# Trusted Computing: Introduction & Applications

## Lecture 7: Trust in Identity Management Systems

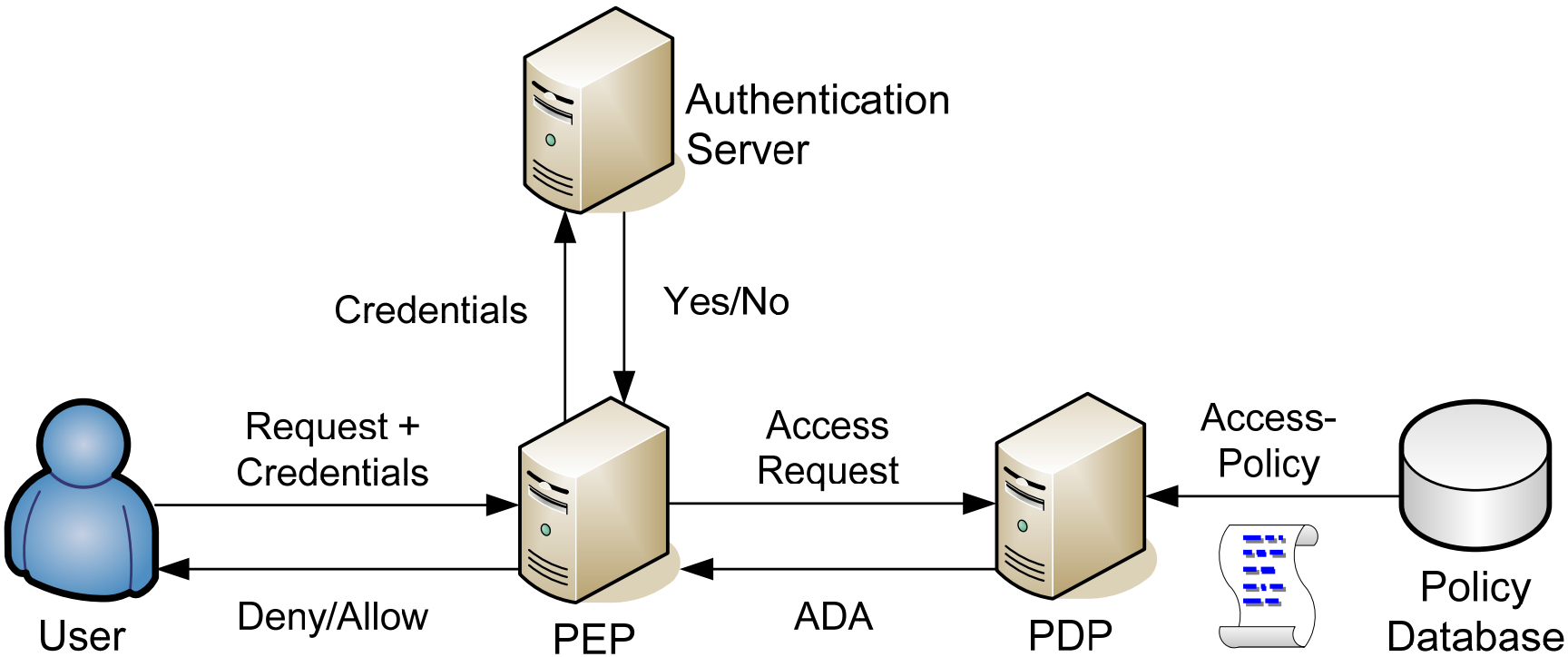

Dr. Andreas U. Schmidt

Fraunhofer Institute for Secure Information Technology SIT,
Darmstadt, Germany

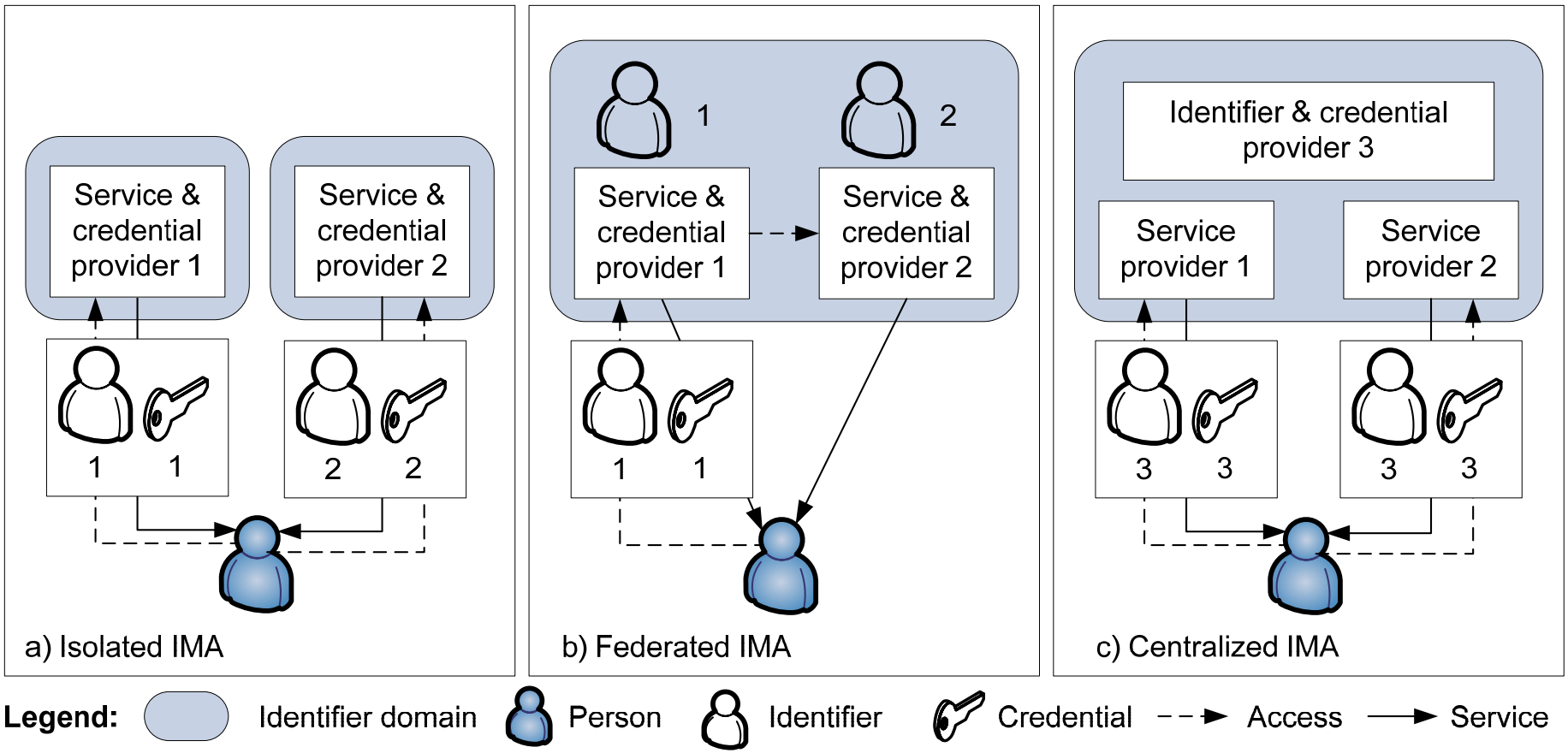
# Literature


1. B. Fichtinger. Trusted Infrastructures for Identities. Diplomarbeit, FH Hagenberg, May 2007
2. AUS & N. Kuntze: Trusted Ticket Systems and Applications. In: New Approaches for Security, Privacy, and Trust in Complex Systems. International Federation for Information Processing, Vol 232, pp. 49-60, Springer, Boston, 2007. Proceedings of the IFIP sec2007. Sandton, South Africa 14-16 May 2007 http://andreas.schmidt.novalyst.de/docs/TC_Ticket_systems.pdf

# Authentication & Authorisation in IdM Architectures



# Identity Management Architectures

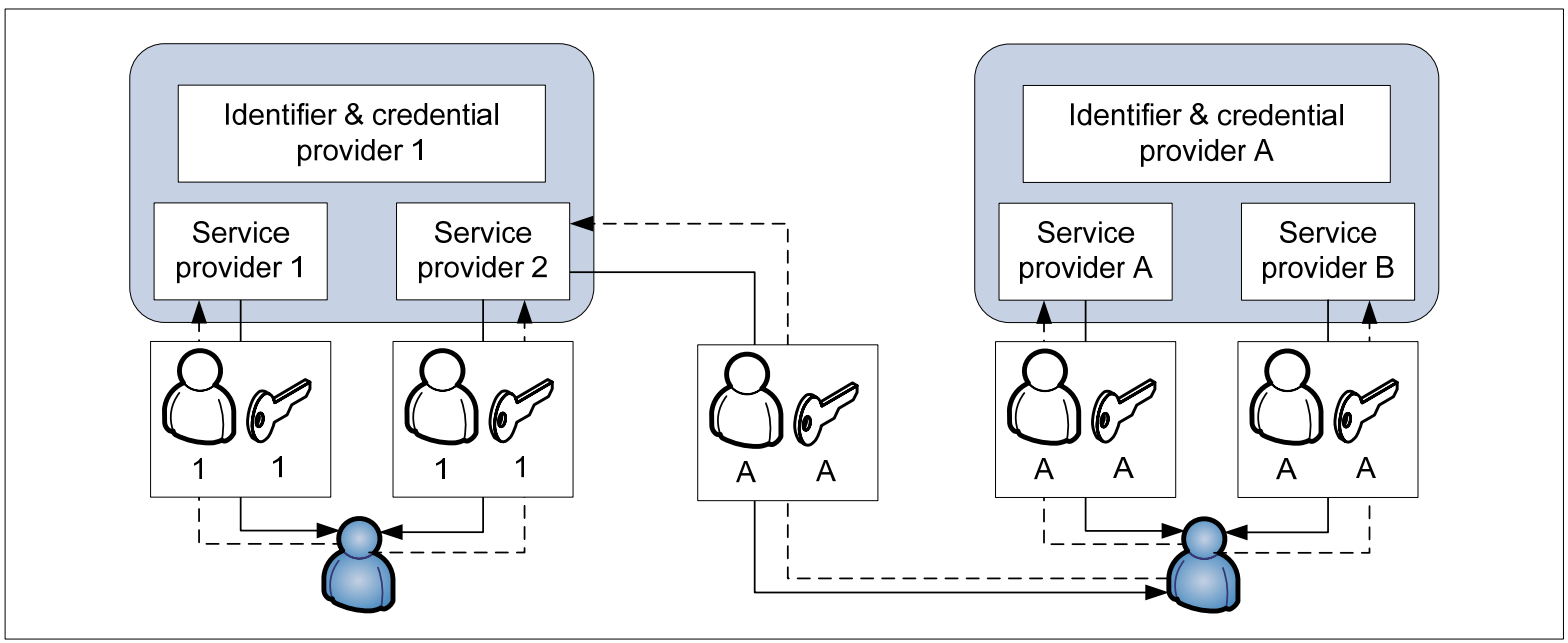


# Problems of conventional IdM

- Mutual trust between identifier domains is hard to establish
  - Traditionally based on existing relationships, e.g. SLAs, or regulated domains, e.g. in e-government
  - Mutual acceptance of credentials for service access must be maintained technically on both sides
  - Problem persists regardless wether a centralised or federated IMA is used
- Conventional technology
  - PKI-based environments,
  - cross certification
  - Spanning CA
- Shortcomings
  - Technical overhead
  - Does not scale for many Id domains

# Principal requirements

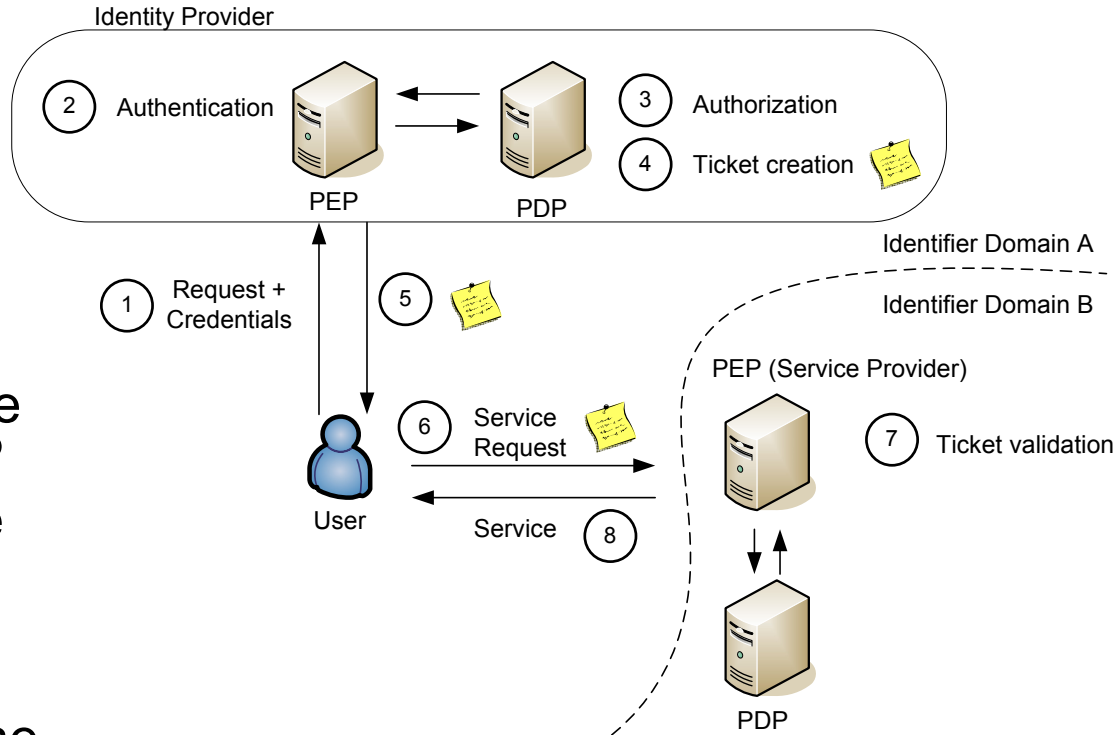
- User from ID A wants to use a ticket (credential) at SP 2
- Requires
  - Id and credntial provider is authorised to issue credentials for the target domain
  - At the moment of issuing the ticket, the Id provider is trustworthy (e.g. adheres to issuance policies, establishes double-spending protection etc.)
- Idea: use TC to prove fulfillment of these requirements



# Basic scenario

- User acquires a ticket from IdP in dom A to use it in B

1. User authentication consisting of request and presentation of the credentials at the PEP
2. PEP authenticates the user possibly with the help of an authentication server
3. After authentication, the PDP is responsible for the authorization decision according to a predefined policy
4. ticket for the user is created
5. ticket is sent back to the user via the PEP



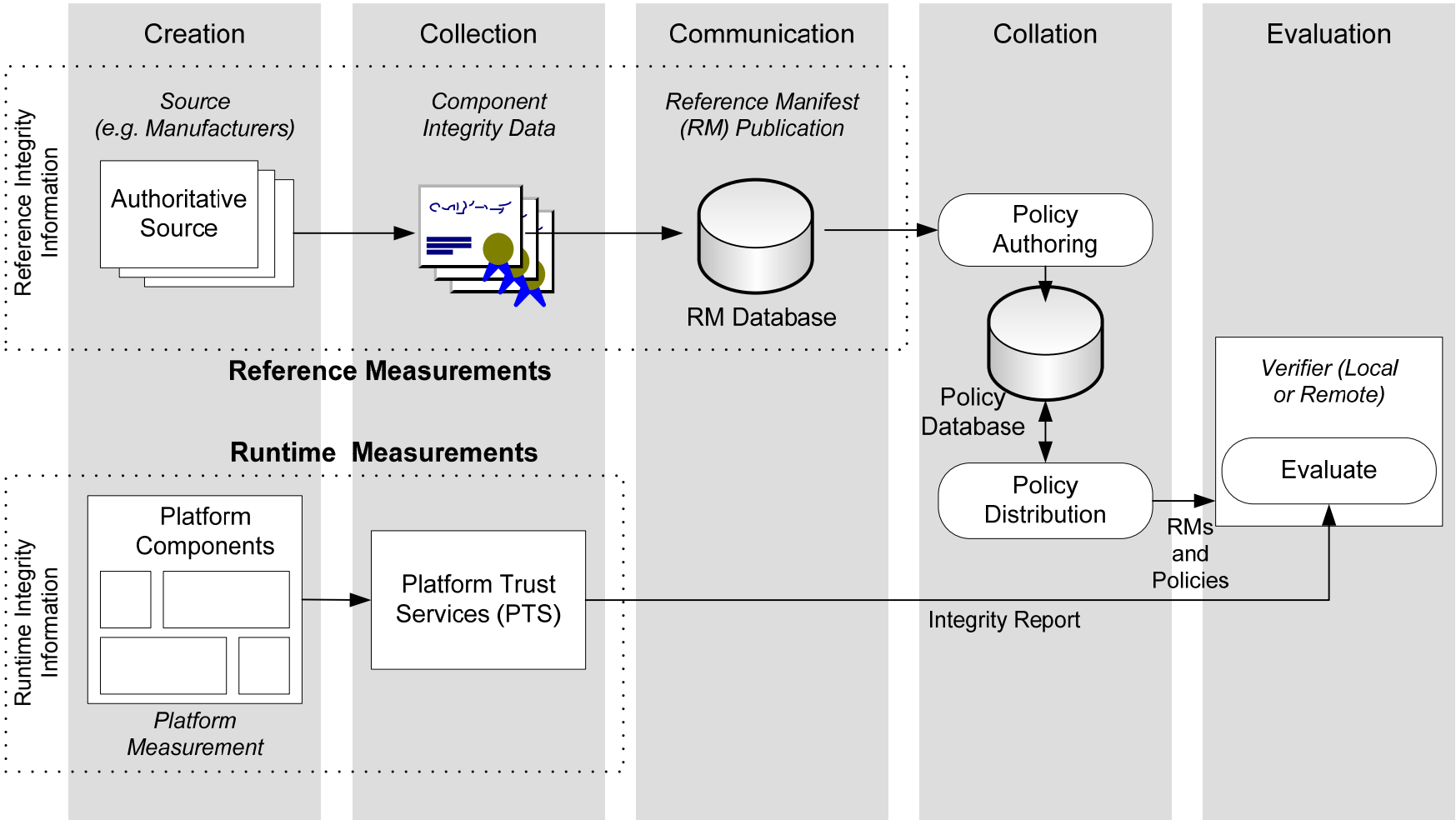

6. ticket presented by the user to the service provider in Dom B
7. PEP validates the ticket with the help of a PDP and the predefined policy in order to decide whether or not the desired service can be granted.
8. the user is granted access to the service or not

# Integrity measurements

Review TCG Infrastructure WG concepts

- Measurement values collected at runtime/loadtime by RTM/OS are compared with
- Reference measurements describing the desired state
- Component-based approach
  - authoritative sources (e.g. the manufacturers) are responsible for the creation of **reference measurements**.
  - They collect and process (usually in XML format) the component integrity data and
  - publish it in a **Reference Manifest** (RM) database
- Relevant integrity data for a target platform is gathered (**collation**)
- In the **evaluation phase**, the reference measurements are compared with the runtime and loadtime measurements

# TCG Integrity measurement process

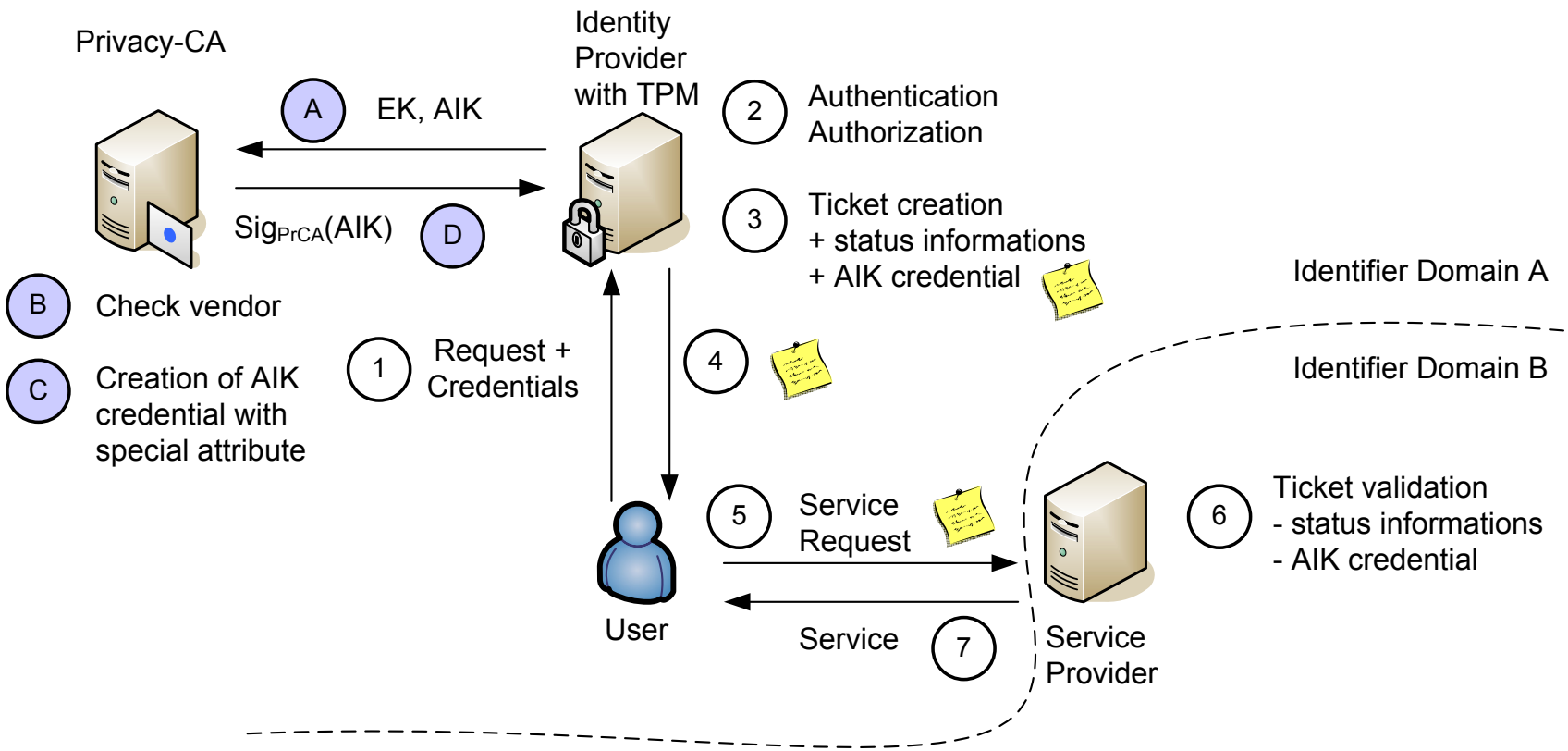


# Authorisation of the IdP

- Two base processes:
  - Ticket acquisition
  - Ticket redemption
- Leverage AIK credentials and privacy CA
  - PCA issues tickets for client TPs based on EK credentials or derived ones (modification of PCA role)
  - Requires that IdPs are built on TPs with TPMs
- Ticket acquisition by issuing IdP involves

A. The identity provider sends a request consisting of EK credential and the public part of the AIK to the PCA.
B. The PCA checks the vendor certificate in the EK credential and decides whether TPMs issued by this vendor are allowed to issue trusted tickets.
C. In the case of a positive decision, the PCA issues an AIK credential containing a **special attribute** attesting that the identity provider owning the certificate is authorised to issue trusted tickets
D. Finally, the AIK credential is sent back to the identity provider and can be used during the identity management process

# Basic ticket acquisition and redemption 1/2

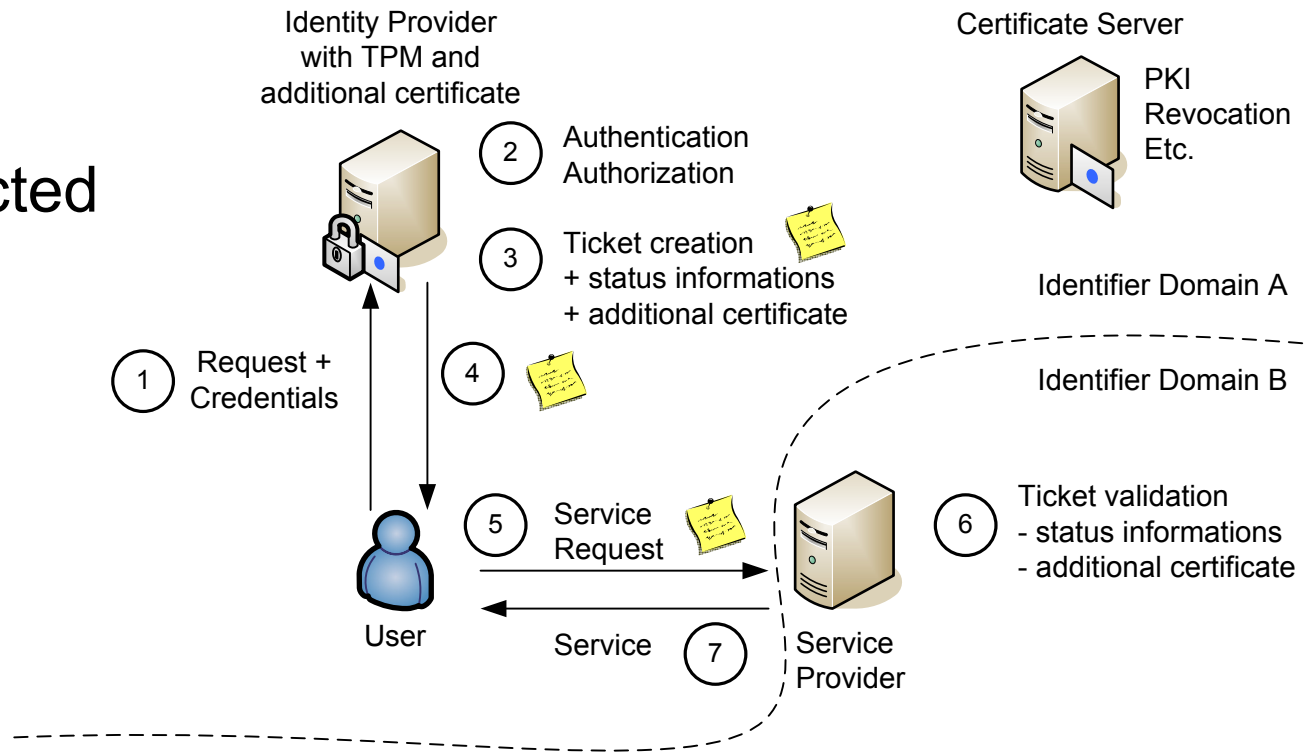


# Basic ticket acquisition and redemption 2/2

- 1. - 2. Request, authentication and authorization.
- 3. In order to embed the authorization information in the ticket, the AIK credential is used. Additionally, the status information describing the trustworthy status of the identity provider has to be included in the ticket.
- 4. The ticket is sent back to the user.
- 5. The user requests a service and includes the issued ticket.
- 6. During the validation of a ticket, the service provider can check whether the AIK credential in the ticket contains the necessary attribute and is issued by a trustworthy privacy-CA. Furthermore, the status of the identity provider during the issuing of the ticket has to be checked.
- 7. The service is either granted or refused.

# Alternative: Additional certificates for ticket issuing IdPs

- TPM of IdP used to deliver status information
- Additional PKI infrastructure to embody the authorisation to issue tickets
- Certificates need to be TPM-protected



# Extra certificate processing

- 1. - 2. Request, authentication and authorization.
- 3. During the ticket creation, status information and the certificate are embedded.
- 4. - 5. The ticket is sent back to the user who requests a service with the help of the ticket.
- 6. The service provider validatea the status information and the additional certificate included in the ticket. In order to validate the ticket, the certificate server which issued the certificate may have to be consulted.
- 7. The service is either granted or refused
- Benefits
  - Independent of TC infrastructure
- Problems
  - Receiver of tickets involved in evaluation of attestation information
  - Additional PKI must be maintained
  - Does not leverage PCA

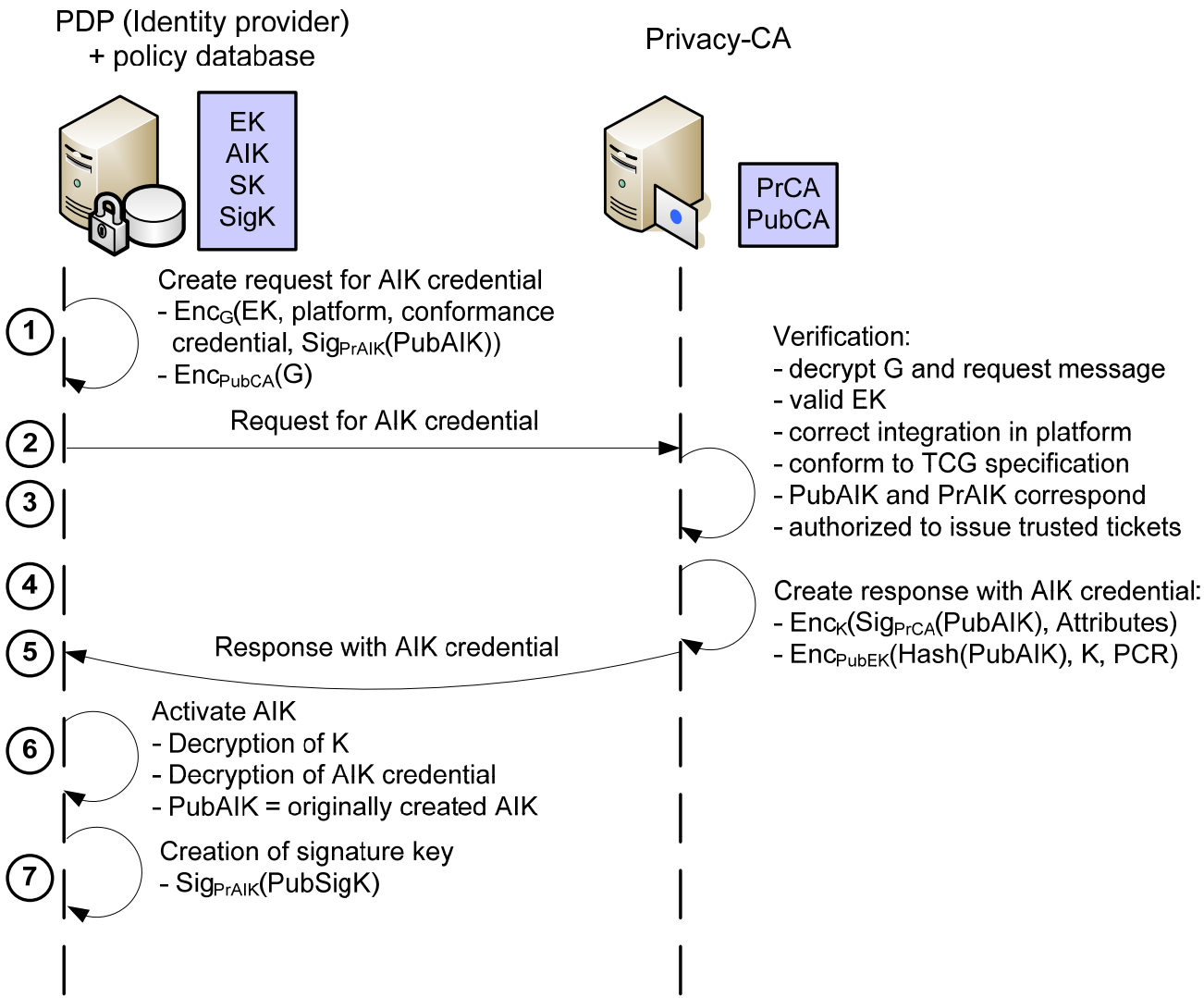
# Identity aspects

- Transitive trust relationship IdPA-user-SPB (IdPB) is established, mediated by PCA
- Access rights must be receiver-agnostic, PCA will not always know which service in Dom B is requested
- Privacy
  - IdPA can stay pseudonymous for receiving SP
  - Accountability maintained since PCA can resolve IdPA‘s identity
  - User privacy cannot be maintained during ticket acquisition
  - But ticket redemption at Dom B service can be pseudonymous
  - Privacy may necessarily be waived to some extent when e.g. accounting tasks are done in Dom B
  - Privacy is strongly use-case dependent, minimal need to know principle can be supported by the architecture

# Identity aspects

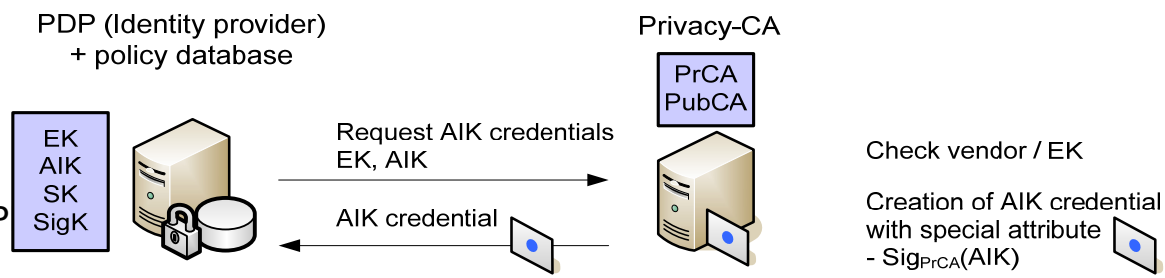
- Authentication remains unchanged
- Authorisation
  - Final decision rests with receiving SP
  - SP may need help from IdP B to evaluate status information and validate tickets
- Non-repudiation
  - Integrity of the tickets to be secured by TPM-based electronic signatures (see later)
  - PCA credentials must not trusted blindly
  - Target service provider cannot be specified in the assertion
  - multi-spending protection is an issue
  - PCA for de-valuation of tickets?
- Confidentiality
  - E2E encryption is not possible since receiver is unknown
  - Parts of ticket‘s data may be encrypted

# AIK Credential creation for IdPA



# AIK credential creation

1. identity provider creates an AIK pair and a request for the AIK credential consisting of the endorsement (includes Pub_EK), platform and conformance credential and of the signature with the private AIK over the public AIK. This request is encrypted with a symmetric key G, which is encrypted with the public key of the privacy-CA and additionally included in the request.
2. The finished request Enc_G(EK,PE,CE cred, Sig_AIK (PubAIK)) and Enc_PubCA(G) is sent to the privacy-CA using a suitable credential management protocol, e.g. CMS for X.509 certs, and XML Key Management Services protocol for XML certs
3. PCA
   - Performs AIK certification request evaluation
   - Evaluates authorisation of IdP to issue tickets, eg. Using Pub_EK, or (one of the) certs
4. PCA creates response
   - Creates AIK cert
   - Adds ticket authority information
   - Encrypts using newly generated key K
   - May be bound to PCR values
5. AIK credential Response
6. AIK activation
7. As the AIK cannot be used to encrypt or sign arbitrary messages,
   - an additional signature key is created and attested by the AIK with the help of a signature with the private AIK over the public part of the newly generated signing key.
   - This attestation states that the signing key has been created by a TPM and is being protected by the TP
   - Stored TPM-protected



# Certified Signing Keys (Step 7)

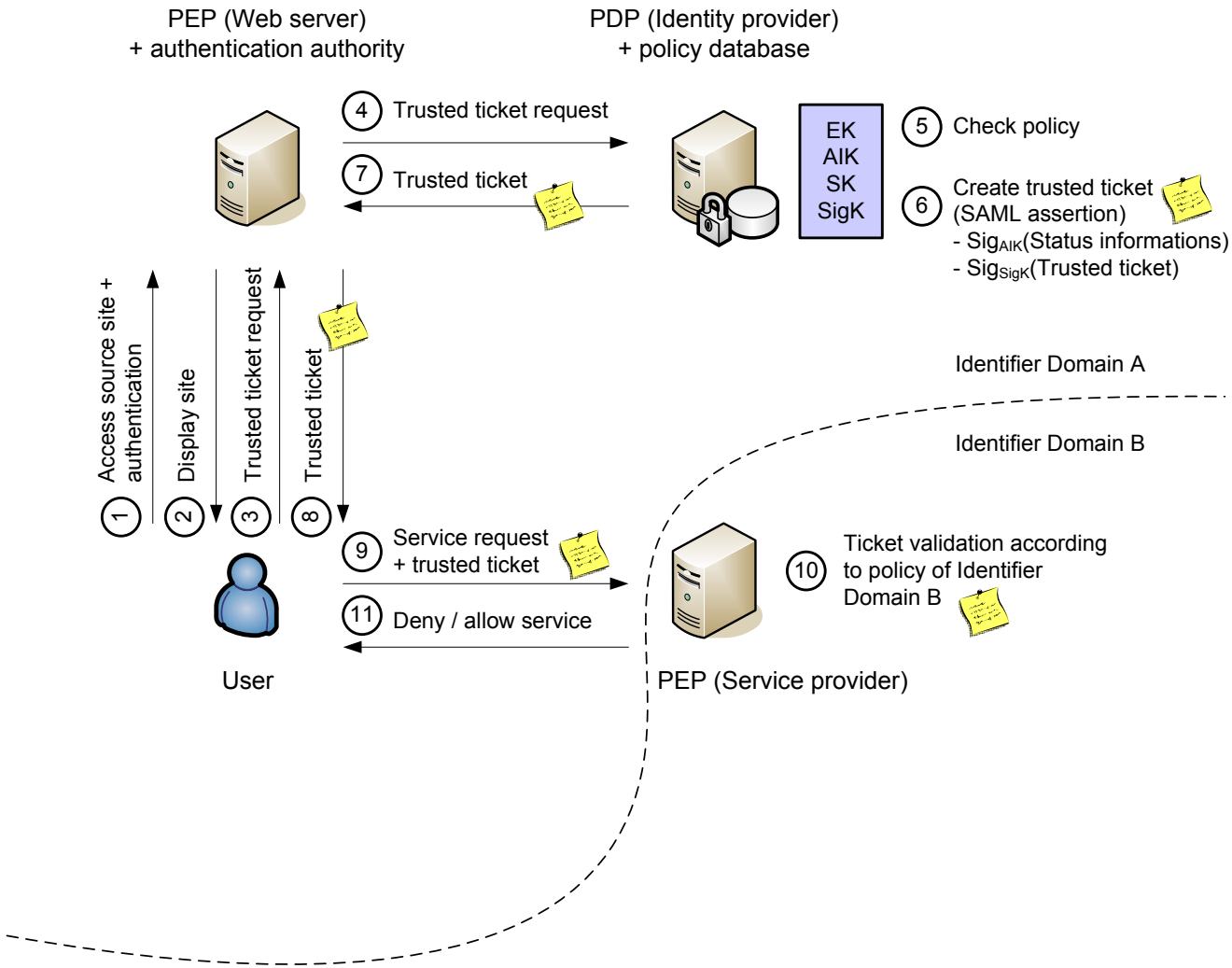
- For security considerations the TPM restricts the usage of AIKs. It is not possible to use AIKs as signing keys for arbitrary data.
- It is therefore necessary to employ an indirection using a TPM generated signing key and certify this key by signing it with an AIK - viz certify it in the parlance 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

- 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.

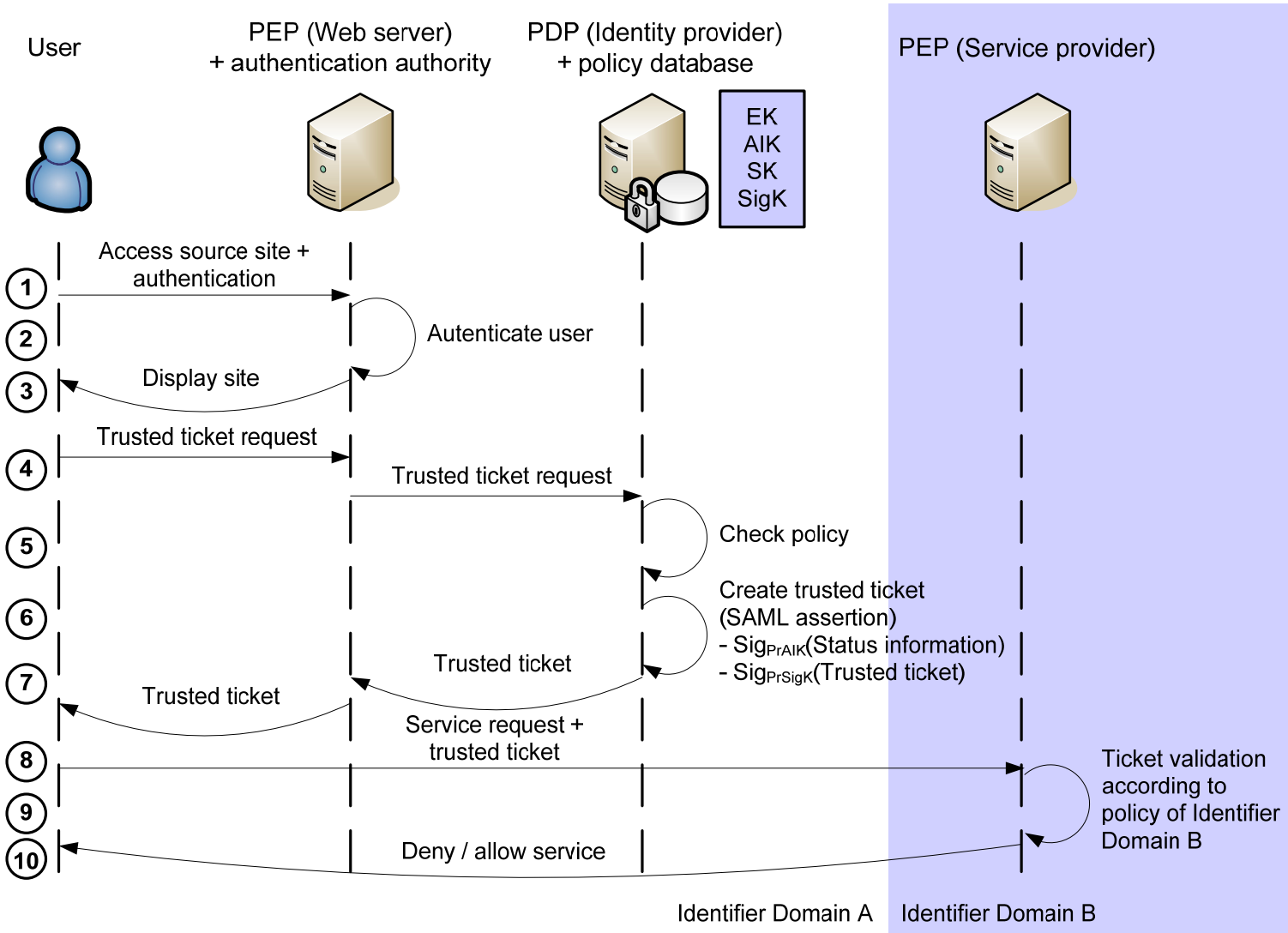
# Requesting and creating trusted tickets 1/3



# Requesting and creating trusted tickets 2/3

- 1. A user accesses a source site at the policy enforcement point (PEP)
- 2.-4. After the successful authentication the web server displays the site for the user, who, can request a trusted ticket for a service provider in identifier domain B. The trusted ticket request is forwarded by the web server to the policy decision point (PDP), the identity provider A.
- 5. In order to decide whether the user is authorized to access the desired service, the policy (stored in the policy database) is checked by the identity provider.
- 6. Next, the trusted ticket, a SAML assertion is created by the identity provider. The ticket has to contain status information about the identity provider which is signed with the identity provider's AIK. Due to integrity issues, the whole ticket has to be signed with the previously created signature key.
- 7.-8. The trusted ticket is forwarded to the user via the web server (Browser/POST profile of SAML)
- 9. Upon receipt of the trusted ticket, the user can request a service from the foreign service provider redeeming the trusted ticket
- 10. - 11. Service provider (PEP) validates the ticket according to the policy of its own identifier domain. Validates authorisation information in the ticket, the signatures and certificates in the ticket. Optionally, the privacy-CA has to be consulted to verify the AIK credentials.

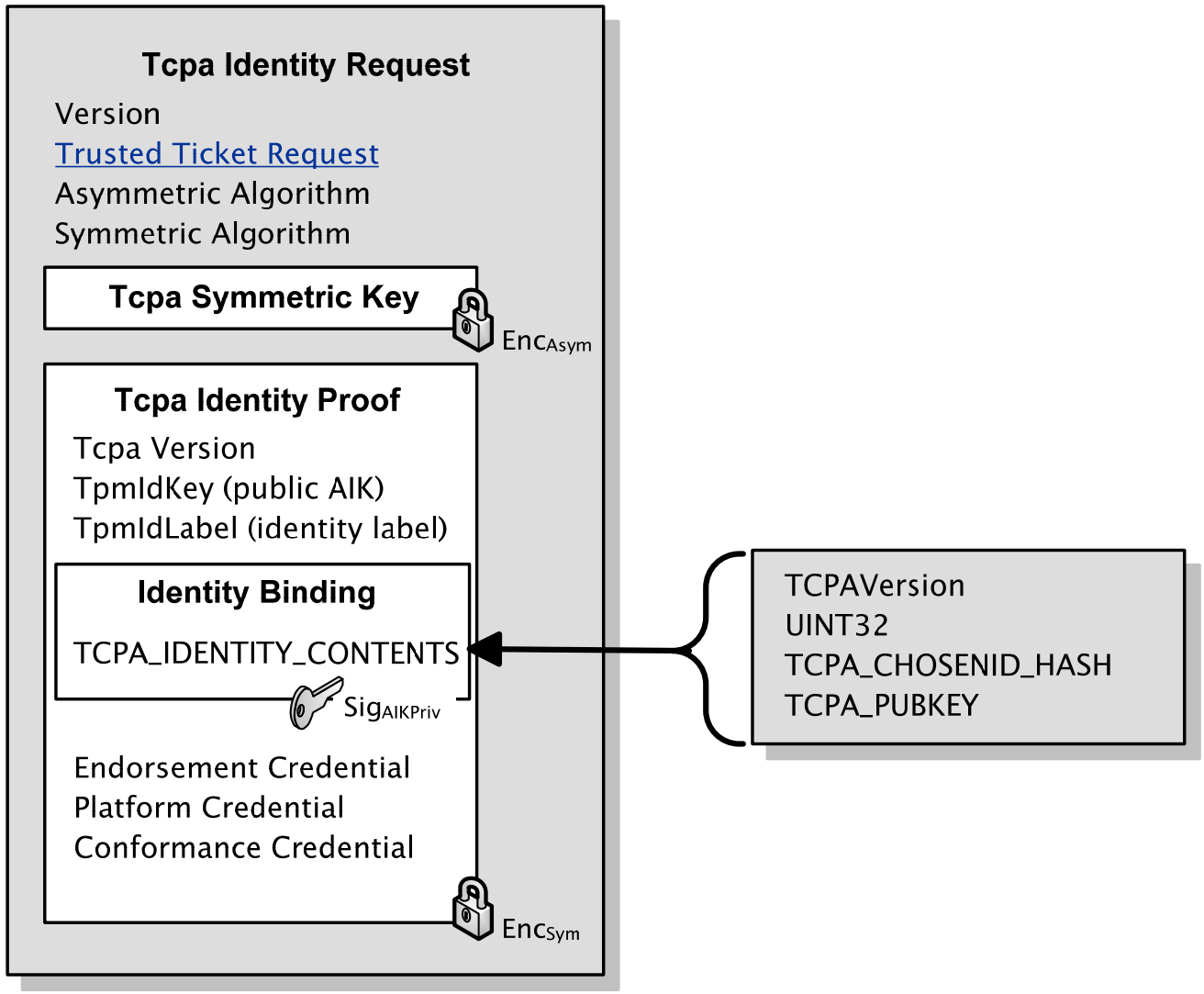
# Requesting and creating trusted tickets 3/3



# AIK credential request

- Tcpa Identity Request message as specified by TCG
- Basic information (version and used asymmetric and symmetric algorithms)
- Message protection: symmetric key asymmetrically encrypted with the public key of the privacy-CA and stored in the Tcpa Symmetric Key field.
- This symmetric key is used to encrypt the content of the Tcpa Identity Proof which consists of version, public AIK, the chosen identity label for the AIK and the endorsement, platform and conformance credentials.
- The identity binding is included in the Tcpa Identity Proof. This identity binding is calculated as the signature value using the private AIK over the data TCPA IDENTITY CONTENTS of the TPM which consists of TCPA version, the ordinal of the MAKE IDENTITY command of the TPM (UINT32), the hash of the concatenation of the chosen identity label, the public key of the privacy-CA (TCPA CHOSENID HASH) and the public AIK (TCPA PUBKEY)
- The request for the authorisation to issue trusted tickets is included as a boolean value in the basic information
  - Does not logically fit into the tight structure of Tcpa Identity Proof.
  - the fact that the identity provider requests the authorisation to issue trusted tickets is not sensitive.

# AIK credential request



# The trusted ticket

- SAML assertion including authentication, attribute and authorisation decision statements
- Authorisation of IdPA is included in attribute statement
- signature with the private AIK over a digest of the PCRs is stored in QuoteValue
- in the EventLog field the SML is transmitted for verification
- AikCredential field stores the AIK credential
- Digital signature according to the XML Digital Signature Standard
- Signing created by TPM and certified with AIK

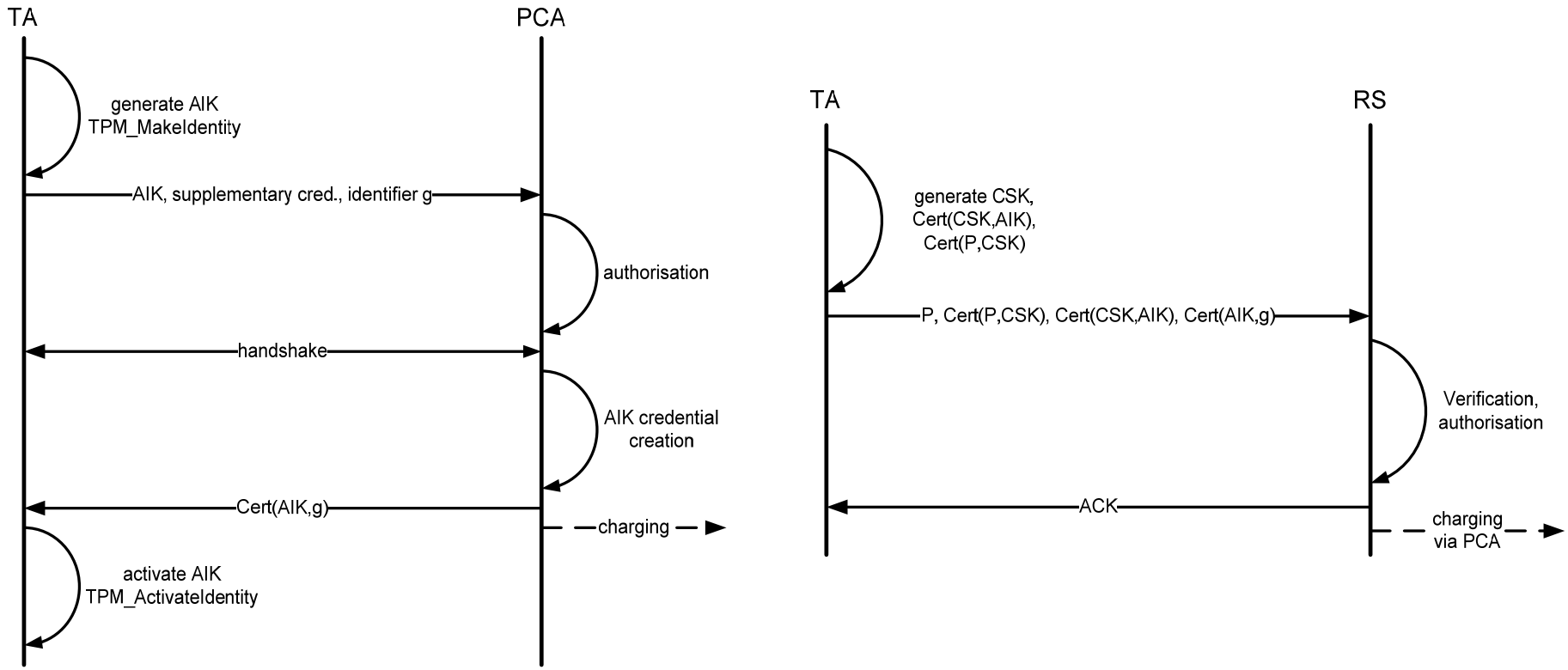
```
<saml:Assertion
  MajorVersion="1"
  MinorVersion="0"
  AssertionID=number
  Issuer="Identity Provider"
  IssueInstant=timestamp>
  <saml:Conditions
    NotBefore=timestamp
    NotOnOrAfter=timestamp />
  <ds:Signature>
    ... DzTJ4vv1xz8QFn ...
  </ds:Signature>
  <saml:AuthenticationStatement
    AuthenticationMethod=method
    AuthenticationInstant=timestamp />
  <saml:AttributeStatement>


  </saml:AttributeStatement>
  <saml:AuthorizationDecisionStatement
    Decision="permit"
    Resource="http://www.x.com/news.jsp">
    <saml:actions />
  </saml:AuthorizationDecisionStatement>
</saml:Assertion>
```

```
<saml:Attribute  AttributeName="QuoteValue"
  AttributeNameSpace="http://www.fh-ooe.at/ns">
  <saml:AttributeValue>
    <QuoteValue>
      <ExternalData>... QFnR ...</ExternalData>
      <Data>... 9gj85 ...</Data>
      <ValidationData> ... VB9gj ...</ValidationData>
    </QuoteValue>
  </saml:AttributeValue>
</saml:Attribute>
<saml:Attribute  AttributeName="EventLog"
  AttributeNameSpace="http://www.fh-ooe.at/ns">
  <saml:AttributeValue>
    <EventLog>
      <Pcr index=1>
        <PcrEvent  index=0>
          <TcTssVersion>x.x.x.x</TcTssVersion>
          <PcrIndex>1</PcrIndex>
          <EventType>12245</EventType>
          <PcrValue> ... E4D2J ... </PcrValue>
          <Event> ... 2J5TY ... </Event>
        </PcrEvent>
        <PcrEvent index=1> ... </PcrEvent>
      </Pcr>
      <Pcr index=2> ... </Pcr>
    </EventLog>
  </saml:AttributeValue>
</saml:Attribute>
<saml:Attribute AttributeName="AikCredential"
  AttributeNameSpace="http://www.w3.org/2000/09/xmldsig#">
  <saml:AttributeValue>
    <X509Certificate>... zTJ5QFnR ...</X509Certificate>
  </saml:AttributeValue>
</saml:Attribute>
```

# Ticket acquisition and redemption isolated

Ticket generation via PCA and redemption at service may be isolated in a Architecturecentred on the PCA-client trust relationship

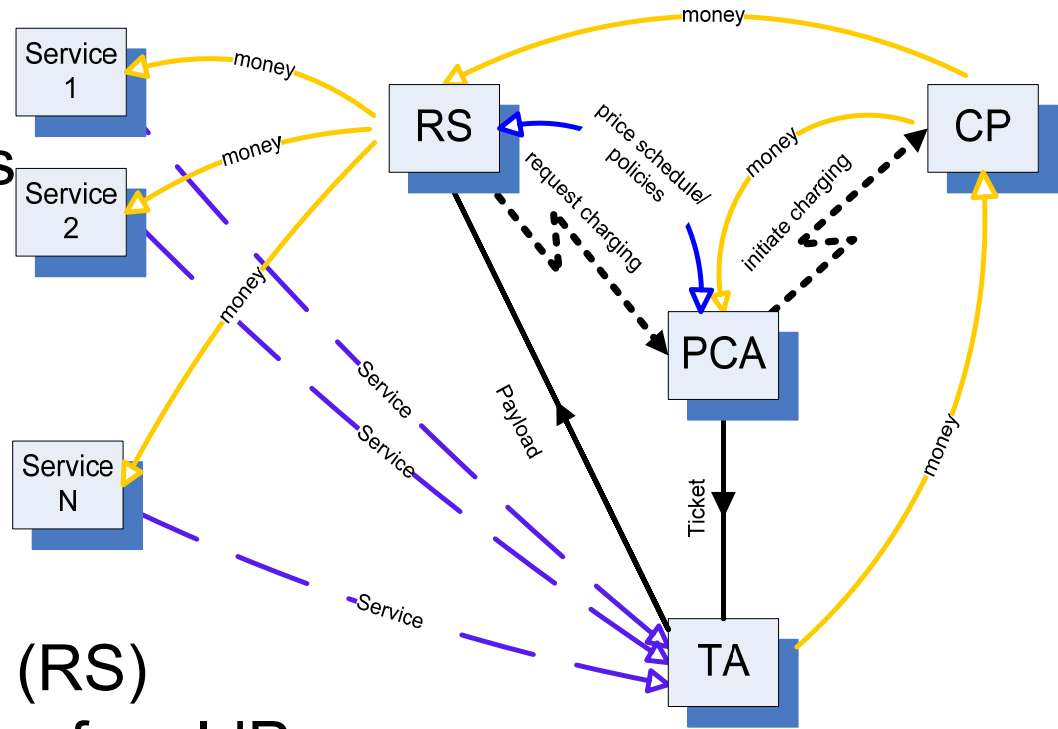


# Trusted ticket system with enhanced PCA

- 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/Receiving System (RS) combination plays the role of an IdP



# Application: Price scheduling for 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.