



CARTA
DI IDENTITÀ
ELETTRONICA

Accesso ai servizi in rete mediante la CIE 3.0

Manuale operativo per le pubbliche amministrazioni e i soggetti privati

Sommario

1. Riferimenti.....	3
2. Pubblicazione del documento e future versioni.....	3
3. Ambito.....	3
4. Schema eID basato su CIE 3.0: caratteristiche.....	4
5. CieID Server.....	10
5.1. Metadati.....	10
5.2. Protocollo.....	10
5.2.1. Richieste di autenticazione.....	11
5.2.2. Challenge mediante la CIE.....	12
5.2.3. Asserzione di risposta ed attributi inviati.....	12
5.2.4. Nome del service provider.....	15
5.2.5. Logout.....	15
5.3. Codici d'errore.....	15
5.4. Pulsante "Entra con CIE".....	16
6. Il processo di Onboarding.....	16
6.1. Richiesta di adesione.....	17
6.2. Federazione.....	18
6.3. Testing.....	18
7. Supporto al cittadino.....	18
8. Supporto e comunicazione agli erogatori di servizi.....	18
9. Elenco degli Enti che erogano servizi fruibili con CIE.....	19
10. Tracciature.....	19
11. APPENDICE A: Schemi di funzionamento.....	19



1. Riferimenti

- [1] - CIE messaggi V.1: specifica dei codici d'errore restituiti dal CIE ID SERVER.
- [2] - Regole tecniche SPID: https://www.agid.gov.it/sites/default/files/repository_files/circolari/spid-regole_tecniche_v1.pdf
- [3] - Portale CIE: <https://www.cartaidentita.interno.gov.it>
- [4] - Portale dei Servizi Demografici del Ministero dell'Interno: <https://dait.interno.gov.it/servizi-demografici>
- [5] - DM del 23 dicembre 2015 recante "Modalità tecniche di emissione della Carta d'Identità elettronica": <http://www.gazzettaufficiale.it/eli/id/2015/12/30/15A09809/sg>
- [6] - DECRETO LEGISLATIVO 7 marzo 2005, n. 82 Codice dell'amministrazione digitale.
- [7] – DECRETO - LEGGE 16 luglio 2020, n. 76 recante "Misure urgenti per la semplificazione e l'innovazione digitale" ("Decreto Semplificazioni"), convertito, con modificazioni, dalla L. 11 settembre 2020, n.120.

2. Pubblicazione del documento e future versioni

Questo documento è disponibile in versione aggiornata sul Portale CIE [3].

3. Ambito

Scopo del presente documento è descrivere le modalità tecniche per l'introduzione nei servizi erogati in rete dalle pubbliche amministrazioni e dai soggetti privati dell'identificazione del richiedente il servizio attraverso l'utilizzo della Carta di Identità Elettronica ("CIE 3.0") ai sensi dell'art. 64 del CAD, così come modificato dall'art. 24, comma 1 – lett. e) nn. 3) e 6) - del Decreto Semplificazioni.

Lo schema di identificazione basato sulla CIE 3.0 dettagliato nel presente documento è compatibile con il Level of Assurance 4 (HIGH) del regolamento UE 910/2014 eIDAS (GUUE C309 del 13 settembre 2019) e consente ai cittadini di fruire dei servizi offerti online dalle pubbliche Amministrazioni e dai soggetti Privati utilizzando gli elementi di sicurezza presenti sulla propria CIE (chiavi crittografiche protette da PIN e Certificati) come credenziali per la propria identificazione.

La nuova Carta d'identità elettronica è il documento di identità rilasciato dai Comuni italiani su richiesta dei cittadini che ne certifica l'identità fisica e digitale. È considerata una piattaforma abilitante ai sensi del Piano Triennale per l'informatica nella Pubblica Amministrazione dal momento che consente l'attivazione di servizi basati sull'utilizzo del microprocessore a radio frequenza di cui è dotata. Nello specifico, per il tramite della CIE 3.0 e del PIN che ciascun cittadino riceve, metà alla richiesta, metà con la carta, è possibile accedere ai servizi erogati in rete dalle PP.AA. e dai soggetti privati con i massimi livelli di sicurezza.



Lo schema di autenticazione con CIE 3.0 si basa su un modello diverso da quello utilizzato per l'accesso in rete mediante la Carta Nazionale dei Servizi "CNS".

Con la CNS, infatti, l'utente utilizza la carta come contenitore della coppia di chiavi di autenticazione TLS. Il middleware CNS consente l'autenticazione verso il sito dell'erogatore del servizio, sul quale ricade interamente l'onere della verifica della validità della catena di certificati della CA Autenticazione del Ministero dell'Interno.

Lo schema di autenticazione con la CIE supera il modello precedente, dal momento che:

- è fruibile anche in ambiente "mobile";
- offre una "user experience" migliore ed uniforme dal momento che consente di fornire in ogni caso d'uso le giuste istruzioni all'utente (es. PIN bloccato, carta scaduta, postazione non configurata);
- è pienamente rispondente alle prescrizioni del GDPR dal momento che prevede il consenso da parte dell'utente all'invio degli attributi richiesti dal servizio;
- è utilizzabile come schema di autenticazione in conformità al regolamento eIDAS;
- offre l'opportunità di conservare in modo semplice la prova dell'avvenuta autenticazione da parte del Ministero dell'Interno che consegna la CIE e i relativi codici al titolare previa identificazione da parte di operatori qualificati dei Comuni e degli Uffici consolari.

Le componenti software che costituiscono lo schema "Entra con CIE" (CIE ID APP, CIE ID SERVER, Software CIE), elaborano la richiesta di autenticazione (vedi par. 5.2.1) confermandone la correttezza e l'autenticità, al momento del rilascio dell'asserzione di avvenuta autenticazione ovvero della comunicazione di un codice di errore (vedi par. 5.2.3). Il processo di autenticazione è garantito mediante la verifica di validità (autenticità e scadenza) del certificato digitale presente a bordo della CIE che viene letto dal microprocessore della carta ed inviato presso la CA Autenticazione (cfr. DM 23 dicembre 2015 *Modalità tecniche di emissione della Carta d'identità elettronica*).

La procedura suindicata garantisce la correttezza delle informazioni sia al Ministero dell'Interno - cui è riservata l'emissione della Carta di identità elettronica (cfr. D.L. n.78/2015, art.10) – che alle pubbliche amministrazioni e ai soggetti privati che consentono l'accesso tramite CIE.

4. Schema eID basato su CIE 3.0: caratteristiche

Lo Schema di identificazione basato sulla CIE per l'accesso ai servizi prevede tre scenari di mutua autenticazione: uno scenario cosiddetto "desktop" in cui l'utente utilizza la sua CIE con una Postazione di lavoro dotata di un lettore di Smart card RF e del cosiddetto "Software CIE", uno scenario "mobile" in cui l'utente utilizza la sua CIE con uno smartphone assieme all'app di autenticazione "CieID" ed uno scenario ibrido che consente di autenticarsi ad un servizio digitale utilizzando una postazione di lavoro di tipo desktop o laptop completando il processo di autenticazione mediante uno smartphone. Lo smartphone deve essere necessariamente dotato di interfaccia NFC (Near Field Communication).

SCENARIO DESKTOP

Lo scenario desktop, raffigurato nello schema in Figura 1. Flusso di utilizzo dello scenario Desktop. prevede l'accesso in modo sicuro al servizio mediante il browser del computer e per il tramite della CIE. Per realizzare tale scenario di autenticazione, l'utente configura sulla sua postazione di lavoro un lettore di Smart card RF e il "Software CIE", un software disponibile per i Sistemi operativi Windows e MacOS disponibile all'indirizzo <https://www.cartaidentita.interno.gov.it/software-cie>, che consente l'integrazione della CIE all'interno del sistema operativo ospite quale token crittografico esterno.

Il Software CIE, in particolare, interagisce con il browser per realizzare, in maniera del tutto sicura e trasparente per l'utente, la comunicazione fra il lettore di Smart card e il microprocessore della CIE ai fini dell'instaurazione di una connessione sicura ed autenticata verso un componente server di autenticazione esposto dal Ministero dell'Interno (CieID Server). Tale componente verifica lo stato di validità del certificato digitale, preleva di attributi legati al titolare della CIE e li propaga, assieme alla conferma di avvenuta autenticazione, al servizio di cui l'utente intende fruire.

Predisposizione dell'ambiente di utilizzo dell'utente (una tantum): Effettuato il download del Software CIE, l'utente procede ad abilitare la CIE sulla sua postazione, inserendo tutte e 8 le cifre del PIN. A seguito del processo di abilitazione, la prima metà del PIN viene cifrata e salvata in una zona sicura della sua postazione di lavoro e non dovrà essere più inserita durante il processo di autenticazione. Il tutto al fine di mitigare il rischio di captazioni illecite di tutta l'informazione segreta (ad esempio attraverso strumenti di key logging).

Utilizzo:

1. L'utente, attraverso un browser web, richiede l'accesso ad un service provider specificando la CIE come meccanismo di autenticazione;
2. Il service provider invia al componente CieID Server una richiesta di autenticazione SAML (tramite il costruito <AuthnRequest>) per l'accesso al servizio;
3. Il componente CieID Server reindirizza l'utente su una pagina WEB del Ministero dell'interno che lo invita ad utilizzare la sua CIE per autenticarsi;
4. L'utente, seguendo le istruzioni a video, avvicina la CIE al lettore RF ed immette la seconda metà del PIN;
5. Verificata la correttezza del PIN, viene creato un canale sicuro HTTPS ed instaurata una sessione sicura con il componente CieID Server;
6. Il componente CieID Server, dalla sessione sicura, riceve il certificato digitale del cittadino letto dalla propria CIE e ne verifica la validità contattando la CA Autenticazione del Ministero dell'Interno. In caso di verifiche positive, recupera dal certificato gli attributi minimali del titolare della carta (nome, cognome, codice fiscale e data di nascita) e li mostra a video chiedendo il consenso a che vengano inviati al service provider;



7. L'utente visualizza sul browser gli attributi che verranno inviati al service provider;
8. L'utente, informato dell'imminente trasmissione degli attributi, conferma la volontà di inviare gli attributi e prosegue l'operazione;
9. Il componente CiED Server reindirizza l'utente verso il service provider inviando a quest'ultimo un'asserzione di avvenuta autenticazione comprensiva degli attributi;
10. Il service provider concede l'accesso al servizio.

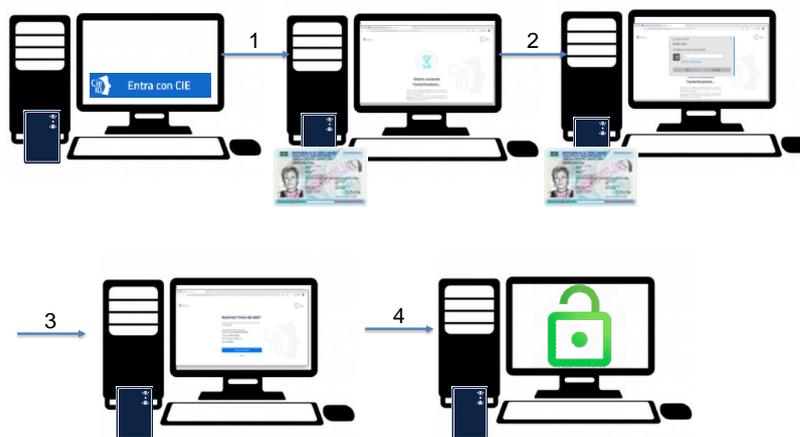


Figura 1. Flusso di utilizzo dello scenario Desktop.



SCENARIO MOBILE

Lo scenario “mobile”, raffigurato nello schema in Figura 2. Flusso di utilizzo dello scenario mobile., prevede l'utilizzo della CIE come strumento di autenticazione per ottenere l'accesso ad un service provider. Requisito necessario per realizzare tale scenario è la disponibilità dell'utente di un terminale mobile con interfaccia NFC che consenta l'interfacciamento della CIE. Allo stato dell'arte lo scenario mobile è fruibile mediante smartphone dotati di sistema operativo Android 6 o superiore, mediante il browser “Chrome”. Non è consentito l'accesso da terminali dotati di sistema operativo iOS a causa dell'impossibilità di impiego del lettore NFC per contesti di utilizzo non approvati da Apple.

Tale schema di identificazione, in dettaglio, prevede che l'utente acceda ad un servizio erogato da un service provider attraverso il browser del suo smartphone e selezioni la modalità d'accesso tramite CIE. Nel momento dell'autenticazione mediante la CIE, egli viene quindi reindirizzato all'app “CieID” che realizza il meccanismo di autenticazione per il tramite della CIE con il componente CieID Server descritto precedentemente.

Predisposizione dell'ambiente di utilizzo dell'utente (una tantum): Effettuato il download dell'app CieID, l'utente procede ad abilitare la CIE sul suo terminale, inserendo tutte e 8 le cifre del PIN. A seguito del processo di abilitazione, la prima metà del PIN viene cifrata e salvata in una zona sicura dello smartphone e non dovrà essere più inserita durante il processo di autenticazione. Il tutto al fine di mitigare il rischio di captazioni illecite di tutta l'informazione segreta (ad esempio attraverso strumenti di key logging).

Utilizzo:

1. L'utente, attraverso il browser del suo terminale mobile, richiede l'accesso ad un service provider specificando la CIE come meccanismo di autenticazione;
2. Il service provider invia al componente CIE ID SERVER una richiesta di autenticazione SAML (tramite il costruito <AuthnRequest>) per l'accesso al servizio;
3. Il componente CieID Server indirizza l'utente verso una pagina WEB del Ministero dell'Interno che lo invita ad utilizzare la sua CIE per autenticarsi ed invia una notifica al terminale mobile che provoca l'avvio dell'app “CieID”;
4. L'utente, seguendo le istruzioni mostrate dall'app, avvicina la CIE al lettore NFC dello smartphone ed immette la seconda metà del PIN;
5. Verificata la correttezza della seconda metà PIN, viene creato un canale sicuro HTTPS/TLS tra l'app CieID e il componente CieID Server;
6. Il componente CieID Server, dalla sessione sicura, riceve il certificato digitale del cittadino letto dalla propria CIE e ne verifica la validità contattando la CA Autenticazione del Ministero dell'Interno. In caso di verifiche positive, recupera dal certificato gli attributi minimali del titolare della carta (nome,



cognome, codice fiscale e data di nascita) e li mostra a video chiedendo il consenso a che vengano inviati al service provider;

7. L'utente visualizza sull'app gli attributi che verranno inviati al service provider;
8. L'utente, informato dell'imminente trasmissione degli attributi, conferma la sua volontà di inviare gli attributi e prosegue l'operazione;
9. Il componente CiID server reindirizza l'utente verso il service provider inviando a quest'ultimo un'asserzione di avvenuta autenticazione comprensiva degli attributi;
10. Il service provider concede l'accesso al servizio che avviene per il tramite del browser del terminale mobile usato al punto 1.

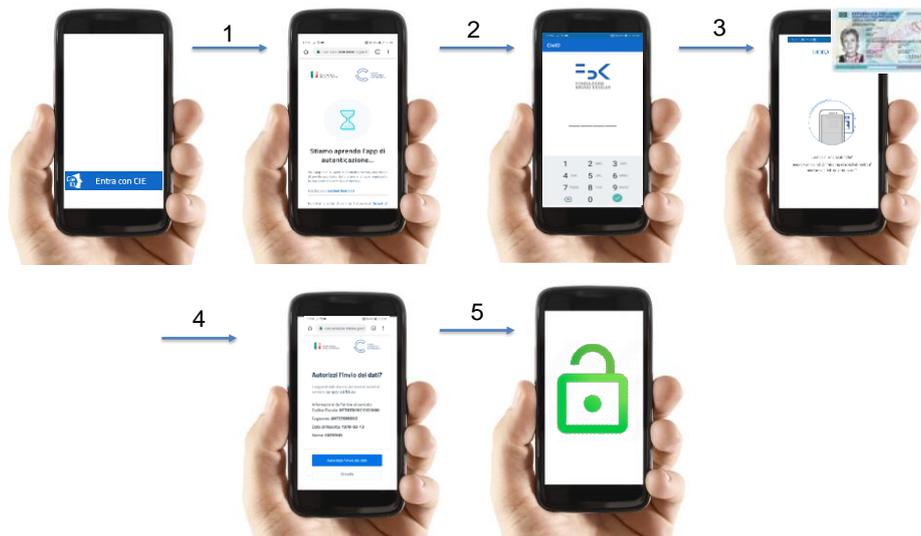


Figura 2. Flusso di utilizzo dello scenario mobile.

SCENARIO “IBRIDO”

Lo scenario “ibrido”, raffigurato nello schema in Figura 3. Schema di funzionamento dello scenario “ibrido” Figura 2. Flusso di utilizzo dello scenario mobile., prevede l’utilizzo della CIE come strumento di autenticazione per ottenere l’accesso ad un service provider. Requisito necessario per realizzare tale scenario è la disponibilità dell’utente di un terminale mobile dotato di fotocamera e di interfaccia NFC che consenta l’interfacciamento della CIE.

Tale schema di identificazione, in dettaglio, prevede che l’utente acceda ad un servizio erogato da un service provider attraverso il browser della sua postazione di lavoro (desktop o laptop). Nel momento in cui si renda necessario procedere all’autenticazione mediante l’utilizzo della CIE, l’utente immette il numero della sua carta (Numero Unico Nazionale), utilizza il suo smartphone e, dopo aver inquadrato un codice QR generato dal Ministero dell’Interno, per il tramite della CIE e della seconda metà del PIN ad ottenere dall’app CielD un codice numerico di 4 cifre, ad utilizzo singolo (one time password). L’utente inserisce quindi questo codice all’interno della apposita sezione fornita dal Ministero dell’Interno sul browser della postazione, fornisce il consenso all’invio degli attributi qualificati al servizio e prosegue quindi con l’accesso a quest’ultimo.

Predisposizione dell’ambiente di utilizzo dell’utente (una tantum): Effettuato il download dell’app CielD, l’utente procede ad abilitare la CIE sul suo terminale, inserendo tutte e 8 le cifre del PIN. A seguito del processo di abilitazione, la prima metà del PIN viene cifrata e salvata in una zona sicura dello smartphone e non dovrà essere più inserita durante il processo di autenticazione. Il tutto al fine di mitigare il rischio di captazioni illecite di tutta l’informazione segreta (ad esempio attraverso strumenti di key logging).

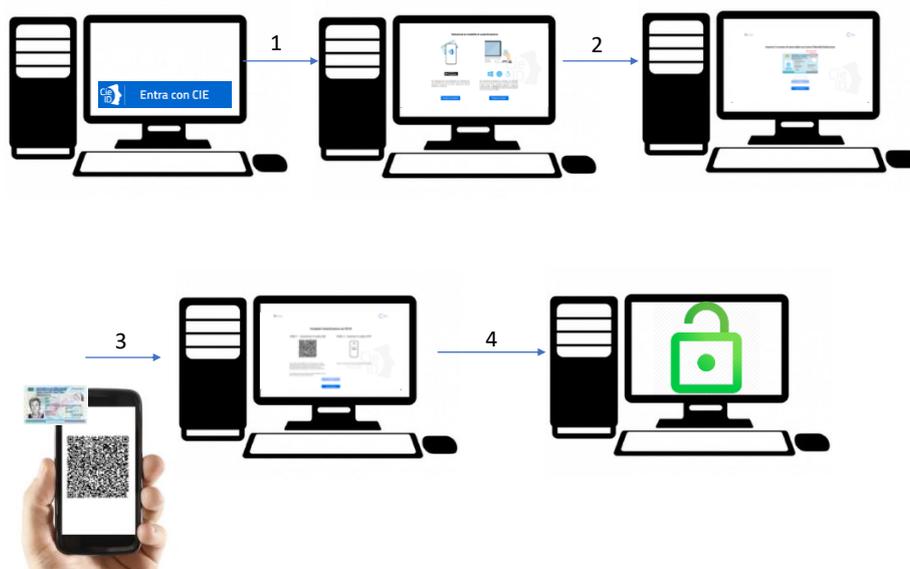


Figura 3. Schema di funzionamento dello scenario “ibrido”



5. CieID Server

L'accesso per il tramite della CIE ai servizi erogati in rete dalle PP.AA. e dai Soggetti Privati è reso possibile mediante CieID Server, un server SAML 2.0 erogato dal Ministero dell'Interno e fruibile attraverso Internet e o SPC.

CieID Server svolge le seguenti funzioni:

- Verifica la validità del certificato a bordo della CIE;
- Effettua l'identificazione informatica dell'utente;
- Ottempera all'obbligo di visualizzazione dei dati che saranno trasmessi all'erogatore di servizio.
- 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.

5.1. Metadati

CieID server è disponibile sia in ambiente di produzione che in ambiente di test/pre-produzione. I metadati XML relativi ai due ambienti sono raggiungibili ai seguenti indirizzi:

PRODUZIONE

<https://idserver.servizicie.interno.gov.it/idp/shibboleth?Metadata>

TEST/PRE-PRODUZIONE

<https://preproduzione.idserver.servizicie.interno.gov.it/idp/shibboleth?Metadata>

5.2. Protocollo

Il protocollo applicativo adottato è SAML v2.0, il profilo adottato è Web/SSO. Nel dettaglio:

- per le richieste di autenticazione (basate su costruito <AuthnRequest>) viene usato il binding **HTTP Redirect** o il binding **HTTP Post**;
- per le risposte SAML (basate su costruito <Response>) viene usato il binding HTTP POST.

Fatte salve alcune piccole differenze sotto indicate e rese necessarie dalla natura dello schema di identificazione, il protocollo adottato è compatibile con quello alla base del sistema [SPID](#).

Con riferimento alla compatibilità con SPID si riporta quanto segue:

- L'attributo "Format" dell'elemento <saml2p:Issuer> non è presente;
- L'attributo "spidCode" non è presente;
- AuthnContextClassRef è valorizzato sempre con SpidL3;



Il set di attributi restituiti è fisso e comprende sempre il **minimum dataset eIDAS**: **nome** di tipo xsd:string, **cognome** di tipo xsd:string, **data di nascita** di tipo xsd:string e valorizzata nel formato yyyy-mm-dd, **codice fiscale** di tipo xsd:string e valorizzata nel formato TINIT-<CODICE FISCALE>. Tutti gli attributi sono nel formato "urn:oasis:names:tc:SAML:2.0:attrname-format:basic".

5.2.1. Richieste di autenticazione

Il processo di autenticazione viene avviato inviando all'URI del CielD Server una richiesta di autenticazione allestita mediante il costrutto **authnRequest** della specifica SAML 2.0 Web/SSO.

CielD server accetta richieste di autenticazione nelle seguenti modalità:

1. RequestedAuthnContext con i medesimi meccanismi di "comparison" di SPID
2. AuthenticationContextClassRef pari ad uno o più dei seguenti valori:
 1. <https://www.spid.gov.it/SpidL1>
 2. <https://www.spid.gov.it/SpidL2>
 3. <https://www.spid.gov.it/SpidL3>

Nel seguito è riportato un esempio di messaggio authnRequest (sono anonimizzate le URI del service provider):

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="..."
  AttributeConsumingServiceIndex="1"
  Destination="https://idserver.servizi cie.interno.gov.it/idp/profile/SAML2/Redirect/SSO"
  ForceAuthn="true"
  ID="_bf19302cebe73ede793f7f19eaa620e8"
  IssueInstant="2018-10-30T21:47:17Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  >
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity" NameQualifier="...">
    https://test.gov.it/sp
  </saml:Issuer>
  <samlp:NameIDPolicy AllowCreate="1"
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
  />
  <samlp:RequestedAuthnContext Comparison="exact/minimum/better/maximum">
    <saml:AuthnContextClassRef>
https://www.spid.gov.it/SpidL1 (con N=1,2,3)
    </saml:AuthnContextClassRef>
  </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```



5.2.2. Challenge mediante la CIE

Dopo la fase di verifica ed elaborazione della richiesta di autenticazione, CieID Server indirizza l'utente su di una pagina che invita a poggiare la CIE sul lettore e che avvia automaticamente il processo di autenticazione mediante la CIE. L'utente deve inserire la seconda metà del PIN e confermare. Terminato il processo di autenticazione CieID Server mostrerà una pagina contenente gli attributi desunti dal certificato digitale a bordo della carta. L'utente, informato degli attributi che si stanno per inviare al servizio, proseguirà con l'operazione.

Verrà, quindi, elaborata l'asserzione di avvenuta autenticazione ed inviata al service provider.

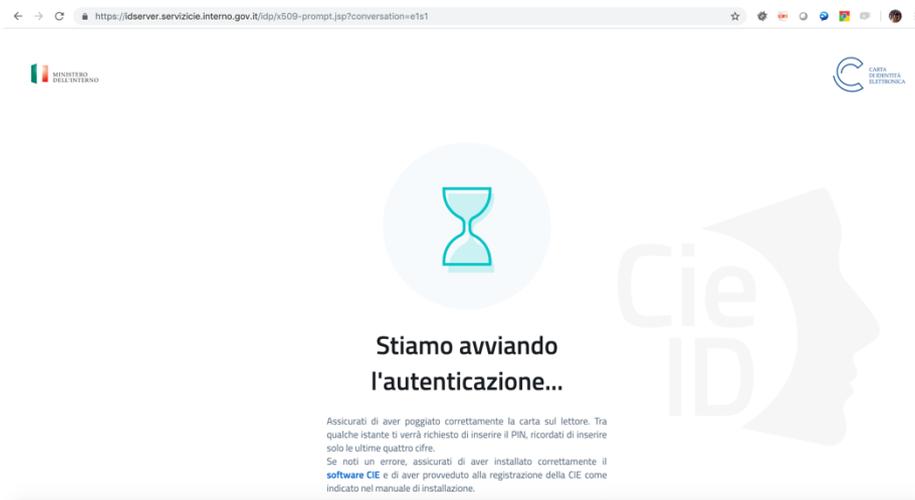


Figura 4. Processo di autenticazione del CieID Server

5.2.3. Asserzione di risposta ed attributi inviati

A seguito della fase di challenge mediante la CIE, CieID server invia in POST al service provider mediante protocollo HTTPS un messaggio di tipo saml2p:Response. Un esempio di messaggio è mostrato nel seguito (sono anonimizzati attributi e URI relative al servizio chiamante):

```
<saml2p:Response
  Destination="..."
  ID="_9a2bc46424d8d5913e68b8ae9a5773e8" InResponseTo="s2dd0fb1a0a7845132e679f9b7a3a185085cbbc134"
  IssueInstant="2019-01-31T11:26:33.825Z" Version="2.0"
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    >https://idserver.serviziocie.interno.gov.it/idp/profile/SAML2/POST/SSO</saml2:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      <ds:Reference URI="#_9a2bc46424d8d5913e68b8ae9a5773e8">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          <ec:InclusiveNamespaces PrefixList="xsd"
            xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transforms>
      </ds:Reference>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256" />
      <ds:DigestValue>IT+MfNiOHS7wtDGzJsWEFC077VZSpKlhnWlqqEH9FdQ</ds:DigestValue>
    </ds:Signature>
  </saml2p:Response>
```




```
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<saml2:Subject>
  <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
    NameQualifier="https://idserver.servizicie.interno.gov.it/idp/profile/SAML2/POST/SSO"
    SPNameQualifier="https://accessosicuro.rete.toscana.it/opensso/sp"
    >AAdzZWNyZXQxJL4i2xwuNAWShy/jW/xQ1b2hLcyjXonv24EUicZ9MEOwVOyAqoRjq5UrLs/JqqrICxD146L2zKtC+ZdKx6ZU4jpbAJyWT
+3WkrRjnz8jJxpFC5T4nPwx1LcPzQvAT9LgkgRO4+CYA79fFyQXmzXeYEQSJkt7tip3KamepjTuUxp/tMNWyRXj6wlvQ==</saml2:NameI
D>
  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml2:SubjectConfirmationData Address="192.168.224.127"
      InResponseTo="s2dd0fb1a0a7845132e679f9b7a3a185085cbbc134"
      NotOnOrAfter="2019-01-31T11:31:33.836Z"
      Recipient="..."
    />
  </saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2019-01-31T11:26:33.825Z"
  NotOnOrAfter="2019-01-31T11:31:33.825Z">
  <saml2:AudienceRestriction>
    <saml2:Audience>...</saml2:Audience>
  </saml2:AudienceRestriction>
</saml2:Conditions>
<saml2:AuthnStatement AuthnInstant="2019-01-31T11:26:32.558Z"
  SessionIndex="_07639bfc4bd74bd9a2896d6fa27add5">
  <saml2:SubjectLocality Address="..." />
  <saml2:AuthnContext>
    <saml2:AuthnContextClassRef>https://www.spid.gov.it/SpidL3</saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
</saml2:AuthnStatement>
<saml2:AttributeStatement>
  <saml2:Attribute FriendlyName="Data di Nascita" Name="dateOfBirth"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xsd:string"><DATE></saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="Codice Fiscale" Name="fiscalNumber"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xsd:string"><CF></saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="Nome" Name="name"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xsd:string"><NAME></saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="Cognome" Name="familyName"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xsd:string"><SURNAME></saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
</saml2:Assertion>
</saml2p:Response>
```



5.2.4. Nome del service provider

All'interno della schermata con la quale viene richiesto all'utente di prendere visione degli attributi qualificati che si stanno per inviare al service provider e di confermare la volontà di proseguire, è presente il **nome del servizio** a cui si sta tentando di accedere.

Tale informazione può essere specificata valorizzando opportunamente una delle seguenti sezioni nei metadati del servizio:

Service name dell'AttributeConsumingService

```
<ServiceName xml:lang="...">NOME DEL SERVIZIO</ServiceName>
```

Utilizzando la sotto sezione "UIInfo" della sezione "Extensions" e il tag "DisplayName"

```
<md:Extensions>
  <mdui:UIInfo>
    <mdui:DisplayName xml:lang="...">NOME DEL SERVIZIO</mdui:DisplayName>
  </mdui:UIInfo>
  .
  .
  .
</md:Extensions>
```

avendo cura di dichiarare il namespace "mdui": `xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"`

5.2.5. Logout

CieID Server accetta richieste "Single Logout" SAML inviate sia in modalità redirect che in modalità POST. A seguito di una richiesta di Logout, la relativa sessione viene distrutta e viene restituita una pagina di conferma come quella mostrata nel seguito. La versione attuale del CieID Server non restituisce LogoutResponse SAML.



Figura 5. Schermata di conferma di avvenuto Logout.

5.3. Codici d'errore

Nel riferimento [1] sono riportati i codici di errore restituiti da CieID Server nei vari scenari e nei vari casi particolari. Il documento evidenzia in particolare anche la "user experience" offerta all'utente da CieID Server

e quella che ciascun service provider dovrebbe implementare, durante il processo di utilizzo dello schema di autenticazione con CIE.

5.4. Pulsante “Entra con CIE”

Per consentire una esperienza utente quanto più possibile omogenea presso tutti i service provider che integrano lo schema di identificazione mediante la nuova CIE è stato allestito un pulsante “Entra con CIE” da utilizzare come “call to action” per innescare il processo di identificazione mediante CieEID Server, Si raccomanda l’utilizzo del kit disponibile all’indirizzo <https://github.com/italia/cie-graphics>.



6. Il processo di Onboarding

La fase di onboarding costituisce il prerequisito fondamentale per il processo di integrazione dello schema di autenticazione “Entra con CIE”. Può essere suddivisa in tre sottofasi distinte:

1. Richiesta formale di adesione;
2. Autorizzazione alla federazione
3. Federazione.

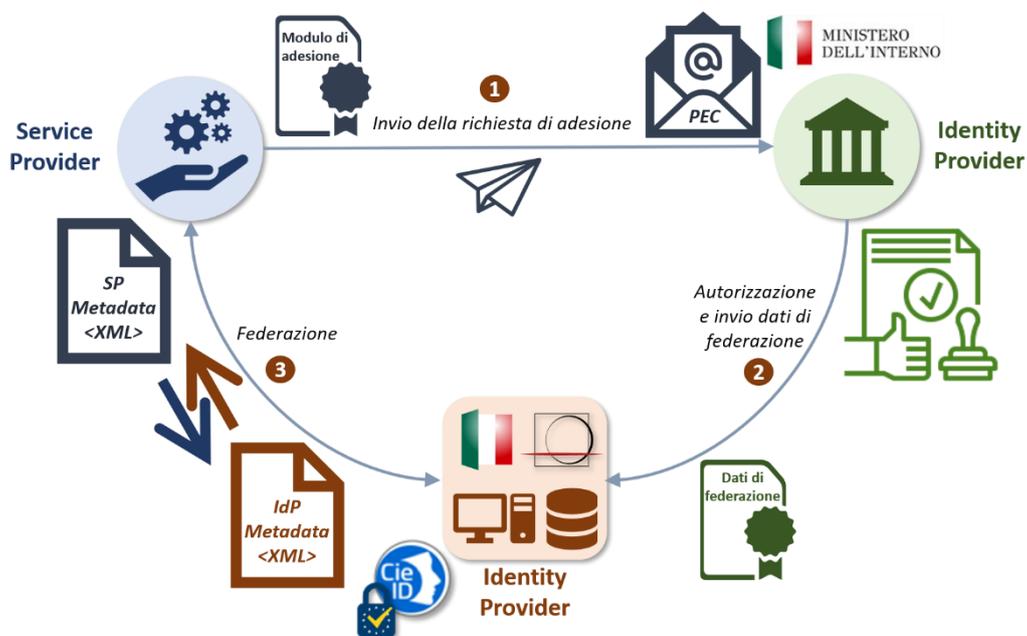


Figura 6: Processo di Onboarding “Entra con CIE”

Terminato con successo il processo di onboarding, il Service Provider può effettuare gli sviluppi software di integrazione e i test applicativi richiesti per completare l’iter di accreditamento all’utilizzo dello schema di autenticazione “Entra con CIE” per consentire ai cittadini l’accesso ai servizi online.



6.1. Richiesta di adesione

La richiesta di adesione costituisce il primo step formale e propedeutico al proseguo delle attività di federazione. Tale fase può essere avviata dal Service Provider mediante un apposito **modulo di adesione**, allegato al presente, che deve essere compilato in tutte le sue parti, firmato digitalmente e inviato all'indirizzo *PEC* del Ministero dell'Interno (**servizidemografici.prot@pec.interno.it**). Tale modulo deve contenere, oltre ai dati amministrativi dell'Ente pubblico o del soggetto privato che effettua la richiesta, anche i dati tecnici relativi al processo di federazione e i dati del referente tecnico designato dal Service Provider a svolgere le attività di integrazione e sviluppo applicativo.

Di seguito sono riportate le principali informazioni richieste:

- Le URI dei metadata di pre-produzione e produzione, raggiungibili attraverso Internet o SPC.
- Un elenco dei servizi per i quali è richiesto l'accesso tramite "Entra con CIE", con relativa breve descrizione.
- È gradito, per maggiore agevolezza nell'esecuzione dei test, che anche l'URI del servizio di pre-produzione sia raggiungibile attraverso Internet o SPC.
- È possibile effettuare esplicita richiesta di CIE di test per agevolare il Service Provider durante le attività tecniche di integrazione, avendo cura di indicare nel modulo i destinatari e gli indirizzi a cui spedire le CIE di test.
- Un elenco degli indirizzi e-mail ai quali sono collegati gli account Google per ricevere il link al download dell'App CieID di test necessaria per effettuare i test con dispositivi mobili sull'ambiente di pre-produzione dell'Identity Provider.
- Qualora il Service Provider disponga di un proprio logo, può renderlo disponibile tramite una URI per consentirne la visualizzazione al cittadino nella pagina informativa relativa all'autorizzazione all'invio dei dati personali.

Ogni modifica dei dati contenuti e sottoscritti nel suddetto modulo di adesione richiede una nuova sottomissione dello stesso. Nel caso di aggiornamento dei soli metadata tramite pubblicazione alla medesima URI indicata all'interno del modulo di adesione, è sufficiente fornire tempestiva comunicazione al referente tecnico del Poligrafico per svolgere le relative attività di aggiornamento dei dati di federazione e, conclusi i test applicativi, inviare comunicazione di avvenuto aggiornamento dei metadata al Ministero dell'Interno tramite *PEC*. In ogni caso, la richiesta di adesione ha una durata quinquennale terminata la quale è necessario effettuare nuovamente l'onboarding con il Ministero dell'Interno.

La sottoscrizione del modulo di adesione obbliga i Service Provider ad ottemperare alle condizioni generali in materia di privacy, trattamento dati e conduzione operativa. La violazione delle suddette condizioni costituisce motivo di revoca immediata dell'abilitazione al sistema di autenticazione "Entra con CIE".



6.2. Federazione

Ricevuta l'autorizzazione formale a procedere da parte del Ministero dell'Interno, il referente tecnico del Service Provider indicato in fase di richiesta di onboarding viene contattato da un referente tecnico del Poligrafico per l'avvio operativo della procedura tecnica di federazione. Quest'ultima consiste nello scambio dei metadati tra l'Identity Provider (Ministero dell'Interno) e il Service Provider che integra l'accesso mediante la CIE. Le modalità operative di creazione e scambio dei metadati, nonché le specifiche tecniche dei protocolli di comunicazione tra il Service Provider e l'Identity Provider sono descritti nel Capitolo 5.

6.3. Testing

Terminato l'onboarding, il service provider potrà avviare la fase test sull'ambiente di pre-produzione, consistente nell'esecuzione dei test funzionali volti a garantire il corretto funzionamento dell'integrazione di "Entra con CIE" all'interno del servizio in questione. Il set minimo di test che dovrà essere eseguito correttamente comprende quelli volti a provare la corretta gestione almeno dei seguenti "error codes", come da riferimento [1]:

1=Success;

21=Timeout durante l'autenticazione

22=Utente sceglie di non proseguire con l'invio degli attributi

23=Utente con CIE scaduta/revocata

25=Processo di autenticazione annullato dall'utente

Il referente, a seguito delle verifiche tecniche svolte congiuntamente con il lato Ministero dell'Interno e con il Poligrafico, verrà contattato per concordare le modalità di rollout in produzione.

7. Supporto al cittadino

L'assistenza ai cittadini su problematiche inerenti all'utilizzo dello schema di identificazione che siano riconducibili a:

1. CieID Server
2. Software CIE
3. App CieID

viene fornita secondo le modalità indicate sul sito www.cartaidentita.interno.gov.it/contatti.

8. Supporto e comunicazione agli erogatori di servizi

L'assistenza agli erogatori di servizi avverrà mediante gli indirizzi di contatto specificati nel paragrafo 2.1: ad essi verrà fornito un numero di telefono e un indirizzo e-mail del servizio di assistenza CIE presso il Viminale, a seguito dell'onboarding.

In caso di disservizio e/o problematiche di sicurezza il Ministero Interno, eventualmente avvalendosi del Poligrafico, contatterà all'indirizzo mail/telefono i referenti comunicati in fase di onboarding.



9. Elenco degli Enti che erogano servizi fruibili con CIE

Sul Portale CIE è disponibile l'elenco degli Enti che erogano servizi fruibili per il tramite della CIE che hanno completato il percorso di onboarding con il Ministero dell'Interno.

10. Tracciature

Per la tracciatura delle asserzioni da parte degli erogatori di servizi e, in generale, delle informazioni afferenti alle transazioni di autenticazione, si rimanda alle buone pratiche previste dalle regole tecniche di SPID [2].

11. APPENDICE A: Schemi di funzionamento

Sono riportati nel seguito dei diagrammi di sequenza che illustrano il meccanismo di funzionamento di dettaglio dello schema di identificazione basato su CIE presentato, sia nello scenario "Desktop" che nello scenario "Mobile"

SCENARIO DESKTOP

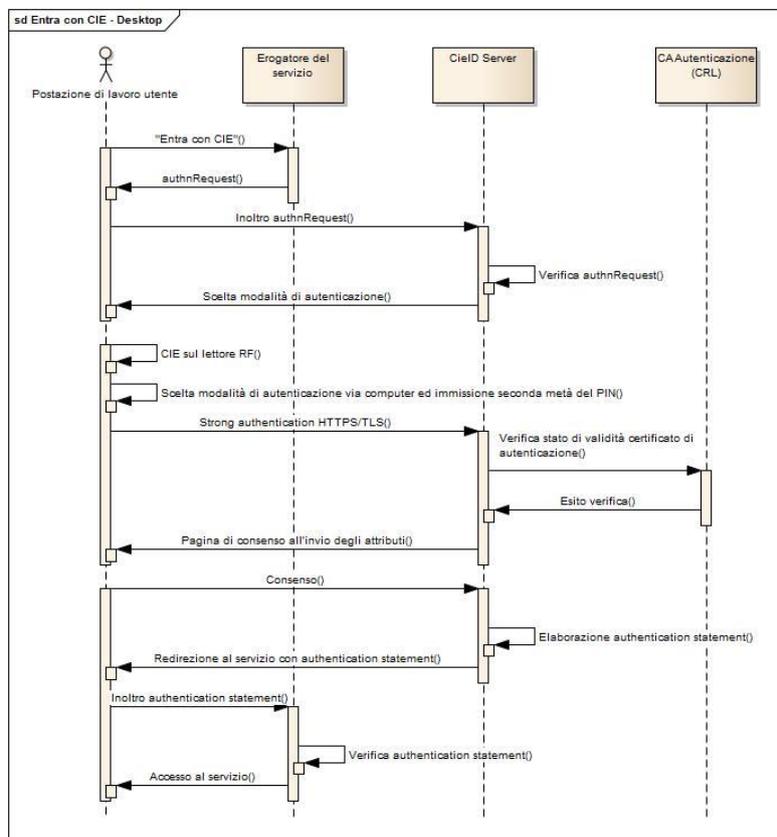


Figura 7. Scenario Desktop per l'accesso ai servizi mediante la CIE

SCENARIO MOBILE

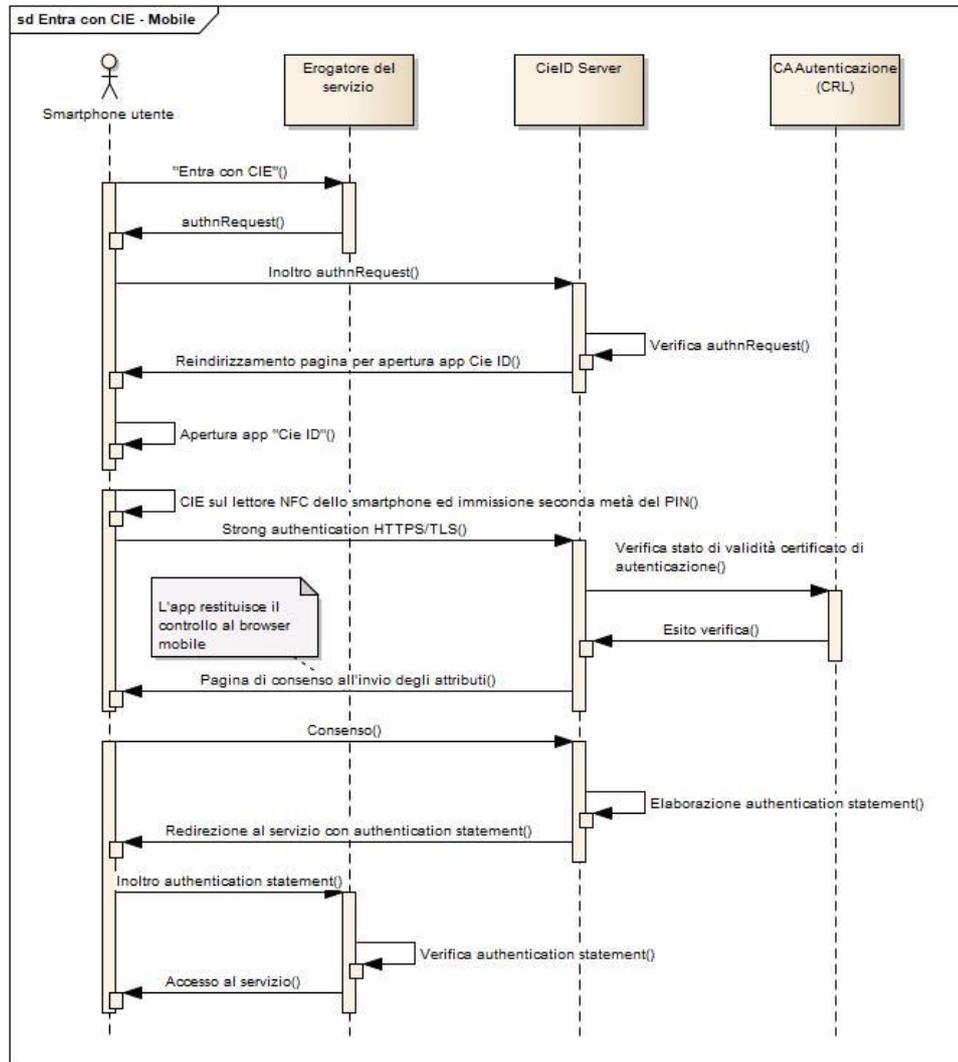


Figura 8. Scenario mobile per l'accesso ai servizi mediante la CIE



SCENARIO "IBRIDO"

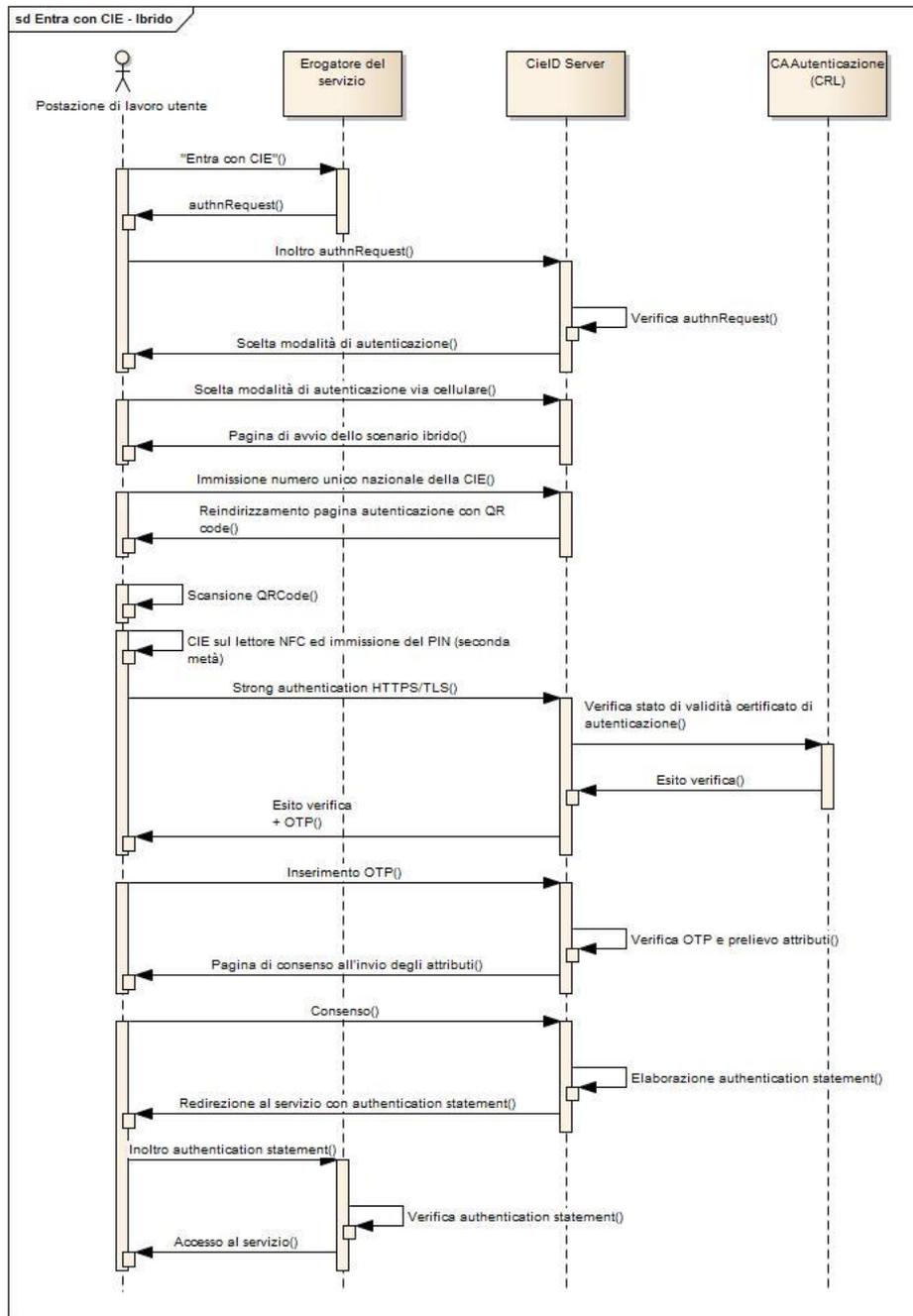


Figura 9. Scenario ibrido per l'accesso ai servizi mediante la CIE

CIE – Messaggi v1

Error code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata IdP (CIE ID SERVER)	Troubleshooting utente	Troubleshooting SP	Note
1	Autenticazione corretta	HTTP POST HTTP Redirect	200	urn:oasis:names:tc:SAML:2.0:status:Success	Fornitore del servizio (SP)				
Anomalie del sistema									
2	Indisponibilità sistema	HTTP POST		n.a.	Utente	Messaggio di errore generico	Ripetere l'accesso al servizio in un secondo momento		
3	Errore di sistema	HTTP Redirect	500	n.a.	Utente	Pagina di cortesia con messaggio "Sistema di autenticazione non disponibile - Riprovare più tardi"	Ripetere l'accesso al servizio in un secondo momento		
Anomalie delle richieste									
Anomalie sul binding									
4	Formato <i>binding</i> non corretto	HTTP Redirect	403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente	Parametri obbligatori: - SAMLRequest - SigAlg - Signature
		HTTP POST							Parametri non obbligatori: - RelayState
5	Verifica della firma fallita	HTTP Redirect	403	n.a.	Utente	Pagina di cortesia con messaggio "Impossibile stabilire l'autenticità della richiesta di autenticazione - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o con certificato non associato al corretto EntityID nei metadati registrati

Error code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata IDP (CIE ID SERVER)	Troubleshooting utente	Troubleshooting SP	Note
6	Binding su metodo HTTP errato	HTTP Redirect	403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non ricevibile - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare metadata CIE ID SERVER	Invio richiesta in HTTP-Redirect su endpoint HTTP-POST dell'identity
		HTTP POST							Invio richiesta in HTTP-POST su endpoint HTTP-Redirect dell'identity
Anomalie sul formato della AuthnReq									
7	Errore sulla verifica della firma della richiesta	HTTP POST	403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o con certificato non associato al corretto EntityID nei metadati registrati
8	Formato della richiesta non conforme alle specifiche SAML	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester ErrorCode nr08	Fornitore del servizio (SP)			Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente	Non conforme alle specifiche SAML - Il controllo deve essere operato successivamente alla verifica positiva della firma
9	Parametro <i>version</i> non presente, malformato o diverso da '2.0'	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:VersionMismatch ErrorCode nr09	Fornitore del servizio (SP)			Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente	
10	Issuer non presente, malformato o non corrisponde all'entità che sottoscrive la richiesta	HTTP POST HTTP Redirect	403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare la conformità del formato del messaggio di richiesta.	

Error code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata IdP (CIE ID SERVER)	Troubleshooting utente	Troubleshooting SP	Note	
11	<i>ID</i> (Identificatore richiesta) non presente, malformato o non conforme	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester ErrorCode nr11	Fornitore del servizio (SP)			Verificare la conformità del formato del messaggio di richiesta.		
12	<i>RequestAuthnContext</i> non presente, malformato o non previsto da scenario eID CIE	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext ErrorCode nr12	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: "Tipologia di autenticazione non supportata"		Informare l'utente	Identificatore necessario per la correlazione con la risposta. L'eventuale presenza dell'anomalia va verificata e segnalata solo a seguito di una positiva verifica della firma.	
13	<i>IssueInstant</i> non presente, malformato o non coerente con l'orario di arrivo della richiesta	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestDenied ErrorCode nr13	Fornitore del servizio (SP)			Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente		
14	<i>destination</i> non presente, malformata o non coincidente con il Gestore delle identità ricevente la richiesta	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr14	Fornitore del servizio (SP)			Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente		
15	attributo <i>isPassive</i> presente e aggiornato al valore true	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoPassive ErrorCode nr15	Fornitore del servizio (SP)			Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente		
16	<i>AssertionConsumerService</i> non correttamente valorizzato	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr16	Fornitore del servizio (SP)			Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente		
17	Attributo <i>Format</i> dell'elemento <i>NameIDPolicy</i> assente o non valorizzato secondo specifica	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr17	Fornitore del servizio (SP)			Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente		
18	Attributo <i>ConsumerServiceIndex</i> malformato o che riferisce a un valore non registrato nei metadati di SP	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr18	Fornitore del servizio (SP)			Riformulare la richiesta con un valore dell'indice presente nei metadati		
19	Riservato			Anomalie derivante dall'utente						

Error code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata IdP (CIE ID SERVER)	Troubleshooting utente	Troubleshooting SP	Note
20	Riservato								
21	Timeout durante l'autenticazione utente	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr21	Fornitore del servizio (SP)		L'operazione di autenticazione deve essere completata entro un determinato periodo di tempo	Fornire una pagina di cortesia che ricorda al cittadino di completare la richiesta di autenticazione entro un determinato periodo di tempo	
22	Utente nega il consenso all'invio di dati al SP in caso di sessione vigente	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr22	Utente; Fornitore del servizio (SP)		Necessario il consenso per la fruizione del servizio	Fornire una pagina di cortesia notificando all'utente che il diniego al consenso ha determinato il mancato accesso al servizio richiesto	
23	Utente con CIE scaduta/revocata	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr23	Utente; Fornitore del servizio (SP)	Viene notificato all'utente una finestra, nel system tray di Windows, che avverte che la CIE potrebbe essere scaduta o revocata	Verificare che la CIE non sia scaduta, verificare che non sia stata revocata; eventualmente contattare l'assistenza CIE a cie.cittadini@interno.it	Notificare all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
24	Riservato								
25	Processo di autenticazione annullato dall'utente	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr25	Utente; Fornitore del servizio (SP)			Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	