ABI Associazione Bancaria Italiana

Roma
8 novembre 2012
Prot. USP/002503

Alle aziende aderenti al SITRAD

Loro Sedi

Revisione delle modalità di scambio delle chiavi del Sistema per la trasmissione telematica di dati (SITRAD)

Con lettera circolare USP/ULG 002193 del 3 ottobre 2012 questa Associazione preavvisava di modifiche alla procedura e normativa di scambio delle chiavi di crittografia e autenticazione nel Sistema per la Trasmissione telematica di Dati (SITRAD).

Lo scambio delle chiavi di autenticazione tra gli utenti del Sistema per la trasmissione telematica di dati (SITRAD) avviene attualmente con modalità manuali formalizzate, sulla base della normativa ABI risalente al 1986.

Nel corso del 2011, su iniziativa della Banca d'Italia, sono state avviate in sede CIPA le attività volte a rinnovare il processo di trasmissione delle chiavi di autenticazione e di crittografia, con l'obiettivo di semplificare e dematerializzare la procedura, contenere i costi e rafforzare i presidi di sicurezza, senza alcun impatto sulle applicazioni.

Il Comitato direttivo della CIPA, nella riunione del 9 maggio 2012, ha approvato la proposta formulata dal gruppo di lavoro CIPA costituito sulla materia, che individua nell'utilizzo della Posta Elettronica Certificata (PEC)[1] la modalità ritenuta al momento più idonea per consentire la trasmissione telematica delle chiavi firmate digitalmente e crittografate con certificati digitali PKI.

In sostituzione quindi dell'attuale modalità cartacea, le aziende aderenti al SITRAD sono chiamate a migrare speditamente verso la nuova modalità di trasmissione telematica,

[1] L'attuale quadro legislativo definisce la PEC come un sistema che consente di inviare e-mail con valore legale equiparato a una raccomandata con ricevuta di ritorno e con relativa attestazione dell'orario esatto di spedizione.

sede legale: 00186 Roma | Piazza del Gesù, 49 | tel. +39.06.67671 | fax +39.06.6767457 | abi@abi.it
uffici: 20123 Milano | Via Olona, 2 | tel. +39.02.721011 | fax +39.02.72101239
B-1000 Bruxelles | Square De Meeus, 38/40 | tel. +32(0) 2.401.6182 | fax +32(0) 2.401.6868

dotandosi degli strumenti tecnici necessari. La modalità di trasmissione cartacea potrà continuare a essere utilizzata in circostanze eccezionali come indicato nella normativa..

La nuova normativa di riferimento, predisposta nell'ambito del citato gruppo di lavoro CIPA, descrive nell'allegato 1 le modalità per l'attuazione della trasmissione telematica attraverso il ricorso alla PEC con l'utilizzo della firma digitale e della cifratura, sulla base dei parametri tecnici riportati nell'allegato 2.

Il nuovo sistema di scambio delle chiavi SITRAD entra in vigore il 10 dicembre 2012.

Da tale data, le aziende aderenti al SITRAD potranno avviare, previo accordo, lo scambio delle chiavi secondo la nuova procedura.

A nove mesi dall'avvio (10 settembre 2013), il nuovo sistema sostituirà completamente l'attuale modalità cartacea di scambio chiavi, che pertanto non potrà più essere utilizzata, fatte salve le ipotesi di "contingency"di cui all'allegato 1.

Nel restare a disposizione per ogni ulteriore necessità e/o supporto, si porgono cordiali saluti.

Giovanni Sabatini
Direttore Generale

ALLEGATI

Allegato 1. Modalità di scambio delle chiavi tra gli utenti del SITRAD

1. Generalità

Le chiavi applicative bilaterali (d'ora in poi, "chiave") devono essere scambiate tra gli utenti[1] del SITRAD che utilizzano applicazioni richiedenti tali chiavi.

Le chiavi di autenticazione sono richieste dalla maggior parte delle applicazioni che si avvalgono del SITRAD (es. procedure riguardanti il sistema dei pagamenti); sono formate da otto caratteri decimali.

Le chiavi di crittografia sono richieste dalle applicazioni i cui messaggi/flussi devono essere trasmessi in forma crittografata (es. applicazioni della Banca d'Italia concernenti la Centrale dei Rischi e le Aste telematiche dei Titoli di Stato); sono formate da sedici caratteri esadecimali.

Ogni coppia di utenti SITRAD (d'ora in poi, "controparti") si scambierà una chiave da utilizzare sia in trasmissione sia in ricezione.

Ogni chiave è accompagnata dalla data d'inizio di validità, a partire dalla quale la chiave deve essere utilizzata.

La presente normativa regola le modalità di scambio delle chiavi tra le controparti che ne fanno uso, definendone i presidi tecnici (es. firma digitale e cifratura). Le chiavi SITRAD oggetto dello scambio, utilizzate a livello applicativo per autenticazione e crittografia, non subiscono alcuna modifica.

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'Italia Digitale (ex DigitPA)[3], personali o funzionali.

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).

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.

---

[1] Es. banche, intermediari finanziari, IMEL, istituti di pagamento, operatori in titoli, Centri Applicativi.

[2] I fiduciari possono appartenere a organizzazioni diverse dalla controparte (es.: capogruppo o società strumentale per banche/intermediari finanziari del gruppo; centri consortili; centri servizi).

[3] http://www.digitpa.gov.it/pec_elenco_gestori.

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

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

3. Scambio della chiave

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.

Trasmissione

La controparte che assume l'iniziativa procede alla spedizione della chiave, secondo le seguenti modalità:

1. La chiave è suddivisa in due parti di uguale lunghezza, denominate A e B.
2. Viene predisposto un documento elettronico (cfr. Allegato 2) per ciascuna parte di chiave, contenente almeno le seguenti informazioni:
   - Codice identificativo[6] della controparte mittente.
   - Codice identificativo della controparte destinataria.
   - Tipo della chiave[7].
   - Identificativo della parte della chiave[8].
   - Parte della chiave.
   - Data di inizio validità della chiave (in formato `GG/MM/AAAA`).
3. Ciascun documento è firmato digitalmente dal fiduciario mittente e la rispettiva parte di chiave è cifrata con i certificati pubblici di cifratura dei fiduciari destinatari[9].
4. Ciascun documento così predisposto è inviato ai fiduciari destinatari tramite Posta Elettronica Certificata, alle caselle segnalate dalla controparte ricevente.

Ricezione

La controparte garantisce che i fiduciari incaricati presidino le caselle PEC per la puntuale ricezione delle chiavi.

La controparte che riceve la chiave controlla la completezza e l'integrità della ricezione. Precisamente, ogni fiduciario deve:

1. Verificare l'integrità del documento ricevuto.
2. Decifrare il documento ricevuto.
3. Verificare la presenza e la corrispondenza della Firma Digitale del fiduciario mittente, la validità del suo certificato pubblico di firma e la validità della Firma Digitale apposta.
4. Verificare la leggibilità della comunicazione e la conformità della parte di chiave al formato atteso.

---

[6] Codice meccanografico (cosiddetto codice ABI).

[7] Autenticazione o crittografia.

[8] A o B.

[9] La controparte mittente deve verificare la validità della firma digitale apposta sul certificato pubblico di cifratura di ciascun fiduciario destinatario, comunicato con la procedura iniziale di designazione.

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]. La controparte che ha assunto l'iniziativa dovrà procedere all'invio di una nuova chiave seguendo la normale procedura.

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.

3. 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.

Per disciplinare le attività tecniche e amministrative connesse con la gestione delle chiavi, la validità della nuova chiave deve decorrere dalle ore 00:01 (mezzanotte e un minuto) di una qualsiasi domenica del mese.

Per permettere il regolare svolgimento delle attività di sostituzione delle chiavi, la procedura di rinnovo deve essere avviata almeno 15 giorni lavorativi prima della data d'inizio di validità delle nuove chiavi.

4. Comunicazioni

Ogni comunicazione ufficiale tra le controparti e i fiduciari[11] dovrà essere inviata tramite PEC.

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].

---

[10] Preferenzialmente tramite lo stesso canale PEC.

[11] Es. accreditamento iniziale, cessazione di un fiduciario, rinnovo di un certificato.

- Identificativo della parte della chiave di cui il fiduciario è responsabile[13].

A titolo esemplificativo, l'Allegato 3 riporta uno schema per la designazione/cessazione del fiduciario, con le informazioni necessarie allo scambio chiavi (tranne il certificato pubblico di cifratura, che il fiduciario dovrà inviare separatamente).

La comunicazione di designazione/cessazione deve essere firmata dal rappresentante della controparte[14] e deve essere inviata a tutti i fiduciari delle controparti con cui si intrattengono rapporti.

Questa comunicazione non è necessaria per i fiduciari già accreditati alla data di decorrenza della presente normativa, che comunque dovranno comunicare alle controparti le informazioni tecniche necessarie all'avvio della nuova procedura (es. indirizzo PEC, certificato pubblico di cifratura).

5. *Contingency*

Nel caso in cui la procedura normale non sia completabile dalle controparti a causa di eventi eccezionali, sono ammesse modalità alternative per garantire la continuità operativa delle chiavi applicative, solo previo accordo tra le controparti.

Indipendentemente dalla modalità adottata, la controparte ricevente deve dare espressa conferma del completamento dello scambio come concordato dalle controparti.

Al decadere delle condizioni di eccezionalità che hanno impedito lo svolgimento della normale procedura di scambio chiavi, la chiave vigente deve essere rinnovata con la procedura normale.

Invalidità dei certificati di firma o cifratura

In caso d'invalidità del certificato di firma del fiduciario mittente o di quello di cifratura del fiduciario destinatario, dopo le verifiche del caso, la procedura d'invio della chiave potrà avvenire in modalità cartacea.

Indisponibilità della Posta Elettronica Certificata

In caso d'indisponibilità della casella di Posta Elettronica Certificata di uno dei fiduciari, potrà essere utilizzata in sostituzione temporanea la sua casella *e-mail* aziendale.

Indisponibilità del canale telematico

In caso d'indisponibilità di una connessione a Internet, la procedura d'invio della chiave potrà avvenire in modalità cartacea.

Condizioni eccezionali

In caso in cui la durata delle condizioni eccezionali sia limitata nel tempo[15] e prevedibile, si potrà richiedere un prolungamento della validità della chiave vigente.

Modalità cartacea

La procedura cartacea di scambio chiavi sostituisce la normale procedura di trasmissione e ricezione nei casi eccezionali già indicati[16].

---

[12] Autenticazione o crittografia.

[13] A o B.

[14] Il documento cartaceo, che riporta la firma autografa del fiduciario – necessaria in caso di *contingency* – dovrà essere digitalizzato e inviato via PEC.

[15] Indicativamente, non oltre cinque giorni lavorativi.

La controparte che assume l'iniziativa procede alla spedizione della chiave, secondo le seguenti modalità:

1. La chiave è suddivisa in due parti di uguale lunghezza, denominate A e B.
2. Viene predisposto un documento cartaceo per ciascuna parte di chiave, contenente le informazioni necessarie all'invio (cfr. par. "Trasmissione" - punto 2).
3. Ciascun documento è firmato dal fiduciario mittente con firma autografa e la rispettiva parte di chiave è chiusa in una busta sigillata[17].
4. Ciascun documento così predisposto è inviato ai fiduciari destinatari tramite corriere privato, assicurata convenzionale o altro mezzo concordato tra le parti.

La controparte che riceve la chiave controlla la completezza e l'integrità della ricezione. Precisamente, ogni fiduciario deve:

1. Verificare l'integrità del plico contenente la chiave e dei sigilli.
2. Estrarre dal plico il documento con la parte di chiave.
3. Verificare sul documento la presenza e la corrispondenza della firma autografa del fiduciario mittente.
4. Verificare la leggibilità del documento e della parte di chiave.
5. Confermare il completamento dello scambio come concordato dalle controparti

[16] La modalità cartacea di scambio chiavi riprende nella sostanza la normativa di scambio chiavi emessa con la lettera circolare ABI TL/VD II 004126 del 4 luglio 1986.

[17] Il contenuto della busta deve essere visibile solo aprendo la busta sigillata.

Allegato 2. Requisiti tecnici

All'avvio del rapporto di scambio chiavi, le controparti verificheranno l'interoperabilità degli strumenti tecnici di firma e cifratura necessari per la procedura di scambio.

Gli strumenti e gli standard di seguito riportati potranno essere oggetto di aggiornamento a seguito delle evoluzioni tecnologiche e dell'esperienza operativa maturata dagli utenti.

Firma Digitale

Il fiduciario che invia le chiavi deve disporre degli strumenti tecnici necessari per la Firma Digitale del documento elettronico di trasmissione delle chiavi stesse.

I requisiti tecnici della firma digitale sono stabiliti dalla Deliberazione CNIPA n. 45/2009 del 21 maggio 2009.

Cifratura

Il fiduciario che invia le chiavi deve disporre degli strumenti tecnici necessari per la cifratura di un file nelle buste crittografiche definite nei formati pkcs#7/CAdES, PAdES e XAdES, utilizzando la chiave pubblica associata al certificato pubblico di cifratura del destinatario.

Gli algoritmi di crittografia utilizzati nel processo di creazione del *file* cifrato sono AES-256-CBC per la cifratura simmetrica e RSA per la cifratura asimmetrica.

Il certificato pubblico di cifratura del destinatario dovrà essere reso disponibile alla controparte mittente nel formato conforme alla Deliberazione CNIPA n. 45/2009 (profilo X 509 V.3).

Documento elettronico

Il documento elettronico con le informazioni relative a ciascuna parte di chiave deve essere in formato PDF o testuale.

Spett.le

_____
(istituto)

Oggetto: Designazione e/o cessazione di un fiduciario per lo scambio chiavi SITRAD.

Il/la _____
(istituto)

con sede legale in _____
(stato) (città) (indirizzo)

codice identificativo (ABI o codice meccanografico): _____

rappresentat_ da: _____
(nome) (cognome) (qualifica)

☐ **comunica il nominativo e i dati del fiduciario autorizzato a effettuare le attività connesse con lo scambio delle chiavi applicative del SITRAD.**

Nome: _____ Cognome: _____

Luogo di nascita: _____ Data di nascita: ☐☐/☐☐/☐☐☐☐
(gg/mm/aaaa)

Codice fiscale (se disponibile): ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Indirizzo postale aziendale[1]: _____
(stato) (città) (indirizzo)

Telefono: _____ Fax: _____

Indirizzo e-mail personale aziendale: _____

Casella PEC per lo scambio chiavi: _____

Responsabilità della chiave di autenticazione: ☐ parte A o ☐ parte B

Responsabilità della chiave di crittografia: ☐ parte A o ☐ parte B
(barrare al più una casella per ciascuna chiave)

Data di decorrenza: ☐☐/☐☐/☐☐☐☐
(gg/mm/aaaa)

_____
(firma del fiduciario)

☐ **comunica la cessazione del fiduciario autorizzato a effettuare le attività connesse con lo scambio delle chiavi applicative del SITRAD.**

Nome: _____ Cognome: _____

Codice fiscale (se disponibile): ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Responsabilità della chiave di autenticazione: ☐ parte A o ☐ parte B

Responsabilità della chiave di crittografia: ☐ parte A o ☐ parte B
(barrare al più una casella per ciascuna chiave)

Data di decorrenza: ☐☐/☐☐/☐☐☐☐
(gg/mm/aaaa)

In fede.

_____, _____
(luogo) (data)

_____
(firma del rappresentante)

[1] L'indirizzo postale, il telefono, il fax, l'e-mail aziendale e lo *specimen* di firma potranno essere utilizzati nelle procedure di *contingency* dello scambio chiavi.