UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

Stato dell'arte della trasmissione certificata di messaggi elettronici senza trusted third party e possibili evoluzioni

Relatore
Prof. Luca Boldrin

Laureando
Tommaso Zanon

ANNO ACCADEMICO 2023-2024
Data di laurea 16/11/2023

Abstract

In un mondo sempre più interconnesso e digitale, emerge la crescente necessità di un sistema per lo scambio di documenti elettronici che possa garantire prove affidabili di spedizione e ricezione. Per sopperire a questo bisogno, sono state introdotte le email certificate, messaggi elettronici che vengono scambiati mediante protocolli di scambio equo. Molti dei servizi esistenti che si occupano di email certificate si basano su intermediari noti come Trusted Third Parties (TTP), che semplificano il processo ma possono comportare problemi tecnici, inefficienze e costi aggiuntivi, oltre a sollevare dubbi sulla loro affidabilità.

In questa tesi viene effettuata: un’analisi dei protocolli di scambio di email certificate esistenti, un esame della normativa italiana ed europea riguardo a questo tema e la presentazione di un modello di architettura per lo scambio di email certificate senza l'uso di intermediari.

Sommario

1 Introduzione

In un mondo sempre più connesso e digitale, nel quale si può accedere ad internet quasi istantaneamente e a costi accessibili, diventa sempre più necessario trovare un sistema che permetta lo scambio di documenti elettronici che garantisca prove dell'avvenuta spedizione e ricezione degli stessi.
Le semplici email non bastano per un servizio del genere, infatti al mittente o al destinatario basta cancellare il messaggio dalla loro casella di posta per dire di non aver mai spedito/ricevuto una certa comunicazione. La controparte non sarà in grado di dimostrare il contrario.
Per questo motivo sono nate le email certificate, le quali vengono scambiate attraverso protocolli di scambio equo, nei quali, alla fine degli stessi, entrambe le parti ottengono ciò che vogliono o nessuna delle due ottiene qualcosa.
I servizi che permettono lo scambio di email certificate forniscono a mittente e destinatario anche prove dell'origine e della ricezione del messaggio, in modo che in caso di disputa una terza parte giudicante (come un giudice) possa capire se una delle parti si sta comportando in modo disonesto.

Molti dei servizi di posta elettronica certificata attualmente in uso si basano sulla presenza di un intermediario, una terza parte fidata anche detta TTP (*trusted third party*), emulando il processo della "lettera raccomandata con ricevuta di ritorno" della posta cartacea tradizionale.

I TTP semplificano le operazioni che deve effettuare un utente che vuole inviare una email certificata e si occupano di produrre le prove di spedizione e ricezione, ma non si può avere garanzia assoluta che un TTP sia realmente affidabile. Infatti possono causare problemi a livello tecnico (ad esempio, possono causare colli di bottiglia, *bottlenecks*, dal punto di vista delle comunicazioni), mancanza di efficienza nei protocolli (ad esempio, rallentare la risoluzione dei problemi) e aumentare il costo dell'esecuzione dei servizi (ad esempio, addebitare tariffe elevate). Inoltre, sono un punto molto sensibile della rete, poiché svolgono un ruolo importante nella sicurezza dei protocolli elettronici e la loro affidabilità è un problema che richiede attenzione, poiché la sicurezza dello scambio può essere infranta se il TTP presenta una qualsiasi vulnerabilità.

Il lavoro è strutturato in quattro sezioni: alla sezione 2 si potranno leggere le definizioni di alcuni dei termini utilizzati, alla sezione 3, dopo aver dato una definizione più accurata di messaggio elettronico certificato, vengono analizzati i diversi protocolli proposti negli anni. Alla sezione 4 viene studiata la normativa e il modello di funzionamento del servizio più diffuso di per lo scambio di email certificate, l'italiana PEC. Alla sezione 5 viene proposto un modello di architettura per scambio di messaggi elettronici certificati che non prevede l'utilizzo di intermediari, i TTP.

2 Definizioni

Email: mail elettronica, messaggio elettronico scambiato su qualsiasi protocollo appropriato (non necessariamente SMPT)

TTP (*trused third party*, terza parte fidata): è un'entità che facilita le interazioni tra due parti che si fidano entrambe della terza parte, quest'ultima esamina tutte le comunicazioni critiche delle transazioni tra le parti, in base alla facilità di creare contenuti digitali fraudolenti.
Il regolamento europeo 910/2014 anche conosciuto come eIDAS definisce i TTP come:
«prestatore di servizi fiduciari», una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato

Scambio equo (*fair exchange*): uno scambio che alla fine garantisce che tutte le parti coinvolte ottengano ciò che si aspettano o che nessuna delle due ottenga niente.

Electronic Registered Delivery Service (abbreviato in eDelivery): servizio elettronico di recapito certificato. Il Regolamento UE n. 910/2014 eIDAS lo definisce come: un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate.

Blockchain: è una struttura dati composta da un elenco crescente di record, denominati "blocchi", collegati tra loro in modo sicuro utilizzando la crittografia. Ogni blocco contiene dati di transazioni, un timestamp e un hash crittografico riferito al blocco precedente.
Quest'ultimo permette di creare un collegamento effettivo tra i vari record, rendendo inoltre impossibile una modifica retroattiva dei dati salvati, in quanto si dovrebbero poi modificare anche tutti i blocchi prodotti successivamente.
La blockchain rientra nella più ampia famiglia dei registri distribuiti (*distributed ledger*), ossia sistemi che si basano su un registro replicato, condiviso e sincronizzato tra più

soggetti, detti nodi, presenti in molteplici luoghi, ma comunque appartenenti alla stessa entità.
Nelle blockchain è garantita la coerenza tra le copie dei *ledger* e l'aggiunta di un nuovo blocco è globalmente regolata da un protocollo chiamato "consenso".
Una volta autorizzata l'aggiunta del nuovo blocco, ogni nodo aggiorna la propria copia privata del *ledger* e informa gli altri nodi della modifica. La natura stessa della blockchain garantisce l'assenza di una sua manipolazione futura.

Transazione in una blockchain
In generale, una transazione si riferisce ad un contratto, accordo, trasferimento o scambio di risorse (asset), tra due o più parti. Solitamente si tratta di denaro o proprietà. In modo simile, una transazione in blockchain è una trasmissione di dati attraverso il network di computer che partecipano ad una blockchain. I computer salvano i dati della transazione nel registro distribuito (della blockchain in questione).

Smart contract: sono protocolli informatici che facilitano, verificano, o fanno rispettare, la negoziazione o l'esecuzione di un contratto. In una blockchain è uno script integrato che automaticamente esegue, controlla e documenta gli eventi e le azioni secondo le regole del contratto stesso.
Lo smart contract possiede un indirizzo unico e lo si invoca eseguendo una transazione verso di esso.

Metodo di consenso: è un metodo utilizzato per raggiungere l'accordo, la fiducia e la sicurezza in una rete di computer decentralizzata. Ne esistono diversi, tra i più famosi il PoW (*Proof of Work*) e il PoS (*Proof of Stake*).

Merkle Tree: è un albero binario completo nel quale ogni foglia ha come etichetta l'hash crittografico di un blocco di dati e ogni nodo che non è foglia è etichettato con l'hash crittografico delle etichette dei figli.

Hash: è il risultato di una hash function, che è una operazione crittografica che viene utilizzata per mappare dati di dimensioni arbitrarie in valori di dimensioni fisse.

Ledger: è un registro digitale o fisico che riporta informazioni. In un sistema finanziario, ad esempio, queste possono essere transazioni.
Le blockchain sono un tipo di sistema di registro decentralizzato progettato per archiviare i dati in modo sicuro.

3 Che cos’è un messaggio elettronico certificato?

Si può analizzare il funzionamento di un messaggio elettronico certificato per analogia con quello sotteso alla raccomandata con avviso di ricevimento.
Quando viene inviata una raccomandata a/r il servizio di poste:

1. Rilascia una ricevuta al mittente quando prende in consegna la lettera;
2. Consegna il messaggio quando viene firmata la ricevuta dal destinatario o da una persona per suo conto.

Quando viene invece inviato un messaggio elettronico certificato, il gestore del servizio:

1. Genera una ricevuta di accettazione quando il mittente invia il messaggio;
2. Genera una ricevuta di consegna quando il messaggio è pervenuto all’indirizzo elettronico indicato dal mittente;

In entrambi i casi (consegna della raccomandata a/r o del messaggio elettronico certificato) l’operazione viene considerata compiuta correttamente, indipendentemente dall’avvenuta presa visione del messaggio, fisico o elettronico, da parte del soggetto destinatario.

La versione elettronica della raccomandata con avviso di ricevimento garantisce l’equità dello scambio senza la presenza di un intermediario fisico coincidente con il postino per la raccomandata a/r.

In tale contesto la letteratura scientifica [1] [2] [3] [4] [5] [6] [7] [8], definisce le mail elettroniche certificate nell’ambito degli scambi equi (*fair exchange*).

Le mail elettroniche certificate diventano dunque parte di uno scambio equo, il quale prevede che venga non solo trasferito un messaggio, ma che vengano anche prodotte delle prove di origine e ricezione dello stesso. Le prove possono essere trasferite contestualmente al messaggio oppure gestite su un diverso canale.

3.1 Requisiti di sicurezza di un protocollo di scambio di email certificato

Nel 2014 Draper-Gil *et al.* pubblicano un lavoro [8] nel quale si occupano anche di raccogliere e riassumere tutti i requisiti che deve avere un protocollo di scambio di email certificate.
Considerato il riconoscimento dato al suddetto lavoro dalla comunità internazionale, si riportano di seguito i 7 requisiti di sicurezza teorici che un protocollo dovrebbe avere (non è detto che i protocolli reali li implementino tutti):

1) Efficacia (*effectivness*): se entrambe le parti si comportano correttamente, il destinatario è in grado di ricevere il messaggio, e il mittente è in grado di provarlo, senza l'intermediazione del TTP;

2) Equità (*fairness*): avvenuto l'invio e la ricezione di un messaggio certificato, ogni parte che si è comportata onestamente riceve ciò che si aspetta. In particolare il destinatario onesto avrà modo di ottenere un messaggio leggibile e una prova della sua origine, laddove il mittente onesto avrà le prove di aver inviato il messaggio e che il destinatario l'ha ricevuto. Se una delle due parti dovesse comportarsi disonestamente, l'altra non sarebbe né avvantaggiata né penalizzata, in quanto nessuna parte riceverebbe le prove che garantiscono che lo scambio è avvenuto;

3) Tempestività (*timeliness*): ogni parte coinvolta nello scambio di messaggi certificati sarà garantita che questo terminerà in un tempo finito e, una volta concluso, il principio di equità verrà mantenuto per le parti che si sono comportate onestamente;

4) Verificabilità del TTP (*verifiability of TTP*): se il TTP si comporta male, causando una possibile perdita di equità per un partecipante onesto, quest'ultimo può dimostrare il comportamento scorretto del TTP;

5) Ricezione non selettiva (*Non-selective reception*): una volta che il destinatario sa di aver ricevuto un messaggio certificato, non può impedirne la consegna;

6) Non ripudio (*Non-Repudiation*): nell'invio di un messaggio certificato che comprende un mittente, un intermediario del mittente, un intermediario del destinatario e un destinatario, nessuno può negare di essere coinvolto o può essere escluso dalla partecipazione allo scambio. In particolare, si definiscono i seguenti servizi di non ripudio:

    - Origine (*origin*) (NRO), il mittente non può negare di aver creato il messaggio certificato;
    - Invio (*submission*) (NRS), il mittente può provare di aver inviato il messaggio certificato al proprio intermediario;
    - Spedizione (*delivery*) (NRD), l'intermediario del destinatario non può negare di aver ricevuto il messaggio certificato;
    - Ricezione (*receipt*) (NRR), il destinatario non può negare di aver ricevuto il messaggio certificato;

7) Confidenzialità (*confidentiality*): il contenuto di un messaggio certificato può essere letto solamente dal mittente e dal destinatario.

3.2 Breve review della letteratura dei protocolli proposti ed esistenti

La modalità di trasmissione di messaggi elettronici certificati è un caso di studio ben noto nella comunità internazionale ed è dal 1980 che vengono pubblicati lavori riguardanti questa tematica.
Cercando di creare un panorama più vasto possibile, nelle prossime sottosezioni verranno elencati i protocolli con e senza l'intermediazione di TTP.

3.2.1 Protocolli con TTP

Per raggiungere l'equità fra le parti, molti dei protocolli proposti fino al giorno d'oggi prevedono che le operazioni di scambio avvengano mediante TTP, i quali sono anche

responsabili di risolvere eventuali problemi che potrebbero sorgere dall'interruzione, malevola o accidentale, dello scambio.

I TTP si possono classificare in 3 categorie:

- *Inline*: agiscono come proxy tra il mittente e il destinatario, essendo coinvolti in ogni fase del protocollo;

- *Online*: sono coinvolti in ogni esecuzione del protocollo, ma non in ogni fase;

- Approccio ottimistico: sono coinvolti solo in caso di controversia, che dovrebbe essere un caso eccezionale.

Dato che la comunicazione via email è una comunicazione asincrona, spesso si deve ricorrere a TTP *inline* per gestire le numerose iterazioni necessarie per eseguire gli scambi di email tra gli utenti. Come riportano Draper-Gil *et al.* [8] nel loro lavoro, molti approcci per lo scambio di email certificate adottano il modello dei *Mail Transfer Agents* (MTA) semi-fiduciari, che agiscono come proxy tra il mittente e il destinatario per garantire equità. Fino al 2014, anno di pubblicazione del lavoro, la maggior parte dei protocolli proposti utilizza un solo MTA. Anche se questi protocolli sono pratici e possono essere distribuiti su Internet, non riflettono pienamente l'architettura decentralizzata della posta elettronica su Internet, perché in questi protocolli i mittenti e i destinatari devono essere registrati presso lo stesso MTA.

Tauber propone nel 2011 [9] un lavoro nel quale analizza lo sfondo legale, le scelte di architettura, i protocolli e altre specifiche di 5 servizi di trasmissione email certificate al tempo utilizzati nel mondo. In particolare vengono analizzati i seguenti servizi: DDS (Austria), PEC (Italia), De-Mail (Germania), Moja.posta.si (Slovenia), ERV (Austria).
Successivamente all'analisi dei servizi appena citati, vengono brevemente descritti altri servizi esistenti e alla fine analizzati alcuni protocolli non ancora implementati.

Draper-Gil *et al.* [8] pubblicano nel 2014 un lavoro nel quale propongono un protocollo ottimistico per email certificate. In questo modello, sia il mittente che il destinatario possono scegliere il loro MTA, evitando TTP *inline* e non verificabili, e fornendo tutte le prove richieste per quanto riguarda l'invio e la ricezione di posta elettronica certificata.

Ferrer-Gomila *et al.* nel 2018 pubblicano un lavoro [10] nel quale propongono un protocollo ottimistico per email certificate con TTP verificabili, nel quale il comportamento di questi ultimi è verificabile e soddisfa i requisiti di sicurezza più comuni riscontrati nelle proposte di posta elettronica certificata ottimistica: efficacia, correttezza, tempestività, riservatezza, non ripudio dell'origine e non ripudio della ricezione.
Gli autori, inoltre, si occupano anche di raccogliere e spiegare brevemente il contenuto di 124 paper sulla posta elettronica certificata e i vari protocolli alla sezione 3, a cui si rimanda per ulteriori approfondimenti

3.2.2 Protocolli senza TTP

Negli anni sono stati sviluppati protocolli che non prevedono l'intermediazione dei TTP, si vedano per esempio [11] [12] [9]. Questi ultimi si basano tutti su un rilascio graduale di informazioni tra le parti coinvolte e un assiduo scambio di messaggi per cercare di approssimare il protocollo ad uno scambio equo.

Anche se i TTP sono ancora una parte fondamentale nei protocolli di scambio equo, con l'avvento degli smart contract e della blockchain si sono potute proporre più possibilità di soluzioni che riducono o non prevedono la loro intermediazione.

In particolare, gli smart contract diminuiscono il bisogno di intermediari fidati o di sistemi di ripudio. Questa nuova tecnologia permette di definire transazioni con regole scritte in un contratto immutabile, in modo che possano avvenire scambi equi tra parti che non si fidano tra loro. Data la dissuasione dal cercare l'imbroglio e il calo del bisogno di intermediari, i servizi dei TTP potrebbero costare meno e ci potrebbe essere anche meno ritardo nelle comunicazioni.

La blockchain, invece, poiché per sua definizione è una catena di blocchi che contengono informazioni, permette di immagazzinare dati al suo interno e di renderli immutabili. Una sua applicazione nell'ambito delle email certificate permetterebbe di limitare il ricorso a TTP, in quanto ci sarebbe meno bisogno di intermediari di trust nella gestione dei dati perché questi sarebbero disponibili e verificabili da tutti direttamente dalla blockchain.
Inoltre, la blockchain incorpora naturalmente una nozione di ordinamento temporale, comportandosi come un orologio che aumenta ogni volta che viene aggiunto un nuovo

blocco. L'esistenza di un orologio/registro affidabile è fondamentale per ottenere la proprietà di equità nei protocolli.

Si rimanda alla sezione 3 intitolata "*State of the Art of Registered eDelivery Services*" del lavoro di Payeras-Capellà *et al.* [13] del 2019 nel quale, oltre a proporre due protocolli per la trasmissione certificata di messaggi elettronici basati su blockchain, è riassunto lo stato dell'arte fino a quell'anno.

Inoltre dal 2019 al 2022 altri protocolli sono stati proposti [14] [15] [16], che prevedono l'utilizzo di transazioni con criptovalute (Bitcoin) o l'utilizzo di smart contract per la trasmissione dei dati e la loro certificazione.

4 La Posta Elettronica Certificata e le sue evoluzioni

La principale implementazione nel mondo di scambio di posta elettronica certificata è il servizio italiano PEC (Posta Elettronica Certificata).

Attivo dal 2005, esso permette ai cittadini italiani possessori di una casella di posta PEC di scambiarsi messaggi con la garanzia di spedizione e di ricezione, come avviene per una raccomandata cartacea con avviso di ricevimento.

4.1 Riferimenti normativi italiani ed europei

In questo capitolo viene presentata l'insieme di norme sullo scambio di messaggi elettronici certificati presenti dell'ordinamento italiano ed europeo e infine, alla sezione 4.2 vengono riassunti i requisiti necessari ad un servizio di scambio di email per poter essere ritenuto a norma di legge.

4.1.1 La nascita di PEC

La posta elettronica certificata (PEC) è stata introdotta in Italia con la legge del 16 gennaio 2003, n. 3 che all'art. 27 comma 8 demanda ad un apposito regolamento l'estensione dell'uso della posta elettronica nell'ambito delle pubbliche amministrazioni e dei rapporti tra Pubblica Amministrazione e privati.

l DPR 11 febbraio 2005 n. 68, stabilisce le regole per l'utilizzo della PEC e le specifiche che il sistema deve avere.

Il Decreto Legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale - CAD) introduce all'art. 6 la possibilità da parte della Pubblica Amministrazione di utilizzare la PEC per ogni scambio di documenti e informazioni con i soggetti che ne hanno fatto richiesta e che hanno dichiarato il proprio indirizzo di posta elettronica certificata. L'art 47 del CAD stabilisce che la comunicazione di documenti tra le pubbliche amministrazioni avvenuta tramite posta elettronica certificata sia valida ai fini del procedimento amministrativo, mentre l'art 48 del CAD prescrive che la trasmissione telematica di

comunicazioni, che necessita di una ricevuta di invio e di una ricevuta di consegna, sia svolta mediante la posta elettronica certificata.

Il Decreto Legge 29 novembre 2008, n.185 (convertito con modificazioni dalla legge 28 gennaio 2009, n.2) introduce con l'art. 16 l'obbligo da parte delle imprese e dei professionisti di creare un indirizzo di PEC e di comunicarlo al Registro delle Imprese e agli Ordini o Collegi di appartenenza.

La Legge 18 giugno del 2009 n.69, all'art. 45 modifica l'art. 137 del Codice di Procedura Civile, stabilendo che se l'atto da notificare è un documento informatico diventa obbligatorio notificarlo mediante PEC al destinatario che ne è possessore. Ne deriva che vi è un onere in capo al possessore di PEC di farsi parte diligente nella frequente consultazione della propria casella, dato che non potrà opporre la non conoscenza di un atto sulla base della mancata apertura dei messaggi ricevuti con PEC.

Il Decreto Legge 18 ottobre 2012, n.179 (convertito con modificazioni dalla legge 17 dicembre 2012, n.221) con l'art. 5, commi 1 e 2 introduce l'obbligo di creare un indirizzo di PEC anche per le imprese individuali, da comunicare al Registro delle Imprese entro il 30 giugno 2013.

Il suddetto decreto aggiorna il CAD, istituendo all'art. 6 bis l'Indice nazionale degli indirizzi di posta elettronica certificata (INI-PEC) delle imprese e dei professionisti presso il Ministero per lo sviluppo economico.

4.1.2 Da PEC a REM

Il Regolamento UE n. 910/2014 eIDAS (electronic IDentification Authentication and Signature) fornisce una base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri e introduce il concetto di Qualified Electronic Registered Delivery Service (QERDS). Esso è stato emanato il 23 luglio 2014 e ha piena efficacia dal 1° luglio del 2016.

Il Decreto Legislativo 26 agosto 2016, n. 179 modifica ed integra il CAD recependo le disposizioni contenute del Regolamento eIDAS.

Il Decreto Legislativo 13 dicembre 2017, n. 217, modifica il CAD prevedendo l'introduzione del domicilio digitale che, sulla base di quanto definito nell'art. 1 comma 1 lettera n-ter e comma 1-ter, può essere un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato

Lo stesso Decreto Legislativo, con l'art.65 abroga l'art. 48 del CAD a decorrere dal 1° gennaio 2019, stabilendo che la PEC è uno strumento tecnologico mediante il quale è possibile eleggere il domicilio digitale.

La nuova PEC europea ha iniziato il suo iter a gennaio 2022 e nel corso dello stesso anno è stato rilasciato lo standard ETSI (European Telecommunications Standards Institute), fondamentale per la realizzazione di un servizio di posta elettronica conforme al Regolamento europeo n. 910/2014 – eIDAS. In Italia, dal 2024, la PEC lascerà quindi il posto alla Registered Electronic Mail (REM), la PEC europea.

Il 3 giugno 2021 è stata presentata la proposta di Regolamento del Parlamento e del Consiglio che modifica il regolamento UE eIDAS, c.d eIDAS 2.0, di cui si è conclusa la discussione e si attende la formalizzazione.

4.2 Requisiti di un servizio di trasmissione di messaggi elettronici certificati in Unione Europea

L'art. 44 del Regolamento UE eIDAS, individua puntualmente i requisiti necessari ai fini della individuazione di servizi elettronici di recapito certificato qualificati (QERDS), come sotto riportati.

"

I QERDS:

a) sono forniti da uno o più prestatori di servizi fiduciari qualificati;

b) garantiscono con un elevato livello di sicurezza l'identificazione del mittente;

c) garantiscono l'identificazione del destinatario prima della trasmissione dei dati;

d) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da

escludere la possibilità di modifiche non rilevabili dei dati;

e)qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;

f)la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata.

Qualora i dati siano trasferiti fra due o più prestatori di servizi fiduciari qualificati, i requisiti di cui alle lettere da a) a f) si applicano a tutti i prestatori di servizi fiduciari qualificati.

"

Le linee guida di European Union agency for cybersecurity (Enisa), pubblicate nel documento "Security guidelines on the appropriate use of qualified electronic registered delivery services" nel 2017, e le "Regole tecniche per i servizi di recapito certificato a norma del regolamento eIDAS n. 910/2014" prodotte da AgID nel 2022, elencano i requisiti che per legge sono richiesti ad un servizio di trasmissione di messaggi elettronici certificati qualificato.

Essi sono di seguito illustrati distinguendoli in 4 categorie (sottosezioni 4.2.1, 4.2.2, 4.2.3 e 4.2.4), in conformità a quanto indicato nelle linee guida di Enisa e nel regolamento di AgID sopra citati.

4.2.1 Proprietà legali

- Ricevuta di consegna: Il mittente riceve una prova contenente data ed ora del momento in cui ha inviato un messaggio ad un destinatario, indipendentemente dalla capacità di quest'ultimo di riceverlo

- Ricevuta di ricezione: Sia il mittente che il destinatario ricevono una prova contenente la data e l'ora del momento in cui il destinatario ha ricevuto o aperto un'email.

- Ricevuta d’integrità: Sia il mittente che il destinatario devono avere la garanzia che il messaggio non venga alterato durante la trasmissione

- Protezione contro il rischio di perdita, furto, danno o alterazioni non autorizzate

4.2.2 Proprietà di sicurezza

- Identificazione del mittente: Il destinatario deve essere certo sull’identità del mittente

- Certezza temporale: tutti i messaggi devono contenere un’indicazione temporale proveniente da una fonte qualificata. Questa indicazione temporale fornisce la presunzione legale dell'accuratezza della data e dell'ora della consegna

- Confidenzialità: Il messaggio non può essere letto da nessuno se non da mittente e destinatario. Vuol dire che il messaggio è criptato con metodo di cifratura end-to-end

- Integrità dei dati

- Controllo degli errori di instradamento (errori di *routing*): questo controllo aiuta l'utente a verificare diversi parametri del destinatario prima della trasmissione e lo informa sulla capacità del ricevitore di accettare il messaggio prima della trasmissione

- Interoperabilità: Un servizio indica al mittente tutti i formati dei messaggi che il destinatario può elaborare e trasformare da un formato all'altro.

4.2.3 Proprietà funzionali

- Invio di file di grandi dimensioni: Il servizio deve permettere l'invio di file di tutte le dimensioni e formati

- Processamento istantaneo: Il servizio deve essere quasi istantaneo

4.2.4 Altre proprietà

- Rischi ridotti: la consegna elettronica registrata qualificata rende impossibile la manipolazione dei dati, la falsificazione delle indicazioni temporali di invio e ricezione o l'accesso non autorizzato al messaggio

- Costi ridotti

- Nessun doppio invio: evita l'invio di un'ulteriore versione firmata, in formato cartaceo, dei dati elettronici

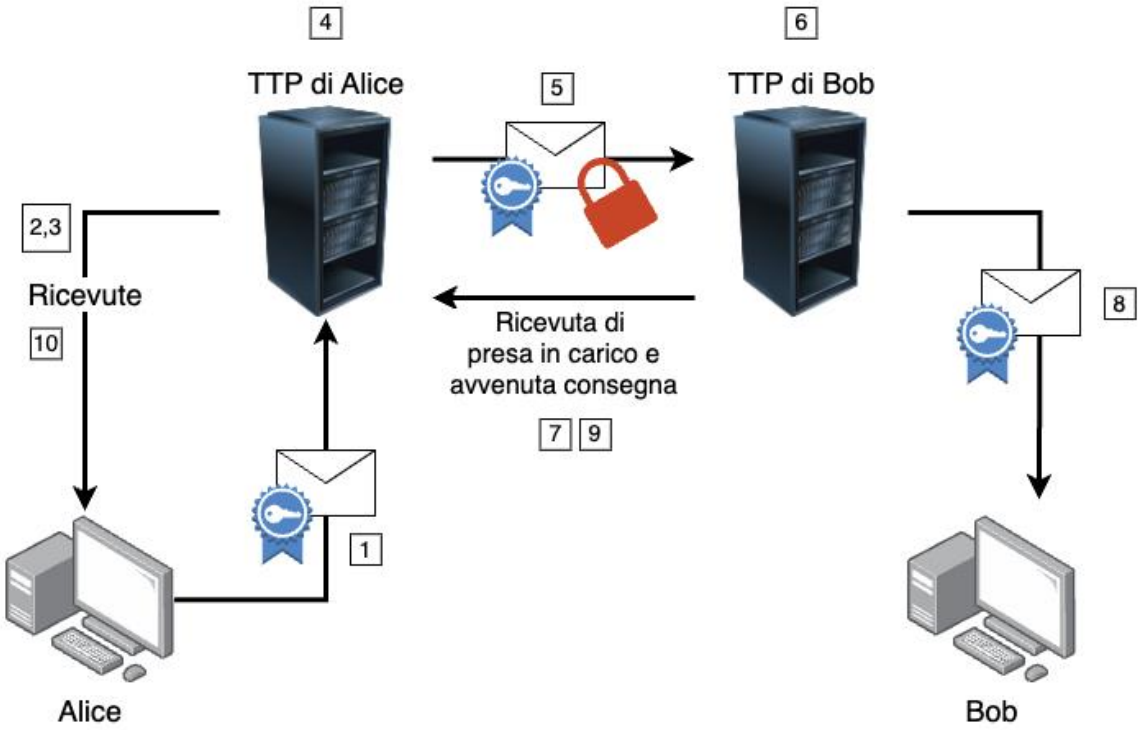
- Gestione degli incidenti e responsabilità: il fornitore di servizi rimane responsabile dei danni causati al cliente per negligenza o omissione.

4.3 Il modello di funzionamento della PEC

Il servizio, reso possibile dalla presenza di due intermediari, uno per il mittente e uno per il destinatario, prevede che un messaggio, per essere ritenuto ricevuto dal destinatario, segua questi passi:

1. Il mittente invia il messaggio al destinatario con server SMTP autenticato via SSL;
2. Il gestore provvede a inviare al mittente una notifica di accettazione/non accettazione del messaggio;
3. La ricevuta riporta data e ora di invio, oggetto, indirizzo di posta del mittente e del destinatario;

4. Il messaggio viene “imbustato” in un nuovo messaggio (busta di trasporto).
   Per busta di trasporto si intende il messaggio creato dal punto di accesso, all’interno del quale sono inseriti il messaggio originale inviato dall’utente di posta elettronica certificata ed i relativi dati di certificazione;
5. La busta di trasporto è firmata con la chiave del gestore di posta elettronica certificata mittente e inviata al destinatario;
6. Il gestore ricevente effettua un controllo sulla firma del gestore mittente e sulla validità;
7. Il gestore ricevente, in caso di verifica positiva, provvede a inviare una ricevuta di presa in carico al mittente passando attraverso il gestore del mittente;
8. Il gestore ricevente rende disponibile il messaggio nella casella del destinatario;
9. Il gestore ricevente invia al gestore mittente una ricevuta di avvenuta consegna;
10. Il mittente riceve nella sua mailbox la ricevuta di avvenuta consegna.



Rispetto al 2005, anno di lancio di PEC, il servizio si è evoluto per garantirne l’aggiornamento con la normativa italiana ed europea in materia di privacy e sicurezza dei dati.

A partire dal 2024 sarà possibile per tutti i cittadini europei utilizzare il servizio REM (Registered Electronic Mail), chiamata anche PEC europea.

4.4 Statistiche di utilizzo PEC

L'Agenzia per l'Italia Digitale (AgID) rilascia ogni anno le statistiche di utilizzo della PEC, in cui viene evidenziato il numero di caselle postali e il numero di messaggi scambiati per bimestre in Italia.

Dai dati analizzati si osserva che ogni anno aumenta l'utilizzo delle PEC, arrivando a registrare a dicembre 2022 un numero di caselle postali attive pari a 14.663.677 che portano ad uno scambio annuale di quasi 2.700.000.000 di messaggi.

5 Proposta di modello di scambio di email certificate senza Terze Parti Fidate (TTP)

In questo capitolo viene presentato un modello originale di architettura per lo scambio di messaggi certificati che non prevede l'uso di TTP. La descrizione del modello si trova nel paragrafo 5.2. Nel paragrafo 5.1 si descrivono principali tecnologie utilizzate per la realizzazione del medesimo. Nei paragrafi successivi si analizza come il modello copra i requisiti generali dell'eDelivery (5.3) e quelli specifici di eIDAS (5.4)

5.1 Gli strumenti

5.1.1 Proof of History (PoH)

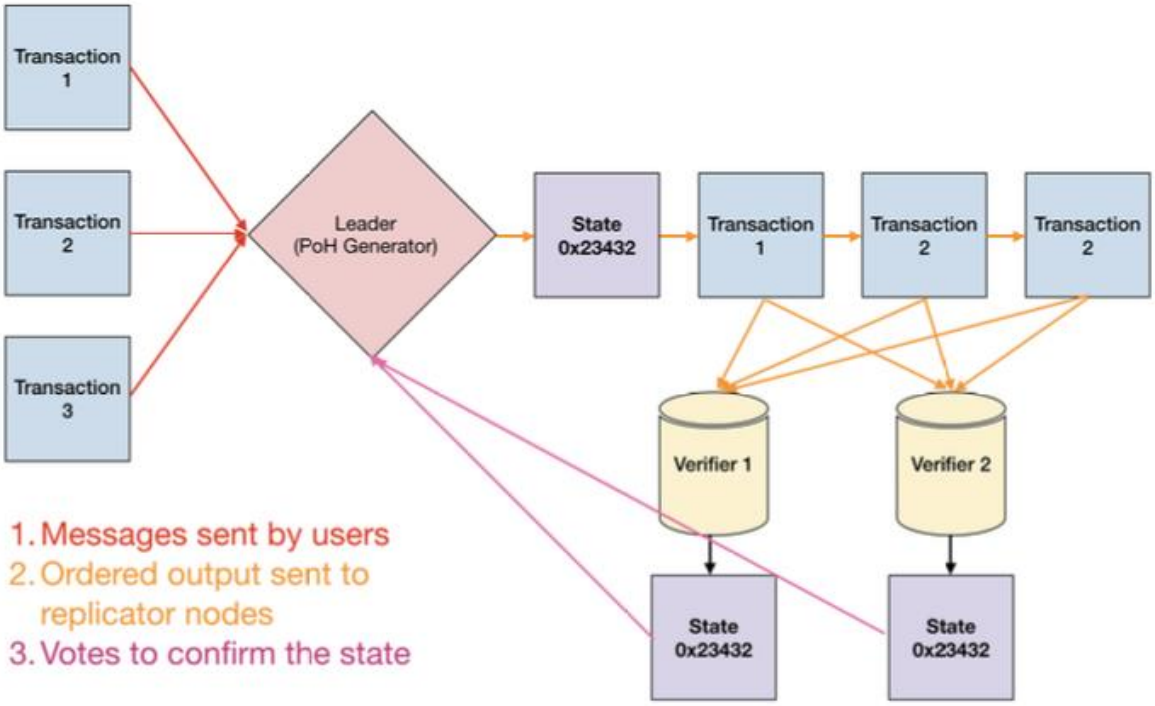
Il Proof of History (PoH) è una sequenza di calcolo che può fornire un modo per verificare crittograficamente il passaggio del tempo tra due eventi. Esso è stato progettato da Anatoly Yakovenko e pubblicato nel white paper intitolato "Solana: Una nuova architettura per una blockchain ad alte prestazioni v0.8.14" da cui vengono tratte tutte le immagini riportate in questa sottosezione.

Viene utilizzato per codificare il passaggio del tempo in modo affidabile in un ledger, una struttura dati *append-only*, nella quale i dati inseriti non possono più essere modificati.

Se il PoH è associato ad un algoritmo di consenso come il Proof of Stake (PoS), il Proof of Work (PoW) o il Proof of Authority (PoA), può ridurre l'overhead della messaggistica tra i nodi di una blockchain, permettendo di eseguire transazioni in tempi molto brevi.

Ogni nodo di una blockchain che implementa il PoH è in grado di fare affidamento sullo scorrere del tempo registrato nel ledger senza eventualmente fidarsi degli altri nodi.

In un sistema che implementa PoH è prevista una struttura del network come illustrato nell'immagine sotto riportata.



Il Leader, un nodo della rete scelto in modo pseudo randomico, ordina le transazioni che arrivano dagli utenti della blockchain in modo che queste possano essere processate efficientemente ed inviate insieme al valore dello stato finale ai *verifiers* (nodi dediti alla verifica e propagazione).
I *verifiers* eseguono le stesse operazioni già compiute dal Leader sulle loro copie dello stato della blockchain.
Il nuovo stato della blockchain viene propagato ed accettato da tutti i nodi quando viene appurato che i valori dello stato finale dei *verifiers* sono identici a quella del Leader.

Il PoH utilizza una funzione crittografica deterministica resistente alle collisioni (ad esempio: sha256, ripemd …) che viene eseguita in sequenza su un singolo *core*. Alla prima esecuzione della funzione si utilizza come input un valore a scelta, ma, a partire dalla seconda, il valore in ingresso è l'output della funzione eseguita precedentemente.
Dato che la funzione è deterministica, ossia restituisce sempre lo stesso risultato per un dato valore in ingresso, e che l'input all'esecuzione *n* è uguale all'output all'esecuzione *n-1*, si può dire che l'output *n* sia legato all'output *n-1*. Data questa correlazione, non serve salvare tutti i risultati di ogni esecuzione per verificare che la funzione venga eseguita correttamente, ma se ne possono prendere solamente alcuni a campione. Si può quindi

creare una tabella nella quale, indicando il numero di volte che è stata eseguita la funzione (index, indice), qual è l'operazione eseguita (Operation) e il suo output (Output Hash), si può verificare la correttezza della sequenza.

PoH Sequence

Index	Operation	Output Hash
1	sha256("any random starting value")	`hash1`
200	sha256(`hash199`)	`hash200`
300	sha256(`hash299`)	`hash300`

La sequenza di hash prodotta dal PoH può anche essere usata per congelare dei dati (in tabella rappresentati da photograph1_sha256 e photograph2_sha256). Un modo per eseguire questa operazione potrebbe semplicemente essere quello di aggiungere all'hash prodotto all'esecuzione *n* le informazioni arrivate (*append*), in modo da cambiare l'output della funzione all'esecuzione *n+1*.

L'hash generato da questa operazione rappresenterebbe il timestamp dei dati come sotto esemplificato.

POH Sequence

Index	Operation	Output Hash
1	sha256("any random starting value")	`hash1`
200	sha256(hash199)	`hash200`
300	sha256(hash299)	`hash300`
336	sha256(append(hash335, photograph1_sha256))	`hash336`
400	sha256(hash399)	`hash400`
500	sha256(hash499)	`hash500`
600	sha256(append(hash599, photograph2_sha256))	`hash600`
700	sha256(hash699)	`hash700`

La sequenza può essere verificata da un computer *multicore* in molto meno tempo rispetto a quello impiegato per crearla, infatti si possono controllare diversi segmenti nello stesso momento e poi confrontare l'hash finale di una sequenza con quello iniziale di un'altra per vedere se combaciano.

Inoltre, per prevenire un errato ordinamento temporale degli eventi, questi ultimi dovrebbero contenere l'hash dell'ultima sequenza ritenuta valida.

PoH Sequence A

Index	Data	Output Hash
10		`hash10a`
20	Event1 = append(event1 data, `hash10a`)	`hash20a`
30	Event2 = append(event2 data, `hash20a`)	`hash30a`
40	Event3 = append(event3 data, `hash30a`)	`hash40a`

Per essere sicuri che ogni nodo esegua la funzione di hash impiegando lo stesso tempo rispetto agli altri è necessario che ci sia un accordo sulla tipologia di hardware da usare.

L'esecuzione del PoH "a vuoto", quindi senza l'inserimento di dati, permette a nodi con un processore con la stessa architettura di avere un concetto di tempo condiviso e sincronizzato, che non necessita di una continua comunicazione tra di essi. In questo modo si ottimizza sia la verifica dei blocchi che i cambi dei turni di Leader e dei *verifiers*.

5.1.2 Proof of Authority (PoA)

Il Proof of Authority [17] [18] è un metodo di consenso che permette ad alcuni membri identificati della blockchain, chiamati *validator*, di validare transazioni o iterazioni con il network e di aggiornate il *ledger* associato alla blockchain medesima.

I validator eseguono un programma che permette loro di inserire transazioni nei blocchi con un processo automatico che non richiede il monitoraggio costante della rete.

Individui o aziende ottengono il diritto di diventare *validator* fornendo prove della loro identità. In tal modo si mira a prevenire un comportamento disonesto da parte dei medesimi, che, in caso contrario, vedrebbero rovinata la loro reputazione nel network.

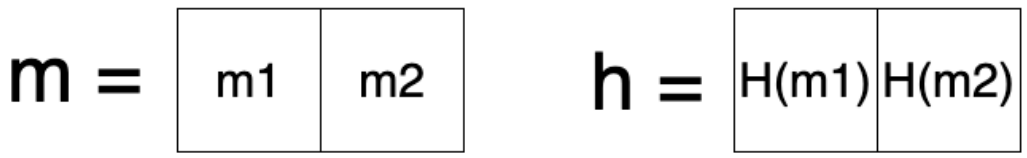
I *validator* sono scelti randomicamente all'interno di un insieme di candidati selezionati sulla base della loro reputazione, mediante votazione da parte di nodi precedentemente autorizzati alla validazione dei blocchi. Ogni *validator* può firmare al massimo uno di una serie di blocchi consecutivi durante il proprio turno di convalida. La varietà dei *validator* e la loro buona reputazione evitano che nodi disonesti possano influenzare la blockchain.

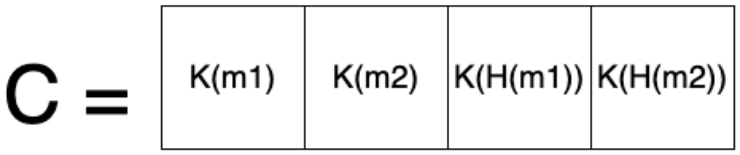
Uno dei punti più criticati di PoA, è che il suo modello rinuncia allo schema di decentralizzazione e distribuzione. In effetti, il protocollo è destinato a un sistema nell'ambito del quale poche persone partecipano alla rete, il che lo rende perfetto per le blockchain private in cui si cerca un alto livello di sicurezza e scalabilità.

5.1.3 Protocollo di scambio di messaggi elettronici certificate basato su blockchain e smart contract

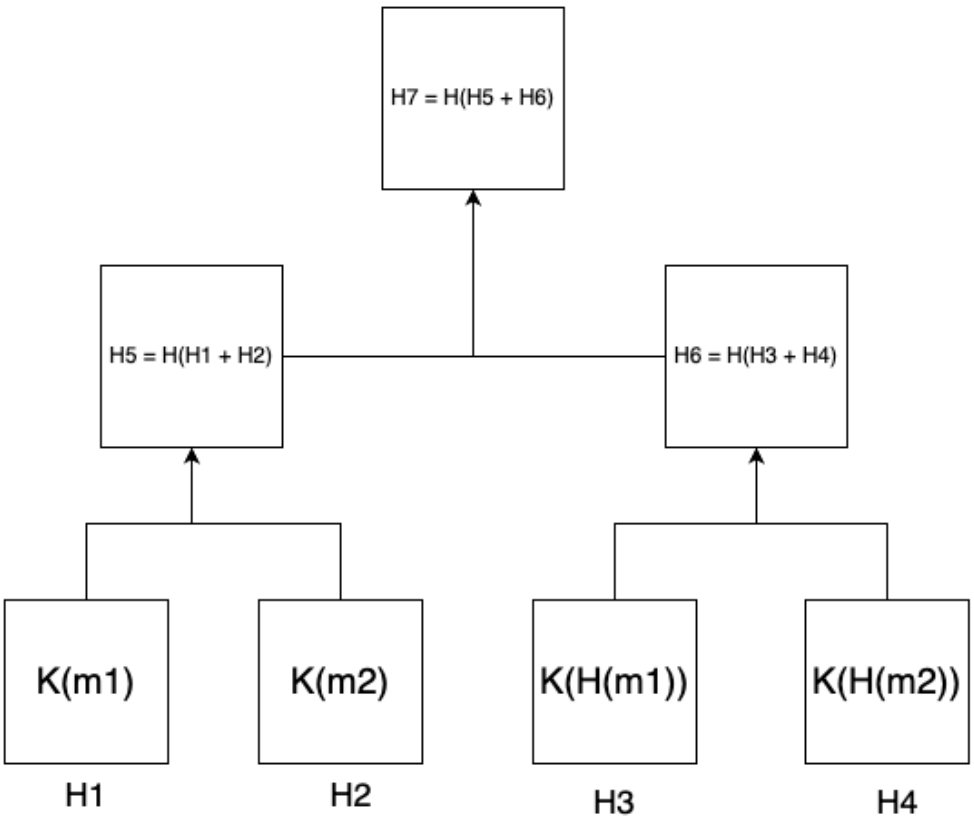
K. Elmaghraby e T. Dimitriou pubblicano nel 2021 un lavoro [14] nel quale propongono un protocollo di scambio di messaggi elettronici certificati basato sulla blockchain Ethereum e smart contract che si comporta come intermediario tra le parti e risolve i conflitti affinché ci sia uno scambio equo.

Nell'ambito del protocollo proposto, il mittente separa il messaggio *m* in *n* blocchi di dimensione predefinita e calcola l'hash h di ogni blocco. In questo modo viene creata una struttura dati C composta dai blocchi non criptati del messaggio originale ai quali si accodano i blocchi con l'hash. Successivamente il mittente genera una chiave simmetrica K e, con questa, cripta ogni blocco di C, come di seguito esemplificato.





Poi il mittente calcola il Merkle Tree di C.



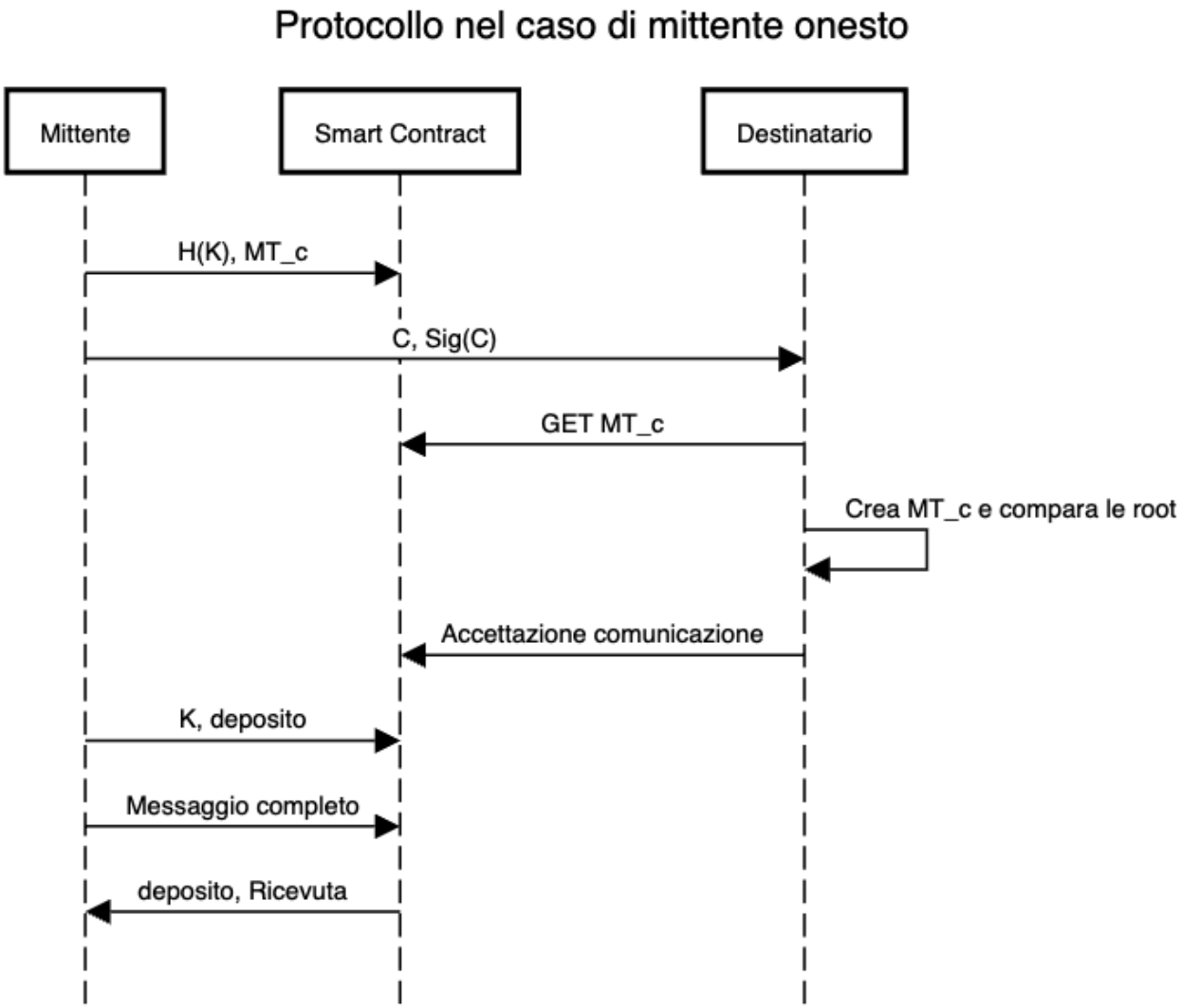
A questo punto il mittente manda al destinatario C firmato (C, Sig(C)) offchain e manda l'hash di K, H(K), e la root del Merkle Tree MT_c allo smart contract.

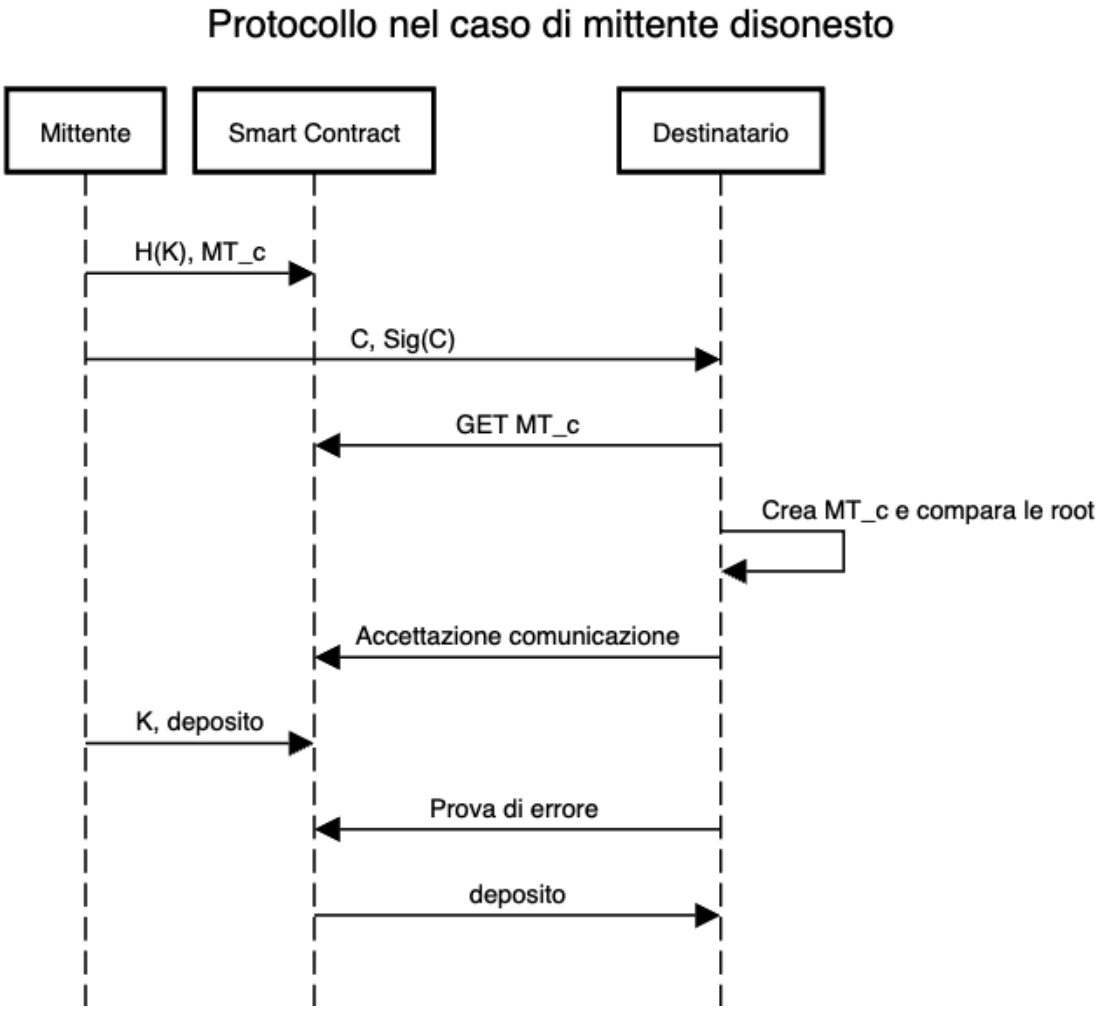
Il destinatario crea il Merkle tree di C mandato dal mittente e compara la root con quella presente nello smart contract. Se sono uguali allora risponde allo smart contract mandando un messaggio di accettazione.
Una volta ricevuta la conferma dell'accettazione del messaggio da parte del destinatario, il mittente manda un piccolo deposito e la chiave K allo smart contract.

Si può subito verificare se K', ossia H(K), caricato nello smart contract, è uguale all'hash di K per controllare che il mittente non abbia caricato chiavi diverse durante il processo. Se viene confermata l'uguaglianza tra gli hash, il destinatario può procedere a decifrare il messaggio.

Ricordando che C, una volta decriptato usando K, è composta dai blocchi del messaggio a cui si accodano blocchi contenenti l'hash dei blocchi stessi, il destinatario controlla che l'hash dei blocchi non criptati sia uguale a quello corrispondente dei blocchi criptati.

Nel caso in cui l'operazione vada a buon fine, al mittente viene restituito il deposito e la ricevuta di consegna, altrimenti, dopo che il destinatario ha fornito le prove di manomissione del messaggio, gli viene accreditato il deposito del mittente come di seguito esemplificato nelle due diverse ipotesi.

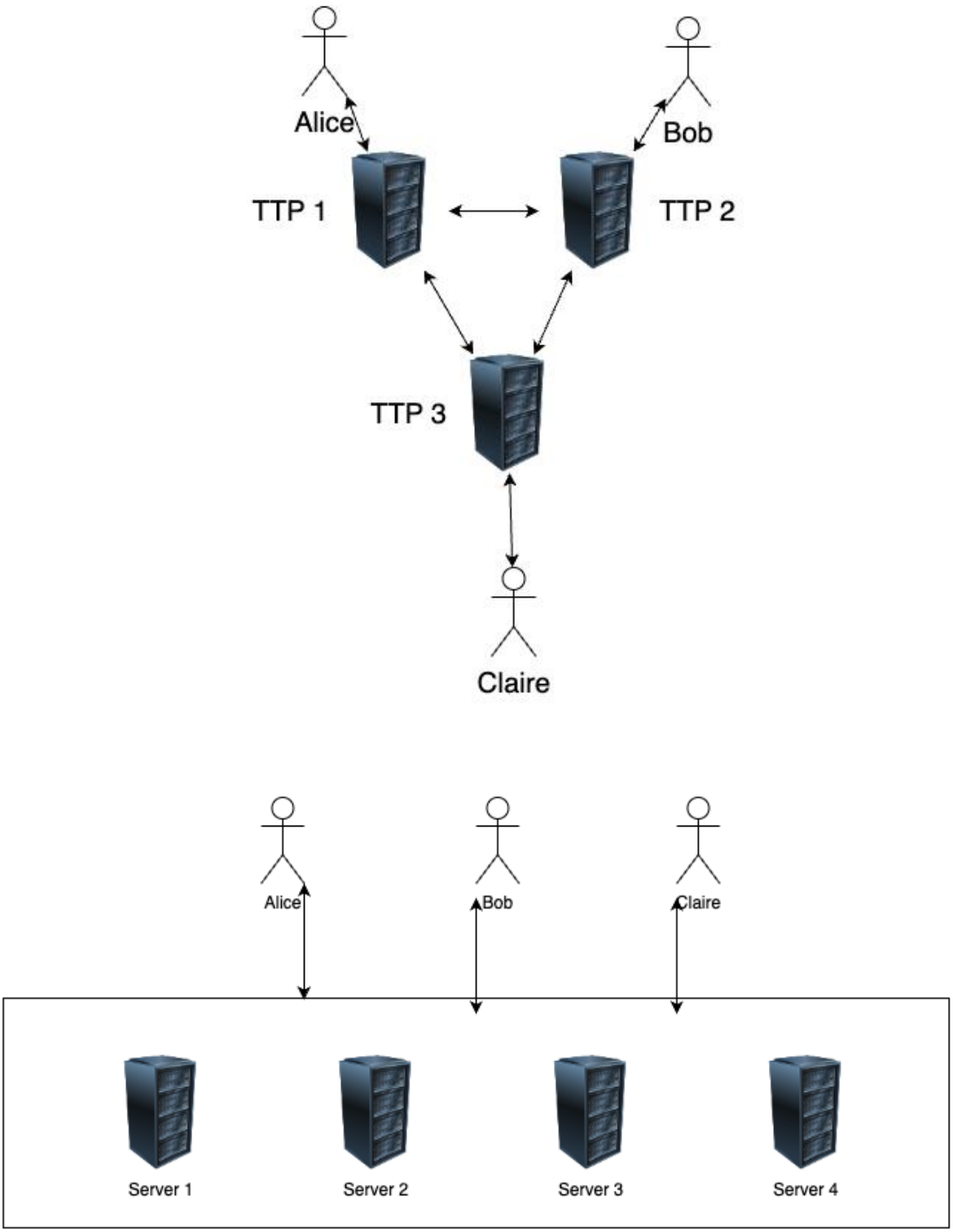




5.2 Il modello

In questa sezione viene proposta un'idea per la creazione di un nuovo modello di scambio di posta elettronica certificata che, anziché basarsi sui TTP, prevede l'esistenza di una *Trusted Infrastructure* (TI).
Una TI è in grado di garantire affidabilità anche se le varie parti da cui è composta non sono fidate (quindi non sono TTP) e non si fidano tra loro.

Di seguito vengono riportate due illustrazioni relative al modello con TTP e quello con TI.



Il lavoro proposto da K. Elmaghraby e T. Dimitriou alla sottosezione 5.1.3 prevede già un protocollo di messaggi certificati che non si basa sui TTP, ma richiede che le parti

coinvolte nello scambio siano online contemporaneamente e non prevede la possibilità di archiviare i messaggi in nessun modo. Il modello proposto in questa sezione ovvia a questi problemi e prevede anche costi inferiori per gli utilizzatori come presentato in seguito.

5.2.1 Il core del modello: la blockchain

Per garantire il funzionamento del modello, le parti che vogliono scambiarsi email certificate devono potersi fidare della TI.
Al fine di un risparmio economico per l'utente finale, si ritiene che sia meglio creare una blockchain dedicata, progettata solo per questo tipo di scambi, anziché usarne una già esistente. Come dimostrato in [14], inviare anche un solo messaggio con la blockchain Ethereum, la più conosciuta che implementa gli smart contract, risulta molto costoso. Vale lo stesso anche per altre criptovalute (ad esempio Solana).

Tutti i componenti della blockchain possono controllare il lavoro eseguito dagli altri nodi, in modo che la fiducia sia garantita.

Per ridurre i costi della TI e renderla poco pesante, senza necessità di asset digitali, il metodo di consenso migliore per la costruzione della blockchain è il PoA. Come indicato alla sottosezione 5.1.2, questo metodo permette di legare l'identità del proprietario del nodo al nodo stesso, a garanzia di un comportamento corretto nei confronti dei partecipanti alla blockchain.

Inoltre nello scambio di email certificate è importante che ci sia un'indicazione temporale su tutti i messaggi. Anziché chiedere ad un TTP di certificare l'istante in cui viene scambiata una email, la TI potrebbe utilizzare il meccanismo del PoH per dare alla blockchain un metodo per misurare lo scorrere del tempo e per ordinare correttamente i messaggi scambiati.

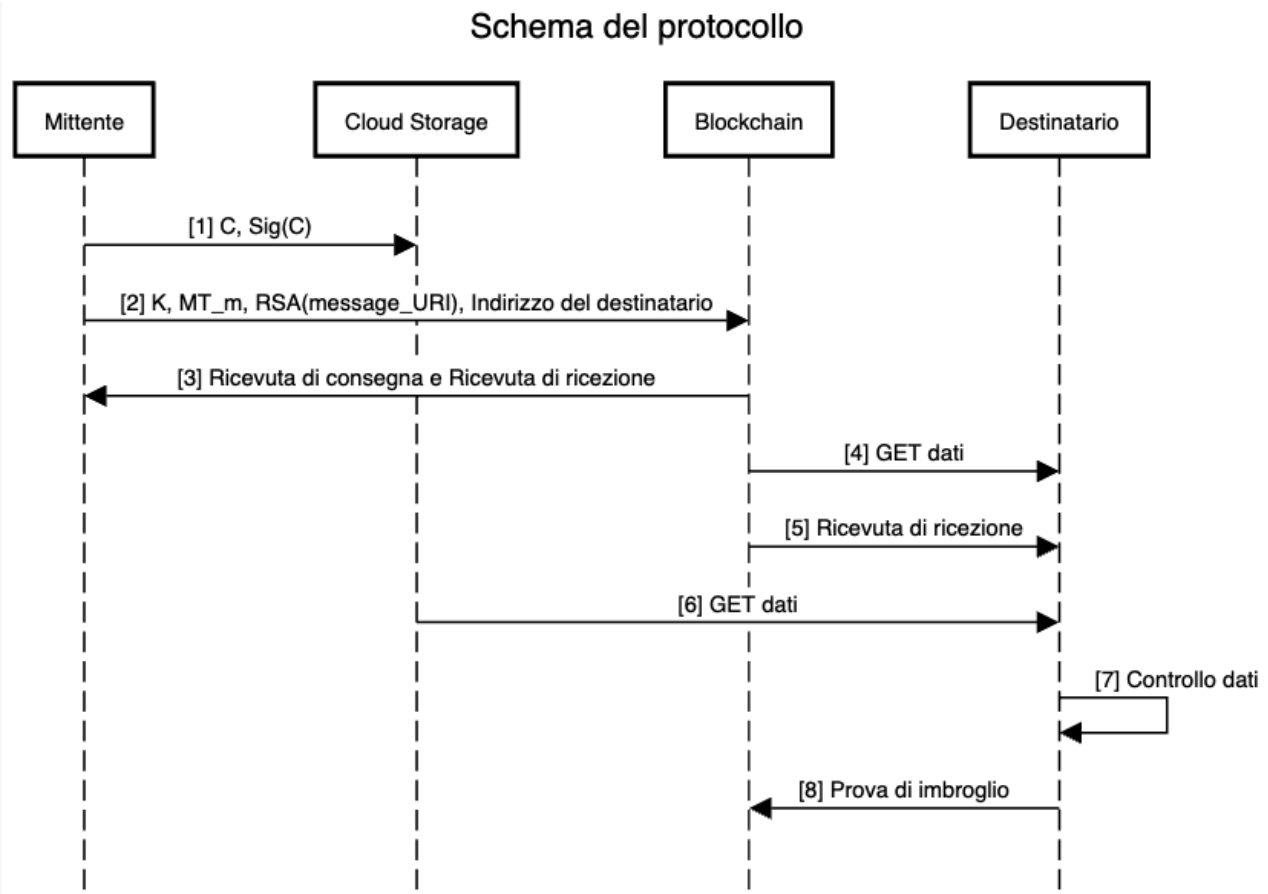
5.2.2 Il protocollo di scambio di email certificate nel dettaglio

Il protocollo di scambio di email certificate proposto ha un funzionamento simile a quello proposto alla sottosezione 5.1.3, ma prevede anche un luogo in cui salvare i messaggi

temporaneamente finché i destinatari non accedono alla loro cartella di posta elettronica certificata.
Questo spazio, reso sempre accessibile perché nel cloud, potrebbe essere alternativamente:

- fornito dagli stessi nodi della blockchain;
- gestito da società terze che salvano i dati in maniera distribuita, magari utilizzando il protocollo InterPlanetary File System (IPFS).

Il protocollo segue le fasi sotto riportate nel *sequence diagram*.



Di seguito sono spiegati punto per punto tutti i passaggi:

1. Il mittente crea una struttura dati M che contiene il messaggio *m* diviso in *n* blocchi e poi altri *n* blocchi che contengono l'hash dei blocchi del messaggio originale. Viene generata K, una chiave simmetrica che cripta tutti i blocchi di M in una struttura dati C. Il mittente carica C firmato (C, Sig(C)) ad un URI (message_URI) specifico;

2. Alice carica una transazione nella blockchain che contiene: la chiave K, la root Merkle Tree MT_m di M, l'indirizzo del destinatario e l'URI della directory in cui è stato caricato il messaggio, quest'ultimo è criptato con chiavi asimmetriche (con algoritmo RSA ad esempio), RSA(message_URI);
3. La blockchain produce la ricevuta di consegna e di ricezione e le invia al mittente;
4. Quando il destinatario accede alla sua casella di posta elettronica certificata, esegue in automatico una ricerca in cui scansiona la blockchain in cerca di messaggi per lui. Se ne trova, richiede i dati e decripta RSA(message_URI).
5. Il destinatario riceve la ricevuta di ricezione relativa al messaggio del quale ha appena richiesto informazioni;
6. Il destinatario fa una richiesta GET per ottenere i dati custoditi all'URI message_URI;
7. Il destinatario controlla che i dati che gli sono arrivati siano corretti. In particolare:
    I. Decripta C utilizzando la chiave K caricata in blockchain (ottenendo quindi M);
    II. Verifica che la root del Merkle Tree di M sia uguale a MT_m caricata in blockchain;
    III. Verifica che gli hash dei primi *n* blocchi di M siano uguali ai valori caricati nei blocchi di M a partire dall'indice *n + 1*
8. Se i dati ricevuti dal destinatario non sono corretti, ossia sono state trovate delle anomalie al punto 7, può inviare una transazione in blockchain in cui comunica l'errore alla rete rendendo il messaggio non valido.

Nel caso in cui il mittente volesse mandare un messaggio a più destinatari, devono essere create più transazioni in cui l'unica cosa che cambia è message_URI e quindi di conseguenza RSA(message_URI).

5.3 Copertura dei requisiti teorici di Draper-Gil *et al.*

Viene ora analizzato il modello proposto secondo i punti proposti da Draper-Gil *et al.* descritti alla sezione 3.1

1. Efficacia (*effectivness*): se entrambe le parti si comportano correttamente, il destinatario è in grado di ricevere il messaggio e il mittente è in grado di provarlo;

2. Equità (*fairness*): è garantita perché il mittente e il destinatario ottengono il risultato desiderato o non ottengono nulla. Nel caso in cui il mittente dovesse agire in modo disonesto inviando la chiave sbagliata K con cui ha criptato C, il destinatario potrebbe facilmente controbattere con la prova dell'imbroglio perché sarebbe in grado di dimostrare che MT_m caricato in blockchain è diverso dal Merkle Tree calcolato su C decriptato con K. Il mittente potrebbe anche indicare un message_URI sbagliato, ma il destinatario potrebbe facilmente provare che l'URI indicato nella transazione in blockchain è vuoto. Il destinatario, invece, non può agire in modo realmente malevolo, poiché le sue uniche interazioni sono quelle di accettare il messaggio e di denunciare un comportamento scorretto. Il destinatario non può creare una falsa prova di imbroglio perché la transazione in blockchain possiede sia la root del Merkle Tree MT_m sia la chiave K inviata dal mittente;

3. Tempestività (*timeliness*): se entrambe le parti coinvolte nello scambio si comportano onestamente, lo scambio termina in un tempo finito. Se il destinatario non accede alla sua cartella di posta elettronica certificata, il mittente è lo stesso in possesso della ricevuta di ricezione in quanto ha già fornito tutte le informazioni utili al destinatario per leggere il messaggio;

4. Verificabilità del TTP (*verifiability of TTP*): non essendo presente un TTP, non è possibile fare un'analisi del modello riguardo questo punto;

5. Ricezione non selettiva (*Non-selective reception*): una volta che il destinatario accede al servizio di posta elettronica certificata, non può impedire che questo verifichi se gli sono arrivati dei messaggi e, di conseguenza, non può impedirne la consegna;

6. Non ripudio (*Non-Repudiation*): nel modello proposto viene prevista la creazione di solo due rispetto alle quattro ricevute di non ripudio originali: quella di consegna (origine) e quella di ricezione. Oltre a queste, viene prevista la creazione di una Prova di imbroglio nel caso in cui il mittente si comporti in modo disonesto. Questa deve essere inviata dal destinatario alla blockchain e deve contenere le prove

dell'errore per essere ritenuta legittima. Se la Prova di imbroglio è corretta, il messaggio certificato risulta non valido. In base alle ricevute generate, non è possibile per il mittente negare l'invio di un messaggio e il destinatario, invece, anche se non dovesse accedere alla propria casella di posta, non potrebbe negare di non aver ricevuto il messaggio perché il mittente è già in possesso della ricevuta di ricezione;

7. Confidenzialità (*confidentiality*): il protocollo garantisce la confidenzialità del messaggio perché C viene inviato ad un URI criptato sconosciuto a tutti se non al mittente e al destinatario. Anche se una terza parte disonesta riuscisse a trovare la directory in cui è stato caricato C, dovrebbe poi provare a decriptare ciò che ha trovato provando tutte le chiavi caricate in blockchain. Inoltre, se il mittente fosse disonesto e cercasse di imbrogliare, al ricevitore basterebbe trovare un'anomalia nel messaggio per poter inviare una Prova di imbroglio per annullare la validità della email. Il destinatario non potrebbe leggere il contenuto del messaggio perché non potrebbe essere decriptato correttamente, garantendo l'equità dello scambio.

5.4 Copertura dei requisiti eIDAS

Il modello proposto soddisfa i requisiti imposti dal regolamento eIDAS 910/2014 già elencati nella sezione 4.2 come di seguito esplicitato.

5.4.1 Proprietà legali

- Ricevuta di consegna: nel momento in cui il mittente carica tutte le informazioni in nel cloud storage e in blockchain, viene automaticamente creata la ricevuta di consegna;

- Ricevuta di ricezione: nel momento in cui il mittente carica tutte le informazioni in nel cloud storage e in blockchain, viene automaticamente creata la ricevuta di ricezione. Il destinatario riceverà tale ricevuta nel momento in cui accederà alla sua cartella di posta elettronica certificata;

- Ricevuta d'integrità: non sono previste manipolazioni del messaggio dalla blockchain, i dati rimangono tali e quali quelli inviati dal mittente. Inoltre, dato che il messaggio è criptato, se dovesse subire delle manomissioni durante il trasporto, il destinatario non potrebbe leggere il contenuto del messaggio e questo verrebbe ritenuto invalido soddisfacendo i requisiti di un protocollo di scambio equo.

- Protezione contro il rischio di perdita, furto, danno o alterazioni non autorizzate: per salvare i dati caricati dal mittente si potrebbe usare un sistema di archiviazione hardware distribuito in modo da ridurre la probabilità di perdita dei dati. Per quanto riguarda la protezione dai furti, invece, l'algoritmo che viene utilizzato per criptare l'URI della directory in cui viene caricato un messaggio è molto difficile da decifrare se non si è in possesso della chiave corretta, perciò si può ritenere che le informazioni contenute nei messaggi siano al sicuro. Alterazioni non autorizzate non sono possibili perché il ledger è un registro append-only, non si può modificare un dato caricato nel passato.

5.4.2 Proprietà di sicurezza

- Identificazione del mittente: al momento della registrazione di un utente alla blockchain, si può fare in modo di legare la sua identità all'account appena aperto magari usando codici univoci relativi al singolo (come il codice fiscale).

- Certezza temporale: la blockchain ha un modo per misurare il tempo identico per tutti i nodi, perciò, in seguito alla validazione di una transazione, tutti i partecipanti al network possono confermare o negare che un evento sia avvenuto in un dato istante.

- Confidenzialità: Il messaggio è criptato ed è leggibile solamente dal destinatario che è in possesso della chiave per decifrare message_URI.

- Integrità dei dati: i dati non possono essere manomessi per proprietà della blockchain

- Controllo degli errori di instradamento (errori di *routing*): la blockchain può verificare l'esistenza di un account prima di permettere al mittente di inviare un messaggio, impedendogli di inviare un messaggio ad un account non esistente
- Interoperabilità: La blockchain può indicare al mittente tutti i formati dei messaggi che il destinatario può elaborare e trasformare da un formato all'altro.

5.4.3 Proprietà funzionali

- Invio di file di grandi dimensioni: il servizio di cloud storage può permettere l'invio di file di tutte le dimensioni e formati

- Processamento istantaneo: In base alle proprietà della blockchain, si può dire che il servizio sia quasi istantaneo

5.4.4 Altre proprietà

- Rischi ridotti: la consegna dell'email certificata rende impossibile:
    a) la manipolazione dei dati per proprietà della blockchain;
    b) la falsificazione delle indicazioni temporali di invio e ricezione, per via del PoH, il meccanismo con il quale vengono ordinati e validati i messaggi;
    c) l'accesso non autorizzato al messaggio per le proprietà dei metodi di cifratura scelti

- Costi ridotti: in fase di implementazione del modello, si può decidere quale sia il massimo numero di *validator* che la blockchain può avere, sia per una questione di efficienza nella propagazione degli stati, sia per una questione economica. Inoltre, dato il grande numero di potenziali utilizzatori (come indicato alla sezione 4.4), probabilmente il costo dell'infrastruttura potrebbe essere ben distribuito tra questi.
  La spesa più elevata potrebbe derivare dallo storage, ma sarebbe distribuita tra molti utenti.

- Nessun doppio invio: evita l'invio di un'ulteriore versione firmata, in formato cartaceo, dei dati elettronici

- Gestione degli incidenti e responsabilità: in caso di negligenza o omissione, non è possibile stabilire chi sia il colpevole. Ogni nodo, però, può controllare il lavoro degli altri partecipanti, rendendo la probabilità di errore molto bassa.

5.4.5 Novità introdotte da eIDAS 2.0

La proposta di Regolamento del Parlamento e del Consiglio dell'UE del 3 giugno 2021, non ancora formalizzata, modifica il regolamento UE eIDAS, c.d eIDAS 2.0.

Le modifiche più interessanti nel contesto della presente tesi sono quelle che concernono gli effetti legali dei registri elettronici (*electronic ledger*). Il punto 39 della proposta in discussione prevede l'inserimento degli artt.45 nonies e 45 decies (45h e 45i nella versione inglese) nel Regolamento eIDAS attualmente vigente.
In particolare l'art. 45 nonies descrive gli effetti giuridici dei registri elettronici:
"

1. A un registro elettronico non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i registri elettronici qualificati;
2. Un registro elettronico qualificato gode della presunzione dell'unicità e dell'autenticità dei dati in esso contenuti, nonché dell'accuratezza della data e dell'ora di tali dati e del loro ordine cronologico sequenziale all'interno del registro.

"

L’art. 45 decies prevede i requisiti per i registri elettronici qualificati come sotto riportati:

“

1. I registri elettronici qualificati soddisfano i requisiti seguenti:
    a) sono creati da uno o più prestatori di servizi fiduciari qualificati;
    b) garantiscono l'unicità, l'autenticità e il corretto sequenziamento dei dati inseriti nel registro;
    c) garantiscono il corretto ordine cronologico sequenziale dei dati nel registro e l'accuratezza della data e dell'ora degli stessi;
    d) registrano i dati in modo tale che sia possibile individuare immediatamente qualsiasi successiva modifica degli stessi.
2. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove un registro elettronico adempia le norme di cui al paragrafo 3.
3. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai processi di esecuzione e registrazione di un insieme di dati in un registro elettronico qualificato e alla creazione di tale registro. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

“

Con l’approvazione dei suddetti emendamenti, eIDAS 2.0 semplifica l’utilizzabilità di un registro elettronico distribuito quale prova valida in un tribunale. Inoltre, se il modello presentato venisse adottato e sviluppato da un TTP, il servizio diventerebbe anche qualificato (art 45 decies punto 1a), rafforzando ancora di più la credibilità del ledger della blockchain.

6 Conclusioni

I servizi che permettono di scambiare email certificate non sono ancora diffusi su larga scala, ma, con la maturazione dei sistemi informatici, l'Unione Europea ne ha già previsto una futura adozione a livello comunitario. Un utilizzo della posta elettronica certificata su così larga scala gioverà molto allo scambio di informazioni tra privati, aziende e Pubblica Amministrazione, semplificando e velocizzando le modalità di comunicazione tra le parti e diminuendo le spese che prima si dovevano sostenere per inviare una comunicazione fisica, forse anche permettendo uno sviluppo economico maggiore.

Molto spesso, forse per motivi di comodità o per motivi di interessi economici, si sceglie di affidarsi a TTP per lo sviluppo dei servizi elettronici. L'analisi contenuta in questa tesi, lungi dal rappresentare un attacco alla scelta di utilizzo dei TTP o dell'utilizzo delle blockchain, rappresenta uno spunto di riflessione su un modo alternativo per sviluppare un servizio di scambio di email certificate.
La forza del modello proposto sta nel fatto che tutte le tecnologie su cui si baserebbe esistono già e funzionano senza errori. Lo sforzo da compiere sarebbe quello di implementarle insieme.
La perdita economica subita dagli intermediari a causa di un servizio che non li contempla potrebbe essere colmata richiedendo agli utenti un abbonamento per la disponibilità di uno spazio di archiviazione per conservare i messaggi scambiati.

Proponendo l'utilizzo della blockchain per salvare i dati relativi allo scambio di email certificate, infine, si garantisce decentralizzazione e tolleranza all'errore, che costituiscono valori aggiunti che un TTP, non assicura allo stesso modo.

7 Bibliografia

[1] M. G. N. H. B. P. B. Abadi, "Certified email with a light on-line trusted third party: Design and implementation," in *Proceedings of the 11th International Conference on World Wide Web, WWW '02*, 2002, pp. 387-395.

[2] B. d. M. M. T. G. Giuseppe Ateniese, "TRICERT: A Distributed Certified E-Mail Scheme," 2001.

[3] M. P.-C. L. H.-R. Josep Lluís Ferrer-Gomila, "A Realistic Protocol for Multi-party Certified Electronic Mail," in *Lecture Notes in Computer Science book series (LNCS,volume 2433)*, 2002.

[4] R. Deng, "Practical protocols for certified electronic mail," *Journal of Network and Systems Management,* vol. 4, no. 3, pp. 279-297, 1996.

[5] J. A. J. Z. a. J. L. Onieva, "Enhancing certified email service for timeliness and multicasting," in *Proc. of 4th International Network Conference (INC'04)*, 2004, pp. 327-336.

[6] M. M. J. L. F. G. L. H. I. R. Puigserver, "Certified e-mail protocol with verifiable third party," in *Puigserver, M. M., Gomila, J. L. F., & Rotger, L. H. I. (2005, March). Certified e-mail protocol with verifiable third party. In 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service*, IEEE, 2005, pp. 548-551.

[7] J. O. J. L. J. Zhou, "Optimized multi-party certified email protocols," in *nformation management & computer security 13, no. 5* , 2005, pp. 350-366.

[8] J. L. F.-G. M. F. H. a. A. T. G. Draper-Gil, "An optimistic certified e-mail protocol for the current Internet e-mail architecture," in *2014 IEEE Conference on Communications and Network Security*, San Francisco, IEEE, 2014, pp. 382-390.

[9] A. Tauber, "A survey of certified mail systems provided on the Internet," in *Computers & Security, Volume 30, Issues 6–7*, 211, pp. 464-485.

[10] M. F. H. G. D.-G. L. H.-R. Josep-Lluís Ferrer-Gomila, "Optimistic protocol for certified electronic mail with verifiable TTP," in *Computer Standards & Interfaces, Volume 57*, 2018, pp. 20-30.

[11] O. G. a. A. L. S. Even, "A randomized protocol for signing contracts," in *Commun. ACM, vol. 28, no. 6,*, 1985, pp. 637-647.

[12] O. G. S. M. a. R. L. R. M. Ben-Or, "A fair protocol for signing contracts," in *IEEE Trans. on Information Theory, vol. 36, no. 1*, 1990, pp. 40-46.

[13] M. M.-P. a. M. A. C.-N. M. M. Payeras-Capellà, "Blockchain-Based System for Multiparty Electronic Registered Delivery Services," in *IEEE Access, vol. 7*, 2019, pp. 95825-95843.

[14] K. E. a. T. Dimitriou, "Blockchain-Based Fair and Secure Certified Electronic Mail Without a TTP," in *IEEE Access, vol. 9*, 2021, pp. 100708-100724.

[15] M. A. C.-N. a. M. M. P.-C. M. Mut-Puigserver, "Removing the Trusted Third Party in a Confidential Multiparty Registered eDelivery Protocol Using Blockchain," in *EEE Access, vol. 8*, 2020, pp. 106855-106871.

[16] J. -L. F.-G. a. L. H.-R. M. F. Hinarejos, "A Solution for Secure Certified Electronic Mail Using Blockchain as a Secure Message Board," in *IEEE Access, vol. 7*, 2019, pp. 31330-31341.

[17] "Proof-of-Authority Chains - Wiki," [Online]. Available: https://openethereum.github.io/Proof-of-Authority-Chains.

[18] Wikipedia, "Proof of authority," [Online]. Available: https://en.wikipedia.org/wiki/Proof_of_authority.

[19] T. W. Alois Paulin, "A universal system for fair non-repudiable certified e-mail without a trusted third party," in *Computers & Security, Volume 32*, 2013, pp. 207-218.

[20] J. A. O. M. P. J. L. Josep Lluis Ferrer-Gomilla, "Certified electronic mail: Properties revisited," in *Computers & Security, Volume 29, Issue 2,*, 2010, pp. 167-179.

[21] S. M. O. Z. J. Kremer, "An intensive survey of fair non-repudiation protocols," in *Computer communications, 25(17)*, 2002, pp. 1606-1621.

[22] R. Oppliger, "Providing certified mail services on the internet," in *IEEE Security & Privacy, 5(1)*, 2007, pp. 16-22.

[23] J. A. J. Z. J. L. Onieva, "Multiparty nonrepudiation: A survey," in *ACM Computing Surveys (CSUR) 41.1* , 2009, pp. 1-43.