Manuale di integrazione per servizi basati sul NIS

Release stabile

italia

28 set 2021

Indice dei contenuti

CAPITOLO 1

Introduzione

Scopo del documento è descrivere il protocollo operativo necessario per utilizzare la Carta di Identità Elettronica 3.0 (CIE) come strumento per la fruizione di servizi fisici di accesso pinless, ovvero senza l'uso del PIN della CIE. Il protocollo può essere applicato ai casi d'uso in cui è richiesto un accesso fisico veloce, come nel casi di mezzi di trasporto, di luoghi di lavoro e aree con accesso controllato. Il protocollo si basa sulla lettura e verifica di autenticità del Numero Identificavo Servizi (NIS), un numero univoco, associato ad ogni CIE, liberamente accessibile sul chip della carta. Nel primo capitolo verranno descritti i controlli necessari per verificare l'autenticità, l'originalità e la validità del NIS. Nel secondo capitolo si descriverà il protocollo di registrazione (Enrollment) per associare e abilitare la CIE all'utilizzo di un servizio fisico pinless. Successivamente si descriverà il protocollo di accesso fisico tramite CIE, previa registrazione, al medesimo servizio.

CAPITOLO 2

Il Numero Identificativo Servizi (NIS)

La Carta d'identità elettronica 3.0 (CIE)[1] è il documento di identità rilasciato dal Ministero dell'Interno su richiesta dei cittadini per la certificazione della propria identità. Oltre ad essere un documento di riconoscimento è anche un documento di viaggio, conforme agli standard internazionali adottati anche per i passaporti e i permessi di soggiorno. Infine, consente l'accesso in sicurezza ai servizi digitali, mediante l'inserimento del PIN, erogati dalla Pubblica Amministrazione e dai privati anche in ambito europeo.

La CIE permette l'utilizzo di tre diverse tipologie di servizio che sono:

- **Identità Digitale**: tramite un certificato di autenticazione, accessibile solo mediante PIN, utilizzata per l'autenticazione ai servizi on-line;
- **Identità Fisica**: i dati di identificazione fisica dei cittadini, conformi allo standard dei documenti di viaggio ICAO 9303;
- **Numero Identificavo Servizi (NIS)**: l'identificativo associato alla carta utilizzato per i servizi fisici di accesso veloce.

Il Numero Identificativo Servizi è un valore numerico univoco composto da 12 cifre, generato in fase di personalizzazione della CIE, dedicato appositamente alla fruizione di servizi ad accesso fisico veloce. Il NIS ha le seguenti caratteristiche:

- E' liberamente accessibile e leggibile senza l'uso di chiavi o PIN;
- E' associato univocamente ad ogni CIE;
- Non è riconducibile direttamente al titolare del documento.

Il servizio di accesso tramite NIS può essere utilizzato, ad esempio, per l'accesso fisico ai luoghi pubblici, ai mezzi di trasporto, oppure per l'identificazione e la registrazione del dipendente in entrata ed uscita dai posti di lavoro in sostituzione del badge aziendale. Il NIS, all'interno del file system della CIE, viene memorizzato sotto il nome di ID Servizi (file EF.ID_Servizi).

[1] https://www.cartaidentita.interno.gov.it/

2.1 Verifica della CIE

Il vantaggio di utilizzare il NIS come identificativo di accesso ai servizi consiste nella possibilità leggere quest'ultimo liberamente e senza operazioni preliminari di autenticazione. E" necessario adottare delle procedure che permettano comunque di verificarne l'integrità, la provenienza da una CIE originale, l'appartenenza ad una CIE autentica e, infine, l'appartenenza ad una CIE valida.

Per evitare di abilitare ad un servizio un utente con documento non valido, contraffatto o revocato, è opportuno applicare le seguenti verifiche che consentano di mitigare tali rischi.

2.1.1 Verifica di Autenticità e Integrità

A seguito della lettura del NIS, è necessario verificarne l'integrità e l'autenticità. Ciò significa attuare dei controlli che consentano di verificare che il dato letto sia effettivamente l'ID Servizi della CIE letta e che sia integro e autentico, cioè inalterato e firmato dal Ministero dell'Interno. A garanzia dell'autenticità e integrità del dato, il NIS memorizzato nella CIE, oltre ad essere liberamente accessibile, è firmato digitalmente e memorizzato in un apposito file insieme al certificato digitale (certificato DS) che contiene la chiave pubblica per la verifica della firma applicata dallo stesso Document Signer. Tale certificato, a sua volta, è firmato dalla Country Sign Certification Authority (CSCA)[2], che attesta l'autenticità del Document Signer. Durante la fase di lettura e verifica di autenticità, il sistema che effettua tale operazione deve poter recuperare dinamicamente o aver memorizzato localmente il certificato emesso dalla CSCA ai fini della verifica di autenticità del certificato DS. La verifica di autenticità del NIS consiste essenzialmente di due step:

1. Verifica dell'integrità del NIS, tramite l'internal authentication"
2. Verifica dell'autenticità del NIS, tramite la verifica del SOD e dei certificati

Se entrambe le verifiche vanno a buon fine, allora il NIS è autentico. Di seguito si riporta uno schema esemplificativo del flusso di verifica.

2.1.2 Verifica di Originalità

Il NIS letto, seppur precedentemente autenticato, potrebbe provenire da una CIE clonata. La verifica di originalità consiste nel controllare che la CIE presentata al lettore sia effettivamente la CIE originale emessa dal Ministero dell'Interno. Si attua un processo di Internal Authentication, di cui uno schema esemplificativo di funzionamento è riportato qui di seguito.

Nella fase di Internal authentication il chip della CIE deve autenticarsi verso il lettore, dimostrando di possedere la chiave privata corrispondente ad una chiave pubblica ritenuta affidabile dal lettore stesso (dato integro e affidabile) (ref. *Verifica di Autenticità e Integrità* (pagina 3)). Il lettore legge la chiave pubblica e avviene un protocollo challenge/response in cui il chip firma un challenge ottenuto dal lettore. Il lettore verifica la correttezza del challenge firmato nella response per assicurarsi che non sia in atto un attacco di Man In The Middle e per assicurarsi che il chip possieda una chiave privata affidabile la cui componente pubblica è firmata nel SOD.

2.1.3 Verifica di Validità

Tale verifica consiste nel determinare se la CIE, autentica ed originale, sia ancora valida. Una CIE, infatti, può essere scaduta o revocata in seguito a furto o smarrimento.

[2] https://csca-ita.interno.gov.it/

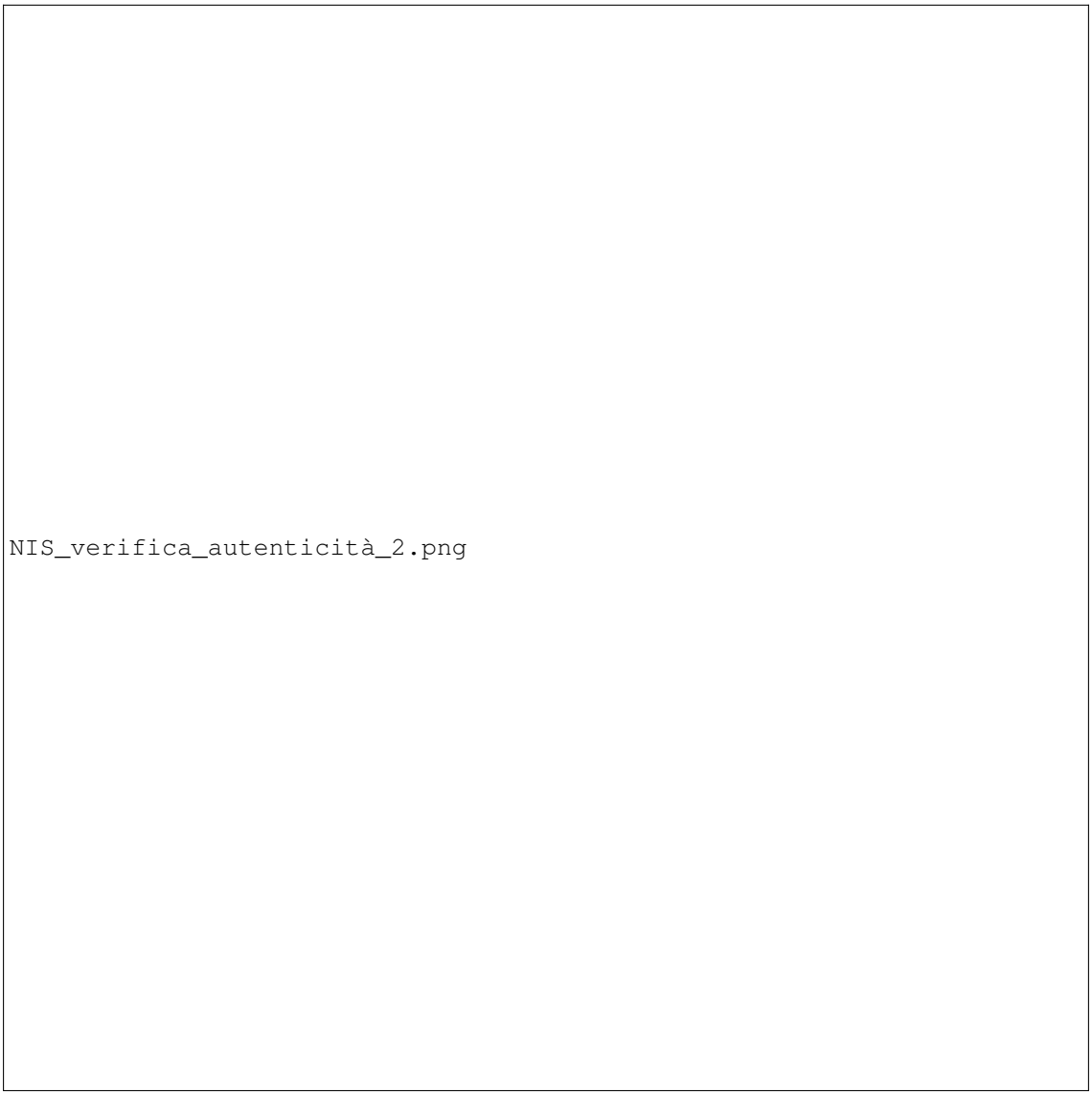

Fig. 2.1: Schema di verifica di autenticità e Integrità del NIS.

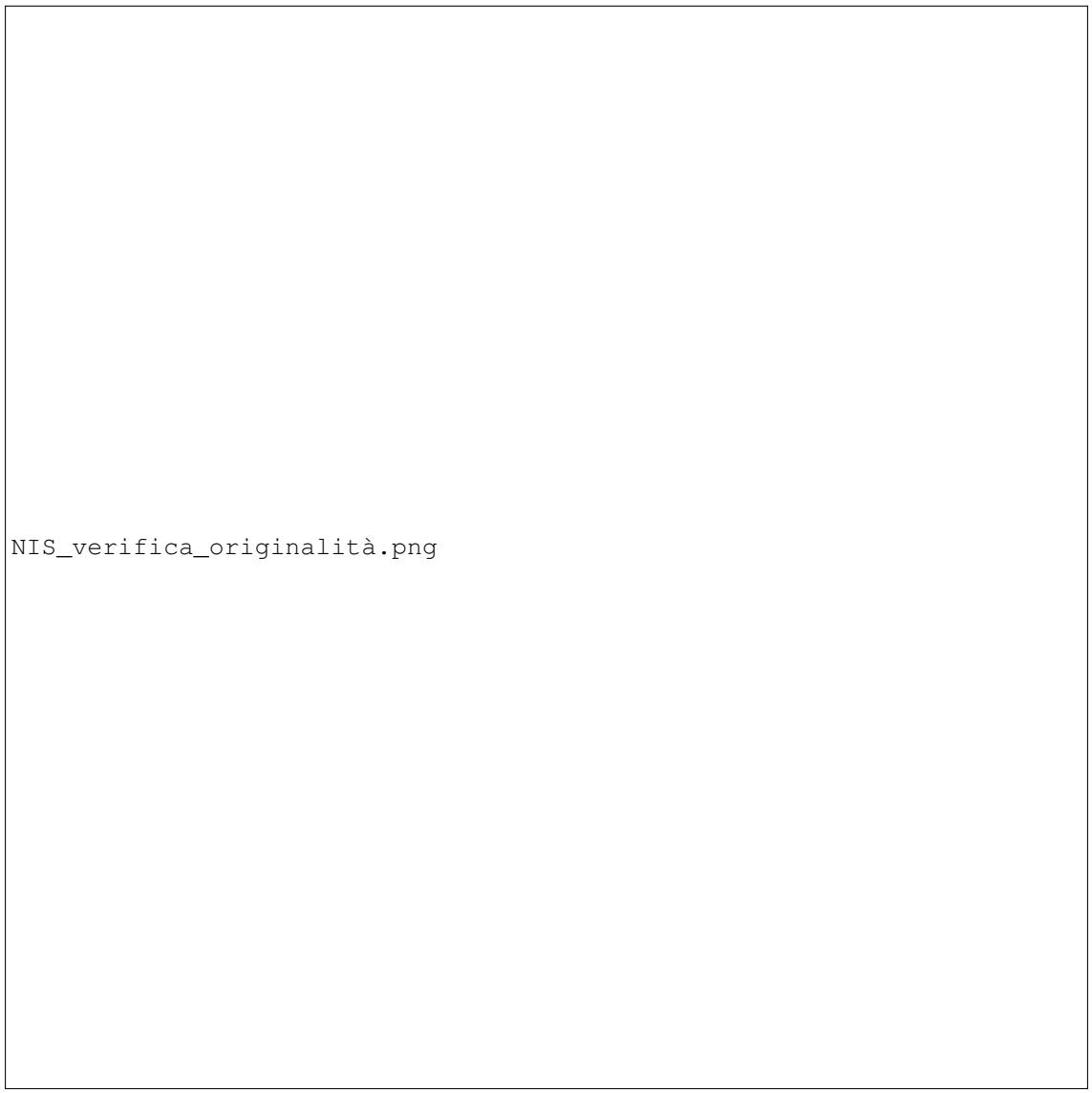

Fig. 2.2: Schema di verifica di originalità della CIE.

Nota: In caso di furto o smarrimento è necessario che il titolare del documento abbia sporto regolare denuncia, così che le autorità competenti possano avviare la procedura di revoca del documento.

Una CIE scaduta non presenta particolari rischi legati alla sicurezza (si richiede comunque un rinnovo al legittimo titolare), una CIE revocata invece può essere detenuta da soggetti fraudolenti con l'intento di utilizzarla sostituendosi ai legittimi titolari del documento ed accedere ai servizi fisici ai quali risulta abilitata.

La verifica di validità della CIE non è disponibile in questa versione.

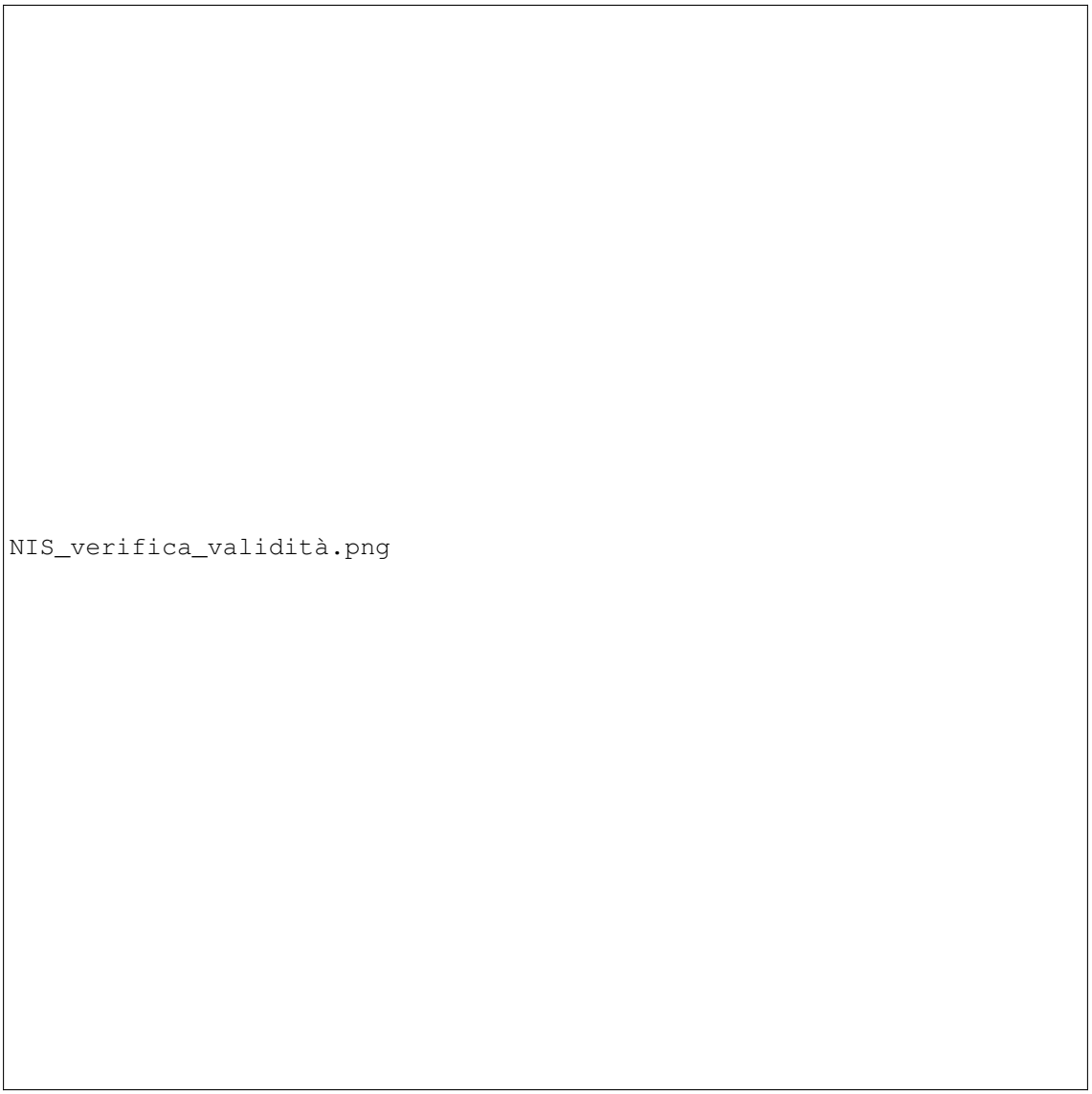

Fig. 2.3: Schema di verifica di validità della CIE.

CAPITOLO 3

Protocollo di registrazione ed accesso tramite NIS

L'abilitazione e la fruizione di un servizio tramite CIE avviene in due fasi:

1. Fase di Enrollment
2. Fase di Accesso

L'Enrollment consiste nella verifica della CIE e nella convalida del NIS controllandone l'autenticità, l'originalità e la validità e, in caso di esito positivo delle verifiche, abilitarlo alla fruizione del servizio. A valle delle verifiche, l'erogatore del servizio dovrà memorizzarsi il NIS e il valore di Hash della Chiave Pubblica $H(K_{PUB})$ restituiti dalla CieNIS-java-sdk. Questa fase prevede dunque di memorizzare nel proprio sistema due valori considerati, a valle delle verifiche, affidabili, ovvero:

La fase di accesso consente all'utente, precedentemente registratosi nella fase di Enrollment, di utilizzare la CIE per accedere al servizio fisico pinless. L'accesso avviene, ad esempio, su un tornello che, verificata l'originalità della CIE mediante i dati salvati in fase di Enrollment, ne autorizza l'accesso. In particolare il sistema verificherà se la coppia NIS e $H(K_{PUB})$ lette in accesso sono presenti nel proprio Database. Si riporta uno schema esemplificativo del protocollo.

3.1 Il processo di Enrollment

L'Enrollment è la fase in cui si procede all'associazione della propria CIE come carta di accesso ad un determinato servizio. In particolare il NIS della CIE, una volta autenticato e validato attraverso le verifiche precedentemente descritte, viene associato all'utente che ne richiede il servizio. Il processo di Enrollment deve essere eseguito una sola volta e può ritenersi valido fino alla revoca del servizio o fino alla revoca della CIE stessa. Tale processo può essere eseguito in due modalità:

1. Enrollment Locale
2. Enrollment Remoto

Si parla di Enrollment di tipo locale quando la CIE viene presentata fisicamente e verificata presso un lettore messo a disposizione dal fornitore del servizio, ad esempio attraverso un totem aziendale, un lettore NFC connesso alla postazione di un operatore autorizzato dall'erogatore dei servizi. Questa modalità fa sì che le fasi di verifica avvengano

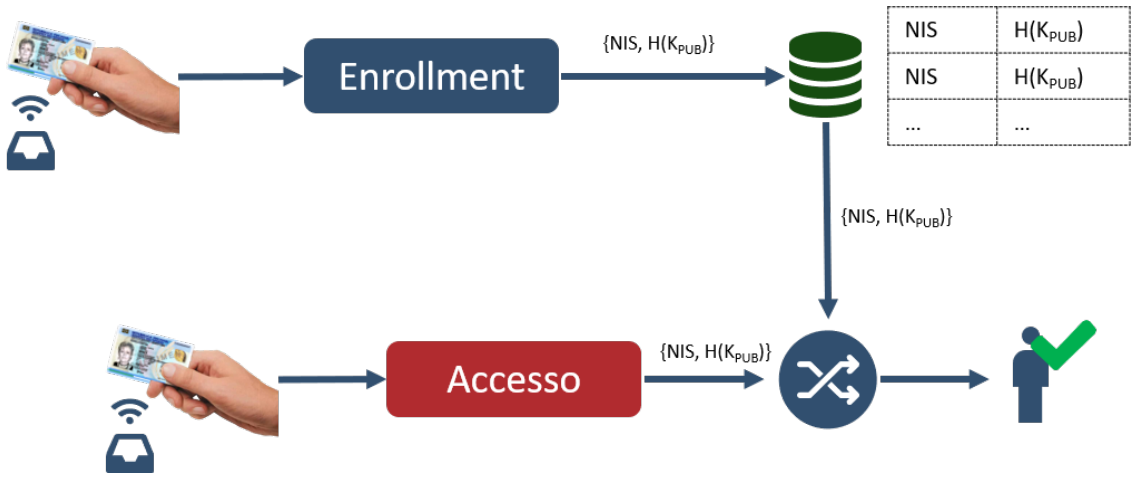

Fig. 3.1: Protocollo di registrazione ed accesso.

direttamente sulla postazione presso la quale ci si sta registrando e il titolare della CIE utilizzi solo lettori e strumenti autorizzati e controllati dall'erogatore stesso.

Si definisce altresì Enrollment di tipo remoto quanto la CIE viene presentata attraverso, ad esempio, lo smartphone del titolare della stessa, in modalità non direttamente sotto la supervisione del fornitore dei servizi. Tale modalità offre la flessibilità di una registrazione dell'utente direttamente in qualsiasi luogo, purchè lo stesso detenga uno smartphone dotato di tecnologia NFC e sia disponibile una connessione ad internet.

Nei successivi paragrafi verranno descritte le modalità di integrazione delle due tipologie di Enrollment.

3.1.1 Enrollment Locale

L'Enrollment di tipo locale consente la verifica del NIS direttamente sul sistema di lettura e/o verifica messo a disposizione dal fornitore dei servizi per il quale il titolare della CIE si sta registrando.

Requisiti Hardware:

- **Lettore NFC**: Lettore NFC in grado di operare secondo lo standard ISO-14443;

Il processo di Enrollment viene schematizzato nella figura che segue.

Fig. 3.2: Schema di Enrollment Locale.

L'utente posiziona la CIE sul lettore NFC, dopodichè, il lettore esegue la lettura del NIS e del valore dell'Hash della chiave pubblica. In seguito vengono eseguite le verifiche di autenticità, integrità, originalità e validità, come descritto nelle sezione precedente. Se tutti gli step da 1 a 4 sono andati a buon fine, è possibile memorizzare il NIS e il valore di $H(K_{PUB})$ della CIE presentata. Tali dati dovranno essere inseriti nella White List del fornitore del servizio. La SDK CieNis-java-sdk sviluppata dal Poligrafico che implementa le verifiche di autenticità e originalità della CIE, restituendo il NIS e l'$H(K_{PUB})$, può essere scaricata dal seguente link:

https://github.com/italia/cie-nis-java-sdk

3.1.2 Enrollment Remoto

Non disponibile in questa versione.

3.2 Il processo di Accesso

Il processo di accesso è la fase in cui l'utente, precedentemente registratosi all'utilizzo di uno specifico servizio, presenta la propria CIE al lettore per usufruire del servizio stesso. Se la fase di Enrollment è andata a buon fine, allora l'utente viene abilitato ad usufruire del servizio. La fase di accesso è caratterizzata dall'implementazione di un protocollo di verifica più «leggero» rispetto a quello di enrollment. Questo per far sì che tale fase possa impiegare pochi millisecondi e rendere il servizio di accesso fisico «veloce» e percepito con positività dall'utente finale. I minori step di verifica non vanno a discapito della sicurezza, in quanto già in fase di Enrollment sono stati svolti tutti i passaggi necessari per garantire la validità della CIE presentata. Le fasi di Enrollment e di Accesso vengono legate nel momento in cui, oltre al NIS, viene memorizzato il valore di $H(K_{PUB})$. In questo modo la chiave pubblica (con il relativo Hash) viene ritenuta affidabile. In fase di accesso, viene implementata la sola verifica di Internal Authentication che consente la verifica che la chiave pubblica letta corrisponda alla relativa chiave privata memorizzata nel chip. Infine il sistema del fornitore di servizi verifica che la coppia $\{NIS, H(K_{PUB})\}$ sia una delle coppie presenti nella WHITE LIST precedentemente memorizzate in fase di enrollement. Si riporta di seguito uno schema riassuntivo del protocollo di accesso.

Fig. 3.3: Schema di Accesso.

Gli step descritti devono essere integrati sui lettori installati nei punti di accesso al servizio.