Manuale Tecnico per gli erogatori di servizi pubblici e privati

Release bozza

italia

23 mag 2022

Indice dei contenuti

CAPITOLO 1

Introduzione

La Carta di Identità Elettronica (CIE), rilasciata dallo Stato italiano, grazie alla presenza di un chip a radiofrequenze nel quale sono contenuti i dati personali e biometrici del titolare e un certificato digitale di autenticazione, estende il tradizionale concetto di identità fisica, configurandosi come strumento di identità digitale che soddisfa i requisiti massimi di sicurezza. Interoperabile anche in ambito europeo, lo schema di identificazione «Entra con CIE», in analogia a quanto previsto da SPID, realizza un sistema di autenticazione federato per l'identificazione dei cittadini presso i soggetti pubblici e privati che aderiscono allo schema. Si basa sul protocollo SAML v2 (Security Assertion Markup Language) per il profilo «Web Browser SSO» (SAML V2.0 Technical Overview[1]) dal quale eredita gran parte dei requisiti tecnici. Lo scopo del presente documento è quello di definire le specifiche tecniche per l'integrazione di Entra con CIE come schema di autenticazione per l'accesso ai servizi in rete erogati da PP.AA. e privati.

[1] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

CAPITOLO 2

Soluzione eID basata sulla CIE

Lo schema di autenticazione Entra con CIE é di tipo Single Sign-On (SSO) federato e dunque prevede l'introduzione di un gestore dell'identitá dell'utente, un Identity Provider (IdP), al quale i fornitori di servizi online, Service Provider (SP), richiedono, previa federazione, la verifica dell'identitá dell'utente. In particolare lo schema Entra con CIE prevede l'istituzione di un IdP unico, il Ministero dell'Interno, che in qualitá di ente responsabile dell'emissione della CIE, ne cura anche gli aspetti legati all'impiego documento come strumento di identitá digitale. Di seguito viene mostrato uno schema logico della soluzione eID basata sulla CIE.

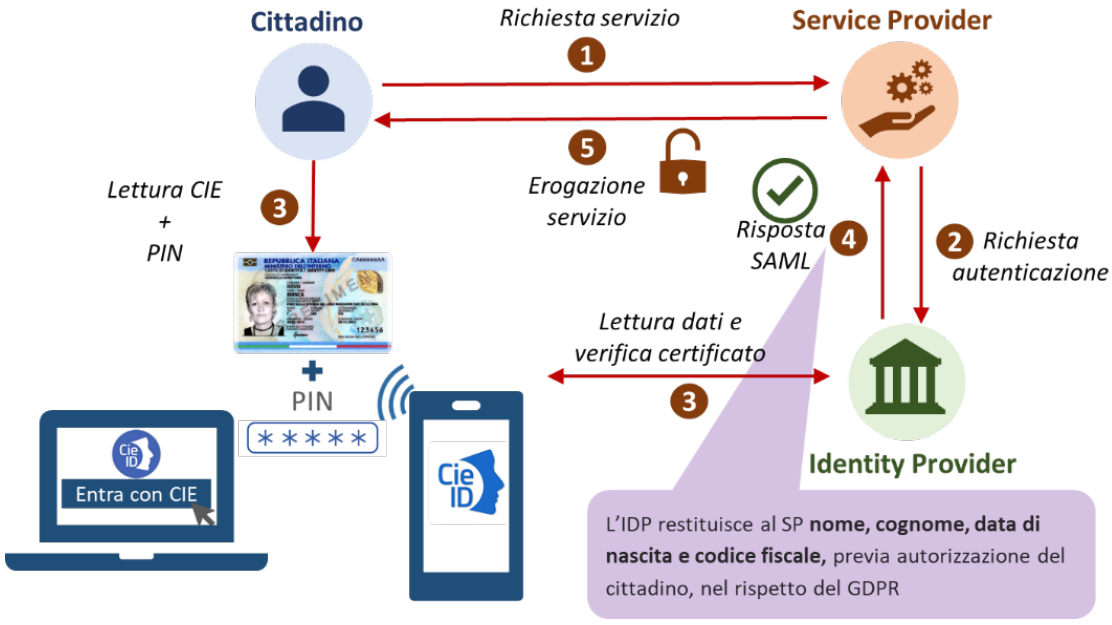

Fig. 2.1: Schema di autenticazione Entra con CIE.

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

sviluppato e gestito dal Poligrafico e Zecca dello Stato S.p.A. (PZS) che riveste il ruolo di partner tecnologico del Ministero dell'Interno, svolge le seguenti funzioni:

- Effettua l'identificazione informatica dell'utente;
- Verifica la validità del certificato a bordo della CIE;
- 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.

Nota: L'interazione con l'utente da parte della componente CieID Server, puó avvenire secondo diverse modalitá

- **Modalitá «desktop»**: l'utente avvia la richiesta del servizio tramite un browser installato sul proprio computer ed effettua l'autenticazione richiesta dall'IdP usando un lettore *contactless* collegato al computer
- **Modalitá «mobile»**: l'utente avvia la richiesta del servizio tramite un browser installato su un dispositivo mobile (smartphone o tablet) dotato di interfaccia NFC e completa la fase di autenticazione avvicinando la CIE al proprio dispositivo;
- **Modalitá «computer + smartphone»**: l'utente avvia la richiesta del servizio tramite un browser installato sul proprio computer ed effettua l'autenticazione avvicinando la CIE al proprio dispositivo mobile dotato di interfaccia NFC

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

1. richiesta del servizio esposto dal portale/app del Service Provider che avviene all'interno del browser dell'utente nel dominio del SP;
2. autenticazione dell'utente effettuata direttamente dall'Identity Provider.

Per quanto concerne il primo punto, la richiesta avviene tramite una «*call to action*» realizzata dal Service Provider tramite un apposito pulsante «Entra con CIE» e che ha come *landing page* un *endpoint* del Ministero dell'Interno il quale innesca il processo di identificazione mediante la componente server CieID dell'IdP. Per consentire una esperienza utente quanto più possibile omogenea presso tutti i service provider che integrano lo schema di identificazione mediante la CIE si deve utilizzare il kit disponibile all'indirizzo https://github.com/italia/cie-graphics.

In riferimento al secondo punto, invece, l'autenticazione dell'utente é avviata dall'Identity Provider che richiede la lettura della CIE e in particolare l'invio del certificato digitale X.509 di autenticazione presente nel chip del documento e protetto dal codice PIN. La comunicazione a basso livello con la carta varia a seconda delle modalitá di utilizzo. Nel caso di modalitá «desktop» é possibile scaricare e installare un appposito software denominato CieID (Middleware) disponibile per i Sistemi operativi Windows, MacOS e Linux 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. Nel caso di autenticazione effettuata tramite un dispositivo mobile, é possibile scaricare gratuitamente e installare l'App «CieID» direttamente dallo Store online (Android[2] o iOS[3]).

Allo stato dell'arte questa modalitá è fruibile mediante smartphone dotati di tecnologia NFC e sistema operativo Android 6 o superiore, mediante il browser "Chrome", e iPhone 7 o superiori con sistemi operativi iOS 13 o superiore[7] , mediante browser Safari. Tutte le componenti software, sia lato server IdP e sia client (Middleware e App CieID), sono sviluppate e gestite dal Poligrafico che cura anche le attività di supporto e assistenza tecnica al Service Provider nell'utilizzo di tali strumenti e durante l'intero iter di integrazione dello schema «Entra con CIE» all'interno dei servizi erogati dai SP.

[2] https://play.google.com/store/apps/details?id=it.ipzs.cieid

[3] https://apps.apple.com/it/app/cieid/id1504644677

[7] Non è consentito l'accesso da terminali dotati di sistema operativo iOS precedenti alla release 13 a causa dell'impossibilità di impiego del lettore NFC per contesti di utilizzo non approvati da Apple.

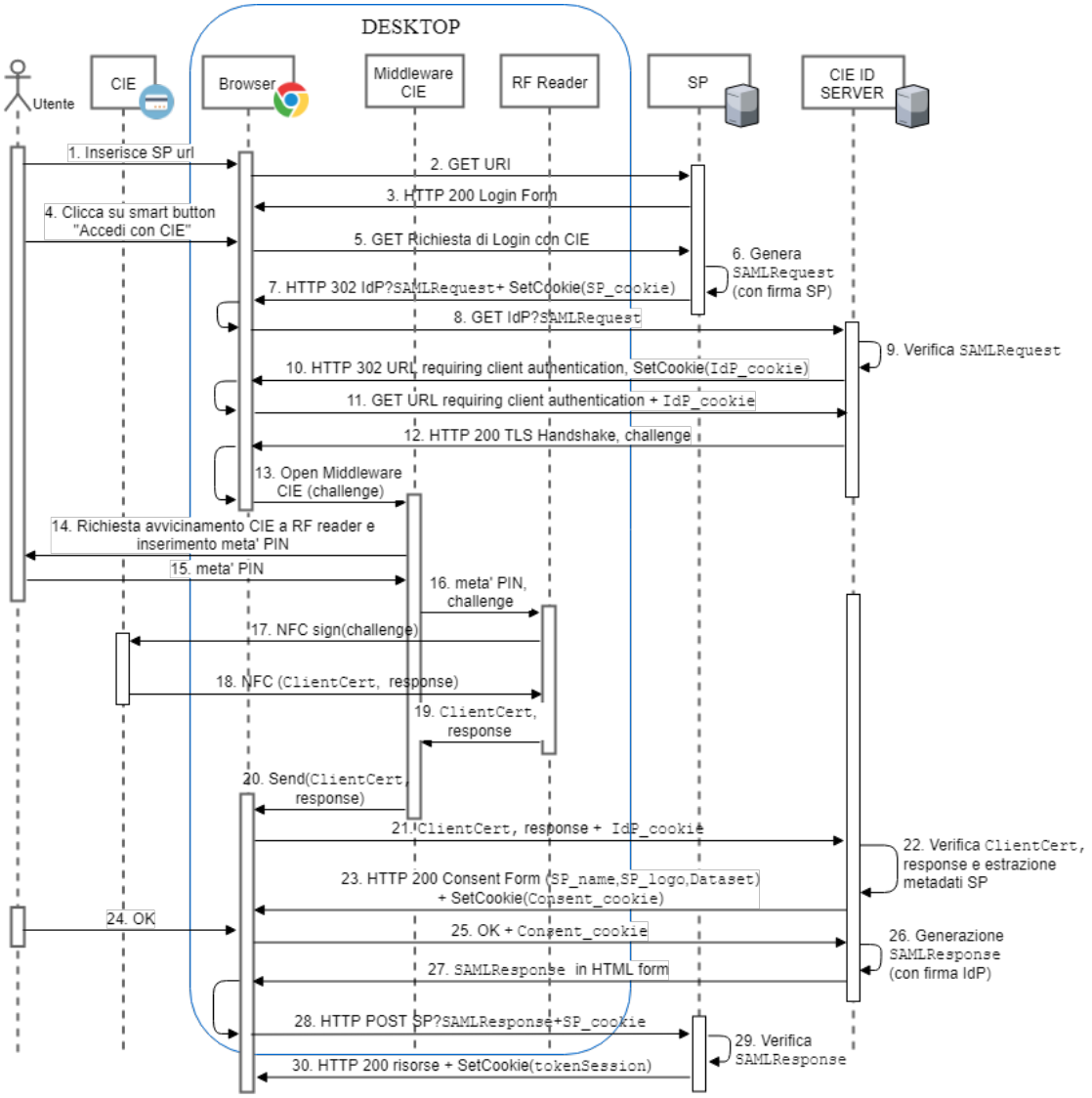

Fig. 2.2: Schema di autenticazione Entra con CIE tramite modalitá «desktop».

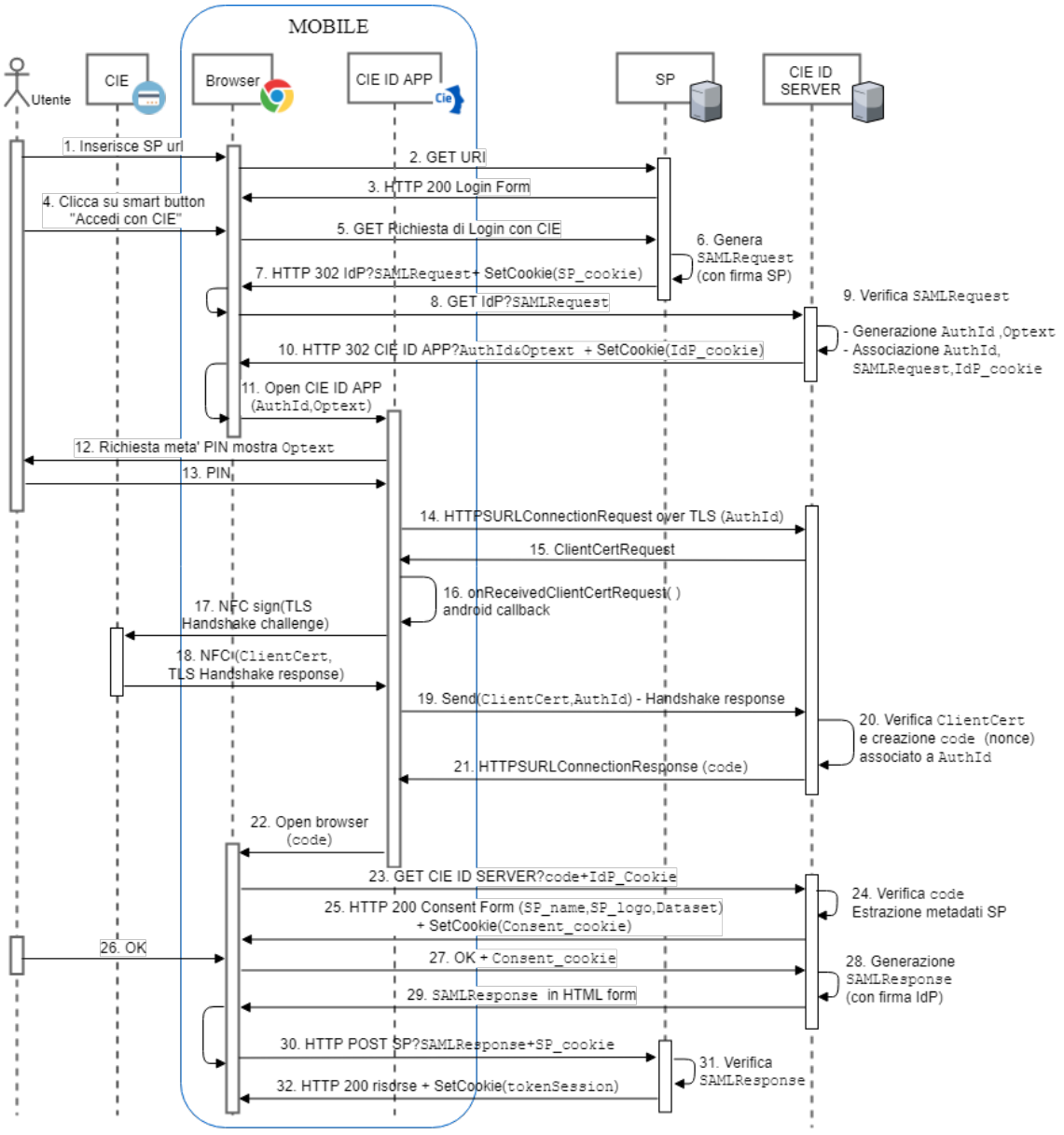

Fig. 2.3: Schema di autenticazione Entra con CIE tramite modalitá «mobile».

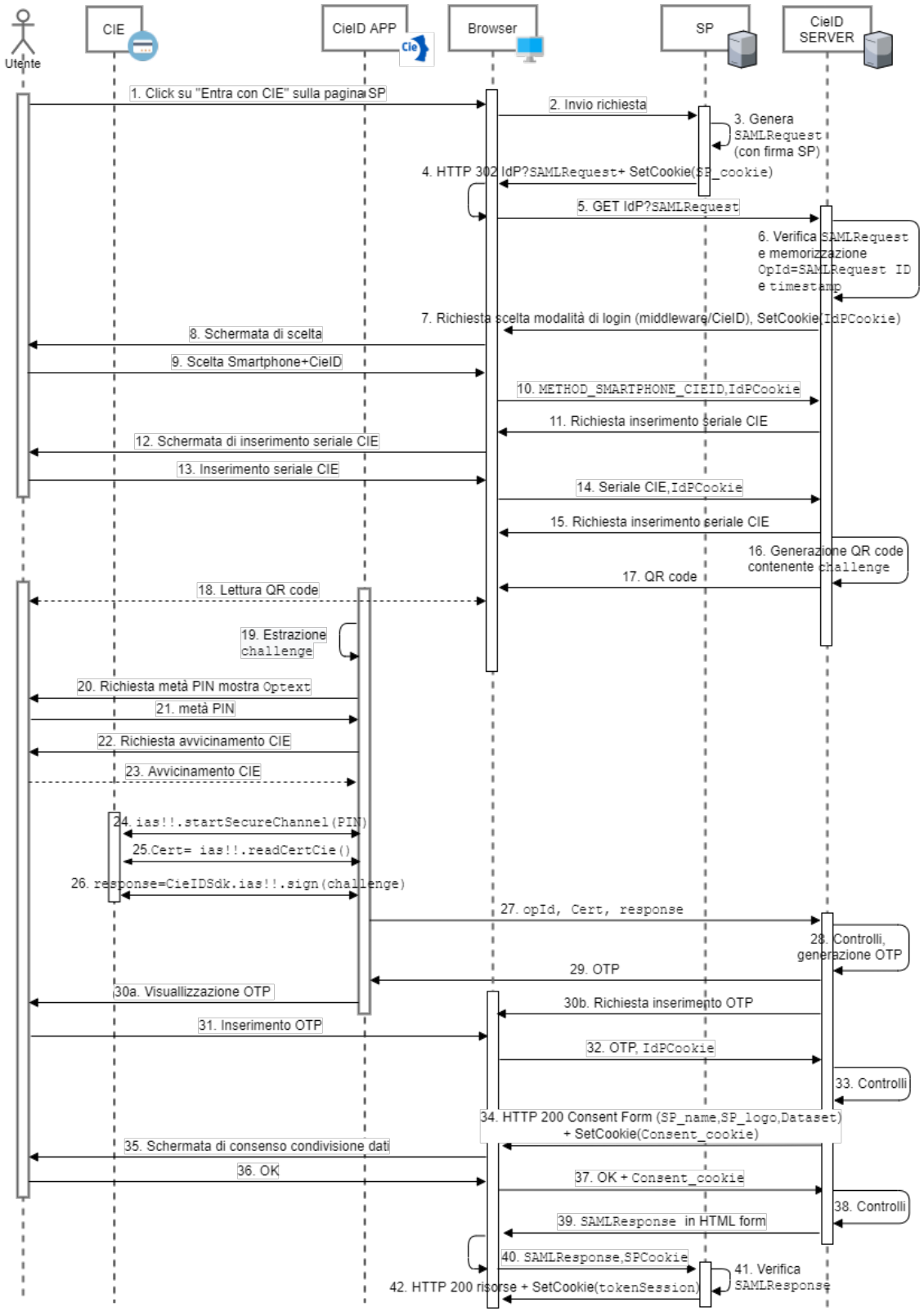

Fig. 2.4: Schema di autenticazione Entra con CIE tramite modalitá «computer + smartphone».

Fig. 2.5: Pulsante ufficiale «Entra con CIE»

Fig. 2.6: App CieID Android - Link per il download

Fig. 2.7: App CieID iOS - Link per il download

Nota: Ai fini di sviluppo, per effettuare i test in ambiente di pre-produzione e di produzione disponibili presso il Ministero dell'Interno, é possibile utilizzare il software CieID disponibile per computer, secondo lo scenario «desktop» appena presentato. Per i test in modalitá «mobile» o «computer + smartphone», non é possibile, invece, usare l'App CieID «ufficiale» in ambiente di pre-produzione ma é necessario installare l'App CieID di test[8] disponibile al seguente link[4] .

Fig. 2.8: App CieID di test - Link per il download

Per effettuare i test in pre-produzione tramite l'App CieID di test o mediante il software CieID e agevolare gli sviluppi applicativi, é possibile usare, in caso di indisponibilitá di una CIE «autentica», le carte di test che é possibile richiedere in fase di onboarding tramite il portale di federazione erogatori di sevizi[5] (cfr. il Manuale operativo per i fornitori di servizi pubblici e privati[6] per ulteriori dettagli sul processo di onboarding).

Per i Service Provider interessati a fornire al cittadino i propri servizi online tramite una App proprietaria, ci sono due modalitá di integrazione:

- Flusso con reindirizzamento: l'App del Service Provider, all'atto della richiesta di autenticazione dell'utente, reindirizza la richiesta all'App CieID che gestisce direttamente l'autenticazione con la CIE.
- Flusso integrato: il processo di autenticazione viene effettuato direttamente in maniera nativa all'interno dell'App del Service Provider, il quale integra la comunicazione con la CIE mediante una libreria software rilasciata e gestita dal Poligrafico.

Agli indirizzi https://github.com/italia/cieid-android-sdk e https://github.com/italia/cieid-ios-sdk, sono disponibili gratuitamente le SDK Android e iOS che mettono a disposizione esempi di codice sorgente per l'integrazione dei due flussi sopra riportati nonché una libreria software per l'integrazione del flusso integrato con esempi.

Indipendentemente dalla modalitá di realizzazione della fase di autenticazione, per realizzare lo schema Entra con CIE é necessario che il Service Provider effettui i seguenti passi operativi:

1. predisposizione dei metadata necessari per la fase di federazione (cfr. *Federazione* (pagina 9));
2. implementazione dei protocolli SAML di comunicazione con l'IdP per gestire correttamente le fasi di Single Sign-On e di Logout (cfr. *Protocolli di comunicazione* (pagina 20) e *Modalitá di trasmissione dei messaggi* (pagina 31));
3. verifica e validazione della corretta implementazione del servizio di autenticazione (cfr. *Testing* (pagina 45)).

Nei paragrafi successivo verranno descritte nel dettaglio le fasi operative appena riportate.

[8] L'App CieID di test é attualmente disponibile solo per dispositivi Android.
[4] https://install.appcenter.ms/users/ipzsapp/apps/cieid-preproduzione/distribution_groups/public%20link
[5] https://federazione.servizicie.interno.gov.it
[6] https://docs.italia.it/italia/cie/cie-manuale-operativo-docs

CAPITOLO 3

Federazione

In accordo con il protocollo SAML, l'accesso al servizio di autenticazione offerto dal Ministero dell'Interno in qualitá di IdP, é consentito tramite un meccanismo preliminare di federazione che consiste nello scambio di metadata che descrivono in un modo standardizzato gli attori coinvolti, le risorse, il supporto e gli endpoint che espletano effettivamente i servizi federati.

3.1 Metadata IdP

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

- Metadati di PRODUZIONE[9]
- Metadati di TEST/PRE-PRODUZIONE[10]

3.2 Metadata SP

Il Service Provider (SP) deve predisporre un file di metadata conforme allo standard SAML v2 e, tramite una apposita sezione presente nel portale di federazione erogatori di sevizi[11], deve effettuare il caricamento del metadata sugli ambienti di pre-produzione e produzione messi a disposizione dal Ministero dell'Interno (cfr. il Manuale operativo per i fornitori di servizi pubblici e privati[12] per ulteriori dettagli sul processo di onboarding). É possibile, inoltre, aggiornare un metadata già federato utilizzando la medesima procedura di caricamento dei metadata prevista dal portale di federazione sopra citato. É consentito, nell'ambito di una richiesta di federazione, il caricamento di un solo file di metadata per ambiente, e ogni caricamento successivo andrà a sostituire il precedente file di metadata.

Nota: Dal punto di vista tecnico i metadata, oltre a ereditare le specifiche dallo standard SAML v2, condividono gran parte della struttura con quella attualmente prevista dalle Regole Tecniche SPID. Le differenze principali riguardano

[9] https://idserver.servizicie.interno.gov.it/idp/shibboleth?Metadata
[10] https://preproduzione.idserver.servizicie.interno.gov.it/idp/shibboleth?Metadata
[11] https://federazione.servizicie.interno.gov.it
[12] https://docs.italia.it/italia/cie/cie-manuale-operativo-docs

sostanzialmente le informazioni aggiuntive e di censimento del Service Provider e dell'eventuale partner tecnologico che cura gli aspetti tecnici di onboarding. Per maggiori dettagli consultare il capitolo *Interoperabilità con SPID* (pagina 34)

3.3 Struttura del metadata

Un file metadata é strutturato gerarchicamente in un elemento radice `<md:EntityDescriptor>` (un server SAML che esegue determinati compiti per conto ad esempio di un SP) e uno o piú elementi ad esso associato. Diversamente da quanto prescritto dallo standard SAML v.2, che consente, tramite l'elemento radice `md:EntitiesDescriptor>`, di inserire in un unico metadata più `<md:EntityDescriptor>`, lo schema «Entra con CIE» prevede obbligatoriamente un solo elemento `<md:EntityDescriptor>` come radice del metadata.

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https:/
↪/service-provider.it/sp">
   [...]
</md:EntityDescriptor>
```

Nota: Ogni entità (Service Provider, Identity Provider, o altra), in una federazione SAML, è tecnicamente identificata e distinta dalle altre entità mediante il suo *EntityID*: una stringa che valorizza l'attributo `entityID` obbligatorio dell'elemento radice di ogni metadata SAML. Il Service Provider è responsabile della scelta di un *EntityID* **unico** per ciascun metadata. Metadata multipli afferenti al medesimo *EntityID* sono rifiutati. Si consiglia di utilizzare, come *EntityID* un URL in https, non eccedente 1024 caratteri, afferente al dominio del soggetto del metadata SAML.

L'elemento `<EntityDescriptor>` costituisce il contenitore al cui interno si trovano le regole e le direttive valide solo ed esclusivamente per quel singolo soggetto. É strutturato internamente come una sequenza di elementi tra i quali il Service Provider deve necessariamente inserire i seguenti, tutti **obbligatori** (e presenti *una e una sola sola volta*, salvo ove espressamente indicato):

- `<Signature>` riportante il sigillo elettronico apposto sul metadadata stesso. Per ulteriori informazioni si faccia riferimento al capitolo sull'*infrastruttura a chiave pubblica* (pagina 50).
- `<SPSSODescriptor>` contenente le principali informazioni su chiavi crittografiche, URL e binding. Tale elemento descrive il ruolo del Service Provider e gli *endpoint* tecnici che espone verso gli altri soggetti della federazione.
- `<Organization>` in cui sono indicati le stringhe identificative dell'organizzazione a cui afferisce il soggetto del metadata.
- Una o due istanze `<ContactPerson>` in cui sono indicati ulteriori dati identificativi del soggetto cui il metadata SAML si riferisce e di un eventuale soggetto che, in veste di partner tecnologico, ne cura gli aspetti tecnici di federazione, sviluppo e messa in esercizio. I dati contenuti nelle istanze `<ContactPerson>` sono regolamentati più avanti.

Si consiglia che i *namespace* XML rilevanti per il metadata SAML (sopratutto quelli utilizzati in più punti del metadata) siano indicati *una tantum* nell'elemento radice dello stesso.

```
<md:EntityDescriptor
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  entityID="https://service-provider.it/sp">
    <ds:Signature> [...] </ds:Signature>
    <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.
↪0:protocol">
```

(continues on next page)

(continua dalla pagina precedente)

```
        [...]
    </md:SPSSODescriptor>
    <md:Organization> [...] </md:Organization>
    <md:ContactPerson> [...] </md:ContactPerson>
    [...]
</md:EntityDescriptor>
```

3.3.1 Sigillo sui metadata

Per ulteriori informazioni si faccia riferimento al capitolo sull'*infrastruttura a chiave pubblica* (pagina 50).

3.3.2 Descrittori di ruolo per il Service Provider

Le informazioni tecnicamente più rilevanti sono contenute nell'elemento `<md:SPSSODescriptor>`:

- la chiave o le chiavi pubbliche utilizzate dal SP per l'autenticazione durante la fase di scambio dei messaggi previsti dal protocollo SAML (per ulteriori informazioni si faccia riferimento al capitolo sull'*infrastruttura a chiave pubblica* (pagina 50));
- gli URL degli *endpoint* dei servizi tecnicamente esposti dal SP verso gli altri soggetti della federazione;
- elenco delle «categorie di attributi» (*attribute set*) SAML che il SP può richiedere all'Identity Provider (IdP).

Nota: In merito a gli attributi richiesti dal SP si precisa che la versione attuale del IdP può accogliere solo richieste realtive alla categoria di attributi *Minimum eIDAS Dataset* (nome, cognome, data di nascita e codice fiscale).

Gli attributi dell'elemento `<SPSSODescriptor>` che **devono** essere presenti sono:

- `protocolSupportEnumeration`: indica il protocollo SAML supportato che nel caso di Entra con CIE é SAML v2.0 e che deve quindi necessariamente essere valorizzato con la stringa `urn:oasis:names:tc:SAML:2.0:protocol`;
- `AuthnRequestsSigned`: booleano che indica se le richieste di autenticazione sono sigillate elettronicamente o meno; **deve** essere valorizzato con `true`;
- `WantAssertionsSigned`: booleano che indica se il SP si aspetta che le asserzioni SAML contenute nella risposta di autenticazione siano sigillate elettronicamente o meno; **deve** essere valorizzato con `true`.

Gli elementi che sono contenuti all'interno dell'`<SPSSODescriptor>` [e la loro cardinalità] sono riportati di seguito:

- `<KeyDescriptor>` [uno o più];
- `<SingleLogoutService>` [uno o più];
- `<NameIDFormat>` [facoltativo, al massimo uno];
- `<AssertionConsumerService>` [uno o più];
- `<AttributeConsumingService>` [uno o più];
- `<Extensions>` [al massimo uno]: Elemento **facoltativo**, riservato ad estensioni SAML relative a funzionalità aggiuntive del SP.

KeyDescriptor

Ciascun elemento `<KeyDescriptor>` contiene una chiave crittografica pubblica utilizzata per le seguenti azioni sui messaggi inviati dal SP:

- apposizione di sigilli elettronici (attributo `use` valorizzato con `signing`),
- cifratura (attributo `use` valorizzato con `encryption`).

Lo schema *Entra con CIE* prevede che ogni SP dichiari **almeno una** chiave pubblica «`signing`», cioè da utilizzare per apporre sigilli elettronici sulle proprie richieste di autenticazione SAML (*request*). All'interno di ciascun `<KeyDescriptor>` è presente un elemento `<KeyInfo>`, conforme con lo standard XML Signature Syntax and Processing[13] del W3C[14]. Gli algoritmi crittografici da utilizzare sono descritti nel capitolo relativo all'*infrastruttura a chiave pubblica* (pagina 50).

SingleLogoutService

Per facilitare la compatibilità con i successivi metodi di log-out, deve essere presente *almeno un* elemento `<SingleLogoutService>`. Ciascun elmento deve contenere i seguenti attributi:

- `Location`: riporta la URL (in https) all'*endpoint* del servizio per la ricezione delle richieste di *single logout*;
- `Binding`: descrive il tipo di binding e può assumere uno dei seguenti valori:
  - `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`, (almeno un'istanza **deve** avere questo metodo per lo schema *Entra con CIE*);
  - `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`;
  - `urn:oasis:names:tc:SAML:2.0:bindings:SOAP`.

Come specificato nella sezione *Logout* (pagina 29), l'IdP server non prevede, attualmente, un meccanismo di *single logout SAML*.

NameIDFormat

L'elemento `<NameIDFormat>` specifica il formato con cui vengono gestiti i `<NameID>` nell'ambito del protocollo SAML per identificare il soggetto a cui si riferisce un'asserzione. In particolare, nel caso specifico di Entra con CIE, se presente tale elemento deve essere valorizzato come `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`, per indicare che le informazioni hanno una validitá transitoria e riferita solo alla specifica sessione di autenticazione.

Assertion Consumer Service

Deve essere presente **almeno una** istanza *Assertion Consumer Service* (**AsCS** - elemento `<AssertionConsumerService>`) dove verrà mappata la URL per l'invio delle risposte SAML, occorre riportare i seguenti attributi (tutti obbligatori salvo ove espressamente indicato):

- `Binding`: valorizzato alternativamente con:
  - `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`;
  - `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`;
- `Location`: URL in https dell'*endpoint* del servizio per la ricezione delle risposte di autenticazione;

[13] https://www.w3.org/TR/xmldsig-core2/
[14] https://www.w3.org

- `index`: valorizzato con un numero intero non-negativo che identifica *univocamente* il AsCS in fase di richiesta di autenticazione;
- `isDefault`: **facoltativo**, è valorizzato con un booleano che indica quale sia il AsCS di default;

Nota: **un solo** AsCS (solitamente quello con `index` pari a `0`) può avere l'attributo `isDefault` valorizzato con `true` (tutti gli altri AsCS possono omettere questo attributo, oppure valorizzarlo con `false`);

Attribute Consuming Service

Deve essere presente **almeno una** istanza di *Attribute Consuming Service* (**AtCS** - `<AttributeConsumingService>`) che descrive la categoria di attributi (*attribute set*) richiesti dal SP. L'elemento contiene un unico attributo:

- `index`: valorizzato con un numero intero non-negativo che identifica *univocamente* l'*attribute set*;

All'interno di ciascun AtCS sono presenti i seguenti elementi [indicati con la loro cardinalità]:

- `<ServiceName>` [uno], contenente un identificativo della classe di servizi relativo all'*attribute set* o, in alternativa un *UUID v.4* dell'*attribute set* richiedibile dal SP, comprensivo dell'attributo `xmlns:lang`, valorizzato con una stringa vuota.
- `<ServiceDescription>` [zero o più], ciascuno contenente una descrizione testuale dell'*attribute set*.
  - Ciascun istanza di questo elemento presenta l'attributo `xmlns:lang`, valorizzato con il codice ISO 639 della lingua in cui è scritta tale descrizione.
- `<RequestedAttribute>` [uno o più], ciascuno contenente i seguenti attributi
  - `Name` (*obbligatorio*) – il nome tecnico dell'attributo da richiedere (senza spazi);
  - `NameFormat` (*facoltativo*) – il formato con cui ci si aspetta venga restituito l'attributo; se presente, è valorizzato con la seguente *alternativa*:
    * `urn:oasis:names:tc:SAML:2.0:attrname-format:basic`,
    * `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`,

I soli *attribute set* utilizzabili come AtCS per lo schema *Entra con CIE* sono quelli che comprendono gli attributi previsti nel *Minimum Dataset eIDAS*:

- `name` (tipo `xsd:string`) **nome** della persona fisica;
- `familyName` (tipo `xsd:string`) **cognome** della persona fisica;
- `dateOfBirth` (tipo `xsd:string`) **data di nascita** della persona fisica;
- `fiscalNumber` (tipo `xsd:string`) **codice fiscale** della persona fisica.

```
<md:AttributeConsumingService index='0'>
    <md:ServiceName xml:lang=''>urn:uuid:bc212b14-d920-4052-900d-86cc5ab48a3a</
↪md:ServiceName>
    <md:RequestedAttribute Name='name' NameFormat="urn:oasis:names:tc:SAML:2.
↪0:attrname-format:basic"/>
    <md:RequestedAttribute Name='familyName' NameFormat="urn:oasis:names:tc:SAML:2.
↪0:attrname-format:basic"/>
    <md:RequestedAttribute Name='dateOfBirth' NameFormat="urn:oasis:names:tc:SAML:2.
↪0:attrname-format:basic"/>
```

(continues on next page)

(continua dalla pagina precedente)

```
    <md:RequestedAttribute Name='fiscalNumber' NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
</md:AttributeConsumingService>
```

3.3.3 Informazioni aggiuntive del Service Provider

L'elemento `<md:Organization>` indica alcune informazioni prioritarie circa la persona giuridica Service Provider. La lingua utilizzata per valorizzare queste informazioni (**obbligatoria** almeno la lingua italiana) è indicata in ciascuno degli elementi figli mediante la valorizzazione del codice ISO 639 della lingua nell'attributo `xmlns:lang`. Ciascuna lingua è indicata con un'istanza della terna *completa* dei seguenti elementi:

- `<OrganizationName>`: Nome completo del SP, così come compare nei pubblici registri, con il corretto uso di maiuscole, minuscole, accenti e altri segni diacritici (p.es. `Istituto Nazionale Previdenza Sociale - INPS`);
- `<OrganizationDisplayName>`: Denominazione del SP - eventualmente senza l'esplicitazione di acronimi (p.es. `INPS`). Il valore di questo elemento è utilizzato dall'Identity Provider per mostrare all'utente (nella schermata di autenticazione) il SP a cui stanno per essere inviati gli attributi richiesti.
- `<OrganizationURL>`: La URL di una pagina web del sito istituzionale dell'organizzazione (con la lingua dei testi della pagina corrispondente a quanto ripotato nel corrispondente attributo `xmlns:lang`).

```
<md:Organization>
    <md:OrganizationName xml:lang="it">Istituto Service Provider</md:OrganizationName>
    <md:OrganizationName xml:lang="en">Service Provider Institute</md:OrganizationName>
    <md:OrganizationDisplayName xml:lang="it">ISP</md:OrganizationDisplayName>
    <md:OrganizationDisplayName xml:lang="en">SPI</md:OrganizationDisplayName>
    <md:OrganizationURL xml:lang="it">https://www.isp.it</md:OrganizationURL>
    <md:OrganizationURL xml:lang="en">https://www.isp.it</md:OrganizationURL>
</md:Organization>
```

3.3.4 Informazioni di censimento e contatto

Il metadata contiene *una o due* istanze di elementi `<ContactPerson>`, entrambe dotate di attributo `contactType`:

- nel caso di Service Provider autonomi (il cui referente tecnico è cioè «interno» al SP), vi è *una* sola istanza con `contactType` pari a `administrative`;
- nel caso di soggetti che si affidano ad un partner tecnologico «esterno» come referente tecnico, vi sono *due* simili istanze:
  - la prima ha il `contactType` valorizzato come `administrative` (con le informazioni identificative del SP, cui afferisce il proprio *referente amministrativo*);
  - l'altra con il `contactType` valorizzato come `technical` (e contenente le informazioni identificative del partner tecnologico, cui afferisce il *referente tecnico* del SP).

I sopraelencati elementi `<ContactPerson>` sono così valorizzati:

- `<Extensions>` *obbligatoria*, contenente i seguenti elementi, tutti che utilizzano il *namespace* XML di CIE (https://www.cartaidentita.interno.gov.it/saml-extensions):
  - Un'*alternativa obbligatoria* tra i seguenti due elementi «vuoti»:
    * `<Public/>` per le **PP.AA.**,

    * `<Private/>` per i soggetti **privati**;

  - `<IPACode>` *obbligatorio* per le **Pubbliche Amministrazioni** (PP.AA.) e i Gestori di Pubblici Servizi, è valorizzato con il **codice IPA** così come risultante dall'"Indice PA[15] (IPA); ad esempio, `ipzsspa` (Istituto Poligrafico e Zecca dello Stato S.p.A.);
  - `<IPACategory>` valorizzato *facoltativamente* per le **PP.AA.** e gli altri soggetti iscritti ad IPA[16], è valorizzato con la sua Categoria IPA[17]; ad esempio, `L6` (Comuni italiani) ovvero `L37` (Gestori di Pubblici Servizi).
  - `<VATNumber>` *obbligatorio* per soggetti **privati** dotati di partita IVA (e *facoltativo* altrimenti), è valorizzato con il numero di **partita IVA** (o *VAT Number* internazionale), comprensivo del codice ISO 3166-1 α2 del Paese di appartenenza, *senza* spazi; ad esempio, `IT12345678901`.
  - `<FiscalCode>` *obbligatorio* per i soggetti **privati** (e *facoltativo* altrimenti), è valorizzato con il **codice fiscale** della persona giuridica; ad esempio: `12345678901`.
  - `<NACE2Code>` (uno o più) *obbligatorio* per i soggetti **privati** (e *facoltativo* per tutti gli altri, se ne sono dotati), è valorizzato con il codice ATECO[18] del soggetto; in caso di soggetti esteri (pubblici e privati), è sempre facoltativo e valorizzato con il codice NACE (rev. 2)[19] (dal quale sono declinati i codici ATECO per l'Italia); ad esempio `12.34.56`. In caso si possieda più codici ATECO o NACE, questi possono essere inseriti mediante istanze mutliple delle'elemento (ciascuna contenente un unico codice)
  - `<Municipality>` *obbligatorio*, è valorizzato con il codice ISTAT del Comune[20] (anche detto «codice Belfiore» - tutto in maiuscolo) ove ha la sede legale il soggetto; nel caso di soggetti esteri, *se presente*, è valorizzato con lo *Zip code* della sede legale; ad esempio `H501` (Roma), `W1F 9AS` (Quartiere Soho di Londra).
  - `<Province>` *facoltativo*, è valorizzato con la sigla automobilistica della Provincia (tutta in maiuscole) dove si trova la sede legale del soggetto; ad esempio `MI`; in caso di soggetti esteri, *se presente*, è valorizzato con `EE`.
  - `<Country>` *obbligatorio* per soggetti **esteri** (e *facoltativo* altrimenti), è valorizzato con il codice ISO 3166-1 α2 del Paese ove è situata la sede legale del soggetto; ad esempio `IT` (Italia).
  - Ulteriori estensioni previste dal Sistema Pubblico delle Identità Digitali (*SPID*), anche se ignorate dallo schema *Entra con CIE*.

- `<Company>` *obbligatorio* e valorizzato con il nome completo del soggetto. Nel caso delle istanze relative al Service Provider (cioè nel caso di istanza con attributo `contactType` valorizzato come `administrative`) tale elemento deve essere valorizzato *esattamente* come l'elemento `<OrganizationName>` (nell'istanza della lingua del Paese dell'organizzazione) presente nell'antenato indiretto `<Organization>`;
- `<EmailAddress>` *obbligatorio* e valorizzato con l'indirizzo di una casella email istituzionale (preferibilmente *non* PEC) per comunicare istituzionalmente con il Service Provider. L'indirizzo email **deve** coincidere con quello indicato in fase di richiesta di adesione riferito, a seconda della tipologia del soggetto cui si riferisce l'elemento `<ContactPerson>`, al referente amministrativo o tecnico.
- `<TelephoneNumber>` *facoltativo* e valorizzato con il numero di telefono (dotato di prefisso internazionale, *senza* spazi - ad esempio `+39061234567`) per comunicare con il soggetto cui si riferisce l'elemento `<ContactPerson>`. **Non** deve essere un numero telefonico personale.

Nota: Nella compilazione degli elementi sopraelencati è necessario assicurarsi che le informazioni riportate siano le medesime inserite in fase di richiesta di adesione. Nel caso di esito negativo a fronte di una verifica, il metadata

[15] https://www.indicepa.gov.it
[16] https://www.indicepa.gov.it
[17] https://www.indicepa.gov.it/public-services/docs-read-service.php?dstype=FS&filename=Categorie_Amministrazioni.pdf
[18] https://www.istat.it/it/archivio/17888#valori
[19] https://ec.europa.eu/eurostat/ramon/nomenclatures/index.cfm
[20] https://www.istat.it/storage/codici-unita-amministrative/Elenco-comuni-italiani.xls

non sarà considerato valido ai fini della federazione. È importante sottolineare che la modalità di compilazione delle informazioni di censimento appena descritte può essere differente rispetto a quanto previsto per lo schema di identificazione SPID in quanto essa riflette le differenti procedure amministrative previste dagli schemi «Entra con CIE» e SPID in relazione alle rispettive fasi di onboarding.

3.3.5 Estensioni SAML

Gli elementi `<Extensions>` opzionalmente presenti nei metadata SAML servono a contenere estensioni proprietarie – dello schema *Entra con CIE* o relative ad altri schemi di identificazione elettronica (quali ad esempio *SPID*). Le implementazioni tecniche che non «riconoscono» particolari ulteriori estensioni oltre a quelle dello schema *Entra con CIE*, **devono** ignorarle (fintanto che siano rappresentate in una sintassi XML formalmente corretta) senza produrre condizioni di errore.

3.3.6 Esempio di metadata

Di seguito si riporta un esempio di metadata per un Service Provider privato che si presenta autonomamente (senza un partner tecnologico «esterno»). Questo esempio include i soli elementi obbligatori previsti dal presente manuale.

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                     xmlns:cie="https://www.cartaidentita.interno.gov.it/saml-extensions"
                     entityID="https://entityidsp">
  <ds:Signature> [...] </ds:Signature>
  <md:SPSSODescriptor AuthnRequestsSigned="true"
                      WantAssertionsSigned="true"
                      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate> [...] </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
                            Location="https://url_esempio_SLO_Redirect" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                                 Location="https://url_esempio_POST"
                                 index="0"
                                 isDefault="true" />
    <md:AttributeConsumingService index="0">
      <md:ServiceName xml:lang="">urn:uuid:86eabbc2-6023-4f8d-a7dc-22401f5ac4fe</md:ServiceName>
      <md:RequestedAttribute Name="name" />
      <md:RequestedAttribute Name="familyName" />
      <md:RequestedAttribute Name="dateOfBirth" />
      <md:RequestedAttribute Name="fiscalNumber" />
    </md:AttributeConsumingService>
  </md:SPSSODescriptor>
  <md:Organization>
    <md:OrganizationName xml:lang="it">Service Provider Privato s.r.l.</md:OrganizationName>
```

(continues on next page)

(continua dalla pagina precedente)

```
    <md:OrganizationDisplayName xml:lang="it">SPP</md:OrganizationDisplayName>
    <md:OrganizationURL xml:lang="it">https://www.esempio_sp_privato.it</
↪md:OrganizationURL>
  </md:Organization>
  <md:ContactPerson contactType="administrative">
    <md:Extensions>
      <cie:Private/>
      <cie:VATNumber>IT01234567890</cie:VATNumber>
      <cie:FiscalCode>9876543210</cie:FiscalCode>
      <cie:NACE2Code>CODICE_ATECO</cie:NACE2Code>
      <cie:Municipality>CODICE_ISTAT</cie:Municipality>
    </md:Extensions>
    <md:Company>Service Provider Privato s.r.l.</md:Company>
    <md:EmailAddress>esempio_sp_privato@spp.it</md:EmailAddress>
    <md:TelephoneNumber>+39061234567</md:TelephoneNumber>
  </md:ContactPerson>
</md:EntityDescriptor>
```

Di seguito si riporta un esempio di metadata per un Service Provider (nell'esempio pubblico) che si presenta per tramite di un partner tecnologico (nell'esempio privato) che funge da referente tecnico «esterno» al SP. Questo esempio include, oltre agli elementi obbligatori, anche alcuni di quelli opzionali.

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                     xmlns:cie="https://www.cartaidentita.interno.gov.it/saml-
↪extensions"
                     entityID="https://entityidsp">
  <ds:Signature> [...] </ds:Signature>
  <md:SPSSODescriptor AuthnRequestsSigned="true"
                      WantAssertionsSigned="true"
                      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
↪">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate> ... </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption">
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:X509Data>
                <ds:X509Certificate> [...] </ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
↪Redirect"
                            Location="https://url_esempio_SLO_Redirect" />
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                            Location="url_esempio_SLO_POST"/>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
                            Location="url_esempio_SLO_SOAP"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</
↪md:NameIDFormat>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
↪POST"
```

(continues on next page)

(continua dalla pagina precedente)

```
                                Location="https://url_esempio_POST"
                                index="0"
                                isDefault="true" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
↪Redirect"
                                Location="https://url_esempio_Redirect"
                                index="1"
                                isDefault="false" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
↪SOAP"
                                Location="https://url_esempio_SOAP"
                                index="2" />
    <md:AttributeConsumingService index="0">
      <md:ServiceName xml:lang="">urn:uuid:a83e1df8-0dd3-46c0-b4e3-f6c650177056</
↪md:ServiceName>
      <md:ServiceDescription xml:lang="it">DESCRIZIONE CATEGORIA SERVIZI ONLINE</
↪md:ServiceDescription>
      <md:RequestedAttribute Name="name" />
      <md:RequestedAttribute Name="familyName" />
      <md:RequestedAttribute Name="dateOfBirth" />
      <md:RequestedAttribute Name="fiscalNumber" />
    </md:AttributeConsumingService>
    <md:AttributeConsumingService index="1">
      <md:ServiceName xml:lang="">urn:uuid:bd042d58-d402-4970-83dc-70cd1882bf62</
↪md:ServiceName>
      <md:ServiceDescription xml:lang="en">ATTRIBUTE SET DESCRIPTION</
↪md:ServiceDescription>
      <md:RequestedAttribute Name="name" />
      <md:RequestedAttribute Name="familyName" />
      <md:RequestedAttribute Name="dateOfBirth" />
      <md:RequestedAttribute Name="fiscalNumber" />
    </md:AttributeConsumingService>
    <md:AttributeConsumingService index="2">
      <md:ServiceName xml:lang="">urn:uuid:a16cb8fd-62c6-4ff5-88ea-7dd3bdcb4c4e</
↪md:ServiceName>
      <md:RequestedAttribute Name="name" />
      <md:RequestedAttribute Name="familyName" />
      <md:RequestedAttribute Name="dateOfBirth" />
      <md:RequestedAttribute Name="fiscalNumber" />
    </md:AttributeConsumingService>
  </md:SPSSODescriptor>
  <md:Organization>
    <md:OrganizationName xml:lang="it">Istituto Service Provider</md:OrganizationName>
    <md:OrganizationName xml:lang="en">Service Provider Institute</
↪md:OrganizationName>
    <md:OrganizationDisplayName xml:lang="it">ISP</md:OrganizationDisplayName>
    <md:OrganizationDisplayName xml:lang="en">SPI</md:OrganizationDisplayName>
    <md:OrganizationURL xml:lang="it">https://www.isp.it</md:OrganizationURL>
    <md:OrganizationURL xml:lang="en">https://www.isp.it</md:OrganizationURL>
  </md:Organization>
  <md:ContactPerson contactType="administrative">
      <md:Extensions>
          <cie:Public/>
          <cie:IPACode>codiceIPA_SP</cie:IPACode>
          <cie:IPACategory>categoriaIPA_SP</cie:IPACategory>
          <cie:NACE2Code>codiceATECO_SP</cie:NACE2Code>
          <cie:VATNumber>IT01234567890</cie:VATNumber>
```

(continues on next page)

(continua dalla pagina precedente)

```
            <cie:FiscalCode>9876543210</cie:FiscalCode>
            <cie:Municipality>codiceISTAT_SP</cie:Municipality>
            <cie:Province>sigla_provincia_SP</cie:Province>
            <cie:Country>IT</cie:Country>
        </md:Extensions>
        <md:Company>Istituto Service Provider</md:Company>
        <md:EmailAddress>info@isp.gov.it</md:EmailAddress>
        <md:TelephoneNumber>+390011223344</md:TelephoneNumber>
    </md:ContactPerson>
    <md:ContactPerson contactType="technical">
        <md:Extensions>
            <cie:Private/>
            <cie:VATNumber>IT01234567890</cie:VATNumber>
            <cie:FiscalCode>9876543210</cie:FiscalCode>
            <cie:NACE2Code>codiceATECO_partnerTecnologico</cie:NACE2Code>
            <cie:Municipality>codiceISTAT_partnerTecnologico</cie:Municipality>
            <cie:Province>sigla_provincia_partnerTecnologico</cie:Province>
            <cie:Country>IT</cie:Country>
        </md:Extensions>
        <md:Company>Partner Tecnologico per Soluzioni di Identità Federata s.r.l.</
↪md:Company>
        <md:EmailAddress>info.cie@partnertecnologicoidfederata.com</md:EmailAddress>
        <md:TelephoneNumber>+390999135792</md:TelephoneNumber>
    </md:ContactPerson>
</md:EntityDescriptor>
```

CAPITOLO 4

Protocolli di comunicazione

Terminata la fase di federazione tramite lo scambio dei metadata opportunamente predisposti come da specifiche riportate nella precedente sezione, il Service Provider viene aggiunto nella *trusted list* dell'Identity Provider ed é quindi possibile lo scambio dei messaggi previsto dal protocollo SAML SSO. Tale protocollo viene avviato al momento in cui l'utente esprime la volontà di accedere al servizio cliccando il tasto «Entra con CIE» nella pagina html del Service Provider. Quest'ultimo prepara di conseguenza una richiesta di autenticazione (`<AuthnRequest>`) che inoltra all'Identity Provider al quale l'utente viene reindirizzato per effettuare l'autenticazione tramite la propria CIE. La componente server dell'Identity Provider (CieID Server) invita l'utente a avvicinare la propria CIE sul lettore avviando automaticamente il processo di autenticazione mediante la CIE. L'utente deve, quindi, inserire la seconda metà del PIN e confermare.

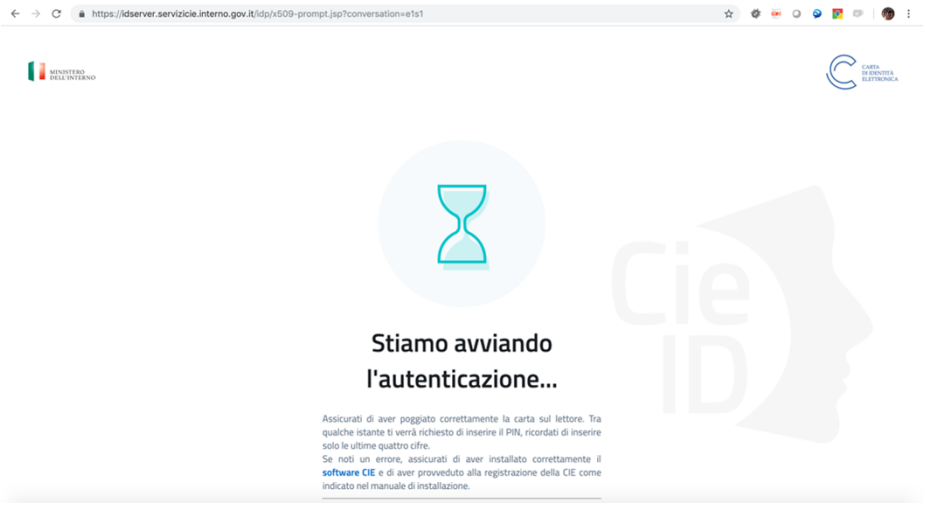

Fig. 4.1: Processo di autenticazione del CieID Server

Terminato il processo di autenticazione il server CieID mostra 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, prosegue con l'operazione e viene reindirizzato nuovamente sul sito del Service Provider, con un'asserzione (`<Response>`) firmata dall'Identity Provider contenente gli attributi richiesti (nome, cognome, data di nascita e codice fiscale).

Nota: All'interno dello schema Entra con CIE solo il *Single Sign-On* viene gestisto tramite protocollo SAML che prevede di tue tipologie di messaggi:

- Richiesta di autenticazione: `<AuthnRequest>`;
- Risposta di autenticazione: `<Response>`.

La gestione del logout, attualmente, non supporta il procollo SAML, ma viene gestite mediante un meccanismo di *Simple Logout* che provvede all'eliminazione della sessione di autenticazione dell'Identity Provider. Pertanto, pur accettando le richieste SAML di *Single Logout*, l'IdP server CieID non restituisce alcuna risposta SAML.

4.1 Richiesta di autenticazione SAML

La richiesta di autenticazione («*request*») è inviata dal Service Provider attraverso il browser dell'utente al *SingleSignOnService* dell'Identity Provider. Il messaggio contenuto in essa deve essere conforme allo standard SAML v2.0 (cfr. Assertions and Protocols for the OASIS SAML V2.0[21]).

L'elemento `<AuthnRequest>` costituisce il contenitore del messaggio e deve avere i seguenti attributi:

- `Destination` rappresenta un URL in https che indica l'indirizzo dell'Identity Provider a cui è inviata la richiesta e deve coincidere con uno degli attributi `Location` presenti nel tag `SingleSignOnService` riportato nel metadata dell'IdP e relativo al particolare binding utilizzato in fase di richiesta (cfr. *Modalitá di trasmissione dei messaggi* (pagina 31) per ulteriori dettagli). L'Identity Provider verifica tale riferimento e, in caso di esito negativo, la richiesta viene scartata.
- `AttributeConsumingServiceIndex` riportante un indice posizionale in riferimento alla struttura `<AttributeConsumingService>` presente nei metadata del Service Provider. A tal proposito si ricorda che gli attributi richiesti nel metadata **devono** contenere il *Minimum Dataset eIDAS*.
- `AssertionConsumerServiceURL` indica la URL a cui inviare il messaggio di risposta alla richiesta di autenticazione (l'indirizzo deve coincidere con quello del servizio riportato dall'elemento `<AssertionConsumingService>` presente nei metadata del Service Provider);
- `ProtocolBinding` identifica il tipo di binding e **deve** essere valorizzato con `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`.
- `ForceAuthn` è **sempre** valorizzato con `true` in quanto si richiede un'autenticazione con massimo livello di sicurezza.
- `IssueInstant` indica l'istante di emissione della richiesta, in formato UTC (p.es. `AAAA-MM-GGThh:mm:ss.sssZ`)
- `ID` univoco basato su un Universally Unique Identifier (**UUID**) o su una combinazione origine + timestamp (quest'ultimo generato con una precisione di almeno un millesimo di secondo per garantire l'univocità).
- `Version` coerentemente con la versione di SAML adottata; attualmente la `2.0`.

Nota:

- **In alternativa**, è ammesso l'uso dell'attributo `AssertionConsumerServiceIndex` al posto degli attributi `AssertionConsumerServiceURL` e `ProtocolBinding`.
- L'attributo `IsPassive` **non** deve essere presente.
- L'attributo `Destination` **deve** essere valorizzato in accordo con lo standard SAML e **non** secondo quanto prescitto dalle Regole Tecniche SPID.

[21] https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

```
<samlp:AuthnRequest
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  AttributeConsumingServiceIndex="0"
  AssertionConsumerServiceIndex="0"
  Destination="https://idserver.servizicie.interno.gov.it/idp/profile/SAML2/Redirect/
↪SSO"
  ForceAuthn="true"
  IssueInstant="2020-10-29T12:51:36.123Z"
  ID="..."
  Version="2.0">
    [...]
</samlp:AuthnRequest>
```

Gli elementi che devono essere presenti all'interno della `<AuthnRequest>` sono:

- `<saml:Issuer>`: identifica in maniera univoca il Service Provider. L'elemento deve essere valorizzato come l'attributo `entityID` riportato nel corrispondente metadata del Service Provider. Prevede, inoltre, i seguenti attributi opzionali:
- `NameQualifier`, dominio a cui afferisce il soggetto che sta effettuando la richiesta di autenticazione e valorizzato come URL riconducibile al Service Provider;
- `Format`, se presente **deve** essere valorizzato con la stringa `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`.
- `<NameIDPolicy>` avente l'attributo `Format` valorizzato con la stringa `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`, mentre invece **non deve** essere presente l'attributo `AllowCreate`.
- `<RequestedAuthnContext>` (ne è presente **una sola** occorrenza) specifica i requisiti del contesto di autenticazione di statement di autenticazione restituite in risposta a una richiesta. Esso è valorizzato come segue:
  - mediante l'attributo `Comparison`, che specifica il metodo di confronto utilizzato per valutare le classi o gli statement di contesto richiesti e può essere valorizzato soltanto come `exact` (default), ovvero `minimum`;
  - contenente l'elemento `<RequestedAuthnContext>`, contiene a sua volta l'elemento `<saml:AuthnContextClassRef>`, valorizzato con uno dei seguenti valori:
    * `https://www.spid.gov.it/SpidL1`
    * `https://www.spid.gov.it/SpidL2`
    * `https://www.spid.gov.it/SpidL3`

Lo schema di autenticazione «*Entra con CIE*», nell'ottica di agevolare gli sviluppi implementativi da parte dei Service Provider che giá hanno aderito al Sistema Pubblico di Identità Digitale (*SPID*), richiede la valorizzazione di tale elemento con una delle suddette stringhe (corrispondenti ai tre livelli di affidabilità dello SPID), sebbene il livello di affidabilità dello schema CIE è sempre analogo al quello massimo previsto per tutti gli schemi di identificazione elettronica a livello europeo (analogo anche al Livello 3 di SPID). Pertanto, per consentire al cittadino di autenticarsi sia a servizi accessibili tramite CIE, che a quelli accessibili tramite qualunque livello di sicurezza SPID, le possibili combinazioni di valori dell'elemento `<RequestedAuthnContextClassRef>` e dell'attributo-antenato `Comparison` sono, rispettivamente:

- autenticazione con CIE ovvero con SPID di Livello 3: `https://www.spid.gov.it/SpidL3` e, equivalentemente, `exact` ovvero `minimum`;
- autenticazione con CIE ovvero con SPID di Livelli 2 o 3: `https://www.spid.gov.it/SpidL2` e `minimum`;

- autenticazione con CIE ovvero con SPID (qualunque Livello): `https://www.spid.gov.it/SpidL1` e `minimum`;

Nota:

- Dipendentemente dal tipo di binding utilizzato per inviare la richiesta di autenticazione può essere presente o meno l'elemento `<Signature>` (**obbligatorio** in caso di binding HTTP POST), che contiene il sigillo elettronico creato dal Service Provider sulla propia *request*. Per maggiori dettagli, si veda il capitolo relativo all'"*infrastruttura a chiave pubblica* (pagina 50).
- Non sono presenti gli elementi `<RequesterID>` e `<Scoping>`.

4.1.1 Esempio di *request* SAML

Si noti che l'elemento XML `<Signature>` nel seguente esempio va inserito solo nel caso di utilizzo del binding HTTP POST; in caso di binding HTTP Redirect, il sigillo elettronico è immerso invece nel parametro `Signature` della *query string*. Per ulteriori informazioni si faccia riferimento al capitolo sull'"*infrastruttura a chiave pubblica* (pagina 50).

```
<samlp:AuthnRequest
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  AttributeConsumingServiceIndex="0"
  AssertionConsumerServiceURL=" [...] "
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Destination="https://idserver.servizicie.interno.gov.it/idp/profile/SAML2/POST/SSO"
  ForceAuthn="true"
  ID="..."
  IssueInstant="2020-11-02T09:01:25Z" Version="2.0">
    <saml:Issuer NameQualifier="https://service_provide_entityID">
        https://service_provider_entityID
    </saml:Issuer>
    <ds:Signature>
        <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="RIFERIMENTO ALL'ID DELL'ATTRIBUTO">
                <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#"␣
↪/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /
↪>
                <ds:DigestValue> [...] </ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue> [...] </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate> [...] </ds:X509Certificate>
```

(continues on next page)

(continua dalla pagina precedente)

```
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" />
    <samlp:RequestedAuthnContext Comparison="minimum">
        <saml:AuthnContextClassRef>https://www.spid.gov.it/SpidL3</saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

4.2 Risposta di autenticazione SAML

Al termine della *challenge* mediante la CIE, effettuata dal server CieID dell'Identity Provider, quest'ultimo invia un messaggio di risposta («*response*») al Service Provider. L'elemento `<Response>` costituisce la radice del messaggio e contiene i seguenti attributi:

- `Destination`: URL del Service Provider a cui è inviata la risposta; coincide con la URL riportata nel metadata cosí come specificato dall'attributo `location` presente nell'elemento `<AssertionConsumerService>`. Il Service Provider deve verificare il riferimento URI e, in caso di esito negativo, deve scartare la risposta;
- `ID`: identificatore univoco basato su un Universally Unique Identifier (**UUID**) o su una combinazione origine + *timestamp* (quest'ultimo generato con una precisione di almeno un millesimo di secondo per garantire l'univocità);
- `InResponseTo`: riferimento all'ID della richiesta a cui si risponde;
- `IssueInstant`: indica l'istante di emissione della richiesta, in formato UTC (`AAAA-MM-GGThh:mm:ss.sssZ`);
- `Version`: riferimento alla versione SAML (2.0) utilizzata dallo schema Entra con CIE.

Gli elementi contenuti nella `<Response>` (tutti dichiarati con il corretto uso dei *namespace* XML) sono:

- `<Issuer>`: in maniera analoga a quanto previsto per la *request*, tale campo indica l'EntityID del soggetto che effettua l'autenticazione (cioè l'Identity Provider stesso) e coincide perciò con l'attributo `entityID` del metadata dell'IdP.
- `<Signature>`: contiene il sigillo elettronico apposto sulla *request* dell'Identity Provider. Per ulteriori informazioni si faccia riferimento al capitolo sull'*infrastruttura a chiave pubblica* (pagina 50).
- `<Status>`: indica l'esito della richiesta di autenticazione e in particolare prevede l'elemento `<StatusCode>` che riporta la codifica di stato SAML attraverso l'attributo `Value`, valorizzato come:
  - `urn:oasis:names:tc:SAML:2.0:status:Success`, nel caso di autenticazione effettuata con successo;
  - in caso di errori, é possibile visualizzare gli attributi `<StatusMessage>` e `<StatusDetail>` per maggiori dettagli sull'errore ricevuto.
- `<Assertion>`: costituisce l'elemento piú importante che attesta l'avvenuta autenticazione e contiene gli attributi dell'utente che ha richiesto l'accesso al servizio. Contiene almeno un elemento `<AuthnStatement>` nel quale sono riportati i dati dell'utente richiesti dal Service Provider. Nel caso l'Identity Provider abbia riscontrato un errore nella gestione della richiesta di autenticazione l'elemento `<Assertion>` non é presente.

4.2.1 Esempio di *response* SAML

```
<samlp:Response
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  Destination="https://service_provide_assertion_consumer"
  InResponseTo="..."
  IssueInstant="2020-10-29T11:36:02.708Z"
  ID="..."
  Version="2.0">
    <saml:Issuer>
        https://idserver.servizicie.interno.gov.it/idp/profile/SAML2/POST/SSO
    </saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        [...]
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion>
        [...]
    </saml:Assertion>
</samlp:Response>
```

4.2.2 L'elemento `<saml:Assertion>`

Nell'elemento `<Assertion>` devono essere presenti i seguenti attributi:

- `ID`: identificatore univoco basato su un *Universally Unique Identifier* (**UUID**) o su una combinazione origine + *timestamp* (quest'ultimo generato con una precisione di almeno un millesimo di secondo per garantire l'univocità);
- `IssueInstant`: indica l'istante di emissione della richiesta, in formato UTC (`AAAA-MM-GGThh:mm:ss.sssZ`);
- `Version`: riferimento alla versione SAML (`2.0`) utilizzata dallo schema *Entra con CIE*.

Gli attributi contenuti nella `<Assertion>` sono i seguenti:

- `<Issuer>`: valorizzato coerentemente con l'*EntityID* (attributo `entityID`) presente nei corrispondenti metadata dell'Identity Provider.
- `<Signature>`: contiene il sigillo elettronico apposto sull'asserzione dell'Identity Provider. Per ulteriori informazioni si faccia riferimento al capitolo sull'*infrastruttura a chiave pubblica* (pagina 50).
- `<Subject>`: serve a qualificare il Service Provider che ha richiesto l'autenticazione. In particolare, contiene due elementi:
  - `<NameID>`: riferimento all'identificativo del SP e contenente principalmente le informazioni che qulificano l'IdP (`NameQualifier`) e il SP (`SPNameQualifier`)
  - `<SubjectConfirmation>`: riporta l'attributo `Method` valorizzato con la stringa `urn:oasis:names:tc:SAML:2.0:cm:bearer`. Tale elemento contiene inoltre l'elemento `<SubjectConfirmationData>` riportante gli attributi:
    - `Recipient` coerente con l'`AssertionConsumerServiceURL` relativa al servizio per cui è stata emessa l'asserzione e l'attributo;

    * `NotOnOrAfter` indica per quanto tempo l'asserzione puó ritenersi legata al *subject*. L'asserzione puó, tuttavia, essere valida per un tempo piú lungo, ma é necessario creare una sessione entro questo intervallo di tempo (per maggiori dettagli consultare la sezione 4.1.4.3. del Profilo Web SSO). Tale intervallo di tempo deve rientrare necessariamente nell'intervallo di tempo riportato nell'elemento `<Conditions>`;
    * `InResponseTo` il cui valore deve fare riferimento all'ID della richiesta;
    * `Address`, facoltativamente presente, contiene un identificativo univoco (ma non riconducibile a informazioni tecnico-implementative) dello specifico server CieID che ha tecnicamente effettuato l'autenticazione;

- `<Conditions>`: contenente gli attributi `NotBefore` e `NotOnOrAfter` che rappresentano le condizioni di validitá dell'asserzione. Inoltre é presente l'elemento `<AudienceRestriction>` riportante a sua volta l'elemento `<Audience>`, valorizzato con l'*EntityID* del Service Provider per il quale l'asserzione è emessa.
- `<AuthnStatement>`: oltre alle informazioni riguardanti il riferimento alla sessione (`SessionIndex`), l'istante temporale di autenticazione dell'utente (`AuthnInstant`). Contiene a sua volta l'elemento `AuthnContext` e il sotto-elemento `<AuthnContextClassRef>` valorizzato con il livello di affidabilità associato all'autenticazione con CIE.
- `<AttributeStatement>`: rappresenta la struttura nella quale sono riportati gli attributi relativi all'utente, così come richiesti dell'omologo elemento della *request* SAML.

In particolare, a fronte della richiesta del *eIDAS Minimum Data Set* l'asserzione contiene quattro elementi di tipo `<Attribute>` (ciascuno contenente l'attributo `Name` valorizzato come segue e l'attributo `NameFormat` valorizzato con `urn:oasis:names:tc:SAML:2.0:attrname-forma`):

- `name` (di tipo `xs:string`), valorizzato con il **nome** del soggetto;
- `familyName` (di tipo `xs:string`), valorizzato con il **cognome** del soggetto;
- `dateOfBirth` (di tipo `xs:string`) **data di nascita** nel formato `YYYY-MM-GG`;
- `fiscalNumber` (di tipo `xs:string`), valorizzato con il **codice fiscale** nel formato `TINIT-<CODICE FISCALE>`.

Nota: L'elemento `<AuthnContextClassRef>` discendente dell'elemento `<AuthnStatement>` è **sempre** valorizzato con `https://www.spid.gov.it/SpidL3` poiché la CIE fornisce un livello di affidabilità massimo a livello europeo, corispondente al Livello 3 del Sitema Pubblico dell'Identità Digitale (*SPID*). Per favorire l'interoperabilitá con SPID da parte dei Service Provider e minimizzare quindi l'impatto nella gestione implementativa delle risposte SAML per i SP che intendono aderere ad entrambi gli schemi di autenticazione, si restituisce dunque una classe analoa a quella usata dagli Identity Provider SPID nelle *response* associate ad autenticazioni avvenute con Livello 3.

Nota: Con riferimento alla compatibilità con SPID si riporta quanto segue:

- L'attributo `Format` dell'elemento `<samlp:Issuer>` non è presente;
- L'elemento `<saml:AuthnContextClassRef>` è valorizzato sempre con il valore **https://www.spid.gov.it/SpidL3**;
- Gli attributi inviati in risposta alla richiesta di autenticazione corrispondono sempre al **Minimum Dataset eIDAS** e non prevedono, nella versione attuale, l'invio di ulteriori attributi quali ad esempio lo *spidCode*.

4.2.3 Verifica della <Response>

Alla ricezione della <Response> qualunque sia il binding utilizzato il Service Provider prima di utilizzare l'asserzione deve eseguire le seguenti verifiche:

- Controllo delle firme presenti all'interno dell'<Assertion> e della <Response>
- Verifica che nell'elemento <SubjectConfirmationData>
  - l'attributo Recipient coincida con la AssertionConsumerServiceURL a cui la <Response> è pervenuta
  - l'attributo NotOnOrAfter non sia scaduto
  - l'attributo InResponseTo si riferisca correttamente all'ID della <AuthnRequest> di richiesta

---

Nota: É, inoltre, a carico del Service Provider garantire che le asserzioni non vengano ripresentate, mantenendo il set di identificatori di richiesta (ID) usati come per le <AuthnRequest> per tutta la durata di tempo per cui l'asserzione risulta essere valida in base dell'attributo NotOnOrAfter dell'elemento <SubjectConfirmationData> presente nell'asserzione stessa.

4.2.4 Esempio di <saml:Response>

Di seguito si riporta un esempio completo di <saml:Response>:

```
<samlp:Response
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  Destination="https://service_provide_assertion_consumer"
  ID="..."
  InResponseTo="..."
  IssueInstant="2020-10-29T11:36:02.708Z" Version="2.0">
    <saml:Issuer>
        https://idserver.servizicie.interno.gov.it/idp/profile/SAML2/POST/SSO
    </saml:Issuer>
    <ds:Signature>
        <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="...">
                <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#"␣
↪/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /
↪>
                <ds:DigestValue> [...] </ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
```

(continues on next page)

(continua dalla pagina precedente)

```
        <ds:SignatureValue> [...] </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate> [...] </ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>

    <saml:Assertion
      ID="..."
      IssueInstant="2020-11-03T09:19:36.785Z"
      Version="2.0">
        <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
            https://idserver.servizicie.interno.gov.it/idp/profile/SAML2/POST/SSO
        </saml:Issuer>
        <ds:Signature>
            <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="...">
                    <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#" />
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc
↪#sha256" />
                    <ds:DigestValue> [...] </ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue> [...] </ds:SignatureValue>
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate> [...] </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </ds:Signature>
        <saml:Subject>
            <saml:NameID
              Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
              NameQualifier="https://idserver.servizicie.interno.gov.it/idp/profile/
↪SAML2/POST/SSO">
                RIFERIMENTO ID ENTE
            </saml:NameID>
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData
                  InResponseTo="..."
                  NotOnOrAfter="2020-11-03T09:24:36.807Z"
                  Recipient="https://service_provider_assertion_consumer" />
            </saml:SubjectConfirmation>
        </saml:Subject>
```

(continues on next page)

(continua dalla pagina precedente)

```
        <saml:Conditions
          NotBefore="2020-11-03T09:19:36.785Z"
          NotOnOrAfter="2020-11-03T09:24:36.785Z">
            <saml:AudienceRestriction>
                <saml:Audience>https://sevice_provider</saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement
          AuthnInstant="2020-11-03T09:19:33.100Z"
          SessionIndex="....">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>https://www.spid.gov.it/SpidL3</
↪saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute FriendlyName="Data di Nascita" Name="dateOfBirth"␣
↪NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml:AttributeValue xsi:type="xs:string">AAAA-MM-GG</
↪saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute FriendlyName="Codice Fiscale" Name="fiscalNumber"␣
↪NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml:AttributeValue xsi:type="xs:string">TINIT-CODICE_FISCALE</
↪saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute FriendlyName="Nome" Name="name" NameFormat=
↪"urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml:AttributeValue xsi:type="xs:string">NOME</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute FriendlyName="Cognome" Name="familyName" NameFormat=
↪"urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <saml:AttributeValue xsi:type="xs:string">COGNOME</
↪saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
```

4.3 Logout

Lo schema di autenticazione Entra con CIE, nella versione attuale, non implementa il Single logout SAML. Il meccanismo di logout previsto gestisce la sola sessione relativa all'Identity Provider non propagando il logout sulle relative sessioni dei Service Provider. A tal proposito é onere del Service Provider garantire il logout al proprio servizio autenticato tramite un apposito endpoint presente nei metadata dell'Identity Provider all'interno del tag `<SingleLogoutService>` che viene invocato mediante HTTP-GET e che reinderizza su una apposita pagina dell'IdP server CieID recante il messaggio «Logout effettuato con successo».

Fig. 4.2: Schermata di conferma di avvenuto Logout.

CAPITOLO 5

Modalitá di trasmissione dei messaggi

Il profilo SAML SSO raccomanda l'uso di TLS 1.2; lo scambio dei messaggi tra le entità della federazione può avvenire secondo due modalità:

- **HTTP-POST:**
- **HTTP-Redirect:**

Le richieste di autenticazione (`<samlp:AuthnRequest>`) **POSSONO** essere trasmesse in entrambe le modalitá.

Nota:

- Nel caso di binding **HTTP-POST SI DEVE** inserire il campo `Signature` all'interno della richiesta di autenticazione SAML `<samlp:AuthnRequest>` cosí come specificato nella sezione *Protocolli di comunicazione* (pagina 20)
- Nel caso di binding **HTTP-Redirect** il campo `Signature` **NON DEVE** essere presente nella richiesta di autenticazione SAML `<samlp:AuthnRequest>`, ma **DEVE** essere inserita nella URL come *query parameter*.

Le risposte inviate dall'Identity Provider (`<saml2:Response>`), invece, **DEVONO** essere trasmesse tramite binding **HTTP-POST**.

5.1 Binding HTTP-POST

In questo tipo di binding, il messaggio HTTP contiene una form HTML all'interno della quale è codificato in formato *Base64* il costrutto SAML firmato in accordo alla specifica XML Digital Signature. Il trasporto del messaggio di richiesta di autenticazione prevede due parametri fondamentali:

- **SAMLRequest** o **SAMLResponse**: contengono, rispettivamente, la codifica della `<AuthnRequest>` e della `<Response>`

- **RelayState**: indica la risorsa originariamente richiesta dall'utente e alla quale dovrà essere trasferito il controllo al termine della fase di autenticazione; puó essere un UUID, un url, un percorso di file o un mini-blob con codifica binaria *Base64*

La codifica *Base64* é richiesta solo per i messaggi del protocollo SAML in formato XML *SAMLRequest* e *SAMLResponse* e non per il *RelayState*, che è un token specifico dell'applicazione usato per identificare lo stato, la cui codifica o decodifica é in carico all'applicazione stessa.

5.2 Binding HTTP-Redirect

Quando si usa un binding di tipo Redirect, la firma viene posta nella URL come *query parameter*. Tutti i parametri sono *URL-encoded*. Il messaggio HTTP trasporta i seguenti parametri

- `SAMLRequest`: Un costrutto SAML codificato in formato *Base64* e compresso con algoritmo *DEFLATE*. Come da specifica, il messaggio SAML non contiene la firma in formato XML *Digital Signature* esteso (come avviene in generale nel caso di binding HTTP-POST). La specifica indica come modalità alternativa quella di specificare con parametri aggiuntivi l'algoritmo utilizzato per firmare (**SigAlg**) e la stringa con la codifica *Base64* URL-encoded dei byte del messaggio SAML (**Signature**).
- `RelayState`: Identifica il servizio originariamente richiesta dall'utente e a cui trasferire il controllo alla fine del processo di autenticazione.
- `SigAlg`: Identifica l'algoritmo usato per la firma prodotta secondo il profilo specificato per SAML utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore;
- `Signature`: Contiene la firma digitale della *query string*, così come prodotta prima di aggiungere questo parametro, utilizzando l'algoritmo indicato al parametro precedente;

5.3 Esempio HTML di utilizzo

Di seguito un esempio di form HTML per trasferire in HTTP-POST la richiesta di autenticazione

```
<html>
    <head>
        [...]
    </head>
    <body onload="javascript:document.forms[0].submit()">
        <form method="post" action="https://idserver.servizicie.interno.gov.it/idp/
↪profile/SAML2/POST/SSO">
            <input type="hidden" name="SAMLRequest"
                value="[...]">
            <input type="hidden" name="RelayState" value="...">
            <input type="submit" value="Invia"/>
        </form>
    </body>
</html>
```

Di seguito un esempio di form HTML per trasferire la risposta in HTTP-POST

```
<html>
    <head>
        [...]
    </head>
    <body onload="javascript:document.forms[0].submit()">
```

(continues on next page)

(continua dalla pagina precedente)

```
        <form method="post" action="https://service_provide_assertion_consumer">
            <input type="hidden" name="SAMLResponse"
                value="[...]">
            <input type="hidden" name="RelayState" value="...">
            <input type="submit" value="Invia"/>
        </form>
    </body>
</html>
```

La form HTML è corredata da uno script che la rende auto-postante (se Javascript è abilitato nel browser dell'utente) all'indirizzo indicato nell'attributo **action**. Quindi, il browser dell'utente elabora la risposta HTTP e invia una richiesta HTTP POST verso il servizio dell'entità destinataria.

CAPITOLO 6

Interoperabilità con SPID

Lo schema di identificazione *Entra con CIE* pur avendo molte analogie con lo schema di identificazione SPID, differisce da quest'ultimo su alcuni aspetti che riguardano:

- la predisposizione dei metadata
- i protocolli di comunicazione SAML.

È importante sottolineare che, per quanto riguarda in paticolare i metadata, le differenze di natura tecnica riflettono i diversi iter amministrativi previsti da AgID nei casi di Soggetti Aggregatori e Gestori di Pubblico Servizio, che nel caso di *Entra con CIE* sono gestiti all'interno del medesimo processo amministrativo di onboarding. In altre parole, la figura dell'Aggregatore (di servizi pubblici o privati) e quella di Gestore di Pubblico Servizio non sono previste nello schema *Entra con CIE*.

6.1 Metadata

In riferimento ai metadata, diversamente da quanto previsto per SPID, lo schema *Entra con CIE* prevede un unico modello di metadata indipendentemente dal ruolo che il soggetto svolge nell'ambito dello schema SPID. In particolare i due elementi nei quali si hanno maggiori impatti sono:

- l'elemento `<AttributeConsumingService>` che contiene il set di attributi richiesti in fase di autenticazione prevede, attualmente, solo e soltanto gli attributi relativi al *Minimum Dataset eIDAS* o suoi sottoinsiemi;
- l'elemento `<ServiceName>` può contenere un *UUID v.4* dell'*attribute set* richiedibile dal SP, comprensivo dell'attributo `xmlns:lang`, valorizzato con una stringa vuota;
- l'elemento `<md:Organization>` che contiene i dati del Service Provider in veste di persona giuridica;
- gli elementi `<ContactPerson>` che dovranno contenere le informazioni di censimento e contatto del Service Provider e dell'eventuale partner tecnologico (cfr. *Federazione* (pagina 9)).

I dati identificativi del Service Provider e del partner tecnologico devono coincidere con quelli inseriti in fase di richiesta di adesione. Per maggiori dettagli consultare il capitolo *Federazione* (pagina 9).

6.2 Protocolli di comunicazione

I protocolli di comunicazione previsti da entrambi gli schemi (*Entra con CIE* e SPID) sono basati sullo standard SAML versione 2.0 e, dunque, ereditano da esso le principali specifiche tecniche. Tuttavia nella modalità specifica secondo la quale gli schemi di identificazione sono declinati è possibile individuare alcune lievi differenze che possono avere un impatto sull'implementazione da parte del Service Provider.

Nella costruzione della richiesta di autenticazione `<AuthnRequest>` è necessario valorizzare l'attributo `Destination` coerentemente con l'attributo `Location` presente nel tag `SingleSignOnService` riportato nel metadata dell'IdP e relativo al particolare binding utilizzato in fase di richiesta (cfr. *Protocolli di comunicazione* (pagina 20) e *Modalitá di trasmissione dei messaggi* (pagina 31) per ulteriori dettagli).

Per quanto riguarda il parsing e la verifica dei messaggi di *response*, il Service Provider deve tenere conto che, diversamente da quanto previsto da SPID,

- l'attributo `Format` dell'elemento `<samlp:Issuer>` non è presente;
- l'elemento `<saml:AuthnContextClassRef>` è valorizzato sempre con il valore `https://www.spid.gov.it/SpidL3**`;
- gli attributi inviati in risposta alla richiesta di autenticazione corrispondono sempre al *Minimum Dataset eIDAS* e non prevedono, nella versione attuale, l'invio di ulteriori attributi quali ad esempio lo *spidCode*.

CAPITOLO 7

SDK App Mobile

I Service Provider che intendono erogare i propri servizi tramite App mobile, hanno la possibilitá di integrare lo schema di autenticazione «Entra con CIE».

- *Flusso con reindirizzamento*: l'App del Service Provider, all'atto della richiesta di autenticazione dell'utente, reindirizza la richiesta all'App CieID che prende in carico la comunicazione e l'autenticazione con la CIE.
- *Flusso integrato*: il processo di autenticazione viene effettuato direttamente all'interno dell'App del Service Provider, il quale integra la comunicazione con la CIE mediante una libreria software.

7.1 SDK Android

La versione del SDK per SO Android ,**CieID-android-sdk**, é disponibile al link https://github.com/italia/cieid-android-sdk. É costituita da una libreria software, realizzata in codice nativo Android *Kotlin*, e integra un app di esempio che descrive le diverse modalitá di integrazione dello schema «Entra con CIE»:

7.1.1 Requisiti di integrazione

L'utilizzo dell'SDK presuppone che il Service Provider sia correttamente federato con l'Identity Provider e che abbia implementato i protocolli SAML v2 previsti dallo schema di autenticazione «Entra con CIE» (cfr. le sezioni relative a *Federazione* (pagina 9), *Protocolli di comunicazione* (pagina 20) e *Modalitá di trasmissione dei messaggi* (pagina 31)).

Inoltre é necessario che i seguenti requisiti siano soddisfatti:

- versione Android 6.0 (API level 23) o successive;
- utilizzo di un dispositivo mobile dotato di tecnologia NFC;
- disponibilitá di una connessione ad internet.

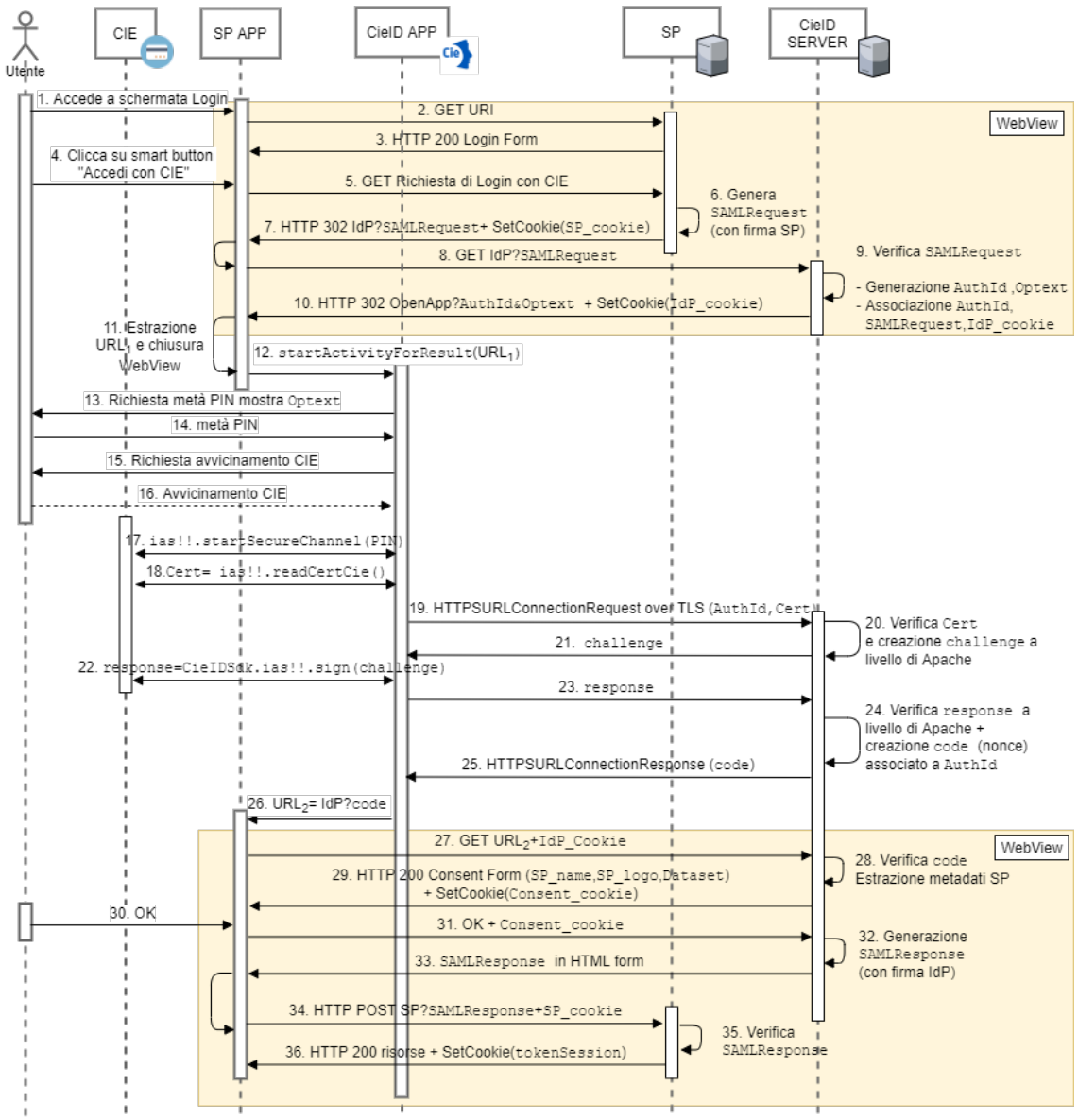

Fig. 7.1: Flusso con reindirizzamento

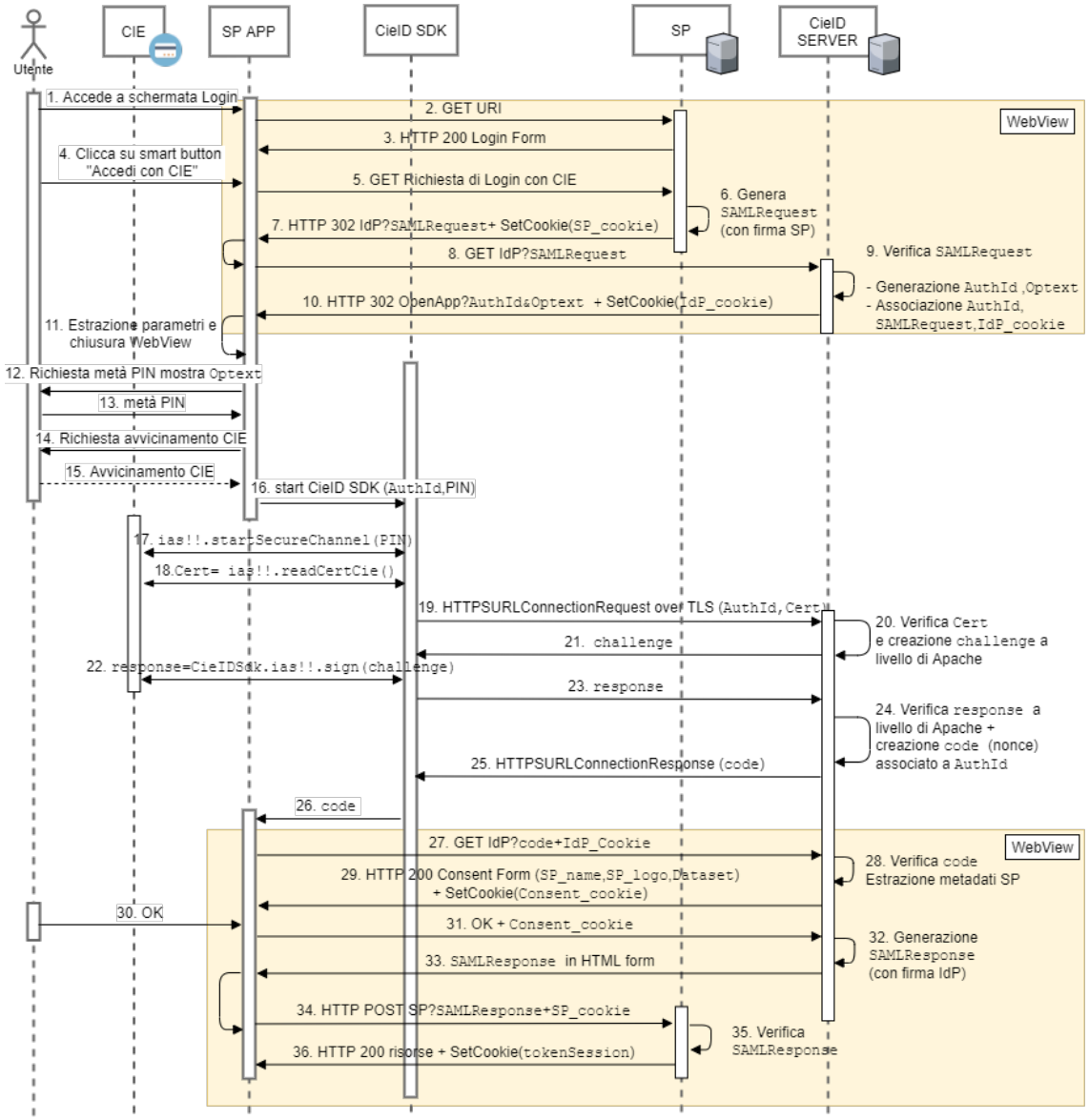

Fig. 7.2: Flusso integrato

7.1.2 Configurazione

L'IdP mette a disposizione due ambienti: uno di **preproduzione**, per gli sviluppi applicativi, e l'altro di **produzione**, per la messa in esercizio. Per tale ragione é necessaria una fase iniziale di configurazione, che dipende dal tipo di flusso integrato.

Entrambi i flussi vengono avviati tramite l'utilizzo di una *Webview*, é necessario caricare la URL del Service Provider che integra il pulsante «Entra con CIE» come mostrato nell'esempio:

```
//inserire url service provider
webView.loadUrl("URL del Service Provider")
```

Flusso con reindirizzamento

Nel caso di *flusso con reindirizzamento*, per far proseguire correttamente il flusso, é necessario selezionare l'applicazione «CieID» a cui indirizzare le richieste di autenticazione. Ció puó essere fatto modificando i commenti dalle righe di interesse, come mostrato di seguito.

```
val appPackageName = "it.ipzs.cieid"
//COLLAUDO
//val appPackageName = "it.ipzs.cieid.collaudo"
```

Flusso integrato

Per quanto riguarda il *flusso integrato*, invece, la fase di autenticazione viene gestita dalla libreria software. In questo caso é necessario integrare il modulo «CieIDSdk»:

L'SDK utilizza *Gradle* con strumento di build automatico. Per configurare correttamente il flusso, é necessario selezionare l'ambiente server dell'Identity Provider a cui indirizzare le richieste di autenticazione. Ció puó essere fatto modificando il file *build.gradle* modificando i commenti dalle righe di interesse, come mostrato di seguito:

```
//AMBIENTI:
//Ambiente di produzione
//buildConfigField "String", "BASE_URL_IDP", "\"https://idserver.servizicie.interno.
↪gov.it/idp/\""

//Ambiente di collaudo
buildConfigField "String", "BASE_URL_IDP", "\"https://preproduzione.idserver.
↪servizicie.interno.gov.it/idp/\""
```

7.1.3 Modalitá di integrazione

L'SDK fornisce un app di esempio, con 2 activity, una per flusso, per facilitare al Service Provider l'integrazione all'interno della propria App. La gestione degli errori è demandata all'app integrante.

Integrazione del flusso con reindirizzamento

Per integrare nativamente le funzionalità dell'SDK é necessario, per prima cosa, intercettare la URL contenente il valore «/OpenApp» ed avviare l'App CieID integrando il codice seguente:

```
val intent = Intent()
try {
    intent.setClassName(appPackageName, className)
    //settare la url caricata dalla webview su /OpenApp
    intent.data = Uri.parse(url)
    intent.action = Intent.ACTION_VIEW
    startActivityForResult(intent, 0)

} catch (a : ActivityNotFoundException) {
    startActivity(
        Intent(
            Intent.ACTION_VIEW,
            Uri.parse("https://play.google.com/store/apps/details?id=$appPackageName")
        )
    )
}
return true
```

Una volta avviata correttamente l'App CieID, avviene l'autenticazione tramite la CIE, e al termine viene restituita una nuova URL da ricarica nella WebView precedente, come mostrato nell'esempio seguente:

```
override fun onActivityResult(requestCode: Int, resultCode: Int, data: Intent?) {
    super.onActivityResult(requestCode, resultCode, data)

    val url = data?.getStringExtra(URL)
    webView.loadUrl(url)
}
```

Integrazione del flusso integrato

Per integrare le funzionalità dell'SDK si utilizzano i seguenti metodi:

```
//Configurazione iniziale
CieIDSdk.start(activity, callback)
//Avvio utilizzo NFC
CieIDSdk.startNFCListening(activity)
//Abilitare o disabilitare i log, da disattivare in produzione
CieIDSdk.enableLog = true
//Bisogna settare la url caricata dalla pagina web dell' SP dalla webview su /OpenApp
CieIDSdk.setUrl(url.toString())
//inserire il pin della CIE
CieIDSdk.pin = input.text.toString()
//Avviare NFC
startNFC()
```

É necessario, inoltre, realizzare le interfacce di Callback implementando i seguenti metodi:

```
override fun onEvent(event: Event) {
//evento
}
override fun onError(e: Throwable) {
//caso di errore
}
override fun onSuccess(url: String) {
//caso di successo con url della pagina da caricare
}
```

7.2 SDK iOS

CieID-iOS-sdk è un SDK per smartphone iOS sviluppato in Swift che include le funzionalità di autenticazione di «Entra con CIE». Utilizzando questo kit, gli sviluppatori di applicazioni terze iOS possono integrare nella propria app l'autenticazione mediante la cartà d'identità elettronica.

7.2.1 Requisiti tecnici

CieID-iOS-sdk richiede versione iOS 13.0 o successive, inoltre è necessario uno smartphone iOS con tecnologia NFC (iPhone 7 o successivo, non è compatibile con iPhone SE di prima generazione - mod 2016).

7.2.2 Requisiti di integrazione

CieID-iOS-sdk necessita che il fornitore del servizio digitale sia un Service Provider federato e che integri la tecnologia abilitante al flusso di autenticazione «Entra con CIE» (cfr. le sezioni relative a *Federazione* (pagina 9), *Protocolli di comunicazione* (pagina 20) e *Modalitá di trasmissione dei messaggi* (pagina 31)).

7.2.3 Come si usa

Il kit integra per il momento il solo flusso di autenticazione con reindirizzamento di seguito descritto. L'integrazione richiede pochi semplici passaggi:

- Importazione del kit all'interno del progetto
- Configurazione dell'URL Scheme
- Configurazione dell'URL di un Service Provider valido all'interno del file Info.plist
- Configurazione dello smart button Entra con CIE all'interno dello storyboard
- Inizializzazione e presentazione della webView di autenticazione
- Gestione dei delegati

7.2.4 Flusso con reindirizzamento

Il flusso di autenticazione con reindirizzamento permette ad un Service Provider accreditato di integrare l'autenticazione Entra con CIE nella propria app iOS, demandando le operazioni di autenticazione all'app CieID. Questo flusso di autenticazione richiede che l'utente abbia l'app CieID installata sul proprio smartphone **in versione 1.2.1 o successiva.**

7.2.5 Flusso interno

Non disponibile in questa versione

7.2.6 Importazione

Trascinare la folder **CieIDsdk** all'interno del progetto xCode

7.2.7 Configurazione URL Scheme

Nel flusso di autenticazione con reindirizzamento l'applicazione CieID avrà bisogno aprire l'app chiamante per potergli notificare l'avvenuta autenticazione. A tal fine è necessario configurare un URL Scheme nel progetto Xcode come segue:

Selezionare il progetto **Target**, aprire il pannello **Info** ed aprire poi il pannello **URL Types**. Compilare i campi **Identifier** e **URL Scheme** inserendo il **Bundle Identifier** dell'app, impostare poi su **none** il campo **Role**.

Il parametro appena inserito nel campo **URL Scheme** dovrà essere riportato nel file **Info.plist**, aggiungendo un parametro chiamato **SP_URL_SCHEME** di tipo **String**, come mostrato nell'esempio:

```
<key>SP_URL_SCHEME</key>
<string>Inserisci qui il parametro URL Scheme</string>
```

A seguito dell'apertura dell'app la webView dovrà ricevere un nuovo URL e proseguire la navigazione. Di seguito si riporta il metodo **openUrlContext** da importare nello **SceneDelegate** che implementa tale logica:

```
func scene(_ scene: UIScene, openURLContexts URLContexts: Set<UIOpenURLContext>) {

        guard let url = URLContexts.first?.url else {

                return

        }

    var urlString : String = String(url.absoluteString)
    if let httpsRange = urlString.range(of: "https://"){

        //Rimozione del prefisso dell'URL SCHEME
        let startPos = urlString.distance(from: urlString.startIndex, to: httpsRange.
↪lowerBound)
        urlString = String(urlString.dropFirst(startPos))

        //Passaggio dell'URL alla WebView
        let response : [String:String] = ["payload": urlString]
        let NOTIFICATION_NAME : String = "RETURN_FROM_CIEID"

        NotificationCenter.default.post(name:       Notification.Name(NOTIFICATION_
↪NAME), object: nil, userInfo: response)

        }

}
```

7.2.8 Configurazione Service Provider URL

Entrambi i flussi vengono avviati tramite l'utilizzo di una WebView, per questo motivo è necessario caricare la URL dell'ambiente di produzione della pagina web del Service Provider che integra il pulsante «Entra con CIE» all'interno del file **Info.plist**, aggiungendo un parametro chiamato **SP_URL** di tipo **String**, come mostrato nell'esempio:

```
<key>SP_URL</key>
<string>Inserisci qui l'URL dell'ambiente di produzione del Service Provider</string>
```

7.2.9 Importazione del pulsante Entra con CIE

Aggiungere nello storyboard di progetto un oggetto di tipo **UIButton** ed inserire nella voce **Class** del menù **Identity inspector** la classe che lo gestisce: **CieIDButton**. L'oggetto grafico verrà automaticamente renderizzato con il pulsante ufficiale Entra con CIE.

7.2.10 Eseguire l'autenticazione

Di seguito un esempio di gestione dell'evento **TouchUpInside** per eseguire il codice necessario per inizializzare e presentare la WebView di autenticazione.

```
@IBAction func  startAuthentication(_ sender: UIButton){

        let cieIDAuthenticator = CieIDWKWebViewController()
        cieIDAuthenticator.modalPresentationStyle = .fullScreen
        cieIDAuthenticator.delegate = self
        present(cieIDAuthenticator, animated: true, completion: nil)

    }
```

La classe chiamante dovrà essere conforme al protocollo **CieIdDelegate** come mostrato nell'esempio.

```
class  ExampleViewController: UIViewController, CieIdDelegate {
...
}
```

L'utente potrà navigare nella webView mostrata che lo indirizzerà sull'app CieID dove potrà eseguire l'autenticazione con la Carta di Identità Elettronica, al termine verrà nuovamente reindirizzato sull'app chiamante in cui potrà dare il consenso alla condivisione delle informazioni personali e portare al termine l'autenticazione.

Al termine dell'autenticazione verrà chiamato il delegato **CieIDAuthenticationClosedWithSuccess**. La chiamata di questo delegato avviene nella classe **CieIDWKWebViewController**. Potrebbe rendersi necessario posticipare la chiamata di questo delegato in base alla logica di autenticazione del Service Provider.

7.2.11 Gestione eventi

Il protocollo impone la gestione dei seguenti eventi mediante delegati

```
    func  CieIDAuthenticationClosedWithSuccess() {

            print("Authentication closed with SUCCESS")

    }
```

```
func  CieIDAuthenticationCanceled() {

        print("L'utente ha annullato l'operazione")

    }
```

```
    func  CieIDAuthenticationClosedWithError(errorMessage: String) {

            print("ERROR MESSAGE: \(errorMessage)")

    }
```

7.3 Licenza

Il codice sorgente è rilasciato sotto licenza BSD (codice SPDX: BSD-3-Clause).

CAPITOLO 8

Testing

Al termine delle attivitá di implementazione, il Service Provider deve effettuare dei test in ambiente di pre-produzione volti alla verifica della corretta funzionalitá del servizio e produrre opportune evidenze in formato immagine (screenshot). Tali evidenze devono essere caricate sul portale di federazione erogatori di sevizi[22] al fine di rendere possibile le verifiche tecniche svolte dal personale del Poligrafico incaricato allo svolgimento di tale attività.

Il set minimo di test che dovrà essere eseguito correttamente comprende quelli volti a provare la corretta gestione almeno dei seguenti "error codes", come dettagliati nell'apposita sezione relativa alla specifica dei codici d'errore restituiti dal CIE ID SERVER (*Codici di errore* (pagina 52))

- 1=Success;
- 21=Timeout durante l'autenticazione
- 22=Utente sceglie di non proseguire con l'invio degli attributi
- 25=Processo di autenticazione annullato dall'utente

Nel caso di esito positivo delle verifiche suddette il Service Provider può procedere con la fase successiva di federazione in ambiente di produzione.

[22] https://federazione.servizicie.interno.gov.it

CAPITOLO 9

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 SPID[23].

[23] https://www.agid.gov.it/sites/default/files/repository_files/circolari/spid-regole_tecniche_v1.pdf

CAPITOLO 10

Assistenza tecnica

L'assistenza agli erogatori di servizi deve avvenire mediante uno specifico indirizzo di posta elettronica messo a disposizione dal Ministero dell'Interno. In caso di problemi di natura amministrativa o tecnica è necessario, dunque, inviare una apposita richiesta di supporto all'indirizzo cie.enti@interno.it fornendo tutte le informazioni necessarie per espletare adeguatamente l'attività di supporto, comprese le informazioni di contatto relative al soggetto richiedente e al Service Provider a cui afferisce.

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.

10.1 Troubleshooting

Prima di procedere con la richiesta di supporto ai referenti tecnici dell'Identity Provider, si consiglia di verificare la correttezza sintattica e semantica dei metadata come specificato nella sezione *Federazione* (pagina 9) nonché la corretta implementazione dei *Protocolli di comunicazione* (pagina 20) e delle *Modalitá di trasmissione dei messaggi* (pagina 31). In particolare, al fine di agevolare le attivitá di integrazione e test dei Service Provider (SP), di seguito si riporta un elenco *non* esaustivo di potenziali problemi che possono impedire la corretta autenticazione con una indicazione relativa di troubleshooting:

Tabella 10.1: Troubleshooting

Schermata IdP (Cie ID Server)	Troubleshooting SP
«L'applicazione a cui hai acceduto non è registrata per l'utilizzo con questo servizio.»	Verificare i dati di federazione o la richiesta di autenticazione. Tale errore puó essere causato dal fatto che il Service Provider sta inviando una richiesta di autenticazione nella quale il valore presente nel campo `<Issuer>` non trova corrispondenza con quello valorizzato nell'attributo `entityID` presente nei metadata
«Il servizio di accesso non è stato in grado di identificate una modalità compatibile per rispondere all'applicazione richiesta. Ciò generalmente è dovuto ad una configurazione errata dell'applicazione e dovrebbe essere segnalata al proprietario o al team di supporto dell'applicazione.»	Verificare che siano rispettati i requisiti relativi ai binding per la corretta trasmissione dei messaggi (`ProtocolBinding`)
«Il servizio di accesso e l'applicazione richiesta non hanno una configurazione di sicurezza compatibile e la richiesta non può essere soddisfatta.»	Problemi relativi alla configurazione di sicurezza. In tal caso puó essere utile verificare che sia rispettato il requisito minimo relativo al TLS (versione almeno pari a 1.2)
«La richiesta non può essere soddisfatta poiché il messaggio ricevuto non rispetta i requisiti di sicurezza del servizio di accesso.»	Potenziale problema sui sigilli elettronici (chiamati anche, impropriamente, «firme digitali») apposti sul metadata del SP stesso e/o sulle *request*. Occorre verificare: 1. la presenza di un sigillo elettronico, nell'elemento `<Signature>` in testa al metadata del SP, afferente al certificato elettronico di cui al punto successivo; 2. la validità del certificato elettronico presente nell'elemento `<Signature>` al punto precedente; 3. la presenza, nella *request*, di un sigillo elettronico (afferente a uno dei certificati elettronici di cui al punto successivo) localizzato, *alternativamente*, nell'elemento `<Signature>` della *request*, nel caso di binding in HTTP POST, *ovvero* nel parametro `Signature` della *query string* veicolante la *request*, nel caso di binding HTTP Redirect; 4. la validitá del certificato elettronico afferente al sigillo di cui al punto precedente; tale certificato, all'interno del metadata del SP, si trova tra gli elementi `KeyDescriptor` con l'attributo `use` valorizzato con `signing`; 5. la coerenza dell'attributo `Destination` nella *request* con l'attributo `Location` del tag `SingleSignOnService` riportato nel metadata dell'IdP in relazione al tipo di binding utilizzato per inviare la *request*. Per ulteriori informazioni si faccia riferimento al capitolo sull'*infrastruttura a chiave pubblica* (pagina 50).
«Il servizio di accesso non è stato in grado di identificate una modalità compatibile per rispondere all'applicazione richiesta. Ciò generalmente è dovuto ad una configurazione errata dell'applicazione e dovrebbe essere segnalata al proprietario o al team di supporto dell'applicazione.»	Ciò può essere dovuto al fatto che non è possibile risolvere l'endpoint di *AssertionConsumerService*. Tale problematica si presenta, ad esempio, quando l'IdP effettua il controllo di base, previsto dal protocollo SAML, sull'AssertionConsumerServiceURL indicato nella richiesta di autenticazione e quello presente all'interno del relativo metadata

Nel caso il Service Provider, a seguito di una corretta autenticazione, non venga reindirizzato correttamente all'URL richiesta, é necessario verificare che gli attributi

- `AttributeConsumingServiceIndex`,
- `AssertionConsumerServiceURL`,

siano correttamente referenziati in modo coerente con quanto riportato all'interno dei metadata (ad esempio, tramite le loro referenze numeriche, assegnate mediante gli attributi `index`).

Nota: Per meglio effettuare l'attivitá di troubleshooting, si suggerisce l'utilizzo di strumenti di debug, quali ad esempio l'estensione di Google Chrome «SAML-Tracer»[24], che consentono di intercettare i messaggi SAML scambiati e poter quindi effettuare le verifiche necessarie dei requisiti previsti per la corretta integrazione dello schema di autenticazione Entra con CIE.

---

[24] https://chrome.google.com/webstore/detail/saml-tracer/mpdajninpobndbfcldcmbpnnbhibjmch?hl=

CAPITOLO 11

Crittografia e infrastruttura a chiave pubblica (PKI)

11.1 Sigilli di federazione

Tutti gli *enti federati*, cioè i soggetti che entrano nella federazione CIE - ad esempio Service Provider (SP) e Identity Provider (Id) - utilizzano *chiavi crittografiche private* sotto il loro esclusivo controllo per:

- creare un sigillo elettronico sul metadata propro di ciascun ente federato;
- creare sigilli elettronici sulle richieste di autenticazione (*request*) inviate dagli SP all'IdP;
- creare sigilli elettronici sulle asserzioni (*assertion*) e sulle risposte di autenticazione (*response*) restituite dall'IdP agli SP;
- zcifrare i messaggi scambiati con altri enti federati.

I sigilli elettronici apposti in modalità *enveloped* sulle evidenze SAML (cioè all'interno dello stesso documento XML che rappresenta il metadata, la *request* o la *response*), denominati *sigilli di federazione*, sono contenuti nell'elemento `<Signature>` in testa all'evidenza. I certificati elettronici per:

- la creazione di sigilli elettronici sulle *request*, le *assertion* e le *response*;
- la cifratura dei messaggi scambiati tra enti federati;

sono contenuti, all'interno di elementi `<KeyDescriptor>` con attributo `<use>` valorizzato, rispettivamente, come `<signing>` o `<encryption>`. I certificati elettronici afferenti a chiavi crittografiche utilizzate dagli enti federati per altri scopi sono contenute in ulteriori estensioni SAML dei metadata. Tutti i sigilli di federazione **devono** essere acclusi per intero mediante elementi `<KeyInfo>` contenenti il *payload* del certificato in un elemento `<X509Certificate>`. Tali elementi rispettano lo standard XML Signature Syntax and Processing[25] del W3C[26], nella versione riportata nelle specifiche SAML di riferimento per lo schema *CieID*.

[25] https://www.w3.org/TR/xmldsig-core2/
[26] https://www.w3.org

11.2 Struttura dei certificati di federazione

I certificati di federazione sono conformi con quanto previsto dalla normativa *RFC 5280* e rispettano anche la normativa comunitaria ETSI in materia di sigilli elettronici avanzati.

I Service Provider possono, per il momento, adottare anche certificati generati in modalità *self-signed*. Tali certificati, però, perdono la denominazione di sigilli di federezione.

In tutti i certificati di *sigillo* elettronico (non trattandosi di certificati di *firma* elettronica), è **vietato** l'uso delle seguenti estensioni X.509 / X.520:

- `name` (OID 2.5.4.41[27]),
- `surname` (OID 2.5.4.42[28]),
- `initials` (OID 2.5.4.43[29]),
- `generationQualifier` (OID 2.5.4.44[30]),
- `familyInformation` (OID 2.5.4.64[31]),
- `pseudonym` (OID 2.5.4.65[32]).

Ulteriori estensioni possono essere presenti nei certificati, purché non vadano in contrasto con le attuali specifiche tecniche e con le norme e standard qui richiamati.

11.3 Algoritmi crittografici

Per la creazione di sigilli elettronici è utilizzato l'algoritmo crittografico RSA con lunghezza delle chiavi di almeno 1024 bit e algoritmo di *hash* SHA-256 o superiore (cioè con lunghezza dell'impronta crittografica pari almeno a 256 bit).

Per gli scopi di cifratura dei messaggi è adottato l'algoritmo crittografico AES con lunghezza delle chiavi di almeno 256 bit.

[27] http://oid-info.com/get/2.5.4.41
[28] http://oid-info.com/get/2.5.4.42
[29] http://oid-info.com/get/2.5.4.43
[30] http://oid-info.com/get/2.5.4.44
[31] http://oid-info.com/get/2.5.4.64
[32] http://oid-info.com/get/2.5.4.65

CAPITOLO 12

Codici di errore

Di seguito si riportano le tabelle con i codici di errore, alcuni dettagli relativi al troubleshooting e le relative azioni che il Service Provider deve effettuare.

Tabella 12.1: Autenticazione corretta

Error code	1
Scenario di riferimento	Autenticazione corretta
Binding	HTTP POST / HTTP Redirect
HTTP status code	200
SAML Status code/Sub Status/StatusMessage	urn:oasis:names:tc:SAML:2.0:status:Success
Destinatario notifica	Fornitore del servizio (SP)
Schermata IdP (CIE ID SERVER)	
Troubleshooting utente	
Troubleshooting SP	
Note	

Tabella 12.2: Anomalie di sistema

Error code	2	3
Scenario di riferimento	Indisponibilità sistema	Errore di sistema
Binding	HTTP POST	HTTP Redirect
HTTP status code		500
SAML Status code/Sub Status/StatusMessage	n.a.	n.a.
Destinatario notifica	Utente	Utente
Schermata IdP (CIE ID SERVER)	Messaggio di errore generico	Pagina di cortesia con messaggio “Sistema di autenticazione non disponibile -Riprovare più tardi”
Troubleshooting utente	Ripetere l’accesso al servizio in un secondo momento	Ripetere l’accesso al servizio in un secondo momento
Troubleshooting SP		
Note		

Tabella 12.3: Anomalie di binding

Error code	4	4	5	6	6
Scenario di riferimento	Formato binding non corretto	Formato binding non corretto	Verifica della firma fallita	Binding su metodo HTTP errato	Binding su metodo HTTP errato
Binding	HTTP Redirect	HTTP POST	HTTP Redirect	HTTP Redirect	HTTP POST
HTTP status code	403	403	403	403	403
SAML Status code/Sub Status/StatusMessage	n.a.	n.a.	n.a.	n.a.	n.a.
Destinatario notifica	Utente	Utente	Utente	Utente	Utente
Schermata IdP (CIE ID SERVER)	Pagina di cortesia con messaggio “Formato richiesta non corretto - Contattare il gestore del servizio”	Pagina di cortesia con messaggio “Formato richiesta non corretto - Contattare il gestore del servizio”	Pagina di cortesia con messaggio «Impossibile stabilire l’autenticità della richiesta di autenticazione - Contattare il gestore del servizio”	Pagina di cortesia con messaggio “Formato richiesta non ricevibile - Contattare il gestore del servizio”	Pagina di cortesia con messaggio “Formato richiesta non ricevibile - Contattare il gestore del servizio”
Troubleshooting utente	Contattare il gestore del servizio	Contattare il gestore del servizio	Contattare il gestore del servizio	Contattare il gestore del servizio	Contattare il gestore del servizio
Troubleshooting SP	Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all’utente	Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all’utente	Verificare certificato o modalità di apposizione firma	Verificare metadata CIE ID SERVER	Verificare metadata CIE ID SERVER
Note	Parametri obbligatori: SAMLRequest SigAlg Signature. Parametri non obbligatori: RelayState	Parametri obbligatori: SAMLRequest. Parametri non obbligatori: RelayState	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	Invio richiesta in HTTP-Redirect su entrypoint HTTP-POST dell’identity	Invio richiesta in HTTP-POST su entrypoint HTTP-Redirect dell’identity

Tabella 12.4: Anomalie della richiesta - codici 7,8,9

Error code	7	8	9
Scenario di riferimento	Errore sulla verifica della firma della richiesta	Formato della richiesta non conforme alle specifiche SAML	Parametro version non presente - malformato o diverso da '2.0'
Binding	HTTP POST	HTTP POST / HTTP Redirect	HTTP POST / HTTP Redirect
HTTP status code	403	n.a.	n.a.
SAML Status code/Sub Status/StatusMessage	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester ErrorCode nr08	urn:oasis:names:tc:SAML:2.0:status:VersionMismatch. ErrorCode nr09
Destinatario notifica	Utente	Fornitore del servizio (SP)	Fornitore del servizio (SP)
Schermata IdP (CIE ID SERVER)	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio"		
Troubleshooting utente	Contattare il gestore del servizio		
Troubleshooting SP	Verificare certificato o modalità di apposizione firma	Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente	Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente
Note	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	Non conforme alle specifiche SAML - Il controllo deve essere operato successivamente alla verifica positiva della firma	

Tabella 12.5: Anomalie della richiesta - codici 10,11,12

Error code	10	11	12
Scenario di riferimento	Issuer non presente - malformato o non corrispondete all'entità che sottoscrive la richiesta	ID (Identificatore richiesta) non presente malformato o non conforme	RequestAuthnContext non presente malformato o non previsto da scenario eID CIE
Binding	HTTP POST / HTTP Redirect	HTTP POST / HTTP Redirect	HTTP POST / HTTP Redirect
HTTP status code	403	n.a.	n.a.
SAML Status code/Sub Status/StatusMessage	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester. ErrorCode nr11	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:statuss:NoAuthnContext. ErrorCode nr12
Destinatario notifica	Utente	Fornitore del servizio (SP)	Fornitore del servizio (SP)
Schermata IdP (CIE ID SERVER)	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio"		Pagina temporanea con messaggio di errore: "Tipologia di autenticazione non supportata"
Troubleshooting utente	Contattare il gestore del servizio		
Troubleshooting SP	Verificare la conformità del formato del messaggio di richiesta.	Verificare la conformità del formato del messaggio di richiesta.	Informare l'utente
Note			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.

Tabella 12.6: Anomalie della richiesta - codici 13,14,15

Error code	13	14	15
Scenario di riferimento	IssueInstant non presente malformato o non coerente con l'orario di arrivo della richiesta	destination non presente malformata o non coincidente con il Gestore delle identità ricevente la richiesta	attributo isPassive presente e attualizzato al valore true
Binding	HTTP POST / HTTP Redirect	HTTP POST / HTTP Redirect	HTTP POST / HTTP Redirect
HTTP status code	n.a.	n.a.	n.a.
SAML Status code/Sub Status/StatusMessage	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestDenied ErrorCode nr13	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr14	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoPassive ErrorCode nr15
Destinatario notifica	Fornitore del servizio (SP)	Fornitore del servizio (SP)	Fornitore del servizio (SP)
Schermata IdP (CIE ID SERVER)			
Troubleshooting utente			
Troubleshooting SP	Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente	Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente	Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente
Note			

Tabella 12.7: Anomalie della richiesta - codici 16,17,18

Error code	16	17	18
Scenario di riferimento	AssertionConsumerService non correttamente valorizzato	Attributo Format dell'elemento NameIDPolicy assente o non valorizzato secondo specifica	AttributeConsumerServiceIndex malformato o che riferisce a un valore non registrato nei metadati di SP
Binding	HTTP POST / HTTP Redirect	HTTP POST / HTTP Redirect	HTTP POST / HTTP Redirect
HTTP status code	n.a.	n.a.	n.a.
SAML Status code/Sub Status/StatusMessage	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported. ErrorCode nr16	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported. ErrorCode nr17	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported. ErrorCode nr18
Destinatario notifica	Fornitore del servizio (SP)	Fornitore del servizio (SP)	Fornitore del servizio (SP)
Schermata IdP (CIE ID SERVER)			
Troubleshooting utente			
Troubleshooting SP	Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente	Verificare la conformità del formato del messaggio di richiesta. Fornire pagina di cortesia all'utente	Riformulare la richiesta con un valore dell'indice presente nei metadati
Note			

Tabella 12.8: Anomalie utente

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

Nota: I codici 19, 20 e 24 sono riservati.