Secure transactions

by testing secure transactions

Dirk Jan van den Heuvel
CEO Collis

4 November 2010

❖ Collis

Content

❖ Introduction

❖ Characteristics of secure transaction systems

❖ Testing secure transaction systems

- Roles and responsibilities

- Test Process

- Examples

❖ What we learned

Introduction to transaction systems

❖ Payment cards

❖ Mobile communication

❖ Electronic Health Record

❖ Public transport

❖ Transport (Tachograph)

❖ Identity management

❖ Collis
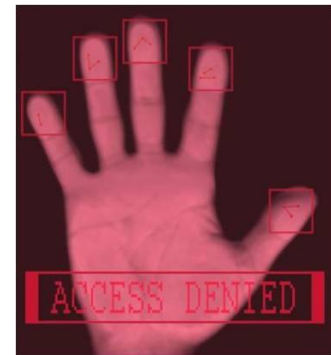
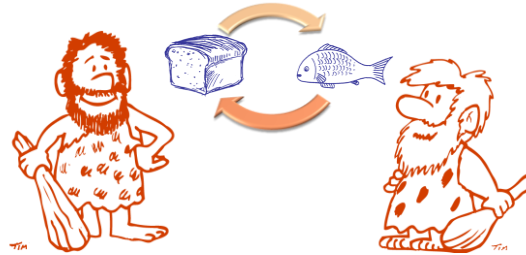# Characteristics

For most Secure Transaction Schemes
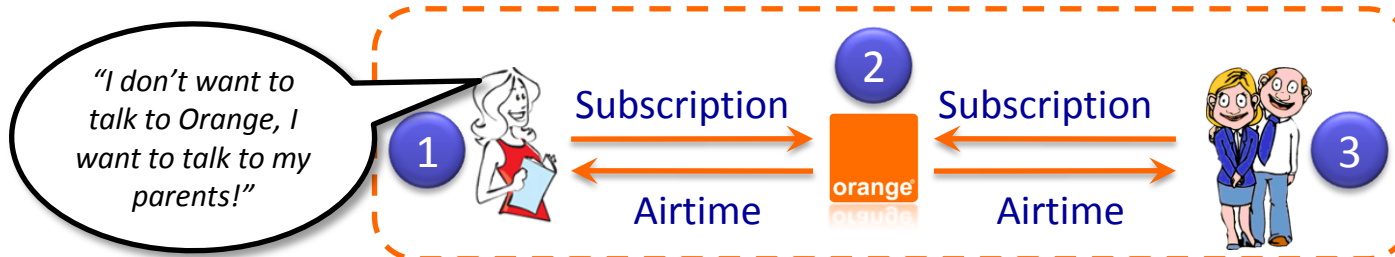
❖ Many users, various parties (2, 3, 4 party model)

❖ Rights / good in exchange for value

❖ Importance of:

- Reliability

- Confidentiality

- Privacy

- Non-repudiation

❖ Through Security and Cryptography

From 2-party to 3-party…

❖ In the old days

❖ Some transactions require a 3rd person…

"The Österbymo photo frame costs € 5,99. I have to pay to IKEA, not to my bank…"

1 → **citi** → 3 (IKEA)

Card fee →
← Credit card

Merchant fee ←
Card terminal →

2

"I don't want to talk to Orange, I want to talk to my parents!"

1 → **orange** → 3

Subscription →
← Airtime

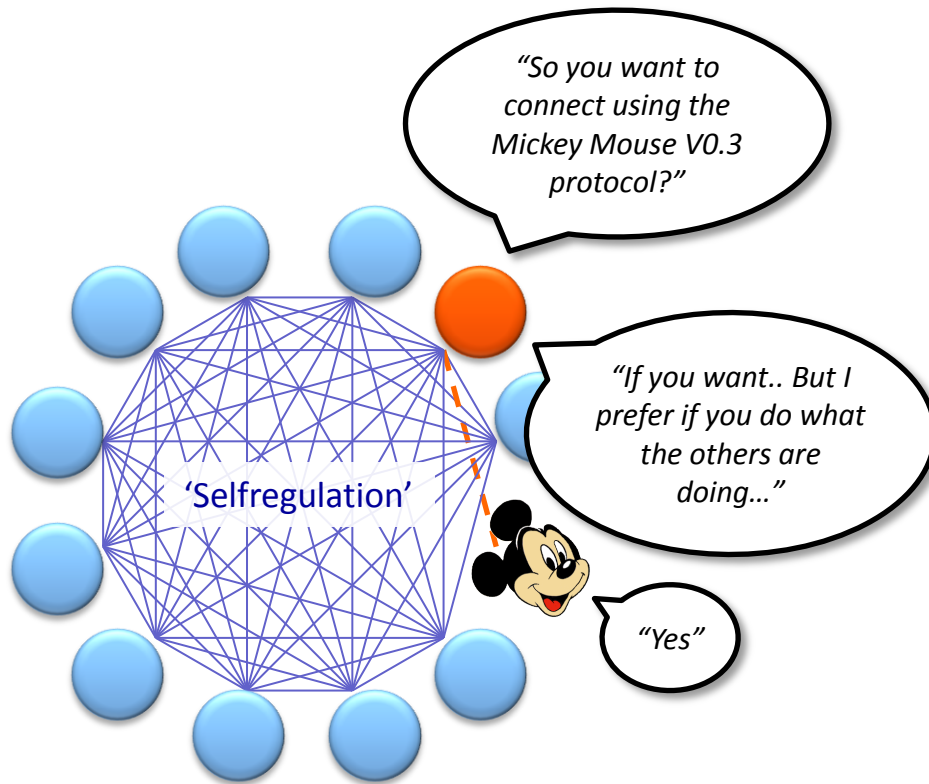← Subscription
Airtime →

2

❖ Collis

4-party transactions

❖ And sometimes Service Providers need competitors in order to deliver their service...
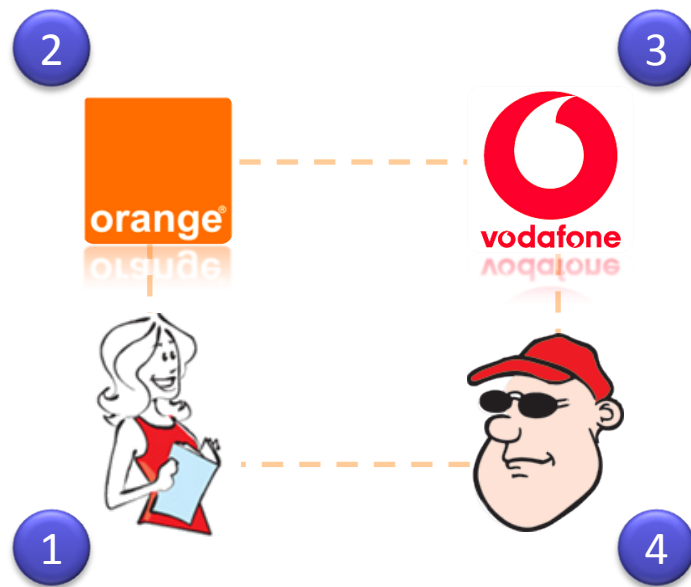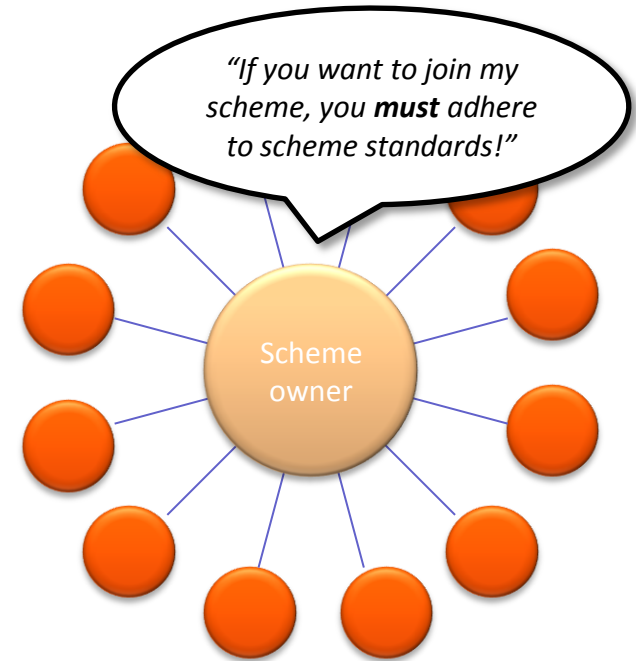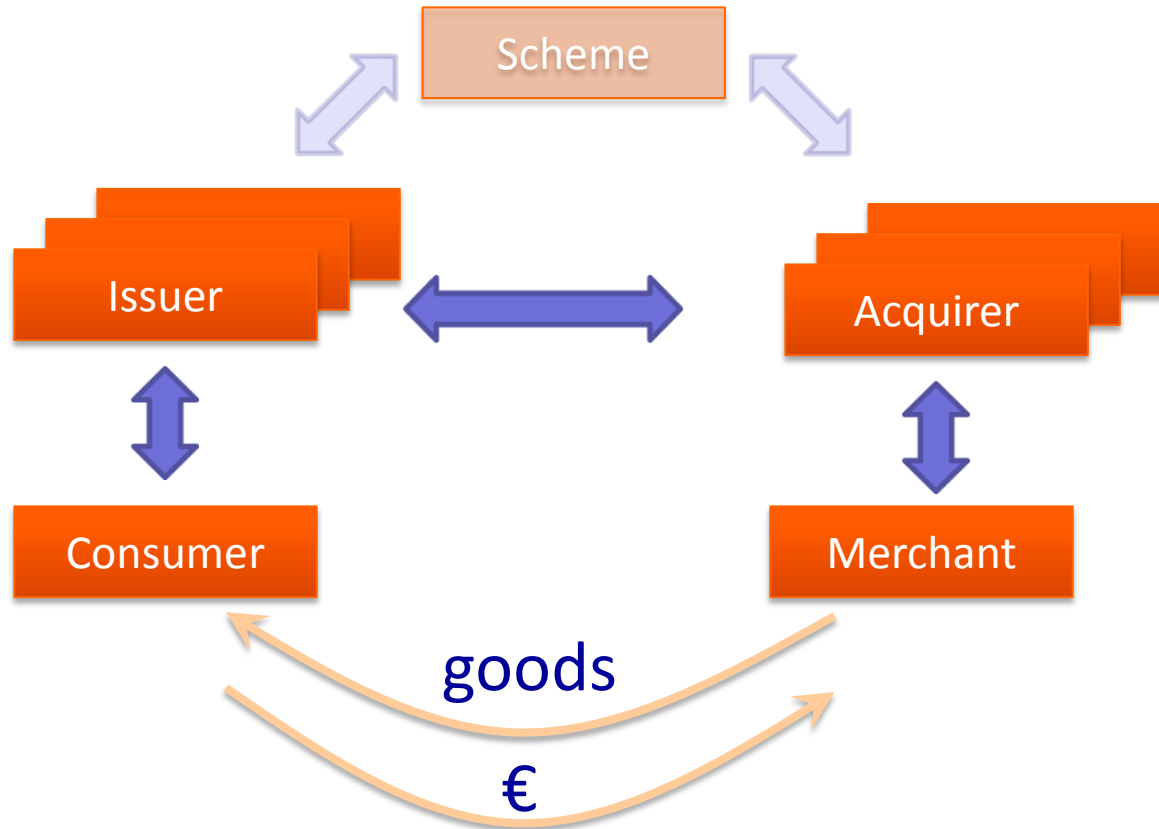
A transaction scheme (1)

❖ Bilateral   &   Multilateral
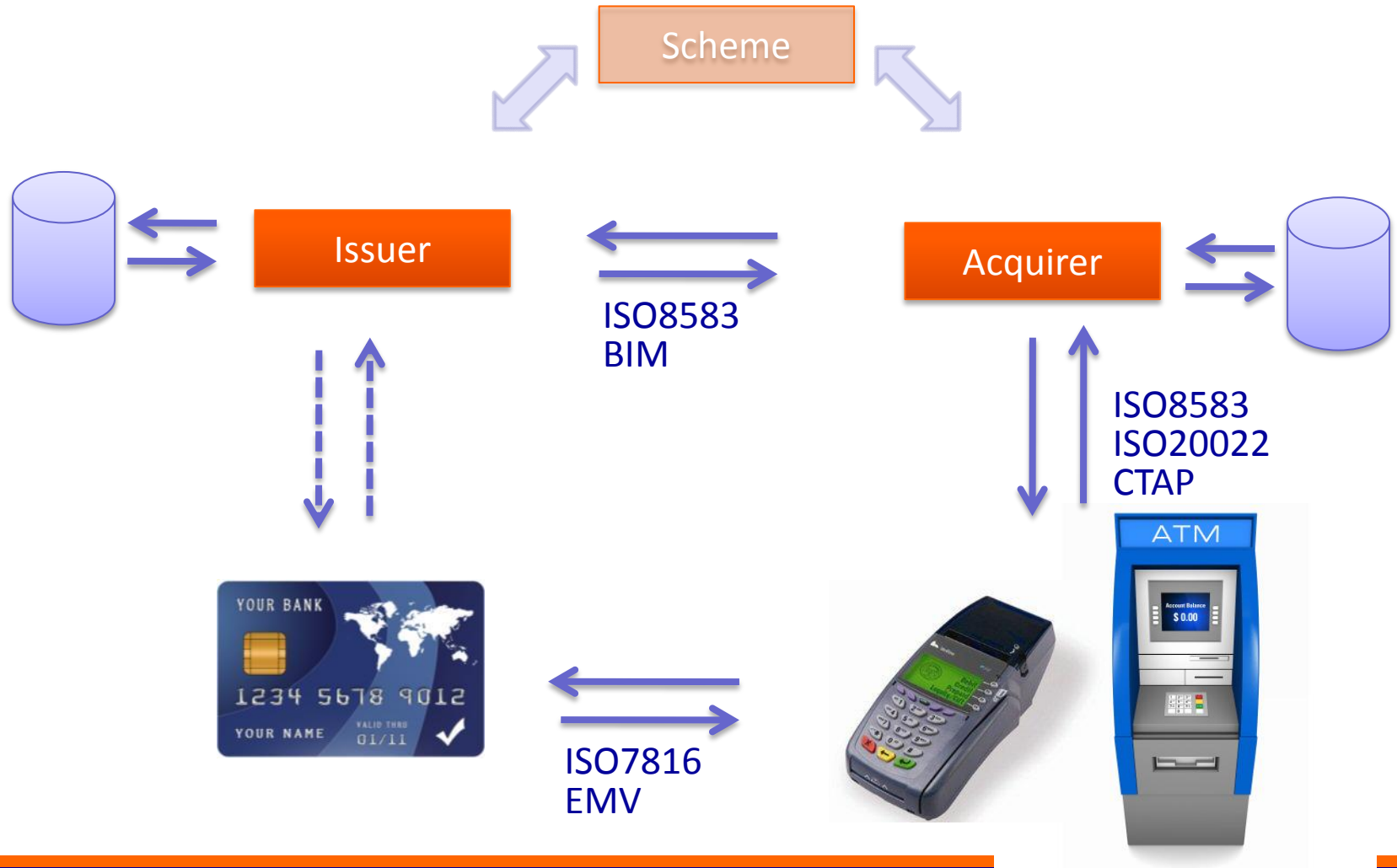
A transaction scheme (2)

❖ Another way to look at it …

Transaction System Testing

❖ **Payment Infrastructure (e.g. PIN, Visa, Meastro)**

- Hard- and software involved
- More party model: Card Holder, Issuers, Acquirers, Merchant, ..
- Security important
- Stability as well (also under stress/load)
- Infrastructure managed by more than one party
- Being offline, even for a short period, is not an option
- Good Change and releasemanagement important

❖ **Very similar for non payment Tx Systems**

Example of the infrastructure

Scheme

Issuer

Acquirer

ISO8583
BIM

ISO8583
ISO20022
CTAP

ISO7816
EMV

ATM

YOUR BANK
1234 5678 9012
YOUR NAME
VALID THRU 01/11

Comparison in focus

❖ Types of testing

| Client-Server App.	Payment System
Functionality	Interoperability
Usability	Data protocols
Security	Conformance
Stability	Certification
	Security
	Stability

Test Process for Secure Tx. Systems

Test Process:

❖ Component testing

❖ Security Evaluation

❖ Integration testing / E-2-E testing

❖ The focus is very much on the first two steps …

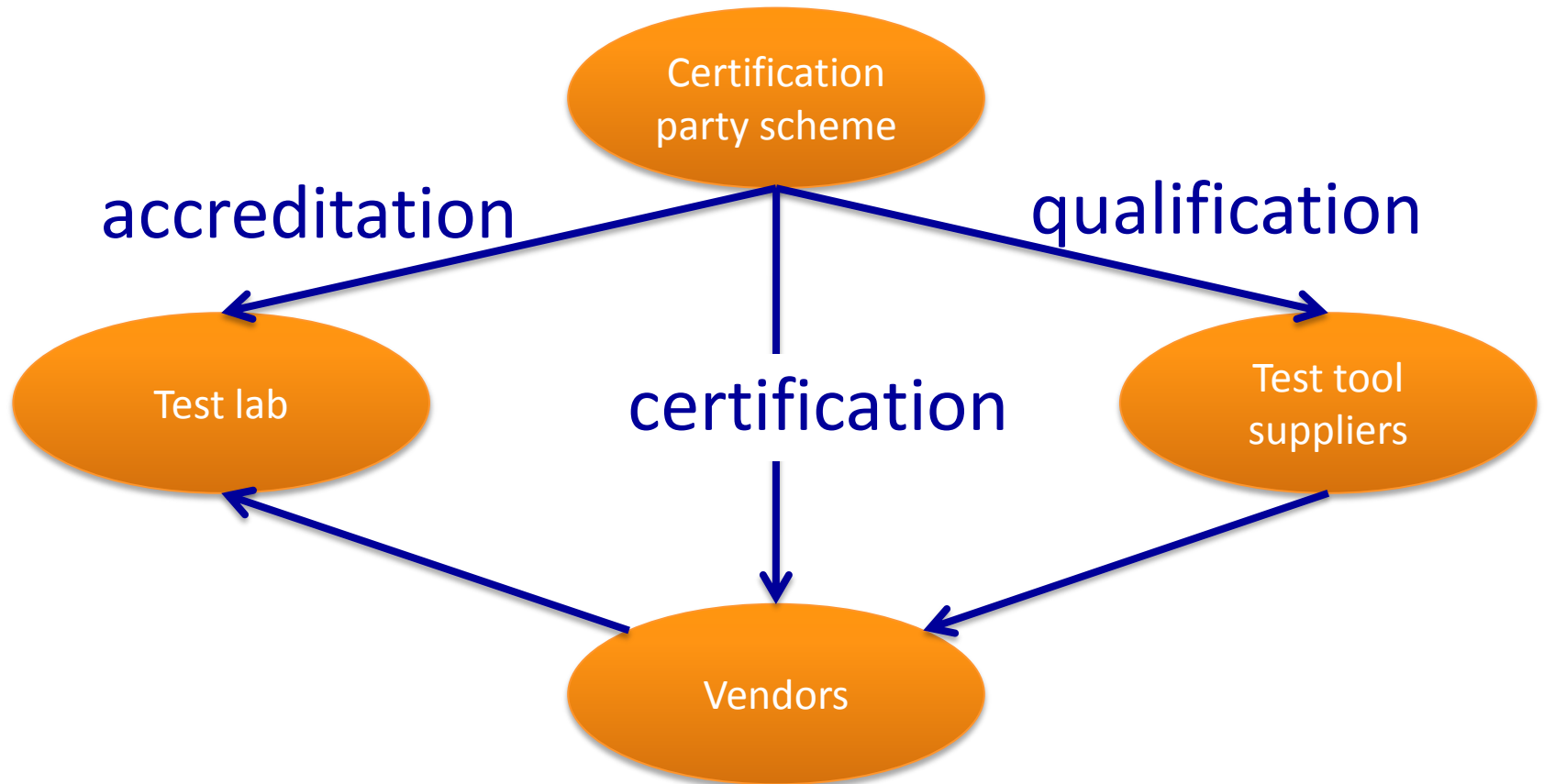❖ Collis focuses on the first and the last

❖ **Collis**

Component testing

❖ The functional testing of a component focuses on conformance to standards (ISO, Visa, …)
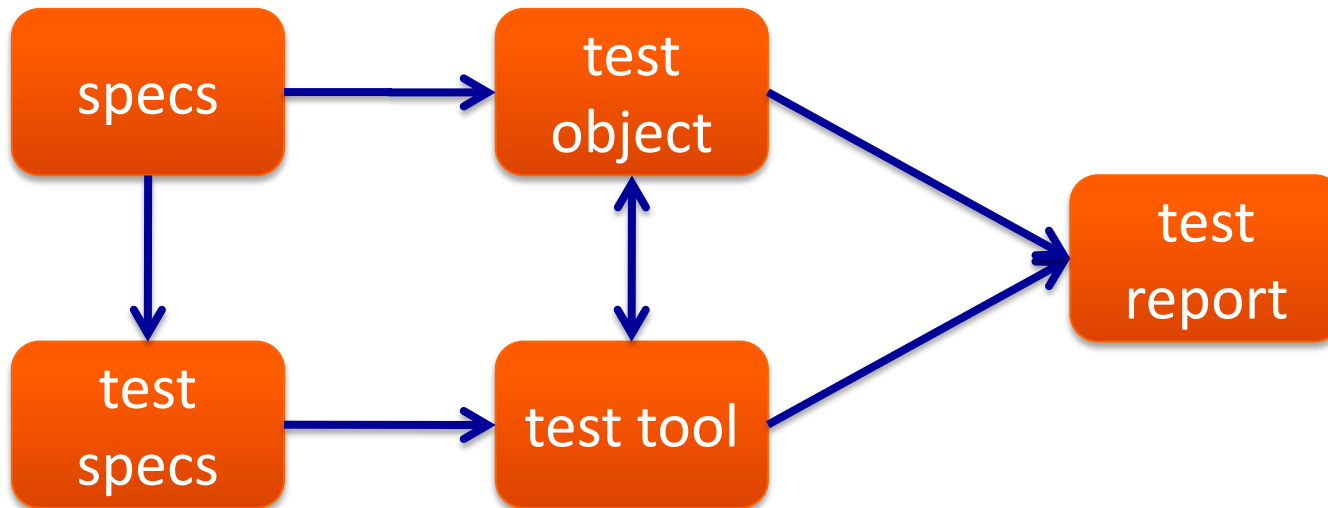
Component Certification Process
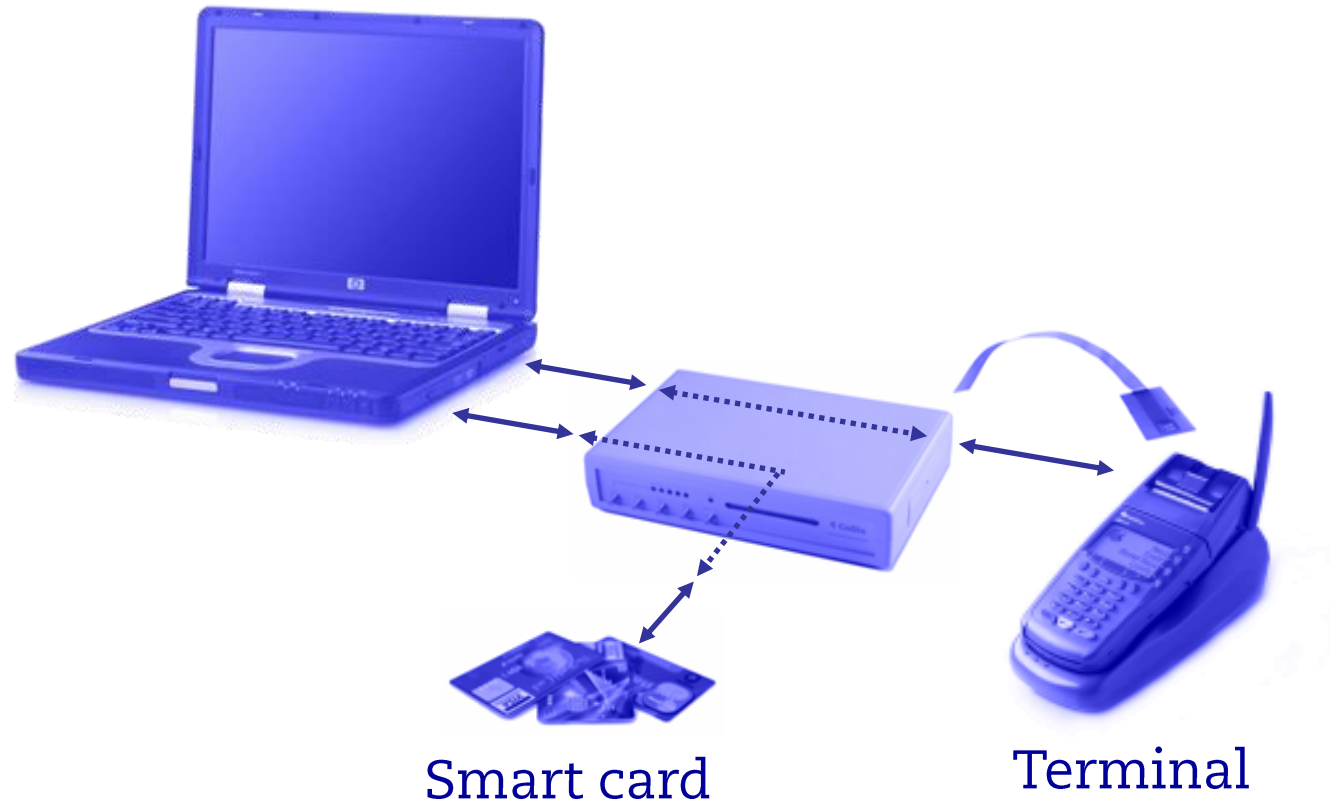
❖ Roles & Responsibilities
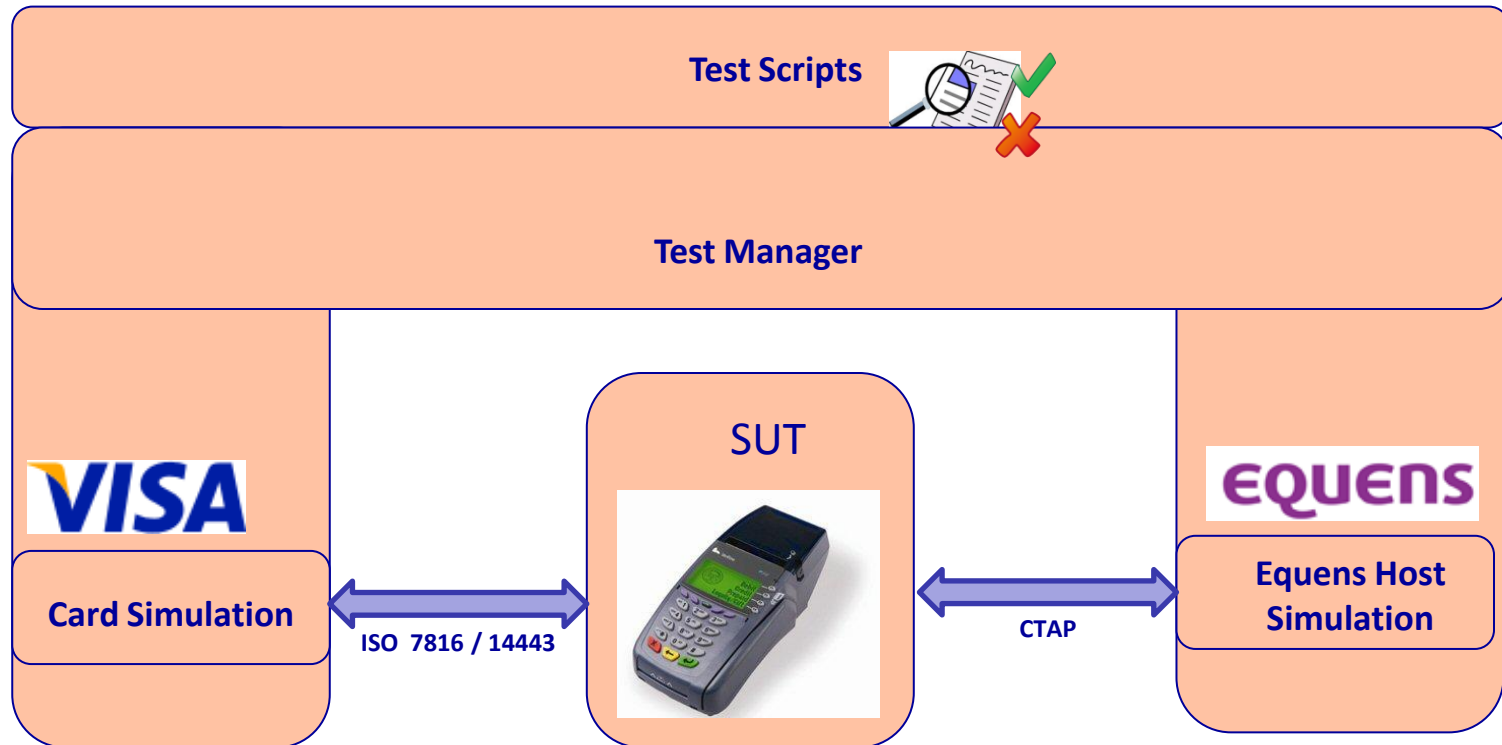
Component testing: Various levels

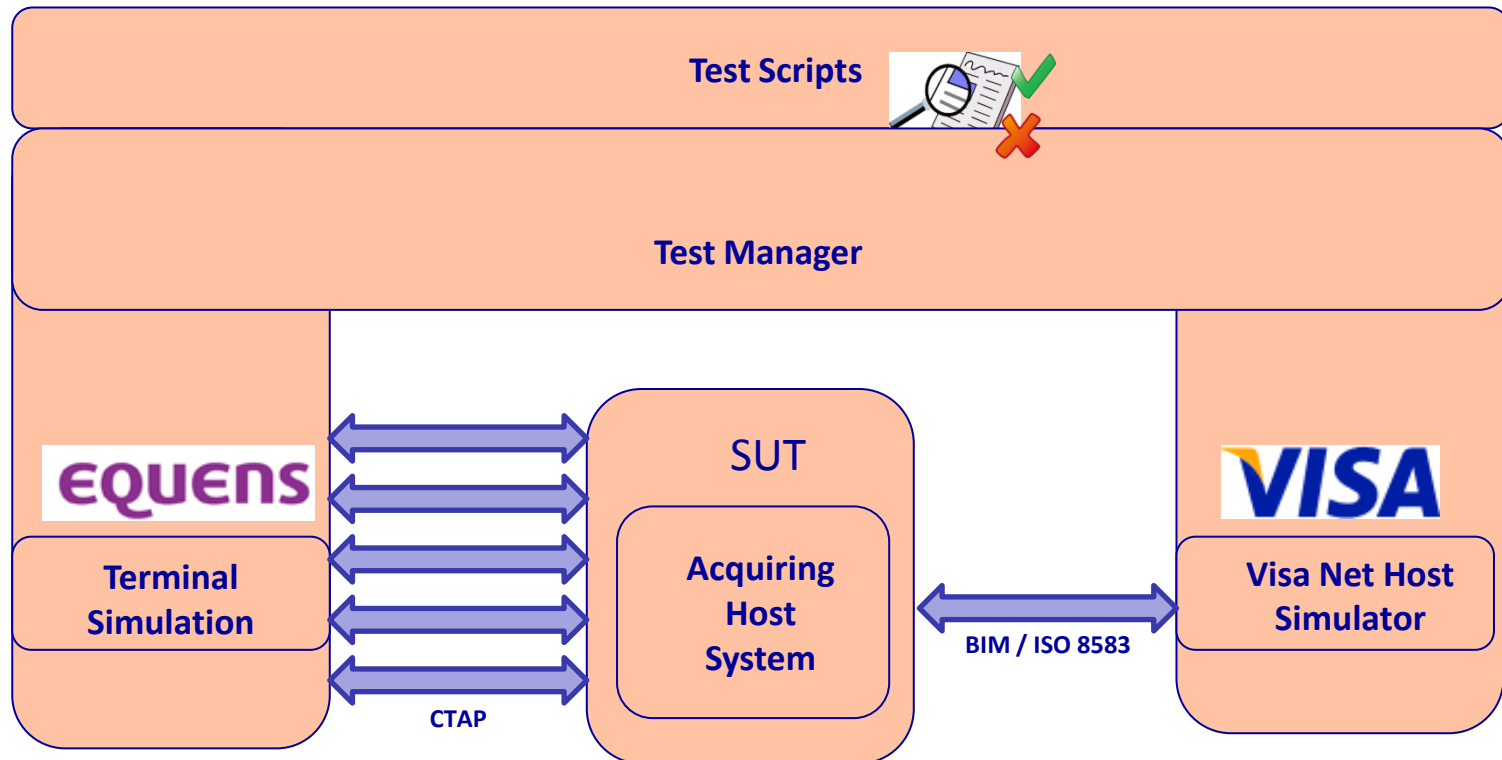❖ Testing Secure Transaction Systems is done at various levels

Component testing: Simulators

Smart card   Terminal

Component testing: Test Harness

Test Scripts

Test Manager

SUT

VISA

Card Simulation

ISO 7816 / 14443

CTAP

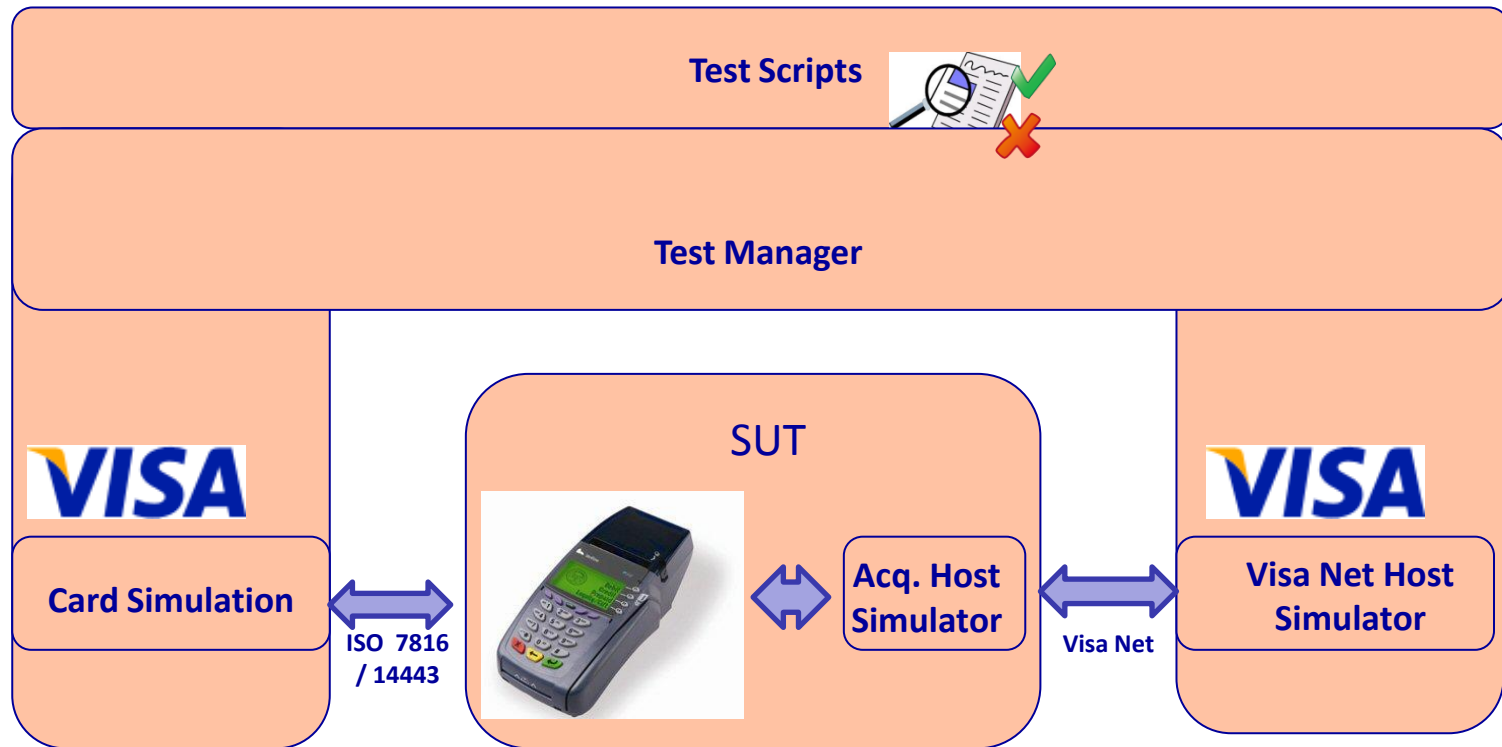**EQUENS**

Equens Host Simulation

Acquiring Host System Testing
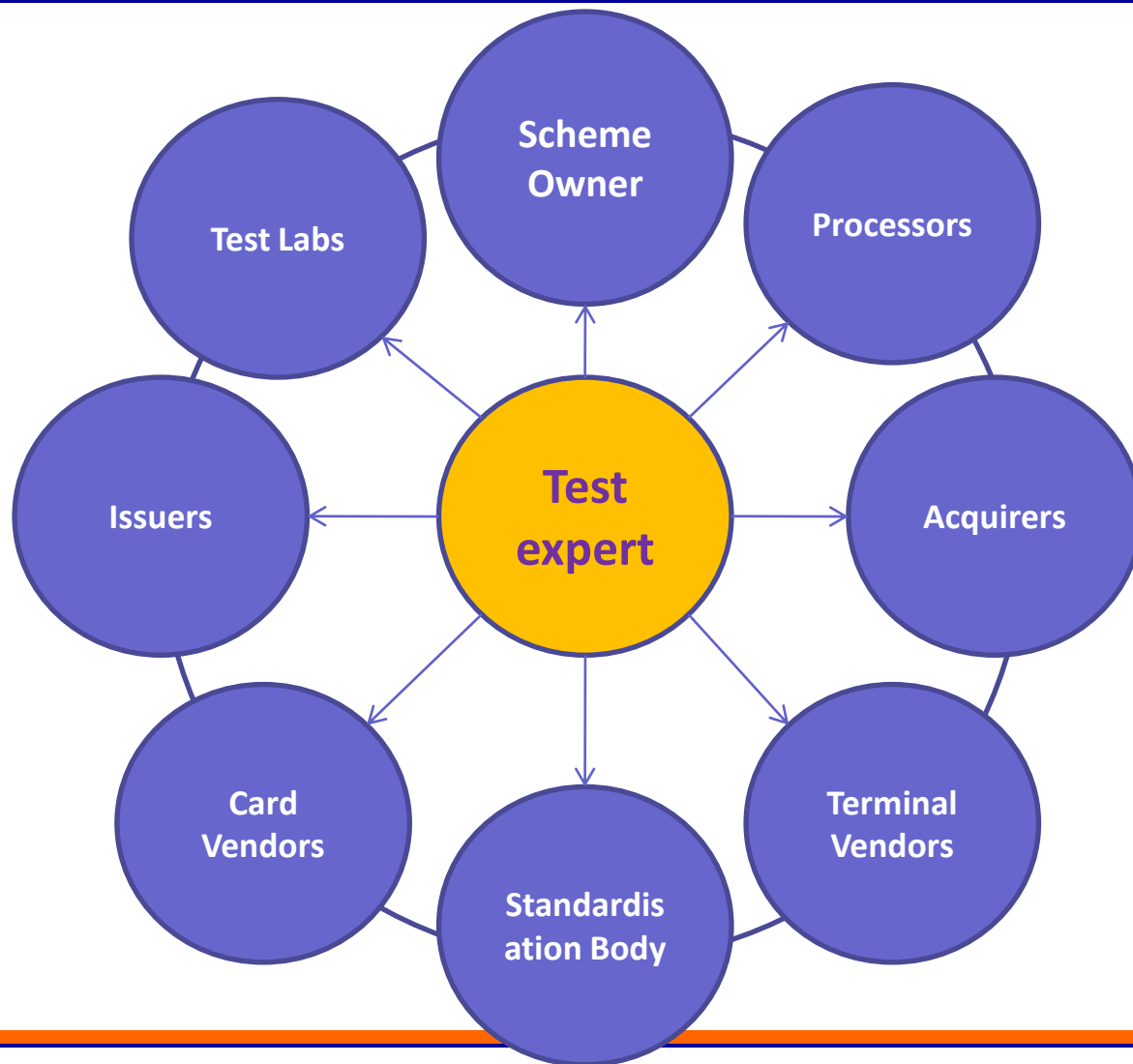
Integration / end-to-end testing

❖ *The final confirmation …*

Examples of 'Tx System bugs'

- ❖ Hardware not compliant to the standard → replacement

- ❖ Certificate of the card expires before the card expires

- ❖ Reading secret keys on chip by creating a file with size 'FF FF'

- ❖ Mixing test keys and production keys

❖ **Collis**

Testing very central …

We learned …

❖ Testing secure transactions systems means

- Multiparty model with (Open) Standards
- Component Testing / conformance testing essential
- Also linked to Interoperability & security
- Security Evaluation essential
- Certification Processes
- Special Hardware / Firmware required
- Load & Performance of Central Systems essential

❖ Is this boring or Interesting? Up to you!

❖ We like it!

Collis

Questions?

Heuvel@collis.nl

www.collis.nl

❖ **Collis**