EVOLUZIONE BANCA DATI SINISTRI

INFRASTRUTTURA SCAMBIO FLUSSI

Specifiche interfaccia HTTP

Versione 1.0

INTRODUZIONE

Questo documento descrive le interfacce che una controparte esterna deve utilizzare per scambiare flussi in modalità A2A con la piattaforma U4F.
Le interfacce sono basate su standard e protocolli aperti ed ampiamente diffusi, non ci sono quindi particolari vincoli rispetto ad ambienti elaborativi, linguaggi, librerie e strumenti da utilizzare per la realizzazione del client.

I paragrafi che seguono descrivono le interfacce utilizzabili per il caricamento dei file tramite protocollo HTTPS in una configurazione in cui U4F implementa funzioni di server HTTP.

1 INTERFACCIA PER LE FUNZIONI DI CARICAMENTO FILE IN MODALITÀ HTTPS

Questo paragrafo descrive l'interfaccia esposta da U4F alle controparti esterne per la funzione di *upload* di un file tramite protocollo HTTPS in una configurazione in cui la Banca ha le funzioni di server HTTP.

Per usufruire dei servizi HTTPS esposti da U4F è necessario dotarsi preventivamente di una credenziale applicativa tramite la quale effettuare le necessarie interazioni [1].
Per la generazione dell'utenza applicativa e la mappatura del certificato X.509 utilizzato dovranno essere seguite le procedure descritte nel capitolo IV del "Manuale di accreditamento e di gestione delle credenziali" disponibile sul sito Internet della Banca http://www.bancaditalia.it
Tramite questa utenza sarà possibile eseguire comandi (*upload* e *download* di file) relativamente alle applicazioni/flussi per i quali tale utenza verrà autorizzata[2].

Le caratteristiche generali da utilizzare nell'accesso al servizio sono le seguenti:

- La connessione del client con il server deve supportare il protocollo TLS (v1.2 e successive);
- E' prevista una mutua autenticazione (*client authentication*) mediante utilizzo di certificati X.509[3];
- i certificati associati alle credenziali applicative (e quelli associati a tutta la relativa *chain*) devono essere firmati con algoritmi basati su *hash* sicuri, evitando il ricorso a quelli diffusamente e notoriamente considerati deboli (es. SHA1)[4];
- l'interfaccia applicativa è di tipo REST e stateless;
- il server comunica l'esito dell'operazione richiesta al client mediante un opportuno codice di ritorno http;
- i dati scambiati a corredo delle segnalazioni (es. metadati che descrivono il file) vengono codificati in formato JSON.

La tabella seguente riporta gli indirizzi dei servizi da contattare nei diversi ambienti.

Ambiente	***Indirizzo servizio REST***
COLLAUDO	https://certscambioflussi.bancaditalia.it/a2a/upload
PRODUZIONE	https://scambioflussi.bancaditalia.it/a2a/upload

[1] un operatore incaricato dalla controparte, dopo essersi registrato al sito della Banca con la propria CNS, registra una credenziale applicativa A2A secondo le modalità previste dalla procedura di *self-registration* dell'Istituto; ad ogni credenziale deve essere associato almeno un certificato digitale di autenticazione e di crittografia (se necessario), quest'ultimo necessario alla Banca d'Italia per cifrare le comunicazioni con la chiave pubblica del ricevente, il medesimo certificato può essere utilizzato per entrambe le funzioni.
[2] La modalità con cui una controparte comunica a Banca d'Italia i flussi a cui l'utenza applicativa deve essere abilitata non rientra nello *scope* del presente documento.
[3] il certificato deve prevedere l'attributo *extended key usage* "TLS WWW Client Authentication".
[4] Non viene fornito in questo ambito un elenco esaustivo dei suddetti algoritmi in quanto questo potrebbe essere aggiornato nel tempo in seguito al mutare delle minacce e con l'evoluzione degli standard di sicurezza.

Per ogni utenza controparte, all'atto della definizione, viene creata in WF una cartella dedicata e una sotto-cartella per ogni applicazione (e ogni modello di flusso) a cui la controparte è abilitata ad accedere per l'esecuzione di comandi di *upload*. Una controparte sarà abilitata e avrà visibilità solamente sulle cartelle relative ai modelli di flussi per i quali è autorizzata.

La controparte (utilizzando l'utenza *A2A-User* acquisita nella fase di registrazione ed il certificato ad essa associato) esegue la richiesta di *upload* di un file utilizzando un comando POST all'indirizzo indicato e ed un formato JSON multipart per la valorizzazione dei metadati necessari.
Di seguito i metadati richiesti per l'identificazione della richiesta:

- applicazione destinataria del flusso (*appName*) e identificativo del modello di flusso (*flowName*): passati nella URL di richiesta con il seguente schema *https://<indirizzo>/a2a/upload/<appName>/<flowName>*;
- file (*Payload*) da spedire: inserito nel *body* della richiesta all'interno di un parametro di tipo *form* denominato P*ayload*, con il contenuto del file e un attributo *filename*, che identifica il nome del file da caricare sulla piattaforma;
- metadati opzionali[5]: inseriti nel *body* della richiesta, in formato JSON (chiave, valore), all'interno di un parametro di tipo *form* denominato *optionalMetadata*.

Property name	Type	Description	Mandatory
optionalMetadata	Object (see below for the properties)	Metadata of the file	N
- opt1	String(min_length=1)	A metadata	N
- optN	String(min_length=1)	Another metadata	N
Payload	Binary	File uploaded + final file name	Y

Nel caso in cui i controlli di tipo formale riportino esito positivo, il servizio risponde alla richiesta dell'applicazione con codice di ritorno 201 e fornendo nella response JSON i seguenti parametri:

- *dataFlowId* : numero di protocollo univoco, costituito da 36 caratteri, che identificherà il flusso di ingresso nell'archivio ARCH-FLW;
- *appName*: stringa che identifica l'applicazione a cui il flusso è destinato;
- *flowName* : stringa che identifica il modello di flusso richiesto;
- *version* : numero intero che identifica versione dell'API di trigger;
- *createdTime* : data di creazione dell'istanza di flussi nell'archivio ARCH-FLW in formato ISO-8601.

Nel caso in cui si siano verificati degli errori, il servizio risponde alla richiesta con i seguenti codici di ritorno:

- 401, per errori verificatisi in fase di autenticazione (es. utente applicativo non presente nel repository della piattaforma di scambio flussi);
- 403, per errori verificatisi in fase autorizzativa (utente applicativo non abilitato all'applicazione/flusso richiesto);
- 404, errori riscontrati nei controlli formali eseguiti in fase di ricezione della richiesta (metadati obbligatori non presenti);
- 400 (Bad Request) nel caso di payload non valorizzato nei metadati.

Per evitare duplicazioni, legate al possibile utilizzo dello stesso nome da parte della controparte, il nome del file che verrà acquisito dalla piattaforma coinciderà con il nome fornito dalla controparte preceduto dal numero di protocollo univoco generato dalla piattaforma U4F.

Di seguito un esempio, tramite comando CURL, di chiamata al servizio di *upload* in ambiente di collaudo per una applicazione denominata *ivass-ebds*, un modello di flusso denominato *prova-ebds-in* ed un file di nome *prova-ebds-in.p7m.p7e*:

```
curl -k -E A2A-cert https://certscambioflussi.bancaditalia.it/a2a/upload/ivass-ebds/prova-ebds-in \
```

[5] Questi metadati, specifici per applicazione, non vengono trattati da U4F e vengono passati direttamente all'applicazione in un *report file* (vedi par. **Errore. L'origine riferimento non è stata trovata.**)

*-F 'payload=@/tmp/prova-ebds-in.p7m.p7e;filename=prova-ebds-in.p7m.p7e' *
-F 'optionalMetadata={"opt1":"Opt1Value","opt2":"OptValue2"}' -X POST

e della relativa risposta[6]

{"dataFlowId":"44888a0e-1ce0-4399-aa2f-ff7355507545","appName":"ivass-ebds","flowName":"prova-ebds-in","version":1,"createdTime":"2021-04-13T15:40:20.876+0000"}

Una volta acquisito il file questo verrà elaborato sulla base delle impostazioni previste in configurazione per la tipologia di flusso a cui il file appartiene e che vengono di seguito riportate[7]:

- cartella applicativa in cui il file (e il *report file* che lo identifica) deve essere depositato;
- cartella applicativa in cui il file di copia probatoria deve essere depositato;
- lista delle operazioni di sicurezza da applicare al file ricevuto (combinazione delle operazioni di verifica antivirus (sempre presente), verifica firma, decifratura e decompressione (eseguita prima o dopo la verifica firma o la decifratura);
- Informazioni relative all'eventuale *web service* da richiamare per notificare l'applicazione della presenza di un nuovo file.

2 INTERFACCIA PER LE FUNZIONI DI DOWNLOAD IN MODALITÀ HTTPS

Questo paragrafo descrive l'interfaccia esposta da U4F e i servizi utilizzabili da una controparte per la funzione di *download* di un file tramite protocollo HTTPS.

La tabella seguente riporta le URL da contattare nei diversi ambienti.

Ambiente	***Indirizzo servizio REST***
COLLAUDO	https://certscambioflussi.bancaditalia.it/a2a/download
PRODUZIONE	https://scambioflussi.bancaditalia.it/a2a/download

Per ogni utenza controparte, all'atto della definizione, viene creata in WF una cartella dedicata e una sotto-cartella per ogni applicazione (e ogni modello di flusso) a cui la controparte è abilitata ad accedere per l'esecuzione di comandi di *download*. Una controparte sarà abilitata e avrà visibilità solamente sulle cartelle relative ai modelli di flussi per i quali è autorizzata.

Servizio di consultazione dei file disponibili

La controparte ha a disposizione un servizio di consultazione che fornisce l'elenco dei file presenti nella cartella di *download*.

L'elenco dei file scaricabili, prodotti da un applicazione (*appName*) e relativi ad un modello di flusso (*flowName*), può essere ottenuto mediante una richiesta (metodo GET) alla URL *https://<indirizzo>/a2a/download/<appName>/<flowName>.*
L'output, codificato in formato JSON, contiene nella proprietà *files* un array di oggetti contenenti le seguenti proprietà:

- *fileName*: stringa contenente il nome del file;
- *lastModifiedTime*: timestamp di ultima modifica (formato Unix time);
- *isRegularFile:* assume il valore *true* o *false* a seconda che l'oggetto sia di tipo file;
- *isDirectory*: assume il valore *true* o *false* a seconda che l'oggetto sia di tipo directory;
- *size*: la dimensione del file (non valorizzata nel caso di directory).

Il servizio verifica che la controparte sia abilitata all'applicazione e al flusso richiesto e, nel caso in cui i controlli abbiano riportato esito positivo, risponde alla richiesta con un codice di ritorno 200.

[6] In questo caso il nome del file acquisito sulla piattaforma sarà *44888a0e-1ce0-4399-aa2f-ff7355507545. prova-ebds-in.p7m.p7e*
[7] Sono le informazioni propedeutiche fornite dai responsabili dell'aplpicazioni ai gestori della piattaforma U4F in fase di configurazione del tipo di flusso.

Nel caso in cui si siano verificati degli errori, il servizio risponde alla richiesta con gli stessi codici indicati al paragrafo precedente.

Di seguito un esempio, tramite comando CURL, di chiamata al servizio di consultazione in ambiente di collaudo per una applicazione denominata *ivass-ebds* e un modello di flusso denominato *prova-ebds-out*

curl -k -E A2A-cert " https://certscambioflussi.bancaditalia.it/a2a/download/ivass-ebds/prova-ebds-out "

e della relativa risposta

```
"files" :
  [    {
      "fileName" : "testout.p7m.p7e",
      "isDirectory" : false,
      "isRegularFile" : true,
      "size" : 5990,
      "lastModifiedTime" : 1618313875425
    }   ]
```

Servizio di scarico di un file

La controparte esegue il comando di *download* di un file, prodotto da un applicazione (appName) e relativo al modello di flusso (flowName) tramite una richiesta (metodo GET) all'indirizzo *https://<indirizzo>/a2a/download/<appName>/<flowName>/<fileName>* con il valore di *fileName* ricavato dall'output del servizio di consultazione descritto al punto precedente.

Il file viene fornito nel body della response.

Di seguito un esempio, tramite comando CURL, di chiamata al servizio di *download* in ambiente di collaudo per una applicazione denominata *ivass-ebds*, un modello di flusso denominato *prova-ebds-out* e un file denominato *testout.p7m.p7e*.

curl -k -E A2A-cert –o /tmp/output_download.txt
"https://certscambioflussi.bancaditalia.it/a2a/download/ivass-ebds/prova-ebds-out/testout.p7m.p7e "