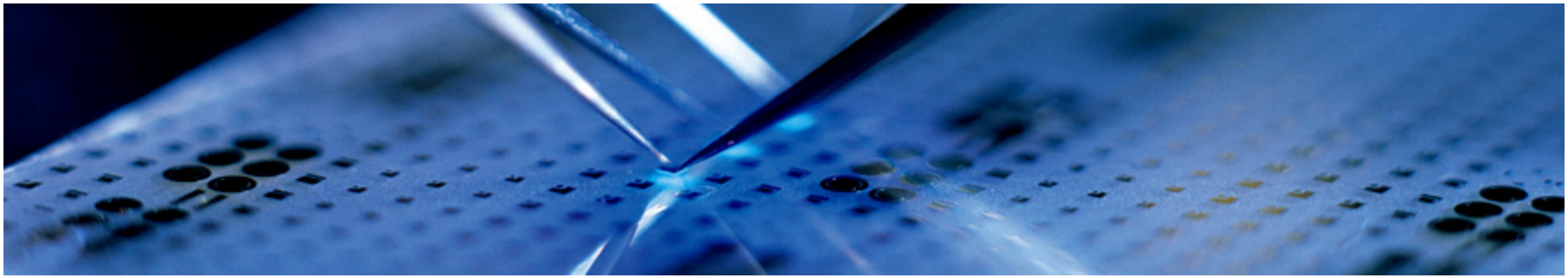


Nicolai Kuntze, Dominique Mähler, Andreas U. Schmidt

Employing Trusted Computing for the forward pricing of pseudonyms in reputation systems

Virtual Goods Workshop/ Leeds
14.12.2006

Fraunhofer Institut Sichere Informations-Technologie

Marketplaces for Virtual Goods

- Market places for virtual goods are increasingly occupied by self-organising communities. These market places exhibit the characteristics of the so-called long tail economy.

- The classical asymmetry between suppliers and consumers is lifted. Buyers and sellers are often even in numbers and may change their roles dynamically.

- Virtual, or physical, goods are offered in large numbers and diversity and with potentially small demand for each single one.

- Matchmaking and orientation of buyers is difficult in a long tail economy, long term relationships are hard to build, and trust between trade partners must be established somehow.

Marketplaces and Reputation Systems

A common approach is to let market players themselves provide the necessary guidance. This is mostly embodied in reputation systems

Buyers and sellers rate each other and the goods sold, trying to establish “the shadow of the future“

The goal is to establish a homogeneous market for honest participants.

That community ratings (of goods) do in fact strongly influence buyer behaviour is shown.

Reputation systems and social frauds 1/2

Existing reputation systems are fragile, in that they can easily be distorted or abused even within the frame of laws governing them.

'Attacks' of this kind threaten the integrity of the informational content stored in the system.

The following attacks can be classified

- *Ballot stuffing*: A seller colludes with a group of buyers in order to be given unfairly high ratings.
- *Bad-mouthing*: Sellers and buyers collude to rate other sellers unfairly low to drive them out of the market.
- *Negative discrimination*: Sellers provide good services only to a small, restricted group of buyers.
- *Positive discrimination*: Sellers provide exceptionally good service to some buyers to improve their ratings.

A situation of controlled anonymity in which the market place knows the identity of participants and keeps track of all transactions and ratings, but conceals the identity of buyers and sellers, is identified as essential to avoid unfair behaviour.

Reputation systems and social frauds 2/2

The best known individual attack on reputation systems uses *Sybils* to obtain a disproportionately large influence.

General problem of **'cheapness' of pseudonyms** in marketplaces and reputation systems, since with name changes dishonest players easily shed negative reputation.

There is also an explicit threshold for the transaction costs for reputations needed to avoid ballot stuffing.

However, an indiscriminate pricing of identities for the submission of ratings poses an undesired entry deterrent. It seems therefore plausible that reputation systems should be based on **pseudonyms** which allow for a flexible forward **pricing**

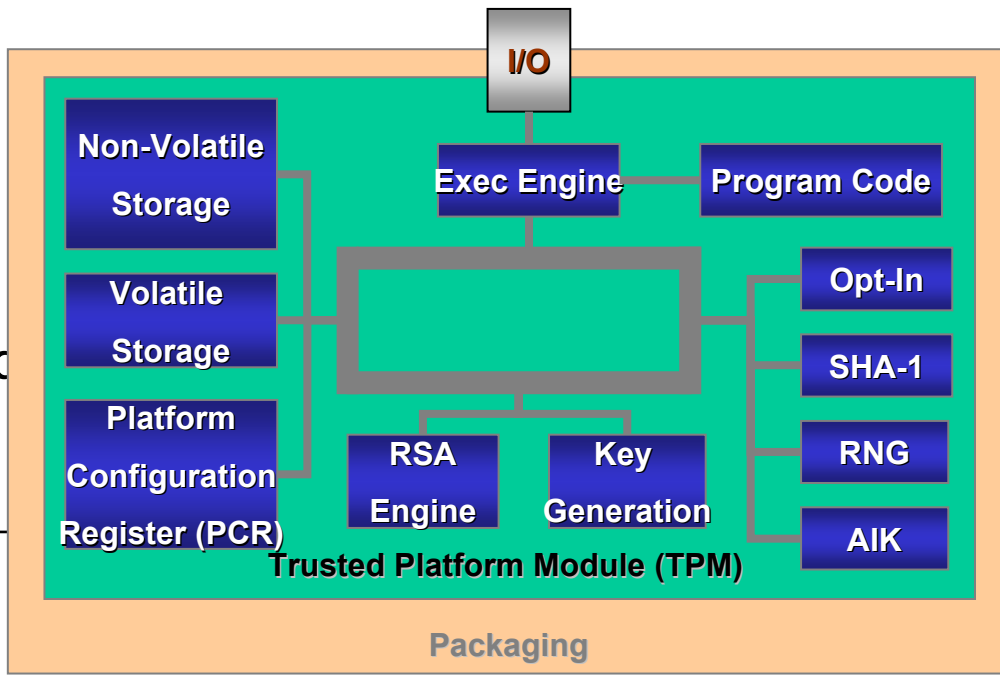
Terminology

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

- Trusted Computing
  - Basically a reporting technology to testify the state of a certain system and the identity of it

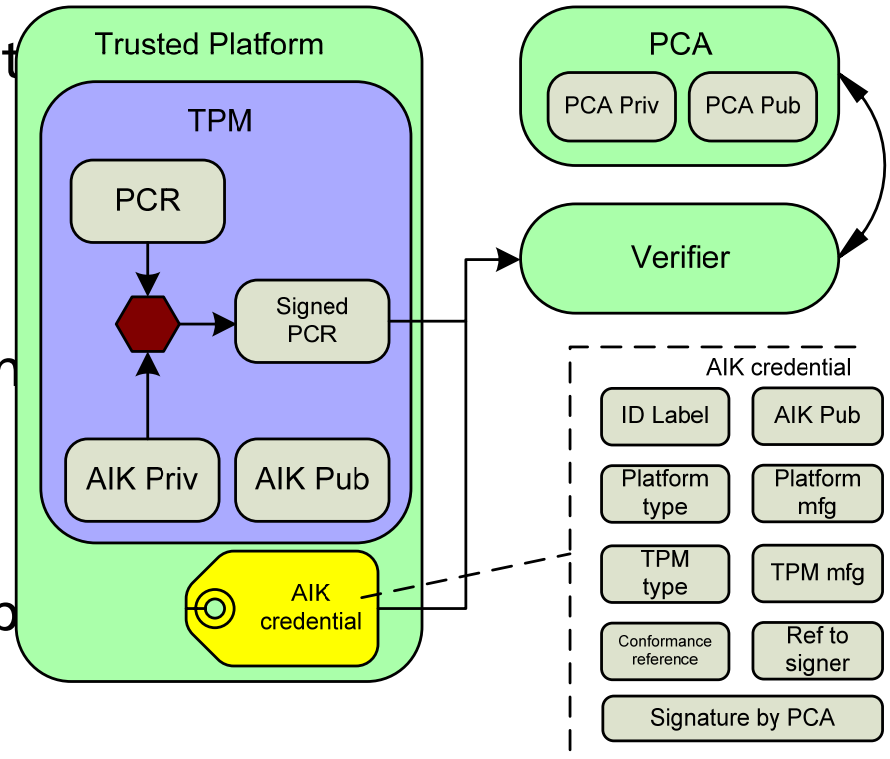
Trusted Computing Essentials

- The Trusted Computing Group defines a set of services as the base for Trusted Computing
  - Trusted Platform Module (TPM)
  - Adding protocols and messages that take advantage of the TPM
- The TPM cannot be moved. It is attached to the platform
- The TPM contains
  - cryptographic engine
  - protected storage
- Functions and storage are isolated



Attestation and pseudonymity

- Trusted Boot
  Measurement of the initial device stat
  and confirmes untemperness of the
  underlying system
- Attestation Process
  Offers a third party evidence about th
  actual system state
- Attestation Identity Keys
  Revealing the identity of the system b
  in the context of the attestation
  process and are produced by the
  Privacy CA (PCA)

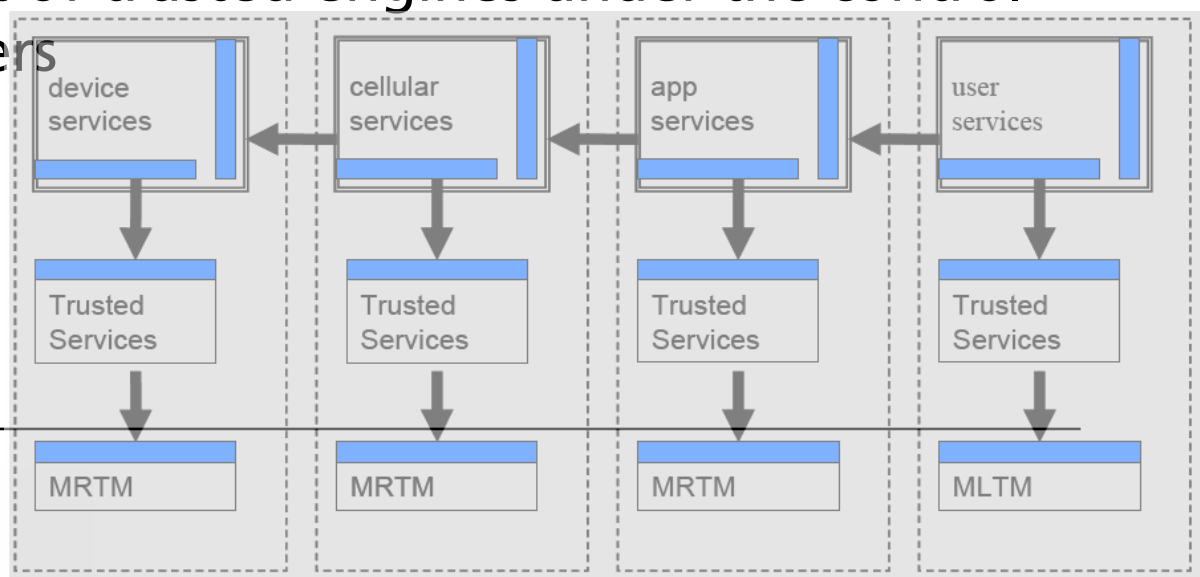


Trusted Computing enables anonymity

- Privacy CA scheme only offers pseudonomy as all credentials are produced to the third party
- Zero knowledge proofs offer a potent solution
- Direct Anonymous Attestation
- Derived from IBM‘s IDEMIX system

Trusted Computing in the mobile domain

- TCG has established a special Mobile Phone Working Group (MPWG), led by Nokia
- This resulted in the specification of the Mobile Trusted Module, a specialised implementation of the TPM concepts for the mobile domain
- Establishes the concept of trusted engines under the control of different stakeholders



Using AIKs as rating ticket

The basic idea is to establish a pseudonymous rating system using the identities embodied in the PCA-certified AIKs.

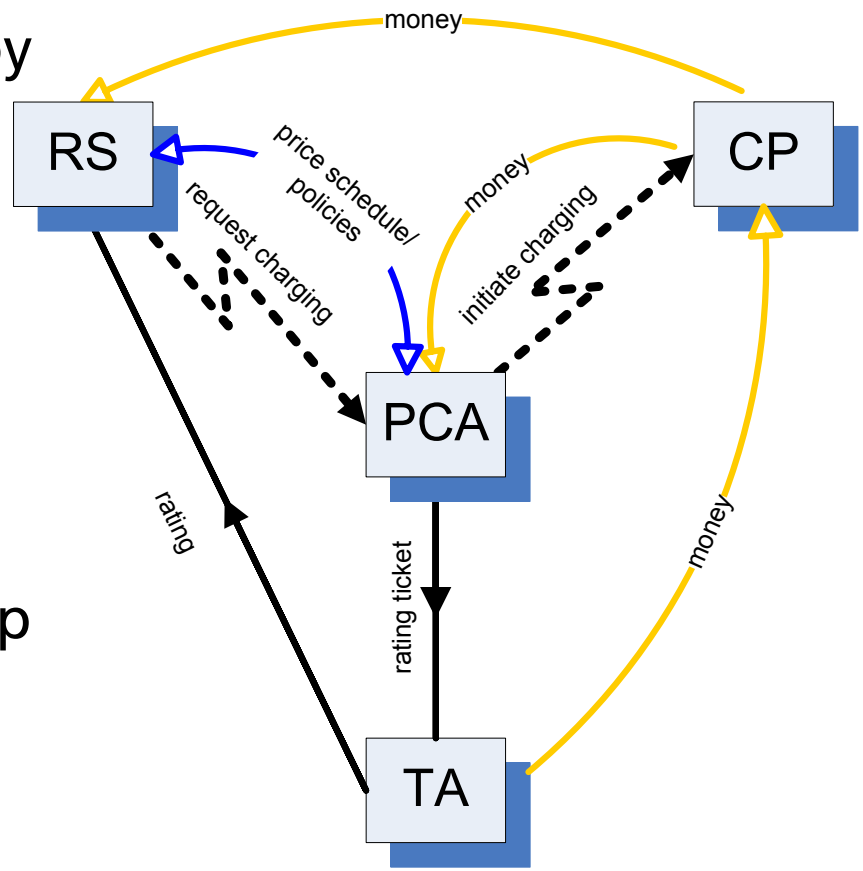
For security considerations the TPM restricts the usage of AIKs. It is not possible to use AIKs as signing keys for arbitrary data.

It is therefore necessary to employ an indirection using a TPM generated signing key and certify this key by signing it with an AIK — viz certify it in the parlance of the TCG.

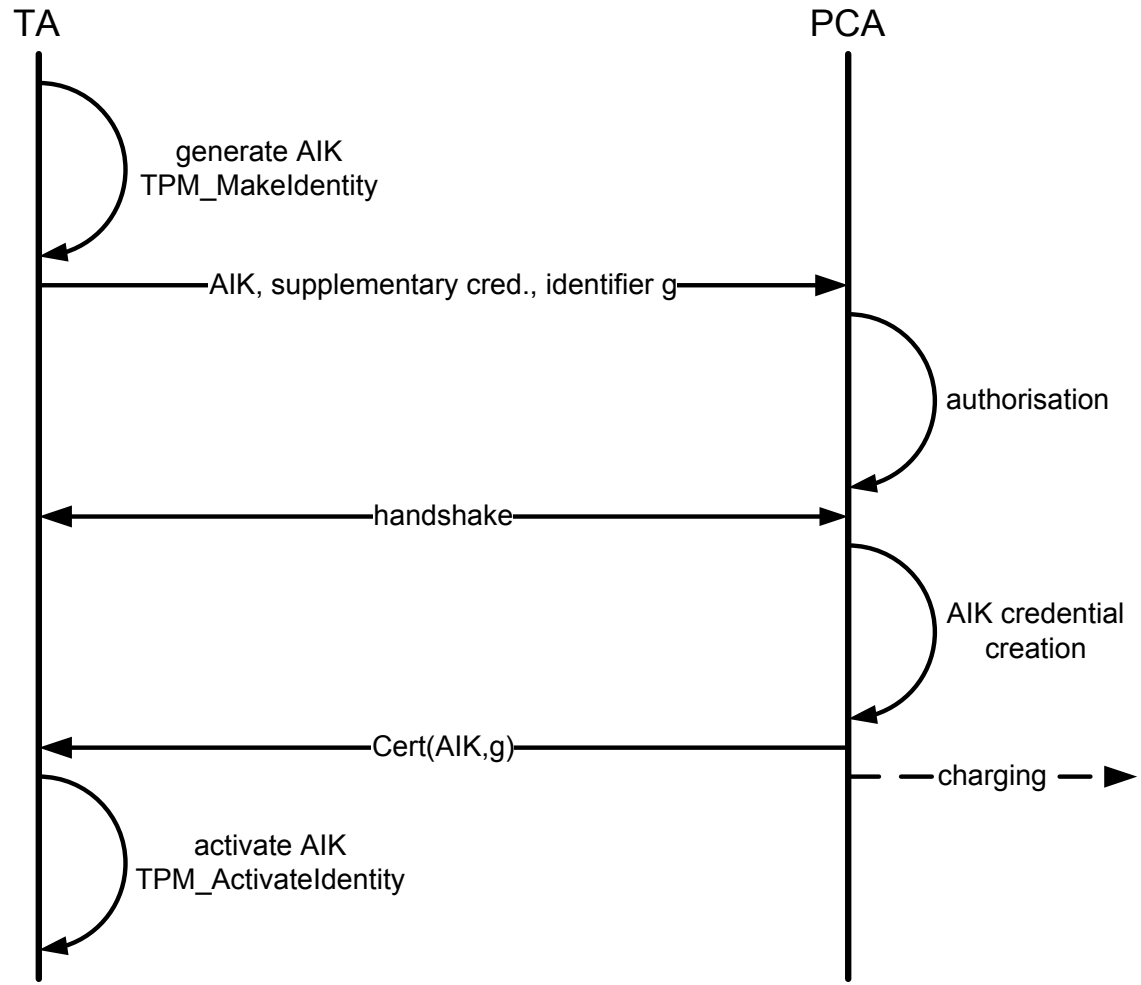
➔Creating a Certified Signing Key (CSK)

Ticket acquisition and rating process

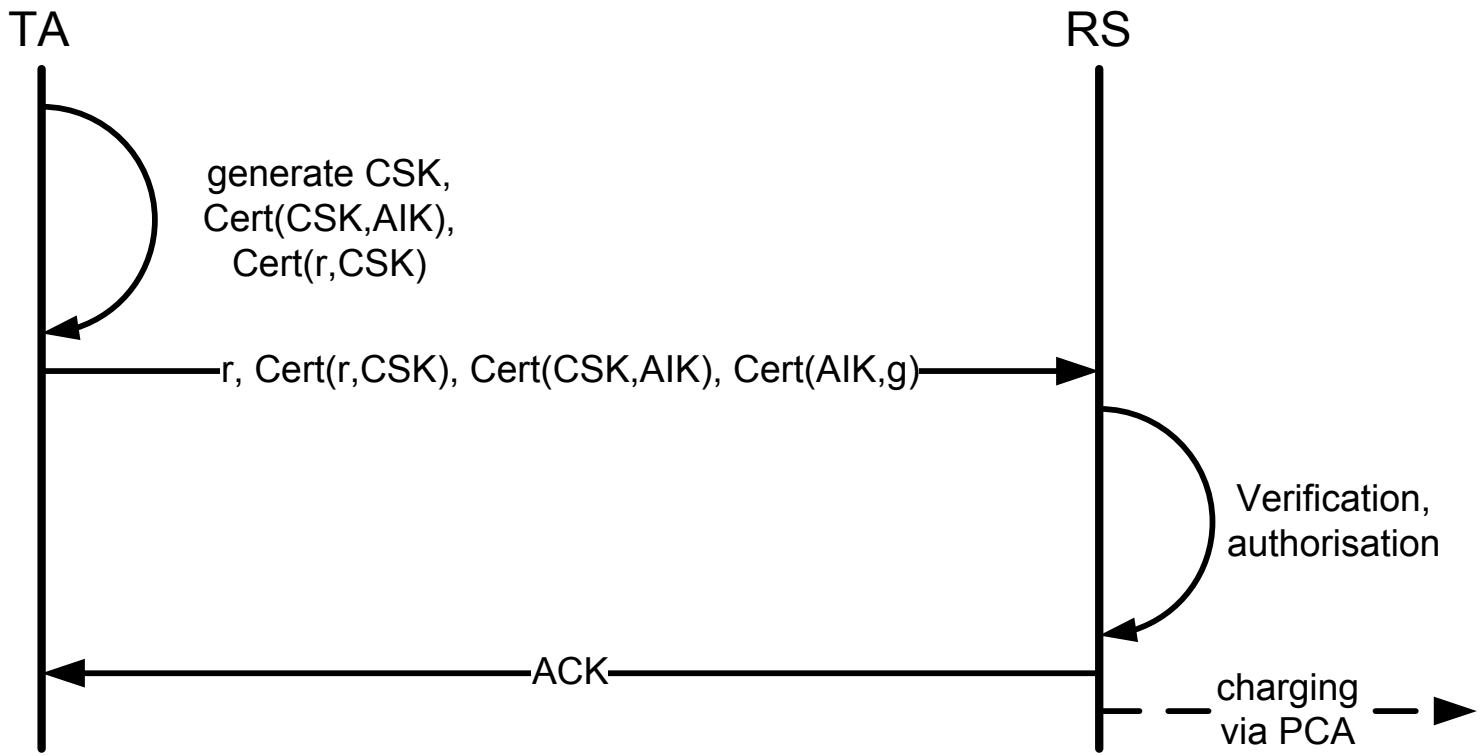
- *Rating Tickets* (RT) are acquired by the *Trusted Agent* from the PCA
- They are redeemed at the *Reputation System*
- A *Charging Provider* occurs as a third party
- Issued RTs are considered as group credentials identifying a price or value, a single device or user



Ticket acquisition process



Ticket redemption process

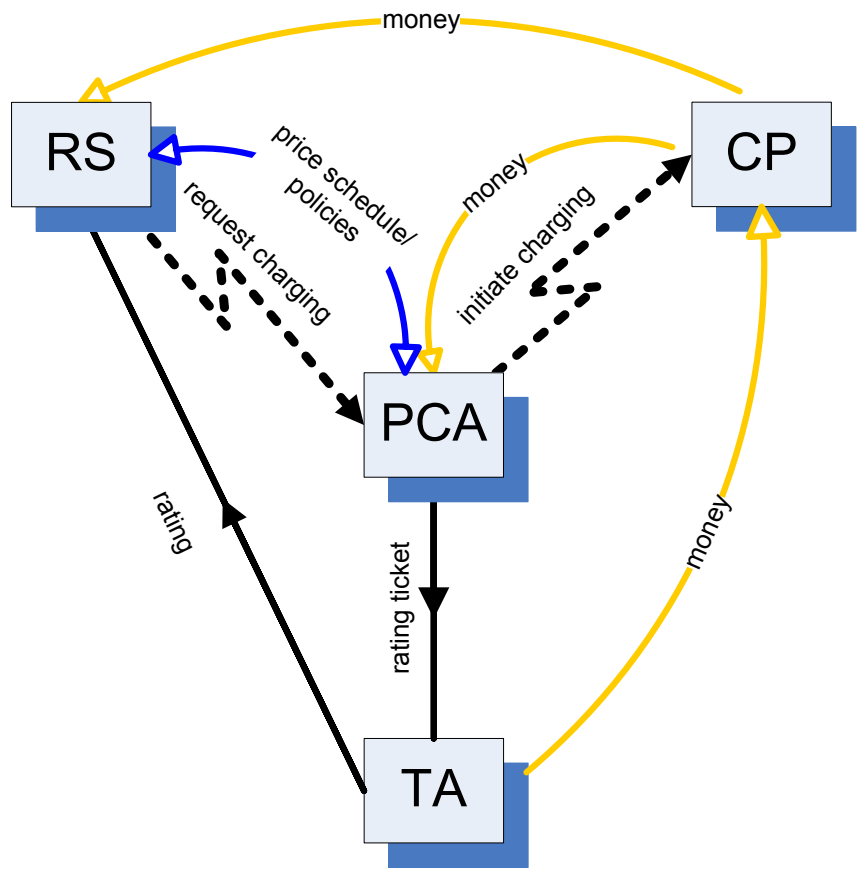


Security and anonymity

- Only PCA can de-anonymise users
- concept relies only on genuine TPM functionality and avoids the usage of trusted software
- Data used in the attestation process can be used to de-anonymise a user
- Since no trust can be laid in the TA for rating ticket management, some kind of double, or multiple, spending protection or usage authorisation is needed at RS upon ticket redemption

Application scenario

- TA likes to express a rating about a user or product
- He buys a rating ticket from the PCA which belongs to a certain group
- TA sends rating to RS
- TA pays to CP at time of redemption
- CP distributes revenue shares between CP, RS, and PCA
- PCA plays a central role to control the identities of the users
- Can be used to model an IDM system



Conclusion and further research

- Base for a generic pseudonymous ticket system
- TA could also express values of tickets by using different (groups of) CSKs
  - In this way ratings could be prioritised
- Support of user side payment scenarios
  - This would require trusted software
- This prsented approach is a very basic ticket system with strong pseudonymity using only basic TPM functionality

Contact

Fraunhofer-Institut SIT
Department „security in mobile systems“

Nicolai Kuntze
Dipl.-Inform.

Rheinstraße 75
D-64295 Darmstadt

Telefon: +49-6151-869-276
Fax: +49-6151-869-224

E-Mail: nicolai.kuntze@sit.fraunhofer.de
Internet: http://www.sit.fraunhofer.de