

# 4tech+

**Knowledge for Advanced Technologies**  
**Network @nd Security Solutions**

**22 Aprile 2010 convegno: Governance e Sicurezza per la Difesa e la P.A.**

**4tech+ srl - Via Morigi, 11 20123 Milano - tel 02 80509454 fax 02 8050220 [www.4techplus.com](http://www.4techplus.com)**

**Safe-Mobile : Strong Authentication e messa in sicurezza di comunicazioni via cellulare**

**Relatore : Mario Bergantini Amm. Delegato**

# Chi siamo

**4tech+** nasce a Milano nel marzo 2004, da un gruppo di professionisti con in comune un'esperienza più che ventennale nel settore ICT e della consulenza organizzativa, tra loro legati da una consolidata stima reciproca e tutti contraddistinti da una robusta pluriennale competenza acquisita in posizioni manageriali e/o imprenditoriali di rilievo.

**4tech+** è una azienda di consulenza organizzativa e tecnologica che **si differenzia per qualità, affidabilità, etica e competenza professionale messe a disposizione dei propri clienti.**



# I nostri mercati e le aree di riferimento

- Banche/Assicurazioni
- Telecomunicazioni
- Grande Distribuzione Organizzata
- Sicurezza
- Business Continuity
- Middleware e progetti speciali wireless e real time



# Safe-Mobile



# Safe-Mobile: il contesto-1

- Il mercato fornisce un'infrastruttura di telecomunicazione che permette l'accesso a contenuti, applicazioni e servizi in modo pervasivo, standard e di semplice uso.
- Il grado di sicurezza di questa infrastruttura è buono ma variabile e, comunque, raramente conforme alle necessità del sistema "difesa".



# Safe-Mobile: il contesto-2

- Lo sviluppo di un'infrastruttura con un livello di sicurezza "military grade" è sempre possibile ma con problemi reali di costi.
- I tentativi di adattare l'infrastruttura civile alle esigenze della difesa hanno portato, fino ad oggi, a soluzioni complesse, difficili da usare e poco pervasive con alcuni punti di vulnerabilità quali ad esempio:

Data Base centralizzati di password

Concentrazione delle chiavi di autenticazione su un unico supporto sempre smarribile e, peggio, utilizzabile da terzi.



# Safe-Mobile: Cos'è?

È un servizio ottimale per farsi identificare in modo univoco e sicuro, usando il proprio cellulare, e con esso poter gestire attività riservate in mobilità, in qualunque momento e dovunque.



# Affidabilità di Safe-Mobile

- Basato su crittografia asimmetrica (chiavi pubbliche/private) fondata su algoritmi a curve ellittiche (chiavi a 256 bit) equivalenti a RSA/DSA a 3072 bit (fonte Nist Sp 800-57)
- Meccanismo di mutua autenticazione (identificazione certa delle due entità)
- Crittografia automatica delle informazioni riservate
- Client dedicato sul cellulare
- PIN definito dall'utente in fase di registrazione al servizio, non condiviso ad alcun livello
- Monitoraggio delle comunicazioni 24 ore su 24, 7 giorni su 7
- Trasporto dati tramite SMS criptato o Mail-like criptata
- Costruito su un'architettura di grid computing che ne garantisce la robustezza, la distribuibilità e la scalabilità

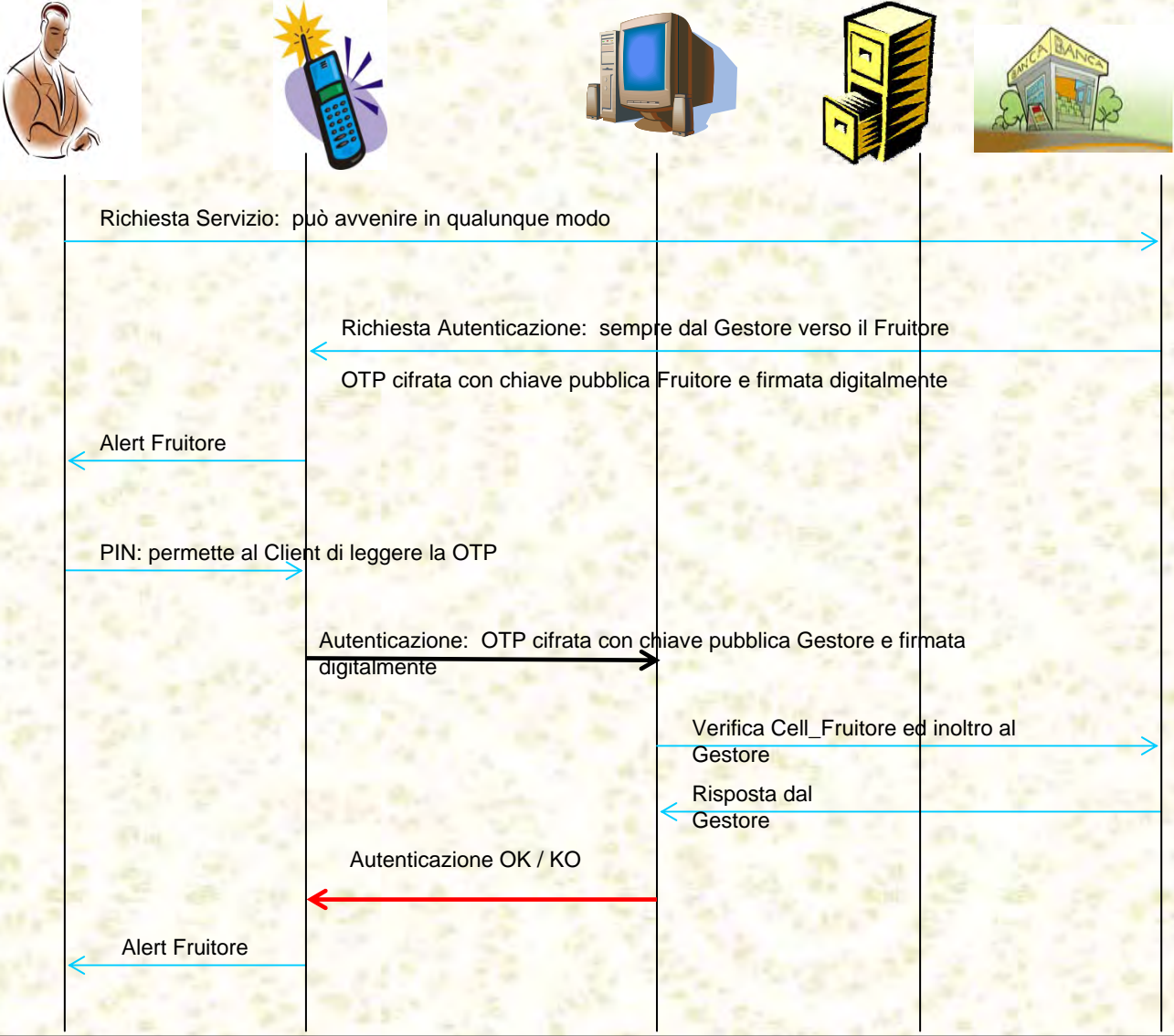


# Safe-Mobile : sicurezza negli accessi

- Punto di forza di Safe-Mobile è l'elevata sicurezza per l'accesso a qualunque sistema, che si sostanzia nell'utilizzo di chiavi per criptare la comunicazione tra Client e sistema e nell'assoluta riservatezza del PIN, che viene impostato dall'utente finale e non viene **mai** condiviso.
- Un ulteriore livello di sicurezza è dato dall'utilizzo di una **session key univoca per ogni comunicazione**, che mette al riparo dall'eventuale intercettazione delle chiavi, che non sono decifrabili senza il PIN conosciuto solo dall'utente.



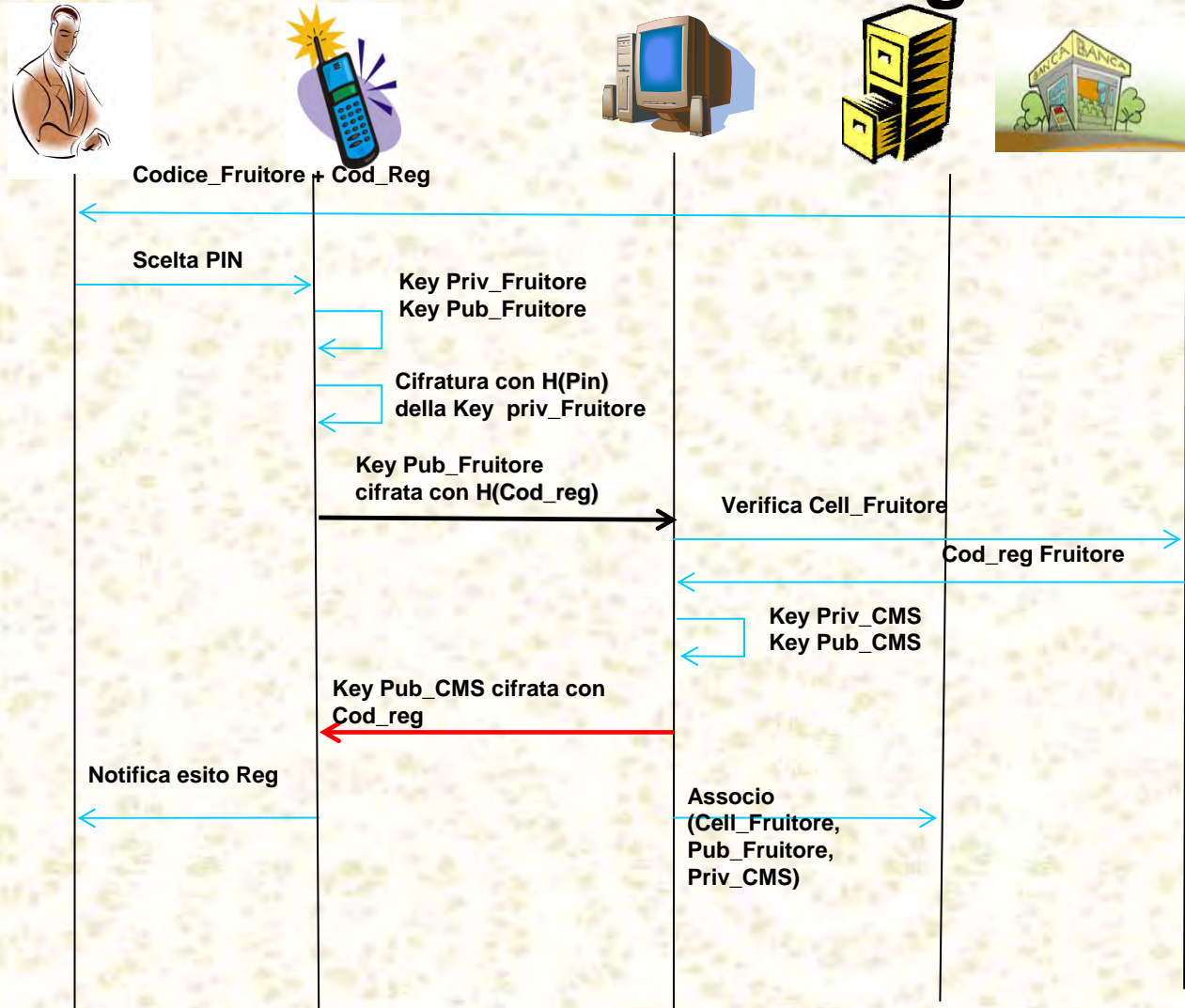
# Safe-Mobile : schema di autenticazione



**Grazie per l'attenzione**  
**Cordiali Saluti**



# Safe-Mobile : schema di registrazione



# Disclaimer

- Tutti i contenuti del presente documento sono proprietà esclusiva e riservata di **4tech+** e sono protetti dalle vigenti norme nazionali ed internazionali in materia di tutela dei diritti di Proprietà Intellettuale e/o Industriale.
- Con la dizione “*Diritti di Proprietà Intellettuale e Industriale*” si intende fare riferimento al complesso dei diritti riconosciuti e tutelati dalle vigenti normative nazionali ed internazionali, tra cui - a titolo esemplificativo e non esaustivo, relativamente a tutti gli Stati del mondo e senza alcun termine - ogni diritto discendente da brevetti (ivi compreso il diritto di deposito della relativa domanda), diritti d'autore presenti o futuri, marchi d'impresa e/o di servizio (sia registrato che utilizzato in via di fatto da **4tech+**), brand, nomi commerciali, ditte, know-how, nomi a dominio, banche di dati e tutte le relative applicazioni.
- Il documento può essere utilizzato per finalità personali ma non per finalità commerciali nel rispetto del diritto di proprietà intellettuale e di ogni altra regola vigente in materia. È vietato ogni uso diverso da quello consentito nelle presenti condizioni d'uso o ogni modifica del contenuto del documento senza la preventiva autorizzazione scritta di **4tech+**.

***“Simplify,  
wherever possible,  
the complex.”***

