

Informativa sulla Policy di custodia e amministrazione delle Cripto-attività

Stato: Approvato

Changelog: Revisione del pacchetto contrattuale per maggiore coerenza tra i diversi documenti

Versione: 2.1.0

Codice documento: informativa-custodia-v2.1.0

Organo approvante: Consiglio di amministrazione

Data di approvazione: 17 febbraio 2026

Data di entrata in vigore: 18 febbraio 2026

La documentazione contrattuale, composta dai Termini di Servizio e dalle Informative applicabili, è pubblicata sul Sito ed è disponibile al Cliente prima e durante la fruizione dei Servizi. La presente Informativa deve essere letta congiuntamente ai Termini di Servizio e alle altre Informative applicabili; in caso di discrepanze, prevalgono i Termini di Servizio. Le informazioni pubblicate sulle pagine del Sito hanno, invece, carattere meramente descrittivo e non sostituiscono quanto previsto nella presente Informativa e nei Termini di Servizio. CheckSig può aggiornare la presente Informativa per riflettere evoluzioni normative, tecnologiche o operative dei Servizi dandone comunicazione al Cliente secondo quanto previsto dai Termini di Servizio.

1 Premessa

1. I termini con iniziale maiuscola non definiti nella presente Informativa hanno il significato attribuito nei Termini di Servizio.
2. La presente Informativa è redatta in coerenza con il Regolamento (UE) 2023/1114 (MiCAR), nei limiti della sua applicabilità e del regime transitorio vigente.
3. L'Informativa illustra, in particolare, i principi fondamentali del servizio di custodia, le misure adottate a tutela delle Cripto-attività dei Clienti, i presidi organizzativi, tecnologici e contrattuali, nonché le modalità di gestione dei rischi operativi e degli eventi rilevanti.

2 Principi generali nella tutela delle Cripto-attività dei Clienti

1. I prestatori di servizi per le Cripto-attività che offrono servizi di custodia e amministrazione per conto dei Clienti sono tenuti a separare le Cripto-attività detenute per conto dei Clienti dal proprio patrimonio e a garantire che i mezzi di accesso alle Cripto-attività dei Clienti siano chiaramente identificati come tali.
2. La Custodia riguarda esclusivamente la conservazione e l'amministrazione delle Cripto-attività, senza alcuna garanzia circa il valore, la stabilità o il funzionamento delle tecnologie sottostanti.
3. In conformità alla normativa applicabile:

- a. le Cripto-attività detenute in custodia sono giuridicamente e operativamente separate dal patrimonio di CheckSig e sono detenute nell'interesse dei Clienti;
- b. i creditori di CheckSig non vantano diritti di rivalsa sulle Cripto-attività dei Clienti nei limiti e secondo le modalità previste dalla normativa applicabile e dalle misure di opponibilità adottate dalla Società;
- c. la proprietà delle Cripto-attività e dei fondi *fiat* resta sempre in capo ai Clienti, anche quando tali disponibilità sono trasferite a CheckSig per la fruizione dei Servizi;
- d. CheckSig non utilizza, investe o impiega le Cripto-attività o i fondi dei Clienti per finalità diverse dall'erogazione dei Servizi richiesti.

3 Presidi di tutela delle Cripto-attività dei Clienti

A tutela delle Cripto-attività dei Clienti, CheckSig adotta presidi articolati su più livelli:

1. Presidi contrattuali

I contratti con i Clienti stabiliscono espressamente che la proprietà delle Cripto-attività resta in capo ai Clienti. Analogamente, gli accordi con fornitori e istituti bancari prevedono misure di segregazione e tutela delle disponibilità dei Clienti.

2. Presidi organizzativi e contabili

CheckSig mantiene evidenze contabili interne idonee a ricostruire in modo puntuale e aggiornato la posizione di ciascun Cliente, distinguendo le Cripto-attività e i fondi *fiat* detenuti per conto della clientela da quelli della Società.

Le evidenze contabili sono aggiornate con continuità operativa, con frequenza giornaliera per i saldi aggregati e periodica per quelli individuali, secondo procedure interne e in funzione delle caratteristiche operative dei sistemi utilizzati.

3. Presidi tecnologici

CheckSig adotta misure idonee a proteggere i mezzi di accesso crittografici (incluse le chiavi private) associati alle Cripto-attività detenute per conto dei Clienti, inclusi meccanismi di crittografia, autenticazione a più fattori, segregazione degli accessi e conservazione dei dispositivi di sicurezza hardware (HSM) in cassette di sicurezza, al fine di prevenire accessi non autorizzati e ridurre i rischi informatici.

4. Presidi assicurativi

CheckSig integra i presidi contrattuali, organizzativi e tecnologici con coperture assicurative private contro il furto delle cripto-attività depositate presso la Società e altri rischi connessi alla custodia (nei limiti e condizioni di polizza).

4 Utilizzi complementari della Custodia

Fermo quanto previsto dai Termini di Servizio e dalle specifiche Informativa applicabili, la Custodia può essere utilizzata per ottenere benefici complementari. Specificatamente:

1. Custodia con Staking protocollare

- a. Il Servizio di Custodia con Staking protocollare è attivato esclusivamente su istruzione e richiesta del Cliente.
 - b. L'attivazione dello Staking può comportare periodi di indisponibilità temporanea delle Cripto-attività oggetto di vincolo, in funzione delle regole del protocollo sottostante e delle relative tempistiche tecniche (ad esempio periodi di attivazione, disattivazione o "timelock").
 - c. Lo Staking può inoltre comportare rischi specifici connessi al funzionamento del protocollo, quali, a titolo esemplificativo, penalità o meccanismi di "slashing" in caso di malfunzionamenti o violazioni delle regole di rete. CheckSig adotta presidi tecnici e organizzativi volti a minimizzare tali rischi, fermo restando che nella misura in cui dipendono dal protocollo sottostante non sono integralmente eliminabili.
 - d. Per le Cripto-attività che supportano lo staking, CheckSig adotta presidi per la gestione e il controllo diretto dei mezzi di accesso crittografici (incluse le chiavi private), per quanto tecnicamente e operativamente possibile.
 - e. Eventuali deleghe a fornitori di infrastrutture o servizi tecnologici sono organizzate in modo da preservare, in modo coerente con il modello di controllo e governance adottato dalla Società, il controllo di CheckSig e prevenire utilizzi non autorizzati, fermo restando quanto tecnicamente richiesto dai protocolli sottostanti e dalle infrastrutture tecnologiche impiegate.
 - f. I proventi eventualmente generati dallo Staking sono attribuiti al Cliente secondo quanto previsto nei Termini di Servizio e nell'Informativa Corrispettivi
- 2. Custodia a Garanzia (escrow)**
- a. Nell'ambito di operazioni di garanzia tra Clienti, CheckSig offre un servizio di custodia e amministrazione delle Cripto-attività vincolate, nel rispetto delle istruzioni contrattualmente concordate.
 - b. CheckSig non svolge attività di promozione, intermediazione, consulenza o concessione di finanziamenti.

5 Modello di custodia

1. Il modello di custodia adottato da CheckSig si basa su un'architettura multilivello progettata per offrire elevati standard di sicurezza, segregazione e controllo.
2. I wallet di Custodia di CheckSig comprendono:
 - a. deposit wallet: utilizzati per la ricezione e il transito iniziale delle Cripto-attività depositate dai Clienti;
 - b. frozen wallet: destinati alla conservazione a massima sicurezza delle Cripto-attività della clientela;
 - c. cold wallet: utilizzati per il transito controllato delle Cripto-attività in uscita dai frozen wallet;
 - d. protocol staking wallet: dedicati alle Cripto-attività vincolate in staking;
 - e. liquidity wallet: utilizzati per esigenze operative temporanee connesse ai Servizi di Trading.

3. CheckSig può inoltre detenere Cripto-attività presso conti aperti presso altri prestatori di servizi per le Cripto-attività autorizzati, esclusivamente nella misura necessaria all'erogazione dei Servizi di scambio ed esecuzione ordini.
4. I frozen wallet, i cold wallet e i protocol staking wallet sono gestiti tramite dispositivi di sicurezza hardware (HSM) e non sono direttamente accessibili tramite Internet.

6 Sicurezza e gestione degli accessi

1. L'accesso ai wallet è protetto da sistemi di autenticazione a più fattori;
2. le operazioni di movimentazione richiedono l'autorizzazione di più soggetti (Multi-Signature o Multi-Party Computation) secondo logiche di segregazione dei ruoli;
3. sono adottate procedure di disaster recovery e business continuity per consentire il ripristino dei fondi in caso di eventi critici.

7 Politiche di movimentazione

1. Le Cripto-attività possono essere movimentate esclusivamente nel rispetto di procedure di autorizzazione predefinite.
2. I depositi sono trasferiti dai deposit wallet ai frozen wallet solo dopo il completamento dei controlli di conformità.
3. I prelievi dai frozen wallet richiedono autorizzazioni multiple, incluso un quorum di agenti terzi per ridurre il rischio di operazioni fraudolente.
4. I prelievi dai cold wallet richiedono autorizzazioni multiple.
5. In caso di incidenti di sicurezza sono attivate procedure di emergenza per il trasferimento controllato dei fondi.

8 Attestazione pubblica delle riserve

1. Con frequenza almeno mensile, CheckSig pubblica una Proof-of-Reserves, intesa come attestazione pubblica verso l'esterno finalizzata a consentire verifiche indipendenti sulla disponibilità delle Cripto-attività detenute in custodia.
2. La Proof-of-Reserves si basa su evidenze verificabili pubblicamente, quali informazioni e transazioni tracciabili sulle blockchain di riferimento e documentazione resa disponibile da CheckSig.
3. L'attestazione consente di verificare la riconducibilità degli indirizzi e dei saldi delle Cripto-attività agli ambienti di custodia di CheckSig e supporta le attività di controllo e riconciliazione.
4. La Proof-of-Reserves attesta, secondo le modalità pubblicate sul Sito, elementi di disponibilità e controllabilità delle Cripto-attività in custodia (indirizzi/saldi e controllo dei mezzi di accesso), ma non costituisce attestazione individuale della posizione del singolo Cliente.

5. La Proof-of-Reserves non rappresenta un bilancio, né una verifica delle passività o degli impegni di CheckSig verso i Clienti. Pertanto, non costituisce una certificazione contabile né una garanzia di solvibilità, ma uno strumento di trasparenza verificabile.

9 Fork

CheckSig monitora costantemente gli eventi di fork. In caso di Fork quantitativamente rilevante, come definito nei Termini di Servizio, la Società valuta la fattibilità tecnica, la conformità normativa e la rilevanza economica dell'evento e delibera se estendere il servizio di custodia alla nuova Cripto-attività. I Clienti sono informati tempestivamente dell'esito.

10 Gestione degli incidenti informatici

1. CheckSig adotta un sistema strutturato di gestione degli incidenti informatici e operativi rilevanti, basato su:
 - a. tempestiva identificazione e classificazione degli eventi;
 - b. attivazione di procedure di contenimento e mitigazione;
 - c. tracciamento e registrazione in apposito registro interno;
 - d. analisi delle cause e definizione di misure correttive e preventive;
 - e. comunicazione agli utenti interessati, ove possibile entro termini coerenti con quanto previsto dai Termini di Servizio;
 - f. comunicazione alle autorità competenti, ove richiesto dalla normativa applicabile.
2. In caso di incidente che possa incidere sulla disponibilità, integrità o sicurezza delle Cripto-attività detenute in custodia, CheckSig attiva procedure di emergenza volte alla protezione dei fondi e alla continuità operativa.
3. CheckSig mantiene un registro degli incidenti rilevanti e adotta misure correttive e preventive adeguate per gestire e mitigare gli eventi, in coerenza con i principi e le migliori prassi di gestione del rischio ICT, anche con riferimento al Regolamento DORA, ove applicabile.

11 Rischi tecnologici e di mercato intrinseci alle Cripto-attività

1. La Custodia e l'amministrazione di Cripto-attività comportano rischi tecnologici, operativi e di mercato intrinseci alla natura delle Cripto-attività e delle tecnologie a registro distribuito (DLT), che non dipendono dalla prestazione del servizio di custodia in quanto tale.
2. In particolare, restano integralmente applicabili e richiamati i rischi descritti nei Termini di Servizio e nelle altre Informative applicabili, inclusi, a titolo esemplificativo e non esaustivo:
 - a. rischi di volatilità dei prezzi delle Cripto-attività, che possono determinare variazioni anche significative e improvvise del loro valore economico;

- b. rischi tecnologici connessi alle reti blockchain e ai protocolli DLT, quali malfunzionamenti, congestioni della rete, attacchi informatici al protocollo, errori di implementazione del codice o vulnerabilità non note;
 - c. rischi di irreversibilità delle transazioni, per cui operazioni confermate sul registro distribuito non possono essere annullate o modificate;
 - d. eventi di fork, aggiornamenti di protocollo o modifiche delle regole di consenso, che possono incidere sul funzionamento della rete, sulla disponibilità delle Cripto-attività o sulle tempistiche operative;
 - e. rischi di interruzione, rallentamento o indisponibilità temporanea delle reti, indipendenti dalla volontà o dal controllo di CheckSig.
3. Tali rischi non sono eliminabili né mitigabili integralmente da CheckSig e non costituiscono di per sé inadempimento del servizio di custodia, fermo restando quanto previsto in materia di responsabilità nei casi di perdita imputabile al servizio prestato, ai sensi dei Termini di Servizio e della normativa applicabile.

12 Coperture assicurative

1. Le coperture assicurative sono strutturate in modo da proteggere la Società e, indirettamente, i Clienti rispetto a specifici rischi operativi, inclusi, a titolo esemplificativo, eventi di natura informatica, frodi interne o esterne, errori operativi e altri eventi che possano determinare perdite patrimoniali connesse al servizio di custodia, nei limiti, alle condizioni e secondo i massimali previsti dalle relative polizze.
2. Le coperture assicurative:
 - a. non sostituiscono né limitano i presidi di segregazione patrimoniale e di sicurezza adottati dalla Società;
 - b. non costituiscono garanzia assoluta di integrale ristoro in ogni circostanza;
 - c. operano esclusivamente nei casi e secondo le modalità previste dalle condizioni di polizza applicabili.
3. Le informazioni aggiornate in merito alle coperture assicurative in essere, inclusi l'identità dell'assicuratore e i principali massimali, sono rese disponibili nella sezione dedicata del Sito.

Storico delle versioni precedenti

Versione	Changelog	Entrata in vigore
2.1.0	Revisione del pacchetto contrattuale per maggiore coerenza tra i diversi documenti	2026-02-18