Portale ABACO – Autenticazione e cifratura dei flussi

SOMMARIO

1 SCOPO

Per accedere alle funzioni del Portale ABACO gli utenti delle controparti dovranno essere preventivamente registrati e dovranno autenticarsi mediante CNS oppure certificato X509[1]. Inoltre, essi dovranno essere associati, su richiesta delle relative controparti, ai ruoli operativi previsti dall'applicazione: Amministratore, Segnalante, Operatore, Firmatario e Ricevente.

Obiettivo del presente documento è delineare i requisiti di sicurezza delle interfacce offerte dal nuovo Portale ABACO: le modalità di autorizzazione e autenticazione delle utenze esterne, nonché le specifiche di firma e cifratura dei flussi.

[1] Per applicazioni che operano in modalità A2A.

2 Il portale ABACO

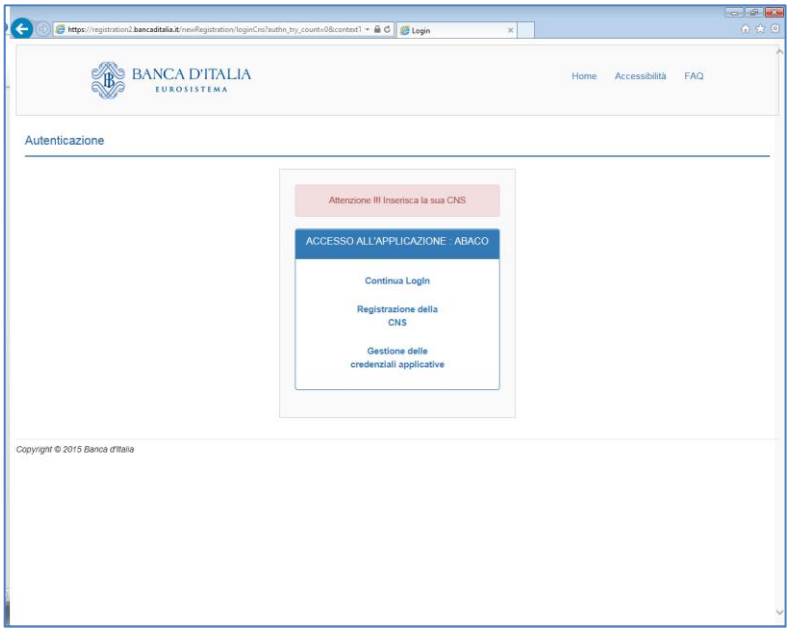
Il Portale ABACO è un'applicazione WEB raggiungibile attraverso le URL:

https://abaco.bancaditalia.it/ per le interazioni U2A mediante browser;
https://abaco.bancaditalia.it/abaco-front-web/rest per le interazioni A2A.

Essa consente agli utenti autorizzati di veicolare le istruzioni relative ai portafogli di prestiti aggiuntivi. Il Portale, inoltre, rende disponibili gli esiti elaborativi delle segnalazioni prodotte dalle istruzioni inviate.
È possibile accedere alle funzionalità offerte dal Portale ABACO sia in modalità U2A che A2A. Le persone fisiche che accedono al Portale devono autenticarsi mediante CNS (Carta nazionale dei Servizi) mentre le applicazioni dovranno autenticarsi mediante certificato X509.

Per accedere al Portale ABACO nella modalità U2A, gli utenti autorizzati, che hanno quindi completato il processo di *self-registration* descritto più oltre, dovranno:

1. inserire la propria CNS nel lettore di badge della postazione in uso;
2. accedere mediante browser alla URL https://abaco.bancaditalia.it/; essi saranno indirizzati sulla pagina web di login.



3. scegliere l'opzione "Continua Login" e digitare il PIN della CNS per accedere alla pagina https://abaco.bancaditalia.it/abaco-front-web/. A questo punto potranno fruire delle funzioni esposte dal Portale ABACO seguendo le istruzioni riportate nei manuali utenti.

2.1 Registrazione e autorizzazione delle utenze

Per accedere alle funzioni esposte dal Portale ABACO, gli utenti delle controparti dovranno essere preventivamente registrati e autorizzati.

2.2 Registrazione delle utenze esterne.

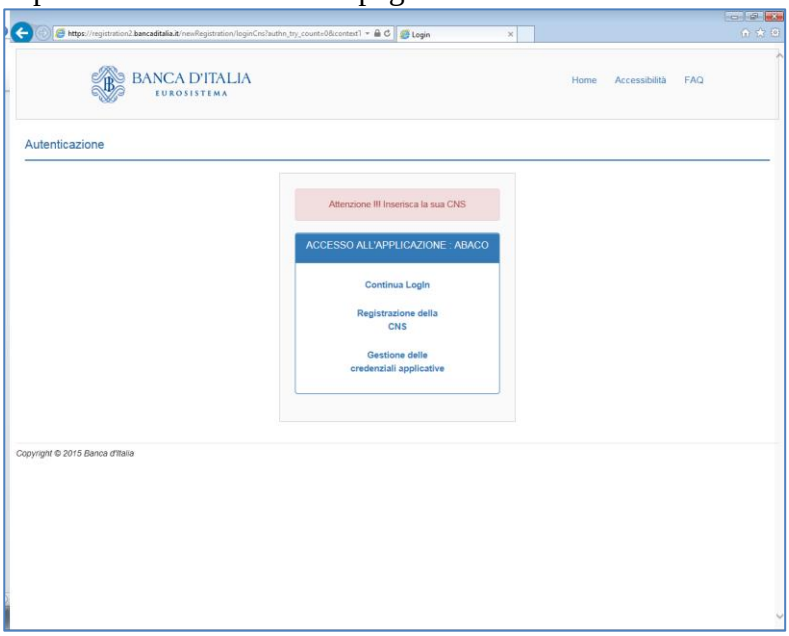
La registrazione degli utenti esterni segue le regole della procedura di *self-registration* presente sul sito della Banca, che può essere attivata accedendo alla URL https://abaco.bancaditalia.it/ oppure alla URL https://rbauth.bancaditalia.it/.

La procedura richiede il possesso della CNS e consente di registrare utenze personali oppure utenze di tipo “ente” (applicative). A queste ultime è possibile associare un certificato X509 per l’autenticazione A2A. A tutte le utenze, inoltre, è possibile associare un certificato di cifratura, necessario per comunicazioni cifrate mediante la chiave pubblica del Ricevente.

La registrazione di un’utenza applicativa e dei relativi certificati è a carico dell’Amministratore, che dovrà essere dotato di CNS che deve aver già effettuato con successo la registrazione per persona fisica.

Per attivare il processo di *self-registration* l’utente esterno deve:

1. Inserire nel lettore di Badge della postazione in uso la propria CNS;
2. Accedere alla URL https://abaco.bancaditalia.it/ oppure https://rbauth.bancaditalia.it/; in risposta sarà visualizzata la pagina web:



3. Scegliere l’opzione “Registrazione della CNS” e seguire le successive istruzioni.

2.3 Autorizzazione delle utenze.

Per filtrare l’accesso alle funzionalità esposte, il Portale ABACO riconosce i ruoli di seguito descritti:

Amministratore: Utente che ha la facoltà di:

- indicare quali utenti della controparte amministrata potranno accedere alle funzioni esposte dal Portale ABACO mediante i ruoli di **Segnalante** o di **Operatore**;
- designare i soggetti che assumono il ruolo di sottoscrittore di flusso (**Firmatario**) per conto della controparte amministrata;
- designare il soggetto che assume il ruolo di **Ricevente** per la controparte Amministrata. Il Portale cifrerà i messaggi destinati alla controparte mediante la chiave pubblica di cifratura associata al Ricevente.

Segnalante: Utente che accede al Portale ABACO per inviare istruzioni e acquisire i relativi esiti elaborativi per conto della banca per cui opera. L’utente segnalante è autorizzato ad accedere alle funzioni di upload e download.

Operatore: Utente che accede al Portale ABACO per richiedere informazioni sui flussi informativi ICAS. L'operatore non può inviare istruzioni né accedere ai relativi esiti elaborativi;

Firmatario: persona autorizzata a firmare i gruppi di istruzioni indirizzate alla procedura della Banca d'Italia per conto di una controparte/erogante[2]. Tali soggetti potrebbero non essere dotati di credenziali di accesso al Portale ABACO. Le controparti/eroganti possono delegare la firma del gruppo di istruzioni alla stessa persona che provvede all'invio (il Segnalante), oppure a una persona autorizzata a firmare le singole istruzioni (che potrebbe non avere credenziali di accesso al Portale ABACO);

Ricevente: è unico per ogni controparte. Individua l'utenza rispetto a cui cifrare i messaggi di risposta destinati alla controparte.

NOTA: Uno stesso soggetto può rivestire più ruoli.

2.3.1 Amministratore del Portale ABACO

Per attribuire a un soggetto il ruolo di Amministratore del Portale ABACO, ogni controparte dovrà inviare alla Banca una esplicita richiesta secondo quanto indicato nella Guida Portafogli. In particolare occorre produrre la documentazione attestante la nomina del soggetto designato a rivestire il ruolo di amministratore debitamente firmata dal rappresentante legale della banca.

Pre-requisiti

1. La banca che chiede alla Banca d'Italia di conferire il ruolo di Amministratore a un determinato soggetto deve essere già censita (come controparte o erogante);
2. L'utente che assumerà il ruolo di Amministratore dovrà dotarsi di una CNS e dovrà aver completato il processo di *self-registration*. Il processo attribuirà al soggetto una userid.

NOTA: Uno stesso soggetto potrebbe rivestire il ruolo di Amministratore per più controparti.

2.3.2 Funzioni riservate all'Amministratore

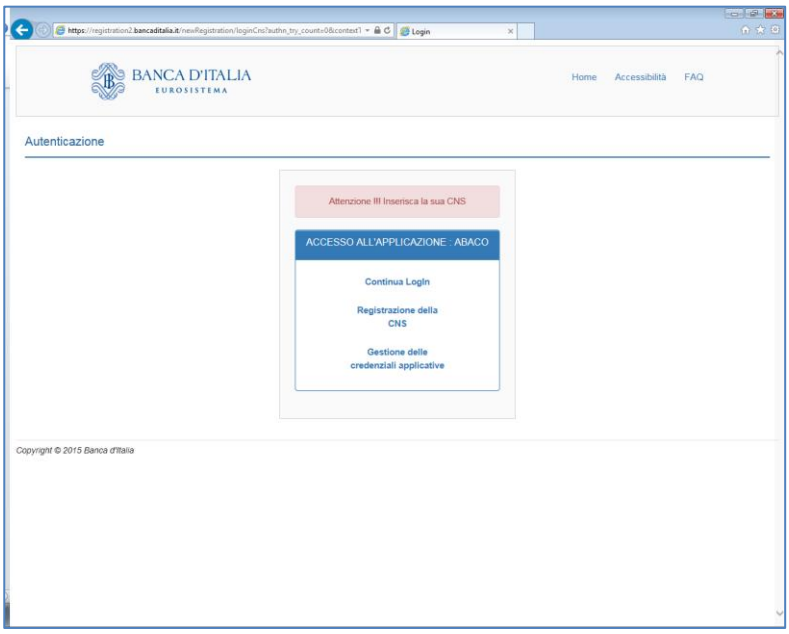
L'utente che opera come Amministratore del Portale ABACO per conto di una banca può conferire ruoli operativi ad altre utenze per conto della stessa banca.

L'Amministratore può definire le associazioni tra utenze e ruoli applicativi (Segnalante, Operatore, Ricevente e Firmatario) accedendo in modalità U2A alla url https://rbauth.bancaditalia.it/ .

A tal fine l'Amministratore deve:

1. Inserire nel lettore di Badge della postazione in uso a propria CNS;
2. Accedere mediante browser alla URL https://rbauth.bancaditalia.it/; in risposta sarà visualizzata la pagina web:

[2] Il gruppo di istruzioni inviato alla procedura della Banca d'Italia è firmato da una persona per assicurarne l'integrità e la provenienza; successivamente è cifrato con la chiave pubblica della Banca (riservatezza).



4. Scegliere l'opzione "ContinuaLogin" e digitare il PIN della CNS per accedere alla pagina https://rbauth.bancaditalia.it/rbauth-wf-web/.

L'accesso all'applicazione permette di associare utenze esterne ai ruoli applicativi riconosciuti dal Portale ABACO[3].

Pre-requisiti.

L'utente cui attribuire uno dei ruoli operativi riconosciuti dal Portale ABACO deve aver completato il processo di *self-registration*, presente sul sito dell'Istituto; l'utente cui attribuire il ruolo di Firmatario potrebbe non essere un utente registrato. In tal caso l'Amministratore inserirà solo il relativo codice fiscale.

Passi operativi

L'Amministratore si autentica mediante CNS e accede al sistema, quindi seleziona la banca per la quale intende operare e per cui è stato designato come Amministratore.
L'Amministratore inserisce la userid dell'utente su cui operare (o il codice fiscale); se l'Amministratore ha inserito una userid registrata il sistema mostra a video i dati anagrafici dell'utente indicato e gli eventuali ruoli ad esso già conferiti.
L'amministratore seleziona dalla lista dei ruoli del Portale ABACO il nuovo ruolo da assegnare al soggetto selezionato; quindi conferma l'operazione richiesta.
Il sistema effettua i necessari controlli di consistenza e, in caso positivo, registra la nuova associazione.

2.4 Autenticazione, cifratura e firma dei flussi.

2.4.1 Flussi in ingresso

Requisiti di sicurezza per i flussi inviati alla Banca dalle controparti. Per 'Firma' e 'Cifratura' si intendono i livelli più esterni del seguente schema:

[3] Più in generale RBAUTH gestirà le autorizzazioni per l'accesso alle funzioni erogate da più applicazioni dell'Istituto.

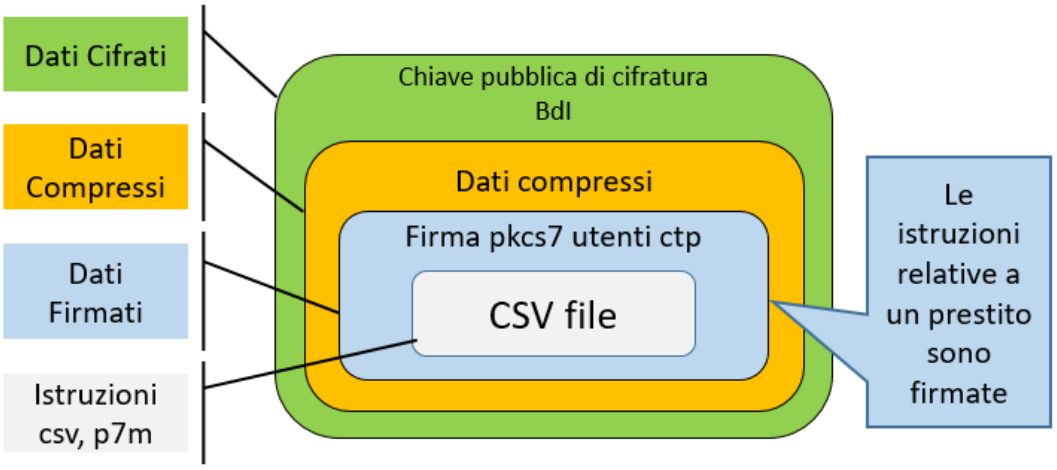


Figura 1 - Struttura di un flusso in entrata al Portale ABACO

2.4.2 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;
- 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 di mercato[4], per gli accessi di tipo A2A. NOTA: nella fase di autenticazione il CLIENT deve presentare il certificato di autenticazione seguito dagli eventuali certificati delle CA intermedie (RFC5246).

Le controparti sono tenute a proteggere i certificati di autenticazione per evitare che le proprie utenze siano utilizzate da persone non autorizzate.

2.4.3 Firma del payload

I dati inviati dalle controparti (i gruppi di istruzioni) devono essere firmati in modo da garantirne l'integrità e il non ripudio.

Per la firma digitale nel caso U2A, l'utente dovrà pertanto dotarsi di un certificato posto su dispositivo sicuro (smart-card[5], chiavetta USB oppure HSM) rilasciato da certificatori accreditati AGID per la firma digitale (https://applicazioni.cnipa.gov.it/TSL/IT_TSL_signed.xml).

Anche nel caso A2A i dati inviati dalle controparti dovranno essere firmati con certificati rilasciati da certificatori accreditati AGID.

Relativamente al formato di firma, saranno accettate firme in formato CADES [R01].

[4] Per ulteriori riferimenti si rimanda a https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.3.3.pdf.

[5] Sul mercato sono disponibili *smart-card* che possono ospitare sia il certificato CNS previsto per l'autenticazione che il certificato necessario alla firma digitale.

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

2.4.4 Cifratura del payload

I dati inviati dalle controparti (i gruppi di istruzioni) devono essere crittografati applicativamente in modo da garantirne la riservatezza.
Per garantire la riservatezza dei dati inviati alla Banca d'Italia, la controparte dovrà utilizzare il certificato di chiave pubblica di cifratura pubblicato sul portale ABACO.
L'operazione di cifratura del file dovrà avvenire in conformità a [R08], con le seguenti specifiche:

- modalità "Enveloped Data Type";
- algoritmo di cifratura simmetrica AES con lunghezza di chiave pari a 256 bit;
- chiave pubblica di cifratura della chiave simmetrica con cui viene cifrato il dato, RSA a 2048 bit;
- certificato di chiave pubblica di cifratura nel formato X.509 Binario codificato DER.

Inoltre, all'interno della busta crittografica, la chiave simmetrica di cifratura dovrà essere crittografata sia mediante la chiave pubblica della Banca, sia mediante la chiave pubblica del mittente. In tal modo, infatti, anche il mittente sarà in grado di accedere al messaggio originariamente inviato.

2.5 Preparazione dei flussi in entrata

Il processo di preparazione dei flussi in entrata può essere riassunto come di seguito. Per le specifiche delle operazioni di firma e cifratura, vale quanto detto nei paragrafi precedenti.

Il punto di partenza è costituito da un gruppo di (una o più) istruzioni, firmate, in formato *.csv.p7m.

I passi di preparazione all'invio del gruppo di istruzioni, sono i seguenti:

1) compressione del gruppo di istruzioni firmato → un file *.csv.p7m.zip
2) cifratura del file firmato → un file *.csv.p7m.zip.p7e

La struttura finale del gruppo di istruzioni, rispecchia quanto mostrato in Figura 1.

2.6 Flussi in uscita

Sono presenti requisiti di sicurezza per i flussi pubblicati dalla Banca a favore delle controparti.
Si tratta di dati che le controparti acquisiscono accedendo alle risorse pubblicate dalla Banca.
Il GruppoRisposte prima di essere pubblicato sarà firmato digitalmente con il certificato applicativo della Banca d'Italia e poi cifrato con la chiave pubblica del ricevente della controparte. Per 'Firma' e 'Cifratura' si intendono i livelli più esterni del seguente schema:

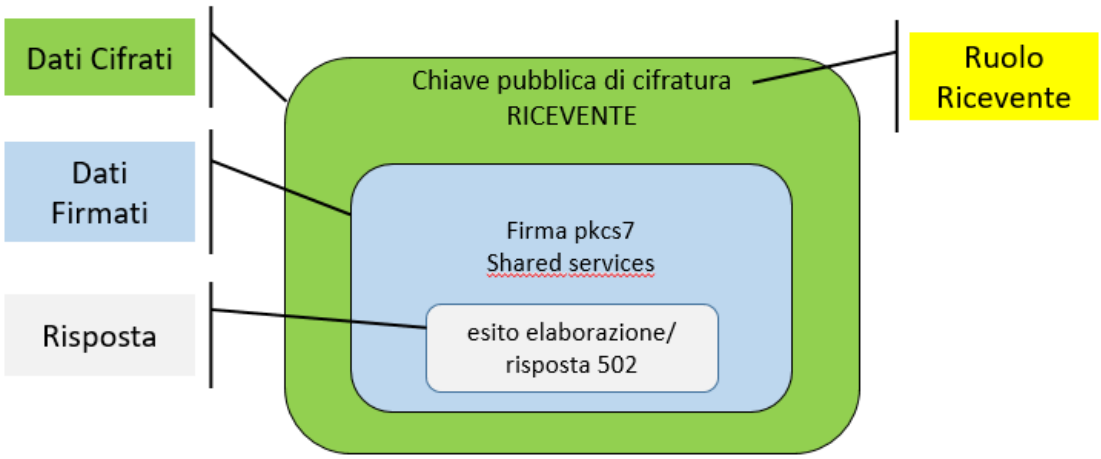


Figura 2 - Struttura di un flusso in uscita

2.6.1 Firma del payload

I dati trasmessi alle controparti (le risposte elaborative e gli estratti conto) devono essere firmati in modo da garantirne l'integrità.
Per quanto concerne il formato di firma, si opta per il formato CADES conformemente ai profili definiti in [R06] e [R07] nella tipologia CADES-B.

2.6.2 Cifratura del payload

I dati trasmessi alle controparti (le risposte elaborative e gli estratti conto) devono essere crittografati applicativamente in modo da garantirne la riservatezza.
Per inviare dati cifrati alle controparti, la Banca d'Italia necessita di un certificato di chiave pubblica di cifratura del ricevente.

Per semplicità di gestione, si richiede alle controparti di acquisire certificati di cifratura (*key usage "key encipherment"*) con lunghezza di chiave pari a 2048 bit, conformi a quanto prescritto nello standard RFC 5280.
Le controparti sono tenute a proteggere adeguatamente il proprio certificato di cifratura per evitare che sia utilizzato da persone non autorizzate. Inoltre, devono implementare un accurato processo di gestione della chiave privata del certificato di cifratura perché in caso di indisponibilità non sarebbe più possibile decifrare i messaggi che la Banca ha criptato con quel certificato.

L'operazione di cifratura del file sarà conforme a [R08], con le seguenti specifiche:

- modalità "Enveloped Data Type";
- algoritmo di cifratura simmetrica AES con lunghezza di chiave pari a 256 bit;
- chiave pubblica di cifratura della chiave simmetrica con cui viene cifrato il dato, RSA a 2048 bit;
- certificato di chiave pubblica di cifratura nel formato X.509 Binario codificato DER.

2.7 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 U2A	Certificato rilasciato da certificatore accreditato AGID per il rilascio di certificati per utilizzo con dispositivo sicuro per l'apposizione della firma digitale
Firma dei dati in ingresso a BDI – caso A2A	Certificato rilasciato da certificatore accreditato AGID per il rilascio di certificati per utilizzo con dispositivo sicuro per l'apposizione della firma digitale
Cifratura dati in ingresso a BDI	Certificato di chiave pubblica di Banca d'Italia, emesso da CA BDI e messo a disposizione sul portale ABACO
Firma dei dati in uscita da BDI	Firma non qualificata mediante certificati emessi da CA BDI
Cifratura dati in uscita da BDI	Certificato di chiave pubblica di cifratura della controparte, (key usage "key encipherment") con lunghezza di chiave pari a 2048 bit, conforme a quanto prescritto nello standard RFC 5280. Si rammenta l'importanza di implementare un accurato processo di gestione della chiave privata associata al certificato di cifratura perché nel caso fosse indisponibile non sarebbe più possibile decifrare i messaggi che la Banca ha criptato con quel certificato.

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;*
- *n.1 certificato di cifratura con lunghezza della chiave a 2048 bit e conforme allo standard RFC5280.*

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

- *n.1 certificato di autenticazione. NOTA: La postazione client deve presentare al server della Banca il certificato di autenticazione seguito dai certificati root delle eventuali CA intermedie*[6] *(cd. Catena di trust)* [R09].

[6] The Transport Layer Security (TLS) Protocol - Version 1.2- https://tools.ietf.org/html/rfc5246#section-7.4.2 . certificate_list.
This is a sequence (chain) of certificates. The sender's certificate MUST come first in the list. Each following certificate MUST directly certify the one preceding it. Because certificate validation requires that root keys be distributed independently, the self-signed certificate that specifies the root certificate authority MAY be omitted from the chain, under the assumption that the remote end must already possess it in order to validate it in any case.
The same message type and structure will be used for the client's response to a certificate request message.

- *n.1 certificato di cifratura con lunghezza della chiave a 2048 bit e conforme allo standard RFC5280*.

2.7.1 Certificato di Banca con cui validare le connessioni ssl

Il certificato con cui validare la connessione SSL con i server della Banca d'Italia può essere acquisito mediante la seguente URL:

https://www.actalis.it/documenti-it/actalis_server_authentication_rootca.zip

Tale certificato deve essere installato su tutte le postazioni client che gestiscono l'handshake SSL con i server della Banca.

2.7.2 Chiave pubblica di cifratura della Banca

La chiave pubblica di cifratura della Banca, che le controparti dovranno usare per cifrare i dati destinati alla Banca d'Italia, può essere acquisita da un apposito link presente nella home page del Portale ABACO.

2.8 Riferimenti

2.8.1 Norme tecniche

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		Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – IETF RFC 5280	N/A	05/2008
R04		OCSP – IETF RFC 6960	N/A	06/2013
R05		Electronic Signatures and Infrastructures; Signature verification procedures and policies – ETSI TS 102 853	1.1.1	07/2012
R06		XAdES Baseline profiles – ETSI TS 103 171	2.1.1	03/2012
R07		CAdES Baseline profiles – ETSI TS 103 173	2.2.1	04/2013
R08	Cifratura	Cryptographic Message Syntax (CMS) – IETF RFC 3852		07/2004
R09	TSL	The Transport Layer Security (TLS) Protocol - Version 1.2- RFC 5246 – https://tools.ietf.org/html/rfc5246#section-7.4.2	1.2	08/2008