

Il progetto CAFE di ESPIRIT

Alta sicurezza digitale dei sistemi di pagamento

Sommario

CAFE(conditional access for Europe) è un progetto in corso nella comunità europea programma ESPIRIT. Lo scopo di CAFE è di sviluppare sistemi innovativi per l'accesso condizionato, e in particolare , per i sistemi di pagamento digitale. Un importante aspetto di CAFE è l'alta sicurezza di tutte le parti interessate, con il vantaggio di essere costretti ad affidarsi ad altre parti solo nel minor numero di casi possibili (la così detta sicurezza multi-parte). Ciò dovrebbe dare una sicurezza giuridica a tutti in ogni momento. Inoltre sia l'emittente di moneta elettronica che i singoli utenti sono meno propensi a manomettere dispositivi rispetto ai soliti sistemi di pagamento digitali. Dato che CAFE mira a un mercato di piccoli pagamenti giornalieri che sono attualmente dominati dai contanti, i pagamenti sono offline e la privacy è un importante problema.

I dispositivi base usati in CAFE sono chiamati portafogli elettronici la cui modalità di azione è abbastanza simile ai calcolatori tascabili oppure alle PDAs(Personal Digital Assistant).

Altre caratteristiche sono:

- 1)**Perdita di tolleranza**: se un utente perde un portafoglio elettronico, ho il portafoglio si rompe o viene rubato, l'utente può ricevere i soldi indietro,nonostante esso sia un sistema di pagamento prepagato.
- 2)**Differenti valute**.
- 3)**Architettura e sistema aperto**.

Il progetto

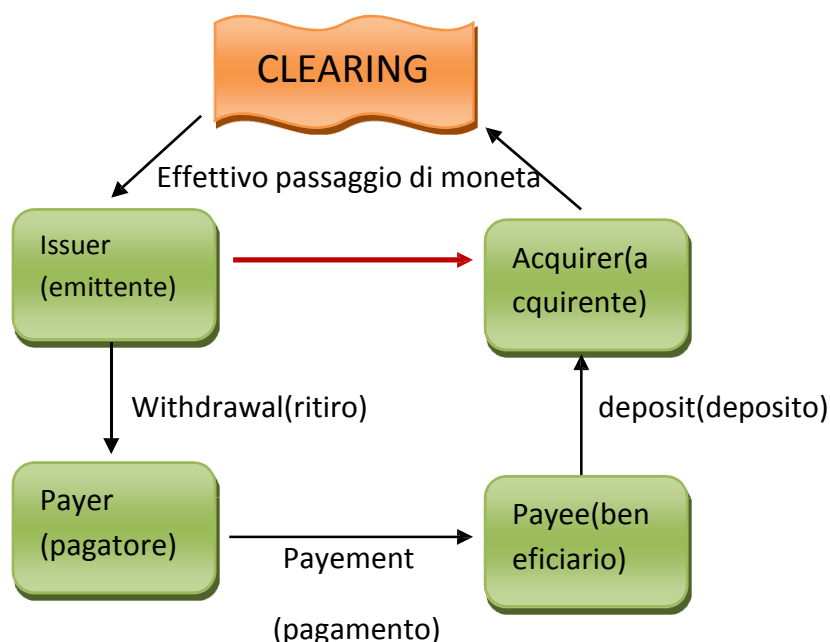
Obiettivi e partecipanti

CAFE è un progetto in programma ESPIRIT della comunità europea(Progetto 7023). Il lavoro sul CAFE iniziò nel dicembre del 1992 e si è concluso nel dicembre del 1995. Il consorzio era composto da gruppi per gli studi sociali e di mercato (Cardware, institut fur Sozialforshung),produttori di software e hardware(Digital Cash,Gemplus,Ingenico,Siemens)e designers di sicuri protocolli crittografici. Il coordinatore del progetto è David Chaum per CWI.

Lo scopo del CAFE è quello di sviluppare sistemi innovativi per l'accesso condizionato,sistemi digitali che amministrano i diritti dei loro utenti come: forme digitali di passaporti, accessi a dati confidenziali oppure sistemi di pagamenti digitali.

Il sistema

Nella seguente figura vengono mostrati i più importanti ruoli nei sistemi di pagamento e le transizioni eseguite:



Il pagatore: un pagatore ritira la moneta elettronica da un emittente e paga i servizi o i beni ad un beneficiario attraverso una transazione.

Il beneficiario: riceve la moneta elettronica da un pagatore mediante una transazione e al deposita a un acquirente tramite una transazione di deposito.

L'emittente: è un organizzatore della banca che emette la moneta elettronica con pagamenti.

Acquirente: raccoglie la moneta elettronica da un beneficiario.

Il clearing: controlla la validità della moneta elettronica accumulata. E inzializza il trasferimento di moneta da una banca all'altra.

Funzionalità di base

Il sistema CAFE è un sistema prepaid (prepagato) e offline.

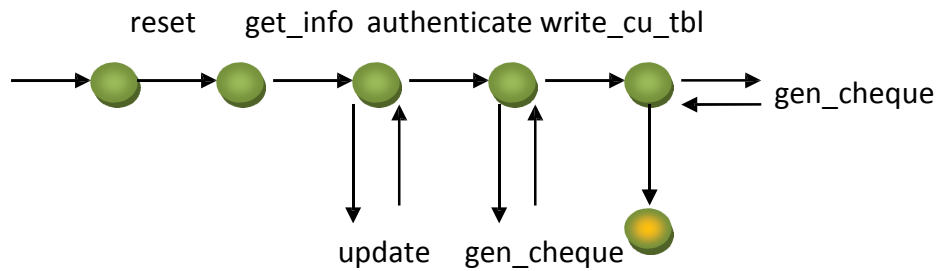
prepaid: significa che un utente deve comprare una così detta moneta elettronica da un emittente di moneta elettronica e caricarla nel suo borsellino prima di effettuare dei pagamenti.

Offline: significa che non c'è bisogno di alcun contatto con un database centrale, di solito un emittente di moneta elettronica, durante il pagamento. Una alternativa, pagamenti online, è troppo costosa: bisognerebbe pagare l'emittente di transazione elettronica per la comunicazione e l'elaborazione.

Transazioni

Le più importanti transazioni nel sistema di pagamento CAFE sono il ritiro il pagamento e il deposito. Queste transazioni sono i servizi chiave del sistema di pagamento.

Ritiro: questa transizione è eseguita tra l'emittente e il pagatore. L'emittente addebita sul conto bancario del pagatore una somma specificata dal pagatore e emette la corrispondente somma in moneta elettronica. Il pagatore può scegliere la sua moneta elettronica da una lista di differenti monete. La figura mostra la composizione del protocollo nella transazione di ritiro:

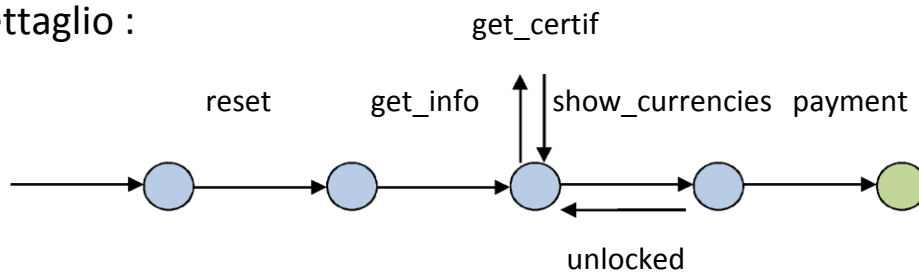


- 1) Il borsellino è inizializzato dal protocollo **reset**.
- 2) Il borsellino presenta i propri dati memorizzati dall'emittente attraverso l'esecuzione del protocollo **get_info**. Se è necessario l'aggiornamento il protocollo di **update** è eseguito.
- 3) Il protocollo di **authenticate** è eseguito. A questo punto l'emittente la sua identità al borsellino, successivamente, il borsellino lo identifica e segna tutti i dati pertinenti all'emittente.

Se una ho più sessioni di pagamento successive alla sessione di precedente ritiro hanno fallito, il protocollo **rec_payments** viene richiamato. Il protocollo **write_cu_tbl** è chiamato nel momento in cui viene nel momento in cui il protocollo **authenticate** viene interrotto per qualsiasi motivo. Mentre l'utente è occupato nell'esecuzione di servizi bancari, l'emittente e il portafoglio possono eseguire il protocollo **gen_cheque**. Se questo protocollo fallisce per qualche ragione il protocollo **authenticate** deve essere rieseguito.

Pagamento: è eseguito tra il pagatore e il beneficiario, alla richiesta del beneficiario il pagatore trasferisce la moneta elettronica al beneficiario. Il beneficiario ne verifica la validità e accetta il pagamento. Nella seguente

figura viene mostrato come avviene la transazione di pagamento nel dettaglio :

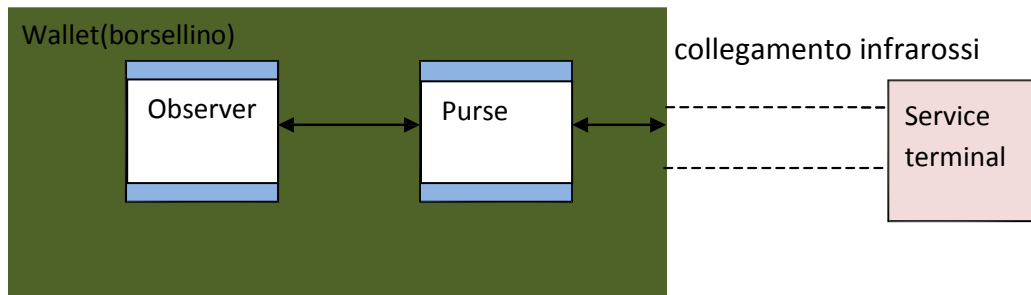


- 1) Il portafoglio elettronico viene resettato usando il protocollo **reset**.
- 2) La cassa inizializza il protocollo **get_info** per verificare che le chiavi pubbliche che saranno richieste sono utilizzabili. Se ciò non si verifica la cassa inizierà il protocollo **get_certif** per richiamare questo dal borsellino.
- 3) Il protocollo **show_currencies** permetterà al pagatore e al beneficiario di calcolare come può essere eseguito il pagamento se la somma di denaro sbloccata è insufficiente per il pagamento il protocollo **unlocked** provvederà allo svolgimento di tale operazione, sempre assistito dal pagatore.
- 4) Compiuta tale operazione viene attuato il protocollo di **payment**.

Deposito: il beneficiario deposita presso l'acquirente la moneta elettronica ricevuta grazie a una transazione. L'acquirente segue la registrazione del deposito sul sistema clearing e sul conto del beneficiario è accreditato un ammontare che corrisponde alla moneta elettronica ricevuta. In tale transazione avviene un'operazione di protocollo cioè il protocollo **deposit** che inoltra il pagamento trascritto all'acquirente.

I dispositivi

Una componente importante nell'architettura del CAFE è il **l'electronic wallet**(portafoglio elettronico). Le entità funzionali che entrano in gioco nel portafoglio elettronico sono mostrate in figura:



Il portafoglio elettronico è un elemento essenziale per la sicurezza del sistema CAFE.

Nel portafoglio elettronico sono inclusi un **observer**(osservatore) e una **purse**(borsa).L'observer si affida all'emittente protegge l'interesse dell'emittente durante le transazioni online e controlla la somma di denaro che il pagatore può spendere . Quindi l'observer deve essere resistente a qualsiasi tipo di manomissione. La purse si affida al pagatore, verifica le azioni del pagatore e impedisce all'observer di compiere azioni indesiderate. In pratica, il purse contiene bottoni o una tastiera e un display per digitare dati di input o output. Per esempio questi possono essere usati per bloccare o sbloccare il portafoglio e per verificare che sia avvenuta la transazione di pagamento.

Ci sono tre differenti tipologie di portafoglio elettronico:

Borsellino α: in questo tipo di portafoglio sia il purse che l'observer possono essere implementati in un unico chip tipicamente incorporato in una smart card. Il purse può comunicare con l'ambiente esterno solo attraverso contatti elettrici della carta. Il pagatore deve fare affidamento

strutture esterne come il PIN. Il dispositivo non rimane sempre sotto il controllo fisico del debitore perché deve essere inserito nel terminale.

La combinazione di observer e purse in un unico dispositivo implica che sia emittente che pagatore devono fidarsi di tale dispositivo. L'emittente deve avere fiducia nel portafoglio affinché non commetta errori e non superi la somma richiesta dal pagatore in accordo con il bilancio del suo borsellino il pagatore deve fidarsi del borsellino , che potrebbe rivelare l'identità del debitore durante l'operazione di pagamento. Il pagatore deve anche avere fiducia nel numero di servizio del terminale. La cassa ,di solito,è implementata da un punto terminale di vendita con un display e una tastiera usati per verificare la somma di pagamento e l'inserimento corretto del PIN .



Borsellino α + :non è altro che un miglioramento del borsellino alpha per quanto riguarda l'interfaccia utente. L'observer di alpha e alpha + sono abbastanza simili. La purse di alpha + è stata ampliata con la funzionalità di interfaccia utente. Ad esempio alcuni pulsanti utilizzati dal pagatore per confermare un'azione.

In sintesi il portafoglio alpha + porta i seguenti miglioramenti rispetto al portafoglio alpha:

- 1) Una singola interfaccia utente per il pagatore.
- 2) Un display per la verifica delle azioni.
- 3) Pulsanti specifici per l'inserimento del PIN e un utente per il riconoscimento delle azioni.
- 4) Maggiori controlli
- 5) Comunicazione esterna da parte di un collegamento infrarossi che consente al pagatore di avere pieno controllo fisico sul portafoglio

Il pagatore inoltre non può controllare la funzionalità del purse del portafoglio alpha perché esso è implementato sullo stesso chip

dell'osservatore. Il purse deve essere attendibile e non contenere informazioni nascoste che potrebbero consentire la perdita di informazioni aggiuntive come l'identità del pagatore. Il borsellino alpha + annulla il bisogno di affidarsi ai terminali di servizio. Il pagatore non dovrà consegnare il borsellino elettronico al beneficiario. L'inserimento del PIN e la verifica delle somme saranno effettuate dal pagatore, usando il display e i pulsanti sul dispositivo.



Borsellino Γ : il portafoglio gamma è un borsellino del tutto funzionale. Esso è costituito da un observerer , implementato da un singolo chip di resistenza alle manomissioni e incorporato in un dispositivo purse . il purse ha capacità di elaborazione ,memoria e input/output facilitati. Esso ha la forma di un piccolo dispositivo tascabile con display tastiera e collegamento raggi infrarossi per la comunicazione con i terminali di servizio.

In sintesi, il borsellino gamma offre i seguenti miglioramenti rispetto a quello alpha +:

- 1) migliore performance perché il purse ha un potere calcolatore e può eseguire parti di protocolli.
- 2) migliori caratteristiche che garantiscono privacy e sicurezza perché il purse è abilitato per la verifica dell'azione dell'osservatore.

3) un'interfaccia utente che può essere adattata in base alle richieste del pagatore.

Il pagatore deve affidarsi all'operatore per effettuare la verifica del PIN. Il purse è responsabile per l'interazione sia con il pagatore che con i terminali di servizio. Inoltre, il purse verifica tutte le azioni effettuate dall'operatore e evita che l'operatore possa rilasciare bits di informazioni al terminale.



Caratteristiche aggiuntive

Il sistema base CAFE prevede le seguenti caratteristiche aggiuntive:

Differenti tipi di moneta: è possibile possedere e utilizzare diversi tipi di moneta elettronica anche nel corso dell'operazione di pagamento.

Assicurazione verso perdita o malfunzionamento del borsellino: se un utente perde il proprio borsello elettronico, o se questo viene rubato o se si guasta, l'utente può avere il denaro indietro, sebbene il sistema sia di tipo pre-paid.

Il sistema base CAFE è, sotto molti aspetti, un **sistema aperto**:

È progettato come sistema universale di pagamento: ogni utente dovrebbe essere in grado, con il proprio borsello, di pagare per i servizi più svariati presso un qualsiasi fornitore di tali servizi. Esempi sono i negozi, il telefono e i trasporti pubblici.

È garantita l'interoperabilità tra un numero qualsiasi di fornitori di denaro elettronico (cioè è possibile effettuare pagamenti tra clienti

di diversi fornitori di moneta). Nuovi fornitori di moneta si potranno aggiungere in seguito.

Solo certi protocolli sono fissati, e non precisi componenti software o hardware. Dunque CAFE è aperto per nuove piattaforme hardware e può essere integrato in altri sistemi. La comunicazione "senza contatto" è in questo contesto particolarmente utile.

Nessuna restrizione per compratore e venditore si rende necessaria, dal momento che CAFE è un sistema di tipo pre-paid.

Borselli elettronici semplici hanno basso costo in una produzione di massa e l'utilizzo di tali borselli e dei rispettivi terminali POS è piuttosto semplice: anche da un punto di vista pratico nessuno è teoricamente escluso dall'utilizzo di CAFE.

Gli speciali obiettivi di sicurezza del progetto CAFE

Le più importanti differenze tra i sistemi di pagamento CAFE e altri digitali sistemi di pagamento off-line è nell'alta sicurezza garantita dal modello CAFE. In questa sezione , vengono esposti gli obiettivi mentre nella seguente vengono trattate le misure tecniche che consentono di effettuare tutti questi obiettivi in maniera simultanea.

La sicurezza multi-parte

La maggior parte dei sistemi di pagamento digitale sono progettati come sistemi one-sided security(sicurezza unilaterale): tutti i partecipanti devono affidarsi alle singole parti, di solito un emittente di moneta elettronica.

Per i sistemi di pagamento la sicurezza one- sided è inadatta poiché non può offrire una certezza legale per alcune delle parti interessate. Per esempio consideriamo **ATM**(automatic teller machine) i così detti

bancomat, quando un cliente usa la sua carta bancaria in un bancomat la sua sicurezza è completamente nelle mani dell' emittente; tutti i dati registrati nella carta li conosce anche la banca, quindi tutte le operazioni che fa il cliente possono anche essere effettuate anche da un banchiere disonesto (Non c'è un ordine di ritiro firmato dal cliente che la banca ha memorizzato come una prova di transazioni in un sistema di pagamenti convenzionale). Nessun tribunale può decidere se un'operazione di ritiro è stata fatta da un cliente oppure da un banchiere disonesto. Quindi nessuna delle 2 parti né banca né cliente ha la sicurezza giuridica di come un tribunale potrebbe agire davanti alla mancata sicurezza causata da frodi. Anche se si accettasse che in alcune banche ci siano più fidati che clienti, la situazione non cambierebbe comunque, la banca potrebbe dimostrare con le sue misure di sicurezza interna che ogni tentativo di frode è impossibile, e comunque è improbabile che una banca possa fare ciò in maniera soddisfacente. Da una parte, nonostante la sicurezza sia apparentemente forte si sono verificati diversi casi di frode [Ande 93], dall'altra il numero di lavoratori è molto alto esso non comprende solo i dipendenti della banca ma anche tutte le istituzioni che dipendono da loro i quali non hanno nulla a che vedere con la progettazione, la produzione, l'installazione e la manutenzione dei sistemi hardware e software dei sistemi di pagamento.

Per evitare tali situazioni IL sistema CAFE ha progettato un sistema di sicurezza multi- parte, tutti i requisiti di una parte sono garantiti senza costringere tale parte di fidarsi di altre. In particolare, la fiducia reciproca tra le varie parti con conflitto di interesse (come cliente e banca) non è assunta. Idealmente, una parte si fida solo di se stessa e della giurisdizione (le decisioni di un tribunale non possono mai essere verificate).

La sicurezza multi -parte è vantaggiosa per tutte le parti:

1) essa incrementa la sicurezza giuridica, dato che le situazioni sono indecidibili ,cosa che invece può verificarsi facilmente in un sistema unilaterale.

2) decrementa gli attacchi degli addetti ai lavori.

3)rende il sistema più soddisfacente per potenziali utenti ed è quindi un argomento di pubbliche relazioni per gli emittenti di moneta elettronica.

La sicurezza multi- parte ha alcune implicazioni sul processo di progettazione e produzione come:

1)tutti i progetto(software e hardware) che sia cruciali per la sicurezza di una parte deve essere sottoposte ad un ispezione della parte(dunque algoritmi segreti sono esclusi da CAFE fatta eccezione per le procedure del fornitore).

2) Deve essere garantito che ogni parte possa fidarsi del proprio dispositivo. Poichè la maggioranza degli utenti non può né produrre né ispezionare il proprio borsello, deve esistere un numero sufficiente di autorità indipendenti e competenti che verifichino sia il progetto che il dispositivo vero e proprio ciò comporta che loro verifichino i campioni dei borsellini appena sono consegnati agli utenti, non in presenza del fabbricante. Le autorità di controllo sono agenzie certificate nella tecnica di controllo di schede.

Protezione dei dati

Previsto per un utilizzo di massa , il sistema CAFE dovrebbe essere particolarmente adatto per i pagamenti di basso importo(shopping giornaliero,chiamate telefoniche ,utilizzo sui trasporti pubblici).

Quando un individuo usa una carta di credito per ogni tipo di pagamento, la compagnia della carta avrà registrato sul profilo dell'utente tutte le operazioni compiute. Vengono registrate l'ora e il luogo in cui è stato

fatto un acquisto in un negozio per esempio, la privacy non viene molto rispettata in queste situazioni.

Invece, al contrario di quello che succede con le carte di credito, chi sfrutta il proprio borsello elettronico risulta **non tracciabile**: il denaro usato non lo identifica né rispetto al venditore né rispetto alla banca. Inoltre pagamenti differenti effettuati dallo stesso utente non sono collegabili, dato che non è possibile sapere, osservando due monete, se queste sono state spese dallo stesso compratore.

Questa forma di non tracciabilità è richiesta anche dagli utenti del sistema:

1) nel sistema di base di CAFE né il beneficiario né l'emittente di moneta elettronica potranno capire l'identità del pagatore da un suo pagamento .

2) come avviene con i contanti, la sicurezza del sistema non esclude che il pagatore possa essere identificato da altri strumenti, per esempio da un protocollo identificativo di crittografia. In particolare si può fissare un limite superiore per la somma che può essere spesa senza identificazioni. Se tutte le misure di sicurezza del protocollo CAFE vengono osservate, tale limite può essere piuttosto alto per esempio 2500 ECU.

Inoltre, potrebbe essere utile avere un limite più basso per esempio 500 ECU oltre il quale i pagamenti debbano essere effettuati on-line pur rimanendo non tracciabili; questo aumenterebbe la sicurezza del fornitore e non danneggerebbe la riservatezza dell'operazione.

Inoltre:

1) per chi riceve il pagamento (venditore) non è richiesta la non tracciabilità: infatti l'utilizzo principale di CAFE sarà l'acquisto di beni o servizi da fornitori che sono in ogni modo conosciuti da compratori.

2) al contrario dei pagamenti, i prelievi e i depositi di denaro sono tracciabili, cioè il cliente viene identificato dall'emittente di moneta

elettronica. Una privacy migliore è vantaggiosa per gli utenti, ma anche per gli emittenti di moneta elettronica, da una parte il sistema viene accettato anche in ambito pubblico diventando così un argomento di pubbliche relazioni, dall'altra riduce il problema della conservazione dei dati sensibili dei clienti riservati degli emittenti di moneta elettronica.

Tolleranza a perdite ed errori

In molti dei sistemi pre-paid un compratore che perde il proprio borsello elettronico perde tutto il denaro memorizzato in esso. Lo stesso accade se il borsello smette di funzionare o viene rubato.

Il sistema CAFE garantisce la restituzione di tale denaro.

L'idea base è quella di tenere copia del denaro dell'utente da qualche parte al di fuori del borsello. Tale copia non deve infrangere la privacy del compratore e dunque deve essere o su una "carta di backup" dell'utente o, in forma crittografata, presso il fornitore di denaro elettronico.

Se l'utente perde il borsello, si valuta il backup in cooperazione con l'utente e con il fornitore: il denaro elettronico è ricostruito, e la parte di esso non ancora spesa è accreditata sul conto dell'utente. La cifra già spesa si ricava confrontando il denaro ricostruito con quello depositato. È da notare che tale tipo di backup non infrange la sicurezza del fornitore: l'utente non può usare la copia del denaro elettronico per effettuare pagamenti poiché non esiste nessun guardiano che dia il proprio assenso ad un tale tipo di operazione.

Esiste un fattore che limita la tolleranza a tali situazioni di emergenza:

Se il borsello (perso o rubato) può essere usato senza alcuna identificazione d'utente (come un PIN), il proprietario non potrà avere indietro quel denaro speso dal ladro (o dal fortunato che ha trovato il borsello).

Per questo motivo CAFE invita i propri utenti a scegliere propri PIN, e in particolare a scegliere il PIN per il pagamento differente dal PIN per il prelievo.

Dispositivi di sicurezza : firma digitale e protocolli crittografici

Questione molto importante è la seguente: come garantire la sicurezza del fornitore di denaro elettronico nei pagamenti off-line? Dopo tutto, il denaro elettronico è solo una stringa di bit. Dunque, anche se un sistema è sicuro nel senso che gli utenti non possono produrre nuovo denaro, cioè una nuova stringa di bit valida, chiunque abbia visto tale stringa potrà riprodurla nel tentativo di spendere la stessa moneta, anche più di una volta. Il sistema CAFE propone la seguente soluzione:

è impossibile spendere due volte lo stesso denaro finché un certo tipo di dispositivo anti-frode è funzionante. Anche nel caso in cui venisse superata la protezione, l'utente che spende lo stesso denaro elettronico più di una volta è identificato e la frode può essergli contestata. Non è richiesto all'utente di riporre fiducia in tale dispositivo, il cui interno è oltretutto inaccessibile all'utente stesso. Esso è infatti distribuito dal fornitore di denaro elettronico e protegge la sicurezza di quest'ultimo.

Una misura di sicurezza standard che deve essere applicata è la firma digitale. Tale tecnica è indispensabile per sistemi con sicurezza multi-parte, anche perché è importante notare che, in un sistema di pagamento, ogni messaggio a cui si voglia far avere un qualche valore legale, deve essere firmato per acquistare certezza legale. La firma digitale o schema di firma digitale è uno schema matematico per dimostrare l'autenticità di un messaggio digitale o di un documento, ovvero dà motivo al destinatario del messaggio, di credere che il messaggio è stato creato da un mittente conosciuto, e che non è stato alterato durante il transito. Uno schema di firma digitale consiste tipicamente di tre algoritmi:

1 Una generazione di chiavi, tramite un algoritmo che seleziona una chiave privata da un insieme di possibili chiavi private. L'algoritmo emette la chiave privata e una chiave pubblica corrispondente.

2 Un algoritmo di firma che, dato un messaggio e una chiave privata, produce una firma.

3 Un algoritmo di verifica della firma che, data la chiave pubblica del messaggio e una firma, accetta o respinge il messaggio.

Deve essere quindi possibile, in primo luogo, poter verificare l'autenticità di un messaggio utilizzando la chiave pubblica corrispondente alla chiave privata del mittente. In secondo luogo dovrebbe poi essere impossibile, a livello computazionale, generare una firma valida per chi non possiede la chiave privata, e quindi dovrebbe risultare impossibile la modifica e/o la falsificazione del messaggio stesso. Inoltre, la firma digitale può anche fornire il non ripudio, che consiste nell'impossibilità da parte del firmatario di sostenere di non aver firmato un dato messaggio, anche se la sua chiave privata rimane segreta.

Motivi fondamentali quindi per l'utilizzo della firma digitale, sono dati dal fatto che il messaggio risulta essere:

- **Autentico**
- **Integro**
- **Non ripudiabile**

Il paradigma nell'utilizzo della firma digitale è il seguente : il mittente, unico possessore della chiave privata, produce un'impronta del messaggio, detta hash e la cifra con la sua chiave privata. L'hash cifrato rappresenta la firma digitale. Il destinatario riceve il messaggio insieme alla firma. Dall'hash, dopo averlo decifrato con la chiave pubblica del

mittente, ricava l'impronta del messaggio com'era al momento della sua spedizione. Se le due impronte così ottenute coincidono si è certi che la firma è stata apposta mediante la chiave privata del mittente e che il messaggio non è stato modificato durante la trasmissione. Vediamo quindi che gli algoritmi di firma digitale si affidano principalmente sulla potenza degli algoritmi di hashing. Essi sono algoritmi one-way che producono, a partire da una stringa a lunghezza variabile, una stringa a lunghezza fissa (tipicamente tra 64 e 255 bit) che è caratteristica della stringa data. La loro potenza è dovuta alle seguenti peculiarità:

- 1. data una stringa di hash è computazionalmente impossibile ricavare il messaggio dal quale è stata generata;**
- 2. è computazionalmente impossibile determinare due messaggi che producono la stessa stringa di hash;**
- 3. qualsiasi messaggio, sottoposto allo stesso algoritmo qualsivoglia numero di volte produce sempre lo stesso valore di hash.**

L'algoritmo di hash elabora qualunque mole di bit ovvero di dati grezzi, restituendo una stringa di numeri e lettere univoca per ogni documento, di cui ne è un identificatore. Perciò l'algoritmo è utilizzabile per la firma digitale. Oltretutto l'algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output ovvero è una funzione unidirezionale.

La funzione hash svolge un ruolo fondamentale in crittografia. Quest'ultima, in generale, utilizza algoritmi a chiave privata, o algoritmi simmetrici ed algoritmi a chiave pubblica. La differenza tra di essi è che i primi usano la stessa chiave per la cifratura e la decifratura, mentre i secondi usano due chiavi differenti, una pubblica e una privata.

Gli algoritmi a chiave privata, o algoritmi simmetrici sono i più comunemente utilizzati. Essi usano la stessa chiave per la cifratura e la decifratura. Entrambi gli interlocutori conoscono la chiave usata per la cifratura, detta chiave privata, o chiave simmetrica, e soltanto loro possono cifrare e decifrare il messaggio. Sulla base del tipo di

computazione si individuano due tipi di cifratura : stream cipher (cifratura sequenziale) e block cipher (cifratura a blocchi).

Gli algoritmi a chiave pubblica usano due chiavi complementari, dette chiave pubblica e chiave privata, create in modo che la chiave privata non può assolutamente essere ricavata dalla chiave pubblica. Sono quindi questi gli algoritmi crittografici usati per la firma digitale.

Tornando al sistema di pagamento CAFE, esso si basa sul valore della moneta rappresentato da una serie di equilibri in portafogli elettronici tenuti da contribuenti. Questo valore può essere aggiornato solo attraverso l'esecuzione di operazioni ben definite supportate da meccanismi crittografici. In oltre la protezione contro la modifica indesiderata dei saldi è supportata da un dispositivo resistente alle manomissioni che può anche implementare la

funzionalità dell'osservatore. Sappiamo che quest'ultimo è un chip smart card dotato di un processore per crittografia inserito all'interno del borsello. Esso cambia l'equilibrio del portafoglio solo se il ritiro è valido o la transazione di pagamento è stata effettuata in modo corretto. La resistenza alla manomissione del chip smart card impedisce al debitore (e altri) di aggirare i meccanismi di crittografia e i protocolli cambiando il saldo tramite il meccanismo di doppia

spesa. Quindi si ha che nessun pagamento è accettato fino a che l'osservatore non da il proprio assenso, il quale risulta essere univocamente dato per ogni unità di denaro elettronico. L'assenso dell'osservatore è tale da non consentire al venditore e al fornitore né di riconoscere quale osservatore l'abbia emesso né di ricavare alcuna informazione sul compratore. In ogni caso l'integrità del dispositivo osservatore dipende molto dalle risorse di chi tenta la frode. Per questo motivo CAFE offre al fornitore, un servizio di protezione retroattiva, la quale garantisce che, anche nello sfortunato caso in cui le difese del guardiano siano superate, l'utente che sfrutta questo guardiano per spendere più denaro di quanto permesso sarà identificato e la sua identità potrà essere provata (e dunque usata in sede

legale). Tale tipo di protezione aggiuntiva non utilizza ulteriori dispositivi hardware anti-frode ma utilizza protocolli crittografici. Il fatto che l'utente onesto ha la propria segretezza, mentre chi spende due volte è identificato, è una caratteristica propria dei sistemi di denaro elettronico off-line.

Protocolli :

Riguardo ai protocolli usati nel sistema CAFE, essi sono i seguenti protocolli di crittografia primitiva:

- **Il protocollo di identificazione di Schnorr e schema di firma derivato**
 - **Il sistema di prova di base**
 - **Lo schema restrittivo di firma cieca**
 - **Lo schema di van Heyst-Pedersen**
 - **Lo schema di firma randomizzato**
 - **Lo schema di firma RSA**
- **La funzione a una strada di versamento del credito telefonico**
 - **Il generatore pseudo-casuale di numeri**
 - **La funzione di hash**

Ecco in breve la descrizione degli stessi :

Lo schema di Schnorr :

La maggior parte dei protocolli sono derivati dal protocollo di identificazione Schnorr.

Questo protocollo consente al verificatore di dimostrare l'identità del provatore, tramite il seguente procedimento:

il dimostratore, prende un impegno a caso e da esso si forma una testimonianza iniziale, che viene inviato al verificatore. Il verificatore restituisce, scelta a caso, una sfida. Il dimostratore calcola quindi una risposta e la rimanda indietro. Il verificatore

calcola quindi un testimone finale da questa risposta (la chiave pubblica del dimostratore) e ne verifica l'uguaglianza con la testimonianza iniziale.

Il sistema di prova di base :

il sistema di prova di base è derivato dal protocollo di identificazione di Schnorr. Questo sistema, lavora tramite l'unico sottogruppo di \mathbf{Z}_p^* di ordine q , indicato come G_q (con p e q primi). Esso permette al firmatario, con la coppia di chiavi : S (la chiave segreta) e $P := g^S \text{ mod } p$, di firmare in modo interattivo un messaggio m appartenente a G_q . La firma su m è costituita da $z := m^S \text{ mod } p$ e la prova da $\log_g P = \log_m z$.

Il regime restrittivo di firma cieca :

Lo schema di firma cieca consente al verificatore di ottenere una firma valida (z, c, r) sul messaggio m , in modo tale che il firmatario non può vedere né il messaggio né la sua firma; in tal modo il firmatario non è in grado di collegare la coppia messaggio-firma all'istanza particolare del protocollo di firma che ha generato questa coppia. Tuttavia, lo schema di firma cieca, garantisce al firmatario che la coppia (m, z) sia derivata dal verificatore utilizzando un insieme limitato di operazioni cieche, sulla coppia $(m_0, z := m_0^S)$, nota sia al firmatario che al verificatore.

Lo schema di van Heyst-Pedersen :

Lo schema di firma di van Heyst-Pedersen è un efficiente schema di firma non-stop basato sul logaritmo discreto. Tale schema di firma fornisce una maggiore sicurezza contro la contraffazione attuata da un avversario molto potente. Nel caso in cui viene creata una firma, il presunto firmatario è in grado di dimostrare che la firma è un falso, provando la manomissione dell'assunzione di base del sistema.

La firma casuale di Schnorr :

ogni volta che l'osservatore Γ e la banca si scambiano un messaggio firmato, la banca Γ deve casualizzare la firma, al fine di evitare che banca ed osservatore si inviino

informazioni tra di loro (vale a dire prevenire l'afflusso / deflusso delle stesse),
attraverso la firma.

Lo schema di firma RSA :

sia il numero n (detto modulo), definito come il prodotto di due numeri primi grandi
 p e q .

Sia : $\lambda(n) := \text{lcm}(p-1, q-1) = ((p-1)(q-1)) / \text{MCD}(p-1, q-1)$.

Il fattore pubblico e è scelto in modo che : $\text{MCD}(e, \lambda(n)) = 1$.

Il fattore segreto d è definito come il più piccolo numero intero non negativo che
soddisfa : $ed \bmod \lambda(n) = 1$

Le chiavi pubbliche e private sono definiti quindi come:

- chiave pubblica $P : n := pq$ ed e
- chiave segreta $S : n$ e d , ed eventualmente p e q .

La funzione a una strada di versamento del credito telefonico :

sia N_{phon} il prodotto di due primi p e q .

La funzione :

$$f : \mathbb{Z}^{N_{\text{phon}}} \rightarrow \mathbb{Z}^{N_{\text{phon}}}$$

$$x \mapsto x^2 \bmod N_{\text{phon}}$$

è usata per codificare gli importi versati sul credito telefonico.

Il generatore pseudo-casuale di numeri :

Il generatore pseudo-casuale (PRSG) genera una sequenza di bit da una stringa
chiamata seme. L'uso ripetuto dello stesso seme è in grado di riprodurre la stessa
sequenza.

Senza conoscere il seme, la sequenza che ne deriva è imprevedibile (per il protocollo
descritto di seguito, ciò vale sotto l'ipotesi che la fattorizzazione di numeri di grande
dimensione è complicata).

L'utilità di questo protocollo la si ritrova nella composizione stessa del denaro elettronico. Infatti il credito elettronico lo si può vedere come una sequenza di bit, suddivisa in blocchi ciascuno costituito da un numero sufficiente di bit pseudo-casuali. Alla procedura di generazione, se ne affiancano naturalmente altre che impediscono che uno stesso blocco venga generato e quindi speso due volte.

Riguardo poi ai protocolli specifici utilizzati per i portafogli realizzati in forma di smart card (sistema a ed a +) ed in forma di calcolatrice tascabile (sistemi Γ) :

- **rec_atomics** : esegue il ripristino delle azioni atomiche (azioni che possono essere interrotte solo in un modo ben definito).
- **reset** : ripristina il portafoglio e si effettua prima di qualsiasi altro protocollo o azione in fase di avvio
- **get_info** : inoltra i valori dei parametri pubblici al terminale. Questo permette al terminale di recuperare le informazioni necessarie per l'esecuzione dei protocolli successivi o dal database del terminale o dal portafoglio.
- **authenticate** : esegue una reciproca identificazione del portafoglio ed emittente.
- **write_cu_tbl**: consente alla banca di fornire il portafoglio con una tavola di nuova moneta corrente
- **gen_cheque** : genera e memorizza nuovi controlli nel portafoglio
- **show_currencies** : inoltra le informazioni sul saldo dall'osservatore al terminale. Se il portafoglio non ha capacità di visualizzare informazioni per l'utente, deve essere usato un display su un terminale.
- **payment** : esegue un trasferimento dal portafoglio alla cassa
- **rec_payments** : esegue il ripristino dei pagamenti interrotti
- **recovery** : esegue il ripristino del valore della valuta memorizzate nl portafoglio
- **PIN** : protocollo di gestione del controllo degli accessi al portafoglio e di blocco dello stesso
- **unlock_amt** : esegue uno sblocco protetto dal PIN nel portafoglio, di un importo specificati dal debitore
- **trasfer** : effettua un trasferimento di valore dall' osservatore gamma a quello alpha
- **rollback**: recupera un protocollo di trasmissione interrotto
- **get_certif** : inoltra chiavi e certificati necessari durante un pagamento alla cassa
- **update** : si compone di due parti ed ognuna aggiorna uno specifico certificato di chiave pubblica proveniente dall'emittente
- **deposit** : trasporta la moneta elettronica dal beneficiario all' acquirente

In aggiunta a questi, per i sistemi implementati a+ si aggiunge il protocollo **load_cheque** che carica un controllo generato in precedenza da un osservatore.

Requisiti minimi di sicurezza:

L'analisi dei protocolli di sicurezza si basa su alcuni presupposti generali quali la resistenza alla manomissione dei dispositivi usati e le relazioni di fiducia. Per l'integrità ogni ruolo si fida solo di se stesso. Per la privacy il debitore si fida della parte della borsa riguardante il portafoglio, ma non dell'osservatore. Si presume quindi che la stazione di ricarica della banca e la cassa del beneficiario del pagamento, siano affidabili. Questo può essere assicurato da misure standard nelle implementazioni dei protocolli. Inoltre si assume che il rilevamento di un errore anche minimo, sia sufficiente alla borsa per non deviare dal suo protocollo, se questo non si interrompe.

Requisiti richiesti dalla banca :

- **Autenticità degli assegni** : nel protocollo *deposit* l'acquirente accetterà solo assegni che sono stati correttamente emessi.
- **Limitazione sul valore** : è impossibile cambiare l'importo massimo del protocollo *max_pay(cu)*, (protocollo che calcola il massimo del saldo).
- **Conservazione del valore** : se il beneficiario deposita un importo ricevuto con un assegno c , può poi usare c per pagare una unica transazione.
- **Correttezza dei tassi di cambio** : il beneficiario può depositare un assegno corrispondente solo al tasso di cambio convalidato dall' acquirente.
- **Impossibilità di un doppio deposito** : l'acquirente accetta al massimo una transazione di deposito dello stesso assegno.
- **Massima integrità** : assumiamo che l'osservatore sia a prova di manomissione. Il pagamento è possibile solo se il quadro monetario è valido e il beneficiario riceve solo i soldi se il quadro della valuta viene addebitato in modo appropriato. Così, dovrebbe essere il trasferimento da un portafoglio Γ a un portafoglio a . Nel trasferimento una unità a , l'osservatore aumenta il saldo corrispondente nella tabella di valuta, di a e non di più. La cooperazione dell'osservatore è necessaria per il pagamento e il trasferimento, e deve essere impossibile costringere l'osservatore

a trasferire un valore negativo, ovvero il sistema Γ richiede che l'osservatore nei portafogli sia a prova di manomissione

- **Identificazione di chi commette la frode** : se un assegno viene versato in due rate differenti, l'emittente deve essere in grado di dimostrare l'identità del pagatore se entrambe le rate sono depositati.

- **Massima integrità durante il recupero** : se gli osservatori sono resistenti alle manomissioni, un pagatore, tramite il protocollo di recupero, non può recuperare più soldi, di quanti ve ne sono in realtà rimasto nel portafoglio. Inoltre, se viene interrotto un recupero di pagamento, il contribuente può recuperare l'importo pagato se il beneficiario non lo ha depositato.

- **Retro-integrità durante il recupero** : il pagatore non può recuperare dalle transazioni soldi in quantità superiore al saldo totale, presente dopo l'ultimo ritiro. Inoltre, nel recupero di una transazione di pagamento interrotta, il pagatore può tornare al più il valore iniziale o massimo dell'assegno.

Requisiti richiesti dal pagatore :

- **Disponibilità di recesso** : è possibile ritirare i soldi se il conto del pagatore contiene denaro sufficiente e il massimo ritiro dal portafoglio non è stato raggiunto.

- **Disponibilità di scambio** : Durante il ritiro, è possibile trasferire valore da un saldo di una valuta a un altro. Se un saldo è pari a zero questa voce può essere sostituita da un altro tipo di valuta.

- **Disponibilità di trasferimento** : il contribuente può in qualsiasi momento di trasferire qualsiasi somma dal portafoglio di una scheda collegata intelligente. Il saldo del ricevitore dovrebbe aumentare esattamente di questo importo.

- **Disponibilità di recupero** : l'interruzione di un protocollo non deve tradursi in una perdita di denaro per il pagatore. Inoltre, se il portafoglio viene perso, rubato o è malfunzionante, il pagatore deve poter recuperare il denaro ivi contenuto.

- **Fungibilità** : Poiché il numero massimo di pagamenti è chiaramente limitata al numero di denaro disponibile, può essere applicata ai protocolli CAFE solo un tipo limitato di fungibilità : per un certo parametro k , che definisce il ritiro, un pagatore può fare una sequenza finita di k pagamenti in qualsiasi valuta finché i rispettivi saldi non si esauriscono e fintanto il massimo ritirabile, non viene superato, sempre per qualsiasi valuta.

Inoltre un contribuente richiede almeno i seguenti elementi del sistema di pagamento:

- **Autorizzazione di operazioni** : n denaro può essere ritirato dal suo conto senza la cooperazione del debitore. In caso di contestazione l'emittente deve fornire una prova che il debitore ha riconosciuto un ritiro dato. L'emittente non può fare una prova senza la cooperazione del debitore. Più in generale qualsiasi cambiamento della quantità di soldi nel portafoglio dovrebbe essere accompagnato da un credito corrispondente un debito, ovvero un cambiamento di conto del pagatore. Allo stesso modo lo scambio avviene solo se il debitore riconosce i tassi delle valute

e gli importi. Operazioni di pagamento e trasferimento hanno bisogno di una qualche forma di autorizzazione. Si possono quindi distinguere due tipi di protezione:

(a) Memorizzare informazioni segrete necessarie per effettuare la spesa, nell'osservatore

(b) Memorizzare informazioni segrete riguardanti il debitore (es. PIN), nel portafoglio

- **Assenza di inquadatura** : non è possibile costruire una prova della doppia spesa, se ciò non è avvenuto.

- **Privacy.**

Al fine di consentire i pagamenti anonimi si distinguono 2 livelli :

1. Anonimato: il contribuente può fare i pagamenti in forma anonima.
2. Unlinkability: le operazioni di pagamento effettuate del pagatore non possono essere collegate le une alle altre o a prelievi corrispondenti.

Requisiti richiesti dal beneficiario :

- **Valute accettabili** : il beneficiario può determinare la scelta di valute accettabili in un'operazione di pagamento.

- **Proprietà del deposito** : il valore di un pagamento effettuato a un beneficiario deve poter essere accreditato sul conto del beneficiario.

- Un beneficiario può sconfessare una falsa dichiarazione di doppio deposito.

Sicurezza del sistema a :

Requisiti della banca :

Def.: siano $(\pi_1, \pi_{2i}) \in G_q \times G_q$ e $(\pi_3, r, c, c_{3-i}) \in G_q \times Z_q \times Z_q \times Z_q$, con $i = 1, 2$. Un assegno valido è una coppia (π_1, π_{2i}) , insieme a (π_3, r, c, c_{3-i}) , tale che $\pi_1 \neq 1$, $c = H(\pi_1, \pi_3, c_1, c_2, a, b)$ con $c_i = H(\pi_{2i})$, $a = G_C^r P_C^r$ e $b = \pi_1^r \pi_2^c$.

- **Autenticità di assegni validi** :

se si ha un assegno (π_1, π_{2i}) valido (ovvero accettato nei pagamenti e nei depositi), allora quest'assegno è stato ritirato dal portafoglio α , tramite la chiave pubblica p_s , tale che $\pi_1 = (p_s h)^{\sigma_3}$, con σ_3 numero scelto dall'osservatore.

- **Limitazione sul valore** :

la quantità $\text{max_pay}(cu)$ (massima quantità di denaro) è un parametro pubblicamente noto, tale che la banca rifiuta il deposito di un pagamento con valore superiore a tale quantità.

- **Conservazione del valore** : Il valore di un pagamento è incluso nella firma (*data da* : l'assegno valido (π_1, π_{2i}) , la sua autenticazione (π_3, r, c, c_{3-i}) , *m* ovvero il valore della funzione hash che ha come entrate l'identità del beneficiario e la somma pagata, p_1, p_2 t.c. $g^{p_1} h^{p_2} = \pi_1 \pi_{2i}^{-m}$) che è fatta dall'osservatore. I messaggi del protocollo di pagamento tra il portafoglio e la cassa costituiscono la registrazione del deposito.

È praticamente impossibile per un nemico produrre una registrazione di deposito valida per uno stesso assegno valido (π_1, π_{2i}) , anche se il deposito di quest'ultimo è già stato registrato, anche perché la registrazione di un nuovo deposito può avere solo due possibili forme:

- stessa m (firma), ma diversi ingressi alla funzione hash;
- m diversa da quella data nella registrazione precedente.

- **Correttezza dei tassi di cambio** :

il tasso di cambio è fissato dalle seguenti quattro protocolli, firmati e quindi assicurati dall'osservatore:

- pay_fro : definisce l'importo da pagare nella valuta del pagatore,
- pay_to : definisce l'importo da pagare nella valuta del beneficiario,
- cu_to e cu_fro : definiscono i codici ISO di entrambe le valute.

- **Doppio deposito** : è soddisfatto dalla definizione dei processi di compensazione.

- **Integrità forte** : Informalmente significa che sotto l'ipotesi di resistenza alla manomissione dell'osservatore α , la quantità di denaro che è prelevata, non superi, l'ammontare depositato. Ciò poiché l'osservatore α , è codificato per diminuire l'equilibrio del saldo, tramite il protocollo cu_tbl , di una cifra pari all'importo pagato, quindi il contatore dell'osservatore α , può essere aumentato solo quando viene prelevato un importo dall'emittente, e l'aumento è pari alla quantità di denaro che la banca addebita sul conto del pagatore.

- **Falsificazione dell'identificazione** : sono definibili dei meccanismi di tracciabilità della moneta che possono essere usati per dimostrare l'uso fraudolento della valuta. Inoltre, questo meccanismo permette anche alla banca di creare una lista nera, in modo che non possano essere fatti nuovi prelievi. Si noti che dal punto di vista crittografico, la banca può solo dimostrare che una parte di un assegno è stato speso almeno due volte, e non può mai dimostrare a terzi che è stato speso, per esempio, mille volte.

- **Integrità forte durante il protocollo recovery** : è facile vedere che questo protocollo non aggiunge nulla ai protocolli esistenti che possono influenzare la sicurezza della banca. L'unica modifica è che durante l'inizializzazione il debitore riceve la sua parte del seme iniziale utilizzato dal portafoglio per ritirare e spendere assegni. Tuttavia, una parte del seme iniziale della banca, rimane sconosciuto per l'utente in modo che il seme effettivamente utilizzato in ritiro e pagamento degli assegni non risulti essere noto. La conoscenza del seme implicherebbe infatti, la conoscenza di tutte le scelte casuali effettuate dal portafoglio e quindi della chiave segreta del portafoglio stesso.

- **Integrità retroattive durante il protocollo recovery** : Se il portafoglio ausiliario che è stata inizializzato per il recupero, è rotto, un aggressore può facilmente inoltrare identificatori di assegni falsi alla banca. Questo problema può essere evitato se la banca mantiene le trascrizioni dei ritiro più recente fatto dal portafoglio. Quindi durante ogni prelievo non solo si controlla π_1 , ma tutte le informazioni c_0 di validità del prelievo per verificare se si adattano alle informazioni memorizzate durante l'ultima operazione.

Requisiti del pagatore :

- **Revoca dell'autorizzazione** : nel sistema α non vi è alcuna possibilità di controllare la quantità di denaro ottenuta durante il prelievo. Pertanto, un PIN viene utilizzato solo per autorizzare il ritiro. Per prevenire le frodi dalla stazione di ricarica, si può mettere una minore quantità di denaro nel portafoglio di addebitato, dal conto del pagatore, o non accreditando l'importo trasferito dal portafoglio, così la banca deve essere in grado di dimostrare che l'importo in un estratto conto corrisponda realmente ai cambiamenti nel portafoglio. Per questo si assume che le stazioni di ricarica ad ogni protocollo `seq_no` ed `write_cu_tbl` firmino lo stato di ricevuta autenticazione. Il contribuente deve inserire il PIN ad ogni operazioni di prelievo.

- **Autorizzazione di pagamento e trasferimento** : il pagatore può bloccare determinate quantità di soldi, ciò significa che i pagamenti sopra una certa quantità richiedono l'uso di un codice PIN. È anche possibile bloccare parte del saldo. In particolare, il pagatore può scegliere di bloccarlo tutto. Quindi tutti i pagamenti saranno protetti da PIN. In caso di perdita del portafoglio, esso sarà segnalato come mancante e sarà iscritto nella lista nera. Solo quantità sbloccate possono essere spesi senza il codice PIN.

- **Privacy** : nell'analisi della privacy del pagatore non consideriamo l'identificazione fisica del portafoglio (né dell'individuo) che può essere facilitata da segni speciali per il portafoglio, quali le informazioni in rilievo e simili, ma l'identificazione dalle informazioni legate al portafoglio ed al proprietario del portafoglio. Per prima cosa, si può verificare che la privacy del pagatore è soddisfatta, osservando che il portafoglio non si identifica, quindi non rilascia informazioni, se non sa che sta comunicando con la banca dell'ordinante. Pertanto il ritiro della somma inizia con l'identificazione della stazione di ricarica stessa, al portafoglio mediante una firma di Schnorr data su richiesta casuale dal portafoglio. La richiesta casuale per questa firma impedisce il riutilizzo della firma stessa.

Inoltre, si ha che un pagamento con un assegno non contiene alcuna informazione sul portafoglio di chi ha ritirato l'assegno, né circa il debitore a meno che l'assegno risulta come una doppia spesa. Così nessuna connessione può essere stabilita tra l'identità di un ordinante e un pagamento, data la conoscenza della banca e beneficiario.

Requisiti del beneficiario :

- **Proprietà del deposito** : col portafoglio α , si ha che il messaggio firmato dallo stesso non può essere modificato e che ID_P , ovvero l'identità del beneficiario è contenuta in quel messaggio (tramite la funzione hash H). Poiché la banca farà un accredito solo sul conto corrispondente a una determinata identità, ne consegue che l'importo di un pagamento che è stato fatto per un beneficiario sarà depositato sul suo conto. Inoltre per evitare che l'assegno stesso venga utilizzato in più di un'occasione con lo stesso beneficiario, è possibile attuare con i dati del beneficiario, firmati dal portafoglio tramite la funzione hash un'unica transazione.

- **Diniego di false accuse** : Sebbene non sia specificato nel sistema α , esiste una protezione crittografica contro le false accuse di doppio deposito che la banca potrebbe portare avanti nei confronti di un beneficiario. Questa funziona come segue : sia E la procedura usata adeguatamente. Nel protocollo di pagamento, il beneficiario sceglie un numero casuale r , calcola $E(r)$ e invia $E(r)$ al portafoglio α . Il portafoglio include allora $E(r)$ nella m scelte che deve firmare. Nel deposito di pagamento, il beneficiario presenta il pagamento alla banca, la quale dopo aver dichiarato che il pagamento non è stato depositato prima, accetta di svolgere l'operazione di rilascio dei soldi. Nel caso in cui la banca dovesse rifiutare falsamente il deposito, il beneficiario potrà esigere che essa rispetti il pagamento. Questa estensione può essere facilmente aggiunta alle specifiche del sistema.

Integrità dei protocolli Γ :

Integrità della banca :

- Integrità forte :

La valutazione dell'integrità forte può essere suddivisa in due parti principali :

- la valutazione del ritiro di importi

- la valutazione di pagamenti o trasferimenti di importi

Il ritiro di un importo è costituito dai seguenti tre fasi :

- identificazione della banca da parte del portafoglio
- identificazione dell'osservatore da parte della banca
- aggiornamento della tabella di valuta nell'osservatore resistente alla manomissione.

Affinché l'integrità sia forte l'operazione di ritiro di un importo deve soddisfare le seguenti condizioni :

- Il tipo di firma che dice ad un osservatore di dichiarare la nuova tavola di valuta (protocollo cu_tbl), deve essere valido e deve esser dato solo dalla banca come detto al precedente punto 3
- Tale firma deve solo stimolare l'osservatore ha completare con successo l'aggiornare del suo cu_tbl. L'importo netto dell'aumento dei saldi del cu_tbl deve essere esattamente l'importo addebitato sul conto corrispondente.
- Tale firma può essere utilizzato solo una volta

I requisiti di integrità forte nelle operazioni di pagamento e di trasferimento che devono essere soddisfatti, sono i seguenti quattro :

- Il pagamento e il trasferimento deve essere possibile solo se il cu_tbl è valido, in modo da essere sicuri che il ritiro ha avuto luogo con validità.
In *payment* e *transfer* (protocolli di pagamento e trasferimento) la validità del cu_tbl è controllato dall'osservatore.
- Il beneficiario, o il α portafoglio possono solo ricevere soldi, se il cu_tbl addebita l'importo corretto.
- La cooperazione dell'osservatore è necessario nei protocolli di *payment*, *transfer* e *rollback*.
- Dall'osservatore non deve essere permesso l'addebito di saldi negativi.

Integrità del pagatore :

l'integrità del pagatore è protetta come segue :

- **Autorizzazione del ritiro:** per poter ritirare i soldi si ha bisogno di una chiave segreta (in questo caso quella dell'osservatore), e del PIN dell'utente (controllato dall'osservatore steso). Risulta quindi che solo il proprietario del portafoglio può effettuare un prelievo, avendo anche la possibilità di vedere il nuovo cu_tbl prima di inviare il suo PIN all'osservatore (consentendo in tal modo il ritiro), l'utente è in pieno controllo della nuova cu_tbl.
- **Autorizzazione dello scambio** : lo scambio che avviene durante un ritiro, è protetto con lo stesso mezzo del ritiro ordinario. Per quanto riguarda lo scambio durante il pagamento, vi si applicano le stesse protezioni dei pagamenti.
- **Autorizzazione di pagamento / trasferimento** : l'integrità del contribuente nei protocolli payment e transfer, è data ed implementata dal fatto che l'utente può controllare quantità e tariffe prima di autorizzare la transazione.
- **False prove di doppia spesa** : una prova di spesa doppia richiede la chiave segreta dell'osservatore. Un corretto pagamento non permette che la chiave venga calcolata. La sicurezza contro tali false accuse dipende in larga misura dalla gestione delle chiavi e dall'inizializzazione degli osservatori, poiché non essendo la chiave nota, non è possibile produrre prove.

I requisiti di privacy sono divisi in due :

- **Non-tracciabilità** : nemmeno con una collusione tra la banca e tutti i beneficiari si può esser in grado di identificare due pagamenti, realizzati con due assegni diversi, fatti dallo stesso portafoglio, con una probabilità significativamente maggiore di quella che si avrebbe se si tentasse di indovinare a caso.
- **Anonimato** :
 - nemmeno con una collusione tra la banca e tutti i beneficiari si è in grado di identificare un dato pagamento, eseguita da un portafoglio privato, con probabilità significativamente maggiore di quella che si avrebbe se si provasse ad indovinare a caso;
 - come risultato dell'esecuzione del protocollo *rec_payments* (registrazione di pagamenti), la banca è solo in grado di risalire al massimo a uno dei pagamenti fatti.
 - come risultato dell'esecuzione del protocollo *recovery*, la banca è solo in grado di rintracciare i pagamenti fatti dopo l'ultima estrazione.

L'utilizzo della firma digitale e la gestione delle chiavi nel sistema CAFE :

Un importante obiettivo di progettazione per il sistema di pagamento CAFE, è quello di mantenere al minimo la necessità di contatto e possibile collusione tra i soggetti che partecipano alla transizione. Per

questo fine ci si basa, per verificare le transazioni, sull'utilizzando di molti tipi di firme digitali. L'integrità e l'autenticità dei parametri di gestione delle chiavi stesse sono ottenute e certificate da una gerarchia presente tra le entità, che si sviluppa su tre livelli.

Un'autorità di certificazione userà la sua firma digitale per rilasciare un certificato sul valore di un parametro concatenato con altri dati come nomi di entità e periodo di validità.

In un sistema aperto come il sistema di pagamento CAFE, è praticamente impossibile richiedere che tutte le entità funzionali memorizzino tutte le chiavi e i parametri di cui hanno bisogno. Molti set di chiavi e parametri sono si ritrovano quindi sotto forma di certificati.

Per iniziare una transizione, l'iniziatore della stessa, su richiesta invia i certificati ad altri soggetti che partecipano alla transazione.

Nel sistema di gestione delle chiavi, le chiavi e parametri sono posseduti e controllati da entità funzionali. La distinzione riguardo la proprietà delle chiavi è importante per osservatori, poiché essendo un osservatore è di proprietà di un emittente, ma sotto il controllo fisico di un debitore, si avrà che la borsa del pagatore impedirà all'osservatore di inviare alcuna informazione non richiesta comprese le informazioni sulle chiavi delle altre entità controllate dall'emittente.

Ecco una breve descrizione dei ruoli presenti nel sistema di gestione delle chiavi :

- **Operatore di sistema** : un singolo operatore di sistema è responsabile della generazione dei valori dei parametri per l'intero sistema.
- **Autorità centrale di certificazione** : una singola autorità centrale di certificazione costituisce il livello superiore della gerarchia di certificazione del sistema CAFE. Questa autorità deve essere considerata attendibile da tutti gli altri ruoli.
- **Autorità di certificazione reale** : più autorità di certificazione reale, costituiscono il secondo livello della gerarchia di certificazione CAFE. Tali autorità sono autorizzate dall'autorità di certificazione centrale e deve essere considerato attendibile da tutti i ruoli.

- Directory : un data base per l'archiviazione sicura delle chiavi pubbliche e dei parametri con certificazione, a cui accedere in seguito da altri soggetti del sistema di gestione delle chiavi, ad esempio, per l'aggiornamento o in caso di controversia.
- Emittente : esistono più emittenti di moneta elettronica, ed ogni emittente è associato uno ed una sola autorità di certificazione reale.
- Acquirente : esistono diversi acquirenti di moneta elettronica ,ed ogni acquirente è associato ad una sola autorità di certificazione reale.
- Sistema di compensazione : Il sistema di compensazione esegue la convalidazione finale degli assegni così come regola il saldo tra emittente e acquirente.

Sono state inoltre introdotte alcune nuove entità funzionali, poiché l'emittente e il debitore controllano rispettivamente diversi tipi di osservatori e portamonete. Di seguito si descrive come alcune delle entità funzionali si riferiscono al sistema di gestione delle chiavi :

- borsello : questa è la parte del portafoglio controllata dall'ordinante. Ogni borsa è associato ad un unico ordinante, un osservatore e un emittente ed è ritenuta attendibile dal pagatore.
- Osservatore : questa è la parte del portafoglio controllata dall'emittente. Ogni osservatore è associato ad un unico borsellino, un pagatore e un emittente. L'osservatore come già detto, è incapsulato in un dispositivo resistente alle manomissioni; esso è un dispositivo di fiducia dell'emittente e tipicamente è un chip della smart card.
- Borsa ausiliaria : questa entità funzionale sostituisce la borsa originale del pagatore nel corso di una operazione di pieno recupero, dopo la perdita di un portafoglio. L'ente può essere funzionalmente equivalente ad una borsa normale o può essere una borsa speciale di recupero utilizzata solo durante l'esecuzione dell'operazione stessa di recupero. Questa entità è considerato attendibile dal debitore.
- Osservatore ausiliario : questa entità funzionale sostituisce l'originale osservatore del pagatore nel corso di una operazione di pieno recupero dopo la perdita di un portafoglio. Tale soggetto può essere funzionalmente equivalente ad un osservatore normale o può essere un osservatore speciale di recupero utilizzato solo durante l'esecuzione dell'operazione di recupero. Questa entità è considerato attendibile da parte dell'emittente.
- Borsa affiliata : ogni portafoglio Γ può avere un portafoglio α affiliato. Questo è la parte della borsa di questo portafoglio affiliato. Essa è ritenuta attendibile dal debitore che controlla il portafoglio α .
- Osservatore affiliato : questa è la parte di un osservatore di un portafoglio α affiliata ad un portafoglio Γ . È un ente di fiducia dell'emittente.
- Stazione del pagatore : questa entità funzionale è utilizzata dal pagatore per conservare le informazioni relative al portafoglio, al di fuori del portafoglio stesso.
- Cassa : una cassa può ricevere pagamenti da un portafoglio. Ogni cassa è associata a un beneficiario ed a un acquirente.
- Produttore : questa entità controlla la produzione degli osservatori.

L'autorità di certificazione centrale costituisce il livello superiore della gerarchia di certificazione. Questa entità certifica i parametri per l'intero sistema. Il livello successivo contiene una serie di autorità di certificazione reale. Queste autorità certificano le chiavi e parametri generati dagli enti principali del sistema di pagamento, come gli osservatori dell'emittente, le stazioni e i portamonete. Le entità principali del sistema di pagamento CAFE si trovano al livello più basso della gerarchia di certificazione. Queste entità generano chiavi e parametri necessari per l'esecuzione dei protocolli di pagamento connessi, come autenticazione dei valori intermedi e dei messaggi. Se la chiave di verifica dell'autorità di certificazione reale, non è stato memorizzato, il tasto verifica del certificato dell'autorità di certificazione centrale, è tenuta a verificare il certificato della chiave di certificazione reale. La chiave di certificazione dell'autorità di certificazione centrale, si presume sia caricata nella configurazione del soggetto. La gerarchia di certificazione CAFE è un caso particolare del sistema di certificazione X 509. La X 509 standard, presenta una struttura generale di certificazione, che può essere modellato come un grafo diretto che ha, come nodi gli enti, e le relazioni di certificazione come i bordi. Questo grafico si riduce ad un albero con un numero specifico di livelli presenti nel sistema di gestione delle chiavi CAFE.

La directory, da cui è eseguito il controllo d'accesso alle entità nonché la registrazione delle entità stesse, sarà accessibile da altri enti funzionali. La certificazione di una chiave di verifica di controllo di un emittente dovrebbe essere interpretata come una certificazione dell'emittente, di essere un membro del club CAFE in un determinato dominio. Come tale, la verifica di un beneficiario del certificato di verifica dell'assegno di un emittente, è un test sul saldo presentato che può essere previsto per

verificare l'acquirente. Si noti che questa certificazione non dà all'emittente il diritto di emettere moneta elettronica in una specifica valuta nazionale.

Si può anche introdurre un altro tipo di autorità reale, in modo che ve ne siano di due tipi :

-certificato bancario reale

-certificato di valuta reale

Un certificato di chiave di verifica di un assegno dell'emittente, deve poi essere in grado di contenere le firme digitali dei vari domini di certificazione.

Presentiamo ora le classi di chiavi e parametri che vengono gestiti dal sistema di gestione di chiavi del sistema CAFE. Alcune di queste classi sono introdotte da protocolli di pagamento, mentre altre sono il risultato del sistema di gestione delle chiavi stesse.

- **Certificazione centrale** : un unico centro di certificazione delle coppie di chiavi, costituisce la parte superiore della gerarchia di certificazione CAFE. Questa coppia di chiavi viene utilizzata per la certificazione delle chiavi per l'intero sistema e per la verifica delle chiavi per le autorità di certificazione reale.

- **Certificazione reale** : esiste un certo numero di coppie di chiavi di certificazione reale, che costituiscono il secondo livello nella gerarchia di certificazione. Queste chiavi sono utilizzati per certificare chiavi generate da entità funzionali direttamente coinvolti nei protocolli di pagamento.

- **Firma del sistema di compensazione** : esiste una coppia di chiavi del sistema di compensazione che serve per le firme sulla lista nere degli assegni spesi più di una volta.

- **Parametri di livello del sistema crittografico** : esistono un certo numero di parametri per l'intero sistema che definiscono specifiche proprietà dei sistemi crittografici utilizzati è richiesti dal sistema di pagamento stesso.
 - **Autenticazione dell'emittente** : una stazione di emissione utilizzerà questo tipo di coppia di chiavi per abilitare l'autenticazione dell'identità e dei messaggi.
 - **Firma di controllo dell'emittente** : una stazione di emissione utilizzerà questo tipo di coppia di chiavi per l'autenticazione degli assegni validi.
 - **Firma dell'osservatore** : un osservatore userà questo tipo di coppia di chiavi per l'autenticazione dei messaggi inviati dall'osservatore stesso. Questa chiave è anche utilizzato per identificare il pagatore associato con un particolare osservatore.
 - **Parametro condiviso** : vi è un parametro condiviso tra una stazione emittente e un portafoglio. Questi parametri possono essere calcolati solo dopo che è stata effettuata la verifica delle chiavi di firma dell'emittente e la verifica delle chiavi di firma dell'osservatore.
 - **Osservatore (parametri PRSG)** : questo tipo di parametro definisce il generatore pseudo-casuale della sequenza nell'osservatore.
 - **Borsello accecante** : un borsello ha una chiave privata utilizzata per verificare i messaggi “ ciechi ” inviati dall'osservatore nonché la corrispondente chiave pubblica per la verifica della correttezza degli stessi.
 - **Card di firma affiliata** : è simile alla chiave di firma osservatore, ma installato in una smart card affiliata al portafoglio.
 - **Parametri non crittografici** : sono presenti vari parametri di sistema che non hanno rilevanza crittografica. Questi parametri determinano limiti diversi, quali il valore più grande che può essere memorizzato in un portafoglio o l'importo massimo che può essere pagato in una transazione di pagamento unico.
- Tra i parametri non crittografici, ad esempio abbiamo i parametri max_pay , max_ticks e max_trans (che definiscono rispettivamente la

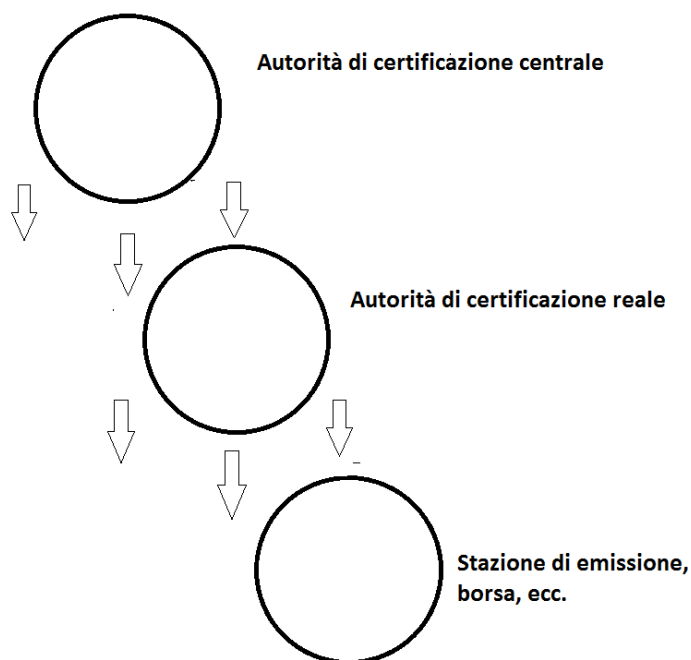
quantità massima di denaro che è possibile usare per gaare, che è possibile ritirare e che è possibile trasferire) .

- **Firma dell'acquirente** : sono le chiavi utilizzate dagli acquirenti per effettuare una serie di tassi di cambio.

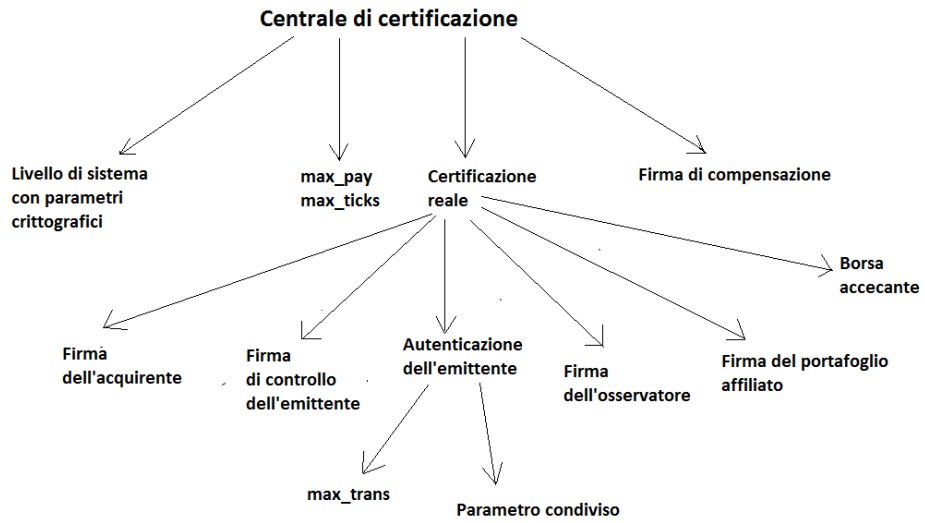
Entità funzionali e gerarchia del sistema di gestione delle chiavi :

Utenti, ruoli ed entità funzionali nel sistema di gestione delle chiavi

Utenti	Ruoli	Entità funzionali
Banca	Emittente	Stazione di ricarica Stazione di recupero Stazione di attivazione Osservatore Osservatore ausiliario Osservatore affiliato
	Acquirente	Stazione di acquisto
	Cancellatore	Sistema di cancellazione
Soggetti individuali che partecipano alla transazione	Pagatore	Borsello Borsello ausiliario Borsello affiliato Stazione di pagamento
	Beneficiario	Cassa
Amministratore	Gestore di sistema	Gestore di sistema
	Autorità di certificazione centrale	Autorità di certificazione centrale
	Autorità di certificazione reale	Autorità di certificazione centrale
	Directory	Directory
Fabbrica	Fabbricante	Fabbricante



Struttura della gerarchia del sistema di gestione delle chiavi



Ubicazione delle classi di parametri nella gerarchia di certificazione delle chiavi