ALLEGATO *B*

Regole tecniche e di sicurezza relative alle tessere di riconoscimento rilasciate dalle amministrazioni dello Stato

Indice

1. Introduzione

1.1 Scopo del Documento

Il presente documento definisce i requisiti e le caratteristiche tecniche delle tessere di riconoscimento rilasciate dalle amministrazioni dello Stato ai sensi del decreto del Presidente della Repubblica 28 luglio 1967, n.851 realizzate con modalità elettroniche.
Definisce inoltre gli attori e le interazioni necessarie per l'emissione di tali documenti.

2. Definizioni

Tessera di riconoscimento – Modello AT elettronico.

Il documento di riconoscimento rilasciato dalle amministrazioni dello Stato ai sensi del decreto del Presidente della Repubblica 28 luglio 1967, n.851 e realizzate con modalità elettroniche.
Utilizza una carta a microprocessore (smart card) in grado di registrare in modo protetto le informazioni necessarie per l'autenticazione in rete. All'esterno contiene gli elementi necessari per l'identificazione a vista.
Acronimo **ATe**

Carta d'Identità Elettronica

Documento di riconoscimento personale a fini di Polizia rilasciato dal comune su supporto informatico
Utilizza una carta a microprocessore (smart card) in grado di registrare in modo protetto le informazioni necessarie per l'autenticazione in rete. All'esterno contiene gli elementi necessari per l'identificazione a vista.
Acronimo **CIE**

Carta Nazionale dei Servizi

Documento informatico, rilasciato da una Pubblica Amministrazione, con la finalità di identificare in rete il titolare della carta
Utilizza una carta a microprocessore (smart card) in grado di registrare in modo protetto le informazioni necessarie per l'autenticazione in rete.
Acronimo **CNS**

DigitPA (già Centro Nazionale per l'informatica nella pubblica amministrazione)

Approva il documento progettuale elaborato dall'Amministrazione emittente di concerto con quanto stabilito nell'articolo 4 del decreto.

E' l'amministrazione che garantisce tramite un parere obbligatorio la conformità del documento progettuale a requisiti di congruità tecnico-economica, garantendo anche la conformità dello stesso alla normativa vigente in materia di CNS e firma digitale

Certificato di autenticazione

L'attestato elettronico che garantisce l'autenticità del circuito che ha emesso il modello ATe.
Certificato X509 v3 della carta, rilasciato da un certificatore accreditato ai sensi dell'articolo 29 del Decreto Legislativo 7 marzo 2005, n. 82.
Acronimo **Cda**

Certificato di firma

L'attestato elettronico che collega i dati utilizzati per verificare la firma elettronica al titolare e conferma l'identità del titolare stesso
Si tratta di un certificato X509 v3, emesso da un certificatore accreditato ai sensi dell'articolo 5 del Decreto Legislativo n.10 del 23 gennaio 2002, che può essere utilizzato per la verifica delle firme digitali emesse in aderenza alla vigente normativa.
Acronimo **Cdf**

Certificatore	*Ente che presta servizi di certificazione delle informazioni necessarie per l'autenticazione o per la verifica delle firme elettroniche* Si tratta di enti abilitati a prestare servizi di certificazione in base all'articolo 29 del Decreto Legislativo 7 marzo 2005, n. 82. Acronimo **Ce**
Ente emettitore	*Ente responsabile della formazione e del rilascio del Modello AT elettronico.* È la Pubblica Amministrazione che rilascia il Modello AT elettronico ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita dell'ATe. Provvede alla realizzazione del progetto di emissione e gestione del ciclo di vita dell'ATe di concerto con IPZS. Acronimo **EE**
Ministero dell'Economia e delle Finanze	*Ente responsabile dei servizi di vigilanza e controllo sulla produzione delle carte valori, degli stampati a rigoroso rendiconto e delle pubblicazioni ufficiali (DM 5 marzo 2004).*
PIN_utente	*PIN utilizzato per l'accesso alle funzioni dell'ATe* È il PIN, necessario al titolare per attivare le operazioni di autenticazione in rete, che viene consegnato dall'ente emettitore con meccanismi di sicurezza.
Istituto Poligrafico e Zecca dello Stato	*Azienda che esegue le fasi di produzione dell'ATe con metodi di sicurezza e qualità produttiva tipici della carta valori.* È l'azienda che provvede alla fornitura ed all'inizializzazione delle carte a microprocessore, predispone opportunamente gli spazi dedicati alla firma digitale, agli elementi biometrici. Provvede alla personalizzazione del documento. Partecipa alla redazione del progetto di emissione e gestione del ciclo di vita dell'ATe insieme all'Ente Emettitore. Può supportare su esplicita richiesta l'Ente Emettitore nell'attuazione di progetti di gestione e diffusione dell'ATe. Acronimo **IPZS**

3. Le caratteristiche della carta

3.1 Utilizzo dell'ATe

Il documento di riconoscimento qui definito, e denominato "Modello ATe", viene utilizzato per:

- Identificazione a vista del titolare
- Autenticazione in rete
- Firma digitale
- Altre funzionalità definite dall'amministrazione emittente

Il modello ATe consente l'identificazione a vista del titolare. Per questo scopo, la carta viene dotata di elementi di sicurezza contro la duplicazione e la contraffazione. Per poter agevolare l'utilizzo come documento valido per l'espatrio, il modello ATe viene dotato di una zona leggibile in maniera automatica (MRZ – Machine Readable Zone). Le caratteristiche fisiche della carta vengono definite nel paragrafo 3.2.

Il modello AT elettronico (ATe) in base a quanto stabilito dall'art. 66, comma 8 del Decreto Legislativo 7 marzo 2005, n. 82 contiene le funzionalità della Carta Nazionale dei Servizi per consentire l'accesso per via telematica ai servizi erogati in rete dalle pubbliche amministrazioni. Le caratteristiche del chip a contatti e dei dati per le funzionalità di accesso in rete sono descritte nel paragrafo 3.3.

L'ATe è predisposto per ospitare il servizio di firma digitale, fornendo al titolare la possibilità di sottoscrivere documenti elettronici secondo la normativa vigente in materia. Il servizio di firma digitale viene gestito come indicato nel paragrafo 6.1.

Per particolari esigenze di sicurezza fisica o logica dell'amministrazione emittente possono essere utilizzate informazioni biometriche come le impronte digitali o il volto del titolare dell'ATe. L'utilizzo di tali informazioni avviene nel rispetto della normativa in materia di protezione dei dati personali, e come descritto al paragrafo 6.3.

L'ATe è opzionalmente dotata di funzionalità contactless, ad esempio per applicazioni di controllo accessi, come descritto al paragrafo 3.3.3.

3.2 Caratteristiche fisiche della carta

L'ATe è una smart card con un supporto fisico costituito da una carta plastica conforme alle norme ISO/IEC 7816-1, 7816-2 e ISO/ID-001 ed è integrato da elementi elettronici, come specificato appresso.

Il supporto fisico è stampato con le tecniche tipiche della produzione di carte valori ed è dotato degli elementi fisici di sicurezza atti a consentire il controllo dell'autenticità del documento visivamente e mediante strumenti portatili e di laboratorio.

Devono essere fatti salvi i vincoli imposti dagli standard internazionali sulle smart card, con particolare riferimento alle norme che regolamentano i Documenti di Identità International Standards Organization (ISO)/IEC 7816-1-2.

Le dimensioni nominali dovranno essere di 53,98 x 85,6 mm come specificato nella norma ISO/IEC 7810: 2003 per la carta di tipo ID-1. La tolleranza, nelle dimensioni, è quella definita dalla norma stessa.

Lo spessore dell'ATe, compresi i film di protezione, dovrà essere conforme alla norma ISO/IEC 7810: 2003.

L'ATe sarà costituito da materiali plastici compatibili con gli strumenti tecnologici in essa contenuti, nonché con i sistemi di personalizzazione utilizzati per la sua compilazione.

L'ATe, per un uso normale nel periodo di validità, dovrà rispondere alle specifiche definite:

- nella norma ISO/IEC 7810: 2003 relativamente a: deformazioni, tossicità, resistenza ad agenti chimici, stabilità dimensionale ed inarcamento con temperatura e umidità, inarcamento con l'uso, infiammabilità e durata.

- nella norma ISO/IEC 11693 per la contaminazione, per la trasmissione della luce attraverso lo spessore della carta e per la resistenza agli agenti atmosferici ed ai test di compatibilità con l'ambiente.

Per quanto attiene alla presenza del microchip la CIE, per un uso normale durante il periodo di validità, deve rispondere alle specifiche definite nella norma ISO/IEC 7816-1.

3.2.1 Sicurezza del supporto fisico

Il documento deve garantire la sicurezza dell'identificazione a vista, sia attraverso il semplice esame visivo, sia mediante strumentazione specifica. Per questo motivo, viene dotato di specifici elementi di sicurezza, classificati in quattro livelli:

Livello 1 (L1): sono tutti gli elementi di sicurezza visibili ad occhio nudo, esaminabili in pochi secondi da parte di personale non specializzato: sfondo di sicurezza multicolore, microscrittura, elementi OVD (Optical Variable Device), inchiostri otticamente variabili (OVI – Optical Variable Ink);

Livello 2 (L2): sono gli elementi di sicurezza verificabili con strumenti portatili utilizzabili da personale non specializzato: inchiostri fluorescenti all'ultravioletto;

Livello 3 (L3): sono gli elementi di sicurezza per la cui verifica sono necessari strumenti e personale specializzati

Livello 4 (L4): elementi speciali di sicurezza per la tracciatura

3.2.2 Numerazione di serie

La numerazione del documento è realizzata con sistema ad incisione laser sul fronte del documento.

3.2.3 Layout della carta

Il layout dell'ATe è unico per tutte le Amministrazioni,come specificato nell'Allegato A

3.2.4 Machine Readable Zone (MRZ)

Sul retro del documento è presente un testo formattato per la lettura ottica (OCR), secondo quanto prescritto dallo standard ICAO 9303.

3.3 Utilizzo della carta come strumento di accesso ai servizi

Coerentemente con quanto stabilito dall'art. 66, comma 8 del Decreto Legislativo 7 marzo 2005, n. 82, la carta contiene le funzionalità della carta nazionale dei servizi per consentire l'accesso per via telematica ai servizi erogati in rete dalle pubbliche amministrazioni.

La carta è quindi dotata di un chip a contatto che espone le interfacce specificate dalle norme che regolano la Carta Nazionale dei Servizi.

3.3.1 Microprocessore

E' richiesta una memoria EEPROM dalla capacità (intesa come spazio disponibile per i dati) non inferiore a 32 Kbyte.

Il microprocessore deve essere conforme agli standard della serie ISO/IEC 7816 di pertinenza e comunque deve rispettare le specifiche del sistema operativo (APDU) e della struttura interna dei dati del microprocessore (file system) pubblicate sul sito di DigitPA.

In particolare il microprocessore deve avere almeno le seguenti caratteristiche generali:

- capacità crittografiche RSA ad almeno 1024 bit e comunque non inferiori a quelle previste per la CNS;
- capacità crittografiche simmetriche 3DES a 128 bit;
- possibilità di generare chiavi RSA all'interno del microprocessore;
- possibilità di caricare chiavi private RSA mediante procedure di sicurezza adeguate;
- possibilità di uso del Secure Messaging in conformità allo standard ISO/IEC 7816;
- conformità alla normativa di riferimento per la firma digitale;
- capacità di ritenzione dei dati di almeno 10 anni;
- numero di cicli di scrittura maggiore di 100.000.

3.3.2 Struttura delle informazioni nel microprocessore

Il file system è conforme con quanto indicato dalle stesse norme. In particolare, il file elementare dei dati personali è codificato secondo le modalità previste per la Carta d'Identità Elettronica con le definizioni specifiche seguenti:

Dato	**MOV**	**Dimensione Max**	**Descrizione**
Emettitore	M	4	Indicazione dell'emettitore
Data di emissione del documento	M	8	Formato GGMMAAAA
Data di scadenza del documento	M	8	Formato GGMMAAAA
Cognome	M	80	
Nome	M	86	
Data di Nascita	M	8	Formato GGMMAAAA
Sesso	M	1	'M' maschile, 'F' femminile
Statura (cm)	O	3	Presente per compatibilità CIE
Codice fiscale	M	16	
Cittadinanza (codice)	O	3	Presente per compatibilità CIE
Comune di Nascita	M	4	
Stato estero di Nascita	O	4	Presente per compatibilità CIE
Estremi atto di nascita	O	10	Assente
Comune di residenza al momento dell'emissione	M	6	
Indirizzo di residenza	O	80	
Eventuale annotazione in caso di non validità del documento per l'espatrio	M	0	Assente

Tabella 2- Definizione Dati Personali

I campi obbligatori (M), opzionali (O) e vuoti (V) sono indicati nella colonna MOV.

3.3.3 Utilizzo di funzionalità contactless

Opzionalmente, e senza alterare le funzionalità di autenticazione in rete e di firma digitale, la carta può gestire la trasmissione dati a radiofrequenza (contactless), per applicazioni specifiche all'amministrazione (es. controllo accessi).

Gli standard di riferimento sono l'ISO 14443 per le proximity card e l'ISO 15693 per le vicinity card.

La definizione del dettaglio dei protocolli applicativi viene lasciata al singolo progetto.

4. Il circuito di emissione

Possono emettere l'ATe le pubbliche amministrazioni di cui al decreto del Presidente della Repubblica 28 luglio 1967, n. 851.

La pubblica amministrazione che intende emettere l'ATe è responsabile:

- della correttezza dei dati identificativi memorizzati nella carta e nel certificato di autenticazione,
- della correttezza del codice fiscale memorizzato nella carta e riportato nel certificato di autenticazione,
- della sicurezza delle fasi di produzione, inizializzazione, distribuzione ed aggiornamento/ritiro della carta.

Ai sensi dell'articolo 8 del decreto del Presidente della Repubblica 2 marzo 2004, n. 117, recante regolamento concernente la diffusione della carta nazionale dei servizi, è cura dell'Ente emettitore inviare i dati identificativi al Ministero dell'interno, CNSD per l'eventuale aggiornamento dell'INA, con modalità e formati definiti da apposita circolare del Ministero dell'interno.

4.1 Modello del circuito di emissione

Di seguito sono illustrate le attività funzionali da realizzare per emettere le carte ATe. Tali attività non sono descritte in modo temporale e l'Ente emettitore potrà definire quelle modifiche che ne rendono più semplice l'attuazione. In ogni caso rimangono di responsabilità esclusiva dell'Ente emettitore il riconoscimento e il rilascio dell'ATe.

Fase	Attività	Descrizione
1	Individuazione servizi ed infrastruttura	L'ente emettitore analizza ed individua i servizi da rendere disponibili in rete mediante ATe. Attiva IPZS e un certificatore accreditato se intende utilizzare la firma digitale.
2	Avviamento del processo di emissione	L'ente emettitore concorda con IPZS l'avviamento del processo di emissione.
3	Produzione dell'ATe	L'IPZS esegue le fasi di produzione ed inizializzazione seguendo le specifiche definite nel presente documento e nel sito del Centro nazionale per l'informatica nella pubblica amministrazione Le carte sono consegnate in modalità protetta all'ente emettitore.
4	Registrazione degli utenti	L'ente emettitore identifica, attraverso un documento di riconoscimento, il cittadino ed attiva la procedura di emissione ATe. o in maniera autonoma o rivolgendosi a strutture delegate.
5	Verifica dati identificativi	L'ente emettitore effettua la verifica della correttezza dei dati identificativi collegandosi, direttamente o tramite struttura delegata, con il CNSD del Ministero dell'Interno.
6	Generazione del certificato ATe	Un certificatore accreditato, scelto dall'Ente emettitore rilascia il certificato che attesta l'autenticità delle informazioni associate ai dati di autenticazione. L'eventuale colloquio tra l'ente emettitore ed il certificatore avviene in modalità protetta.
7	Personalizzazione dell'ATe	L'ente emettitore, mediante IPZS, esegue la personalizzazione dell'ATe, inserendo i dati personali del cittadino ed il certificato di autenticazione, stampa gli stessi sulla carta; produce il PIN ed il PUK necessari all'utilizzo dell'ATe in rete e della eventuale firma digitale. Ove previsto aggiunge i servizi opzionali.
8	Consegna dell'ATe	L'ente emettitore, tramite strutture proprie o esterne, consegna l'ATe al titolare. L'ente emettitore illustra al titolare le modalità di uso della carta e le procedure che dovranno essere utilizzate in caso di problemi. Fornisce al titolare un numero telefonico per l'assistenza (call center) ed il numero telefonico per la sospensione o revoca.
9	Gestione dell'ATe	L'ente emettitore provvede alla gestione dell'ATe emesse predisponendo le strutture per l'assistenza agli utenti, la gestione dei malfunzionamenti e l'eventuale sostituzione o rinnovo delle carte in scadenza. Per le funzioni di gestione delle carte l'ente può avvalersi di strutture delegate. L'eventuale software consegnato al cittadino deve garantire l'interoperabilità con la CIE.
10	Ritiro dell'ATe	L'ATe può essere ritirato per rinnovo a seguito di problemi di funzionamento della smart card o dopo aver raggiunto il naturale termine di scadenza. L'ente emettitore è responsabile del suo ritiro prima dell'emissione di una nuova carta o del suo rinnovo

Tabella 3 – Funzioni relative all'emissione e gestione dell'ATe

Nei successivi paragrafi si descrivono le attività di maggiore complessità.

4.1.1 Attività di produzione

Il processo di produzione prevede la produzione della carta plastica e la sua inizializzazione tramite la generazione del file system e la creazione delle condizioni per controllare l'accesso ai file.

L'operazione di Inizializzazione è finalizzata a produrre in maniera sicura delle carte che siano pronte ad essere personalizzate, ossia risultino in uno stato definito "Attivate".

4.1.2 Attività di registrazione

Consiste nell'identificazione del titolare attraverso un documento di riconoscimento valido.

Le modalità applicate per questa attività sono sotto la responsabilità dell'ente emettitore.

4.1.3 Verifica dei dati identificativi ed allineamento anagrafi

Prima di personalizzare l'ATe l'ente emettitore verifica i dati identificativi, direttamente o tramite struttura delegata, mediante il sistema informativo del Ministero dell'Interno – Centro Nazionale dei Servizi Demografici.

4.1.4 Generazione del certificato di autenticazione

Le informazioni anagrafiche ottenute in fase di registrazione congiuntamente con la chiave pubblica generata in fase di personalizzazione, sono utilizzate dal Certificatore per generare il certificato di autenticazione, secondo le specifiche definite dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione e pubblicate sul sito dello stesso Centro.

4.1.5 Attività di personalizzazione

La personalizzazione delle carte è condotta dall'ente emettitore anche per mezzo di strutture esterne.
Nel corso dell'attività di personalizzazione, vengono inserite le informazioni utente necessarie per l'identificazione in rete e per gli altri servizi previsti.
Viene inoltre generato il PIN utente ed il PUK, utilizzabile per lo sbocco della carta nel caso di iterata digitazione errata del PIN. Il PIN ed il codice PUK sono stampati in buste retinate atte a garantire la riservatezza di tali informazioni.

4.1.6 Attività di rilascio

In questa fase l'ATe viene consegnato al titolare dopo averne verificata l'identità, unitamente alla busta contenente il PIN ed il codice PUK. L'ente emettitore deve illustrare al titolare le modalità di uso della carta e le procedure che dovranno essere utilizzate in caso di anomalie o disservizi. Deve fornire al titolare un numero telefonico per l'assistenza ed il numero telefonico per la sospensione o revoca.

4.1.7 Interdizione della carta

Le procedure da seguire per l'interdizione dell'ATe sono contenute nel manuale operativo pubblicato dall'amministrazione emittente.

Le liste di revoca dei certificati di autenticazione sono gestite dal corrispondente certificatore accreditato secondo le modalità utilizzate per la firma digitale.

4.2 Modalità di connessione al Centro Nazionale dei Servizi Demografici

L'interconnessione al CNSD è realizzata attraverso la porta applicativa di accesso ai servizi del CNSD.
L'interconnessione al CNSD avverrà sul backbone INA/SAIA attraverso la porta applicativa di accesso del CNSD secondo le seguenti modalità:

- tramite il Sistema Pubblico di Connettività (SPC);
- tramite altre reti a cui sono connesse le amministrazioni locali;
- tramite rete Internet.

Le modalità di interconnessione al CNSD, al fine della verifica dei dati identificativi dovranno essere conformi a quanto definito dal decreto 8 novembre 2007 e successive modifiche recante "Regole tecniche della carta d'identità elettronica".

4.3 La gestione dell'ATe

L'ente emettitore è responsabile della gestione del circuito di emissione che a lui fa capo. L'ente dovrà definire le procedure di gestione, personalizzazione e rilascio degli ATe e descriverle in un apposito manuale operativo reso disponibile ai titolari.

L'ente emettitore predispone altresì, eventualmente avvalendosi di terzi, le strutture per l'assistenza agli utenti, la gestione dei malfunzionamenti e l'eventuale sostituzione o rinnovo delle carte in scadenza.

L'ente emettitore che emette gli ATe è responsabile di definire un servizio di "contact center" per l'assistenza, nonché la revoca o sospensione degli ATe.

L'ente emettitore può procedere al rinnovo dell'ATe a seguito di problemi di funzionamento della smart card, di furto, smarrimento o per il fatto che questa ha raggiunto il naturale termine di scadenza, in tal caso è responsabile della revoca automatica dell'ATe prima dell'emissione di una nuova carta o del suo rinnovo.

L'ente emettitore ha la facoltà di procedere di propria iniziativa alla revoca dell'ATe; in tal caso ha l'obbligo di avvertire il titolare esplicitando le motivazioni della revoca.

Gli enti che erogano servizi accessibili tramite ATe, dovranno consentire l'utilizzo degli stessi mediante CIE, secondo quanto previsto dal decreto del Ministro dell'Interno del 8 novembre 2007, e successive modifiche, recante "Regole tecniche della carta d'identità elettronica".

4.4 Requisiti per la partecipazione al circuito di emissione dell'ATe

4.4.1 Produttori

Ai fini della sicurezza dell'intero circuito di emissione, i fornitori di smart card che intendono offrire i propri servizi agli enti emettitori per le fasi di inizializzazione delle smart card, devono rispettare le specifiche previste nel presente documento.
In particolare, i fornitori sono vincolati al rispetto delle specifiche del sistema operativo (APDU) e della struttura interna della carta (file system) pubblicate sul sito del Centro Nazionale per l'informatica nella pubblica amministrazione e sul sito della Carta d'Identità Elettronica.

4.4.2 Ente emettitore

Gli enti emettitori devono rispettare caratteristiche di qualità e di affidabilità tali da garantire la sicurezza dell'intero circuito.
In particolare devono:

- Definire le procedure del sistema di emissione e gestione dell'ATe in modo conforme alle specifiche di qualità previste dalla norma ISO 9000/2000 e successive modifiche;
- realizzare l'analisi del rischio e delle misure di sicurezza nella gestione dell'intero ciclo di vita dell'ATe;
- definire modalità di interazione con i produttori ed i certificatori che forniscano adeguate garanzie di affidabilità e sicurezza;
- predisporre un manuale operativo che evidenzi le procedure seguite per la gestione di tutte le fasi del processo di emissione e di gestione dell'ATe;
- predisporre un manuale utente che illustri le modalità d'uso dell'ATe, i modi per usufruire dei servizi in rete e le procedure da seguire in caso di smarrimento, furto o timore di compromissione della carta;
- organizzarsi in modo da costituire il riferimento per ogni problema di funzionalità, disponibilità o sicurezza del circuito di emissione, rendendo disponibile un recapito telefonico costantemente attivo;
- predisporre il piano della sicurezza relativo all'intero circuito di emissione.

L'ente emettitore mantiene la responsabilità della sicurezza del circuito di emissione e del rispetto delle normative vigenti in merito alla tutela dei dati personali.

4.4.3 Certificatori

Possono operare come emettitori dei certificati di autenticazione dell'ATe esclusivamente i certificatori accreditati di cui all'articolo 29 del Decreto Legislativo 7 marzo 2005 , n. 82.
Tali soggetti devono operare in aderenza alle vigenti norme che regolano l'emissione e la gestione dei certificati qualificati.
I certificatori che rilasciano certificati di autenticazione per l'ATe sono iscritti in un elenco consultabile in via telematica, tenuto dal Centro nazionale per l'informatica nella pubblica amministrazione. Questo elenco è lo stesso che contiene le informazioni inerenti i certificatori che rilasciano certificati di autenticazione per l'ATe.

4.4.4 Struttura del certificato di autenticazione e interoperabilità con la CIE

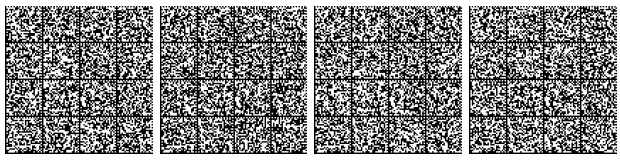
La struttura del certificato di autenticazione, l'interoperabilità con la CIE e le relative modalità di aggiornamento sono pubblicate in un'apposita sezione del sito web di DigitPA.

5. Misure di sicurezza

Poiché l'ATe è da considerare carta valori il supporto informatico deve essere prodotto dall'Istituto Poligrafico e Zecca dello Stato (IPZS).

Tutte le misure di sicurezza adottate da IPZS, nel caso che esso sia su delega dell'amministrazione l'ente emettitore, sono concordate con l'amministrazione stessa. In particolare devono essere oggetto di specifico accordo le modalità di:

- trasmissione delle anagrafiche dei titolari;
- trattamento dei dati personali dei titolari;
- caricamento delle informazioni inerenti la firma digitale;
- caricamento delle informazioni di tipo biometrico;
- caricamento delle informazioni per eventuali servizi installati nell'ATe.



6. Servizi erogabili

6.1 La firma digitale

L'ATe può essere predisposto per le funzionalità di firma digitale. L'ente responsabile della certificazione delle chiavi di firma è stabilito dall'ente emettitore nell'ambito del circuito di emissione;

L'ente emettitore o di struttura da questi delegata ha il compito di predisporre una procedura atta a far sì che il titolare dell'ATe possa disporre della firma digitale al momento del rilascio della carta. La firma può essere attivata in un secondo momento.

La predisposizione della smart card per la firma digitale può avvenire utilizzando altre procedure che garantiscano l'aggiornamento del file system in conformità alla certificazione di sicurezza ISO/IEC 15408 (Common Criteria), ITSEC o equivalente della stessa smart card.

6.1.1 I certificati dell'ATe

L'ATe contiene un certificato di autenticazione della carta utilizzato per tutte le funzioni di riconoscimento in rete e che, in combinazione con il PIN utente, permette l'utilizzo dei servizi in rete da parte del titolare. Tra le informazioni, il certificato contiene anche, nel campo common name, il codice fiscale del titolare.
L'ATe, nel caso in cui venisse installato il servizio di firma digitale, contiene almeno un certificato di firma digitale conforme alla normativa vigente in materia.
Ulteriori certificati possono essere aggiunti purché non siano alterate le funzionalità degli altri certificati installati.

6.1.2 Struttura del certificato di autenticazione e interoperabilità con la CIE

La struttura del certificato di autenticazione, l'interoperabilità con la CIE e le relative modalità di aggiornamento sono pubblicate in un'apposita sezione del sito web di DigitPA.

6.2 I dati biometrici

I dati biometrici presenti sull' ATe sono prelevati e memorizzati secondo procedure che garantiscono la protezione dei dati personali. Essi sono inseriti nel file system dell'ATe a discrezione dell'ente emettitore per specifici scopi di sicurezza dell'amministrazione stessa.
In ogni caso è fatto divieto all'ente emettitore di memorizzare in banche dati le informazioni biometriche prelevate ai titolari dell'ATe.

La scelta della rappresentazione informatica dei dati biometrici deve essere conforme al documento "Linee guida per la rappresentazione informatica dei dati biometrici nelle carte elettroniche della pubblica amministrazione" pubblicato in una apposita sezione del sito istituzionale di DigitPA.

10A09545