S.I.P.S.E.

SISTEMA DELLE ISTITUZIONI DEI POPOLI PER LA SOVRANITÀ ECONOMICA

CANCELLERIA GENERALE
SEGRETERIA TECNICA PER L'EFFETTIVITÀ E LA CONFORMITÀ DEI DIRITTI

PROTOCOLLO TECNICO GENERALE

IDENTITÀ DIGITALE, FIRMA ELETTRONICA, MARCATURA TEMPORALE, INTEGRITÀ CRITTOGRAFICA E REGISTRO DISTRIBUITO

Sistema: SIPSE-CCJC
Atto: n. 07/CCJC
Codice documentale: SIPSE-CCJC-PROT-07/2026
Versione: 1.0
Data di predisposizione: 13 novembre 2026
Stato: Schema tecnico sottoposto ad approvazione e validazione specialistica

Classificazione: Documento tecnico-organizzativo generale.

Ambito: Emissione, sottoscrizione, identificazione, registrazione, conservazione e verifica dei certificati SIPSE-CCJC.

PREAMBOLO

Il Sistema delle Istituzioni dei Popoli per la Sovranità Economica (SIPSE),

considerata la necessità di dotare il sistema volontario di certificazione SIPSE-CCJC di un'infrastruttura tecnologica affidabile, verificabile, sicura e documentata;

considerata l'esigenza di garantire l'identificazione univoca dei documenti, la tracciabilità delle operazioni, l'integrità delle registrazioni e la verifica indipendente dei certificati;

ritenuto necessario distinguere l'identità digitale, l'autenticità della sottoscrizione, l'integrità del documento, il riferimento temporale e lo stato amministrativo della certificazione;

richiamati, per quanto applicabili:

- Regolamento (UE) n. 910/2014 (eIDAS), come modificato;
- Regolamento (UE) 2016/679 (GDPR);

- normativa europea e nazionale sulla sicurezza informatica;
- standard ISO/IEC 27001 e ISO/IEC 27002, nelle versioni applicabili;
- standard ISO/IEC 27037 per l'identificazione, raccolta e conservazione delle evidenze digitali;
- standard ISO/IEC 27041, 27042 e 27043, ove pertinenti;
- standard ISO/IEC 18014 per i servizi di marcatura temporale;
- standard ETSI applicabili alle firme elettroniche e ai servizi fiduciari;
- specifiche tecniche IETF relative ai protocolli crittografici e alla sicurezza delle comunicazioni;

adotta il presente Protocollo.

TITOLO I – PRINCIPI, OGGETTO E ARCHITETTURA

Articolo 1 – Oggetto

1. Il presente Protocollo disciplina l'architettura tecnica di identificazione, sottoscrizione, integrità, registrazione temporale, conservazione e verifica dei documenti prodotti nell'ambito del sistema SIPSE-CCJC.
2. Esso definisce:
   a. identificazione dei soggetti e degli operatori;
   b. identificazione dei certificati;
   c. gestione delle credenziali e delle chiavi crittografiche;
   d. firma e sigillo elettronico;
   e. generazione e verifica delle impronte digitali;
   f. marcatura temporale;
   g. registrazione degli eventi;
   h. eventuale utilizzo di registri distribuiti;
   i. conservazione e protezione dei documenti;
   j. verifica pubblica;
   k. gestione degli incidenti e delle emergenze.
3. Il Protocollo si applica alle componenti tecnologiche del SIPSE-CCJC e ai fornitori incaricati di gestirle.

Articolo 2 – Obiettivi di sicurezza

L'infrastruttura deve assicurare, secondo il livello di rischio:

1. autenticità;
2. integrità;
3. riservatezza;
4. disponibilità;
5. tracciabilità;
6. non ripudio nei limiti degli strumenti giuridicamente validi;
7. separazione dei ruoli;

8. verificabilità indipendente;
9. resilienza;
10. continuità operativa.

Articolo 3 – Distinzione delle verifiche

Il sistema distingue obbligatoriamente:

Verifica	Domanda a cui risponde
Identità	Chi è il soggetto identificato?
Autorizzazione	Aveva il potere di compiere l'operazione?
Firma	Chi ha sottoscritto il documento e con quale strumento?
Integrità	Il documento è rimasto invariato rispetto alla versione registrata?
Tempo	Quando è stato attestato il documento o il relativo hash?
Registrazione	L'evento è stato inserito nel sistema?
Stato	La certificazione è attualmente valida, sospesa, scaduta o revocata?

Nessuna di queste verifiche sostituisce automaticamente le altre.

Articolo 4 – Architettura generale

1. L'infrastruttura SIPSE-CCJC è organizzata in componenti funzionalmente separate:
   a. sistema di identificazione;
   b. sistema di autenticazione;
   c. sistema di autorizzazione;
   d. motore documentale;
   e. servizio di firma e sigillo;
   f. servizio di impronta crittografica;
   g. servizio di marcatura temporale;
   h. Registro Generale SIPSE-CCJC;
   i. archivio riservato;
   j. portale pubblico di verifica;
   k. sistema di monitoraggio e sicurezza.
2. Le componenti possono essere realizzate mediante infrastrutture proprietarie, servizi esterni o soluzioni miste.
3. L'architettura deve essere documentata e sottoposta a verifica prima dell'attivazione.
4. Nessun componente tecnico può modificare autonomamente una decisione di certificazione.

Articolo 5 – Separazione degli ambienti

1. Devono essere distinti almeno:
   a. ambiente di sviluppo;
   b. ambiente di collaudo;
   c. ambiente di produzione;
   d. ambiente di conservazione e backup.
2. I dati reali non devono essere utilizzati in ambienti di sviluppo o test, salvo necessità documentata e adeguate misure di protezione.

3. Le credenziali di produzione devono essere separate da quelle di sviluppo e collaudo.
4. Il rilascio di nuove versioni deve seguire una procedura autorizzata e tracciabile.

TITOLO II – IDENTITÀ DIGITALE E AUTORIZZAZIONE

Articolo 6 – Identificazione degli operatori

1. Ogni operatore che accede alle funzioni riservate deve essere identificato individualmente.
2. Non sono ammesse credenziali amministrative condivise per le attività ordinarie.
3. L'identificazione deve consentire di associare ogni operazione a un soggetto autorizzato.
4. Il livello di identificazione deve essere proporzionato alla criticità dell'operazione.
5. Quando necessario, l'identità deve essere verificata mediante documenti o strumenti affidabili, nel rispetto della normativa applicabile.

Articolo 7 – Profili di identità

Sono istituiti i seguenti profili:

Profilo	Funzione
Amministratore tecnico	Gestione dell'infrastruttura
Responsabile del Registro	Supervisione delle registrazioni
Operatore di Cancelleria	Gestione amministrativa
Valutatore	Consultazione e inserimento evidenze autorizzate
Organo deliberante	Adozione delle decisioni
Responsabile sicurezza	Controlli e incident response
Revisore	Verifica delle operazioni
Richiedente	Consultazione del proprio fascicolo
Verificatore esterno	Consultazione delle informazioni pubbliche

I profili devono essere assegnati secondo il principio del minimo privilegio.

Articolo 8 – Autenticazione

1. L'accesso alle funzioni riservate avviene mediante autenticazione individuale.
2. Per le funzioni amministrative, deliberative e di gestione delle chiavi è obbligatoria l'autenticazione a più fattori.
3. Il sistema deve prevedere:
   a. credenziali individuali;
   b. autenticazione multifattore;
   c. gestione sicura delle sessioni;
   d. scadenza delle sessioni inattive;

e. protezione dai tentativi ripetuti di accesso;
f. revoca immediata delle credenziali compromesse.

4. Le modalità di autenticazione devono essere riesaminate periodicamente.

Articolo 9 – Autorizzazione delle operazioni

1. L'autenticazione non attribuisce automaticamente il potere di eseguire ogni operazione.
2. Il sistema applica autorizzazioni distinte per:
   a. consultazione;
   b. inserimento;
   c. modifica;
   d. approvazione;
   e. sottoscrizione;
   f. pubblicazione;
   g. sospensione;
   h. revoca;
   i. gestione delle chiavi.
3. Le operazioni critiche richiedono una specifica autorizzazione.
4. Le decisioni di certificazione sono registrate esclusivamente dopo l'adozione da parte dell'organo competente.
5. Gli amministratori tecnici non possono attribuirsi il potere di deliberare certificazioni.

Articolo 10 – Revoca delle autorizzazioni

1. Le autorizzazioni devono essere revocate quando:
   a. termina l'incarico;
   b. cambia il ruolo;
   c. viene meno il presupposto dell'accesso;
   d. si verifica un incidente di sicurezza;
   e. emerge un conflitto di interesse;
   f. il soggetto non è più autorizzato.
2. La revoca deve essere registrata.
3. Le autorizzazioni sono sottoposte a riesame periodico.

TITOLO III – IDENTIFICAZIONE DEI DOCUMENTI

Articolo 11 – Identificativo documentale

1. Ogni documento ufficiale SIPSE-CCJC riceve un identificativo univoco.
2. Il formato generale è:

SIPSE-CCJC-[TIPO]-[ANNO]-[NUMERO]

3. Esempi:

    - SIPSE-CCJC-CERT-2026-000001;
    - SIPSE-CCJC-DEC-2026-000001;
    - SIPSE-CCJC-AUD-2026-000001;
    - SIPSE-CCJC-VER-2026-000001.
4. L'identificativo non deve essere riutilizzato.
5. Il sistema deve impedire duplicazioni accidentali.

Articolo 12 – Identificazione delle versioni

1. Ogni documento deve indicare la propria versione.
2. La versione deve essere associata a:
   a. identificativo;
   b. data di creazione;
   c. data di approvazione;
   d. data di emissione;
   e. soggetto responsabile;
   f. eventuale documento sostitutivo.
3. Le versioni precedenti devono essere conservate secondo la politica documentale.
4. La modifica di un documento già sottoscritto deve produrre una nuova versione, non una sovrascrittura dell'originale.

Articolo 13 – Formati documentali

1. I documenti ufficiali devono essere prodotti in formati idonei alla conservazione e alla verifica.
2. Sono preferibili:
   a. PDF/A per i documenti destinati alla conservazione;
   b. XML o JSON per i dati strutturati;
   c. CSV per gli scambi tabellari;
   d. formati aperti e documentati per le esportazioni.
3. Il formato scelto deve essere registrato.
4. Le conversioni devono essere documentate.
5. Il documento sottoscritto deve rimanere distinguibile dalle copie di consultazione o dalle versioni convertite.

Articolo 14 – Metadati minimi

Ogni documento ufficiale deve contenere o essere associato ai seguenti metadati:

1. identificativo;
2. titolo;
3. tipologia;
4. versione;
5. data di emissione;
6. soggetto emittente;
7. soggetto destinatario, ove pertinente;
8. riferimento alla procedura;
9. riferimento alla decisione;
10. stato;

11. impronta crittografica;
12. algoritmo utilizzato;
13. riferimento temporale;
14. firma o sigillo, se applicabile;
15. ubicazione nell'archivio.

TITOLO IV – CRITTOGRAFIA E INTEGRITÀ DOCUMENTALE

Articolo 15 – Principi crittografici

1. Il sistema utilizza algoritmi crittografici riconosciuti e adeguati al livello di rischio.
2. Gli algoritmi devono essere selezionati in base a:
   a. sicurezza attuale;
   b. disponibilità di implementazioni affidabili;
   c. interoperabilità;
   d. supporto tecnico;
   e. aggiornabilità;
   f. resistenza alle vulnerabilità note.
3. Non è consentito utilizzare algoritmi obsoleti o deboli per le nuove registrazioni.
4. La Segreteria Tecnica mantiene un inventario degli algoritmi autorizzati.

Articolo 16 – Impronta SHA-256

1. Ogni certificato ufficiale deve essere associato a un'impronta crittografica.
2. L'algoritmo inizialmente adottato è SHA-256.
3. L'impronta è calcolata sul contenuto esatto del file sottoposto a registrazione.
4. Il sistema deve registrare:
   a. algoritmo;
   b. valore esadecimale;
   c. nome e identificativo del file;
   d. dimensione del file;
   e. formato;
   f. data e ora del calcolo;
   g. componente che ha eseguito l'operazione.
5. La procedura di calcolo deve essere ripetibile e documentata.
6. La verifica consiste nel ricalcolare l'impronta del file e confrontarla con quella registrata.
7. Una corrispondenza positiva dimostra che il contenuto esaminato coincide con quello cui l'impronta era stata associata, non la veridicità sostanziale del documento.

Articolo 17 – Evoluzione degli algoritmi

1. Il sistema deve poter sostituire o affiancare gli algoritmi crittografici quando necessario.
2. La sostituzione può essere determinata da:
   a. vulnerabilità;

b. obsolescenza;
c. nuove raccomandazioni tecniche;
d. esigenze di interoperabilità;
e. evoluzione delle capacità di calcolo.

3. Le impronte storiche non devono essere cancellate.
4. Il passaggio a un nuovo algoritmo deve essere documentato.
5. Il sistema deve conservare la relazione tra impronta originaria e nuova impronta, quando la migrazione viene effettuata.

Articolo 18 – Cifratura dei dati

1. I dati riservati devono essere protetti mediante cifratura adeguata al rischio.
2. Per la cifratura dei dati archiviati è preferibile l'utilizzo di algoritmi moderni come AES-256-GCM, con corretta gestione delle chiavi e dei parametri crittografici.
3. Le comunicazioni devono essere protette mediante protocolli sicuri e configurazioni aggiornate.
4. Le chiavi non devono essere conservate in chiaro insieme ai dati cifrati.
5. Devono essere previste procedure di rotazione, revoca e recupero controllato delle chiavi.

Articolo 19 – Separazione tra cifratura e firma

1. La cifratura assicura la riservatezza del contenuto.
2. La firma elettronica è destinata a collegare il documento al firmatario e a consentire verifiche di integrità.
3. Le due funzioni devono essere trattate separatamente.
4. Il possesso di una chiave di cifratura non attribuisce automaticamente il potere di sottoscrivere documenti.
5. Le chiavi di firma e le chiavi di cifratura devono essere gestite secondo politiche distinte.

TITOLO V – FIRMA ELETTRONICA E SIGILLO

Articolo 20 – Principio generale

1. Gli atti ufficiali sono sottoscritti dai soggetti legittimati mediante strumenti appropriati alla natura dell'atto.
2. Il sistema deve identificare il firmatario e verificare il suo potere di sottoscrizione.
3. La firma deve essere verificabile e collegata al documento effettivamente sottoscritto.
4. La firma non può essere apposta automaticamente senza un'azione autorizzata o un procedimento validamente delegato.

Articolo 21 – Livelli di sottoscrizione

Il sistema distingue:

1. firma elettronica semplice;
2. firma elettronica avanzata;
3. firma elettronica qualificata;
4. sigillo elettronico;
5. sigillo elettronico qualificato;
6. altre modalità di sottoscrizione riconosciute dalla normativa applicabile.

La qualificazione giuridica dipende dai requisiti effettivamente soddisfatti e non dalla denominazione utilizzata dal SIPSE.

Articolo 22 – Firma qualificata e servizi fiduciari

1. Quando si intende utilizzare una firma elettronica qualificata o un sigillo qualificato ai sensi del quadro eIDAS, devono essere utilizzati prestatori e dispositivi che soddisfino i requisiti previsti.
2. Il SIPSE non può dichiarare qualificato un proprio servizio senza averne i requisiti giuridici e tecnici.
3. Il sistema può integrare servizi fiduciari esterni qualificati.
4. Il riferimento al prestatore, al certificato e allo stato della firma deve essere conservato nel fascicolo documentale.

Articolo 23 – Firma degli atti di certificazione

1. Il certificato è sottoscritto dal soggetto o dai soggetti autorizzati secondo l'ordinamento interno SIPSE.
2. La decisione di certificazione deve essere adottata prima dell'emissione del certificato.
3. Il sistema conserva:
   a. documento sottoscritto;
   b. identificazione del firmatario;
   c. certificato digitale utilizzato, ove presente;
   d. riferimento temporale;
   e. esito della verifica;
   f. riferimento all'atto deliberativo.
4. La firma dell'operatore amministrativo non sostituisce la decisione dell'organo competente.

Articolo 24 – Verifica della firma

La verifica deve consentire, ove tecnicamente disponibile:

1. identificazione del firmatario;
2. controllo della validità del certificato digitale;
3. verifica della catena di certificazione;
4. verifica della revoca;
5. controllo dell'integrità del documento;
6. verifica della marca temporale;
7. controllo del periodo di validità;
8. registrazione dell'esito.

L'esito deve distinguere una firma valida, non valida, non verificabile o verificabile solo parzialmente.

Articolo 25 – Firma multipla e approvazione collegiale

1. Gli atti che richiedono approvazione collegiale devono documentare la decisione e i soggetti legittimati.
2. Possono essere utilizzate:
   a. firme multiple;
   b. firma del presidente dell'organo con verbale allegato;
   c. firma del segretario verbalizzante;
   d. sigillo istituzionale, ove legittimamente disponibile.
3. La procedura deve permettere di ricostruire chi ha deliberato e chi ha sottoscritto.
4. Un sigillo istituzionale non sostituisce una deliberazione quando questa è richiesta.

TITOLO VI – MARCATURA TEMPORALE

Articolo 26 – Finalità

1. La marcatura temporale associa un riferimento temporale a un documento o alla sua impronta.
2. Essa è utilizzata per documentare che un determinato contenuto era stato presentato a un servizio temporale in un dato momento.
3. Gli effetti giuridici dipendono dal servizio utilizzato e dalla normativa applicabile.

Articolo 27 – Marcatura temporale qualificata

1. Quando è necessario ottenere gli effetti propri di una marca temporale qualificata ai sensi del quadro eIDAS, deve essere utilizzato un prestatore qualificato di servizi fiduciari.
2. Il sistema deve conservare la prova della marca temporale e i dati necessari alla sua verifica.
3. Una semplice registrazione interna dell'orario non deve essere denominata marca temporale qualificata.
4. Il SIPSE può utilizzare un servizio temporale interno per la tracciabilità operativa, distinguendolo chiaramente dal servizio qualificato.

Articolo 28 – Riferimento temporale degli eventi

1. Ogni evento critico deve essere associato a un riferimento temporale.
2. Il sistema deve utilizzare fonti temporali affidabili e sincronizzate.
3. Gli orari sono registrati in formato interoperabile, preferibilmente UTC, con indicazione del fuso orario quando necessario.
4. Devono essere conservati:
   a. data e ora dell'evento;
   b. fonte temporale;
   c. identificativo dell'operazione;

d. eventuale marca temporale esterna;
e. esito della verifica.

TITOLO VII – REGISTRO DEGLI EVENTI E REGISTRO DISTRIBUITO

Articolo 29 – Registro cronologico

1. Tutte le operazioni critiche sono inserite in un registro cronologico degli eventi.
2. Ogni registrazione comprende:
   a. identificativo dell'evento;
   b. tipo di evento;
   c. data e ora;
   d. utente o componente responsabile;
   e. documento interessato;
   f. esito;
   g. riferimento all'autorizzazione;
   h. impronta dell'evidenza, ove applicabile.
3. Le registrazioni devono essere protette da modifiche non autorizzate.
4. Le rettifiche sono effettuate mediante nuovi eventi collegati a quelli precedenti.

Articolo 30 – Catena di integrità

1. Il SIPSE può adottare un sistema di concatenazione crittografica degli eventi.
2. Ogni evento può includere l'impronta dell'evento precedente.
3. Il meccanismo permette di rilevare modifiche o interruzioni nella sequenza registrata.
4. La catena di integrità deve essere conservata in modo separato dai dati operativi ordinari.
5. Il meccanismo non garantisce da solo che gli eventi originari siano veritieri o correttamente autorizzati.

Articolo 31 – Alberi di Merkle

1. Per la verifica di insiemi di documenti o eventi può essere utilizzata una struttura crittografica ad albero di Merkle.
2. Le impronte dei documenti costituiscono le foglie dell'albero.
3. Le impronte intermedie sono calcolate secondo una procedura documentata.
4. La radice di Merkle può essere utilizzata come riferimento sintetico per attestare l'integrità di un insieme di registrazioni.
5. Devono essere conservate le prove necessarie a verificare l'appartenenza di un documento all'insieme registrato.
6. La radice di Merkle non dimostra da sola la correttezza giuridica o sostanziale dei documenti.

Articolo 32 – Registro distribuito

1. Il SIPSE può adottare un registro distribuito, anche permissioned, per la registrazione delle impronte e degli eventi.
2. La decisione di adozione deve essere preceduta da una valutazione di sicurezza, governance, costi, interoperabilità e protezione dei dati.
3. Il registro distribuito deve essere considerato una componente di supporto e non il sostituto del Registro Generale SIPSE-CCJC.
4. Le informazioni inserite devono essere limitate a dati tecnici minimizzati, preferibilmente impronte e riferimenti non direttamente identificativi.
5. Non devono essere registrati in chiaro dati personali, credenziali, documenti riservati o segreti commerciali.
6. La governance della rete deve indicare:
   a. nodi partecipanti;
   b. soggetti amministratori;
   c. regole di ammissione;
   d. procedure di aggiornamento;
   e. gestione delle chiavi;
   f. modalità di verifica;
   g. procedure di emergenza.
7. Il registro distribuito non conferisce automaticamente effetti giuridici universali o riconoscimento da parte di Stati e organizzazioni internazionali.

Articolo 33 – Nodi e validatori

1. Se viene adottata un'infrastruttura permissioned, i nodi validatori sono gestiti da soggetti previamente autorizzati.
2. I validatori operano secondo regole tecniche documentate.
3. Il protocollo deve prevedere:
   a. identificazione dei nodi;
   b. autenticazione reciproca;
   c. protezione delle chiavi;
   d. controllo degli aggiornamenti;
   e. monitoraggio;
   f. procedure per nodi compromessi.
4. Il numero dei nodi e il meccanismo di consenso devono essere scelti in base al modello di minaccia e al volume delle operazioni.
5. Non è sufficiente moltiplicare i nodi per ottenere automaticamente indipendenza: devono essere valutati anche proprietà, amministrazione e dipendenze comuni.

Articolo 34 – Governance del registro distribuito

1. La governance è approvata con specifico atto tecnico.
2. L'atto deve definire:
   a. titolarità dell'infrastruttura;
   b. responsabilità dei partecipanti;
   c. criteri di ammissione;
   d. poteri di amministrazione;
   e. gestione delle controversie tecniche;
   f. procedure di aggiornamento;
   g. continuità operativa;
   h. cessazione del servizio.

3. Nessun nodo può modificare unilateralmente le decisioni di certificazione.
4. Gli aggiornamenti del protocollo devono essere tracciati e comunicati ai partecipanti.

Articolo 35 – Ancoraggio esterno delle impronte

1. Il SIPSE può ancorare periodicamente le radici crittografiche del proprio registro a servizi o infrastrutture esterne.
2. L'ancoraggio può rafforzare la verificabilità indipendente della sequenza temporale.
3. Devono essere documentati:
   a. infrastruttura utilizzata;
   b. data;
   c. impronta;
   d. identificativo della transazione o registrazione;
   e. modalità di verifica.
4. L'ancoraggio esterno non equivale a riconoscimento pubblico o certificazione da parte del gestore dell'infrastruttura utilizzata.

TITOLO VIII – GESTIONE DELLE CHIAVI CRITTOGRAFICHE

Articolo 36 – Politica delle chiavi

1. Il SIPSE adotta una politica formale di gestione delle chiavi crittografiche.
2. La politica disciplina:
   a. generazione;
   b. custodia;
   c. distribuzione;
   d. utilizzo;
   e. rotazione;
   f. revoca;
   g. backup;
   h. recupero;
   i. distruzione.
3. Le chiavi sono associate a una finalità e a un titolare organizzativo.
4. Non è consentito utilizzare una stessa chiave per finalità incompatibili.

Articolo 37 – Generazione delle chiavi

1. Le chiavi devono essere generate mediante procedure crittograficamente sicure.
2. La generazione deve avvenire attraverso dispositivi o ambienti affidabili.
3. Le chiavi private non devono essere generate o conservate in ambienti non protetti.
4. Le operazioni devono essere documentate.
5. Per le chiavi istituzionali e di firma è preferibile l'utilizzo di dispositivi dedicati o moduli di sicurezza hardware, in funzione del rischio.

Articolo 38 – Custodia delle chiavi

1. Le chiavi private devono essere protette da accessi non autorizzati.
2. Le chiavi di maggiore criticità devono essere custodite mediante HSM o soluzioni equivalenti adeguatamente valutate.
3. Può essere adottato un modello di autorizzazione multipla.
4. Il sistema può prevedere una struttura di controllo a soglia, purché:
   a. il numero dei custodi sia definito;
   b. la soglia minima sia documentata;
   c. le procedure di recupero siano testate;
   d. gli accessi siano tracciati;
   e. sia previsto un piano di emergenza.
5. Il modello di custodia deve evitare che un singolo operatore possa compromettere l'intera infrastruttura.

Articolo 39 – Separazione delle chiavi

Devono essere mantenute distinte almeno le seguenti categorie:

1. chiavi di firma dei documenti;
2. chiavi di sigillo;
3. chiavi di cifratura;
4. chiavi di autenticazione;
5. chiavi di amministrazione;
6. chiavi dei nodi distribuiti;
7. chiavi di backup e recupero.

Articolo 40 – Rotazione e revoca

1. Le chiavi sono sottoposte a rotazione secondo un calendario documentato e in funzione del rischio.
2. La revoca è immediata quando:
   a. una chiave risulta compromessa;
   b. viene perso il controllo della custodia;
   c. il titolare perde l'autorizzazione;
   d. l'algoritmo o il dispositivo diventano inadeguati;
   e. sussiste un rischio concreto per la sicurezza.
3. La revoca deve essere registrata.
4. Le firme storiche devono poter essere verificate, quando tecnicamente e giuridicamente possibile, mediante le evidenze conservate al momento della sottoscrizione.

Articolo 41 – Compromissione delle chiavi

1. In caso di compromissione, il Responsabile della Sicurezza attiva la procedura di emergenza.
2. Le misure comprendono:
   a. blocco della chiave;
   b. revoca dei certificati digitali, ove applicabile;
   c. sospensione delle operazioni interessate;

d. verifica degli atti sottoscritti;
e. emissione di nuove chiavi;
f. analisi dell'incidente;
g. comunicazione agli interessati, quando necessaria.

3. Gli atti la cui autenticità risulti dubbia sono contrassegnati come oggetto di verifica.
4. Nessun documento sospetto deve essere considerato automaticamente autentico solo perché reca un'impronta precedentemente registrata.

TITOLO IX – CONSERVAZIONE E VERIFICA

Articolo 42 – Archivio digitale

1. I documenti sono conservati in un archivio digitale organizzato.
2. L'archivio deve garantire:
   a. integrità;
   b. disponibilità;
   c. riservatezza;
   d. reperibilità;
   e. controllo degli accessi;
   f. tracciabilità;
   g. gestione delle versioni.
3. Il sistema deve consentire l'esportazione dei documenti e dei relativi metadati in formati documentati.
4. La conservazione deve rispettare gli obblighi normativi applicabili.

Articolo 43 – Conservazione a lungo termine

1. Per i documenti destinati a conservazione prolungata deve essere adottata una strategia di preservazione digitale.
2. La strategia comprende:
   a. verifica periodica dell'integrità;
   b. controllo dei formati;
   c. migrazione documentale;
   d. conservazione delle evidenze di firma;
   e. conservazione dei riferimenti temporali;
   f. documentazione degli algoritmi utilizzati.
3. Quando la normativa richiede un servizio qualificato o uno specifico sistema di conservazione, il SIPSE utilizza un soggetto o un servizio conforme.
4. L'archivio interno non deve essere presentato come sistema di conservazione legalmente accreditato, salvo che ne ricorrano effettivamente i requisiti.

Articolo 44 – Verifica pubblica

1. Ogni certificato pubblicabile deve disporre di un riferimento univoco di verifica.

2. La verifica può avvenire tramite:
   a. codice identificativo;
   b. QR code;
   c. collegamento ufficiale;
   d. impronta crittografica;
   e. verifica della firma.
3. Il portale pubblico deve distinguere:
   a. autenticità del documento;
   b. integrità del documento;
   c. stato attuale del certificato;
   d. validità della firma, ove verificabile.
4. La verifica deve mostrare la data e l'ora della consultazione.
5. La disponibilità del portale non sostituisce la conservazione dell'originale.

Articolo 45 – API di verifica

1. Il SIPSE può rendere disponibile un'interfaccia applicativa per la verifica automatizzata.
2. L'API deve consentire, nei limiti autorizzati:
   a. ricerca per codice;
   b. verifica dello stato;
   c. consultazione dei metadati pubblici;
   d. verifica dell'impronta;
   e. recupero delle informazioni sulla versione.
3. L'API deve applicare limiti di utilizzo, autenticazione ove necessaria e protezioni contro gli abusi.
4. Le risposte devono utilizzare formati documentati e versionati.
5. L'API non deve esporre dati riservati o consentire l'accesso ai fascicoli di audit.

Articolo 46 – Verifica indipendente

1. Il sistema deve permettere a un verificatore esterno di controllare l'autenticità e l'integrità di un certificato senza dover accedere all'archivio riservato.
2. Il verificatore deve poter:
   a. identificare il certificato;
   b. consultare lo stato;
   c. verificare l'impronta;
   d. verificare la firma, quando tecnicamente disponibile;
   e. consultare il riferimento temporale;
   f. distinguere il documento originale dalle copie.
3. Le istruzioni di verifica devono essere pubblicate.
4. La verifica indipendente non attribuisce al verificatore poteri di certificazione o di annullamento.

TITOLO X – SICUREZZA, INCIDENTI E CONTINUITÀ

Articolo 47 – Monitoraggio

1. L'infrastruttura è sottoposta a monitoraggio tecnico.
2. Sono monitorati almeno:
   a. disponibilità;
   b. accessi;
   c. tentativi di autenticazione;
   d. operazioni amministrative;
   e. modifiche;
   f. errori;
   g. anomalie;
   h. utilizzo delle chiavi;
   i. integrità dei registri.
3. I sistemi di monitoraggio devono essere protetti contro la manomissione.
4. Gli eventi sono conservati secondo una politica documentata.

Articolo 48 – Test di sicurezza

1. Prima dell'attivazione devono essere eseguiti test di sicurezza.
2. Sono previsti:
   a. test funzionali;
   b. test di autenticazione;
   c. test di autorizzazione;
   d. test di integrità;
   e. test di backup;
   f. test di ripristino;
   g. test di vulnerabilità;
   h. test di continuità.
3. I test di intrusione devono essere autorizzati, delimitati e documentati.
4. Le vulnerabilità rilevate devono essere classificate e gestite secondo priorità.
5. L'attivazione in produzione è subordinata alla chiusura delle criticità incompatibili con il livello di sicurezza richiesto.

Articolo 49 – Gestione degli incidenti

1. Ogni incidente di sicurezza deve essere registrato.
2. La procedura prevede:
   a. rilevazione;
   b. classificazione;
   c. contenimento;
   d. analisi;
   e. ripristino;
   f. comunicazione;
   g. documentazione;
   h. misure preventive.
3. Gli incidenti che coinvolgono dati personali sono gestiti secondo il GDPR, ove applicabile.
4. Gli incidenti che incidono sull'autenticità dei certificati devono essere comunicati agli interessati e riportati nel Registro, nei limiti necessari.
5. Il sistema deve mantenere un registro degli incidenti e delle relative misure correttive.

Articolo 50 – Continuità operativa

1. Il SIPSE predispone un piano di continuità operativa.
2. Il piano definisce:
   a. componenti essenziali;
   b. tempi obiettivo di ripristino;
   c. perdita massima tollerabile dei dati;
   d. sistemi alternativi;
   e. procedure di emergenza;
   f. responsabilità;
   g. modalità di comunicazione.
3. Il piano è sottoposto a test periodici.
4. In caso di indisponibilità, deve essere mantenuta, ove possibile, una modalità alternativa di verifica dei certificati.

Articolo 51 – Sospensione tecnica

1. In presenza di un rischio grave per l'integrità o l'autenticità del sistema, il Responsabile della Sicurezza può richiedere la sospensione tecnica delle funzioni interessate.
2. La misura deve essere proporzionata e documentata.
3. La sospensione tecnica non equivale automaticamente alla sospensione giuridica di un certificato.
4. L'organo competente valuta gli eventuali effetti sulle certificazioni.
5. Il ripristino avviene dopo verifica documentata della sicurezza.

TITOLO XI – INTEROPERABILITÀ E STANDARD TECNICI

Articolo 52 – Interoperabilità

1. L'infrastruttura deve utilizzare, ove possibile, protocolli e formati aperti e documentati.
2. Devono essere evitate dipendenze tecniche non necessarie da un singolo fornitore.
3. Le interfacce devono essere documentate.
4. Il SIPSE deve poter esportare i dati e i documenti essenziali in formati interoperabili.

Articolo 53 – Standard di riferimento

Il sistema può adottare, secondo pertinenza e dopo verifica delle versioni vigenti:

- ISO/IEC 27001 – sistemi di gestione della sicurezza delle informazioni;
- ISO/IEC 27002 – controlli di sicurezza;
- ISO/IEC 27017 – sicurezza dei servizi cloud;
- ISO/IEC 27018 – protezione dei dati personali nei servizi cloud pubblici;
- ISO/IEC 27701 – gestione delle informazioni sulla privacy;
- ISO/IEC 27035 – gestione degli incidenti;

- ISO/IEC 27037 – evidenze digitali;
- ISO/IEC 15408 – criteri comuni per la valutazione della sicurezza informatica;
- standard ETSI per firme elettroniche e servizi fiduciari;
- specifiche IETF per protocolli crittografici e comunicazioni sicure.

Il richiamo a uno standard non equivale a una certificazione o a un accreditamento del SIPSE rispetto allo stesso.

Articolo 54 – Neutralità tecnologica

1. Il SIPSE non vincola il sistema a un unico fornitore o prodotto.
2. Le tecnologie sono selezionate sulla base di sicurezza, affidabilità, interoperabilità e sostenibilità.
3. Le soluzioni proprietarie devono essere sottoposte a valutazione del rischio di dipendenza tecnologica.
4. Le decisioni tecniche devono essere documentate.

TITOLO XII – GOVERNANCE E RESPONSABILITÀ

Articolo 55 – Responsabile del Protocollo

1. La Segreteria Tecnica nomina un Responsabile del Protocollo.
2. Il Responsabile coordina:
   a. applicazione delle specifiche;
   b. aggiornamento tecnico;
   c. verifica della conformità;
   d. gestione delle vulnerabilità;
   e. coordinamento con i fornitori;
   f. reportistica.
3. Il Responsabile non può modificare le decisioni di certificazione.

Articolo 56 – Comitato tecnico di sicurezza

1. È istituito un Comitato tecnico di sicurezza SIPSE-CCJC.
2. Il Comitato formula proposte e pareri su:
   a. algoritmi;
   b. architettura;
   c. gestione delle chiavi;
   d. sicurezza;
   e. interoperabilità;
   f. continuità;
   g. evoluzione tecnologica.
3. Il Comitato può proporre la sospensione tecnica di componenti vulnerabili.

4. Le decisioni operative sono adottate dai soggetti competenti secondo le deleghe formalmente attribuite.

Articolo 57 – Fornitori tecnologici

1. I fornitori devono essere selezionati secondo criteri documentati.
2. I contratti devono disciplinare:
   a. livelli di servizio;
   b. sicurezza;
   c. riservatezza;
   d. protezione dei dati;
   e. localizzazione e trasferimento dei dati;
   f. gestione degli incidenti;
   g. continuità;
   h. esportazione dei dati;
   i. cessazione del servizio.
3. Il fornitore non acquisisce il potere di decidere sulle certificazioni.
4. Il SIPSE deve mantenere il controllo organizzativo sui dati e sui processi di propria competenza.

Articolo 58 – Verifica periodica del Protocollo

1. Il Protocollo è sottoposto a revisione almeno annuale o in presenza di eventi significativi.
2. La revisione considera:
   a. evoluzione normativa;
   b. nuove vulnerabilità;
   c. modifiche tecnologiche;
   d. incidenti;
   e. risultati degli audit;
   f. esigenze di interoperabilità.
3. Ogni versione deve essere identificata, approvata e archiviata.
4. Le modifiche critiche sono comunicate agli operatori interessati.

TITOLO XIII – ATTIVAZIONE E COLLAUDO

Articolo 59 – Condizioni preliminari

L'infrastruttura non può essere dichiarata operativa prima di:

1. identificazione del soggetto giuridico responsabile;
2. nomina dei responsabili tecnici;
3. definizione dei ruoli;
4. approvazione della politica di sicurezza;
5. definizione della politica di gestione delle chiavi;

6. verifica della protezione dei dati;
7. configurazione dell'archivio;
8. implementazione del Registro;
9. configurazione del servizio di verifica;
10. esecuzione dei test;
11. approvazione delle procedure di emergenza;
12. documentazione delle responsabilità dei fornitori.

Articolo 60 – Fase di collaudo

1. Prima dell'attivazione è prevista una fase di collaudo.
2. Il collaudo comprende almeno:
   a. generazione di un certificato di prova;
   b. sottoscrizione;
   c. generazione dell'impronta;
   d. verifica dell'impronta;
   e. registrazione temporale;
   f. inserimento nel Registro;
   g. verifica mediante QR;
   h. simulazione di sospensione;
   i. simulazione di revoca;
   j. verifica dei backup;
   k. prova di ripristino.
3. I risultati sono raccolti in un verbale.
4. Le criticità rilevate devono essere risolte o formalmente accettate con motivazione e misure compensative, ove compatibile con la sicurezza.

Articolo 61 – Attivazione in esercizio

1. L'attivazione in produzione è autorizzata dall'organo competente.
2. L'autorizzazione deve indicare:
   a. versione del Protocollo;
   b. componenti attivate;
   c. responsabili;
   d. data di attivazione;
   e. esito del collaudo;
   f. eventuali limitazioni.
3. L'attivazione parziale deve essere chiaramente dichiarata.
4. Nessuna funzione non collaudata può essere presentata come operativa.

Articolo 62 – Fase sperimentale

1. Il SIPSE può avviare una fase sperimentale con certificati pilota.
2. I certificati pilota devono essere chiaramente identificati come tali.
3. Durante la sperimentazione non possono essere formulate dichiarazioni ingannevoli circa la sicurezza, l'affidabilità o il riconoscimento del sistema.
4. I risultati sono valutati prima dell'estensione a regime.

TITOLO XIV – DISPOSIZIONI FINALI

Articolo 63 – Coordinamento normativo

Il presente Protocollo si coordina con:

1. Disciplinare Generale SIPSE-CCJC-REG-01;
2. Deliberazione istitutiva n. 01/CCJC;
3. Decreto organizzativo n. 02/CCJC;
4. Manuale di valutazione e audit n. 03/CCJC;
5. Regolamento economico e tariffario n. 04/CCJC;
6. Contratto generale n. 05/CCJC;
7. Regolamento del Registro n. 06/CCJC;
8. Politica di sicurezza informatica;
9. Politica di conservazione documentale;
10. Politica di protezione dei dati;
11. Manuale d'uso del marchio.

Articolo 64 – Prevalenza delle norme imperative

1. Il presente Protocollo è applicato nel rispetto della normativa inderogabile pertinente.
2. In caso di contrasto prevalgono le disposizioni imperative applicabili.
3. Nessuna disposizione attribuisce al SIPSE poteri pubblici, competenze di accreditamento o effetti giuridici non riconosciuti dall'ordinamento competente.

Articolo 65 – Entrata in vigore

1. Il presente Protocollo entra in vigore dalla data della sua approvazione.
2. Le componenti tecnologiche sono attivate soltanto dopo il completamento delle verifiche previste.
3. La Cancelleria Generale cura la diffusione agli organi e agli operatori interessati.
4. Ogni aggiornamento è registrato nel sistema di gestione documentale.

ALLEGATO A – MATRICE TECNICA MINIMA

Componente	Requisito	Evidenza di verifica
Identità	Account individuali	Registro utenti
Autenticazione	MFA per ruoli critici	Test di accesso
Autorizzazione	Ruoli separati	Matrice dei privilegi
Integrità	SHA-256	Rapporto di verifica
Firma	Firma verificabile	Esito di validazione
Tempo	Riferimento temporale documentato	Token o ricevuta

Registro	Codici univoci	Test di duplicazione
Log	Tracciabilità	Rapporto di audit
Cifratura	Protezione dati	Configurazione verificata
Backup	Copie protette	Verbale di ripristino
Registro distribuito	Governance documentata	Verbale di collaudo
Portale	Verifica pubblica	Test QR/API

ALLEGATO B – PROCEDURA DI EMISSIONE DEL CERTIFICATO

1. L'organo competente adotta la decisione positiva.
2. La decisione riceve un identificativo documentale.
3. Il sistema verifica la corrispondenza tra decisione e fascicolo.
4. Il certificato viene generato con i metadati obbligatori.
5. Il documento viene sottoscritto dal soggetto autorizzato.
6. Viene verificata la sottoscrizione.
7. Viene calcolata l'impronta SHA-256.
8. Viene acquisito il riferimento temporale previsto.
9. Il certificato viene registrato nel Registro Generale.
10. L'eventuale ancoraggio distribuito viene effettuato secondo il protocollo autorizzato.
11. Viene generato il collegamento univoco di verifica.
12. Il certificato viene consegnato al titolare.
13. Il Registro pubblico viene aggiornato, nei limiti consentiti.

ALLEGATO C – PROCEDURA DI VERIFICA DEL CERTIFICATO

Il verificatore:

1. accede al portale ufficiale;
2. inserisce il codice o scansiona il QR;
3. verifica la corrispondenza del titolare;
4. controlla lo schema;
5. controlla il perimetro;
6. verifica lo stato;
7. controlla la data di scadenza;
8. verifica l'impronta del documento;
9. verifica la firma, se disponibile;
10. consulta il riferimento temporale;
11. salva la ricevuta di verifica, se necessaria.

L'esito è presentato separando le verifiche effettuate e quelle non disponibili.

ALLEGATO D – PROCEDURA DI EMERGENZA PER COMPROMISSIONE DELLE CHIAVI

1. Rilevazione dell'evento.
2. Apertura del fascicolo incidente.
3. Blocco della chiave sospetta.
4. Revoca dei certificati digitali interessati, ove applicabile.
5. Sospensione delle operazioni di firma coinvolte.
6. Analisi delle firme e dei documenti potenzialmente compromessi.
7. Comunicazione agli organi competenti.
8. Generazione di nuove chiavi.
9. Verifica dell'integrità del Registro.
10. Ripristino controllato.
11. Relazione conclusiva.
12. Misure preventive.

ALLEGATO E – VERBALE DI COLLAUDO

Codice collaudo: SIPSE-CCJC-TEST-[ANNO]-[NUMERO]

Ambiente: [Sviluppo / Collaudo / Produzione]

Data: [●]

Responsabile tecnico: [●]

Test	Esito	Evidenza	Note
Identificazione	[●]	[●]	[●]
MFA	[●]	[●]	[●]
Autorizzazioni	[●]	[●]	[●]
Generazione certificato	[●]	[●]	[●]
Firma	[●]	[●]	[●]
SHA-256	[●]	[●]	[●]
Marcatura temporale	[●]	[●]	[●]
Registro	[●]	[●]	[●]
QR	[●]	[●]	[●]
Revoca	[●]	[●]	[●]
Backup	[●]	[●]	[●]
Ripristino	[●]	[●]	[●]

Esito complessivo:

[ ] Positivo

[ ] Positivo con prescrizioni

[ ] Negativo

Prescrizioni: [●]

Firma del Responsabile tecnico: _____

Firma del Responsabile del Registro: _____

Approvazione della Cancelleria Generale: _____

APPROVAZIONE DEL PROTOCOLLO

Luogo: [●]

Data: [●]

Per l'organo competente SIPSE

Nome e qualifica: [●]

Firma: _____

Per la Cancelleria Generale

Nome e qualifica: [●]

Firma: _____

Per la Segreteria Tecnica SIPSE-CCJC

Nome e qualifica: [●]

Firma: _____

FINE DEL PROTOCOLLO TECNICO GENERALE SIPSE-CCJC – ATTO N. 07/CCJC

Codice documentale: SIPSE-CCJC-PROT-07/2026
Versione: 1.0
Stato: Schema sottoposto ad approvazione e validazione specialistica.

Architettura tecnica minima SIPSE-CCJC

1. PORTALE SIPSE-CCJC

Domande · Fascicoli · Certificati · Verifica pubblica

Identità e accessi

Account, MFA, ruoli

Motore documentale

PDF, metadati, versioni

Firma e tempo

Firma, sigillo, timestamp

Integrità

SHA-256, Merkle, log

REGISTRO GENERALE SIPSE-CCJC

Codici univoci · Stato · Cronologia · Archivio riservato

Registro pubblico

QR · API · Verifica certificati

Registro distribuito

Ancoraggio impronte · Prove di integrità

Le prime decisioni tecnologiche

Componente	Scelta iniziale raccomandata
Identificazione	Account individuali e MFA
Documenti	PDF/A e metadati strutturati
Integrità	SHA-256
Firma	Integrazione con servizi di firma conformi alla normativa applicabile
Marcatura temporale	Servizio qualificato esterno, quando necessario
Cifratura	AES-256-GCM, con gestione sicura delle chiavi
Registro	Database centrale con log append-only
Registro distribuito	Fase successiva, dopo valutazione tecnica
Verifica	Portale pubblico con codice univoco e QR

Una raccomandazione strategica: non renderei la blockchain un requisito indispensabile per rilasciare il certificato. Prima bisogna assicurare che il sistema centrale funzioni correttamente, che le decisioni siano indipendenti e che le firme siano verificabili. Il registro distribuito potrà poi aggiungere una seconda prova di integrità senza diventare un punto di dipendenza dell'intero servizio.