Trusted Network Connect (TNC)

3rd European Trusted Infrastructure Summer School
September 2008

Josef von Helden
University of Applied Sciences and Arts, Hanover
josef.vonhelden@fh-hannover.de

Ingo Bente
Jörg Vieweg
Bastian Hellmann

Content

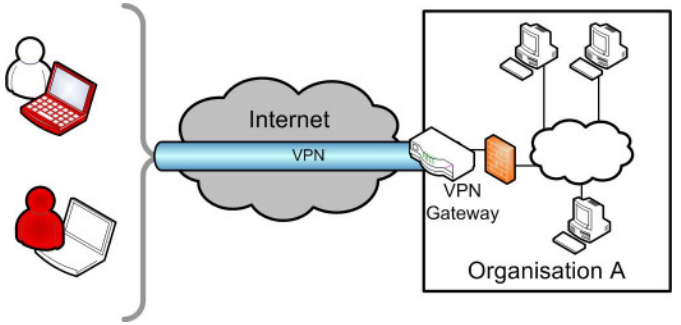
- **Introduction**
- Network Access Control (NAC)
- Trusted Network Connect (TNC)
- TNC@FHH
- tNAC
- Conclusion

Introduction: Motivation

- Changing network structures
  - from static and homogeneous to dynamic and heterogeneous
  - mobile endpoints connect to and communicate with various networks
    - employees using their notebooks at home and at work
    - guest devices, e.g. consultants, students, …
- hackers adapting their strategies
  - attacking the weakest IT component of a network: endpoints
  - stay hidden, waiting for crucial moments e.g.
    - spy on passwords,
    - eavesdrop on transactions,
    - doing evil work with the user's privileges after his/her successful authentication to a service

Introduction: Threats

- compromised endpoints are a threat to any network they are connecting to
- traditional security mechanisms like firewalls, IDS, VPNs, user authentication do not protect against those threats



- What is basically needed?
  - check the integrity status of every endpoint…
  - … before it‘s getting access to my network
  - compare the integrity status against my policy
  - decide if (or how far) the endpoint is allowed to join my network
  - enforce the decision

☞ Network Access Control (NAC)

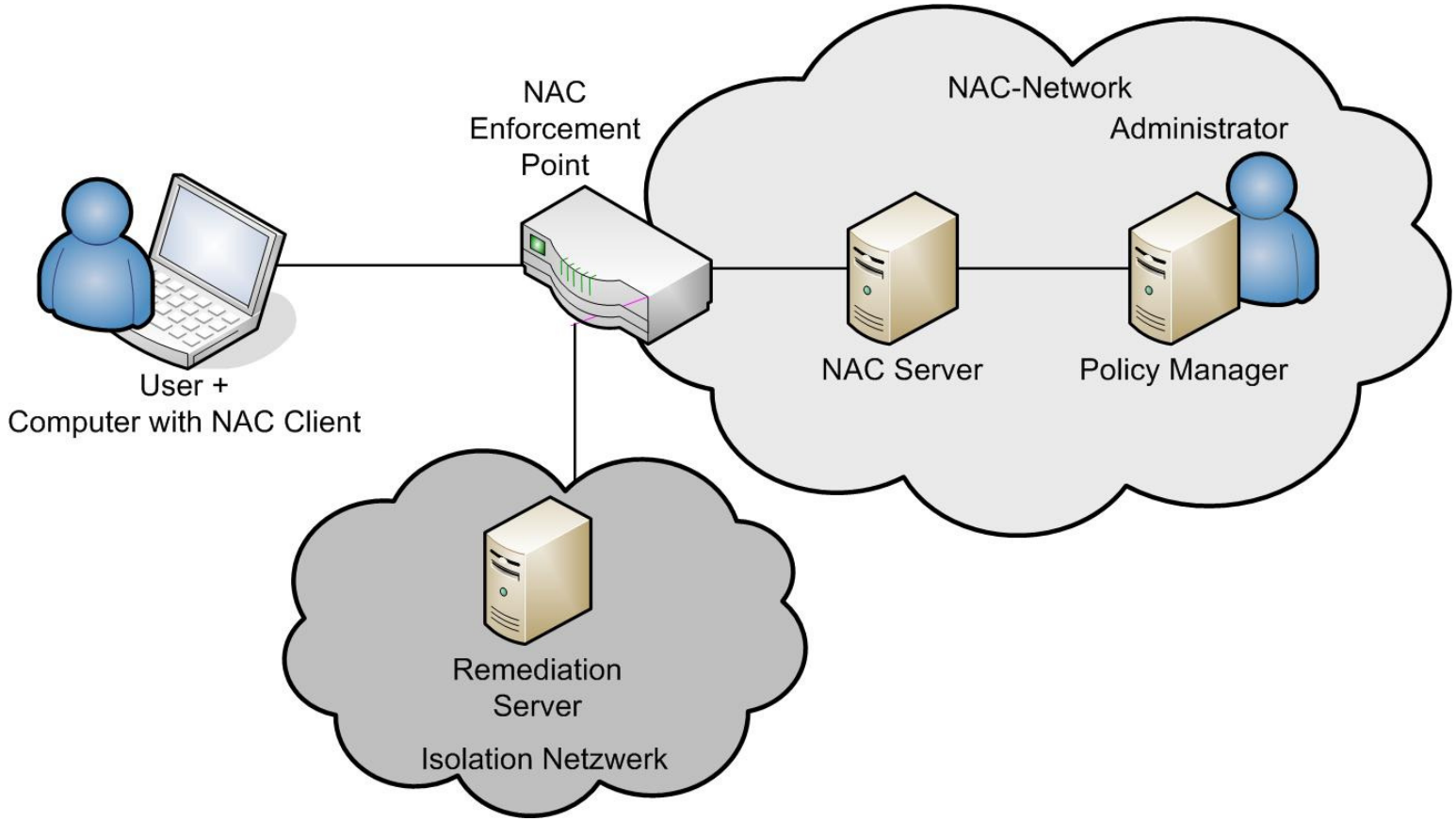
Content

- Introduction
- **Network Access Control (NAC)**
- Trusted Network Connect (TNC)
- TNC@FHH
- tNAC
- Conclusion

NAC: basic funcionalities

- User Authentication, e.g.
  - based on passwords or certificates
  - via VPN and IEEE 802.1X
- Configuration Assessment
  - Configuration measurement before network access
    - e.g. installed software like antivirus scanner and firewall
  - Compare measurements to policies of the network to access
  - ➔ Integrity check of the computer system
  - Re-assess accepted computer systems in regular intervals
- Policy Enforcement
  - Enforce policies to non-compliant computer systems

NAC: typical topology



NAC: solutions

- NAC solutions are already available on the market
- The most prominent:
  - Cisco Network Admission Control (Cisco NAC)
  - Microsoft Network Access Protection (NAP)
- And many more:
  - Juniper Unified Access Control
  - StillSecure Safe Access
  - …

NAC: requirements

- NAC solutions meet the basic requirements for checking the integrity status of endpoints “by definition”.
- To gain significant benefit (at least) two important requirements have to be fulfilled
  - interoperability
    - enabling multi-vendor support
    - enabling customer’s choice of security solutions and infrastructure
  - unforgeability
    - i.e. the network (resp. a security server in the network) can really trust in the integrity information provided by the endpoint (countering the “lying endpoint problem”)

NAC: limitations of current solutions

- Today, no available NAC solution meets the requirements of interoperability and unforgeability
  - Cisco's NAC and Microsoft's NAP are both proprietary by design
    - first interoperability approaches
      - Microsoft opened their NAP-Client-Server-Protocol „SoH“
  - NAC-components themselves can get compromised
    - e.g. shown on Cisco CTA at BlackHat conference 2007
- In general: unforgeability presumes having
  - (a) hardware based root of trust which
  - (b) also is standardised to meet interoperability

☞ Trusted Network Connect (TNC)

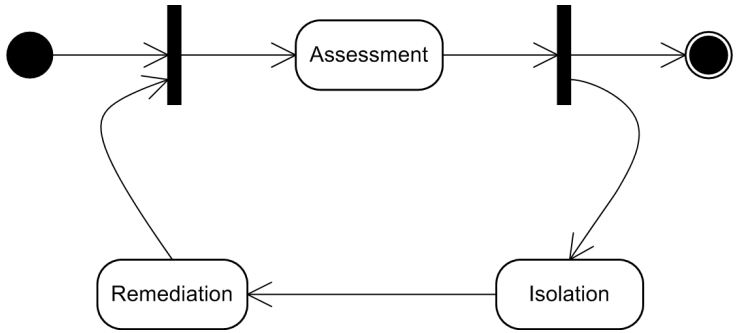
Content

- Introduction
- Network Access Control (NAC)
- **Trusted Network Connect (TNC)**
- TNC@FHH
- tNAC
- Conclusion

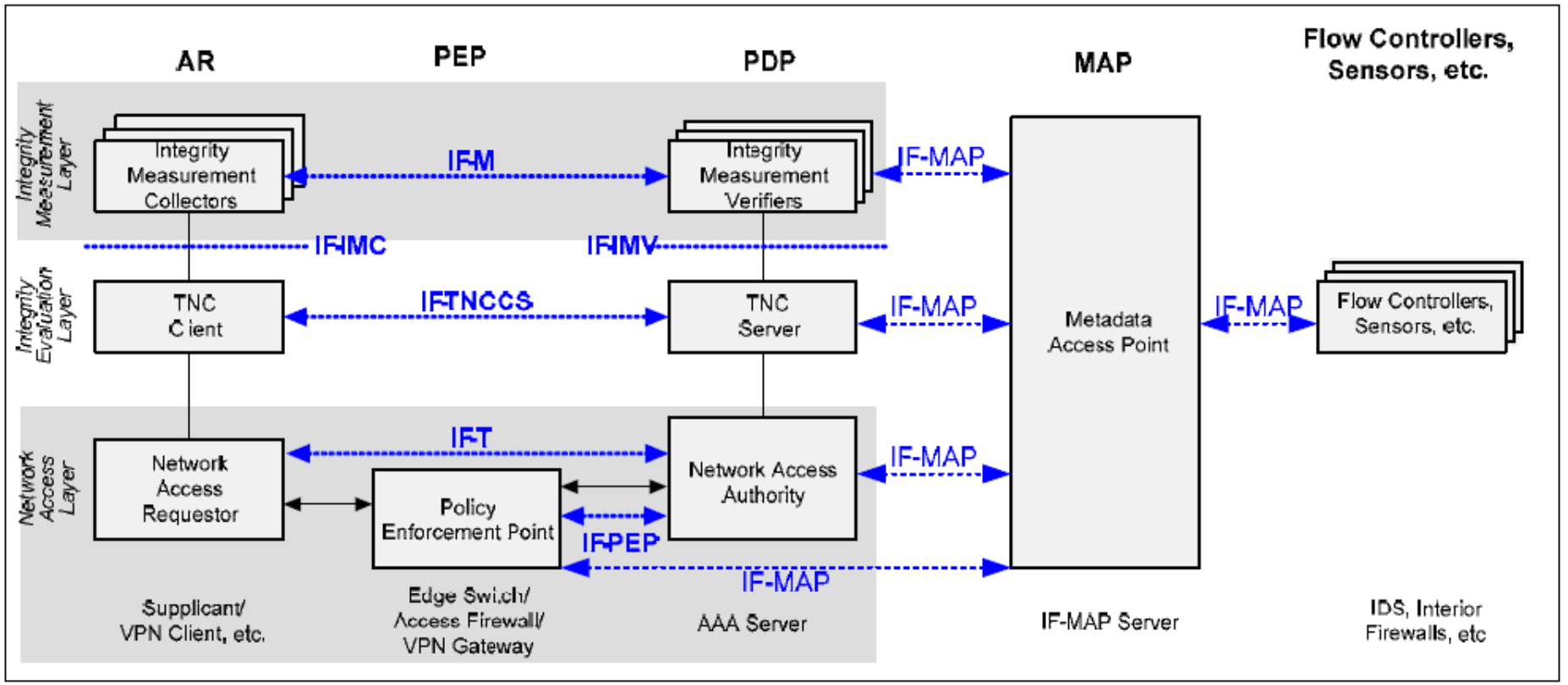
TNC: overview

- Open Architecture for NAC
  - Specified by the TNC Subgroup of the TCG
  - All specifications are publicly available
    - Enables multi-vendor interoperability
  - Supports existing technologies (802.1X, EAP)

- TNC Handshake consists of 3 phases
  - Assessment
    - TNC Platform Authentication
      - Identity + integrity of platform
  - Isolation
    - Quarantine non-healthy endpoints
  - Remediation
    - Fix problems and make endpoint healthy again



TNC: basic architecture

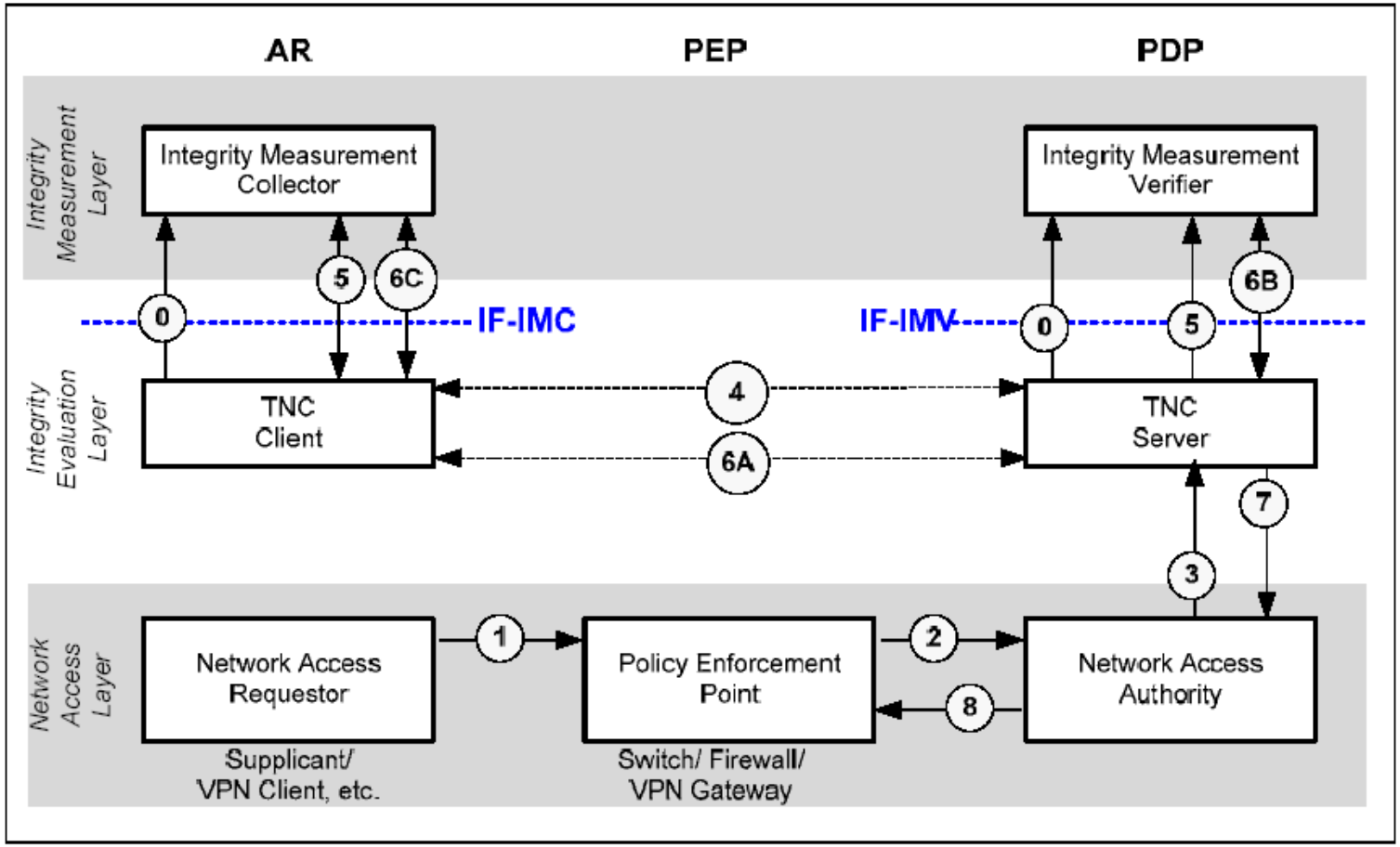


[TNC Architecture for Interoperability Specification version 1.3 revision 6]

TNC: entities

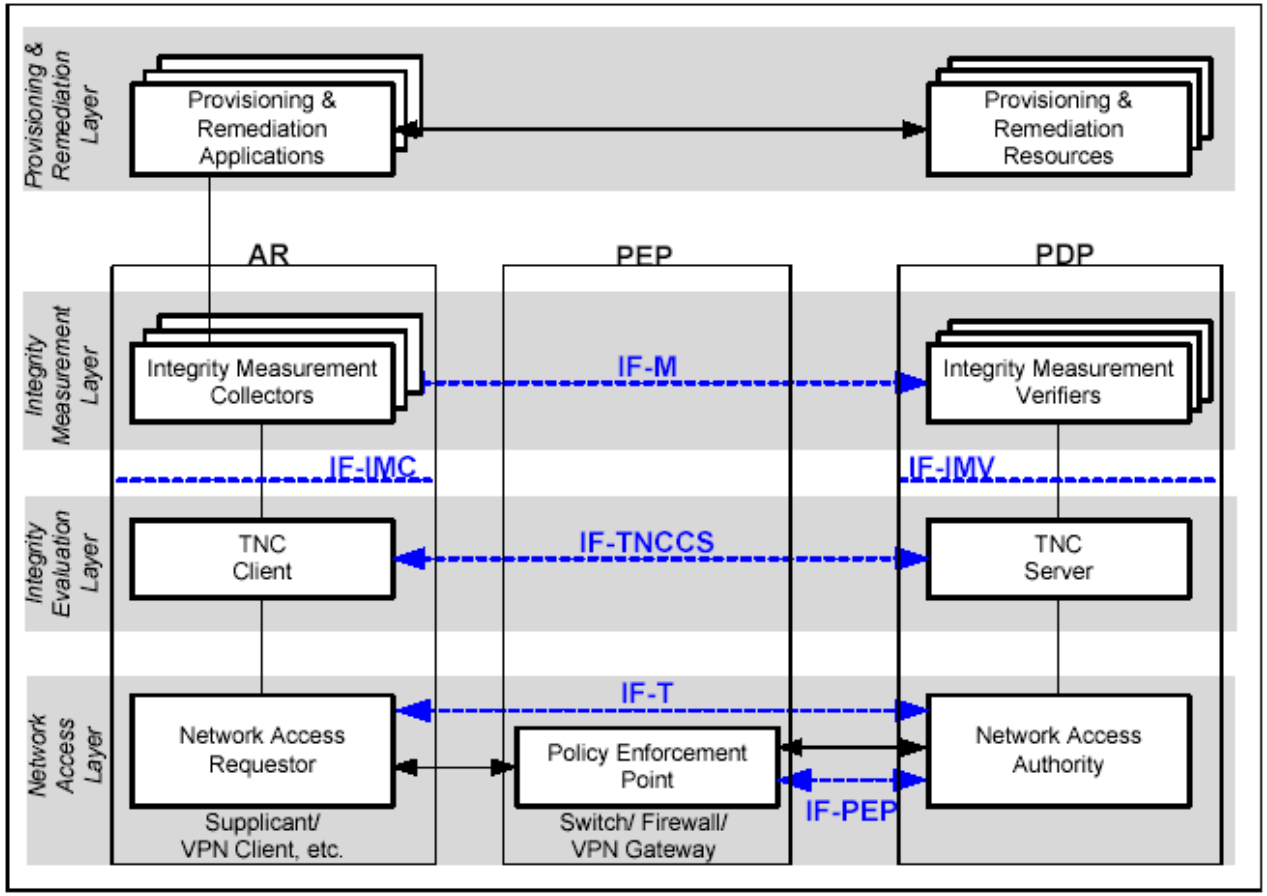
- Access Requestor (AR)
  - requests access to a protected network
    - typically the endpoint, e.g. notebook, desktop, ...
- Policy Decision Point (PDP)
  - performing the decision-making regarding the AR's request, in light of the access policies.
    - typically a network server
- Policy Enforcement Point (PEP)
  - enforces the decisions of the PDP regarding network access
    - typically a switch, access point or VPN gateway

TNC: basic message flow



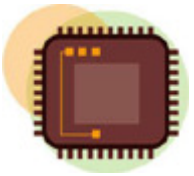
[TNC Architecture for Interoperability Specification version 1.3 revision 6]

TNC: Provisioning and Remediation Layer



[TNC Architecture for Interoperability Specification version 1.3 revision 6]

TNC: TPM support



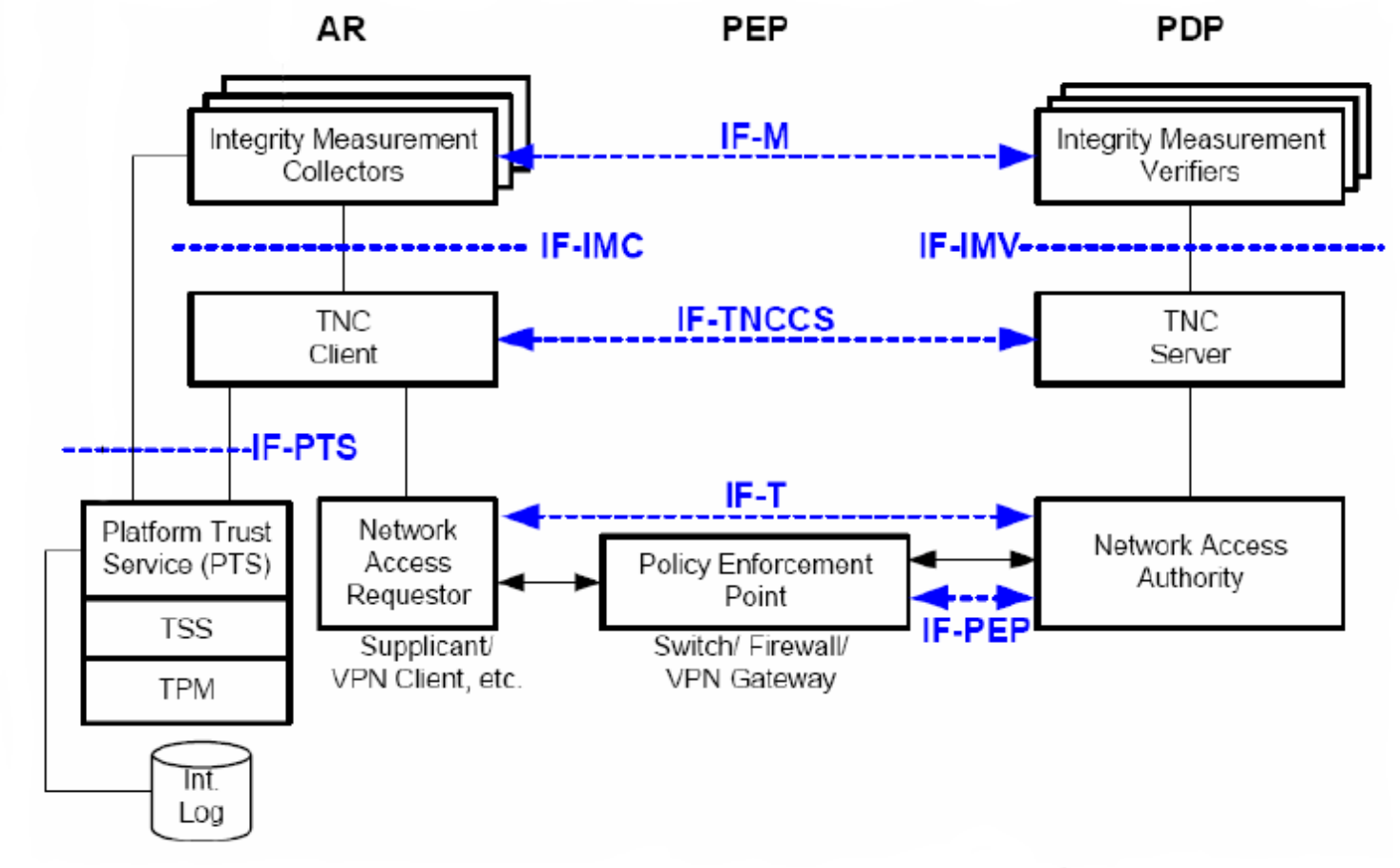
- One main advantage of TNC compared to other NAC solutions
  - Supports use of the TPM during TNC Handshake
  - Promising approach to solve the „lying endpoint problem“
  - Goal: Ensure integrity of TNC subsystem located on the AR
- Idea: Use TPM capabilities during TNC Handshake
  - Create integrity reports
    - Including signed PCR values
  - AR sends integrity report to PDP
  - PDP compares received values to known good reference values
    - PDP can verify integrity of TNC subsystem
- AR cannot successfully lie about its current integrity state!

TNC: TPM support – additional components

- PTS (Platform Trust Services)
  - System service on the AR
  - Exposes Trusted Platform capabilities to TNC components

- Further components
  - TPM (Trusted Platform Module)
    - Implements Trusted Platform's capabilities
  - TSS (Trusted Software Stack)
    - Exposes high level interface to TPM for applications
  - IML (Integrity Measurement Log)
    - Stores list of integrity measurements on AR

TNC: TPM extended architecture



[TNC Architecture for Interoperability Specification version 1.3 revision 6]

TNC: Reflecting interoperability / unforgeability

- interoperability
  - generally:
    - fulfilled, because all specifications are publicly available
  - in reality:
    - some experiences with TNC@FHH (see below …)
- unforgeability
  - generally:
    - fulfilled because TPM support is integrated in the design of the architecture
  - in reality:
    - futher reasearch and devolopment needed (see tNAC slides below…)

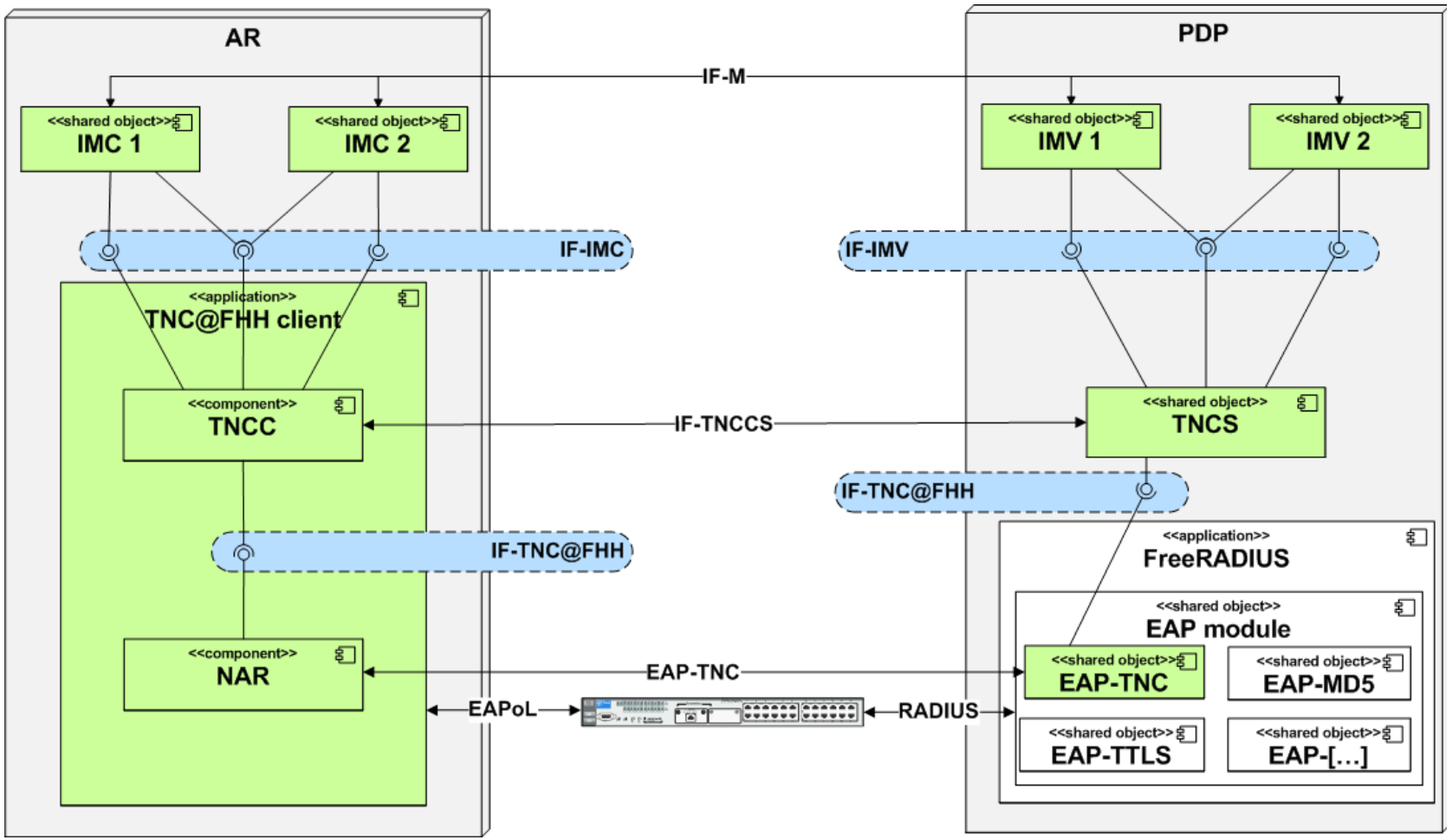
Content

- Introduction
- Network Access Control (NAC)
- Trusted Network Connect (TNC)
- **TNC@FHH**
- tNAC
- Conclusion

TNC@FHH: overview

- Open source implementation of TNC
- Developed at University of Applied Sciences and Arts, Hanover
- Implements all core TNC components/layers/interfaces
- No TPM support … yet

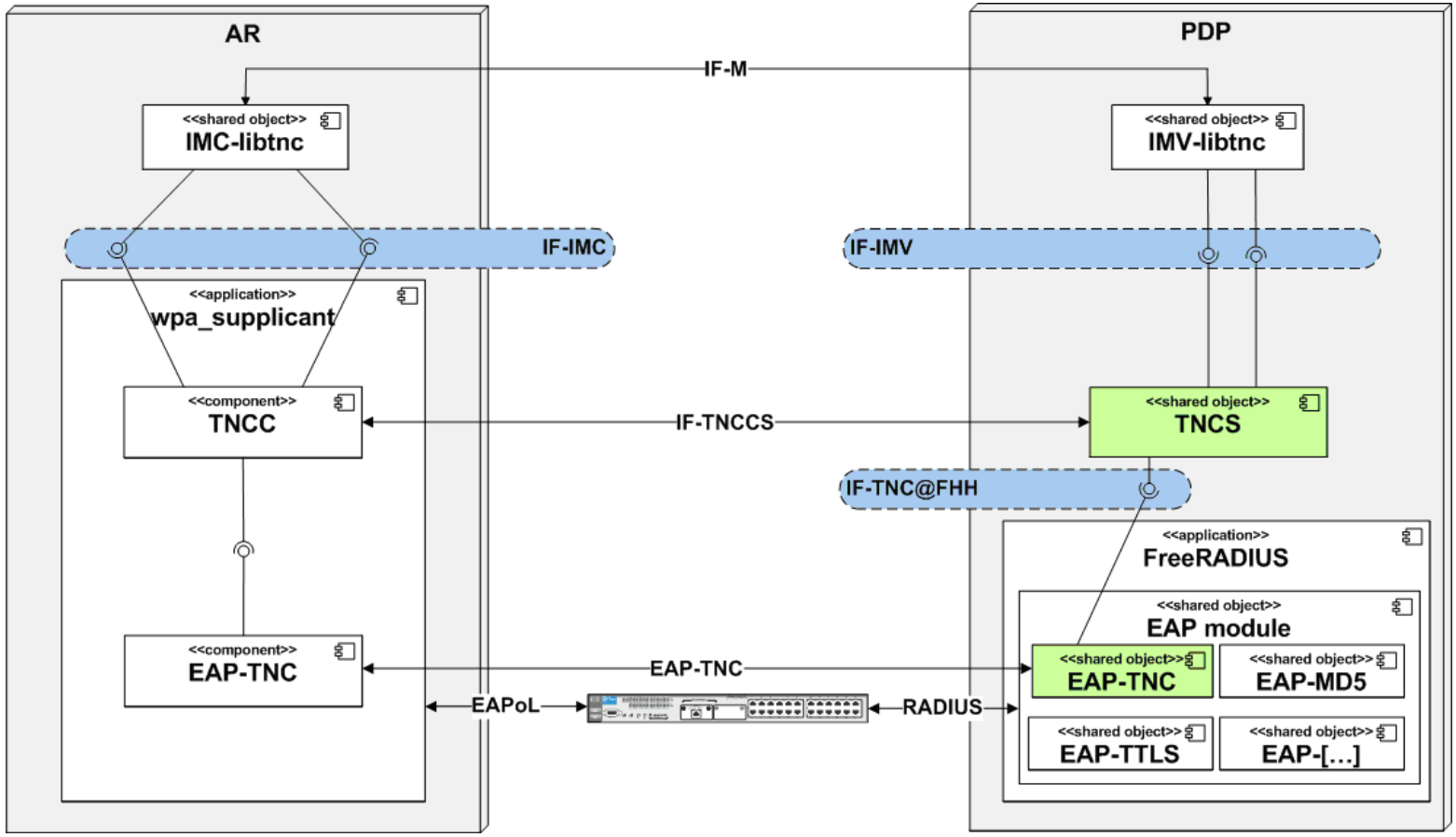
TNC@FHH: architecture



TNC@FHH: interoperability tests

- results from TNC plugfest in March 2008
  - different TNC implementations, mainly from open source developments, worked together (almost) without additional effort
  - conclusion:
    high degree of interoperability between main TNC components due to high quality of the specifications, especially
    - IMCs and TNC Client, due to IF-IMC
    - IMVs and TNC Server, due to IF-IMV
    - TNC Client and TNC Server, due to IF-TNCCS
    - NAR and NAA, due to IF-T
    - NAA and PEP, due to IF-PEP

TNC@FHH: TNC plugfest 2008



TNC support by commercial products

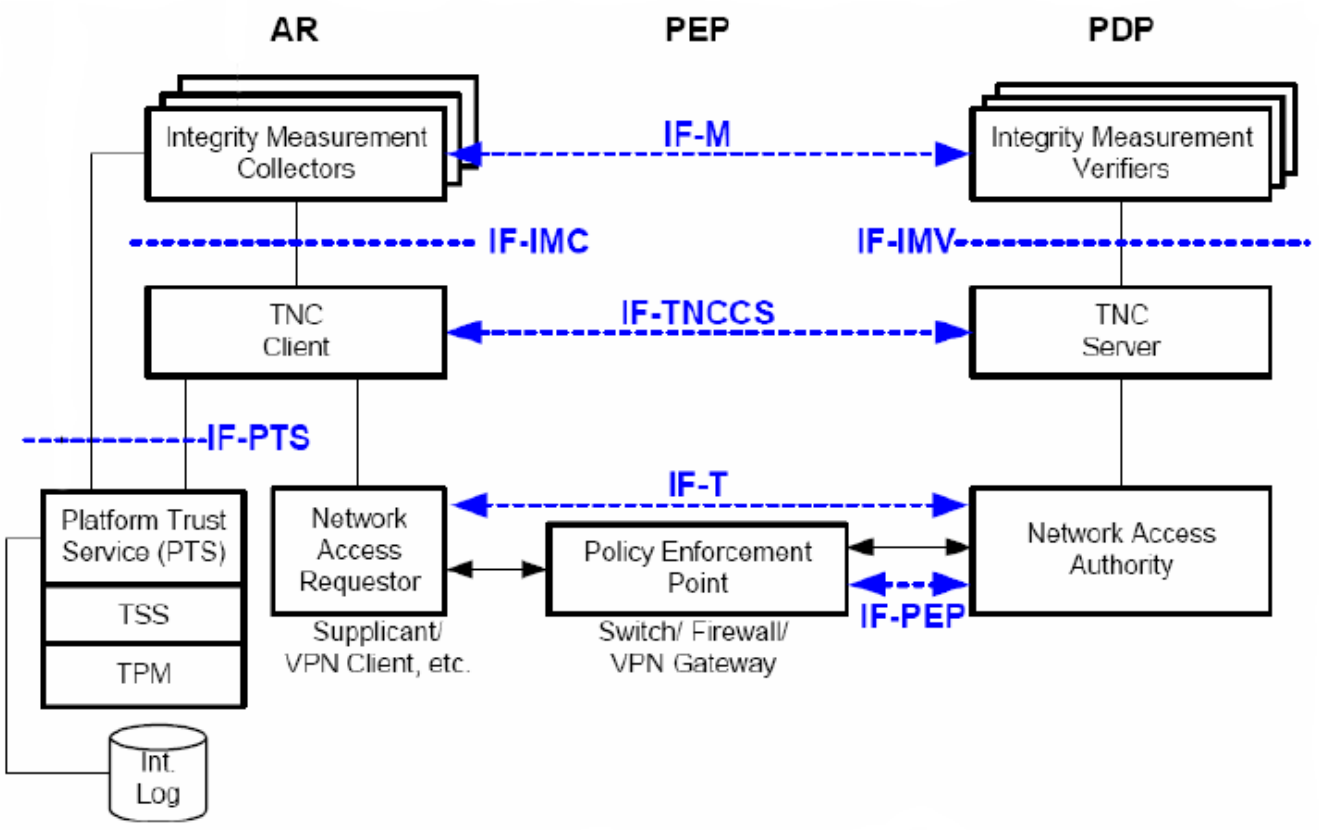
- results from researches in August 2008
  - only few commercial products support the TNC specification partly, i.e.
    - IF-IMC / IF-IMV to integrate IMC/IMV-pairs from different vendors
    - IF-PEP to support various PEPs
  - no commercial product supporting IF-TNCCS could be found

Content

- Introduction
- Network Access Control (NAC)
- Trusted Network Connect (TNC)
- TNC@FHH
- **tNAC**
- Conclusion

TNC: coming back to unforgeability…

- … remember the TPM extended architecture



TNC: PTS features

- Creates integrity reports
  - Makes them available to IMCs / TNCC
  - Enables them to be used during TNC Handshake
  - Ensures that they are rendered in an standardised format
    - TCG Schema Specifications

- Measures integrity status of …
  - TNC components
  - On disk & in memory measurements
  - Appends measurements to IML

- Why should one trust the PTS ?

TNC: PTS & The Chain of Trust

- PTS must be part of the Chain of Trust
  - Measure PTS before execution
  - Not supported by „normal“ OS
    - Need for a Trusted OS
- PTS responsible for measuring (at least) TNC components
  - TNC components become part of Chain of Trust, too
- Benefit
  - Chain of Trust up to Application Level
    - Especially including TNC components on the AR
  - Integrity of TNC subsystem can be ensured
    - No lying endpoint problem anymore
- How are integrity reports communicated between AR and PDP ?

TNC: PTS IMC/IMV

- Special IMC/IMV pair
  - What ?
    - Responsible for communicating integrity reports
    - PTS-IMC interfaces with PTS to obtain integrity reports
    - Communicates them to PTS-IMV during TNC handshake
    - PTS-IMV evaluates received integrity reports
  - How ?
    - Open issue
    - IF-M protocol between IMC/IMV generally implementation specific
    - TCG expects to standardise widely useful IF-M protocols
      - Like IF-M between PTS-IMC/IMV
      - Essential for interoperability between a PTS-IMC and a PTS-IMV from different vendors

TNC: Establishing TNC Subsystem Integrity

- Collection of Integrity Data
  - Pre-OS Boot
    - Starting from RTM : BIOS, OS-Loader, OS-Image
  - Pre-PTS Startup
    - OS must measure PTS (including TSS)
  - PTS Operation
    - Measure TNC components (NAR, TNCC, PTS-IMC, further IMCs)
    - Render measurements in interoperable format
  - PTS-IMC Collection
    - Obtain Integrity report containing Chain of Trust from PTS
- Reporting to PTS-IMV via IF-M
  - PTS-IMV evaluates integrity report
  - Provides access decision – along with all other IMVs

TNC: Further Integrity Checks

- Motivation
  - Check integrity of further applications on the AR
  - E.g. Anti Virus, Firewall … in addition to its configuration
- (At least) two possible approaches
  - Application specific IMC/IMV pair interacting with PTS
    - IMC/IMV pair measures configuration and integrity
    - Needs to interact with PTS … standardised but quite advanced
    - What about standardised IF-M?
  - PTS-IMC/IMV measures further integrity aspects
    - IF-M must support that PTS-IMV requests integrity checks of arbitrary components
    - No need for application specific IMC/IMV pair to care about PTS
    - Very complex process of decision making

tNAC: the project

tNAC
trusted network access control

- Research Project:
  - Started on July, 1st 2008
  - Scheduled for 3 years
- Consortium consisting of
  - University of Applied Sciences and Arts Hanover
  - University of Applied Sciences Gelsenkirchen
  - Ruhr-University Bochum
  - Datus AG
  - Sirrix AG
  - Steria Mummert Consulting AG
  - and some other companies
- Sponsored by the
  Federal Ministry of Education and Research

SPONSORED BY THE
Federal Ministry
of Education
and Research

tNAC: objectives

- Develop a Trusted Network Access Control Solution
  - TNC compatible NAC solution with full TPM support
- Analyse requirements & evaluate effectiveness of tNAC
  - Based upon real world scenarios
- Participate in TCG‘s specification process
  - Contribution to IF-M between PTS-IMC/IMV
- Management
  - Keep (t)NAC manageable (Policy-Manager, Management-Console)
    - Focus on usability as well as technology

tNAC: Turaya and TNC@FHH

- Combine results of two research projects
- Turaya
  - Open source security platform
  - Developed by the former EMSCB-Project
  - Supports strong isolation of security critical processes in “compartments”
- TNC@FHH
  - Open source based implementation of TNC
  - Developed at University of Sciences, Hanover
  - Implements all core TNC components/layers/interfaces
  - No TPM support … yet

tNAC: adoption of TNC in real world scenarios

- first analyses (two master thesis) in 2008 with focus on
  - adoption of TNC in the LAN environment of a company
  - adoption of TNC in the VPN environment of a company
- summary of the results
  - security benefit of a TNC solution is evident and desired (by the companies)
  - several handicaps prevent the adoption today, especially
    - high complexity of policy definition and enforcement
    - efforts and investments required for integration of TNC into the existing IT infrastructure
    - today's impossibility to achieve unforgeability due to the lack of TPM support in standard operating systems

Content

- Introduction
- Network Access Control (NAC)
- Trusted Network Connect (TNC)
- TNC@FHH
- tNAC
- **Conclusion**

Conclusion (1/2)

- TNC seems to be the most hopeful approach towards a real interoperable, real trusted NAC solution:
  - interoperability and unforgeability included by design
  - interoperability in TNC is obviously actually good
    - although: today commercial products supporting TNC are rare
  - unforgeability is well designed but hard to achieve
    - further research and development activities as well as further specifications and standardisations are needed

Conclusion (2/2)

- The need for such a solution will grow according to
  - the increasing importance of endpoint security for the overall network security and
  - the strongly increasing security threats to endpoints.
- TCG and many others (like the tNAC consortium) are working on further developments and enhancements required for a real interoperable, real trusted NAC solution.