Trusted Ticket Systems and Applications

Trusted Ticket Systems and Applications

A new security approach for tickets

Nicolai Kuntze and Andreas U. Schmidt

Fraunhofer SIT
Institut
Sichere Informations-
Technologie

Outline

Basics of Trusted Computing

Trusted Ticket System

Ticket application scenarios

Conclusion

Fraunhofer SIT Institut Sichere Informations-Technologie

Ticket Systems

Concept which is at the heart of Identity Management

User receives token which facilitate the user to do something

Systems relying on tickets:

- Kerberos
- Liberty / SAML
- Shibboleth

Trusted Computing – What is trust?

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

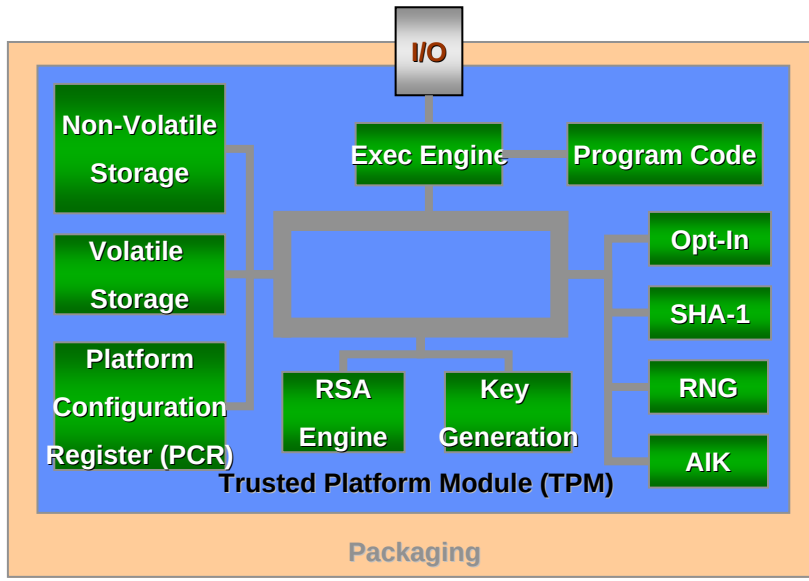
The Trusted Computing Group defines a set of services as the base for Trusted Computing

- 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



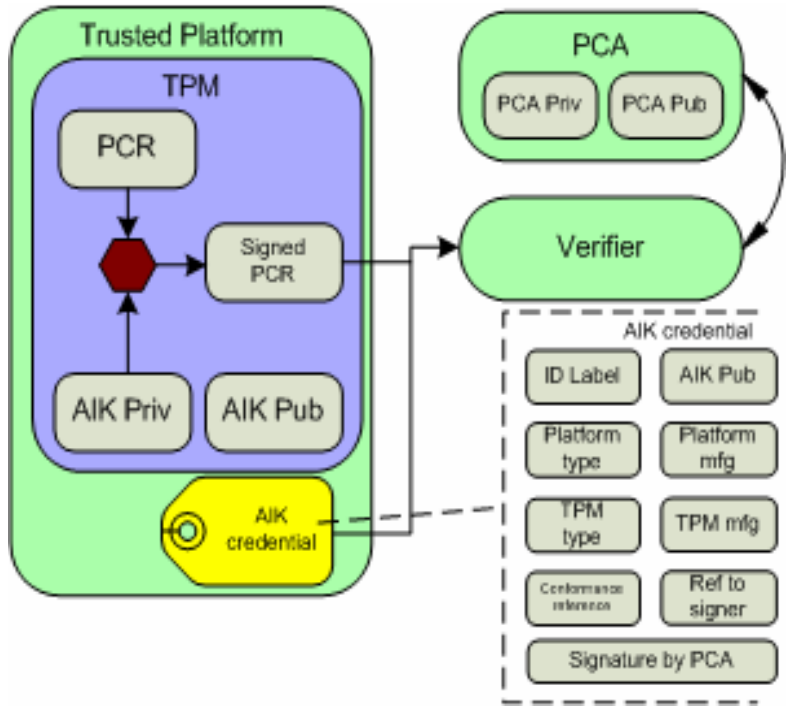
Fraunhofer SIT Institut Sichere Informations-Technologie

Trusted Computing – Remote Attestation

Trusted Boot
Measurement of the initial device state and confirms integrity of the underlying system

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

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



Fraunhofer SIT Institut Sichere Informations-Technologie

Tickets and Trusted Computing

- The basic idea is to establish a (pseudonymous) ticket system using the identities embodied in the PCA-certied AIKs.

- Specific about our design is the tickets are generated locally on the (mobile) device of the user.

- Ticket acquisition an redemption rests solely on trusted computing methods implemented in the TPM chip embedded in the users platform.

- We first describe how AIKs can be turned into tickets that can be used in a ticket-based service accessor identity management architecture, and then develop the processes for their acquisition and redemption.

AIKs as tickets

- 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.

- TPM_CMK_CreateKey returns an asymmetric key pair where the private portion is encrypted by the TPM for use within the TPM only.

- TPM_CertifyKey certyifies the key.

- This indirection creates to each AIK a certified key that can be used for signing data.

➔ certified signing key (CSK).

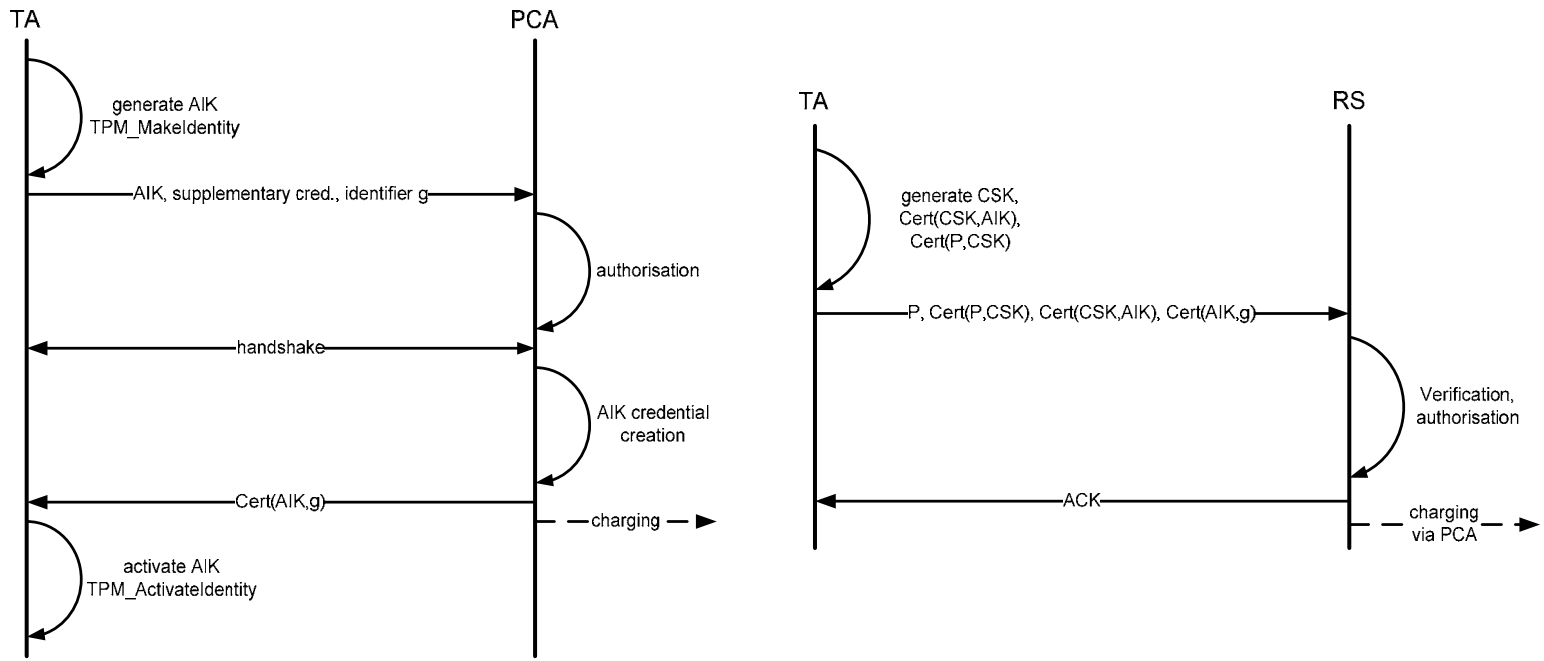
➔ CSK, AIK, together with a certificate by the PCA attesting the validity of that AIK, are the ingredients that realize a ticket for a single operation, e.g., a service access.

Certifying a key says that…

- This key is held in a TPM-shielded location.
- It will never be revealed.

For this statement to have veracity, a challenger or verifier must trust the policies used by the entity that issued the identity and the maintenance policy of the TPM manufacturer.

Ticket acquisition and redemption



Fraunhofer SIT Institut Sichere Informations-Technologie

Generic architecture 1/2

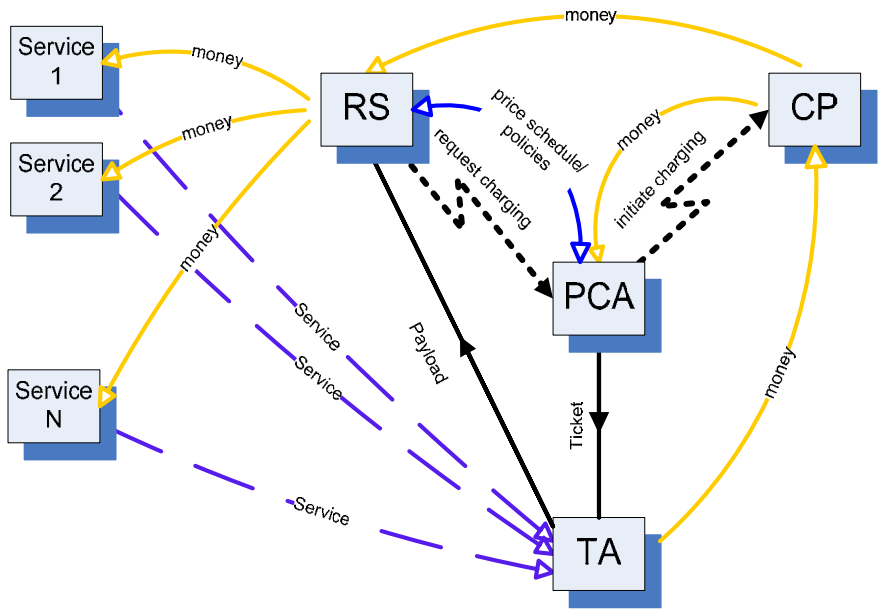
The embedding of the described ticket acquisition and redemption into an application system and business context offers many variants.

Ticket belongs to a certain group

User issues a service request as payload in the ticket redemption toward RS

TA pays for the ticket at the CP at the time of redemption

CP distributes revenue shares between himself, PCA, and RS

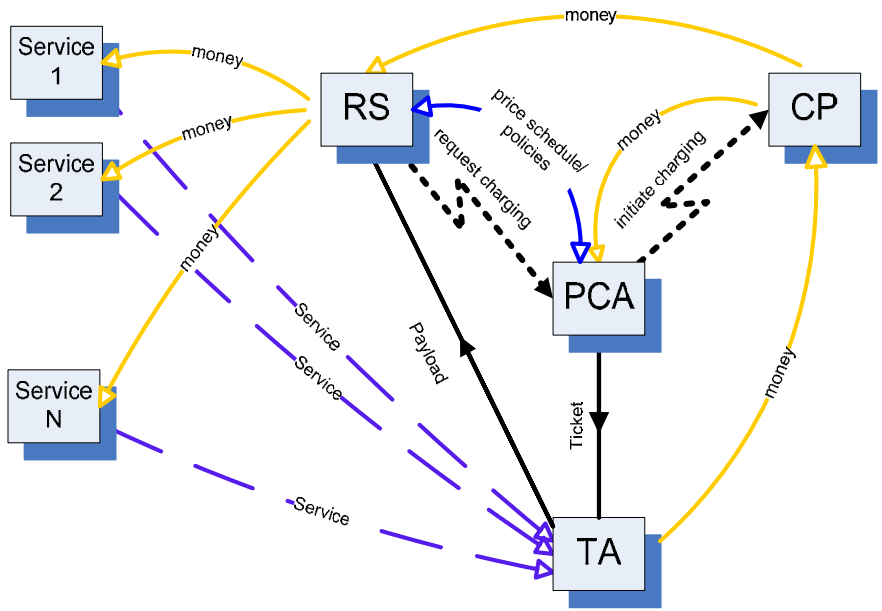


Fraunhofer SIT Institut Sichere Informations-Technologie

Generic architecture 2/2

This realises an access control scheme to multiple services mediated by PCA and RS, yielding three essential benefits:

1. **non-repudiation** by the chain of credentials,
2. **accountability** by resolution of the TA's identity through PCA,
3. **pseudonymity** by separation of duties. The PCA/RS combination plays



Fraunhofer Institut Sichere Informations-Technologie

Price Scheduling in Pseudonymous Rating Systems

Electronic market places for physical and information goods are increasingly occupied by self-organising communities

A common approach is to let market players themselves provide the necessary guidance by issuing recommendations

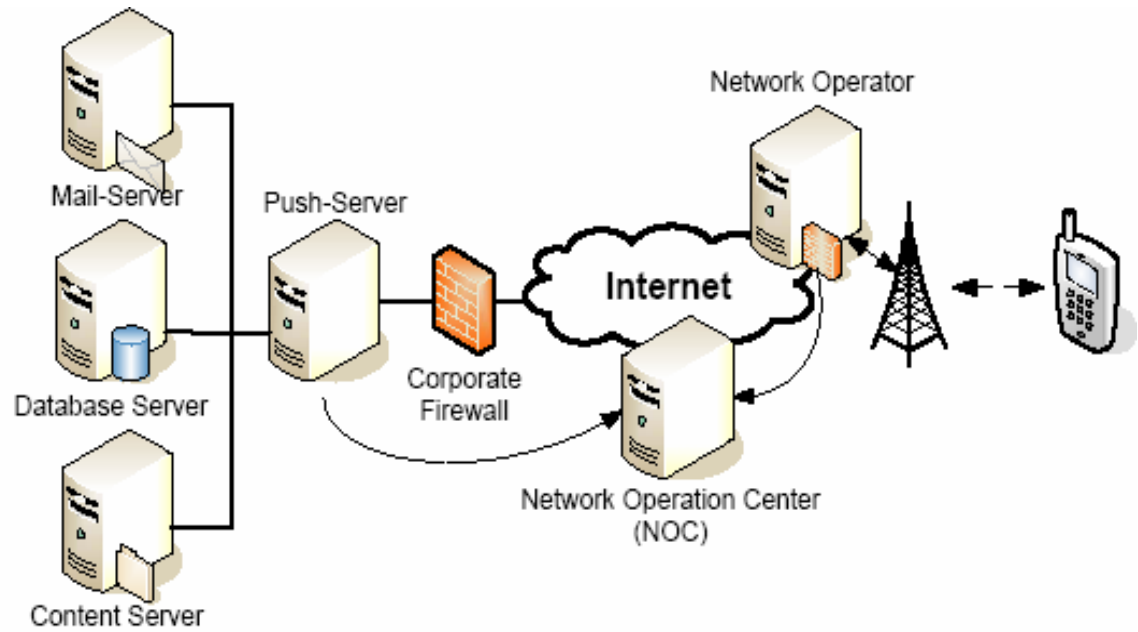
➔ The goal is to establish a homogeneous market for honest participants.

General problem lies within the `cheapness' of pseudonyms in marketplaces and reputation systems, since with name changes dishonest players easily shed negative reputation

Reputation systems could be based on pseudonyms which allow for a fexible forward pricing using the separation of duties between PCA and RS in our ticket system

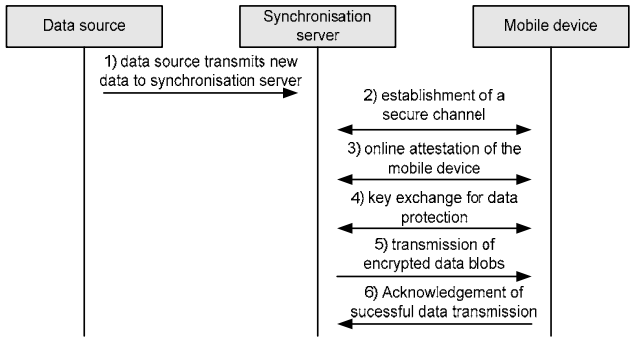
The result would be a rating statement about another participant of the rating system which is **trustworthy**, **accountable**, but protected as a **pseudonym**. This offers **accountability** of users, i.e., the possibility to trace back malicious ones and threaten them with consequences.

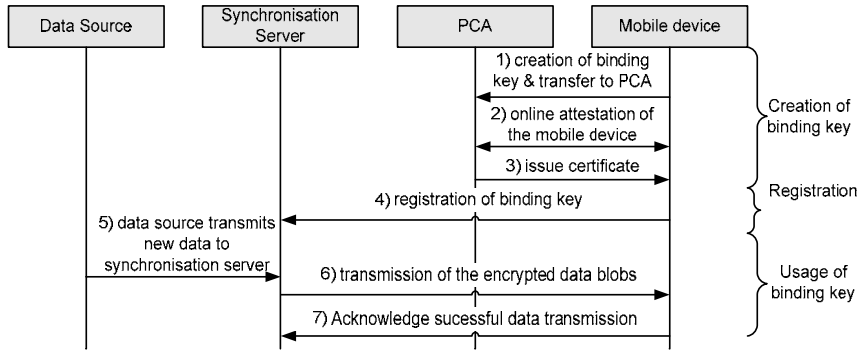
Content Protection for Push Services 1/2



Fraunhofer SIT Institut Sichere Informations-Technologie

Content Protection for Push Services 2/2





Two basic possibilities

- Sealing of blobs
- Binding of keys

Fraunhofer SIT Institut Sichere Informations-Technologie

Conclusion

- The presented method for the management of tickets provides for perfect pseudonymity of the participants toward the system.

- In fact, only PCA is able to de-anonymise users.