

**Decreto 3 agosto 2004**  
**“Regole tecniche e di sicurezza relative al permesso ed alla carta di soggiorno.”**

G.U. 6 ottobre 2004, n. 235

IL MINISTRO DELL'INTERNO

di concerto con

IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE

- Visti gli articoli 5 e 9 del decreto legislativo 25 luglio 1998, n. 286, recante il «testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione giuridica dello straniero in Italia», e successive modificazioni ed integrazioni;
- Visti gli articoli 11 e 16 del decreto del Presidente della Repubblica 31 agosto 1999, n. 394, recante il regolamento di attuazione del predetto testo unico;
- Visto il decreto legislativo 30 giugno 2003, n. 196, recante il codice in materia di protezione dei dati personali;
- Visto il regolamento CE n. 1030/2002 del 13 giugno 2002 che istituisce un modello uniforme per i permessi di soggiorno rilasciati a cittadini di Paesi terzi;
- Visto il proprio decreto ministeriale 3 aprile 1986, con il quale è stato approvato il vigente modello del permesso di soggiorno;
- Rilevata l'esigenza di provvedere alla modifica del vigente modello del permesso di soggiorno conformemente alle previsioni introdotte dal regolamento CE n. 1030/2002 e dai citati articoli 5, comma 9, del decreto legislativo 25 luglio 1998, n. 286 e 11 e 16 del decreto del Presidente della Repubblica 31 agosto 1999, n. 394; Sentito il Garante per la protezione dei dati personali;

ADOTTA

il seguente decreto:

**Regole tecniche e di sicurezza relative al permesso ed alla carta di soggiorno**

Omissis

**Capo II - Regole tecniche di base e norme procedurali**

**Articolo 5 - Supporto fisico ed informatico**

1. Il supporto fisico del documento di soggiorno è costituito da una carta plastica conforme alle norme ISO/IEC 7816-1, 7816-2 e ISO/ID-001 ed è integrato da un supporto informatico.

2. 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 di soggiorno visivamente e mediante strumenti portatili e di laboratorio.
3. Il supporto fisico è dotato di una banda ottica per la memorizzazione, con modalità informatiche di sicurezza, dei dati riportati graficamente sul documento, nonché di un microprocessore per la memorizzazione delle informazioni necessarie alle operazioni connesse alle procedure di autenticazione in rete del documento di soggiorno ed alla verifica della presenza del titolare durante il suo utilizzo telematico. Gli standard internazionali, le caratteristiche tecniche e l'architettura logica del supporto informatico sono conformi alle specifiche indicate nell'allegato B.

#### **Articolo 6 - Produzione, inizializzazione e formazione del documento**

1. La produzione del documento di soggiorno è riservata all'Istituto che vi provvede ottemperando alle norme che disciplinano la produzione delle carte valori e dei documenti di sicurezza della Repubblica italiana e agli standard internazionali di sicurezza previsti per l'emissione delle carte di pagamento.
2. Nella fase di produzione dei documenti di soggiorno di cui al presente decreto, l'Istituto, nell'ambito del proprio stabilimento, costituisce uno speciale settore con accesso limitato ai dipendenti addetti alle specifiche lavorazioni e sorvegliato dalle Forze di polizia, dotato altresì delle sicurezze fisiche antieffrazione e dei sistemi di sorveglianza elettronici definiti d'intesa con il Ministero dell'interno ed il Ministero dell'economia e delle finanze.
3. Nella fase di inizializzazione dei documenti di soggiorno, l'Istituto provvede a strutturare il supporto fisico e quello informatico secondo le procedure di sicurezza descritte nell'allegato B.
4. Nella fase di formazione dei documenti di soggiorno, l'Istituto, ricevuta la necessaria abilitazione ad emettere i documenti di soggiorno da parte di SSCE-PSE, utilizzando le chiavi di sicurezza di cui all'art. 7, comma 1, lettera c), memorizza, secondo le modalità indicate nell'allegato B, i dati identificativi della persona e quelli relativi ai figli minorenni nella banda ottica e nel microprocessore, in quest'ultimo memorizza anche la chiave biometrica. L'Istituto, garantendo l'allineamento con i dati memorizzati nel microprocessore, effettua la personalizzazione grafica del documento di soggiorno riportando i dati identificativi della persona e quelli relativi ai figli minorenni.
5. L'Istituto, utilizzando le chiavi di sicurezza, comunica al SSCE-PSE il completamento delle attività di cui ai precedenti commi. L'Istituto non conserva traccia dei dati utilizzati per la formazione e personalizzazione del documento di soggiorno.

#### **Articolo 7 - SSCE-PSE e software di sicurezza**

1. Per l'attuazione degli articoli 2 e 4 del presente decreto, il Ministero dell'interno Dipartimento della pubblica sicurezza, con l'utilizzo dell'infrastruttura informatica già operante per il sistema di sicurezza del circuito di emissione della carta d'identità elettronica:
  - a. assicura la realizzazione, la gestione e la manutenzione del SSCE-PSE;

- b. fornisce alle questure il software di sicurezza finalizzato a garantire l'integrità e la riservatezza di dati durante la trasmissione delle informazioni necessarie alla formazione dei documenti di soggiorno;
  - c. fornisce all'Istituto le chiavi di sicurezza finalizzate a garantire l'integrità e la riservatezza dei dati durante la trasmissione delle copie elettroniche dei documenti di soggiorno e durante le fasi di formazione;
  - d. fornisce agli enti il software di sicurezza per l'attivazione ed il rilascio del documento di soggiorno.
2. Le questure, nei casi di furto, smarrimento o revoca, procedono all'interdizione dell'operatività del documento di soggiorno secondo le modalità descritte nell'allegato B.

Omissis

### **Articolo 9 - Procedure di sicurezza per la consegna e l'attivazione del documento**

1. L'attivazione informatica e la consegna del documento di soggiorno avvengono nel rispetto della seguente procedura di sicurezza:
  - a. l'Ente, utilizzando le funzionalità del software di sicurezza di cui all'art. 7, comma 1, lettera d), identificato il titolare, secondo le modalità indicate nell'allegato B, e ricevuta la necessaria abilitazione da parte del SSCE-PSE, attiva il documento di soggiorno;
  - b. l'Ente genera il PIN, lo stampa su carta chimica retinata in grado di garantire la riservatezza dell'informazione e lo consegna, insieme al documento di soggiorno, al titolare.

Omissis

### Allegato A

Legenda:

Nome: Cognome e Nome del Titolare

Valido fino al: Data di scadenza del documento

Luogo e data rilascio

Tipo documento

Note: Codice Fiscale + Zona a disposizione dell'autorità per campi aggiuntivi (fino a 5 righe)

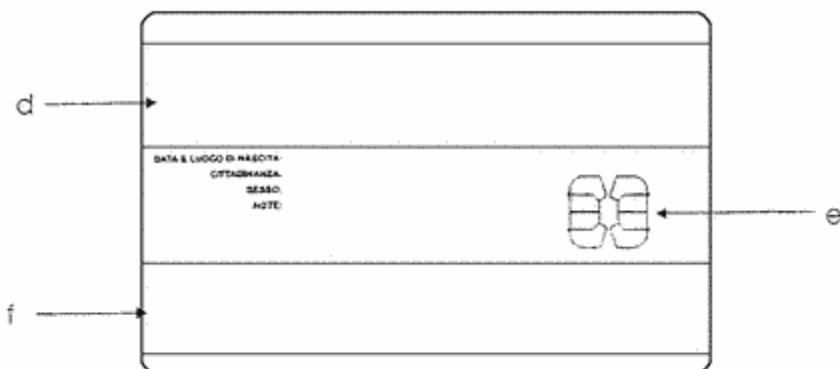
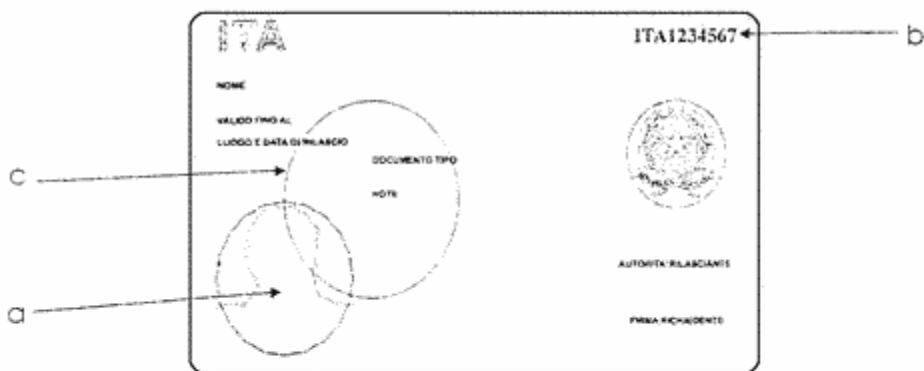
Firma dell'autorità rilasciante

Firma del richiedente

a. Fotografia del titolare

b. Numero assegnato al documento in bianco

c. Zona con elemento DOVID



Data e luogo di nascita

Cittadinanza

Sesso

Note: Zona a disposizione dell'autorità per campi aggiuntivi (fino a 3 righe)

d. Banda a memoria ottica

e. Modulo Chip

f. Spazio riservato alla codifica ICAO con caratteri OCRB

## **Allegato B**

### **REGOLE TECNICHE PER L'EMISSIONE DEL PERMESSO DI SOGGIORNO ELETTRONICO - PSE -**

#### **1. Introduzione**

##### **1.1. Scopo del documento**

Il presente documento descrive le caratteristiche tecniche del nuovo permesso di soggiorno elettronico (PSE) e l'architettura del circuito di emissione, con particolare attenzione ai requisiti di sicurezza nella loro accezione più ampia ed agli aspetti di interoperabilità con il documento di identità elettronico (CIE).

L'architettura è stata realizzata al fine di garantire:

- la sicurezza del circuito di produzione e formazione del nuovo permesso di soggiorno, per diminuire i rischi di contraffazioni e di furti;
- la sicurezza del circuito di emissione/produzione;
- l'integrità, la certificazione e la riservatezza dei dati;
- la sicurezza del supporto fisico del documento, ai fini dell'identificazione a vista;
- la salvaguardia degli investimenti attraverso il riuso delle infrastrutture già presenti, utilizzate per analoghe applicazioni;
- la interoperabilità con la carta d'identità elettronica;
- il contenimento dei costi.

##### **1.2. Obiettivi del permesso di soggiorno elettronico**

I motivi ispiratori che hanno guidato la definizione dell'architettura del nuovo permesso di soggiorno sono:

- rispondere alla esigenza di produrre uno strumento sicuro sotto i diversi aspetti della produzione, rilascio nonché utilizzo da parte del titolare. La sicurezza non solo deve accompagnare tutti i flussi informatici, ma deve anche essere presente sul supporto fisico al fine di scoraggiare facili contraffazioni, nonché di consentire una identificazione certa da parte delle istituzioni competenti;
- fornire un supporto standard, perfettamente in linea con le indicazioni dell'Unione Europea e per garantire la massima apertura al mercato dei fornitori dei supporti;
- consentire un migliore monitoraggio dei confini del Paese, grazie ad uno strumento flessibile ed efficace in grado di agevolare i controlli nei punti di ingresso al Paese.

##### **1.3 La struttura del Permesso di Soggiorno Elettronico**

Il raggiungimento degli obiettivi presuppone l'utilizzo di materiali e tecnologie standard, affidabili e nello stesso tempo in grado di garantire alti livelli di sicurezza. Il solo utilizzo di un supporto plastico, per quanto sofisticato, non sarebbe sufficiente a soddisfare tutte le esigenze sopra esposte.

Per questo la scelta è stata quella di una carta ibrida in grado di ospitare anche un supporto informatico, costituito da un microprocessore, e un supporto ottico costituito da una banda a memoria ottica.

Il supporto informatico consente di memorizzare:

- i dati presenti sul documento in forma grafica, introducendo una duplicazione delle informazioni fondamentale ai fini della sicurezza;
- ulteriori informazioni e l'immagine digitalizzata della fotografia. Viene inoltre previsto lo spazio per registrare le impronte digitali quando, come previsto con la nuova Direttiva europea in corso di promulgazione, il loro utilizzo sarà possibile in tutti i Paesi dell'Unione Europea.

Il supporto ottico consente di:

- replicare nella memoria ottica i dati presenti sul documento in forma grafica;
- riprodurre con una incisione laser visibile (embedded hologram) alcune informazioni relative al titolare ed al documento (fotografia, Cognome, Nome, N. Documento e Data di scadenza), in modo da innalzare i livelli di sicurezza del documento e rendere più sicura l'identificazione a vista.

Le caratteristiche grafiche del PSE sono riportate nell'allegato A.

## 2. Il circuito di emissione

### 2.1. Infrastruttura Organizzativa

Nel circuito di emissione intervengono gli enti nel seguito descritti:

<b>Ufficio Territoriale di Governo (Sportello Unico)</b>	<i>Ente responsabile del procedimento, ai sensi del Regolamento di cui all'art. 34 comma 1 della legge n. 189/2002.</i>
<b>Questure</b>	<i>Ente responsabile degli accertamenti, per verificare l'inesistenza di motivi ostativi al rilascio del permesso di soggiorno elettronico, e dei rilievi fotodattiloscopici.</i>
<b>Dipartimento P.S.</b>	<i>Sistema Informativo della Polizia Scientifica, responsabile del Sistema di Sicurezza del Circuito d'Emissione del Permesso di Soggiorno.</i>
<b>Istituto Poligrafico e Zecca dello Stato</b>	<i>Ente a cui è riservata l'inizializzazione, la produzione e la formazione dei Permessi di Soggiorno Elettronico</i>
<b>Enti</b>	<i>Gli Uffici responsabili dell'attivazione informatica e della consegna del Permesso di Soggiorno Elettronico</i>

### **3. Infrastruttura di rete**

#### **3.1 Le Infrastrutture condivise tra CIE e PSE**

Come indicato negli obiettivi, una delle principali finalità che si prefigge il Permesso di Soggiorno elettronico è quella della interoperabilità con la CIE e, anche per favorire economie di spesa, di condividerne le infrastrutture nel modo più ampio possibile.

Nonostante la diversità dei due documenti e le differenti modalità di realizzazione, molte sono le componenti riusabili, specialmente quelle presso il sistema centrale e quelle presso i Comuni che potranno provvedere, in alternativa alle Questure, all'attivazione del documento stesso attraverso la generazione, stampa e consegna dei codici segreti personali I (PIN, PUK e CIP).

Il PUK è il codice identificativo personale necessario all'utilizzo telematico del documento, il PUK è il codice da utilizzare per modificare il PIN e, infine, il CIP è il codice da comunicare in caso di furto o smarrimento del permesso di soggiorno.

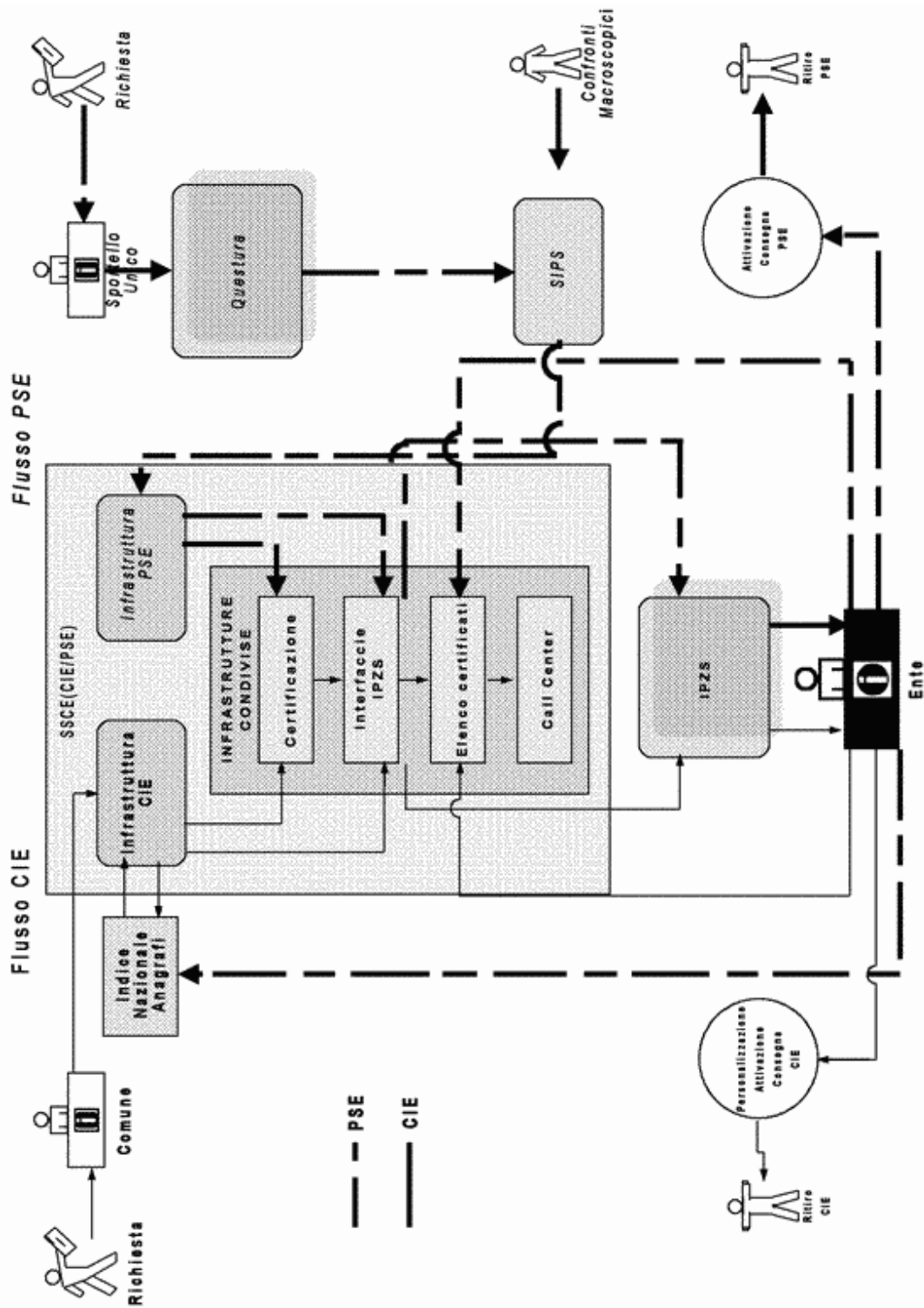
Nello figura 1 è riportato uno schema che illustra graficamente la distinzione tra i flussi della CIE e quelli del PSE, con particolare riferimento alla infrastruttura di certificazione, elemento di condivisione e garanzia per l'interoperabilità tra i due documenti.

La condivisione delle infrastrutture oltre a rendere il permesso di soggiorno, alla stregua della carta d'identità elettronica, strumento per l'accesso ai servizi di «e-government», semplifica e rende maggiormente sicure le procedure di iscrizione e di variazione anagrafica del titolare del titolo di soggiorno.

#### **3.2 Dotazioni delle Questure**

- connessione al Sistema Informativo della Polizia Scientifica (SIPS), tramite le infrastrutture di rete della Polizia di Stato, i cui collegamenti sono attivi in tutte le Questure della Repubblica;
- software di sicurezza versione *client*, per la trasmissione al SIPS dei dati relativi al PSE.

Fig.1-L'infrastruttura di certificazione condivisa



### 3.3 Dotazioni del SSCE-PSE

- connessione alle Questure per consentire la visualizzazione dei permessi di soggiorno e renderne possibile l'eventuale revoca;
- Connessione all'INA - Centro Nazionale dei Servizi Demografici (CNSD), per la notifica delle variazioni anagrafiche;

- connessione diretta con l'IPZS per l'interscambio d'informazioni nella fase d'inizializzazione, di stampa e di notifica dei permessi di soggiorno stampati;
- software di sicurezza versione server per le funzionalità connesse alle diverse fasi di produzione, formazione, attivazione e rilascio del PSE. Tale software è il risultato di un adeguamento di quello realizzato per la CIE da cui è mutuato;
- infrastruttura di certificazione, per la generazione dei certificati di sicurezza e per la verifica dello stato dei certificati stessi. Per tali funzioni viene utilizzata la stessa infrastruttura di rilascio della CIE.

### **3.4 Dotazioni degli Enti**

Gli Enti periferici, sono abilitati ad attivare e consegnare i permessi di soggiorno elettronici, limitando le loro funzioni alle fasi di: attivazione, stampa dei codici segreti (PIN), e comunicazione a SSCE-PSE dell'avvenuta consegna ed invio.

La notifica e la trasmissione del record PSE, per gli aggiornamenti anagrafici, sarà effettuata direttamente dal SIPS al CNSD.

Gli Enti dovranno essere dotati di uno specifico applicativo distribuito da SSCE-PSE che consentirà l'attivazione del permesso di soggiorno e la notifica dell'avvenuto rilascio al sistema SSCE-PSE.

## **4. Materiali, Standard di Riferimento e Tracciato record**

La realizzazione del permesso di soggiorno elettronico, essenziale per innalzare i livelli di sicurezza del documento, si è resa necessaria per rispondere ai requisiti imposti dall'Unione Europea per unificare i singoli documenti nazionali (*Regolamento (CE) n. 1030/2002.*)

L'esigenza di uniformità ha portato a definire, in ambito comunitario, le informazioni stesse presenti nel permesso di soggiorno che impone vincoli soprattutto per quanto attiene ai dati previsti quali obbligatori ed al «lay-out» del documento stesso.

La scelta nazionale, inoltre, di dotare il supporto fisico della componente elettronica, microprocessore, comporta l'adeguamento ai previsti standard internazionali, anche a garanzia del raggiungimento degli obiettivi prefissati.

### **4.1 Il Supporto Fisico**

#### **4.1.1 Le dimensioni Nominali e le componenti**

Il supporto fisico deve essere conforme alle norme che regolamentano i Documenti di Identificazione, International Standards Organization (ISO)/IEC 7816-1, 7816-2 2.

Le dimensioni nominali dovranno essere di 53,98 x 85,6 mm come specificato nella norma ISO/IEC 7810: 1995 per la carta di tipo ID-1. La tolleranza, nelle dimensioni, è quella definita dalla norma stessa.

Lo spessore del PSE, compresi eventuali «film» di protezione, dovrà essere conforme alla norma ISO/IEC 7810: 1995.

Il PSE, sarà costituito da materiali plastici compatibili con gli strumenti tecnologici in esso contenuti, nonché con i sistemi di personalizzazione utilizzati per la sua compilazione.

Il PSE, dovrà rispondere alle specifiche definite:

- nella norma ISO/IEC 7810: 1995 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 il PSE, per un uso normale durante il periodo di validità, deve rispondere alle specifiche definite nella norma ISO/IEC 7816 - 1.

## 4.2 Il Microprocessore

È il microcircuito composto da un circuito stampato, che esercita le funzioni di interfaccia verso l'esterno, e da un circuito integrato *chip*, incastonati sulla scheda.

La capacità di elaborazione propria del microcircuito *chip* permette di annoverare il PSE come una *smartcard* (carta intelligente).

La presenza di un vero sistema operativo e di una memoria riscrivibile e non volatile (EEPROM), rende possibile proteggere i dati memorizzati ed eseguire istruzioni e programmi, in modo del tutto simile ad un vero computer.

La caratteristica, propria del microcircuito, di poter nascondere informazioni all'*esterno* di esso, ed al contempo di poter eseguire istruzioni o programmi *interni*, rende possibile il riconoscimento sicuro della carta per via telematica ed aumentare la capacità di controllo sul territorio, abbinando al tradizionale controllo *a vista* anche un più moderno e sicuro riconoscimento elettronico.

La capacità di autenticazione *in rete* del documento, inoltre, ne può consentire un suo utilizzo per l'accesso a servizi telematici.

Abbinando alle potenzialità intrinseche dei microprocessori e dei certificati di autenticazione anche la presenza del *template* dell'impronta digitale, sarà possibile il confronto in locale tra il template contenuto sulla carta e quello letto da un eventuale terminale lettore di impronte digitali oltre all'autenticità della carta, anche la presenza del titolare.

In termini di capacità di memoria, il PSE dovrà utilizzare un microcircuito con una EEPROM dalla capacità minima di 32 Kb al fine di poter ospitare tutte le informazioni necessarie per il permesso di soggiorno.

Un'altra caratteristica del microcircuito è la presenza del co-processore crittografico, che rende estremamente veloci le operazioni di cifratura e di decifratura. Il motore crittografico presente sul PSE è in grado di eseguire, in modalità nativa, *almeno* l'operazione di RSA *signature* con chiavi di lunghezza non inferiore a 1024 bit.

Il circuito stampato, che protegge il *chip* dallo sforzo meccanico e dall'elettricità statica, deve essere conforme alla norma ISO 7816-3 che fornisce cinque punti di collegamento per potenza e dati.

Gli standard di riferimento, per il microcircuito e per i comandi del sistema operativo da esso ospitato, sono i seguenti ISO 7816-3,4,8.

Le specifiche per i comandi, nella forma di APDU, devono obbligatoriamente rispettare gli standard citati, essere in linea con quanto specificato per la CIE ed integrabili sulla base di eventuali future evoluzioni.

### 4.3 La Carta a memoria ottica

La carta ottica è realizzata in policarbonato, un materiale plastico di provenienza aeronautica, che garantisce un'ottima trasparenza per la scrittura su banda ottica, una elevata resistenza, una maggiore durata nel tempo ed un intervallo termico di utilizzo molto ampio (-40° +100°).

Il film è composto da diversi strati di materiale ed il supporto ottico registrabile è incapsulato tra due livelli di materiale protettivo trasparente che (sulla faccia esterna) è rinforzato da un ulteriore strato *antigraffio*.

La capacità di memoria di una carta ottica, a seconda dei modelli, va dai 4,1 Mb ai 6 Mb (ma tramite tecniche di compressione si può arrivare oltre i 20 Mb), che scendono a 2,86 Mb o a 4,89 Mb, a seconda dei modelli, in caso di pieno utilizzo della capacità d'identificazione e correzione degli errori.

Ogni carta ottica permette la creazione di settori variabili basati su tracce, consentendo così l'archiviazione di informazioni multiple ed indipendenti.

### 4.4 I Dati

Nel prosieguo sono indicate le informazioni contenute nel PSE, che sono riportate graficamente sul supporto plastico e memorizzate all'interno del microprocessore e della banda ottica.

I dati contrassegnati con una asterisco [\*] sono, inoltre, incisi in maniera visibile sul supporto ottico.

#### **Descrizione Campo**

---

Numero assegnato al documento [1] [\*]

---

Cognome [\*]

---

Nome [\*]

---

Data di scadenza del documento [\*]

---

Data di rilascio del documento

---

Luogo di rilascio del documento

---

Documento Tipo (Stato di emissione)

---

Sesso

---

Data di nascita

---

Cittadinanza

---

Nota 1 (Nome figlio)

---

Nota 2 (Nome figlio)

---

Nota 3 (Nome figlio)

---

Nota 4 (Nome figlio)

---

Nota 5 (Nome figlio)

---

Nota 6 (Nome figlio)

---

Nota 7 (Nome figlio)

---

Nota 8 (Nome figlio)

---

Nota 9 (Nome figlio)

---

Nota 10 (Nome figlio)

---

Firma del richiedente

---

Fotografia 23x28mm - 300dpi - 16 Ml di colori (a 24 bit) [\*]

---

n. 2 (due impronte digitali, in formato immagine (1" x 1" - 500

---

dpi - 256 livelli di grigio) e in formato numerico (template)

[1] Il numero assegnato al documento è composto da un prefisso di tre caratteri che indica lo stato in cui il PSE viene rilasciato e da un progressivo alfanumerico di sette caratteri. Ad esempio per l'Italia potrebbe essere «ITA0000001».

## 5. Misure di sicurezza

Nel presente paragrafo sono descritte le modalità e l'architettura attraverso le quali ottenere in tutte le fasi della produzione e dell'utilizzo del PSE i corretti livelli di sicurezza e di interoperabilità del documento.

### 5.1 Sicurezza del Supporto Fisico

Il principio ispiratore è stato quello di garantire al PSE un supporto plastico difficilmente riproducibile e falsificabile se non con tecnologie molto sofisticate e costose.

Nel seguito sono elencati gli elementi utilizzabili per la sicurezza del supporto e per accertarne l'autenticità, anche attraverso il semplice esame visivo.

Questi elementi di sicurezza sono tipici del settore bancario e vengono applicati al supporto plastico in fase di produzione. La verifica dell'alterazione/presenza di questi elementi può essere facilmente eseguita sia visivamente sia utilizzando strumenti presenti sul mercato a costi contenuti.

Infine, la scelta del polycarbonato per la realizzazione del supporto fisico, oltre a garantire la durata del supporto, costituisce un altro elemento di sicurezza. Infatti, il polycarbonato rispetto al più usuale PVC aggiunge difficoltà in fase di personalizzazione non facilmente superabili con gli apparati reperibili sul mercato.

#### 5.1.1 Elementi di Sicurezza grafici e di stampa

Gli elementi grafici stampati sul fronte e sul retro del PSE sono realizzati con accorgimenti propri delle carte valori:

- motivi antiscanner ed antifotocopiatura a colori;
- stampa con effetto rainbow (a sfumatura di colore graduale e progressiva);
- motivi grafici multicolore richiedenti elevata qualità di registro di stampa;
- personalizzazione con tecnica laser engrave (incisione grafica su polycarbonato);
- inchiostri otticamente variabili (OVI - Optical Variable Ink);
- inchiostri fluorescenti visibili all'ultravioletto.

### 5.2 Sicurezza della fase di personalizzazione

La personalizzazione del PSE sarà effettuata in forma centralizzata e, pertanto, potranno essere utilizzate tecniche di stampa sofisticate, quali ad esempio il *laser engrave*.

La tecnica del *laser engrave* consente di personalizzare il documento senza utilizzare inchiostri che potrebbero essere facilmente contraffatti. La stampa avviene per microforature del supporto, ottenute con delle piccole bruciature del materiale plastico. Le informazioni così ottenute non sono, ovviamente, più modificabili.

L'unica informazione che, per consentire un più agevole confronto a vista, rimane stampata con tecniche tradizionali, è la fotografia che, comunque, è replicata insieme agli altri dati nel microprocessore.

### 5.3 Affidabilità dei dati

Al fine di rendere sicuri i dati riportati nel permesso di soggiorno, gli stessi sono replicati all'interno del microprocessore in modo da evidenziare, con un controllo elettronico, eventuali difformità tra le informazioni riportate graficamente sul supporto e quelle memorizzate all'interno del microcircuito.

Esistono due distinti livelli di protezione dei dati conservati nel microcircuito: un livello fisico, ed un livello logico. La protezione a livello fisico è gestita dal produttore del *chip* che provvede a *mascherare* sulla carta, in maniera indelebile, il sistema operativo proteggendolo mediante una chiave segreta di cui esso solo è a conoscenza.

Il livello logico è invece gestito sia dall'entità che inizializza il PSE che dall'ente che la personalizza. Per i PSE le due entità coincidono e pertanto la sicurezza è ulteriormente garantita.

Tre sono le tipologie di dati che il microcircuito contiene:

- a. le informazioni specifiche dell'hw e del sw;
- b. le informazioni anagrafiche e identificative del titolare;
- c. i dati relativi alla carta servizi, cioè necessari alla fruizione dei servizi erogati da un server remoto.

Per quanto riguarda la prima e la seconda tipologia di dati, la registrazione può avvenire soltanto dopo il superamento di particolari condizioni di test ed una volta effettuata, comporta la modifica dei diritti di accesso ai dati alla sola lettura.

Relativamente alla terza tipologia di dati, che fanno riferimento alla fruizione dei servizi, si deve far riferimento alla classificazione, standard e qualificati, ed alle modalità di registrazione definite per la carta d'identità elettronica, al fine di garantire la piena compatibilità.

### 5.4 La sicurezza del circuito

La migliore garanzia contro tentativi di contraffazioni, falsificazioni e utilizzo di carte rubate, si trova nella centralizzazione virtuale prevista dall'architettura del circuito d'emissione del PSE, che presenta caratteristiche analoghe a quello della CIE. In aggiunta, per il permesso di soggiorno, la personalizzazione centralizzata offre ulteriori sicurezze derivanti dal fatto che l'inizializzazione dei documenti e la loro personalizzazione avvengono in modalità sequenziale ed all'interno dello stesso edificio.

In tale logica, il Sistema di Sicurezza del Circuito d'Emissione dei PSE traccia tutte le operazioni al fine di garantire il rispetto della normativa vigente sulla riservatezza delle informazioni e dei dati personali, per impedire l'emissione di documenti falsi e per individuare facilmente l'utilizzo fraudolento di documenti rubati e la contraffazione di documenti autentici.

#### **5.4.1 La sicurezza degli accessi ai dati**

Passando da un documento cartaceo ad uno di formato elettronico, il SSCE-PSE che certifica, rendendola sicura, l'emissione del documento, mantiene una copia elettronica del permesso di soggiorno.

Ciò pone nella necessità, a fini di sicurezza e nel rispetto delle norme di legge, di consentire l'accesso e la visualizzazione dei cartellini elettronici ai soli soggetti autorizzati.

A tal fine, il Sistema di Sicurezza (SSCE-PSE), garantisce la tracciabilità di tutte le attività per ogni singolo documento consentendo di risalire, in qualsiasi momento, alle informazioni di *chi ha fatto cosa e quando*, nel rispetto delle attuale normativa, durante tutte le fasi di formazione, compilazione, rilascio e rinnovo dei documenti.

Tutte le informazioni, verso gli utenti abilitati, vengono trasmesse cifrati a 128 bit in modalità «3 DES».

In tal modo pur migliorando e semplificando l'accesso ai dati agli Uffici autorizzati, non sono minimamente modificati i livelli di autorizzazione.

#### **5.4.2 Furto delle Carte**

I rischi derivanti da furti e falsificazioni, con l'adozione del modello elettronico, sono notevolmente ridotti, principalmente in virtù della natura del supporto e delle garanzie di inalterabilità delle informazioni riportate all'interno del microprocessore.

Il controllo a vista del documento, inoltre, è assicurato dalle particolari modalità di personalizzazione grafiche che utilizzano la tecnica del *laser engrave*, per la stampa del supporto plastico, e quella dell'*Embedded Hologram* per la replica di alcune informazioni sulla banda ottica. Le due tecnologie concorrono a realizzare una personalizzazione immodificabile, garantendo il contenuto da qualsiasi attacco.

Gli eventuali interventi meccanici che modifichino strutturalmente o fisicamente il PSE sarebbero immediatamente visibili.

Relativamente al microchip, questi non permette - grazie alla sicurezza del suo stesso sistema operativo, di modificare o scrivere informazioni se non alla presenza di determinate autorizzazioni.

Inoltre tutte le informazioni sensibili, sul chip, sono garantite contro l'alterazione, perché «firmate» elettronicamente.

#### **5.4.3 Controlli a vista**

L'intero circuito di sicurezza attraverso l'adozione dell'architettura a centralizzazione virtuale consente di innalzare il livello di qualità dei controlli, c.d. a vista, effettuati dalle Forze di Polizia per verificare l'identità delle persone sottoposte ai controlli stessi grazie all'utilizzo di particolari tecniche di stampa del documento e di certificazione delle informazioni in esso contenute.

Le sicurezze adottate durante la fase di inizializzazione e formazione del documento, comprese le repliche dei dati nel supporto elettronico ed in quello ottico, lo rendono molto più affidabile del modello cartaceo.

Laddove nascesse l'esigenza di un approfondimento sulla autenticità del PSE, due sono le possibili soluzioni:

- Controllo dei dati memorizzati nel chip. La lettura delle informazioni nel microprocessore, comprese quelle firmate con la chiave privata del circuito di emissione, consente di

verificare la autenticità delle informazioni o la loro eventuale alterazione, immediatamente evidenziabili in fase di lettura.

- Controllo delle informazioni presso il SSCE-PSE. A differenza del passato oggi le Questure possono, collegandosi al SSCE-PSE, verificare, immediatamente se le informazioni in esso contenute corrispondono con quelle riportate nel documento.

#### 5.4.4 Il servizio di validazione dei documenti

Presso il SSCE-PSE è presente un servizio telematico, che permette di controllare la validità dei documenti e stabilire se un PSE è interdetto, sconosciuto, oppure valido. Tale servizio è indispensabile per impedire l'operatività del PSE in caso di smarrimento, furto dello stesso o revoca del titolo.

Le procedure da seguire per l'interdizione della carta vengono descritte nel successivo paragrafo 8.

### 6. Processo di Emissione

Nel presente capitolo sono descritte in dettaglio le fasi operative previste dal circuito d'emissione. Per una migliore comprensione del processo d'emissione si riporta un glossario di riferimento.

<b>Fp</b>	<b>Fornitori microprocessori</b>
<b>IPZS</b>	<b>Istituto Poligrafico Zecca dello Stato</b>
<b>SSCE-PSE</b>	<b>Sistema di sicurezza del circuito di emissione per il permesso di soggiorno elettronico</b>
<b>E</b>	<b>Ente che attiva e consegna il PSE</b>
<b>R_PSE</b>	<b>Record Permesso di Soggiorno Elettronico.</b> È composto dai dati anagrafici del titolare, da una sua fotografia e dai nominativi dei minori.
<b>ID_PSE</b>	<b>Numero identificativo del PSE</b> Numero assegnato al documento, generato dal SSCE-PSE al momento della formattazione del record PSE.
<b>C_PSE</b>	<b>Certificato anticontraffazione del permesso di soggiorno</b> - Certificato che lega il numero identificativo del documento alla coppia di chiavi asimmetriche ( <b>Kpri e Kpub</b> ), generate all'interno del microprocessore e, per quanto riguarda Kpri non esportabile all'esterno. Il certificato di sottoscrizione risponde alle direttive della normativa vigente e contiene il riferimento codice fiscale del titolare nel campo COMMON NAME. - È rilasciato dal SSCE-PSE e viene riportato nel microprocessore.

<b>Dati_processore</b>	<b>È un file elementare che riporta alcuni dati univoci del processore</b> Le informazioni che contiene sono: <b>Fp, numero seriale e data fabbricazione.</b>
<b>Dati_banda_optica</b>	<b>È un file elementare che riporta alcuni dati univoci del supporto ottico</b> Le informazioni che contiene sono: <b>Fb, numero seriale e data fabbricazione.</b>
<b>PIN firma digitale</b>	È il PIN necessario al titolare per farsi installare da un certificatore il servizio di firma digitale.
<b>PIN utente</b>	È il PIN necessario al titolare per utilizzare la chiave privata Kpri per le <b>operazioni di autenticazione in rete</b> . Viene consegnato dall'Ente o con meccanismi di sicurezza (es. busta in carta chimica protetta).

## 6.1 Produzione microprocessore

I Fornitori di microprocessori (Fp) provvedono alla fabbricazione dei supporti informatici ed alla mascheratura in ROM(EEPROM) del Sistema Operativo.

Applicano, in fase di produzione, un numero seriale progressivo univoco, sui supporti informatici da loro forniti e predispongono una distinta, cartacea ed elettronica, che riporta le seguenti indicazioni: ID fornitore, numero seriale, numero del lotto di produzione, data di produzione.

I fornitori, successivamente, inviano i loro prodotti, accompagnati dalle distinte, direttamente all'Istituto Poligrafico dello Stato (IPZS).

Al fine di garantire la totale compatibilità tra i microprocessori, anche in presenza di forniture effettuate da produttori diversi, i microprocessori dovranno essere certificati tramite specifiche prove funzionali da effettuarsi presso l'istituto Poligrafico e Zecca dello Stato e presso il Servizio Polizia Scientifica.

## 6.2 Produzione, inizializzazione e formazione del Permesso di Soggiorno Elettronico.

Per meglio comprendere le diverse fasi del circuito di emissione, è bene fare dei brevi cenni sull'organizzazione e sulla normalizzazione delle informazioni nel microprocessore.

### 6.2.1 Struttura delle informazioni nel microprocessore

Per consentire la registrazione delle informazioni nella memoria del microprocessore e garantire la completa interoperabilità dello stesso con quello della carta d'identità elettronica, per il PSE viene adottata una struttura fisica e logica coerente con quella della CIE, a cui si fa riferimento.

### 6.2.2 Struttura delle informazioni sulla banda ottica

Sulla banda ottica vi sono due aree di memorizzazione differenti ma sincrone:

- Una **area dati** che contiene, codificati in record di formato opportuno ( $R_d$ ), i necessari dati della carta, del titolare e i servizi installati.

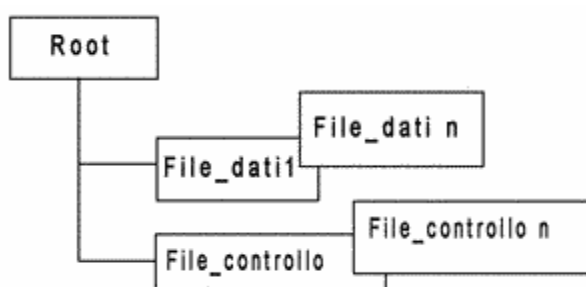
- Una **area di controllo** che contiene, codificate in formato opportuno ( $R_c$ ), le informazioni di controllo e verifica dei corrispondenti  $R_d$ .

L'area controllo è assimilabile ad un registro incrementale delle operazioni avvenute sulla carta, e consente di stabilire con certezza *chi, dove e quando* ha effettuato ed autorizzato ogni operazione. La certezza viene stabilita dall'uso incrociato dei «sigilli» apposti da:

- Istituto Poligrafico dello Stato;
- SSCE.

A ciascun record  $R_d$  dell'area dati corrisponde un record  $R_c$  dell'area di controllo. I record dati possono avere formati multipli secondo necessità.

La successiva figura descrive graficamente la struttura di memorizzazione interna alla banda a memoria ottica:



### 6.3 Le fasi preliminari

L'Istituto Poligrafico, responsabile della produzione, inizializzazione e formazione del PSE riceve, dal Ministero dell'interno - Dipartimento della Pubblica Sicurezza, la stima del fabbisogno annuale di documenti.

La consegna agli Enti, delegati alla attivazione e al rilascio dei permessi di soggiorno, avviene dopo che l'Istituto Poligrafico e Zecca dello Stato ha eseguito la Formazione del documento. Pertanto, il PSE, non subirà nessun trasferimento fisico fino a quando non sarà completamente personalizzato.

Nel seguito viene riportata una tabella di sintesi con le varie sottofasi e l'indicazione degli Enti competenti per l'attività.

ATTIVITÀ	ENTE
PRODUZIONE SUPPORTI	IPZS
GESTIONE RICHIESTA	UTG (Sportello Unico)
ACCERTAMENTI	QUESTURA
FORMATTAZIONE RECORD PSE	SSCE-PSE
INIZIALIZZAZIONE E FORMAZIONE	IPZS-SSCE-PSE
ATTIVAZIONE E RILASCIO	ENTI PERIFERICI - SSCE- PSE
PUBBLICAZIONE CERTIFICATI	SSCE - PSE

### 6.3.1 Produzione Supporti

L'IPZS, attiva le procedure necessarie ai fini della:

- predisposizione del supporto fisico;
- inserimento nel supporto fisico del microprocessore e della banda ottica;
- stampa del logo e degli elementi grafici costanti e di sicurezza;
- inizializzazione elettrica del microprocessore;
- colloquio telematico con SSCE-PSE.

### 6.3.2 Gestione Richiesta

L'Ufficio Territoriale di Governo (sportello unico), ricevute le richieste di permesso di soggiorno, effettua:

- le verifiche sulla documentazione e sull'ammissibilità di concessione;
- trasmette alla Questura la documentazione necessaria per gli accertamenti;
- rilascia una ricevuta al richiedente e stabilisce, d'intesa con la Questura, la data per i rilievi fotodattiloscopici.

### 6.3.3 Accertamenti

La Questura, ricevuta la documentazione dall'UTG, esegue:

- gli accertamenti per verificare l'inesistenza di motivi ostativi al rilascio;
- i rilievi fotodattiloscopici;
- trasmissione per via telematica al Sistema Informativo della Polizia Scientifica delle informazioni necessarie alla predisposizione del permesso di soggiorno.

### 6.3.4 Formattazione PSE e trasmissione record a IPZS

Il SSCE-PS, ricevuti i record:

- formatta R\_PSE e genera il numero univoco nazionale ID\_PSE. Il record, in attesa di divenire PSE, viene memorizzato nel database di SSCE-PSE;
- cifra il record, utilizzando la cifratura «3DES» con chiave a 128 bit, lo certifica, con la sua firma elettronica (Kpri di SSCE-PSE), e lo trasmette all'Istituto Poligrafico.

### 6.3.5 Inizializzazione e Formazione

Le sottofasi di inizializzazione e formazione, sono le più delicate dell'intero processo di emissione in quanto viene realizzato definitivamente il permesso di soggiorno elettronico e, i due elementi che lo costituiscono, supporto fisico e microprocessore, divengono un unico elemento inscindibile.

Dopo la fase di integrazione fisica del supporto plastico, con il microprocessore e la banda ottica, l'inizializzazione provvede alla integrazione logica tramite l'apposizione di codici univoci. La formazione, invece, è la fase nella quale avviene la personalizzazione grafica del documento e la memorizzazione, delle stesse informazioni, all'interno del microprocessore.

Inizializzare il PSE, di fatto, consiste nello strutturare il microprocessore, in «directory» e nell'impostare le condizioni di test necessarie a definire i diritti di accesso alle directory stesse.

La directory serve per tracciare tutte le fasi di inizializzazione e personalizzazione della Carta, per consentire l'installazione di servizi e per normalizzare le informazioni relative al titolare (informazioni alfanumeriche e fotografia) ed ai figli minori.

Durante la fase di formazione del PSE, invece, IPZS riporta i dati in formato elettronico su microprocessore e banda ottica, e in forma grafica sul supporto fisico e su quello ottico (embedded hologram).

La criticità maggiore, in entrambe le attività (che potrebbero essere eseguite sia separatamente che contestualmente), risiede nel fatto che qualsiasi inconveniente possa verificarsi non deve mettere a rischio l'integrità dei dati (per esempio scrivendo informazioni diverse sui vari supporti). Allo scopo si suggerisce di garantire agli apparati preposti alle attività continuità elettrica. L'applicazione di gestione della formazione delle carte, inoltre, dovrà prevedere controlli sull'intero flusso di lavorazione.

In particolare, IPZS, ricevuto il record dati da SSCE-PSE, provvede alla:

- generazione della struttura dati interna del microprocessore;
- generazione della struttura dati interna della banda ottica;
- scrittura dei file elementari che riportano i dati specifici del microprocessore e della banda ottica;
- impostazione delle condizioni di accesso a tali file;
- memorizzazione dei dati all'interno del microprocessore e della banda ottica. Al fine di consentire una identificazione sicura, e dare certezza sulla originalità del PSE, i dati memorizzati nel microprocessore devono essere firmati con il bollo elettronico di SSCE-PSE (Chiave privata di SSCE-PSE);
- stampa grafica dei dati sul supporto fisico;
- stoccaggio della carta e spedizione sorvegliata agli Enti responsabili dell'attivazione e del rilascio. Il permesso di soggiorno elettronico deve essere disponibile, presso gli Enti, entro 15 giorni.

### 6.3.6 Attivazione e Rilascio

Al termine della precedente sottofase il PSE è completo ma non ancora attivato. Ciò vuol dire che ad un eventuale controllo elettronico, locale o telematico, il documento risulterebbe «non emesso». Per trasformarlo in documento «valido» deve essere attivato e rilasciato.

Le fasi di attivazione e rilascio devono essere effettuate da una struttura decentrata in quanto, entrambe, richiedono la presenza del titolare.

Durante la presente sottofase l'ENTE esegue le seguenti attività:

- riceve da IPZS i «documenti formati» non ancora attivati;
- tramite il software di sicurezza identifica il titolare;
- tramite connessione ad SSCE-PSE;
- il record relativo alle informazioni anagrafiche prelevate dal PSE attivato, al fine di garantire l'aggiornamento anagrafico dell'INA, viene notificato da SSCE al CNSD;

- tramite il software di sicurezza stampa la busta contenente i codici utente di sicurezza (PIN, PUK e CIP) e comunicano l'avvenuta attivazione del documento a SSCE-PSE. Il relativo record (R-PSE) memorizzato in SSCE-PSE passa dallo stato di «non emesso» a quello di «valido».

### **6.3.7 Pubblicazione Certificati**

Per ogni permesso di soggiorno SSCE-PSE pubblica il certificato in una lista elettronica accessibile dagli utenti autorizzati ai controlli o ad erogare i servizi.

Analogamente per ogni documento revocato, il certificato viene pubblicato in una lista di certificati revocati (CRL o black list), anch'essa consultabile in rete.

I certificati presenti nelle liste, essendo emessi dalla stessa infrastruttura, sono interoperabili con quelli delle carte d'identità elettronica ed entrambe le liste condivisibili.

## **7. Interdizione dell'operatività del PSE**

Le caratteristiche principali del nuovo PSE, che lo differenziano dal modello cartaceo, sono rappresentate dalla presenza del supporto informatico e dalla gestione centralizzata del flusso di emissione. Entrambi gli elementi da un lato aumentano il livello di sicurezza del nuovo documento e dall'altro offrono la possibilità di utilizzo del documento in modalità elettronica, sia in locale che per via telematica.

Proprio la possibilità di un utilizzo da remoto del documento, consente di revocare con meccanismi più rapidi ed efficienti un documento anche, per esempio, in caso di furto o smarrimento, al fine di impedirne un uso improprio.

Nel seguito vengono descritte le modalità a cui è necessario attenersi in caso di furto o smarrimento di un PSE.

1. il titolare telefona al numero verde del Call Center di SSCE-PSE e comunica l'avvenuto smarrimento/furto del PSE;
2. per motivi di sicurezza, l'interdizione temporanea del PSE avviene dopo aver verificato il codice di identificazione personale (uno dei codici assegnati in fase di rilascio);
3. a seguito di tale comunicazione nel record relativo al PSE viene apposto un «flag» e, per un periodo indeterminato il PSE non è in grado di accedere a servizi;
4. immediatamente dopo la comunicazione telefonica, il titolare del PSE deve presentare regolare denuncia ad uno degli uffici delle Forze di Polizia;
5. se si dovessero verificare condizioni da far decadere la necessità di presentare la denuncia (ad es. il PSE viene ritrovato), il titolare deve eseguire analoga procedura, a quella utilizzata per denunciare la scomparsa, per rendere il PSE nuovamente «NON interdetto».