SERVIZI ON-LINE PER CITTADINI E IMPRESE
PIANO DI E@GOVERNMENT

COMMENTI E PROPOSTE OPERATIVE SULLE PROBLEMATICHE
LEGATE ALL'AUTENTICAZIONE DI CITTADINI E IMPRESE
- terza versione a fronte dell'entrata in vigore del Decreto 23/01/2002, n.10 -

SINTESI DELLO SCENARIO

Le linee guida (chiamate Avviso) proposte dal Governo per la presentazione dei progetti di e@government forniscono delle indicazioni molto precise in merito alle problematiche relative all'autenticazione dei soggetti fruitori, cittadini e imprese, di servizi online messi a disposizione dalle pubbliche amministrazioni
(Allegati 1 e 4).

Il recepimento della Direttiva Europea sulla firma elettronica
E' da tempo definito, anche se in continua evoluzione, un quadro normativo di riferimento che identifica degli strumenti "nazionali" di autenticazione. Il DPR 445/2000, art. 38, comma 2, definisce che:

"Le istanze e le dichiarazioni inviate per via telematica sono valide se sottoscritte mediante la firma digitale o quando il sottoscrittore è identificato dal sistema informatico con l'uso della carta d'identità elettronica".

Come accennato il quadro normativo è in evoluzione, soprattutto in base all'urgente necessità di recepimento della Direttiva Europea in materia di Firma Elettronica. E' entrato infatti in vigore lo scorso 3 Marzo (Pubblicato sulla Gazzetta Ufficiale del 15 febbraio) il decreto legislativo del 23 Gennaio 2002, n.10, che recepisce la direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche. Le differenze sostanziali tra firma elettronica debole, introdotta dalla normativa comunitaria, e firma elettronica forte, così come definita nella nostra legislazione, sono di carattere formale. La "firma elettronica forte", detta più propriamente rispetto alla direttiva europea Firma Qualificata, è basata su dispositivi di firma sicuri (dispositivi programmabili solo all'origine, quindi tipicamente smart card) con certificati emessi da operatori qualificati in ambito nazionale attraverso apposita procedura di accreditamento. Nel caso italiano si parla di certificati su carte a microprocessore (necessariamente rispondenti a dei livelli internazionali di certificazione sulla sicurezza – ITSEC-E3 o superiore) rilasciati da certificatori iscritti all'Albo Nazionale tenuto dall'Aipa. Una firma elettronica forte è per definizione riconosciuta per legge a priori. La "firma elettronica debole" è invece basata su certificati emessi da un qualsiasi operatore di mercato del territorio comunitario anche senza che questi si sia accreditato presso alcun organismo nazionale. Il processo informatico è attivabile anche senza l'uso di dispositivi di firma sicuri. Una firma elettronica debole non può essere rifiutata come prova in un tribunale di uno stato membro ma ha l'onere della prova (deve cioè essere dimostrata cioè la bontà o l'inefficacia della sua implementazione dal punto di vista tecnico-organizzativo).

Il decreto entrato in vigore introduce il nuovo concetto (per l'Italia) di firma elettronica debole, implementabile anche attraverso la prestazione di servizi di certificazione da operatori non necessariamente qualificati da alcun procedimento nazionale. Nel citato schema viene anche proposta la modifica del sopra riportato art. 38 del Dpr. 445/2000. La modifica proposta prevede però l'introduzione come ulteriore meccanismo di riconoscimento valido della sola Carta Nazionale dei Servizi.
Il suddetto decreto introduce altresì modifiche al Dpr. 445/2000, al citato art. 38, comma 2, che ora diviene:

Le istanze e le dichiarazioni inviate per via telematica sono valide:
a) se sottoscritte mediante la firma digitale, basata su di un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura;
b) ovvero quando l'autore e' identificato dal sistema informatico con l'uso della carta d'identita' elettronica o della carta nazionale dei servizi."

Strumenti di autenticazione e strumenti di Firma Digitale
Il citato art. 38, nel tentativo di assegnare alla Carta di Identità Elettronica (in seguito brevemente indicata con CIE) e alla Carta Nazionale dei Servizi (in seguito brevemente CNS) la valenza di strumenti di riconoscimento anche in rete, introduce una prima confusione. Il DPR. 513/97 ha a suo tempo assegnato alla Firma Digitale la valenza probatoria della firma autografa, sgombrando contemporaneamente il campo dalla possibilità di utilizzare quello stesso strumento come sistema di autenticazione in rete. La firma digitale apposta ad un documento elettronico sancisce la volontà, costante nel tempo, di una certa persona rispetto al contenuto dello stesso. Il documento firmato deve

essere conservato, secondo specifiche regole tecniche, e l'associazione tra firmatario e documento mantenuta nel tempo secondo le regole tradizionali tutt'ora valide (ad esempio contratti di un certo tipo per dieci anni).
L'autenticazione è invece un atto istantaneo nel tempo, un azione che viene eseguita su un particolare sistema informativo. Eseguire una determinata azione attraverso uno strumento di identificazione riconosciuto per legge significa assegnare la non ripudiabilità all'azione stessa, ma le informazioni eventualmente introdotte dall'utente sul sistema non vengono, come avviene per definizione con la firma digitale, associate, costantemente e immodificabili nel tempo, all'esecutore. Questa era l'impostazione ante DPR 445/2000.
Ora invece si attribuisce il medesimo valore, limitatamente al rapporto tra soggetto e Pubblica Amministrazione, sia alla Firma Digitale a norma Aipa sia ad uno strumento di autenticazione (benchè basato sulla medesima tecnologia dei certificati) legalmente molto diverso come la CIE. In questo nuovo contesto paradossalmente la Firma Digitale è necessaria solo più nei rapporti tra privati (e evidentemente all'interno della stessa PA). Nel rapporto tra privati e pubblico la CIE e la CNS diventano lo strumento di riferimento, essendo d'altra parte strumenti forniti dalla stessa PA ai suoi soggetti fruitori.

La Carta Nazionale dei Servizi

La Carta Nazionale dei Servizi nasce come idea qualche mese fa, dopo un breve periodo di monitoraggio delle prime sperimentazioni sul campo della CIE (Torino ricordiamo è una delle città coinvolte nel progetto). Il governo ha evidenziato problemi strutturali, sia dal punto di vista tecnico, sia dal punto di vista organizzativo, i quali stanno tutt'ora rallentando in modo inaspettato la diffusione dello strumento. Da possibile volano per la diffusione dei servizi telematici della PA ai cittadini la CIE è divenuta paradossalmente un freno.
Parallelamente negli ultimi mesi si è finalmente assistito ad una prima diffusione, non senza problemi e impatti per le organizzazioni ma essenzialmente in linea con le esigenze delle amministrazioni locali, di strumenti di Firma Digitale a norma Aipa attraverso accordi tra il pubblico e le società private accreditate presso l'Aipa per la prestazione di servizi di certificazione. In questo contesto ricordiamo l'accordo tra la Pubblica Amministrazione Piemontese (attraverso il Csi-Piemonte) e il certificatore Infocamere. Ma anche la Firma Digitale (ricordiamo emessa da quattordici differenti certificatori) è tutt'ora afflitta dal problema dell'interoperabilità. Un posto di lavoro attrezzato per gestire la Firma Digitale di un certo certificatore non è oggi in grado di gestire l'analogo strumento di nessun altro certificatore.

In questo contesto il governo italiano nell'ultimo semestre si è posto il problema di animare il mercato dei produttori di smart card e dei prestatori del servizio di certificazione per identificare quale potesse essere lo strumento di riferimento per i prossimi tre-cinque anni, in attesa che la CIE andasse a regime. Questo strumento, fino a qualche settimana fa ancora non definito tecnologicamente, è stato definito Carta Nazionale dei Servizi. Prima ancora di giungere ad una preciso disegno tecnico-organizzativo della Carta Nazionale dei Servizi il governo si è preoccupato, per accelerare i tempi, di presentare un disegno di legge per la modifica dell'art. 38 del Dpr. 445/2000, aggiungendo tra gli strumenti validi per la transazioni in rete tra soggetto privato e pubblica amministrazione anche la CNS, in aggiunta alle già presenti CIE e Firma Digitale.

Il concetto di Carta Nazionale dei Servizi in questo nuovo scenario normativo (ancora incompiuto formalmente) è dunque ripreso con forza nell'Avviso per la presentazione dei progetti nell'ambito del piano di e@government.

Tale strumento è stato essenzialmente introdotto dall'attuale governo per i seguenti motivi:
la Carta di Identità Elettronica, riconosciuta da tutti come lo strumento di riferimento per l'autenticazione online di cittadini e imprese, stenta ad essere massivamente diffusa, soprattutto a causa di problemi tecnici (eccessiva giovinezza della tecnologia della banda laser), organizzativi (alto impatto sull'organizzazione dei comuni) e di approvvigionamento (l'Istituto Poligrafico e Zecca dello Stato non ha oggi un impianto tecnico-organizzativo per la fornitura di milioni di carte/anno).
I comuni coinvolti nella fase di sperimentazione sono pochi, come sono poche le carte CIE bianche ad essi assegnate, impedendo di fatto la costruzione di servizi ad adeguata ricaduta sul territorio
Alcuni comuni italiani hanno intrapreso negli ultimi anni la costruzione di iniziative locali basate su carte a microprocessore (Parma, Siena, alcuni regioni con le schede carburanti) o meccanismi analoghi di riconoscimento (Bologna, e ovviamente Torino e prima cintura metropolitana con l'iniziativa CittàPiùFacile). Tutte queste iniziative, lodevoli per iniziativa e bontà di impostazione, spesso anche con risultati significativi, hanno dimostrato come un'azione non coordinata dal centro di fatto non possa garantire l'interoperabilità delle diverse soluzioni. Un cittadino di Parma non potrà mai fruire di un servizio di Torino come un cittadino di Collegno, nel caso fosse proprietario di una casa a Bologna, non potrà mai pagarne l'ICI online. Analogo discorso vale per i diversi PIN messi in circolazione dagli organismi centrali (INPS, Ministero delle Finanze, Poste).

Le soluzioni di Firma Digitale a norma Aipa non sono interoperabili tra loro (se non a livello di formalizzazione del documento firmato –struttura PKCS#7).

Il Governo ha dunque inizialmente recuperato il concetto di Firma Digitale come strumento per l'autenticazione dei cittadini, essendo di fatto equivalente rispetto al citato art. 38. La proposta dell'estate 2001 indicava dunque alle Pubbliche Amministrazioni, in via ancora non ufficiale, la distribuzione di carte di Firma Digitale come soluzione per la diffusione di carte servizi dei cittadini riconosciute per legge e interoperabili a livello nazionale. La proposta era dunque di assurgere a carta dei servizi per la pubblica amministrazione tutte le carte di Firma Digitale regolarmente emesse dai Certificatori iscritti all'Albo Nazionale dell'Aipa a patto che il mercato risolvesse il citato problema dell'interoperabilità delle diverse soluzioni sui posti di lavoro. Oggi, mese di Gennaio, attraverso lo sviluppo di opportuni software da parte di aziende del settore il problema dell'interoperabilità sembra superato.

Nell'Allegato 4 dell'Avviso però si evidenzia come la CNS sia invece definita come semplificazione della Carta di Identità Elettronica. Anche questa impostazione, se pur molto differente dalla precedente, a chi scrive sembra comunque plausibile. Definire uno standard di riferimento che, partendo da stringenti definizioni tecnologiche (la CIE) ma contemporaneamente scevro di alcune complessità organizzative, possa permettere la diffusione di uno strumento (legalmente riconosciuto e interoperabile a livello nazionale) secondo tempi e modalità organizzative definite localmente dalla singole amministrazioni, può apparire altrettanto accettabile.
Per dovere di completezza si evidenzia come la seconda impostazione sia molto meno accettabile della prima da parte dei diversi produttori di carte a microprocessore. Infatti molti di questi oggi sono in grado di offrire al mercato una carta per Firma Digitale[1], mentre solo uno (Siemens) sarebbe pronto a fornire una carta perfettamente compatibile con la CIE, perché proprio questo ha collaborato da almeno un anno alla definizione dei contenuti tecnologici dello strumento con il Ministero dell'Interno.

I diversi livelli di servizio e di autenticazione definiti nell'Avviso
Prendendo spunto da alcune esperienze rilevanti del panorama nazionale lo scenario sugli strumenti di autenticazione apparsi negli ultimi anni può essere così sintetizzato:

Strumento	Tipo	Validità legale	Interoperabilità	Criticità
PIN INPS	Password	Nessuna de facto	Nessuna	Implementazione mono-provider
Siena Card	Smart Card senza firma digitale	Nessuna de facto	Nessuna	Implementazione locale e mono-provider
PIN Ministero Finanze	Password	Verticale (grazie ad eccezione inserita ad hoc nella legge)	Nessuna	Implementazione mono-provider
TorinoFacilissima CittàPiùFacile CA Sistema Piemonte	Certificato per browser (o su smart card per dipendenti pubblici come per la Regione Piemonte – Smarty)	Firma elettronica debole	Livello regionale	Implementazione regionale Manca recepimento direttiva europea
CIE	Certificato del Ministero dell'Interno su smart card	Piena, sia online sia offline	Per definizione	Difficoltà alla diffusione per almeno tre-cinque anni
CNS	Certificato del Ministero dell'Interno su smart card	Piena online	Per definizione	Mancano dettagli tecnici e organizzativi. Tempi anche qui incerti.
Firma Digitale a norma Aipa	Firma Digitale a norma Aipa	Piena online	Per definizione	Nessuna

Dopo aver analizzato sinteticamente il panorama nazionale degli strumenti di autenticazione, si procede ora ad una breve analisi dei diversi livelli di servizio definiti nell'Avviso al bando di e@government .

[1] Tecnologicamente sono carte RSA attive, con anche solo 8 Kb di EEPROM, certificate ITSEC-E3

E' obiettivo di questa analisi giungere ad una associazione tra i diversi livelli definiti con i diversi strumenti di autenticazione, per verificare se esistano tutti i presupposti, tecnici e organizzativi, per la realizzazione nel breve periodo, in modo compliant con il presente Avviso, di servizi online a cittadini e imprese.
Si riportano in modo schematico le definizione riprese dall'Avviso.
Livelli di interazione (cluster europeo)
Liv 1 informativo
Liv 2 one way (scarico moduli pdf con compilazione off-line su carta e spedizione fisica)
Liv 3 two way (seguita da conclusione nel mondo fisico – es spedizione cartaceo, pagamento a sportello)
Liv 4 transazione "one stop shop" compresa di pagamento e conclusione

Livelli di autenticazione
Liv 0 nessuno
Liv 1 username e password (compreso CIP veicolato attraverso la carta CittàPiùFacile)
Liv 2 firma elettronica debole (firma attivabile con il certificato rilasciato con CittàPiùFacile)
Liv 3 firma elettronica forte (firma Aipa - Infocamere, CIE, CNS)

In modo meno didascalico e analitico (quindi passibile di errata intepretazione di chi scrive) dall'Avviso si possono anche "leggere" a questo punto le ricercate associazioni tra livello di servizio e livello di autenticazione.

Associazione tra livelli di servizio e livello di autenticazione (deduzioni)

Livello di interazione	Livello di autenticazione richiesto
Liv 1 informativo	Liv 0 nessuno
Liv 2 one way	Liv 1 username e password (compreso CIP, PIN)
Liv 3 two way	Liv 2 firma elettronica debole (firma CittàPiùFacile, Sistema Piemonte)
Liv 4 transazione	Liv 3 firma elettronica forte (firma Aipa, CIE, CNS)

In ultimo, secondo l'apprezzabile suddivisione ad eventi dei servizi al cittadino e alle imprese, si evince che i servizi definiti PRIORITARI, quelli per i quali il governo auspica la maggior concentrazione delle risorse organizzative ed economiche, sono quasi sempre associabili ai livelli di interazione 3 e 4. In conclusione i servizi online della pubblica amministrazione locale potrebbero essere erogati, nella maggior parte dei casi, da strumenti quali CittàPiùFacile (equiparabile alla firma elettronica debole), mentre solo alcuni di essi richiederebbero strumenti come la Firma Digitale a norma Aipa, la CIE o la CNS.
Secondo però l'impostazione del governo volta a garantire l'interoperabilità e la riusabilità dei servizi al di là della singola amministrazione che li ha predisposti, tutti i servizi, anche quelli per cui potrebbe essere sufficiente la firma elettronica debole, devono poter essere fruiti dalla CIE e dalla CNS, secondo una inusuale quanto però comprensibile nei bisogni "compatibilità verso l'alto". Infatti l'Allegato 4 dice:

"… Ogni Amministrazione, che intenda erogare servizi che richiedono un forma di autenticazione dell'utente, può scegliere in piena autonomia quale tipo di autenticazione richiedere ai propri cittadini, garantendo comunque che l'accesso ai propri servizi possa sempre avvenire anche tramite la CIE /CNS …"

Se l'analisi ha fin qui portato alla prima conlcusione che l'impostazione data dall'Avviso è dal punto di vista generale condivisibile, nei paragrafi successivi verranno analizzate le problematiche che possono in diversa misura compromettere questo scenario e limitarne, se non bloccarne l'applicabilità nel breve periodo.

LE PRINCIPALI PROBLEMATICHE

Come sopra riportato uno dei requisiti essenziali per la predisposizione di servizi online nell'ambito del piano di e@government è la compatibilità con la CNS.
Definire un servizio compatibile con la CNS è essenzialmente definire la sua compatibilità con la CIE. Infatti, per come definito, la CNS eredita la struttura dati del chip della CIE in ogni sua parte, anche se non si evince nell'Avviso chi rilasci il certificato di autenticazione memorizzato su di essa.

L'Avviso (Allegato 4) infatti definisce:

Carta Nazionale dei Servizi (CNS): caratteristiche e modalità di emissione
"… Il centro di produzione della CNS può essere un qualsiasi fornitore di microchip che ha dichiarato la compatibilità dei propri supporti con quelli standard della CIE e che ha ricevuto le specifiche di formattazione e di inizializzazione da SSCE …"

Problematiche organizzative

Dalla sintetica analisi sulla CNS presente nell'Allegato 4 dell'Avviso non si evincono in nessun modo:

- Se ad oggi esistono nel panorama nazionale fornitori già accreditati dal Ministero dell'Interno
- Se il certificato di autenticazione necessario per l'autenticazione con la CNS è comunque emesso dal Ministero dell'Interno come per la CIE
- Se l'emissione della CNS avviene per mezzo di apposito software messo a disposizione dal Ministero dell'Interno come per la CIE
- Se è già operativo, come per la CIE, un Centro Servizi in grado di gestire CRL/CSL[2] dei certificati emessi

Problematiche tecniche

Parallelamente, dal punto di vista squisitamente tecnico, si evidenzia alcune criticità. E' stato rilasciato il software di interfacciamento della CIE secondo lo standard Microsoft CSP e RSA PKCS#11. Questo permette, ed è stato effettivamente già testato con successo, l'interfacciamento della CIE con i più comuni browser. La stessa cosa presumibilmente sarà possibile con la CNS. Purtroppo però il meccanismo di autenticazione più comune si basa sul protocollo SSLv3 che, verificando e analizzando il certificato utente memorizzato su una carta, permette l'accesso ad un determinato servizio. Il certificato del Ministero dell'Interno non è però esaustivo in termini di informazioni veicolate. Tale certificato diviene funzionale all'accesso ad un sito web solo se accompagnato dall'invio da parte della carta del file contenente i dati anagrafici del cittadino, dati che nel certificato sono solo riportati come Hash (SHA-1 o MD5) degli stessi. E' dunque fondamentale, per implementare un processo di autenticazione basato su CIE o CNS, lo sviluppo di un Applet o di un plug-In per browser che interfacci lo strato di middleware sul client (Metacomandi Dll) per interagire con la carta in modo non standard. I problemi di questa impostazione sono evidenti. La tecnologia degli Applet (ancorchè necessariamente firmati per accedere a risorse locali) è in molti settori considerata ormai superata, anche per problemi di compatibilità e portabilità rispetto ai due diversi tipi di browser. Analogo difetto è evidenziabile per i plug-in, i quali devono ulteriormente tenere in conto delle diverse versioni e delle evoluzioni dei browser della piattaforma client.

Il problema potrebbe essere risolto se il Centro Servizi della CIE e della CNS (che dovrà obbligatoriamente detenere la lista dei certificati emessi, sospesi e revocati) mantenesse anche in linea, disponibili ai server che implementano i servizi, i tracciati anagrafici dei cittadini a cui è rilasciata la carta, il cui digest[3] è contenuto nel certificato, unico elemento da reperire dalla carta inserita sulla piattaforma client. In questo modo il servizio applicativo del comune dovrebbe semplicemente ricevere dal client il certificato e attraverso il numero seriale dello stesso reperire dal Centro Servizi il tracciato da verificare sulla base dell'hash. In questo modo il servizio potrebbe riconoscere in modo rapido, centralizzato e sicuro un cittadino in rete.

Ad oggi però, in base alle informazioni che pervengono dal governo e dalle strutture tecniche ad esso associate, non è semplice definire l'impostazione progettuale dei servizi per le amministrazione locali, al di là di una semplice quanto teorica dichiarazione di compatibilità delle proprie applicazioni con la CNS.

Problematiche normative

Partendo dal presupposto che entro pochi mesi il quadro normativo venga reso compiuto anche per quanto riguarda la CNS, ulteriore elemento di incertezza che in diversi ambiti, soprattutto nei servizi verso le imprese, sta ostacolando la fase di analisi e progettazione è la problematica relativa alle deleghe e alle svariate figure di intermediazione che spesso intervengono fra Pubblica Amministrazione e i soggetti fruitori. Professionisti per la presentazione, ad esempio, di pratiche edilizie per conto del cittadino, consulenti del lavoro che operano con la provincia in nome e per conto delle imprese sono figure di intermediazione e casistiche che oggi intervengono spesso nei confronti della Pubblica Amministrazione. Quale modello organizzativo può essere seguito da parte di un comune che voglia rilasciare la CNS ad un professionista che è residente in un altro comune ma operi sul suo territorio? E come può il comune essere certo che la presentazione della pratica online sia effettuata non solo da Mario Rossi, ma effettivamente da Mario Rossi regolarmente iscritto all'Albo degli Architetti della Provincia?

---

[2] CRL/CSL: Lista dei certificati revocati (sospesi).

[3] Risultato del procedimento di hashing (SHA-1, MD5, RIPEMD-160) ad un determinato insieme di informazioni

PROPOSTA OPERATIVA

In base ai requisiti imposti dal governo per la pertecipazione al bando, ma anche in riferimento ai problemi evidenziati, l'unica impostazione oggi perseguibile in concreto, che possa garantire ricadute sul sistema provinciale in tempi brevi, può essere:

diffusione dello strumento CittàPiùFacile ai comuni della provincia, in modo da accrescere la nuova cultura dello sportello in rete nelle amministrazioni locali e iniziare un nuovo rapporto, telematico, diretto e interattivo, con i cittadini del territorio. Questo strumento, previa verifica di dettaglio con le opportune figure tecniche della commissione di valutazione, dovrebbe permettere la diffusione di servizio di livello 3 (secondo la tabella 3 dell'Allegato 1) ai cittadini della provincia di Torino.

diffusione dello strumento Firma Digitale a norma Aipa alle imprese, attraverso l'accordo con la Camera di Commercio e con il Certificatore Infocamere, per la realizzazione di servizi anche di livello 4 alle imprese (secondo la tabella 3 dell'Allegato 1).

implemetazione dei precedenti servizi attraverso portali territoriali che per mezzo della loro centralizzazione permettano facilmente l'implementazione tecnica, non appena i presupposti definiti in precedenze lo permetteranno, di una effettiva compatibilità verso la CIE e la CNS.

CONCLUSIONI

Se in questa impostazione si deve muovere una lucida quanto oggettiva critica al governo è essenzialmente sui seguenti punti:
Scarsa chiarezza dei tempi sulla disponibilità dell'impianto organizzativo per mettere nelle condizioni le amministrazioni locali di emettere massivamente CNS per avere una ricaduta significativa e nel breve periodo sul territorio;
Scarsa chiarezza nei requisiti tecnici, spesso frammentati e reperiti da diverse fonti disallineate tra loro;
Scarso coinvolgimento tecnico delle amministrazioni locali sul tema della sicurezza e del riconoscimento in rete (soprattutto auspicabile per chi, come il Piemonte, in questa materia non si è limitata alla mera disquisizione tecnica), quando questo viene essenzialmente instaurato con aziende private il cui interesse in materia evidentemente definisce priorità e scelte spesso non convergenti con quelle della pubblica amministrazione.

Tuttavia, da questa rapida e forse incompleta panoramica, si evince come lo strumento Carta Nazionale dei Servizi, secondo il parere di chi scrive, possa essere ritenuta per le amministrazioni locali un'importante opportunità. La CNS è prima di tutto uno strumento riconosciuto per legge (nuovo art. 38), la cui diffusione potrà essere però guidata localmente in base alle esigenze delle singole amministrazioni. Non ultimo la termografia, come anticipato nell'Allegato 4, sarà liberamente definita dal comune e quindi utilizzabile come strategico strumento di marketing territoriale. Ricordiamo invece come per diverse ragioni sia la CIE sia la Firma Digitale abbiamo stringenti vincoli sull'impostazione del loro layout.