Manuale Utente

Specifiche Tecniche - Autenticazione del fornitore di soluzioni software

Versione	1	Data Versione:	05 / 02 / 2025
Descrizione modifiche	Prima pubblicazione		
Motivazioni			

Indice

1 Introduzione al documento

1.1 Scopo e campo di applicazione del documento

Lo scopo del documento è fornire le specifiche tecniche per l'utilizzo dei servizi di autenticazione del fornitore di soluzioni software.

1.2 Livello di riservatezza

Pubblico	Uso interno	Riservato
X		

1.3 Precedenti emissioni

Versione		Data Versione:	
Descrizione modifiche			
Motivazioni			

1.4 Termini e definizioni

Di seguito i termini specifici di questo documento:

Termine	Descrizione
mTLS	mutual Transport Layer Security, metodo per l'autenticazione reciproca secondo RFC 8705

2 Servizi di Autenticazione

I servizi messi a disposizione da Infocamere sfruttano l'autenticazione con protocollo OAuth 2.0 tramite access token. Per la corretta fruizione di questi servizi è necessaria una preventiva autenticazione all'IAM (Identity & Access Management) server Infocamere.

Pertanto, è necessario utilizzare il servizio di autenticazione per ottenere l'access token, quest'ultimo poi va utilizzato per fruire di tutti i servizi di business. L'access token ha una durata limitata, superata la quale è necessario aggiornarlo.

Per l'ottenimento di un token autorizzativo valido dall'IAM Infocamere, il cliente deve aver completato correttamente la procedura di onboarding tramite l'invio della richiesta di fruizione alla casella mail PEC specifica.
Alla richiesta di fruizione del servizio dovrà essere allegata la parte pubblica del certificato client, preventivamente censita in fase di onboarding del cliente.
Infocamere, in caso di accettazione della richiesta di fruizione, fornirà in risposta i parametri necessari per la chiamata all'IAM server Infocamere, tra cui i parametri

- client_secret
- client_id

Il certificato client dovrà essere un certificato qualificato emesso da un prestatore di servizi fiduciari qualificato (Qualified Trust Service Provider) ai sensi del Regolamento (UE) n. 910/2014.
Il certificato di tipo qWAC, secondo la normativa eIDAS 2.0, deve certificare la software house che ha sottoscritto le condizioni di servizio, garantendo il riconoscimento della stessa da una terza parte qualificata.
Il certificato client utilizzato in fase di autenticazione deve essere quello la cui chiave pubblica è stata indicata durante il processo di onboarding.

L'access token fornito rispetta le specifiche RFC 6749. Di seguito è riportato un esempio del contenuto della risposta dell'IAM server Infocamere, in caso di autenticazione corretta*:*

```
{
    "access_token":"ey...5Q",
    "id_token": "ey...n0.",
    "refresh_token": "RT...9Z",
    "token_type": "Bearer",
    "expires_in": 300,
    "scope": "<scope>"
}
```

2.1 Auntenticazione mTLS

Il servizio di autenticazione viene richiamato configurando la chiamata secondo il protocollo mTLS.

URL

- collaudo: https://iamocl.infocamere.it/syncope-wa/oidc/oidcAccessToken
- produzione: https://iamo.infocamere.it/syncope-wa/oidc/oidcAccessToken

La chiamata deve essere di tipo GET ed avere i seguenti query params:

```
"grant_type"="client_credentials"
"client_id"="<valorizzato con il client_id fornito da InfoCamere>"
"client_secret"="<valorizzato con il client_secret fornito da
InfoCamere>"
"scope"="<scope del servizio>"
```