

LA CARTA NAZIONALE DEI SERVIZI E IL T-GOVERNMENT

di Giovanni Manca

La televisione digitale terrestre (TDT) costituisce un importante strumento tecnologico per la diffusione di informazioni in modo incisivo e completo. Considerando la grande diffusione delle apparecchiature televisive nelle famiglie italiane, si può prevedere che la TDT sia in grado di veicolare anche le applicazioni innovative nell'area dei servizi pubblici, che al momento si stanno diffondendo mediante la rete Internet.

La trasformazione dei servizi della pubblica amministrazione in servizi on line, sia che il loro utilizzo avvenga sulla rete Internet, sia che avvenga mediante il TDT (T-GOVERNMENT), richiede modalità di accesso sicure, facili e in grado di essere utilizzate nel modo più generale possibile.

Per favorire la convergenza degli strumenti di identificazione digitale paralleli alla Carta d'Identità Elettronica (CIE), emessa dai Comuni in sostituzione della carta d'identità tradizionale, è stato definito lo standard della Carta Nazionale dei Servizi (CNS). La CNS, progettata coerentemente alla CIE, al fine di anticiparne le funzioni di accesso ai servizi in rete, rappresenta il punto di riferimento per l'emissione di carte multiservizi. Mediante la CNS è possibile ottenere servizi sanitari, fiscali, usufruire di sistemi di pagamento bancari e postali e utilizzare la firma digitale. In particolare, è possibile accedere a strumenti di pagamento come BankPass web che già oggi viene utilizzato dai servizi di e-government in perfetta integrazione con l'autenticazione offerta dalla CNS.

Ma la CNS è utilizzabile per accedere in modo sicuro ai servizi innovativi offerti nell'ambito del cosiddetto T-GOVERNMENT ?

La risposta è positiva, ma il processo per il raggiungimento di questo risultato è tutt'altro che ovvio e facile. Vediamo quindi di esplorare questa nuova problematica di integrazione tra la smart card che fisicamente costituisce la CNS e il decoder utilizzato per la ricezione della TDT.

Tutti i decoder in commercio sono paragonabili a dei computer specializzati che operano in conformità alla piattaforma di riferimento Multimedia Home Platform (MHP) con lo scopo di consentire l'utilizzo delle caratteristiche specifiche della TDT. Tali decoder hanno almeno una slot per l'inserimento della smart card: alcuni ne hanno due.

La presenza di questi dispositivi è dovuta alla derivazione tecnologica dei decoder che prevedono di base l'utilizzo di smart card per la decodifica dei canali a pagamento. Tali smart card sono definite tecnicamente "conditional access smart card".

Le conditional card, al momento, non sono state previste nella diffusione nazionale. La loro tipologia di tipo "proprietario" introduce anche il rischio dell'utilizzo e conseguente diffusione da parte dei broadcaster di sistemi "condizionali" differenti. Questa situazione si è già verificata per il sistema di diffusione via satellite ed è stata risolta nel recente passato con grande difficoltà.

In ogni caso, queste slot sono a tutti gli effetti dei lettori di smart card in grado di supportare gli standard fisici e elettrici di riferimento (ISO 7816 parti 1-2-3).

Il software di interfaccia conforme allo standard ISO 7816-4 per l'interazione tra la smart card e il terminale non è ancora disponibile. Ciò significa che al momento non è possibile, senza sviluppi specifici, utilizzare nei decoder la CNS.

Per risolvere il problema è necessario prevedere una particolare implementazione del software di interfaccia con la smart card. In particolare è necessario scrivere del codice che tenga in conto che la piattaforma MHP è di tipo Java. Inoltre è necessario che l'ambiente di riferimento sia riconosciuto come standard internazionale.

Bisogna anche prevedere che le realizzazioni dei protocolli di interfaccia siano indipendenti per le varie tipologie di carte, altrimenti sarà indispensabile una specifica navigazione a menu o addirittura lo spegnimento e riaccensione del decoder.

Per la creazione di un ambiente software di riferimento per interfacciare la smart card va tenuto sicuramente in considerazione il SATSA (Security And Trust Services API) proposto da Sun Microsystems. Tale ambiente si colloca perfettamente nella piattaforma Java 2, Micro Edition e quindi è compatibile con MHP. Va tenuto però in conto che, al momento, nella piattaforma MHP l'ambiente di riferimento è Open Card Framework (OCF) da tempo non più supportato dal consorzio di aziende che lo hanno creato. Anche in questo caso sarà necessario un aggiornamento degli ambienti di riferimento.

Dal punto di vista pratico è significativo sottolineare che è stato possibile leggere informazioni da una CNS, utilizzando il cosiddetto "file dei dati personali". Questo file tra l'altro contiene l'anagrafica del titolare della carta compreso il codice fiscale. La lettura di questo file e il suo utilizzo nella transazione evita all'utente la complessa digitazione dei dati tramite telecomando.

Il passo successivo dovrà essere quello di realizzare una autenticazione forte tipo SSL/TLS verso i servizi offerti in rete dalla pubblica amministrazione e dai privati. Naturalmente tale tipologia di servizi dovrà essere utilizzata tramite canale di ritorno sicuro con meccanismi simili ma non identici a quelli utilizzati da un tradizionale personal computer.

Tutte queste attività sono in corso di svolgimento: sull'utilizzo della CNS con il decoder, il CNIPA sta progettando di promuovere a breve un seminario. Tale seminario coinvolgerà i principali attori di riferimento su queste problematiche, prima fra tutte la Fondazione Ugo Bordoni (FUB), e costituirà un importante momento di riflessione sull'argomento dell'interazione con le smart card.

Anche le proposte che verranno formulate nei bandi CNIPA e FUB, di prossima conclusione, contribuiranno a stimolare ulteriormente le soluzioni che dovranno diventare gli standard di riferimento per l'offerta di mercato.