Confidential Matching Infrastructure

Il livello di evidenza che verifica senza vedere il contenuto.

La promessa della blockchain

CertiSigma è ciò che molti si aspettavano dalle blockchain pubbliche, riportato alla dimensione di una primitiva infrastrutturale: quattro righe di codice, un hash calcolato nel perimetro del cliente, una prova indipendentemente verificabile.

Per quindici anni una sola idea ha attraversato tutti i settori dell'economia digitale: rendere gli eventi verificabili. Tracciare i passaggi di una filiera senza affidarsi alla parola dei singoli nodi. Provare che un documento esisteva prima di una certa data senza trasformare ogni passaggio in un atto notarile. Permettere a parti che non si fidano l'una dell'altra di cooperare su uno stato condiviso. Costruire audit automatici, supply chain trasparenti, registri di proprietà intellettuale, antifrode interbancaria, identità portabili, provenienza scientifica, custodia digitale e incident response cross-organizzativa.

La tecnologia per farlo era già disponibile. I Merkle tree appartengono agli anni Settanta, le firme ECDSA agli anni Novanta, Bitcoin esiste dal 2009, i timestamp qualificati eIDAS sono regolamentati dal 2014, OpenTimestamps è disponibile dal 2016. La promessa tecnica non è mai mancata; è mancata l'interfaccia che potesse entrare nei sistemi reali senza trasformare ogni integrazione in un progetto politico.

Per registrare un evento su una blockchain pubblica bisognava scegliere una blockchain, gestire wallet, pagare gas in una valuta volatile, scrivere smart contract, sottoporli ad audit, convincere un consorzio di settore, definire governance, risolvere questioni di data protection, spiegare perché dati o riferimenti permanenti venissero collocati fuori dal perimetro operativo ordinario. Tre anni di progetto per integrare ciò che avrebbe dovuto comportarsi come una primitiva elementare.

I consorzi che hanno provato a portare questa promessa dentro settori regolamentati — logistica, alimentare, energia, commodity finance — hanno spesso prodotto demo, standard incompleti o piattaforme che sopravvivono solo

dove un singolo attore riesce a imporre il proprio modello. Il problema non era la matematica. Il problema era l'interfaccia.

CertiSigma è la stessa promessa, con l'interfaccia che mancava.

Una chiamata HTTP

```
client.attest(hash_hex, source="gate-47")
```

Una riga inserita nel punto di transito in cui un evento diventa rilevante. Il cliente calcola localmente un digest SHA-256 e invia al servizio soltanto quell'impronta; il contenuto sottostante resta nel suo ambiente, insieme alla responsabilità di costruire correttamente il flusso di lavoro, normalizzare gli input, proteggere eventuali chiavi HMAC e conservare la propria catena di custodia.

La valutazione privacy cambia natura: l'oggetto del trattamento non è una copia del dato sostantivo trasferita a un fornitore, ma una rappresentazione crittografica, i metadati operativi eventualmente associati e le capacità di accesso che il cliente decide di abilitare. Questo non elimina l'analisi del DPO; la sposta sul piano corretto, dove contenuto, impronta, claim, metadati e operazioni vengono trattati come oggetti distinti.

CertiSigma non è un registro segreto di attestazioni: è una piattaforma di attestazione pubblicamente verificabile. Hash, payload, firme, prove Merkle, timestamp, ancoraggi e chiavi pubbliche possono essere verificati da terzi; ciò che resta fuori dal servizio è il contenuto originale. I metadati organizzativi restano invece nel piano privato del claim/API key o, quando previsto, sono cifrabili lato client. Gli identificativi di attestazione sono riferimenti alla prova e non devono essere interpretati come indicatori di sequenza, volume, identità del cliente o progressione cronologica.

Sotto questa chiamata, in modo invisibile a chi integra, si producono tre livelli complementari di evidenza.

T0: Firma ECDSA P-256 immediata

Il servizio riceve il digest, costruisce un payload canonico che include versione del formato, digest e timestamp di registrazione, e firma quel payload con la chiave privata di firma del servizio. La firma T0 consente a chiunque disponga del

digest, del payload, della firma e della chiave pubblica corrispondente di verificare che CertiSigma abbia osservato quell'impronta e firmato quel preciso payload in quel momento dichiarato.

Nota sul valore probatorio del timestamp T0

Il timestamp T0 è un dato applicativo generato dal servizio con risoluzione al microsecondo. Esso non costituisce una validazione temporale qualificata ai sensi del Regolamento eIDAS, né produce di per sé una presunzione legale di accuratezza della data e dell'ora.

La validazione temporale qualificata, ove disponibile, è fornita dal livello T1, nel quale una Time Stamping Authority qualificata esterna emette un timestamp RFC 3161 sulla Merkle root del batch. Il livello T2 aggiunge un ancoraggio pubblico verificabile tramite OpenTimestamps/Bitcoin, ma non costituisce un servizio fiduciario qualificato né un registro elettronico qualificato.

Il timestamp T0 conserva valore di evidenza tecnica, che il giudice o l'autorità competente valuteranno secondo il diritto applicabile, le circostanze del caso, la catena di custodia e gli altri elementi probatori disponibili.

La funzione di T0 è l'immediatezza: rendere l'evento provabile appena entra nel registro applicativo, senza attendere le fasi asincrone di aggregazione e ancoraggio. Le chiavi pubbliche, gli identificativi di chiave e le informazioni necessarie alla verifica devono essere pubblicati in modo che la prova non dipenda dalla disponibilità futura del servizio.

T1: Timestamping qualificato su Merkle root

Gli hash ricevuti in una finestra temporale vengono aggregati in una struttura Merkle. La radice viene sottoposta a una Time Stamping Authority qualificata esterna, che emette un token RFC 3161 secondo il regime eIDAS applicabile alla TSA. La Merkle proof collega il digest specifico alla radice timestampata e permette a un verificatore di controllare il percorso dall'impronta individuale al timestamp qualificato.

La formulazione è importante: CertiSigma non diventa per questo una TSA qualificata e non attribuisce identità, volontà o paternità al contenuto sottostante. Il livello T1 aggiunge una validazione temporale qualificata sulla

radice del batch; il valore probatorio concreto dell'evidenza resta quello attribuito dall'autorità competente nel contesto del caso, della catena di custodia e degli altri elementi disponibili.

T2: Ancoraggio Bitcoin via OpenTimestamps

La radice giornaliera viene ancorata alla blockchain Bitcoin tramite OpenTimestamps. Una volta confermato, l'ancoraggio consente di verificare l'esistenza temporale della radice rispetto a un blocco Bitcoin reale, senza dipendere da CertiSigma come intermediario di verifica. L'ancoraggio Bitcoin/OpenTimestamps non costituisce un registro elettronico qualificato eIDAS e non produce le presunzioni proprie dei qualified electronic ledgers. Se il servizio dovesse scomparire, le evidenze T2 già prodotte resterebbero verificabili nei limiti in cui restino disponibili la prova OpenTimestamps, i riferimenti alla blockchain Bitcoin e gli altri elementi necessari alla verifica.

T0 fornisce immediatezza, T1 aggiunge una validazione temporale qualificata sulla radice, T2 aggiunge un ancoraggio pubblico di lungo periodo. Tre livelli, tre modelli di verifica, una sola interfaccia.

La promessa della blockchain pubblica viene così riportata alla dimensione in cui un sistema aziendale può davvero usarla: una chiamata HTTP che non richiede wallet, gas, smart contract, governance consortile o migrazione di contenuto.

Il livello che verifica senza vedere il contenuto

Ciò che è stato costruito non è semplicemente un servizio di attestazione. È un livello di evidenza che non conosce, e non deve conoscere, il contenuto o la semantica operativa degli eventi che attesta.

Un sensore al gate di un porto legge un tag RFID e attesta una stringa. Un terminale di pagamento attesta l'hash di una transazione sopra una certa soglia. Un sistema KYC bancario attesta la presentazione di un documento d'identità. Un dispositivo IoT industriale attesta il superamento di una soglia. Un sistema di gestione documentale attesta la firma di un contratto. Un sistema di custodia attesta la presa in carico di una prova. Un sistema di trasporto attesta un transito.

Un laboratorio attesta una versione di dataset. Un CSIRT attesta un indicatore. Un brand attesta un seriale o un lotto.

Per CertiSigma, tutti questi eventi arrivano come stringhe di 64 caratteri esadecimali. Il servizio non deve sapere se l'impronta rappresenta un contratto, un sensore, un pagamento, una prova forense, un componente software o un file riservato. Questa ignoranza strutturale non è una lacuna informativa; è la proprietà che rende il sistema infrastruttura e non prodotto verticale.

Lo stesso endpoint può servire dogana, banca, ospedale, porto, studio legale, autorità di sicurezza nazionale, brand owner, giornalista d'inchiesta, CSIRT, ricercatore scientifico e magistrato che riceve una segnalazione. Questi soggetti non devono conoscersi, non devono coordinarsi, non devono adottare lo stesso schema dati e non devono aderire allo stesso consorzio. Ciascuno sceglie quale stringa attestare, quale formato canonico costruire nel proprio dominio, quali campi includere, quale chiave HMAC usare per input prevedibili, quanto frequentemente attestare e quali metadati associare.

Da questa pluralità di integrazioni nasce un registro temporale di impronte verificabili che non impone una semantica unica al mondo. Ogni organizzazione conserva il proprio linguaggio interno; il livello comune è l'impronta.

Contenuto protetto, operazioni dimostrabili

Il modello giuridico e tecnico di CertiSigma poggia su una distinzione che molti sistemi di confidenzialità non fanno con sufficiente precisione: la separazione tra il piano del contenuto e il piano delle operazioni.

Il piano del contenuto: content-blind per architettura

Il contenuto riservato resta sotto il controllo del cliente. Il file, il documento, il dataset, il log o l'artefatto digitale da cui viene calcolato il digest non lascia l'ambiente del cliente. I metadati operativi sensibili, quando presenti, possono essere cifrati lato client prima dell'invio; in quel caso il servizio conserva ciphertext opaco e non dispone della chiave necessaria a ricostruire il plaintext.

Questa architettura produce un effetto più forte di una semplice policy di riservatezza. Il servizio può essere materialmente impossibilitato a fornire il

contenuto originale o il plaintext di metadati cifrati perché quegli oggetti non sono nella sua disponibilità tecnica. L'indisponibilità non nasce da una promessa commerciale, ma dal fatto che il contenuto non entra nel sistema e che la chiave di cifratura resta presso il cliente.

La precisione è indispensabile anche sul piano privacy. Un digest SHA-256 non è necessariamente un dato personale per sua sola natura tecnica, ma può assumere rilevanza privacy quando l'input è enumerabile o prevedibile, quando rappresenta identificativi diretti o strutturati, oppure quando viene correlato a metadati, account, API key o altri elementi di contesto.

In questi casi l'hash nudo non basta: servono derivazioni keyed, HMAC, normalizzazione controllata, segregazione per tenant, cifratura client-side dei metadati, limitazione degli accessi e valutazione del rischio nel flusso di lavoro del cliente.

Il piano delle operazioni: imputabilità per progettazione

La riservatezza del contenuto non deve diventare irresponsabilità dell'accesso. Le operazioni che abilitano attestazione, metadata, share token, derived lists, webhook e accessi di terze parti devono poter essere attribuite, limitate e ricostruite nei limiti di ciò che il sistema conserva e di ciò che il cliente integra nei propri log.

L'imputabilità operativa non deriva dalla visibilità del contenuto, ma dalla progettazione delle capacità: scope delle API key, restrizioni di rete, share token, access log, derived list access log, webhook firmati, anti-replay, delivery history e audit log locali del cliente.

Il punto non è creare un sistema senza tracce. Il punto è fare in modo che le tracce giuste sopravvivano senza esporre il contenuto sbagliato. Una chiave può avere uno scope limitato, una rete autorizzata, una durata, un ruolo e una finalità. Uno share token può aprire una finestra di evidenza definita. Una derived list può concedere una capacità di matching controllata. Un webhook firmato può notificare il completamento di T1 o T2 in un flusso SIEM o forense. L'accesso resta dimostrabile, mentre il contenuto resta protetto.

Molti sistemi di confidenzialità proteggono tutto, comprese le tracce che servono in audit, incident response e contenzioso. Molti sistemi di audit fanno l'errore opposto: per tracciare devono vedere il contenuto e introducono così un punto di compromissione della riservatezza. CertiSigma tiene i due piani ortogonali. Il piano dell'evidenza crittografica — hash, payload, firme, prove, timestamp e ancoraggi — è pubblico o pubblicamente verificabile; il piano del claim è privato per chiave, cifrabile lato client, scoped per ruolo e vincolabile a reti autorizzate.

Questa è la funzione centrale: privacy del contenuto, imputabilità dell'operazione.

Confidential Matching Infrastructure

L'attestazione di esistenza temporale è il gesto elementare: un evento, un file, un documento, un seriale, una transazione o un indicatore vengono ridotti a un'impronta crittografica e quell'impronta viene osservata, firmata, aggregata, timestampata e ancorata in modo indipendentemente verificabile. Questa è la base. Il salto decisivo avviene quando l'impronta smette di essere soltanto una prova del passato e diventa il punto minimo di contatto tra perimetri informativi che non possono aprirsi.

Ogni organizzazione conserva archivi che non può consegnare: file riservati, seriali industriali, documenti KYC, transazioni sospette, indicatori cyber, dataset scientifici, prove digitali, lotti di produzione, componenti software, fascicoli legali, log operativi. Questi archivi sono troppo sensibili per essere copiati in una data room, troppo strategici per essere pubblicati, troppo regolamentati per essere trasferiti a una piattaforma terza, troppo specifici per entrare in uno schema comune imposto da un consorzio.

Eppure molte decisioni critiche dipendono da una domanda semplice, quasi primitiva: quello che ho io tocca qualcosa che sai tu?

Un file apparso fuori dal perimetro apparteneva davvero all'archivio di un'azienda. Un documento presentato in una pratica bancaria è già comparso in un circuito antifrode. Un seriale trovato su un marketplace appartiene a una produzione autentica o a una famiglia di contraffazioni. Un indicatore raccolto da un CSIRT coincide con qualcosa osservato da un'altra organizzazione. Un

componente software presente in una supply chain compare in un inventario compromesso. Un dataset scientifico corrisponde a una versione esistente prima di una pubblicazione, di una revisione o di una contestazione.

Il modello tradizionale costringe a scegliere tra chiusura e divulgazione. Se l'archivio resta chiuso, la cooperazione muore. Se l'archivio viene condiviso, il controllo si perde. Nascono copie, obblighi di custodia, superfici di attacco, conflitti di governance, accordi bilaterali, data processing agreement, esportazioni, consorzi, piattaforme verticali, promesse di fiducia. CertiSigma introduce una terza geometria: il perimetro resta chiuso, ma può concedere a soggetti autorizzati una capacità limitata, revocabile e dimostrabile di verificare un contatto.

Questa capacità è il cuore della Confidential Matching Infrastructure. Il database non viene consegnato, l'inventario non viene esposto come tale e la semantica interna dei record non viene pubblicata. Questo non significa assenza assoluta di esposizione informativa: significa sostituire la condivisione del dato con una capacità limitata, governata e verificabile di interrogazione. Viene concessa una domanda, entro un perimetro definito: questo candidato produce una corrispondenza con qualcosa che il tuo mondo conosce?

La derived list HMAC è una delle forme tecniche di questa domanda.

Nota sulla protezione dei dati personali

Una derived list HMAC non è di per sé priva di rischi per la privacy. Se gli elementi della lista originale costituiscono dati personali, ad esempio identificativi di persone fisiche, indirizzi e-mail, codici fiscali o altri identificativi diretti o indiretti, e la capacità di derivazione o interrogazione viene concessa a una terza parte, quest'ultima può generare l'HMAC di un candidato e verificare l'eventuale coincidenza. In tali casi, la derived list e le relative operazioni di matching possono configurare un trattamento di dati personali ai sensi del GDPR o della LPD, a seconda del contesto.

È responsabilità del cliente che genera la derived list valutare se lo scenario richieda garanzie aggiuntive, quali limitazione degli accessi a soggetti autorizzati, minimizzazione degli input, segregazione per tenant, scadenza, revoca, logging, rate limit o, nei casi più sensibili, protocolli interattivi come PSI o tecniche

crittografiche più forti. CertiSigma mette a disposizione strumenti tecnici quali HMAC, scope delle chiavi, log di accesso, scadenza e revoca, ma non determina le finalità sostanziali perseguite dal cliente, né seleziona gli elementi da includere nella derived list o i soggetti con cui il cliente decide di abilitare il matching.

Un'organizzazione prende un insieme di elementi scelti nel proprio dominio operativo — tipicamente hash di file, valori normalizzati, fingerprint, seriali trattati con le cautele necessarie, indicatori o altri identificativi — e li trasforma mediante una funzione HMAC-SHA256 con una chiave. Il risultato non è l'inventario originale, non è il contenuto e non è una pubblicazione del database sorgente. È una superficie crittografica derivata, costruita per permettere matching a chi possiede o esercita una specifica capacità autorizzata.

Questa distinzione è essenziale. Una derived list non è assenza assoluta di divulgazione e non deve essere venduta come magia. Non è un protocollo zero-knowledge in senso stretto e non elimina ogni rischio di inferenza. È una delega crittografica limitata: chi dispone della capacità di matching può testare candidati; per questo quella capacità deve avere durata, scope, revoca, rate limit, tracciabilità e responsabilità. Quando gli input sono prevedibili o a bassa entropia, la protezione non può poggiare su un semplice hash nudo: servono derivazioni keyed, normalizzazione controllata, segregazione per tenant, politiche di rotazione e, nei casi più sensibili, protocolli interattivi più forti. La forza del modello non sta nel fingere che il rischio non esista, ma nel trasformarlo in un oggetto governabile.

Gestione e revoca delle chiavi HMAC

La chiave utilizzata dal cliente per generare una derived list è un segreto crittografico e deve essere conservata con misure di sicurezza adeguate, ad esempio in un vault, in un HSM o in un ambiente segregato. Nei flussi in cui la derivazione è effettuata lato cliente, CertiSigma riceve la lista già derivata e non ha bisogno di conoscere la chiave HMAC originaria.

La revoca di una derived list o di una capacità di matching non equivale necessariamente a cancellare la conoscenza già acquisita da chi abbia precedentemente ricevuto materiale chiave, una list key, un token o un artefatto derivato. Se una capacità è stata distribuita a terzi, la revoca impedisce gli usi

futuri nei limiti tecnici della piattaforma, ma non elimina eventuali copie, risultati di matching o informazioni già ottenute prima della revoca.

In caso di compromissione della chiave o della capacità di interrogazione, il cliente deve generare una nuova derived list con nuovo materiale crittografico, revocare la lista o le capacità precedenti, aggiornare i soggetti autorizzati e valutare l'impatto degli accessi già effettuati sulla base dei log disponibili.

CertiSigma consente di associare alle derived lists capacità di interrogazione con scadenza, limiti di utilizzo, revoca e log di accesso. La sicurezza complessiva del modello di confidential matching dipende tuttavia anche dalla corretta gestione delle chiavi, dei token, delle capacità distribuite e dei soggetti autorizzati da parte del cliente.

Da qui nasce la differenza tra condivisione di dati e confidential matching. La condivisione di dati sposta dati da un dominio all'altro e crea copie che qualcuno dovrà custodire, giustificare, cancellare, proteggere e spiegare. Il confidential matching sposta una capacità: la possibilità di riconoscere un contatto puntuale tra due perimetri senza fondere i perimetri stessi. Due organizzazioni possono avere tassonomie diverse, database diversi, processi diversi, classificazioni diverse e obblighi diversi; non devono concordare un significato comune per ogni campo, perché il minimo comune denominatore non è il campo, è l'impronta.

Census rende locale questa geografia. Scansiona ambienti, calcola impronte, costruisce manifest, esegue controlli di integrità, prepara report ed evidence bundle, mantiene memoria crittografica, audit log, snapshot e timeline forensi, e può alimentare flussi SIEM, SBOM, provenance e CI/CD. Prima dell'incidente misura il territorio. Dopo l'incidente consente di riconoscere il contatto. Un file trapelato non deve essere riconosciuto perché qualcuno ricorda di averlo visto; può essere confrontato con una memoria attestata prima della fuga. Un archivio aziendale non deve essere aperto per dimostrare di essere stato toccato; può restare chiuso mentre una sua superficie derivata risponde a domande puntuali. La fuga non viene impedita dalla crittografia dell'evidenza, ma smette di essere un evento indistinguibile: lascia una collisione, una precedenza, una relazione verificabile.

La stessa logica vale in antifrode cooperativa, dove banche, assicuratori e marketplace vedono frammenti diversi dello stesso ecosistema criminale ma

non possono riversare i propri archivi in un'unica piattaforma. Vale nella contraffazione, dove un brand non può pubblicare la lista dei seriali validi senza aiutare chi falsifica, ma può consentire controlli puntuali a dogane, marketplace, distributori e investigatori. Vale nella cyber intelligence, dove un CSIRT non può esporre tutto ciò che osserva senza rivelare visibilità, fonti e capacità, ma può consentire a una parte autorizzata di verificare se un artefatto combacia con un indicatore noto. Vale nella ricerca scientifica, dove un laboratorio può provare l'esistenza temporale di una versione di dataset senza consegnare materiale riservato. Vale nel legal tech e nel forensic, dove uno studio legale o un perito possono condividere evidenze verificabili entro finestre definite senza aprire l'intero fascicolo.

Il contenuto resta riservato, il dato sostantivo resta nel perimetro del cliente, i metadati sensibili possono essere cifrati lato client e il servizio può trovarsi materialmente impossibilitato a ricostruire il plaintext. Le operazioni, però, devono lasciare memoria: quale chiave ha attestato, quale scope aveva, da quale rete autorizzata ha operato, quale share token è stato generato, quale derived list è stata interrogata, quale controparte ha avuto accesso, entro quale scadenza e con quali limiti.

La riservatezza del contenuto non diventa irresponsabilità dell'accesso. CertiSigma separa ciò che deve restare segreto da ciò che deve restare imputabile. Il segreto resta segreto, ma il modo in cui viene usato diventa attribuibile. Il perimetro resta chiuso, ma può rispondere. L'archivio resta privato, ma può riconoscere contatti. La prova resta verificabile, ma non richiede di vedere il contenuto.

Confidential Matching Infrastructure significa questo: organizzazioni che non possono condividere dati possono comunque scoprire se condividono evidenze.

La grammatica della cooperazione: primitive, non prodotti

Sopra il livello base dell'attestazione, CertiSigma espone un insieme di primitive che possono essere combinate in flussi di lavoro diversi senza trasformarsi in un prodotto verticale unico. La stessa infrastruttura può sostenere filiere, antifrode, KYC distribuito, incident response tra organizzazioni, provenienza nella catena di

fornitura, riproducibilità scientifica, digital twin, custodia forense e intelligence cooperativa, proprio perché non impone uno schema semantico comune.

Claim multi-tenant per attestazione

Lo stesso hash può avere claim privati indipendenti da parte di più organizzazioni. Ogni claim ha il proprio source, il proprio extra_data e i propri tag, visibili soltanto al proprietario autenticato e gestibili secondo le autorizzazioni della chiave che li ha prodotti o che è abilitata a leggerli. Due organizzazioni che attestano lo stesso documento possono riferirsi alla stessa impronta pubblica, mantenendo però contesti operativi separati.

Questa proprietà permette la cooperazione senza piattaforma di settore. Il punto comune è l'impronta; tutto il resto resta nel linguaggio interno di ciascun attore.

Derived lists HMAC

Una derived list consente a un'organizzazione di concedere a una terza parte una funzione interrogativa sul proprio inventario senza esporre l'inventario stesso come database consultabile. Ogni elemento viene trasformato con una chiave in un hash derivato; soltanto chi dispone della capacità autorizzata di derivazione o interrogazione può verificare se un proprio candidato produce una corrispondenza.

La terza parte può chiedere se un elemento in suo possesso compare nel perimetro dell'altra organizzazione e ricevere una risposta di matching controllato, senza ricevere il database originale, il contenuto, i metadati privati o la semantica interna dell'inventario. La lista può avere scadenza, revoca, firma di integrità, limiti d'uso e log di accesso. La list key o l'equivalente capacità di matching deve essere trattata come materiale sensibile: non trasferisce il dataset, ma consente test puntuali e quindi deve essere governata con modello di minaccia, durata, scope, rate limit, revoca e tracciabilità adeguati.

Questa primitiva abilita sanctions screening interbancario, antifrode cooperativa, leak detection, IP protection, counterfeit detection, due diligence M&A e cooperazione CSIRT su indicatori di compromissione. In tutti questi casi un soggetto conserva un'asimmetria informativa che non vuole perdere, mentre un altro soggetto ha bisogno di un controllo puntuale.

Share token

Uno share token consente a un'organizzazione di aprire una finestra limitata su un set definito di attestazioni. L'accesso può essere in sola lettura, limitato nel tempo, limitato nel numero di accessi e associato a log. È la primitiva forense per condividere evidenze con analisti esterni, auditor, controparti in contenzioso, autorità competenti o assicuratori senza aprire l'inventario completo e senza trasformare i metadati privati del claim in pubblicazione generalizzata.

L'evidenza diventa guardabile senza trasformare il perimetro informativo del cliente in una copia incontrollata che continuerà a circolare dopo la fine del rapporto.

Tag scoped per API key

I tag non sono etichette pubbliche. Sono uno stato operativo privato. Dentro la stessa organizzazione, dipartimenti diversi possono classificare le stesse attestazioni con schemi distinti senza interferire tra loro. Un team può usare tag di processo, un altro tag di rischio, un altro tag di lotto, un altro tag di stato forense.

La prova resta pubblica nella sua impronta, mentre il significato operativo resta privato e, quando necessario, cifrabile lato client. Questa è la proprietà che permette di usare CertiSigma come substrato comune senza obbligare l'organizzazione a negoziare un unico schema di metadati tra reparti.

RBAC con scope granulari

Ogni API key deve portare soltanto i permessi necessari al compito per cui è stata emessa. Una chiave può attestare, un'altra leggere metadati, un'altra generare share token, un'altra operare su derived lists, un'altra ricevere o verificare webhook. Una chiave compromessa non deve diventare compromissione dell'organizzazione intera; l'impatto deve restare limitato alla capacità concreta che quella chiave era autorizzata a esercitare.

La sicurezza non è un accessorio del modello. È la condizione che rende possibile la cooperazione tra segreti.

IP allowlist e blast radius controllato

Una chiave può essere vincolata a IP o reti specifiche. Se viene copiata fuori dal perimetro autorizzato, non diventa automaticamente utilizzabile ovunque. Combinata con RBAC, questa proprietà riduce il blast radius e trasforma la chiave da segreto universale a capacità localizzata.

Un attaccante che voglia usare una chiave esfiltrata deve trovarsi anche dentro la rete autorizzata o compromettere l'ambiente da cui la chiave è abilitata a operare. In quel caso il problema non è più soltanto la chiave; è un incidente infrastrutturale che può essere trattato come tale.

Webhook firmati

Gli eventi asincroni, come il completamento di T1 o T2, possono essere notificati tramite webhook firmati, con meccanismi anti-replay, deduplicazione e storia di consegna. La notifica entra così nei sistemi del cliente come parte di una chain of custody applicativa e può alimentare flussi di lavoro di audit, SIEM, incident response o archiviazione forense. La firma del webhook permette al cliente di distinguere un evento effettivamente emesso dal servizio da una notifica simulata o riutilizzata.

Combinazioni che abilitano ecosistemi

Combinando queste primitive, lo stesso servizio può diventare un sistema di antifrode cooperativa tra banche, un protocollo di filiera del lusso anticontraffazione, uno strato di incident response per CSIRT che condividono indicatori senza divulgazione dell'intero inventario, un sistema di provenienza scientifica, un registro distribuito di versioni d'opera, un'infrastruttura di whistleblowing protetto o un substrato di custodia digitale per evidenze forensi tra giurisdizioni diverse.

CertiSigma non coincide con nessuno di questi sistemi. È il livello sotto cui tutti questi sistemi possono essere costruiti.

La disciplina dell'overclaim

Un'infrastruttura di evidenza deve essere ambiziosa nella visione e precisa nei confini. CertiSigma attesta l'esistenza temporale e l'integrità di digest crittografici osservati dal servizio; non trasforma automaticamente quel digest in verità del contenuto, attribuzione di autore, titolo di proprietà, consenso, liceità, conformità normativa o prova legale conclusiva.

Il servizio non sostituisce il notaio, la firma elettronica qualificata, il sigillo elettronico qualificato, la conservazione a norma, il deposito d'autore, la consulenza del perito, il giudizio dell'auditor o la valutazione dell'autorità competente. Può integrarsi con questi strumenti e rafforzare un flusso probatorio, ma non deve essere rappresentato come un sostituto di funzioni giuridicamente diverse.

Questa disciplina non indebolisce la promessa; la rende vendibile nei luoghi in cui la promessa deve reggere. Un sistema che vuole servire banche, ospedali, studi legali, autorità, assicuratori, filiere critiche e organizzazioni regolamentate deve poter dire con la stessa precisione cosa prova e cosa non prova. La credibilità dell'infrastruttura nasce anche da questa architettura negativa.

Codice open e verificabile

Gli SDK Python e JavaScript e il client Census rendono l'integrazione ordinaria, ma il punto più importante è che l'evidenza non deve restare prigioniera del servizio che l'ha generata. I formati T0, T1 e T2 si basano su primitive standard: SHA-256 per l'impronta, ECDSA P-256 per la firma immediata, RFC 3161 per il timestamp qualificato sulla radice e OpenTimestamps per l'ancoraggio Bitcoin.

Le chiavi pubbliche, le prove, i payload canonici e i test vector devono essere pubblicati in modo da permettere verifica indipendente. Se CertiSigma non fosse più disponibile, una prova già prodotta dovrebbe poter essere verificata da chi possiede gli elementi necessari: digest, payload canonico, firma T0, identificativo di chiave e chiave pubblica applicabile, Merkle proof, TSA token, eventuali certificati e informazioni di verifica del TSA, prova OpenTimestamps e riferimenti alla blockchain Bitcoin.

Questa è la differenza tra un servizio e un'infrastruttura: il servizio eroga una funzione mentre esiste; l'infrastruttura produce evidenze che devono sopravvivere al fornitore.

Trasparenza operativa e governance

La fiducia in un'infrastruttura content-blind non nasce dalla quantità di contenuto che il servizio vede, ma dalla chiarezza delle sue chiavi, dei suoi confini, dei suoi processi e delle sue impossibilità tecniche. La documentazione operativa deve quindi coprire key management, pubblicazione e revoca delle chiavi pubbliche, modello di minaccia, controlli di accesso, trattamento dei metadati, segregazione dei claim, log applicativi, gestione dei token, derived lists, webhook firmati e procedure di divulgazione.

La posizione giuridica deve essere altrettanto esplicita. Il servizio opera sotto giurisdizione svizzera, riceve digest e metadati operativi nei limiti del flusso scelto dal cliente, non ospita il contenuto originale e può essere tecnicamente impossibilitato a fornire ciò che non possiede. Le richieste legittime dell'autorità possono essere soddisfatte soltanto nei limiti di ciò che è materialmente custodito dal servizio e secondo il quadro giuridico applicabile.

Questa trasparenza non è un optional reputazionale. È la condizione perché il sistema possa essere adottato in ambienti regolamentati senza confondere riservatezza, assenza di controllo e irresponsabilità.

Prendi un endpoint e cambi il tuo mondo

Quattro righe di codice. Una chiamata HTTP. Una stringa attestata in un punto di transito qualunque.

Da quel momento in poi, quell'impronta ha una storia verificabile. È stata osservata, firmata, aggregata, collegata a una radice timestampata, eventualmente ancorata a Bitcoin, e può essere verificata da terzi senza chiedere al sistema originario di essere creduto. Il contenuto resta nel perimetro del cliente, ma la sua impronta può entrare in una geografia di prove, claim privati, condivisioni controllate e matching riservato.

Il mondo digitale non ha bisogno di un’altra piattaforma che chieda a tutti di trasferire dati, adottare uno schema comune e fidarsi di un nuovo centro. Ha bisogno di un livello minimo in cui gli eventi possano diventare evidenze, i segreti possano rispondere senza rivelarsi e le operazioni possano restare dimostrabili senza esporre il contenuto.

CertiSigma è quel livello: un endpoint nel punto di transito, una prova fuori dal sistema che la dichiara, una superficie di contatto tra archivi che non possono aprirsi.

Hai inserito una chiamata HTTP nel tuo flusso di lavoro e hai cambiato il tuo mondo.

https://certisigma.ch/legal/imprint