“Entra con CIE”
Manuale

Italia

05 giugno 2023

1 Acronimi e definizioni

CIE	Carta di Identità Elettronica
SP	Service Provider ovvero Erogatore del servizio
IdP	Identity Provider ovvero Gestore di Identità digitale
IPZS	Istituto Poligrafico e Zecca dello Stato S.p.A.
SAML	Security Assertion Markup Language
OIDC	OpenID Connect
NFC	Near Field Communication
PIN	Personal Identification Number

2 Introduzione

La Carta di Identità Elettronica (CIE), rilasciata dal Ministero dell'Interno, grazie alla presenza di un chip a radiofrequenze nel quale sono contenuti i dati personali e biometrici del titolare e un certificato digitale di autenticazione, estende il tradizionale concetto di identità fisica e si configura come uno strumento di identità digitale per l'accesso ai servizi in rete andando a costituire il principale cardine dello schema di identificazione digitale "Entra con CIE". Interoperabile anche in ambito europeo, lo schema di identificazione «Entra con CIE» realizza un sistema di autenticazione federato per l'identificazione dei cittadini presso i soggetti pubblici e privati che erogano servizi digitali in rete.

Tale schema risulta essere in linea con il Regolamento Europeo (UE) n. 910/2014 (c.d. "eIDAS").

Si basa sia sul protocollo SAML v2 (Security Assertion Markup Language) con profilo «Web Browser SSO» (SAML V2.0 Technical Overview[1]) dal quale eredita gran parte dei requisiti tecnici, sia sul protocollo OpenID Connect (OIDC), quest'ultimo di più recente adozione. I soggetti pubblici e privati che aderiscono allo schema possono scegliere uno o l'altro protocollo secondo le loro necessità.

Lo schema di identificazione "Entra con CIE" offre diversi meccanismi di accesso ai servizi in rete secondo il livello di sicurezza richiesto dal particolare SP aderente e, in particolare:

1) un livello di accesso cosiddetto "*basso*" (livello 1), che prevede l'impiego di credenziali *username/password* attivabili dal titolare di CIE mediante procedura guidata dal portale www.cartaidentita.it;
2) un livello di accesso cosiddetto "*significativo*" (livello 2), che prevede, in aggiunta alle credenziali di livello 1, l'impiego di un secondo fattore di autenticazione o di un meccanismo di autenticazione che certifichi il possesso di un dispositivo (es. codice temporaneo OTP inviato via SMS o notifica push, scansione QR code);
3) un livello di accesso cosiddetto "*elevato*" (livello 3), che prevede la lettura della CIE (caratterizzata da un processore e da un certificato digitale di autenticazione) mediante un lettore NFC, e l'inserimento del PIN della carta.

Tale schema può essere utilizzato da un personal computer (sia Windows, che MacOS che Linux) o da uno smartphone in mobilità, eventualmente combinando le due modalità di accesso, come meglio spiegato nel corso del presente documento.

Lo schema di autenticazione "Entra con CIE" segue il modello dell'identità federata e dunque prevede l'introduzione di un gestore dell'identità dell'utente, un Identity Provider (IdP), al quale i fornitori di servizi online, Service Provider (SP), richiedono, previa federazione, la verifica dell'identità dell'utente.

In particolare, prevede l'istituzione di un IdP unico, il Ministero dell'Interno, che in qualità di ente responsabile dell'emissione della CIE, ne cura anche gli aspetti legati all'impiego documento e delle credenziali di livello basso e significativo ad esso connesso, come strumento di identità digitale. Di seguito viene mostrato uno schema logico della soluzione eID basata sulla CIE.

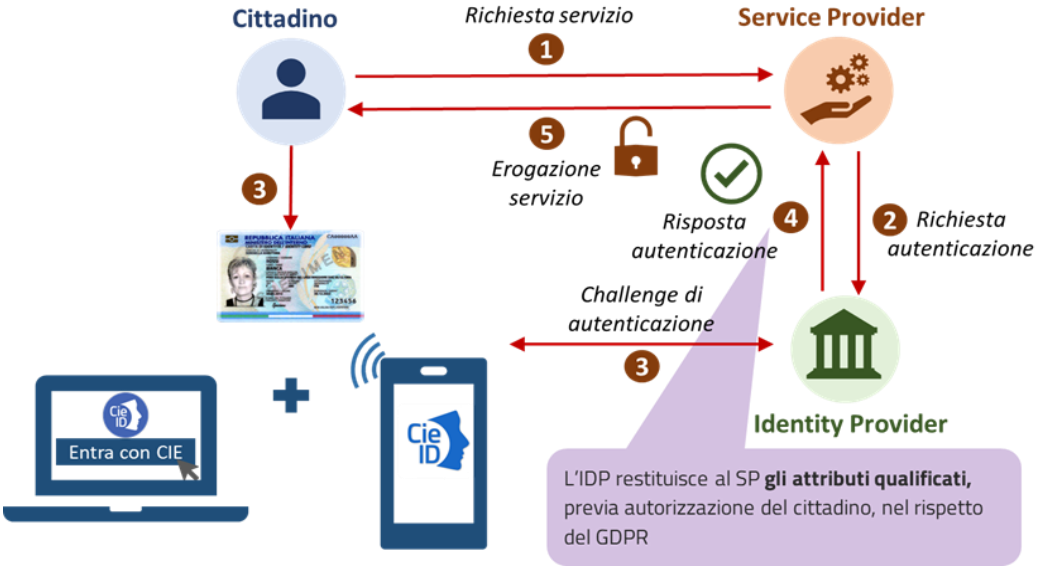

Fig. 2.1: Schema di autenticazione. Entra con CIE.

L'accesso mediante la CIE ai servizi erogati in rete dalla Pubblica Amministrazione è reso possibile attraverso il CieID Server, sito presso il Ministero dell'Interno e fruibile attraverso Internet e/o SPC. Tale componente server, che si configura tanto come un server SAML 2.0 che come un OpenID Provider (OP), è realizzato e manutenuto dall'Istituto Poligrafico e Zecca dello Stato S.p.A. (IPZS) che riveste il ruolo di partner tecnologico del Ministero dell'Interno. Esso svolge le seguenti funzioni:

- Accetta richieste di autenticazione SAML o OIDC a servizi digitali erogati da enti federati ed inviate attraverso il protocollo HTTPS;
- Effettua l'identificazione informatica dell'utente mediante l'esecuzione della fase di challenge secondo il livello di sicurezza richiesto dal SP/scelto dall'utente;
- Nel caso di accesso mediante livello di sicurezza "alto", verifica la validità del certificato a bordo della CIE cooperando con la CA Autenticazione;
- Mostra l'elenco degli attributi qualificati che saranno trasmessi all'erogatore di servizio chiedendo all'utente il consenso alla trasmissione di essi;
- Invia una asserzione di autenticazione sigillata con sigillo riconducibile al Ministero dell'Interno all'erogatore del servizio; tale asserzione costituisce prova di avvenuto riconoscimento dell'utente da parte di CieID Server e del Ministero stesso.

L'interazione con l'utente può avvenire secondo diverse modalità:

- Modalità «**desktop**»: l'utente si autentica mediante un browser installato sul proprio computer. Nel caso di accesso di livello 3, utilizza la CIE mediante un lettore contactless collegato al computer;
- Modalità «**smartphone**»: l'utente si autentica al servizio tramite un browser installato su un dispositivo mobile (smartphone o tablet) dotato dell'app CieID. Nel caso di accesso di livello 3, il dispositivo mobile deve essere necessariamente dotato di interfaccia NFC e la fase di autenticazione si completa avvicinando la CIE al proprio dispositivo;
- Modalità «**desktop + smartphone**»: l'utente si autentica al servizio tramite un browser installato sul proprio computer e, nel caso di accesso di livello 2 o 3 completa l'autenticazione mediante l'app CieID eventualmente avvicinando la CIE al proprio dispositivo mobile dotato di interfaccia NFC.

Lo schema Entra con CIE si realizza dunque mediante due macro-fasi distinte:

1. richiesta di accesso al servizio digitale, che avviene all'interno del browser dell'utente, nel dominio dell'ente (Service Provider) che eroga il servizio;
2. autenticazione dell'utente effettuata direttamente dall'Identity Provider secondo i passi riportati in precedenza.

Per quanto concerne il primo punto, la richiesta avviene tramite una «call to action» realizzata dal Service Provider tramite un apposito pulsante «Entra con CIE» e che atterra su di una pagina del Ministero dell'Interno, dalla quale viene innescato il processo di identificazione vero e proprio. Per consentire una esperienza utente quanto più possibile omogenea presso tutti i service provider che integrano lo schema di identificazione mediante la CIE si deve utilizzare il kit disponibile all'indirizzo https://github.com/italia/cie-graphics.

3 Credenziali di livello 1 e livello 2

Le credenziali di livello 1 e 2 associate alla CIE consentono di accedere ai servizi digitali con maggiore comodità sebbene con un livello di sicurezza inferiore, senza cioè necessariamente utilizzare la carta ed il codice PIN di 8 cifre ad essa associato (livello 3). Il tutto, sulla base del livello di accesso effettivamente richiesto dal servizio online.

Le credenziali sono collegate alla validità della CIE ovvero hanno una durata pari a quella della carta più ulteriori 90 giorni per dare la possibilità al cittadino di rinnovare il documento.

3.1 Credenziali di livello 1

Le credenziali CIE di livello 1 sono costituite da una coppia di valori, *username* e *password*, che seguono le logiche di seguito descritte:

- Username: uno dei dati di seguito riportati che il cittadino può utilizzare in maniera indifferente:
  - codice fiscale;
  - numero di serie della CIE
  - indirizzo e-mail (solo se certificato)
- Password: parola segreta impostata direttamente dal cittadino in fase di attivazione delle credenziali di livello 1 e 2 sul sito www.cartaidentita.it così come descritto al paragrafo 3.3.

  La password prevede almeno:
  - lunghezza minima di 10 caratteri alfanumerici;
  - almeno una lettera maiuscola, una minuscola, un numero, un carattere speciale;
  - divieto di inserire più di due caratteri uguali consecutivi;
  - divieto di utilizzo delle ultime cinque password impostate.

  La password ha una validità di **180 giorni**.

Il cittadino può recuperare la password mediante apposita funzionalità disponibile sotto la buca di immissione della password stessa, previo inserimento di codice fiscale e numero di serie della carta. Il sistema verifica la correttezza dei dati e, se validi, invia al cittadino sui canali certificati, un codice temporaneo OTP (nell'ordine, indirizzo e-mail o numero di telefono cellulare). Il cittadino inserisce il codice ricevuto nella procedura online di recupero password, visualizza le proprie username e crea una nuova password.

3.2 Credenziali di livello 2

Le credenziali CIE di livello 2 richiedono l'impiego di un secondo fattore di autenticazione. Nel dettaglio è possibile effettuare un accesso di livello 2:

- autenticandosi con le credenziali di livello 1 (*username* e *password*) e
  - immettendo un codice OTP inviato tramite SMS al proprio smartphone certificato oppure
  - cliccando la notifica push inviata all'app CieID sul proprio dispositivo certificato;
- inquadrando un codice QR mediante l'app CieID.

Il cittadino sceglie la modalità di autenticazione in fase di attivazione delle credenziali di livello 1 e 2 come descritto al paragrafo 3.3.

3.3 Procedura di attivazione delle credenziali CIE (livello 1 e livello 2)

La procedura di attivazione delle credenziali CIE di livello basso e significativo può essere eseguita da cittadini:

1. in possesso di dispositivo dotato di tecnologia NFC e del codice PIN della CIE, mediante autenticazione all'area riservata del portale www.cartaidentita.it;
2. dotati della prima metà del codice PUK della CIE, mediante apposita funzionalità disponibile sull'area pubblica del portale www.cartaidentita.it - a condizione che in fase di richiesta della CIE abbiano fornito i propri contatti (indirizzo e-mail e numero di cellulare).

3.3.1 Attivazione mediante autenticazione di livello 3 all'area riservata del Portale CIE

Il cittadino, seguendo la procedura guidata presente sull'area pubblica del portale www.cartaidentita.it, si autentica all'area riservata con la sua CIE (quindi mediante livello 3) e procede con l'attivazione contestuale delle credenziali di livello 1 e di livello 2.

Il cittadino può inserire i propri dati di contatto (cellulare ed e-mail) ovvero verificare o modificare quelli dichiarati all'operatore presso l'ufficio anagrafico in fase di richiesta di rilascio della sua CIE e procedere alla verifica (mediante convalida di un codice temporaneo OTP che riceve).

Dimostrato il possesso dei suddetti canali, il cittadino specifica la password personale, seleziona la modalità di autenticazione ai servizi online (App CieID oppure codice OTP via SMS) e conclude l'attivazione delle credenziali CIE (livello 1 e livello 2).

Durante la procedura di attivazione il portale rende evidente al cittadino che può utilizzare come username di accesso ai servizi online, in maniera indifferente, uno dei dati di seguito riportati:

- codice fiscale,
- numero di serie della CIE,
- indirizzo e-mail (solo se certificato).

Se il cittadino sceglie di autenticarsi ai servizi in rete mediante utilizzo dell'App CieID, può scaricare dallo store – se non lo ha già fatto – l'App e procedere alla certificazione del dispositivo come descritto al paragrafo.

3.3.2 Attivazione mediante codice PUK, numero di serie della CIE e codice fiscale

Il cittadino, seguendo la procedura guidata presente sull'area pubblica del portale www.cartaidentita.it, senza alcuna autenticazione allo stesso, immette nella schermata il proprio codice fiscale, il numero di serie della carta e alcune cifre della prima metà del codice PUK (richieste dal sistema in maniera randomica).

Il Portale, verificata la correttezza delle informazioni, richiede al cittadino di verificare - mediante l'invio di un codice temporaneo OTP - il possesso dei canali di contatto dichiarati all'operatore presso l'ufficio anagrafico.

La verifica dei canali (quella del numero cellulare è obbligatoria) è propedeutica all'attivazione delle credenziali, pertanto, se i dati di contatto non sono stati rilasciati al comune in maniera corretta, il cittadino può:

- accedere all'area riservata del portale con il livello 3 e inserirli/modificarli;
- recarsi presso un qualsiasi comune e richiederne l'aggiornamento.

Dimostrato il possesso dei suddetti canali, il cittadino specifica la password personale, seleziona la modalità di autenticazione ai servizi online (App CieID oppure codice OTP via SMS) e conclude l'attivazione delle credenziali CIE (livello 1 e livello 2).

Durante la procedura di attivazione il portale rende evidente al cittadino che può utilizzare come username di accesso ai servizi online, in maniera indifferente, uno dei dati di seguito riportati:

- Codice fiscale,
- Numero di serie della CIE,
- Indirizzo e-mail (solo se certificato).

Se il cittadino sceglie di autenticarsi ai servizi in rete mediante utilizzo dell'App CieID, può scaricare dallo store – se non lo ha già fatto – l'App e procedere alla certificazione del dispositivo come descritto al paragrafo 3.3.3.

3.3.3 Certificazione del dispositivo

La procedura di certificazione del terminale mobile è richiesta nel caso in cui il cittadino intenda utilizzare le credenziali di livello 2 mediante l'app CieID. In tal caso, la procedura di certificazione prevede che il cittadino:

1. inserisca le credenziali di livello 1 sull'app CieID (username e password);
2. dimostri il possesso del numero di telefono cellulare mediante la ricezione via SMS di un codice temporaneo (OTP) da inserire sull'app CieID;
3. crei un codice personale di protezione dell'app ("codice app CieID") e, se supportato dal dispositivo e se di interesse per il cittadino, attivi l'utilizzo della biometria in sostituzione di tale codice;

   Il codice app CieID deve contenere sei caratteri alfanumerici di cui almeno un numero e una lettera, non più di due numeri ripetuti, non contenere tre numeri in sequenza (crescente e decrescente);
4. abiliti – se di interesse - l'invio delle notifiche push da parte dell'app CieID;
5. imposti – se di interesse - un nome dispositivo.

È possibile certificare più dispositivi la cui lista sarà consultabile nella propria area personale sul portale www.cartaidentita.it.

Il cittadino potrà però utilizzare per l'accesso ai servizi online un solo dispositivo definito "predefinito". Un dispositivo certificato è impostato come "predefinito" nelle seguenti modalità:

1. l'ultimo dispositivo certificato viene impostato di default come predefinito;
2. accedendo all'area riservata del portale www.cartaidentita.it impostando manualmente la scelta tra la lista di dispositivi certificati. Nella medesima aerea è possibile anche rimuovere un dispositivo dalla lista.

4 Credenziali di livello 3

L’autenticazione di livello 3 è realizzata mediante utilizzo della CIE e del PIN. Nel caso in cui il cittadino operi dal suo personal computer, deve necessariamente dotarsi di un lettore RF, scaricare dal Portale CIE il **Software CIE** e procedere ad installarlo e configurarlo con la sua CIE, come spiegato nel manuale di utilizzo fornito a corredo.

Nel caso, invece, in cui un cittadino intenda servirsi del suo smartphone, deve essere in possesso di un dispositivo dotato di lettore NFC, procedere a scaricare l’app CieID e a configurarla con la sua CIE.

Nel momento in cui deve autenticarsi, verrà a lui richiesto (sul browser del suo computer o sull’app CieID del suo smartphone) di poggiare la CIE sul suo lettore e di utilizzare le **ultime 4 cifre** del PIN. Digitate le ultime 4 cifre del PIN sarà possibile proseguire.

Terminata l’autenticazione sarà possibile rimuovere la carta dal lettore e proseguire normalmente con la navigazione.

Nel caso in cui si digiti un PIN errato per tre volte consecutive la carta risulterà bloccata e sarà necessario sbloccarla mediante le 8 cifre del PUK. L’operazione di sblocco è possibile tanto da computer, mediante il Software CIE, quanto dallo smartphone mediante l’app CieID.

5 Modalità di utilizzo delle credenziali CIE (livello 1, livello 2 e livello 3)

Le credenziali di livello 1 e livello 2 possono essere utilizzate per l'autenticazione ai servizi della Pubblica Amministrazione e dei privati aderenti allo schema di identificazione «Entra con CIE», sia da desktop che da mobile, alla stregua di quanto avviene mediante autenticazione di livello 3 (elevato) utilizzando cioè la CIE ed un lettore NFC o RFID.

Per ciascuna autenticazione, inclusa l'area riservata del portale www.cartaidentita.it, il cittadino riceve una notifica sul canale di contatto certificato (nell'ordine, indirizzo e-mail o numero di telefono cellulare). Al cittadino che non ha una mail certificata che abbia utilizzato il cellulare quale strumento di autenticazione per ricevere l'OTP via SMS non è inviato un secondo SMS con il suddetto avviso.

Gli scenari di utilizzo delle credenziali sono i seguenti:

Livello 1 (basso)

- Scenario di accesso da personal computer - il cittadino accede alla pagina di autenticazione del Service Provider e:
  - inserisce username/password;
  - conferma l'invio dei propri dati (nome, cognome, codice fiscale e data di nascita) al Service Provider e accede al servizio.

- Scenario di accesso da smartphone - il cittadino accede alla pagina di autenticazione del Service Provider e:
  - inserisce username/password;
  - conferma l'invio dei propri dati (nome, cognome, codice fiscale e data di nascita) al Service Provider e accede al servizio.

  oppure

  - seleziona il banner "Hai l'app CieID?" nella pagina e:
    - se dispositivo certificato:
      - conferma la sua identità tramite codice app CieID (o se attivo mediante biometria);
      - conferma sul browser l'invio dei propri dati (nome, cognome, codice fiscale e data di nascita) al Service Provider e accede al servizio.

    oppure

    - se dispositivo non certificato:
      - se installata, si apre in automatico l'app CieID e inserisce le credenziali username/password; in alternativa, se app CieID non installata, visualizza istruzioni per il download e la configurazione;
      - conferma sul browser l'invio dei propri dati (nome, cognome, codice fiscale e data di nascita) al Service Provider e accede al servizio.

Livello 2 (significativo)

- Scenario di accesso da personal computer - il cittadino accede alla pagina di autenticazione del Service Provider e:
  - inserisce username/password;
  - conferma il secondo fattore di autenticazione:
    - inserendo nella pagina di autenticazione il codice temporaneo OTP ricevuto tramite SMS sul numero di cellulare certificato;

      oppure

    - cliccando la notifica push inviata all'app CieID sul proprio dispositivo certificato e confermando l'identità tramite codice app CieID (o se attivo mediante biometria).

  oppure

    - scansiona il QR-Code, contenente un codice temporaneo OTP silente, da app CieID su dispositivo certificato e conferma l'identità tramite codice app CieID (o se attivo mediante biometria);
  - conferma sul browser l'invio dei propri dati (nome, cognome, codice fiscale e data di nascita) al Service Provider e accede al servizio.

- Scenario di accesso da smartphone - il cittadino accede alla pagina di autenticazione del Service Provider e:
  - inserisce username/password;
  - conferma il secondo fattore di autenticazione:
    - inserendo nella pagina di autenticazione il codice temporaneo OTP ricevuto tramite SMS sul numero di cellulare certificato;

      oppure

    - cliccando la notifica push inviata all'app CieID sul proprio dispositivo certificato e confermando l'identità tramite codice app CieID (o se attivo mediante biometria).

  oppure

  - seleziona il banner "Hai l'app CieID?" nella pagina e:
    - se dispositivo certificato:
      - conferma la sua identità tramite codice app CieID (o se attivo mediante biometria);
      - conferma sul browser l'invio dei propri dati (nome, cognome, codice fiscale e data di nascita) al Service Provider e accede al servizio.

    oppure

    - se dispositivo non certificato:
      - se installata, visualizza un messaggio di errore con le istruzioni per la configurazione dell'app; in alternativa, se app CieID non installata, visualizza istruzioni per il download e la configurazione.

Livello 3 (elevato)

- Scenario di accesso da personal computer + smartphone con tecnologia NFC: - il cittadino accede alla pagina di autenticazione del Service Provider dal browser del PC e seleziona il pulsante "Entra con lettura carta CIE" e:
  - sceglie la modalità "Prosegui con smartphone" e inserisce il numero di serie della CIE;
  - scansiona il QR-Code da app CieID con CIE già registrata, inserisce il PIN della CIE (o se attiva utilizza la biometria), prosegue con la lettura della carta e inserisce manualmente sul browser del PC un codice temporaneo OTP che l'app ha presentato a video dopo la lettura della carta.

- Scenario di accesso da personal computer
  - il cittadino appoggia la CIE sul lettore RF e seleziona il pulsante "Entra con lettura carta CIE":
  - seleziona il certificato digitale associato alla CIE registrata sul PC all'interno del Software CIE;
  - digita le ultime 4 cifre del codice PIN;
  - conferma l'invio dei propri dati (nome, cognome, codice fiscale e data di nascita) al Service Provider e accede al servizio.

- Scenario di accesso da smartphone: - il cittadino accede alla pagina di autenticazione dal browser dello smartphone e:
  - se carta registrata:
    - si apre in automatico l'app CieID ed inserisce la seconda metà del codice PIN (o, se questa è stata memorizzata in fase di registrazione della CIE, viene richiesto l'utilizzo della biometria);
    - appoggia la carta sullo smartphone per avviare il processo di autenticazione;
    - conferma l'invio dei propri dati (nome, cognome, codice fiscale e data di nascita) al Service Provider e accede al servizio.

  oppure

  - se carta non registrata:
    - si apre in automatico l'app CieID che richiede la registrazione della CIE; completata la procedura, il cittadino accede al servizio come descritto nello scenario "accesso mobile con carta registrata".

6 Gestione dell'identità digitale CIE

Il cittadino gestisce la propria identità digitale CIE (livello 1, livello 2 e livello 3) mediante la propria area riservata sul portale www.cartaidentita.it. L'accesso al Portale è consentito con credenziali di livello 2 e 3.

Di seguito le funzionalità accessibili previa autenticazione sul portale con credenziali almeno di livello 2;

- nella sezione "Gestione CieID":
  - modifica password;
  - gestione e-mail (inserimento/modifica/certificazione);
  - gestione numero di cellulare (modifica/certificazione);
  - gestione dispositivi certificati (visualizzazione elenco/rimozione dispositivo/definizione del dispositivo predefinito che è il solo a poter essere utilizzato per l'autenticazione);
  - revoca credenziali di livello 1 e 2;
  - sospensione a tempo (48 ore) delle credenziali di livello 3.
- nella sezione "Elenco accessi":
  - visualizzazione elenco accessi ai servizi in rete con tutti i livelli di autenticazione (livello 1, livello 2 e livello 3);

Di seguito le funzionalità aggiuntive rispetto alle precedenti accessibili previa autenticazione sul portale con credenziali almeno di livello 3:

- primo inserimento dei dati di contatto (numero cellulare).

Un avviso ai contatti certificati (nell'ordine, indirizzo e-mail o numero di telefono cellulare) è inviato al cittadino nei seguenti casi:

- ad ogni modifica dei dati di contatto certificati,
- ad ogni modifica delle credenziali.

Ognuna delle operazioni sopra elencate genera una registrazione nei log che è conservata per 24 mesi garantendone l'integrità, la disponibilità e la riservatezza attraverso un apposito sistema di log management.

6.1 Revoca delle credenziali di livello 1 e 2

Il cittadino ha la possibilità, nella propria area riservata del portale www.cartaidentita.it di revocare le credenziali di livello 1 e livello 2 in completa autonomia.

Tale funzionalità prevede la cancellazione dal sistema delle stesse.

Il cittadino può anche richiedere la rimozione delle eventuali informazioni associate (numero di telefono cellulare, e-mail, dispositivi certificati, ecc.).

Nel caso in cui il cittadino non richieda sul portale di cancellare tali informazioni associate, queste saranno conservate fino alla naturale scadenza della CIE.

6.2 Sospensione delle credenziali di livello 3

Al fine di cautelare il cittadino che abbia il dubbio di aver smarrito la propria CIE, è resa disponibile una funzionalità che, previa autenticazione all'area riservata del portale www.cartaidentita.it con credenziali di livello 2, consente la sospensione delle credenziali di livello 3 per un periodo di 48 ore al fine di consentirgli di verificare l'effettiva perdita di possesso della CIE, effettuare la denuncia e procedere con la conseguente revoca.

6.3 Revoca delle credenziali di livello 3

In caso di furto o smarrimento della sua CIE, Il cittadino può revocare le credenziali di livello 3 seguendo le indicazioni riportate nella sezione “Assistenza” del portale www.cartaidentita.it.

La revoca della CIE comporta inoltre l’inibizione delle credenziali di livello 1 e livello 2 ad essa associate.

6.4 Visualizzazione elenco accessi

Lo schema di identificazione “Entra con CIE” prevede la generazione e conservazione dei log delle richieste di accesso effettuate dagli utenti negli ultimi 24 mesi con qualunque livello di credenziali (1, 2 e 3).

L’area riservata del portale www.cartaidentita.it consente al cittadino la consultazione e salvataggio in formato Excel dell’elenco delle richieste di autenticazione effettuate tramite “Entra con CIE”.

Tale funzione rappresenta uno strumento di autotutela per il cittadino, che può monitorare l’utilizzo della propria identità digitale CIE. Per ciascuna richiesta di autenticazione, il relativo log contiene le seguenti informazioni:

- numero di serie CIE;
- codice fiscale del titolare dell’identità digitale (non visualizzato dal cittadino);
- data e ora;
- dispositivo utilizzato per l’accesso;
- indirizzo IP da cui è originata la richiesta;
- livello di autenticazione;
- erogatore del servizio acceduto;
- esito della richiesta di autenticazione;
- ID accesso (identificativo univoco della richiesta di autenticazione).