IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

EVOLUZIONE BANCA DATI SINISTRI

INFRASTRUTTURA SCAMBIO FLUSSI

Checklist verifica accesso all'infrastruttura scambio flussi

Versione 1.0

Ambiente di collaudo

Il seguente documento riassume le attività da eseguire da parte di una controparte esterna per verificare il corretto accesso all'infrastruttura di scambio flussi fornita da Banca d'Italia in modo da risolvere eventuali problematiche di base legate all'utilizzo dei certificati di autenticazione, firma e cifratura utilizzati dalla controparte.

1. Fase di registrazione nel portale di Banca

Per accedere al servizio di scambio flussi la controparte deve dotarsi di una propria credenziale applicativa (utenza da utilizzare nei successivi scambi) registrandosi sul sito https://certscambioflussi.bancaditalia.it.
Per eseguire la registrazione è necessario essere in possesso di una CNS in corso di validità o di una credenziale SPID di livello 3.
Una volta registratosi l'utente può richiedere la creazione di una nuova credenziale applicativa (A2A-<xxxxxx>) alla quale saranno associati un certificato di autenticazione ed uno di cifratura (possono anche coincidere).

NOTA1 : I certificati di autenticazione e cifratura applicativa devono essere rilasciati da certificatori (CA Certification Authority) il cui certificato "ROOT" sia presente nella lista riconosciuta dai browser più comuni (es. per *Mozilla* la lista è consultabile al sito https://wiki.mozilla.org/CA/Included_Certificates). I certificati di autenticazione devono contenere l'Extended Key Usage "TLS Web Client Authentication".

NOTA2: Nel caso in cui il certificato sia firmato da una o più CA intermedie, i certificati delle CA intermedie (e della ROOT CA) **non devono** essere incluse nel *file* caricato.

2. Firma del file da spedire

Il servizio di Banca di verifica firma richiede in ingresso esclusivamente una firma digitale (ossia una firma che garantisca il non ripudio) con un certificato rilasciato da un certificatore accreditato AGID (la lista è consultabile al sito https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia).
Relativamente al formato di firma deve essere utilizzato il formato CADES che genera un file firmato con estensione p7m (non è supportato il formato SMIME).

3. Cifratura del file da spedire

La cifratura di un file deve essere eseguita utilizzando il certificato pubblicato da Banca al seguente indirizzo: https://www.bancaditalia.it/statistiche/raccolta-dati/centrale-rischi/doc-tecnica-cr/index.html
(sezione "Certificati digitali – cifratura" -> "Certificato di cifratura Banca d'Italia - utilizzato a partire dal 28 maggio 2021").
Per eseguire la corretta cifratura di un file precedentemente firmato (*nomefile.p7m*) si può utilizzare il seguente comando:
openssl cms -encrypt -binary -aes256 -in nomefile.p7m -outform DER -out nomefile.p7m.p7e - cifraturasharedservices.bancaditalia.it.crt

4. Spedizione del file

Come sopra indicato la spedizione di un file in modalità A2A richiede l'utilizzo della corretta sequenza di preparazione del flusso (prima firma e poi cifratura del file da spedire).
Il protocollo da utilizzare per la comunicazione di rete deve essere TLS v1.2 (non sono permessi SSL v3 o TLS v1.0).
Per la corretta autenticazione del file deve essere utilizzato il certificato associato all'utenza A2A in fase di generazione dell'utenza (vedi par.1): non è ammesso l'utilizzo di certificati *self-signed* o rilasciati da certificatori non presenti nel *CA-Bundle* di *Mozilla*.

Per verificare il corretto accesso all'infrastruttura di Banca si richiede di eseguire il seguente comando (per un flusso applicativo di tipo segnalazioni-in), preferibilmente da una piattaforma Linux[1]:

curl -v -k --trace-time -E cert_auth https://certscambioflussi.bancaditalia.it/a2a/upload/ivass-ebds/segnalazioni-in -F "payload=@nomefile.p7m.p7e;filename= nomefile.p7m.p7e" -X POST

dove

- *nomefile.p7m.p7e* è il file risultante dalle operazioni di firma e cifratura di cui al punto precedente (quando lo si usa con la varibile *payload* indicare il *path* completo in cui il file è memorizzato);
- *cert-auth* è il certificato di autenticazione in formato PEM contenente la chiave privata, il certificato pubblico e a seguire i certificati di tutte le eventuali CA intermedie (non inserire il certificato della ROOT CA).

La seguente tabella riporta alcune verifiche da eseguire in autonomia per la risoluzione di eventuali problemi riscontrati a seguito dell'utilizzo del comando curl.

Problema	***Verifiche***
Non si completa la fase di handshake SSL (la CURL non ritorna esito positivo)	Verifica utilizzo del protocollo TLS v1.2. Verifica che la CA di Banca sia "trusted" (inserire opzione –k nella CURL). Verificare che il file del certificato sia effettivamente "letto" dalla CURL (provare ad indicare un nome sbagliato e assicurarsi che la CURL ritorni l'errore) Verifica che il certificato di autenticazione non sia di tipo "*self-signed*". Verifica che il certificato di autenticazione sia rilasciato da una CA "trusted". Verifica che il file contenente il certificato di autenticazione contenga tutte le eventuali CA intermedie (ma non la ROOT CA).
La CURL ritorna errore 401 e il messaggio di errore "*Certificate not found*"	Verificare che il certificato di autenticazione utilizzato nella coincida con quello precedentemente registrato
La CURL non ritorna errori e fornisce come risposta un numero di protocollo (*dataFlowId*) ma la risposta applicativa contiene l'errore bloccante *ERRBFLU003*	L'errore indica che è stato riscontrato un virus nel file spedito
La CURL non ritorna errori e fornisce come risposta un numero di protocollo (*dataFlowId*) ma la risposta applicativa contiene l'errore bloccante *ERRBFLU004*	L'errore indica un problema in fase di decifratura. Verifica dell'utilizzo del certificato di cifratura pubblicato da Banca d'Italia Verifica utilizzo formato di cifratura (CMS) Verifica utilizzo algoritmo di cifratura (consigliato AES256)
La CURL non ritorna errori e fornisce come risposta un numero di protocollo (*dataFlowId*) ma la risposta applicativa contiene l'errore bloccante *ERRBFLU005*	L'errore indica un problema in fase di verifica firma. Verifica dell'utilizzo di un certificato di firma rilasciato da un certificatore accreditato AGID Verifica utilizzo del formato CADES (file generati con estensione p7m)

[1] Per piattaforme Windows si è riscontrato in alcuni casi la non corretta gestione delle opzioni "--cert" e "-E" della CURL che comportano errori nella fase di autenticazione (il certificato non viene correttamente acquisito e fornito): per verificare che non si ricada in questo caso provare a fornire il nome di un file certificato non presente e assicurarsi che venga ritornato un errore. Inoltre per W10 potrebbe essere necessario, nell'uso dell'opzione -F, utilizzare l'apice in sostituzione delle virgolette.