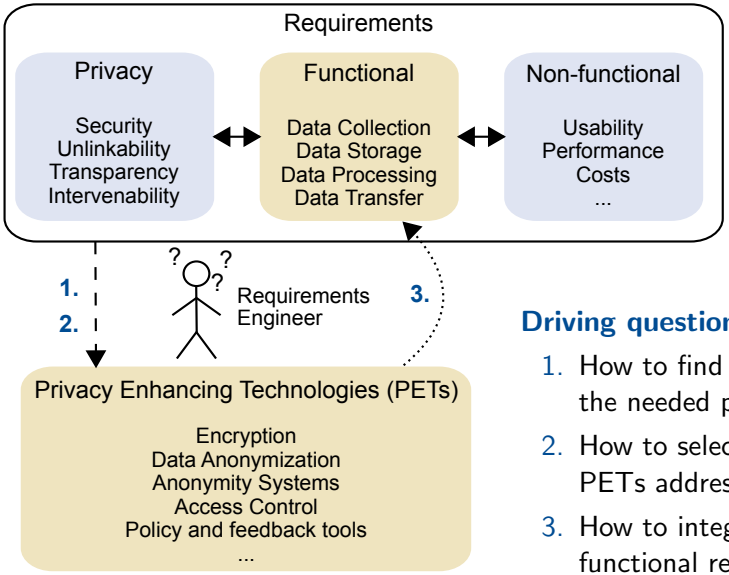
Pattern-based Representation of Privacy Enhancing Technologies as Early Aspects

Rene Meis Maritta Heisel

PALUNO
The Ruhr Institute for Software Technology
University of Duisburg-Essen, Duisburg, Germany

September 7, 2017



Driving questions

1. How to find PETs operationalizing the needed privacy requirements?
2. How to select among different PETs addressing the privacy needs?
3. How to integrate PETs into the functional requirements?

Problem

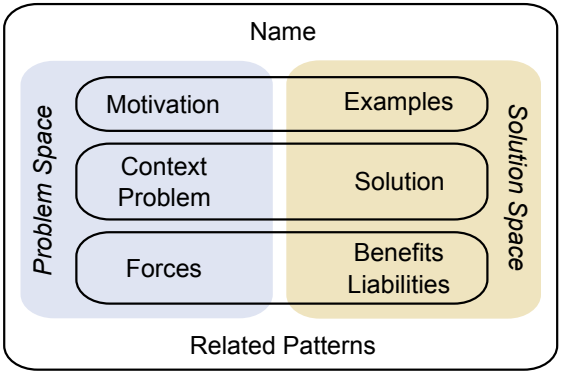
1. How to find PETs operationalizing the needed privacy requirements?
2. How to select among different PETs addressing the privacy needs?

Solution

PET patterns containing:

- Solution provided by the PET
- Context of applicability
- Problem addressed
- PET's impact on privacy and non-functional requirements
- Application examples

Consumers: Requirements Engineers



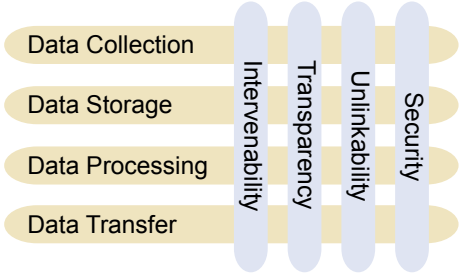
Problem

3. How to integrate PETs into the functional requirements?

Solution

Aspect-Oriented Requirements Engineering

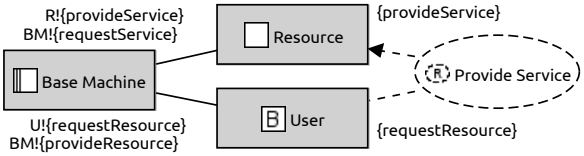
- Privacy Requirements are cross-cutting
- PETs can be described independently of the application scenario
- Cross-cutting concerns are extracted in AORE and expressed mostly independently from the functionality they cross-cut
- Join points specify how aspects can be integrated (weaved) into other functionalities

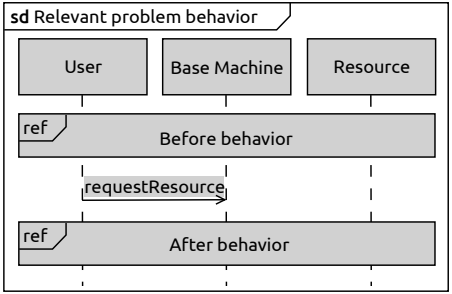


Name Attribute-Based Credentials, Privacy-ABCs

Motivation A cigarette vending machine shall sell cigarettes only to adults, without identifying individuals or linking purchases.

Context/Problem A machine manages user requests for accessing a specific resource providing a service. Users' requests contain personal information (PI) or at least information about PI. This information needs to be checked for authenticity and legitimacy, while minimal PI is revealed.





[1] based on ABC4Trust deliverables (http://abc4trust.eu)

Privacy Forces

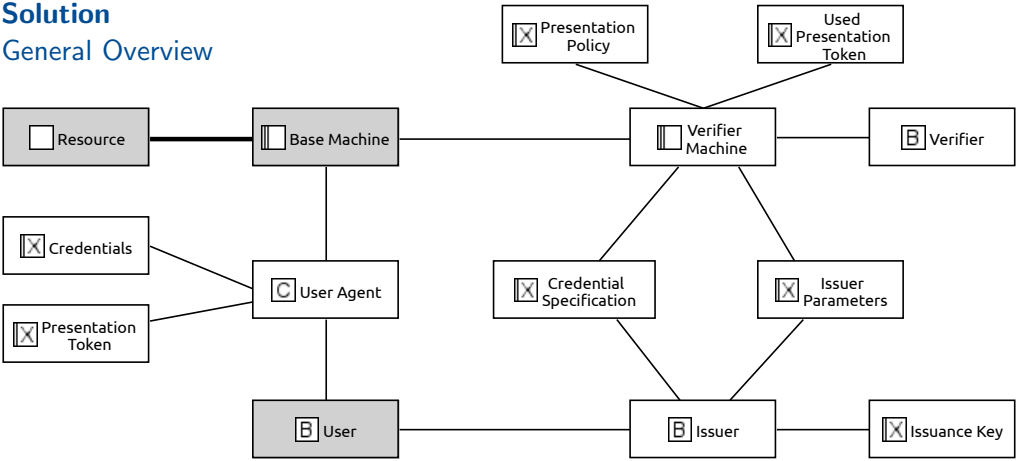
Confidentiality	Only proofs that PI has certain properties is needed, the actual PI shall not be disclosed
Integrity	The provided information shall be authentic and correct
Anonymity/Data unlinkability	The service provider shall not be able to link the collected data to the user or to data from other interactions.
Collection information	Users shall be informed about the PI that is collected

General Forces

End-user friendliness	needs to be balanced with degree of privacy protection needed
Performance	needs to be balanced with degree of privacy protection needed
Costs	needs to be balanced with degree of privacy protection needed
Abuse of PET	It shall not be possible to get access to the service by providing incorrect data
Revocation	It may be wished to re-identify an individual user in specific cases

Solution

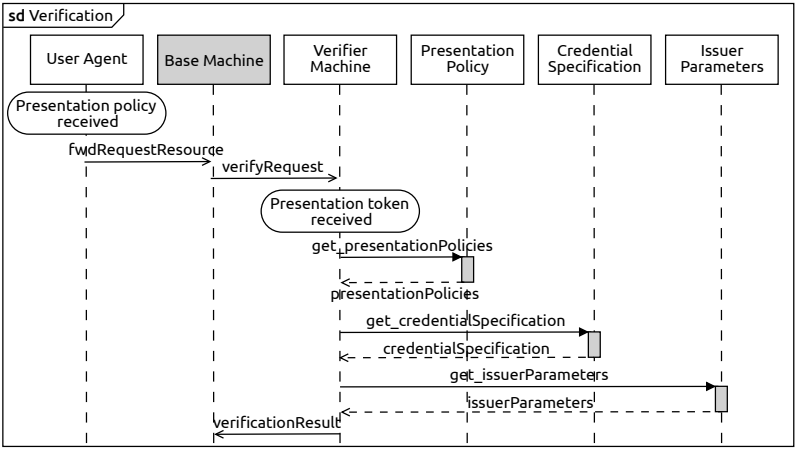
General Overview



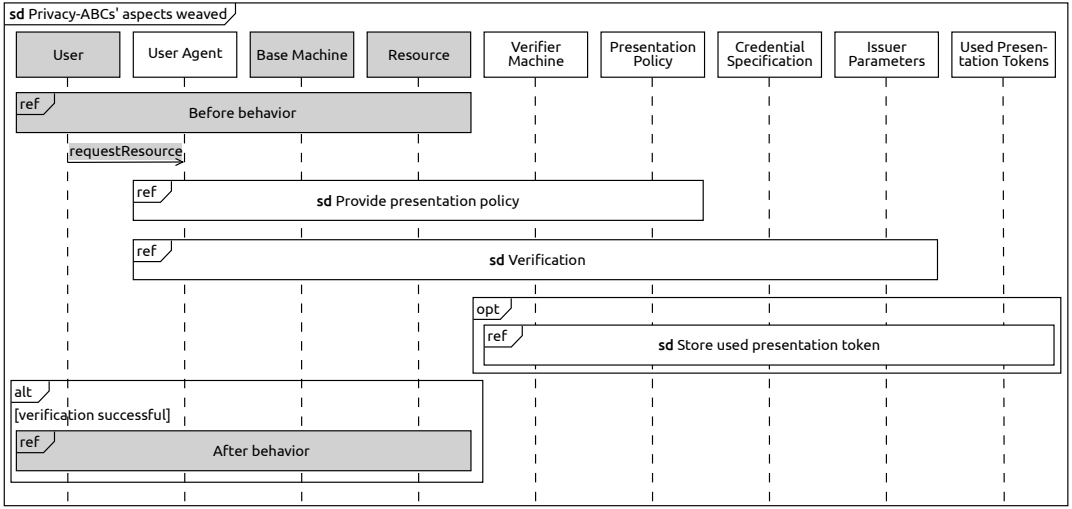
Assumptions about User, User Agent, and Issuer

Aspects

1. Provide presentation policy to User Agent
2. Verify received presentation token
3. Store used presentation token



Weaving



Base Problems inlcude the definition of the presentation policy

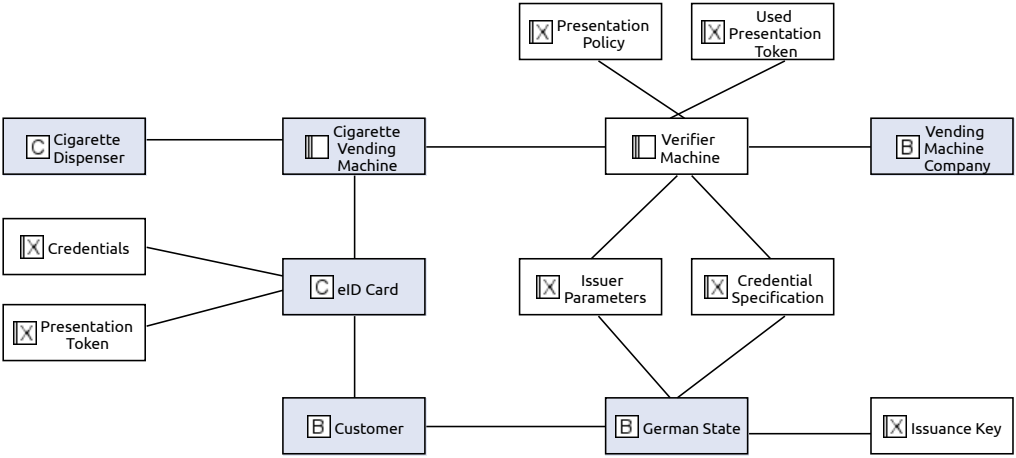
Privacy Consequences

	Benefits	Liabilities
Confidentiality	Proofs about credentials' properties can be generated	Presentation policy has to request only minimal PI
Integrity	Credentials cannot be modified, presentation tokens can only be created based on credentials	Necessary changes of the credentials require a revocation of old credentials
Anonymity/ Data unlinkability	Presentation tokens are not linkable to their user or other tokens	The information contained in the presentation token could allow to create links
Collection Information	The presentation policy specifies which PI is collected	Verifiers still need to inform about the purpose of PI collection if this is necessary

General Consequences

	Benefits	Liabilities
End-user friendliness	Positive if an existing ABC infrastructure is used	User friendliness strongly depends on the user agent
Performance	-	A higher response time is expected
Costs	Relative low if an existing ABC infrastructure is used	High if an own ABC infrastructure is set up and maintained
Abuse of PET	Corrupted tokens can be detected and issuer guarantees correctness	If the software-to-be can be misused, it is hardly possible to identify the malicious user
Revocation	-	Revocation is not supported, but extensions including revocation exist

Examples Instantiation for cigarette vending machine:



Related Patterns Privacy-ABCs with Revocation Authority, Privacy-ABCs with Inspector

Contributions

1. Pattern format for the presentation of PETs
   Addressing:
   - How to find PETs operationalizing the needed privacy requirements?
   - How to select among different PETs addressing the privacy needs?
2. Description of PETs as early aspects
   Addressing:
   - How to integrate PETs into the functional requirements?
3. PET pattern for Attribute-Based Credentials based on the ABC4Trust project[2]

Future directions

- Creation of a (machine-readable) library of PET patterns
- Adding explicit references to threats that are mitigated by a PET

[2] https://abc4trust.eu