



Università Degli Studi Di Perugia

Sicurezza Informatica A.A. 2011/2012

Il protocollo S.E.T. (Secure Electronic Transaction)

Andrea Valentini Albanelli
Fabrizio Cardellini

S.E.T.

- **INTRODUZIONE**
- **PROTOCOLLO**
 - ATTORI**
 - DOPPIA FIRMA**
 - SET IN AZIONE**
- **VANTAGGI E SVANTAGGI**

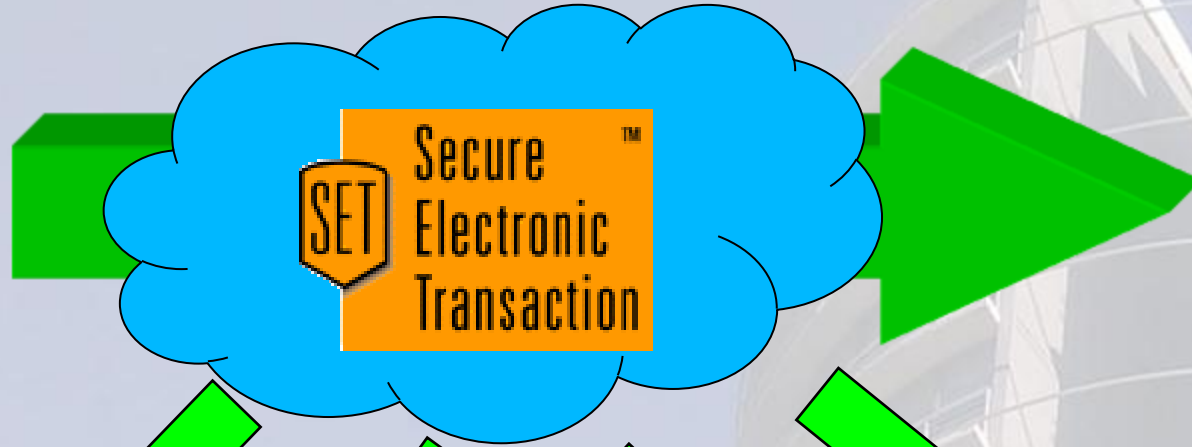


PERCHÈ S.E.T.?

SVILUPPATORI



INTRODUZIONE



DES

X.509

SHA-1

RSA

Strumenti utilizzati

- **DES**
- **RSA**
- **SHA-1**
- **X.509**

S.E.T.

- **INTRODUZIONE**
- **PROTOCOLLO**
 - ❑ **ATTORI**
 - ❑ **DOPPIA FIRMA**
 - ❑ **SET IN AZIONE**
- **VANTAGGI E SVANTAGGI**

ATTORI



CARDHOLDER



COMMERCIANTE



EMITTENTE



ACQUIRENTE



PAYMENT GATEWAY



CA

ATTORI



CARDHOLDER

Soggetto autorizzato ad utilizzare una carta di credito



COMMERCIANTE

Persona o organizzazione che vuole vendere beni o servizi ai CARDHOLDER



EMITTENTE

Istituto finanziario (es. banca) che fornisce una carta di credito per il CARDHOLDER

ATTORI



ACQUIRENTE

**Istituto
finanziario che
ha un rapporto
con i
commercianti**



PAYMENT GATEWAY

**Interfaccia tra
acquirente e reti
di pagamento
con carte
bancarie**



CA

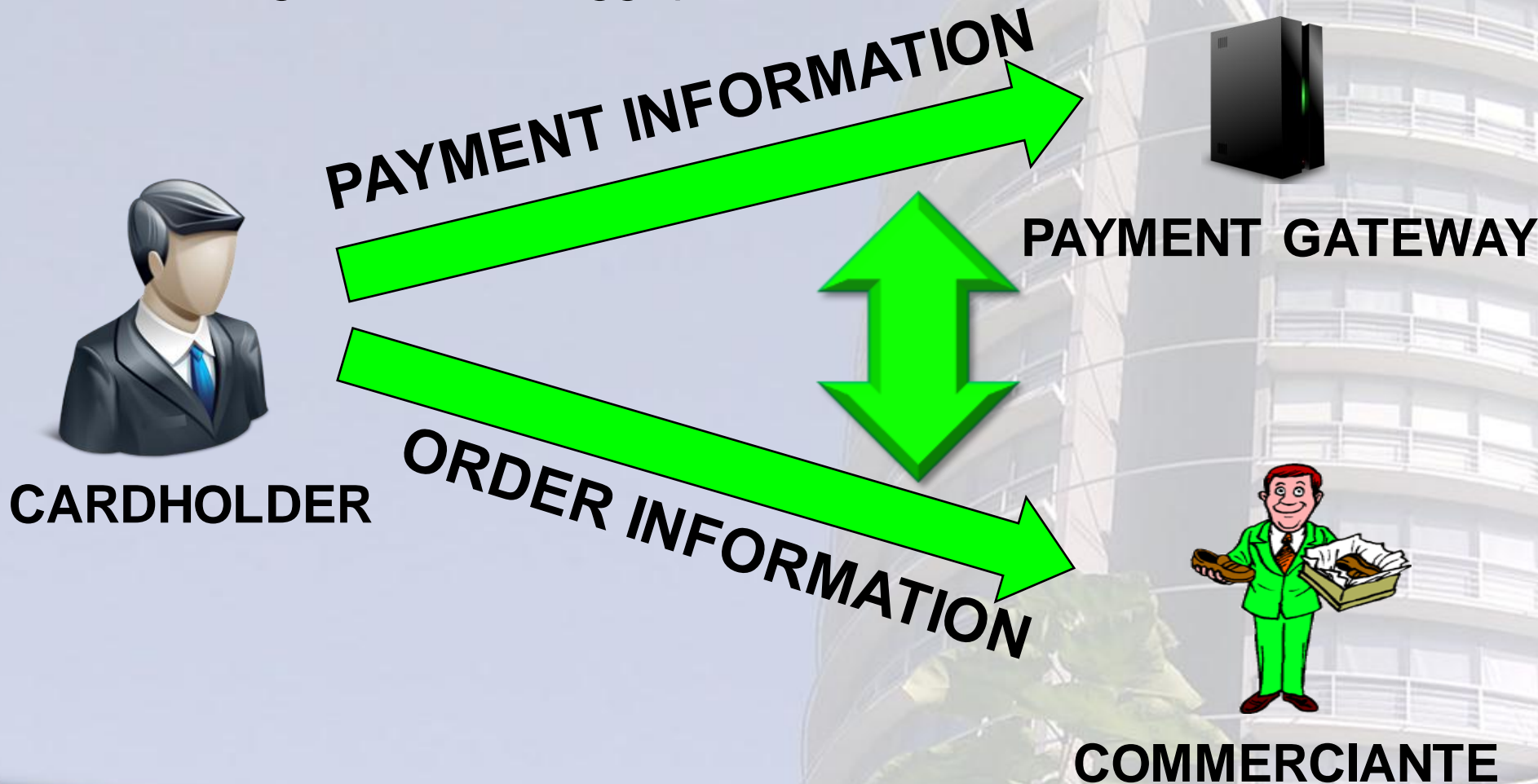
**Entità atta a
rilasciare
certificati per
titolari,
commercianti e
payment gateway**

S.E.T.

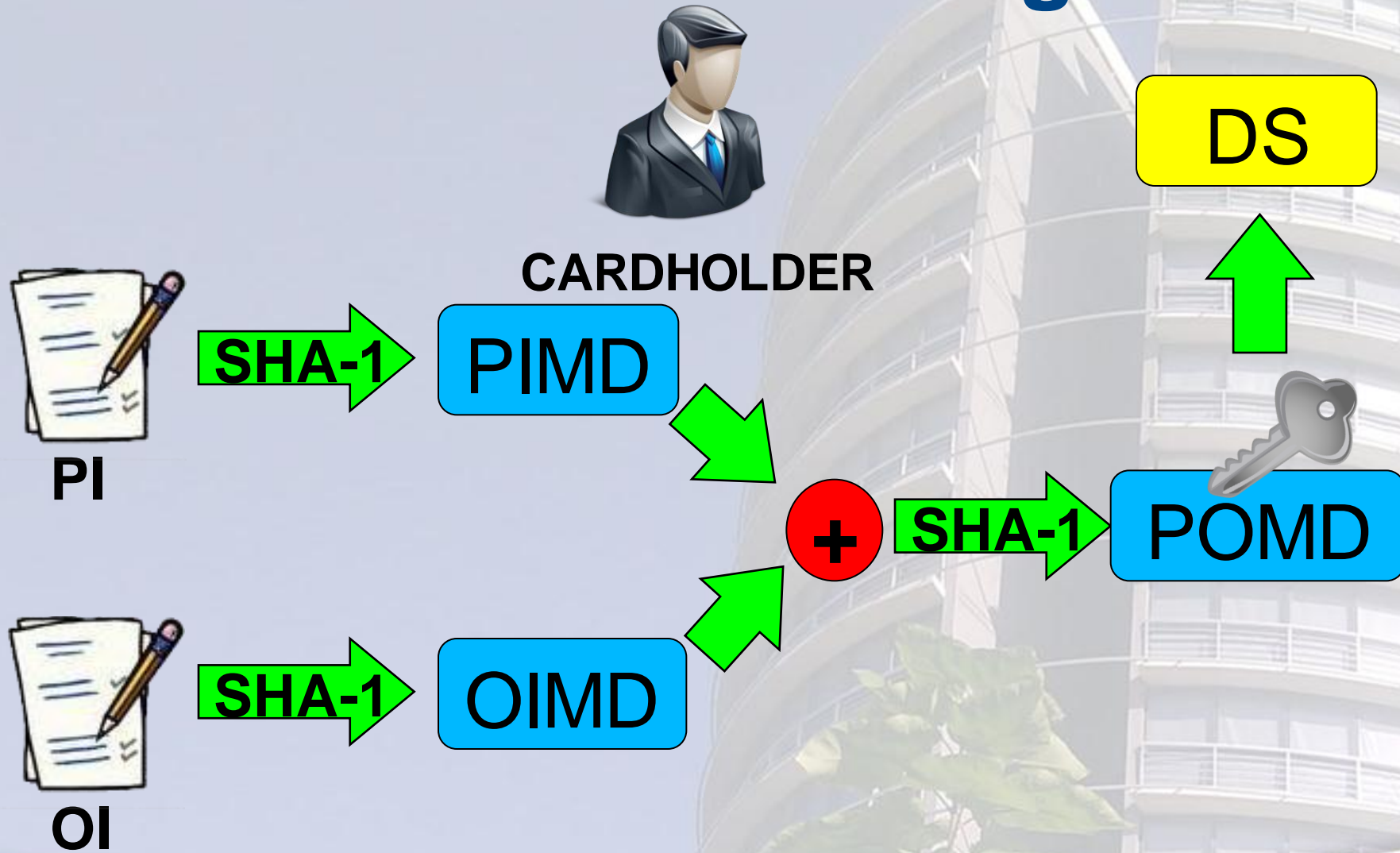
- **INTRODUZIONE**
- **PROTOCOLLO**
 - ❑ **ATTORI**
 - ❑ **DOPPIA FIRMA**
 - ❑ **SET IN AZIONE**
- **VANTAGGI E SVANTAGGI**

Dual Signature

- Collegare 2 messaggi per 2 differenti destinazioni



Creazione della Dual Signature



Verifica della Dual Signature

DS

PIMD



COMMERCIANTE



OI



CLIENTE

PIMD



OIMD



POMD



OI

Verifica della Dual Signature

DS

PIMD



COMMERCIANTE



OI



CLIENTE

PIMD



OIMD



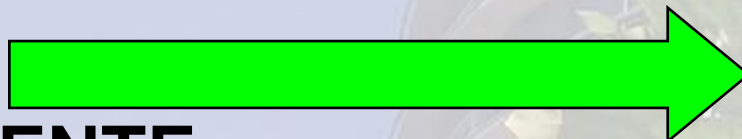
POMD



DS



CLIENTE



POMD

Verifica della Dual Signature

DS

OIMD



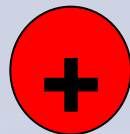
PI



CLIENTE

PAYMENT GATEWAY

OIMD



PIMD



POMD



PI

Verifica della Dual Signature

DS

OIMD



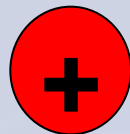
PI



CLIENTE

PAYMENT GATEWAY

OIMD



PIMD



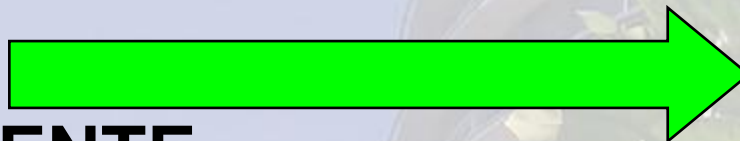
POMD



DS



CLIENTE



POMD

S.E.T.

- **INTRODUZIONE**
- **PROTOCOLLO**
 - ❑ **ATTORI**
 - ❑ **DOPPIA FIRMA**
 - ❑ **SET IN AZIONE**
- **VANTAGGI E SVANTAGGI**

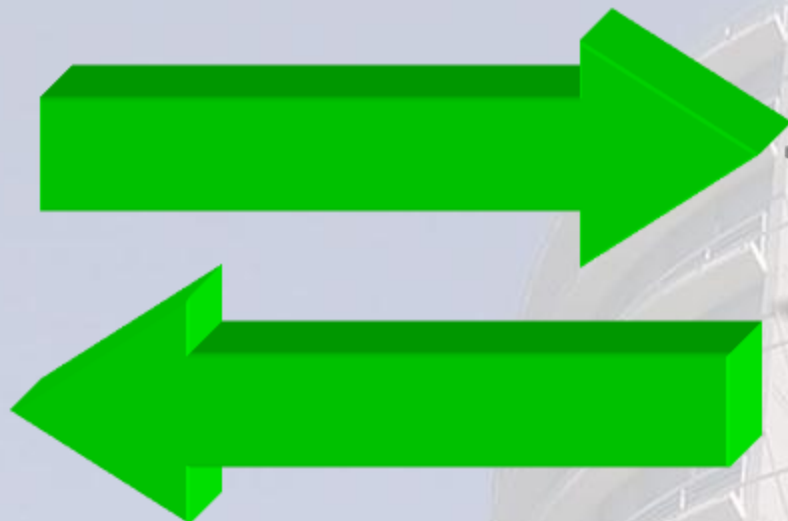
SET IN AZIONE

- **Le fasi previste dallo standard sono:**
 - ➔ Registrazione del cardholder
 - ➔ Registrazione del commerciante
 - ➔ Sottomissione di un ordine
 - ➔ Autorizzazione del pagamento
 - ➔ Adempimento delle due parti

Registrazione del cardholder



CARDHOLDER



EMITTEnte



Il cardholder acquista una carta di credito dall'emittente che gliela rilascia insieme ad un **certificato** e ad un **e-wallet**

Registrazione del commerciante



COMMERCIANTE



ACQUIRENTE



Il commerciante ottiene **2 certificati**: Il suo e quello dell'acquirente, e un **thin-wallet**

Sottomissione di un ordine

GIVE ME YOUR
CERTIFICATE AND
PAYMENT GATEWAY'S
CERTIFICATE!



CARDHOLDER

COMMERCIANTE

- Il cardholder, navigando nel sito web del commerciante, decide di effettuare un ordine
- Invia un messaggio di **Initiate Request**

Sottomissione di un ordine



CARDHOLDER



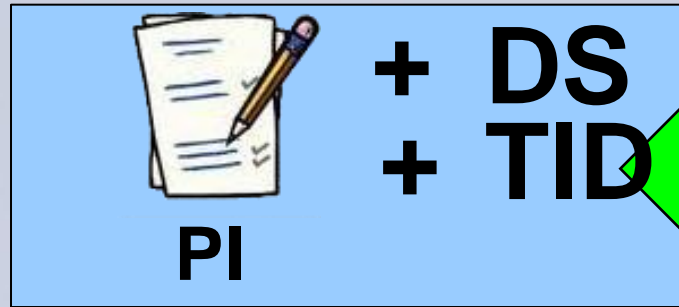
COMMERCIANTE

- Il commerciante risponde con un messaggio di **Initiate Response**
- Fornisce i certificati richiesti ed un **TID** criptato con la sua chiave privata

Sottomissione di un ordine

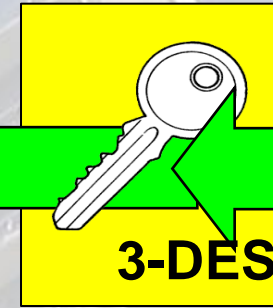


CARDHOLDER



OI

+ DS + TID



P.G.

- Il cardholder prepara le informazioni di pagamento (**PI**), le informazioni sull'ordine (**OI**), il certificato e crea una doppia firma (**DS**)

Sottomissione di un ordine



CARDHOLDER

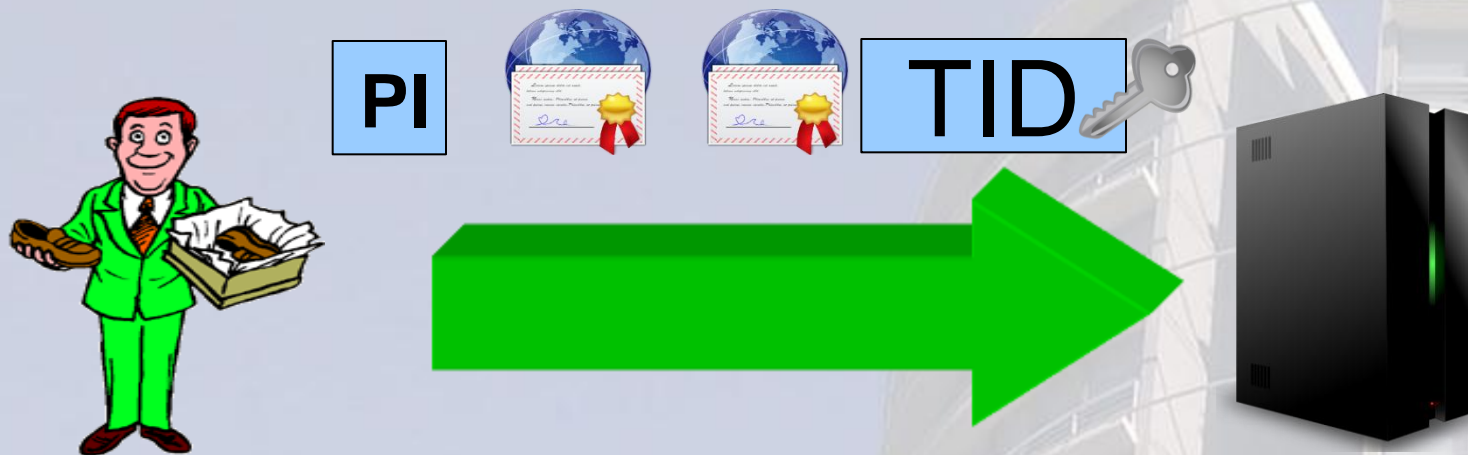
Purchase Request



COMMERCIANTE

- Il cardholder invia tutto il messaggio preparato precedentemente al commerciante.
- E' un messaggio di **Purchase Request**

Autorizzazione del pagamento



COMMERCIANTE

➤ Il commerciante invia le PI criptate, il suo certificato e il certificato del cardholder al payment gateway.

➤ Il payment gateway può:

- leggere le PI
- verificare l'integrità del pagamento
- autenticare entrambe le parti

PAYMENT GATEWAY

Autorizzazione del pagamento



- Deve esistere un **canale di comunicazione sicuro** tra payment gateway ed emittente
- Il payment gateway comunica i PI all'emittente che, dopo averli verificati, fornisce l'**autorizzazione**

Autorizzazione del pagamento



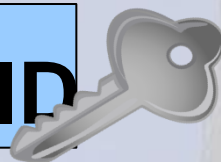
Autorizzazione del pagamento



CARDHOLDER

Purchase Response

ACK + TID



COMMERCIANTE



- Il commerciante invia una **notifica (ACK)** ed il **TID** criptate con la sua chiave privata
- E' un messaggio di **Purchase Response**

Adempimento delle 2 parti



CARDHOLDER

COMMERCIANTE

- Viene effettuato l'addebito sulla carta di credito del cardholder
- Il commerciante viene rimborsato dall'acquirente
- Il commerciante fornisce il bene o il servizio acquistato

S.E.T.

- **INTRODUZIONE**
- **PROTOCOLLO**
 - ATTORI**
 - DOPPIA FIRMA**
 - SET IN AZIONE**
- **VANTAGGI E SVANTAGGI**

VANTAGGI

- **INTEGRITÀ**
- **AUTENTICAZIONE**
- **PRIVACY**
- **CONFIDENZIALITA'**

VANTAGGI

➤ IMMUNE A MOLTI ATTACCHI

- Uno sniffer non ricaverebbe informazioni interessanti
 - Attacchi di replica inefficaci

SVANTAGGI

➤ **ATTACCO ALL'E-WALLET**

➤ **COMPLESSITA'**

➤ **CONFIDENZIALITA' E PRIVACY NON
GARANTITE PER OI**

CONCLUSIONE

- **SET HA BUONE CARATTERISTICHE DI SICUREZZA**
- **COMPLESSITA' ELIMINABILE?**
- **TORNERA' AD ESSERE USATO?**