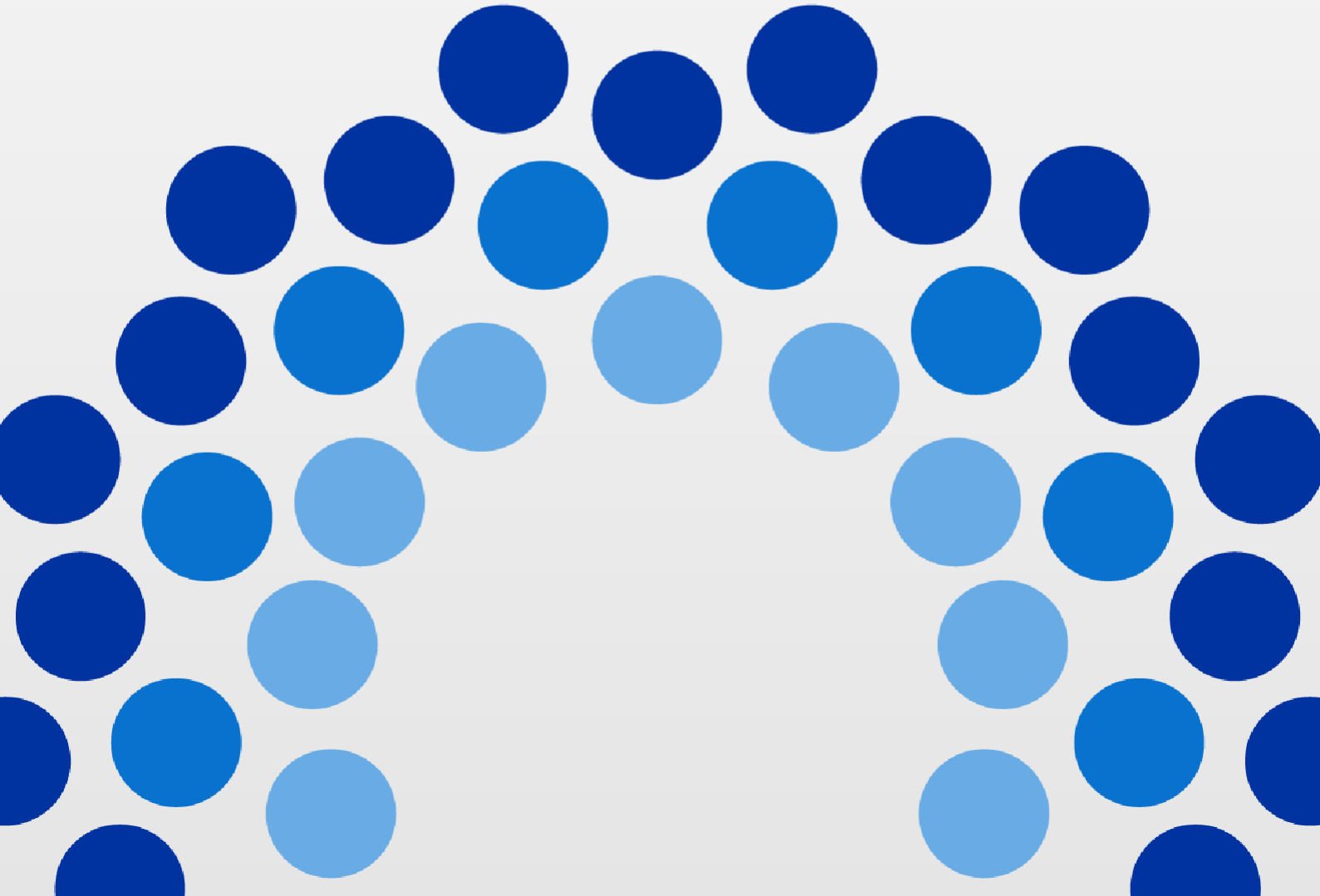
InfoCamere

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

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, "OIDS-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**

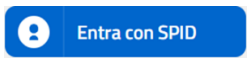
Tutti i servizi sono realizzati in architettura "REST" ed implementano il protocollo di autenticazione standard "OIDC" – **OpenId Connect.**

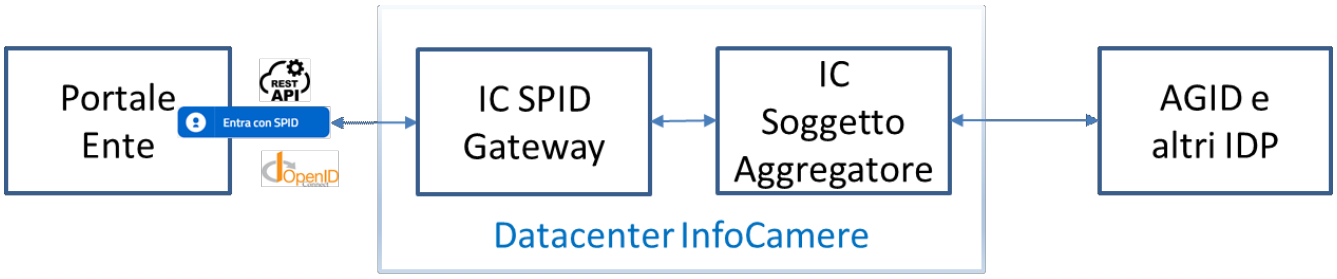
I servizi sono erogati direttamente dai Data Center InfoCamere mediante configurazioni ridondate e scalabili che garantiscono un'elevata affidabilità e continuità nell'erogazione degli stessi.

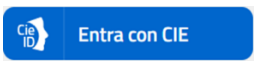
Questa implementazione offre i seguenti **vantaggi**:

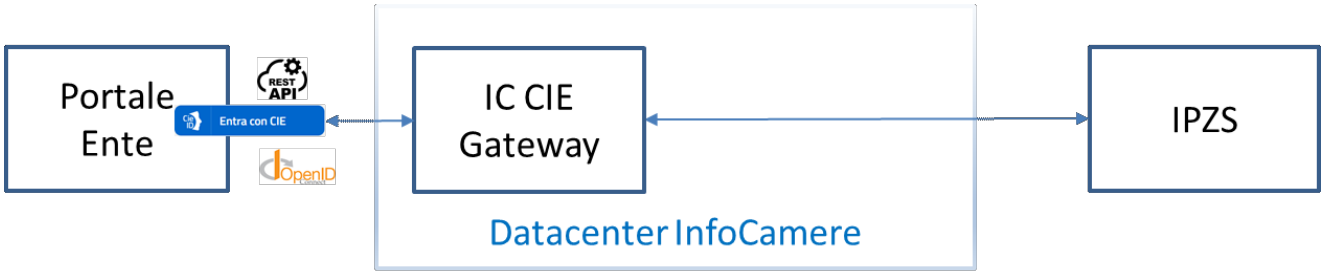
- Garantisce sicurezza nello scambio di dati, criptati e firmati digitalmente con chiave asimmetrica
- Semplicità di interfacciamento, utilizzando standard ampiamente diffusi
- Interoperabilità con qualsiasi sistema "client", essendo i servizi per l'autenticazione esposti con il protocollo HTTPS, comunemente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

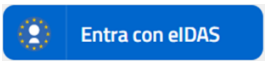
I servizi per l'autenticazione "OIDS-AUTH" si interpongono ai diversi servizi istituzionali di autenticazione semplificandone l'accesso e riducendo quanto più possibile le differenze tecniche necessarie ad implementare direttamente nell'applicazione le diverse modalità di autenticazione previste per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

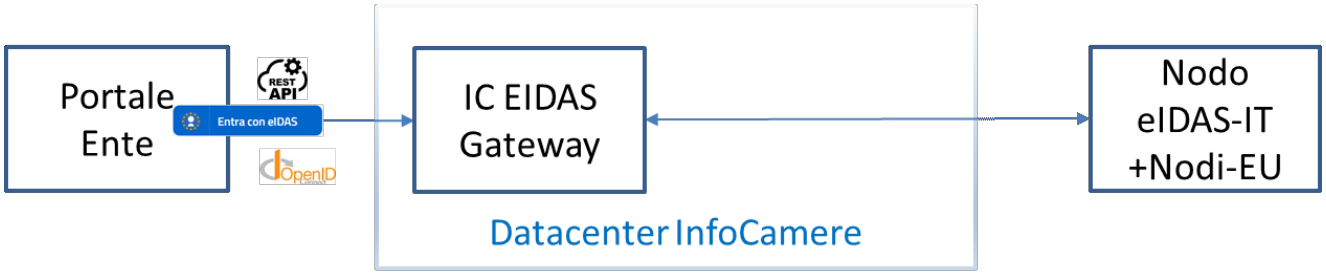
SPID: 



CIE: 



eIDAS: 



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".

- I loghi ufficiali dei pulsanti di autenticazione vengono recuperati autonomamente dall'Ente ed inseriti staticamente nella pagina di login nel portale dell'Ente stesso.

La prima modalità prevede l'inserimento dinamico dei pulsanti e dei loghi ufficiali da parte del servizio per l'autenticazione "OIDS-AUTH" nella pagina web dell'Ente. Anche le funzioni associate all'attivazione di ciascun pulsante saranno gestiti dai servizi per l'autenticazione. Questa prima modalità viene indicata come "da preferire" in quanto garantisce l'adeguamento automatico dei loghi ufficiali ed ogni loro variazione senza la necessità di adeguamenti da parte dell'Ente utilizzatore.

La seconda modalità, non prevede l'utilizzo dei servizi "OIDS-AUTH" per il caricamento dei pulsanti, e richiede che sia l'Ente utilizzatore a verificare periodicamente l'utilizzo dei loghi ufficiali aggiornati e l'invocazione delle funzioni associate all'attivazione di ciascun pulsante.
Questa seconda modalità viene messa a disposizione qualora l'Ente utilizzatore utilizzi sistemi "chiusi" (ad es. portali) che non possono essere modificati nella parte HTML e che prevedono la possibilità di configurare il sistema per l'utilizzo di un provider esterno mediante le funzionalità del protocollo standard OIDC - "Open-id Connect".

Una volta completata l'autenticazione SPID, CIE o EIDAS da parte dell'utente, i dati personali vengono restituiti alla pagina indicata dal servizio chiamante sotto forma di un token JWT.

Il token può essere inviato sotto forma di fragment (protocollo IMPLICIT FLOW)
oppure nel "body" della risposta (protocollo CODE-FLOW).

Esempio di token JWT (criptato) come fragment:
<REDIRECT_URI>#access_token=eyJraWQiOiJJZFBJbmZvQ2FtZXJlMjAxODA4LnB1YmxpY19rZXkuZGVy
IiwiYWxnIjoiUlM1MTIifQ.eyJzdWIiOiJUSU5JVC1HUlJHTEc3M0wwNkE2NjJSIiwiZmFtaWx5TmFtZSI6Ikdhcn
JhcGEiLCJpblJlc3BvbnNlVG8iOiJfODkwMWRkYTVhNWUzNGU0ODQyOTk0YzBmODZhYjE3ZmQiLCJpc3
MiOiJodHRwczpcL1wvc3BzHN2LmludHJhLmluZm9jYW1lcmUuaXRcL29pZGMiLCJuYW1lIjoiR2lhbmx1aW
dpIiwic3BpZENvZGUiOiJBSURQMTIzNDUwMDQwNiIsImRhdGVPZkJpcnRoIjoiMTk3My0wNy0wNiIsImV4c
CI6MTYyNTA1MDQwNiwiZmlzY2FsTnVtYmVyIjoiVElOSVQtR1JSR0xHNzNMMDZBNjYyUiJ9.OYGIRpkd15
Pfs1fkZvK6wWyXlEhdEIF57ddv8cn3PDzBvlayhKsea6b2I3-
1uqfv2gtS3G5f3d1irSFXcJ8AyZ9J9V7acj33H22Ad4sQjr3n9AJ1erm85ngEvZ_y6AO5SwnA99WLxY_FjNdU4

RL7cPbnsY1w_YCsXl1V0mHkDfGokRBKD-c6dOb65rNF5tDvgjQbtRjIyN5-05cev2KXZ5uSIDcq3CaK87n-
17SoE1VGU-
bw39McBxLFfWPTtTAqGikDCg9NXK0mp4dWihNHl8UWLg_pOLoThKJKl6yqvkODCbN5bAzUU78SJWh7K_
3P9qg112iLHg5O_K2bWRu2ug&id_token=eyJraWQiOiJJZFBJbmZvQ2FtZXJlMjAxODA4LnB1YmxpY19rZX
kuZGVyIiwiYWxnIjoiUlM1MTIifQ.eyJhdF9oYXNoIjoiNzdIbVBxeEZZMkhsZ0E1cDY2RjFYRTNOc1BLWk9ZZjI
2b25YQmRobFJsOCIsInN1YiI6IlRJTklULUdSUkdMRzczTDA2QTY2MlliLCJpc3MiOiJodHRwczpcL1wvc3Bp
ZHN2LmludHJhLmluZm9jYW1lcmUuaXRcL29pZGMiLCJzcGlkQ29kZSI6IkFJRFAxMjM0NTAwNDA2IiwiZGF
0ZU9mQmlydGgiOiIxOTczLTA3LTA2IiwiYXVkIjoiaWMudGVzdCIsImZhbWlseU5hbWUiOiJHYXJyYXBhIiwia
W5SZXNwb25zZVRvIjoiXzg5MDFkZGE1YTVlMzRlNDg0Mjk5NGMwZjg2YWIxN2ZkIiwibmFtZSI6IkdpYW5s
dWlnaSIsImV4cCI6MTYyNTA1MDQwNiwiaWF0IjoxNjI1MDQ2ODA2LCJmaXNjYWxOdW1iZXIiOiJUSU5JVC
1HUlJHTEc3M0wwNkE2NjJSIn0.QpncH5KNrByDdUrfYNr45r5nWnafWOjmi9TTdby4_ofh4yJaZmwzQshv4m

OZwAliaNk82mW9AkC6AhkQDiXF7Tb525cz-QnbghaFBrX6tdgbVS-
Tn6t9_rlKGmZMTWfDZ7A2u_PGL3qkmNaLn9oYhjKaFppDkBrxW04jMzFlAD3sqxR_HPr31UP-
0D3002BiO_-eLzNUmBeukq6tvnGk9sywleZ6VFN_nwo6XxXkbf5-
T3vBUfoTjSLeEkwMZ4nMSngahImBMzKoJmD0gT9XCOQa6lT21lw_krbX7cxcLJ6tMGuFRHJcWK2PF_zEl_
_IfR2FamDWS7aOqtdE7mgpCA&expires_in=3600&token_type=Bearer

2.1.1 Dati personali ottenibili con autenticazione

Nel caso di autenticazione effettuata con il metodo "**Entra con SPID**" 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. Tipologia Identità (es. ID p.f., ID p.g.)	2. Estremi Documento Identità
3. Nome	4. Numero telefono mobile

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:

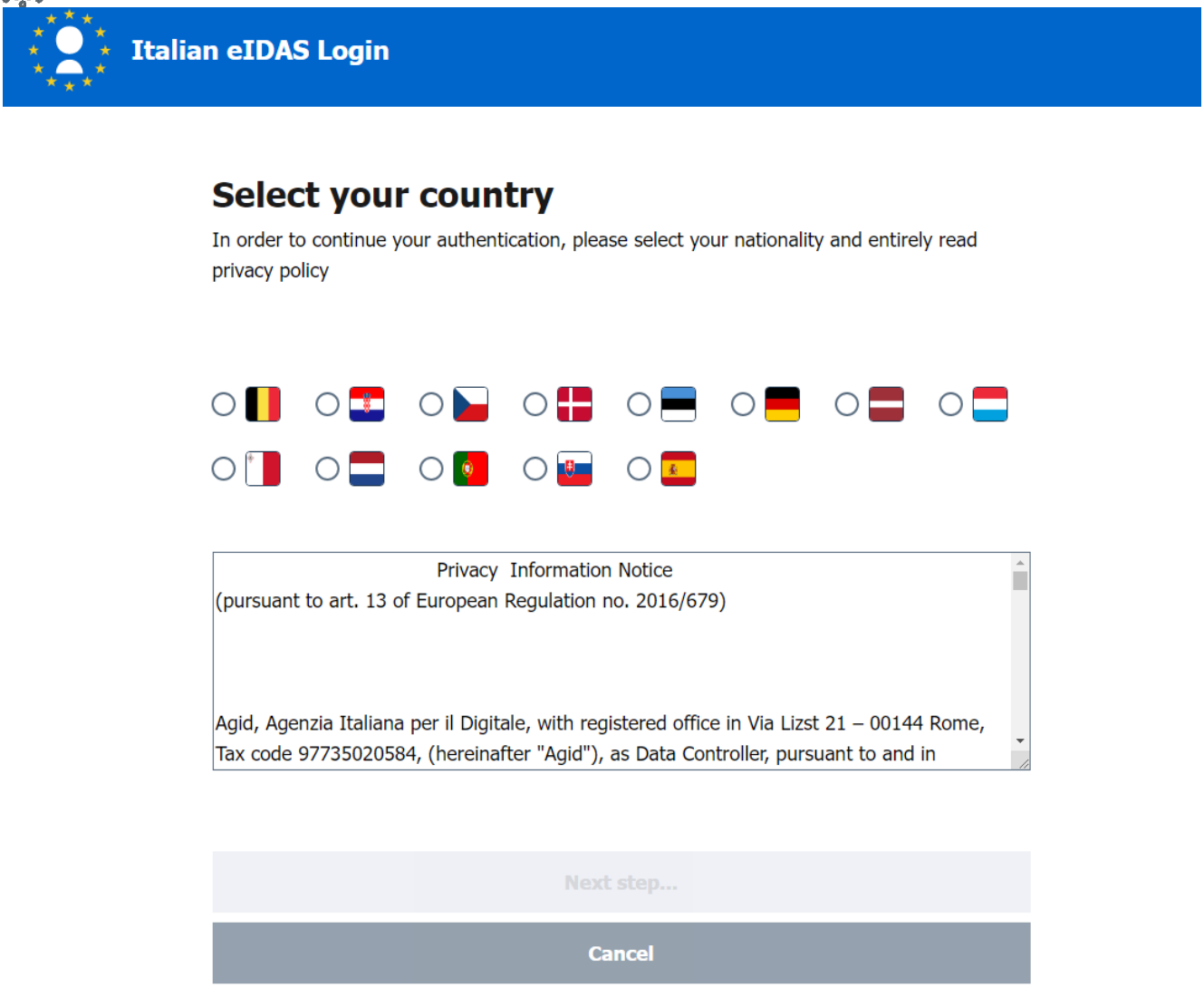
Il pulsante **CIE** sarà visualizzato in questo modo:

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

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:



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>
```

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

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

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

<script type="text/javascript" src="[<URLdelServizioOIDS-AUTH>]/spid-gw-fe/oids-auth/EIDAS/authorize?client_id=***<client_id>***&redirect_uri=***<redirect_uri>***&scope=openid&resp 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 all'interno della pagina web.

*** ***
*** ***
*** ***

➔ 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=SplxlOBeZQQYbYS6WxSbIA
```

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.

Un esempio di token JWT restituito è il seguente:

{"***access_token***":"eyJraWQiOiJJZFBJbmZvQ2FtZXJlMjAxODA4LnB1YmxpY19rZXkuZGVyIiwiYWxnIjoiUlM
1MTIifQ.eyJzdWIiOiJUSU5JVC1HUlJHTEc3M0wwNkE2NjJSIiwiZmFtaWx5TmFtZSI6IkdhcnJhcGEiLCJpbIJI
c3BvbnNlVG8iOiJfYTEyZTBkYWRmNWMwNjJhMjY0YjM2OWM4MTIwMWIwOWIiLCJpc3MiOiJodHRwczpc
L1wvc3BpZGNsLmluZm9jYW1lcmUuaXRcL29pZGMiLCJuYW1lIjoiR2lhbmx1aWdpIiwic3BpZENvZGUiOiJB
SURQMTIzNDUwMDQwNiIsImRhdGVPZkJpcnRoIjoiMTk3My0wNy0wNiIsImV4cCI6MTYyNDUyMzM2OSwi
ZmlzY2FsTnVtYmVyIjoiVElOSVQtR1JSR0xHNzNMMDZBNjYyUiJ9.gOvvWZJyQ96ai6o1B-
xepOLi7giGNT0xaCz54ANcrHYRUvJJrPlfidT4uSM63wsP92prpPVMIj5mGeC1mC0pdcmSxMDCHR9MDRjC
8uROuKXIlJY81hbatKYmhDLZT3ZVs0wUJomzi-
AL7ntcxf4gi6dJViQI3IX5K7kQx3KEbB7fWtlrpvlU7KuKHP3GOw-bNMGCkzyxeGvYZiw5g8OfrzKNO8l_BJ-
mjxMqg5mWvnjgsjQAe5_MvpZPvQCIOkuPbAdcn5Ci-TRd2VN5gTZAarTFensrPN-V-YIQtyXR-
U3XgNDkIXKU3qXcQzVcMsGRSX3H5zY_ZwMYWyOyUhe68Q","***id_token***":"eyJraWQiOiJJZFBJbmZvQ2Ft
ZXJlMjAxODA4LnB1YmxpY19rZXkuZGVyIiwiYWxnIjoiUlM1MTIifQ.eyJhdF9oYXNoIjoiX3Q4QXBrd1k5RzQy
aDhsSGZwbWN1ZHl3amFRNWNKOUNoZ29SbHREay1LMCIsInN1Yil6IlRJTklULUdSUkdMRzczTDA2QTY
2MlIiLCJpc3MiOiJodHRwczpcL1wvc3BpZGNsLmluZm9jYW1lcmUuaXRcL29pZGMiLCJzcGlkQ29kZSI6IkFJ
RFAxMjM0NTAwNDA2IiwiZGF0ZU9mQmlydGgiOiIxOTczLTA3LTA2IiwidHlwIjoiQmVhcmVyIiwibm9uY2UiOiI
2Nzg5MCIsImF1ZCI6ImljLnRlc3QiLCJmYW1pbHlOYW1lIjoiR2FycmFwYSIsImluUmVzcG9uc2VUbyI6Il9hMT
JlMGRhZGY1YzA2MmEyNjRiMzY5YzgxMjAxYjA5YiIsIm5hbWUiOiJHaWFubHVpZ2kiLCJleHAiOjE2MjQ1Mj
MzNjksImlhdCI6MTYyNDUxOTc2OSwiZmlzY2FsTnVtYmVyIjoiVElOSVQtR1JSR0xHNzNMMDZBNjYyUiJ9.
SOmf9-
DPYL46s8KDA_16z_iZGgIzCuOEGs_EiycSnI2fsUa1OkTKb4FlkDQ6mIW_Zep2ulnmT3KTqLxmjLs5xL5KaB
CmKdtnaV2S0VjC7T8HrH2WWz-nEh21KaFon-LqA1z3k1f6HIUOV9F-
xtWfp0k9BIekVEGaJcyY9Opesdo1IvlLqwmFUHhsB0Qk8Kys1YPceNnvwuZW0JmHTIlNKROw1defw4CGEtr
oqfrlZ8uVtVFdV7Ybockvk4rtmfoT8Wt5F8XTXf5L57s9Xjh4hnv077yV5VI5kboPWJnu_NNIsfLWKkPv5gP09O
M9HU7TlUJvHmtYN-SptjjN3pg0iQ","***token_type***":"Bearer","***expires_in***":3600}

I JWT "access_token" e "id_token" sono codificati e firmati digitalmente.

La chiave pubblica per verificare la firma verrà fornita da InfoCamere.

Il campo "expires_in" è espresso in secondi e può essere configurato a seconda delle esigenze dell'applicazione client.

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 OIDC)

… 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":

https://<redirect_uri_cliente>#***access_token***=eyJraWQiOiJJZFBJbmZvQ2FtZXJlMjAxODA4LnB1YmxpY19rZXkuZGVyIiwiYWxnIjoiUlM1MTIifQ.eyJzdWIiOiJUSU5JVC1HUlJHTEc3M0wwNkE2NjJSIiwiZmFtaWx5TmFtZSI6IkdhcnJhcGEiLCJpblJlc3BvbnNlVG8iOiJfYTEyZTBkYWRmNWMwNjJhMjY0YjM2OWM4MTIwMWIwOWIiLCJpc3MiOiJodHRwczpcL1wvc3BpZGNsLmluZm9jYW1lcmUuaXRcL29pZGMiLCJuYW1lIjoiR2lhbmx1aWdpIiwic3BpZENvZGUiOiJBSURQMTIzNDUwMDQwNiIsImRhdGVPZkJpcnRoIjoiMTk3My0wNy0wNiIsImV4cCI6MTYyNDUyNDA4OCwiZmlzY2FsTnVtYmVyIjoiVElOSVQtR1JSR0xHNzNMMDZBNjYyUiJ9.nexM_xmewJ-4H_tGt8I-XUhwl2CJZuqaUAIJgNH7yPlclcXOrU6_BgvBufyF5lY0XVpZ8fiqf0zPiXB1BCYR66kKFlig2buosV-IKpI9fdio364Tcr7Q4ZaoM2r7BbZTzNBU8O9G7Al9DSrJlXD6uOTBqQ2tz2gIfPUAXg7flRhQ837g1luws7uHm0sfRYjL5rA7mw5_biY2fdjSebuk4Ljg46gMUiEzxDv7cdngr43cjlraDhqdNFvcIf_Ud1r6bFlnwOB0feFNYp3gK_pL7QWId2qW2-YdnX-OxX195pvs-Su1M-DPYNtx-re17fwEtWGbtMSCAC2uhk60YC251g&***id_token***=eyJraWQiOiJJZFBJbmZvQ2FtZXJlMjAxODA4LnB1YmxpY19rZXkuZGVyIiwiYWxnIjoiUlM1MTIifQ.eyJhdF9oYXNoIjoiU2V3U3NjbVV3ZjhuT1EteXhWdjl4dTUwMzhYeEl3elJ5TFNucWM5aGY5VSIsInN1YiI6IlRJTkIULUdSUkdMRzczTDA2QTY2MlliLCJpc3MiOiJodHRwczpcL1wvc3BpZGNsLmluZm9jYW1lcmUuaXRcL29pZGMiLCJzcGlkQ29kZSI6IkFJRFAxMjM0NTAwNDA2IiwiZGF0ZU9mQmlydGgiOiIxOTczLTA3LTA2IiwiYXVkIjoiaWMudGVzdCIsImZhbWlseU5hbWUiOiJHYXJyYXBhIiwiaW5SZXNwb25zZVRvIjoiX2ExMmUwZGFkZjVjMDYyYTI2NGIzNjljODEyMDFiMDliIiwibmFtZSI6IkdpYW5sdWlnaSIsImV4cCI6MTYyNDUyNDA4OCwiaWF0IjoxNjI0NTIwNDg4LCJmaXNjYWxOdW1iZXIiOiJUSU5JVC1HUlJHTEc3M0wwNkE2NjJSIn0.fd2t7h4POzsdudUXqjnH6r9HuSDj_Mu9novvGhh7QPljAsnpbl56xEAVkN74vNPtL9AktHq6rLBz3qKMpKXKM8zHV8ESydEt3Kw4MSuvDM4qa-DHB1_mggrMsfcET_jqfUtHFhPP7oCGIfsYmioRtezrAFDifNddpKI0sB6651OrvA1laZmw_wqVzV0Cqn6_6c_J0SLn0jJOTmxZqAW0GBIah4CkELpHGumPLzyitIR2xc-WAZCeLYfRTuhhUzjITAVBKQciJVNhOMkih_1FZTlu1CER_q8SM2szsjzcndh5meEGn88r03MXAB1uDkQiy_XbJK_qEY8IcJVC5NM3qw&***expires_in***=3600&***token_type***=Bearer

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=SplxlOBeZQQYbYS6WxSbIA
```

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.