Mutual Attestation of IoT Devices

Connect Security World September 2016 Marseille

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

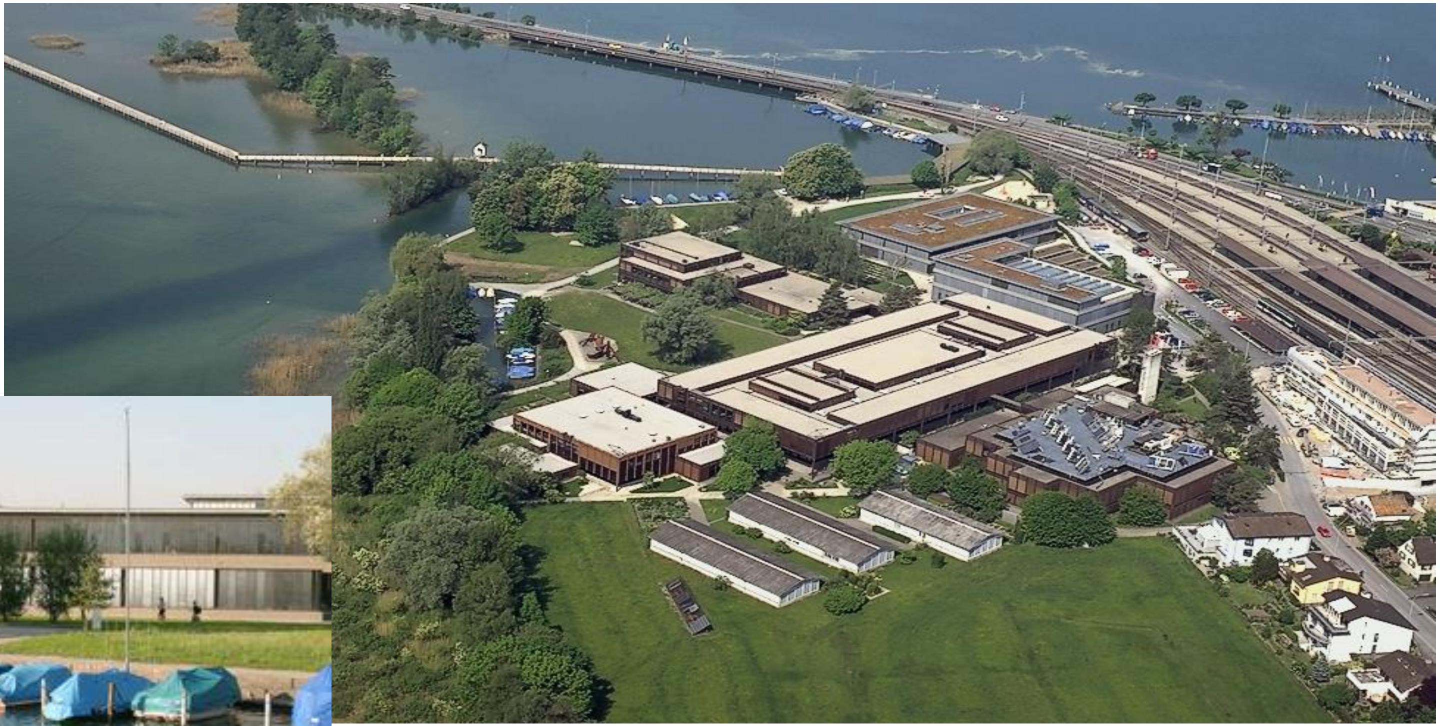
strongswan

HSR - Hochschule für Technik Rapperswil

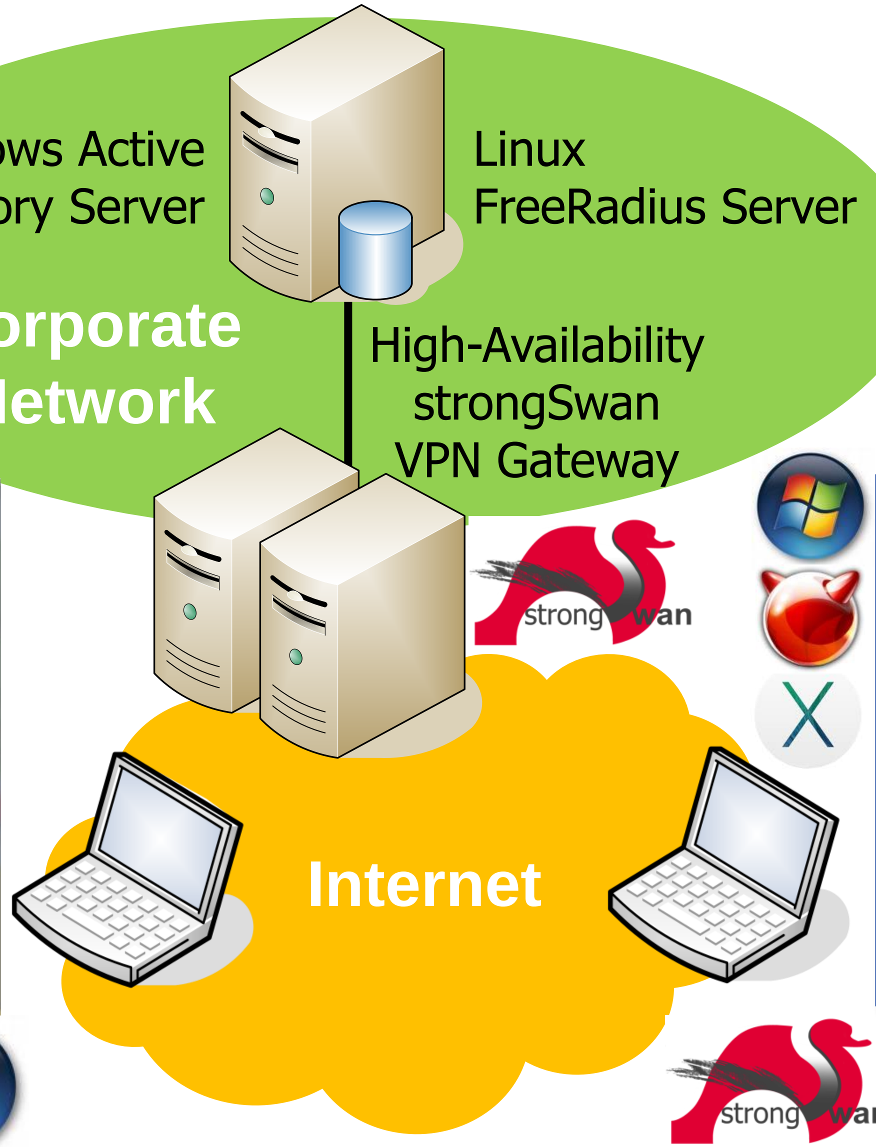
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

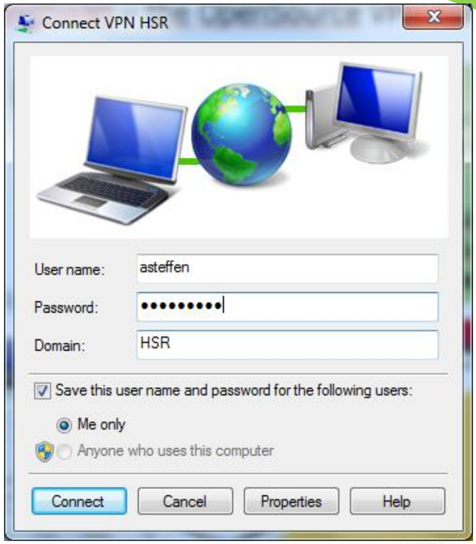
FHO Fachhochschule Ostschweiz

- Swiss 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


Windows Active Directory Server
Linux FreeRadius Server
Corporate Network
High-Availability strongSwan VPN Gateway
strongSwan
Internet



Connect VPN HSR

User name: asteffen

Password: •••••••••

Domain: HSR

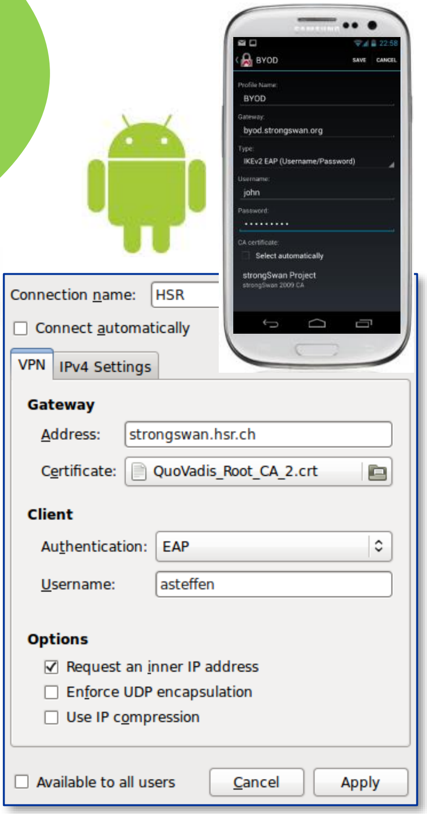
☑ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

Connect | Cancel | Properties | Help

Windows 7/8/10
Agile VPN Client



BYOD SAVE CANCEL

Profile Name: BYOD

Gateway: byod.strongswan.org

Type: IKEv2 EAP (Username/Password)

Username: john

Password: •••••••••

CA certificate: □ Select automatically

strongSwan Project
strongSwan 2009 CA

Connection name: HSR

□ Connect automatically

VPN | IPv4 Settings

Gateway

Address: strongswan.hsr.ch

Certificate: QuoVadis_Root_CA_2.crt

Client

Authentication: EAP

Username: asteffen

Options

☑ Request an inner IP address

□ Enforce UDP encapsulation

□ Use IP compression

□ Available to all users

Cancel | Apply

strongSwan
Linux Client

Mutual Attestation of IoT Devices

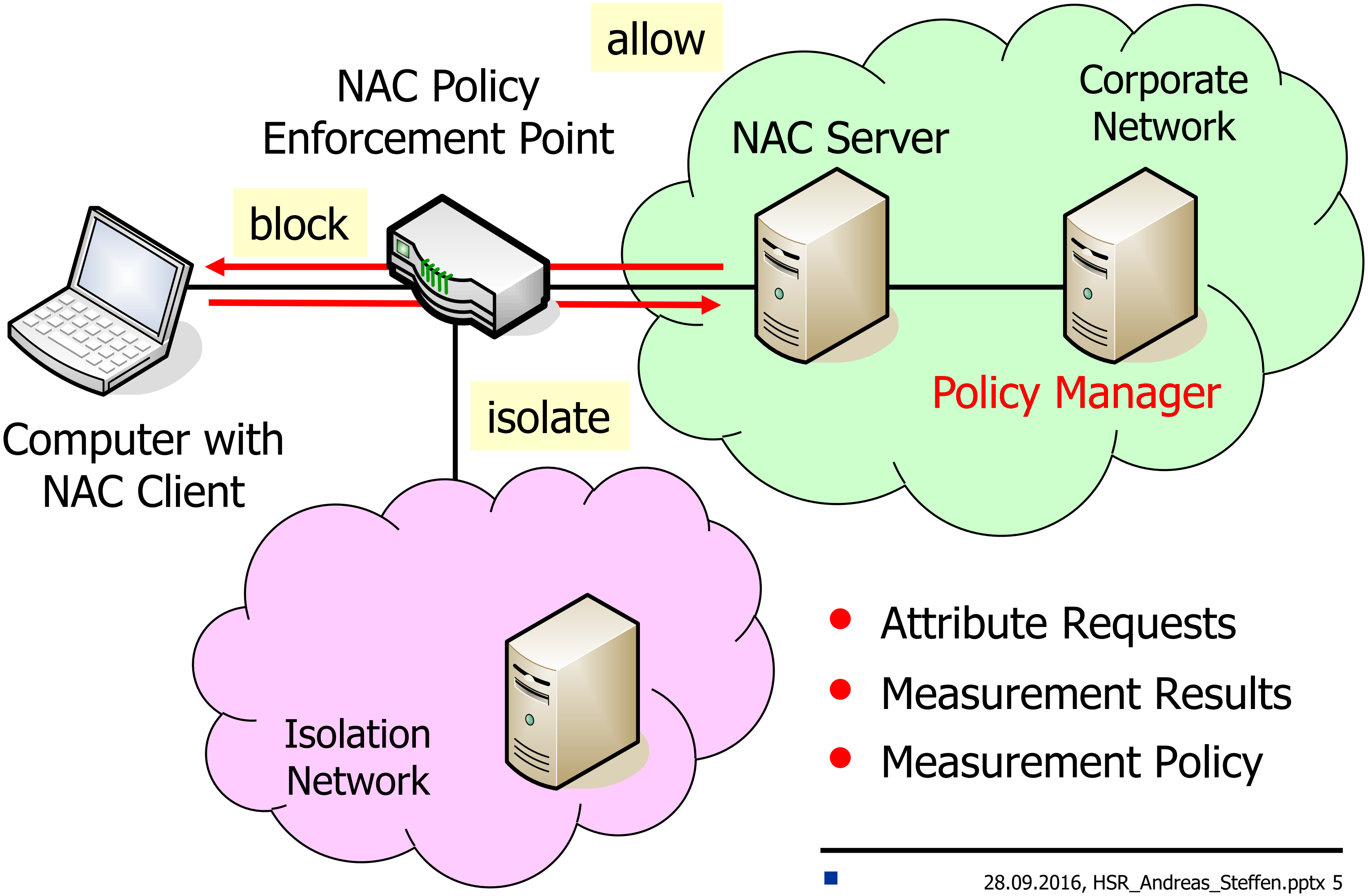
Connect Security World September 2016 Marseille

The Standards:
IETF Network Endpoint Assessment (NEA)
TCG Trusted Network Connect (TNC)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

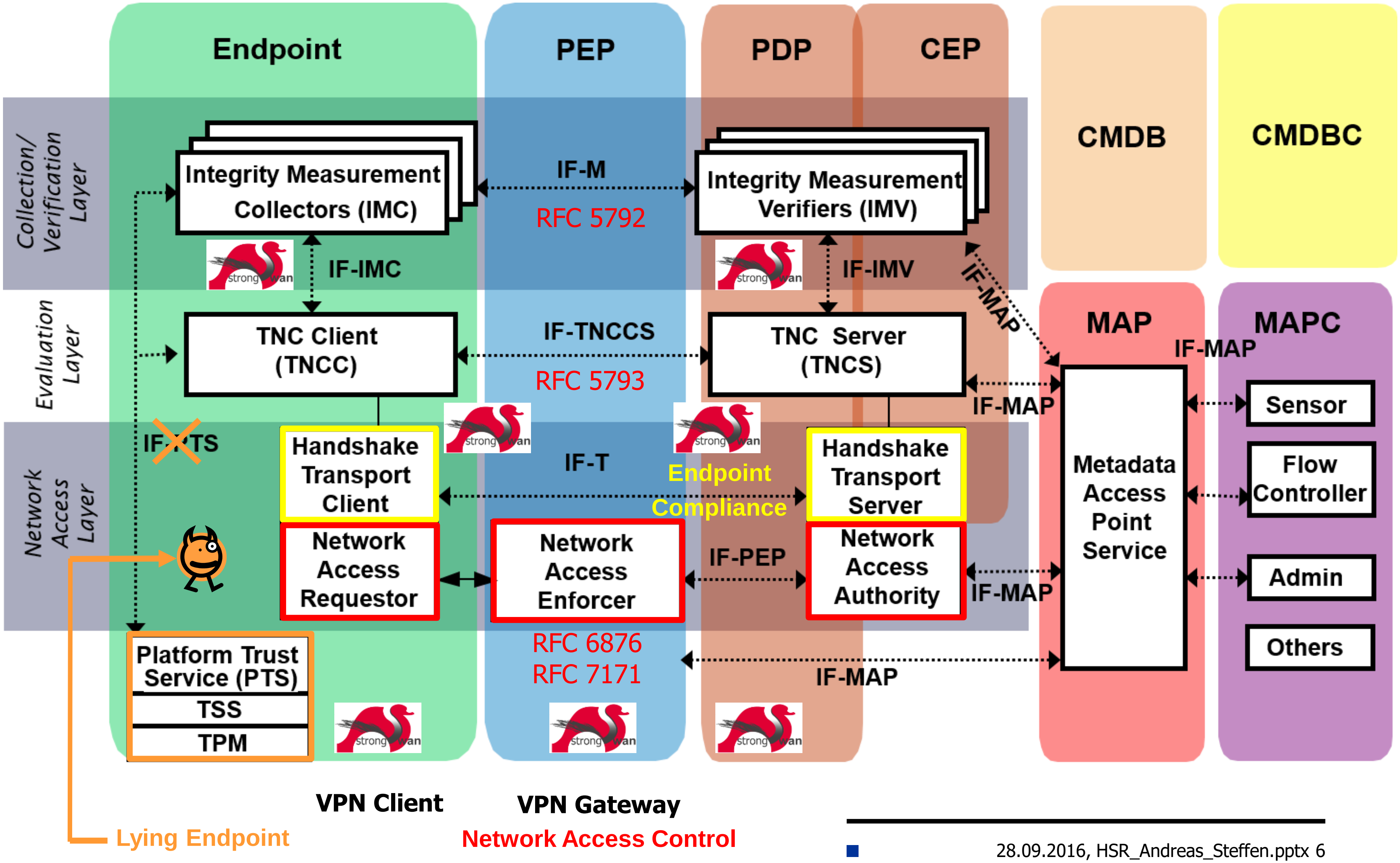
FHO Fachhochschule Ostschweiz

Network Access Control (NAC)



- Attribute Requests
- Measurement Results
- Measurement Policy

TCG TNC Architecture



Endpoint

PEP

PDP

CEP

CMDB

CMDBC

Collection/ Verification Layer

Evaluation Layer

Network Access Layer

Integrity Measurement Collectors (IMC)

IF-M

RFC 5792

Integrity Measurement Verifiers (IMV)

IF-IMC

IF-IMV

IF-MAP

MAP

MAPC

TNC Client (TNCC)

IF-TNCCS

RFC 5793

TNC Server (TNCS)

IF-MAP

IF-MAP

Sensor

IF-PTS

Handshake Transport Client

IF-T

Endpoint Compliance

Handshake Transport Server

Metadata Access Point Service

Flow Controller

Network Access Requestor

Network Access Enforcer

IF-PEP

Network Access Authority

IF-MAP

Admin

Platform Trust Service (PTS)

TSS

TPM

RFC 6876

RFC 7171

IF-MAP

Others

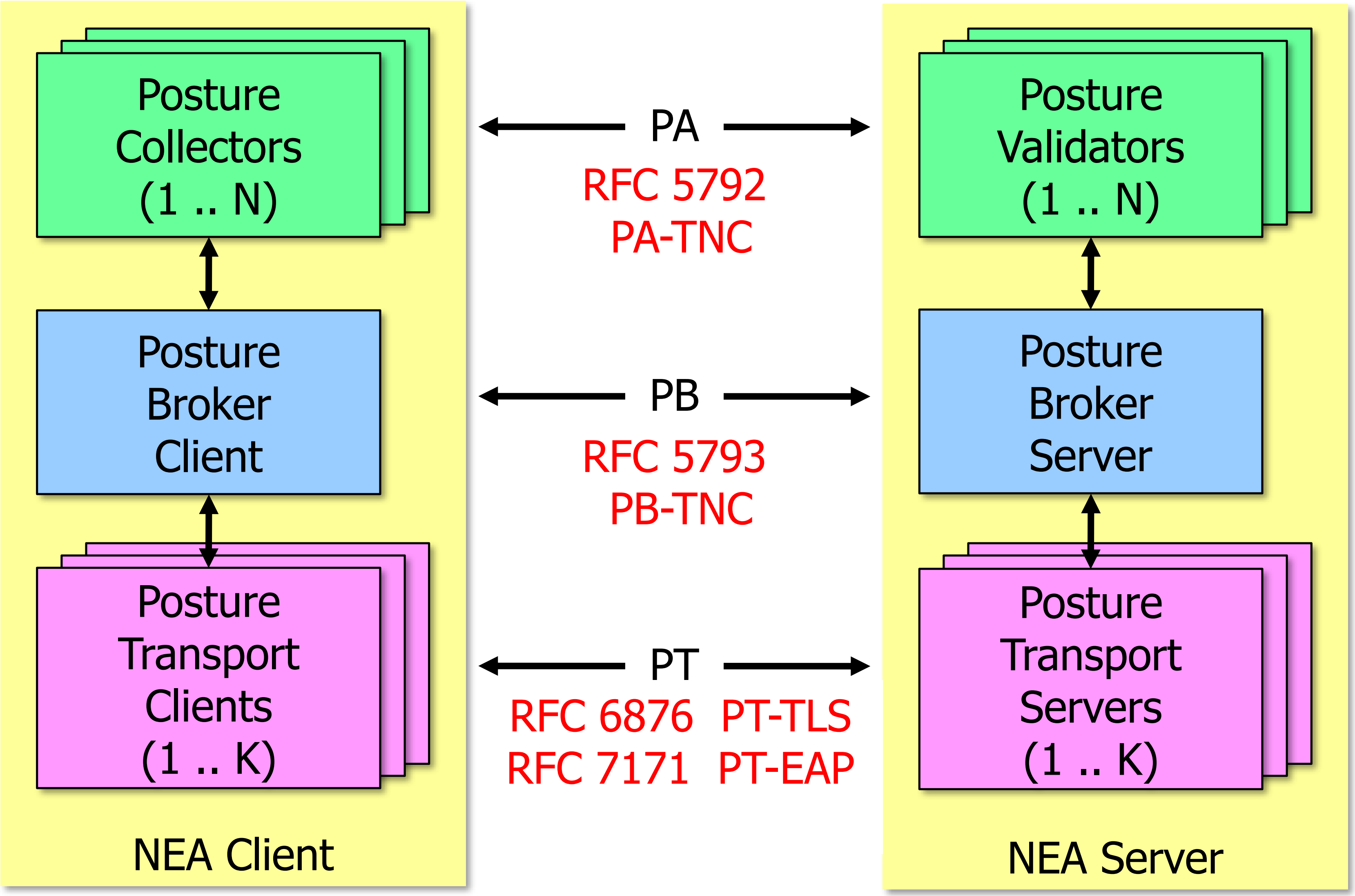
VPN Client

VPN Gateway

Lying Endpoint

Network Access Control

Network Endpoint Assessment (RFC 5209)



Layered TNC Protocol Stack

- 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]
```

strongSwan supports TPM-based Attestation

2010 Implemented the TCG TNC IF-TNCCS 2.0 Client/Server and TCG TNC IF-M Measurement protocols.

2011 Implemented the TCG Attestation Protocol Binding to TNC IF-M using TrouSerS stack under Linux [later ported to Windows].

2012 Implemented TPM 1.2 based attestation using the Linux Integrity Measurement Architecture (IMA).

2015 Implemented the TCG TNC IF-M Segmentation Protocol allowing the transport of huge IF-M attributes over IF-T for EAP Methods. IF-T for TLS transport also profits from large buffer savings.

2016 Implemented TPM 2.0 based Attestation using the Intel TSS2 SAPI under Linux and an Intel PTT Firmware TPM.

2016 Implemented TPM 2.0 based Attestation using the Intel TSS2 SAPI under Linux and an Infineon Hardware TPM.

Mutual Attestation of IoT Devices

Connect Security World September 2016 Marseille

Trusted Network Communications (TNC)

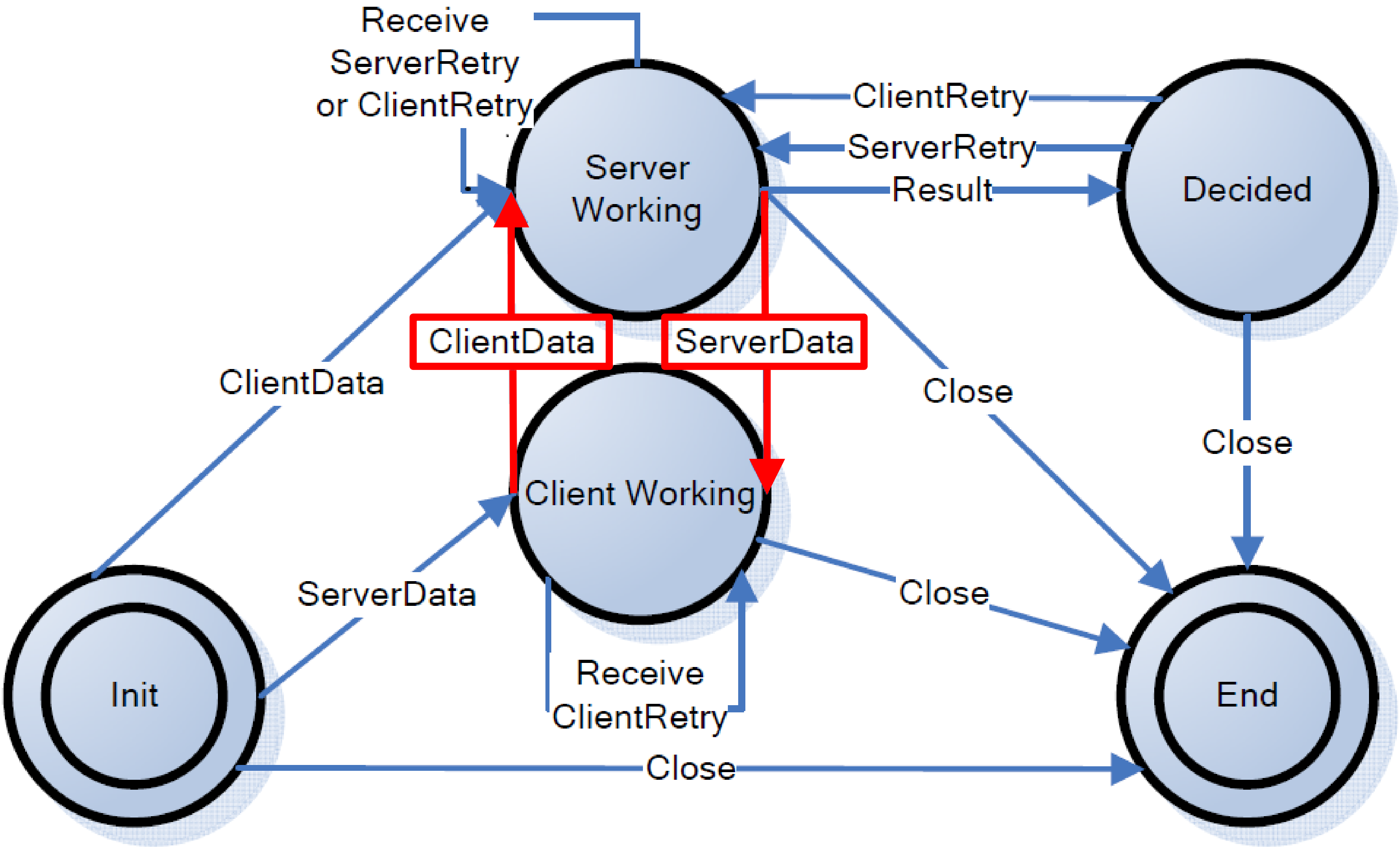
New Use Case:

Mutual Measurements of Endpoints

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

PB-TNC / IF-TNCCS 2.0 State Machine



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

Why do Mutual TNC Measurements work?

- 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.

Mutual Measurements in Half-Duplex Mode

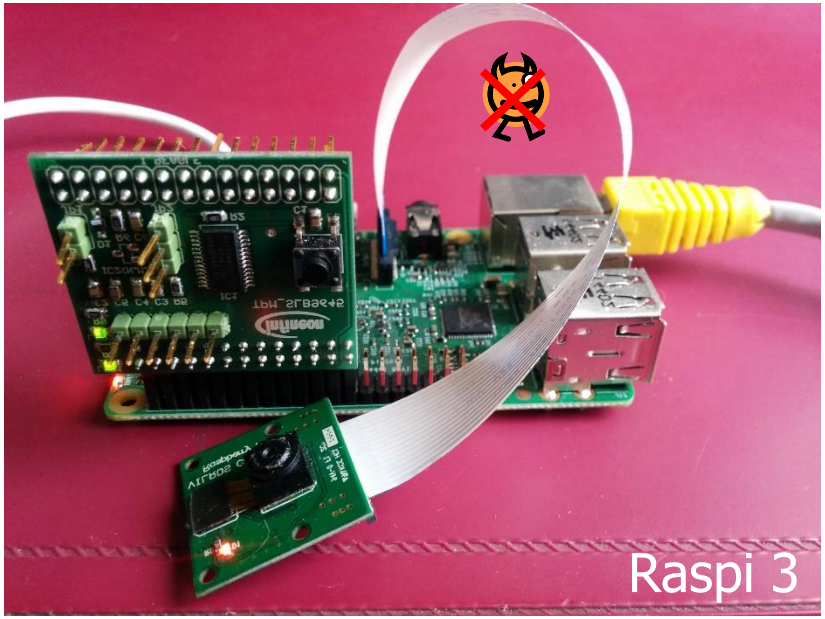
Initiator		PB-TNC Batch[PB-TNC Messages]		Responder
TNC Client	→	CDATA[PB-MUTUAL, PB-PA]	→	TNC Server
TNC Client	←	SDATA[PB-MUTUAL, PB-PA]	←	TNC Server
TNC Server	→	SDATA[]	→	TNC Client
TNC Server	←	CDATA[PB-PA]	←	TNC Client
TNC Client	→	CDATA[PB-PA]	→	TNC Server
TNC Client	←	RESULT[PB-ASSESSMENT]	←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

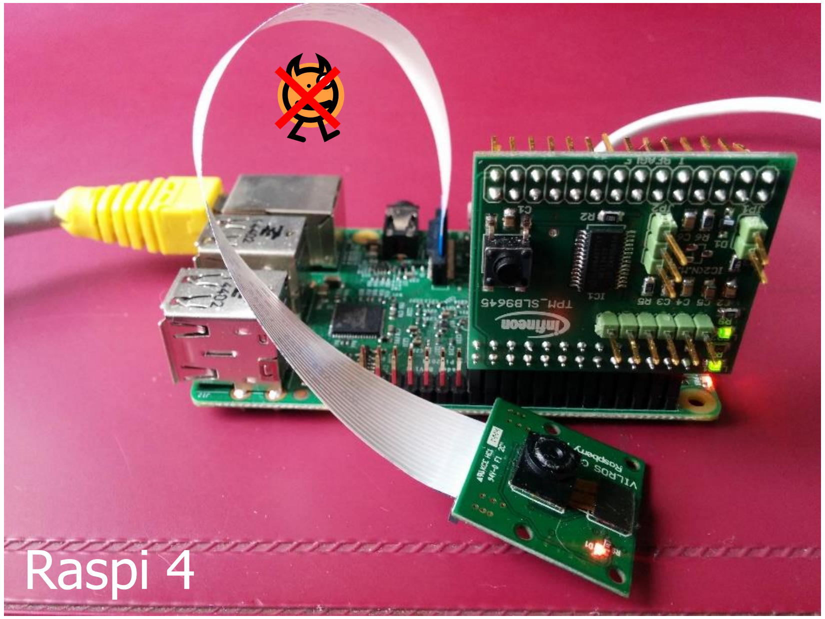
- The initiating TNC client sends CLOSE batch last
- Works over PT-EAP and PT-TLS

Example: Mutually Trusted Video Phones

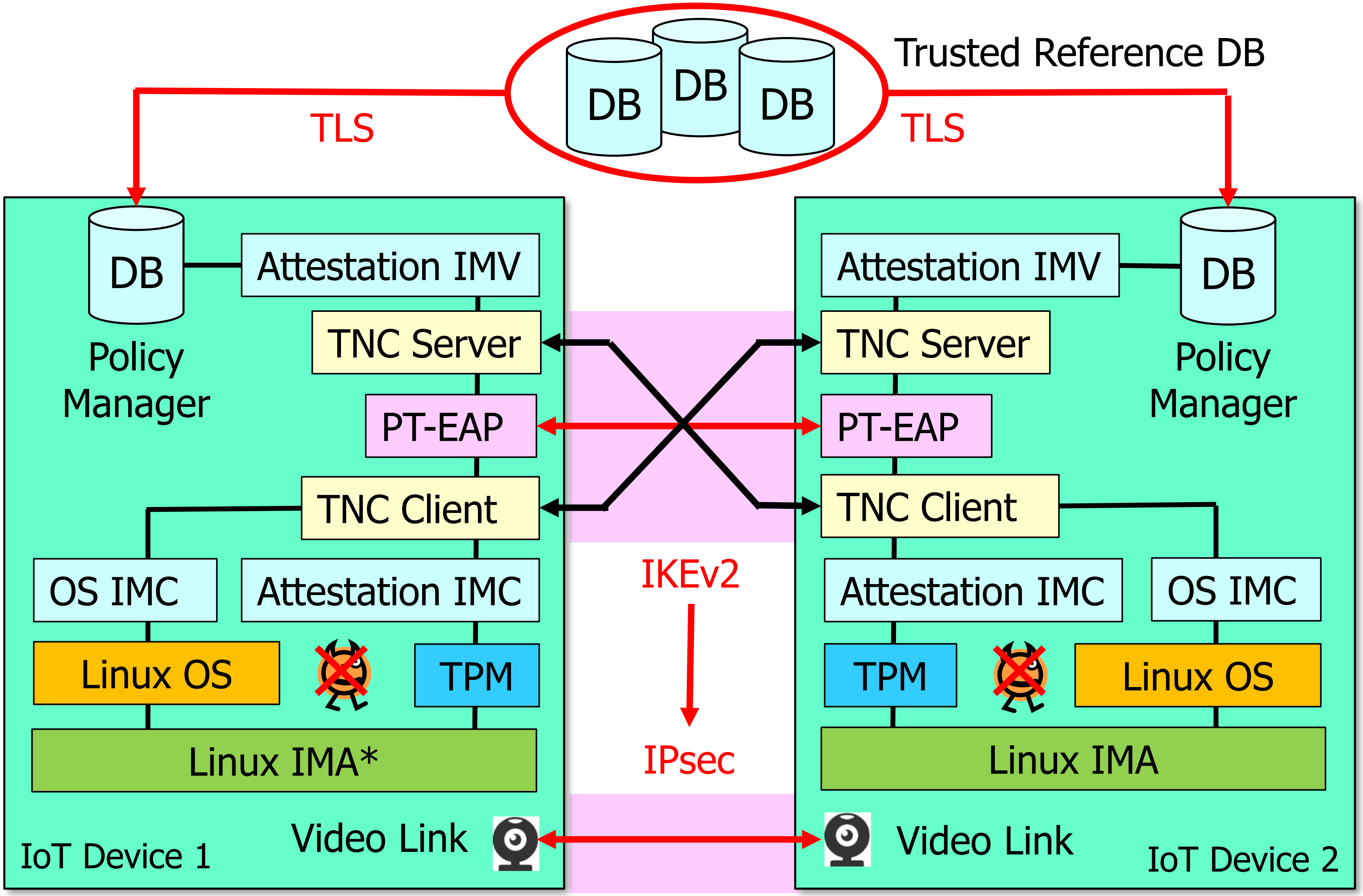
Demo Setup:

Raspberry Pi 2 IoT Platform
Raspian OS (Debian 7/8)
Infineon HW TPM:
 TPM 1.2 with TrouSerS
 TPM 2.0 with Intel TSS 2.0



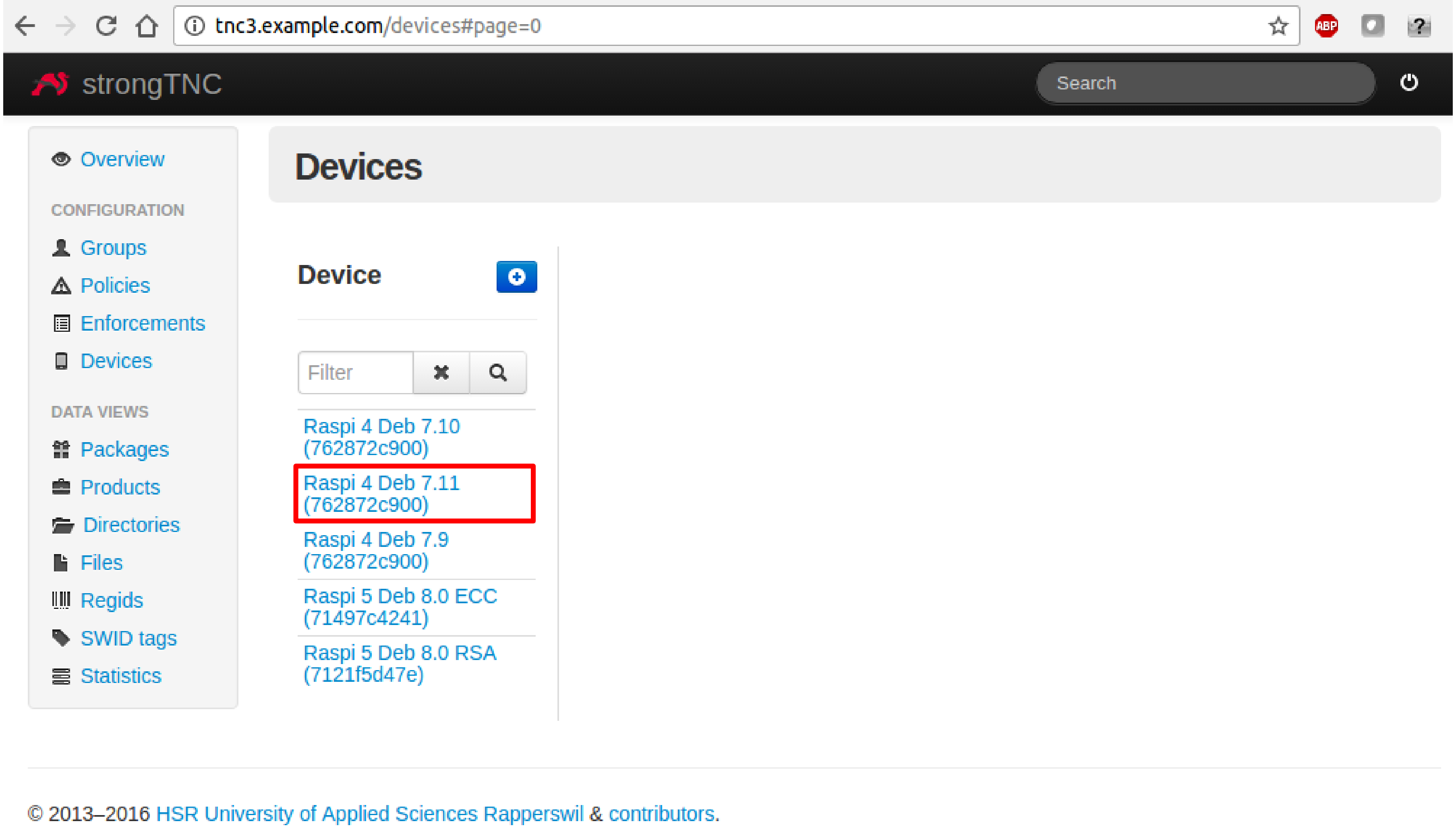


Mutual Attestation of IoT Devices



* IMA: Integrity Measurement Architecture

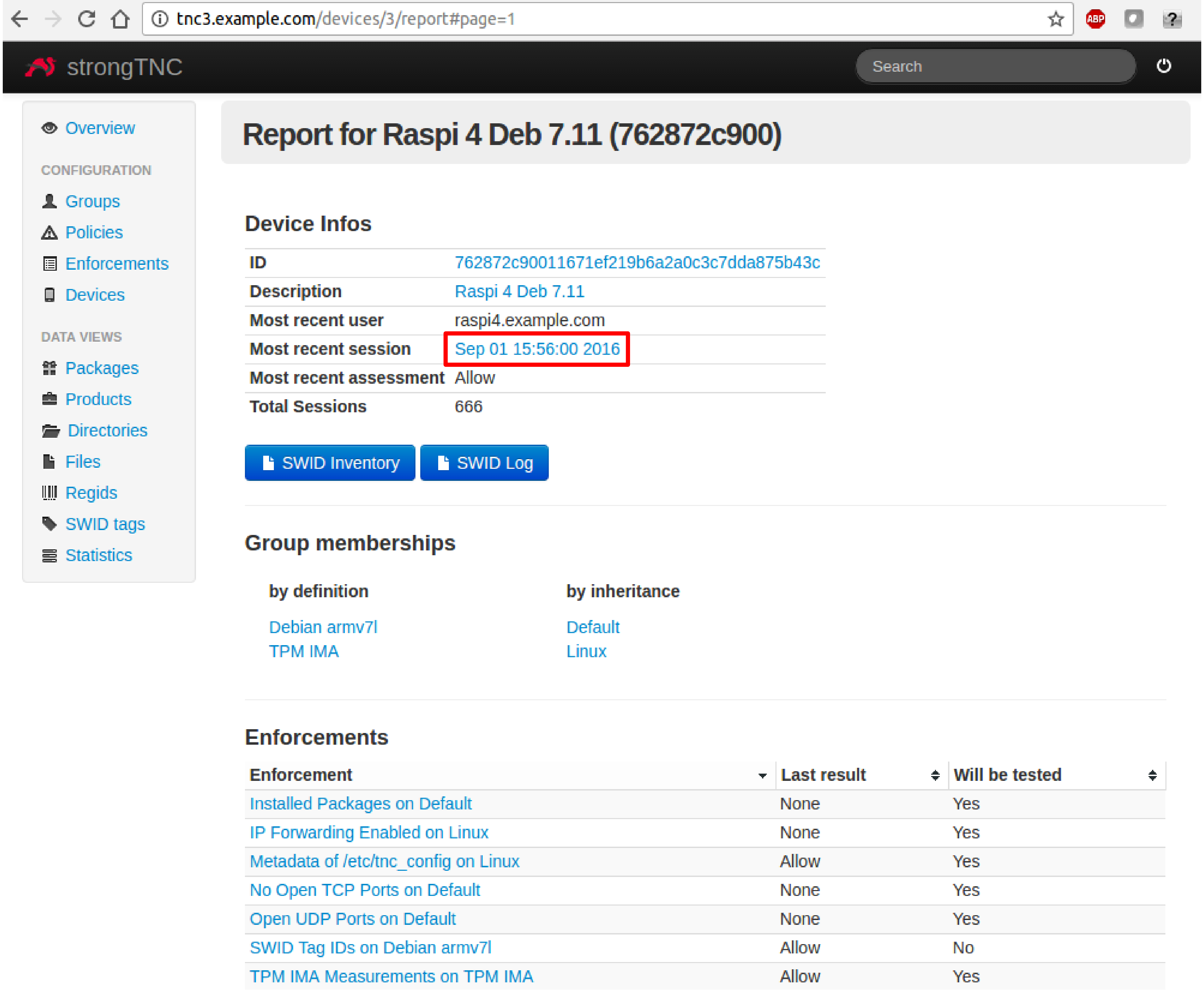
strongTNC Open Source Policy Manager



Devices

Device

- Raspi 4 Deb 7.10 (762872c900)
- Raspi 4 Deb 7.11 (762872c900)
- Raspi 4 Deb 7.9 (762872c900)
- Raspi 5 Deb 8.0 ECC (71497c4241)
- Raspi 5 Deb 8.0 RSA (7121f5d47e)



Report for Raspi 4 Deb 7.11 (762872c900)

Device Infos

ID	762872c90011671ef219b6a2a0c3c7dda875b43c
Description	Raspi 4 Deb 7.11
Most recent user	raspi4.example.com
Most recent session	Sep 01 15:56:00 2016
Most recent assessment	Allow
Total Sessions	666

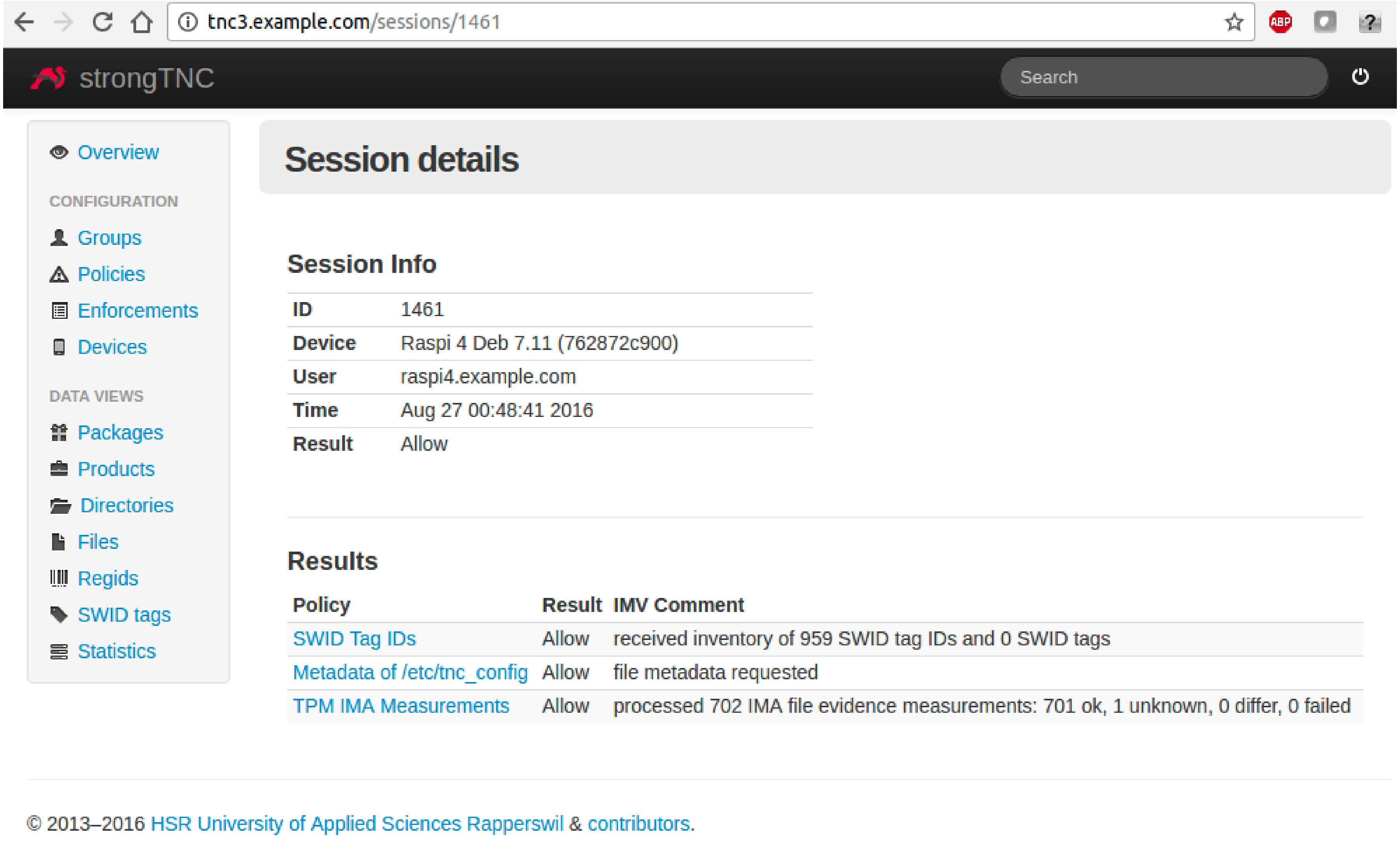
Group memberships

by definition	by inheritance
Debian armv7l	Default
TPM IMA	Linux

Enforcements

Enforcement	Last result	Will be tested
Installed Packages on Default	None	Yes
IP Forwarding Enabled on Linux	None	Yes
Metadata of /etc/tnc_config on Linux	Allow	Yes
No Open TCP Ports on Default	None	Yes
Open UDP Ports on Default	None	Yes
SWID Tag IDs on Debian armv7l	Allow	No
TPM IMA Measurements on TPM IMA	Allow	Yes

End Point Raspi 4: Session Details



Session details

Session Info

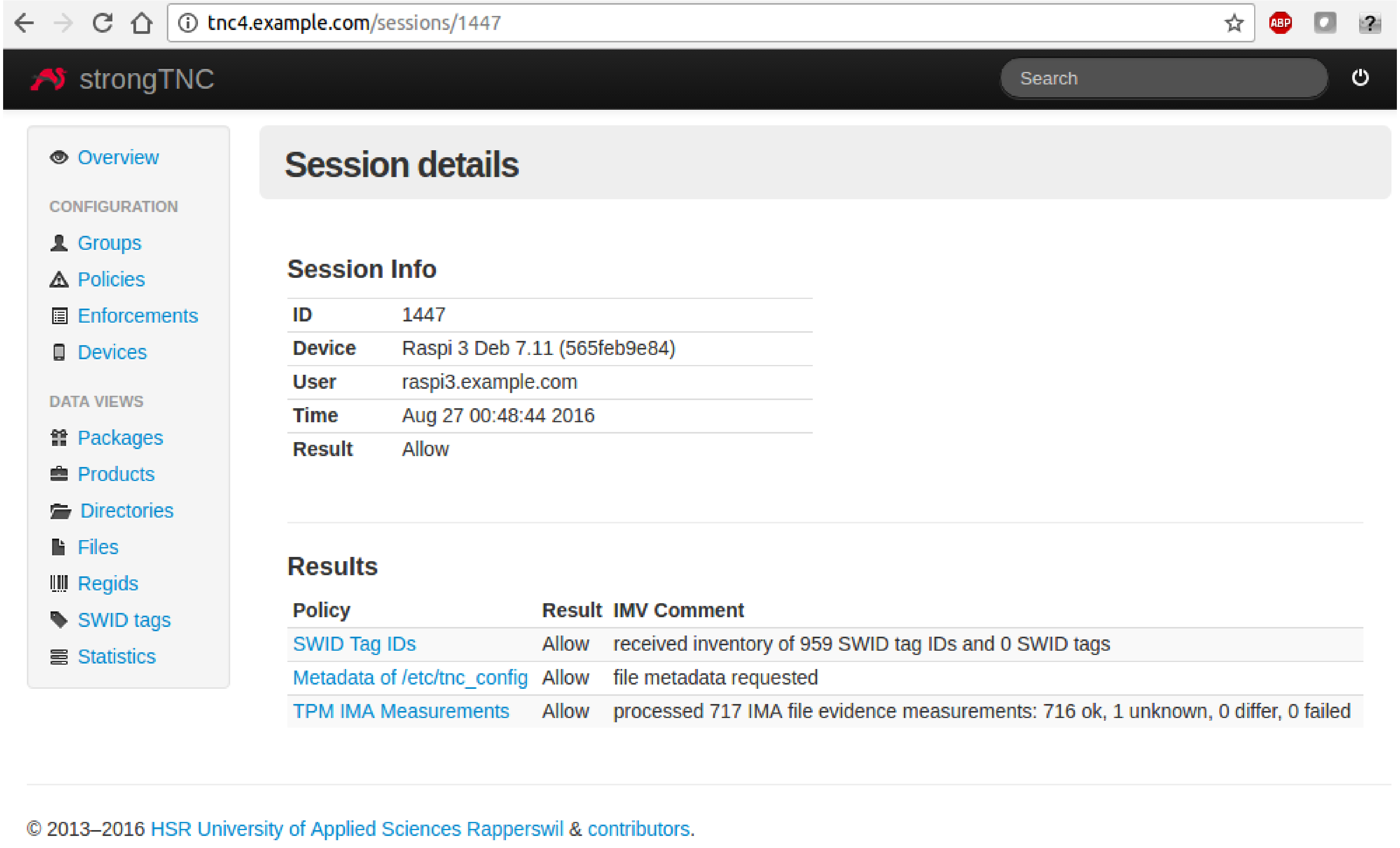
ID	1461
Device	Raspi 4 Deb 7.11 (762872c900)
User	raspi4.example.com
Time	Aug 27 00:48:41 2016
Result	Allow

Results

Policy	Result	IMV Comment
SWID Tag IDs	Allow	received inventory of 959 SWID tag IDs and 0 SWID tags
Metadata of /etc/tnc_config	Allow	file metadata requested
TPM IMA Measurements	Allow	processed 702 IMA file evidence measurements: 701 ok, 1 unknown, 0 differ, 0 failed

© 2013–2016 HSR University of Applied Sciences Rapperswil & contributors.

End Point Raspi 3: Session Details



Session details

Session Info

ID	1447
Device	Raspi 3 Deb 7.11 (565feb9e84)
User	raspi3.example.com
Time	Aug 27 00:48:44 2016
Result	Allow

Results

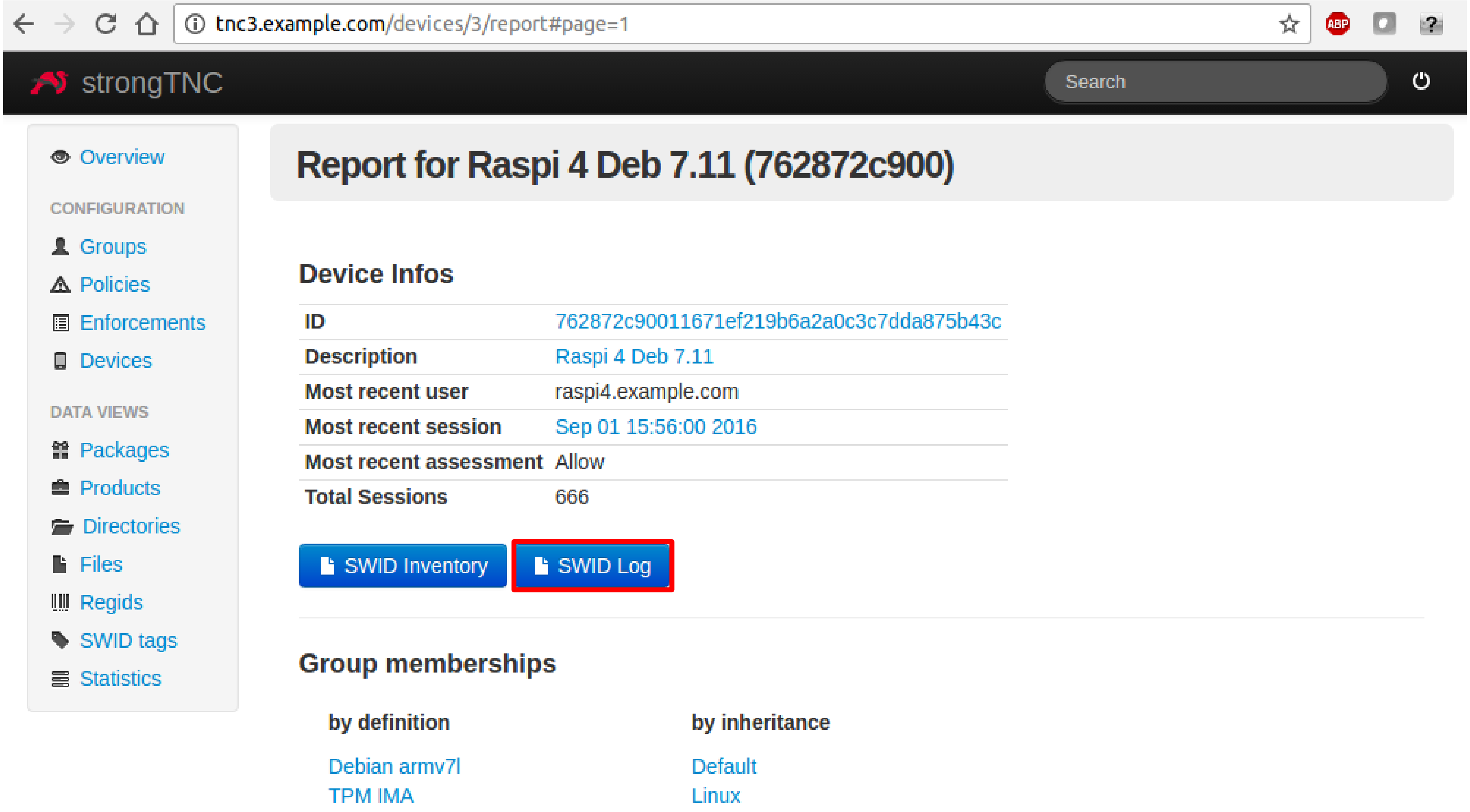
Policy	Result	IMV Comment
SWID Tag IDs	Allow	received inventory of 959 SWID tag IDs and 0 SWID tags
Metadata of /etc/tnc_config	Allow	file metadata requested
TPM IMA Measurements	Allow	processed 717 IMA file evidence measurements: 716 ok, 1 unknown, 0 differ, 0 failed

File Version Management using SWID Tags

- ISO/IEC 19770-2:2015 Software Asset Management Part 2: Software Identification Tag:

```
<SoftwareIdentity xmlns=http://standards.iso.org/iso/19770/-2/2015/schema.xsd
   name="libssl1.0.0" tagId="Ubuntu_14.04-x86_64-libssl1.0.0-1.0.1f-1ubuntu2.15“
   version="1.0.1f-1ubuntu2.15" versionScheme="alphanumeric">
  <Entity name="strongSwan Project" regid="strongswan.org“ role="tagCreator"/>
  <Payload>
    <File location="/lib/x86_64-linux-gnu" name="libcrypto.so.1.0.0"/>
    <File location="/lib/x86_64-linux-gnu" name="libssl.so.1.0.0"/>
    <File location="/usr/share/doc/libssl1.0.0" name="copyright"/>
    <File location="/usr/share/doc/libssl1.0.0" name="changelog.Debian.gz"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libpadlock.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libcswift.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="lib4758cca.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libaep.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libubsec.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libchil.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libgost.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libgmp.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libcapi.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libnuron.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libsureware.so"/>
    <File location="/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines" name="libatalla.so"/>
  </Payload>
</SoftwareIdentity>
```

SWID Tag Support



tnc3.example.com/devices/3/report#page=1

strongTNC

Search

- Overview

CONFIGURATION

- Groups
- Policies
- Enforcements
- Devices

DATA VIEWS

- Packages
- Products
- Directories
- Files
- Regids
- SWID tags
- Statistics

Report for Raspi 4 Deb 7.11 (762872c900)

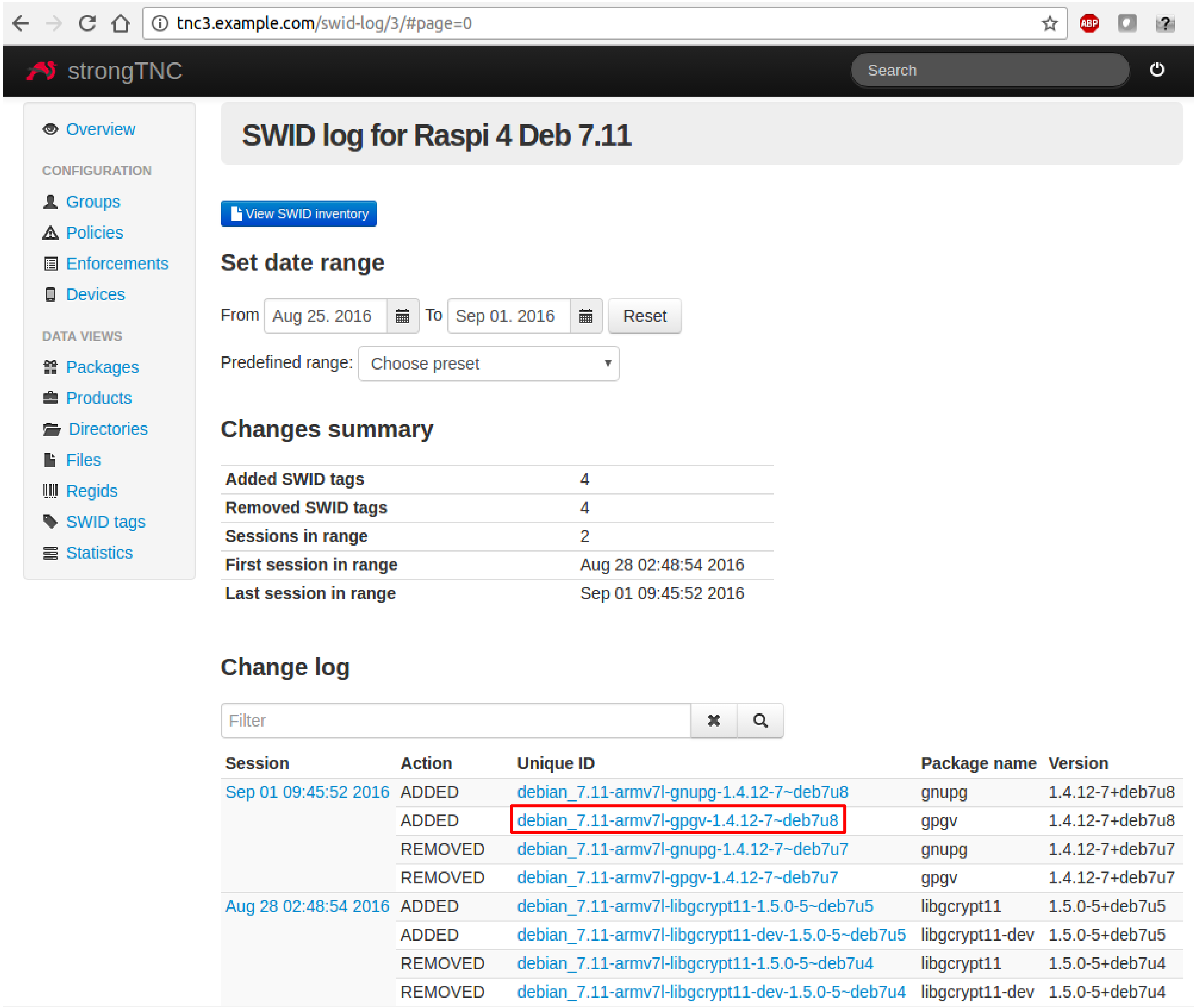
Device Infos

ID	762872c90011671ef219b6a2a0c3c7dda875b43c
Description	Raspi 4 Deb 7.11
Most recent user	raspi4.example.com
Most recent session	Sep 01 15:56:00 2016
Most recent assessment	Allow
Total Sessions	666

SWID Inventory SWID Log

Group memberships

by definition	by inheritance
Debian armv7l	Default
TPM IMA	Linux



SWID log for Raspi 4 Deb 7.11

Set date range

From Aug 25. 2016 To Sep 01. 2016

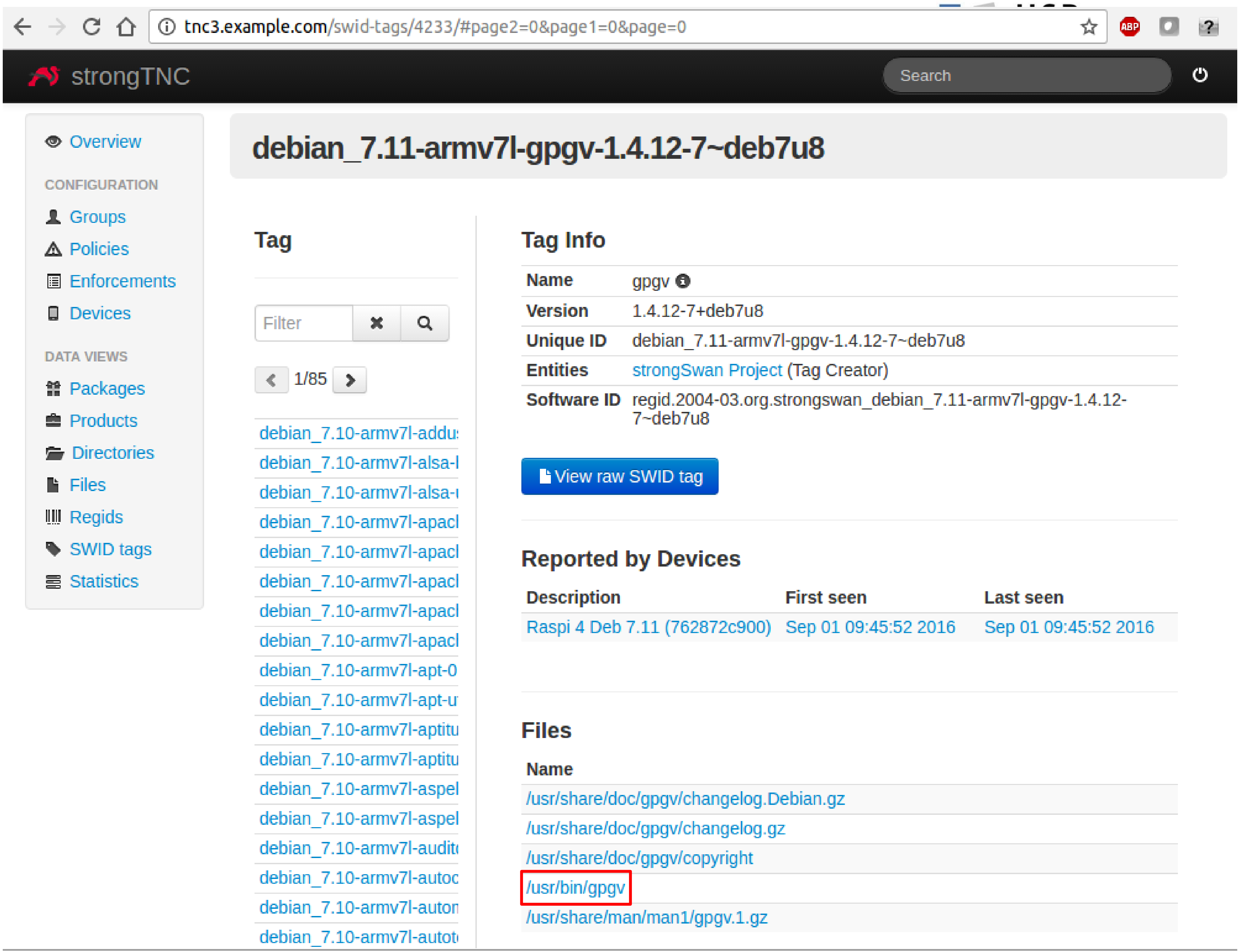
Predefined range: Choose preset

Changes summary

Added SWID tags	4
Removed SWID tags	4
Sessions in range	2
First session in range	Aug 28 02:48:54 2016
Last session in range	Sep 01 09:45:52 2016

Change log

Session	Action	Unique ID	Package name	Version
Sep 01 09:45:52 2016	ADDED	debian_7.11-armv7l-gnupg-1.4.12-7~deb7u8	gnupg	1.4.12-7+deb7u8
	ADDED	debian_7.11-armv7l-gpgv-1.4.12-7~deb7u8	gpgv	1.4.12-7+deb7u8
	REMOVED	debian_7.11-armv7l-gnupg-1.4.12-7~deb7u7	gnupg	1.4.12-7+deb7u7
	REMOVED	debian_7.11-armv7l-gpgv-1.4.12-7~deb7u7	gpgv	1.4.12-7+deb7u7
Aug 28 02:48:54 2016	ADDED	debian_7.11-armv7l-libgcrypt11-1.5.0-5~deb7u5	libgcrypt11	1.5.0-5+deb7u5
	ADDED	debian_7.11-armv7l-libgcrypt11-dev-1.5.0-5~deb7u5	libgcrypt11-dev	1.5.0-5+deb7u5
	REMOVED	debian_7.11-armv7l-libgcrypt11-1.5.0-5~deb7u4	libgcrypt11	1.5.0-5+deb7u4
	REMOVED	debian_7.11-armv7l-libgcrypt11-dev-1.5.0-5~deb7u4	libgcrypt11-dev	1.5.0-5+deb7u4



debian_7.11-armv7l-gpgv-1.4.12-7~deb7u8

Tag

debian_7.10-armv7l-addu
debian_7.10-armv7l-alsa-l
debian_7.10-armv7l-alsa-u
debian_7.10-armv7l-apacl
debian_7.10-armv7l-apacl
debian_7.10-armv7l-apacl
debian_7.10-armv7l-apacl
debian_7.10-armv7l-apacl
debian_7.10-armv7l-apt-0
debian_7.10-armv7l-apt-u
debian_7.10-armv7l-aptitu
debian_7.10-armv7l-aptitu
debian_7.10-armv7l-aspel
debian_7.10-armv7l-aspel
debian_7.10-armv7l-audit
debian_7.10-armv7l-autoc
debian_7.10-armv7l-autor
debian_7.10-armv7l-autot

Tag Info

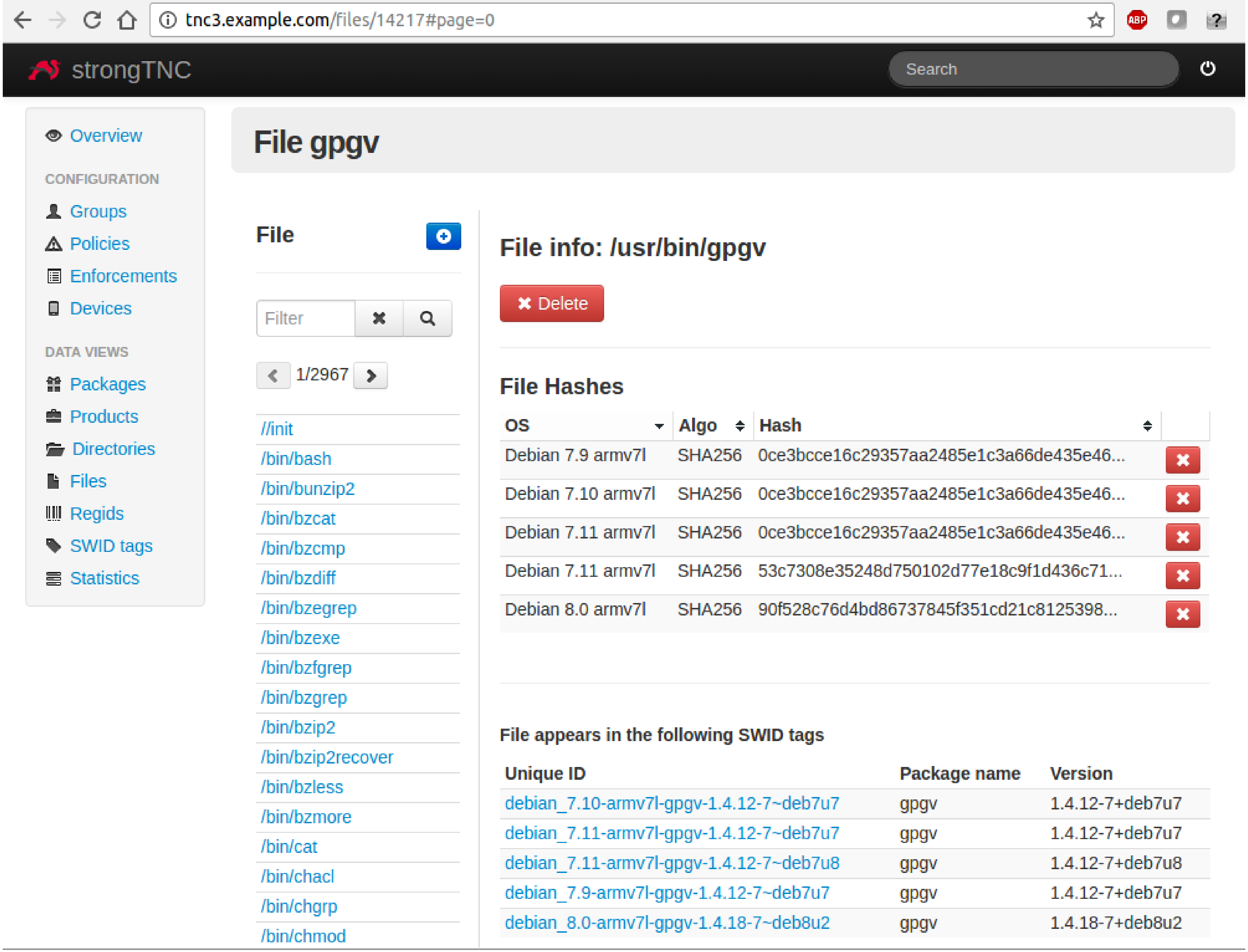
Name	gpgv
Version	1.4.12-7+deb7u8
Unique ID	debian_7.11-armv7l-gpgv-1.4.12-7~deb7u8
Entities	strongSwan Project (Tag Creator)
Software ID	regid.2004-03.org.strongswan_debian_7.11-armv7l-gpgv-1.4.12-7~deb7u8

Reported by Devices

Description	First seen	Last seen
Raspi 4 Deb 7.11 (762872c900)	Sep 01 09:45:52 2016	Sep 01 09:45:52 2016

Files

Name
/usr/share/doc/gpgv/changelog.Debian.gz
/usr/share/doc/gpgv/changelog.gz
/usr/share/doc/gpgv/copyright
/usr/bin/gpgv
/usr/share/man/man1/gpgv.1.gz



tnc3.example.com/files/14217#page=0

strongTNC

File gpgv

File

//init
/bin/bash
/bin/bunzip2
/bin/bzcat
/bin/bzcmp
/bin/bzdiff
/bin/bzegrep
/bin/bzexe
/bin/bzfgrep
/bin/bzgrep
/bin/bzip2
/bin/bzip2recover
/bin/bzless
/bin/bzmore
/bin/cat
/bin/chacl
/bin/chgrp
/bin/chmod

File info: /usr/bin/gpgv

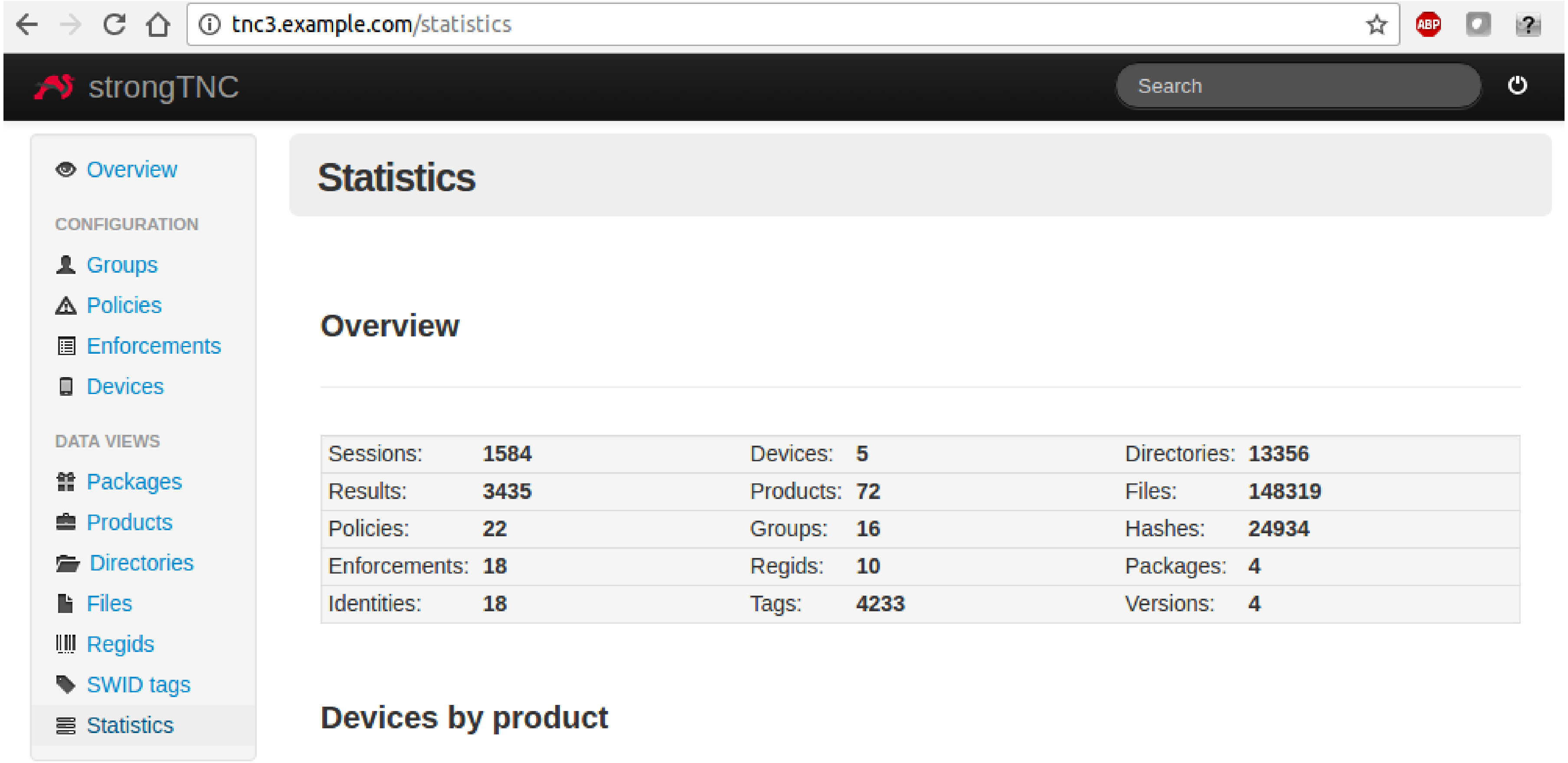
File Hashes

OS	Algo	Hash	
Debian 7.9 armv7l	SHA256	0ce3bcce16c29357aa2485e1c3a66de435e46...	✖
Debian 7.10 armv7l	SHA256	0ce3bcce16c29357aa2485e1c3a66de435e46...	✖
Debian 7.11 armv7l	SHA256	0ce3bcce16c29357aa2485e1c3a66de435e46...	✖
Debian 7.11 armv7l	SHA256	53c7308e35248d750102d77e18c9f1d436c71...	✖
Debian 8.0 armv7l	SHA256	90f528c76d4bd86737845f351cd21c8125398...	✖

File appears in the following SWID tags

Unique ID	Package name	Version
debian_7.10-armv7l-gpgv-1.4.12-7~deb7u7	gpgv	1.4.12-7+deb7u7
debian_7.11-armv7l-gpgv-1.4.12-7~deb7u7	gpgv	1.4.12-7+deb7u7
debian_7.11-armv7l-gpgv-1.4.12-7~deb7u8	gpgv	1.4.12-7+deb7u8
debian_7.9-armv7l-gpgv-1.4.12-7~deb7u7	gpgv	1.4.12-7+deb7u7
debian_8.0-armv7l-gpgv-1.4.18-7~deb8u2	gpgv	1.4.18-7+deb8u2

Statistics: Two IoT Clients run over 5 Months



Statistics

Overview

Sessions:	**1584**	Devices:	**5**	Directories:	**13356**
Results:	**3435**	Products:	**72**	Files:	**148319**
Policies:	**22**	Groups:	**16**	Hashes:	**24934**
Enforcements:	**18**	Regids:	**10**	Packages:	**4**
Identities:	**18**	Tags:	**4233**	Versions:	**4**

Devices by product

Conclusions

- Attestation of IoT devices using either a TPM 1.2 or TPM 2.0 is feasible and takes less than 60 seconds.
- The regular use case is periodic reporting of attestation results by all IoT devices to a central Policy Decision Point. IF-T transport is usually based on TLS.
- Mutual attestation can be used e.g. by mission-critical routers in the energy grid in order to establish mutual trust into the hardware identity and integrity of the IoT devices. IF-T transport can be based on IKEv2-EAP if IPsec is used to protect the traffic exchanged by the devices anyway.
- Using the strongSwan and strongTNC open source software, IoT attestation solutions can be easily implemented!

Thank you for your attention!

Questions?

www.strongswan.org/tnc/