



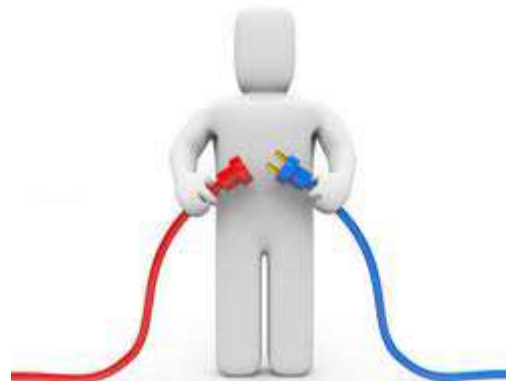
Net1 U.E.P.S.

Universal Electronic Payment System

Broccoletti Jenny
Sistoni Marika




- Fornitore di metodi di pagamento alternativi per popolazioni in via di sviluppo
- Permette transazioni off-line sicure e accessibili





- è un sistema di pagamento per transazioni off-line
- si basa su FTS (Funds Transfer System)
- offre soluzioni outsourced
- promuove un'economia "non-cash"



U.E.P.S. Banking

Trasferimento fondi:

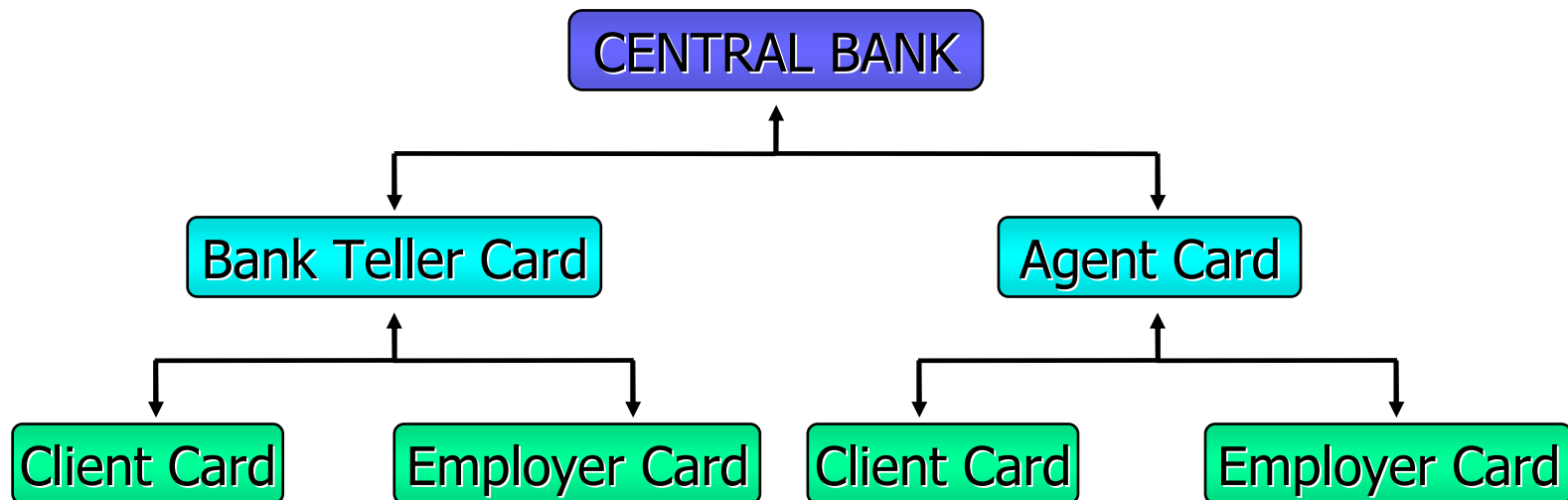
- sistema Stand-A-Lone
- pagamenti “Once-off”

[Caratteristiche principali]

- Affordability
- Security
- Simplicity

Sicurezza

- Triple DES e nonce
- Gerarchia delle smart card (procedura end-to-end):



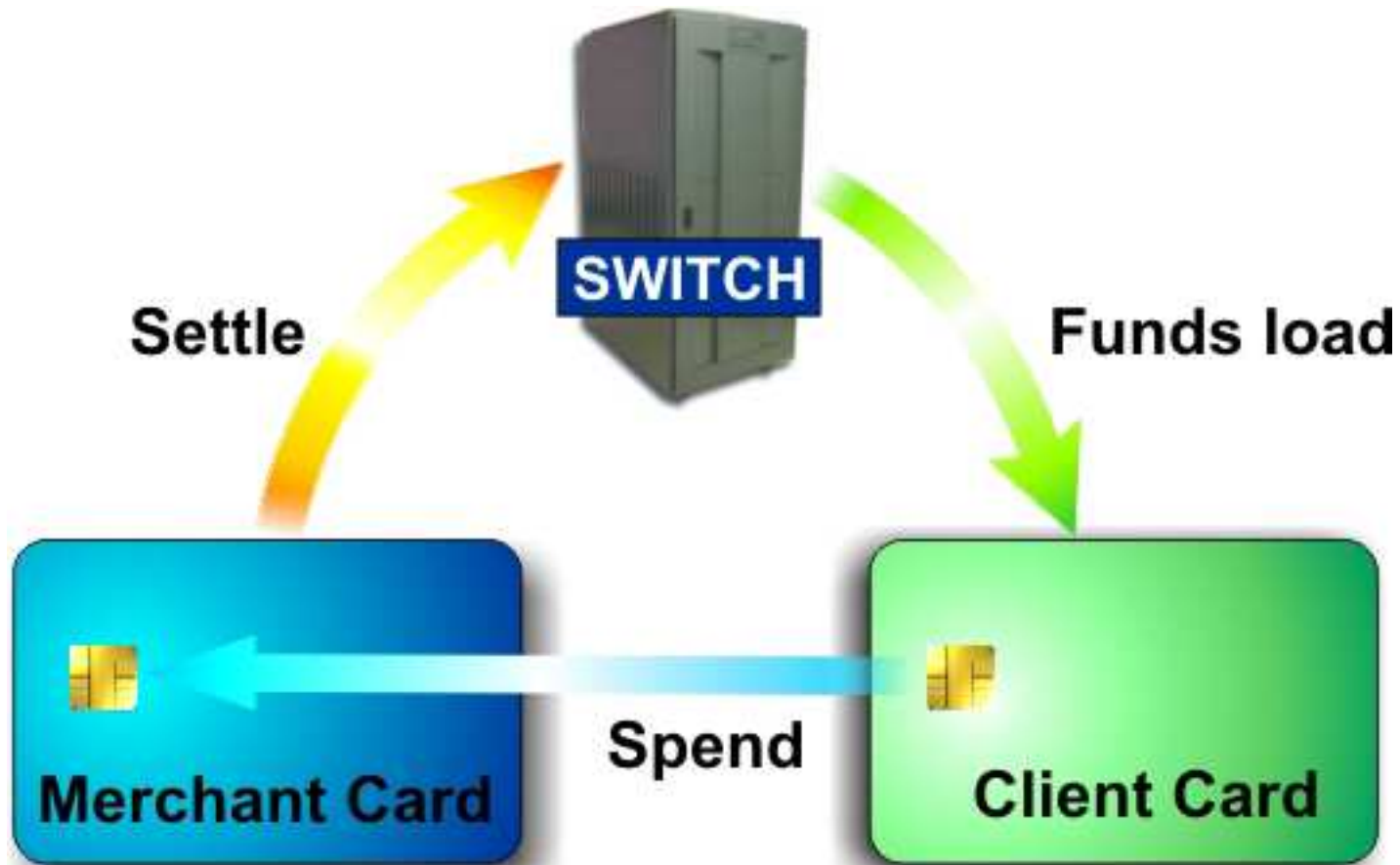
- Challenge-response protocol

Funzionalità U.E.P.S.

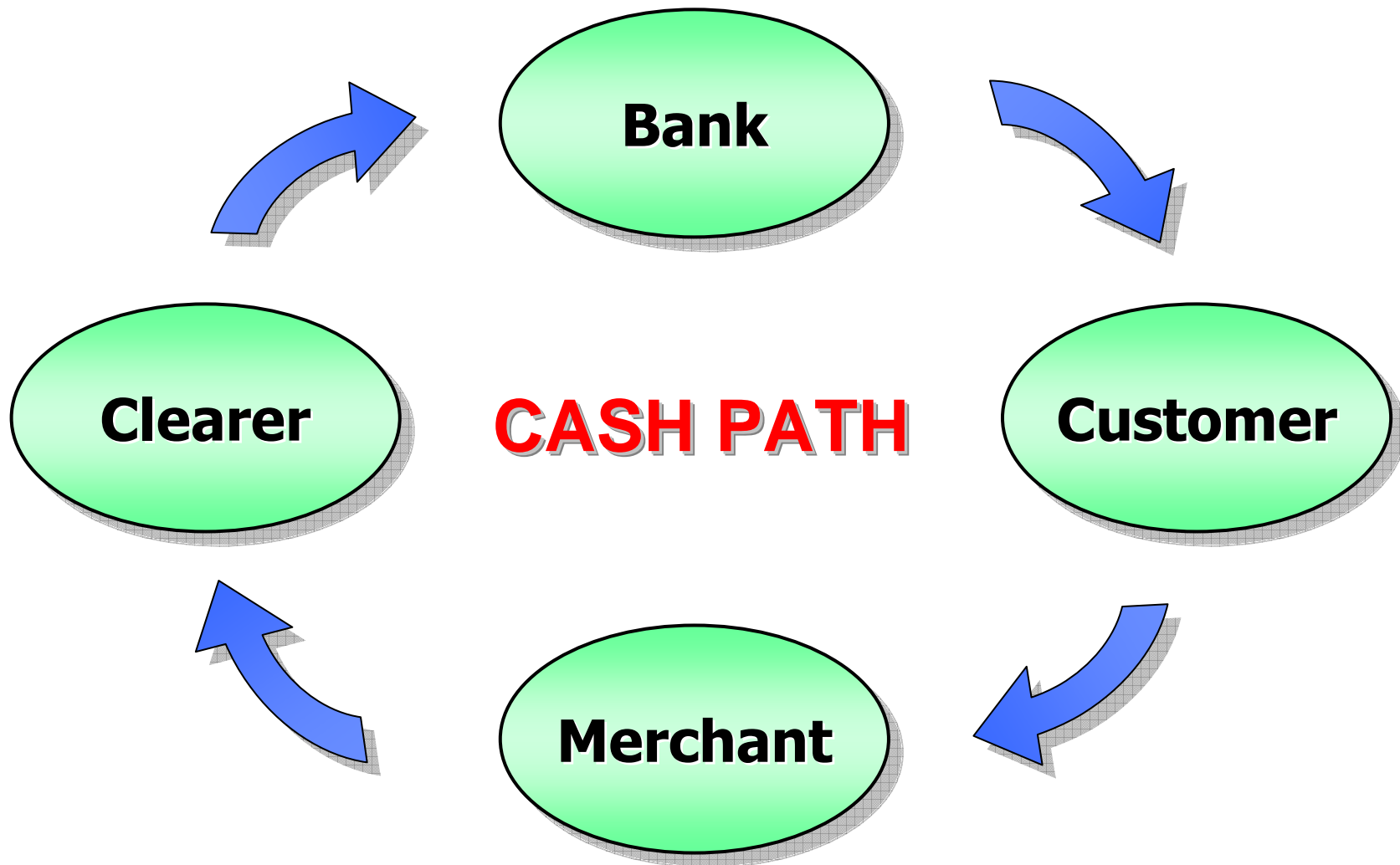
- Mutual authentication:
 - chiave di sessione casuale basata su nonce
 - attacco brute force
- Transparent and automatic recovery
- Transaction cancellation
- Refunds
- Multiple audit trails for off-line U.E.P.S. transactions
 - preserva l'integrità del sistema

-
- 10-digit signature code
 - Off-line loading
 - Biometric identification
 - sistemi a banda magnetica con firma o PIN
 - vs supporti U.E.P.S. di dati biometrici
 - Continuous debit
 - Multiple and restricted wallets
 - portafogli protetti e non
 - Automatic credit and debit
-

- Meccanismi di “loading, spending, settlement”:



THE NET1 UEPS



Protocollo U.E.P.S.

L'integrità del cash path viene garantita dal protocollo U.E.P.S.

A7

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

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

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

Diapositiva 11

A7

Transazione di acquisto schematizzata

Dati:

C=nome del cliente

R=nome del rivenditore

X=assegno elettronico

Nc=nonce generato dal cliente

NR=nonce generato dal rivenditore

k=chiave segreta, generata appositamente
per la transazione, condivisa da cliente e
rivenditore

Asus, 5/1/2012

Per validarlo consideriamo un protocollo semplificato:

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

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

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



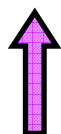
Analizziamolo con la Logica BAN

Ts: $R \mid \equiv X$ A1



the jurisdiction rule

$[R \mid \equiv C \Rightarrow X$ A2 e $R \mid \equiv C \mid \equiv X]$ A3



the nonce verification rule

$[\{C, N_C\}_K]$

$[R \mid \equiv \# (X)$ A4 e $R \mid \equiv C \mid \sim X]$ A5



$[\{C, N_C, R, N_R, X\}_K]$

$[\{C, N_C\}_K]$

Diapositiva 13

A1

R=rivenditore
X=assegno elettronico

R crede X
ovvero: R si comporta come se X fosse vero
ovvero: R si deve fidare di X
Asus, 4/29/2012

A2

R=rivenditore
C=cliente
X=assegno elettronico

R ritiene che C abbia giurisdizione su X
ovvero: R crede C sia un'autorità su X e perciò
bisogna fidarsi a riguardo
ovvero: R si fida di C per quanto riguarda X
Asus, 4/29/2012

A3

R=rivenditore
C=cliente
X=assegno elettronico

R crede che C creda X
ovvero: R crede che C dica X
Asus, 4/29/2012

A4

R=rivenditore
X=assegno elettronico

R crede che X sia una quantità fresh
Asus, 4/29/2012

A5

R=rivenditore
C=cliente
X=assegno elettronico

R crede che C abbia detto una volta X
ovvero: R crede che X sia stato inviato da C
ovvero: R crede che C abbia inviato un messaggio
che contenga X; C crede X quando lo inviò
Asus, 4/29/2012

Problema: la Logica BAN non tratta il concatenamento chiavi

Soluzione: si è aggiunto un postulato di simmetria alla message meaning rule (già esistente nella Logica BAN)

Message meaning rule

$$R \mid \equiv C \stackrel{K}{\leftrightarrow} R \text{A8} \text{ e } R \triangleleft \{X\}_K \text{A9} \implies R \mid \equiv C \mid \sim X \text{A10}$$

Regola di simmetria

$$R \mid \equiv C \stackrel{K}{\leftrightarrow} R \text{ e } R \triangleleft \{X\}_K \implies R \mid \equiv C \mid \sim K \text{A11}$$

Diapositiva 14

A8

R=rivenditore
C=cliente
K=chiave segreta

R crede che K sia una chiave condivisa con C
Asus, 4/29/2012

A9

R=rivenditore
X=assegno elettronico
C=cliente
K=chiave segreta condivisa tra C e R

R ha ricevuto un messaggio che contiene X cifrato con K, nel passato o in questa esecuzione del protocollo; R può leggere X e ripeterlo
Asus, 4/29/2012

A10

R=rivenditore
C=cliente
X=assegno elettronico

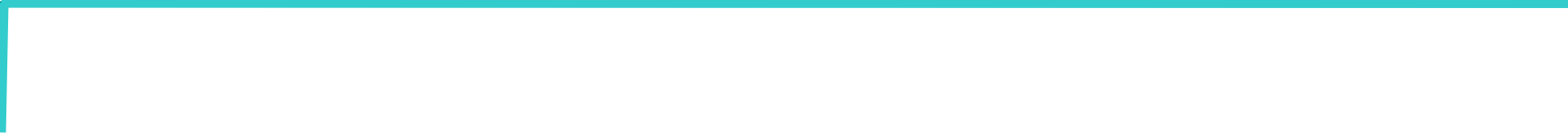
R crede che C abbia detto una volta X
ovvero: R crede che C abbia inviato un messaggio
che contenga X, C crede X quando lo inviò
ovvero: R crede che X sia stato trasmesso da C
Asus, 4/29/2012

A11

R=rivenditore
C=cliente
K=chiave segreta condivisa tra R e C

R crede che C abbia utilizzato una volta K
Asus, 4/29/2012

**Il sistema U.E.P.S. fu un
successo commerciale**



Grazie per l'attenzione!!

