***Specifiche tecniche di***

***cooperazione cie-anpr   
Versione 2***

**INDICE**

[1. Premessa 4](#_Toc478654952)

[2. Glossario 5](#_Toc478654953)

[3. Modalità di accesso 7](#_Toc478654954)

[3.1 Soluzione 1 7](#_Toc478654955)

[3.2 Soluzione 2 8](#_Toc478654957)

[3.3 Soluzione 3 8](#_Toc478654958)

[4. Struttura generale dei messaggi 10](#_Toc478654959)

[4.1 Envelope 10](#_Toc478654960)

[4.2 Header 10](#_Toc478654961)

[4.3 Body 10](#_Toc478654962)

[4.4 Messaggi di richiesta 10](#_Toc478654963)

[4.4.1 Testata richiesta 10](#_Toc478654964)

[4.4.2 Corpo richiesta 10](#_Toc478654966)

[4.4.3 Specifiche delle interfacce di richiesta di ciascun servizio 11](#_Toc478654967)

[4.5 Messaggi di risposta 12](#_Toc478654968)

[4.5.1 Testata risposta 12](#_Toc478654969)

[4.5.2 Corpo risposta 12](#_Toc478654970)

[4.6 Rappresentazione dei dati 12](#_Toc478654971)

[5. Struttura del corpo dei messaggi dei servizi di ANPR 14](#_Toc478654972)

[5.1 Interrogazione dati anagrafici 14](#_Toc478654973)

[5.1.1 Struttura dati richiesta 15](#_Toc478654974)

[5.1.2 Struttura dati risposta 15](#_Toc478654975)

[5.2 Comunicazione di avvenuta emissione CIE 15](#_Toc478654976)

[5.2.1 Struttura dati richiesta 16](#_Toc478654977)

[5.2.2 Struttura dati risposta 16](#_Toc478654979)

[5.3 Comunicazione di annullamento CIE 16](#_Toc478654982)

[5.3.1 Struttura dati richiesta 17](#_Toc478654984)

[5.3.2 Struttura dati risposta 17](#_Toc478654986)

[5.4 Subentro di un Comune in ANPR 17](#_Toc478654987)

[5.4.1 Struttura dati richiesta 18](#_Toc478654988)

[5.4.2 Struttura dati risposta 18](#_Toc478654989)

[6. Riepilogo dei servizi 18](#_Toc478654990)

[7. Processi 19](#_Toc478654991)

[7.1 Interrogazione dati anagrafici 20](#_Toc478654992)

[7.2 Comunicazione avvenuta emissione CIE 22](#_Toc478654993)

[7.3 Comunicazione annullamento CIE 23](#_Toc478654994)

[7.4 notifica subentro 24](#_Toc478654995)

[Esempio SAML Authentication Assertion da inserire nel WS-SECURITY 30](#_Toc478654996)

# Premessa

Il documento descrive le modalità di colloquio del sistema ANPR con la piattaforma CIEOnline offerta agli ufficiali di anagrafe per l’espletamento dei processi di emissione della Carta di Identità elettronica. Titolare di entrambe le piattaforme software è il Ministero dell’Interno.

Una prima sezione descrive le modalità di accesso, l’architettura generale dei sistemi e degli standard utilizzati.

La seconda sezione illustra la struttura dei messaggi, specificando anche dal punto di vista della sicurezza, gli standard adottati.

La terza sezione, infine, contiene per ciascun servizio:

* la descrizione del funzionamento, evidenziando il flusso logico della transazione cui è associato;
* l’elenco dei campi di input e di output dei web services utilizzati, in formato di tabella excel;
* il nome del file XSD associato a ciascuno servizio.

# Glossario

|  |  |  |
| --- | --- | --- |
| **Termine** | **Descrizione** | **Note** |
| AE | Agenzia delle Entrate |  |
| ANPR | Anagrafe Nazionale della Popolazione Residente | Rappresenta il sistema centrale di ANPR che eroga i servizi |
| Corporichiesta | Insieme di oggetti che contengono i parametri da indicare, a cura del comune e specifici per l’operazione che si richiede |  |
| Corporisposta | Insieme di oggetti che contengono le informazioni restituite da ANPR a fronte della richiesta inoltrata dal comune |  |
| datiCF | Dati che concorrono alla formazione del codice fiscale | Sono costituiti dal cognome, nome, sesso, data di nascita, luogo di nascita identificato attraverso il codice catastale (o codice Belfiore) che identifica il comune e la provincia “vigenti” al momento della nascita o dallo stato estero attuale |
| WS | Web Services | Il comune opera in modalità WS quando per le registrazioni anagrafiche (iscrizion mutazioni cancellazioni), utilizza il proprio sistema gestionale integrato con i WS di ANPR. |
| CIE |  | Carta di identità elettronica |
| CIEOnline |  | La piattaforma WEB utilizzata dagli ufficiali di anagrafe per l’emissione delle CIE. |

# Modalità di accesso

L’accesso al sistema ANPR da parte della piattaforma CIEOnline avviene tramite un end-point distinto da quelli utilizzati dai comuni.

In merito alle politiche di sicurezza da implementare, sono possibili tre soluzioni; l’ obiettivo è scegliere la soluzione più veloce ed economica da implementare, conforme alle vigenti norme di legge.

## Soluzione 1

**saml-completo** – la piattaforma CIEOnline utilizzata dall’ufficiale di anagrafe attraverso la sua postazione di lavoro CIE, utilizzando il certificato di postazione installato su quest’ultima, si autentica come l'operatore che sta effettuando l'operazione, esattamente come qualsiasi altro accesso ANPR. È descritta in dettaglio in allegato1[[1]](#footnote-1).

In questa ipotesi, l’operatore del Comune che esegue l’interrogazione deve essere censito in ANPR ed il certificato di postazione, rilasciato dalla CA ANPR, deve essere presente presso la piattaforma CIEOnline congiuntamente alla sua chiave privata. L’utente è identificato dal codice fiscale; la postazione si desume dal certificato. Entrambi sono ricavati dall’asserzione SAML.

**•Benefici:**

•Lato SOGEI, il codice di autenticazione funziona nello stesso modo per tutto.

•Si mantengono i requisiti di tracciamento previsti dal DPCM 194/2014

**•Problemi:**

•Complessità di deployment e supporto lato CIE.

Eg, serve configurare certificati correttamente, dare supporto ai comuni, tracciare puntualmente le informazioni di tutte le postazioni dispiegate ...

•Maggiore complessità implementativa lato CIE.

Eg, implementare piena autenticazione SAML.

## Soluzione 2

**•saml-account-tecnico** – analoga alla precedente ma si utilizza una sola coppia certificato-chiave assegnata al sistema CIEOnline.

In questa ipotesi, l’operatore del comune deve essere censito in ANPR ed il certificato di postazione del server è rilasciato dalla CA ANPR. Il codice fiscale dell’operazione si desume dall’asserzione SAML. Occorre prevedere nell’asserzione qualcosa che identifichi la postazione del comune (per esigenze di tracciamento).

**•Benefici:**

•Lato SOGEI, il codice di autenticazione funziona nello stesso modo per tutto.

**•Problemi:**

•Bisogna verificare conformità con DPCM

•Maggiore complessità implementativa lato CIE

Da completare con allegato tecnico qualora si scelga questa soluzione.

## Soluzione 3

•tls-machine-to-machine - il sistema CIEOnline coopera con il sistema ANPR su una connessione HTTPS/TLS dedicata. Viene adottato un meccanismo di autenticazione standard realizzato per mezzo di certificati X509 emessi dalle PKI CIE e ANPR per quanto di competenza. Viene inoltre inserita la firma del messaggio in quanto il solo utilizzo di un canale cifrato non garantisce l’integrità dei dati.

In questa ipotesi, un identificativo dell’operatore del Comune che esegue l’interrogazione e della postazione utilizzata dall’operatore stesso saranno indicate in modo esplicito nel body soap del messaggio. Nessuno dei due è censito nel sistema di Identity di ANPR e quindi è il sistema CieOnline avrà cura di assicurare il tracciamento completo (chi e da dove) per la parte di competenza; ANPR traccerà le operazioni eseguite dall’utente e dalla postazione “dichiarate” nel messaggio.

**•Benefici:**

•Minore complessità implementativa lato CIE dato che non è necessario implementare l’autenticazione SAML

•Gestione del ciclo di vita dei certificati molto semplice

•Nessuna perdita in termini di sicurezza

**•Problemi**:

•Dobbiamo verificare conformità con DPCM.

•SOGEI deve implementare un meccanismo di autenticazione solo per CIE, dedicato a CIE, che dovrà essere monitorato e manutenuto negli anni.

I dati necessari al tracciamento delle interrogazioni (postazione e utente) vanno gestiti a livello applicativo nei dati contenuti nel messaggio.

Da completare con allegato tecnico qualora si scelga questa soluzione.

# Struttura generale dei messaggi

## Envelope

Come da standard SOAP.

## Header

Come da standard SOAP.

Contiene, tra l’altro, le informazioni previste dall’allegato C del II DPCM ANPR, che garantiscono la sicurezza ed il tracciamento.

## Body

Come da standard SOAP

Il body è strutturato in due parti:

* testata della richiesta (testatarichiesta) o della risposta (testatarisposta)
* corpo della richiesta (corporichiesta) o della risposta (corporisposta).

## Messaggi di richiesta

#### Testata richiesta

La testata della richiesta/risposta contiene le parti comuni a tutti i messaggi di richiesta/risposta, mente la parte corpo contiene i dati specifici dell’operazione che si sta effettuando.

#### Corpo richiesta

Il corpo della richiesta varia in funzione dell’operazione che si richiede; l’elenco delle operazioni disponibili è riportato nel paragrafo 6.

#### Specifiche delle interfacce di richiesta di ciascun servizio

Per ciascuna operazione, le specifiche di interfaccia sono costituite da:

* File in formato di tabella Excel, allegato al presente documento, il cui nome è codiceServizioOperazione.xls, che contiene l’elenco dei campi previsti per ciascun servizio;
* il file xsd associato; il nome del file è codiceServizioOperazione.xsd;
* la descrizione del flusso della transazione, riportata nel presente documento.

I dati contenuti nei messaggi di richiesta e di risposta sono costituiti dall’unione di oggetti complessi che si ripetono nelle varie strutture. Il contenuto di tali oggetti in formato Excel, è contenuto nella cartella oggetti.

È opportuno osservare che alcuni oggetti possono, a loro volta, possono includere uno o più oggetti.

L’elenco dei campi indicati nei file Excel, previsti per ciascun oggetto è costituito da:

* Prog.: progressivo di ordinamento della struttura; non compare nel file xml;
* Tag di livello 1: tag principale nella struttura xml;
* Tag di livello 2: oggetto compreso nel tag di livello 1; ulteriori oggetti compresi all’interno di un tag di livello 2 sono evidenziati in carattere grassetto e gli elementi che lo compongono sono rientrati;
* Formato: contiene uno dei valori riportati nel paragrafo 4.3.3;
* Lunghezza del dato: se il valore è preceduto da “Max”, si indica la lunghezza massima, in caso contrario il dato deve avere la lunghezza fissa specificata;
* Valori ammessi: indica i valori che può assumere il dato che, a volte, possono essere contenuti in una tabella (l’elenco completo delle tabelle è disponibile a questo link <https://www.anpr.interno.it/portale/tabelle-di-riferimento>)
* Descrizione del dato;
* Obbl.: obbligatorietà; se il campo è definito obbligatorio, il tag dovrà essere necessariamente presente.

## Messaggi di risposta

#### Testata risposta

La testata della risposta contiene le parti comuni a tutti i messaggi di risposta, mente la parte body contiene i dati specifici relativi all’esito dell’operazione che è stata effettuata.

Il campo EsitoOperazione della testata della risposta, in particolare, contiene l’esito complessivo dell’operazione effettuata dal Comune, secondo quanto riportato nella tabella che segue:

|  |  |  |
| --- | --- | --- |
| **Codice esito** | **Descrizione** | **Note** |
| 0000 | Operazione completata con successo | E’ possibile che una operazione terminata con successo contenga anomalie non bloccanti |
| 01NN | Sono presenti più soggetti che verificano alle condizioni richieste | NN può variare in funzione della richiesta; la registrazione NON è stata effettuata |
| XXXX | Sono presenti errori che non consentono di proseguire nella elaborazione | La registrazione NON è stata effettuata |

#### Corpo risposta

Il corpo risposta varia in funzione del servizio che è stato richiesto e dell’esito dell’operazione. In caso di esito negativo, in particolare, il contenuto della riposta è descritto nel file.

L’elenco completo dei codici di errore è contenuto nel file Elenco errori restituiti da ANPR, pubblicato nel portale informativo www.anpr.interno.it.

## Rappresentazione dei dati

Per una corretta interpretazione dei dati deve essere utilizzata la codifica UTF-8 e l’insieme dei caratteri UNICODE ISO 10646. Ciascuno dei dati previsti, in ogni caso, possiede regole che fissano l’insieme dei caratteri ammessi.

Per tale motivo, nelle tabelle Excel che contengono l’elenco dei dati previsti, viene esplicitamente riportata una notazione che indica i caratteri ammessi e, in alcuni casi, il loro formato, secondo quanto riportato nella tabella che segue:

|  |  |  |  |
| --- | --- | --- | --- |
| **Notazione** | **Caratteri ammessi** | **Formato** | **Note** |
| A | Solo lettere dell’alfabeto inglese |  |  |
| N | Sono numeri |  |  |
| AN | Lettere e numeri |  |  |
| Char | Lettere, numeri e caratteri speciali ammessi |  |  |
| Date | Come da standard W3C | Data nel formato YYYY-MM-DD |  |
| Date time | Come da standard W3C | Data e ora nel formato YYYY-MM-DDThh:mm:ss |  |
| Dia | Lettere con segno diacritico. |  | Vedi tabella 40 pubblicata nel portale www.anpr.interno.it. |
| Dia1 | Lettere con segno diacritico ed i caratteri apice, virgola, trattino, punto |  | Vedi tabella 40 pubblicata nel portale www.anpr.interno. |
| Dia2 | Lettere con segno diacritico ed i caratteri apice, virgola, trattino |  | Vedi tabella 40 pubblicata nel portale www.anpr.interno. |

# Struttura del corpo dei messaggi dei servizi di ANPR

L’integrazione tra i sistemi CIEOnline e ANPR è resa possibile mediante l’adozione di un servizio esposto da ANPR verso il CIEOnline che prevede diverse operation associate ai seguenti casi d’uso:

* interrogazione dei dati anagrafici;
* comunicazione di avvenuta emissione;
* comunicazione di annullamento.

e da un servizio di subentro esposto dal sistema CIEOnline verso ANPR, dotato di un’unica operation, che consente di contrassegnare un Comune come subentrato sul nuovo Anagrafe Nazionale della popolazione residente ed abilitare le operazioni di comunicazione avvenuta emissione CIE e annullamento CIE.

## Interrogazione dati anagrafici

L’operazione consente di ricercare i dati della persona che ha richiesto la carta di identità.

E’ obbligatoria l’indicazione del comune di residenza, che può non coincidere con quella del comune che effettua la richiesta.

È possibile effettuare la ricerca specificando, uno dei seguenti parametri o gruppi di parametri:

* codice fiscale

Le operazioni di interrogazione inviate dalla piattaforma CIEOnline avvengono per codice fiscale, essendo quest’ultimo un dato **obbligatorio** ai fini del rilascio della CIE.

E’ obbligatorio, inoltre, indicare il comune di residenza (o il comune di iscrizione AIRE); è possibile, inoltre, indicare che la persona è iscritta all’AIRE.

Qualora il comune sia subentrato, la ricerca avviene su ANPR; in caso contrario la ricerca avviene:

* su AIRE centrale se indicato nella richiesta che la persona è iscritta all’AIRE,
* su INA, se la condizione di cui al punto precedente non è verificata;
* su AE se la persona non è presente su INA; in tal caso, si richiama il servizio di AE di interrogazione per codice fiscale.

In assenza di errori, il servizio restituisce:

* generalità anagrafiche complete;
* sesso, data e luogo di nascita;
* dati dei genitori se la persona è un minore iscritto in ANPR;
* fonte dei dati (ANPR, INA, AIRE centrale, AE);
* dati completi di residenza per i soli soggetti presenti in ANPR o nell’AIRE centrale, Comune di residenza se il cittadino è presente su INA.

A carico del sistema “chiamante” è la verifica di ammissibilità dei dati.[[2]](#footnote-4)

#### Struttura dati richiesta

#### Struttura dati risposta

## Comunicazione di avvenuta emissione CIE

L’operazione consente di comunicare ad ANPR il dati relativi alla CIE emessa, comprensivi del seriale della CIE, della data di emissione e della data di scadenza .

Il seriale della CIE in particolare è automaticamente calcolato dal sistema CIEOnline durante l’inserimento della richiesta di emissione a cura dell’uffiiciale di anagrafe. Ciò consente di aggiornare automaticamente la scheda individuale[[3]](#footnote-5) nel momento in cui viene richiesta l’emissione del documento al termine della fase di istruttoria.

Da valutare se acquisire i dati della carta emessa anche per i soggetti residenti in comuni non subentrati.

I dati da specificare nella richiesta di aggiornamento sono i seguenti:

* codice fiscale;
* identificativo soggetto attribuito da ANPR (alternativo al codice fiscale e solo per i comuni subentrati);
* cognome o indicatore di assenza cognome (obbligatorio);
* nome o indicatore di assenza nome (obbligatorio);
* data nascita, luogo di nascita, sesso (obbligatorio);
* seriale della carta di identità elettronica (numero unico nazionale, obbligatorio);
* data di emissione della carta di identità elettronica (obbligatorio);
* data di scadenza della carta di idnetità elettronica (obbligatorio).

In assenza di errori, ANPR conferma l’avvenuto aggiornamento.

#### Struttura dati richiesta

#### Struttura dati risposta

## Comunicazione di annullamento CIE

Si utilizza questa operazione per comunicare ad ANPR l’avvenuto annullamento di una CIE in precedenza emessa.

L’operazione di annullamento viene avviata automaticamente dal CIEOnline a seguito di un’operazione di revoca (o interdizione) di una CIE. L’interdizione può essere:

1. richiesta presso il Comune, nel qual caso viene effettuata ad opera di un ufficiale di anagrafe. Se il motivo è lo smarrimento o il furto del documento, il cittadino deve fornire copia della denuncia;
2. richiesta al servizio di assistenza CIE, nel qual caso viene effettuata dal Ministero dell’Interno. Se il motivo è lo smarrimento o il furto del documento, il cittadino deve fornire copia della denuncia.

Pertanto, limitatamente ai comuni subentrati, a fronte della comunicazione, si provvede all’aggiornamento della scheda individuale.

I dati da specificare nella richiesta di aggiornamento sono i seguenti:

* codice fiscale;
* identificativo soggetto attribuito da ANPR (alternativo al codice fiscale e solo per i comuni subentrati);
* cognome o indicatore di assenza cognome (obbligatorio);
* nome o indicatore di assenza nome (obbligatorio),
* data nascita, luogo di nascita, sesso (obbligtorio);
* seriale della carta di identità elettronica (obbligatorio).

In assenza di errori, ANPR conferma l’avvenuto aggiornamento.

#### Struttura dati richiesta

#### Struttura dati risposta

## Subentro di un Comune in ANPR

Le operazioni di Comunicazione avvenuta emissione CIE e annullamento CIE sono possibili solo per i Comuni subentrati sul nuovo Anagrafe Nazionale della Popolazione residente. Per abilitarle comunicando tra l’altro l’operazione di subentro, ANPR invoca un opportuno servizio esposto dalla piattaforma CIEOnline.

I dati da specificare nella notifica di subentro sono i seguenti:

* Codice ISTAT del Comune subentrato;
* Data del subentro.

In assenza di errori, CIEOnline conferma ad ANPR l’avvenuto aggiornamento.

#### Struttura dati richiesta

#### Struttura dati risposta

# Riepilogo dei servizi

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Servizio** | **Operation** | **Dettagli** | **Note** | **ServizioOperazione (Codice da indicare nel HeaderRequest)** |
| CIE0 | InterrogazioneDatiAnagrafici | Consente di ottenere i dati di un cittadino |  | CIE2 |
| CIE0 | ComunicazioneEmissione | Consente di comunicare i dati della CIE emessa |  | CIE8 |
| CIE0 | ComunicazioneAnnullamento | Consente di comunciare l’annullamento di una CIE |  | CIE7 |
| ANPRNotificaSubentroService | NotificaSubentro | Consente di notificare l’avvenuto subentro di un Comune in ANPR |  | - |

# Processi

Si riportano nel seguito, utilizzando il formalismo degli Activity Diagrams UML, alcuni diagrammi che illustrano i flussi software relativi all’integrazione CIE-ANPR.

## Interrogazione dati anagrafici

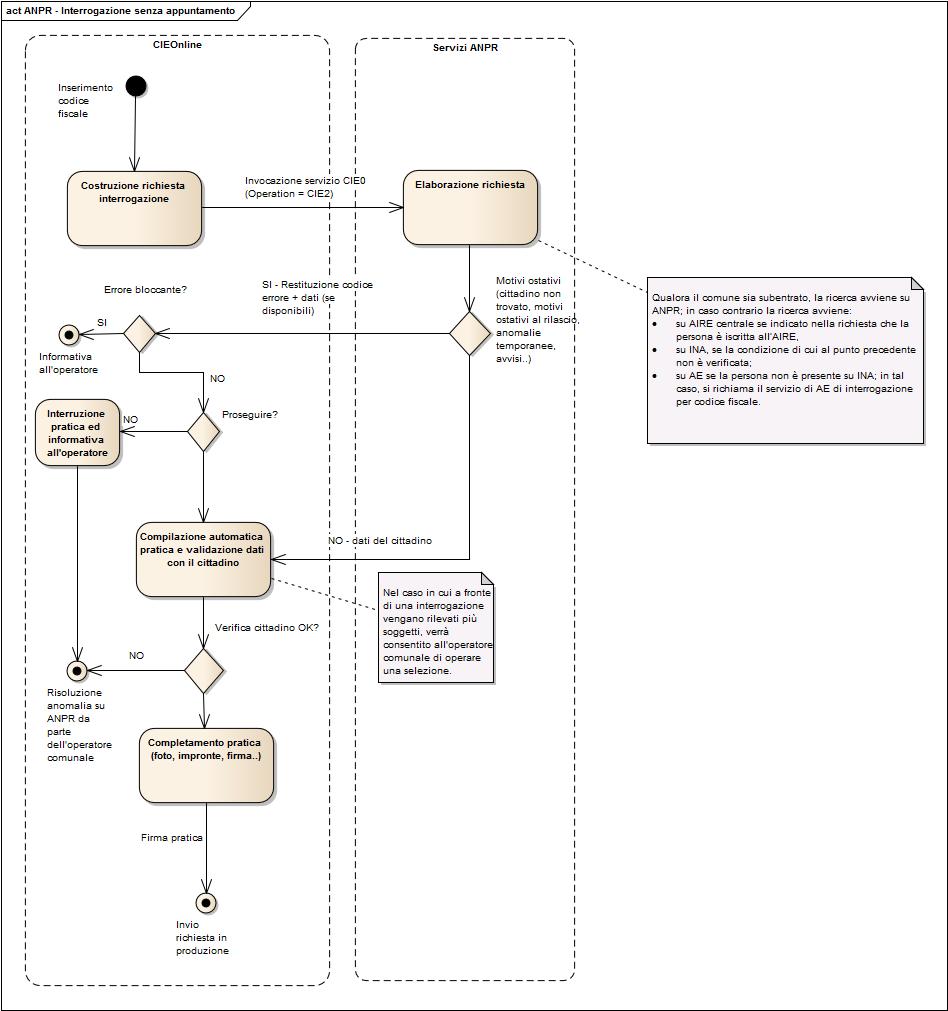


Figura 1. Interrogazione dati nel caso di richiesta senza appuntamento su Agenda CIE.

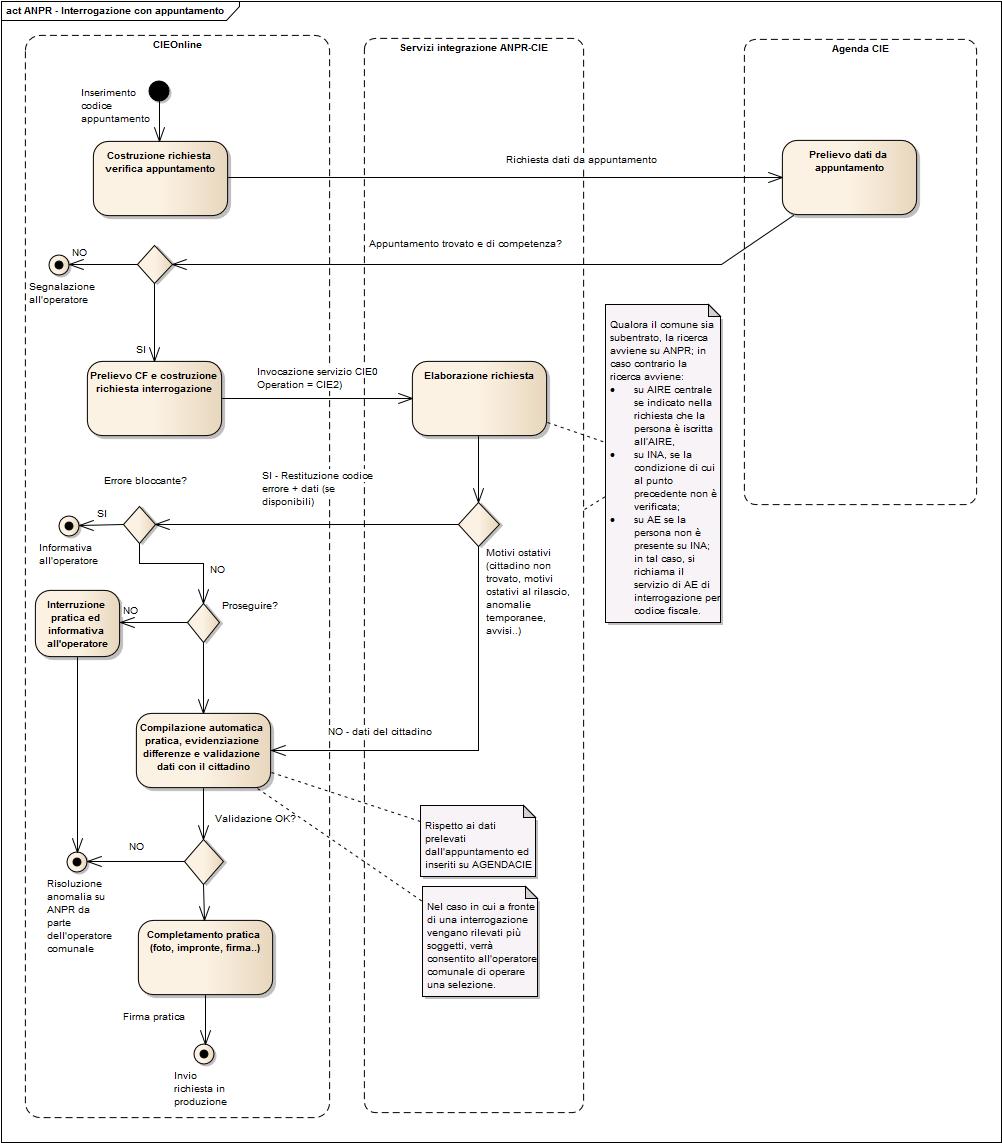


Figura 2. Interrogazione dati nel caso di richiesta con appuntamento su Agenda CIE.

## Comunicazione avvenuta emissione CIE

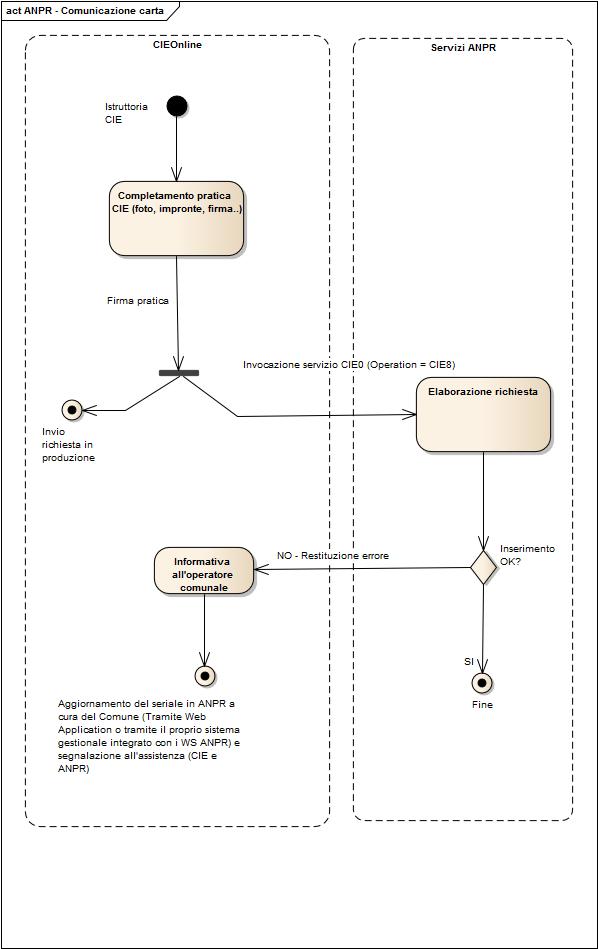


Figura 3. Comunicazione avvenuta emissione CIE

## Comunicazione annullamento CIE

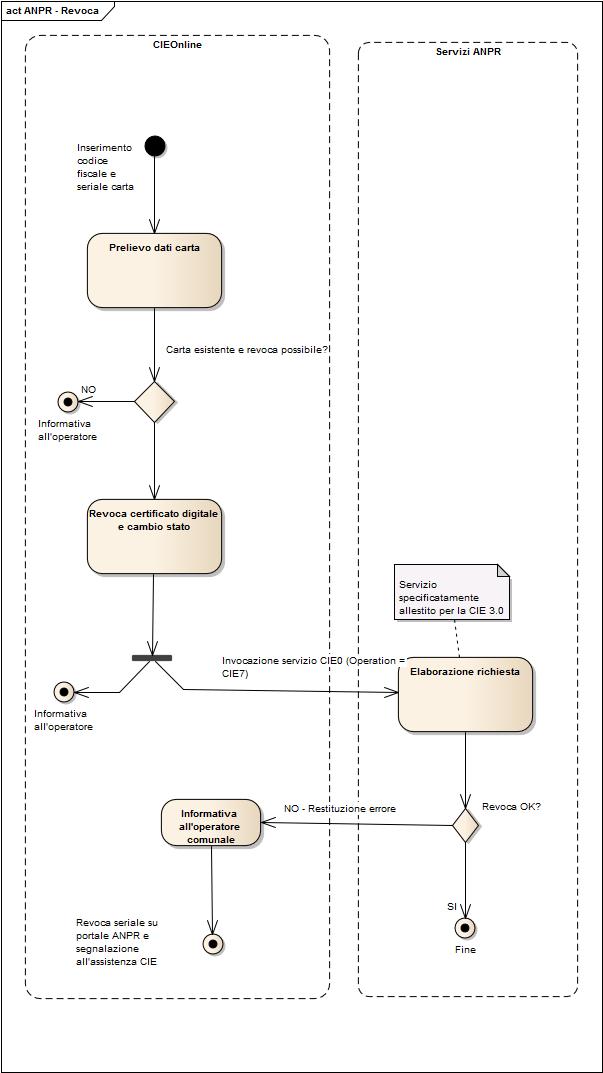


Figura 4. Comunicazione annullamento CIE

## notifica subentro

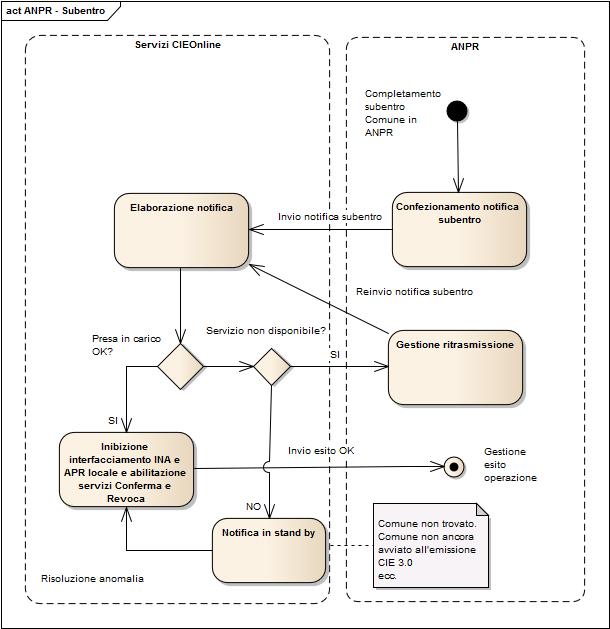


Figura 5. Notifica subentro in ANPR.

**Allegato 1**

Nella soluzione adottata per l’integrazione CIEOnline – ANPR, il comune accede ad ANPR tramite WS integrato nel sistema stesso. In tale ipotesi, il DPCM 194/2014 prevede i seguenti requisiti di sicurezza:

* l’utilizzo di un certificato identificativo,  riferito   alla   postazione, memorizzato al suo interno, emesso dalla Certification Authority di ANPR;
* il riconoscimento dell'operatore tramite la userid  e  password utilizzata per accedere ai servizi dei sistemi informativi  comunali, che garantiscono  l'autenticazione  dell'utente  e  la  verifica  dei diritti di accesso dello stesso alle varie funzionalità applicative;
* l’utilizzo di un certificato associato al CIEOnline emesso dalla Certification Authority di ANPR.

L'operatore accede autenticandosi tramite la userid e la password utilizzate per accedere ai servizi dei sistemi informativi comunali.

Per garantire   il   riconoscimento   dell'operatore   e   della postazione, autorizzata dal comune, nonchè l'integrita' dei dati,  i messaggi inviati prevedono:

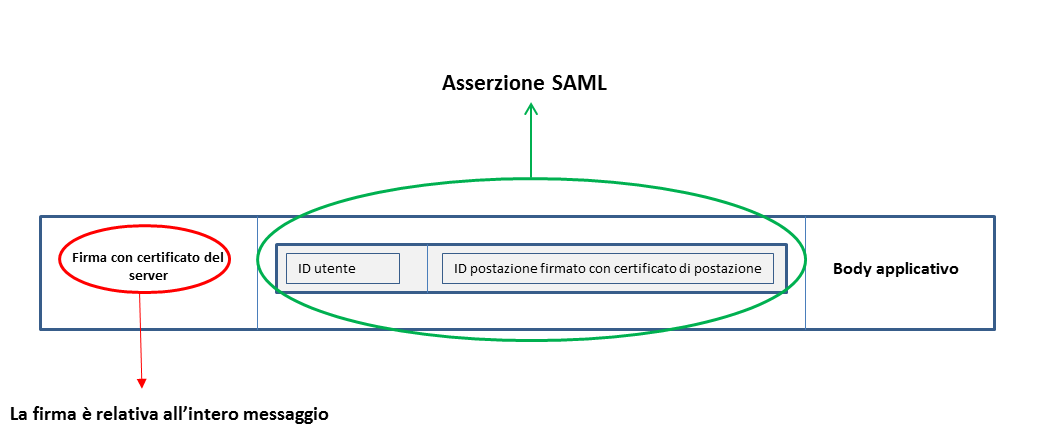
* identificativo  postazione  firmato  con  la chiave privata associata al certificato  di postazione;
* identificativo utente;
* firma  dell'intero  messaggio  mediante la chiave privata associata al   certificato  rilasciato al CIEOnline, secondo i meccanismi  standard  del protocollo Ws Security.

Alla  ricezione  del  messaggio,  ANPR  verifica  la  firma   del messaggio ed il sistema di Identity & Access management  verifica  la validità dell'identificativo della postazione,  nonchè  l'esistenza dell'utente e la rispondenza dell'operazione  richiesta  in  base  al profilo assegnato;  in  caso  di  esito  positivo,  ANPR  elabora  il messaggio.

Da ciò consegue che:

* l’utente del comune che utilizza CIEOnline deve essere censito nel sistema ANPR;
* la postazione che si utilizza deve essere munita di un certificato di postazione di ANPR.

Il messaggio da predisporre quando si invoca un servizio di ANPR, inoltre, comporta l’esecuzione di alcuni passaggi, schematizzati nella figura che segue.



Nel caso relativo all’utilizzo dei servizi dedicati all’emissione della CIE, per la firma dell’intero messaggio al CIEOnline verrà rilasciato un certificato dalla PKI ANPR, avente CN …

~~Il CN di tale certififcato sarà costituito come segue :~~ **~~[~~*~~codice istat comune~~*~~] -CI-0001~~**~~.~~

Lo standard dei web services per trasferire queste informazioni in maniera sicura è la WS Security. La ws security prevede diverse modalità di rappresentazione (token di sicurezza); si è scelto il token SAML, che garantisce anche l’attivazione di meccanismi per garantire l’autenticità del messaggio e per trasportare in maniera sicura le informazioni richieste dalla norma sopra riportata (identificativo dell’utente e postazione); questo standard, per altro, è referenziato nelle specifiche AgID.

Per la produzione del token SAML si possono utilizzare le librerie open source indicate nelle specifiche che contengono anche la necessaria documentazione; non è richiesto, in particolare di realizzare una infrastruttura di Identità Federata (IDP) basata su SAML come già indicato nelle specifiche. E’ sufficiente  usare un server nel quale sono configurate  le librerie SAML (anche open source), già indicate nelle specifiche, per applicare lo standard WS Security.

Viene utilizzato lo standard “SAMLTokenProfile” della WS-Security che prevede, per la fase di autenticazione/autorizzazione dell’utente, l’utilizzo dello standard SAML.

In particolare, in questo specifico caso, ANPR è il fornitore del servizio (Service Provider SP) mentre il CIEOnline che accede tramite web service ricopre il ruolo di fornitore di identità (Identity Provider IdP): il CIEOnline effettua il riconoscimento del proprio utente egenera l’asserzione SAML, firmata digitalmente, da inserire nel WS-Security Header della SOAPRequest inviata ai server di ANPR.

ANPR, alla ricezione della richiesta, verifica la validità dell’asserzione contenuta nel WS-Security Header della SOAPRequest, controllando la correttezza della firma digitale apposta e, in caso positivo, concede l’accesso al servizio richiesto.

L’asserzione SAML prodotta dal comune, oltre a contenere l’identificativo dell’utente (**IdOperatore**) come identità principale alla quale è stata rilasciata l’asserzione stessa, deve contenere nei propri attributi le seguenti informazioni:

* **IdSede** - Codice ISTAT del comune (es. 058091);
* **IdPostazione** - Identificativo della postazione contenuto nel certificato della postazione (assegnato dal sistema al momento del censimento utenti/postazioni);
* **IdPostazioneFirmato** - Identificativo della postazione firmato con lo stesso certificato di postazione;
* **IdApplicazione** - Identificativo dell’applicazione (nel caso specifico si dovrà utilizzare l’identificativo dell’applicazione che consente l’emissione della CIE).

L’identificativo della postazione firmato è il Base64 di un PKCS #7 Signed Data e rappresenta il risultato della firma dell’identificativo di postazione, ottenuta con la chiave privata del certificato di postazione. Il PKCS #7 deve includere il certificato per permettere la verifica della firma.

Per realizzare la firma PKCS #7, oltre a librerie crittografiche commerciali, sono disponibili librerie open source.

Il sistema descritto si basa su una relazione di trust tra il sistema del comune ed ANPR che utilizza certificati X509 per verificare la relazione stessa.

Il comune si dovrà, pertanto, dotare dei componenti che assicurino le funzionalità, disponibili anche all’interno di librerie open source.

La modalità di interazione tra l’applicazione del Comune e il sistema ANPR prevede l’utilizzo dello standard di federazione SAML.

L’applicazione richiede al proprio Identity Provider la generazione di un’asserzione SAML, firmata digitalmente con la chiave privata collegata al certificato di autenticazione del Comune emesso dalla Certification Authority (CA) di ANPR.

L’asserzione SAML, oltre a contenere l’identificativo di un utente (IdOperatore), al quale verrà imputata la richiesta, come identità principale alla quale è stata rilasciata l’asserzione, deve includere anche le seguenti informazioni in attributi dell’asserzione stessa:

* IdSede - codice ISTAT del Comune;
* IdPostazione - identificativo della postazione di lavoro intesa come il server dal quale viene effettuata la richiesta;
* IdPostazioneFirmato - PKCS#7, codificato in Base64, contenente:
* la firma dell’identificativo del server (prodotta utilizzando la chiave privata del certificato del server);
* il certificato di postazione (cioè del server) emesso dalla CA di ANPR (necessario per la validazione della firma).
* IdApplicazione - identificativo dell’applicazione del Comune chiamante (nel caso specifico si dovrà utilizzare l’identificativo dell’applicazione che consente l’emissione della CIE).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asserzione SAML** | | | | |
| **Authentication Statement** | **Attribute Statement** | | | |
| **Subject** | **Attribute** | **Attribute** | **Attribute** | **Attribute** |
| IdOperatore | IdSede | IdPostazione (Server) | IdPostazioneFirmato (PKCS#7 Server) | IdApplicazione |

L’asserzione SAML è firmata con la chiave privata collegata al certificato digitale X.509 rilasciato dalla CA ANPR al CIEOnline e sarà contenuta nell’header di ws security del messaggio SOAP di richiesta. L’intero messaggio SOAP può essere firmato sempre con il certificato assegnato al Comune e specificatamente prodotto per l’emissione della CIE.

L’applicazione del Comune produce la SOAP Request e la invia al sistema ANPR, ad una URL gestita da un apparato di sicurezza specializzato.

Il server di ANPR riceve la richiesta, verifica la validità dell’asserzione contenuta nel WS-Security Header della SOAPRequest, controllando la correttezza della firma digitale apposta, e, in caso positivo, concede l’accesso al servizio richiesto.

# Esempio SAML Authentication Assertion da inserire nel WS-SECURITY

L’esempio riportato è inerente ad entrambi gli scenari di accesso ai servizi ANPR erogati tramite web service.

**<saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0" ID="SAML-3c6ff72e-a40a-4d2a-be34-4a23948a29da" IssueInstant="2015-07-14T14:19:25Z">**

**<saml2:Issuer>XS</saml2:Issuer>**

**<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">**

**<SignedInfo>**

**<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>**

**<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>**

**<Reference URI="#SAML-3c6ff72e-a40a-4d2a-be34-4a23948a29da">**

**<Transforms>**

**<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>**

**<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>**

**</Transforms>**

**<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>**

**<DigestValue>qX2uM9tvgkvL9JFMqYlqPUwQOKc=</DigestValue>**

**</Reference>**

**</SignedInfo>**

**<SignatureValue>mBblfDbqz1jTI4v+BG..................lJfEmXSEeiwAx9NpY=</SignatureValue>**

**<KeyInfo>**

**<X509Data>**

**<X509Certificate>MIIEWTCCA0GgAwIBAgID.................rn3asP7f+tyf7hiA==</X509Certificate>**

**<X509IssuerSerial>**

**<X509IssuerName>CN=CA ANPR, O=Ministero degli Interni, C=it</X509IssuerName>**

**<X509SerialNumber>42789</X509SerialNumber>**

**</X509IssuerSerial>**

**</X509Data>**

**</KeyInfo>**

**</Signature>**

**<saml2:Subject>**

**<saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">IdOperatore</saml2:NameID>**

**<saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">**

**<saml2:SubjectConfirmationData NotBefore="2015-07-14T14:19:25Z" NotOnOrAfter="2016-07-13T14:19:25Z"/>**

**</saml2:SubjectConfirmation>**

**</saml2:Subject>**

**<saml2:Conditions NotBefore="2015-07-14T14:19:25Z" NotOnOrAfter="2016-07-13T14:19:25Z"/>**

**<saml2:AuthnStatement AuthnInstant="2015-07-14T14:19:25Z" SessionNotOnOrAfter="2016-07-13T14:19:25Z">**

**<saml2:SubjectLocality Address="26.2.103.103"/>**

**<saml2:AuthnContext>**

**<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml2:AuthnContextClassRef>**

**</saml2:AuthnContext>**

**</saml2:AuthnStatement>**

**<saml2:AttributeStatement>**

**<saml2:Attribute Name="IdSede" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">**

**<saml2:AttributeValue>H501</saml2:AttributeValue>**

**</saml2:Attribute>**

**<saml2:Attribute Name="IdPostazione" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">**

**<saml2:AttributeValue>H5012</saml2:AttributeValue>**

**</saml2:Attribute>**

**<saml2:Attribute Name="IdPostazioneFirmato" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">**

**<saml2:AttributeValue>YgXWjSwNewE2Y5cQ.........omissis.........FrNaPnXGw7SgcE2A=</saml2:AttributeValue>**

**</saml2:Attribute>**

**<saml2:Attribute Name="IdApplicazione" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">**

**<saml2:AttributeValue>12345</saml2:AttributeValue>**

**</saml2:Attribute>**

**</saml2:AttributeStatement>**

**</saml2:Assertion>**

1. Questo allegato conterrà le specifiche di dettaglio relative alla soluzione prescelta. Al momento è presente la specifica relativa alla soluzione 1. [↑](#footnote-ref-1)
2. Da sviluppare con analisi di dettaglio (vedi stato validazione CF) [↑](#footnote-ref-4)
3. In considerazione del fatto che il sindaco è titolare delle registrazioni di competenza (cfr DPCM 194/2014, art. 3, comma 3), l’aggiornamento di ANPR è consentito a condizione che l’operazione sia innescata da un operatore del comune [↑](#footnote-ref-5)