Mutual Attestation of IoT Devices

TCG Members Meeting June 2015 Edinburgh

Prof. Andreas Steffen
Institute for Internet Technologies and Applications
HSR University of Applied Sciences Rapperswil
andreas.steffen@hsr.ch

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

strongSwan

Where the heck is Rapperswil?

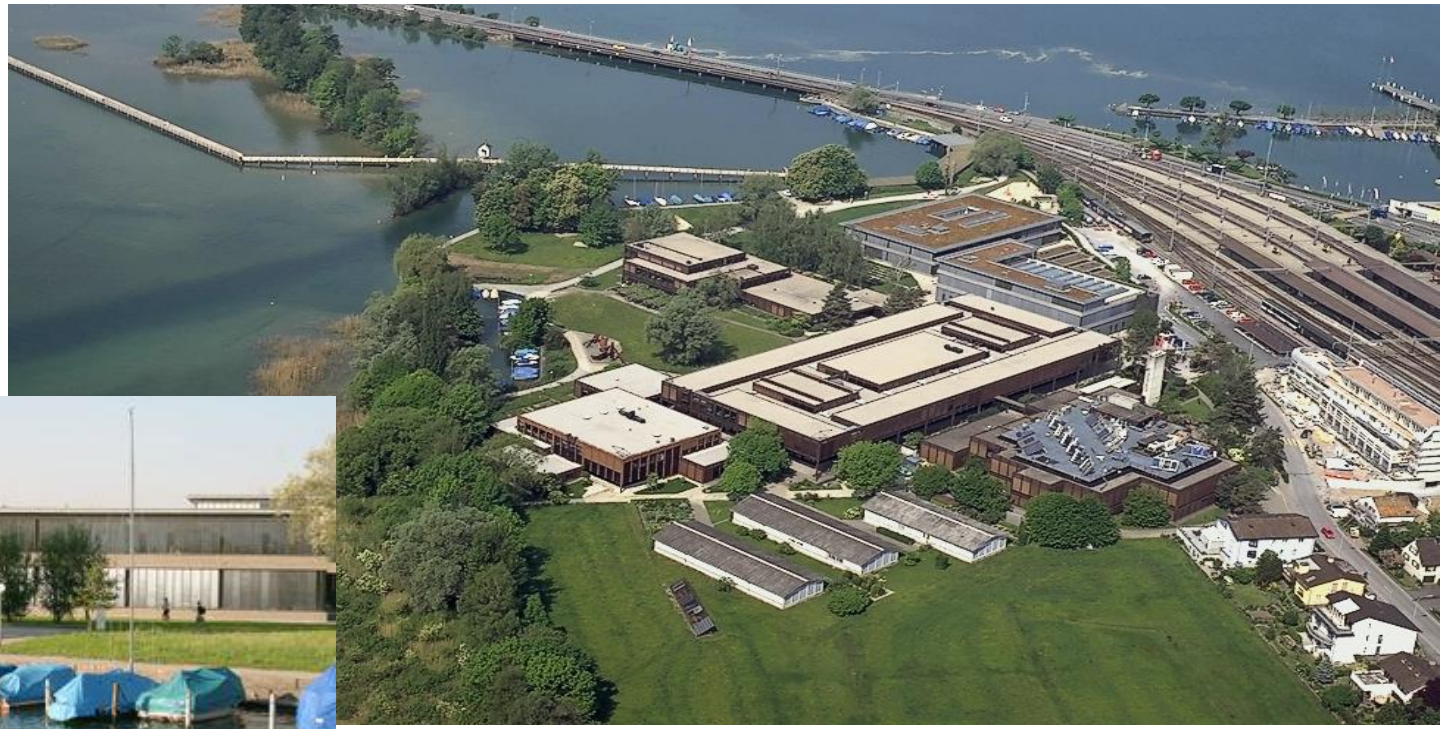
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

HSR - Hochschule für Technik Rapperswil

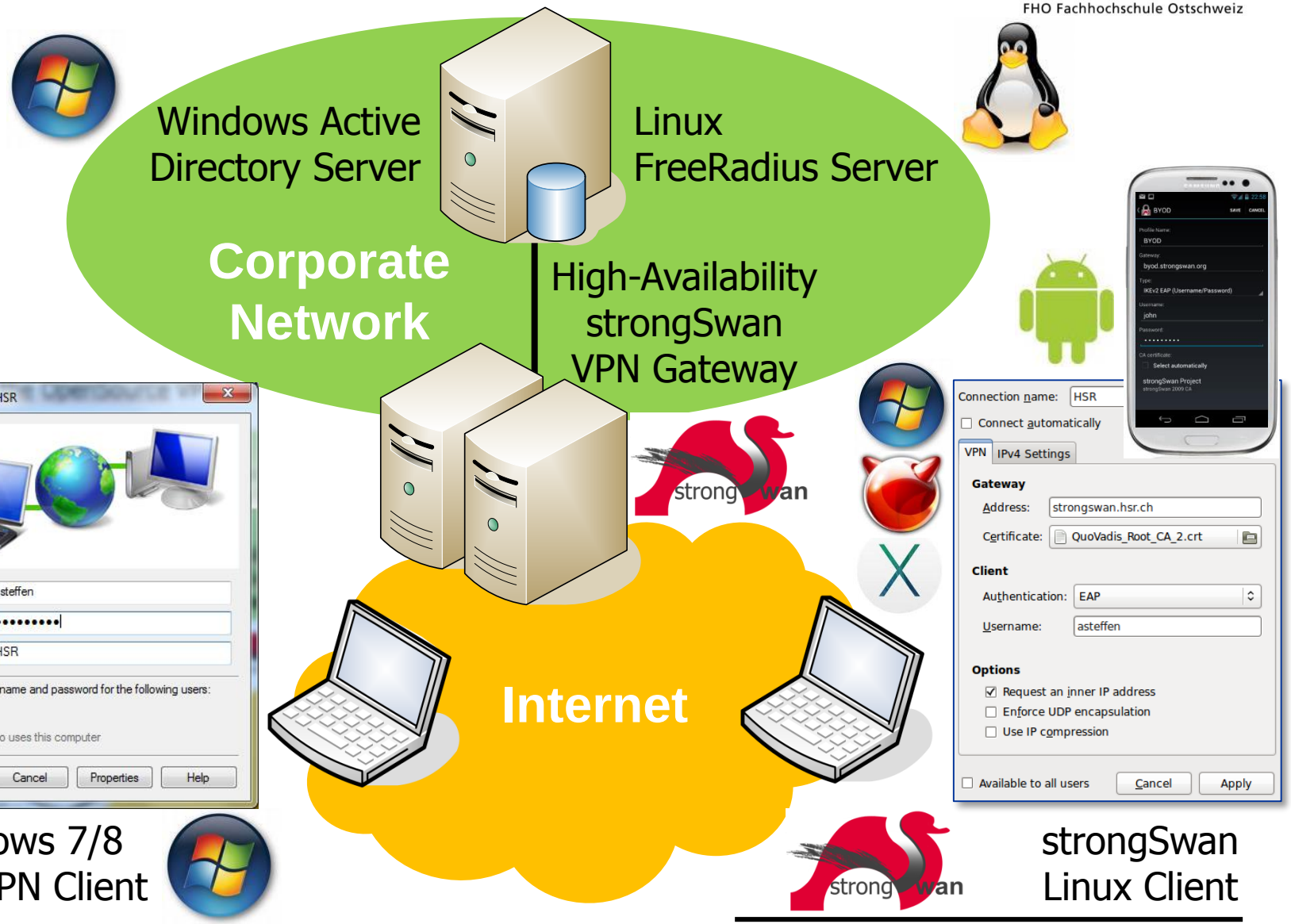
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

- University of Applied Sciences with about 1500 students
- Faculty of Information Technology (300-400 students)
- Bachelor Course (3 years), Master Course (+1.5 years)



strongSwan – the OpenSource VPN Solution

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz



Windows 7/8 Agile VPN Client

strongSwan Linux Client

Mutual Attestation of IoT Devices

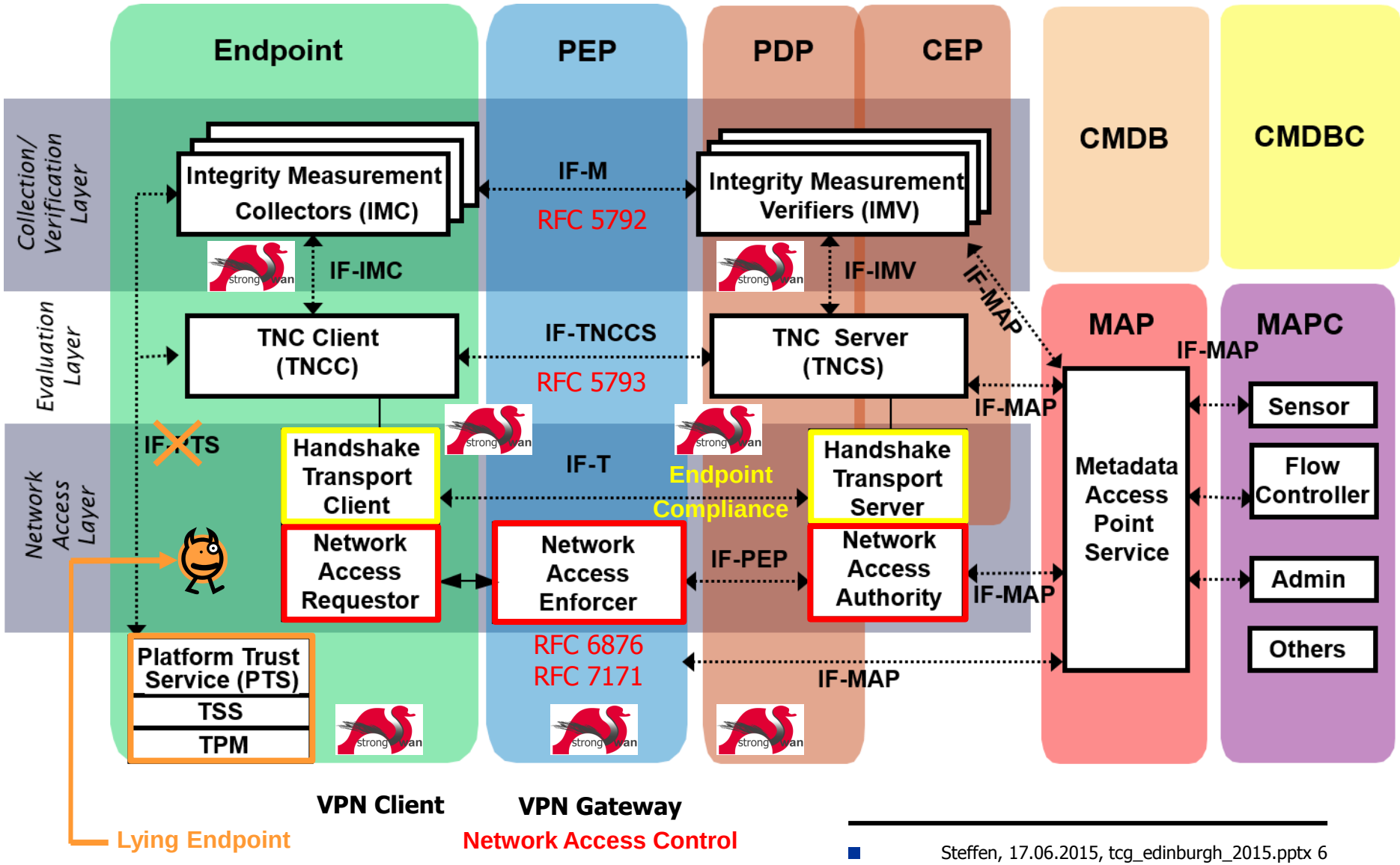
TCG Members Meeting June 2015 Edinburgh

Trusted Network Communications (TNC)
Current Use Cases:
Network Access Control & Endpoint Compliance

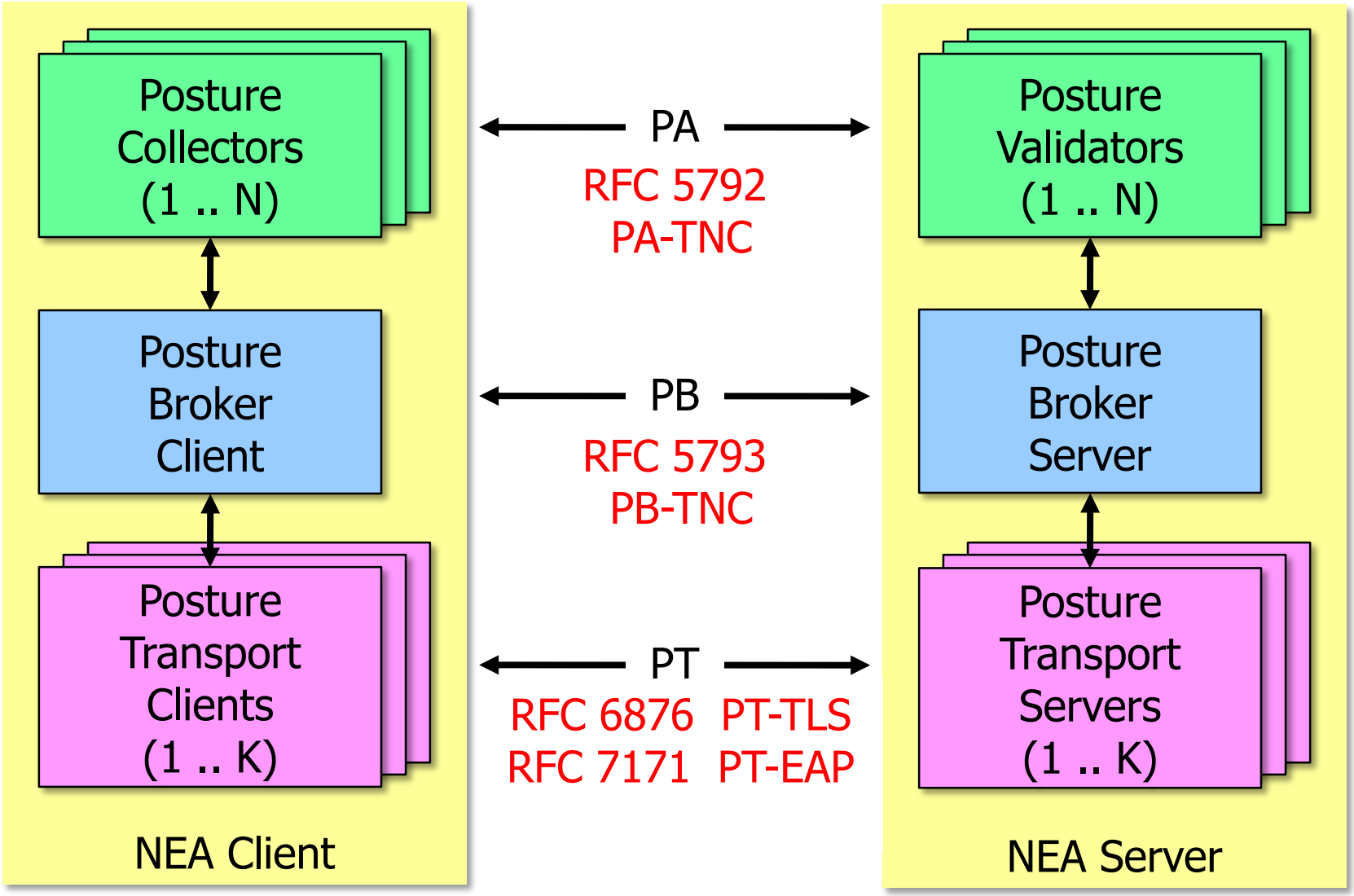
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

TNC Architecture



Network Endpoint Assessment (RFC 5209)



Layered TNC Protocol Stack

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- TNC Measurement Data

```
[IMV] operating system name is 'Android' from vendor Google
[IMV] operating system version is '4.2.1'
[IMV] device ID is cf5e4cbcc6e6a2db
```

- IF-M Measurement Protocol — PA-TNC (RFC 5792)

```
[TNC] handling PB-PA message type 'IETF/Operating System' 0x000000/0x00000001
[IMV] IMV 1 "OS" received message for Connection ID 1 from IMC 1
[TNC] processing PA-TNC message with ID 0xec41ce1d
[TNC] processing PA-TNC attribute type 'IETF/Product Information' 0x000000/0x00000002
[TNC] processing PA-TNC attribute type 'IETF/String Version' 0x000000/0x00000004
[TNC} processing PA-TNC attribute type 'ITA-HSR/Device ID' 0x00902a/0x00000008
```

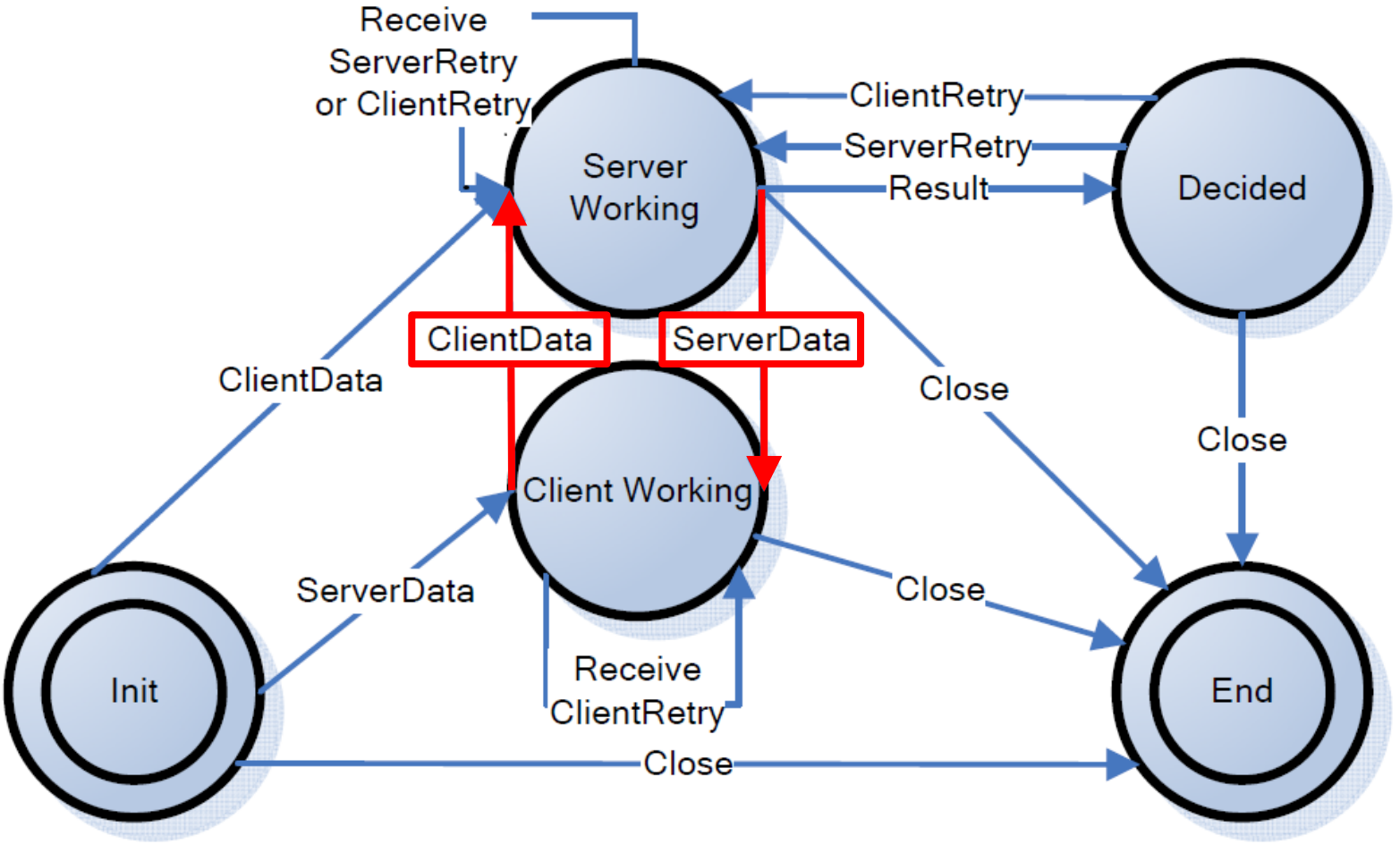
- IF-TNCCS TNC Client-Server Protocol — PB-TNC (RFC 5793)

```
[TNC] received TNCCS batch (160 bytes) for Connection ID 1
[TNC] PB-TNC state transition from 'Init' to 'Server Working'
[TNC] processing PB-TNC CDATA batch
[TNC] processing PB-Language-Preference message (31 bytes)
[TNC] processing PB-PA message (121 bytes)
[TNC] setting language preference to 'en'
```

- IF-T Transport Protocol — PT-EAP (RFC 7171)

```
[NET] received packet: from 152.96.15.29[50871] to 77.56.144.51[4500] (320 bytes)
[ENC] parsed IKE_AUTH request 8 [ EAP/RES/TTLS ]
[IKE] received tunneled EAP-TTLS AVP [EAP/RES/PT]
```

PB-TNC / IF-TNCCS 2.0 State Machine



Exchange of PB-TNC Client/Server Data Batches containing PA-TNC Messages

Mutual Attestation of IoT Devices

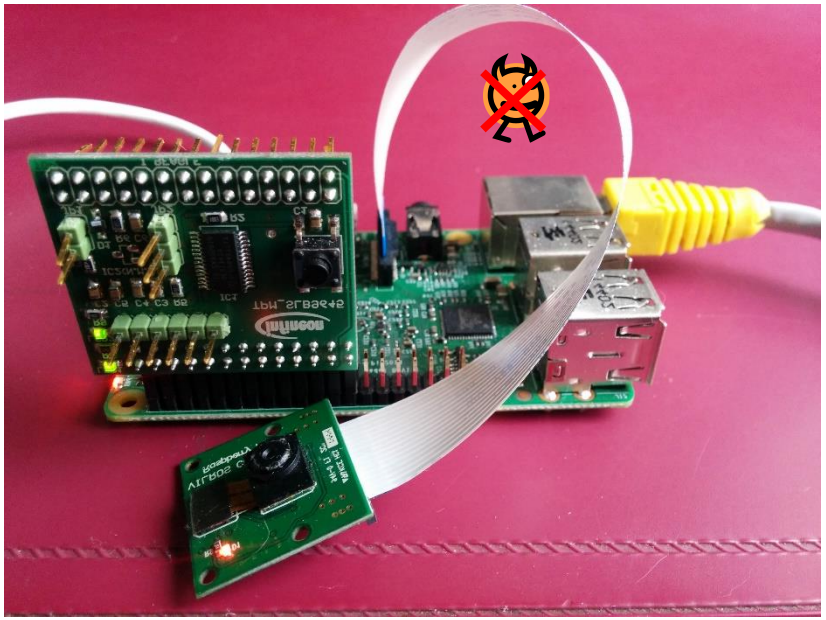
TCG Members Meeting June 2015 Edinburgh

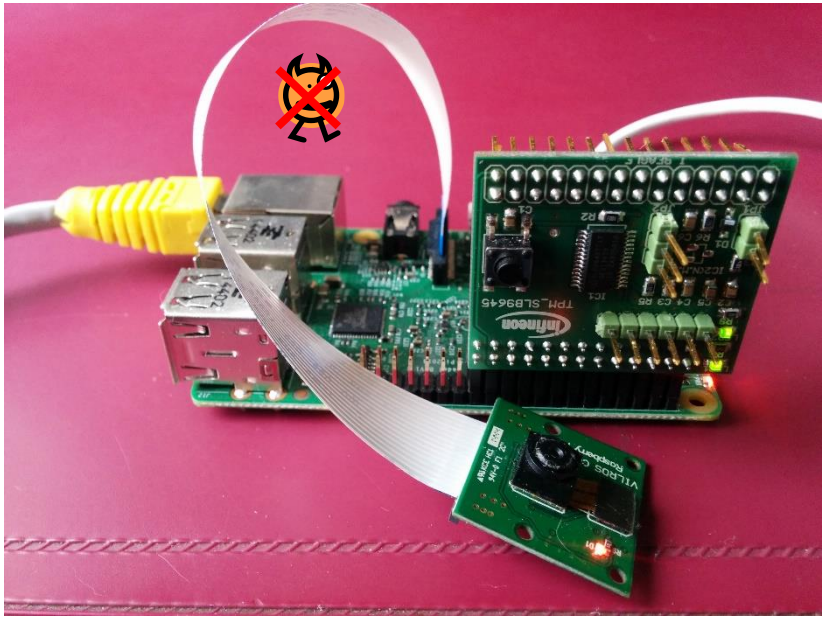
Trusted Network Communications (TNC)
New Use Case:
Mutual Measurements of Endpoints

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

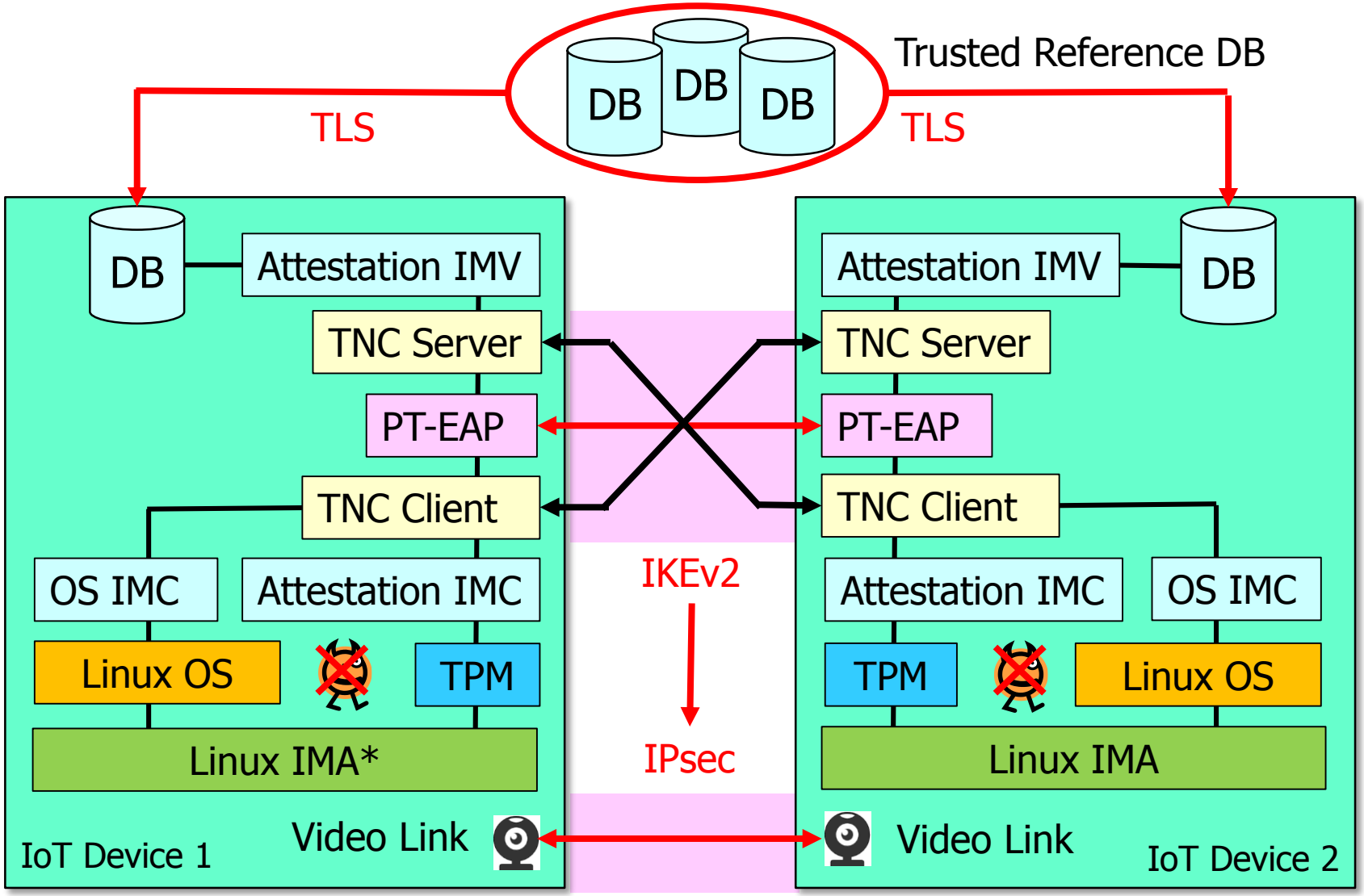
Example: Mutually Trusted Video Phones





Mutual Attestation of IoT Devices

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz



* IMA: Integrity Measurement Architecture

Why do Mutual TNC Measurements work?

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Definition of PB-TNC Batch Header in RFC 5793

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Version    |D|     Reserved                          | B-Type|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Batch Length                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Directionality (D) (1 bit)

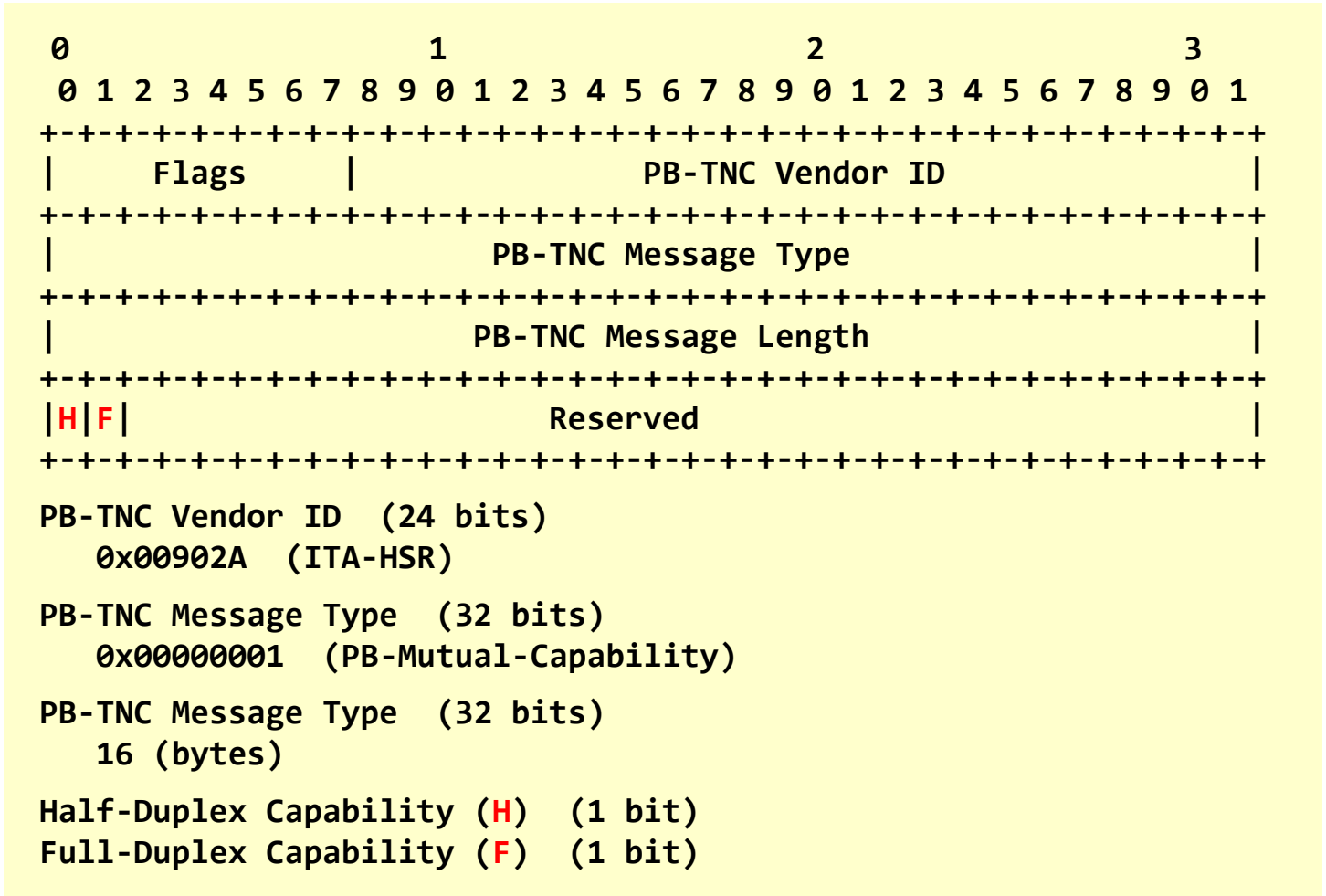
When a Posture Broker Client is sending this message, the Directionality bit MUST be set to 0.
When a Posture Broker Server is sending this message, the Directionality bit MUST be set to 1.
This helps avoid any situation where two Posture Broker Clients or two Posture Broker Servers engage in a dialog. It also helps with debugging.

- Idea: Use the Directionality Flag to multiplex two IF-TNCCS 2.0 connections in opposite directions over a common IF-T transport channel.

PB-TNC Mutual Capability Announcement

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- PB-Mutual-Capability Message defined in ITA-HSR Namespace



Mutual Measurements in Half-Duplex Mode

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

Initiator		PB-TNC Batch[PB-TNC Messages]		Responder
TNC Client	→	CDATA[PB-MUTUAL, PB-PA]	→	TNC Server
TNC Client	←	SDATA[PB-MUTUAL, PB-PA]	←	TNC Server
TNC Server	→	SDATA[]	→	TNC Client
TNC Server	←	CDATA[PB-PA]	←	TNC Client
TNC Client	→	CDATA[PB-PA]	→	TNC Server
TNC Client	←	RESULT[PB-ASSESSMENT]	←	TNC Server
TNC Server	→	SDATA[PB-PA]	→	TNC Client
TNC Server	←	CDATA[PB-PA]	←	TNC Client
TNC Server	→	RESULT[PB-ASSESSMENT]	→	TNC Client
TNC Server	←	CLOSE[]	←	TNC Client
TNC Client	→	CLOSE[]	→	TNC Server

- The initiating TNC client sends CLOSE batch last
- Works over PT-EAP and PT-TLS

Mutual Measurements in Full-Duplex Mode

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

Initiator		PB-TNC Batch[PB-TNC Messages]		Responder
TNC Client	→	CDATA[PB-MUTUAL, PB-PA]	→	TNC Server
TNC Client	←	SDATA[PB-MUTUAL, PB-PA]	←	TNC Server
TNC Server	←	CDATA[PB-PA]	←	TNC Client
TNC Client	→	CDATA[PB-PA]	→	TNC Server
TNC Server	→	SDATA[PB-PA]	→	TNC Client
TNC Client	←	RESULT[PB-ASSESSMENT]	←	TNC Server
TNC Server	←	CDATA[PB-PA]	←	TNC Client
TNC Server	→	RESULT[PB-ASSESSMENT]	→	TNC Client
TNC Server	←	CLOSE[]	←	TNC Client
TNC Client	→	CLOSE[]	→	TNC Server

- The initiating TNC client sends CLOSE batch last
- Works over PT-TLS only

Conclusions

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Mutual TNC measurements can be easily implemented without changes in the existing PB-TNC IETF standard.
- The announcement of the mutual TNC measurement capability is done via a PB-Mutual-Capability PB-TNC message currently defined in the ITA-HSR namespace.
- If the mutual TNC measurement capability is of general interest then the announcement message should be standardized either in the TCG or IETF namespace.
- Another interesting use case for the mutual measurement capability would be an initiating endpoint wanting to attest a cloud server before connecting to it.

Thank you for your attention!

Questions?

www.strongswan.org/tnc/