L'identificazione in rete

di *Pierluigi Ridolfi*[1]

1. I sistemi informatici e il problema dell'identificazione dell'utente

L'architettura di un sistema informatico è basata generalmente su tre macrocomponenti:

- un complesso di elaborazione (un sistema centrale oppure un insieme distribuito di server oppure una soluzione basata sulle moderne tecnologie di *cloud computing*) che gestisce una o più applicazioni informatiche;
- un numero più o meno vasto di persone, ognuna dotate di un personal computer (o equivalente), interessate a utilizzare le applicazioni informatiche (*utenti*);
- una rete in grado di collegare gli utenti al complesso di elaborazione.

In genere si pone il problema di verificare in modo certo l'identità di ogni singolo utente che accede alle applicazioni del sistema, anche al fine di proteggere il sistema informatico e le applicazioni stesse da interventi di persone *estranee*.

A questo proposito si intendono con:

- "*identificazione informatica*" o "*identificazione in rete*", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità dell'utente;
- "*credenziali di identificazione*", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'identificazione informatica;
- "*profilo di autorizzazione*", l'insieme delle informazioni, univocamente associate ad una persona, che consente al complesso di elaborazione di individuare a quali applicazioni essa può accedere;
- "*sistema di autorizzazione*", l'insieme degli strumenti elettronici e delle procedure che abilitano l'accesso alle applicazioni, in funzione del profilo di autorizzazione del richiedente.

2. Aspetti normativi

La terminologia "*identificazione informatica*" è relativamente recente: introdotta dal Dlgs. 235 del 31 dicembre 2010 (che modifica il Dlgs. 82/05, Codice dell'Amministrazione digitale, brevemente "CAD", dando vita a quello che nel linguaggio corrente è chiamato "nuovo CAD"), ha sostituito la precedente definizione di "*autenticazione informatica*"[2].

Di autenticazione informatica trattano il Codice per la protezione dei dati personali (Dlgs. 196/03, art. 4, comma 3) e il CAD (art. 1, comma 1, punto u-*ter*), prima dell'intervento del nuovo CAD. In quest'ultimo l'*identificazione informatica* è formalmente definita come "*la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco a un soggetto, che ne consentono l'individuazione*

[1] Università di Bologna, già Componente del Collegio del Cnipa e Presidente della Commissione interministeriale sulla dematerializzazione.

[2] Nella letteratura internazionale questo concetto è noto con il termine inglese di "authentication", la cui traduzione corretta è "di sicura origine". L'*autenticazione*, nella terminologia giuridica italiana, si riferisce esclusivamente a un tipico processo notarile

nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso". La definizione non è un capolavoro di chiarezza, ma rende l'idea.

Il tema è ripreso nell'articolo 64 che descrive le modalità di accesso ai servizi erogati dalle pubbliche amministrazioni. Il testo nel nuovo CAD è il seguente:

1. *La carta di identità elettronica* (CIE) *e la carta nazionale dei servizi* (CNS) *costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica*.
2. *Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da essi erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio*.

A questo punto è necessario fare un po' di storia e ricostruire come si è arrivati a queste formulazioni.

L'accesso ai servizi in rete è trattato per la prima volta, anche se marginalmente, nel Testo Unico sulla documentazione amministrativa (DPR445/2000). Infatti, al comma 4 dell'articolo 36 si legge: "*La carta d'identità elettronica può altresì essere utilizzata per il trasferimento elettronico dei pagamenti tra soggetti privati e pubbliche amministrazioni*", norma che rivela uno straordinario ottimismo nel legislatore, visto che dopo oltre dieci anni nulla del genere risulta ancora possibile. Interessante è anche il comma 6 dello stesso articolo che apre la strada alle soluzioni moderne di erogazione dei servizi in rete: "*Nel rispetto della disciplina generale fissata dai decreti di cui al presente articolo e delle vigenti disposizioni in materia di protezione dei dati personali, le pubbliche amministrazioni, nell'ambito dei rispettivi ordinamenti, possono sperimentare modalità di utilizzazione dei documenti* [ossia la CIE] *di cui al presente articolo per l'erogazione di ulteriori servizi o utilità*".

La CIE è stata introdotta nel nostro ordinamento dalla Legge 127 del 1997, che ne affida la responsabilità al Ministero dell'Interno. Purtroppo, per vari motivi - tuttora non superati - la diffusione della CIE si rilevò estremamente più lenta del previsto: nacque pertanto, su sollecitazione del Ministro per l'Innovazione, la CNS - tecnicamente simile alla CIE, ma senza le funzioni di identificazione anagrafica - come soluzione provvisoria, proprio per consentire l'accesso alle reti in attesa della CIE.

La CNS è stata introdotta dalla Legge 3 del 2003 e disciplinata dal DPR 117 del 2004. In questo DPR era presente una norma, voluta dal Ministero dell'Interno, che stabiliva che chi aveva la CIE non poteva avere la CNS: poiché all'atto pratico questo controllo risultò operativamente quasi impossibile, anche la CNS stentò a decollare.
Come palliativo, fu emanata una nuova norma che consentiva, non oltre una certa data però, l'emissione della CNS senza controllare se il cittadino disponesse già di una CIE.

Tutta questa materia è stata successivamente rielaborata nel CAD che, all'articolo 64 (*Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni*), prendendo evidentemente atto delle scarsa diffusione di entrambe le carte, consente l'accesso alle reti anche con "strumenti diversi". Sulla natura di questi "strumenti diversi" ritorneremo in seguito.

Il testo originale dell'articolo 64, risalente al 2005, è il seguente:

FONDAZIONE SIAV ACADEMY
Via Porciglia, 14 - Padova | tel 049 897 97 97 fax 049 897 88 00 | info@fondazionesiavacademy.it www.fondazionesiavacademy.it

1. *La CIE e la CNS costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'autenticazione informatica.*
2. *Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'autenticazione informatica anche con strumenti diversi dalla CIE e dalla CNS, purché tali strumenti consentano di accertare l'identità del soggetto che richiede l'accesso. L'accesso con CIE e CNS è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.*
3. *Ferma restando la disciplina riguardante le trasmissioni telematiche gestite dal Ministero dell'economia e delle finanze e dalle agenzie fiscali, con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e d'intesa con la Conferenza unificata …. è fissata la data, comunque non successiva al 31 dicembre 2007, a decorrere dalla quale non è più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni, con strumenti diversi dalla CIE e dalla CNS. È prorogato alla medesima data il termine relativo alla procedura di accertamento preventivo del possesso della CIE, di cui all'articolo 8, comma 5, del DPR 117/04, limitatamente alle richieste di emissione di CNS da parte dei cittadini non residenti nei comuni in cui è diffusa la CIE.*

Confrontando questo testo con quello del nuovo CAD, sopra riportato, si possono notare alcune differenze sostanziali.

Il comma 1 di questa "vecchia" versione è uguale a quello della versione vigente, tranne per la dicitura "*autenticazione informatica*" sostituita da "*identificazione informatica*".

La prima parte del comma 2 è sostanzialmente uguale nelle due versione. La seconda parte esiste solo nella "vecchia" ed è stata provvidenzialmente eliminata in quella attuale. Infatti, sembra evidente che ci sia stata in origine un po' di confusione tra due azioni nettamente diverse: l'identificazione del soggetto e l'accesso alle applicazioni. La CIE e la CNS servono a identificare il soggetto, ma non danno automaticamente accesso alle applicazioni, per le quali ogni Amministrazione può richiedere una specifica abilitazione.
Con quelli che il CAD definisce "strumenti diversi", come vedremo in seguito, si ottiene in un solo passaggio l'identificazione dell'utente e il controllo della sua abilitazione. Pertanto, le due azioni (CIE o CNS rispetto agli "strumenti diversi") non sono esattamente equivalenti.

Il comma 3 stabilisce dei termini per la durata del regime misto, di cui al comma 2, e per l'accertamento della pre-esistenza di una CIE. Detti termini si rilevarono ben presto non congrui e furono più volte prorogati, fino ad arrivare alla completa eliminazione del comma 3 nella versione attuale del CAD.

Riassumendo: in base all'articolo 64, attualmente l'accesso in rete è consentito sia con la CIE, sia con la CNS, sia con altri metodi che consentano l'individuazione del soggetto che richiede il servizio. Può darsi che con la progressiva introduzione delle nuove Tessere Regionali Sanitarie, dotate di alcune delle proprietà previste per le CNS, l'accesso alla rete attraverso una carta elettronica possa conquistare una maggiore diffusione, almeno in alcune regioni: nel frattempo però si va affermando sempre di più l'utilizzo dei più volte citati "strumenti diversi".

FONDAZIONE SIAV ACADEMY
Via Porciglia, 14 - Padova | tel 049 897 97 97 fax 049 897 88 00 | info@fondazionesiavacademy.it www.fondazionesiavacademy.it

3. Strumenti di identificazione diversi dalle carte elettroniche

A parte poche righe nel Codice in materia di protezione dei dati personali (nel seguito: Codice della Privacy), non è stato finora pubblicato alcun documento che stabilisca dei criteri, in una visione strategica di Amministrazione digitale, sugli "strumenti diversi" citati nell'articolo 64 del CAD.
A mio parere, è giunto il momento di disciplinare, sia pure entro certi limiti, questi "strumenti diversi". Nel seguito, prima di indicare alcune delle possibili strade, passeremo in rassegna, per sommi capi, allo "stato dell'arte".

Le possibilità offerte dal mercato, innumerevoli, sono tutte basate su più livelli di identificazione.

Il primo livello è, di solito, legato a una "caratteristica" oggettiva dell'utente: può trattarsi di un parametro biometrico (ad esempio, un'impronta digitale) oppure di un codice alfanumerico. Limitiamo l'esame a quest'ultimo caso che, peraltro, nelle applicazioni amministrative è quello di gran lunga più frequente.

Di solito il codice è assegnato dall'Amministrazione, ma, in certi casi, può essere scelto dall'utente. In entrambi i casi, il codice, una volta assegnato, resta immutato senza limiti di tempo. A questo codice è dato il nome di "*codice utente*" o "*codice identificativo*".

Se l'identificazione dell'utente avviene tramite CIE o CNS, il codice è sempre assegnato dall'Amministrazione ed è registrato sulla banda magnetica e/o sul microchip della carta elettronica. L'identificazione avviene in due fasi: nella prima si "striscia" la carta oppure la si "inserisce" nell'apposito lettore.
Nella seconda fase l'utente immette tramite tastiera un proprio codice segreto, presente anche, in modo cifrato, nella carta elettronica. La procedura elettronica di riconoscimento, molto complessa, è basata su tecniche simili a quelle della firma digitale e offre garanzia di massima sicurezza[3]. Dopodiché, l'utente, essendo stato identificato dal sistema, potrebbe essere chiamato a compiere un ulteriore passo per vedere riconosciuta la propria abilitazione ad accedere a una determinata applicazione. In realtà, l'idea originaria, che aveva ispirato la nascita della CNS, presupponeva che l'accesso a tutte le Amministrazioni potesse avvenire con lo stesso codice, il che si è rivelato ben lontano dalla realtà, anche all'interno della stessa comunità locale (Regione, Provincia, Comune, Enti collegati). Per rimediare a questo limite, è stato consentito - almeno su un piano teorico - il possesso di più CNS in carico allo stesso soggetto, ognuna emessa da un'amministrazione diversa.

Nel caso si impieghi una carta , si può osservare dunque che:

- il terminale con il quale si vuole accedere alla rete deve essere dotato di un dispositivo di lettura della carta;
- la procedura con le carte non sempre è sufficiente per accedere alle applicazioni.

Se non si utilizza una carta, l'inserimento del codice avviene manualmente attraverso la tastiera.

La lunghezza del codice è data dal numero di caratteri alfanumerici impiegati. Il codice può essere di lunghezza fissa o variabile. Nel primo caso, una lunghezza adottata di frequente è di 8 caratteri: se questi sono dati dalle 26 lettere dell'alfabeto standard, maiuscole e minuscole, e le 10 cifre, le combinazioni possibili sono $62^8 \approx 200.000$ miliardi. Per accedere a una zona riservata occorre

[3] Questo processo è definito di "strong authentication", cioè di "identificazione forte".

FONDAZIONE SIAV ACADEMY
Via Porciglia, 14 - Padova | tel 049 897 97 97 fax 049 897 88 00 | info@fondazionesiavacademy.it www.fondazionesiavacademy.it

conoscere il codice: chi non lo conosce non può che procedere per tentativi. È evidente che con simili valori la protezione all'accesso è praticamente assicurata, a meno che l'interessato non lo comunichi a persone terze o se lo lasci incautamente copiare. Risulta pertanto inutile adottare codici lunghi, che, tra l'altro, potrebbero portare facilmente a errori nel caso di immissione manuale. Anche per questo motivo a volte si preferisce limitare la variabilità dei caratteri (ad esempio, alcuni *devono* essere solo numerici). Nel caso, ad esempio, di un codice di 6 caratteri di cui 3 numerici e 3 alfabetici di sole maiuscole, le combinazioni possibili sono circa 18 milioni, numero così elevato da scoraggiare qualunque tentativo di accesso non autorizzato.
Una soluzione a volte adottata nell'ambito della pubblica amministrazione consiste nell'adozione del codice fiscale come codice identificativo: si tratta di un codice molto lungo, con il vantaggio però di essere facilmente ricordato o consultabile[4].

Un malintenzionato potrebbe però effettuare questi tentativi non manualmente, ma mediante una procedura automatica governata da un computer, una specie di automa, per il quale ordini di grandezza di quelli sopra indicati potrebbero essere gestibili. Allo scopo di impedire ciò, a volte è introdotto un livello "zero" di identificazione che ha il solo scopo di assicurare il sistema informatico centrale che dall'altra parte della rete c'è una persona reale e non un automa. L'accorgimento si basa sull'invio di un messaggio che richiede una risposta intelligente, che un automa non può dare: tipico è il caso dei codici Captcha[5].

Oltre al primo livello d'identificazione, quello di tipo "oggettivo", e all'eventuale precedente livello "zero", che esclude gli interventi dolosi di tipo automatico, è sempre aggiunto un secondo livello, basato su un codice lasciato di solito alla scelta soggettiva dell'utente. Normalmente si tratta di un codice alfanumerico per il quale possono essere stabilite condizioni analoghe a quelle del primo codice (lunghezza fissa o variabile, limitazioni nella tipologia dei caratteri). A questo codice è dato il nome di "codice personale"[6]. Il codice personale è registrato in forma cifrata all'interno del sistema e non è accessibile se non al gestore del sistema stesso con severi controlli di sicurezza. Su questo specifico argomento il Codice della Privacy, nell'allegato B ("Disciplinare tecnico sulle misure minime di sicurezza"), stabilisce la regola che il codice personale dovrebbe essere composto da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'utente; se assegnato dal sistema deve essere modificato dall'utente al primo utilizzo e, successivamente, almeno ogni sei mesi.

---

[4] Il codice fiscale è riportato anche nella tessera sanitaria, normalmente presente tra i documenti personali che ogni cittadino porta con sé.

[5] L'acronimo CAPTCHA deriva dall'inglese "***C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part*" (Test di Turing pubblico e completamente automatico per distinguere computer e umani). Il principio di funzionamento è il seguente: il sistema centrale genera una breve stringa di caratteri casuali, ad esempio, "ifhkfp", produce un'immagine con questi caratteri sfuocati o disallineati (v. figura) e la invia all'utente, invitandolo a decifrala e

a rispondere inviando la decodifica, cioè la sequenza corretta di caratteri. Se questo accade, significa che chi si trova dall'altra parte della rete è un "umano".
Poiché è stato notato che questo sistema non sarebbe "accessibile" ai sensi della Legge 4/04, in quanto non utilizzabile da un vedente, esiste una versione di Captcha in cui vengono *pronunciate* alcune cifre numeriche con un tono variabile e leggermente alterato, invitando l'ipotetica persona a trascrivere la sequenza stessa.

[6] Sono anche utilizzati altri nomi come, ad esempio, "Codice di sicurezza" oppure "Parola chiave" oppure "Password". Nella terminologia inglese, se questo codice consiste in un numero, si utilizza spesso la sigla PIN, come acronimo di "Personal Identification Number". Questa soluzione, adottata spesso nelle carte di credito, non consente di solito la scelta del PIN da parte dell'utente.

FONDAZIONE SIAV ACADEMY
Via Porciglia, 14 - Padova | tel 049 897 97 97 fax 049 897 88 00 | info@fondazionesiavacademy.it www.fondazionesiavacademy.it

Nel caso di CIE o CNS il codice personale è memorizzato in modo cifrato all'interno della carta: ciò porta necessariamente a importanti varianti nel processo di abilitazione dell'utente.

L'accesso alla rete avviene pertanto attraverso la seguente sequenza:

- Fase 1: l'utente si collega con il sistema in cui si trova l'applicazione che gli interessa.
- Fase 2: l'utente individua l'applicazione e chiede di accedere.
- Fase 3 (facoltativa): il sistema si assicura che l'utente sia un "umano" mediante una procedura di tipo Captcha.
- Fase 4: il sistema richiede il codice identificativo dell'utente e, una volta ricevutolo, controlla che sia tra quelli autorizzati.
- Fase 5: il sistema richiede il codice personale dell'utente e, una volta ricevutolo, controlla che sia quello corrispondente al codice identificativo precedentemente trasmesso.
- Fase 6: l'applicazione si "apre" alle esigenze dell'utente.
- Fase 7 (facoltativa): in alcune applicazioni, se la richiesta dell'utente è particolarmente importante (transazioni con valore economico, abilitazioni, revoche) può essere richiesta una convalida della richiesta attraverso l'immissione in un ulteriore codice ad hoc[7].

Spesso le Fasi 4 e 5 sono congiunte e i controlli della correttezza del codice identificativo e di quello personale vengono fatti in un unico passaggio. Nel caso di utilizzo di CIE o CNS le Fasi 4 e 5 seguono altri protocolli.

4. Proposta di criteri da adottare nell'ambito della pubblica amministrazione

Non c'è procedura di accesso uguale in due amministrazioni diverse: ciò costringe l'utente a dover ricordare altrettante coppie di codici diversi (codice utente e relativo codice personale), a scapito della sicurezza e a favore di errori. Nella prospettiva di avere in futuro un sistema omogeneo di identificazione rete per l'intero sistema amministrativo nazionale, a mio parere, è giunto il momento di cominciare a predisporre dei criteri per dettare poi delle Linee guida, come è stato fatto in passato per altri temi di rilevanza operativa (protocollo, rilevazione della customer satisfaction, siti web, contratti ICT).

Le modalità potrebbero passare per un tavolo tecnico, formati da esperti della materia, con il compito di:

- realizzare un inventario delle soluzioni esistenti;
- individuarne pregi e difetti;
- segnalare le realizzazioni più valide;
- raccomandare i criteri da adottare per le soluzioni future.

Al solo scopo di attivare una discussione costruttiva, elenco alcune di quelle che potrebbero essere le raccomandazioni proposte da questo tavolo tecnico:

[7] Le varie soluzioni tecniche hanno lo scopo di assicurare il complesso informatico centrale che la persona che si trova dall'altra parte della rete è veramente quella che dice di essere. Una soluzione consiste nel consegnare al cliente al momento della sua registrazione una tabella di codici solo a lui riservati: volendo fare una verifica gli si chiede di inserire uno di questi codici ("inserire il codice corrispondente alla casella xx della tabella in suo possesso" dove la coordinata xx viene attribuita casualmente per ogni transazione). Un altro sistema consiste nel richiedere all'utente di inserire tempestivamente un codice che gli arriverà tempestivamente come messaggio sul proprio telefono cellulare.

FONDAZIONE SIAV ACADEMY
Via Porciglia, 14 - Padova | tel 049 897 97 97 fax 049 897 88 00 | info@fondazionesiavacademy.it www.fondazionesiavacademy.it

- non utilizzare la codifica Captcha (tecnicismo eccessivo);
- come codice utente utilizzare come standard il codice fiscale; nel caso di codici diversi, limitarsi a 8 cifre nel caso di codici solo numerici e a 5 caratteri nel caso di codici alfanumerici, evitando in questo caso i caratteri O e I e le cifre 1 e 0;
- consentire che detto codice possa essere "ricordato" nel personal computer e possa essere richiamato automaticamente (ciò elimina la possibilità di sbagliare nell'inserire i caratteri);
- come codice personale lasciare libera la scelta dell'utente, nell'ambito di una lunghezza massima di 8 caratteri;
- non pretendere una periodica modifica del codice personale (che è invece espressamente richiesta dal Codice della Privacy).

Mi sembra anche opportuno raccomandare che, come azione a lungo termine, venga sviluppata un'interfaccia di accesso da proporre identicamente a tutte le amministrazioni: ciò, tra l'altro, potrebbe aprire la strada alla realizzazione, da molti sostenuta, dell'accesso da parte del cittadino a qualunque amministrazione collegata alla stessa rete mediante un'unica procedura (il cosiddetto "SSO - Single Sign-On"), possibile solo se tutte le amministrazioni hanno la stessa modalità di accesso. Questa possibilità sarebbe particolarmente valida nell'ambito dello stesso territorio (amministrazioni regionali, provinciali, comunali, ASL, scuole, ecc.).

5. Il progetto FEDERA

Nella regione Emilia Romagna è stato realizzato un portale per l'identificazione in rete a disposizione di tutte le amministrazioni comunali e altri enti interessati – denominato FEDERA – in cui il cittadino si registra ottenendo "user" e "password" che saranno poi validi per tutti i servizi erogati da tutte le amministrazioni aderenti al progetto.

Al momento l'identificazione prevede tre livelli di "affidabilità": basso, medio e alto: il primo si ottiene con una semplice registrazione on-line, per il secondo bisogna indicare il numero di cellulare, per il terzo invece bisogna completare la registrazione con un riconoscimento a norma della 445/00 che comporta la consegna del proprio documento di identità o direttamente presso uno sportello comunale oppure inviando un fax.
Nell'ambito del livello di affidabilità alto, inoltre, il portale prevede tre livelli di "password policy", con la password liberamente impostabile dall'utente:

- livello 1: accesso a dati generici - la password non è soggetta a scadenza;
- livello 2: accesso a dati personali – la scadenza è a 6 mesi;
- livello 3: accesso a dati sensibili – la scadenza è a 3 mesi.

Al momento sono in fase di attivazione e rilascio, in particolare, alcuni grandi gruppi di servizi on-line, che riguardano lo Sportello Unico per le Attività Produttive e i servizi Demografici.

Visto che l'accesso a questi servizi è finalizzata alla presentazione di istanze, si applica l'art. 64 del CAD, secondo cui, come già visto, "Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio."; quindi per presentare istanze alla pubblica amministrazione è sufficienti disporre di user e password. In tutti questi casi l'utente però deve essere autenticato al livello più alto.

FONDAZIONE SIAV ACADEMY
Via Porciglia, 14 - Padova | tel 049 897 97 97 fax 049 897 88 00 | info@fondazionesiavacademy.it www.fondazionesiavacademy.it