Posizionamento giuridico del servizio CertiSigma

1. Natura del servizio

CertiSigma è un servizio di attestazione crittografica dell'esistenza temporale e dell'integrità di valori di hash. Il servizio è erogato da Ten Sigma Sagl, società a garanzia limitata di diritto svizzero con sede in Via Carzo 8, 6900 Paradiso (Cantone Ticino), iscritta al Registro di commercio del Cantone Ticino in data 5 febbraio 2015, numero di identificazione delle imprese CHE-498.705.818.

Il marchio verbale «CertiSigma» è registrato presso l'Istituto Federale della Proprietà Intellettuale (IPI/IGE) come marchio individuale, marchio n. 839028, domanda n. 16124/2025, con data di deposito 27 ottobre 2025, data di registrazione 6 novembre 2025, pubblicazione in Swissreg il 6 novembre 2025, classi di Nizza 38, 42 e 45, e protezione fino al 27 ottobre 2035, come risulta dal registro Swissreg allo stato del 7 novembre 2025.

Il servizio opera su valori crittografici — specificamente, digest SHA-256 di 32 byte — calcolati dal cliente nel proprio ambiente e trasmessi al servizio per essere oggetto di attestazione.

Il servizio non riceve, non elabora, non conserva e non rende disponibile a terzi il contenuto originale dei file, documenti, dati o materiali da cui i digest sono calcolati. Il modello operativo è definito content-blind nel senso che la natura informativa del contenuto sottostante è strutturalmente inaccessibile al servizio, in virtù della proprietà di resistenza alla preimmagine (preimage resistance) della funzione hash SHA-256.

Resta salvo il caso di input sottostanti appartenenti a spazi di valori ristretti, prevedibili o facilmente enumerabili. In tali ipotesi la resistenza alla preimmagine di SHA-256 non elimina, da sola, il rischio di correlazione mediante tentativi sistematici o dizionari; il cliente deve pertanto adottare misure appropriate, quali HMAC con chiave segreta, derived lists o altri meccanismi di derivazione non enumerabile, prima della trasmissione del digest al servizio.

L'attestazione prodotta è strutturata su tre livelli complementari di evidenza crittografica. Il livello T0 consiste in una firma ECDSA su curva P-256 (algoritmo ECDSA-P256-SHA256) apposta da CertiSigma su un payload canonico che

include il digest, un identificativo di versione del formato, e un timestamp di registrazione con precisione al microsecondo in fuso UTC.

Il timestamp T0 è rappresentato con risoluzione al microsecondo in UTC. Tale risoluzione descrive il formato e la granularità del dato applicativo registrato da CertiSigma e non costituisce, di per sé, validazione temporale qualificata. La validazione temporale qualificata, ove disponibile, è quella del livello T1 rilasciata dal TSA esterno sulla Merkle root del batch.

Il livello T1 aggrega un insieme di digest in una struttura Merkle conforme alla domain separation di RFC 6962, e sottopone la radice della struttura a un servizio di validazione temporale qualificato erogato da una Time Stamping Authority esterna, qualificata ai sensi del Regolamento (UE) n. 910/2014 (eIDAS), conforme allo standard RFC 3161 e verificabile nelle EU Trusted Lists applicabili al momento della verifica; il TSA token risultante reca l'identità di Ten Sigma Sagl quale operatore del batch presso il TSA.

Il livello T2 ancora la radice giornaliera del batch alla blockchain pubblica di Bitcoin tramite il protocollo OpenTimestamps.

Il livello T2 costituisce un ancoraggio crittografico pubblicamente verificabile e non un servizio di registro elettronico qualificato (qualified electronic ledger) ai sensi del Regolamento eIDAS, come modificato. CertiSigma non opera come prestatore qualificato di servizi relativi a registri elettronici e l'ancoraggio OpenTimestamps/Bitcoin non produce, di per sé, gli effetti giuridici o le presunzioni proprie di un registro elettronico qualificato.

Ciascuno dei tre livelli è indipendentemente verificabile da terzi attraverso meccanismi crittografici standard, senza necessità di accesso ai sistemi di CertiSigma e senza intermediazione del servizio stesso. La verifica di T0 richiede il digest, il payload canonico ricostruibile, la chiave pubblica ECDSA pubblicata da CertiSigma e la firma stessa. La verifica di T1 richiede il digest, la Merkle proof, e il TSA token verificabile contro l'infrastruttura del TSA esterno. La verifica di T2 richiede il file di prova OpenTimestamps verificabile contro la blockchain pubblica di Bitcoin.

2. Qualificazione giuridica del servizio

CertiSigma non si qualifica come, e non offre, alcuno dei seguenti servizi giuridicamente regolamentati. L'elencazione che segue è esplicativa e necessaria al fine di disambiguare correttamente la natura del servizio rispetto a istituti contigui ma distinti.

CertiSigma non opera come notaio o pubblico ufficiale rogante. Il servizio non riceve dichiarazioni di volontà delle parti, non identifica i soggetti delle dichiarazioni, non conferisce pubblica fede agli atti, non opera autenticazione di firme né di copie, e non produce atto pubblico o scrittura privata autenticata nel senso degli ordinamenti nazionali svizzero, italiano o europeo. Le funzioni notarili restano integralmente di competenza dei notai abilitati nelle rispettive giurisdizioni.

CertiSigma non opera come prestatore di servizi fiduciari qualificati ai sensi del Regolamento (UE) n. 910/2014 (eIDAS). In particolare, il servizio non offre firma elettronica qualificata, sigillo elettronico qualificato, servizio elettronico di recapito certificato qualificato o certificati qualificati di autenticazione di sito web. Il servizio non produce firma elettronica qualificata né sigillo elettronico qualificato sui contenuti del cliente, né sull'identità del cliente attestante. La presunzione legale di integrità e di attribuzione che caratterizza la firma elettronica qualificata o il sigillo elettronico qualificato eIDAS non è prodotta dal servizio CertiSigma.

CertiSigma non opera come Time Stamping Authority qualificata. Il livello T1 dell'attestazione utilizza un servizio di validazione temporale qualificato erogato da una TSA esterna la cui qualificazione deve risultare dalle EU Trusted Lists applicabili al momento della verifica, e che produce il timestamp RFC 3161 sulla radice Merkle aggregata. CertiSigma è cliente del TSA qualificato esterno per la sottomissione della Merkle root, non è essa stessa TSA. La qualificazione del timestamp T1 deriva quindi dal TSA esterno e dai suoi certificati, secondo il regime eIDAS applicabile al TSA, e non da CertiSigma.

CertiSigma non opera come servizio di firma elettronica avanzata (FEA) o qualificata (FEQ) sul contenuto del cliente. I servizi di FEA/FEQ sono funzionali ad attestare l'attribuzione di una firma a un soggetto firmatario identificato e l'integrità del contenuto firmato. CertiSigma non identifica i soggetti che richiedono l'attestazione, non firma il contenuto del cliente, e non produce

attribuzione di una firma a un soggetto firmatario. Ove un workflow richieda contemporaneamente attestazione di esistenza/integrità (CertiSigma) e attribuzione di firma a un soggetto identificato (FEA/FEQ), i due servizi operano in modo complementare e non sostitutivo.

CertiSigma non opera come Certificate Authority per certificati X.509 di firma o di autenticazione. Le chiavi crittografiche di CertiSigma sono utilizzate esclusivamente per la firma T0 sul payload canonico delle attestazioni e per la firma dei derived lists; non vengono emessi certificati di firma a favore dei clienti, non viene operata attività di Registration Authority, e non partecipa ad alcuno schema di Public Key Infrastructure pubblica nel senso del trust model X.509 commerciale.

CertiSigma non conserva, non rende accessibili, non distribuisce e non comunica al pubblico i contenuti originali dei clienti. Ai fini della Direttiva 2000/31/CE sull'eCommerce, del Digital Services Act (Regolamento (UE) 2022/2065) e della normativa nazionale equivalente, l'eventuale qualificazione del servizio deve essere valutata in relazione alle sole informazioni effettivamente ricevute e conservate dal servizio — valori di hash e, ove forniti, metadati operativi — non rispetto a contenuti originali, che non vengono ricevuti né ospitati. In ogni caso, dai valori di hash crittografici non è tecnicamente possibile ricostruire il contenuto sottostante in virtù delle proprietà crittografiche della funzione hash.

CertiSigma non opera come operatore di servizio di comunicazione elettronica ai sensi della Direttiva (UE) 2018/1972 (Codice europeo delle comunicazioni elettroniche) né come operatore di telecomunicazioni nel senso della legislazione svizzera applicabile (LTC). Il servizio non veicola comunicazioni tra parti, non intermedia messaggi, e non costituisce servizio di comunicazione interpersonale.

CertiSigma non opera come intermediario finanziario ai sensi della legge svizzera sul riciclaggio di denaro (LRD), non gestisce mezzi di pagamento per conto di terzi, non opera scambi di valuta, e non emette strumenti monetari. Il servizio non rientra nelle attività soggette a obblighi di KYC ai sensi della LRD.

CertiSigma non opera come servizio fiduciario di archiviazione qualificata di documenti elettronici. L'archiviazione del contenuto sostantivo dei documenti del cliente è di competenza del cliente stesso e dei sistemi di archiviazione

documentale che il cliente utilizza, eventualmente certificati secondo gli schemi applicabili nella giurisdizione del cliente. CertiSigma conserva esclusivamente la propria infrastruttura crittografica e le proprie registrazioni di attestazione.

CertiSigma non opera come servizio di registro elettronico qualificato o come prestatore qualificato di servizi fiduciari relativi a registri elettronici ai sensi del Regolamento eIDAS, come modificato. L'uso del protocollo OpenTimestamps e della blockchain pubblica Bitcoin al livello T2 ha funzione di evidenza crittografica indipendente e non comporta l'assunzione delle qualifiche, degli obblighi o delle presunzioni legali proprie dei qualified electronic ledgers.

3. Cosa il servizio dichiara e attesta

Alla luce delle qualificazioni sopra indicate, il servizio dichiara e attesta esclusivamente quanto segue.

Il digest SHA-256 ricevuto in input dall'API di attestazione è stato osservato dal servizio in un momento temporale puntualmente registrato. Tale osservazione si traduce nella produzione di un payload canonico in formato documentato (versione del formato, digest, timestamp di registrazione) e nella firma di tale payload con la chiave ECDSA P-256 di CertiSigma pubblicata e verificabile. La firma T0 attesta che CertiSigma ha osservato il digest e ha prodotto la firma su quel preciso payload canonico, entro l'istante temporale dichiarato.

Il digest è stato incluso, nel processo asincrono di aggregazione batch del servizio, in una struttura Merkle insieme ad altri digest osservati nello stesso intervallo di batching. La radice di tale struttura è stata sottoposta a un servizio di validazione temporale qualificato erogato da una TSA esterna, conforme a RFC 3161 e verificabile nelle EU Trusted Lists applicabili al momento della verifica, il quale ha emesso un timestamp token recante il proprio certificato qualificato e la propria evidenza temporale. La Merkle proof che collega il digest specifico alla radice timestampata è disponibile e verificabile in modo indipendente.

La radice giornaliera del batch è stata ancorata alla blockchain pubblica di Bitcoin tramite il protocollo OpenTimestamps, e il file di prova OpenTimestamps è disponibile e verificabile contro la blockchain Bitcoin in modo indipendente, senza intermediazione di CertiSigma.

Ciascuna di queste affermazioni è verificabile crittograficamente in modo indipendente da CertiSigma, attraverso meccanismi standard di verifica ECDSA, RFC 3161 e OpenTimestamps. Il valore probatorio di tali verifiche è quello che il giudice o l'autorità competente ascrive alla forma di evidenza in questione, secondo il diritto applicabile e le circostanze del caso.

4. Cosa il servizio non dichiara e non attesta

Il servizio non dichiara e non attesta nulla in merito a quanto segue. L'elencazione è non esaustiva e va letta come esplicitazione di posizioni che il servizio non assume e che il servizio non può tecnicamente assumere.

Il servizio non identifica e non attesta l'identità del soggetto che ha richiesto l'attestazione di un singolo digest, fatto salvo quanto custodito nel claim metadata privato all'API key del richiedente. Nelle attestazioni effettuate tramite il front-end pubblico ExistBefore senza autenticazione, l'identità del richiedente non è acquisita, non è verificata, e non è registrata.

Il servizio non identifica, non attesta e non ha modo di conoscere l'identità del soggetto che ha generato il contenuto originale corrispondente al digest. La funzione hash SHA-256 è priva di informazione sull'origine, sull'autore, sul possessore o sul titolare giuridico del contenuto da cui è calcolata.

Il servizio non attesta la paternità del contenuto, intesa come autorialità intellettuale ai sensi del diritto d'autore svizzero, italiano o europeo. L'attestazione di esistenza temporale di un digest non equivale a deposito d'autore, non equivale a registrazione SIAE o equivalente, e non costituisce di per sé prova di anteriorità autorale nel senso del diritto d'autore. L'utilità eventuale dell'attestazione in un contenzioso di diritto d'autore è valutata dall'autorità giudiziaria nel contesto delle prove offerte e del diritto applicabile.

Il servizio non attesta la proprietà o la titolarità giuridica del contenuto. L'attribuzione di proprietà o di titolarità è materia di diritto contrattuale, di diritto reale, di diritto della proprietà intellettuale o di diritto di famiglia/successioni, a seconda del contenuto, e non è prodotta né presunta dal servizio.

Il servizio non attesta la veridicità, l'accuratezza, la completezza o la non fuorvianza del contenuto. L'esistenza temporale di un digest che corrisponde a

un contenuto falso o fuorviante è attestabile esattamente come quella di un contenuto vero; il servizio è semanticamente neutro.

Il servizio non attesta la liceità del contenuto. L'esistenza temporale di un digest corrispondente a contenuto illecito è tecnicamente attestabile, e il servizio non ha modo di sapere — per costruzione — se un digest corrisponde a contenuto lecito o illecito. La responsabilità della liceità del contenuto sottostante resta integralmente in capo all'utente attestante, secondo i Terms of Service del servizio e secondo la legge applicabile.

Il servizio non attesta il consenso di soggetti terzi rispetto al contenuto, ove tale consenso sia giuridicamente rilevante. Il consenso al trattamento di dati personali, il consenso a riproduzione di immagini, il consenso contrattuale e altre forme di consenso non sono materia di verifica del servizio.

Il servizio non attesta la conformità del contenuto, dei processi o dell'organizzazione del cliente a un quadro normativo specifico, inclusi senza limitazione NIS2, DORA, ISO 27001, ISO 27037, GDPR, LPD svizzera. L'attestazione fornisce un riferimento crittografico verificabile che può supportare la documentazione di conformità predisposta dal cliente o dal suo consulente, ma non costituisce di per sé certificazione di conformità.

Il servizio non costituisce prova legale conclusiva di alcun fatto. Il valore probatorio dell'attestazione è quello che il giudice o l'autorità competente attribuiscono all'evidenza secondo il diritto applicabile, la catena di custodia, il processo di raccolta delle evidenze, il contesto fattuale e l'insieme degli elementi probatori disponibili.

Il servizio non sostituisce il giudizio dell'auditor, del consulente, del perito, del legale o dell'autorità giudiziaria nei rispettivi ambiti di competenza. L'attestazione è uno strumento che rafforza la posizione evidenziale di chi la utilizza, non un sostituto del giudizio qualificato che la legge o il contesto richiedono.

5. Cosa il servizio non può fornire per ragioni strutturali

Indipendentemente dalla volontà di Ten Sigma Sagl, e a prescindere da eventuali richieste di terzi, inclusi soggetti che esercitino poteri istruttori secondo procedure giuridicamente valide, alcune categorie di informazioni

non sono tecnicamente nella disponibilità del servizio in virtù di scelte architetturali. Questa sezione individua tali categorie.

Il servizio non può fornire il contenuto originale dei file, documenti, dati o materiali dei clienti, perché tali contenuti non vengono mai trasmessi al servizio. Il modello operativo è strutturato in modo che il cliente calcoli il digest SHA-256 localmente, nel proprio ambiente, e trasmetta al servizio esclusivamente il digest di 32 byte. La preimage resistance della funzione SHA-256 rende computazionalmente irrealizzabile la ricostruzione del contenuto a partire dal digest.

Il servizio non può fornire informazioni sui metadati operativi opzionalmente associati a un'attestazione (campi source, extra_data e tags) a soggetti diversi dal claim owner autenticato. Tali metadati, ove forniti dal cliente, sono custoditi in associazione al claim_id dell'API key che ha effettuato l'attestazione e non sono mai esposti sugli endpoint pubblici. Ove il cliente, come suggerito, abbia optato per la cifratura client-side AES-256-GCM dei metadati extra_data, il servizio conserva esclusivamente il ciphertext opaco e non dispone della chiave di cifratura, che resta nella custodia esclusiva del cliente; in tal caso il servizio è tecnicamente impossibilitato a fornire il plaintext anche su richiesta giudiziaria valida, in nessuna circostanza.

Il servizio non può fornire correlazione applicativa tra attestazioni e indirizzi IP dei richiedenti. L'IP sorgente delle richieste è visibile a livello di trasporto per finalità di rate limiting infrastrutturale, ma non viene scritto in tabelle applicative associate alle attestazioni. Eventuali log infrastrutturali transitori, ove presenti per finalità tecniche legittime di sicurezza operativa, non sono indicizzati né correlati al digest attestato.

Il servizio non può fornire identificazione del soggetto attestante per le attestazioni effettuate tramite il front-end pubblico ExistBefore. Tale identificazione non è acquisita per scelta architetturale, in conformità al modello «no account, no upload, no identification» che caratterizza tale endpoint.

Il servizio non può fornire l'identità del titolare giuridico del contenuto sottostante un digest attestato. Ciò per la ragione strutturale che tale identità non è mai stata comunicata al servizio e che il digest stesso non veicola, per costruzione matematica, alcuna informazione sull'origine, sull'autorialità o sulla titolarità del contenuto.

Il servizio non può fornire conferma o smentita rispetto al fatto che uno specifico contenuto del mondo reale corrisponda a un digest attestato, in assenza del contenuto stesso. La verifica può essere effettuata esclusivamente da chi possiede il contenuto, calcolando il SHA-256 del contenuto e confrontandolo con il digest attestato. Il servizio non dispone di alcun meccanismo di reverse lookup contenuto-digest, perché il contenuto è strutturalmente assente dai propri sistemi.

L'identità di Ten Sigma Sagl che appare nel TSA token RFC 3161 al livello T1 è l'identità del soggetto richiedente del timestamping della Merkle root del batch, e non è l'identità di alcuno dei clienti attestanti i cui digest sono inclusi come foglie nella Merkle tree. Il TSA esterno non conosce, non riceve e non ha modo di dedurre l'identità dei singoli clienti attestanti.

6. Posizione giurisdizionale e quadro normativo applicabile

Ten Sigma Sagl è società di diritto svizzero, con sede in Svizzera. Il diritto applicabile in via principale al rapporto tra Ten Sigma Sagl e i propri clienti, e all'erogazione del servizio, è il diritto svizzero, salvo diverse pattuizioni contrattuali per singoli rapporti commerciali.

Il foro competente per le controversie relative al servizio è il foro svizzero indicato nei Terms of Service, salvo diverse pattuizioni contrattuali, e salve le norme inderogabili in materia di consumatori.

Con specifico riferimento a richieste provenienti da autorità di paesi terzi, nei limiti dell'assetto societario e infrastrutturale dichiarato del servizio, Ten Sigma Sagl non è normalmente destinataria diretta di ordini ai sensi del CLOUD Act statunitense o di FISA Section 702, in quanto non è una società di diritto statunitense e non dichiara una presenza giurisdizionale negli Stati Uniti. Resta ferma la necessità di valutare separatamente eventuali fornitori terzi, infrastrutture, affiliati, conti, servizi cloud o altri soggetti sotto giurisdizione USA, che possono avere obblighi propri di divulgazione. Eventuali richieste di divulgazione provenienti da autorità di paesi terzi nei confronti di Ten Sigma Sagl sono gestite, ove applicabile, attraverso i canali di cooperazione giudiziaria bilaterale previsti dai trattati applicabili (Mutual Legal Assistance Treaty e accordi equivalenti) e, ove pertinente, con il vaglio dell'autorità svizzera competente.

L’infrastruttura tecnologica che eroga il servizio è ospitata presso Infomaniak Network SA, società di diritto svizzero con sede a Ginevra, che dichiara di progettare e gestire data center ubicati esclusivamente sul territorio svizzero. Infomaniak Network SA dichiara sul proprio sito ufficiale di essere titolare, allo stato della verifica condotta, delle certificazioni ISO/IEC 27001:2022 (sistema di gestione della sicurezza delle informazioni), ISO 9001:2015 (gestione della qualità), ISO 14001:2015 (gestione ambientale) e ISO 50001:2018 (gestione dell’energia), nonché dei label svizzeri Swiss Made Software, Swiss Hosting e Swiss Made. Tali elementi sono riferiti a Infomaniak Network SA in quanto fornitore infrastrutturale e, secondo quanto dichiarato dal fornitore, documentano la localizzazione svizzera della sede societaria, dello sviluppo software prevalente o esclusivo, e dell’hosting o esecuzione dei dati cliente e dei servizi interessati in data center situati in Svizzera. Essi non costituiscono certificazione del servizio CertiSigma in sé, la cui qualificazione resta autonoma; sono qui richiamati al fine di documentare il profilo svizzero dell’infrastruttura sottostante.

Allo stato dichiarato dell’architettura del servizio, la terminazione TLS e il trattamento applicativo delle richieste verso gli endpoint API di CertiSigma non sono interposti da Content Delivery Network, reverse proxy applicativi, servizi di terminazione TLS, servizi di mitigazione DDoS o servizi di filtraggio del traffico gestiti da fornitori terzi sotto giurisdizione di paesi terzi diversi dalla Svizzera. In particolare, per l’infrastruttura sotto il controllo di Ten Sigma Sagl, non risultano interposti provider riconducibili a gruppi societari soggetti alla giurisdizione statunitense o a regimi analoghi di accesso extra-svizzero ai dati. Resta salvo il routing Internet ordinario, il peering e il transito di rete non controllabile end-to-end da Ten Sigma Sagl, che non comportano di per sé terminazione applicativa o accesso al contenuto delle richieste cifrate.

La localizzazione svizzera dell’infrastruttura non esclude eventuali obblighi propri di Infomaniak Network SA o di Ten Sigma Sagl nei confronti di autorità svizzere competenti, nei limiti previsti dal diritto svizzero applicabile e da atti giuridicamente validi. Tale profilo non incide tuttavia sulla natura content-blind del servizio: il contenuto originale dei clienti non è ricevuto né conservato da CertiSigma, e resta quindi indisponibile anche in presenza di una richiesta giuridicamente valida.

Resta ferma la valutazione, che il cliente è invitato a condurre separatamente, sui propri sistemi, fornitori, dispositivi e canali di comunicazione utilizzati per interagire con il servizio, che possono presentare proprie esposizioni indipendenti da quelle qui descritte e non sono nella sfera di controllo di Ten Sigma Sagl.

Il regime di protezione dei dati personali applicabile al servizio è la Legge federale svizzera sulla protezione dei dati (LPD), nella sua versione revisionata in vigore dal 1° settembre 2023. Per i clienti stabiliti nell'Unione europea o per il trattamento di dati personali di persone fisiche stabilite nell'Unione europea, ove configurato, può applicarsi anche il Regolamento (UE) 2016/679 (GDPR), nei limiti del suo ambito territoriale.

Il 15 gennaio 2024, la Commissione Europea ha pubblicato il proprio report sulla revisione delle decisioni di adeguatezza adottate sotto la previgente Direttiva 95/46/CE, confermando che la Svizzera garantisce un livello adeguato di protezione dei dati personali anche ai sensi del Regolamento (UE) 2016/679 (GDPR). La decisione di adeguatezza relativa alla Svizzera, originariamente adottata nel 2000, resta pertanto in vigore. A seguito di tale conferma, i dati personali trasferiti dall'Unione Europea verso la Svizzera possono continuare a fluire liberamente, senza la necessità di garanzie aggiuntive specifiche, come rilevato anche dall'Incaricato federale della protezione dei dati e della trasparenza (EdöB). Restano salve eventuali condizioni, aggiornamenti o trasferimenti ulteriori verso paesi terzi.

Si osserva, in linea con la qualificazione del servizio offerta nelle sezioni precedenti, che un digest SHA-256 non è, per sua sola natura tecnica, necessariamente un dato personale ai sensi dell'art. 4(1) GDPR né ai sensi della definizione equivalente della LPD. Può tuttavia diventarlo quando, tenuto conto dei mezzi ragionevolmente utilizzabili dal titolare o da terzi, consente o facilita l'identificazione diretta o indiretta di una persona fisica, ad esempio in caso di input enumerabili o prevedibili (indirizzi e-mail, numeri di documento d'identità, identificativi strutturati con spazio degli input limitato), metadati correlabili, associazione con account o API key, o altri elementi di contesto. In tali casi il regime di protezione dei dati personali può applicarsi anche all'hash stesso. Il servizio offre meccanismi di mitigazione (HMAC con chiave, derived lists, cifratura client-side dei metadati) per gestire tali casi e raccomanda al cliente di utilizzarli ove pertinente.

Nei casi in cui un trattamento di dati personali dovesse configurarsi, Ten Sigma Sagl agisce quale titolare autonomo del trattamento per i trattamenti da essa determinati in relazione alla gestione del servizio, alla sicurezza operativa, ai log di sistema, alla prevenzione degli abusi, alla fatturazione, alla contabilità e alla gestione del rapporto contrattuale. Con riferimento ai digest e ai metadati conferiti dal cliente tramite API e trattati per l'erogazione del servizio di attestazione nell'ambito delle finalità determinate dal cliente, Ten Sigma Sagl agisce, ove applicabile, quale responsabile del trattamento ai sensi dell'art. 28 GDPR e dell'art. 9 LPD, secondo il relativo Data Processing Agreement o clausole contrattuali equivalenti. Resta salvo che, quando Ten Sigma Sagl determini autonomamente finalità e mezzi di specifici trattamenti, o quando i dati trattati non siano qualificabili come dati personali, la qualificazione privacy deve essere valutata in relazione al concreto trattamento.

7. Obblighi di registrazione e conservazione dati

Ten Sigma Sagl non è soggetta, in base al diritto svizzero e alla qualificazione del servizio descritta nella sezione 2, a obblighi specifici di registrazione dell'identità degli utilizzatori del servizio per finalità di sorveglianza, prevenzione del riciclaggio o cooperazione di intelligence. Gli obblighi di due diligence e KYC in materia antiriciclaggio ai sensi della LRD si applicano ai soggetti e alle attività che integrano la qualifica di intermediario finanziario; essi non derivano dalla mera fatturazione di un servizio tecnologico, né dalla sola erogazione del servizio di attestazione crittografica qui descritto. Resta ferma la conservazione dei dati contrattuali, fiscali e contabili relativi ai clienti di fatturazione secondo le norme applicabili.

Ten Sigma Sagl mantiene, per finalità interne di operatività e di obbligo civilistico contabile (Codice delle obbligazioni svizzero, art. 957 ss.), le registrazioni necessarie alla gestione del rapporto commerciale con i clienti di fatturazione, secondo i tempi e le modalità previsti dalle norme applicabili in materia di documentazione contabile e fiscale.

Le scelte architetturali del servizio in materia di registrazione di metadati associati alle attestazioni — in particolare l'assenza di scrittura applicativa dell'IP sorgente associato al digest, e il regime di privacy del claim metadata — non costituiscono adempimento di obblighi normativi specifici, in quanto tali

obblighi non sussistono, ma costituiscono scelte di progettazione del servizio funzionali al modello «content-blind by architecture» che caratterizza l'offerta commerciale.

Si segnala che il servizio è strutturato in modo che la cooperazione con autorità giudiziaria svizzera competente, ove richiesta tramite atti giuridicamente validi nel quadro della giurisdizione svizzera, sia tecnicamente possibile nei limiti di ciò che è materialmente custodito dal servizio. La sezione 5 del presente documento delinea le categorie di informazioni che, in virtù delle scelte architetturali, non sono nella disponibilità del servizio e che pertanto non possono essere fornite a nessun soggetto, incluse le autorità nei limiti di richieste giuridicamente valide.

8. Responsabilità dell'utente attestante

L'utente attestante è il soggetto che richiede l'attestazione di un digest, sia tramite l'API autenticata tramite API key (canale CertiSigma propriamente detto), sia tramite il front-end pubblico ExistBefore. L'utente attestante è l'unico responsabile per la liceità, la veridicità, l'accuratezza e l'appropriatezza del contenuto sottostante il digest che richiede di attestare.

L'utente attestante dichiara, mediante accettazione dei Terms of Service del servizio, di non utilizzare il servizio per finalità contrarie alla legge applicabile nella propria giurisdizione o nella giurisdizione in cui il contenuto sottostante è destinato a produrre effetti. L'attestazione di un digest non costituisce, e non può essere rappresentata da parte dell'utente, come avallo, validazione o certificazione del contenuto da parte di Ten Sigma Sagl.

L'utente attestante è inoltre responsabile per la rappresentazione corretta del valore probatorio dell'attestazione presso terzi. La rappresentazione del servizio CertiSigma come servizio di firma elettronica qualificata, come servizio notarile, come certificazione di conformità a un quadro normativo, o come prova legale conclusiva di alcun fatto, costituisce overclaim non autorizzato e potenzialmente fuorviante, e l'utente che effettua tali rappresentazioni se ne assume l'integrale responsabilità.

Nei contesti di workflow che richiedono attestazione di esistenza/integrità e contemporaneamente attribuzione di firma a un soggetto identificato (firma elettronica avanzata o qualificata, FEA/FEQ, eIDAS qualified signature), è responsabilità dell'utente o dell'integratore predisporre il workflow in modo che

entrambe le funzioni siano coperte dai servizi qualificati appropriati. CertiSigma si occupa della prima funzione; la seconda è di competenza di prestatori di servizi fiduciari qualificati ai sensi della normativa applicabile.

9. Divulgazione su richiesta dell'autorità

In caso di richieste di divulgazione provenienti da autorità giudiziaria svizzera competente, espresse mediante atti giuridicamente validi nel quadro del diritto svizzero applicabile, Ten Sigma Sagl coopera nei limiti dell'ordine ricevuto e nei limiti di ciò che è materialmente custodito dal servizio. Si rinvia alla sezione 5 per la descrizione delle categorie di informazioni che non sono tecnicamente nella disponibilità del servizio.

In caso di richieste provenienti da autorità di paesi terzi non veicolate attraverso i canali di cooperazione giudiziaria bilaterale di cui la Svizzera è parte (MLAT e equivalenti), Ten Sigma Sagl non è tenuta a darvi seguito né è esposta a obbligo esecutivo diretto. Le richieste in questione devono passare attraverso il canale formale della cooperazione giudiziaria ed essere vagliate dall'autorità svizzera competente.

Ten Sigma Sagl si riserva la facoltà, nel rispetto del diritto applicabile, di informare il cliente interessato dell'esistenza di una richiesta di divulgazione che lo riguardi, salvo nei casi in cui tale informazione sia preclusa da specifico obbligo di riservatezza imposto dall'autorità richiedente nel quadro di un atto giuridicamente valido.

10. Posizionamento rispetto a istituti complementari

Per la corretta comprensione del valore del servizio e del suo posizionamento nei workflow operativi del cliente, si articolano di seguito i rapporti complementari tra CertiSigma e istituti adiacenti.

CertiSigma e notariato

Il notaio attesta dichiarazioni di volontà, identifica le parti, conferisce pubblica fede ad atti e fatti, e produce atto pubblico o scrittura privata autenticata. CertiSigma attesta l'esistenza temporale di un digest crittografico. Un atto notarile può avere il proprio digest attestato da CertiSigma, e in tal caso

l'attestazione CertiSigma fornisce una prova di esistenza temporale aggiuntiva e indipendente del documento; l'atto notarile rimane integralmente competenza e responsabilità del notaio.

CertiSigma e firma elettronica qualificata eIDAS

La firma qualificata eIDAS assicura, secondo il relativo regime giuridico, l'attribuzione della firma a un soggetto identificato e l'integrità del contenuto firmato. CertiSigma attesta l'esistenza temporale di un digest. I due servizi sono complementari: un documento sottoscritto con firma qualificata eIDAS può avere il proprio digest attestato da CertiSigma, e in tal caso si ottengono entrambe le funzioni — attribuzione di firma al soggetto identificato (eIDAS) ed esistenza temporale con percorso evidenziale multilivello T0/T1/T2 (CertiSigma). Questa è precisamente la configurazione che si realizza, ad esempio, in workflow NIS2 in cui i fornitori sottoscrivono con FEA/FEQ il report di evidenza, e l'integrità complessiva del dossier è attestata da CertiSigma.

CertiSigma e la posta elettronica certificata

La PEC italiana e equivalenti nazionali producono prova legale dell'invio e della ricezione di una comunicazione tra due caselle PEC identificate. CertiSigma attesta l'esistenza temporale di un digest. Una comunicazione PEC contenente un allegato può vedere il digest dell'allegato attestato da CertiSigma per documentarne anteriorità e integrità rispetto a momenti precedenti all'invio PEC.

CertiSigma e timestamping qualificato eIDAS

Il timestamp qualificato eIDAS, prodotto da un TSA qualificato, ha l'effetto giuridico previsto dall'art. 41 del Regolamento (UE) n. 910/2014 di presunzione di accuratezza della data e dell'ora indicate e di integrità dei dati ai quali tale data e ora sono associate, nei limiti previsti dalla norma applicabile. Il livello T1 di CertiSigma utilizza un servizio di validazione temporale qualificato erogato da un TSA esterno conforme al regime eIDAS e verificabile nelle EU Trusted Lists applicabili al momento della verifica; il TSA token T1 contiene il timestamp qualificato riferito alla Merkle root del batch. La Merkle proof collega in modo crittograficamente verificabile il digest specifico alla radice timestampata. La presunzione eIDAS si applica direttamente solo alla radice timestampata; la Merkle proof estende l'integrità, ma non automaticamente la presunzione legale al digest individuale, salvo valutazione giudiziale.

CertiSigma e registri elettronici qualificati eIDAS

Il registro elettronico qualificato eIDAS è un servizio fiduciario distinto, soggetto a requisiti propri e gestito da uno o più prestatori qualificati. CertiSigma non offre tale servizio: l'ancoraggio OpenTimestamps/Bitcoin del livello T2 serve a rendere verificabile pubblicamente l'esistenza della radice giornaliera, ma non trasforma CertiSigma in prestatore qualificato di registro elettronico né attribuisce automaticamente all'ancoraggio le presunzioni legali previste per i qualified electronic ledgers.

CertiSigma e deposito d'autore

Il deposito d'autore presso autorità o enti competenti, servizi nazionali di deposito o registrazione, o altri strumenti probatori riconosciuti nella giurisdizione applicabile, può produrre specifici effetti probatori in materia di anteriorità autoriale. CertiSigma non sostituisce il deposito d'autore e non produce gli effetti probatori specificamente connessi a tale istituto, ma può fornire un'evidenza di esistenza temporale di una versione specifica di un'opera utile in workflow di documentazione iterativa o di evidenza pre-deposito.

CertiSigma e archiviazione qualificata

L'archiviazione qualificata di documenti elettronici, in particolare nel sistema italiano della conservazione a norma, produce specifici effetti probatori e di equiparazione tra documento elettronico conservato e documento cartaceo. CertiSigma non sostituisce l'archiviazione qualificata e non assolve gli obblighi di conservazione documentale a norma applicabili al cliente, ma può integrarli fornendo evidenze di esistenza temporale di documenti puntuali nel ciclo di vita della conservazione.

CertiSigma e GDPR/LPD

Il quadro di protezione dei dati personali si applica al trattamento di dati personali in capo al titolare del trattamento. CertiSigma, quando l'input e i metadati non consentono l'identificazione diretta o indiretta di una persona fisica tenuto conto dei mezzi ragionevolmente utilizzabili, non tratta dati personali relativamente al contenuto sottostante. Quando l'input è qualificabile come dato personale o indirettamente identificante, oppure quando l'hash è associato a metadati, account, API key o altri elementi correlabili a una persona

fisica, il regime di protezione dei dati può applicarsi anche all'hash o ai metadati. CertiSigma offre meccanismi di mitigazione (HMAC, derived lists, client-side encryption dei metadati) che il cliente è responsabile di utilizzare appropriatamente.

Quanto ai ruoli privacy, Ten Sigma Sagl opera quale titolare autonomo per i trattamenti propri connessi alla gestione del servizio, ai log di sistema, alla sicurezza, alla fatturazione e alla contabilità; opera invece, ove applicabile, quale responsabile del trattamento per i digest e i metadati conferiti dal cliente e trattati per conto del cliente nell'ambito del servizio, ai sensi dell'art. 28 GDPR e dell'art. 9 LPD.

11. Limitazione di responsabilità

Salvo quanto diversamente previsto nei Termini di Servizio applicabili al rapporto contrattuale con il cliente, e nei limiti massimi consentiti dal diritto applicabile, la responsabilità complessiva di Ten Sigma Sagl verso il cliente, a qualsiasi titolo derivante o comunque connessa all'erogazione, all'utilizzo, alla mancata disponibilità, al malfunzionamento, alla verifica o all'interpretazione delle attestazioni prodotte dal servizio CertiSigma, è limitata all'importo dei corrispettivi effettivamente pagati dal cliente a Ten Sigma Sagl nei dodici mesi precedenti l'evento dannoso.

In nessun caso Ten Sigma Sagl risponde per danni indiretti, consequenziali, speciali, incidentali, punitivi o esemplari, né per perdita di profitto, perdita di ricavi, perdita di opportunità commerciali, perdita di avviamento, perdita di dati, perdita di chance, interruzione dell'attività, costi di sostituzione, danni reputazionali o pretese di terzi, anche qualora Ten Sigma Sagl sia stata informata della possibilità del verificarsi di tali danni.

La limitazione di responsabilità di cui al presente articolo si applica indipendentemente dal titolo della pretesa fatta valere, inclusi, senza limitazione, responsabilità contrattuale, extracontrattuale, precontrattuale, garanzia, indennizzo, responsabilità per inadempimento, responsabilità per inesatto adempimento o altra base giuridica.

Restano in ogni caso salve le responsabilità che non possono essere escluse o limitate ai sensi del diritto applicabile, incluse, ove applicabile, le ipotesi di dolo o colpa grave e ogni altra responsabilità inderogabile prevista da norme

imperative. Ai sensi dell'art. 100 del Codice delle obbligazioni svizzero, è nulla ogni pattuizione volta a escludere o limitare preventivamente la responsabilità per dolo o colpa grave, nei limiti previsti dal diritto applicabile.

La presente limitazione costituisce elemento essenziale dell'equilibrio economico e contrattuale del servizio, tenuto conto della natura content-blind dell'attestazione, dell'assenza di accesso ai contenuti originali del cliente, della funzione meramente evidenziale e non sostitutiva del servizio rispetto a valutazioni notarili, giudiziarie, peritali, legali, di conformità o di archiviazione qualificata, nonché della necessità che il cliente mantenga autonomamente adeguati processi di conservazione, verifica, backup, gestione del rischio e documentazione probatoria.

12. Modifiche del presente documento

Il presente documento descrive il funzionamento del servizio e le posizioni giuridiche di Ten Sigma Sagl alla data della sua pubblicazione. Modifiche al servizio o all'organizzazione di Ten Sigma Sagl possono comportare aggiornamenti del presente documento, che saranno comunicati con preavviso adeguato e ragionevole ai clienti contrattuali e resi disponibili pubblicamente.

In caso di discrepanza tra il presente documento e i Terms of Service contrattualmente sottoscritti da un cliente, prevalgono i Terms of Service nella versione applicabile al rapporto contrattuale di quel cliente, salvo che la discrepanza riguardi descrizione tecnica del servizio, nel qual caso prevale la documentazione tecnica pubblicata dal servizio nella versione vigente al momento dell'erogazione.

https://certisigma.ch/legal/imprint