Migliorare l’efficacia operativa

- Correlated alerts to prioritise vulnerabilities
- Prioritised patch management
- Co-management of non core tasks

# LA MINACCIA – La visione dell'utente



- + *“...consumers that have a high level of trust ... are most likely to use the bank for a wider variety of complex online banking tasks than those who don't have such a degree of faith in their bank”*
- + *“...57 per cent of interviewees who stated they have a high trust in their primary bank will stop ... using the bank's online services in the event of a single privacy breach.”*
- + *“...there are lots of security measures which are not user-friendly. The challenge is to find a balance between the amount of security and user-friendliness.”*

**SOURCE:** Datamonitor - Online Banking Strategies in Europe Report 2006

<http://www.datamonitor.com/~f9ebf933ee3b40b1bacfbb6b9b40f4cb~/industries/research/?pid=DMFS1950&type=Report>

# LA MINACCIA – Crimine Organizzato

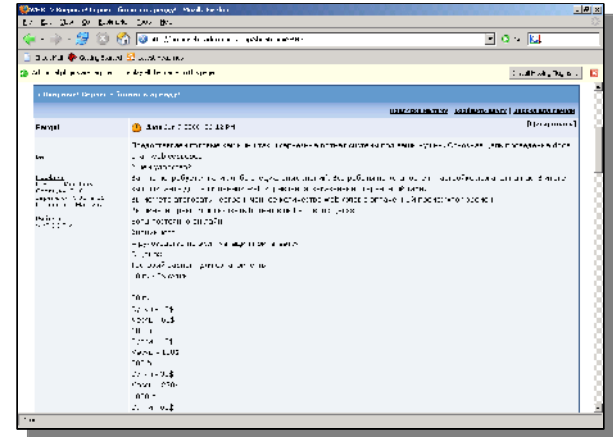
## + Il Crimine organizzato è maturato da diventare un'industria

- Per divertimento
- Per notorietà
- Per profitto (non organizzato)
- Per profitto (poco organizzato)
- Per profitto (Molto ben organizzato)



# LA MINACCIA - Botnets in vendita o in affitto

- + **10 botnets**
  - \$5 per 24 ore di test e familiarizzazione
  
- + **50 botnets**
  - \$10 per un periodo di 24 ore, \$60 al mese
  
- + **100 botnets**
  - \$15 per 24 ore, \$120 al mese
  
- + **500 botnets**
  - \$30 per 24 ore, \$220 al mese
  
- + **1,000 botnets**
  - \$60 per 24 ore, \$550 al mese



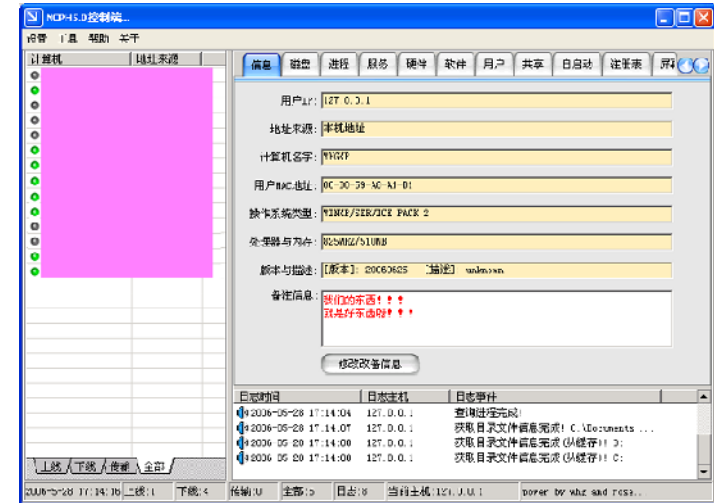
June 2006 posting on Russian hacker forum

***“I servizi di consulenza e di setup sono gratuiti.  
Sconti significativi nel caso di **partnership operations**.”***

SOURCE: iDefense Intelligence Report July 2006

# LA MINACCIA – Offerte di lavoro x hacker

- + **N.C.P.H: Network Crack Program Hacker**
  - Condotta da “Wicked Rose” in Sichuan, China
- + **Una società sconosciuta paga \$625 al mese**
  - Exploit/rootkit development work



**NCPH 5.0 rootkit control console**

SOURCE: iDefense Intelligence Report ID# 448399, May 19, 2006 NCPH Forum

# LA MINACCIA – Definizione di Frode Online

## + **Definizione VeriSign di Frode Online nel settore bancario**

- Account takeover
- Application fraud
- Online CNP (card not present)

# Account takeover – MINACCE

## + **Esempi correnti**

- Phishing
- Pharming
- Man in the middle
- Socially engineered phone calls or SMS
- Trojans delivering key loggers

## + **Emergenti o previsti**

- Trojan Phishing (MetaFisher)
- “Contact us” phishing

# Application fraud – MINACCE

## + **Esempi correnti**

- “Dumpster” Diving
- Trojans delivering key loggers
- Packet sniffing

## + **Emergenti o previsti**

- “Phoraging”
- The impact of semantic Web

# Online Card Not Present – MINACCE

## + **Esempi correnti**

- Lost
- Stolen
- Counterfeit
- Stolen CC records
- Man in the Middle
- Packet sniffing

## + **Emergenti o previsti**

- Nessuno noto al momento

## + **Banca fortemente orientata ai canali online:**

- **Prima Banca in Italia ad inviare documenti online ai clienti**

- + **Banca fortemente orientata al cliente:**
  - Sondaggio interno sulla soddisfazione dei clienti nei riguardi della sicurezza dell'e-banking: clienti molto soddisfatti.
  - Nonostante i risultati del sondaggio, si è avviato il progetto sulla “Strong Authentication”.

## + **Problematiche da anticipare:**

- Phishing/Pharming
- Fiducia dell'utente nell'e-banking → aumento numero utenti online
- Semplificazione procedura autenticazione

## + Un approccio integrato al furto di identità

- **Formazione clientela su procedure sicurezza e call center (sezione sito: SICUREZZA ONLINE)**
- **Monitoraggio e protezione del brand (Antiphishing e Antipharming)**
- **Autenticazione del sito all'utente**
- **Autenticazione dell'utente al sito**
- **Messaggi email e/o SMS all'utente per ogni attività sul sito di Internet Banking: collegamento, cambio pwd, cambio indirizzo email, operazioni dispositive.**

# Monitoraggio e Protezione del Brand: Servizi Anti-Phishing / Anti-Pharming

**CREDEM**

Violazione del Marchio Registrato  
Opinioni negative  
Attivismo di boicottaggio

REPUTATION  
MANAGEMENT  
SERVICES

**ANTI-  
PHISHING  
SERVICES**

**Utilizzo fraudolento  
del brand per profitti  
illeciti**

**Furto di identità  
dell'utente**



Rappresentazione non corretta del brand

Violazione dei requisiti di affiliazione

AFFILIATE  
MANAGEMENT  
SERVICES

ANTI-  
COUNTERFEIT  
SERVICES

Produzione e vendita  
illegale di beni contraffatti

Distribuzione al mercato nero  
di prodotti validi

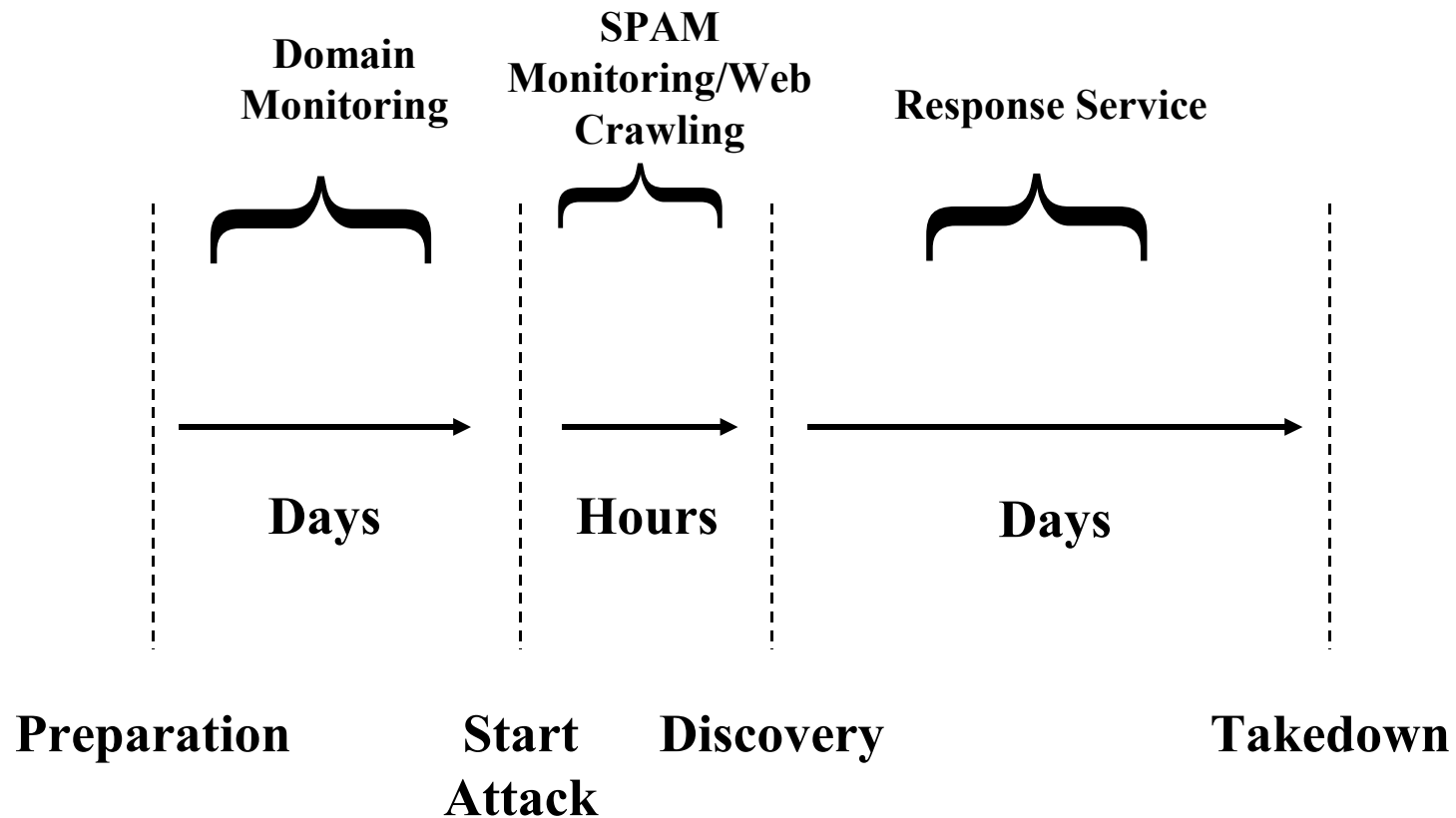
**DETECT** + “Scan” globale di milioni di sorgenti alla settimana

**PRIORITIZE** + In funzione dell’importanza degli incidenti

**ANALYZE** + Strumenti avanzati di ricerca e messagistica per l’analisi e la gestione di casi individuali

**RESPOND** + Importanti relazioni con oltre 400 registrar e ISPs in più di 80 paesi  
+ Take downs  
+ Uso di soli metodi accettati commercialmente, per es. no attacchi di Denial of Service  
+ Monitoraggio dopo l’attacco

# Tempistiche di un attacco di Phishing



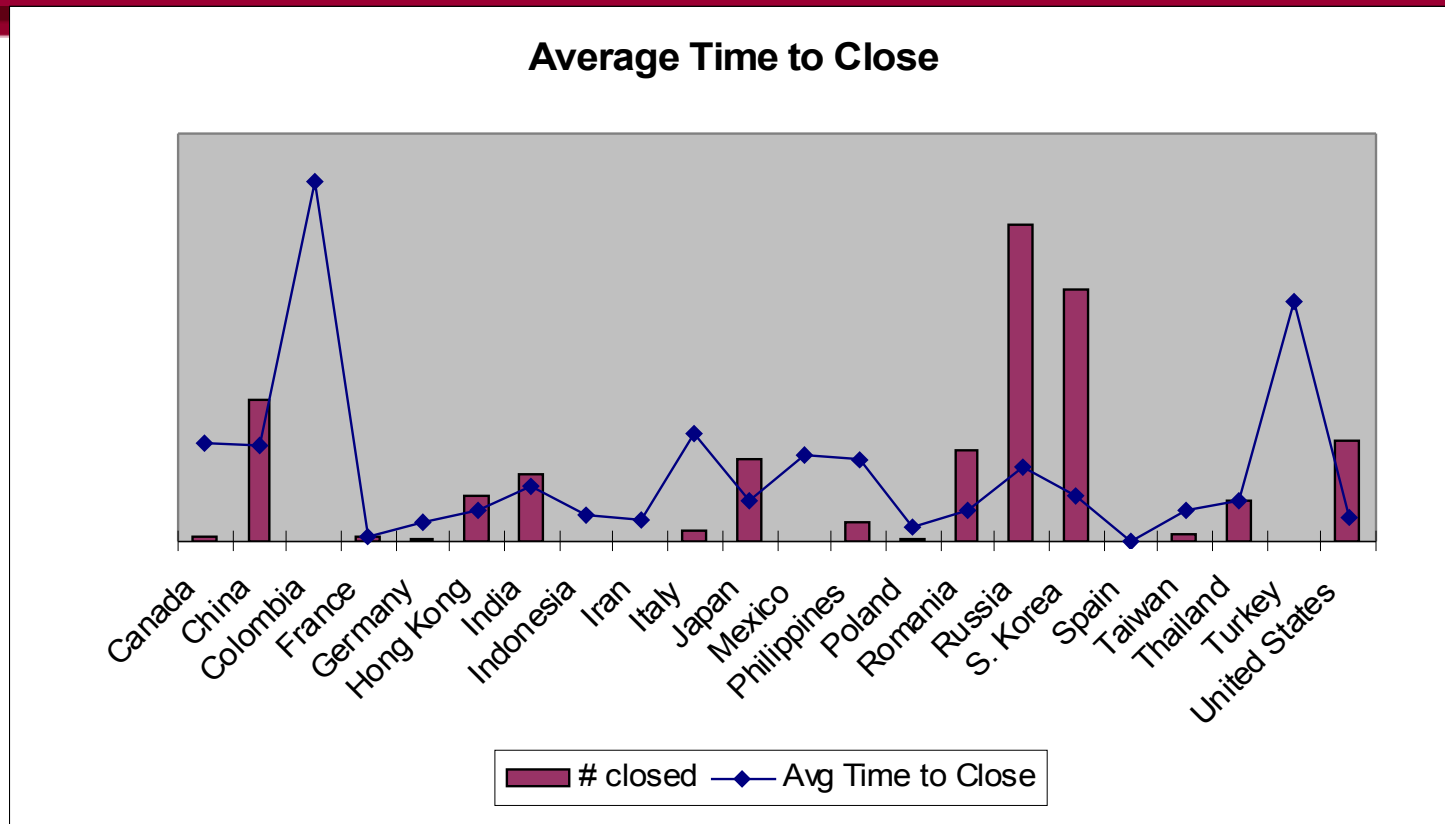
# VeriSign Brand Protection and Fraud Detection Offering

- + To address phishing concerns, the detection offering uses a rule based SPAM trap to scan assess, and identify incidents via email.
- + Specifically, the service monitors the Internet for the following:
  - Domain names that include customer brands or identity in a form that indicates possible fraudulent use
  - Junk emails with sender addresses that appear to come from Customer's mail servers
  - Junk emails that indicated fraudulent use of Company's corporate identity, including phishing and other types of online scam.
  - Unauthorized web sites that include content consistent with customer's corporate identity: logos, text, or linked text from the corporate website.

# Phishing Response Service

- + Started in 2003
  - Leveraged existing Payment Fraud team expertise
- + Single goal – Promptly and permanently remove Phishing websites hosted in any country across the world
- + 24x7 rapid response team which can analyze phishing attacks and contact ISPs, registrars and other agencies to remove the websites
  - Maintain close relationships with global ISPs, Registrars, CERTS, and local law enforcement authorities in more than 80 countries
  - Continuously monitor the site to ensure it does not host the attack again
- + Keep up with latest Phishing attack tactics of Phishers and develop counter-strategies and solutions
- + Shutdown 1000+ incidents per month and 10,000+ to date
- + Expanding base of over 50 customers

# I tempi di “TAKE DOWN” variano con i paesi



## Overall Metrics

- 25% of cases closed in < 2 hours
- 50% of cases closed in < 5 hours
- 80% of cases closed in < 12 hours

# Autenticazione del sito all'utente

## + SSL

- Fornisce sicurezza e autenticità
- La sicurezza è chiara attraverso il lucchetto, l'autenticità è nascosta
- Il VeriSign Secured Seal aumenta la fiducia



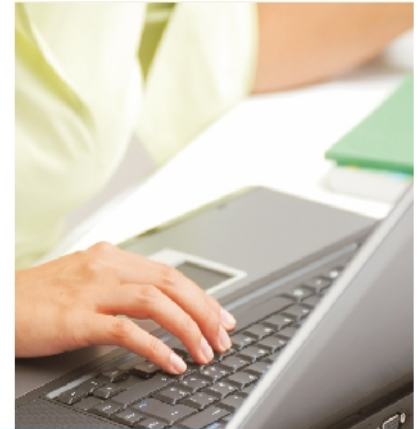
## + Next generation of SSL - Extended validation

- Fornisce una chiara autenticità in IE7



# Autenticazione dell'utente al sito – Mr. Pin

- Autenticazione forte a due fattori con token OTP
- Autenticazione forte per:
  - l'accesso al sito e-banking (a discrezione dell'utente)
  - le dispositive (obbligatorio)



**CHIAMA**  
800  
27183336  
CREDEM

800 CreDEM  
è facile da ricordare  
Digita 800 e componi  
CREDEM sulla tastiera

**ATTIVALO  
SUBITO**  
È GRATIS  
FINO AL 31.12.2006

 La sicurezza di Mr. Pin  
è garantita da VeriSign

Fondata nel 1996, VeriSign è leader di mercato nella fornitura di servizi di sicurezza dei siti, di sicurezza gestita e di autenticazione. VeriSign è una società quotata al Nasdaq, stato riferimento (NYSEM), che fornisce servizi di infrastruttura intelligente consentendo alle aziende e ai singoli individui di collegarsi, proteggere ed effettuare transazioni nelle complesse reti globali di oggi.  
VeriSign Italia permette alle aziende e alle persone di creare o di far crescere un'identità online, aiutandoli ad accedere la fiducia in Internet necessaria a valorizzare e sviluppare le funzioni di e-commerce.

**Internet Banking  
ancora più sicuro  
con Mr. Pin**



**CREDEM**

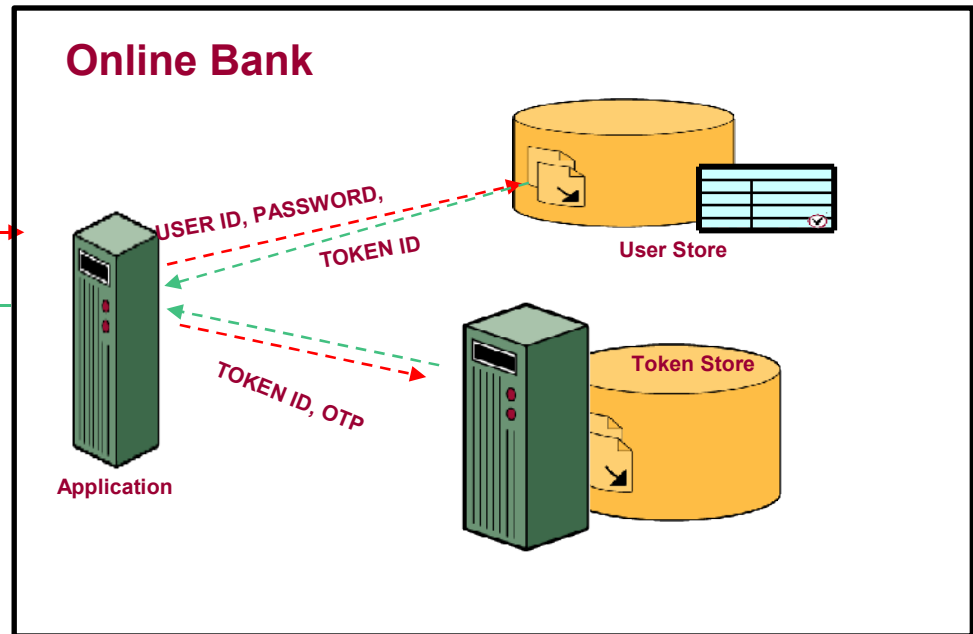
VeriSign e Mr. Pin sono marchi registrati con il marchio del logo VeriSign e il logo Mr. Pin. © 2006 VeriSign Inc. Tutti i diritti sono riservati. VeriSign e Mr. Pin sono marchi registrati con il marchio del logo VeriSign e il logo Mr. Pin.

# Architettura - VeriSign Unified Authentication

**CREDEM**



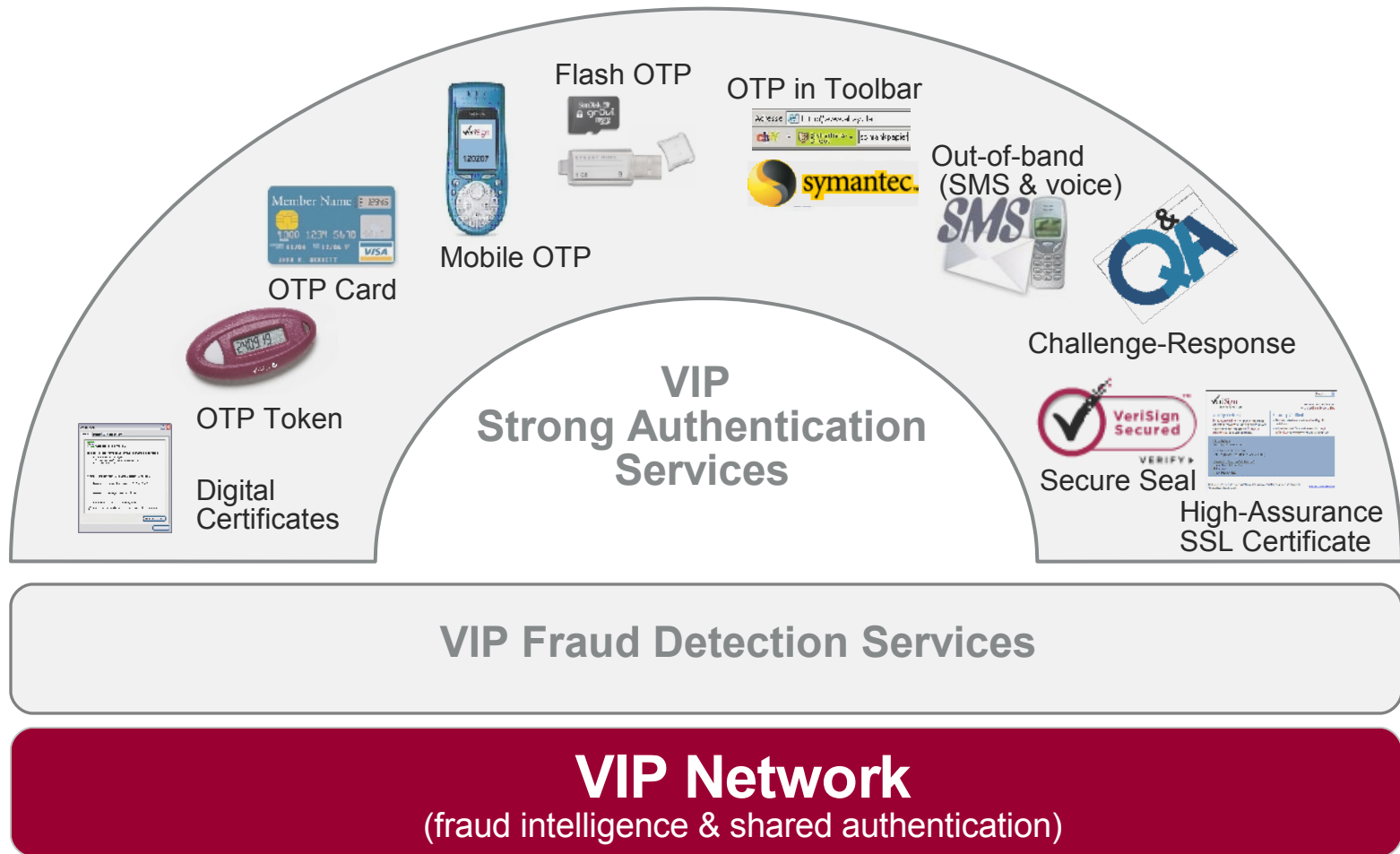
ONLINE BANK USER ID,  
- - - PASSWORD, OTP



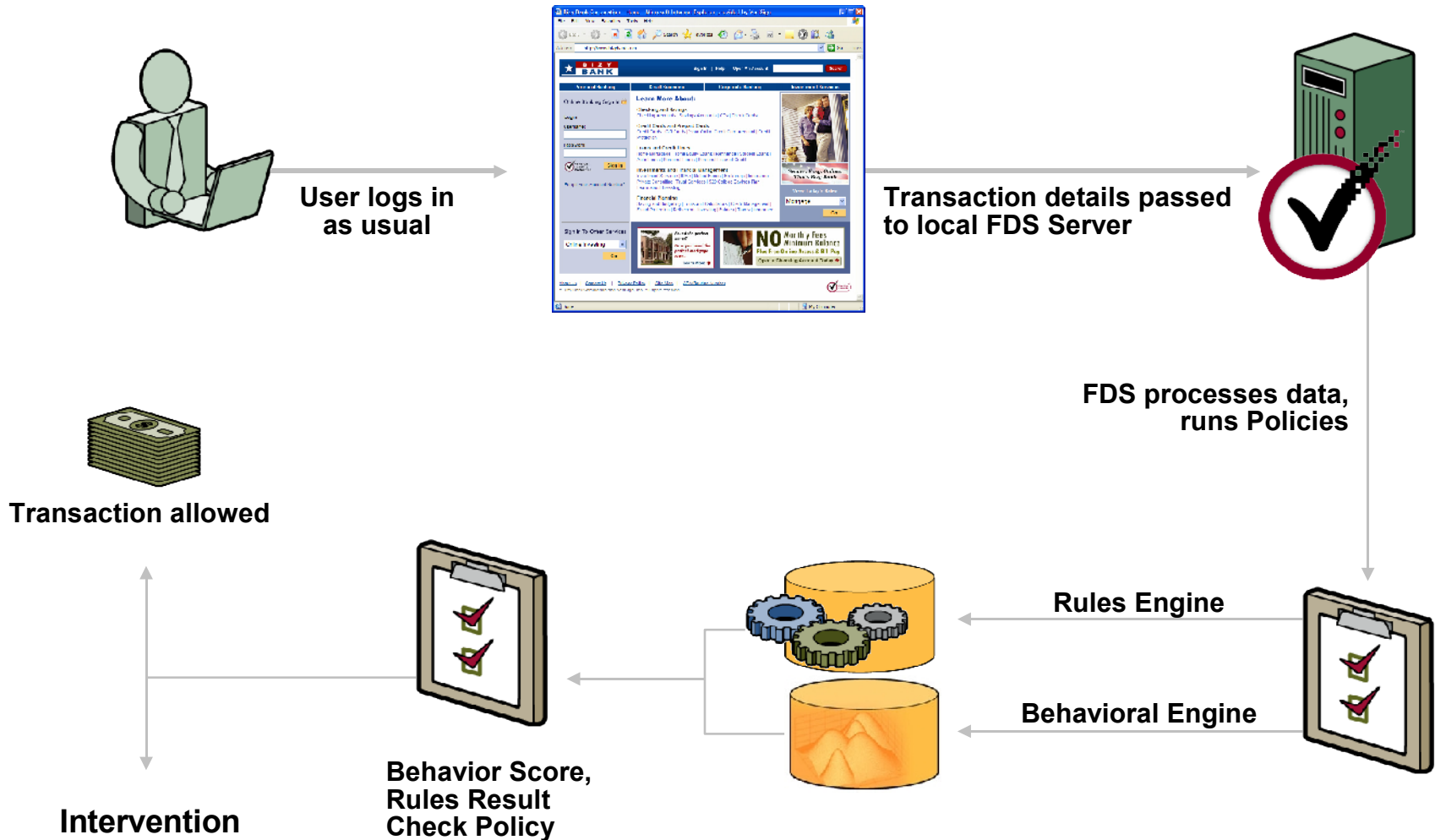
# Evolutioni future...

- + DIVERSI METODI/STRUMENTI DI AUTENTICAZIONE
- + FRAUD DETECTION SYSTEM
- + VERISIGN IDENTITY PROTECTION NETWORK

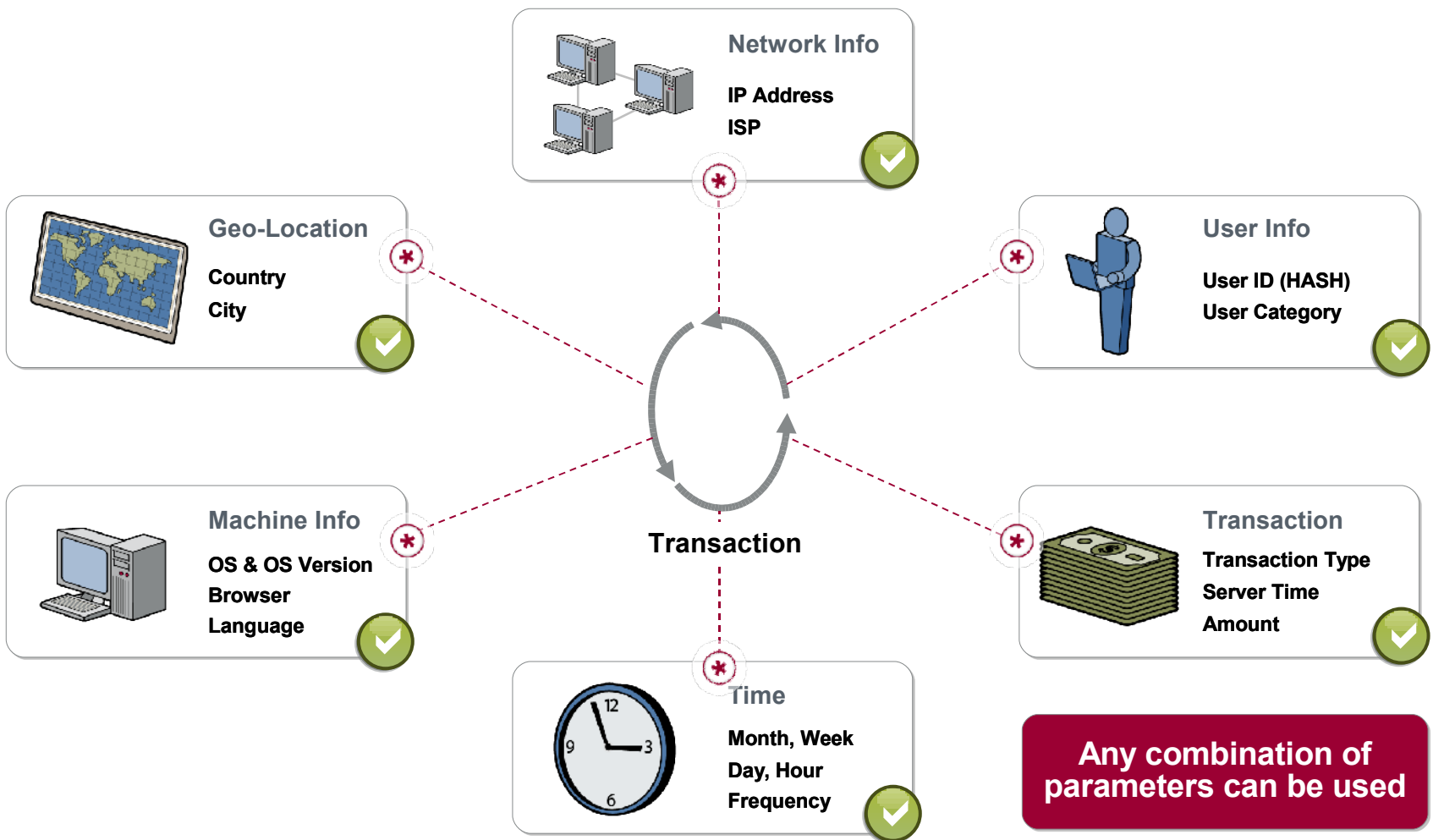
# Una Suite completa per l'autenticazione dell'utente



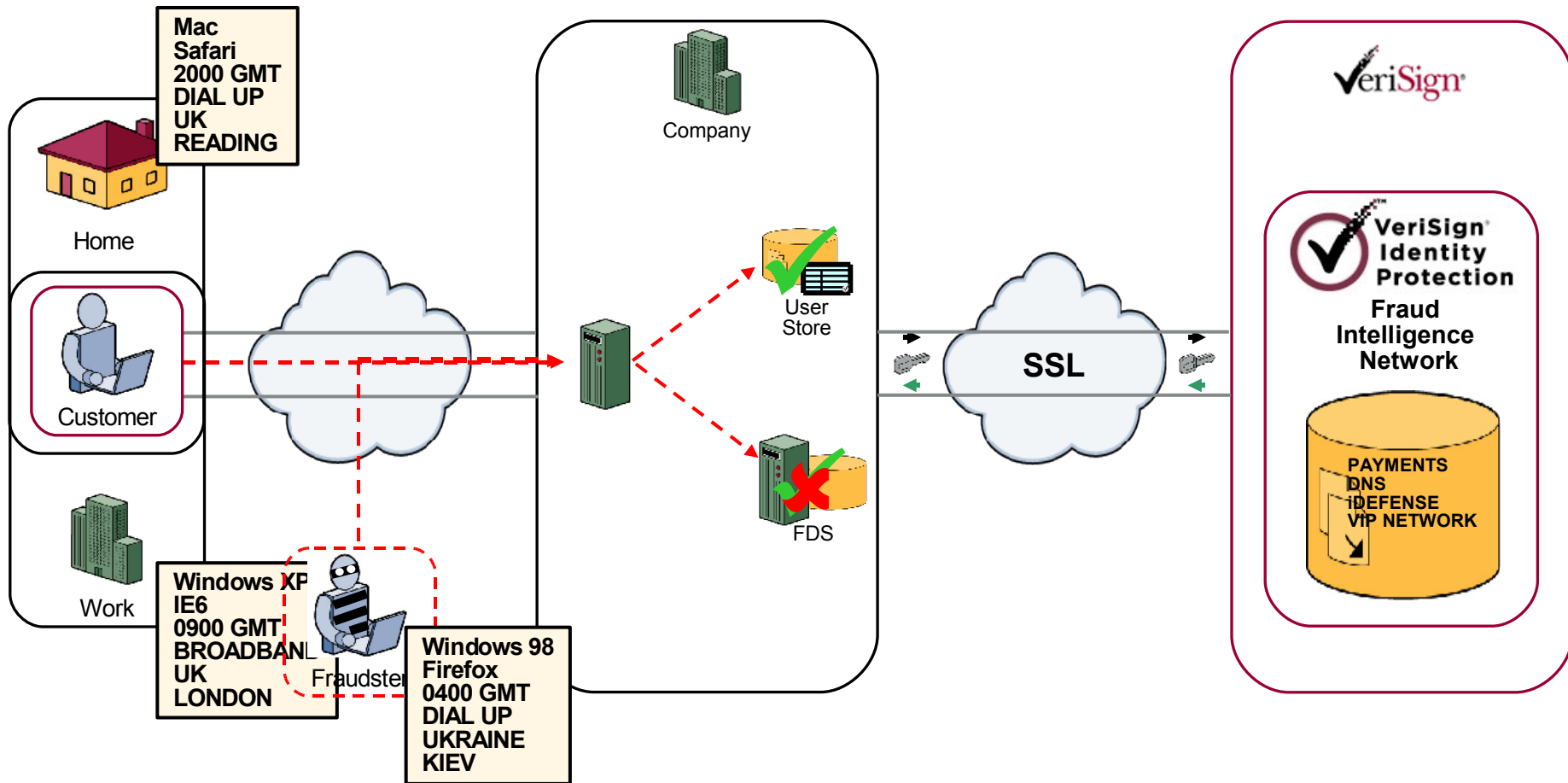
# Fraud Detection System: Risk Based Authentication



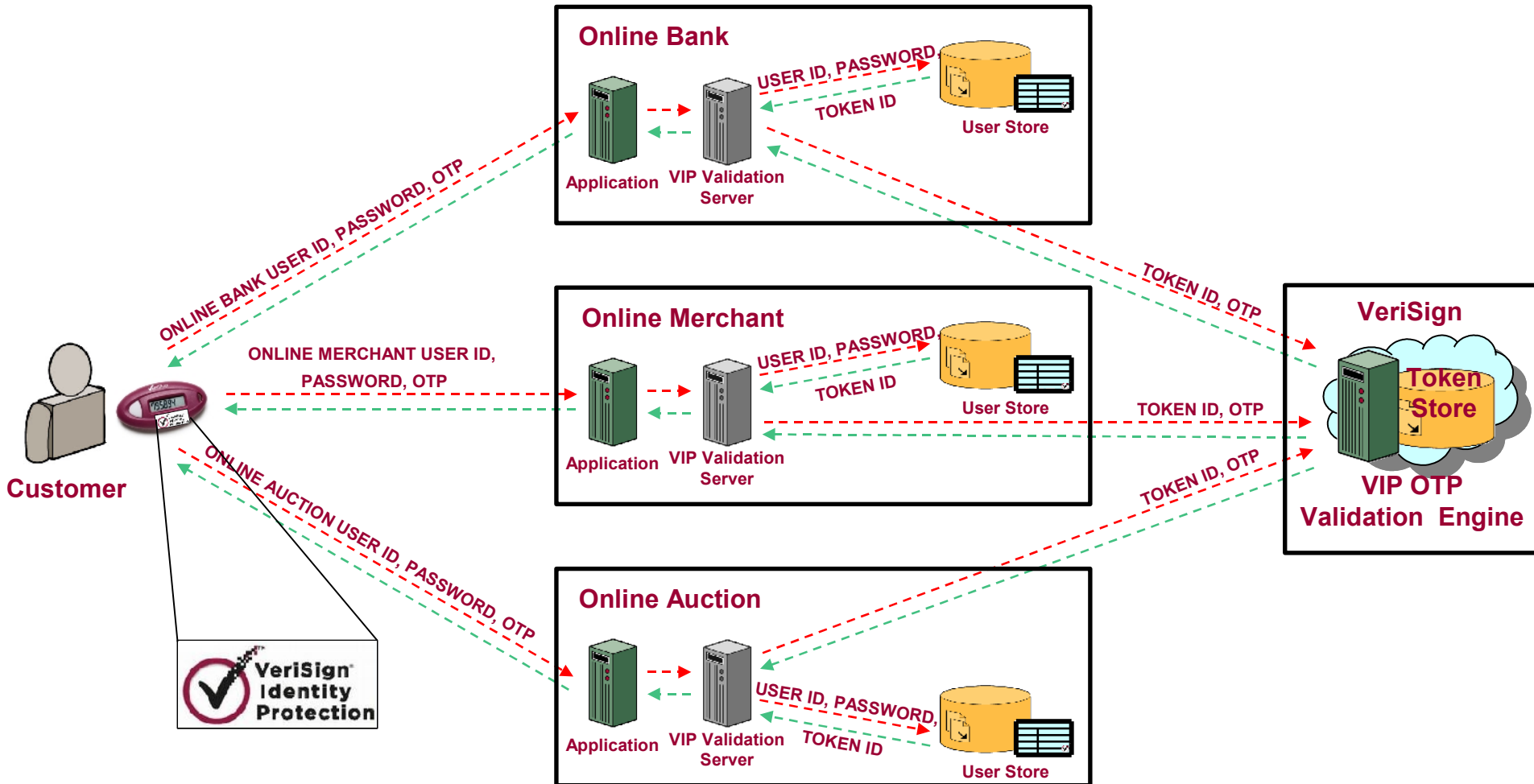
# Fraud Detection System – Parametri



# Fraud Detection System – Risk Based Authentication



# VeriSign Identity Protection



# VeriSign Identity Protection



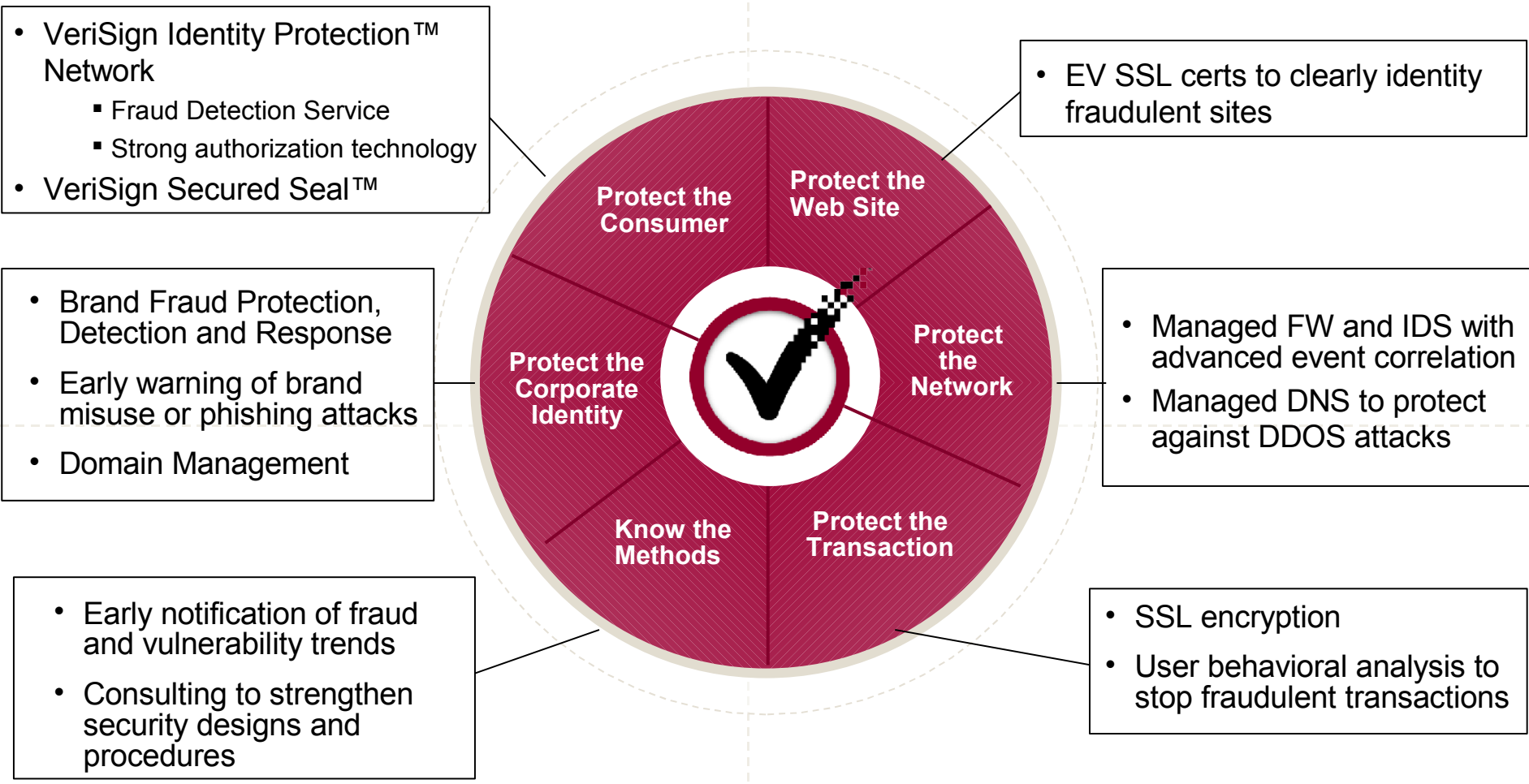
# VeriSign Identity Protection: PayPal



[www.paypal.com/securitykey](http://www.paypal.com/securitykey)

- + **Prima implementazione globale di VIP**
- + **Partenza da 4 paesi (1 milione di token)**
  - + **Germania, US, Giappone, Australia**
- + **Entro l'anno a tutti i clienti PayPal**

# VeriSign's Online Fraud Management Portfolio



**Layered VeriSign Services are responsive, comprehensive and flexible.**

# Questions + Answers



QUESTIONS + ANSWERS