Trust in the P2P Distribution of Virtual Goods

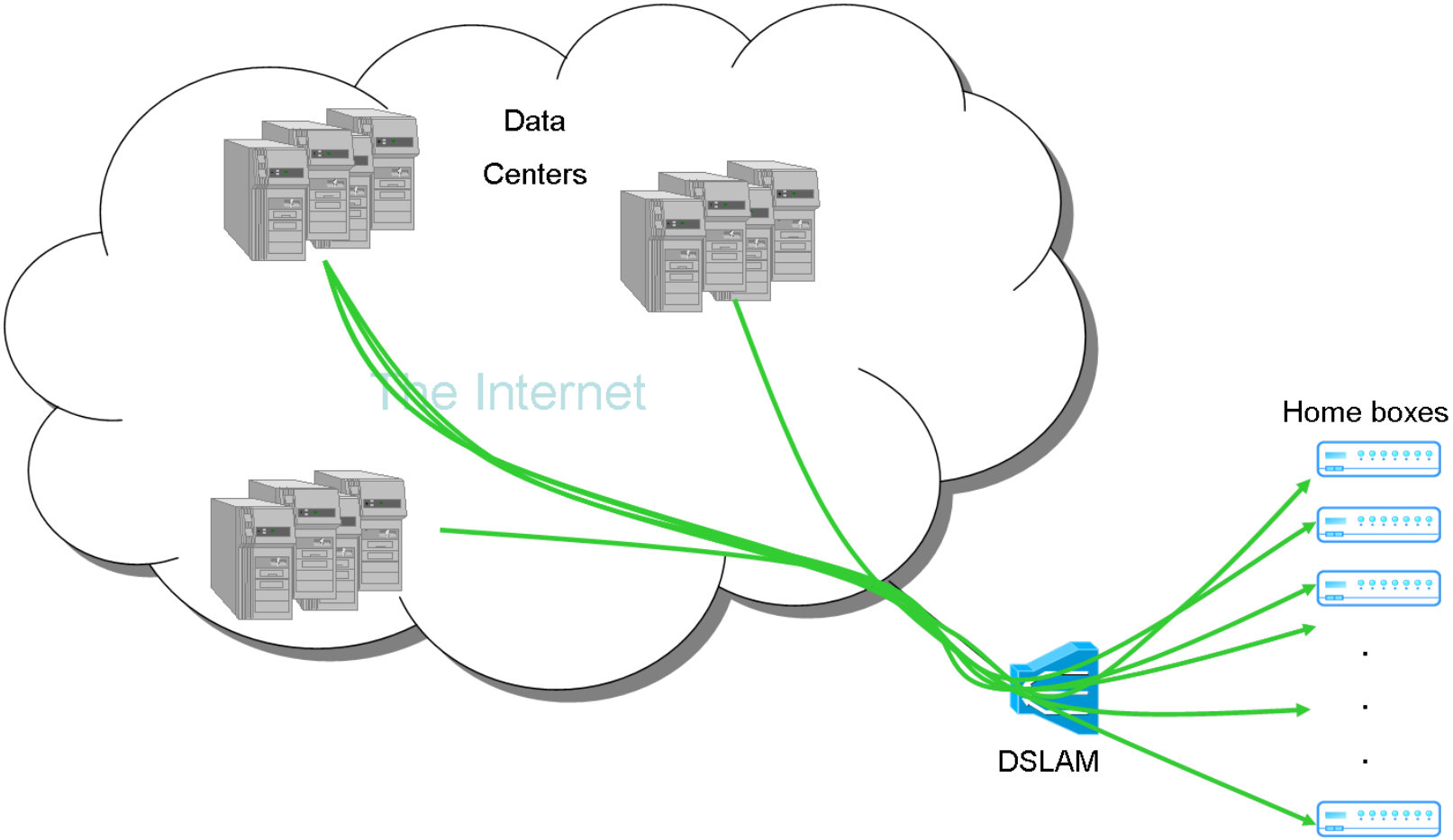
Nicolai Kuntze[1], Jürgen Repp[1], Martin May[2], Fabio Picconi[2], Renata Teixeira[3]

[1]Fraunhofer Institute for Secure Information Technology (SIT)
Darmstadt, Germany
[2]THOMSON S.A.
Paris, France
[3]Lip6
Paris, France

September 2009 / Virtual Goods 2009

Outline

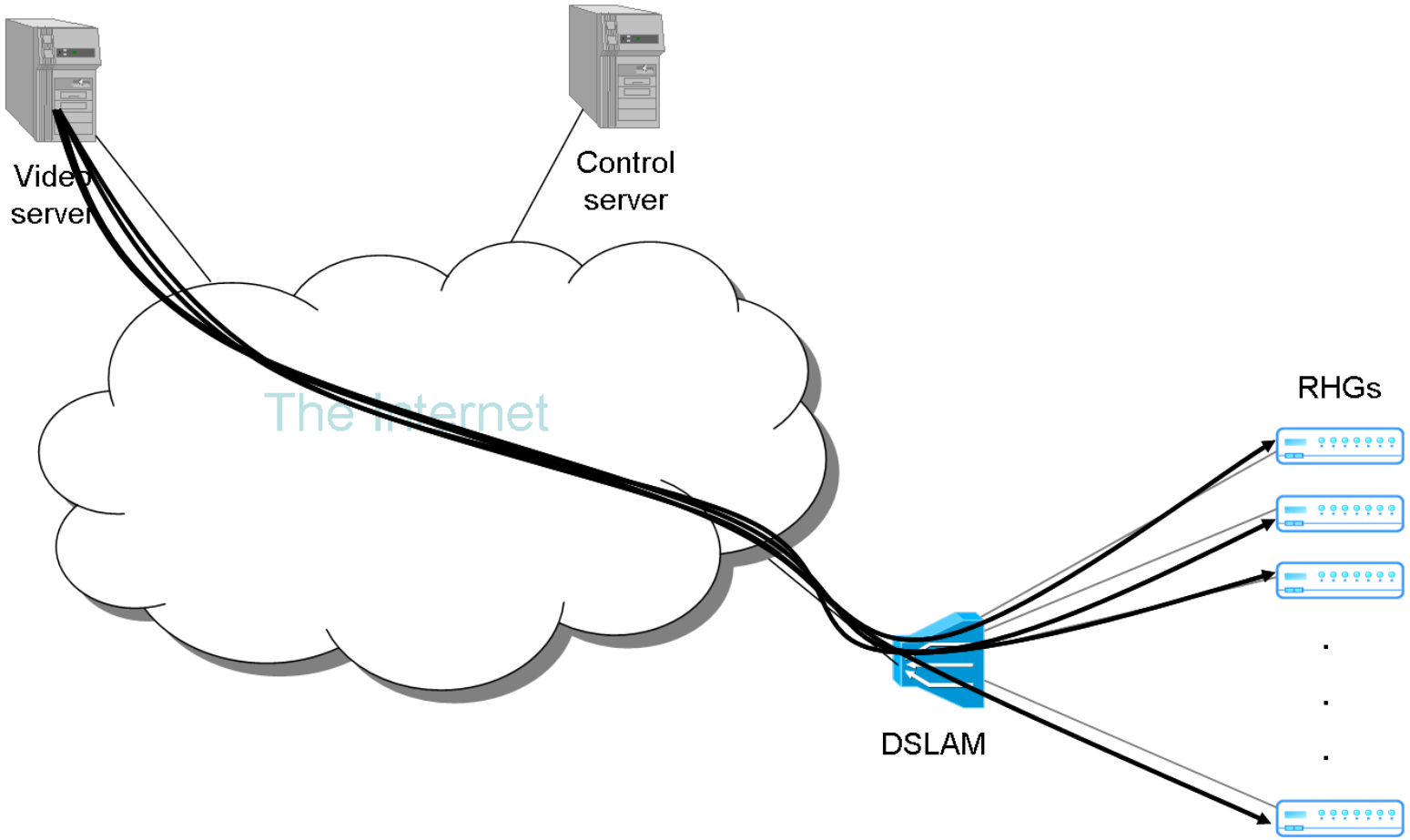
The current model: Data centers



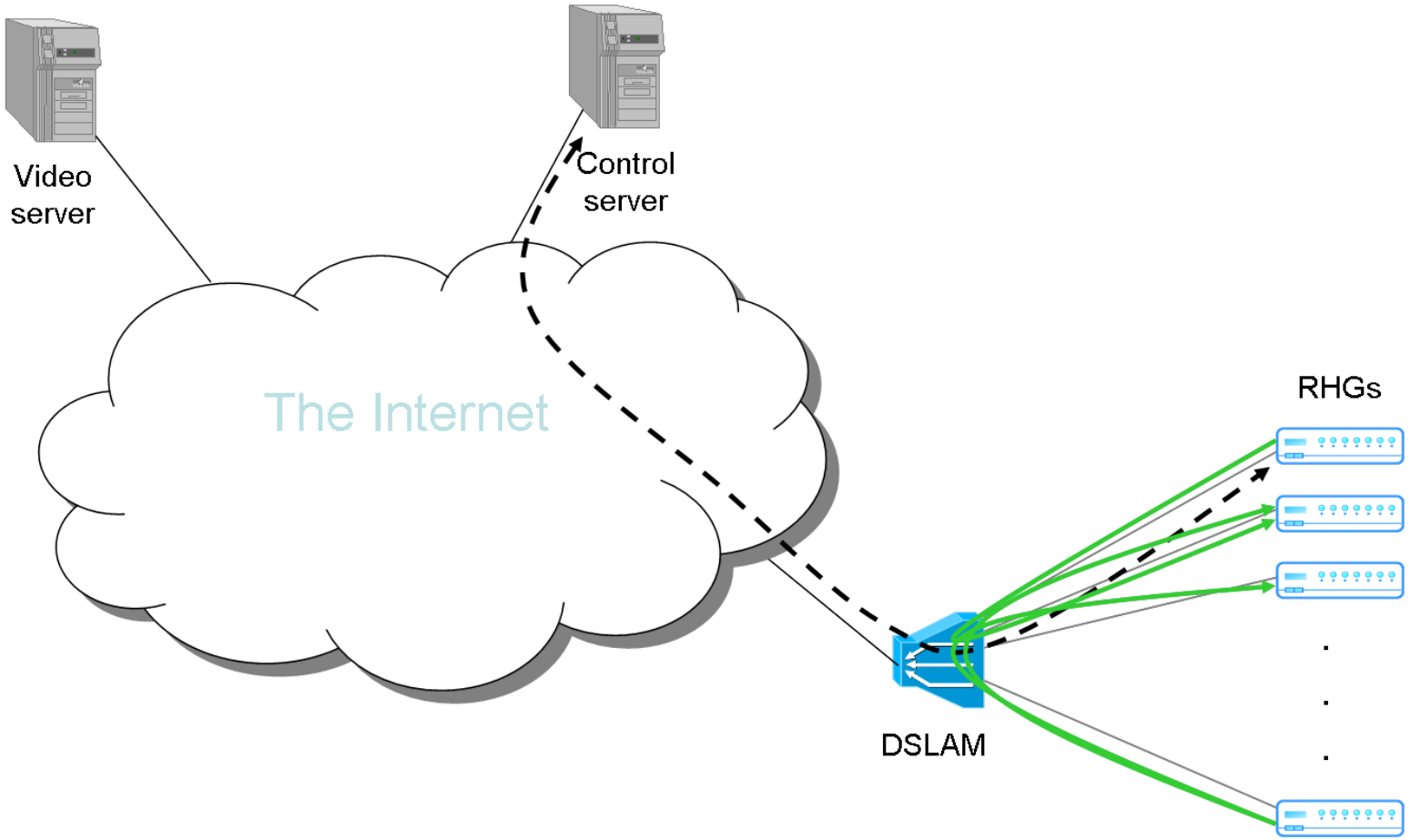
The current model: XPU

- The security coprocessor of the SMP863x is mainly responsible for encryption/decryption tasks but it also provides secure storage of secret keys. The private part of an RSA keypair cannot be extracted from the XPU therefore it is a secure device for DRM related tasks.
- There is an AES core embedded in the XPU.
- The XPU is also responsible for the initial boot of the system, controlled by the XOS.

The nano data center model



The nano data center model

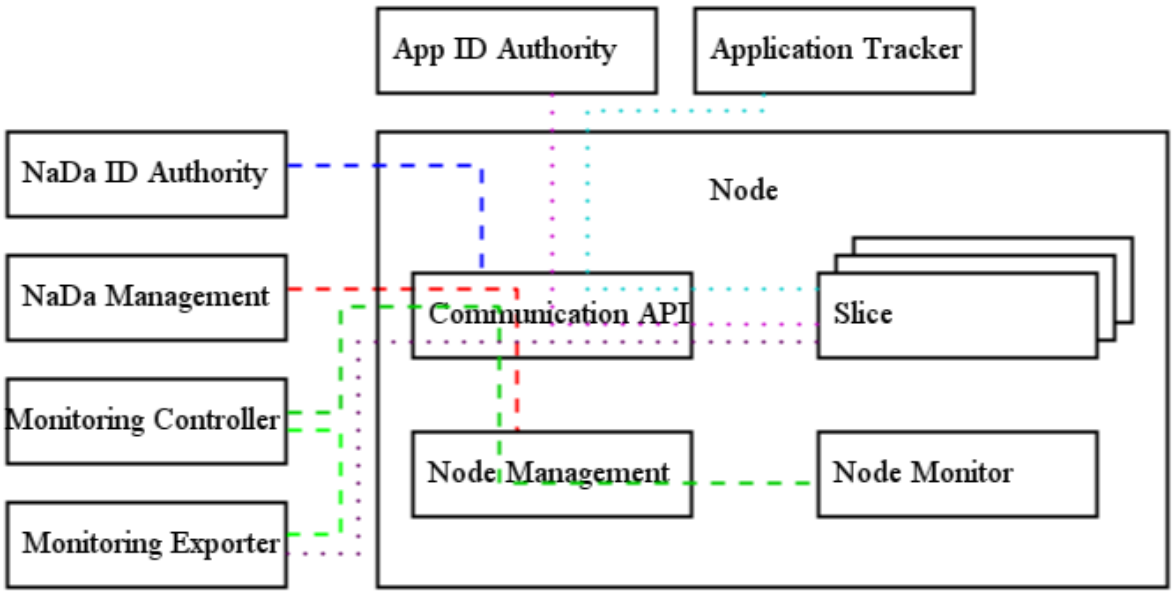


NaDa Objectives

- To provide a new distributed hosting edge infrastructure
  - Using a large number of geographically dispersed nano data centers to complement data centers
  - To optimise the performance experienced by the user
- To provide a new secure and managed P2P content delivery paradigm
  - With advanced monitoring capabilities
  - Incentive mechanisms for those who provide access to edge resources
- Reduce overall energy consumed in content delivery

Multi Stakeholder Environment

- Each node supports a multitude of stakeholder slices
- The service provided by the slices of one stakeholder is considered as one application



Security requirements analysis

- In this paper we concentrate on those requirements that can be supported by the underlying platform and that provide a security basis used by applications to build their own security system
- If a stakeholder considers certain data as to be protected he has to take appropriate measures

Isolation of Stakeholders

Information Governance is the central requirement of the

- isolation of the different stakeholder applications
- identity of each node and slide
- status of the node and resp. applications hosted by it
- integrity of the content

Hardware-based trust anchor

- NaDa establishes nodes in the households of the end-users
- Strong identities and reporting technologies are required
- Hardware-based security approaches like Smart Cards and Trusted Computing promise the required base to implement adequat protection schemes

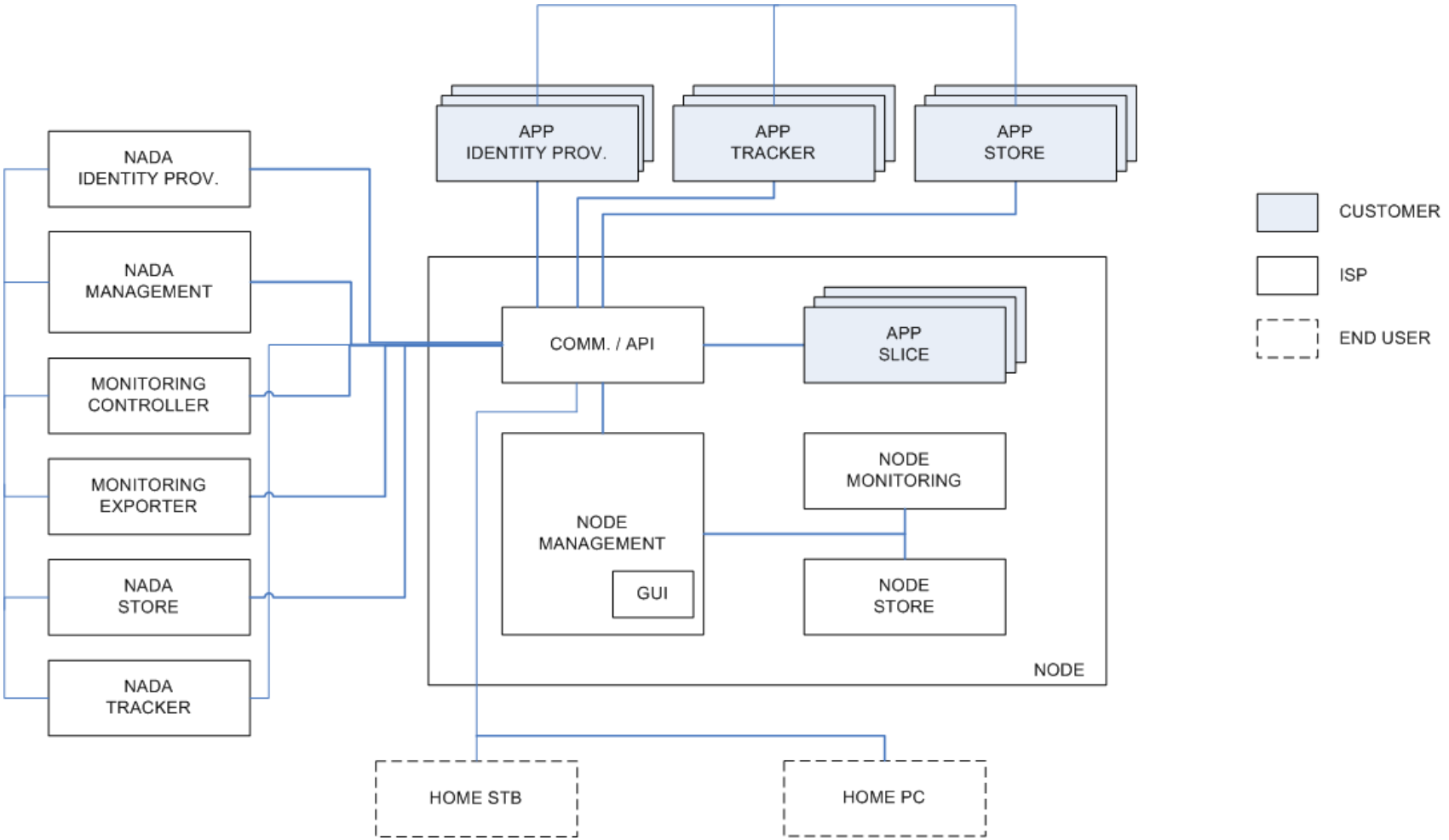
Aims of the NaDa security architecture (brief)

- NaDa security architecture has to cover the full business process to allow all involved stakeholders to put trust into the platform
- Trust on a technical level just says that a system will always behave in an expected manner
- Architetcure has to be defined on the level of the individual node, it's interaction, and the supporting infrastructure

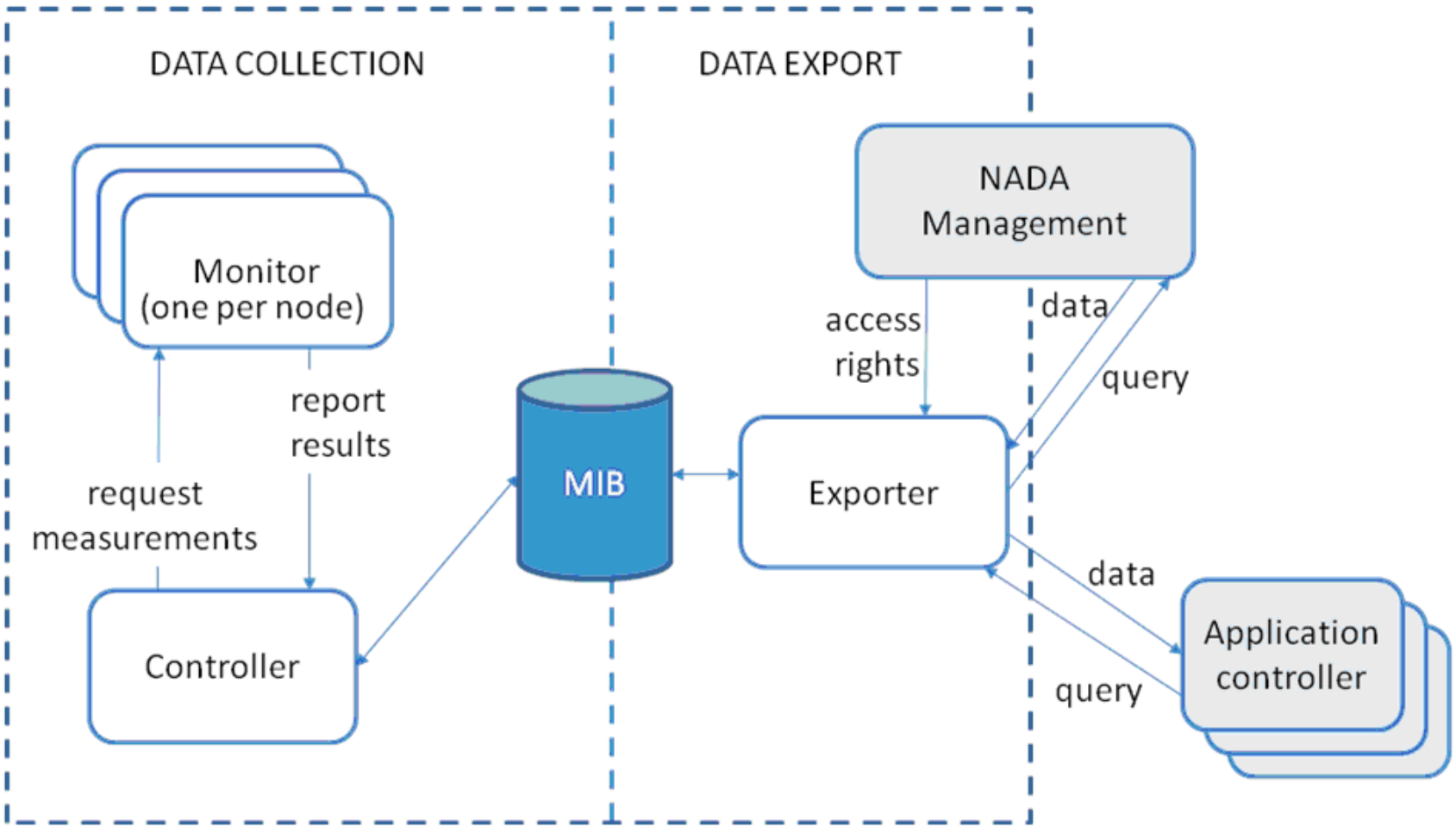
Node design

- Stakeholders represented by their software need to be isolated from each other in terms of access and resource control
- tampered or malicious nodes need to be excluded from the P2P network
  - A node has to provide a proper identity showing that it belongs to the network
  - A node has provide proof that it complies to a defined state (“authenticity of behaviour”)

NaDa node architecture



NaDa monitoring architecture



authenticity of behaviour

- Remote Attestation is the key functionality used to provide proof on the behaviour of the node
- Timing is a big challenge for streaming of media content
- Each verifier need a data base containing all reference values of possible node states. Therefore it is required to introduce a time saving alternative (in terms of transferred data and computational cost)

Conclusion NaDa

- The change in the distribution scheme as proposed by NaDa introduces new challenges in terms of resilience of the used hard- and software
- The presented architecture is based on available standard hardware and has the potential to spur the implementation of real word applications
- Other applications for the results aside the distribution of multimedia content are also possible and under research

What is Trust?

Trust An entity can be trusted if it always behaves in the expected manner for the intended purpose

Definitions

Attestation

1. an act of attesting. 2. an attesting declaration; testemony; evidence
Source: www.dictionary.com

Measurement

The process of obtaining the identity of an entity. Normally this is an cryptographic hash
Source: TCG documents

Security

A condition that results form the establishment and maintenance of protective measures that ensure a state of inviolability form hostile acts or influences

Definitions

Attestation

1. an act of attesting. 2. an attesting declaration; testemony; evidence
Source: www.dictionary.com

Measurement

The process of obtaining the identity of an entity. Normally this is an cryptographic hash
Source: TCG documents

Security

A condition that results form the establishment and maintenance of protective measures that ensure a state of inviolability form hostile acts or influences

Definitions

Attestation

1. an act of attesting. 2. an attesting declaration; testemony; evidence
Source: www.dictionary.com

Measurement

The process of obtaining the identity of an entity. Normally this is an cryptographic hash
Source: TCG documents

Security

A condition that results form the establishment and maintenance of protective measures that ensure a state of inviolability form hostile acts or influences

What is Trusted Computing?

Trusted Platform Module

- Defines a set of services
- Adds protocols and messages that take advantage of the TPM

TPM is a platform component

- It is bound to the platform

The TPM contains

- cryptografic engine
- protected storage

Isolation

- Functions and storage are isolated
- Provides a “trust boundary”

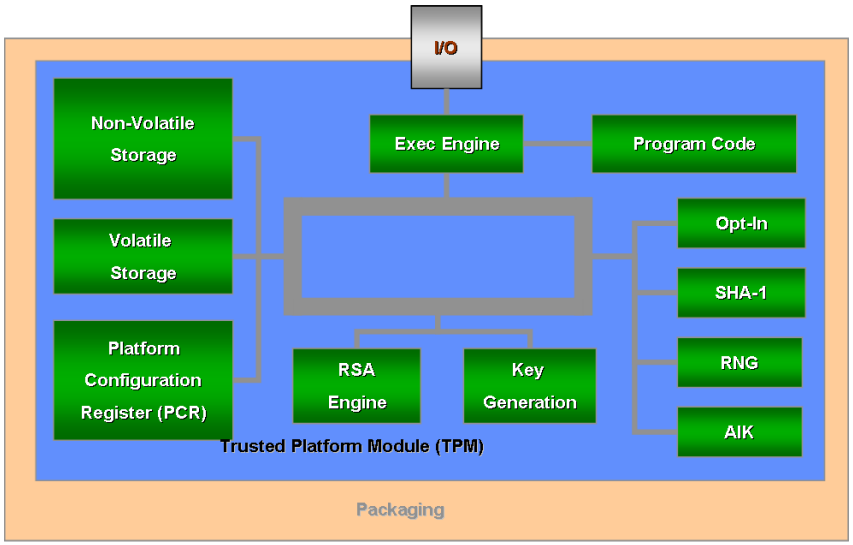
Roots of Trust

Root of Trust for Measurement (RTM) Establishing and extension of trust from an initially trusted security anchor up to further used components of a system while boot-up

Root of Trust for Reporting (RTR) is responsible for establishing platform identities, reporting platform configurations, protecting reported values, and providing a function for attesting to reported values

Root of Trust for Storage (RTS) provides protection on data in use by the TPM but held in external storage devices. The RTS provides confidentiality and integrity for the external blobs.

Trusted Platform Module

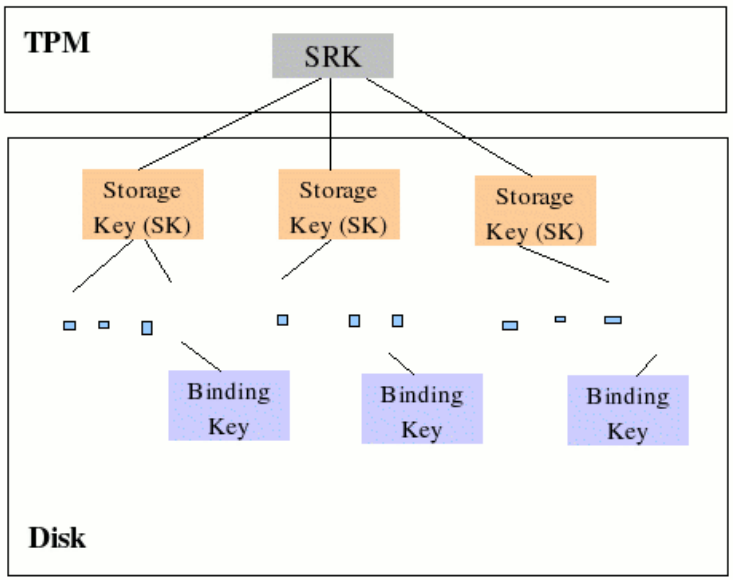


- Cryptografic engine
  - RSA 2048 bit keys
  - SHA 1 (160 bit hash values)
  - Random number generator
- Implements RTR and RTS
- Keeps two persistent keys
  - Endorsement Key (EK)
  - Storage Root Key (SRK)

TCG PC Client H/W Design

- TPM is attached to motherboard
- TPM can not be removed, the attachment is permanent
- TPM communicates through Low Pin Count (LPC) Bus
- LPC Bus is existent at all PC platform as the BIOS is attached to it

Root of Trust for Storage



Storage Root Key Created during “take ownership”

Storage key RSA key that is only used to encrypt other keys

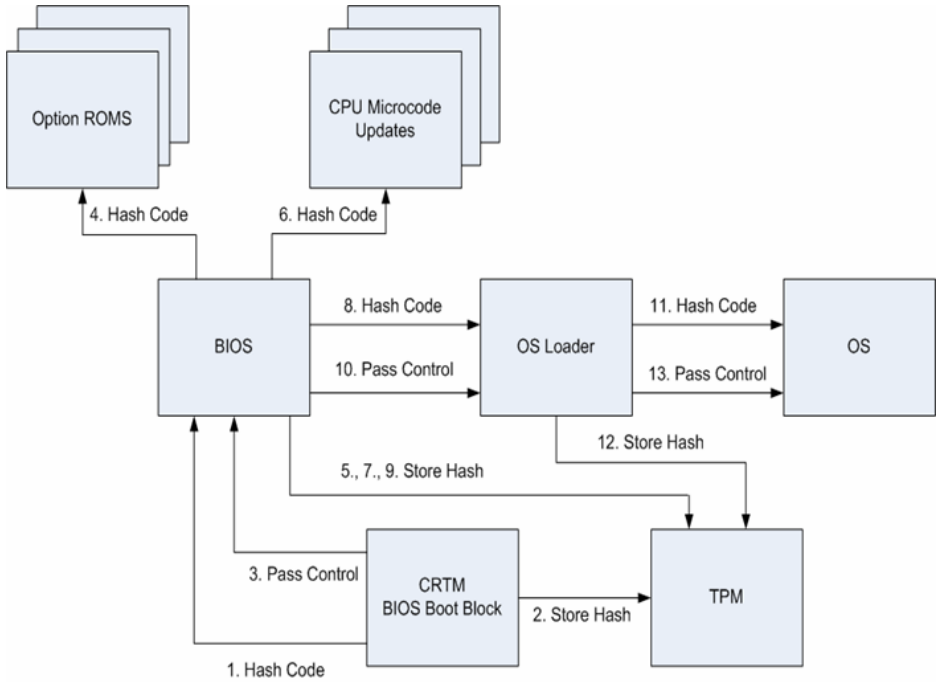
Binding key RSA key that is used to encrypt (small amount of) generic data or other symmetric keys (to encrypt larger amount of data)

Root of Trust for Reporting

- Main aim of Trusted Computing is to provide evidence on the state of a device to an external verifier
- The verifier decides on the trustwothiness based on the reported state and presented credentials
- We destinguish between a static root of trust (e.g. as part of the BIOS) and a dynmic root of trust (established later)

Trusted Boot - Measurement of System State (RTM usage)

- Measurement of the initial device state and confirms integrity of the underlying system
- TPM acts as the RTR, BIOS as the RTM
- Each component is measured before it is started
- This is not transitive

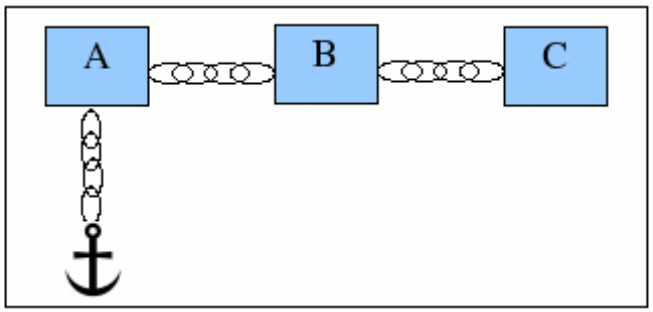


Measurement in Detail

- Platform Configuration Register (PCR) store a representation of the system state
- Measurements are stored in the Stored Measurement List (SML)
- The next state is calculated according to

$$\text{PCR}_i = \text{SHA-1}(\text{PCR}_i \mid \text{new value})$$

- TPM offers 15 registers
- PCRs can be used as a key restriction used by the RTS



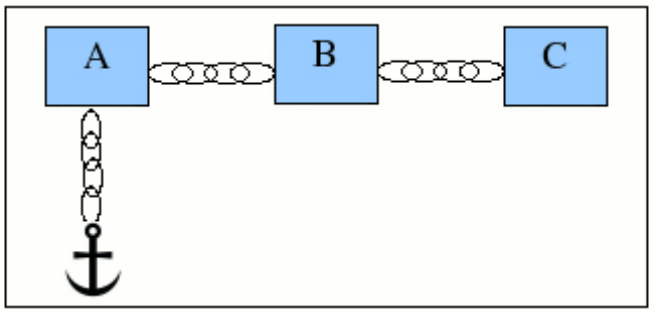
- "chain of trust"

Measurement in Detail

- Platform Configuration Register (PCR) store a representation of the system state
- Measurements are stored in the Stored Measurement List (SML)
- The next state is calculated according to

$$\text{PCR}_i = \text{SHA-1}(\text{PCR}_i \mid \text{new value})$$

- TPM offers 15 registers
- PCRs can be used as a key restriction used by the RTS



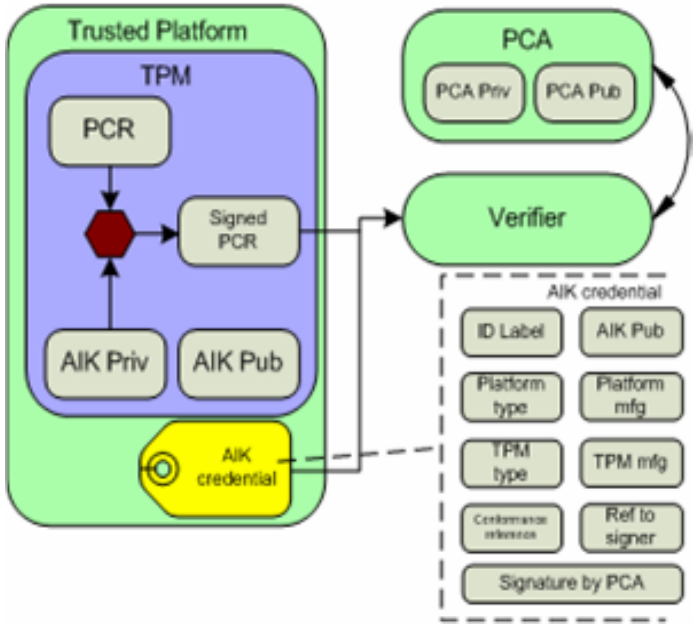
- “chain of trust”

Remote Attestation

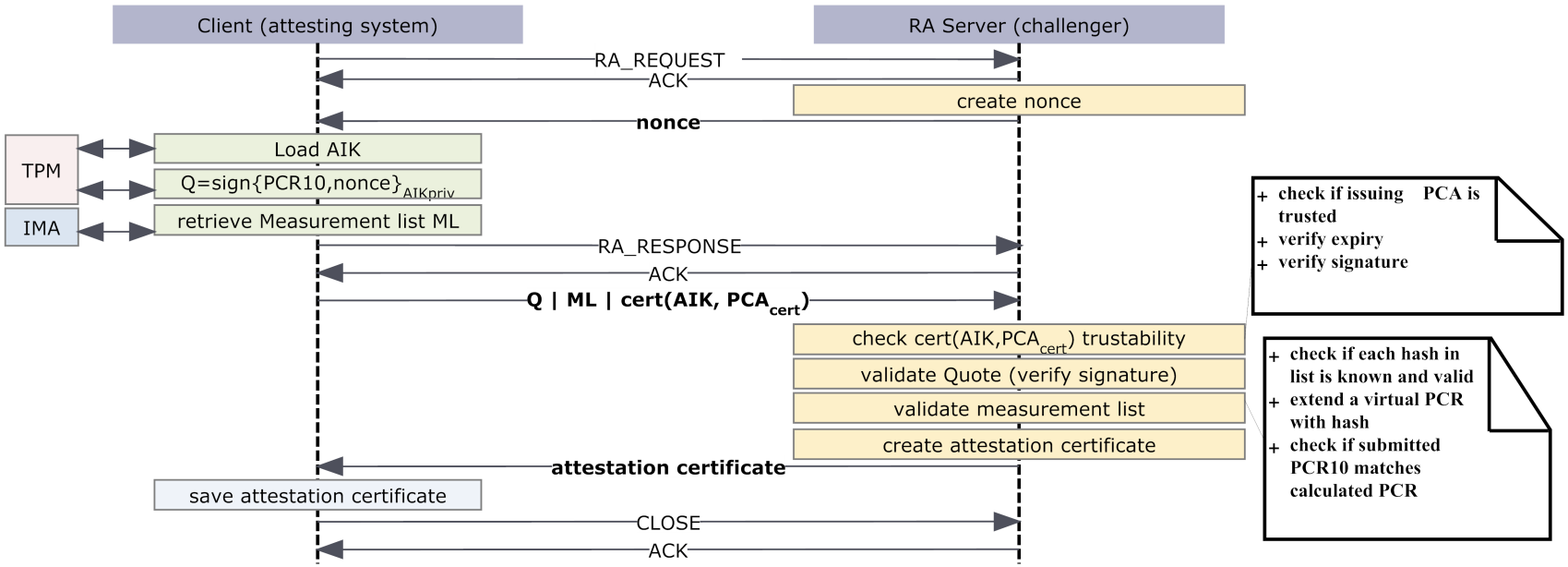
Trusted Boot Provides the measurements used to state the system state

Attestation Process Offers a third party evidence about the actual system state

Attestation Identity Keys Revealing the identity of the system by in the context of the attestation process and are produced by the Privacy CA (PCA)



Remote Attestation Protocol



More privacy in Remote Attestation

- In each attestation the AIK is presented, therefore it is linkable
- Direct Anonymous Attestaion was introduced to prevent profile creation
- System builds up on the Idemix approach using zero-knowledge proofs

EK and AIK details

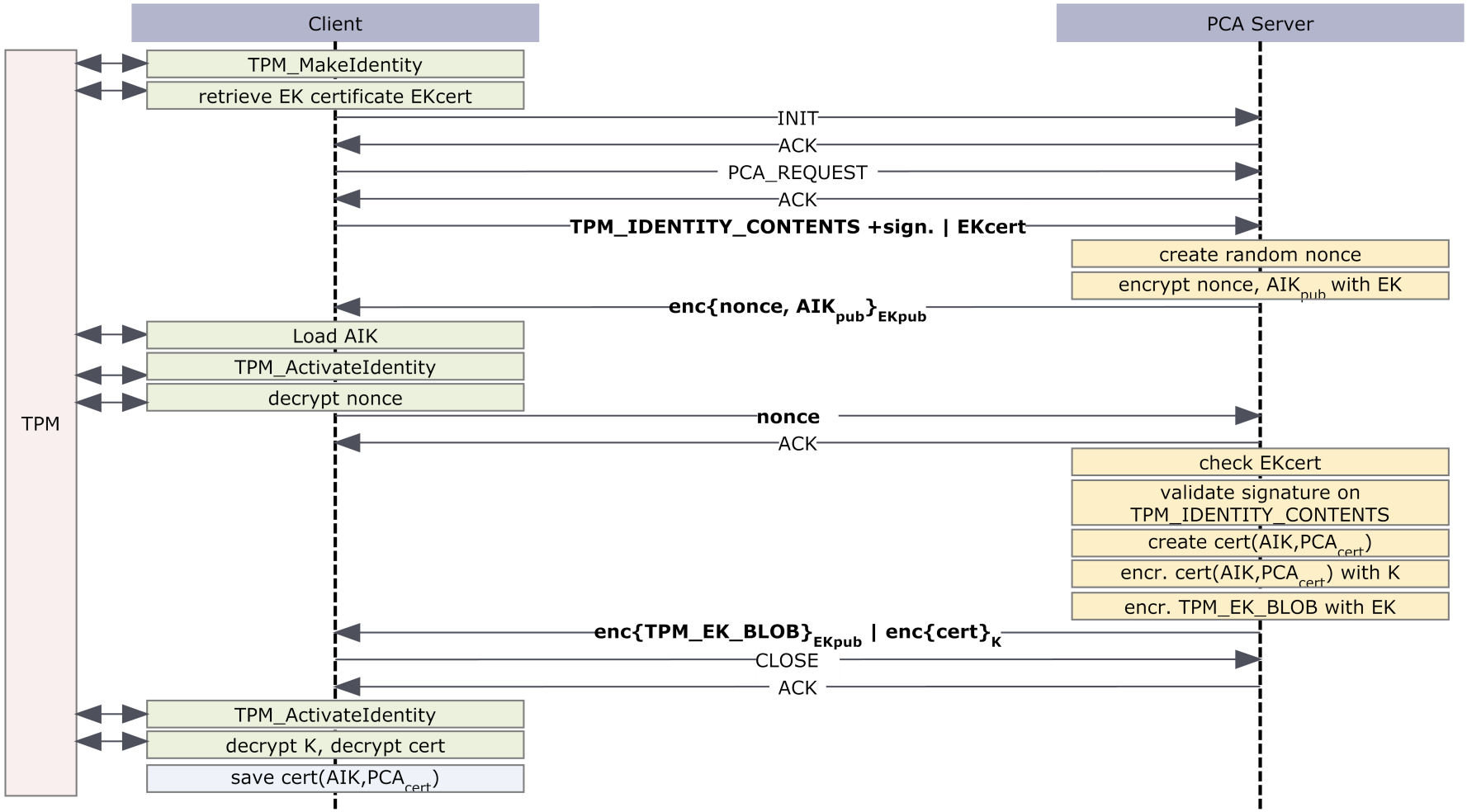
Endorsement Key

- Each TPM has a unique ID represented by the Endorsement Key
- can ONLY encrypt data used in the AIK creation process
- can NOT sign data (!)

Attestation Identity Key

- can ONLY sign data created by the TPM (PCRs and keys)
- TCG introduced the Attestation Identity Keys (AIK) as representatives protecting the privacy

AIK creation



More functions

Monotonic counters Provides an ever-increasing incremental value.

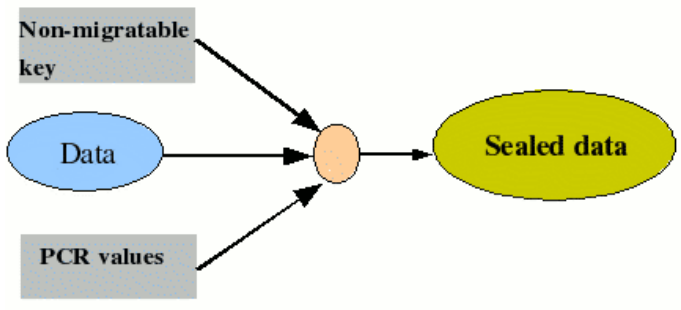
- **Internal Base** Internally by the TPM
- **External Counter** 7 years of increments every 5 seconds without hardware failure

Time Source Specialised Counter that is initilised with zero at power up and a session Nonce

Protect data with TPM

Data binding A (migratable) binding key is generated and used to encrypt data

Data sealing Data is encrypted, bound to a specific TPM platform and a particular configuration



Implicit Attestation

- Sealing leads to interesting possibilities in the area of Remote Attestation.
- Assume a key α that can only be used by entity A in a defined state σ
- Assume entity B who knows A and the desired state σ
- Attestation process:
  1. B->A: B Sends Nonce to A
  2. A->B: A responds by sending $Sig(Nonce)_{\alpha}$
- A testified that it is in posession of the key α

Attack scenarios

TPM Reset Attack Connected to the system over the Low Pin Count Bus (LPC) the TPM can be reset by connecting the LRESET pin of the LPC bus to ground.

Platform Reset Attack Also known as cold boot attack, this side channel attack relies on the fact that data stored in volatile memory remains readable for a small amount of time after the system power has been removed.

Cross Certification Vulnerability If a user calls the TPM_CertifyKey command to obtain a certificate for a key k using AIK_s as a signing key, the attacker intercepts the command and replaces the key handle and HMAC parameters for k with those for a key k_a he owns. Thus the TPM generates a certificate for the attacker's key.

Conclusion Trusted Computing

- Trusted Computing offers a new security paradigm
- Still it is not used largely
- Adoption to other platforms (e.g. embedded or mobile devices) is missing
- Research on use cases is required
  - Virtualisation
  - autonomous systems