BANCO POPOLARE
GRUPPO BANCARIO

E-commerce e on-line banking
Effettiva sicurezza crittografica

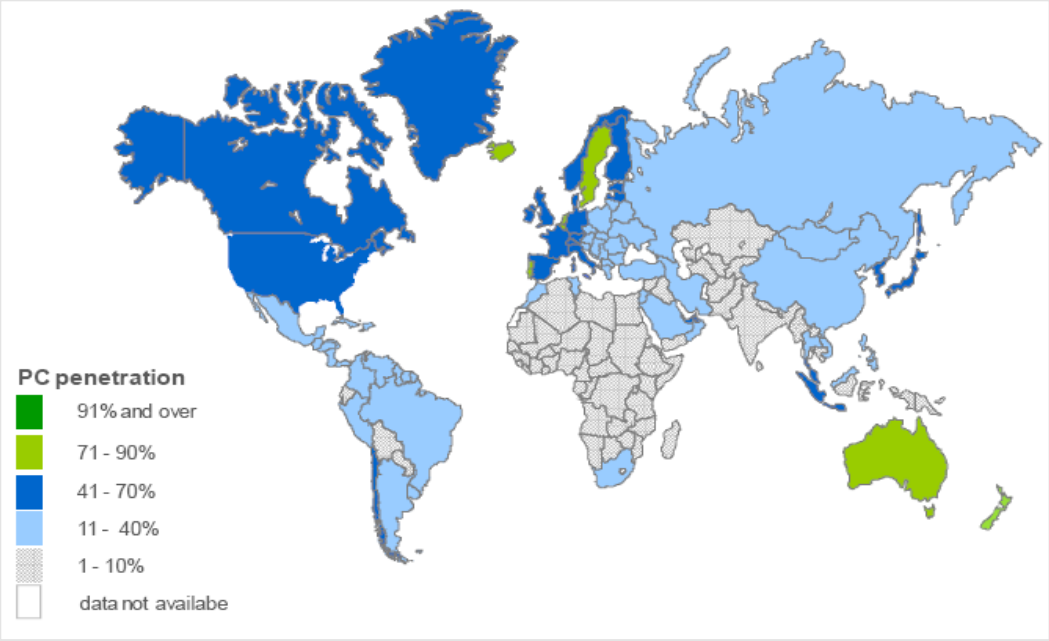
Università di Trento - Dipartimento di Matematica

"sicurezza nei sistemi di on-line banking"
un caso concreto

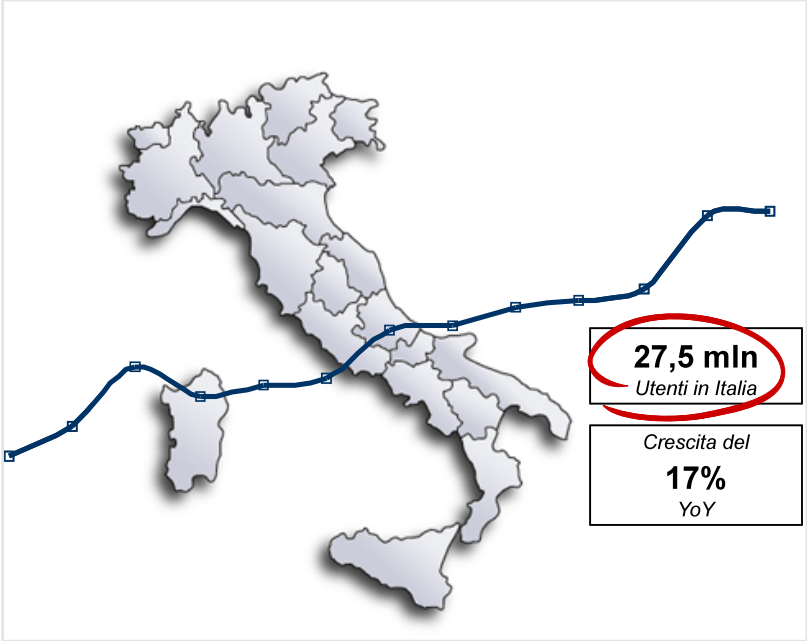
Pier Luigi Giacomello
A.D.Tecmarket Servizi – Corporate Banking CBI
Responsabile Canali Innovativi – SGS BP
Gruppo Banco Popolare

pierluigi.giacomello@sgsbp.it

- Penetrazione personal computer nel mondo -



- Utenti online in Italia -



Fonte: Elaborazione su dati Google - dati a gennaio 2011

Gruppo Banco Popolare - Online Banking - 2011

Volumi / Clienti	quantità	transazioni effettuate	importo (milioni di euro)
Privati	485.000	3.800.000	2.800
Imprese	175.000	65.800.000	233.300
TOTALI	660.000	69.600.000	236.100

SICUREZZA NELL' ON-LINE BANKING

Insieme di attività, sistemi, strumenti, regole e organizzazione

per proteggere il cliente

ANCHE SE OPERA IN UNA POSTAZIONE COMPROMESSA

(e lui non lo sa)

attività
intelligence
monitoraggio

sistemi
Fraud prevention
Sistema autorizzativo
Meccanismi di Alerting

strumenti
Strong Authentication
Tastierino Virtuale
Protezione dati cliente

regole
comportamenti
informazione

ATTIVITA'

intelligence

monitoraggio

Tentativi di accesso

Impronta del collegamento

- indirizzo ip, browser,
- service pack,
- sistema operativo,
- configurazione sw

Operatività

- IBAN destinatari
- time stamp operazioni

Comportamento cliente

evidenze / anomalie / comportamenti difformi

SISTEMI

fraud prevention

Connesso al monitoraggio e al sistema autorizzativo

Unico per tutti i sottosistemi e tutti i canali

Regole da applicare a fronte di eventi e/o comportamenti anomali

sistema autorizzativo

Attua le policies che derivano dai sistemi di monitoraggio e di fraud prevention

Autorizzazione alla operazione può essere rilasciata, sospesa in attesa di verifica, bloccata

meccanismi di alerting

Notifica via e-mail e/o via sms di:

- Pagamento autorizzato (con o senza soglia, per tipologia, …)
- Accesso effettuato / tentato, password cambiata, …

STRUMENTI (1 di 2)

strong authentication

combinazione di 2 elementi tra

1) **quello che sai**
2) **quello che sei;**
3) **quello che possiedi**

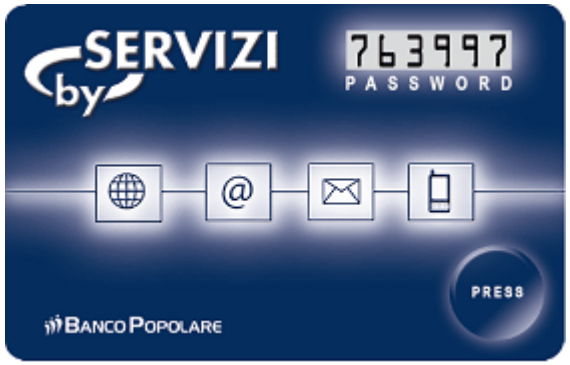
OneTimePassword a tempo

Richiesta al logon iniziale

Ogni operazione “sensibile” richiede, nel suo percorso, almeno 2 volte l’inserimento del codice OTP

Validità 30 secondi

3 soluzioni differenziate per tipologia cliente, ma tutte con gli stessi principi



STRUMENTI (2 di 2)

tastierino virtuale

Combinazione randomica dei tasti in base ai dati reali della disposizione di pagamento per prevenire attacchi “man in the middle”

Protezione dati sensibili

Per modifiche/nuovi inserimenti è richiesto un codice OTP, per prevenire eventuali frodi differite nel tempo

REGOLE

Regole comportamentali

Stabilire e comunicare fin DALL' INIZIO DEL RAPPORTO le regole comportamentali e le modalità con cui la banca comunicherà con il cliente telematico

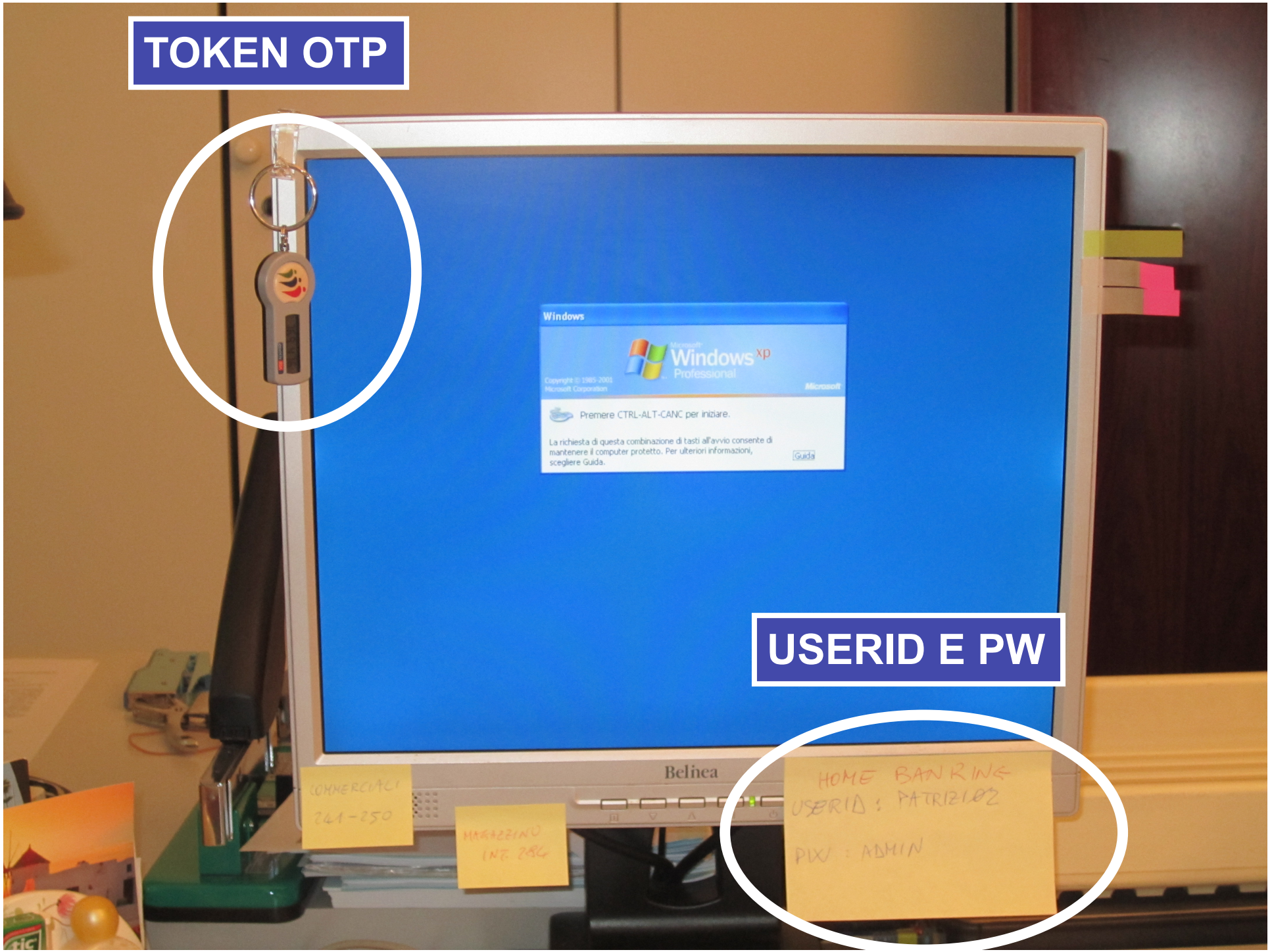
Invitare il cliente ad adottare regole comportamentali adeguate

Sensibilizzazione e informazione

NON E'

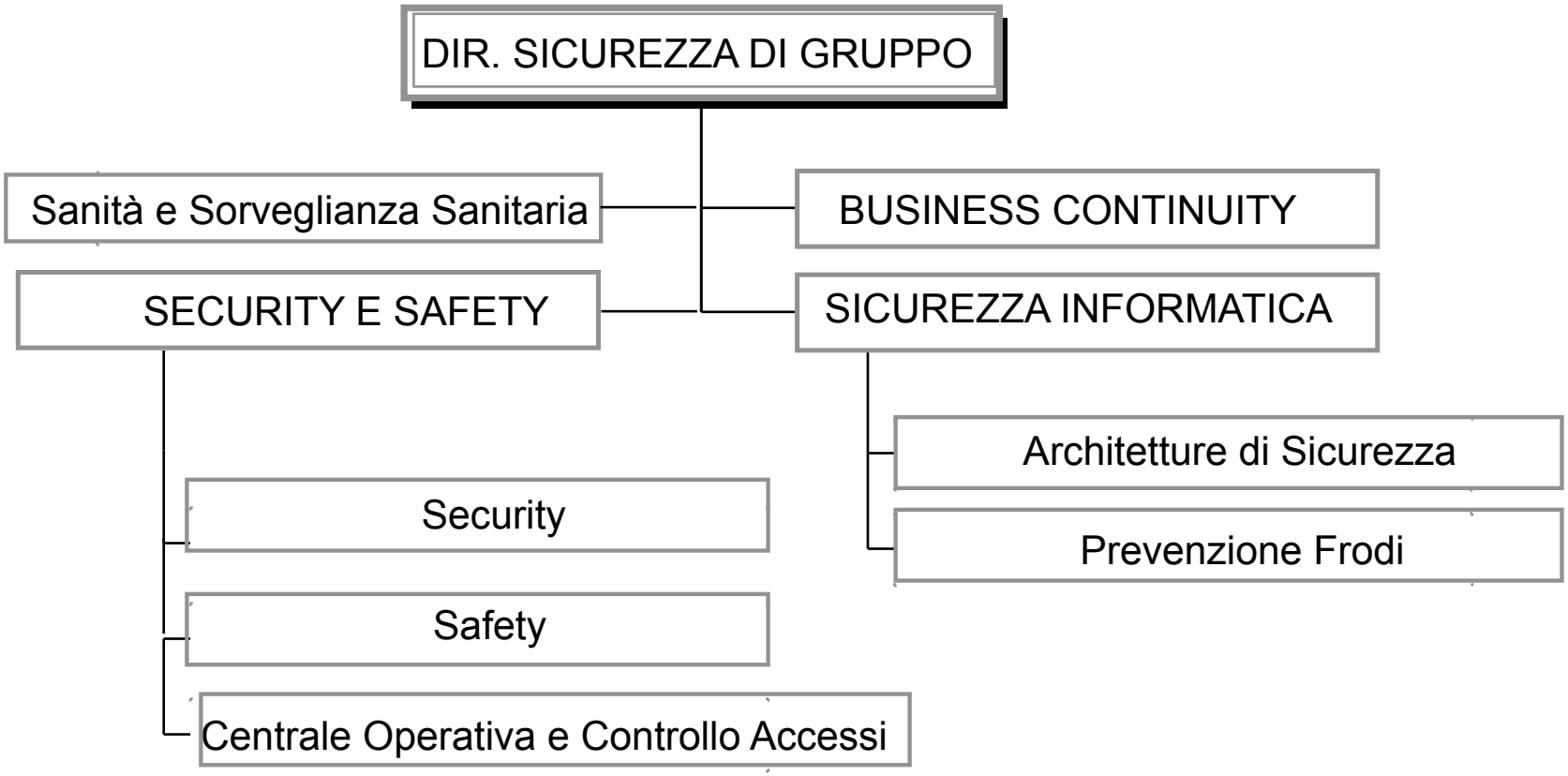
MAI

ABBASTANZA


TOKEN OTP
Windows
Windows xp
Professional
Premere CTRL-ALT-CANC per iniziare.
La richiesta di questa combinazione di tasti all'avvio consente di mantenere il computer protetto. Per ulteriori informazioni, scegliere Guida.
Guida
Belinea
USERID E PW
HOME BANKING
USERID : PATRIZIO2
PW : ADMIN

ORGANIZZAZIONE

La sicurezza va gestita a 360 gradi, con una organizzazione aziendale che consenta di ottimizzare gli sforzi e di evitare la dispersione di informazioni che provengono da un canale e potrebbero essere rilevanti per un altro



non è più il poliziotto che insegue il ladro…

è l'uomo della sicurezza che deve correre più del frodatore

GRAZIE PER L' ATTENZIONE

Pier Luigi Giacomello

pierluigi.giacomello@sgsbp.it