QUADERNO IV

LA CHIAVE PRIVATA

Accesso, segreto e potere nell'era della proprietà digitale

La chiave privata non protegge soltanto un valore:
decide chi può esistere davanti a quel valore.

FLORIANO RIGHETTI

ESTRATTO GRATUITO | QUADERNO IV

La Chiave Privata

Quaderni di Custodia Digitale · Quaderno IV

Floriano Righetti

Edizione definitiva · settembre 2026

florianorighetti.ch

Questo quaderno ha finalità culturali e informative. Non costituisce consulenza finanziaria, legale, fiscale o d'investimento. Le indicazioni vanno valutate rispetto agli strumenti e alle circostanze concrete.

Non inserire segreti reali nei modelli del libro. I documenti compilati restano riservati anche quando non contengono credenziali. Le scene narrative sono esempi illustrativi.

Testo e riferimenti verificati il 12 settembre 2026.

ESTRATTO GRATUITO

Capitolo 1: Non una password (pp. 7-14).

Il testo e la numerazione delle pagine riproducono l'edizione integrale. L'indice presenta il libro completo: i capitoli non inclusi in questa anteprima non sono collegati.

La pagina finale rimanda alla scheda del quaderno sul sito dell'autore.

Indice

Nota al lettore

Il quaderno esamina la chiave privata come strumento di firma e come responsabilità di custodia. Distingue segreti, accesso operativo e recupero, senza proporre una configurazione universale. Gli esempi riguardano soprattutto wallet crittografici: altre applicazioni delle chiavi possono avere regole e procedure diverse.

La custodia digitale è un territorio dove le parole semplici possono diventare pericolose. Possedere, perdere, firmare, salvare, condividere, proteggere: sembrano verbi ordinari. Ma quando entrano in sistemi crittografici assumono conseguenze nuove. Una distrazione può trasformarsi in perdita definitiva. Una frase conservata male può diventare accesso per qualcun altro. Un gesto compiuto in fretta può avere effetti che nessuno sportello potrà annullare.

Questo non significa che la self-custody sia un atto eroico riservato a pochi specialisti. Significa l'opposto: se il digitale diventa valore, identità, memoria e accesso, allora la cultura della custodia deve diventare più comune, più sobria, più comprensibile. Non basta dire alle persone di stare attente. Bisogna dare forma a ciò a cui dovrebbero fare attenzione.

La chiave privata è il punto in cui questa responsabilità diventa concreta. Non è soltanto un elemento tecnico. È una soglia. Decide chi può autorizzare, chi può provare, chi può muovere, chi può perdere, chi può trasmettere. Nel mondo fisico, molte porte hanno copie, fabbri, registri, testimoni, sportelli, procedure di recupero. Nel mondo crittografico, alcune porte non hanno un custode centrale. La libertà che ne deriva è reale, ma non è gratuita.

La scelta della custodia dipende da competenze, patrimonio, frequenza d'uso e persone coinvolte. Assistenza, controlli condivisi e procedure successorie possono essere necessari. Conta che il sistema sia comprensibile, sostenibile, verificabile e trasmissibile nel contesto concreto.

Leggere questo quaderno significa rallentare davanti a un oggetto invisibile. La chiave privata non si vede come una chiave di metallo, non pesa in tasca, non tintinna sul tavolo, non si riconosce per forma. Eppure può aprire più di una porta. Può aprire valore, identità, memoria, contratti, prove, accessi. Può anche chiuderli per sempre.

1 Non una password

Una parola troppo piccola

Abbiamo chiavi di casa, chiavi dell'auto, chiavi dell'ufficio, chiavi di sicurezza, chiavi di lettura. Sappiamo che una chiave apre qualcosa, che va conservata, che non andrebbe lasciata ovunque. La parola porta con sé un'intera educazione materiale: il gesto di girare una serratura, il rumore del metallo, il mazzo in tasca, la copia consegnata a qualcuno di fidato, la paura di averla persa.

Una chiave privata è un dato segreto usato da un algoritmo crittografico. Nel contesto della firma, consente di produrre un risultato verificabile mediante la chiave pubblica corrispondente. Questa verifica riguarda dati e chiavi: non identifica da sola la persona né dimostra il titolo con cui agisce.

Una password, di solito, si presenta a un servizio. Il servizio la confronta, la accetta o la rifiuta. Dietro la password c'è un sistema che può cambiarla, sospenderla, resettarla, rafforzarla con un secondo fattore, recuperarla tramite procedure di identità. Anche quando la password protegge qualcosa di importante, resta spesso dentro una relazione amministrativa: l'utente da una parte, il servizio dall'altra.

In molti sistemi decentralizzati, l'operazione richiede una firma valida insieme ad altre condizioni: fondi disponibili, regole del protocollo, eventuali soglie o vincoli del contratto. La firma prova una relazione crittografica; la validità dell'operazione dipende dall'insieme dei controlli.

La differenza riguarda il percorso di autorizzazione e recupero. Una password può proteggere anche un archivio cifrato senza assistenza capace di recuperarlo; una chiave può invece essere inserita in un sistema con sostituzione dei firmatari. Il nome dello strumento non basta a descrivere l'architettura.

Password, PIN, seed phrase, chiave privata

Una delle prime confusioni nasce dal fatto che molti elementi della custodia digitale sembrano codici segreti. Password, PIN, seed phrase, chiave privata: tutti possono apparire come stringhe da non mostrare. Ma non sono la stessa cosa.

Una password è spesso una credenziale scelta o impostata per accedere a un servizio. Può essere cambiata. Può essere inserita male alcune volte. Può essere recuperata tramite email, telefono, documento, assistenza. Non sempre, ma abbastanza spesso da aver educato la nostra immaginazione al recupero.

Un PIN è di solito un codice breve che sblocca un dispositivo o autorizza un'azione locale. Protegge l'accesso a uno strumento, non necessariamente il valore ultimo. Può essere importante, ma spesso agisce come barriera pratica davanti a qualcosa di più profondo.

Una seed phrase è una sequenza di parole da cui possono derivare chiavi. È spesso il punto di recupero più delicato di un wallet non custodial. Chi possiede quella frase può, in molti casi, ricostruire l'accesso. Per questo fotografarla, inviarla, salvarla in un cloud o dettarla a qualcuno significa esporre non una password, ma una radice.

La chiave privata è il segreto crittografico che consente di firmare. Può essere generata e gestita dal wallet, derivata da una seed phrase o conservata in forme diverse. L'utente non sempre la vede direttamente, e spesso è bene che non debba manipolarla come testo. Ma la sua funzione resta fondamentale: permette l'atto.

Le conseguenze dipendono dall'elemento coinvolto. Perdere un PIN può bloccare l'uso di un dispositivo; esporre una password può compromettere un account. Una seed phrase può permettere di ricostruire molte chiavi, mentre una singola chiave privata espone le operazioni per cui è valida. Passphrase e condizioni di firma possono aggiungere requisiti.

Dall'entropia all'indirizzo

In un percorso comune, BIP-39 codifica casualità generata dal software in parole con un controllo di integrità. Dalle parole e dall'eventuale passphrase si ricava un seed; BIP-32 descrive come derivarne una gerarchia di chiavi. Gli indirizzi seguono poi le regole della rete e dello script. Le parole non vanno inventate né scelte come una frase personale. [1] [2]

Questa catena non è universale. BIP-39 è molto diffuso, ma non tutti i wallet, protocolli o sistemi di identità usano la stessa codifica, lo stesso percorso di derivazione o gli stessi algoritmi. Un backup deve quindi conservare non soltanto un segreto, ma abbastanza contesto da ricostruire la corretta architettura.

Passphrase e derivazione

Nel percorso BIP-39, la passphrase partecipa alla derivazione del seed e non coincide con il PIN. Una passphrase diversa, anche per un errore di battitura, genera altre chiavi: il sistema può mostrare un wallet valido ma diverso. La sua perdita può rendere inutilizzabile il backup delle sole parole. [1]

Anche il percorso di derivazione e il tipo di script o account possono influire sulla ricostruzione. La prudenza non consiste nel caricare il lettore di formule, ma nel fissare una regola: prima di dichiarare completo un backup bisogna sapere quale processo dovrà ricostruire.

Catena minima di derivazione

Livello	Funzione	Errore da evitare
Entropia	Origine casuale del segreto	Generarla con metodi improvvisati
Mnemonic/seed phrase	Rappresentazione di recupero in alcuni standard	Trattarla come una password recuperabile
Seed e chiave master	Radice della gerarchia	Confondere la radice con una singola chiave
Chiave derivata	Firma per uno specifico percorso o ruolo	Ignorare derivazione e policy
Chiave pubblica e indirizzo	Verifica e identificazione secondo la rete	Usarli come sinonimi

L'indirizzo non è il segreto

Un indirizzo identifica una destinazione secondo le regole della rete. Può essere comunicato per ricevere, ma non è la chiave privata e non consente, da solo, di spendere. Non tutti gli indirizzi corrispondono a una singola coppia di chiavi: possono rappresentare script o contratti con condizioni più articolate.

Nel mondo fisico, questa distinzione è intuitiva. Sapere dove si trova una casa non significa avere le chiavi. Conoscere un IBAN non significa poter svuotare un conto. Vedere una targa non significa guidare l'auto. Nel mondo

digitale, però, la forma astratta degli elementi può generare ansia o leggerezza: alcune persone temono di mostrare ciò che può essere pubblico, altre espongono ciò che dovrebbe restare segreto.

La cultura della custodia comincia da questa alfabetizzazione minima: pubblico non significa irrilevante, privato non significa misterioso. Un indirizzo pubblico può rivelare informazioni, abitudini, relazioni, saldi, cronologie, e quindi va comunque trattato con attenzione. Ma non è il segreto che consente di firmare. La chiave privata, invece, non va mai trattata come semplice informazione da comunicare.

Firmare senza chiedere permesso

Nel mondo fisico, firmare significa lasciare un segno che collega una persona a un atto. Una firma può essere contestata, verificata, confrontata, falsificata, autenticata. Ha un valore legale e culturale perché una società ha costruito istituzioni attorno a quel gesto: documenti, testimoni, notai, tribunali, archivi.

Nel mondo crittografico, firmare significa produrre una prova matematica legata a una chiave privata. La firma permette a un sistema di verificare che l'atto provenga da chi controlla quella chiave, senza rivelare la chiave stessa. È una cosa potente: si può dimostrare controllo senza consegnare il segreto.

Ma proprio perché è potente, va desacralizzata e rispettata allo stesso tempo. Firmare non deve essere immaginato come un incantesimo incomprensibile. È un gesto tecnico. Eppure non deve nemmeno diventare un click distratto. Alcune firme autorizzano movimenti di valore. Altre concedono permessi. Altre collegano un'identità a una richiesta. Altre possono sembrare innocue e produrre conseguenze indirette.

Un pulsante, una finestra, un messaggio tecnico, un conto alla rovescia, un sito che promette accesso, una richiesta che appare normale. L'utente vede un gesto piccolo. Il sistema vede un atto. La differenza tra gesto percepito e atto reale è uno dei punti più delicati della custodia digitale.

Quando non c'è sportello

La frase più dura da accettare è anche la più semplice: in alcuni sistemi, nessuno può rimettere tutto com'era.

Questa assenza non è un difetto accidentale. È parte della promessa. Un sistema che non permette a un'autorità centrale di muovere i fondi al posto nostro può proteggerci da censura, abuso, blocchi arbitrari, dipendenze

opache. Ma lo stesso sistema può non poterci salvare quando perdiamo la chiave, firmiamo l'atto sbagliato o consegniamo il segreto a qualcuno.

La cultura dell'utente digitale è stata formata da decenni di recuperabilità. Abbiamo dimenticato password, perso carte, bloccato account, cancellato file, chiesto assistenza. Quasi sempre qualcuno o qualcosa poteva intervenire. Questa esperienza produce una fiducia implicita: se sbaglio, ci sarà un percorso di recupero.

Non sempre in modo totale, perché esistono soluzioni ibride, custodie terze, multisig, procedure di recupero sociale, architetture più adatte a persone diverse. Ma il principio resta: dove la chiave privata è davvero il punto di controllo, il recupero non può essere pensato dopo. Deve essere progettato prima.

Questa è la maturità richiesta dalla custodia. Non eroismo tecnico, non paranoia, non culto dell'autonomia. Progettazione. Chi deve poter accedere? In quali condizioni? Con quali limiti? Che cosa accade se il titolare muore, si ammala, dimentica, litiga, si sposta, perde il dispositivo, subisce pressione? Che cosa accade se una persona fidata diventa non fidata? Che cosa accade se la procedura è così sicura da non essere più usabile?

Glossario minimo del capitolo

- Password: credenziale usata per accedere a un servizio o a un ambiente gestito.
- PIN: codice breve che sblocca o autorizza, spesso a livello locale o dispositivo.
- Seed phrase: sequenza di parole da cui possono derivare chiavi; va trattata come radice di accesso.
- Chiave privata: segreto crittografico che consente di firmare e dimostrare controllo.
- Chiave pubblica: elemento derivato dalla chiave privata, usato per verificare firme o costruire identificatori secondo il sistema. Indirizzo: rappresentazione o identificatore ricavato secondo regole specifiche della rete. Chiave pubblica e indirizzo sono collegati, ma non equivalenti.
- Firma: prova prodotta tramite chiave privata, verificabile senza rivelare la chiave.

Il falso senso di possesso

Molte persone credono di possedere qualcosa perché lo vedono su una schermata. Un saldo, un indirizzo, un nome asset, una cronologia, un grafico. La schermata è convincente perché parla il linguaggio quotidiano del controllo: mostra, aggiorna, conferma. Ma nel digitale vedere non significa sempre poter agire. Un saldo visibile può essere irraggiungibile. Un indirizzo può essere osservabile senza essere controllabile. Un wallet può ricordare un rapporto con il valore senza poter più produrre l'atto che quel valore richiede.

Nel mondo fisico, la vista e il possesso sono spesso vicini. Se una persona tiene una banconota in mano, la distanza tra percezione e controllo è minima. Se ha le chiavi di una casa, almeno può provare ad aprire. Se ha un documento, può mostrarlo. Nel digitale questa vicinanza si rompe. L'interfaccia può continuare a mostrare ciò che l'utente non controlla più. Il valore può restare rappresentato mentre la capacità operativa è scomparsa.

La custodia deve verificare quali strumenti permettono ancora di agire e recuperare il sistema. La presenza delle chiavi è una parte di questa verifica; contano anche configurazione, condizioni della rete e poteri legittimi. La schermata, da sola, non li dimostra.

La grammatica della prova

In molti contesti ordinari, una persona dimostra chi è attraverso documenti, volto, voce, firma manuale, presenza fisica, credenziali, testimoni, procedure amministrative. Questi elementi non sono perfetti, ma appartengono a un mondo in cui l'identità è costruita attraverso più segnali. Una banca può riconoscere un cliente anche se dimentica una password. Un ufficio può ristampare un documento. Un notaio può registrare un atto dentro una catena di responsabilità.

La prova crittografica è più stretta. Non domanda tutta la persona. Domanda se un certo atto è stato firmato dalla chiave corretta. Questa precisione è la sua forza. Riduce ambiguità, permette verifiche rapide, non richiede di consegnare il segreto. Ma è anche la sua povertà umana: una prova valida non racconta automaticamente intenzione, consenso informato, contesto o giustizia.

Capire questa grammatica significa smettere di chiedere alla rete ciò che la rete non può sapere. La rete può verificare la firma. Non può sapere se la persona era lucida, se era sotto pressione, se aveva letto, se stava sbagliando,

se era vittima di un inganno. Quelle condizioni devono essere protette prima, attraverso educazione, interfacce migliori, procedure, pause, verifiche indipendenti.

Visibilità, operatività e recupero

È utile distinguere tre capacità, senza considerarle una scala universale di proprietà.

La prima è la visibilità: consultare saldi, indirizzi e cronologia. Un explorer o un wallet di sola osservazione può mostrarli senza disporre di chiavi per firmare. Anche questa consultazione può rivelare informazioni private a chi fornisce il servizio.

Il secondo è il controllo operativo: poter usare il wallet, accedere al dispositivo, conoscere il PIN, produrre firme, spostare valore, revocare permessi, modificare una configurazione. Qui il possesso diventa azione. Ma anche questo livello non è sempre sufficiente, perché una persona può avere accesso operativo momentaneo senza possedere la radice di recupero. Può usare un dispositivo finché funziona, ma essere perduta se il dispositivo si rompe.

La terza è il recupero: ricostruire l'accesso dopo un guasto o una perdita. Può richiedere parole, passphrase, dati di configurazione, più firmatari o servizi previsti dal sistema. Chi possiede un solo componente non dispone necessariamente dell'intero percorso.

Molte persone confondono questi livelli. Credono di avere controllo radicale perché hanno controllo visivo. Credono di essere al sicuro perché un wallet si apre. Credono che il dispositivo sia la proprietà, quando in realtà il dispositivo può essere solo una finestra temporanea su una proprietà il cui accesso profondo è altrove.

La consultazione, l'uso e il recupero richiedono protezioni distinte. Le informazioni di osservazione restano riservate quando collegano una persona al patrimonio. Le credenziali operative e i segreti di recupero richiedono inoltre misure che ne limitino l'uso e la copia.

Tre profili di custodia

Il primo profilo è la persona sperimentale. Possiede piccoli importi, prova strumenti, impara, sbaglia con danni limitati. Per lei la priorità è l'alfabetizzazione: distinguere chiave e password, capire la firma, evitare le

esposizioni più banali, non usare lo stesso ambiente per test e riserva. Troppa complessità iniziale può essere controproducente.

Il secondo profilo è la persona patrimoniale. Il valore custodito è significativo. La perdita avrebbe effetti reali sulla vita familiare o professionale. Qui servono separazione degli ambienti, backup robusti, procedure ereditarie, eventuale coinvolgimento di fiduciari o soluzioni condivise. La domanda non è più come imparo, ma come riduco il rischio sistemico attorno a un valore importante.

Il terzo profilo è l'organizzazione. Azienda, fondazione, associazione, team, famiglia imprenditoriale. Qui una chiave non può dipendere dalla memoria o dalla disponibilità di una sola persona. Servono ruoli, autorizzazioni, registri, procedure di sostituzione, limiti, audit, separazione tra chi propone un atto e chi lo autorizza.

Fonti e approfondimenti

Le fonti sostengono i chiarimenti richiamati nel testo. Documentazione consultata il 12 settembre 2026. Funzioni dei servizi, termini e norme vanno verificati nel contesto applicabile prima di un intervento.

[1] Bitcoin Improvement Proposals. BIP-39: Mnemonic code for generating deterministic keys. Parole, seed e passphrase.
Consulta la fonte

[2] Bitcoin Improvement Proposals. BIP-32: Hierarchical Deterministic Wallets. Gerarchia delle chiavi e derivazione.
Consulta la fonte

[3] Ethereum Improvement Proposals. ERC-2612: Permit Extension for EIP-20 Signed Approvals. Autorizzazioni mediante messaggi firmati.
Consulta la fonte

[4] SatoshiLabs. SLIP-39: Shamir's Secret-Sharing for Mnemonic Codes. Soglie, ricostruzione e differenze da BIP-39.
Consulta la fonte

[5] NIST. Multi-Party Threshold Cryptography. Calcolo distribuito e firme a soglia senza ricomporre la chiave durante l'operazione.
Consulta la fonte

QUADERNI DI CUSTODIA DIGITALE

La lettura continua

La Chiave Privata

Floriano Righetti · Quaderno IV

Hai letto un estratto dell'edizione definitiva di settembre 2026. Nella scheda del quaderno trovi la presentazione del volume e gli aggiornamenti sulla sua disponibilità.

SCOPRI IL QUADERNO

florianorighetti.ch/it/quaderni/
la-chiave-privata

Sette quaderni, un percorso

Custodia, proprietà digitale, eredità, chiavi private, wallet, cold storage e fiducia.

Esplora la collana completa