

CONTRATTO

per l'attuazione del Progetto di “Estensione dell'utilizzo delle piattaforme nazionali di identità digitale – SPID CIE” (PNRR - Misura 1.4.4)

tra

CCIAA di Rieti - Viterbo, con sede in Viterbo, Via Fratelli Rosselli, 4, C.F. 02265670568, in persona del Segretario Generale, Francesco Monzillo (di seguito, “**Camera**” o “**Soggetto Attuatore**”);

e

InfoCamere S.C.p.A., Società Consortile di Informatica delle Camere di Commercio Italiane per Azioni, con sede legale in Roma, Via G.B. Morgagni 13, C.F. 02313821007, in persona del Direttore Generale, Dott. Paolo Ghezzi (di seguito, “**InfoCamere**” o “**Soggetto Esecutore**”);

premesso che

- A)** il 30 maggio 2022, la Presidenza del Consiglio dei ministri - Dipartimento per la trasformazione digitale (di seguito, “**Dipartimento**”), ha pubblicato un avviso per la presentazione di domande di ammissione al finanziamento a valere sul Piano Nazionale di Ripresa e Resilienza – Missione 1 – Componente 1 – Investimento 1.4, Servizi di Cittadinanza Digitale, Misura 1.4.4 relativa alla “*Estensione dell'utilizzo di piattaforme nazionali di identità digitale – SPID CIE*”, rivolto ad amministrazioni pubbliche diverse da comuni e istituzioni scolastiche (di seguito, “**Avviso**”);
- B)** la Camera ha presentato domanda di ammissione al finanziamento di cui all'Avviso e, il 27 settembre 2022, è stata ammessa quale “Soggetto Attuatore” a ricevere un contributo di importo complessivo pari ad Euro 14.000,00 (quattordicimila/00) per l'attuazione del progetto di “*Estensione dell'utilizzo di piattaforme nazionali di identità digitale – SPID CIE*” (di seguito, “**Progetto**”);
- C)** in base a quanto previsto dall'Avviso e dai relativi allegati, nella realizzazione del Progetto la Camera ha la facoltà di avvalersi di fornitori esterni e/o soggetti aggregatori, definiti anche “Soggetti Realizzatori o Esecutori”, da individuarsi nel rispetto della normativa eurounitaria e nazionale applicabile;
- D)** InfoCamere è la società consortile di informatica delle Camere di Commercio che ha il compito di approntare, organizzare e gestire nell'interesse e per conto delle Camere stesse e con criteri di economicità gestionale, un sistema informatico nazionale in grado di trattare e distribuire in tempo reale, anche a soggetti terzi, atti, documenti ed informazioni che la legge dispone siano oggetto di pubblicità legale o di pubblicità notizia o che comunque scaturiscano da registri, albi, ruoli, elenchi e repertori tenuti dalle medesime Camere;
- E)** InfoCamere, inoltre, avvalendosi del proprio sistema informatico, può provvedere in favore dei propri soci allo svolgimento di attività di gestione ed elaborazione dati, di consulenza e di

assistenza informatica, nonché di fornitura di prodotti e di servizi anche informatici e di collegamento telematico miranti ad ottimizzare l'efficienza funzionale del sistema; InfoCamere può, altresì, prestare ulteriori servizi necessari al perseguimento delle finalità istituzionali della Camere di Commercio;

- F) la Camera intende avvalersi della propria società *in house* InfoCamere per la realizzazione del Progetto ed affidarle il ruolo di Soggetto Esecutore di cui all'Avviso e ai relativi allegati;
- G) InfoCamere è in possesso dei requisiti e delle capacità necessarie per la realizzazione del Progetto quale Soggetto Esecutore, secondo le previsioni di cui all'Avviso e ai relativi allegati;
- H) con particolare riferimento all'integrazione "SPID" di cui al Progetto, InfoCamere è qualificata soggetto aggregatore SPID ed è iscritta al Registro SPID di cui all'art. 1, comma 1, lett. s) del DPCM 24 ottobre 2014. In tale contesto, InfoCamere, in qualità di soggetto aggregatore, e la Camera, in qualità di soggetto aggregato, hanno previamente sottoscritto in data **07/03/2023** (data sottoscrizione Accordo) apposito accordo ai sensi dell'art. 2, comma 1, lett. a) della "Convenzione per l'adesione dei Soggetti Aggregatori di servizi pubblici al sistema pubblico per le identità digitali" conclusa tra AGID ed InfoCamere l'8 marzo 2021 (di seguito, "**Accordo di Aggregazione SPID**"); il contenuto dell'Accordo di Aggregazione SPID si intende qui richiamato e forma parte integrante del presente contratto (di seguito, "**Contratto**");

tutto ciò premesso si conviene e stipula quanto segue:

Art. 1 - Premesse e allegati

1.1 Le premesse e il manuale tecnico allegato (All. A) formano parte integrante e sostanziale del presente Contratto.

Art. 2 - Oggetto

2.1 Con il presente Contratto la Camera affida ad InfoCamere la realizzazione del Progetto in qualità di Soggetto Esecutore come richiamato dall'Avviso e dai relativi allegati.

2.2 In particolare, le Parti concordano che ai fini della realizzazione del Progetto, InfoCamere svolga le seguenti attività in relazione al solo servizio online

Iscrizione esami mediatori

scelto dalla Camera (di seguito, "**Attività**");

- a) integrazione alla piattaforma di identità digitale SPID (Sistema Pubblico di Identità Digitale);
- b) integrazione alla piattaforma di identità digitale CIE (Carta d'Identità Elettronica);
- c) integrazione al nodo italiano eIDAS.

2.3 Resta inteso tra le Parti che la regolamentazione di ulteriori attività di assistenza e/o manutenzione del servizio online scelto dalla Camera ai fini del mantenimento dell'integrazione alle piattaforme SPID e CIE e al nodo italiano eIDAS saranno oggetto di separato accordo tra le Parti.

Art. 3 - Obblighi della Camera

3.1 La Camera si impegna al rispetto di tutti gli obblighi previsti dall'Avviso e dai relativi allegati a carico dei Soggetti Attuatori.

3.2 La Camera, ai fini della realizzazione del Progetto, deve garantire l'avvio tempestivo di tutte le fasi operative così come previsto nell'Avviso e nei relativi allegati, nonché nel manuale tecnico allegato, anche al fine di non incorrere in ritardi attuativi. In tale contesto, la Camera si impegna a collaborare con InfoCamere ai fini della corretta esecuzione delle Attività da parte di quest'ultima impegnandosi, in particolare, a:

- coordinare le Attività rispettando le tempistiche indicate nell'Avviso e nei relativi allegati;
- fornire tutte le informazioni relative al Soggetto Esecutore che siano richieste dal Dipartimento all'interno della "Piattaforma" (così definita nell'Avviso);
- trasmettere tempestivamente al Dipartimento sulla "Piattaforma" i dati di cui all'art. 11, comma 1, lett. k), dell'Avviso ("Obblighi del Soggetto Attuatore");
- occuparsi direttamente della diffusione e promozione del Progetto in conformità a quanto previsto dall'art. 12.5, comma 3, dell'Avviso ("Informazione, pubblicità e comunicazione");
- informare tempestivamente InfoCamere in merito ad eventuali comunicazioni/richieste trasmesse dal Dipartimento.

3.3 Le Parti prendono atto ed accettano che la Camera è tenuta ad inoltrare al Dipartimento la domanda di erogazione del finanziamento contenente la relazione finale, il certificato di regolare esecuzione emesso dal RUP della Camera ed ogni altro documento previsto espressamente dall'art. 13 dell'Avviso ("Modalità di erogazione e rendicontazione").

Resta inteso tra le Parti che la Camera dovrà inserire tali documenti sulla "Piattaforma" entro e non oltre 20 (venti) giorni dalla ricezione dell'attestazione di completamento delle Attività da parte di InfoCamere di cui al successivo art. 4.4, dandone contestualmente avviso ad InfoCamere.

Art. 4 - Obblighi di InfoCamere

4.1 InfoCamere si impegna ad eseguire il presente Contratto con la diligenza professionale richiesta dalla natura, dall'oggetto e dalla tipologia delle Attività, nel pieno rispetto di tutte le disposizioni indicate nell'Avviso e nei relativi allegati e in conformità alle prescrizioni di cui al manuale tecnico allegato.

4.2 InfoCamere si impegna, altresì, a fornire una soluzione tecnica di integrazione di SPID/CIE/eIDAS con il servizio online scelto dalla Camera attraverso l'utilizzo dello standard OpenID Connect in conformità a quanto previsto dall'allegato 2 dell'Avviso e in ogni caso dalla normativa *pro tempore* vigente.

4.3 InfoCamere dichiara di essere a conoscenza della normativa attualmente in vigore in materia di CIE e che è in corso di adozione una procedura da parte delle Autorità competenti che disciplinerà il ruolo dei soggetti aggregatori anche per la CIE. A tal fine, InfoCamere si impegna a porre in essere le

attività necessarie per adeguarsi alla prassi applicativa che dovesse entrare in vigore nel corso della durata del presente Contratto e a concordare con la Camera eventuali modifiche/integrazioni al presente Contratto.

4.4 Con particolare riferimento agli adempimenti previsti a carico della Camera richiamati dal precedente art. 3.3, InfoCamere si impegna a trasmettere l'attestazione di completamento delle Attività (ed ogni altro documento necessario alla redazione del certificato di regolare esecuzione da parte del RUP della Camera) entro e non oltre 10 (dieci) giorni dalla integrazione del servizio online alle piattaforme SPID e CIE e al nodo eIDAS.

Art. 5 - Durata e recesso

5.1 La durata del presente Contratto è fissata in 12 (dodici) mesi e decorre dalla data di sottoscrizione del presente Contratto. È escluso il rinnovo tacito. Resta inteso tra le Parti che tutte le Attività di cui al Progetto dovranno essere completate da InfoCamere entro il termine di 10 (dieci) mesi dalla data di sottoscrizione del presente Contratto.

5.2 Le Parti hanno la facoltà di recedere anticipatamente dal presente Contratto, dandone comunicazione all'altra Parte per iscritto con almeno 30 (trenta) giorni di preavviso. Resta inteso che la Camera si impegna a provvedere al pagamento in favore di InfoCamere del corrispettivo di cui al successivo art. 8 per le Attività già avviate da InfoCamere alla data del ricevimento della comunicazione di recesso.

Art. 6 - Corrispettivo

6.1 Per la realizzazione del Progetto, le Parti concordano che la Camera dovrà corrispondere ad InfoCamere un importo pari ad Euro 8.000,00 (ottomila/00), oltre IVA.

6.2 InfoCamere provvederà ad emettere la relativa fattura a seguito dell'emissione del certificato di regolare esecuzione da parte del RUP della Camera.

6.3 La Camera, a seguito dell'accredito del contributo da parte del Dipartimento, provvede tempestivamente all'erogazione del corrispettivo di cui al precedente art. 6.1 e, in ogni caso, entro e non oltre 15 (quindici) giorni dalla data di accredito.

6.4 Resta inteso che le modalità di fatturazione e di pagamento del corrispettivo tengono conto delle previsioni di cui all'art. 13, commi 7 e 8, dell'Avviso ("Modalità di erogazione e rendicontazione") oltre che della normativa applicabile.

6.5 Le Parti espressamente convengono che la Camera sarà tenuta al pagamento in favore di InfoCamere del corrispettivo di cui al precedente art. 6.1, anche nel caso in cui il Dipartimento dovesse procedere per qualsivoglia causa alla revoca, totale o parziale, del contributo concesso alla Camera e al recupero delle eventuali somme già erogate per cause non imputabili ad InfoCamere.

Art. 7 - Responsabilità e manleva

7.1 Fermo restando quanto previsto dal precedente art. 6.5, la Camera è responsabile nei confronti

del Dipartimento per l'adempimento di tutti gli obblighi previsti a carico del Soggetto Attuatore nell'Avviso e nei relativi allegati, pertanto la Camera si obbliga a tenere indenne e manlevare InfoCamere da qualsiasi conseguenza pregiudizievole, per fatti direttamente o indirettamente ricollegabili a inadempimenti e/o negligenze della Camera, quali a titolo esemplificativo ritardi attuativi o omesse comunicazioni ad InfoCamere.

7.2 Fermo restando quanto previsto dal precedente art. 6.5, la Camera è esclusiva responsabile della documentazione presentata al Dipartimento e per le informazioni dichiarate in sede di domanda di ammissione al finanziamento all'interno della "Piattaforma".

7.3 La Camera prende atto che InfoCamere non potrà essere considerata responsabile qualora l'inadempimento agli obblighi di cui al presente Contratto sia dovuto a caso fortuito, forza maggiore, provvedimenti di Autorità o qualsiasi altra causa non direttamente imputabile ad InfoCamere.

Art. 8 - Comunicazioni e modifiche

8.1 Qualsiasi comunicazione da effettuarsi ai fini del presente Contratto sarà inviata a mezzo PEC ai seguenti indirizzi:

- per la Camera: cciaa@pec.rivt.camcom.it
- per InfoCamere: protocollo@pec.infocamere.it

8.2 Il presente Contratto non può essere modificato o integrato se non tramite relativo accordo scritto tra le Parti.

Art. 9 - Trattamento dei dati personali

9.1 Le Parti si impegnano a trattare i dati personali oggetto del presente Contratto secondo i principi di liceità, correttezza e minimizzazione dei dati, esclusivamente per le finalità di cui al precedente articolo 2 secondo le modalità fissate nei regolamenti attuativi dell'AGID, nel rispetto di quanto previsto dalla normativa vigente in materia di protezione dei dati personali, di cui al Regolamento (UE) 2016/679 ("**GDPR**") e al Decreto Legislativo n.196/2003 e ss.mm.ii ("**Codice della privacy**").

9.2 Le Parti sono tenute, ciascuna per le attività di propria competenza, a garantire nell'esecuzione del Contratto, l'adozione delle misure tecniche ed organizzative idonee di cui all'art. 32 del GDPR, in modo tale che il trattamento dei dati personali soddisfi i requisiti previsti dal GDPR e garantisca la tutela dei diritti dell'interessato.

9.3 I dati trattati da InfoCamere riguardano i dati personali degli utenti che vengono trasmessi dagli Identity Provider, per mezzo della infrastruttura del Soggetto Aggregatore, in ordine alle richieste di autenticazione informatica per l'accesso al servizio online erogato dalla Camera, individuato all'art. 2.2 del presente Contratto.

9.4 La Camera, nel determinare le finalità e gli strumenti del trattamento dei dati personali nell'ambito del servizio online erogato in qualità di Service Provider nonché di titolare, si impegna a fornire l'informativa ai sensi di legge ai soggetti interessati da tali trattamenti.

9.5 Le Parti si danno atto che, in relazione al trattamento dei dati personali concernenti lo specifico servizio online erogato dalla Camera, la stessa tratta i dati in qualità di Titolare del trattamento, nel

rispetto di quanto previsto dall'art. 24 del GDPR e InfoCamere opera quale Responsabile del trattamento ai sensi dell'art. 28 del GDPR, in conformità all'atto di Nomina sottoscritto tra le Parti in attuazione dell'art. 8 del Regolamento Consortile di InfoCamere.

Art. 10 - Registrazione

10.1 Il presente Contratto è soggetto a registrazione solo in caso d'uso, essendo a carico della Camera il relativo assolvimento.

10.2 InfoCamere provvederà al versamento dell'imposta di bollo che sarà assolta dalla medesima in modo virtuale (Autorizzazione Agenzia Entrate UT Padova - 123110_2022_362 del 10 giugno 2022).

Art. 11 - Ampia negoziazione

11.1 Le Parti si danno reciprocamente atto che il contenuto del presente Contratto è stato negoziato e discusso in ogni sua singola pattuizione, con la conseguenza che non trovano applicazione gli articoli 1341 e 1342 c.c.

Art. 12 - Legge applicabile e foro competente

12.1 Il presente Contratto è regolato dalla legge italiana.

12.2 Qualsiasi controversia che dovesse insorgere tra InfoCamere e la Camera in relazione al presente Contratto, ed in particolare qualsiasi controversia in ordine alla validità, interpretazione, esecuzione e risoluzione dello stesso, sarà preventivamente sottoposta al tentativo di mediazione ai sensi del D.lgs. 28/2010 così come successivamente integrato e modificato, presso il servizio di mediazione della Camera Arbitrale di Roma, il cui Regolamento le Parti dichiarano di conoscere e accettare.

In caso di esito negativo del tentativo di mediazione, con riferimento a qualsiasi controversia si applicheranno gli ordinari criteri di competenza territoriale previsti dal codice di procedura civile.

Luogo **Viterbo**, data **07/03/2023**

Firmato digitalmente da: GHEZZI PAOLO
Data: 13/03/2023 15:12:43

(InfoCamere S.c.p.A.)

 Firmato digitalmente da:
MONZILLO FRANCESCO
Segretario Generale
Firmato il 07/03/2023 13:52
Seriale Certificato: 292752
Valido dal 02/04/2021 al 02/04/2024
InfoCamere Qualified Electronic Signature CA

(CCIAA di Rieti - Viterbo)

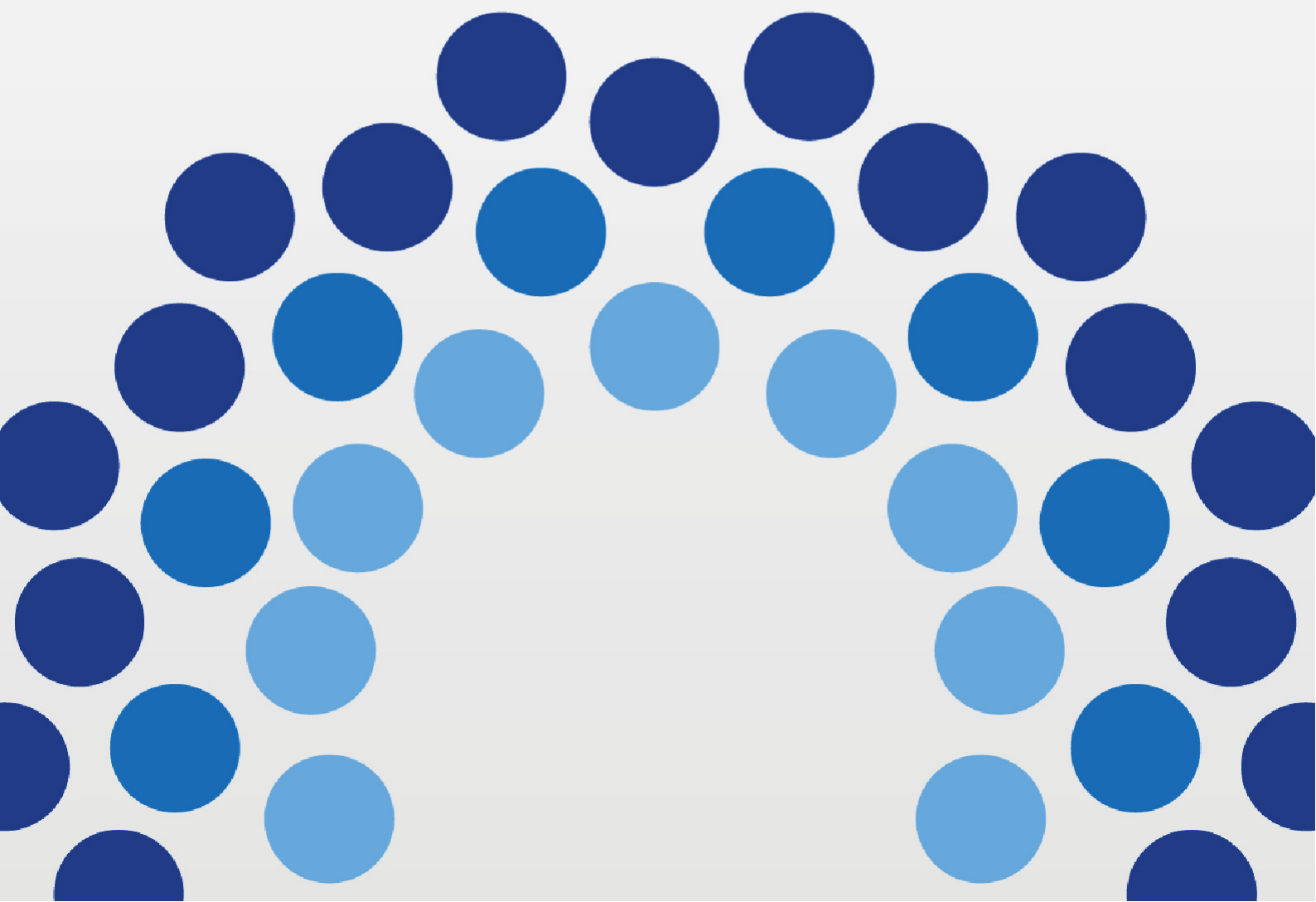
Allegati:

Allegato A – Manuale tecnico



Servizi per l'Autenticazione SPID/CIE/eIDAS

Manuale Tecnico (Allegato A)



Versione	2	Data Versione:	23 / 01 / 2023
Descrizione modifiche	Aggiornamenti ai riferimenti tecnici e alle Norme variate dalla prima formulazione		
Motivazioni	non applicabile		
Struttura emittente :	Soluzioni ITIL, Devops e Access Mgmt, Direzione Tecnologie ed Impianti, InfoCamere		

Indice

Sommario

Indice	3
1 Introduzione al documento	4
1.1 Scopo e campo di applicazione del documento	4
Livello di riservatezza	4
1.2 Termini e definizioni	5
2 Panoramica e descrizione del servizio	6
2.1 Modalità di interfacciamento ai servizi per l'autenticazione	7
2.1.1 Dati personali ottenibili con autenticazione	8
2.1.2 Registrazione degli eventi e dei dati di sessione	9
2.2 Modalità supportate dal protocollo OIDC	9
2.2.1 Pulsanti caricati dai Servizi "OIDC-AUTH"	9
2.2.2 Pulsanti gestiti dall'applicazione client (Ente Fornitore di Servizi)	17
2.3 Ruoli e Competenze	18
2.4 Logging degli eventi e log degli amministratori	19
2.5 Cifratura dei dati	19
2.6 Sincronizzazione dei clock	19
2.7 Incidenti di sicurezza	19
2.8 Comunicazione dei cambiamenti	19
2.9 Assistenza verso il Cliente	19
2.10 Localizzazione dei dati	19

1 Introduzione al documento

1.1 Scopo e campo di applicazione del documento

Il documento ha l'obiettivo di descrivere dal punto di vista tecnico le modalità di interfacciamento al servizio di autenticazione SPID, CIE ed eIDAS verso un Service Provider utilizzando i servizi di intermediazione forniti da InfoCamere.

Livello di riservatezza

	Livello	Ambito di diffusione consentito
	Pubblico	Il documento può essere diffuso all'esterno dell'azienda.
X	Uso interno	Il documento può essere diffuso solo all'interno dell'azienda. Le terze parti a cui viene comunicato, hanno l'obbligo di non diffusione.
	Riservato	Il documento non può essere diffuso all'interno dell'azienda. La sua visibilità è limitata ad un gruppo ristretto di persone. L'indicazione "Riservato" DEVE essere riportata anche nel Piè-di-pagina del documento .

Riferimenti

[1] SPID - <https://www.spid.gov.it/>

[2] OIDC - <https://openid.net/connect/>

[3] CIE - <https://www.cartaidentita.interno.gov.it/>

1.2 Termini e definizioni

Termine	Descrizione
OIDC	Protocollo OpenId Connect
SPID	Sistema Pubblico di Identità Digitale
CIE	Carta d'identità elettronica
eIDAS	IDentification, Authentication and trust Services
AGID	Agenzia per l'Italia Digitale
JWT	Json Web token, "messaggio" utilizzato per lo scambio criptato di informazioni di tipo Json tra i vari servizi
REST	Sistema di trasmissione di dati basati su protocollo HTTPS, perciò facilmente implementabili e testabili da parte di altre applicazioni.
IDP	Identity Provider: Soggetti Terzi per il rilascio di identità digitali e alla loro verifica in fase di autenticazione. Tale soggetto è "L' Istituto Poligrafico e Zecca dello Stato (IPZS)" per la CIE. Per eIDAS tutti i soggetti relativi all'identificazione utente dei paesi della Unione Europea.
Service Provider	Fornitori di Servizi Pubblici che adottano il sistema SPID per la verifica dell'identità digitale dell'utente.

2 Panoramica e descrizione del servizio

I servizi per l'autenticazione o, in gergo, "OIDC-AUTH" sono una serie di servizi messi a disposizione da InfoCamere per consentire ad applicazioni terze l'utilizzo dei seguenti sistemi di autenticazione istituzionali:

- **SPID**
- **CIE**
- **eIDAS**

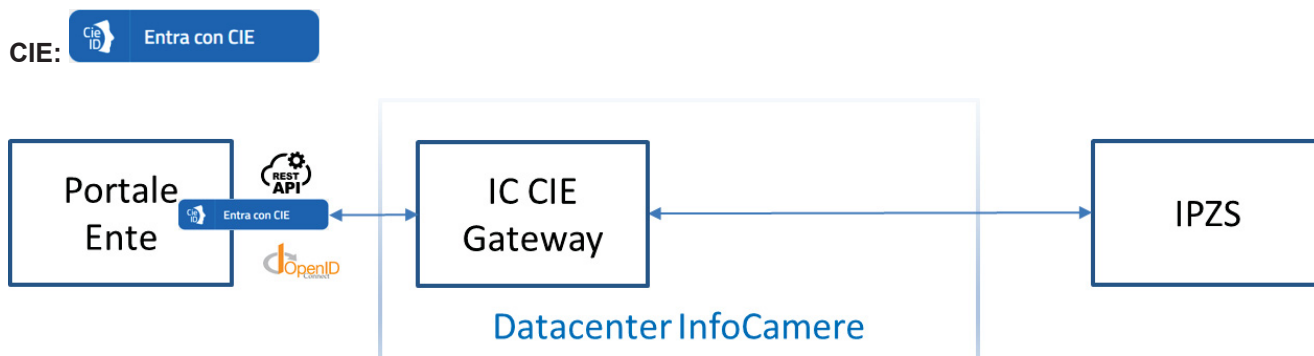
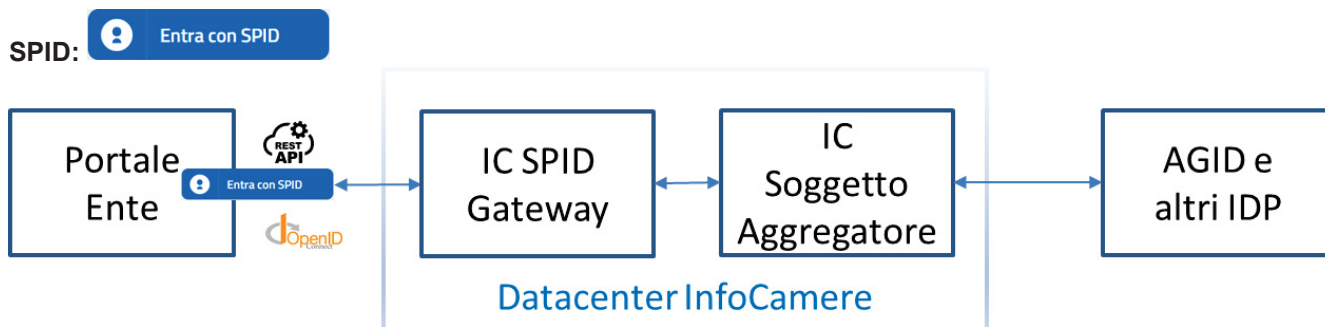
Tutti i servizi sono realizzati in architettura "REST" ed implementano il protocollo di autenticazione standard "OIDC" – **OpenId Connect**.

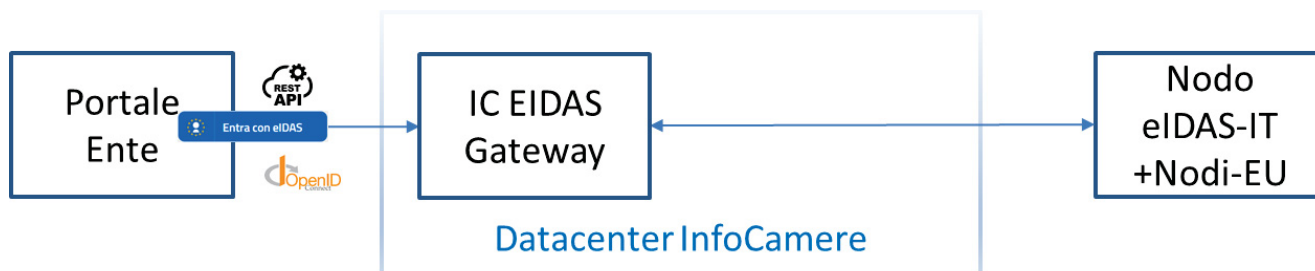
I servizi sono erogati direttamente dai Data Center InfoCamere mediante configurazioni ridondate e scalabili che garantiscono un'elevata affidabilità e continuità nell'erogazione degli stessi.

Questa implementazione offre i seguenti **vantaggi**:

- Garantisce sicurezza nello scambio di dati, criptati e firmati digitalmente con chiave asimmetrica
- Semplicità di interfacciamento, utilizzando standard ampiamente diffusi
- Interoperabilità con qualsiasi sistema "client", essendo i servizi per l'autenticazione esposti con il protocollo HTTPS, comunemente utilizzato in Internet e disponibile in ogni piattaforma tecnologica.

I servizi per l'autenticazione "OIDC-AUTH" si interpongono ai diversi servizi istituzionali di autenticazione semplificandone l'accesso e riducendo quanto più possibile le differenze tecniche necessarie ad implementare direttamente nell'applicazione le diverse modalità di autenticazione previste per ogni metodo secondo gli schemi seguenti:





Come si evince dagli schemi, il servizio per l'autenticazione “OIDS-AUTH” installato nei data center InfoCamere consente ad un Ente, fornitore di servizi on line ai propri utenti, di implementare in un unico set di servizi, diverse modalità di accesso ai servizi di autenticazione istituzionali, mediante una componente intermedia realizzata da InfoCamere. Tale componente, garantisce che eventuali variazioni nelle modalità di collegamento, secondo le regole tecniche emanate da AGID o dal Ministero dell'Interno, verso i soggetti Fornitori di servizi non si riverberino automaticamente nei portali degli Enti utilizzatori.

2.1 Modalità di interfacciamento ai servizi per l'autenticazione

I servizi per l'autenticazione SPID, CIE/eIDAS prevedono i pulsanti “Entra con SPID”, “Entra con CIE” ed “Entra con eIDAS” non modificabili da inserire nella pagina HTML del portale/servizio che vuole adottarli.

Il pulsante deve utilizzare i loghi ufficiali messi a disposizione dai referenti tecnici istituzionali (AGID - IPZS) che gestiscono queste tipologie di autenticazione.

A questo scopo il recepimento dei loghi ufficiali nel portale dell'Ente può avvenire in due modalità differenti:

- I loghi ufficiali dei pulsanti di autenticazione (SPID/CIE/eIDAS) vengono inseriti dinamicamente nella pagina web dell'Ente attraverso specifici servizi forniti in “OIDS-AUTH”.

5. Cognome	6. Indirizzo di posta elettronica
7. Luogo di nascita	8. Domicilio fisico
9. Provincia di nascita	10. Data di scadenza Identità
11. Data di nascita	12. Domicilio digitale (es. PEC)
13. Sesso	14. Partita IVA
15. Ragione o Denominazione Sociale	16. Codice Fiscale Persona Giuridica
17. Sede Legale	18. Identità professionale
19. Codice Fiscale	20. Contesto di autenticazione (es. SpidL1, 2, o 3)
21. IDP	

Nel caso di autenticazione effettuata con il metodo “**Entra con CIE**” sarà possibile, da parte dell'applicazione chiamante, disporre di un Token JWT che, una volta decodificato, conterrà le informazioni personali ritenute congrue e necessarie al chiamante, una o più tra le seguenti:

1. Nome	2. Cognome
3. Codice Fiscale	4. Data di nascita

Nel caso di autenticazione effettuata con metodo “**Entra con eIDAS**” i dati ottenuti saranno i seguenti:

1. Nome	2. Cognome
3. Data di Nascita	4. Codice univoco (a seconda del paese Europeo di autenticazione)

2.1.2 Registrazione degli eventi e dei dati di sessione

La registrazione degli eventi relativi alle richieste di accesso ai servizi (log), vengono effettuate all'interno dei servizi per l'autenticazione InfoCamere e rispettano pienamente la Normativa AGID.

Questo, tuttavia, non esonera il Fornitore di Servizi (Service Provider) dal mantenere dei propri log di accesso ai servizi offerti, ponendoli in correlazione con i servizi di intermediazione, per i fini previsti dalla normativa vigente.

2.2 Modalità supportate dal protocollo OIDC

Le modalità del protocollo OpenID Connect - OIDC implementati nei Servizi “**OIDS-AUTH**” sono i seguenti:

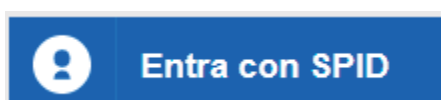
- CODE-FLOW
- IMPLICIT-FLOW

Si descrive di seguito come invocare queste modalità con sia con i pulsanti caricati dai servizi per l'autenticazione che con i pulsanti gestiti dalla pagina web dell'Ente.

2.2.1 Pulsanti caricati dai Servizi “**OIDS-AUTH**”

In questo paragrafo vedremo un esempio di come invocare i servizi per l'autenticazione al fine di “iniettare” i pulsanti e loghi ufficiale nella pagina html del servizio cliente.

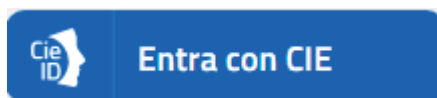
Il pulsante **SPID** sarà visualizzato in questo modo:



Cliccando sul pulsante comparirà un menu a tendina con la lista degli identity provider (IDP) accreditati SPID simile a questo:



Il pulsante **CIE** sarà visualizzato in questo modo:



Cliccando sul pulsante CIE il browser mostrerà la pagina di autenticazione:

Seleziona la modalità di autenticazione



Per autenticarti tramite uno smartphone con Android 6.0 o superiore, o iOS 13 o superiore, dotati di tecnologia NFC, munisciti della nuova Carta d'identità elettronica e assicurati di avere l'applicazione **Cie ID** installata e configurata correttamente.

Prosegui con smartphone

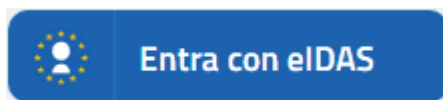


Per autenticarti con un lettore di smartcard contactless utilizzando un computer con Windows, Mac o Linux, dotati della nuova Carta d'identità elettronica. Assicurati inoltre di avere il **software Cie** installato e configurato correttamente e di appoggiare la carta sul lettore prima di cliccare sul pulsante **prosegui**.

Prosegui con computer

A questo punto si dovrà seguire la procedura guidata per autenticarsi.

Il pulsante **eIDAS** verrà visualizzato in questo modo:



Cliccando sul pulsante eIDAS il browser mostrerà la pagina di autenticazione:



Select your country

In order to continue your authentication, please select your nationality and entirely read privacy policy



Privacy Information Notice
(pursuant to art. 13 of European Regulation no. 2016/679)

Agid, Agenzia Italiana per il Digitale, with registered office in Via Lizst 21 – 00144 Rome,
Tax code 97735020584, (hereinafter "Agid"), as Data Controller, pursuant to and in

Next step...
Cancel

Anche in questo caso si dovrà seguire la procedura guidata per autenticarsi.

Il tutto viene gestito dai servizi per l'autenticazione "OIDS-AUTH".

2.2.1.1 Protocollo OIDC: CODE-FLOW

La modalità "CODE-FLOW" viene utilizzata nel caso in cui l'applicazione del Service Provider gestisca l'autenticazione lato server applicativi.

Per poter utilizzare il caricamento dinamico dei pulsanti da parte dei servizi "OIDS-AUTH" si devono inserire nella pagina HTML le seguenti direttive, tenendo presente che il parametro "[<URLdelServizioOIDS-AUTH>]" è specifico di ciascun Ente utilizzatore e verrà comunicato all'avvio dei servizi.

Un esempio di [<URLdelServizioOIDS-AUTH>] per potrebbe essere il seguente:

`https://icapis.infocamere.it/ic/pe/gate/gate/rest`

`<head>`

`...`

`<!-- N.B. INSERIRE ALL'INIZIO IL RIFERIMENTO A JQUERY utilizzando la versione più recente del .js disponibile qui https://developers.google.com/speed/libraries#jquery -->`

`<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.0/jquery.min.js"></script>`

Versione: 1

```
<link rel="stylesheet" href="https://spid.infocamere.it/spid/css/spid-sp-access-button.min.css">
```

```
<script type="text/javascript" src="[<URLdelServizioIDS-AUTH>]/spid-gw-fe/oids-
auth/SPID/authorize?client_id=<client_id>&redirect_uri=<redirect_uri>&scope=openid&resp
onse_type=code&state=<state>&nonce=<nonce>"></script>
```

```
<script type="text/javascript" src="[<URLdelServizioIDS-AUTH>]/spid-gw-fe/oids-
auth/CIE/authorize?client_id=<client_id>&redirect_uri=<redirect_uri>&scope=openid&resp
onse_type=code&state=<state>&nonce=<nonce>"></script>
```

```
<script type="text/javascript" src="[<URLdelServizioIDS-AUTH>]/spid-gw-fe/oids-
auth/EIDAS/authorize?client_id=<client_id>&redirect_uri=<redirect_uri>&scope=openid&re
sp onse_type=code&state=<state>&nonce=<nonce>"></script>
```

```
<script type="text/javascript">
    $( document ).ready(function() {
        pushButtonSpid();
    });
</script>
```

```
<script type="text/javascript">
    $( document ).ready(function() {
        pushButtonCie();
    });
</script>
```

```
<script type="text/javascript">
    $( document ).ready(function() {
        pushButtonEidas();
    });
</script>
```

```
...
</head>
```

```
<body>
...
<div id="buttonSpid"></div>
<div id="buttonCie"></div>
<div id="buttonEidas"></div>
```

```
...
</body>
```

```
<link rel="stylesheet" href="https://spid.infocamere.it/spid/css/spid-sp-access-button.min.css">
```

→ Riferimento fogli di stile per i bottoni

<client_id>

→ Nome identificativo del servizio dell'Ente che utilizza i servizi per l'autenticazione.

<redirect_uri>

→ Url a cui puntare dopo l'autenticazione (a cui inviare il token JWT con i dati di autenticazione).

<state>

→ Alfanumerico random di 12 caratteri. Questo dato viene re-inviato all'applicazione cliente dai servizi di autenticazione. Può essere usato dal client come dato per verificare l'attendibilità del server.

<nonce>

→ Alfanumerico random di 12 caratteri. L'utilità è la stessa dello state.

```
<script type="text/javascript">
    $( document ).ready(function() {
        pushButtonSpid();
```

```
});
```

```
<script type="text/javascript">
    $( document ).ready(function() {
        pushButtonCie();
    });
```

```
</script>
```

```
<script type="text/javascript">
    $( document ).ready(function() {
        pushButtonEidas();
    });
```

```
</script>
```

- Si tratta di 3 funzioni JQUERY che servono ad “iniettare” il codice HTML dei pulsanti in elementi di tipo `<div></div>` all'interno della pagina web.

```
<div id="buttonSpid"></div>
```

```
<div id="buttonCie"></div>
```

```
<div id="buttonEidas"></div>
```

- Questi elementi “div” conterranno i SPID/CIE/eIDAS.

Cliccando sul pulsante si procederà all'autenticazione.

Dopo la fase di autenticazione, i servizi “OIDS-AUTH” invieranno in query string un parametro di tipo “code”, oltre allo “state”.

Questo parametro dovrà essere utilizzato dall'applicazione chiamante per effettuare una ulteriore chiamata di questo tipo:

```
POST /oids-auth/token HTTP/1.1
Host: [<URLdelServizioOIDS-AUTH>]/spid-gw-fe/
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

grant_type=authorization_code
&code=Splxl0BeZQQYbYS6WxSbIA
```

passando come parametri

code: *il code inviato nella chiamata precedente*

grant_type=authorization_code

Bisogna anche scrivere nell'header http la seguente coppia chiave-valore:

Key: *Authorization*

Value: *<stringa Base64>*

Il valore non è altro che la rappresentazione base 64 di una stringa crittografata che contiene al suo interno il *client_id* ed una password. La stringa verrà fornita da InfoCamere durante le fasi preliminari di registrazione del cliente.

N.B. Tra "Basic" e la stringa Base64 deve esserci uno spazio.

Questa chiamata risponderà con un "200 Found" e scriverà nel body della response le informazioni di autenticazione richieste. A questo punto è possibile estrarre dal body le informazioni dell'utente autenticato sotto forma di token JWT.

2.2.1.2 Protocollo OIDC: IMPLICIT-FLOW

Il protocollo “IMPLICIT-FLOW” viene utilizzato nel caso in cui l'autenticazione venga gestita lato client, ovvero su una pagina HTML mediante linguaggio di scripting (javascript - jquery ecc...).

Le modifiche da effettuare sulla pagina HTML per visualizzare i pulsanti di autenticazione sono identiche al caso “CODE-FLOW”, l'unica differenza è nella direttiva:

```
... response_type=code...
```

Che in questo caso può essere di tre tipi (secondo gli standards OI DC)

```
... response_type=id_token token...
... response_type=id_token ...
... response_type=token ...
```

Specificando il parametro “token” verrà restituito, nel JWT, l”access_token”, mentre con il parametro “id token” verrà restituito l”id token”.

In questo caso il JWT verrà restituito alla url chiamante direttamente sotto forma di “fragment”, quindi non c’è la necessità di effettuare la seconda chiamata come nel caso “CODE-FLOW”.

Di seguito un esempio di risposta di tipo “id token token”:

[illegible]

L'access_token e l'id_token sono codificati con firma digitale. La chiave pubblica per la decodifica verrà fornita da InfoCamere in fase di avvio del servizio.

Il campo “expires in” può essere configurato a seconda delle esigenze dell'applicazione client.

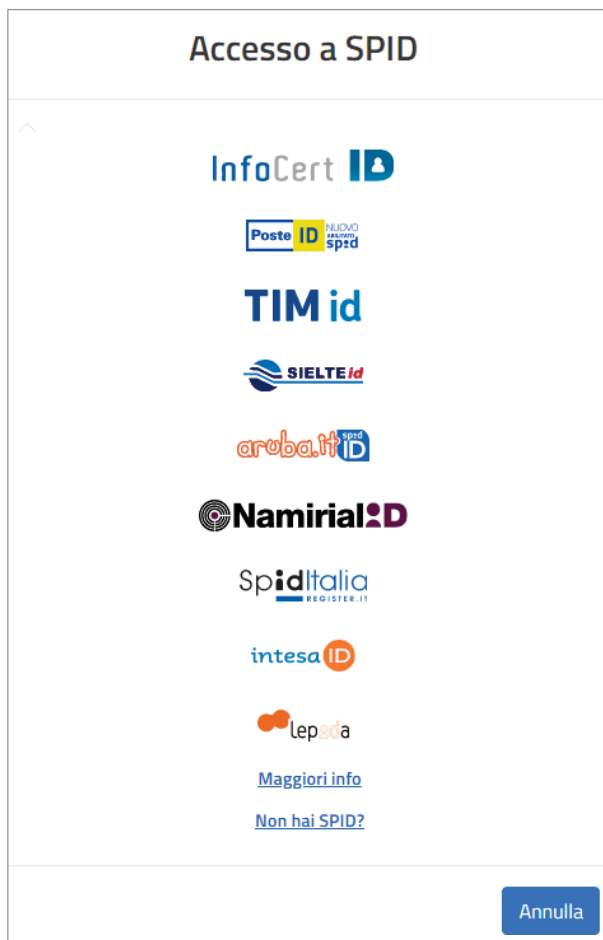
2.2.2 Pulsanti gestiti dall'applicazione client (Ente Fornitore di Servizi)

In questo caso verranno invocati gli end points dei servizi di autenticazione e non quelli per iniettare i pulsanti e i relativi loghi nella pagina.

I pulsanti sono gestiti dall'applicazione dell'Ente utilizzatore che dovrà provvedere ad utilizzare esclusivamente i loghi ufficiali come previsto da AGID-IPZS-eIDAS.

Il logo può essere scaricato dal sito ufficiale degli enti preposti (AGID).

Nel caso di SPID la lista degli IDP, poiché non “iniettata” dai servizi per l'autenticazione, sarà visualizzata dopo aver cliccato sul pulsante “entra con SPID” sotto forma di finestra modale simile alla seguente:



2.2.2.1 Applicazione client con CODE-FLOW

Nel caso in cui l'URL da contattare comunicato all'Ente sia, ad esempio,

<https://icapis.infocamere.it/ic/pe/gate/ga00/rest/>

per questa tipologia di chiamata servirà effettuare due chiamate come di seguito dettagliato:

```
HTTP/1.1 302 Found
Location: https://icapis.infocamere.it/ic/pe/gate/ga00/rest/spid-gw-fe/oids-
auth/services/<spid|cie|eidas>/authorize?
    response_type=code
    &scope=openid
    &client_id=<CLIENT_ID>
```

```
&state=<STATE>  
&nonce=<NONCE>  
&redirect_uri=<REDIRECT_URI>
```

Questa prima chiamata mostrerà a video le schermate SPID/CIE/eIDAS di autenticazione fornite dagli Identity Providers. A valle dell'autenticazione i servizi restituiranno, alla url chiamante (redirect_uri), il parametro "code" oltre allo "state".

Il parametro "code" viene utilizzato per effettuare la seconda chiamata:

```
POST /oids-auth/token HTTP/1.1  
Host: https://icapis.infocamere.it/ic/pe/gate/ga00/rest/spid-gw-fe/  
Content-Type: application/x-www-form-urlencoded  
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW  
  
grant_type=authorization_code  
&code=Splxl0BeZQQYbYS6WxSbIA
```

Questa chiamata è del tutto analoga a quella descritta nel paragrafo 2.2.1.1.

2.2.2.2 Applicazione client con IMPLICIT-FLOW

In questo caso c'è un'unica chiamata da effettuare:

```
HTTP/1.1 302 Found  
Location: https://icapis.infocamere.it/ic/pe/gate/ga00/rest/spid-gw-fe/oids-auth/services/<spid|cie|eidas>/authorize?  
response_type=id_token token  
&scope=openid  
&client_id=<CLIENT_ID>  
&state=<STATE>  
&nonce=<NONCE>  
&redirect_uri=<REDIRECT_URI>
```

Che restituirà sotto forma di fragment l'"access_token" e l'"id_token" in modo analogo a quanto descritto nel paragrafo 2.2.1.2

2.3 Ruoli e Competenze

InfoCamere è competente per il funzionamento, l'aggiornamento e la manutenzione dell'infrastruttura mediante la quale è erogato il servizio per l'autenticazione.

InfoCamere può fornire assistenza e risolvere problemi esclusivamente per quanto di propria competenza.

InfoCamere non si sostituisce agli IDP nell'autenticazione degli utenti e non risponde delle malfunzioni di questi o di fornitura di dati dell'utente non conformi o non idonei.

Il Cliente è competente per il funzionamento, l'aggiornamento e la manutenzione del sito o del servizio autenticato, nonché per la scelta dei profili e dei privilegi da attribuire a ciascun soggetto autenticato/utente (ad esempio sulla base del codice fiscale e/o altri attributi forniti dall'Identity Provider). È competenza del Cliente, in tal senso, operare l'eventuale discriminazione tra le utenze (ad esempio ad uso interno, di tipo *back office*, oppure esterno e, fra queste, individuare quelle privilegiate).

Il Cliente risponde dell'uso delle Identità Digitali presso il proprio Sito/Servizio e della custodia dei relativi dati ricevuti.

Il Cliente è responsabile della corretta gestione del codice nei casi in cui, secondo il presente manuale, è richiesto il suo intervento. In tal senso, il Cliente dovrà attenersi alle istruzioni ivi indicate, avendo cura di non alterare il codice stesso e/o le configurazioni richieste da InfoCamere ai fini del corretto funzionamento del servizio salvi i casi in cui, in ragione di specifici accordi, InfoCamere non abbia in gestione anche i servizi

autenticati e il Cliente, conseguentemente, non abbia la possibilità materiale di svolgere tali attività.

2.4 Logging degli eventi e log degli amministratori

I log amministrativi sui sistemi gestiti da InfoCamere sono raccolti e monitorati da InfoCamere, ai sensi della normativa vigente.

I log relativi alle applicazioni e servizi dell'Ente sono di esclusiva competenza di quest'ultimo, salvi i casi in cui, in ragione di specifici accordi, InfoCamere non abbia in gestione anche i servizi autenticati.

2.5 Cifratura dei dati

Ogni scambio di dati con il cliente avviene, come detto, utilizzando chiamate di tipo “REST” utilizzando il protocollo sicuro **https://** nella versione più recente, il **TLS v.1.2**. InfoCamere si riserva la facoltà di adottare versioni più aggiornate di tale protocollo, qualora disponibili, concordando con il Cliente tempi e modi di tale adeguamento.

2.6 Sincronizzazione dei clock

Il clock dei sistemi è fornito da InfoCamere mediante sincronizzazione con protocollo NTP ad un pool “time server” aziendali in alta affidabilità. A loro volta i “time server” aziendali sono tenuti aggiornati via GPS come fonte primaria e con l'Istituto Nazionale di Ricerca Metrologica di Torino come fonte secondaria.

2.7 Incidenti di sicurezza

InfoCamere gestisce ogni incidente seguendo il proprio processo di *incident management* e fornirà, su richiesta del cliente, report sugli incidenti, sulle soluzioni adottate e sullo SLA erogato.

Per conoscere lo stato o l'esito di un incidente di sicurezza, il Cliente può contattare il *service desk* di InfoCamere o fruire di canali di contatto specifici che verranno comunicati puntualmente prima dell'avvio del servizio.

2.8 Comunicazione dei cambiamenti

Le modifiche ai sistemi e al software che hanno o possono avere effetti sul servizio sono predisposte con modalità tali da ridurre al minimo i possibili disservizi. A tal fine, le modifiche vengono comunicate al Cliente con un preavviso di almeno 10 giorni, tramite i dati di contatto specifici, puntualmente comunicati prima dell'avvio del servizio.

Eventuali esigenze di cambiamento per cause di particolare urgenza/sicurezza saranno comunicati tempestivamente al Cliente e svolti nel più breve tempo possibile, compatibilmente con le esigenze del Cliente, concordate di volta in volta.

In caso di variazione dei dati di contatto di una delle Parti nel corso dell'erogazione del servizio, sarà onere di Questa comunicarli all'Altra appena possibile, in modo da disporre sempre dei dati di contatto più recenti.

2.9 Assistenza verso il Cliente

In caso di richieste di assistenza su aspetti tecnici del servizio o per richiesta di informazioni, il Cliente può contattare InfoCamere attraverso il servizio di *service desk* o tramite i canali di contatto specifici puntualmente comunicati prima dell'avvio del servizio.

2.10 Localizzazione dei dati

I server mediante i quali viene erogato il servizio si trovano in Italia, presso i Datacenter InfoCamere di Padova e Milano.