



ACCESSO AI SERVIZI TELEMATICI REQUISITI DEL TOKEN DI AUTENTICAZIONE

PREMESSA E SCOPO DEL DOCUMENTO

Al fine di garantire la sicurezza e l'autenticazione forte ai servizi telematici (PolisWeb e processo civile telematico), le regole tecniche in vigore richiedono l'uso di smart card che garantiscano il necessario livello di sicurezza.

Il D.M. 17/7/2008 prevede infatti:

- Art. 30, comma 1: *“L'autenticazione dei soggetti abilitati esterni avviene secondo le specifiche previste dalla carta nazionale dei servizi”*
- Art. 36, comma 2: *“La postazione di lavoro dei soggetti abilitati esterni è dotata dell'hardware e del software necessario alla gestione della firma digitale su smartcard, e all'autenticazione nei confronti del punto di accesso, secondo le caratteristiche tecniche della carta nazionale dei servizi”*
- Art. 62, comma 3: *“L'autenticazione dei soggetti abilitati esterni avviene secondo le specifiche della Carta Nazionale dei Servizi; possono essere utilizzati i dispositivi crittografici non conformi alla Carta Nazionale dei Servizi, purché emessi entro il 31 dicembre 2008”*

Per garantire la massima diffusione dei servizi telematici sono state adottate come specifiche di riferimento quelle della *Carta Nazionale dei Servizi* e della *Carta d'Identità Elettronica* in modo tale che qualsiasi utente in possesso di una CIE o CNS abbia la possibilità di iscriversi e accedere ai servizi stessi.

Poiché CIE e CNS non hanno ancora raggiunto la diffusione auspicata, sono stati da più parti richiesti all'Amministrazione maggiori chiarimenti sulle specifiche e sui requisiti che i token di autenticazione debbano soddisfare affinché ne sia ammesso l'uso per l'accesso ai punti di accesso (PdA).

In particolare ci si chiede se siano ammissibili solo CNS vere e proprie (e quindi del tutto aderenti alle linee guida CNIPA per l'emissione e utilizzo della CNS) oppure se siano sufficienti delle carte *“CNS-like”* che rispettino determinati requisiti.

In questo documento vengono forniti i necessari chiarimenti tecnici e vengono in particolare definiti i requisiti minimi che un token di autenticazione deve rispettare perché possa essere utilizzato nell'ambito dei servizi telematici forniti da questo Ministero.

È opportuno precisare che ci si riferisce ai requisiti del token di autenticazione e non del token di firma: per questi ultimi si fa riferimento alla normativa in vigore per la firma digitale. Questo non toglie che alcuni dei requisiti del token di autenticazione possano derivare dalla normativa in vigore per la firma digitale.

REQUISITI DEL TOKEN DI AUTENTICAZIONE

Affinché un token crittografico (smart card, chiavetta USB o altro dispositivo sicuro) possa essere utilizzato per l'autenticazione ad un PdA è necessario che vengano garantiti i seguenti tre requisiti principali:



1. Il certificato di autenticazione deve essere rilasciato da una Certification Authority (CA) accreditata che si fa garante dell'identità del soggetto; al riguardo si faccia riferimento alla lista delle CA accreditate dal CNIPA. Questo requisito è importante al fine di consentire la validità del certificato sulla base di una catena di "trust" definita e non-ambigua.
2. Il certificato di autenticazione deve rispettare il profilo del certificato previsto per le CNS; al riguardo si faccia riferimento all'Appendice 1 del documento rilasciato dal CNIPA: "*Linee guida per l'emissione e l'utilizzo della Carta Nazionale dei Servizi*". L'estensione Certificate Policy (2.5.29.32) può essere valorizzata con uno degli Object Identifier (OID) previsti per la CNS in base alle norme CNIPA (ad esempio 1.3.76.16.2.1) o con altro OID definito dalla CA.
3. Il token deve rispettare i requisiti tecnici minimali che garantiscano la sicurezza e l'interoperabilità per quanto attiene l'accesso ai servizi offerti dai PdA, descritti nel seguito.

REQUISITI DI SICUREZZA

Dal punto di vista della sicurezza, i dispositivi ammessi come token di autenticazione sono gli stessi ammessi per la firma digitale e quindi smart card e token USB (si veda in proposito d.lg. 23 gennaio 2002, art. 10, comma 1 e in riferimento allo schema nazionale adottato con DPCM del 30 ottobre 2003: questo si concretizza nel requisito che i dispositivi sicuri devono essere certificati Common Criteria EAL4 con traguardo di sicurezza o profilo di protezione conforme alle disposizioni comunitarie).

REQUISITI DI INTEROPERABILITÀ

A seconda del tipo di sistema operativo utilizzato dal token, a seconda del costruttore e a seconda del chipset utilizzato l'interfaccia di dialogo e il file system possono variare significativamente da token a token.

I requisiti minimi di interoperabilità affinché un token sia ammissibile per l'autenticazione ai servizi telematici sono:

- a) disponibilità di entrambe le interfacce PKCS#11¹ e CSP². In particolare entrambe le interfacce devono consentire l'accesso alla procedura di autenticazione forte mediante digitazione del PIN da parte dell'utente.
- b) strutturazione del file system come da specifiche CNS.

¹ PKCS#11 definisce un'interfaccia di programmazione che consente di accedere alle funzionalità crittografiche del token: tramite l'opportuna sequenza di chiamate al token per mezzo dell'interfaccia PKCS#11 è possibile implementare la procedura di autenticazione.

² Nel mondo Microsoft, e quindi nel mondo dei PC Windows, lo standard di fatto è il così detto Crypto Service Provider (CSP) che, dal punto di vista logico è del tutto assimilabile al PKCS#11.