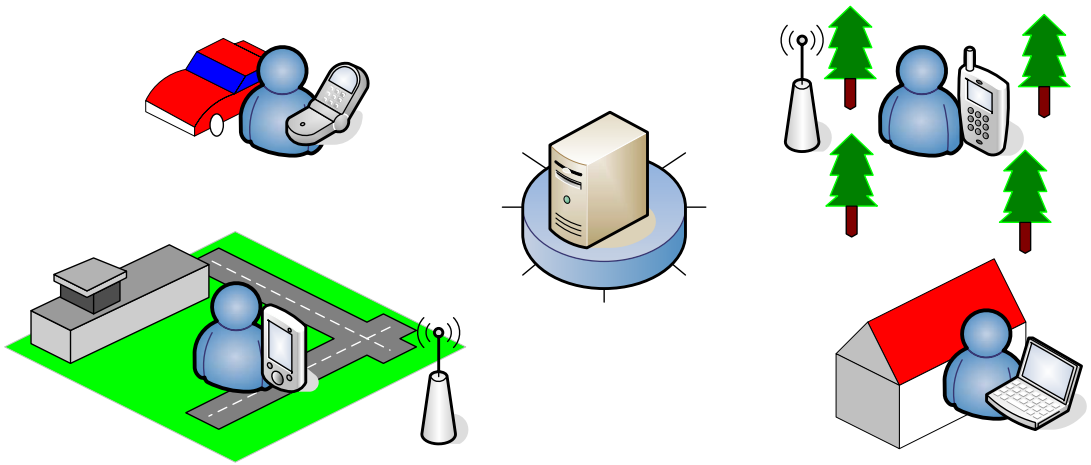
Towards Privacy Protection in a Middleware for Context-awareness

Linda Pareschi, Daniele Riboni, Sergio Mascetti, Claudio Bettini

University of Milan, Italy

Adaptive services in context-awareness



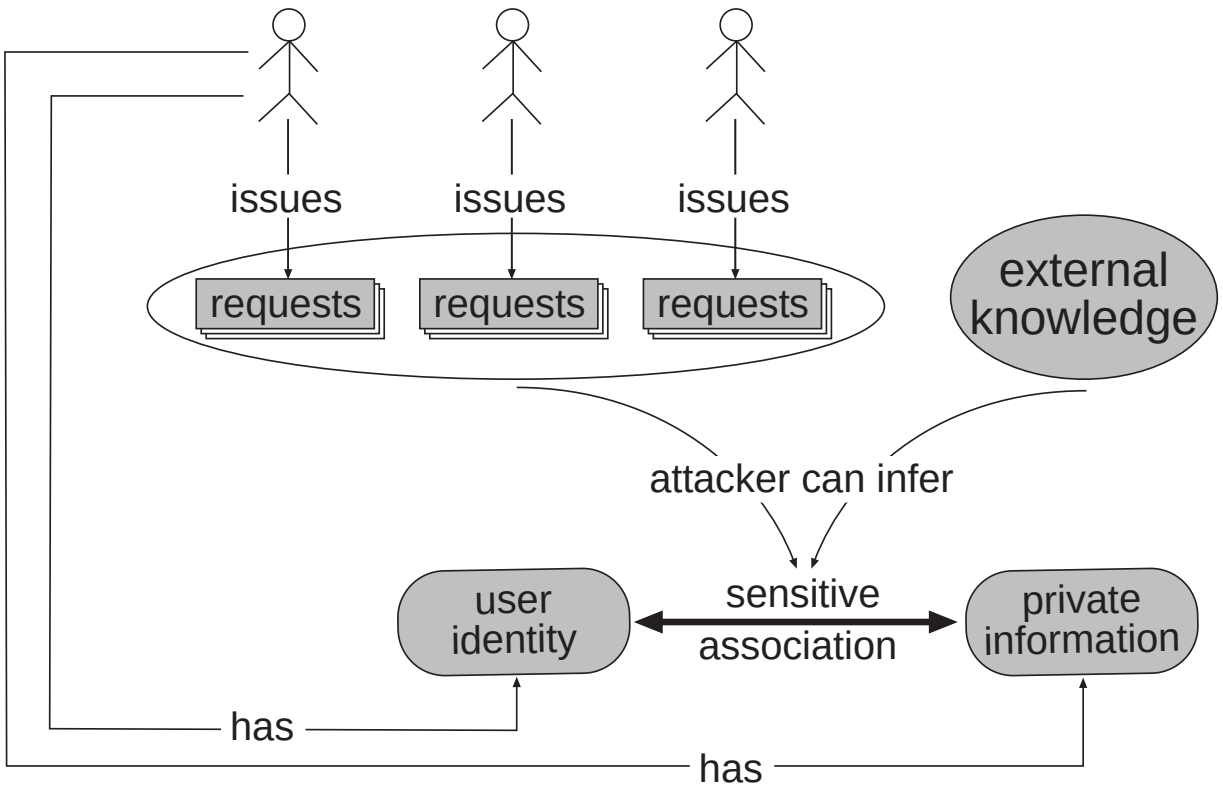
Adaptive Services

- Services that adapts themselves to the *current* situation of the user, i.e. to the user *Context*

Context - Dey, 2001

Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves.

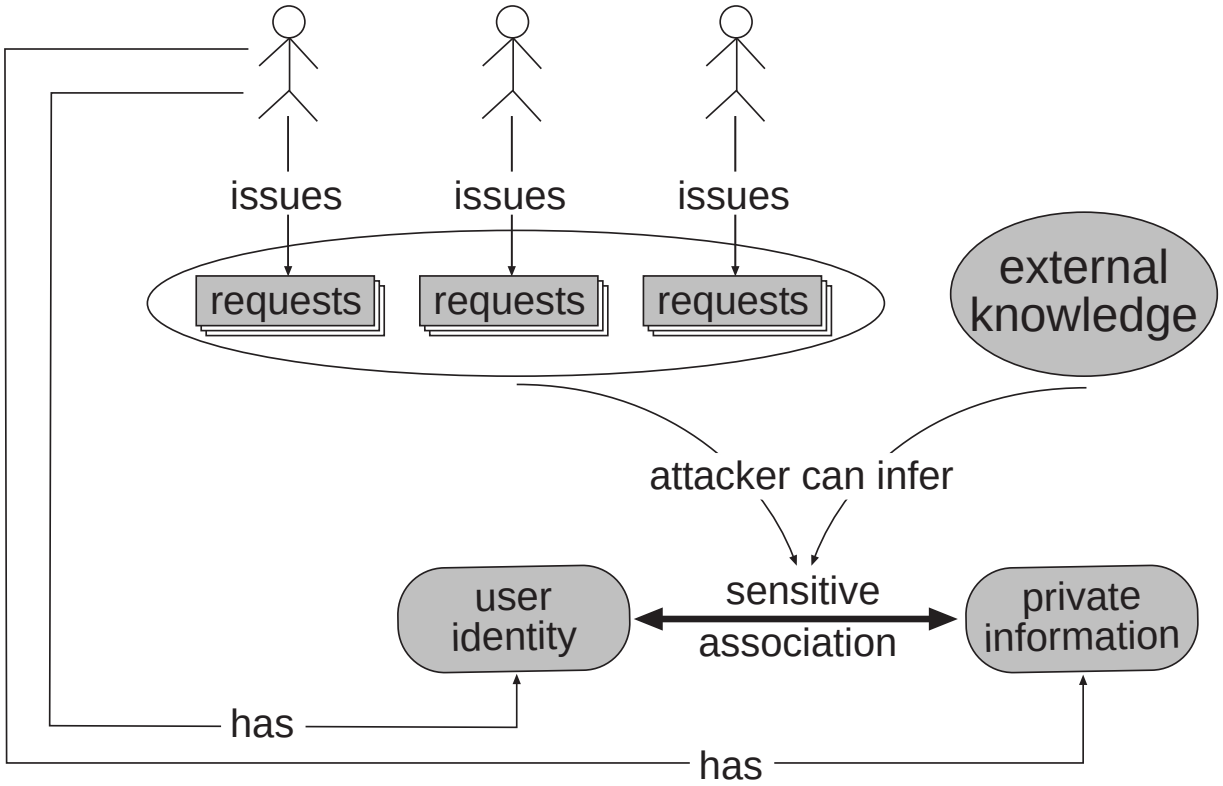
Privacy Threat in Adaptive Services



Privacy concerns

- Final users do not desire to reveal their private information.
- Mobile devices contain personal data.
- Internet requests by mobile devices may lead to personal data disclosure.

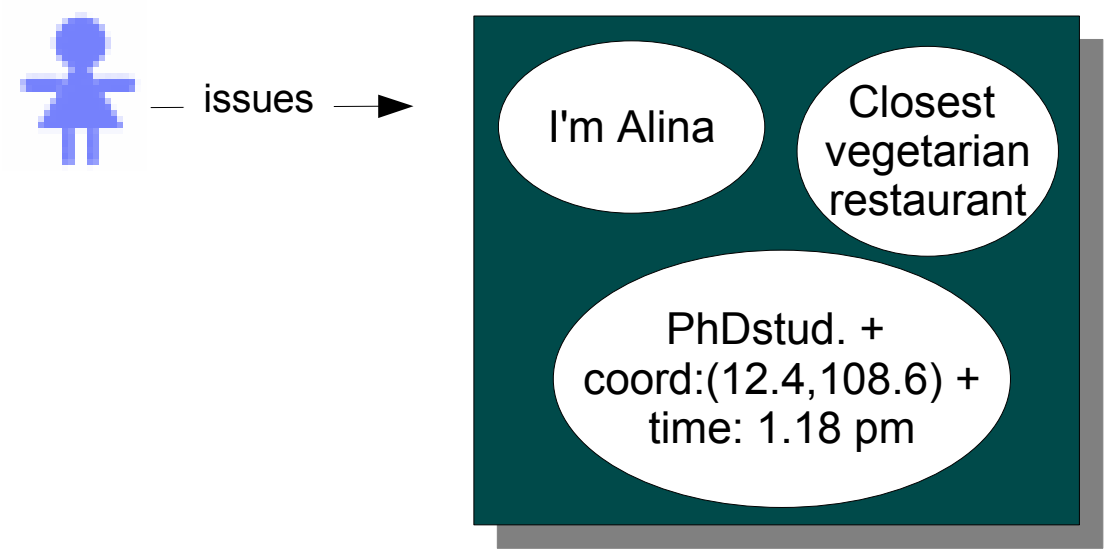
Privacy Threat in Adaptive Services



General privacy threat

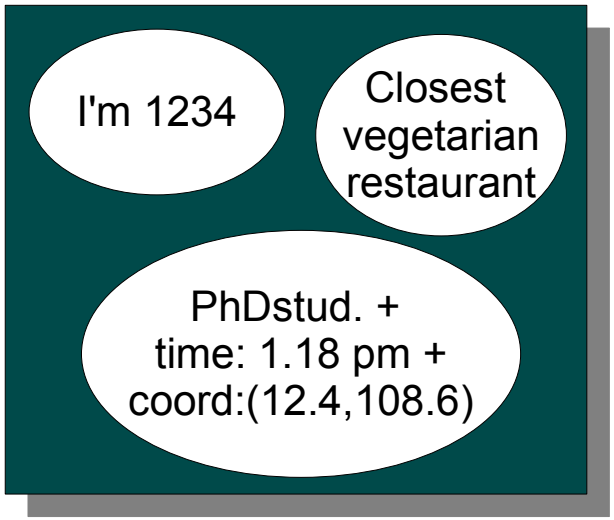
The possibility an attacker associates the user's identity to information considered private.

Example



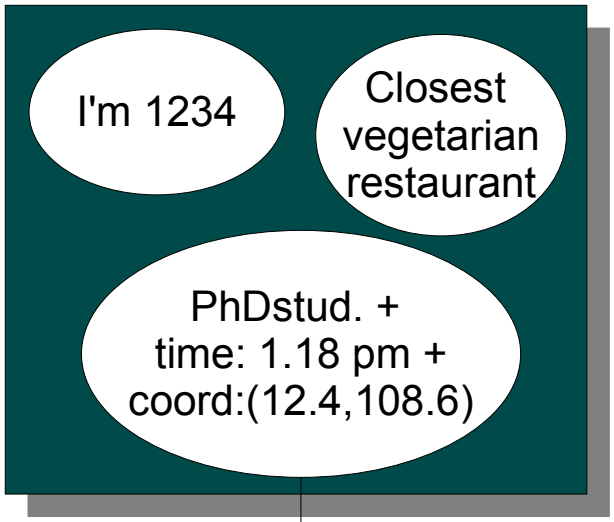
- Sensitive association: *Alina is vegetarian*
- PI : *closest vegetarian restaurant*
- QI : depend on the external knowledge

Example



ID	Role	Time	Coordinate
.....	.....	.....	.....
Jane	Stud	1.45pm	(32.7, 215,9)
Alina	PhDstud	1.18pm	(12.4, 108.6)
Marc	PhDstud	1.32pm	(13.9, 112.4)
Bob	Stud	4pm	(12.2,101.3)
Carl	Stud	12am	(16.3, 100.8)
.....	.....	.....	.....

Example



ID	Role	Time	Coordinate
.....	.....	.....	.....
Jane	Stud	1.45pm	(32.7, 215,9)
Alina	PhDstud	1.18pm	(12.4, 108.6)
Marc	PhDstud	1.32pm	(13.9, 112.4)
Bob	Stud	4pm	(12.2,101.3)
Carl	Stud	12am	(16.3, 100.8)
.....	.....	.....	.....

Alina = 1234
Alina is vegetarian

Problems statements

Problem statements

- Data must be effectively generalized in order to preserve the user privacy
- The loss of information due to the generalization leads to a lower level of the quality of the service

Anonymity

- Precise values of QI are substituted by generalized data.

LBS-k-anonymity
Gruteser,Grunwald - Mobisys03

- Idea: generalize QI data in order to make the actual issuer indistinguishable among at least other $k-1$ potential issuers.

Issue

The generalization must consider the type of context-data

numerical $v \longrightarrow [v_1, v_2]$ s.t. $v \in [v_1, v_2]$

categorical v in a taxonomy T $\longrightarrow$ ancestor $v' \in T$

Anonymity

- Precise values of QI are substituted by generalized data.

LBS-k-anonymity
Gruteser,Grunwald - Mobisys03

- Idea: generalize QI data in order to make the actual issuer indistinguishable among at least other $k-1$ potential issuers.

Issue

The generalization must consider the type of context-data

numerical $v \longrightarrow [v_1, v_2]$ s.t. $v \in [v_1, v_2]$

categorical v in a taxonomy T $\longrightarrow$ ancestor $v' \in T$

Anonymity

- Precise values of QI are substituted by generalized data.

LBS-k-anonymity Gruteser,Grunwald - Mobisys03

- Idea: generalize QI data in order to make the actual issuer indistinguishable among at least other $k-1$ potential issuers.

Issue

The generalization must consider the type of context-data

numerical	$v \longrightarrow [v_1, v_2]$ s.t. $v \in [v_1, v_2]$
categorical	v in a taxonomy T $\longrightarrow$ ancestor $v' \in T$

Example

ID	Role	Time	Coordinate
.....	.....	.....	.....
Jane	Stud	1.45pm	(32.7, 215,9)
Alina	PhDstud	1.18pm	(12.4, 108.6)
Marc	PhDstud	1.32pm	(13.9, 112.4)
Bob	Stud	4pm	(12.2,101.3)
Carl	Stud	12am	(16.3, 100.8)
.....	.....	.....	.....

Alina =?= 1234
Marc =?= 1234
Carl =?= 1234

Alina is 3-anonymouse

Stereotypes

- The adaptation will not be based on individual profiles.

Stereotypes

The service customization is performed according to the social role of the issuer

Pseudo-id

- Authentication
- Sessions management

Stereotypes

- The adaptation will not be based on individual profiles.

Stereotypes

The service customization is performed according to the social role of the issuer

Pseudo-id

- Authentication
- Sessions management

Stereotypes

- The adaptation will not be based on individual profiles.

Stereotypes

The service customization is performed according to the social role of the issuer

Pseudo-id

- Authentication
- Sessions management

Context-aware privacy policies

- A user may desire to define policies affecting the trade-off between privacy and quality of service.

Context-based privacy policies

For each context data:

- maximum level of generalization
- global level of privacy
- priority over context data

p_1: *activity=working* $\Rightarrow$ *anonymity:=high*

p_2: *activity=shopping* $\Rightarrow$ *anonymity:=low*

p_3: *activity=walking* $\Rightarrow$ *provide-accurate-loc*

Context-aware privacy policies

- A user may desire to define policies affecting the trade-off between privacy and quality of service.

Context-based privacy policies

For each context data:

- maximum level of generalization
- global level of privacy
- priority over context data

p_1: *activity=working* $\Rightarrow$ *anonymity:=high*
p_2: *activity=shopping* $\Rightarrow$ *anonymity:=low*
p_3: *activity=walking* $\Rightarrow$ *provide-accurate-loc*

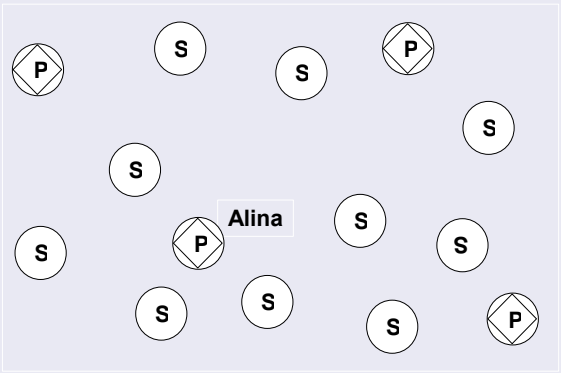
Context-aware privacy policies

- A user may desire to define policies affecting the trade-off between privacy and quality of service.

Context-based privacy policies

For each context data:

- maximum level of generalization
- global level of privacy
- priority over context data



p_1: *activity=working* $\Rightarrow$ *anonymity:=high*

p_2: *activity=shopping* $\Rightarrow$ *anonymity:=low*

p_3: *activity=walking* $\Rightarrow$ *provide-accurate-loc*

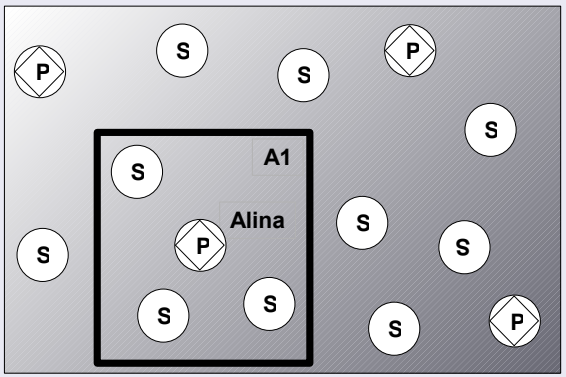
Context-aware privacy policies

- A user may desire to define policies affecting the trade-off between privacy and quality of service.

Context-based privacy policies

For each context data:

- maximum level of generalization
- global level of privacy
- priority over context data

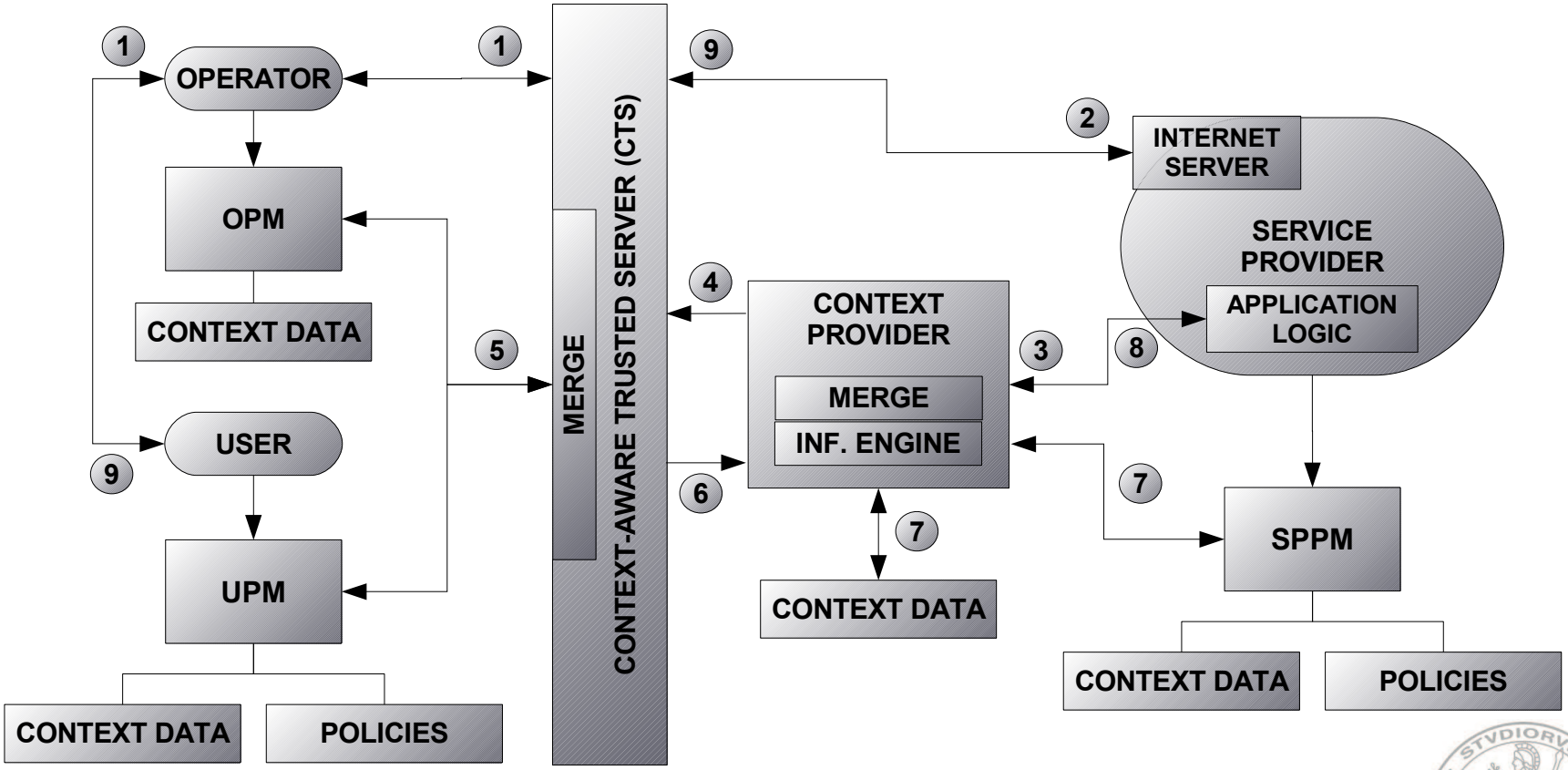


p_1: *activity=working* $\Rightarrow$ *anonymity:=high*

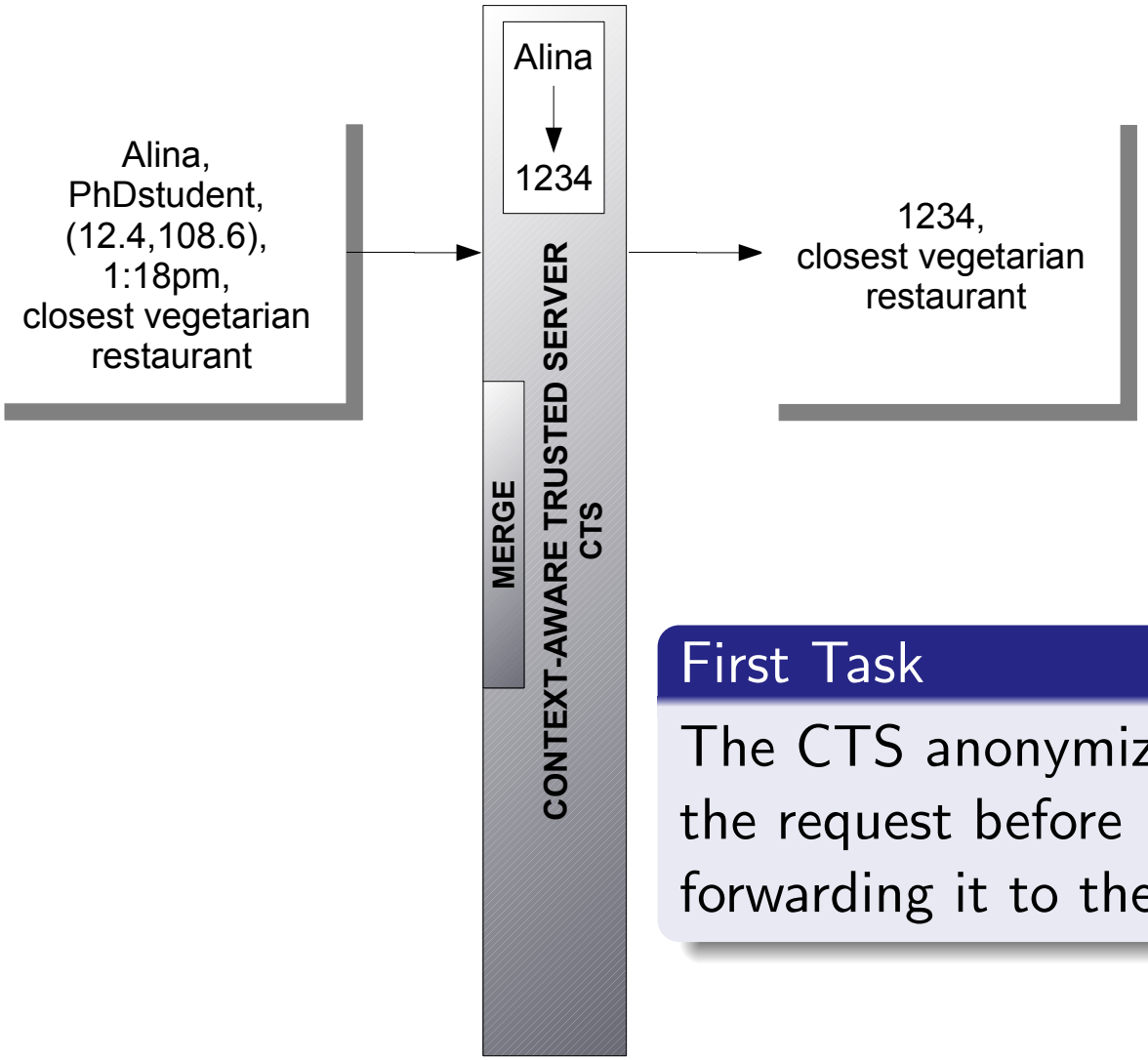
p_2: *activity=shopping* $\Rightarrow$ *anonymity:=low*

p_3: *activity=walking* $\Rightarrow$ *provide-accurate-loc*

The CARE Architecture



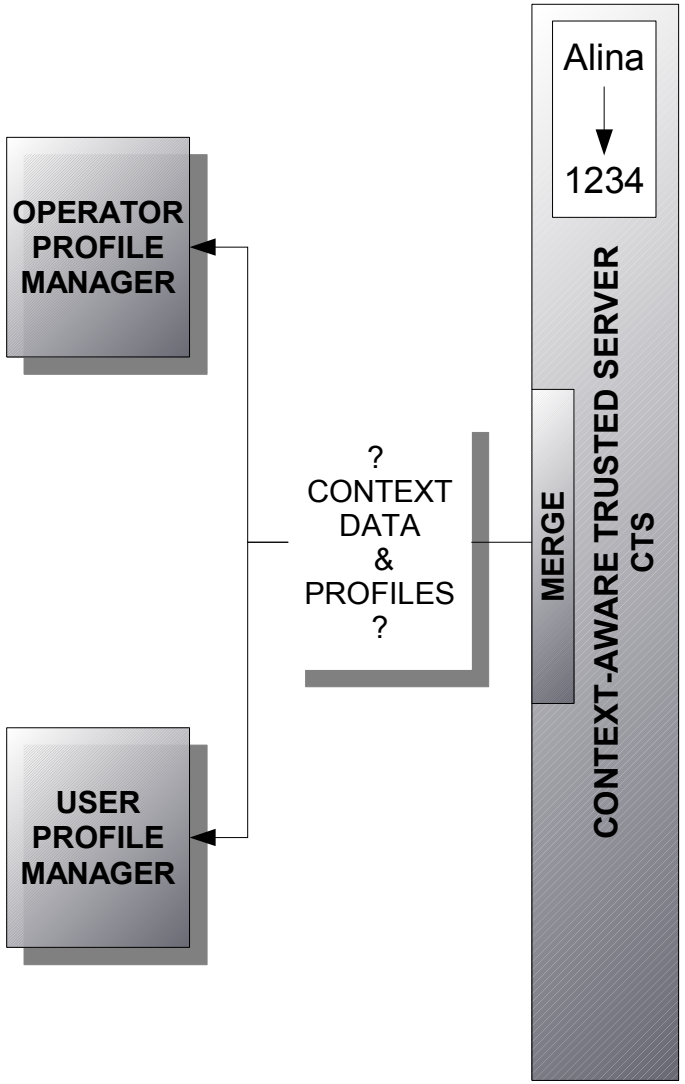
The role of the CTS



First Task

The CTS anonymizes the request before forwarding it to the SP.

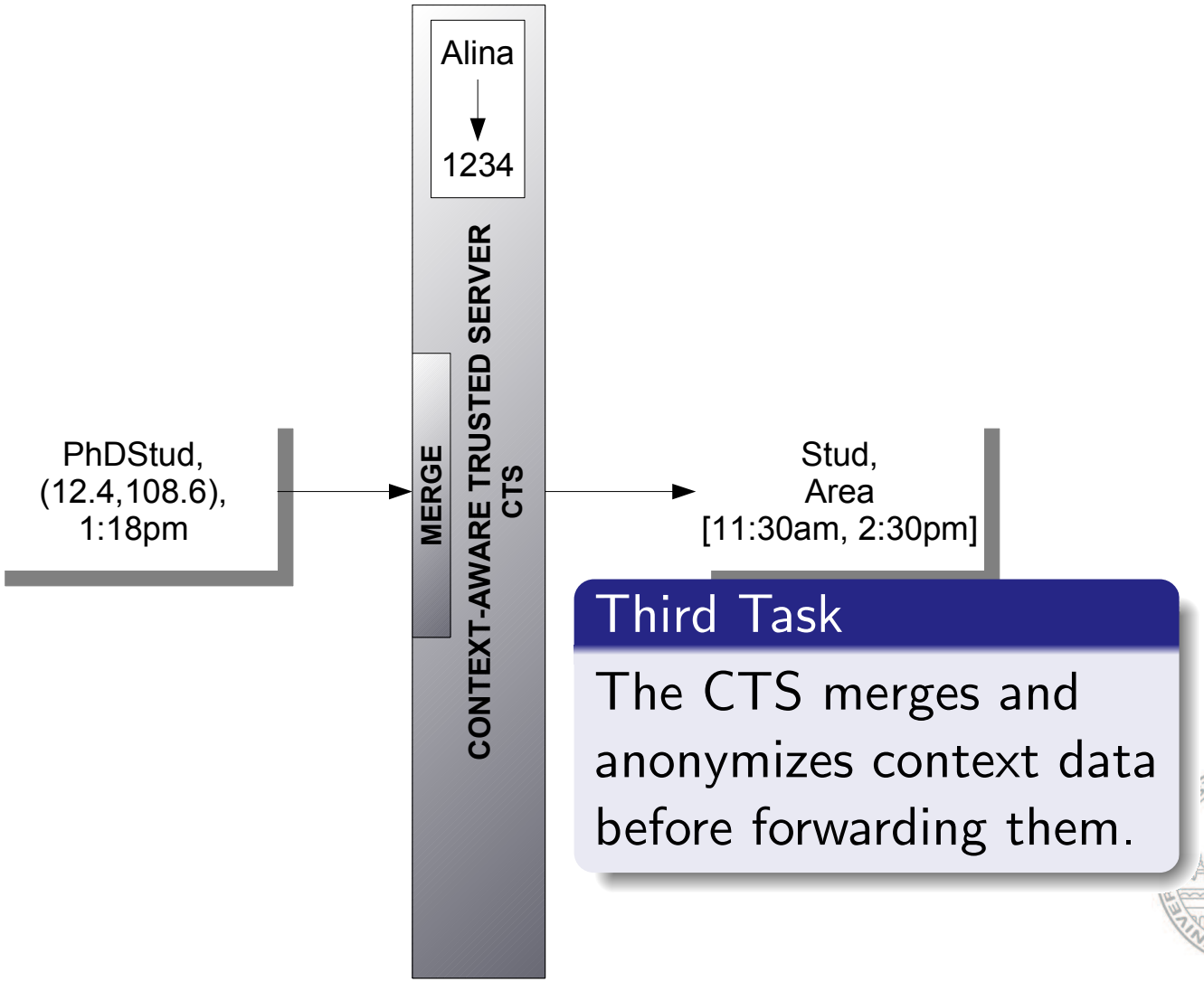
The role of the CTS



Second Task

The CTS asks for context data to entities in the user's domain.

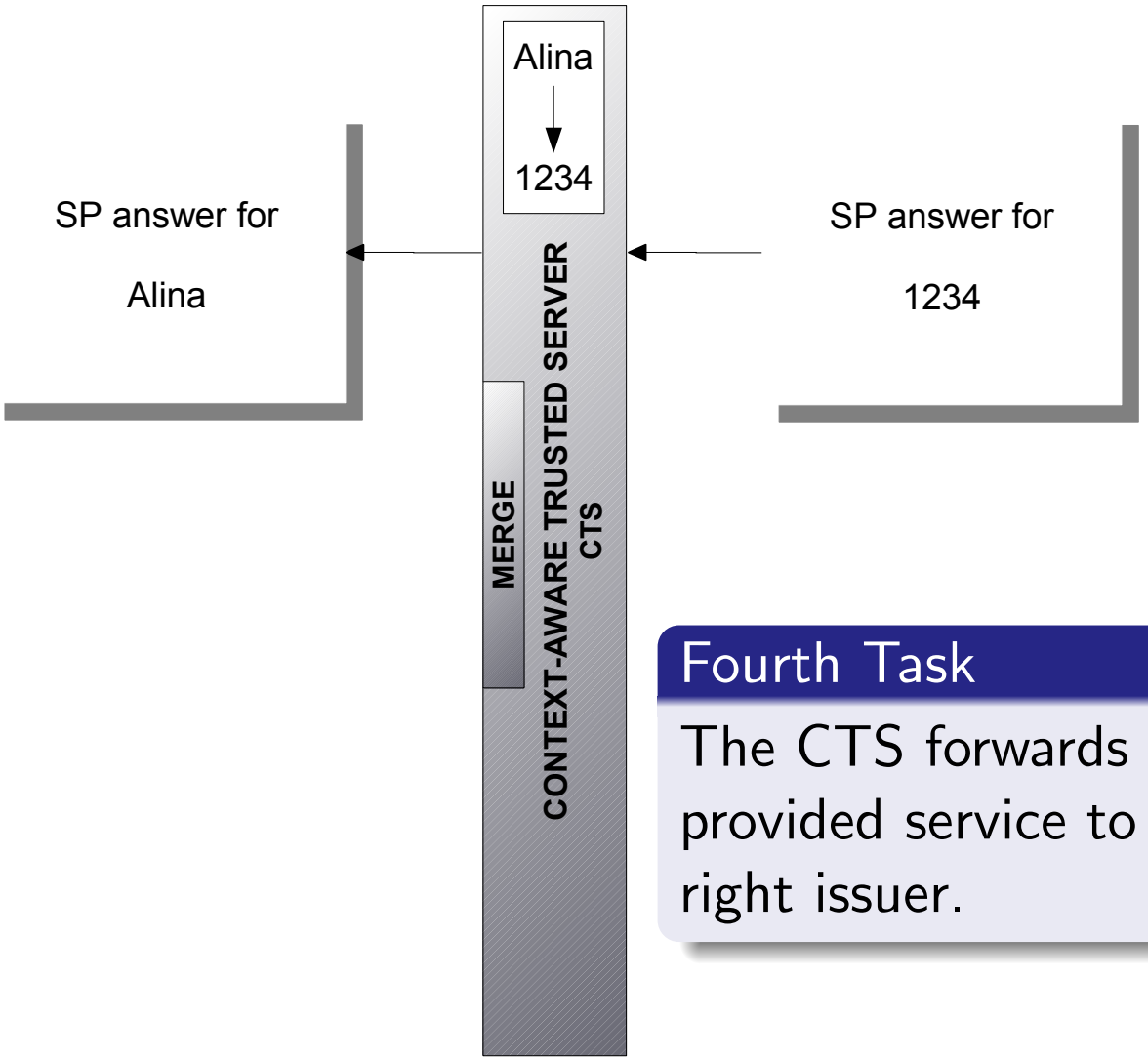
The role of the CTS



Third Task

The CTS merges and anonymizes context data before forwarding them.

The role of the CTS



Fourth Task

The CTS forwards the provided service to the right issuer.

Conclusion and future work

Conclusion

- Obfuscation techniques must be applied to context data in order to protect the user privacy with respect to the user preferences about the level of adaptation.
- We propose the integration of a module for the privacy preservation in a middleware for adaptive services.

Future Work

- Implementation of the CTS module
- Experimental evaluation of the anonymization mechanisms
- Experimental evaluation of the user satisfaction

References

- C. Bettini, D. Maggiorini, D. Riboni. **Distributed Context Monitoring for the Adaptation of Continuous Services**, World Wide Web Journal, Springer, 2007.
- C. Bettini, S. Mascetti, X.S. Wang, S. Jajodia. **Anonymity in Location-based Services: Towards a General Framework**, in Proc. of the 8th International Conference on Mobile Data Management (MDM-2007), IEEE Computer Society, 2007.
- C. Bettini, L. Pareschi, S. Jajodia. **Anonymity and Diversity in LBS: a Preliminary Investigation**, in Proc. of the Fifth IEEE International Conference on Pervasive Computing and Communications (PERCOM-07), Work in progress session, pp. 577-580, IEEE Computer Society, 2007.

Thank you.