

Informativa sulla Policy di trasferimento delle Cripto-attività

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. 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 descrive in modo specifico le caratteristiche, le modalità operative, i presidi di sicurezza e i principali rischi del servizio di trasferimento di cripto-attività prestato da CheckSig.
3. Le informazioni qui fornite al Cliente includono anche elementi relativi ai requisiti tecnici dei dispositivi utilizzati, ai principali presidi organizzativi e tecnologici adottati dalla Società e ai rischi operativi e di cybersicurezza connessi al Servizio, in conformità alla normativa applicabile.
4. Le commissioni per l'esecuzione del Servizio di Trasferimento di Cripto-attività applicate da CheckSig sono indicate nell'*Informativa sui Corrispettivi per la fruizione dei Servizi* (di seguito, anche "**Informativa Corrispettivi**").
5. Il Cliente può in ogni momento richiedere via e-mail una copia digitale della Policy sul servizio di trasferimento di cripto-attività.

2 Natura del Servizio di Trasferimento

1. Il Servizio di Trasferimento consiste nell'esecuzione, su istruzione del Cliente, di operazioni di prelievo di Cripto-attività detenute in Custodia verso indirizzi esterni ovvero di deposito di Cripto-attività verso wallet riconducibili a CheckSig nell'ambito della Custodia.
2. Il Servizio è accessorio alla Custodia e non costituisce servizio di pagamento né trasferimento di fondi fiat. Il trasferimento avviene mediante registrazione su tecnologia a registro distribuito (DLT) ed è disciplinato dalle regole del protocollo blockchain di riferimento.
3. Il Servizio è prestato esclusivamente con riferimento a indirizzi di Cripto-attività riconducibili al Cliente, previamente validati e associati al suo profilo. CheckSig non presta servizi di trasferimento verso o per conto di soggetti terzi.
4. Il Servizio non è prestato in relazione a token qualificabili come EMT, non integra attività di consulenza e non copre rischi connessi a wallet esterni non gestiti da

CheckSig. Inoltre, il Servizio non garantisce tempi certi di regolamento sulla blockchain, in quanto tali tempi dipendono dal funzionamento della rete sottostante.

5. L'accesso al Servizio richiede l'utilizzo di dispositivi compatibili con browser aggiornati o applicazione ufficiale, connessione Internet sicura e abilitazione dell'autenticazione multifattoriale.
6. Il Cliente è responsabile dell'adeguatezza e sicurezza dei dispositivi utilizzati per accedere al Servizio (quali computer, smartphone e connessioni Internet), inclusa la protezione da malware, accessi non autorizzati e vulnerabilità software. L'utilizzo di dispositivi non sicuri o compromessi può comportare rischi di accesso abusivo, alterazione delle istruzioni di trasferimento o perdita delle Cripto-attività, non imputabili alla Società.

3 Procedura operativa di trasferimento

1. Il Cliente può disporre un trasferimento esclusivamente tramite App, mediante autenticazione forte e successiva conferma dell'operazione secondo le procedure rese di volta in volta disponibili da CheckSig.
2. L'autorizzazione del trasferimento è prestata dal Cliente in forma elettronica, attraverso l'accesso autenticato all'App e la conferma finale dell'istruzione di trasferimento, ed è registrata nei sistemi di CheckSig unitamente ai relativi dati informatici di tracciamento.
3. Per effettuare un trasferimento, il Cliente deve fornire almeno le seguenti informazioni:
 - a. la tipologia di cripto-attività;
 - b. l'importo da trasferire;
 - c. l'indirizzo di destinazione;
 - d. la rete blockchain selezionata;
 - e. eventuali ulteriori informazioni richieste ai fini dei controlli di sicurezza e conformità.
4. Prima della conferma, il sistema mostra in modo chiaro:
 - a. l'indirizzo di destinazione;
 - b. la rete selezionata;
 - c. l'importo;
 - d. le eventuali commissioni;
 - e. un'avvertenza esplicita sull'irreversibilità dell'operazione.
5. Il Cliente è tenuto a verificare attentamente i dati prima della conferma.
6. Gli indirizzi di destinazione devono essere preventivamente verificati e associati al Cliente secondo le procedure interne; indirizzi non validati non sono abilitati all'operatività.
7. Ogni richiesta è soggetta a controlli interni, inclusi quelli previsti dalla normativa antiriciclaggio e Travel Rule, verifiche su blacklist e strumenti di blockchain analytics, controlli sui limiti operativi e, ove necessario, procedure rafforzate in funzione del profilo di rischio dell'operazione. CheckSig può sospendere o ritardare l'esecuzione qualora siano richiesti ulteriori accertamenti.

8. Le operazioni di uscita dai wallet di custodia sono sottoposte a meccanismi di autorizzazione multilivello (Multi-Signature o MPC), con segregazione dei ruoli e tracciabilità delle attività. Una volta trasmessa alla rete blockchain e confermata secondo le regole del protocollo, la transazione è tecnicamente irreversibile.
9. Ai fini della determinazione del momento di ricezione, fa fede la registrazione con marca temporale generata dal sistema informatico di CheckSig al completamento dell'autenticazione forte.
10. Le istruzioni ricevute entro le ore 18:00 (CET/CEST) in un giorno lavorativo sono prese in carico nella medesima giornata operativa; quelle ricevute oltre tale orario si considerano ricevute nel giorno lavorativo successivo. In ogni caso, l'esecuzione dell'istruzione resta soggetta al Tempo tecnico di disponibilità delle Cripto-attività (fino a 10 giorni lavorativi; in condizioni operative ordinarie la disponibilità è usualmente immediata — cfr. art. 2.22 dei Termini di Servizio).
11. I tempi di regolamento sulla blockchain restano invece dipendenti dal protocollo sottostante e non sono nella disponibilità di CheckSig.
12. Per ciascuna Cripto-attività supportata, CheckSig riporta nell'Appendice A l'indicazione della rete DLT utilizzata per il trasferimento, il numero di conferme necessarie affinché una transazione sia considerata completata, e il tempo medio stimato per il buon esito della transazione in condizioni normali. I tempi effettivi e il numero di conferme possono tuttavia variare in base alle condizioni della rete (ad esempio, in caso di traffico elevato o variazioni delle commissioni), fattori che non dipendono da CheckSig. CheckSig aggiorna periodicamente l'Appendice A per riflettere eventuali cambiamenti nelle cripto-attività supportate, nelle reti utilizzate o nei criteri adottati per determinare quando una transazione può essere considerata completata (o irreversibile).
13. Dopo l'esecuzione del trasferimento, il Cliente riceve in App le seguenti informazioni:
 - a. ammontare e tipologia di cripto-attività trasferite o ricevute;
 - b. indirizzo DLT o numero di conto cripto del beneficiary (destinatario) e, ove applicabile, dell'originator (mittente);
 - c. nominativo/denominazione dell'originator e del beneficiary, ove applicabile;
 - d. data/ora e data valuta di addebito o accredito (debit/credit value date);
 - e. un riferimento univoco dell'operazione che consenta al Cliente di identificarla (es. TXID);
 - f. eventuali oneri/commissioni addebitati da CheckSig in relazione al trasferimento, (nel caso in cui non siano previsti, l'importo è indicato come pari a zero) e, ove pertinente, indicazione separata tra oneri di servizio e altri costi
14. Tali informazioni sono rese disponibili gratuitamente in formato elettronico per ciascun trasferimento.
15. L'eventuale mancata visualizzazione della conferma del trasferimento in App non incide sulla corretta ricezione ed esecuzione dell'istruzione, ove la stessa risulti validamente registrata nei sistemi informatici aziendali. In tale eventualità, CheckSig assicura la messa a disposizione della conferma su supporto durevole mediante canali alternativi ufficiali e/o idonei a garantire tracciabilità e conservazione (quali, a

titolo esemplificativo, invio tramite e-mail all'indirizzo registrato o comunicazione tramite assistenza clienti con successiva trasmissione documentale).

16. L'autorizzazione è registrata nei sistemi di CheckSig e costituisce prova dell'istruzione impartita dal Cliente.
17. Il Cliente può revocare l'istruzione di trasferimento esclusivamente fino al momento in cui la stessa non sia stata presa in carico operativamente da CheckSig. Una volta avviato il processo tecnico di esecuzione o trasmessa la transazione alla rete blockchain, l'istruzione diviene irrevocabile e non modificabile.

4 Diritti del Cliente

1. Il Cliente ha diritto a:
 - a. impartire istruzioni di trasferimento nei limiti dei Termini di Servizio;
 - b. ricevere informazioni chiare sui costi, i tempi stimati ed i rischi;
 - c. essere informato senza ingiustificato ritardo in caso di ritardi significativi o incidenti rilevanti;
 - d. ottenere evidenza tecnica del trasferimento (es. transaction ID);
 - e. presentare reclamo secondo la Policy sulla gestione dei reclami.
2. Il Cliente può revocare l'Ordine fino al momento in cui l'istruzione non sia stata presa in carico operativamente da CheckSig. Una volta avviato il processo tecnico di esecuzione o trasmessa la transazione alla rete blockchain, l'istruzione diviene irrevocabile e non modificabile.
3. Il Cliente può consultare lo storico delle operazioni in qualsiasi momento tramite App.

5 Responsabilità del Cliente e segnalazioni

1. Il Cliente è responsabile:
 - a. della correttezza e completezza delle informazioni fornite;
 - b. della correttezza dell'indirizzo blockchain indicato;
 - c. della correttezza della rete selezionata;
 - d. della custodia delle proprie Credenziali.
2. Errori nell'indicazione dei dati possono comportare la perdita definitiva delle Cripto-attività.
3. Il Cliente deve segnalare senza indugio eventuali operazioni di trasferimento non autorizzate o erroneamente eseguite, utilizzando esclusivamente i canali ufficiali. La segnalazione deve avvenire entro 2 giorni dalla conoscenza dell'operazione e deve contenere tutte le informazioni utili alla ricostruzione dell'operazione contestata.
4. In caso di operazione non autorizzata imputabile a carenze del servizio, la responsabilità di CheckSig è disciplinata dai Termini di Servizio e dalla normativa applicabile, inclusi gli articoli 75 e 82 MiCAR.
5. CheckSig comunica al Cliente l'esito delle verifiche e le eventuali misure adottate.
6. Il Cliente prende atto che le transazioni su blockchain sono, per loro natura, irreversibili.

6 Responsabilità di CheckSig

1. CheckSig è responsabile nei confronti del Cliente per i trasferimenti di cripto-attività non autorizzati, non disposti o eseguiti in modo non corretto, nei limiti previsti dalla normativa applicabile.
2. In tali casi, CheckSig:
 - a. adotta misure ragionevoli per rimediare all'errore;
 - b. ove tecnicamente possibile, supporta il recupero delle cripto-attività;
 - c. nei casi previsti dalla legge, può essere tenuta al ristoro del danno subito dal Cliente.
3. CheckSig non è responsabile nei casi in cui l'errore o l'impossibilità di recupero derivi da:
 - a. informazioni inesatte o incomplete fornite dal Cliente (incluso l'indirizzo di destinazione);
 - b. selezione errata della rete blockchain;
 - c. caratteristiche intrinseche della tecnologia DLT, inclusa l'irreversibilità delle transazioni;
 - d. eventi al di fuori del controllo della Società, inclusi casi di forza maggiore.

7 Rischi specifici del Servizio

1. Il Servizio di Trasferimento comporta rischi intrinseci quali:
 - a. irreversibilità delle transazioni;
 - b. errori di digitazione dell'indirizzo;
 - c. selezione errata della rete;
 - d. congestione della blockchain;
 - e. attacchi informatici ai wallet esterni del Cliente;
 - f. sospensioni o restrizioni per obblighi normativi.
2. Il Servizio di Trasferimento comporta ulteriori rischi connessi alla sicurezza informatica del Cliente, quali:
 - a. rischi derivanti dall'utilizzo di dispositivi del Cliente non adeguatamente protetti (es. malware, phishing, compromissione delle credenziali);
 - b. rischi connessi a vulnerabilità dei sistemi informatici, attacchi informatici o eventi di cyber security che possano incidere sulla disponibilità, integrità o riservatezza del Servizio;
 - c. rischi operativi residui derivanti da possibili malfunzionamenti, indisponibilità temporanee o errori nei processi, nonostante i presidi adottati.
3. Tali rischi non sono integralmente eliminabili e non costituiscono di per sé inadempimento del Servizio.

8 Politiche di sicurezza

- 1.

2. CheckSig adotta un sistema integrato di misure organizzative, tecniche e procedurali volto a garantire la sicurezza, l'integrità, la disponibilità e la tracciabilità delle Cripto-attività e delle operazioni di trasferimento, in coerenza con i presidi adottati nel Servizio di Custodia e amministrazione delle Cripto-attività.
3. In particolare, la Società adotta i seguenti presidi:
 - a. Segregazione dei wallet e modello omnibus: la Società adotta un modello di custodia di tipo omnibus. In tale contesto, la segregazione dei wallet è realizzata su base logica e funzionale, mediante distinzione dei wallet per finalità operative. La segregazione dei wallet non implica, nel modello omnibus adottato dalla Società, la creazione di wallet on-chain individuali per ciascun Cliente. La separazione delle disponibilità della clientela è assicurata principalmente a livello giuridico, contabile e organizzativo, mediante sistemi interni di registrazione, riconciliazione e controllo che consentono in ogni momento l'identificazione e la ricostruzione della posizione individuale di ciascun Cliente;
 - b. Gestione e custodia delle chiavi crittografiche: i processi di generazione, distribuzione, conservazione, utilizzo e revoca delle chiavi crittografiche sono disciplinati da procedure interne che prevedono l'utilizzo di tecnologie di protezione avanzate (tra cui HSM, MPC o multi-signature), la frammentazione dei poteri di controllo e la prevenzione dell'accesso unilaterale alle chiavi.;
 - c. Architettura multilivello dei wallet: le Cripto-attività sono detenute mediante una struttura articolata su più livelli (es. wallet di deposito, liquidity wallet e cold storage), con prevalente utilizzo di wallet offline per la conservazione e utilizzo limitato di wallet operativi per l'esecuzione delle operazioni;
 - d. Controlli di accesso e segregazione dei ruoli: l'accesso ai sistemi è limitato secondo il principio del "least privilege" ed è soggetto a autenticazione forte, tracciamento e logging. Le funzioni operative, autorizzative e di controllo sono segregate tra soggetti distinti, al fine di prevenire conflitti di interesse e accessi non autorizzati;
 - e. Monitoraggio e sicurezza informatica: i sistemi sono protetti mediante monitoraggio continuo delle operazioni e delle infrastrutture, utilizzo di sistemi di logging, rilevazione delle anomalie e strumenti di analisi delle transazioni su blockchain, nonché presidi di sicurezza logica e fisica delle infrastrutture;
 - f. Procedure operative e tracciabilità: tutte le operazioni sono eseguite nel rispetto di procedure operative formalizzate che disciplinano l'intero ciclo di vita del trasferimento, dalla ricezione dell'istruzione alla sua esecuzione. Tali procedure prevedono controlli multilivello, automatici e, ove necessario, manuali, nonché la registrazione e tracciabilità completa delle attività nei sistemi informativi della Società, al fine di garantire la verificabilità delle operazioni, la ricostruibilità degli eventi e la coerenza con le evidenze contabili interne e i presidi di sicurezza adottati;
 - g. Protezione dei dati: i dati e le comunicazioni sono protetti mediante protocolli sicuri e tecniche di cifratura, sia in transito sia, ove applicabile, a riposo, al fine di prevenire accessi non autorizzati, alterazioni o perdita di informazioni;

- h. Gestione degli incidenti e continuità operativa: la Società adotta procedure strutturate di gestione degli incidenti ICT e piani di business continuity e disaster recovery, inclusa la disponibilità di infrastrutture ridondate e procedure di ripristino, finalizzati a garantire la resilienza dei sistemi e la continuità del servizio anche in scenari di indisponibilità parziale;
- 4. Controlli e verifiche periodiche: i presidi di sicurezza sono soggetti a verifiche periodiche, inclusi controlli interni, attività di audit e, ove applicabile, test di sicurezza (quali vulnerability assessment e penetration test), al fine di assicurarne l'efficacia e l'aggiornamento rispetto all'evoluzione delle minacce.
- 5. Le comunicazioni ufficiali relative al Servizio avvengono esclusivamente tramite App o email con dominio ufficiale. Canali di messaggistica istantanea hanno natura accessoria e non sostitutiva.
- 6. CheckSig non richiede mai chiavi private o seed phrase.
- 7. La Società si avvale di risorse umane specializzate e di infrastrutture tecnologiche adeguate alla gestione dei rischi operativi e di cybersicurezza, tra cui sistemi di monitoraggio continuo, controlli sugli accessi, soluzioni cloud resilienti e strumenti di sicurezza avanzati. Tali risorse sono organizzate secondo un modello di governance che prevede ruoli e responsabilità definiti nella gestione degli incidenti ICT e nella protezione delle infrastrutture, al fine di garantire una risposta tempestiva, efficiente e completa agli eventi avversi.
- 8. Nonostante i presidi adottati, permangono rischi residui legati alla natura delle tecnologie utilizzate e a possibili attacchi informatici sofisticati, che non possono essere completamente eliminati.

9 Gestione degli incidenti

- 1. In caso di frode sospetta o effettiva, accesso non autorizzato o tentato accesso non autorizzato, compromissione o sospetta compromissione delle credenziali, minaccia alla sicurezza o incidente ICT suscettibile di incidere sulla sicurezza dell'account del Cliente, sulla corretta esecuzione dei trasferimenti o sulla disponibilità del Servizio, CheckSig attiva una procedura sicura di notifica al Cliente senza ingiustificato ritardo, non appena ciò sia compatibile con le esigenze di contenimento del rischio, con la tutela dell'integrità dei sistemi e con eventuali obblighi di legge.
- 2. La notifica è resa, di norma, tramite App e, ove opportuno, mediante e-mail inviata all'indirizzo registrato dal Cliente o tramite altri canali ufficiali, sicuri e tracciabili previamente messi a disposizione dalla Società.
- 3. La comunicazione indica, ove possibile:
 - a. la natura dell'evento o della minaccia rilevata;
 - b. il momento della rilevazione;
 - c. i possibili effetti sul Servizio o sui trasferimenti di cripto-attività;
 - d. le misure cautelative o correttive adottate da CheckSig;
 - e. le eventuali azioni richieste al Cliente.
- 4. CheckSig non richiede mai al Cliente, nell'ambito di tali notifiche, la comunicazione di chiavi private, seed phrase o credenziali complete di autenticazione. Eventuali azioni

richieste al Cliente sono eseguite esclusivamente tramite App o altri canali autenticati ufficialmente indicati da CheckSig.

10 Sospensione o rifiuto del trasferimento

1. CheckSig adotta presidi di monitoraggio e controllo dei trasferimenti basati su un approccio proporzionato al rischio, al fine di prevenire frodi, accessi non autorizzati e utilizzi illeciti del servizio.
2. In presenza di obblighi normativi, sospetti di frode, accessi non autorizzati, minacce alla sicurezza o rischi operativi rilevanti, CheckSig può:
 - a. sospendere, ritardare o rifiutare l'esecuzione del trasferimento;
 - b. sottoporre l'operazione a verifiche aggiuntive;
 - c. richiedere informazioni o documentazione al Cliente;
 - d. adottare misure di contenimento e mitigazione del rischio.
3. Le decisioni sono adottate secondo un approccio basato sul rischio, che tiene conto, tra l'altro dell'importo dell'operazione, della novità o rischiosità dell'indirizzo di destinazione, di eventuali alert generati dai sistemi di monitoraggio blockchain e degli obblighi derivanti dalla normativa applicabile, inclusa la normativa antiriciclaggio e la Travel Rule.
4. In tali casi, CheckSig informa il Cliente senza ingiustificato ritardo, nei limiti consentiti dalla legge, via email, notifiche nell'App e/o altri canali di comunicazione sicuri messi a disposizione.
5. Le comunicazioni includono, ove possibile:
 - a. la natura dell'evento o del rischio rilevato;
 - b. le misure adottate da CheckSig;
 - c. le eventuali azioni richieste al Cliente ai fini del completamento o della sicurezza dell'operazione.

Appendice A: Cripto-attività e reti supportate e tempi di conferma

La presente Appendice A costituisce parte integrante dell'Informativa sul servizio di trasferimento di cripto-attività.

Per ciascuna cripto-attività supportata, la Società indica di seguito:

- la rete basata su tecnologia a registro distribuito (DLT) supportata per il trasferimento;
- il numero ragionevolmente stimato di conferme di blocco necessario affinché il trasferimento sia considerato irreversibile, ove tale parametro sia applicabile;
- il tempo ragionevolmente stimato affinché il trasferimento sia considerato irreversibile sulla relativa rete DLT, ovvero sufficientemente irreversibile in caso di regolamento probabilistico.

I valori indicati nella presente Appendice rappresentano **stime ragionevoli** formulate dalla Società sulla base delle caratteristiche della rete DLT, delle relative regole di funzionamento e delle prassi operative adottate. Tali valori possono variare in funzione, tra l'altro, della congestione della rete, delle condizioni operative della blockchain, di eventuali eventi tecnici, fork, aggiornamenti del protocollo o altri fattori esterni.

Cripto-attività	Nome	Rete DLT supportata	Numero minimo conferme	Tempo minimo stimato
BTC	Bitcoin	Bitcoin	3	circa 30 min
ETH	Ether	Ethereum	50	circa 15 min
SOL	Solana	Solana	1	circa 1–2 min
XRP	Xrp	Ripple	1	circa 1–2 min
AAVE	Aave	Ethereum	50	circa 15 min
ENA	Ethena	Ethereum	50	circa 15 min
FLOKI	Floki	Ethereum	50	circa 15 min
GRT	Graph	Ethereum	50	circa 15 min
INJ	Injective	Ethereum	50	circa 15 min
LINK	Chainlink	Ethereum	50	circa 15 min
MKR	Makerdao	Ethereum	50	circa 15 min
ONDO	Ondo	Ethereum	50	circa 15 min
PEPE	Pepe	Ethereum	50	circa 15 min
SHIB	Shiba-Inu	Ethereum	50	circa 15 min
SKY	Sky	Ethereum	50	circa 15 min
UNI	Uniswap	Ethereum	50	circa 15 min
WBTC	Wrapped-Bitcoin	Ethereum	50	circa 15 min

PENGU	Pudgy-Penguins	Solana	1	circa 1–2 min
RENDER	Render	Solana	1	circa 1–2 min
TRUMP	Official-Trump	Solana	1	circa 1–2 min
POL	Polygon	Polygon	250	circa 10–15 min
BCH	Bitcoin-Cash	Bitcoin Cash	15	circa 150 min
ADA	Cardano	Cardano	15	circa 60 min
TIA	Celestia	Celestia	n.a.	circa 60 min
ALGO	Algorand	Algorand	n.a.	circa 60 min
AVAX	Avalanche	Avalanche	n.a.	circa 60 min
TAO	Bittensor	Bittensor	n.a.	circa 60 min
DOGE	Dogecoin	Dogecoin	40	circa 60 min
APT	Aptos	Aptos	n.a.	circa 60 min
FIL	Filecoin	Filecoin	200	circa 100 min
ICP	Internet-Computer	Internet Computer Protocol	n.a.	circa 60 min
DOT	Polkadot	Polkadot	n.a.	circa 60 min
XLM	Stellar	Stellar	n.a.	circa 60 min
SUI	Sui	Sui	1000	circa 60 min
ZEC	Zcash	Zcash	50	circa 60 min
ARB	Arbitrum	Arbitrum One	40	circa 60 min
ETC	Ether-Classic	Ethereum Classic	2880	circa 12 ore
LTC	Litecoin	Litecoin	12	circa 60 min
NOT	Notcoin	The Open Network	n.a.	circa 60 min

Laddove la Società valuti l'irreversibilità o la sufficiente irreversibilità del trasferimento prevalentemente sulla base del tempo di consolidamento della rete o di altri parametri tecnico-operativi, anziché in funzione di un numero predeterminato di conferme di blocco, la colonna "Numero minimo conferme" reca l'indicazione "n.a.".

- **Nome documento:** informativa-trasferimento
- **Stato:** Approvato
- **Organo approvante:** Amministratore delegato
- **Data di approvazione:** 2026-07-13

Storico delle versioni

Versione	Changelog
1.2.1	Sostituito riferimento ad "Area Privata" con "App"
1.2.0	1. integrata la descrizione delle misure organizzative e tecnologiche adottate per la segregazione delle Cripto-attività, con specifico riferimento all'operatività in regime di wallet omnibus; 2. ampliata la descrizione dei presidi di sicurezza adottati; 3. inserito un riferimento all'Informativa sui Corrispettivi per la fruizione dei Servizi circa le commisione applicate al Servizi di Trasferimento di Cripto-attività.
1.1.0	1. revisione organica dell'informativa sul servizio di trasferimento di cripto-attività per allinearla ai rilievi dell'Autorità e rendere più puntuale la descrizione del servizio, dei presidi di sicurezza e dei rischi applicabili; 2. chiarito all'articolo 2 il perimetro del Servizio, precisando che i trasferimenti sono consentiti esclusivamente da e verso indirizzi riconducibili al Cliente, previamente validati e associati al suo profilo, con esclusione di trasferimenti verso o per conto di soggetti terzi; 3. integrato l'articolo 3 sulla procedura operativa, specificando le modalità di autorizzazione elettronica, i dati minimi richiesti per impartire l'istruzione, i controlli preliminari, la verifica preventiva degli indirizzi, il momento di ricezione dell'ordine, la revocabilità dell'istruzione fino alla presa in carico operativa e la registrazione dell'autorizzazione nei sistemi di CheckSig; 4. precisate le regole sui tempi di esecuzione, chiarendo che la presa in carico giornaliera resta distinta dai tempi tecnici di disponibilità delle cripto-attività e dai tempi di regolamento della rete blockchain; 5. riorganizzati i contenuti già presenti nel previgente articolo 6 ("Tempi di esecuzione e irreversibilità"), ora assorbiti e sviluppati nell'articolo 3 e nella nuova Appendice A; 6. introdotta l'Appendice A, quale parte integrante dell'informativa, contenente per ciascuna cripto-attività supportata la rete DLT utilizzata, il numero di conferme richieste o, ove non applicabile, l'indicazione che la valutazione avviene secondo altri parametri tecnico-operativi, nonché il tempo stimato per la sufficiente irreversibilità del trasferimento; 7. integrata la disciplina dei diritti del Cliente e della responsabilità delle parti, anche con riguardo ai casi di operazioni non autorizzate, informazioni inesatte fornite dal Cliente, irreversibilità tecnica delle transazioni ed eventi fuori dal controllo della Società; 8. rafforzate le sezioni sui rischi specifici del Servizio, includendo in modo espresso i rischi operativi e di cybersicurezza connessi ai dispositivi del Cliente, a malware, phishing, compromissione delle credenziali, indisponibilità temporanee e altri eventi ICT; 9. ampliata la descrizione dei presidi organizzativi e tecnologici adottati da CheckSig, inclusi monitoraggio continuo, controlli sugli accessi, infrastrutture resilienti e governance interna nella gestione degli incidenti; 10. integrata la sezione sulla gestione degli incidenti, prevedendo notifiche al Cliente in caso di frode sospetta o effettiva, accessi non autorizzati, compromissione delle credenziali, minacce alla sicurezza o altri incidenti ICT rilevanti; 11. riformulata la disciplina sulla sospensione, ritardo o rifiuto del trasferimento, chiarendo il ruolo dei controlli basati sul rischio, delle verifiche aggiuntive e delle comunicazioni al Cliente nei limiti consentiti dalla legge.

1.0.0	prima emissione
-------	-----------------