

**CONVENZIONE INTERBANCARIA  
PER I PROBLEMI DELL'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. 5 della Convenzione).

**Maggio 2004**

# REQUISITI TECNICI, FUNZIONALI E DI SICUREZZA E STANDARD DI COLLOQUIO

## 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".

## Requisiti

Ferma restando la rispondenza alla normativa comunitaria e nazionale e alle indicazioni emanate dalle autorità competenti, 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.

## 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. Ridondanza dei dispositivi centrali e di rete (compresi i dispositivi dei sistemi di gestione e monitoraggio) realizzata con apparati di riserva in hot stand by, in grado di attivarsi automaticamente quando il dispositivo primario si renda indisponibile.
3. Disponibilità di linee di accesso alla rete affiancate da linee di riserva, stese su percorsi differenziati, con caratteristiche identiche alle linee primarie e disponibili all'impiego, in automatico, in caso di indisponibilità di queste ultime.
4. Eliminazione dall'infrastruttura di single-point-of-failure e comunicazione preventiva agli utenti di potenziali single-point-of-failure residui.
5. Flussi di traffico "protetti"<sup>1</sup> anche nel caso di utilizzo promiscuo di risorse di rete per altre finalità.
6. 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.
7. Disponibilità di ambienti di test e collaudo, per ogni tipologia di servizio, separati da quelli di produzione e con caratteristiche equivalenti in termini di livelli di servizio.
8. Adozione di un sistema di segnalazione immediata della indisponibilità dei singoli punti di accesso.
9. Disponibilità di almeno un sito tecnologico alternativo in hot stand by per il ripristino dell'operatività in caso di evento disastroso.

---

<sup>1</sup> attraverso l'applicazione di meccanismi crittografici a livello di protocollo (es. *tunnel* basati sullo standard IPSec).

10. Accesso consentito alla rete in generale e agli apparati in particolare esclusivamente a utenti identificati univocamente e muniti di specifica autorizzazione.
11. Disponibilità di funzioni di gestione del QoS (Quality of Service) a livello di protocollo.

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

1. Modello di riferimento: ISO-OSI (International Standard Organization - Open System Interconnection).
2. Protocolli di comunicazione IETF (Internet Engineering Task Force) come: TCP/IP (Transmission Control Protocol/ Internet Protocol), UDP/IP, (User Datagram Protocol/ Internet Protocol), MPLS (Multiprotocol Label Switching).
3. Capacità di interfacciamento di protocolli di comunicazione esistenti (es. SNA, BSC, X25, ecc.).

## **C. Capacità di trasporto**

1. Capacità trasmissiva adeguata ai livelli di traffico, tale da garantire la qualità del servizio stabilita contrattualmente.
2. Adeguamento tempestivo del dimensionamento della rete in base al variare del fabbisogno e alle evoluzioni prevedibili (scalabilità).

## **Requisiti funzionali**

### **A. Interoperabilità**

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

### **B. Continuità di servizio**

1. Operatività della rete assicurata per 24 ore per 7 giorni a settimana.
2. Formalizzazione di un piano di "Continuità di servizio", conforme a quanto previsto nel successivo capitolo "Requisiti di sicurezza", contenente gli interventi organizzativi e tecnologici atti ad assicurare la continuità dei servizi resi, classificati secondo categorie di criticità in relazione all'impatto delle eventuali discontinuità operative.
3. Revisione periodica del piano di cui al precedente punto 2; adeguati interventi di formazione e aggiornamento per le risorse umane coinvolte; effettuazione di prove periodiche con cadenza almeno annuale.

### **C. Livelli di Servizio**

1. Definizione contrattuale dei livelli minimi di servizio garantiti (*Service Level Agreement - SLA*).

2. Disponibilità minima garantita del servizio pari al 99,98% sull'intera rete e al 99,75% sul singolo collegamento, con riguardo a un periodo di osservazione di sei mesi solari (*si definisce interruzione una perdita di servizio superiore a 30 secondi*).
3. Tempo massimo garantito di ripristino del servizio, in caso di interruzioni:  
30 secondi sull'intera rete, 4 ore sul singolo punto di accesso nell'80% dei casi, 6 ore nel 100% dei casi.
4. Definizione contrattuale, per ciascun punto di accesso, di un numero massimo di interruzioni del servizio nel mese.
5. Tempo di attraversamento<sup>2</sup> di un pacchetto (da misurare su un campione di 1.000 eventi):  
200 millisecondi nel 95% dei casi.
6. Tempo di servizio:
  - per il servizio transazionale: < 2 secondi nel 95% dei casi e < 10 secondi nel 100% dei casi;
  - per il servizio di *Message Switching*:
    - a) per i messaggi a priorità elevata: < 30 secondi nel 95% dei casi e < 3 minuti nel 100% dei casi;
    - b) per i rimanenti messaggi: < 15 minuti ;
  - per il servizio di *File Transfer*: < 130 secondi per un file della dimensione di 1 Megabyte con una sola sessione attiva.
7. Predisposizione di *report* periodici contenenti i dati di traffico, il livello dei servizi erogati, il dettaglio dei disservizi e dei malfunzionamenti, i tempi di ripristino e il confronto con i livelli prefissati.
8. Previsione contrattuale di specifiche penali per la mancata osservanza dei livelli di servizio stabiliti.

## Requisiti di sicurezza

### A. Autorizzazione

1. Identificazione degli utenti che accedono ai componenti di rete.
2. Applicazione del principio del minimo privilegio per l'accesso a tutti i componenti della rete.
3. Accesso alle informazioni trattate dalla rete ai soli utenti che dispongono delle necessarie abilitazioni.
4. Attribuzione differenziata delle abilitazioni di accesso in relazione agli specifici ruoli svolti.

---

<sup>2</sup> Si intende il tempo impiegato per trasmettere un pacchetto, di dimensioni 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.

## **B. Riservatezza**

1. Crittografia dei flussi veicolati sulla rete mediante protocolli conformi a standard internazionali (es. IPSec).
2. Crittografia delle comunicazioni che comportano accesso remoto ai componenti della rete.
3. Uso di algoritmi di crittografia conformi allo standard FIPS 140-1.

## **C. Integrità**

1. Tutela degli apparati di crittazione con dispositivi *tamper resistant*; rilevazione tempestiva dei tentativi di manomissione e/o di modifica della configurazione dei dispositivi.
2. Adozione di meccanismi di “sigillo” dei dati veicolati sulla rete che ne rendano accertabile l’integrità.

## **D. Autenticazione**

1. Adozione di meccanismi di “autenticazione forte” per l’accesso remoto ai componenti di rete (es. certificato digitale + PIN, *token card* + PIN, ecc.).
2. Controllo di qualità delle *password* per l’accesso ai componenti di rete e limitazione temporale della validità.
3. Mutua autenticazione tra tutti i componenti di rete (es. *routers*, *encryptors*).

## **E. Auditability**

1. Protezione e conservazione dei *log* relativi alle sessioni di rete.
2. Tracciamento degli accessi a tutti i dispositivi critici (es. apparati di crittazione).

## **F. Monitoring di sicurezza**

1. *Monitoring* dei tentativi di attacco e della vulnerabilità del software di rete.
2. Gestione accentrata degli *alert* per i tentativi di effrazione degli apparati di crittazione.

## **G. Disaster Recovery**

1. Formalizzazione di un piano per l’attivazione degli apparati tecnologici di *recovery* (*Technology recovery*) e per l’utilizzo delle risorse umane (*Human resource recovery*) in caso di evento disastroso.
2. Effettuazione, con cadenza almeno semestrale, di prove di *recovery* delle risorse tecnologiche e umane, con rilevazione dei tempi di ripristino dei servizi, compatibili con i tempi fissati negli SLA.

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

I requisiti previsti dall'art. 5 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) certificazione, rilasciata dai competenti organismi, attestante la conformità delle procedure e dei processi operativi della società, connessi con le attività di trasporto telematico di dati, ai seguenti standard internazionali:

ISO 9001 per la progettazione ed erogazione dei servizi;  
BS 7799-2-2002 per la sicurezza.

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 della CIPA (c/o Banca d'Italia – SISI – Largo Guido Carli, 1 – 00044 Frascati).

L'istanza di ammissione, previa istruttoria da parte della Segreteria, 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 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 della CIPA, a cadenza triennale, idonea documentazione atta a dimostrare la permanenza dei requisiti inizialmente richiesti.

L'ammissione può essere revocata, con delibera del Comitato direttivo della CIPA, per sopravvenuta mancanza di uno o più dei requisiti richiesti.

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