Ministero della Giustizia

Dipartimento dell'organizzazione giudiziaria, del personale e dei servizi

Direzione generale per i sistemi informativi automatizzati

Realizzazione di un Sistema Sicuro di Accesso ai sistemi informatici della Giustizia

Carta Multiservizi della Giustizia
Direttive per il rilascio ed uso

Autori: Maria Grazia Salari – Ministero della Giustizia

SOMMARIO

1 Premessa 4
2 Scopo della direttiva 9
3 Requisiti e distribuzione della Carta Multiservizi della Giustizia 10
3.1 Requisiti di base 10
3.2 Distribuzione 10
3.3 Validità 10
4 Struttura e funzioni della CMG 12
4.1 Titolarità 12
4.2 Struttura 12
4.3 Funzioni della CMG 12
4.3.1 Identificazione 13
4.3.2 Autenticazione 15
4.3.3 Certificato per l'identificazione e l'autenticazione in rete 16
4.3.4 Certificati e formati per la Firma Digitale 17
4.3.5 Certificati di autenticazione e crittografia 19
4.3.6 Interoperabilità con CIE e CNS 20
4.4 Informazioni presenti sulla CMG 21
4.4.1 Dati personali 21
4.4.2 Dati biometrici 21
4.4.3 Certificati digitali 21
4.4.4 PIN e PUK 22
4.5 Descrizione dell'organizzazione 22

4.6 Descrizione dei Ruoli ... 23
4.6.1 Responsabile Periferico del Servizio ... 23
4.6.2 Operatore Periferico ... 24
4.6.3 L'Amministratore ... 25
4.6.4 L'Amministratore Centrale ... 25
5 Procedure di acquisizione dati e rilascio ... 27
5.1 Acquisizione dei dati ... 27
5.1.1 Applicazione di acquisizione ... 27
5.1.2 Formato della fotografia ... 28
5.1.3 Acquisizione delle impronte digitali ... 28
5.1.4 Gestione dei casi di difformità fra i dati presenti nel data base del personale e i dati rilevati al momento dell'acquisizione ... 30
5.2 Emissione della CMG e suo rilascio ... 31
5.3 Gestione dei casi di doppia firma digitale ... 32
6 Procedure di revoca, sospensione, riattivazione ... 34
7 ALLEGATO 'A' – Formato Dati sulla CMG ... 37
7.1 Dati Personali Invariabili ... 38
7.2 Dati Personali Aggiuntivi ... 38
7.3 Dati Certificati Invariabili ... 39
7.4 Dati Biometrici Invariabili ... 39
8 ALLEGATO 'B' – Delega del Responsabile Amministrativo Periferico ... 40
8.1 Avvicendamento del Responsabile Amministrativo Periferico ... 40
8.2 Delega per svolgere i compiti del Responsabile Amministrativo Periferico ... 42
8.3 Nomina/Sostituzione dell'Operatore Periferico ... 43
9 ALLEGATO 'C' – Bozza Richiesta emissione/rinnovo CMG ... 44
10 ALLEGATO 'D' – Modulo riepilogativo dati per emissione CMG ... 45
11 ALLEGATO 'E' – Modulo ICAO di riferimento per il rilascio della Foto ... 46
12 ALLEGATO 'F' – Registro di Consegne CMG **Errore. Il segnalibro non è definito.**
13 ALLEGATO 'G-0' Bozza Richiesta di Sospensione/Revoca della CMG ... 50
14 ALLEGATO 'G-1' Bozza Richiesta di Sospensione/Revoca della CMG Interna all'Amministrazione ... 51
15 ALLEGATO 'H' – FAC SIMILE di una CMG ... 52
15.1 FRONTE della CMG ... 52
15.2 RETRO della CMG ... 52

1 Premessa

L'esigenza di incrementare il livello di sicurezza del sistema informativo della Giustizia attraverso l'adozione di misure di sicurezza a tutela dei dati e preservarli da accessi non autorizzati, ha imposto la necessità di implementare un Sistema di Accesso Sicuro e Biometrico ai sistemi informativi ed alle loro applicazioni. In particolare, per quanto concerne le modalità di autenticazione per l'accesso alle risorse informatiche ed agli applicativi "critici", è inderogabile nelle organizzazioni come i Tribunali penali, le Procure della Repubblica e le Direzioni Distrettuali Antimafia (DDA), dislocate sul territorio e distribuite geograficamente, l'utilizzo di strumenti di autenticazione informatica.

Tali sistemi devono verificare che l'utente sia abilitato ad accedere alle risorse di sistema ed ai dati, al fine di garantire il controllo delle informazioni che gli utenti possono utilizzare e dei programmi che essi possono eseguire. Mentre in passato tale protezione era demandata a meccanismi tradizionali "utente/password" facilmente aggirabili, la disponibilità di nuove e più affidabili tecnologie di riconoscimento ed autenticazione degli utenti, consente di ripensare le modalità con le quali è effettuato il logon alle risorse informatiche, al fine di rendere sempre più difficile l'utilizzo fraudolento degli strumenti informatici e l'accesso non autorizzato alle informazioni in essi contenute.

Il tradizionale processo di autenticazione basato su *Username* e *Password* può essere quindi sostituito da sistemi di autenticazione più robusti che ricorrono all'utilizzo delle tecnologie biometriche ed offrono sistemi di autenticazione più affidabili e sicuri, basati sulla autenticazione dell'utente abilitato all'accesso alle risorse tramite impronta digitale.

Il sistema più diffuso è basato sulla memorizzazione delle credenziali biometriche, sotto forma di template, su un dispositivo di memorizzazione sicuro (quale ad esempio una smartcard) consegnato al Titolare.

In fase di accesso al sistema, un applicativo di controllo accessi richiede all'utente di qualificare le proprie credenziali, leggendo la propria impronta digitale mediante un lettore fingerprint e confrontando il template dello stesso con quello precedentemente memorizzato sulla smartcard. In caso di coincidenza di template, si ha la garanzia dell'identità del Titolare e si prelevano dalla smartcard le credenziali utente per l'accesso al sistema.

L'autenticazione biometrica appena descritta consente quindi di stabilire in maniera certa l'identità del soggetto che sta richiedendo un determinato servizio informatico.

Nell'utilizzo di tecnologie biometriche per l'autenticazione dell'utente assume particolare rilevanza la segretezza nel trattamento dei dati di identificazione dell'individuo ed è per tale ragione che non si usa archiviare sulla smartcard l'immagine dell'impronta digitale, ma una sua rappresentazione numerica non reversibile, il template, che non consente di risalire al dato di partenza. Le informazioni biometriche vengono normalmente archiviate su una smartcard che è custodita direttamente dal Titolare e non conservate in basi dati centrali. Le postazioni di lavoro sono dotate di un dispositivo di lettura dell'impronta digitale e della smartcard e di un software in grado di consentire l'accesso alla postazione di lavoro solo dopo avere verificato con successo la corrispondenza tra impronta dell'utente richiedente l'accesso ed il template dell'impronta memorizzato sulla smartcard.

Le esigenze innanzi esposte sono alla base dei criteri ispiratori del presente progetto promosso dal Ministero della Giustizia.

Il Ministero ha riscontrato, infatti, la duplice esigenza di dotare il proprio personale di uno strumento di identificazione al contempo a vista ed elettronico. Per tale ragione, nello specifico ha deciso di attivare il progetto di **C**arta **M**ultiservizi della **G**iustizia (CMG), che si inquadra nel più ampio programma di iniziative intraprese dalla **P**ubblica

Amministrazione (PA), finalizzate a dotare il personale della PA di strumenti elettronici di identificazione sia fisica che logica.

Il progetto si propone in particolare di fornire una smartcard a tutto il personale delle sedi della Giustizia operanti nelle Regioni Obiettivo 1 che consenta sia l'identificazione fisica del Titolare che l'identificazione in rete.

Accanto alla distribuzione di un documento di identificazione a vista ed elettronico, l'Amministrazione Giustizia si propone di attivare una sperimentazione atta ad introdurre l'utilizzo di meccanismi di autenticazione degli utenti alle infrastrutture informatiche, basati su tecnologie biometriche.

Di seguito sono descritte le principali caratteristiche della CMG:

CMG come documento di riconoscimento	Permette di operare l'identificazione del possessore: • a vista, con i dati riportati sulla tessera stessa; • in modo elettronico, con i dati contenuti nel microchip (in questo caso è possibile verificarne l'autenticità); • in rete tramite certificato digitale. La CMG garantisce inoltre la piena e completa interoperabilità con la Carta d'Identità Elettronica (CIE) e la Carta Nazionale Servizi (CNS) che in futuro saranno utilizzate da tutti i cittadini. Le informazioni riportate sulla carta sono completate con il codice "International Civil Aviation Organization" (ICAO).
Impronte digitali	All'interno del microchip sono contenute le impronte digitali del Titolare sotto forma di template. La CMG può essere utilizzata per effettuare il riconoscimento biometrico del possessore.
Dati personali	Sulla tessera e nel microchip sono presenti i dati del possessore. In particolare, le informazioni di natura privata sono contenute esclusivamente sul microchip e sono accessibili solo digitando un

	PIN.
Certificati digitali	E' possibile memorizzare sulla carta più certificati digitali; nella prima fase saranno installati un certificato di autenticazione rilasciato dalla PKI interna all'Amministrazione Giustizia ed, eventualmente un certificato di autenticazione, ed uno di firma rilasciati da una Certification Authority a norma CNIPA.
Smartcard	La carta è di tipo multiapplicativo. Possiede le capacità crittografiche richieste per l'esecuzione delle operazioni di firma digitale e cifratura dei dati. Inoltre dispone di una memoria per le applicazioni pari a 32 Kb. Il chip ed il sistema operativo sono certificati Common Criteria EAL5+. Ciò realizza il livello più elevato di certificazione di sicurezza richiesto in Europa per le smartcard usate per la firma digitale.
Applicazioni	La CMG ospita, quale servizio qualificato, le informazioni necessarie a gestire un sistema di accesso sicuro alle applicazioni informatiche critiche dell'Amministrazione Giustizia ed alle risorse di rete sensibili. Per le postazioni che trattano informazioni particolarmente critiche, l'accesso viene eseguito mediante tecnologie biometriche.

Alla base dell'idea di una Carta Multiservizi per i dipendenti del Ministero della Giustizia (CMG), vi sono i concetti di interoperabilità (dei servizi primari) e diversificazione (delle funzioni ancillari). Come in tutte le Carte Multiservizi, il mezzo è in grado di offrire due categorie di servizi: la prima comune a tutte le Amministrazioni; la seconda che raccoglie le specificità proprie di ciascun Ente.

I servizi primari della CMG sono di seguito elencati:

- l'identificazione "a vista";

- l'identificazione "elettronica";
- l'identificazione "in rete";
- la firma digitale (elettronica avanzata).

Nella seconda categoria rientra il servizio di:

- controllo accessi per mezzo di tecniche biometriche

Per i primi due servizi elencati, come apparirà chiaro nel seguito del paragrafo, la compatibilità è estesa anche al circuito della Carta d'Identità Elettronica.

La CMG è il cardine univoco per l'adozione futura di numerose procedure informatiche atte ad automatizzare procedimenti funzionali omologhi (es. Gestione del Personale, Controllo Accessi fisici e logici, Gestione Logistica, ecc.). In tale contesto l'uniformità del contenitore dei dati, sia in termini di formato che di supporto fisico, consentirà una facile applicazione di procedure elettroniche sviluppate in ambito Giustizia a livello generalizzato, con conseguente risparmio in termini di investimento.

Pertanto, l'utilizzo di qualunque altra tipologia di carte dovrà essere considerato un'eccezione derivante da ben precise motivazioni.

2 Scopo della direttiva

La Carta Multiservizi della Giustizia è ormai una concreta realtà, anche nella considerazione che i programmi in esecuzione hanno consentito all'Amministrazione Giustizia di avviare l'Istituto Poligrafico e Zecca dello Stato alla realizzazione delle infrastrutture per la produzione delle carte e per la relativa distribuzione.

Appare ora necessario regolamentare l'impiego della CMG e, pertanto, il presente documento stabilisce i principi fondamentali di gestione con specifiche norme circa il ciclo di vita e l'impiego della carta medesima.

In considerazione della elevata velocità evolutiva dei sistemi informatici – e, fondamentalmente, la CMG è uno strumento informatico – la struttura della presente direttiva è stata concepita in modo da renderne semplici le prevedibili modifiche/innovazioni tecnologiche ovvero gli eventuali nuovi ambiti d'impiego.

Per quanto precede, oltre ad un corpo centrale concettuale, sono stati previsti alcuni allegati che definiscono nel particolare gli aspetti normativi e tecnologici.

Si è cercato, inoltre, di esplicare durante la trattazione il significato dei numerosi acronimi e/o definizioni ricorrenti.

3 Requisiti e distribuzione della Carta Multiservizi della Giustizia

3.1 Requisiti di base

Il progetto relativo alla Carta Multiservizi della Giustizia prevede che essa abbia una valenza giuridica sia "Interna"che "Esterna" all'Amministrazione della Giustizia.

In particolare, la carta potrà essere utilizzata a "vista" e in forma elettronica in modo che:

- assicuri una identità elettronica pienamente rispondente alle attuali normative di legge;
- Costituisca "Documento di Riconoscimento" (identità personale);
- contenga i dati biometrici;
- Costituisca una parziale interoperabilità a livello:
    - Nazionale, con la Carta d'Identità Elettronica (CIE);
- sia perfettamente interoperabile in ambito Giustizia.

3.2 Distribuzione

Per quanto precede, la Carta Multiservizi della Giustizia sarà distribuita a **tutti** gli appartenenti al comparto Giustizia **in servizio** secondo criteri analoghi al possesso dell'attuale Mod. AT.

La distribuzione avverrà da parte dell' "**I**stituto **P**oligrafico e **Z**ecca dello **S**tato (IPZS)".

3.3 Validità

La Carta Multiservizi della Giustizia ha la validità di cinque anni.

Non è previsto il rinnovo, alla scadenza sarà riemessa una nuova carta con i nuovi certificati.

Nel corso di validità, potrà essere riemessa in caso di:

- Variazione documentata del codice fiscale;
- Modifica sostanziale dei dati somatici/biometrici;
- Malfunzionamento della parte elettronica;
- Incongruenza dei dati memorizzati con quelli riportati a stampa;
- Estrema usura invalidante dei dati a stampa;
- Furto o Smarrimento.

Non danno adito a sostituzione i trasferimenti, le promozioni.

La stessa non sarà ritirata al personale transitato in quiescenza, per il quale è prevista soltanto l'invalidazione dei certificati di autentificazione. Al successivo rinnovo sarà emessa la versione cartacea.

4 Struttura e funzioni della CMG

4.1 Titolarità

Titolare della CMG è il personale amministrativo e di magistratura del Ministero della Giustizia

I centri logistici su base locale sono stati individuati con le diverse Sedi di Corte d'Appello presenti sul territorio.

4.2 Struttura

La Carta Multiservizi della Giustizia è, in sintesi, l'unione di tre strutture complesse:

- Un supporto in materiale sintetico con elevata resistenza all'usura e con caratteristiche di sicurezza produttiva quali microstampa, superficie olografica, etc che serve sia quale contenitore di informazioni "a vista" sia come supporto per la parte elettronica della carta;
- Un "chip elettronico" dotato di contatti elettrici nel quale risiede l'intelligenza della carta e dove vengono depositate le informazioni necessarie agli ulteriori usi della medesima.

La Carta Multiservizi della Giustizia è una carta elettronica del tipo "smart" ovvero dotata di una intelligenza interna che ne consente un impiego più articolato e complesso rispetto alle semplici carte passive o a memoria (es. Bancomat e Carte Abbonamento Trasporti). Si deve, tuttavia, sempre tenere presente che la carta elettronica è in ogni caso un "contenitore complesso" di informazioni e che qualunque impiego è strettamente correlato alle strutture esterne e alle procedure che interagiscono con la carta e ne sfruttano le sue capacità applicative.

4.3 Funzioni della CMG

La CMG, come indicato dal nome, è una carta *multiservizi*. Essa, peraltro, è anche una carta *multifunzione*. Ciò significa che un unico strumento è capace di erogare diverse

funzioni ciascuna delle quali può, a sua volta, essere utilizzata per creare molteplici servizi.

Ad esempio, la carta mette a disposizione la *funzione* di identificazione elettronica del Titolare; questa stessa funzionalità può essere utilizzata per un servizio di controllo accessi.

Per quanto detto, è dunque possibile precisare con maggior dettaglio solo le funzioni principali della CMG. Per quanto riguarda i servizi, essi non vengono qui esplicitati in quanto il numero complessivo e la natura degli stessi è passibile di variare col tempo.

Le funzioni principali della CMG sono di seguito elencate:

4.3.1 Identificazione

La CMG è in grado di identificare "a vista", cioè senza ausilio di strumenti elettronici di verifica. Tale procedura viene effettuata in modo identico alla identificazione tramite i documenti tradizionali di tipo cartaceo. Nel caso della CMG il legame tra i dati personali ed il dato biometrico (foto) che permette l'associazione visiva del Titolare, è costituito dal supporto plastico che possiede le opportune garanzie di non riproducibilità e anticontraffazione. Pertanto l'incaricato del controllo sarà in grado di:

- Verificare che la foto sulla carta corrisponda al viso del Titolare;
- Verificare che l'*overlay olografico* posto a protezione dei caratteri stampati sul supporto sia integro (l'ologramma recante la figura dell'Italia deve risultare non interrotto all'interno del supporto);
- Leggere i dati personali del Titolare stampati sul fronte e sul retro della carta.

La CMG è in grado anche di identificare per via "elettronica", grazie alle informazioni memorizzate all'interno del microcircuito. Questo secondo tipo di identificazione è indicato nei seguenti casi:

- Per verifiche di falso documentale, in quanto fornisce una prova inconfutabile che la carta è autentica e i dati non sono stati falsificati, senza richiedere all'esaminatore una particolare esperienza in questo tipo di controllo;
- In caso di uso della carta per procedure automatiche di controllo accessi, che generalmente sfruttano anche i dati biometrici (template di impronte digitali DX e SX);
- In tutti i casi ove la semplice verifica elettronica dell'identità sia sufficiente ad assolvere allo scopo.

La verifica può essere di tipo "**leggero**" o "**pesante**"; le procedure da seguire nei due casi sono descritte di seguito:

4.3.1.1 Verifica "leggera"

E' utile in molti casi, perché veloce (ad es., per segnalare la fruizione del pasto in una mensa).

Corrisponde ad una delle seguenti tipologie:

- lettura semplice dell'ATR (*Answer To Reset*) della carta;
- lettura del numero di serie della CMG;
- lettura semplice del file Dati Personali e/o dei template delle impronte digitali del Titolare.

L'ATR (*Answer To Reset*) della carta contiene le informazioni univoche che permettono di risalire tipo di carta (una CMG) e ad un numero di identificazione univoco del chip.

Il numero di serie proprio della CMG, dopo essere stato letto, può essere confrontato con quello stampato sul supporto.

I dati personali (inclusi i template delle impronte), una volta letti, possono essere utilizzati in procedure di vario tipo (es. per registrare il Titolare che ritira/restituisce una pratica).

4.3.1.2 Verifica "pesante"

E' raccomandata solo in casi molto particolari (es. verifica del falso documentale), in quanto molto più lenta ed onerosa. Aggiunge alla terza tipologia descritta al paragrafo precedente la verifica della firma digitale. Ciò consente di garantire in modo inconfutabile che la carta è autentica e che il dato non è stato falsificato (basta verificare che la firma è valida).

Va ricordato peraltro che sia l'ATR, che il numero di serie, che infine il file Dati Personali sono evidenze inalterabili (WRITE ONLY), quindi questo tipo di verifica, salvo il caso sopra ricordato, non è generalmente necessario.

4.3.2 Autenticazione

La funzione di autenticazione permette l'uso della CMG come strumento di accesso alla postazione di lavoro ed alle applicazioni appositamente predisposte.

La differenza tra la funzione di autenticazione e quella di identificazione elettronica, precedentemente descritta, consiste nella possibilità della prima di essere utilizzata da remoto (ossia in rete) garantendo l'identificazione certa della CMG. A differenza dell'identificazione elettronica, tuttavia, va tenuto presente che l'autenticazione non garantisce l'identità del Titolare, ma solo della carta. Ciò è dovuto al fatto che non risulta possibile verificare, da remoto, che il Titolare non abbia ad es. prestato la sua carta ad un altro soggetto, dandogli conoscenza anche del proprio codice di accesso (PIN).

La procedura di autenticazione richiede la presenza sulla carta della componente privata di una coppia di chiavi asimmetriche (RSA) (generate on-board durante la fase di personalizzazione) e di un certificato digitale di autenticazione.

4.3.3 Certificato per l'identificazione e l'autenticazione in rete

L'identificazione è il processo con cui l'utente si dichiara a un sistema o a un'applicazione, l'autenticazione è il processo che consente al sistema o all'applicazione di accertare l'identità dell'utente. Il protocollo SSL/TLS è garantito da una libreria di programmi che consentono di stabilire un canale di comunicazione tra Browser e WEB Server che può garantire:

- riservatezza del contenuto dei messaggi;
- integrità dei messaggi;
- mutua autenticazione delle parti coinvolte.

Tali caratteristiche vengono ottenute con i seguenti procedimenti:

- per la riservatezza ed integrità dei messaggi
  - il protocollo che prevede l'autenticazione tra server e client, può basarsi su diversi meccanismi (RSA, Fortezza, alcune versioni dell'algoritmo di Diffie-Hellman);
  - dopo l'iniziale fase di negoziazione della chiave di sessione, tutti i dati trasmessi sono crittografati, la crittografia è di tipo simmetrico;
  - la connessione garantisce l'integrità dei messaggi utilizzando funzioni di hash.

- per l'autenticazione delle parti:
  - SSL/TLS prevede l'uso di certificati digitali del tipo X509v3 e di coppie di chiavi asimmetriche utilizzate sia dal web server che dal browser e quindi si presta ad essere utilizzato con smart card crittografiche quali la Carta Nazionale dei Servizi (CNS) e la Carta di Identità Elettronica (CIE).

Il grosso vantaggio offerto da SSL/TLS con dei certificati X509v3 risiede nel fatto che web browser e web server sono già predisposti per utilizzare tale protocollo e quindi qualunque applicazione WEB può sfruttare le caratteristiche di sicurezza sopra esposte. Occorre solo configurare opportunamente le opzioni di sicurezza del browser e del web server. L'applicazione web, dopo la fase di autenticazione, può procedere a successive fasi di autorizzazione all'accesso ai servizi in funzione degli specifici diritti e privilegi

dell'utente. Per fare ciò ha la necessità di riconoscere l'utente estraendo lo "Username" e eventualmente altre informazioni dal certificato.

4.3.3.1 Configurazione del Client Internet Explorer

Se si dispone della CNS (o della CIE), il client potrà utilizzare la coppia di chiavi contenute nella carta a microprocessore.

Nel sistema operativo Windows, le funzioni di crittografia sono gestite dal modulo CSP (Cryptographic Service Provider). Quando le chiavi di cifratura sono memorizzate su smart card, il CSP deve essere in grado di interagire con quest'ultima. Sul sito del CNIPA sono descritte le linee guida (ver.3.0) mediante le quali, quest'ultimo rende disponibile i passi per configurare il software "IE" all'uso della CNS da parte dei cittadini e delle amministrazioni.

4.3.3.2 Configurazione di browser open source (Netscape, Mozzilla, ecc.)

I browser Netscape e Mozilla non utilizzano le funzioni del CSP ma interagiscono con le librerie della smart card in modalità PKCS #11. Anche in questo caso sul sito del CNIPA sono descritte le linee guida (ver 3.0) mediante le quali, quest'ultimo rende disponibile i passi per configurare browser diversi da IE all'uso della CNS da parte dei cittadini e delle amministrazioni.

4.3.4 Certificati e formati per la Firma Digitale

In accordo con quanto previsto dalla normativa vigente alla data del presente documento, il certificato di firma digitale per l'utilizzo di una smart card (come strumento di sottoscrizione di documenti elettronici) deve essere conforme allo standard RFC 2459 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (alla data sostituito da RFC 3280) e contenere almeno le seguenti informazioni:

- numero di serie del certificato di sottoscrizione;
- ragione o denominazione sociale del certificatore;
- codice identificativo del titolare presso il certificatore (campo subject del certificato = common name + description);

- nome cognome e data di nascita del titolare;
- valore della chiave pubblica;
- tipo di algoritmi di generazione e verifica della sottoscrizione del titolare;
- inizio e fine del periodo di validità della coppia di chiavi;
- tipo di algoritmo di sottoscrizione utilizzato dal certificatore;
- eventuali limitazioni nell'uso della coppia di chiavi.

In particolare il common name, (object ID = 2.5.4.3), ha la seguente struttura:
<cognome>/<nome>/<codice fiscale>/<identificativo titolare presso il certificatore>.
Il campo description (object ID = 2.5.4.13), ha la seguente struttura:

" C="<cognome esteso>"/ N="<nome esteso>"/ D="<data di nascita>["/ R="<ruolo titolare>]

Le estensioni necessariamente presenti nei certificati e quindi, secondo la specifica pubblica RFC 3280, sono:

- Authority Key Identifier: identifica la chiave pubblica corrispondente alla chiave privata utilizzata dal Certificatore per sottoscrivere il certificato;
- Subject Key Identifier: identifica certificati che contengono una particolare chiave pubblica;
- Key usage (estensione critica): indica l'uso delle chiavi (non repudiation);
- Certificate Policies: specifica la policy di riferimento del certificato ed il sito di distribuzione del manuale operativo;
- CrlDistributionPoint: contiene l'indirizzo che indica dove reperire la Certificate Revocation List che eventualmente conterrà le informazioni di revoca relative al certificato.

Questi certificati devono essere utilizzati per verificare la firma di documenti prodotti con la chiave privata a cui fanno riferimento. Il tentativo di usarli in un browser con il protocollo di mutua autenticazione SSL/TLS produrrebbe il rifiuto del certificato da

parte del browser, causato dal Key Usage che, essendo una estensione critica, è obbligatoriamente verificata.

Il formato dei dati e le buste crittografiche utilizzate per la firma digitale fanno riferimento ai seguenti standard:

- PKCS#1 (RSA Laboratories - RSA Cryptography Standard);
- PKCS#7 (RFC 2315).

PKCS#1 è lo standard di riferimento per la crittografia a chiave pubblica applicata, fra gli altri, alla Firma Digitale di documenti elettronici e per i processi di autenticazione e crittografia in rete Internet.

PKCS#7 è lo standard di riferimento per le buste crittografiche create per contenere la firma e il documento al quale si riferisce.

Le smart card conformi allo standard ISO 7816-8/9 (vedere paragrafo relativo agli standard di interoperabilità tra le carte) ammettono il formato PKCS#1 e, nei confronti delle operazioni di Digital Signature, si comportano nel seguente modo:

- controllano che l'oggetto chiave privata sia identificabile come chiave di firma digitale e non come chiave di autenticazione o di crittografia;
- se la precedente condizione è verificata forzano automaticamente il formato dei dati di firma secondo lo standard PKCS#1 descritto nella figura precedente.

Se si tentasse di utilizzare una chiave di autenticazione o di "encryption" con un comando di Segnature la smart card restituirebbe un codice di errore.

4.3.5 Certificati di autenticazione e crittografia

Sono di seguito rappresentate le caratteristiche salienti dei certificati di autenticazione e crittografia secondo lo standard X509v3, soprattutto per ciò che concerne le differenze con i certificati per la firma digitale. Le differenze salienti, cioè quelle che ne vincolano l'utilizzo, sono contenute nelle estensioni ed in particolare nel Key Usage e nello Extended Key Usage.

Sono previsti dallo standard X509v3 (RFC 3280) i seguenti key Usage Type:

digitalSignature (0),
nonRepudiation (1),
keyEncipherment (2),
dataEncipherment (3),
keyAgreement (4),
keyCertSign (5),
cRLSign (6),
encipherOnly (7),
decipherOnly (8)

Gli attributi precedenti (configurati a livello di template nella CA interna all'Amministrazione) permetteranno di utilizzare il certificato e la coppia di chiavi a cui esso si riferisce, nei seguenti ambienti:

- Browser WEB per l'autenticazione tramite il protocollo SSLv3;
- User Agent di posta elettronica per la produzione di e-mail cifrate e firmate elettronicamente secondo il formato standard S/MIME.

La componente Signature del Key Usage non è riferita alla Firma Digitale ma alla firma elettronica del formato S/MIME 2. Ricordiamo infatti che il Key Usage per la firma digitale è : **non repudiation**.

La Carta di Identità Elettronica e Carta Nazionale dei Servizi usano, per i processi di autenticazione in rete, un certificato con le caratteristiche sopra descritte.

4.3.6 Interoperabilità con CIE e CNS

La CMG assicura l'interoperabilità con la Carta d'Identità Elettronica e con la Carta Nazionale dei Servizi a livello delle informazioni di identificazione.

In particolare l'interoperabilità è garantita per il formato dei dati personali memorizzati sul chip delle carte; sarà possibile utilizzare gli stessi applicativi per leggere i dati personali delle diverse smart card.

I certificati di Autenticazione usati hanno caratteristiche diverse dovute alle applicazioni ad oggi esistenti nelle diverse organizzazioni; in alcuni casi, ad esempio, è richiesta la presenza del Codice Fiscale, Nome e Cognome (come attualmente presente nel Certificato di Autenticazione CMG) per il circuito di Acquisizione.

4.4 Informazioni presenti sulla CMG

I seguenti paragrafi descrivono i principali gruppi di informazioni presenti sulla CMG.

4.4.1 Dati personali

I dati personali presenti sulla CMG sono rappresentati nella tabella dell'Allegato 'A' dove è contenuta la struttura dei dati memorizzati nei rispettivi file sulla CMG, il formato degli stessi e la lunghezza.

4.4.2 Dati biometrici

I dati biometrici presenti sulla CMG sono costituiti dai template di due impronte digitali, una del dito indice della mano sinistra e una del dito indice della mano destra.

I template sono codici numerici che vengono derivati dall'immagine dell'impronta. Essi garantiscono la privacy del Titolare, in quanto da un template non è possibile risalire all'impronta.

4.4.3 Certificati digitali

Sulla CMG sono previsti 3 coppie di chiavi RSA a 1024 bit e 3 (tre) certificati digitali ad esse corrispondenti, di seguito elencati:

- Certificato di autenticazione/attestazione (estensioni previste: SSL AUTHENTICATION, NON REPUDIATION);
- Certificato di Smart Card Logon;
- Certificato di firma digitale.

4.4.4 PIN e PUK

Sulla CMG sono previsti due codici PIN:

- PIN/Biometria di firma digitale, per la sola operazione di firma digitale (a valore legale);
- PIN carta, per tutte le altre operazioni.

Sulla CMG è previsto un unico codice PUK, per lo sblocco di entrambi i codici PIN precedentemente descritti.

4.5 Descrizione dell'organizzazione

La Carta multiservizi, sostituisce il modello AT cartaceo attualmente in uso per i dipendenti della Giustizia, in ragione di ciò l'attività di acquisizione dei dati anagrafici e biometrici dei dipendenti ricalcherà le strutture ed i processi organizzativi previsti ed attuati per il rilascio delle AT cartacee.

I centri preposti alla raccolta dei dati saranno le Sedi di corte d'Appello situate presso i Capoluoghi di Provincia delle singole Regioni.

Gli Uffici incaricati della realizzazione della procedura sanno i medesimi attualmente investiti dello stesso ruolo e rappresentano una sorta di **l'UFFICIO DELEGATO presso la Corte d'Appello** , che avrà il compito di seguire le procedure di Acquisizione dati dei dipendenti, rilascio delle smart card (CMG) ed infine gestire i casi di Sospensione, Revoca e Ri-emissione della Carta.

A tal fine si evidenzia che il software SEC consente, oltre che eseguire la mera procedura di acquisizione, anche la gestione dello storico con particolare riferimento ai casi di scadenza, revoca o ri-emissione.

Si identificano le seguenti figure:

- **il Responsabile Periferico del Servizio**
- **L'Operatore Periferico**
- **L'Amministratore**

- **Amministratore Centrale**

4.6 Descrizione dei Ruoli

4.6.1 Responsabile Periferico del Servizio

Questa figura si identifica con il Funzionario dell'Ufficio periferico, nominato dal Presidente della Corte d'Appello o dal Dirigente, quale Responsabile del progetto ed ha il compito sia di approvare le richieste di emissione delle CMG, sia di garantire l'autenticità dei dati acquisiti.

Egli valida l'attività degli operatori incaricati dell'acquisizione dei dati ed interagisce con l'Istituto Poligrafico e Zecca dello Stato (IPZS). In particolare verificherà che le procedure di riconoscimento dell'identità del dipendente siano effettuate secondo quanto previsto dalla normativa e firmerà digitalmente i dati acquisiti attraverso l'applicativo SEC (Sistema di Emissione Carte). E' il Responsabile anche del trattamento dei dati personali in riferimento all'attuazione di quanto previsto dalla normativa sulla Privacy.

E' previsto il caso di delega delle funzioni ad un altro funzionario previa autorizzazione del Presidente della Corte o del Dirigente e comunicazione all'Ufficio I del Capo Dipartimento (fax. 06/68620511).

La comunicazione dovrà contenere almeno le seguenti informazioni (vedere Allegato 'B'):

- Identificazione certa del delegante (citando l'identificativo della CMG, Cognome, Nome, Codice Fiscale);
- il motivo della delega;
- Individuazione certa del delegato (citando l'identificativo della CMG, Cognome, Nome, Codice Fiscale).

Poiché la delega delle funzioni prevede la richiesta di emissione di una smart card con Firma Digitale da utilizzare nella procedura di acquisizione dei dati, occorrerà

provvedere anche alla suddetta richiesta direttamente alla Società Postecom previa compilazione della documentazione prevista per il rilascio.

L'istituto della delega dovrà ritenersi straordinario e da utilizzare solo in casi di sostituzione definitiva del Responsabile.

Il Responsabile Periferico è il responsabile dell'Emissione delle CMG, il responsabile delle variazioni dei dati e dei certificati delle CMG dei dipendenti appartenenti al proprio distretto di Corte d'Appello che si avvalgono del suo centro di Certificazione.

4.6.2 Operatore Periferico

Questa figura s'identifica con il dipendente, funzionario e non, che svolge i seguenti compiti:

- ✓ interagisce con l'utente destinatario della carta;
- ✓ verifica i documenti identificativi ed i dati personali del richiedente;
- ✓ richiede la sottoscrizione dell'informativa sulla Privacy;
- ✓ esegue l'inserimento dei template dell'impronte, la fotografia e la firma;
- ✓ ed infine, sottoporrà, nei soli casi previsti (tutti i magistrati e dipendenti dal grado funzionale più elevato fino al livello B3), la firma del modulo in doppia copia relativo al rilascio della firma digitale. Una copia di detto modulo sarà consegnata all'utente, l'altra sarà inviata via fax, al responsabile della Registrazione della C.A. (Fax 0659585028, fax. 0659585049), e successivamente imbustata, unitamente al modulo di identificazione SEC, ed inviato alla Società :

  Postecom S.p.A.
  Certification Authority - Registrazione
  V.le Europa, 175 - 00144 Roma

L'Operatore è la figura dell'Ufficio Periferico che ha il compito di acquisire i dati Personali, Amministrativi e Sensibili (Foto, Firma, Impronte Digitali) del personale cui deve essere rilasciata la CMG.

Per portare a termine questa attività L'Operatore utilizza la procedura SEC che funziona sulla **rete giustizia** ed acquisisce i dati dal Database PRE ORG del Ministero e li completa con un processo di inserimento dati.

L'Operatore è il responsabile della corretta acquisizione dei dati del dipendente a cui rilasciare la CMG.

4.6.3 L'Amministratore

Si identifica con il dipendente, esperto informatico, nominato come referente tecnico dal Dirigente CISIA competente per distretto. Cura gli aspetti squisitamente tecnici e può assegnare, all'interno del Sistema di Emissione Carte (SEC) i ruoli di Responsabile o Operatore ad uno qualsiasi dei dipendenti già presenti nel database.

Sarà cura dell'Amministratore analizzare e risolvere le problematiche di tipo tecnico legate al funzionamento del Sistema di Emissione Carte (SEC) che dovessero presentarsi.

4.6.4 L'Amministratore Centrale

E' la figura che, a livello centrale, cura gli aspetti tecnico-organizzativi del processo di Emissione Carte nel suo insieme. Ha visibilità massima su tutto il Sistema, può assegnare i ruoli di Responsabile o Operatore, esegue la procedura di sincronizzazione dei dati fra il Sistema SEC ed il data base PreOrg ed, infine, può validare/invalidare l'invio dei dati all'Istituto Poligrafico.

Rappresenta l'interfaccia, per ciò che concerne i processi organizzativi attinenti al progetto, fra i Responsabili Periferici Amministrativi e l'Amministrazione Centrale.

RUOLO	MASSIMA VISIBILITÀ	ALLINEAMENTO DB - PreOrg	GESTIONE RUOLI	INVIO IPZS E INVALIDA
Responsabile Amministrativo Periferico	Distretto/Circ	NO	NO	SI (solo interni al distretto)
Operatore Periferico	Distretto/Circ	NO	NO	NO

Amministratore	Distretto	NO	SI (solo interni al distretto)	SI (solo interni al distretto)
Amministratore Centrale	Territorio	SI	SI	SI

5 Procedure di acquisizione dati e rilascio

5.1 Acquisizione dei dati

La procedura acquisizione dei dati, il cosiddetto ***enrollment***, avviene attraverso un processo di identificazione ed autenticazione del richiedente presso gli uffici periferici secondo le seguenti modalità:

- L'Operatore effettua l'identificazione del dipendente secondo le vigenti disposizioni di legge. L'operazione viene svolta presso l'Ufficio di Corte d'Appello di appartenenza del Titolare della carta e prevede l'acquisizione dei dati personali, delle impronte e della foto. Inoltre l'operatore fa firmare al dipendente il modulo di identificazione (Allegato 'D') che egli stesso controfirma;
- il Responsabile Periferico del Servizio è il responsabile della richiesta di rilascio delle CMG ed ha il compito di validare i dati, firmarli digitalmente ed inviarli all'ente emettitore, Istituto Poligrafico e Zecca dello Stato.

5.1.1 Applicazione di acquisizione

Di seguito la sequenza delle operazioni necessarie per la predisposizione dei dati per l'emissione di una CMG (Emissione ed Approvazione Dati):

1. L'Operatore entra sul portale di acquisizione SEC (Sistema Emissione Carte) inserendo i suoi dati identificativi (Utente, Sede e Password);
2. Il Dipendente da acquisire comunica i dati Personali e Amministrativi e fornisce in visione un suo documento di identità;
3. L'Operatore scatta la foto;
4. Il Dipendente rilascia le impronte digitali e la firma;

Successivamente:

1. Il Responsabile Periferico dal Servizio, Firma Digitalmente con la propria CMG i dati appena acquisiti;

2. Attraverso la Firma Digitale, automaticamente, la procedura trasmette le informazioni al Database di Acquisizione dei dati;
3. Il Responsabile Periferico accede al portale di Acquisizione e visualizza le acquisizioni effettuate o le scarica sul proprio computer;
4. Il Responsabile Periferico procede con l'approvazione o il rifiuto delle acquisizioni effettuate o direttamente dal portale o con la procedura in locale;
5. Una procedura richiede per il dipendente i certificati alla CA interna;
6. Vengono inviati i dati su canale sicuro ad IPZS.

5.1.2 Formato della fotografia

Il formato della Fotografia è standard ICAO ed eredita tutte le caratteristiche stabilite per la Carta d'Identità Elettronica.

La fotografia da acquisire deve essere fatta in modo che le condizioni di luminosità e contrasto dell'immagine siano sufficienti per un riconoscimento a vista. L'inquadratura deve mostrare in modo evidente le caratteristiche del volto.

Lo sfondo che deve essere predisposto per l'inquadratura della foto è celeste opaco.

Per la tipologia di luminosità e caratteristiche generali si rimanda al documento ICAO (Allegato 'E').

5.1.3 Acquisizione delle impronte digitali

L'acquisizione dell'impronta non è facoltativa, ma obbligatoria per tutti coloro che richiederanno la CMG elettronica.

Sarà cura del l'Operatore, chiarire al dipendente che l'impronta non sarà conservata, ma distrutta subito dopo l'emissione della carta e che l'operazione in corso non consente in alcun modo di poter rintracciare l'impronta associandola poi alla persona.

Il rilascio delle impronte digitali avviene attraverso 2 dita; indice della mano destra e indice della mano sinistra. Dove non fosse possibile rilasciare l'impronta di un dito per ciascuna mano è possibile rilasciare l'impronta di due dita differenti della stessa mano. Per questo motivo l'applicativo che permette l'acquisizione delle impronte digitali richiede l'acquisizione delle: "Prima Impronta" e "Seconda Impronta".

Il rilascio delle impronte digitali DEVE avvenire secondo la seguente modalità:

- **Prima Impronta**: INDICE della mano sinistra (se non disponibile procedere con il medio, anulare, mignolo quindi il pollice). SOLO nel caso in cui non sia possibile acquisire un dito della mano sinistra procedere con l'INDICE della mano destra (se non disponibile procedere con il medio, anulare, mignolo quindi il pollice);
- **Seconda Impronta**: INDICE della mano destra (se non disponibile o già acquisito procedere con il medio, anulare, mignolo quindi il pollice, scegliendo comunque un dito non acquisito ancora). SOLO nel caso in cui non sia possibile acquisire un dito della mano destra procedere con l'INDICE della mano sinistra (se non disponibile o già acquisito procedere con il medio, anulare, mignolo quindi il pollice, scegliendo comunque un dito non acquisito ancora).

Operativamente il processo di rilascio delle impronte digitali **deve avvenire** secondo i seguenti passi:

- Far posizionare il primo dito sul lettore;
- Far sollevare il dito dal lettore;
- Verificare l'impronta acquisita riposizionando lo stesso dito sul lettore (per 2 volte);
- Far posizionare il secondo dito sul lettore;
- Far sollevare il dito dal lettore;
- Verificare l'impronta acquisita riposizionando lo stesso dito sul lettore (per 2 volte);
- Salvare.

Il processo di acquisizione e verifica deve essere fatto facendo sollevare il dito al dipendente in questione; se questo non avviene l'impronta che verrà memorizzata potrebbe non essere di qualità accettabile per un corretto riconoscimento quando necessario.

Si sottolinea l'importanza della fase di verifica dell'impronta, in quanto se essa non viene portata a termine con cura, la carta potrebbe creare problemi durante l'uso ad esempio in un'applicazione di controllo accessi.

5.1.4 Gestione dei casi di difformità fra i dati presenti nel data base del personale e i dati rilevati al momento dell'acquisizione

E' possibile ipotizzare 2 tipologie di difformità fra i dati presenti nel data base del personale dell'Amministrazione PREORG e quelli rilevati/dichiarati al momento della procedura di acquisizione.

1) Difformità dei dati "FORTI"

Si intendono per dati forti tutti quei dati che contribuiscono alla formazione del Codice Fiscale e cioè: NOME, COGNOME, DATA e COMUNE di NASCITA, SESSO, oltre allo stesso CODICE FISCALE e la QUALIFICA, LOCALITÀ DI SERVIZIO e UFFICIO DI SERVIZIO.

Qualora l'Operatore Periferico rilevi una difformità tra i dati presenti nel data base del SEC (Sistema Emissione Carte) ed uno qualsiasi dei dati forti sopra elencati, **interrompe la procedura di acquisizione**, acquisisce una fotocopia del documento di identità dell'interessato e provvede ad inoltrare comunicazione, prodotta direttamente dal sistema SEC, all'Ufficio I del Capo Dipartimento. Fax 06 68853127 Specificando la natura del documento.

Il suddetto Ufficio provvederà ad interessare gli Uffici competenti del Ministero per avviare la modifica dei dati sui diversi Registri e sul data base del personale PRE ORG.

Il Funzionario incaricato del PRE ORG comunicherà l'avvenuta modifica sia al Responsabile Periferico del Servizio sia al responsabile del Sistema di Active Directoty nazionale deputato al rilascio dei certificati di autenticazione in rete.

Solo in seguito alla "REGOLARIZZAZIONE" dei dati anagrafici sarà possibile riavviare la procedura di acquisizione per l'emissione della CMG.

Resta inteso che non sarà possibile emettere la Smart Card a coloro che permangono in situazioni di irregolarità.

2) Difformità dei dati "DEBOLI"

Si intendono per dati "DEBOLI" tutti quei dati presenti nella maschera di acquisizione dati SEC che non appartengono alla lista dei dati Forti e cioè: STATO CIVILE, INDIRIZZO DI RESIDENZA, CITTADINANZA, STATURA, COLORE OCCHI, COLORE CAPELLI E SEGNI PARTICOLARI.

Qualora l'Operatore Periferico rilevi una difformità tra i dati presenti nel data base ed uno qualsiasi dei dati DEBOLI sopra elencati, **procede nella procedura di acquisizione** ed effettua la registrazione dei dati comunicati sul sistema SEC .

Eseguirà in seguito le medesime procedure previste per il normale rilascio della CMG.

Il Sistema di Emissione Carte metterà a disposizione del data base di PRE ORG delle "VISTE" con l'elenco delle variazioni effettuate al fine di consentirne l'aggiornamento.

5.2 Emissione della CMG e suo rilascio

La CMG viene emessa dall' Istituto Poligrafico e Zecca dello Stato e contiene oltre il layout, anche elementi che la rendono non replicabile; in particolare viene impresso con una tecnologia di laser engraving l'identificativo progressivo della carta.

L' Istituto Poligrafico e Zecca dello Stato è responsabile della personalizzazione elettrica (chip) e grafica (layout) della CMG.

Fasi:

1. L' Istituto Poligrafico e Zecca dello Stato riceve per via informatica i dati crittografati dei dipendenti per i quali è stata effettuata la procedura di acquisizione;
2. L' Istituto Poligrafico e Zecca dello Stato installa a bordo della CMG i certificati previsti, inserisce i dati personali nel chip e personalizza la carta graficamente;
3. Avvia l'emissione, comunicando al Sistema di Emissione Carte le diverse fasi di produzione della carta;
4. L' Istituto Poligrafico e Zecca dello Stato provvede quindi alla spedizione delle Carte emesse alle relative Corti d'Appello tramite furgone blindato e scorta. Invierà le buste contenenti i codici di blocco e sblocco della carta, PIN e PUK, direttamente all'Ufficio di appartenenza del dipendente dichiarato al momento dell'acquisizione dei dati;
5. Il Responsabile Periferico Amministrativo riceve in consegna le CMG che dovrà successivamente consegnare al Titolare previa attenta identificazione;
6. Il Titolare ritira la carta e verifica che i dati riportati sulla CMG corrispondano ai suoi, mentre ritirerà presso il suo Ufficio di appartenenza la busta chiusa contenente i codici di sblocco;
7. Il Responsabile Periferico tiene traccia delle operazioni fatte con un registro di consegne sul sistema SEC

5.3 Gestione dei casi di doppia firma digitale

Molti Funzionari dell'Amministrazione della Giustizia possiedono ed utilizzano da diversi anni smart card contenenti i certificati di firma digitale. La distribuzione della CMG comporterà, in alcuni casi, la duplicazione del servizio in quanto il dipendente si

troverà ad avere la precedente smart card di firma e l'attuale CMG contenete anch'essa un ulteriore certificato di firma.

In questi casi è prevista l'attivazione della procedura di revoca della smart card di firma digitale già in possesso, secondo procedure note ai possessori, per favorire l'utilizzo di un'unica Carta Multiservizi della Giustizia.

6 Procedure di revoca, sospensione, riattivazione

Di seguito alcune linee guida per attivare la procedura di Revoca:

- La carta CMG, in quanto Carta Multiservizi del Ministero della Giustizia, deve essere oggetto della massima attenzione da parte del titolare nella cura e nella conservazione della stessa, per questo motivo, l'attività di sospensione e/o riattivazione della stessa non è permessa, l'unica attività possibile è la sua riemissione.

- Il processo di Revoca dei certificati non inficia la validità della carta, che continua nella sua funzione di riconoscimento del titolare (a "vista"). La revoca di uno dei certificati "interni" presenti sulla carta (Autenticazione SSL e/o SmartCard-Logon), o esterni (certificato di Firma Digitale), annulla l'efficacia della carta che dovrà essere riemessa con nuovi certificati. Pertanto la procedura di revoca è da riferirsi alla validità dei certificati ivi contenuti e sono di stretta competenza del circuito d'emissione che si attiva, generalmente, su segnalazione delle autorità competenti.

- Per iniziare la fase di revoca, il Titolare dovrà recarsi presso l'Ufficio del Responsabile Amministrativo Periferico, esibire un documento d'identità valido, consegnare copia dell'eventuale documentazione a giustificazione della richiesta, e compilare, sottoscrivere e consegnare al Responsabile il modulo di richiesta di revoca.
- Il Processo di Revoca può essere di due tipi:
  - Revoca di un Certificato della CMG
  - Revoca della Carta

Revoca di un Certificato della CMG

Un Certificato si può revocare per uno dei seguenti motivi:

- compromissione o sospetta compromissione della relativa chiave privata;

- cambio di almeno uno dei dati pubblicati nel certificato o dati errati;
- il titolare ha violato apertamente i suoi obblighi relativi alla titolarità del certificato;
- furto, smarrimento o distruzione del dispositivo che contiene la relativa chiave privata (CMG).

Casi previsti per la revoca di un Certificato:

(a) Revoca del Certificato di Firma Digitale

- In questo caso la CMG continua a valere come documento di identificazione e/o autenticazione, mentre vengono rese non valide le operazioni di firma e/o cifra.
- Per effettuare il rinnovo del certificato il titolare deve far richiesta di una nuova carta al Responsabile Amministrativo Periferico.

(b) Revoca del Certificato di Autenticazione SSL e/o SmartCard Logon

- In questo caso la CMG continua a valere come documento di identificazione, mentre vengono rese non valide le operazioni di autenticazione (Dominio ed SSL).
- Per effettuare il rinnovo del certificato il titolare deve far richiesta di una nuova carta al Responsabile Amministrativo Periferico.

Revoca della Carta CMG

La revoca può essere richiesta dal Titolare o dal Responsabile Amministrativo Periferico e comporta sempre e comunque la "distruzione" del supporto.

Casi previsti per la revoca della carta CMG:

(a) Revoca su richiesta del Titolare o del Responsabile Periferico

- Per compromissione o sospetta compromissione della CMG;

- Per compromissione o sospetta compromissione del certificato di autenticazione;
- Per scadenza della CMG;
- Per dati non variabili errati (ad es. il codice fiscale, il cognome, il nome, etc);
- Per violazione degli obblighi relativi alla titolarità della CMG (ad esempio cessione della CMG);
- Per smarrimento o distruzione dei codici PIN/PUK;
- Per furto, smarrimento o distruzione della CMG, in tal caso il possessore dovrà svolgere regolare denuncia presso le autorità competenti (Polizia, Carabinieri).

(b) Revoca su iniziativa del Responsabile Amministrativo Periferico:

- oltre che per i motivi elencati al paragrafo precedente;
- errato funzionamento del processo d'emissione della CMG;
- sospetto o certezza di compromissione della chiave privata della CA interna all'Amministrazione;
- cessazione d'attività di CA.

- La revoca prevede che il Responsabile Amministrativo Periferico:
  1- distrugga il supporto materiale (CMG);
  2- aggiorni il sistema SEC con il nuovo status della carta;
  3- ne dia comunicazione al Certificatore Postecom per quanto attiene alla revoca dei certificati di Firma Digitale ed tramite la procedura di revoca.
  4- inoltrare immediatamente via fax, al Responsabile della Registrazione della C.A. (fax n. 0659585028 oppure 0659585049), la richiesta di revoca e la relativa documentazione, anticipandola telefonicamente al numero 0659582098 l'inoltro del fax.
- Si ricorda che il **Processo di Revoca,** comporta la riemissione della CMG.

7 ALLEGATO ‘A’ – Formato Dati sulla CMG

Contiene i dati dell’utente. Alcuni campi sono opzionali nelle specifiche CNS, come indicato dalla colonna (M(obbligatorio)/O(opzionale)/V(vuoto)).

7.1 Dati Personali Invariabili

Dato	Codifica	M/O/V	Dimensione Max	Descrizione
Emettitore	ASCII	M	4	Codice derivante dai seriali standard; Es. per il Min. Giustizia "6905"
Data di emissione del documento	ASCII	M	8	Formato GGMMAAAA
Data di scadenza del documento	ASCII	M	8	Formato GGMMAAAA
Cognome	ASCII	M	26	
Nome	ASCII	M	26	
Data di Nascita	ASCII	M	8	Formato GGMMAAAA
Sesso	ASCII	M	1	'M' per maschio, 'F' per femmina
Codice fiscale	ASCII	M	16	
Comune di Nascita	ASCII	M	4	
Comune di residenza al momento dell'emissione	ASCII	M	4	
Qualifica	ASCII			
Ufficio d'Appartenenza	ASCII			

7.2 Dati Personali Aggiuntivi

Dato	Codifica	M/O/V	Dimensione Max	Descrizione
Statura (cm)	ASCII	O	3	Presente per compatibilità CIE
Occhi (colore)	ASCII	O	Tbd	
Capelli (colore)	ASCII	O	Tbd	
Indirizzo di residenza	ASCII	O	80	
Eventuale annotazione in caso di non validità del documento per l'espatrio	ASCII	V	Tbd	Presente per compatibilità CIE
Porto d'Armi	ASCII	V	2	
Immagine Firma	tbd	O	Tbd	

7.3 Dati Certificati Invariabili

Dato	Codifica	M/O/V	Dimensione Max	Descrizione
Certificato di Smart Card Logon		M	NA	
Certificato di Autenticazione SSL		M	NA	Presente per compatibilità CNS
Certificato Firma Digitale		O	NA	

7.4 Dati Biometrici Invariabili

Dato	Codifica	M/O/V	Dimensione Max	Descrizione
Template impronta Dx e SX		M	NA	

8 ALLEGATO 'B' – Delega del Responsabile Amministrativo Periferico

8.1 Avvicendamento del Responsabile Amministrativo Periferico

Oggetto: COMUNICAZIONE DI CESSAZIONE/ASSUNZIONE

Data

_____

UFFICIO: _____

Cognome RESPONSABILE PERIFERICO CEDENTE:_____

Nome RESPONSABILE PERIFERICO CEDENTE: _____

CODICE FISCALE RESPONSABILE PERIFERICO CEDENTE:_____

ID DELLA CMG RESPONSABILE PERIFERICO CEDENTE:_____

Cognome RESPONSABILE PERIFERICO SUBENTRANTE:_____

Nome RESPONSABILE PERIFERICO SUBENTRANTE:_____

CODICE FISCALE RESPONSABILE PERIFERICO SUBENTRANTE:_____

ID DELLA CMG RESPONSABILE PERIFERICO SUBENTRANTE:_____

Firma Autografa/Digitale Responsabile Periferico (Cedente/Subentrante)

8.2 Delega per svolgere i compiti del Responsabile Amministrativo Periferico

Oggetto: RICHIESTA DI DELEGA per lo svolgimento TEMPORANEO dei compiti di Responsabile Amministrativo Periferico.

Data

_____

UFFICIO: _____

Cognome RESPONSABILE PERIFERICO TITOLARE:_____

Nome RESPONSABILE PERIFERICO TITOLARE: _____

CODICE FISCALE RESPONSABILE PERIFERICO:_____

ID DELLA CMG RESPONSABILE PERIFERICO :_____

Cognome RESPONSABILE PERIFERICO DELEGATO:_____

Nome RESPONSABILE PERIFERICO DELEGATO:_____

CODICE FISCALE RESPONSABILE PERIFERICO DELEGATO:_____

ID DELLA CMG RESPONSABILE PERIFERICO DELEGATO:_____

Firma Autografa/Digitale Responsabile Periferico

8.3 Nomina/Sostituzione dell'Operatore Periferico

Oggetto: NOMINA/SOSTITUZIONE dell'Operatore Periferico

Data

_____

UFFICIO: _____

Cognome RESPONSABILE PERIFERICO:_____

Nome RESPONSABILE PERIFERICO: _____

CODICE FISCALE RESPONSABILE PERIFERICO:_____

ID DELLA CMG RESPONSABILE PERIFERICO :_____

Elenco degli Operatori

Qualifica	Nome Cognome	N° CMG	Codice Fiscale

Firma Autografa/Digitale Responsabile Periferico

9 ALLEGATO 'C' – Bozza Richiesta emissione/rinnovo CMG

Data

_____

Il sottoscritto _____

Qualifica Cognome e Nome

Chiede (barrare la casella relativa) :

☐ Emissione della CMG

☐ Rinnovo della CMG

Codice fiscale del richiedente:

Firma Richiedente

_____

Firma Responsabile Periferico

_____

10 ALLEGATO 'D' – Modulo riepilogativo dati per emissione CMG

Richiesta TESSERA DI RICONOSCIMENTO
MODELLO AT

Ministero della Giustizia

IL/ La sottoscritto/a: SALINI SXOBRINXO
in attività di servizio presso:
TRIBUNALE PER I MINORENNI 2
con figura professionale/qualifica:
105 - A1

CHIEDE CHE VENGA RILASCIATA LA TESSERA DI RICONOSCIMENTO – MODELLO AT

A SE MEDESIMO
nato a: AUSTRALIA (EE) il: 01 Ago 1959
residente in: ROMA (RM)
indirizzo: Via ponte Lungo
cittadinanza: IT
sesso: F stato civile:
statura: 180 capelli: castani occhi: marroni
segni particolari:
Esiste provvedimento di separazione legale o consensuale: NO
Acconsente affinché la tessera sia resa valida per l'espatrio: NO
Porto d'armi senza permesso: NO

Il sottoscritto dichiara, sotto la propria responsabilità:

- di non trovarsi in alcuna delle condizioni ostative al rilascio del passaporto o documento equipollente, di cui all'art. 3 lettere b, d, e, g, della legge 1185/67
- di essere a conoscenza delle disposizioni dettate dal D.P.R. n. 649 del 6/8/1974 *"Disciplina dell'uso della carta di identità e degli altri documenti equipollenti al passaporto ai fini dell'espatrio"*
- che i dati trascritti rispondono a verità e di essere a conoscenza delle sanzioni penali previste dalla normativa vigente per le dichiarazioni mendaci
- che la fotografia allegata è la propria

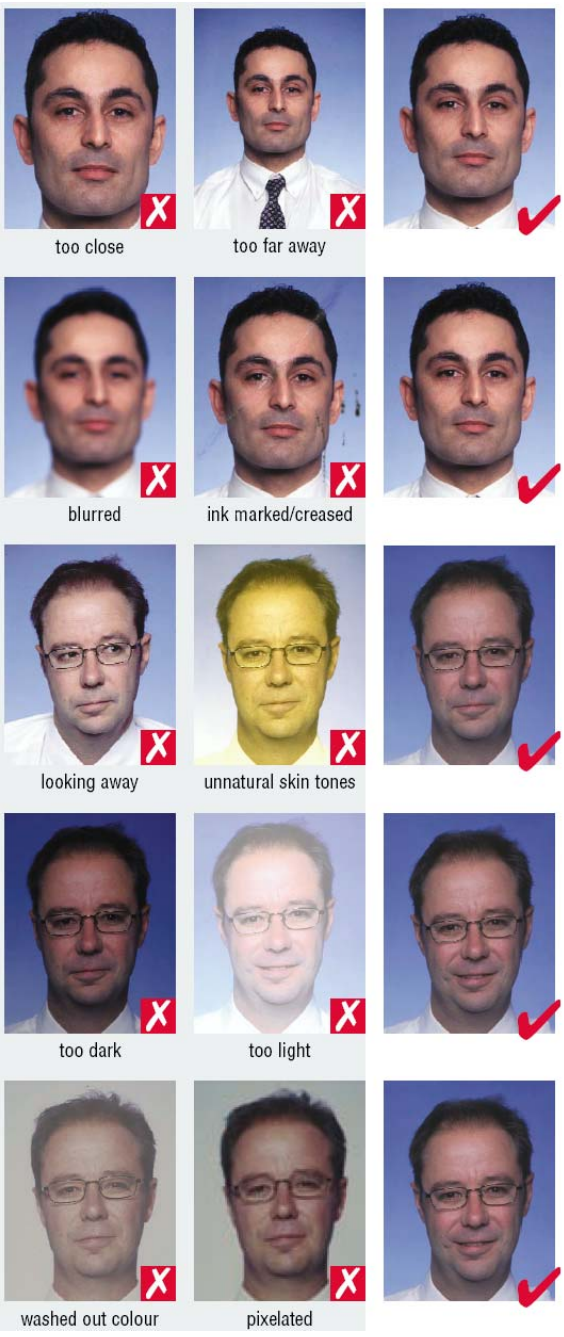
Data 20 Nov 2006

(firma del richiedente)

(firma dell'operatore)

11 ALLEGATO ‘E’ – Modulo ICAO di riferimento per il rilascio della Foto

Di seguito vengono riportate le caratteristiche che deve avere la foto per rispettare le norme internazionali ICAO (senza considerare le dimensioni che per il caso della CMG sono 320x240 e il fatto che la foto è acquisita all’istante)



Photograph quality

The photographs must be:

- close up of your head and top of your shoulders so that your face takes up 70–80% of the photograph
- in sharp focus and clear
- of high quality with no ink marks or creases

The photographs must:

- show you looking directly at the camera
- show your skin tones naturally
- have appropriate brightness and contrast
- be printed on high quality paper, and at high resolution

Photographs taken with a digital camera must be high quality colour and printed on photo-quality paper.

Style and lighting

The photographs must:

- be colour neutral
- show your eyes open and clearly visible—no hair across your eyes
- show you facing square on to the camera, not looking over one shoulder (portrait style) or tilted, and showing both edges of your face clearly
- be taken with a plain light-coloured background
- be taken with uniform lighting and not show shadows or flash reflections on your face and no red eye

Glasses and head covers

If you wear glasses:

- the photograph must show your eyes clearly with no flash reflection off the glasses, and no tinted lenses (if possible, avoid heavy frames—wear lighter framed glasses if you have them)
- make sure that the frames do not cover any part of your eyes.

Head coverings:

- are not permitted except for religious reasons, but your facial features from bottom of chin to top of forehead and both edges of your face must be clearly shown.

Expression and frame

Your photographs must:

- show you alone (no chair backs, toys or other people visible), looking at the camera with a neutral expression and your mouth closed.

12 ALLEGATO ‘G-0’ Bozza Richiesta di Sospensione/Revoca della CMG

DATI PERSONALI DEL RICHIEDENTE

Cognome ..... Nome .....

Codice Fiscale ..... Sesso ❑ M ❑ F

Nato a ..... Provincia ..... Nazione ..... il .....

Residente in .....

C.A.P. ..... Comune ..... Provincia .....

Documento ..... n° .....

Rilasciato da ..... il .....

DATI DEL TITOLARE PER CUI SI INTENDE EFFETTUARE LA RICHIESTA

Cognome ..... Nome .....

Codice Fiscale ..... Codice identificativo univoco del titolare .....

TIPOLOGIA DI RICHIESTA

Il richiedente in qualità di ❑ Titolare ❑ Terzo interessato ❑ Referente

❑ chiede la REVOCA del certificato/i sopra descritto a far data dal ..... / ..... / 20.....
(la decorrenza deve coincidere con un giorno feriale)

❑ chiede la SOSPENSIONE del certificato/i sopra descritto a far data dal ..... / ..... / 20..... e fino a tutto il ..... / ..... / 20.....
(la decorrenza deve coincidere con un giorno feriale)

❑ chiede la RIATTIVAZIONE del certificato/i sopra descritto a far data dal ..... / ..... / 20.....
(la decorrenza deve coincidere con un giorno feriale) e allega la ricevuta di pagamento di 20 euro sul conto corrente postale n° 13892211 intestato a Postecom SpA

con le seguenti motivazioni:

.....

.....

.....

Eventuale documentazione allegata:

.....

Luogo e data ..... , ... / ..... / .....

Firma del richiedente

.....

SPAZIO DA COMPILARE A CURA DELL'UFFICIO DELEGATO

Frazionario ufficio delegato ..... Ufficio delegato di .....

Indirizzo: ..... C.A.P. .....

Comune ..... Provincia ..... Telefono .....

Ai sensi e per gli effetti di quanto previsto dalla normativa vigente in materia, si dichiara di aver identificato la persona sopra indicata i cui dati corrispondono a quelli riportati sui documenti di identità a me esibiti.

Data identificazione

..... , ... / ..... / .....

Timbro dell'ufficio delegato

Firma leggibile dell'addetto ufficio delegato

.....

Attenzione: la richiesta va presentata almeno due giorni feriali prima del termine di decorrenza indicato nella stessa.

13 ALLEGATO 'G-1' Bozza Richiesta di Sospensione/Revoca della CMG Interna all'Amministrazione

Il sottoscritto _____

Qualifica Cognome e Nome

in qualità di _____della SEDE_____

Responsabile Periferico o Titolare di certificato

Chiede il/la :

☐ Sospensione della CMG n°

☐ Revoca della CMG n°

Codice fiscale del Titolare della CMG interessata:

Motivo ed eventuale limite temporale:

_____

_____

Note (Indicare il protocollo del modulo di denuncia della CMG fatta presso le autorità di PP.SS. se la CMG è stata smarrita ed allegarne Fotocopia)

_____

_____

IL TITOLARE DEL CERTIFICATO

IL RESPONSABILE PERIFERICO

14 ALLEGATO ‘H’ – FAC SIMILE di una CMG

14.1 FRONTE della CMG

14.2 RETRO della CMG

FINE DEL DOCUMENTO