

Net1 U.E.P.S. (Universal Electronic Payment System)

Net1

Net1 è il fornitore più importante di canali di transazioni tra aziende e individui con e senza conto corrente.

Nazioni sviluppate hanno molti networks sofisticati che forniscono cash machines, l'uso di carte di debito-credito nei punti vendita, pagamenti interbancari, e altri tipi di transazioni. Dal momento che il settore delle infrastrutture di telecomunicazioni è diventato sempre più veloce e affidabile, questi sistemi sono sempre più online e centralizzati, e la loro esistenza indebolisce il bisogno di introdurre nuove tecnologie crittografiche come le smartcards.

L'apertura delle economie che prima erano centralizzate nell'Europa dell'est, nell'India, America Latina, Africa, ha creato un aumento improvviso della domanda per banche moderne e metodi di pagamento a loro associati.




Ad ogni modo le telecomunicazioni sono un problema serio: decenni di negligenza hanno lasciato molti di questi paesi con pessime reti telefoniche, e i villaggi sono spesso senza alcuna connessione. Le linee che esistono sono spesso non abbastanza buone per supportare le comunicazioni modem: scambi manuali sono ancora diffusi. Le transazioni devono essere spesso effettuate off-line e, il rischio di frodi con carte contraffatte è dovuto al fatto che le tecniche con le carte standard con la banda magnetica ISO col PIN associato non possono essere usate.

D'altro canto questo problema è stato un'opportunità: questi paesi hanno saltato due generazioni di tecnologia di pagamenti elettronici, e hanno proseguito direttamente da sistemi manuali di contabilità a processi distribuiti basati su smartcards e portafogli elettronici. Ridurre i costi delle transazioni di un ordine di grandezza potrebbe favorire la crescita economica ed eliminare un serio ostacolo di sviluppo economico. Le povere telecomunicazioni in homelands e townships, più il bisogno di tenere i costi bassi, hanno portato naturalmente ad un approccio basato su portafogli elettronici. I soldi sono trasferiti tra cards bancarie, carte di clienti e di commercianti usando terminali off-line che possono essere portati se necessario.

Attraverso la tecnologia dei chip card e di sistemi come U.E.P.S., Net1 fornisce soluzioni di pagamento alternative per popolazioni con economie in via di sviluppo che non hanno, o in numero limitato, accessi ai servizi bancari tradizionali.

Net1 sviluppa, implementa e lavora condividendo Automated Teller Machines (ATM) / Point-Of-Sale (POS) sistemi di scambio e smartcards, borsellini elettronici, applicazioni su misura per permettere transazioni sicure e accessibili.

Inoltre U.E.P.S. si distingue dai competitori, fornendo soldi, assegni, carte di debito credito, e altre smart cards su cui si basano i sistemi di pagamento, nel seguente modo:

-  Non è richiesta nessuna o una piccola tecnologia o nessuna sicurezza in particolare per ridurre i costi e permettere l'effettiva proliferazione dei punti di commercio.
-  La rete del terminale può operare con o senza l'utilizzo di infrastrutture di comunicazione.
-  I protocolli crittografici di sicurezza permettono ai detentori delle carte di

ricevere istruzioni per caricare fondi, da una terza parte attraverso canali di comunicazione sicuri.

Tecnologia

Net1 si basa sul primo sistema di pagamento sviluppato, usando FTS Patents (Funds Transfer System – “sistema di trasferimento fondi”), chiamato U.E.P.S.

"Universal electronic payment system". È il primo borsellino elettronico commerciale mai lanciato. Il brevetto FTS descrive un metodo con il quale i fondi possono essere trasferiti da una smartcard ad un'altra in modo sicuro ed off-line.

Il termine “off-line” si riferisce alle transazioni che sono effettuate senza bisogno di contattare o comunicare con l'emittente nel momento della transazione, dal momento che sono le smartcards stesse a fornire le autorizzazioni richieste.

Il brevetto FTS descrive anche come le smartcards possono essere caricate o ri-caricate con dei fondi e come se ne può ritirare il valore in ambienti bancari e non. U.E.P.S. è un metodo pienamente integrato di transazioni elettroniche, con tutti i benefici dell'uso dei soldi ma con nessuno dei rischi connessi.

Può sostituire tutti i sistemi correnti di consegna finanziaria come banconote e monete, carte di credito e debito, scontrini e libretti di banca.

Utilizzando questa tecnologia brevettata, Net1 ha sviluppato e implementato una varietà di sistemi unici che aprono la porta a un-banked, under-banked and banked markets (mercati con conto corrente, senza, e che non dispongono di fondi per aprirlo), nelle economie emergenti su scala mondiale. Il sistema U.E.P.S. è stato progettato per eliminare mancanze premature incontrate in sistemi di pagamento di fondi elettronici e per migliorare lo stile di vita dei suoi clienti. Il sistema è facile da usare (user-friendly) e compatibile con tutti i sistemi bancari internazionali.

U.E.P.S. è un prodotto di transizioni di fondi elettronici utilizzato in paesi in via di sviluppo, dove la carenza di telecomunicazioni hanno reso le operazioni offline necessarie. Il sistema utilizza smartcards sicure e operative in tempo reale ma off-line. La sua capacità off-line permette ai titolari delle carte di effettuare transazioni con altri utenti in ogni momento e luogo.

È stato creato intorno a funzioni di portafoglio elettronico basato su smartcard: i soldi sono caricati dalla banca, attraverso carte di credito, alle customer card, poi alla merchant card, e infine nuovamente alla banca attraverso un clearing system (La clearing house o stanza di compensazione è un'infrastruttura di mercato che si pone come controparte nelle transazioni regolamentate. I "sistemi di regolamento su base netta" o clearing system, che elaborano o trasmettono, tramite computer, informazioni relative a clienti di banche diverse, comportano l'accumulazione di un certo numero di transazioni in modo da compensare il totale dei crediti con il totale dei debiti).

U.P.E.S. offre soluzioni outsourced capaci di gestire, su larga scala, pagamenti fatti verso riceventi senza conti bancari (outsourcing = contratto atipico con cui un cliente trasferisce ad un soggetto terzo giuridicamente autonomo, outsoucer, il compimento di una propria attività. Lo scopo di tale trasferimento è di contenere gli oneri finanziari e i costi di gestione e di migliorare la qualità dei servizi trasferiti.

In ambito informatico e bancario le attività che vengono "esternalizzate", ossia

trasferite, riguardano la gestione degli strumenti di pagamento elettronici). Ciò riduce costi amministrativi e di gestione dei soldi, facilita la gestione dello stato delle informazioni di pagamento e crea registri di transazioni verificabili per individui, agenzie di governo, datori di lavoro, commercianti e altri fornitori di servizi finanziari.

Net1 con U.E.P.S. permette la circolazione di soldi elettronici e promuove una economia non-cash (cioè promuove l'utilizzo di strumenti di pagamento elettronici in alternativa al contante).

U.E.P.S. "smart card transaction and settlement switching system", fornisce card payment system come un'alternativa ai soldi (cash), offre un sistema con un registro per l'iter di controllo che garantisce transparency, interoperability e longevity.

Il sistema NET1 è costruito intorno ad un set di hardware e software che insieme formano un meccanismo contiguo di transazioni e controllo dei pagamenti.

Il software gira principalmente su tre dispositivi: la smartcard, il dispositivo POS e il sistema di hosting (hosting = computer o terminale collegato ad una rete che controlla e gestisce dati e programmi a cui accedono tutti gli altri computer collegati alla stessa rete).

Quando un sistema è venduto ad un cliente Net1 offre tutto il software richiesto per utilizzare l'U.E.P.S, incluse le funzionalità per le smartcards, i dispositivi POS che permettono alle smartcards di effettuare transazioni tra di loro in modo off-line, e anche un sistema terminale che come funzione primaria registra e tiene traccia di tutte le transazioni effettuate.

U.E.P.S è un semplice meccanismo di consegna che gestisce il flusso di fondi tra fornitori di servizi finanziari (in genere una banca), clienti e venditori.

Tutte le transazioni gestite attraverso U.E.P.S. si verificano tra due carte presso Point-Of-Sale (POS), tutte le informazioni rilevanti necessarie per eseguire transazioni finanziarie si svolgono sulle carte, compresi i dettagli sui fondi a disposizione per la transazione del titolare della carta.

U.E.P.S. Banking

Net1 permette alle tradizionali istituzioni finanziarie di sorpassare le offerte dei competitori attraverso le innovazioni tecnologiche disponibili nelle soluzioni U.E.P.S.

Il sistema U.E.P.S. può operare come un sistema Stand-A-Lone per cui istituzioni finanziarie possono distribuire smart cards ai loro clienti come un conto corrente (Bank Account).

U.E.P.S. offre una varietà di opzioni per sicuri trasferimenti di fondi locali da un Sender a un Recipient (ricevente) utilizzando smart card technology.

I fondi sono inviati elettronicamente e in sicurezza usando biometric fingerprint identification per caricare i fondi sulla smart cards e lo spendere con le smart cards richiede lo stesso tipo di identificazione. Cash collections (ritiri dei contanti) sono nella forma di Cash Transfer Collections (ritiri di trasferimenti soldi) che permette ad una persona unbanked di ricevere soldi da un Sender usando the U.E.P.S.

Non-Cardholder Cash Transfer Collection installato presso impianti U.E.P.S. POS o ATMs. I titolari di carte che già hanno un conto bancario tradizionale esistente possono trasferire fondi alle loro smartcards dal loro conto e vice-versa.

Una caratteristica di pagamento permette ai cardholders di effettuare pagamenti elettronici once-off verso conti bancari di una "terza parte beneficiaria" (deposito di garanzia). Il pagamento once-off è un pagamento che non si verifica su base regolare; l'importo totale dovuto è versato in una sola volta, invece che ad esempio su base mensile, al fine di regolare i conti. Il cardholder seleziona l'opzione del menù Once-Off Payments su U.E.P.S. POS/ATMs ed entra nei dettagli del conto del ricevente così come il beneficiario possiede il numero di conto del titolare della carta.

Caratteristiche principali

- ✚ Affordability (Accessibilità): La maggior parte dei costi di transazione sono a carico delle organizzazioni che si avvalgono del canale, ci sono anche minimi canoni mensili fissi a carico dei titolari.
- ✚ Security (Sicurezza): La carta serve come un sostituto dei contanti, ma prevede la tolleranza per la perdita di smart cards ovvero: protegge il titolare della carta in caso di carte smarrite o rubate.
- ✚ Simplicity (Semplicità): un sistema di identificazione biometrica delle impronte digitali viene utilizzato dal titolare della carta per accedere alla card ed effettuare transazioni.

Sicurezza

L'esplosione del commercio elettronico (e-commerce) continua ad essere ostacolato dalle leggi di sicurezza, dal difetto della verifica e la riluttanza dei clienti a divulgare informazioni circa crediti instabili o conti di debito su internet.

Questa architettura è molto esigente dal punto di vista della sicurezza, e la sua protezione comporta una combinazione di fattori come la resistenza alla contraffazione delle smartcard usate; un sistema di contabilità, back-end (le interfacce utilizzate per l'amministrazione o manutenzione dell'apparato che eroga il servizio) che stabilisce le transazioni riportate da clienti e venditori nel giro di pochi giorni e dunque individua squilibri derivanti da modifiche o contraffazione di carte; e una modalità di elaborazione, fall-back (cioè un sistema di recupero dati andati persi), in cui, anche se il sistema di sicurezza elettronica è stato penetrato, le carte possono ancora essere utilizzate all'interno del sistema esistente di controllo. La sicurezza del sistema non dipende dall'hardware del terminale o dalle reti di comunicazioni che sono utilizzate per trasferire le informazioni.

Il protocollo di sicurezza è progettato in modo da prevenire frodi opportunistiche e far rispettare il corretto flusso delle transazioni.

Lo standard symmetric triple data encryption ("tripla criptatura simmetrica di ogni blocco"), o DES, è utilizzato moltissimo insieme ad un generatore di numeri casuali nativo che garantisce che tutte le transazioni siano eseguite utilizzando una coppia di chiavi di sessione casuali.

Ogni messaggio scambiato durante una transazione nomina ambo le parti coinvolte nella transazione, include informazioni uniche per garantire la "freschezza" e dipende esplicitamente da tutti i messaggi che sono avvenuti prima di esso.

La soluzione NET1 fa uso della gerarchia delle smartcard ognuna delle quali svolge una specifica funzione, come la carta del cliente, la carta del venditore, la carta

dell'agente, la carta del dipendente o una combinazione di queste, ma tutte incorporano una porzione critica del sistema di sicurezza complessivo.

Ad esempio, nel caso di sistemi multi-istituzione, i fondi garantiti su ogni banca dalla Central Bank, sarebbero resi disponibili ad un numero di smartcard.

Queste smartcard avrebbero la possibilità di trasferire parte dei fondi ad una carta di livello più basso, come uno sportellista di banca o la carta di un agente.

Queste a loro volta avrebbero la possibilità di trasferire i fondi al livello più basso di smartcard, ovvero le card dei clienti e dei venditori.

In qualsiasi momento durante la vita del sistema, la somma dei fondi di tutte le carte menzionate sopra dovrebbe essere uguale alla quantità dei fondi autorizzati dalla Central Bank.

Questo fatto è il primo controllo giornaliero eseguito dal sistema che garantisce che l'integrità del sistema non sia stata compromessa.

Ogni card nel sistema ha l'abilità di comunicare in modo sicuro con una card del livello ad essa direttamente superiore. Questo viene ottenuto attraverso la seguente procedura end-to-end ("da capo a piedi"). La soluzione end-to-end permette transazioni veloci, aumenta il controllo del cliente sul processo di pagamento, diminuisce i costi di transazione e aumenta la soddisfazione del cliente, consente di attuare un sistema di gestione centralizzata delle transazioni che fornisce l'avviamento dei pagamenti e gestisce segnalazioni di mancati pagamenti.

La sicurezza di U.E.P.S. è basata su due livelli di autenticazione.

Lo strumento base di pagamento è un assegno elettronico di controllo che è generato dalla client card, trasferito alla carta rilasciata e quindi attraverso un sistema centrale compensazione (clearing system), alla banca del cliente.

L'assegno ha due codici di autenticazione: uno generato con una chiave conosciuta solo dall'emittente del modulo di sicurezza della banca e alla carta cliente, e uno generato con una chiave controllata dall'ente di compensazione e caricato sulla carta prima che venga fornita alla banca.

Questo ultimo codice è controllato prima che i fondi siano accreditati al rivenditore che presenta l'assegno, mentre il primo è controllato solo in caso di controversia.

Se una tecnologia a chiave pubblica fosse stata disponibile nelle smart cards a basso costo, sarebbe stato possibile per il commerciante controllare la firma digitale sull'assegno attraverso la smartcard. Così è stato progettato un protocollo di transazione per ridurre al minimo la probabilità che assegni vuoti entrassero nel sistema. Questo è challenge-response protocol (protocollo sfida-risposta) attraverso cui entrambe le carte in ogni transazione si verificano a vicenda e portano avanti in sicurezza la sessione. Infatti il commerciante si "fida" di un'operazione che avviene nella smartcard del cliente, acquirente e negoziante devono "fidarsi" della banca anche se il negoziante non può verificare immediatamente l'assegno; questo garantisce l'autenticità dell'assegno elettronico.

Simili protocolli di transazione sono usati tra banche e clienti, e tra clienti e la stanza di compensazione, e l'utilizzo di meccanismi di sicurezza indipendenti (codici di autenticazione e protocolli sfida-risposta) permettono di soddisfare le esigenze di adattamento, elasticità: l'intero sistema non dovrebbe essere esposto alle frodi attraverso la compromissione di alcune chiavi o del dispositivo.

Questa è la teoria, tuttavia, nella realtà c'è spesso la possibilità che un errore di progettazione potrebbe lasciare aperto un buco che un utente malintenzionato potrebbe scoprire e sfruttare opportunisticamente.

Chiavi caratteristiche

La tecnologia U.E.P.S. Include funzionalità che permettono:

- Ⓜ Mutua autenticazione;
- Ⓜ Recupero automatico e trasparente;
- Ⓜ Cancellazione;
- Ⓜ Rimborsi;
- Ⓜ Iteri di controllo multipli;
- Ⓜ codice di firma a dieci cifre;
- Ⓜ Caricamento Off-line ;
- Ⓜ Identificazione biometrica;
- Ⓜ Debito Continuo;
- Ⓜ Portafogli multipli e ristretti;
- Ⓜ Credito automatico;
- Ⓜ Debito Automatico.

Ⓜ **Mutual authentication**

Per i pagamenti elettronici sono richieste tre autenticazioni:

- ✓ Autenticazione dell'acquirente dal terminale (per le smart card);
- ✓ Autenticazione del terminale da parte della carta (per evitare terminali fraudolenti);
- ✓ Autenticazione dell'assegno elettronico (Per assicurare il venditore).

Questo protocollo permette alle card di creare una chiave di sessione casuale basata su un generatore di numeri casuali nativo (nonce). Questa chiave di sessione varia per ogni singola transazione nel sistema, e dal momento che nessun dato chiaro è reso disponibile, il protocollo può subire solo l'attacco brute force (ovvero un attacco basato su tentativi casuali fatti "alla cieca", il che richiede molto molto tempo e raramente va a buon fine. Si tratta di controllare sistematicamente tutte le possibili chiavi fino a quando la chiave corretta è stata trovata).

Questo attacco viene prevenuto limitando il numero totale di transazioni che può essere effettuato da ogni singola carta durante il suo ciclo di vita.

Inoltre più è lunga la chiave da decifrare più è difficile decifrarla (Questo numero può essere diviso per 2^{56} per determinare il potenziale tasso di successo di un attacco su una specifica chiave di sessione. Inoltre, dal momento che due numeri casuali a 64-bit vengono scambiati durante il processo, il triplo algoritmo DES può essere utilizzato, aumentando tale numero per valutare il tasso di successo di un attacco brute force a 2^{112}).

Quando la chiave di sessione è stata stabilita questa verrà modificata ad ogni funzione di input o output di una delle cards coinvolte nella transazione. L'autenticazione è dunque eseguita da ognuna delle cards come parte intrinseca di ogni elemento di una transazione finanziaria.

La mutua autenticazione permette una ripresa automatica nel caso che la transazione fallisca a causa di problemi hardware o della prematura rimozione della carta del cliente o del venditore. Lo stesso meccanismo è applicato per gestire la cancellazione di una transazione, della transazione all'inverso e per gestire risarcimenti sicuri.

Le versioni delle chiavi possono essere intodotte a priori all'interno delle cards dei clienti se si considera la durata di vita media di una card e il numero di tentativi necessari per ottenere tramite brute force ogni diversificato set di chiavi.

Ogni client card contiene una loading key ("chiave di caricamento"), una session initiation key ("chiave di inizializzazione di sessione"), una chiave di smistamento e un set di chiavi di certificazione dell'emittente.

Questi certificati sono tutti mutualmente esclusivi, e dunque nessuna singola entità può frodare un'altra. Non c'è bisogno di nessun controllo per assicurare una transazione U.E.P.S attraverso una rete di telecomunicazione.

Questo è dovuto al protocolli end-to-end che come abbiamo descritto assicurano che gli attacchi non possano essere effettuati attraverso il monitoraggio, con la ripetizione o la modifica di alcun elemento delle transazioni U.E.P.S..

Ⓜ Transparent and Automatic Recovery

Questa caratteristica assicura che se una carta (di un cliente o di un venditore) viene rimossa dal terminale POS prematuramente, sarà possibile la risincronizzazione delle due carte e delle attività, come se la transazione non avesse avuto atto.

Questa caratteristica rimuove il bisogno di monitorizzare i lettori di card per prevenire la rimozione prematura di una card durante una transazione.

Ⓜ Transaction cancellation

Una delle funzioni più difficili e rischiose che dev'essere effettuata da un terminale POS è la cancellazione di una transazione. Questa può sorgere quando, per qualsiasi ragione, la somma della transazione è stata inserita in modo scorretto, o se il cliente cambia idea all'ultimo momento e decide di non procedere più con la transazione.

Cancellare una transazione implica che la carta del compratore debba essere risarcita. Questo è equivalente al caricare nuovi fondi nella card dell'acquirente, una funzione che può essere eseguita solo dall'emittente della card o dal suo agente (qualcuno che agisce per, o per conto di, un altro con la sua autorizzazione).

Nell'ambiente U.E.P.S., i fondi possono essere caricati utilizzando una card del venditore che sia stata attivata per agire anche come una card di un agente.

Le cards degli agenti sono tuttavia normalmente controllate da un numero limitato di persone, dal momento che i fondi sono di responsabilità del venditore o dell'agente partecipante. La funzione di cancellazione di una transazione permette il rovesciamento di qualsiasi transazione immediatamente dopo che essa sia avvenuta.

Questo significa che una transazione effettuata su un dispositivo POS possa essere cancellata senza alcun rischio per il compratore o il venditore, finquando non avvenga alcuna altra transazione prima che la cancellazione sia effettuata.

L'implementazione di questa funzione utilizza il meccanismo di recupero automatico descritto sopra.

Ⓜ Refunds

Quando la merce viene riportata al venditore, per qualsiasi ragione, è a discrezione del venditore se risarcire o cambiare la merce in questione.

Nel caso che venga concordato un risarcimento, il venditore in qualche modo deve essere in grado di risarcire il cliente. Questo può avvenire utilizzando denaro contante, un assegno o un trasferimento diretto di denaro sul conto del cliente. Nel caso delle smartcards, il cliente desidererebbe essere risarcito direttamente sulla sua card. Questo può essere ottenuto caricando la somma appropriata da una agent card gestita dal venditore. L'U.E.P.S. garantisce che questo tipo di transazione possa essere effettuata senza eccessivi rischi per il venditore.

Multiple audit trails for off-line U.E.P.S. Transactions

L'U.E.P.S, come sistema off-line, deve garantire che tutte le transazioni effettuate off-line vengano concluse, in un determinato momento, dal sistema back-end. Il saldo (“settlement”) è un punto critico per garantire che nessun fondo possa andar perso per i possessori di una card, anche nel caso in cui un terminale POS, la sua documentazione cartacea o la card del venditore vadano perdute, rubate o distrutte. In modo importante, tutte le transazioni tra smartcards hanno effetto finanziario sui bilanci individuali delle smartcard e devono quindi essere saldati per preservare l'integrità del sistema. La funzionalità di documentazione a più flussi dell'U.E.P.S è pensata per garantire che la smartcard erogata in sostituzione di una persa, distrutta, etc... contenga la giusta quantità di fondi.

L'U.E.P.S offre l'abilità di attivare la documentazione a più flussi (“multiple-stream audit trails”) attraverso il download dei profili dei terminali POS.

I multiple-stream audit trails sono distribuiti tra le smartcard attive e sono completamente trasparenti a tutti i possessori di card. Quando la smartcard di un cliente è inserita in un qualsiasi terminale POS per effettuare una o più transazioni, incluso saldo, carico, prelievo, credito automatico o debito automatico, la transazione corrente viene scritta sia sulla card del cliente, sia su quella del venditore.

La precedente transazione o gruppo di transazioni scritta sulla smartcard del venditore da un altro cliente viene scritta anche sulla smartcard del cliente che sta facendo l'attuale transazione. Questo processo garantisce che ogni transazione o gruppo di transazioni effettuati su una smartcard di un cliente venga distribuita direttamente su una seconda smartcard di un venditore e indirettamente su una terza smartcard di un venditore. Il terzo trasferimento avviene scrivendo la transazione o il gruppo di transazioni sulla smartcard di un altro cliente che trasferisce a sua volta la stessa cosa alla smartcard di un altro venditore. Il numero di stream può essere selezionato attraverso i profili del dispositivo POS o del venditore.

10-digit signature code

Il back-end system U.E.P.S. genera un unico ten-digit signature code per uno specifico importo da caricare su una smart card. La ten-digit signature code può essere applicata solo a quella smart card una volta ed essere influenzata soltanto da quella particolare carta.

Quando un ten-digit signature è presentato, in un qualsiasi dispositivo POS off-line, alla smart card per la quale è stato creato, il codice, dopo la convalida, permette di dar credito a uno dei suoi portafogli interni con la giusta quantità.

Quando i codici sono stati creati per una specifica smart card, questi possono essere presentati ad una smart card in un ordine diverso da quello in cui i codici sono stati creati.

📍 **Off-line loading**

Nelle economie in via di sviluppo e nei paesi che non godono di infrastrutture di telecomunicazione avanzate o affidabili, può rivelarsi difficile attuare sistemi che si basano in larga misura su autorizzazioni on-line.

Dal momento che i fondi non possono essere caricati alle carte in un modo semplice e universale, l'interesse per questi sistemi tende a morire in uno spazio di tempo relativamente breve.

U.E.P.S., tuttavia, permette ai fondi di essere distribuiti attraverso le infrastrutture esistenti come il servizio postale, telefoni fissi, telefoni cellulari e simili.

Il back-end system U.E.P.S. genera un unico numero a dieci cifre per un importo specifico da caricare su una carta specifica.

Questa 10-digit signature quando viene presentata la carta in un dispositivo off-line, dopo la convalida, consente alla scheda di accreditare i fondi richiesti nel suo portafoglio interno.

Questa funzione può essere usata per trasferire fondi a distanza per il pagamento di salari, pensioni, rimborsi, trasferimenti di terzi, etc.

📍 **Identificazione biometrica**

I sistemi di banda magnetica delle carte di credito e di debito disponibili oggi utilizzano una firma scritta o un PIN, nel tentativo di verificare l'identità del cliente e ridurre al minimo il rifiuto delle transazioni. Tuttavia i numeri o codici PIN possono essere invalidati, ovvero le bande magnetiche possono essere clonate oppure una carta può essere rubata insieme al suo numero PIN e può essere usata per fare transazioni finché non ne è denunciato il furto o finché i suoi limiti off-line non sono stati raggiunti. Il PIN e la carta possono anche essere utilizzati per accedere alle informazioni del conto e quindi per truffare ulteriormente il titolare vero e proprio della carta. Pertanto, la verifica offline del titolare della carta è fondamentale per garantire che un sistema di pagamento non effettua transazioni fraudolente.

Allo stesso tempo, il sistema deve garantire che le operazioni del titolare vero e proprio della carta non vengono respinte. Una forma alternativa di identificazione del cliente è rappresentata da supporti U.E.P.S. di dati biometrici sotto forma di riconoscimento delle impronte digitali. Scanner biometrici sono utilizzati per registrare immagini di impronte digitali di un cliente.

I modelli di impronte digitali che ne derivano, sono memorizzati nella smart card del titolare e utilizzati per l'identificazione ogni volta che la smart card viene utilizzata. Prima che una smart card sia rilasciata, si verifica il seguente processo di registrazione di impronte digitali:

- ✓ tutte le dieci dita vengono catturate con tre immagini di impronte digitali acquisite per ogni dito.
- ✓ Le tre immagini di impronte digitali per ogni dito sono consolidate e filtrate per creare l'immagine migliore per quel dito.
Ciò ha come risultato: dieci immagini di ottima qualità, una per ogni dito.
- ✓ Le dieci immagini delle impronte digitali sono segnate e utilizzate per generare i modelli delle impronte digitali. Un modello di impronta digitale è una rappresentazione geometrica unica di tale impronta.
- ✓ Il titolare della carta viene identificato tramite il confronto con questi modelli di impronte digitali; la più alta corrispondenza dell'impronta digitale

garantirà il migliore processo di riconoscimento e quindi l'accettazione del titolare. Questo processo aiuta ad eliminare le truffe in quanto si eseguirà istantaneamente il rifiuto di autenticare il titolare di carta in caso di un riconoscimento erraneo rispetto al modello delle impronte digitali (cioè non vi è compatibilità tra il modello e il reale).

- ✓ I modelli delle impronte digitali sono firmati da un "emittente smart card" e memorizzati su smart card del titolare della carta.

Quando una transazione viene eseguita, le impronte digitali del titolare della carta sono verificate paragonandole a quelle memorizzate sulla smart card.

Il processo di verifica avviene in una sessione sicura tra la smart card e il lettore di impronte digitali. Durante la fase di verifica viene utilizzata una moderata soglia corrispondente ai modelli, per compensare le variazioni delle condizioni di impronte digitali del titolare.

Questa funzione di identificazione biometrica è stata progettata per proteggere i titolari di carta contro le frodi, aiuta ad eliminare il ripudio delle transazioni e riduce la complessità associata a sistemi di gestione delle tessere e il costo dei sistemi utilizzati per trattare con carte rubate e perse.

🔒 **Debito continuo**

La caratteristica di addebito continuo dei U.E.P.S. elimina la necessità dei clienti di acquistare unità prepagate, consentendo loro di utilizzare le proprie smart card per pagare questi servizi come e quando ne hanno bisogno. Tutto quello che un cliente deve fare è di inserire la sua smart card nelle apparecchiature apposite e la smart card addebiterà a se stessa ogni volta che una unità di servizio viene utilizzata.

La caratteristica di debito continuo fornisce una significativa flessibilità finanziaria per i clienti e può essere su misura per essere utilizzato in qualsiasi ambiente "pay as you go" (paga mentre vai), compreso l'accesso a Internet. Operazioni di addebito continuo sono tipicamente un gran numero di piccole operazioni che possono riempire rapidamente lo spazio su un file di transazione di una smart card.

Il problema è stato eliminato progettando U.E.P.S. per ridurre al minimo lo spazio del file che queste operazioni richiedono, ovvero consentendo alle operazioni successive di svolgere sostituzioni e aggregazioni con le operazioni fatte in precedenza, in modo da trattare transazioni multiple come una transazione globale.

🔒 **Portafogli ristretti e multipli**

Grazie alla caratteristica di portafoglio multiplo di UEPS i titolari possono utilizzare la loro smart card per gestire i loro bilanci. Fino a 255 portafogli per titolare possono essere configurati e attivati sulla memoria elettricamente cancellabile e programmabile a sola lettura, o EEPROM, disponibile sulla particolare smart card.

Ciascuno dei portafogli può essere configurato per soddisfare le specifiche esigenze del titolare della carta, e può essere utilizzato per interessi che generano risparmi, utilità pre-pagate, ordini di gestione dei farmaci, credito e di debito, e per molti altri fini.

Inoltre, un portafoglio può essere protetto o no. Portafogli protetti richiedono la verifica biometrica del titolare della carta per effettuare transazioni.

Portafogli non protetti sono normalmente utilizzati per operazioni di piccolo importo come il trasporto (di denaro su una carta) per il quale la velocità di elaborazione è critica (minima). Dal momento che l'iter di controllo di tutte le transazioni effettuate dai portafogli attivi è memorizzata sul file di storia della smart card, i titolari della carta possono fornire a terzi un rapporto completo delle loro storie di transazione, che

può attestare pagamenti, quali premi di assicurazione e dimostrano un regolare flusso di reddito dai salari o altre fonti. I portafogli possono anche essere limitati.

Portafogli con restrizioni consentono alle operazioni di essere eseguite solo presso i commercianti specifici. Per esempio, se un datore di lavoro desidera sovvenzionare i costi di trasporto di un dipendente, un portafoglio, che può essere configurato, consente al titolare di passare solo il valore, caricato in quel portafoglio, di specifici punti ovvero quelli di trasporto. Portafogli con restrizioni possono essere utilizzati anche dai governi per prevenire l'esclusione dei beneficiari dalle sovvenzioni sociali da utilizzare per pagamenti di particolari beni o servizi.

Credito automatico

Questo comando di credito automatico consente alla client card U.E.P.S. di accreditare se stessa automaticamente con un pre-configurato importo su un'informazione specifica.

Il numero dei crediti di una smart card che è in grado di eseguire e il periodo di tempo tra pagamenti sono completamente configurabili. Queste operazioni devono essere effettuate alla presenza di un agente o di una carta del commerciante.

Durante il saldo, il back-end è informato dei valori di credito.

Questa istruzione di credito automatico permette ai nostri titolari di ricevere regolarmente i pagamenti di importo fisso presso dispositivi POS, che non possono avere la capacità di eseguire funzioni on-line.

I partecipanti ad una transazione di credito automatico sono: l'iniziatore del credito automatico, il titolare della carta e il commerciante.

L'iniziatore di credito automatico è l'emittente che crea un'istruzione automatica di credito con un particolare portafoglio di un titolare specifico.

Il titolare della smart card è il beneficiario delle istruzioni del credito automatico che è stato approvato dal promotore. Il commerciante è un qualsiasi rivenditore che partecipa al sistema U.E.P.S. ed ha un dispositivo POS per attivare le istruzioni automatiche di credito ad un titolare della carta. I titolari di carte vanno ai punti designati per registrare un'istruzione di credito automatico. Mentre sul dispositivo POS, l'iniziatore di credito presenta una domanda per un'istruzione di credito automatico al sistema back-end. L'applicazione può avvenire off-line o on-line.

Una volta che il sistema back-end ha convalidato le informazioni del beneficiario, si crea un Automatic Credit instruction signature che viene inviato al dispositivo POS e viene quindi registrato sulla smart card. Il giorno in cui il titolare della carta deve ricevere un pagamento, lui inserisce la smart card in qualsiasi dispositivo POS.

Nel caso in cui l'istruzione di credito automatico è giusta e valida, la smart card del titolare della carta è caricata automaticamente.

Debito automatico

La funzione di addebito automatico consente una smart card di ridurre il saldo, in qualsiasi dei propri portafogli attivi, su un dato specifico e per un importo predeterminato. Questa funzione può avvenire in un ambiente off-line presso qualsiasi dispositivo POS. La funzione di addebito automatico riduce i rischi connessi alla raccolta dei premi assicurativi e altri pagamenti regolari, garantendo che eventuali fondi caricati alla smart card vengono prima posti al servizio del debito automatico e solo in seguito vengono messi a disposizione del titolare della carta per un uso generale.

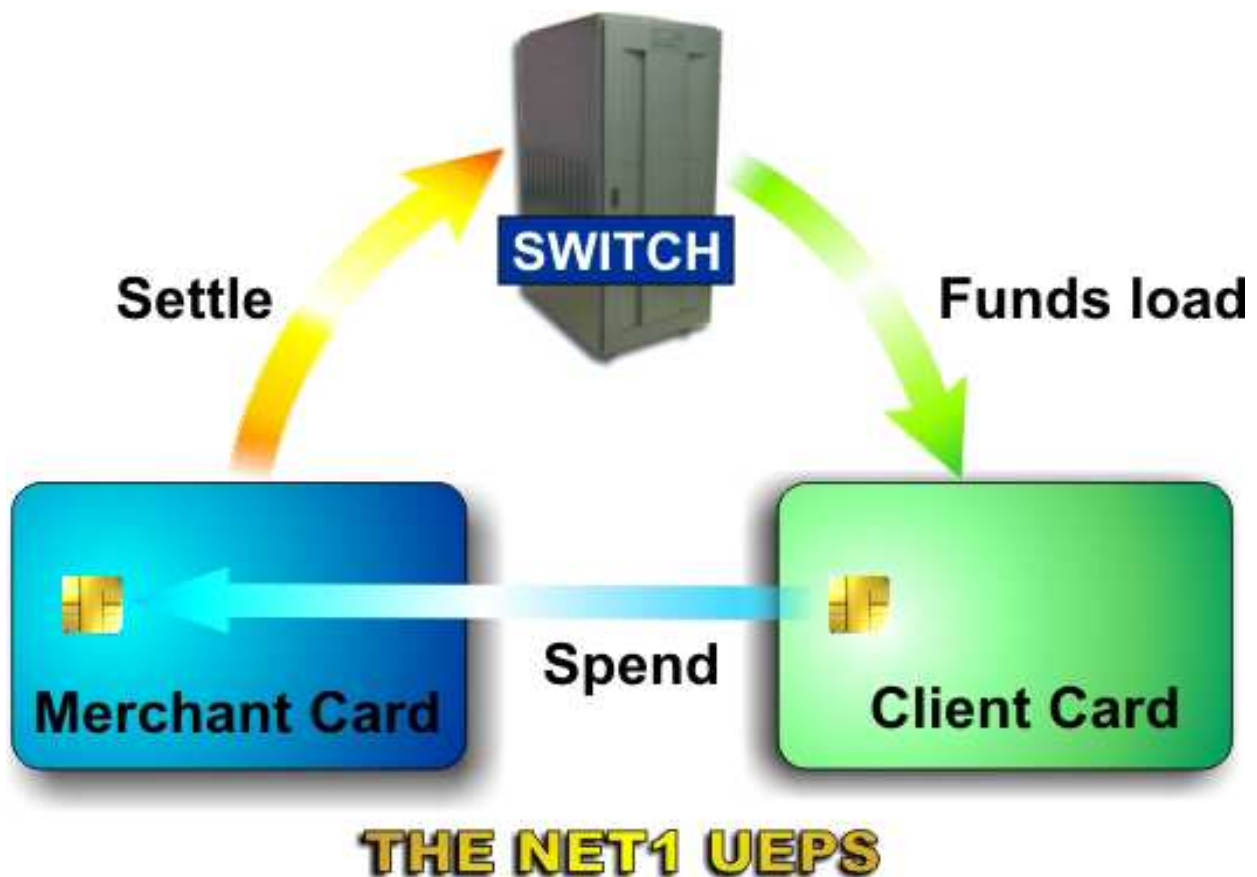
I partecipanti ad un'operazione di addebito automatico sono l'iniziatore di addebito automatico, il commerciante e il titolare della carta.

L'iniziatore di addebito automatico è l'emittente che crea un'istruzione di addebito automatico per un portafoglio particolare di un titolare di una specifica carta.

Il commerciante è un qualsiasi rivenditore che è un partecipante al sistema e ha un dispositivo POS per attivare, ad un titolare della carta, le istruzioni di addebito automatico. Il titolare della carta è la persona che deve pagare il premio o il 'pagamento'. I titolari di carte si registrano per ordine di addebito automatico presso gli uffici dell'iniziatore dell'addebito automatico. Mentre sul dispositivo POS, l'iniziatore di credito presenta una domanda per un'istruzione di addebito automatico al sistema back-end. Ciò può avvenire off-line o on-line. Una volta che il sistema back-end ha convalidato le informazioni del beneficiario, si crea un Automatic Debit instruction signature che viene inviato indietro al dispositivo POS e viene quindi registrato sulla smart card. Il giorno che il titolare della carta deve pagare un premio o altro, il titolare della carta inserisce la smart card in qualsiasi dispositivo POS. Nel caso in cui l'istruzione di addebito automatico è scaduta, la smart card del titolare della carta viene automaticamente addebitata.

Meccanismi di "loading, spending, settlement"

Ciò che segue descrive come i titolari di carte possono caricare quantità nelle loro smart cards e spendere la quota che esse ricevono. Inoltre descrive come i commercianti risolvono le transazioni con il loro sistema back-end.



➤ **Loading** (Caricamento)

I titolari possono caricare le loro smart cards in differenti modi.

Se il valore elettronico della carta del titolare è stato creato attraverso 10-digit signature code, poi il titolare ha tre opzioni. Può effettuare un on-line auto load (auto caricamento: dal conto alla carta), in cui il dispositivo POS si connette in tempo reale col sistema back-end, che poi inoltra alcuni ten-digit signature codes disponibili e presenti nel conto del titolare. Questi codici sono caricati dalla smart card automaticamente se la rete di comunicazione è inaffidabile e instabile, 10-digit signature codes possono essere scaricati dal dispositivo POS di un commerciante partecipante nelle vicinanze dove e quando la rete è operativa.

Il titolare può effettuare off-line auto load per cui alcuni ten-digit signature codes presenti nel dispositivo POS sono caricati nelle smart cards. Se una connessione di rete è disponibile, il titolare può digitare il suo ten-digit signature code e l'ammontare da caricare. In tutti gli scenari la smart card può essere accreditata solo se il ten-digit signature code è decifrato con successo dalla smart card. Se la smart card del titolare della carta viene inizializzata con una o più istruzioni di Credito Automatico, la smart card vi si accrediterà come se descrivessimo l' "Automatic Credit" caratteristica di cui sopra.

➤ **Spending** (Spesa)

Non appena il valore è stato caricato a una smart card, il titolare della carta può acquistare beni o servizi, effettuare prelievi di contante, avviare trasferimenti di denaro, prestiti su richiesta, pagamenti automatici, effettuare pagamenti a terzi, attivare ordini di Automatic Credit e Debit, tutti off-line in qualsiasi negozio in cui il commerciante è un partecipante al sistema ed ha un dispositivo POS.

Per eseguire un'operazione, il titolare di carte inserisce la sua smart card all'estremità del lettore di smart card nel dispositivo POS e seleziona la funzione appropriata. L'identificazione biometrica delle impronte digitali è necessaria per proteggere i titolari di carta contro gli utilizzi impropri o fraudolenti dei loro fondi.

Una ricevuta stampata visualizza i dettagli della transazione effettuata e comprende altre informazioni dell'iter di controllo del sistema.

➤ **Settlement** (Saldo)

Mentre la spesa per una smart card U.E.P.S. si verifica off-line, il saldo delle transazioni commerciali con il sistema back-end deve avvenire entro due giorni "window settlement", periodo previsto da contratto, o comunque per quando la carta del commerciante diventa piena. Il saldo può essere eseguito on-line o off-line.

I commercianti che hanno accesso ad una infrastruttura di rete possono utilizzare l'opzione settlement sui loro dispositivi POS per la connessione al sistema back-end e sistemare le loro merchant smart cards on-line. Una volta che il commerciante seleziona l'opzione settlement sul dispositivo POS (operazione effettuata on-line), le transazioni sono tolte dalla smart card del commerciante, i valori di transazione vengono accumulati e le tasse di transazione vengono pagate dal commerciante.

Il pagamento avviene attraverso il sistema bancario tradizionale del paese.

Se un commerciante non ha accesso ad una rete di comunicazione, il commerciante può utilizzare la nostra funzione "milking" ("mungitura = spillare soldi") con una milking card (carta per prelevare).

Questa smart card ha una maggiore funzionalità rispetto a una normale carta e quindi richiede un chip con una grande memoria per memorizzare le operazioni e in più i hot card files (elenco di carte disabilitate al servizio, solitamente registrate in maniera elettronica. Una hot card è una carta di debito o credito che non può essere utilizzata perchè ne è stato denunciato lo smarrimento o il furto; se il ladro o chiunque altro tenta di utilizzare una hot card, la transazione verrà rifiutata.), un certificato di freschezza, e tutte le altre variabili, incluse le spese e / o tariffe di interesse che devono essere aggiornate sulle merchant cards che operano in zone profonde e rurali. La milking smart card viene inserita nel fondo del lettore di smart card di un dispositivo POS e i commercianti inseriscono le carte dei commercianti nel lettore di smart card in alto con lo scopo di prelevare. Durante questo processo di risoluzione, le operazioni sono tolte dal file della history delle transazioni della carta del commerciante e allo stesso tempo, il nuovo hot card file, il certificato freschezza, la struttura delle commissioni, gli interessi delle tariffe e ogni altro parametro che richieda modifiche vengono aggiornati. La "milking" smart card viene poi consegnata materialmente alla sede centrale per aggiornare il sistema back-end.

Al momento del saldo, tutte le transazioni vengono eliminate dalla carta del commerciante, aggregate e pagate sul conto bancario indicato del commerciante. I commercianti possono selezionare il loro client smart card come loro conto designato, nel qual caso il valore da pagare è aggiunto alla client smart card del commerciante.

È stata progettata e sviluppata una dual functionality smart card chiamata NET1 Combi-Card per l'utilizzo in ambienti rurali e negozi molto piccoli o venditori ambulanti. Venditori ambulanti sono in genere piccoli commercianti che vendono cibo o merce da una posizione sul lato della strada o su un pavimento.

Questa smart card viene inizializzata con entrambe le funzionalità: merchant e client. Mentre per la contrattazione, la sezione della smart card del commerciante viene utilizzata per la memorizzazione delle transazioni che, una volta risolte, permetterà al negoziante di utilizzare la stessa carta per effettuare acquisti o qualsiasi altra funzione finanziaria.

Lo SWITCH (commutatore) è un dispositivo di rete, o nodo interno di rete, che si occupa di commutazione a livello 2 (livello data-link) ovvero di indirizzamento e di instradamento, all'interno di reti locali, attraverso indirizzi MAC (Media Access Control è l'indirizzo hardware) inoltrando selettivamente i frame (pacchetti dati) ricevuti verso una porta di uscita cioè verso un preciso destinatario grazie ad una corrispondenza univoca tra porta-indirizzo.

Protocollo U.E.P.S.

Il protocollo di transazione U.E.P.S. è usato per garantire l'integrità di ogni passaggio del cash path (percorso di cassa), dalla banca al cliente al commerciante alla clearer alla banca. Con il termine clearer si intende compensazione che è un meccanismo che permette alle banche e istituzioni finanziarie di regolare tra loro i rapporti di dare e avere generati da transazioni finanziarie.

La compensazione si realizza calcolando il saldo netto che ogni parte deve dare o prendere.

Ad ogni passo, ogni transazione è resa unica dalle sfide casuali, o sequenze di numeri o entrambe. Importante è implementare un modo di fare ciò conforme ai requisiti di sicurezza del cliente entro i limiti tecnici della carta. È stata utilizzata la doppia crittografia con il concatenamento della chiave per ottenere un'implementazione compatta.

Sia C il nome del cliente, N_C un **nonce** generato da lui (un numero a caso), R il nome del rivenditore, N_R un nonce generato da lui (operazione numero di sequenza), e X l'assegno elettronico.

La transazione di acquisto può essere idealizzata (schematizzata) come segue:

$$C \rightarrow R: \{C, N_C\}_K$$

$$R \rightarrow C: \{R, N_R\}_L \quad \text{ove } L = \{C, N_C\}_K$$

$$C \rightarrow R: \{X\}_M \quad \text{ove } M = \{R, N_R\}_L$$

Tale protocollo ha la robusta proprietà che tutte le reciproche informazioni tra le due parti vengono rese esplicite essendo state inserite all'interno delle chiavi del messaggio. In effetti il prodotto intermedio di ogni doppia codifica è usato come seconda chiave nella crittografia seguente.

In questo modo ogni blocco funge da autenticatore per tutti i messaggi precedenti nel protocollo e le informazioni possono essere scambiate efficientemente.

All'interno di ogni messaggio c'è una ridondanza, al fine di verificare che la crittografia è stata eseguita con la chiave giusta. Con il concatenamento della chiave, abbiamo bisogno solo di un ridondante blocco dati, vale a dire che l'ultimo messaggio è quello che fa sì che il valore venga accreditato nella carta ricevente.

Per validare il protocollo, ovvero dimostrarne l'autenticità, si è dovuto, però, considerarne uno semplificato dove l'informazione viene accumulata senza concatenamento:

$$C \rightarrow R: \{C, N_C\}_K$$

$$R \rightarrow C: \{R, N_R, C, N_C\}_K$$

$$C \rightarrow R: \{C, N_C, R, N_R, X\}_K$$

questo può essere analizzato in un modo semplice usando la logica BAN.

La logica BAN non si limita a verificare la mutua autenticazione e lo scambio delle chiavi ma è anche uno strumento utile e pratico per il design di un protocollo crittografico efficiente. Il trucco è quello di partire dal risultato desiderato e lavorare a ritroso, in questo caso, si dimostra che il rivenditore deve fidarsi dell'assegno, cioè $R \mid \equiv X$ (un assegno è buono se e solo se è genuino e fresco).

Ora $R \mid \equiv X$ seguirà sotto la regola di competenza (the jurisdiction rule) da

$R \mid \equiv C \Rightarrow X$ (R ritiene C abbia giurisdizione su X) e $R \mid \equiv C \mid \equiv X$ (R crede che C

creda X). La condizione precedente segue dal vincolo hardware, che nessuno tranne C avrebbe potuto pronunciare un testo del modulo $\{C, \dots\}_K$.

Quest'ultimo, che $R \mid \equiv C \mid \equiv X$, deve essere dedotto utilizzando la regola di verifica

nonce (the nonce verification rule) da $R \models \#(X)$ (R crede che X sia fresco) e $R \models C \mid \sim X$ (R crede che C abbia pronunciato X). $R \models \#(X)$ consegue la sua presenza in $\{C, N_C, R, N_R, X\}_K$ che contiene il numero di sequenza N_R , mentre $R \models C \mid \sim X$ consegue dal vincolo hardware. Poiché la logica BAN non prevede alcun meccanismo per trattare in concatenamento chiave utilizzato nel protocollo reale, è stato trovato un modo per districare $\{X\}_{R;N_R}\{C;N_C\}_K$ da $\{C, N_C, R, N_R, X\}_K$. Durante la progettazione di U.E.P.S., è stato risolto questo problema aggiungendo un ulteriore postulato. La regola del significato del messaggio (the message meaning rule) dice che se P ritiene che la chiave K è condivisa con Q e P vede un messaggio cifrato X in K ($P \models Q \stackrel{K}{\leftrightarrow} P, P \triangleleft \{X\}_K$), poi P crederà che Q ha detto una volta X ($P \models Q \mid \sim X$). A questo abbiamo aggiunto una regola simmetrica nel senso che se P cerca una chiave K per decifrare un blocco, e P riconosce il risultato come proveniente da Q ($P \models Q \stackrel{K}{\leftrightarrow} P, P \triangleleft \{X\}_K$), poi P crederà che Q infatti ha usato K ($P \models Q \mid \sim K$).

In U.E.P.S. la convalida, che tuttavia viene eseguita, dimostra che il cliente non riceve alcuna conferma della transazione, ma semplicemente la consapevolezza che è presente una carta valida del rivenditore.

Nella transazione la client card si addebita dopo la fase 2, momento in cui la carta cliente si è già impegnata nella transazione, mentre il rivenditore non ha ancora ricevuto l'assegno. Se il processo subisse un denial-of-service attack (attacco da un terminale falso) la procedura consisterebbe nel rimborsare al cliente qualsiasi importo mancante che rimane non depositato in banca, dopo 21 giorni, ma se il denaro fosse depositato, la controversia sarebbe stata risolta confrontando i due dati relativi alle carte, o ispezionando il rotolo di scontrini dal terminale del commerciante.

Questo attacco non trae alcun beneficio finanziario e gli incidenti sono abbastanza rari che possono essere trattati manualmente; per questo motivi si usa la procedura di rimborso.

Conclusioni

Il sistema U.E.P.S. fu un successo commerciale tanto da essere adottato da VISA come COPAC electronic wallet.

Ha fornito stimoli intellettuali di una certa portata a progettisti e programmatori e ha rafforzato, notevolmente, la fiducia del cliente nel sistema.

Bibliografia

www.net1.com

“U.E.P.S. Technical Overview
Universal Electronic Payment System”

www.cl.cam.ac.uk/~rja14/Papers/uepsbook.pdf

“The formal verification of a payment system” di Ross J. Anderson

Di Broccoletti Jenny
e Sistoni Marika