CONVENZIONE INTERBANCARIA
PER L'AUTOMAZIONE
(CIPA)

SISTEMA PER LA TRASMISSIONE TELEMATICA DI DATI

REQUISITI TECNICI, FUNZIONALI E DI SICUREZZA E STANDARD DI COLLOQUIO

Il presente documento riporta i requisiti tecnici, funzionali e di sicurezza delle infrastrutture e gli standard di colloquio del Sistema, previsti dall'art. 3 della "Convenzione per la partecipazione al Sistema per la trasmissione telematica di dati", nonché le modalità di istruttoria delle richieste che dovessero essere avanzate da soggetti interessati a svolgere, nell'ambito del Sistema, le funzioni di gestore di infrastrutture telematiche (art. 6 della Convenzione).

Maggio 2018

Ambito di applicazione

Infrastrutture telematiche che offrono supporto ad applicazioni e servizi rientranti nell'ambito della "Convenzione per la partecipazione al Sistema per la trasmissione telematica di dati".

Ferma restando la rispondenza alla normativa comunitaria e nazionale e alle indicazioni emanate dalle autorità competenti in materia di sicurezza delle informazioni e delle reti, continuità operativa, sicurezza nei servizi di pagamento, protezione dei dati personali[1], nonché l'aderenza ai principali standard internazionali e alle *best practices* in materia organizzativa e di sicurezza informatica, di seguito sono riportati i requisiti tecnici, funzionali e di sicurezza delle infrastrutture telematiche e gli standard di colloquio del Sistema.

Premessa

Le infrastrutture telematiche, costituite da componenti hardware, software, collegamenti e protocolli di comunicazione, consentono lo scambio in modo sicuro e affidabile di dati riguardanti l'attività bancaria e finanziaria tra i partecipanti al Sistema.

Esse implementano due strati di servizio sovrapposti:

- lo strato più basso implementa servizi di rete (es. *Internet Protocol* - IP);
- lo strato più alto, avvalendosi dei servizi dello strato sottostante, implementa servizi di trasporto e interoperabilità (es. scambio di messaggi o *file*).

Nell'ambito dei servizi di trasporto e interoperabilità, l'accesso degli utenti alle infrastrutture telematiche può avvenire in due modalità: "*application to application*" (A2A) e "*user to application*" (U2A).

Per accesso in modalità A2A si intende l'accesso degli utenti alle infrastrutture telematiche e lo scambio di dati come messaggi o *file* attraverso i servizi di trasporto e interoperabilità con due modalità di trasferimento: "*real-time*" e/o "*store-and-forward*".

Con i termini messaggio e *file* si intende una sequenza di *byte* con una lunghezza massima predefinita (il *file* ha valori più alti rispetto al messaggio), funzione della modalità di trasferimento utilizzata.

La modalità "*real-time*" si basa su un modello di interazione *query/response* tra mittente e destinatario entro un intervallo temporale limitato e predefinito scaduto il quale il mittente riceve una notifica che la propria richiesta non ha avuto esito dal destinatario.

La modalità "*store-and-forward*" si basa su un meccanismo di consegna dal mittente al destinatario che non richiede la contestuale connessione delle due parti, permettendo l'inizio della spedizione anche quando il destinatario non è disponibile. In tal caso, il servizio di trasferimento conserva i messaggi*/file* e provvede alla loro spedizione appena il destinatario è di nuovo disponibile.

Per accesso in modalità U2A si intende l'accesso da parte di una persona che utilizza un *browser* standard. Tale modalità è disponibile unicamente nel contesto di interfacce basate su HTML con protocollo HTTP(s) e non può essere utilizzata per alcun tipo di trasferimento dati in modalità "*application-to-application*".

[1] Es. direttiva UE 2016/1148 (NIS), Regolamento UE 2016/679 (GDPR), normativa emanata dall'EBA, Circolare della Banca d'Italia n. 285, Linee guida della Banca d'Italia in materia di continuità operativa delle infrastrutture di mercato.

I punti di accesso alle infrastrutture telematiche, costituiti da componenti hardware e software collocati presso gli utenti e collegati alle infrastrutture stesse, permettono di utilizzare i servizi di rete e i servizi di trasporto e interoperabilità.

Tali componenti definiscono il confine di responsabilità del gestore dell'infrastruttura telematica per i servizi offerti agli utenti.

REQUISITI TECNICI

A. **Architettura**

1. Rete di tipo "magliato" che, in caso di interruzione di un tratto di rete, consenta l'instradamento automatico del traffico su percorsi alternativi.
2. Applicazione del principio "*no single point of failure"*.
3. Flussi di traffico "protetti" [2] anche nel caso di utilizzo promiscuo di risorse di rete per altre finalità.
4. Architettura idonea all'erogazione di servizi *end-to-end*, da un punto di accesso a un qualsiasi altro punto di accesso della stessa rete, nonché da e verso altre reti interoperabili.
5. Ambienti di test e collaudo, per ogni tipologia di servizio, separati da quelli di produzione e con caratteristiche funzionali equivalenti in termini di componenti di sistema e di rete e di configurazione del software. Segregazione logica del traffico tra i diversi ambienti.
6. Sistema di segnalazione immediata della indisponibilità dei singoli punti di accesso agli utenti interessati.
7. Funzionalità, procedure e strumenti per assicurare i livelli di qualità del servizio concordati con gli utenti.
8. Presidi in grado di garantire la riservatezza e l'integrità di tutti i dati in transito tra gli utenti collegati all'infrastruttura telematica (es. tunnel IPSec VPN).

B. **Standard di colloquio – Protocolli di comunicazione**

1. Protocolli di comunicazione standard di mercato (es. famiglia TCP/IP – *Transmission Control Protocol/Internet Protocol*).

C. **Capacità trasmissiva**

1. Capacità trasmissiva commisurata ai livelli di traffico da supportare, tale da garantire la qualità del servizio stabilita contrattualmente con gli utenti.
2. Adeguamento tempestivo del dimensionamento della capacità trasmissiva in base al variare del fabbisogno (periodicamente stimato e aggiornato) e alle evoluzioni prevedibili (scalabilità), nonché ai risultati del monitoraggio continuo sull'utilizzo della rete di cui al punto F.

[2] attraverso l'applicazione di meccanismi crittografici a livello di protocollo (es. tunnel basati sullo standard IPSec).

REQUISITI FUNZIONALI

A. **Disponibilità**

1. Servizi di trasporto e interoperabilità disponibili in modalità A2A:
   - "*store-and-forward*" di messaggi con dimensione fino a 1 MB;
   - "*store-and-forward*" di *file* con dimensione fino a 250 MB;
   - "*real-time*" per messaggi con dimensione fino a 32 KB.
2. Operatività della rete assicurata per 24 ore per 7 giorni a settimana (24x7x365), con l'esclusione di finestre di manutenzione compatibili con i servizi offerti e preventivamente comunicate agli utenti.

B. **Continuità operativa**

1. Formalizzazione del piano di continuità operativa, comprensivo di piani di risposta e ripristino dei servizi in caso di incidente e/o disastro, in conformità alle "Linee guida in materia di continuità operativa delle infrastrutture di mercato", emanate dalla Banca d'Italia, e agli standard e migliori prassi internazionali (es. ISO/IEC 22301).
2. Formalizzazione di un documento di sintesi sulle misure di continuità operativa previste, comprensive dei livelli di servizio assicurati in caso di crisi e le soluzioni di continuità poste in atto dal fornitore di servizi.
3. Continuità operativa assicurata in modo trasparente agli utenti, cioè senza alcun intervento o impatto sulla configurazione tecnica degli utenti stessi. Comunicazione agli utenti interessati di eventuali cambiamenti intervenuti rispetto all'infrastruttura primaria, se ritenuti di potenziale impatto sull'operatività degli utenti medesimi.

C. **Interoperabilità**

1. Piena interoperabilità, sul piano funzionale, con le altre reti operanti nell'ambito del Sistema.

D. **Livelli di Servizio**

1. Definizione contrattuale dei livelli minimi di servizio garantiti (*Service Level Agreement* - SLA).
2. Disponibilità minima garantita per i servizi di trasporto e interoperabilità pari almeno al 99,98% sull'intera rete e al 99,75% sul punto di accesso in configurazione atta a garantire la continuità operativa calcolata su base semestrale, a meno delle finestre di manutenzione programmate e delle interruzioni riconducibili a responsabilità dell'utente.
3. Tempo di attraversamento dal punto di accesso del mittente al punto di accesso del destinatario, all'interno delle componenti di rete del gestore:
   - per il servizio "*real-time*":< 2 secondi nel 95% dei casi e < 10 secondi nel 100% dei casi;
   - per il servizio "*store-and-forward*" di messaggi:
     - per i messaggi a priorità elevata: < 30 secondi nel 95% dei casi e < 3 minuti nel 100% dei casi;
     - per i rimanenti messaggi: < 15 minuti;

- per il servizio "*store-and-forward*" di *file*: < 130 secondi per un *file* della dimensione di 1 megabyte con una sola sessione attiva.

4. Tempo massimo garantito di ripristino del servizio, in caso di interruzioni e/o degrado della qualità del servizio:

- 30 secondi sull'intera rete;
- 4 ore sul punto di accesso.

5. Tempo di attraversamento di un pacchetto IP di lunghezza pari a 512 byte da un punto di accesso alla rete a un altro punto di accesso della rete stessa, ovvero a un punto di interconnessione con altra rete (da misurare su un campione di 1.000 eventi):

200 millisecondi nel 95% dei casi

E. **Funzioni di servizio**

1. I servizi di trasporto e interoperabilità devono assicurare le seguenti funzionalità in relazione ai dati trattati:
   - garanzia di consegna al destinatario (modalità *store-and-forward*);
   - non duplicazione in fase di ritrasmissione;
   - garanzia dell'integrità dei dati (non modificabilità del "*payload*").
2. Conservazione e validazione nel tempo per un periodo minimo di 3 mesi di evidenze di scambio di messaggi/*file* (incluse le marche temporali apposte durante lo scambio).

F. **Monitoraggio delle risorse**

1. Monitoraggio delle risorse dell'infrastruttura telematica al fine di garantire una capacità trasmissiva adeguata ai livelli di traffico e una qualità del servizio corrispondente a quella stabilita contrattualmente con gli utenti.

G. **Gestione dei malfunzionamenti e degli incidenti di sicurezza informatica**

1. *Service Desk* contattabile 24 ore al giorno per 7 giorni a settimana, con personale in grado di attivare la procedura di *escalation.*
2. Sistema di *trouble ticketing* centralizzato in cui registrare tutte le azioni intraprese a seguito di un malfunzionamento e/o incidente, corredate dal *timestamp* (data e ora). Accessibilità del sistema da parte degli utenti e degli altri soggetti interessati.
3. Gestione dei malfunzionamenti e degli incidenti di sicurezza informatica in linea con le previsioni normative vigenti e successive modifiche e integrazioni e comunicazione tempestiva agli utenti interessati.

H. **Gestione dei cambiamenti**

1. Processo di gestione dei cambiamenti delle risorse ICT in linea con le previsioni normative vigenti e successive modifiche e integrazioni.

I. Reportistica e documentazione

1. Predisposizione di report periodici contenenti i dati di traffico, il livello dei servizi erogati, il dettaglio dei disservizi, dei malfunzionamenti e degli incidenti di sicurezza, i tempi di ripristino e il confronto con i livelli prefissati, da rendere disponibili, su richiesta, alla CIPA, all'ABI, a BANCOMAT S.p.A., nonché ai Centri Applicativi e agli utenti, fermi restando gli obblighi di segnalazione di malfunzionamenti e di incidenti nei confronti della Banca d'Italia o di altra autorità competente ai sensi della vigente normativa.
2. Documentazione relativa ai servizi offerti, da fornire agli utenti:

- accordi sui livelli di servizio, redatti in coerenza con gli indicatori definiti in questo documento;
- manuale operativo;
- manuale della procedura di *escalation*;
- guide utente per i servizi offerti, comprensive delle informazioni tecniche di dettaglio necessarie per utilizzare i servizi stessi.

REQUISITI DI SICUREZZA

A. Aspetti generali

1. Definizione della *policy* di sicurezza informatica in linea con le previsioni normative vigenti e successive modifiche e integrazioni.
   Verifica periodica e aggiornamento della *policy* e comunicazione della stessa al personale, agli utenti e agli altri soggetti interessati.
2. Predisposizione e aggiornamento di un inventario degli *asset* dell'infrastruttura telematica e loro classificazione in termini di riservatezza, integrità e disponibilità. Indicazione dei responsabili degli *asset*.
3. Processo di analisi del rischio informatico in linea con le previsioni normative vigenti e successive modifiche e integrazioni.

B. Sicurezza delle informazioni e delle risorse ICT

Sicurezza delle informazioni e delle risorse ICT in linea con le previsioni normative vigenti e successive modifiche e integrazioni.

In tale quadro si collocano i seguenti requisiti:

- <u>Riservatezza</u>

1. Crittografia del traffico scambiato sulla infrastruttura telematica mediante protocolli conformi ai recenti standard internazionali con l'impiego di algoritmi pubblici non deprecati e in linea con quanto prescritto da norme di legge.
2. Crittografia delle comunicazioni che comportano accesso remoto alle componenti di rete.
3. Uso di algoritmi di crittografia per le componenti di telecomunicazione (es. *firewall*, VPN) in linea con le raccomandazioni del *National Institute of Standards and Technology* (NIST) riguardanti le suddette componenti.
4. Presidi in grado di assicurare che ciascun utente possa accedere unicamente al traffico di competenza.

5. Divieto per il personale del gestore dell'infrastruttura telematica di accesso o copia dei dati in chiaro, salvo che tali attività siano oggetto di controlli d'accesso, registrazione e reportistica ai soggetti competenti.

- Integrità

1. Integrità delle componenti software che forniscono i servizi di trasporto e di sicurezza. Adozione di dispositivi *tamper resistant*, rilevazione tempestiva e automatica dei tentativi di manomissione e delle modifiche (intenzionali o accidentali) della configurazione dei dispositivi e segnalazione immediata ai soggetti interessati. Protezione contro codice malevolo.
2. Integrità dei dati veicolati sull'infrastruttura telematica mediante l'adozione di meccanismi di "sigillo" che ne rendano accertabile l'integrità stessa con utilizzo di algoritmi di *digest* robusti e non obsoleti (es. SHA 2).
3. Controllo dell'integrità di tutti gli *audit log* dell'infrastruttura telematica allo scopo di garantire la non modificabilità delle registrazioni in essi contenute.

- Autorizzazione

1. Autorizzazione delle connessioni di ogni utente e/o applicazione sulla base di una identità che determina i privilegi di accesso a dati/funzioni assegnati dalla procedura di autorizzazione. Identificazione univoca del personale coinvolto nella gestione degli *asset* e del personale e delle applicazioni degli utenti che utilizzano i servizi offerti.
2. Applicazione del principio del minimo privilegio per l'accesso a tutte le componenti della rete.
3. Accesso alle informazioni trattate dalla rete consentito ai soli utenti che dispongono delle necessarie abilitazioni.
4. Attribuzione differenziata delle abilitazioni di accesso in relazione agli specifici ruoli svolti.

- Autenticazione

1. Meccanismi sicuri per l'autenticazione del personale del gestore e dell'utente che accede agli *asset*, appropriati in relazione alla classificazione dei dati a cui consentono di accedere:
   a) in caso di '"autenticazione forte", meccanismi basati su più fattori e canali diversificati (es. OTP, certificati digitali, dispositivi di riconoscimento biometrico);
   b) in caso di autenticazione tramite *password*, controllo di qualità delle stesse, limitazione temporale della validità e loro trasmissione non in chiaro.
2. Meccanismi di autenticazione dei messaggi/flussi applicativi.
3. Mutua autenticazione tra tutte le componenti di sicurezza (es. *encryptors*).

- *Auditability*

1. Funzionalità di registrazione (*logging*) in tutti i dispositivi di rete e di crittografia.
2. *Logging* delle sessioni stabilite tra gli utenti e l'infrastruttura telematica, dei cambiamenti operati sulle componenti dell'infrastruttura, degli attacchi informatici e delle violazioni

derivanti da alterazioni e accessi non autorizzati; protezione dei relativi *file* di *log* e conservazione per un periodo non inferiore a 24 mesi.

- Monitoraggio di sicurezza

1. Monitoraggio continuativo e capacità di correlazione e analisi degli eventi di sicurezza (tentativi di attacco, minacce e vulnerabilità) specificatamente rivolte al settore finanziario, anche in collaborazione con il CERT Finanziario Italiano (CERTFin) e con fornitori di servizi di analisi e *threat intelligence*.
2. Gestione accentrata degli *alert* per i tentativi di effrazione degli apparati contenenti quantità di sicurezza.

- Verifiche di conformità

1. Verifica periodica della conformità dei sistemi e delle procedure di trattamento dei dati alla *policy* definita e agli standard di riferimento.

MODALITÀ DI ISTRUTTORIA DELLE RICHIESTE DI SOGGETTI INTERESSATI A SVOLGERE LE FUNZIONI DI GESTORE DI INFRASTRUTTURE TELEMATICHE

I requisiti previsti dall'art. 6 della Convenzione per i soggetti interessati a svolgere, nell'ambito del "Sistema per la trasmissione telematica di dati", le funzioni di gestori delle infrastrutture telematiche sono:

a) società aventi un capitale sociale non inferiore a 10 milioni di euro;

b) offerta, da almeno due anni, di servizi telematici per la trasmissione di dati;

c) conformità di procedure e processi operativi a standard di qualità e di sicurezza riconosciuti a livello internazionale.

* * *

La verifica del possesso dei suddetti requisiti verrà effettuata attraverso l'esame della seguente documentazione, che dovrà essere presentata dal soggetto richiedente:

a) statuto della società e, per le società aventi sede in Italia, certificato di vigenza rilasciato dal Registro delle Imprese e, per quelle aventi sede all'estero, analogo documento rilasciato dalle competenti autorità del paese di origine;

b) dichiarazione firmata dal legale rappresentante della società, contenente la descrizione dei servizi telematici per la trasmissione di dati offerti e la data da cui ha avuto inizio lo svolgimento di tali servizi, il numero e le tipologie degli utenti collegati, il traffico trasportato annualmente;

c) documento sul sistema di *compliance* aziendale per la conformità alle leggi e ai regolamenti, per il mantenimento delle certificazioni aziendali e l'aggiornamento del modello di organizzazione e gestione aziendale ex d.lgs. n. 231/2001;

d) certificazioni, rilasciate dai competenti organismi, attestanti la conformità delle procedure e dei processi operativi della società, connessi con la fornitura di servizi telematici, agli standard internazionali ISO/IEC 22301:2012 (sistema di *business continuity*) e ISO/IEC 27001:2013 (sistema di gestione della sicurezza delle informazioni) e successive modifiche

oppure

e) documento, redatto da *auditors* esterni, contenente i risultati di *assessment* in materia di qualità e sicurezza delle procedure e dei processi operativi della società, connessi con la fornitura di servizi telematici per la trasmissione di dati, effettuato sulla base delle indicazioni formulate da organismi internazionali specializzati nel settore (es. ISAE 3000 report).

Per quanto attiene ai requisiti tecnico-funzionali e di sicurezza delle infrastrutture e agli standard di colloquio del Sistema, dovrà essere presentata idonea documentazione tecnica atta a dimostrare il rispetto di quanto stabilito nelle pagine precedenti.

* * *

I soggetti interessati a svolgere, nell'ambito del Sistema, le funzioni di gestore di infrastrutture telematiche devono inoltrare apposita istanza, corredata della prescritta documentazione, alla Segreteria Tecnica della CIPA (c/o Banca d'Italia – Dipartimento Informatica – Servizio Sviluppo informatico – Via Nazionale, 91 – 00184 Roma).

L'istanza di ammissione, previa istruttoria da parte della Segreteria Tecnica, è sottoposta al Comitato direttivo della CIPA, che delibera in proposito. L'eventuale non accoglimento dell'istanza, adeguatamente motivato, viene comunicato per iscritto, a cura della Segreteria Tecnica entro trenta giorni dalla data della relativa delibera, al soggetto richiedente. Quest'ultimo può chiedere un riesame della decisione da parte dell'Assemblea della CIPA.

Il soggetto ammesso a operare nel Sistema in qualità di gestore di infrastrutture telematiche è tenuto a fornire alla Segreteria Tecnica della CIPA, a cadenza triennale, una dichiarazione attestante la permanenza dei requisiti inizialmente richiesti ovvero le eventuali variazioni intervenute.

L'ammissione può essere revocata, con delibera del Comitato direttivo della CIPA, in caso di sopravvenuta mancanza di uno o più dei requisiti inizialmente richiesti. La revoca viene comunicata per iscritto, a cura della Segreteria Tecnica entro trenta giorni dalla data della relativa delibera, al soggetto interessato. Quest'ultimo può chiedere un riesame della decisione da parte dell'Assemblea della CIPA

Il soggetto operante nel Sistema in qualità di gestore di infrastrutture telematiche può rinunciare all'espletamento del servizio, dandone comunicazione scritta alla Segreteria Tecnica della CIPA e agli utenti interessati con un preavviso non inferiore a dodici mesi.

L'elenco dei soggetti ammessi a operare nel Sistema in qualità di gestori di infrastrutture telematiche è pubblicato sul sito Internet della CIPA (www.cipa.it).