Accesso ai servizi in rete mediante la CIE 3.0

Manuale operativo per gli erogatori di servizi

Data ultimo aggiornamento: 25/11/2019

Sommario

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

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 dalle organizzazioni private dell'identificazione del richiedente il servizio attraverso l'utilizzo della Carta di Identità Elettronica ("CIE 3.0") come previsto dall'art. 64 del CAD).
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 dalle organizzazioni private 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. 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 del 23 dicembre 2015).

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. 78/2015, art.10) – che alle pubbliche amministrazioni e ai soggetti erogatori di servizi pubblici e 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 due 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" ed uno scenario "mobile" in cui l'utente utilizza la sua CIE con uno Smartphone Android dotato di interfaccia NFC assieme all'app di autenticazione "CieID".

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 costrutto <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 CieID 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.

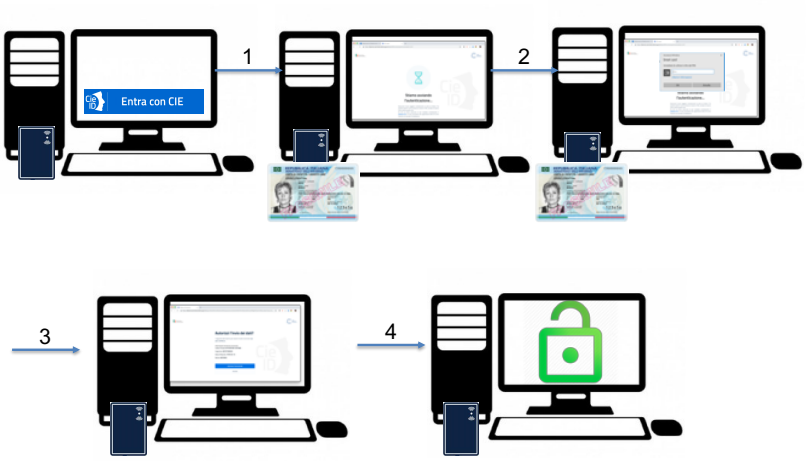

Figura 1. Flusso di utilizzo dello scenario Desktop.

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 costrutto <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 CieID 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.

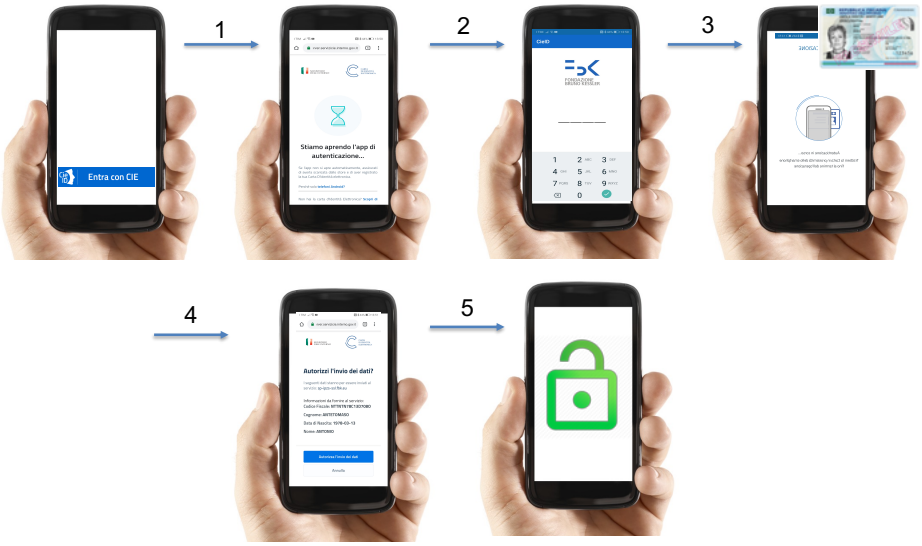

Figura 2. Flusso di utilizzo dello scenario mobile.

5. CieID Server

L'accesso per il tramite della CIE ai servizi erogati in rete dalle PP.AA. 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

TEST/PRE-PRODUZIONE
https://idserver.servizicie.interno.gov.it:8443/idp/shibboleth

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 costrutto <AuthnRequest>) viene usato il binding **HTTP Redirect** o il binding **HTTP Post**;
- per le risposte SAML (basate su costrutto <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 valorizzato 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 CieID Server una richiesta di autenticazione allestita mediante il costrutto **authnRequest** della specifica SAML 2.0 Web/SSO.

CieID 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:
   a. `https://www.spid.gov.it/SpidL1`
   b. `https://www.spid.gov.it/SpidL2`
   c. `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.servizicie.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/SpidL<N> (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.

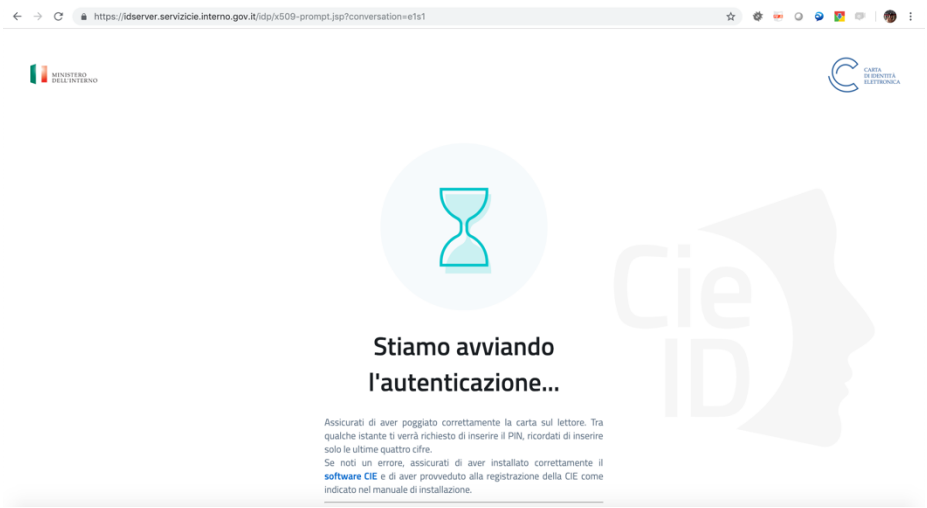

Figura 3. Processo di autenticazione del CieID Server

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.servizicie.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:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>IT+MfNiOHS7wtDGzJsWEFC077VZSpKIhnWlqqEH9FdQ=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
```

```
<ds:SignatureValue>pBOjTPYAKsChGIQGKm3W8wCcLPwPpD/CF58H/vxcrj9sjIPEshiMPmeVYkEjPQhEdRIUfIOrXzVspNNhBKc5VzPO
z6juIh06+D5Uoj1SL95tdX5K6NG0Da6LeMrIhCSzlukZMnG5oHl9KVJT1BEEiSXaRrW/4zMrX/+PjOr8KEaK84iaQyU+um7kiN5UwD16CNC
q7ymua7EINbEi27YdgIas/8TjlAk+D5BTcdTmfH17J3b/VX/YmRDiOYlEtCN/v0/POKrJQmkeaHr43yJMhbnO/OzGnVEC0xLYrYW8M7fU87
Xy+LpHxjxCuztw8903CEemhqLaF+tS8wDIPdW4Sw==</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>

<ds:X509Certificate>MIIDdTCCAl2gAwIBAgIUU79XEfveueyClDtLkqUlSPZ2o8owDQYJKoZIhvcNAQELBQAwLTErMCkG
                    A1UEAwwiaWRzZXJ2ZXIuc2Vydml6aWNpZS5pbnRlcm5vLmdvdi5pdDAeFw0xODEwMTkwODM1MDVa
                    Fw0zODEwMTkwODM1MDVaMC0xKzApBgNVBAMMImlkc2VydmVyLnNlcnZpemljaWUuaW50ZXJuby5n
                    b3YuaXQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDHraj3iOTCIILTlOzicSEuFt03
                    kKvQDqGWRd5o7s1W7SP2EtcTmg3xron/sbrLEL/eMUQV/Biz6J4pEGoFpMZQHGxOVypmO7Nc8pkF
                    ot7yUTApr6Ikuy4cUtbx0g5fkQLNb3upIg0Vg1jSnRXEvUCygr/9EeKCUOi/2ptmOVSLad+dT7Ti
                    RsZTwY3FvRWcleDfyYwcIMgz5dLSNLMZqwzQZK1DzvWeD6aGtBKCYPRftacHoESD+6bhukHZ6w95
                    foRMJLOaBpkp+XfugFQioYvrM0AB1YQZ5DCQRhhc8jejwdY+bOB3eZ1lJY7Oannfu6XPW2fcknel
                    yPt7PGf22rNfAgMBAAGjgYwwgYkwHQYDVR0OBBYEFK3Ah+Do3/zB9XjZ66i4biDpUEbAMGgGA1Ud
                    EQRhMF+CImlkc2VydmVyLnNlcnZpemljaWUuaW50ZXJuby5nb3YuaXSGOWh0dHBzOi8vaWRzZXJ2
                    ZXIuc2Vydml6aWNpZS5pbnRlcm5vLmdvdi5pdC9pZHAvc2hpYmJvbGV0aDANBgkqhkiG9w0BAQsF
                    AAOCAQEAVtpn/s+lYVf42pAtdgJnGTaSIy8KxHeZobKNYNFEY/XTaZEt9QeV5efUMBVVhxKTTHN0
                    046DR96WFYXs4PJ9Fpyq6Hmy3k/oUdmHJ1c2bwWF/nZ82CwOO081Yg0GBcfPEmKLUGOBK8T55ncW
                    +RSZadvWTyhTtQhLUtLKcWyzKB5aS3kEE5LSzR8sw3owln9P41Mz+QtL3WeNESRHW0qoQkFotYXX
                    W6Rvh69+GyzJLxvq2qd7D1qoJgOMrarshBKKPk+ABaLYoEf/cru4e0RDIp2mD0jkGOGDkn9XUl+3
                    ddALq/osTki6CEawkhiZEo6ABEAjEWNkH9W3/ZzvJnWo6Q==</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </saml2p:Status>
    <saml2:Assertion ID="_beeacdd8c64be12d6c2e9ac905673168" IssueInstant="2019-01-31T11:26:33.825Z"
        Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <saml2:Issuer>https://idserver.servizicie.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="#_beeacdd8c64be12d6c2e9ac905673168">
                    <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:Transform>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                    <ds:DigestValue>WVU3hFTIWNlwjTLO1PtT5N4OLe0NJ0/VcC8B18Bqet0=</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>

<ds:SignatureValue>ty0hOoLydEI8ilcERvSIq21AIp3mtkJOyl0sVSDy68JEENscInJ/Jwz1rxBsCjbloVLCsOzY4Q6bMBZMIh5+7ETZ
B5yzei3F5uYBupDaSBbJRJUzl+aybOm4Qp9JIuisSaG6at6MU80qvKg0er8AEG6OVeKQpIP/1L3Y0InCCo1YgYCjcKRdRiKWreUxmTDwM8/
/x26ZoUdJcscrmGIgE9hNmeDta6dtq1911gkovZqCl+45ENnctQoZszX3iIceTgy/3waiLLlyMikH/7iJ1zKzKl71ij08IcQraqU64LuySU
amDeUUIx2lqANeH1/vp4dVZ0LaF+pW2H5EHzYZUg==</ds:SignatureValue>
            <ds:KeyInfo>
                <ds:X509Data>

<ds:X509Certificate>MIIDdTCCAl2gAwIBAgIUU79XEfveueyClDtLkqUlSPZ2o8owDQYJKoZIhvcNAQELBQAwLTErMCkG
                        A1UEAwwiaWRzZXJ2ZXIuc2Vydml6aWNpZS5pbnRlcm5vLmdvdi5pdDAeFw0xODEwMTkwODM1MDVa
                        Fw0zODEwMTkwODM1MDVaMC0xKzApBgNVBAMMImlkc2VydmVyLnNlcnZpemljaWUuaW50ZXJuby5n
                        b3YuaXQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDHraj3iOTCIILTlOzicSEuFt03
                        kKvQDqGWRd5o7s1W7SP2EtcTmg3xron/sbrLEL/eMUQV/Biz6J4pEGoFpMZQHGxOVypmO7Nc8pkF
                        ot7yUTApr6Ikuy4cUtbx0g5fkQLNb3upIg0Vg1jSnRXEvUCygr/9EeKCUOi/2ptmOVSLad+dT7Ti
                        RsZTwY3FvRWcleDfyYwcIMgz5dLSNLMZqwzQZK1DzvWeD6aGtBKCYPRftacHoESD+6bhukHZ6w95
                        foRMJLOaBpkp+XfugFQioYvrM0AB1YQZ5DCQRhhc8jejwdY+bOB3eZ1lJY7Oannfu6XPW2fcknel
                        yPt7PGf22rNfAgMBAAGjgYwwgYkwHQYDVR0OBBYEFK3Ah+Do3/zB9XjZ66i4biDpUEbAMGgGA1Ud
                        EQRhMF+CImlkc2VydmVyLnNlcnZpemljaWUuaW50ZXJuby5nb3YuaXSGOWh0dHBzOi8vaWRzZXJ2
                        ZXIuc2Vydml6aWNpZS5pbnRlcm5vLmdvdi5pdC9pZHAvc2hpYmJvbGV0aDANBgkqhkiG9w0BAQsF
                        AAOCAQEAVtpn/s+lYVf42pAtdgJnGTaSIy8KxHeZobKNYNFEY/XTaZEt9QeV5efUMBVVhxKTTHN0
                        046DR96WFYXs4PJ9Fpyq6Hmy3k/oUdmHJ1c2bwWF/nZ82CwOO081Yg0GBcfPEmKLUGOBK8T55ncW
                        +RSZadvWTyhTtQhLUtLKcWyzKB5aS3kEE5LSzR8sw3owln9P41Mz+QtL3WeNESRHW0qoQkFotYXX
                        W6Rvh69+GyzJLxvq2qd7D1qoJgOMrarshBKKPk+ABaLYoEf/cru4e0RDIp2mD0jkGOGDkn9XUl+3
                        ddALq/osTki6CEawkhiZEo6ABEAjEWNkH9W3/ZzvJnWo6Q==</ds:X509Certificate>
                </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/xQ1b2hLcyjXonv24EUIcZ9MEAOwVOyAqoRjq5UrLs/JqqrICxDl46L2zKtC+ZdKx6ZU4jpBAJywT
+3WkrRjnz8jJxpFC5T4nPwx1LcPzQvAT9LgkgRO4+CYA79fFyQXmzXeYEQSJkt7tip3KamepjTuUxp/tMNWyRXj6w1vQ==</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="_07639bfcb4bd74bd9a2896d6fa27add5">
            <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>
```

5.3. 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 CieIEID Server, Si raccomanda l'utilizzo del kit disponibile all'indirizzo https://github.com/italia/cie-graphics.

6. Procedura di onboarding e testing

6.1. Onboarding

Perché un service provider possa fruire di accedere a CieID server è richiesta una prima fase di **onboarding** con il Ministero dell'Interno, da eseguire una tantum. La fase di onboarding consiste nello scambio dei metadati tra CieID server e il service provider che integra l'accesso mediante la CIE.

Per richiedere l'onboarding dei propri metadati, ciascun service provider deve inviare una richiesta via mail all'indirizzo PEC servizidemografici.prot@pec.interno.it, specificando in un documento digitalmente sottoscritto nel corpo della e-mail aderente al template fornito in allegato:

1. L'URI di produzione a cui raggiungere i metadati del servizio in cui integrare "Entra con CIE";
2. L'URI di test/collaudo a cui raggiungere i metadati del servizio in cui integrare "Entra con CIE";
3. L'URI del servizio di produzione;
4. L'URI del servizio di collaudo;
5. L'indirizzo e-mail di un referente per il servizio in questione, quale riferimento per le fasi di test e supporto durante l'esercizio;
6. Un contatto telefonico del suddetto referente;
7. Un indirizzo e-mail e un recapito telefonico del servizio di assistenza tecnica relativo al sistema in questione;
8. Se necessita di CIE di test e, in tal caso, l'indirizzo a cui spedire tali supporti;
9. Se intende utilizzare la versione di pre-esercizio dell'app "CieID". In tal caso è necessaria l'iscrizione al Google Group appositamente creato disponibile all'indirizzo: https://groups.google.com/d/forum/cie-id. L'iscrizione al gruppo, oltre a permettere di unirsi alla community di sviluppo di CieID, fornisce il diritto al download della versione di test dell'app CieID di test con la quale è possibile eseguire l'autenticazione con l'ambiente di pre-esercizio del Ministero dell'Interno.
10. L'elenco dei servizi con le relative descrizioni, che verranno resi fruibili per il tramite della CIE.

Qualora il service provider disponga di un proprio logo e ne comunichi l'URI per consentirne il download, esso verrà utilizzato dal CieID Server, nella pagina informativa relativa all'invio degli attributi.

Le URI dei metadati di pre-produzione e produzione e tutte le URI contenute all'interno dei 2 set di metadati (pre-produzione e produzione) devono essere raggiungibili attraverso Internet o SPC.

È gradito, per maggiore agevolezza nell'esecuzione dei test, che anche l'URI del servizio di pre-produzione sia raggiungibile attraverso Internet o SPC.

6.2. 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

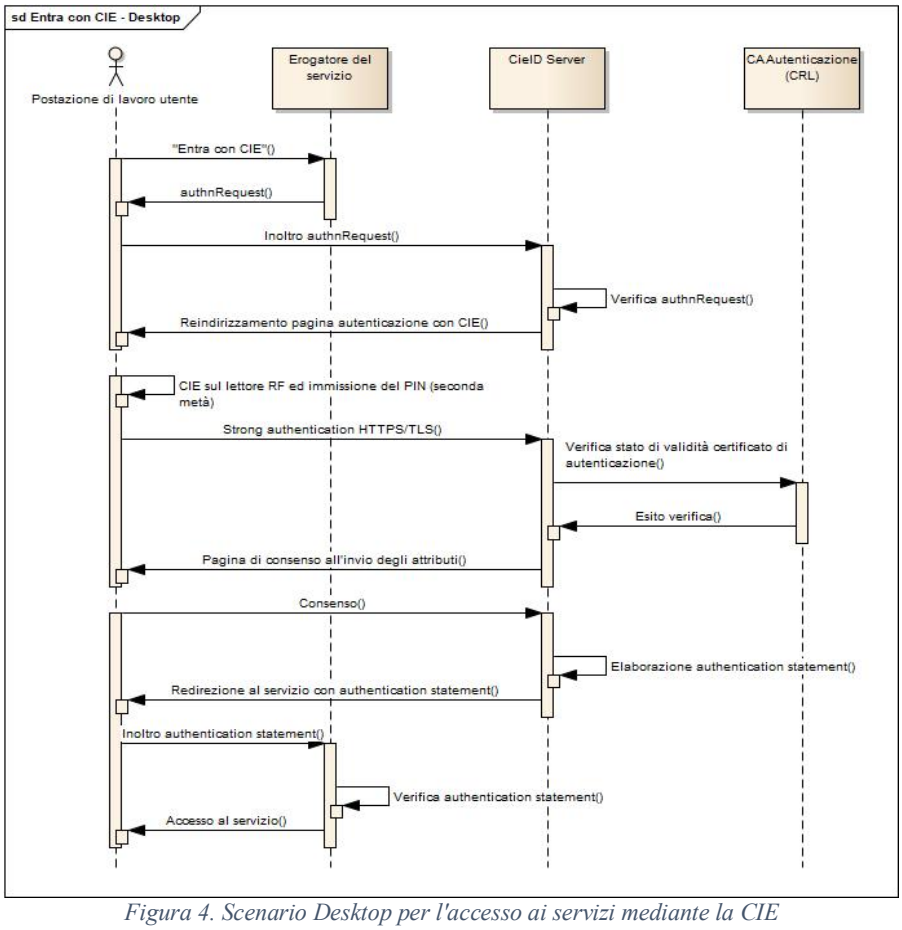

Figura 4. Scenario Desktop per l'accesso ai servizi mediante la CIE

SCENARIO MOBILE

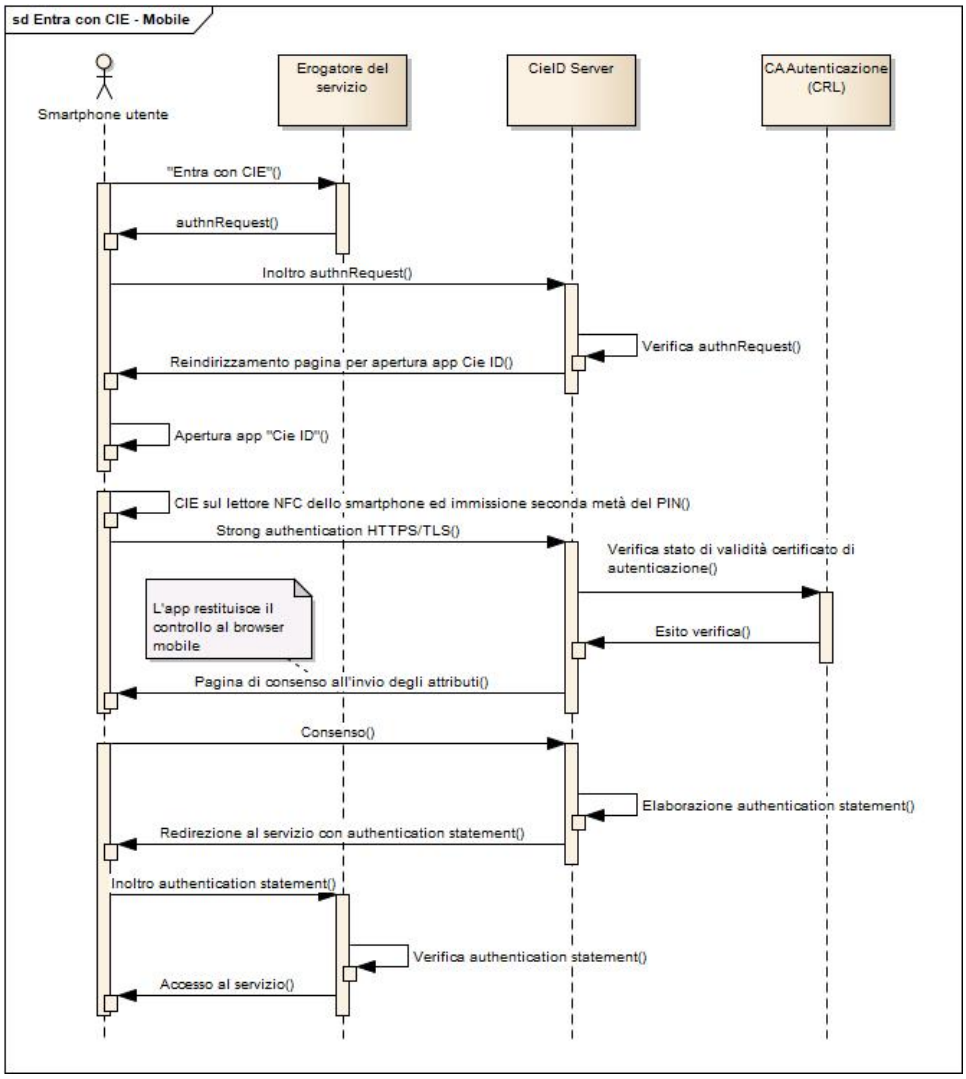

Figura 5. Scenario mobile per l'accesso ai servizi mediante la CIE