BANCA D'ITALIA
EUROSISTEMA

SERVIZIO DICHIARAZIONE SOSTITUTIVA DI PROTESTO

Autenticazione e autorizzazione delle utenze. Firma dei flussi

Febbraio 2017

Sommario

Versione	Autore	Data	Modifiche
Ottobre 2016		20-10-2016	Cap. 3.1.3
Novembre 2016		11-11-2016	Cap 3.3 – tabella, Cap. 3.1.2

1 Obiettivo

Obiettivo del presente documento è delineare i requisiti di sicurezza delle interfacce offerte dalla procedura. In particolare, sono indicate le modalità di autorizzazione e autenticazione delle utenze esterne, nonché le specifiche di firma dei flussi.

2 Registrazione e autorizzazione delle utenze

Gli utenti esterni devono essere preventivamente registrati e autorizzati ad accedere alle funzioni della procedura INSOLUTI.

2.1 Registrazione delle utenze esterne.

La soluzione prevede che la registrazione degli utenti esterni (amministratori e segnalatori) segua le regole della procedura di *self-registration* sul sito della Banca d'Italia;

Saranno rese note le regole per la registrazione delle utenze di tipo "ente" (utenze applicative).

2.2 Autorizzazione delle utenze.

Ogni trattario può designare gli utenti che assumono il ruolo di amministratore per la procedura INSOLUTI (amministratori INSOLUTI). Tali soggetti devono aver preventivamente completato il processo di *self-registration* ed essere in possesso di un identificativo utente (userid).

Per registrare un amministratore INSOLUTI, il trattario deve inviare alla Banca d'Italia un modulo precompilato riportante le seguenti informazioni[1]:

- Nome;
- Cognome;
- Codice fiscale;
- Userid ottenuto nel processo di *self-registration*;
- Identificativo del trattario per cui il soggetto deve operare;
- Tipo di identificativo del trattario (ABI, CF ecc.);
- Servizio applicativo d'interesse (Insoluti);

Gli amministratori INSOLUTI possono accedere alle interfacce grafiche della procedura della Banca per assegnare i ruoli necessari a operare sulla procedura.

Gli amministratori INSOLUTI possono assegnare i seguenti ruoli:

Segnalatore: Utente che può inviare flussi. Il segnalatore, inoltre, può acquisire le risposte elaborative prodotte dalla procedura INSOLUTI. Il segnalatore può accedere alle funzioni di *upload*, *download* e *inquiry* dei messaggi.

Firmatario: Utente che può Firmare le richieste di DSP per il trattario.

[1] Il trattario può inviare anche richieste di revoca del ruolo di Amministratore.

3 Autenticazione e firma dei flussi.

3.1 Flussi in ingresso

Di seguito si riportano i requisiti di sicurezza per i flussi inviati alla Banca d'Italia.

3.1.1 Autenticazione

Le misure di sicurezza previste sono:

- utilizzo del protocollo TLS v1.2 per la protezione dei dati trasmessi su rete Internet;
- autenticazione forte per le interazioni U2A (solo per le funzione di gestione degli utenti previste per l'amministratore);
- autenticazione basata su certificato X509 per le interazioni A2A.

Ciò considerato, per soddisfare i suddetti requisiti è necessario instaurare un canale:

- SSL 2-way (scambio certificati *client*/*server*) per gli accessi di tipo U2A;
- SSL 2-way (scambio certificati *client*/*server*) per gli accessi di tipo A2A.

Di conseguenza, alle controparti è richiesto:

- di dotare i propri utenti di un dispositivo CNS, contenente certificati rilasciati da certificatori accreditati AGID, per gli accessi di tipo U2A. L'elenco degli enti abilitati al rilascio di tali dispositivi è disponibile al sito: https://applicazioni.cnipa.gov.it/TSL/IT_TSL_CNS.xml;
- di dotarsi di un certificato applicativo con *extended key usage* "*TLS WWW Client Authentication*", rilasciato da certificatori riconosciuti dai principali *browser* web, per gli accessi di tipo A2A;

3.1.2 Firma del *payload* (flusso)

I dati ricevuti dai trattari devono essere firmati in modo da garantirne l'integrità.

Relativamente al formato, sono accettate firme in conformità con lo standard XADES (così come definito dall'ETSI), nei formati *Baseline* e *Time-stamping*; le strutture di *packaging* sono "*Enveloping*" ed "*Enveloped*" .

Nella tabella di seguito è riassunto il formatoi della tipologie:

Formato *Baseline*	*Timestamping*	*Enveloping*	*Enveloped*
XAdES-B	XAdES-T	SI	SI

La firma digitale deve essere apposta sul documento intero e non sono accettate firme multiple su parti diverse dello stesso documento.

Per la verifica della firma si fa riferimento agli standard [R03], [R04] e [R05].

3.1.3 Verifica della firma delle immagini degli assegni

Le immagini degli assegni dovranno essere firmate digitalmente secondo le modalità indicate nel regolamento Banca d'Italia[2].

La firma digitale deve essere apposta in formato PAdES sul documento intero.

3.2 Flussi in uscita

Si tratta di dati che le controparti acquisiscono accedendo alle risorse pubblicate dalla Banca.

Le risposte non sono firmate, tranne le singole DSP e gli attestati di non protestabilità.

3.2.1 Firma delle DSP

I dati trasmessi alle controparti delle DSP e gli attestati di non protestabilità devono essere firmati in modo da garantirne l'integrità.

Per quanto concerne il formato di firma, si opta per il formato PAdES.

3.3 Riepilogo dei certificati digitali in uso

Obiettivo	**Certificato richiesto**
Autenticazione U2A	Certificato di autenticazione su CNS rilasciato da certificatore accreditato AGID per il rilascio di certificati di autenticazione
Autenticazione A2A	Certificato applicativo di autenticazione rilasciato da certificatore appartenente alla lista dei certificatori riconosciuta dai browser più comuni
Firma dei dati in ingresso a BDI – caso A2A	Certificato di firma rilasciato da certificatore accreditato AGID per il rilascio di certificati per utilizzo con dispositivo sicuro per l'apposizione della firma digitale

Dotazione di certificati digitali per i singoli utenti persone fisiche presso le controparti (accessi U2A):

- *n.1 certificato di autenticazione su CNS*
- *n.1 certificato di firma rilasciato da certificatori accreditati AGID*

Dotazione di certificati digitali per le singole controparti (accessi A2A):

[2] Regolamento ex art. 8, comma 7, lett. e), del decreto-legge 13 maggio 2011, n. 70, convertito dalla legge 12 luglio 2011, n. 106.

- *n.1 certificato di autenticazione.*

Riferimenti

Ref.	Requisito	Standard di riferimento	Versione	Data
R01	Firma digitale	XAdES Specifications – ETSI TS 101 903	1.4.2	12/2010
R02		CAdES Specifications – ETSI TS 101 733	2.2.1	04/2013
R03		PADES Specifications – ETSI TS 102 778		
R04		Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – IETF RFC 5280	N/A	05/2008
R05		OCSP – IETF RFC 6960	N/A	06/2013
R06		Electronic Signatures and Infrastructures; Signature verification procedures and policies – ETSI TS 102 853	1.1.1	07/2012
R07		XAdES Baseline profiles – ETSI TS 103 171	2.1.1	03/2012
R08		CAdES Baseline profiles – ETSI TS 103 173	2.2.1	04/2013
R09		PADES Baseline Profiles – ETSI TS 103 172	2.1.1	