Nuova modalità di scambio delle chiavi SITRAD

(Sistema per la trasmissione telematica di dati)

Introduzione

Dal 10 settembre 2013 il nuovo sistema per lo scambio delle chiavi SITRAD, disciplinato dalla lettera circolare emanata dall'ABI con protocollo USP/002503 dell'8 novembre 2012, ha sostituito la precedente modalità cartacea, che potrà essere utilizzata esclusivamente in circostanze eccezionali.

Questa guida descrive le modalità operative con cui la Banca d'Italia ha recepito la normativa ABI, con riferimento, in particolare, all'Allegato 1 ("Modalità di scambio delle chiavi tra gli utenti del SITRAD") della citata lettera.

Questo documento non ha pretese di esaustività e si pone semplicemente l'obiettivo di fornire precisazioni su alcuni punti specifici della predetta normativa, al fine di rendere chiari gli adempimenti in carico agli aderenti e le scelte operative della Banca d'Italia nei casi in cui viene lasciata libertà di azione ai soggetti coinvolti.

Presupposti

Nella sezione 2 vengono definiti i presupposti per l'utilizzo di tale procedura. In sostanza gli aderenti si devono dotare autonomamente di una casella PEC e di due certificati elettronici: uno per la firma digitale e uno per la cifratura.

Analizziamo nel dettaglio tale sezione:

2. Presupposti

Controparti e fiduciari

Ogni controparte designa due o più fiduciari, persone univocamente identificate e responsabili del trattamento delle chiavi, per l'invio o la ricezione[2].

Ciascuna controparte deve disporre di una o più caselle PEC (Posta Elettronica Certificata) rilasciate da uno dei gestori accreditati presso l' Agenzia per l'It[illegible]Digitale (ex DigitPA)[3] personali o funzionali.

La PEC è un servizio per lo scambio di messaggi tramite la rete Internet, molto simile alla normale posta elettronica, ma disciplinata da precise disposizioni legislative che le fanno assumere rilevanza legale. Wikipedia ne fornisce la seguente definizione:

"La posta elettronica certificata (PEC) è una tipologia particolare di posta elettronica, disciplinata dalla legge italiana, che permette di dare a un messaggio di posta elettronica lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale garantendo così il non ripudio. Anche il contenuto può essere certificato e firmato elettronicamente oppure criptato garantendo quindi anche autenticazione, integrità dei dati e confidenzialità."

Per ulteriori riferimenti, vedere http://it.wikipedia.org/wiki/Posta_elettronica_certificata

In altre parole, gli aderenti devono necessariamente acquisire, prima di utilizzare questo servizio, una casella PEC da uno dei fornitori disponibili. Come specificato nella nota 3 del documento, la lista dei soggetti a cui potersi rivolgere è indicata all'indirizzo

http://www.digitpa.gov.it/pec_elenco_gestori

Per la Banca d'Italia è possibile utilizzare lo stesso indirizzo PEC per più fiduciari della stessa controparte.

In aggiunta, gli aderenti devono dotarsi di un certificato per la Firma Digitale e di un altro certificato per la cifratura dei dati.

Con certificato di Firma digitale si intende un insieme di dati in forma elettronica utilizzati come metodo di identificazione informatica e basati su un certificato qualificato e su un sistema di chiavi crittografiche. Consente al titolare della firma stessa di rendere manifesta la provenienza e l'integrità di uno o più documenti informatici.

I fornitori di tale servizio sono elencati all'indirizzo :

http://www.digitpa.gov.it/firma-digitale/certificatori-accreditati/certificatori-attivi

Ciascun fiduciario deve disporre di un certificato di Firma Digitale rilasciato da uno dei gestori accreditati DigitPA[4] e di un certificato di cifratura (cfr. Allegato 2).

Analogamente alla Firma Digitale, un certificato di cifratura è costituito da un insieme di dati in forma elettronica che permettono la crittografia di uno o più documenti informatici.

Di norma, i fornitori di certificati di Firma Digitale forniscono anche certificati di cifratura, ma esistono anche molte altre società che offrono tali servizi sul mercato.

Nell'Allegato 2 della lettera circolare dell'ABI sono riportate le specifiche tecniche delle due tipologie di certificati.

La sezione continua definendo i soggetti fiduciari coinvolti nel processo.

La chiave viene sempre scambiata in due parti separate e ciascun fiduciario è responsabile di una sola parte della stessa chiave[5]. Deve essere assegnato almeno un fiduciario per ciascuna parte di chiave. Ciascuna parte di chiave può avere più fiduciari.

[5] Eventuali deroghe possono essere concordate tra le controparti. L'invio avverrà comunque in forma separata, seguendo la normale procedura.

Banca d'Italia NON concederà deroghe in nessun caso.

La Banca d'Italia richiede quindi necessariamente un fiduciario per ogni parte della chiave.

Scambio della chiave

La sezione 3 descrive le modalità per lo scambio della chiave tra le controparti. Si richiama l'attenzione sui primi due capoversi di tale sezione.

> Ciascuna coppia di controparti si accorda per decidere chi prenderà l'iniziativa di generare e trasmettere la chiave. La controparte che assume l'iniziativa potrà cambiare a ogni successivo rinnovo della chiave. Al rinnovo, in assenza di accordi bilaterali specifici, la controparte che precedentemente ha assunto l'iniziativa ha il compito di attivare lo scambio della nuova chiave.
>
> La Banca d'Italia assume sempre l'iniziativa di generazione e trasmissione della chiave per le proprie controparti.

Si ribadisce, come indicato nella normativa, che dal 10 settembre 2013 la Banca d'Italia assume SEMPRE l'iniziativa per la trasmissione delle chiavi. Le banche che in precedenza avevano in essere l'alternanza di invio con la Banca d'Italia devono ritenere decaduta tale facoltà a partire dalla data suddetta.

Circa le modalità di comunicazione delle irregolarità e di conferma delle operazioni, si precisa che la Banca d'Italia utilizza esclusivamente il canale PEC.

> Irregolarità
>
> Se una controparte mittente o ricevente riscontra una qualsiasi irregolarità nella procedura di scambio o ritiene compromessa una chiave o una sua parte, deve comunicarlo all'altra controparte[10].
>
> [10] Preferenzialmente tramite lo stesso canale PEC.

Banca d'Italia richiede OBBLIGATORIAMENTE l'utilizzo della PEC.

Le comunicazioni vanno inviate all'indirizzo CHIAVI.SITRAD@Pec.bancaditalia.it

NOTA: le comunicazioni di irregolarità vanno inviate esclusivamente alla seguente casella PEC:

CHIAVI.SITRAD@Pec.bancaditalia.it

Tale indirizzo NON va confuso con la casella PEC che la Banca d'Italia utilizza per l'invio delle chiavi, ovvero:

ELI@Pec.bancaditalia.it

Per quel che riguarda la conferma di comunicazione, la Banca d'Italia NON richiede altre conferme oltre a quelle inviate dal sistema di Posta Elettronica Certificata (PEC).

In altre parole non è necessario inviare NESSUNA comunicazione per confermare il ricevimento delle chiavi.

Per Banca d'Italia è sufficiente la conferma di ricezione inviata automaticamente dallo strumento PEC.

Conferma

La controparte mittente considererà completato lo scambio chiavi quando saranno disponibili le ricevute in "forma completa" dell'avvenuta consegna, rilasciate dalla PEC, per ciascuna parte di chiave inviata.

La controparte ricevente considererà completato lo scambio chiavi quando non riscontrerà irregolarità nella ricezione di tutte le parti di chiave.

Rinnovo della chiave

A partire dall'entrata a regime del nuovo sistema, le chiavi di autenticazione saranno automaticamente rinnovate dalla Banca d'Italia ogni 6 mesi. Successivamente, al termine della fase di migrazione di tutte le controparti al nuovo sistema digitale, anche la chiave di crittografia seguirà lo stesso iter.

Rinnovo della chiave

Il rinnovo deve avvenire a intervalli ritenuti adeguati a garantire la sicurezza. Le chiavi di autenticazione devono comunque essere rinnovate a intervalli non superiori a sei mesi.

Banca d'Italia provvederà a rinnovare le chiavi di autenticazione ogni 6 mesi.

Comunicazioni

Per questa sezione si descrive in dettaglio il processo di comunicazione della designazione dei fiduciari e delle relative variazioni.

Ogni comunicazione ufficiale tra le controparti e i fiduciari dovrà essere inviata tramite PEC.

L'indirizzo da utilizzare per le comunicazioni con Banca d'Italia è sempre

CHIAVI.SITRAD@Pec.bancaditalia.it

Designazione dei fiduciari

La designazione di fiduciari e le relative variazioni (es. per cessazione dal servizio del precedente fiduciario) devono essere effettuate con una comunicazione riportante:

- Nome dell'istituto per il quale si svolge il ruolo di fiduciario.
- Codice identificativo dell'istituto indicato.
- Dati anagrafici del fiduciario.
- Codice fiscale del fiduciario, se disponibile.
- Indirizzo postale del fiduciario.
- Numero di telefono e di fax del fiduciario.
- *Specimen* di firma del fiduciario.
- Indirizzo della casella *e-mail* aziendale del fiduciario.
- Indirizzo della casella PEC utilizzata dal fiduciario.
- Certificato pubblico di cifratura del fiduciario, firmato digitalmente dal fiduciario stesso.
- Tipo della chiave di cui il fiduciario è responsabile[12].
- Identificativo della parte della chiave di cui il fiduciario è responsabile [13].

[12] Autenticazione o crittografia.

[13] A o B.

Per l'invio della comunicazione di Designazione del Fiduciario si consiglia l'utilizzo dell'Allegato 3 riportato nella normativa ABI di riferimento compilato in tutte le sue parti.

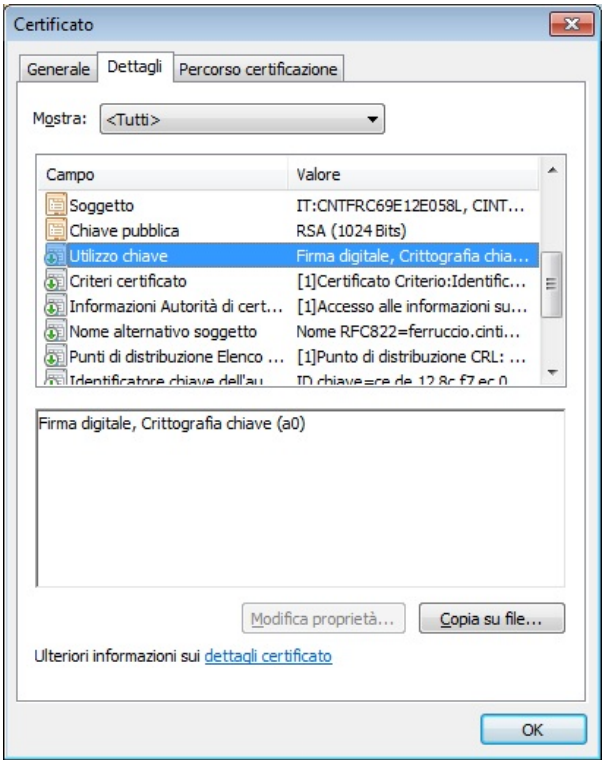
ATTENZIONE: Accertarsi che la Chiave Pubblica del certificato di cifratura riporti nei dettagli

UTILIZZO CHIAVE: Cifratura Dati e/o Cifratura Chiave

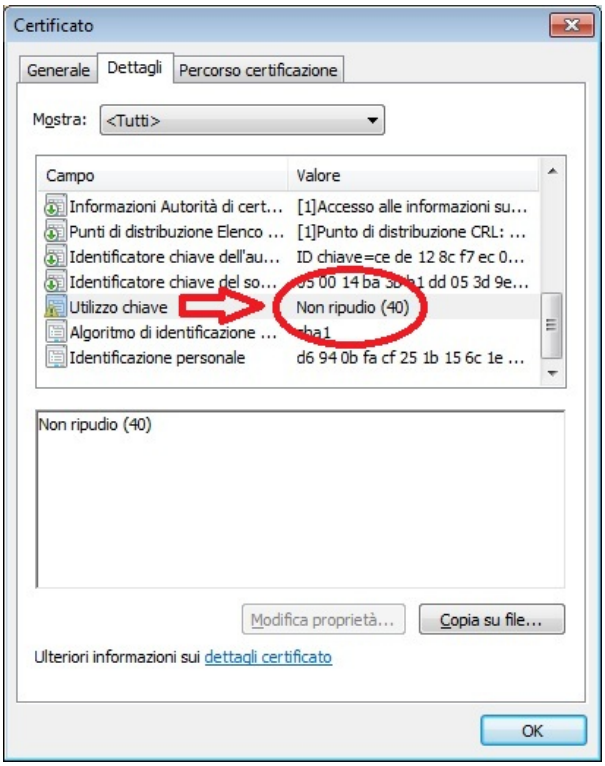
Da non confondere con il certificato di Firma Digitale che riporta invece

UTILIZZO CHIAVE: Non rifiuto

Per meglio specificare quanto evidenziato nell'ultimo BOX di colore Rosso, si riporta un esempio di Certificato Pubblico di Cifratura da inviare alla Banca d'Italia:



Il Certificato Pubblico di Cifratura non va confuso con il Certificato di Firma Digitale, che invece riporta nella scheda dettagli la seguente informazione (e quindi non è idoneo per la cifratura dei dati):

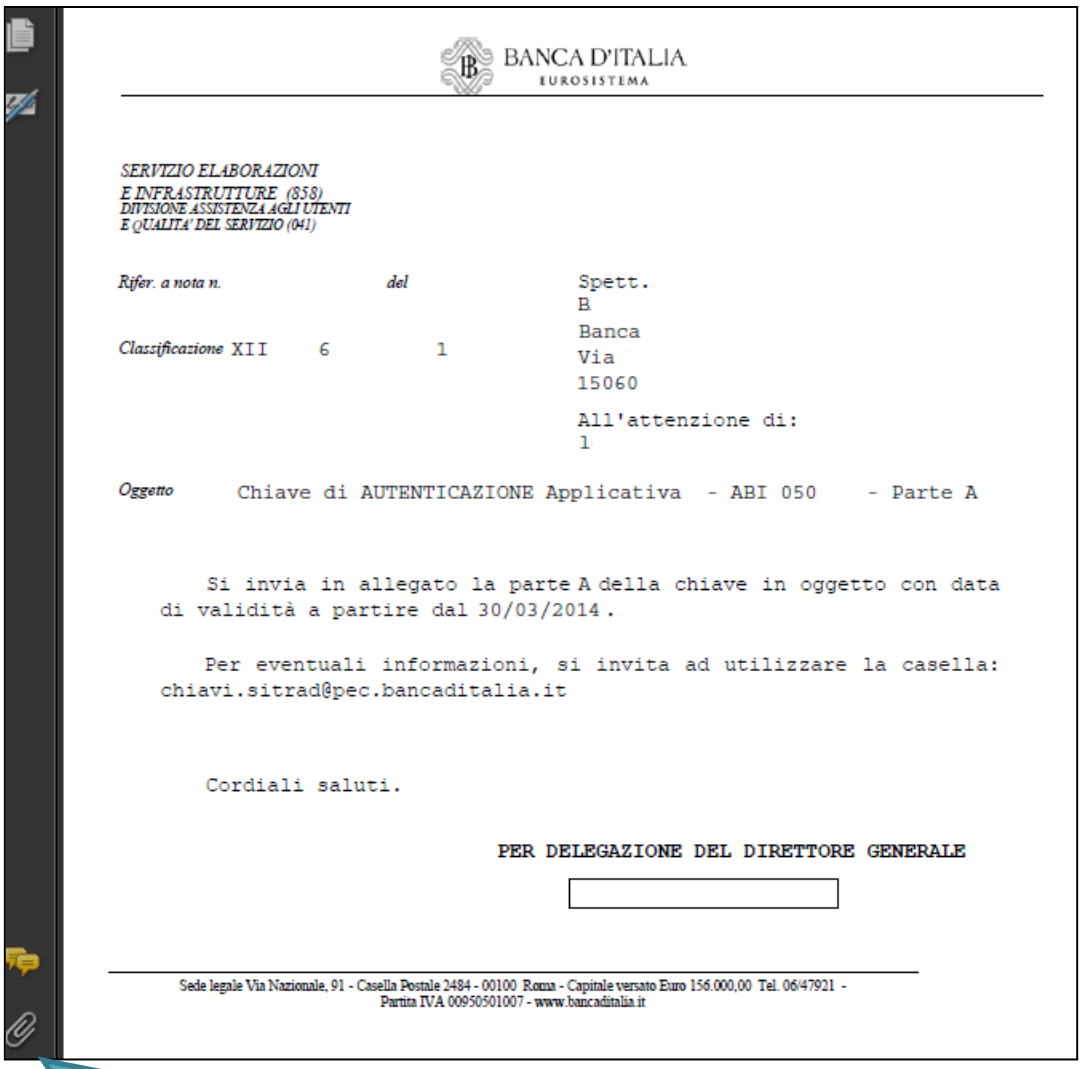


Formato dei file PDF trasmessi per PEC

In questa sezione si vuole dettagliare il formato dei file pdf che vengono trasmessi ai fiduciari designati dalle controparti e che contengono le informazioni sulle chiavi generate.

Per visualizzare il documento PDF ricevuto per PEC occorre aprirlo utilizzando il software Adobe Acrobat Reader

Ogni file PDF trasmesso al fiduciario designato ha, come allegato, un altro file pdf che contiene le informazioni sulla chiave generata e che è cifrato con il certificato pubblico del fiduciario.



BANCA D'ITALIA
EUROSISTEMA

SERVIZIO ELABORAZIONI
E INFRASTRUTTURE (858)
DIVISIONE ASSISTENZA AGLI UTENTI
E QUALITA' DEL SERVIZIO (041)

Rifer. a nota n. *del*

Spett.
B
Banca
Via
15060

Classificazione XII 6 1

All'attenzione di:
1

Oggetto Chiave di AUTENTICAZIONE Applicativa - ABI 050 - Parte A

Si invia in allegato la parte A della chiave in oggetto con data di validità a partire dal 30/03/2014 .

Per eventuali informazioni, si invita ad utilizzare la casella: chiavi.sitrad@pec.bancaditalia.it

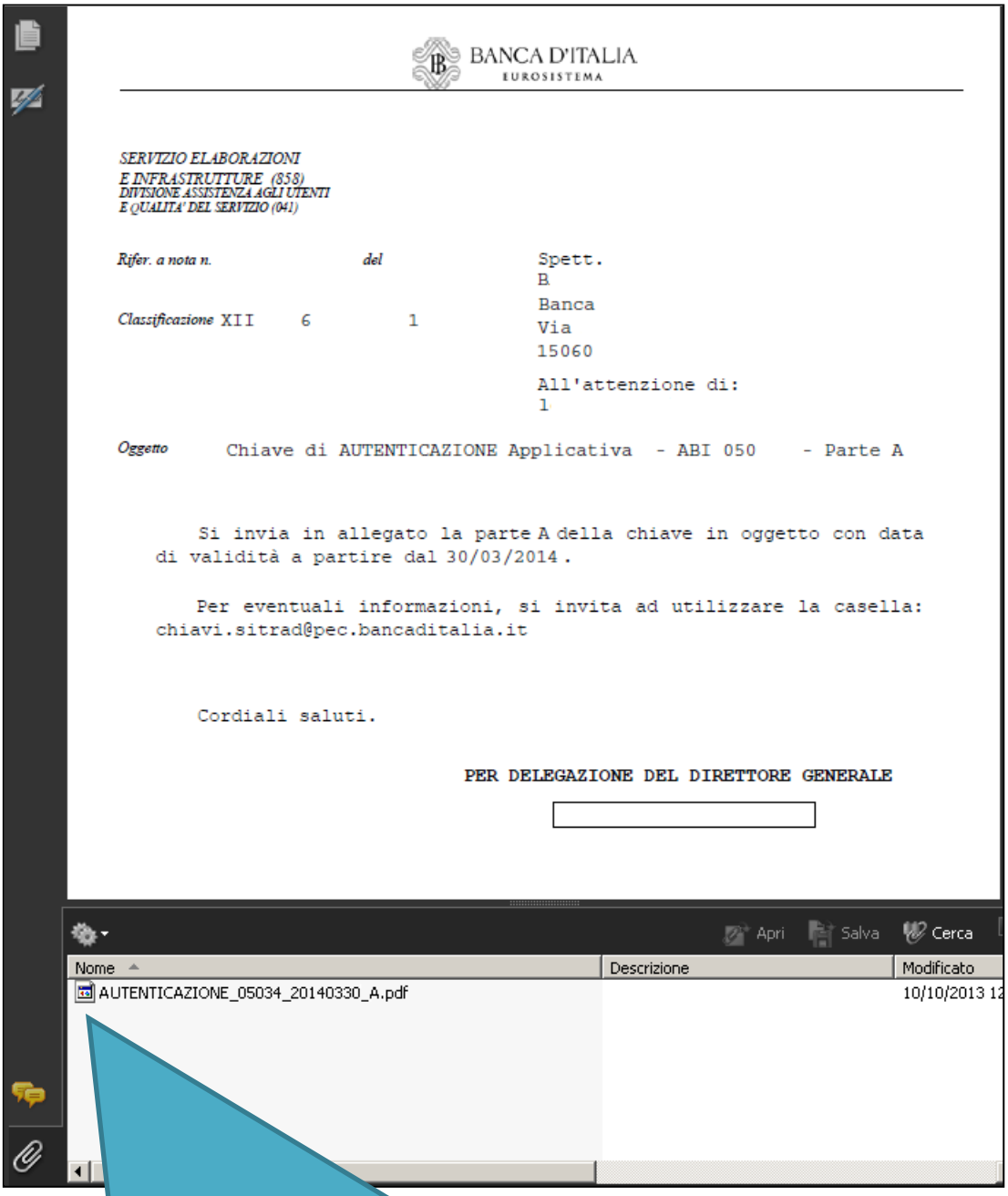
Cordiali saluti.

PER DELEGAZIONE DEL DIRETTORE GENERALE

Sede legale Via Nazionale, 91 - Casella Postale 2484 - 00100 Roma - Capitale versato Euro 156.000,00 Tel. 06/47921 -
Partita IVA 00950501007 - www.bancaditalia.it

Per visualizzare il documento pdf allegato basta cliccare sull'icona rappresentante una graffetta che è localizzata qui in basso a sinistra sulla pagina del reader.

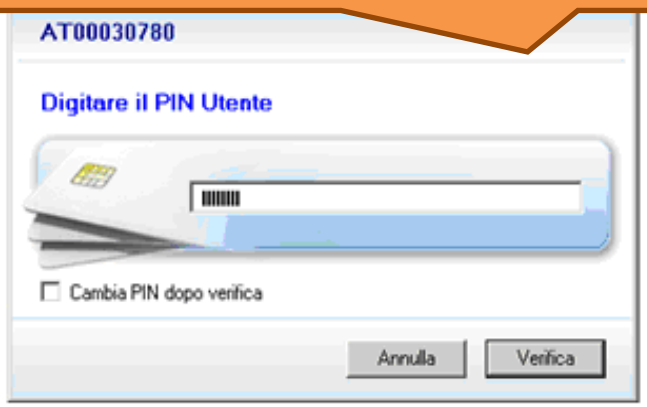
Nella parte bassa della finestra viene quindi data evidenza della presenza di un documento allegato che può essere visualizzato cliccando sul nome del file:



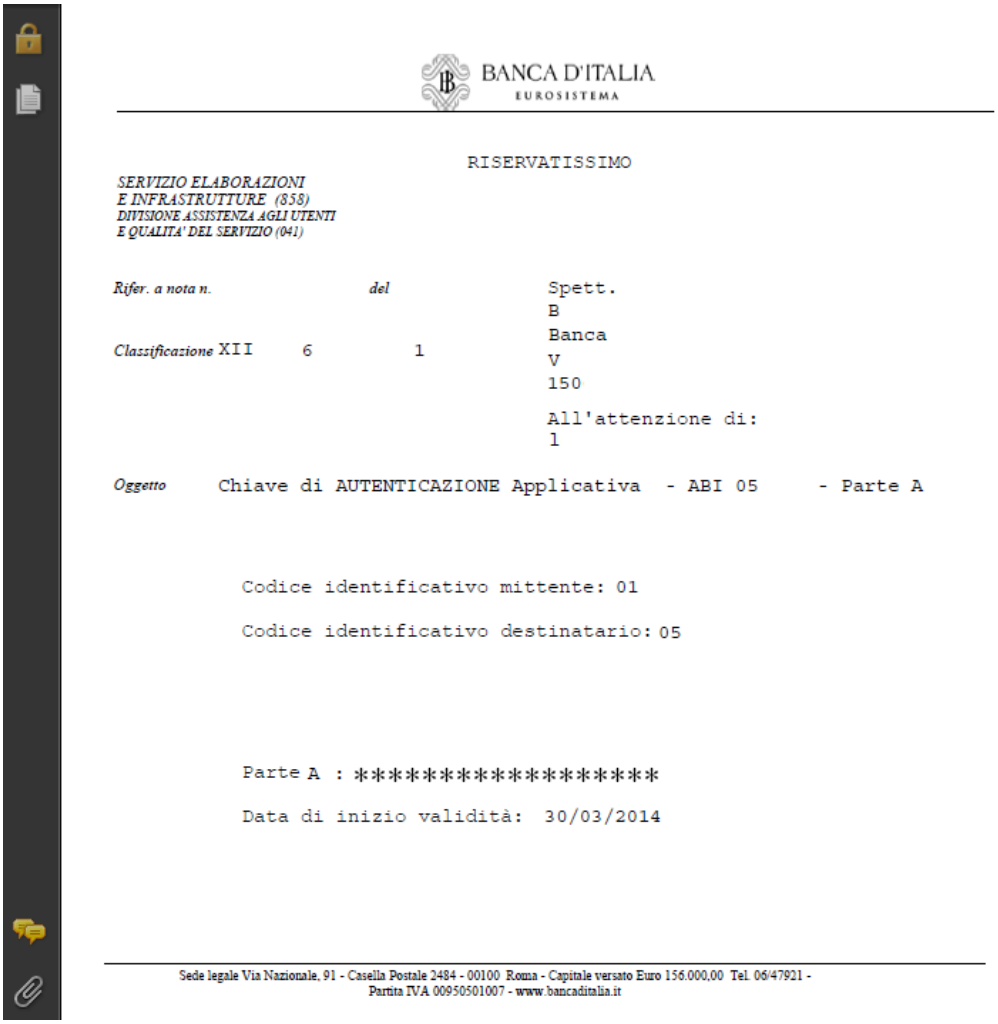
Il nome del pdf cifrato è conforme al seguente formato :

[Tipologia della chiave]_[Codice identificativo_destinatario]_[Data di validità della chiave]_[Parte della Chiave].pdf

Poiché l'allegato è un documento PDF cifrato, occorre inserire la smart card nel lettore per poterlo visualizzare. Viene quindi richiesto il codice pin della smart card



Se l'autenticazione va a buon fine, viene mostrato il documento in chiaro e il fiduciario può prendere visione della chiave che è stata generata.



BANCA D'ITALIA
EUROSISTEMA

RISERVATISSIMO

SERVIZIO ELABORAZIONI
E INFRASTRUTTURE (858)
DIVISIONE ASSISTENZA AGLI UTENTI
E QUALITA' DEL SERVIZIO (041)

Rifer. a nota n. *del*

Classificazione XII 6 1

Spett.
B
Banca
V
150

All'attenzione di:
l

Oggetto Chiave di AUTENTICAZIONE Applicativa - ABI 05 - Parte A

Codice identificativo mittente: 01

Codice identificativo destinatario: 05

Parte A : **********

Data di inizio validità: 30/03/2014