

LA CARTA NAZIONALE DEI SERVIZI: PROGETTO O MITO?

Claudio Beretta

Ormai da molti anni si parla di distribuire ai cittadini italiani una smart card.

Per primo, e sono passati quasi 10 anni, era la carta del cittadino, poi si è parlato di carta sanitaria, di carta di identità elettronica e, infine, di carta dei servizi.

Durante questi anni sono state annunciate con grande clamore una serie quasi infinita di sperimentazioni (dalla carta del cittadino a quella della carta di identità elettronica, alla carta sanitaria europea), di cui nessuno, però, si è preso cura di informare poi sull'effettivo svolgimento di queste sperimentazioni e sul risultato ottenuto, probabilmente per evitare brutte figure.

Nessuna, infatti, delle sperimentazioni tentate negli anni '90 ha avuto esito positivo e, molto spesso, non è nemmeno effettivamente iniziata.

Ora, però, si è arrivati finalmente ad un punto di svolta: sembrano condivise le tecnologie da adottare, gli ambiti di utilizzo, le possibilità di integrazione e le modalità di distribuzione.

Soprattutto, lo sviluppo tecnologico ed il sistema industriale sembrano adeguati alla bisogna e il Governo, con un decreto del Ministro per l'Innovazione Tecnologica, è sul punto di varare il decreto che definisce in concreto cosa sia, a cosa serva e chi possa distribuire questa smart card (sempre che non sorgano ostacoli improvvisi, che, al momento, sembrano improbabili).

Il nome scelto è "Carta Nazionale dei Servizi", CNS in sigla, e, nel seguito, cercheremo di spiegare cos'è, cosa sta succedendo al riguardo e quali prospettive di distribuzione ci si possono, realisticamente, attendere.

Perché la CNS ?

L'idea che sta alla base della Carta Nazionale dei Servizi è molto semplice.

L'utilizzo dell'informatica, anche nei rapporti tra

Pubblica Amministrazione e cittadino, si sta facendo sempre più frequente e porta effettivamente enormi vantaggi in termini di tempo risparmiato e trasparenza amministrativa: allora, perché non scegliere di utilizzare un unico strumento per accedere con sicurezza (sia per la P. A. che per il cittadino) ai servizi informatici della P. A.?

Questo strumento di sicurezza altro non è che uno strumento di autenticazione che consente, al contempo, di stabilire un canale di collegamento sicuro, utilizzando la cifratura dei dati; la sicurezza comprende, quindi, sia il concetto di autenticazione che quello di sicurezza del canale di trasmissione.

Questa scelta porterebbe enormi vantaggi, in termini economici di affidabilità tecnica.

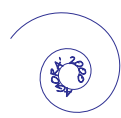
L'esistenza di un unico strumento di sicurezza permette di minimizzare gli investimenti per la realizzazione dell'infrastruttura tecnologica necessaria, ma porta, soprattutto, ad enormi risparmi nella costruzione degli adeguamenti tecnici ai sistemi informatici, già in uso nelle Pubbliche Amministrazioni, necessari per rendere disponibili per via informatica i servizi al cittadino.

La possibilità pratica di avere un unico strumento di autenticazione nasce dal fatto che, praticamente, il mercato offre un solo mezzo efficace per svolgere questo compito: una smart card dotata di un meccanismo di "firma elettronica".

Sarà sufficiente normare le caratteristiche tecniche di questo oggetto, adottando gli standard più diffusi e spingendo gli operatori privati a raggiungere accordi tra loro su questo argomento, per poter disporre di uno strumento comune senza penalizzare alcun operatore.

Questa opportunità è concretamente praticabile ora per tre ragioni.

La prima, il mercato della firma elettronica è ancora agli inizi, e i cambiamenti di formato, l'adozione



di un nuovo file system o l'implementazione di nuovi comandi nel sistema operativo non richiedono grossi investimenti né sono difficili da realizzare.

Secondo, anche se il mercato della firma elettronica è agli inizi, la tecnologia che utilizza è matura ed affidabile: le carte a microprocessore, le reti di comunicazione, i lettori di smart card sono strumenti affidabili, distribuiti in milioni di esemplari o usati da milioni di persone contemporaneamente; ciò rende possibile utilizzarli in un progetto di queste dimensioni (decine di milioni di smart card in tutta Italia).

Terzo, questo mercato non riesce a decollare: ha bisogno della spinta (e degli investimenti) della Pubblica Amministrazione per poter raggiungere una dimensione significativa, ha bisogno dell'impegno dello Stato e degli Enti Locali per poter essere credibile nei confronti dei consumatori.

In questo modo l'azione normativa del Governo non è vista come un'indebita ingerenza dagli operatori privati, ma è da loro richiesta a gran voce.

Inoltre, anche se non in Italia, alcune iniziative nel

settore si sono già svolte con successo in Europa: la più nota è la Carta di Identità Elettronica distribuita ai Finlandesi, ma è doveroso citare anche la Carta Sanitaria del sud dell'Irlanda.

Infine, anche in Italia la situazione ha cominciato a modificarsi: il progetto lombardo di Sistema Informativo Socio Sanitario si è evoluto in Carta Regionale dei Servizi, portando ad una sperimentazione effettiva, nella provincia di Lecco, con 305.000 smart card distribuite.

Quindi, adesso o mai più: il Governo deve agire ora se vuole rendere possibile l'adozione di un unico strumento di sicurezza per l'accesso ai servizi informatici della Pubblica Amministrazione.

Questo strumento è appunto la Carta Nazionale dei Servizi.

La Firma Elettronica

Come anticipato sopra, lo strumento che consente di fare tutte queste cose, e con un grado di sicurezza molto elevato, è una smart card, o carta a microprocessore, dotata di "firma elettronica".

Una smart card altro non è che un calcolatore por-



tatile, dotato di propria capacità elaborativa, propria memoria e proprio sistema operativo: non possiede alimentazione autonoma e non ha dispositivi di input / output e può, quindi, essere utilizzato solo attraverso un lettore apposito.

Le smart card e i loro lettori sono ormai oggetti standard, e le specifiche di collegamento elettrico e informativo sono definite, condivise ed utilizzate da tutti i produttori.

L'impulso principale alla diffusione delle smart card viene dalla telefonia mobile: le "schede telefoniche" che tutti noi usiamo sono smart card inserite in un lettore (dotato di batteria, display e tastiera) che è il telefonino.

Queste smart card, che oramai costano pochi euro, hanno microprocessori anche a 32 bit e memorie fino a 64 Kbyte, possono essere utilizzati per contenere una "firma elettronica", che si basa sull'esistenza di una coppia di "chiavi di cifratura" che agiscono asimmetricamente: una stringa di caratteri cifrata con una chiave può essere decifrata dall'altra, e viceversa.

Una chiave (la chiave privata) rimane sulla smart card e, quindi, in possesso del proprietario della "firma elettronica", mentre la seconda (chiave pubblica) è messa a disposizione di tutti; ciò avviene a cura di un ente emittitore (Certification Authority), che emette dei "certificati" (ovviamente in formato elettronico) con cui si assume la responsabilità della regolarità dell'intero processo; questo certificato viene collocato, assieme alla chiave privata, sulla smart card e contiene l'indirizzo Internet del proprio sito.

Su questo sito la Certification Authority si deve preoccupare di pubblicare le chiavi pubbliche, di tener aggiornata l'elenco dei certificati validi, di quelli scaduti, sospesi o revocati.

Così un documento cifrato con la chiave privata può essere attribuito con certezza al proprietario della smart card (firma), ed è leggibile da tutti utilizzando la chiave pubblica, mentre un documento cifrato con la chiave pubblica sarà leggibile solo da chi possiede la smart card (riservatezza) con la chiave privata corrispondente; ovviamente, è consentito l'uso reiterato della cifratura, ottenendo così l'invio riservato di un documento firmato.

Questo meccanismo, chiamato sinteticamente "firma elettronica", è riconosciuto e regolato dalla normativa europea ed italiana, consente di stabilire connessioni sicure tra client e server,

consente di stabilire la "non ripudiabilità" dei documenti elettronici e la loro trasmissione riservata al destinatario.

Per ragioni normative (i regolamenti comunitari e nazionali vietano l'utilizzo della chiave di firma come chiave di cifratura), la chiave utilizzata per l'autenticazione sarà diversa da quella utilizzata per la sicurezza del canale trasmissivo, e, di conseguenza, il meccanismo di "firma elettronica" descritto qui è dotato di due chiavi e di due certificati.

Cos'è la CNS

Abbiamo detto che è lo strumento per garantire la sicurezza nell'accesso ai servizi informatici.

Deve poter identificare il cittadino, assicurare che il collegamento sia con il server voluto, garantire la costruzione di un canale di collegamento sicuro tra chi chiede e chi eroga il servizio, impedendo sia la visibilità dei dati ad estranei sia la loro sostituzione durante la trasmissione.

Deve permettere la tracciabilità degli eventi e consentire che si possa dimostrare, a distanza di tempo, chi ha chiesto un servizio e chi ha messo a disposizione un documento.

Materialmente, la CNS altro non è che una carta a microprocessore dotata dei meccanismi di "firma elettronica" descritti in precedenza.

La CNS è pensata come "chiave d'accesso" ai servizi informatici della Pubblica Amministrazione: solo chi la possiede potrà interagire con Enti e Ministeri attraverso il proprio PC, ad esempio per presentare la dichiarazione dei redditi, per consegnare una richiesta, per ottenere un certificato.

Il fatto che sia una "chiave d'accesso" comporta che la smart card non venga, almeno di norma, utilizzata per immagazzinare dati: sulla smart card troveranno posto i soli dati identificativi del proprietario, le chiavi di firma e di cifratura e i rispettivi certificati.

Sono la limitata capacità di memoria e il crescente bisogno di spazio dei servizi informatici a costringere a questa scelta: i dati dovranno essere memorizzati su server accessibili via rete.

Il fatto che l'accesso ai servizi sia consentito via rete e che i dati siano memorizzati su server distribuiti sulla rete pone il problema dell'infrastruttura: parlare di CNS, perciò, significa parlare anche della costruzione di una infrastruttura comune di comunicazione accessibile sia ai cittadini che alle Amministrazioni.

In più, visto che tutte le Pubbliche Amministrazioni sono coinvolte nel progetto, si pone il problema di

chi emette la CNS e di chi garantisca la sicurezza anche per gli altri.

Quello dell'emissione è strettamente collegato agli altri strumenti elettronici previsti da vari decreti e leggi: la carta sanitaria, la carta di identità elettronica, il tesserino fiscale.

Infine, c'è il problema principale ovvero quello dei servizi.

Uno strumento di accesso ai servizi ha senso solo se i servizi ci sono e ci si può accedere: attualmente non si può dire che nella P. A. italiana abbondino i servizi utilizzabili con strumenti informatici; inoltre, senza risolvere il problema dell'infrastruttura non si avrebbe la possibilità di accedervi.

Il decreto di cui si sta completando la stesura, oltre a stabilire gli standard tecnologici, deve risolvere almeno il problema dell'emissione, cioè chi può emettere la CNS e che garanzie deve dare alle altre amministrazioni in materia di sicurezza nel rilascio e nella gestione.

Per quanto riguarda gli standard tecnologici, tutto sembra a posto.

Chi emette la CNS potrà usare la smart card che crede, scegliendo liberamente processore e sistema operativo; basterà assicurare 30 Kbyte di memoria libera. Uno strato software distribuito assieme ai lettori permetterà di caricare le librerie software adatte a quella smart card: questo "switch software" è già disponibile per tutte le smart card in commercio.

Il formato del certificato dovrà recepire l'accordo già raggiunto tra gli operatori privati riuniti nell'Assocertificatori: quindi ci sarà un unico formato di certificato per tutti i tipi di firma elettronica disponibili, in quanto il formato dell'Assocertificatori è valido anche per la firma elettronica a valore legale. Questo semplificherà significativamente e renderà meno costoso lo sviluppo del software di back office di integrazione con gli strumenti di autenticazione.

Per quanto riguarda le garanzie, chi emette la CNS deve dare le garanzie di un comune certificatore: la Certification Authority non dovrà necessariamente essere accreditata presso il Ministro dell'Innovazione.

Per quanto riguarda l'emissione, sembra raggiunto l'accordo che qualunque Pubblica Amministrazione (Comuni, Regioni, Ministeri) può emettere la CNS, anche avvalendosi di un certificatore esterno.

È su questo argomento che sono possibili delle sor-

prese, anche se i contrasti tra Regioni, Comuni e Ministero sembrano risolti e gli accordi sono stati recepiti a livello politico.

Infatti, se è vero che sono possibili molte CNS diverse, c'è un accordo sostanziale tra tutti su una preminenza dei Comuni come Enti emettitori: i Comuni hanno in carico l'aggiornamento dei dati anagrafici e sono i più diffusi sul territorio: sono, quindi, i più adatti a distribuire le smart card.

Questo potrà consentire la convergenza della CNS con la CIE (Carta di Identità Elettronica), che viene emessa dal Ministero dell'Interno ma è distribuita dai Comuni, e renderà possibile, attraverso una convenzione con la Regione di appartenenza, l'uso della CNS come Carta Sanitaria; infatti la carta sanitaria ha bisogno di un proprio file system per i pochi dati sensibili (dati di emergenza, esenzioni) memorizzati sulla smart card.

È, però, sempre in agguato il ritorno di fiamma di qualche Ministero che, per spirito centralistico o per qualche ragione inconfessata, si voglia sostituire alle Amministrazioni locali.

0

Sono quello relativo all'infrastruttura di collegamento e quello dell'adeguamento del back office delle Pubbliche Amministrazioni.

Per quanto riguarda l'accessibilità dei servizi della P. A., questo è ovviamente il problema principale, quello che ha bisogno dei più grossi investimenti (miliardi di euro, certamente), quello con i tempi più lunghi di risoluzione ma, paradossalmente, il meno importante oggi.

L'importanza degli investimenti, le riorganizzazioni di processo coinvolte, i lunghissimi tempi di realizzazione rendono il processo di adeguamento del back office difficilmente governabile, molto dipendente dalle dinamiche di mercato.

Le esperienze europee dimostrano chiaramente che sarà il chiarimento normativo sugli strumenti tecnici e soprattutto la distribuzione in quantità significative di smart card per l'accesso ai servizi a stimolare il mercato ed a provocare un'accelerazione nella offerta informatica di servizi.

Il problema dell'infrastruttura di comunicazione rischia di essere molto più complicato e, non a caso, non è previsto che il decreto sulla CNS lo affronti.

Dire "infrastruttura di comunicazione" è tecnicamente corretto, ma rischia di essere interpretato in modo riduttivo.

La realizzazione di questa infrastruttura di comuni-

cazione è in pratica la costruzione di un sistema informativo estremamente complesso, quello che lega assieme i sistemi informativi di tutti gli Enti Locali e di tutta l'Amministrazione Centrale (Ministeri) e periferica (Prefetture) dello Stato.

I sistemi informativi dei vari Enti continuano ad essere gli stessi, completamente diversi l'uno dall'altro per scelte tecnologiche, architettura informatica e filosofia di rapporto con il cittadino, ma, verso l'utente esterno (cittadini o altri Enti), utilizzano lo stesso sistema di sicurezza (la CNS) e la stessa rete di trasporto.

L'uso di un comune strumento di sicurezza e di una stessa rete informatica rendono corretta l'affermazione che esiste un "unico" sistema informativo della P. A.

Su quale sia la rete fisica di trasporto esistono pochi dubbi: deve essere la rete Internet, l'unica accessibile da tutti, l'unica attualmente usata per erogare i pochi servizi che la P. A. ha reso accessibili per via informatica.

Su questa, per garantire la sicurezza (inesistente in Internet), devono essere implementati gli strumenti di rete virtuale (VPN, dal nome inglese) basati sulla facoltà di cifratura del meccanismo di firma elettronica.

Quale siano gli strumenti da scegliere, chi abbia l'incarico di controllarli, chi di gestirli, come le P. A. debbano adeguare i propri sistemi informativi non è stato deciso, non si sa cosa e come verrà deciso, e molteplici soluzioni, tra loro alternative, sono state proposte.

In origine si era proposto il modello della RUPA (senza chiarire, però, come potesse estendersi agli Enti Locali o collegarsi con il livello locale), poi il Centro Tecnico ha abbandonato la RUPA ed è stato lanciato il progetto della Rete Nazionale (anche qui, senza chiarire i dettagli tecnici delle modalità di collegamento tra i vari componenti), ora sembra rientrata in auge la RUPA e sembra fallito il progetto di Rete Nazionale.

Ovviamente, tutto "sembra" e nulla è certo, in quanto solo notizie informali sono disponibili, e nessuna sembra in grado di fornire informazioni certe, definite ed affidabili.

Nel frattempo, ognuno si comporta come vuole: con il rischio che quanto realizzato sia incompatibile con il disegno complessivo.

Per concludere, la situazione attuale, pur avendo definito in modo abbastanza definitivo quasi tutte le caratteristiche tecniche della Carta Nazionale dei Servizi, è ancora di estrema confusione sulle moda-

lità operative da adottare per la sua diffusione. Speriamo che questa fase si risolva rapidamente, per dar modo di iniziare un processo che, per le dimensioni numeriche e per il gran numero di sistemi informativi coinvolti, avrà tempi di realizzazione molto lunghi ma che, al suo termine, potrà rappresentare il salto decisivo in tema di semplicità di accesso ai servizi e di trasparenza della Pubblica Amministrazione.

