“E-payment Security”

Professor *Massimiliano Sala* – Dipartimento di Matematica, Università di Trento

8 marzo 2013

Abstract dell'intervento di

Dott. Emiliano Sparaco e Dott. Alberto Ferro – Poste Italiane

"La sicurezza di TITAN – Innovazione per Smartcard e Terminali Pol"

L’intervento rappresenta un focus sugli aspetti di sicurezza (“ OR 7- Modelli e Tecnologie per la Security”) analizzati nell’ambito del “Progetto TITAN –Sistema di moneta elettronica e servizi a valore aggiunto”.
Gli studi sono stati condotti per introdurre aspetti innovativi relativi a due tipologie di strumentazione che rappresentano la base di un sistema di pagamenti elettronici, ovvero smartcard e terminali.
Il modello smartcard presentato rappresenta la massima espressione della multi-applicazione, grazie all’applicazione dell’architettura logica GlobalPlatform, la gestione dei Security Domains e la mutua autenticazione tra smartcard e entità off-card tramite Secure Channel Protocol.
Durante le attività di analisi del rischio, è stato applicato (per la prima volta a dei componenti di sistemi di pagamento con carta) il sistema S.T.R.I.D.E. di Microsoft, concepito per studiare la sicurezza di ambiti prettamente sistemistici, attraverso la modellazione delle minacce applicabili ad un sistema.
Il modello del terminale presentato introduce delle modifiche strutturali nell’architettura dei classici terminali installati attualmente nella rete di accettazione dell’area SEPA. In particolare viene utilizzato esclusivamente il lettore di carte a chip, e tutte le operazioni crittografiche svolte dal terminale vengono realizzate tramite un modulo software che rimpiazza il processore crittografico hardware. Gli impatti delle modifiche architetturali sulla sicurezza del sistema, sono state oggetto di un risk assessment che ha consentito di valutare eventuali modifiche nelle probabilità di accadimento di alcuni tipi di attacchi, e, in corrispondenza di un loro incremento, sono state valutate le tecniche di mitigazione. Le operazioni crittografiche svolte dal terminale attraverso il layer crittografico, vengono realizzate tramite algoritmi innovativi quali ECC e AES che sostituiscono i classici algoritmi crittografici RSA e TDES adottati dai terminali Pol attuali.