Servizi evoluti su piattaforma Mobile

Security Watching

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Security Watching (1/3)

- **Obiettivo**: l'evidenziazione di nuovi trend nel campo della sicurezza informatica, contestualizzati alla particolare realtà del cliente. Il servizio consente di effettuare scelte "sicure" non solo nel breve ma anche nel medio/lungo periodo e permette di anticipare i rischi imminenti. Il servizio è svolto in collaborazione con realtà collegate al mondo della ricerca, dell'innovazione e della formazione.

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Security Watching (2/3)

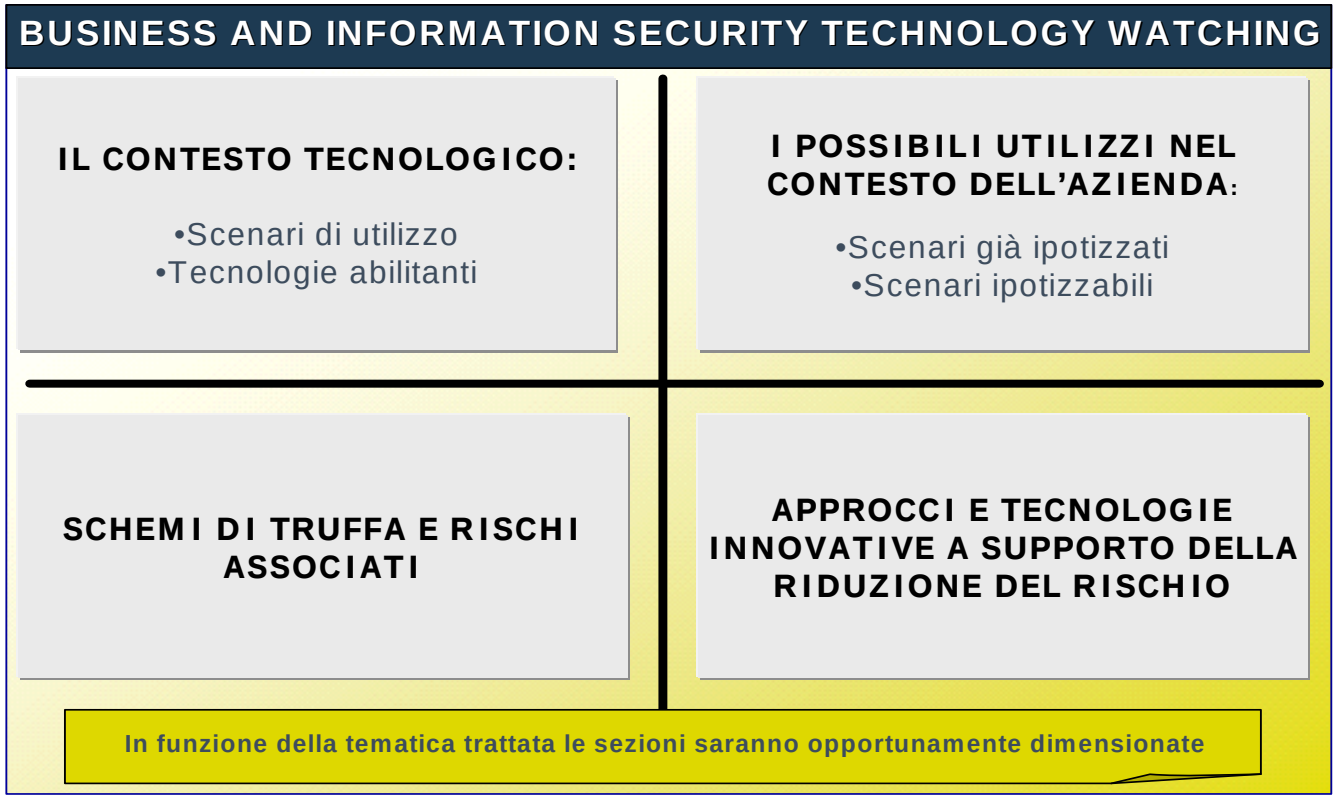
➔ **Esempi di argomenti:**

- Introduzione delle carte a microcircuito EMV
- Servizi evoluti su piattoforme Mobile
- Threats Management (gestione delle minacce)
- Metodi di autenticazione basati su canali alternativi
- Sicurezza nella rete Voice over IP
- Instant Messaging e Peer-to-Peer Networks
- Sviluppo sicuro
- Security Information and Event Management
- Autenticazione biometrica

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Security Watching (3/3)

➔ **L'output sono dei report documentali**, un esempio della struttura è riportato di seguito.



Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Canale Mobile: tipologie di servizi

- I servizi offerti tramite l'utilizzo del canale mobile si suddividono sostanzialmente nelle seguenti macro categorie:
  - **Servizi informativi:** per l'invio di informazioni nella modalità **pull** per movimenti del conto e delle carte di pagamento, estratto conto, l'invio di news e pubblicità, per avviso di ricevimento raccomandate. Nella modalità **push** in tempo reale (solitamente via SMS) per operazioni di particolare entità e/o sospette, per tracking della spedizione di pacchi;
  - Servizi dispositivi per l'esecuzione di transazioni;
  - Servizi di autenticazione basati su canali alternativi.

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Per Mobile Banking si intendono solitamente le transazioni bancarie e tutte le attività correlate ad un conto corrente effettuate attraverso un dispositivo mobile (smartphone, palmare, ecc.).

Le tipologie di servizio che possono essere offerte rientrano nelle seguenti categorie:

- ➔ Informazioni conto (movimenti, estratto conto, ecc.);
- ➔ Operazioni bancarie (bonifici, giroconti, ricariche carte, ecc.);
- ➔ Informazioni finanziarie (tassi di interesse, cambi, ecc.);
- ➔ Operazioni finanziarie.

Il contenuto dei servizi, in genere di carattere informativo, è naturalmente legato al tipo di canale mobile utilizzato, in particolare alla quantità di informazioni che si possono trasmettere e dal tipo di interazione necessaria.

I servizi elencati si appoggiano in parte ad infrastrutture dei carrier di telefonia mobile ed in parte ad infrastrutture della banca.

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

- USSD (Unstructured Supplementary Service Data)
- SMS (Short Message Service)
- MMS (Multimedia Message Service)
- WAP (Wireless Application Protocol)
- HTTP (Hyper Text Transfer Protocol)

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Gli scenari

- Servizi bancari informativi
- Servizi bancari dispositivi
- Mobile Banking
- Tracking servizi postali
- Ricevuta via sms per raccomandate
- Servizi di autenticazione per servizi web

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

I servizi di sicurezza che possono essere applicati alla attuale tecnologia mobile riguardano:

- ➔ Funzionalità avanzate dei dispositivi mobili: è possibile implementare la sicurezza dei dispositivi mobili agendo direttamente sui dispositivi, infatti è possibile realizzare tool in grado di generare e gestire certificati. Tale modalità permette di offrire servizi di sicurezza end-to-end;
- ➔ Funzionalità avanzate della SIM: è possibile offrire servizi di sicurezza avanzati utilizzando le opzioni di sicurezza fornite dall'operatore della rete mobile, in questo caso la sicurezza verrà demandata e gestita interamente dai Telco.

Funzionalità avanzate dei dispositivi mobili (1/4)

Vi sono tre principali tecnologie disponibili per i cellulari:

- ➔ Applicazioni JAVA (J2ME)
- ➔ Applicazioni per Symbian OS
- ➔ Applicazioni per Microsoft PocketPC Phone Edition

Ciascuna delle alternative tecnologiche offerte dal mercato è in grado di fornire sistemi di cifratura lato end-point. Per end-point si intende un qualsiasi dispositivo mobile in grado di comunicare con il servizio bancario utilizzando vari canali quali USSD, SMS, WAP, HTTP, ecc.

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Funzionalità avanzate dei dispositivi mobili (2/4)

- La J2ME offre un pacchetto, denominato SATSA (Security And Trust Services Api), che contiene cinque gruppi di API: tre gruppi di API per la comunicazione con elementi sicuri come la SIM e le smart card e due gruppi per la gestione delle firme digitali, dei certificati e le operazioni di crittografia.

- Il gruppo che, in questo caso, interessa di più, è denominato SATSA-CRYPTO.

- Tuttavia, nonostante si tratti di uno standard aperto, non mancano alcune caratteristiche che possono causare problemi di interoperatività fra terminali differenti. A tal proposito alcune case costruttrici hanno definito una serie di librerie proprietarie che risiedono solo sui propri terminali e che permettono di controllare alcune funzionalità del telefono.

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Funzionalità avanzate dei dispositivi mobili (3/4)

- Symbian OS è un sistema operativo con delle librerie associate, una struttura per l'interfaccia utente e implementazioni di riferimento per tool prodotti da Symbian.
- Nokia, Sony Ericsson, Panasonic, Samsung, Siemens and Ericsson sono proprietari di Symbian.
- Per quanto riguarda la sicurezza, Symbian OS, utilizza un sistema di gestione dei certificati.
- Utilizzando le classi e le funzioni predefinite è possibile creare applicazioni proprietarie per le funzionalità crittografiche.

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Funzionalità avanzate dei dispositivi mobili (4/4)

- Pocket PC è una piattaforma definita su misura da Microsoft per utenti che utilizzano Pocket PC e consiste in un insieme di profili minimi di software e hardware supportati

- Mediante alcune funzioni permette di codificare/decodificare dati, scambiare chiavi di sessione, generare chiavi simmetriche e asimmetriche e generare firme digitali

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Funzioni avanzate della SIM

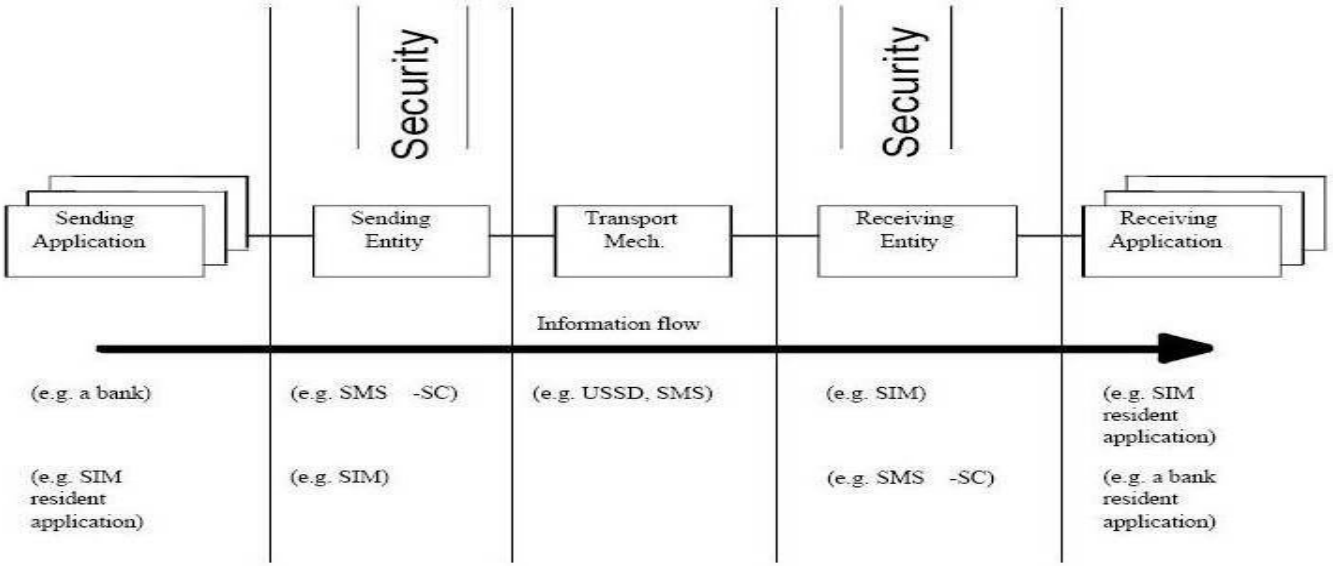
- Alcuni operatori di telefonia mobile offrono un servizio di sicurezza su canale SMS. Tale servizio sfrutta la tecnologia SAT per installare un motore di crittografia dei messaggi direttamente sulle SIM degli utenti interessati al servizio. Gli operatori sono in grado, così, di offrire un servizio di SMS sicuro rispettando i parametri di autenticazione del mittente, confidenzialità e integrità della comunicazione, richiesti in ambito mobile banking.

- Il principale vantaggio di questa soluzione riguarda la massima compatibilità con i telefoni attualmente in commercio, infatti il software di crittografia risiede interamente sulla SIM card dell'utente. L'unico requisito necessario per questa soluzione riguarda la memoria disponibile nella SIM, infatti sono richiesti almeno 64kbyte di memoria per poter ospitare l'applicazione.

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Funzioni avanzate della SIM: SAT (1/3)

- Il SIM Application Toolkit è uno standard approvato dall'ETSI (European Telecommunications Standard Institutes)
- Le funzioni del SIM Application Toolkit permettono di realizzare funzioni che consentono alla SIM di colloquiare con l'utente. Mediante queste funzioni si può realizzare una sorta di Graphical User Interface (GUI) che estende e affianca quella già presente nel dispositivo mobile.



Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Funzioni avanzate della SIM: SAT (2/3)

- La comunicazione sicura viene realizzata attraverso cinque attori principali: Sending Application, Sending Entity, Transport Mechanism, Receiving Entity, Receiving Application.
  - La Sending Application prepara un Application Message e lo inoltra alla Sending Entity con indicati i parametri di sicurezza che vi devono essere applicati.
  - La Sending Entity attacca un Security Header all'Application Message; dopo questa operazione, applica la sicurezza richiesta ad una parte del Security Header e a tutto l'Application Messsage.
  - La Receiving Entity, che riceve il pacchetto, lo svolge in osservazione ai parametri di sicurezza inseriti nel Security Header.
  - La Receiving Entity inoltra l'Application Message alla Receiving Application indicando le opzioni di sicurezza che erano state applicate al pacchetto.

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Funzioni avanzate della SIM: SAT (3/3)

- Se richiesto nel Security Header, la Receiving Entity può creare un pacchetto di risposta sicuro. Un Response Secure Packet consiste in un Security Header e, opzionalmente, a dati forniti dalla Response Application.

- Il Security Header che precede i dati sicuri nel pacchetto è composto da campi, utilizzati anche dai protocolli di comunicazione, per la verifica di errori e di manomissioni come il Redudancy Check (RC), Cryptographic Checksum (CC), Digital Signature (DS), Security Parameter Indicator (SPI), Ciphering Key Identifier (KIc), Key Identifier (KID).

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Funzioni avanzate della SIM: Mobile Signature Device

- Un particolare utilizzo del SAT consiste nell'implementare la firma elettronica sul dispositivo mobile.

- L'ETSI ha lavorato ad uno standard di firma elettronica utilizzando un approccio alternativo, capitalizzando il fatto che la maggior parte dei cittadini possiede il cellulare: un dispositivo contenente una smart card e in grado di fungere da personal card reader. Sono stati emessi dei TR e dei TS.

- La creazione della firma basata su smart card è effettuata tramite il processore crittografico presente nella SIM card. La richiesta di firma attiva l'immissione del pin di conferma e consente di visualizzare del testo relativo alla transazione che si sta per autorizzare.

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

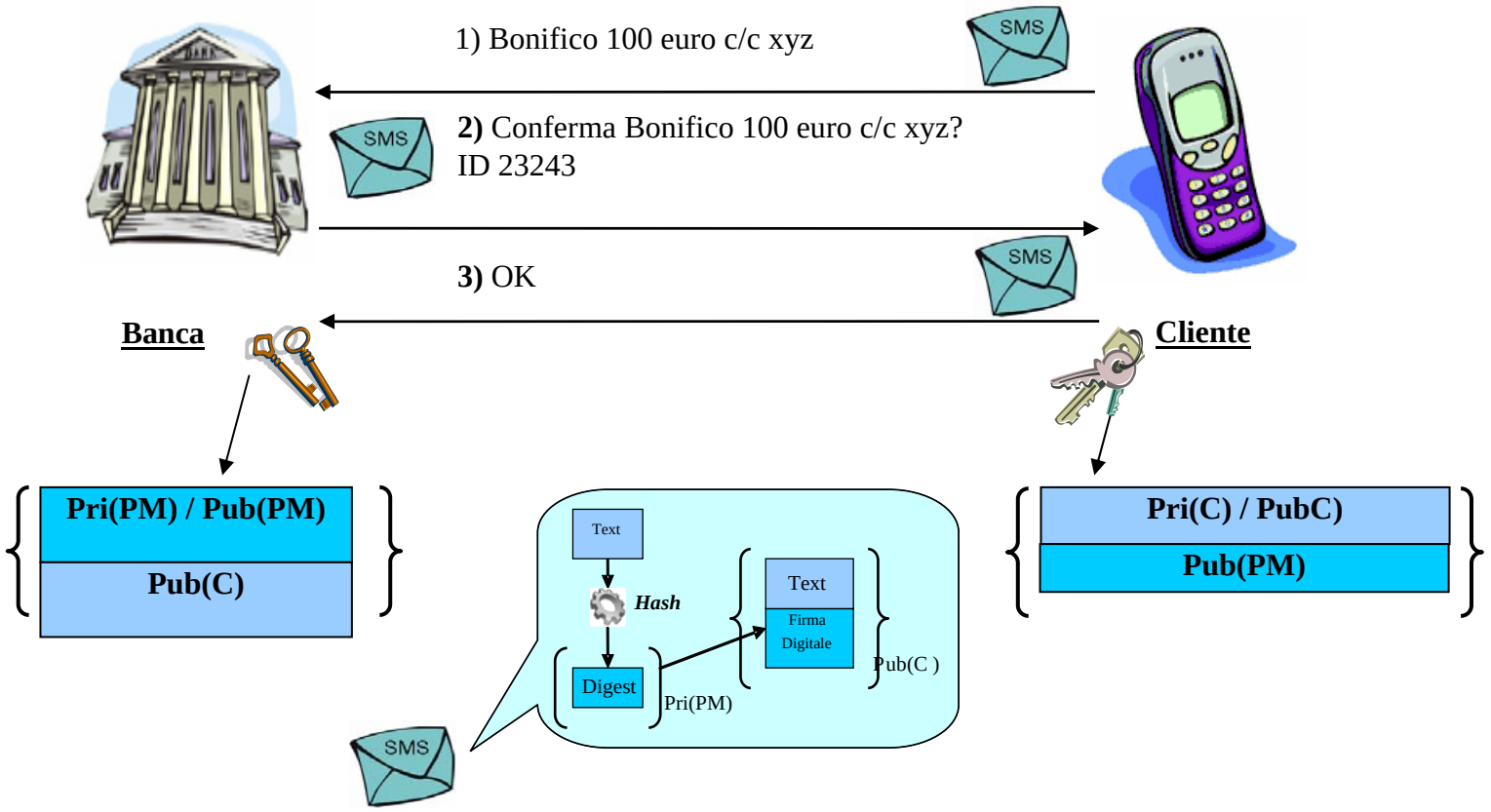
Considerazioni su SAT

- Le funzionalità SAT sono strettamente legate al provider telefonico, infatti, in tutti i casi presentati è richiesto l'utilizzo di SIM dello specifico provider telefonico.

- In questa modalità il provider di servizi mobili gestisce tutti gli aspetti di sicurezza, ne consegue che:
  - Il Telco gestisce interamente la struttura di sicurezza della rete, deve esserci quindi un rapporto di fiducia con il gestore;
  - Chi vuole offrire il servizio di mobile banking alla maggioranza dei propri utenti deve stipulare un contratto di SMS sicuro con i maggiori operatori di telecomunicazioni a livello nazionale.

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Scenari di utilizzo: Mobile Banking con SMS (1/2)



Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Scenari di utilizzo: Mobile Banking con SMS (2/2)

- Per questa tipologia di servizio offerto l'ambiente di sviluppo di più semplice diffusione e con il maggior supporto da parte dei terminali risulta essere il SIM Application Toolkit (SAT) per i seguenti motivi:
  - L'integrazione di tale servizio coinvolgerebbe tutti i sistemi mobili basati sulla SIM;
  - Il software potrebbe essere installato automaticamente sulle SIM dalla rete mobile;
  - L'applicazione verrebbe totalmente contenuta nella SIM.

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Scenari di utilizzo: HTTPS

- I principali vantaggi dell'utilizzo di Mobile Banking tramite l'accesso a sito HTTPS riguardano:
  - L'impiego di una tecnologia ampiamente utilizzata nel contesto Internet che fornisce una soluzione testata e continuamente aggiornata. Ma il phishing?
  - Utilizzo del protocollo TCP/IP e quindi la completa compatibilità con siti Internet, ne consegue una notevole riduzione della complessità infrastrutturale, infatti, è possibile utilizzare lo stesso back-end sia per l'erogazione dei servizi bancari via internet che per l'erogazione del servizio di mobile banking essendo effettivamente realizzabili sulla stessa piattaforma.
  - Una buona diffusione di dispositivi mobili in grado di supportare applicazioni HTTPS
  - Il basso costo di realizzazione del servizio, infatti è possibile appoggiarsi ad un infrastruttura esistente ed ampiamente utilizzata, ovvero l'infrastruttura di Internet. La realizzazione di siti di Mobile Banking non differisce di molto rispetto alla realizzazione di pagine WEB tradizionali.
  - Non è necessaria la modifica dei dispositivi mobili, infatti i terminali di nuova generazione dispongono già del supporto alle pagine HTTPS, in questo caso l'utente può usufruire immediatamente del servizio di mobile banking via HTTPS, senza nessuna installazione di software sul terminale

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Servizi di autenticazione (1/2)

- Il canale GSM per alcune sue caratteristiche di sicurezza si presta particolarmente ad essere impiegato come canale complementare per l'autenticazione. L'infrastruttura GSM, infatti, dispone già di un proprio metodo di autenticazione basato, come elemento abilitante, sulla dotazione agli utenti della SIM.

- La rete GSM si presta come canale complementare principalmente per i seguenti fattori:
  - Il numero di SIM registrate e attive relative al territorio nazionale è pari al 114% della popolazione, l'adozione di un sistema basato su canale complementare GSM non è quindi un elemento limitante per il servizio;
  - Quando un utente genera una chiamata, informazioni relative all'utente come il codice identificativo, la cella su cui si è attestato e il codice del dispositivo mobile vengono comunicate attraverso il canale di segnalazione direttamente alla centrale telefonica. Queste informazioni possono essere utilizzate nel contesto della strong authentication;

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

Servizi di autenticazione (2/2)

- Non ci sono costi di distribuzione e acquisto di dispositivi di autenticazione per gli utenti come Card Reader o Token RSA;
- Ogni utente telefonico è dotato di una SIM che può essere utilizzata come mezzo di autenticazione. Se dotata di un software di cifratura e di una chiave privata è possibile utilizzare la SIM come sistema di autenticazione con firma digitale. Il livello di sicurezza delle smart card e la difficoltà nella clonazione o estrazione del codice, fanno di questo mezzo un ottimo elemento di autenticazione.

➔ Alcuni vendor presentano implementazioni di sistemi di Strong Authentication ad alto livello di sicurezza utilizzando la rete GSM come canale complementare, basati sulla capacità di utilizzare le informazioni della rete GSM per identificare univocamente l'utente oppure con una tecnologia che consente, attraverso l'utilizzo della SIM del dispositivo mobile, di poter validare delle transazioni attraverso una firma digitale.

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it

?

Roberto Ugolini – Security Service Unit
roberto.ugolini@postecom.it