
Invited Talk – EuroCAT 2009

Trust Management in Context-Aware and Service-Oriented Architectures

Ricardo Neisse

Ricardo.Neisse@iese.fraunhofer.de

Outline

- Background and research interests (1)
- Talk divided in 3 parts
 1. Trust management for context-aware services (18)
 2. Context-based policy management (12)
 3. Trust and policy management for service oriented architectures (14)
- Wrap-up and discussion

Slide 2/55

Background



AWARENESS

FREEBAND



Universiteit Twente
de ondernemende universiteit

- Researcher at Fraunhofer IESE in Kaiserslautern, Germany
- Areas of interest:
 - Context-aware service platforms
 - Service-oriented architectures
 - Trust management
 - Policy management

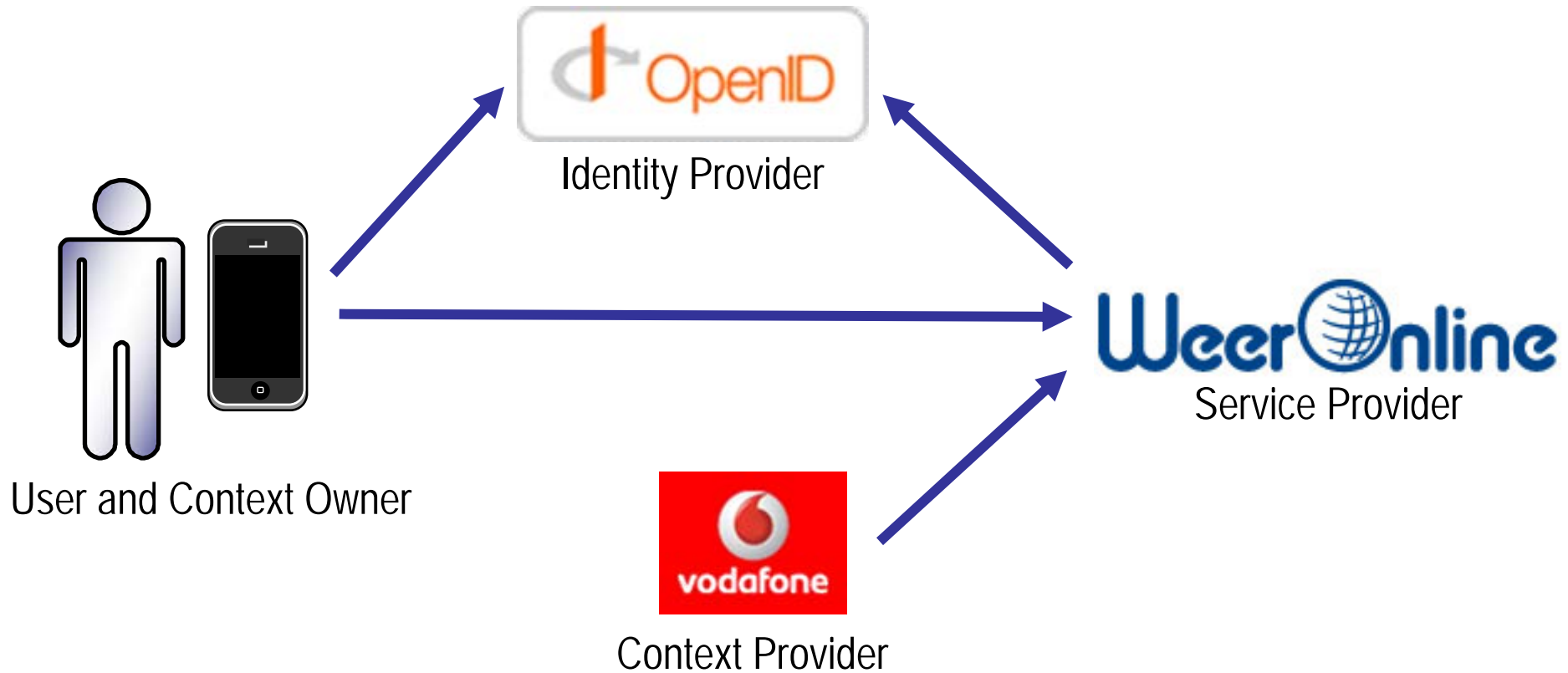
Slide 3/55

Part 1. Trust Management for Context-Aware Services

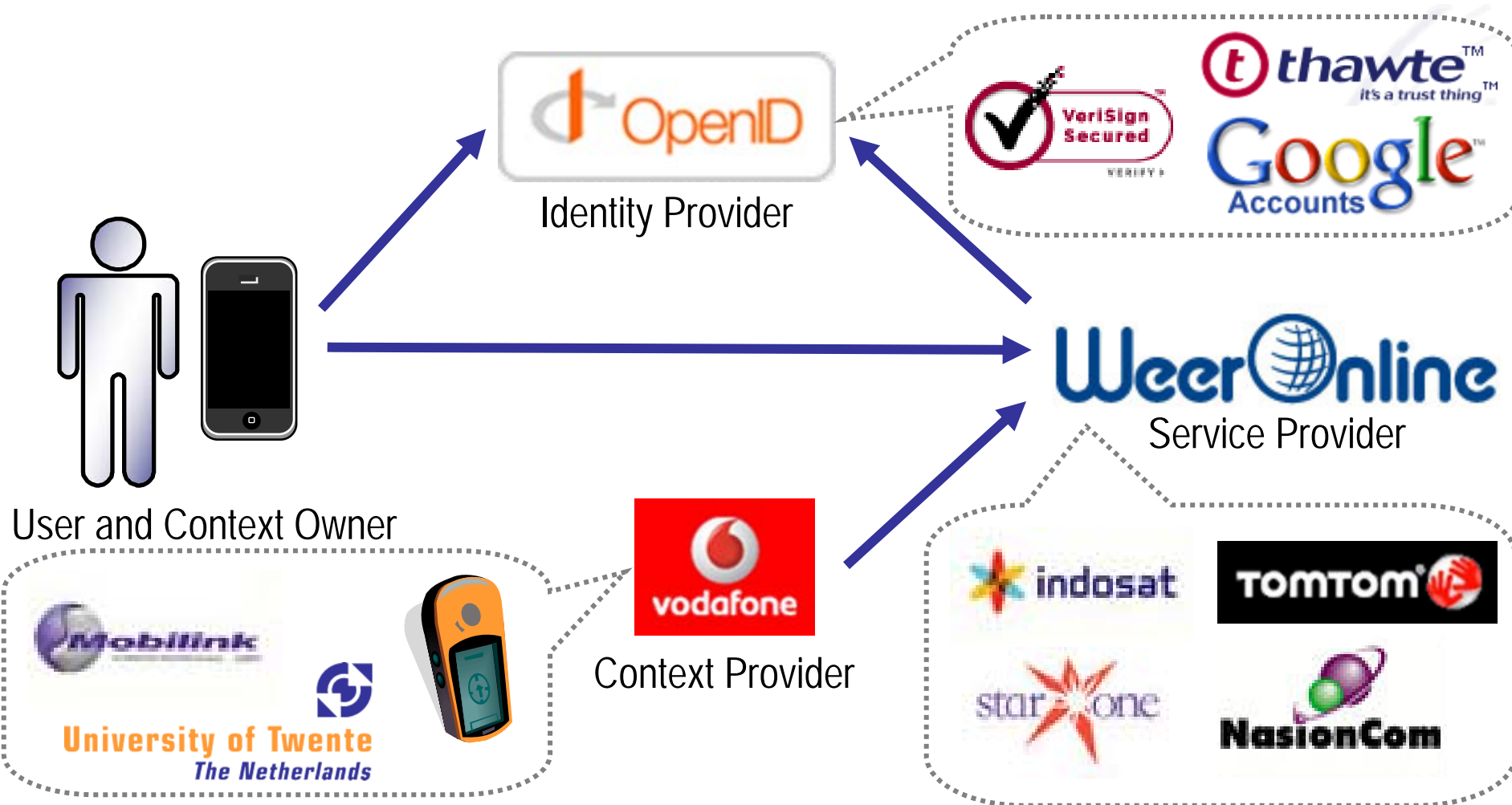
- Trust relationships in a context-aware service platform
- Trust management model and mechanisms
- Validation results
- Conclusions

Slide 4/55

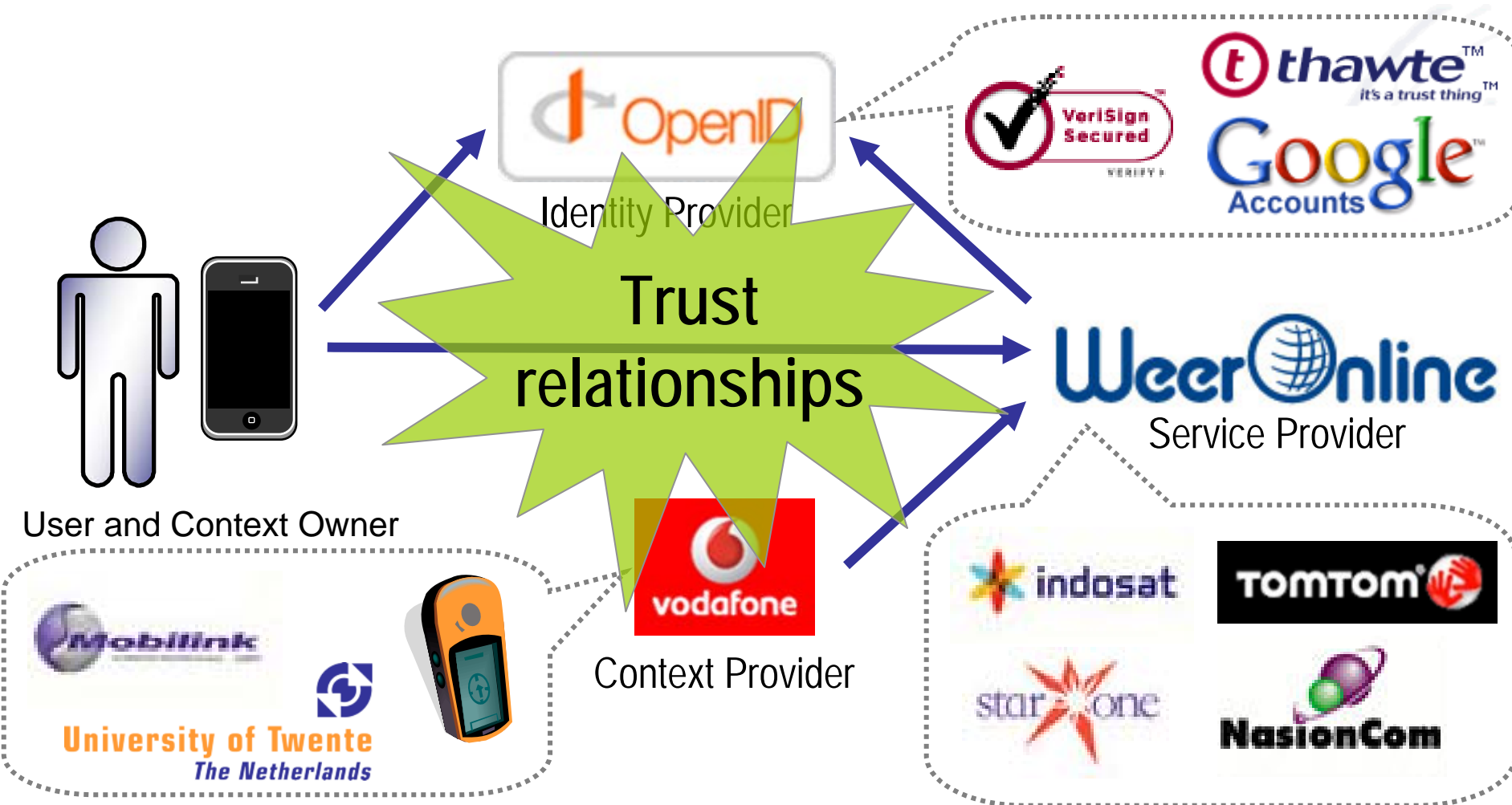
An Example Scenario



An Example Scenario



An Example Scenario



Context-Aware Service Platform

- Available everywhere anytime
- Information from service users retrieved from sensors in the surrounding physical environment to adapt the services
- Multiple administrative domains have to collaborate and trust each other
- Our goal: support the users in the management of the trade-off between privacy and context-based service adaptation

Slide 8/55

Trust Management and Trusted Computing

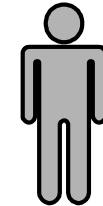
Informational trust:

- Trust degree
- Trust aspects
- Trust management

Technical trust:

- Trusted Computing Platform (TCP)

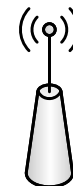
Social
(human perspective)



Informational
(conceptual models)



Technical
(cryptography and TCP)



Slide 9/55

Trust Management – Trust Definition

- Trust is: *the measurement of the belief from a trusting party point of view (trustor) with respect to a trusted party (trustee) focused on a specific trust aspect and behavior that possibly implies a risk*
- Risk is implied if Trustor chooses to depend on the trustee for aspect and behavior

Slide 10/55

Trust Management

- Trust information model
- Bootstrapping of trust degrees
- (Time-based) evolution (increase/decrease) of trust degrees
- Analysis of stakeholders' goals and dependencies
- Trust management for decision support in the selection of trustworthy entities

Slide 11/55

Trust Management – Trust Belief

- Trust belief:
 - Trustor/Trustee
 - Behavior
 - Aspect
 - Degree
- Example: Alice trusts at a high degree that Bob is competent to write a computer program in the Java language

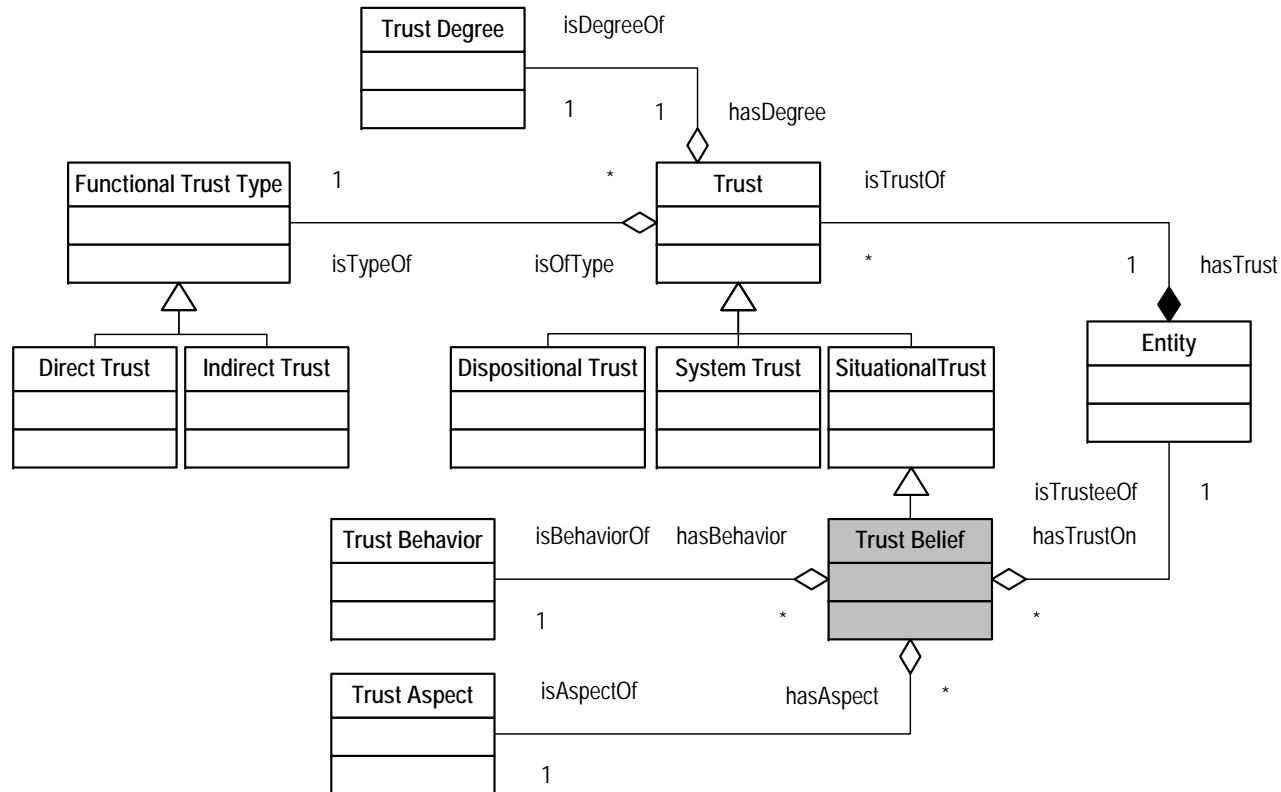
Slide 12/55

Trust Management – Conceptual Model

- Social trust concepts [Mayer et al.]
 - Dispositional
 - System
 - Situational
 - Trust belief
- Functional type
 - Direct: personal experience
 - Indirect trust: recommendations

Slide 13/55

Trust Management – Model



Slide 14/55

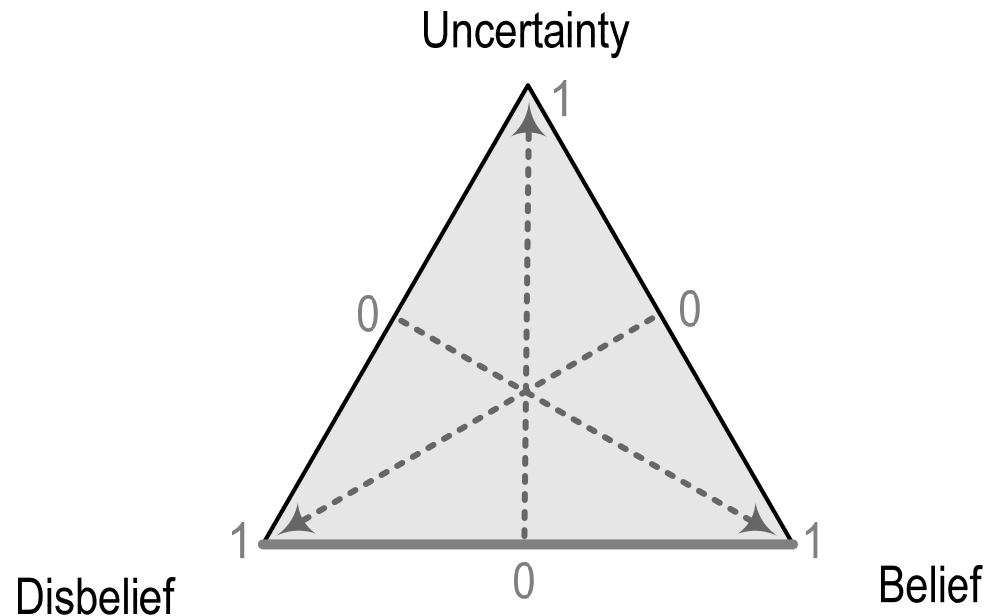
Trust Degrees using Subjective Logic

- Subjective Logic (SL) is a probabilistic logic that is able to explicitly express uncertainty about the probability values.
 - There is always uncertainty
 - Truth is always expressed from an individual perspective
- Subjective logic operators: consensus, discount, smooth average

Slide 15/55

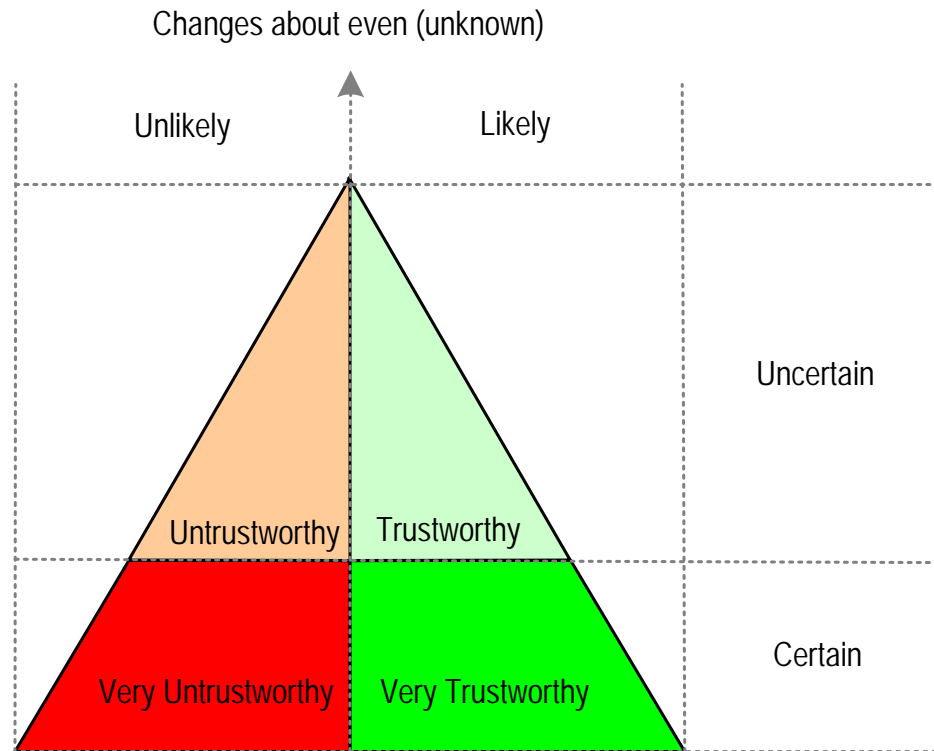
Trust Degree – Subjective Logic Opinion

- Subjective Logic
- Opinion $b+d+u=1$
 - Belief
 - Disbelief
 - Uncertainty
- Operators: discount, addition, consensus, ...



Slide 16/55

Subjective Logic Triangle



Slide 17/55

Our Trust Management Approach

- Trust Provider:
 - manages direct/indirect trust database
 - Combines trust aspects
 - evaluates the resulting trust in the context-aware service
- Trust aspects in the context-aware service platform:
 - Identity Provisioning, Privacy Enforcement, Context Provisioning, Recommendations, ... model is extensible

Slide 18/55

Mechanisms to Obtain Trust Values

- Identity Provisioning: authentication method, User registration policy
- Privacy Enforcement: P3P policy specification, confidentiality level of information, consumer protection associations
- Context information: cryptography (PKI like), statistical analysis of providers, aggregators to increase trust, context source type (QoC)
- For trust in general: experience and recommendations

Slide 19/55

Trustworthiness Evaluation

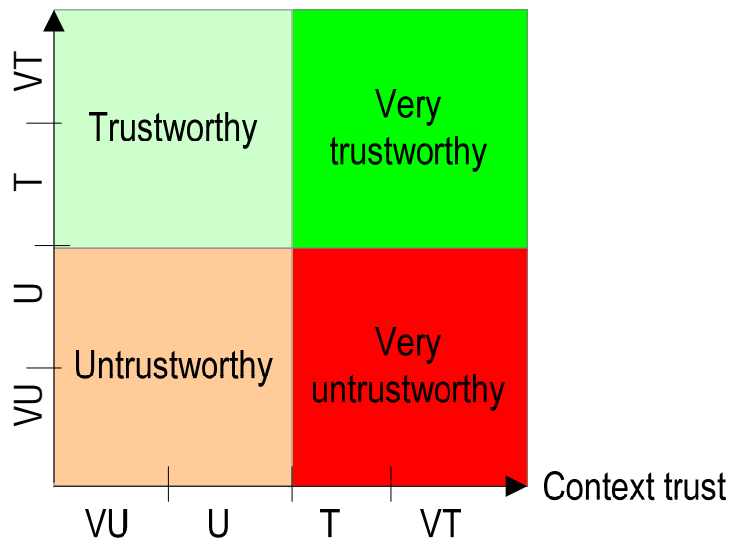
- Objective is to support selection of stakeholders/providers
- Decision is based on:
 - Stakeholders' identity
 - Tasks
 - Goals
 - Trust requirements
- For context-aware service users: trade-off between privacy and service reliability

Slide 20/55

Trustworthiness Evaluation of Context-Aware Service

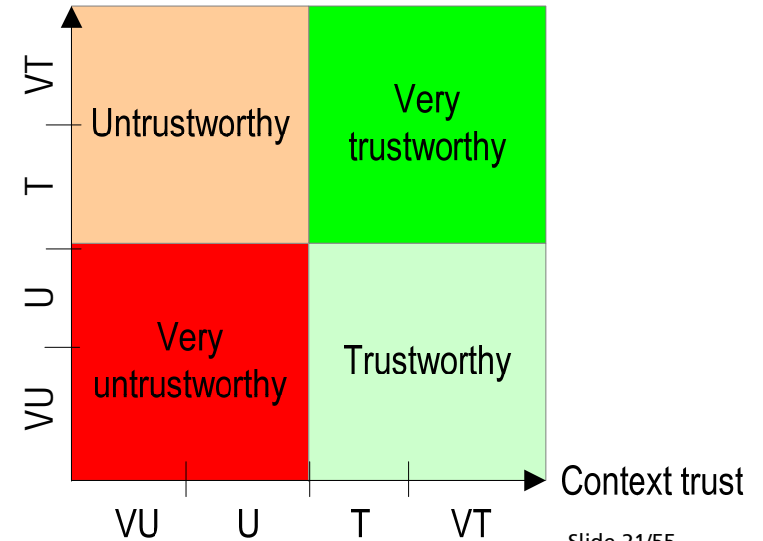
Resulting Trust in the Service for
Privacy Focused user

Privacy trust



Resulting Trust in the Service for
Service Focused user

Privacy trust



Slide 21/55

Validation

- Implementation
- User survey (60 technical participants)
 - Users' choices of entities
 - Users' beliefs
 - Output of our trust management mechanism
 - Usability and usefulness questions

Slide 22/55

Implementation

Context-aware Platform User Agent

Context Aware Services | Context Providers | Identity Providers

User identity: Ricardo Neisse (issued by Personal Identity Provider)
 Context provider: Personal GPS device
 User primary goal: Service adaptation
 Privacy enforcement

Entity	Trust in context-aware service provisioning
Health Care Anywhere Service	<div style="width: 100%; height: 10px; background-color: #90EE90;"></div>
Weather Service	<div style="width: 100%; height: 10px; background-color: #00FF00;"></div>
Tourist Guide Service	<div style="width: 100%; height: 10px; background-color: #00FF00;"></div>

(double-click entity to see trust details)

Context-aware Platform User Agent

Context Aware Services | Context Providers | Identity Providers

User identity: Ricardo Neisse (issued by Personal Identity Provider)
 Context provider: Personal GPS device
 User primary goal: Service adaptation
 Privacy enforcement

Entity	Trust in context-aware service provisioning
Health Care Anywhere Service	<div style="width: 100%; height: 10px; background-color: #FF0000;"></div>
Weather Service	<div style="width: 100%; height: 10px; background-color: #00FF00;"></div>
Tourist Guide Service	<div style="width: 100%; height: 10px; background-color: #00FF00;"></div>

(double-click entity to see trust details)

Trustworthiness and QoC Management

Context provider discovery

Context type: Ambient temperature
 Context owner: Ricardo Neisse

Discover

Discovery results

- Ambient temperature provider (1) (trustworthy)
 - Context owner: *
 - Precision: +-0.5 degrees celcius
 - Timestamp resolution: hour
- Ambient temperature provider (2) (untrustworthy)

Query selected provider

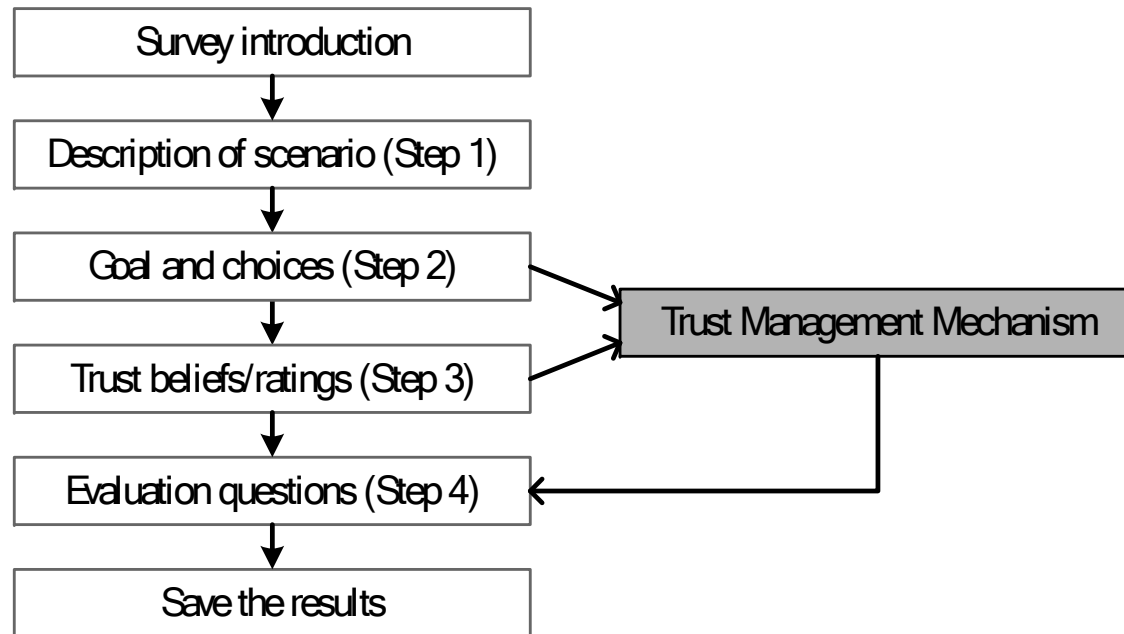
Query result for: Ambient temperature provider (1)

Context owner: Ricardo Neisse Trustworthiness: trustworthy
 Context: 23.5 Celcius Precision: +- 0.5
 Timestamp: 2008/05/01 10 AM Timestamp resolution: hour

Trustworthiness feedback:

Slide 23/55

Structure of Survey

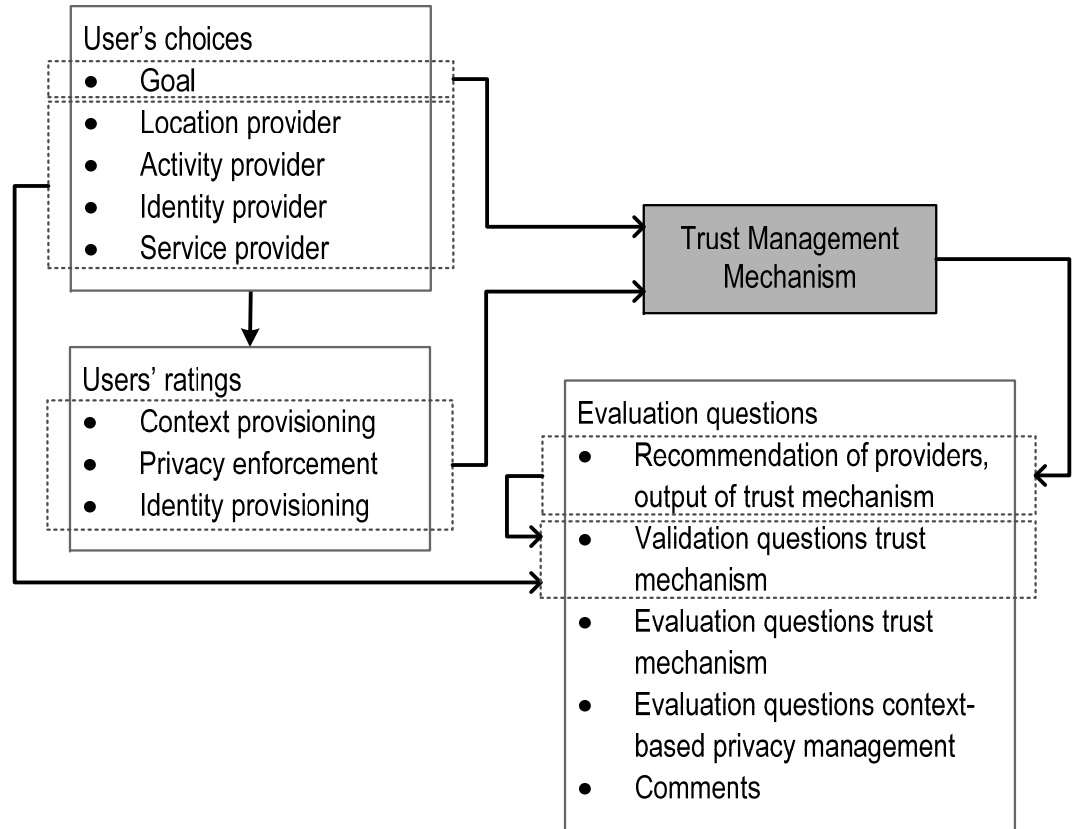


Slide 24/55

Friend Radar Service



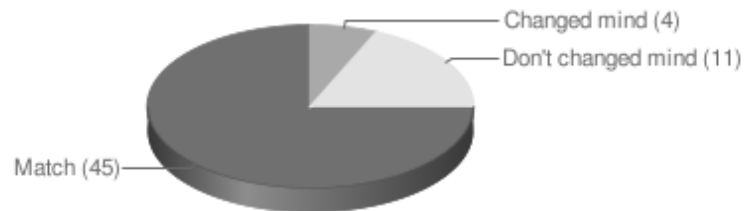
Structure of Survey



Slide 26/55

Survey Results (1/2)

- User agreement with our mechanism:
 - 85% for context providers
 - 89% for identity providers
 - 82% for service providers



Slide 27/55

Survey Results (2/2)

- We learned that:
 - The survey participants understand the different trust aspects (95%)
 - They think that privacy is more important than the service (75%)
 - Other important trust aspects that should be considered in future approaches: coverage, cost, fun, integration with other services
 - Limitations of our results: what people say and what they actually do

Slide 28/55

Conclusions (end of part 1)

- Trust management mechanism for context-aware service platforms with different trust aspects
- Relation between QoC and trust
- Support users in the selection of trustworthiness entities
- Validated from the technical and user perspective
- OTM/IS 2007 publication

Slide 29/55

Part 2. Context-Based Policy Management

- Requirements and limitations of existing approaches
- Context-aware management domains
- Validation results
- Conclusions

Slide 30/55

Context-Based Policy Management

- Authorization and Obligations policies
- Policies that are personalized to the user situation
- Example: patient being treated in a hospital

Slide 31/55

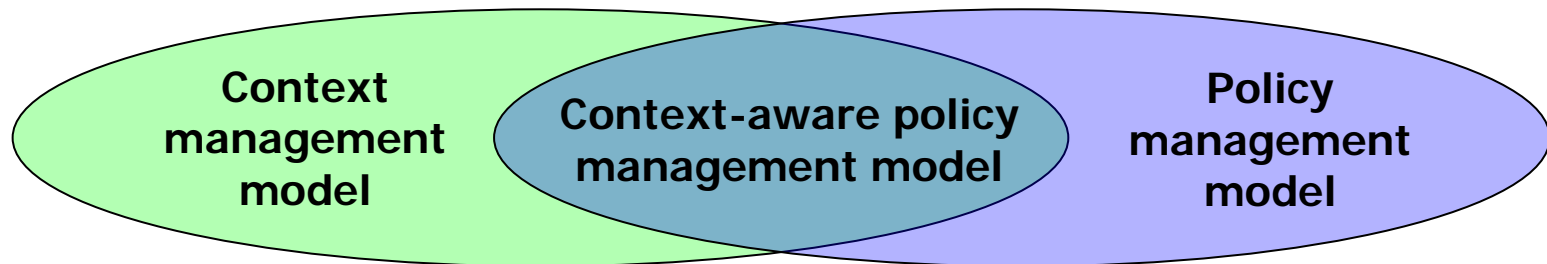
Limitations of Existing Approaches

- Static management of policies, entities are unknown at policy specification time
- Context-based solutions focus on at most one area:
 - eXtensible Role Based Access Control
 - Context-aware trust management
- Attribute-based context-aware policies poorly support obligations, events, and temporal constraints (Location = X, Activity = Y)
- No support for personalized context-based policies

Slide 32/55

Our proposal

- New concept called: Context-Aware Management Domains (CAMDs)
- Combines a situation based context model with a policy management model
- Enables flexible context-aware policy management



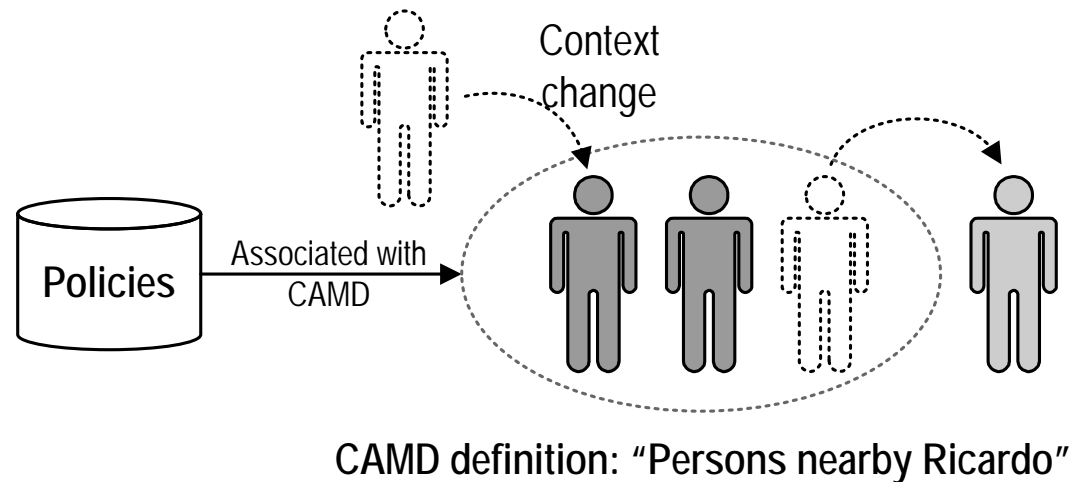
Slide 33/55

Context-Aware Management Domains

Specialization of Ponder2

Support for Context-Based Usage Control

- Authorizations and Obligations



Slide 34/55

Policy example using CAMDs

- When a patient is having a seizure, nearby caregivers should be authorized to access his/her location and health data
- All the patient data accessed by the caregiver should be deleted afterwards
 - Context situation of interest: Seizure
 - Events: EnterTrue/False(Seizure)
 - Entities: Patient, Nearby Caregivers
 - Policies: authorization and privacy obligation

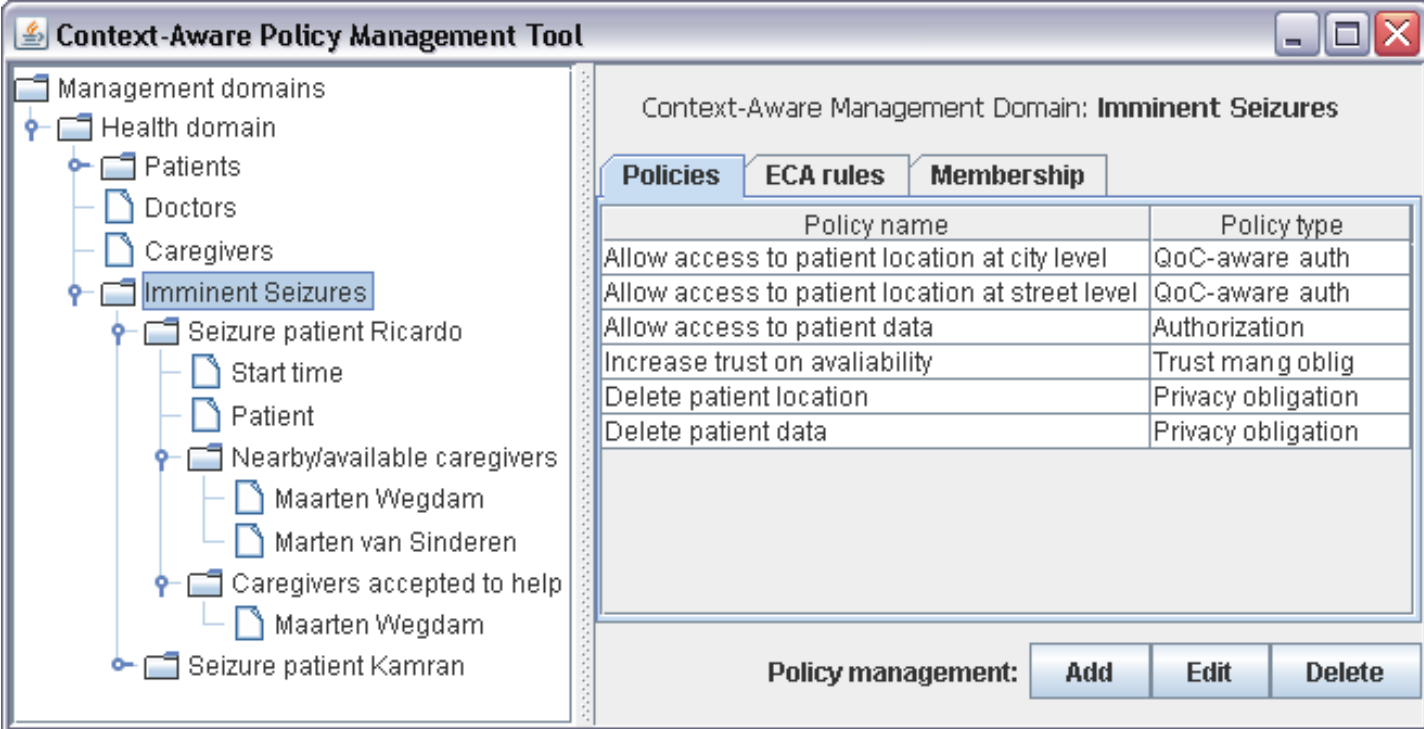
Slide 35/55

Validation

- Implementation using Ponder2 and XACML
- Different levels of granularity for policy specification
 - Allow/deny all
 - Templates (context-based)
 - Template editor
- Templates defined based on interview with users of a context-aware service
- Quiz mechanism to check if users understand their policies
- Policy conflict/overlap mechanism
- **User survey to validate usability and usefulness**

Slide 36/55

Implementation – Ponder2



Context-Aware Policy Management Tool

Context-Aware Management Domain: **Imminent Seizures**

Management domains

- Health domain
 - Patients
 - Doctors
 - Caregivers
 - Imminent Seizures**
 - Seizure patient Ricardo
 - Start time
 - Patient
 - Nearby/available caregivers
 - Maarten Wegdam
 - Marten van Sinderen
 - Caregivers accepted to help
 - Maarten Wegdam
 - Seizure patient Kamran

Policies ECA rules Membership

Policy name	Policy type
Allow access to patient location at city level	QoC-aware auth
Allow access to patient location at street level	QoC-aware auth
Allow access to patient data	Authorization
Increase trust on availability	Trust mang oblig
Delete patient location	Privacy obligation
Delete patient data	Privacy obligation

Policy management: **Add** **Edit** **Delete**

Slide 37/55

Implementation - XACML

The screenshot displays a web application interface with a sidebar on the left and a main content area on the right. The sidebar, titled "Buddies", shows the user's status as "Online" and privacy preferences set to "Everybody can see me". It also includes a "Buddy" list and "Add" and "Delete" buttons. The main content area features a 3D architectural rendering of a building complex, a small 3D building icon labeled "In building:", and a satellite map of a city street grid. The map includes navigation controls and a "Move map automatically" checkbox. The map shows streets such as "de Kotten", "Roessinghsbleekweg", "Lyceumlaan", "Minister Dr de Visserstraat", "Drienerweg", "Kotendijk", "Dauningersstraat", "Mekkeing", "Patrijss", "Hopstraat", and "Beekstraat".

Implementation - XACML

Your status is

Online

Privacy preferences

Everybody can see me
 Only buddies can see me

Click "Options..." for custom preferences

How you will appear to:

buddies

Privacy preferences

Everybody Buddies are allowed to see:

<input type="checkbox"/>	<input type="checkbox"/>	my location when I am inside the office building
<input type="checkbox"/>	<input type="checkbox"/>	my location when I am outside the office building during office hours
<input type="checkbox"/>	<input type="checkbox"/>	my location when I am outside the building during non office hours
<input type="checkbox"/>	<input type="checkbox"/>	my daily activities from outlook all the time

Specify your personalized privacy preferences in 3 steps and click "Include preference"

Steps:

1	When I am...	<input type="text" value="inside the building"/>	during	<input type="text" value="all the time"/>	<input type="button" value="..."/>
2	access to my ...	<input type="text" value="location"/>	<input type="text" value="in/out the building"/>	<input type="button" value="..."/>	
3	should be permitted to...	<input type="text" value="everybody"/>	when they ...	<input type="text" value="in any situation"/>	<input type="button" value="..."/>

Personalized preferences:

Access to my location(in/out the building) is allowed to everybody in any situation

User Survey



Survey Results

- 72% of the survey participants think they need personalized context-based policies
- 97% think they need a “privacy preview”
- 70% think the privacy quiz mechanism is useful
- We learned:
 - Requirements of context-based personalized policies that users would like to specify

Slide 41/55

Conclusions (end of part 2)

- Personalized context-based policy management
- Support for authorizations and obligations
- Different levels of granularity for policy specification
- POLICY 2008 paper

Slide 42/55

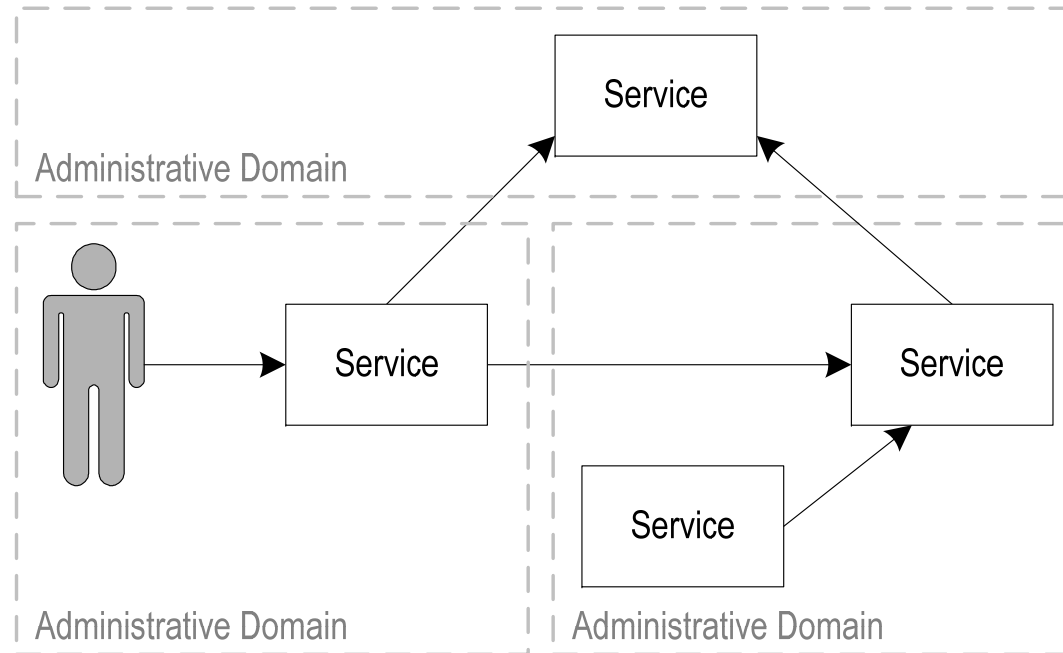
Part 3. Trust and policy management for SOAs

- Service oriented architectures
- Trust and policy management
- Trusted Computing Platform (TCP) support
- Functionalities and preliminary results
- Conclusions

Slide 43/55

Service Oriented Architectures (SOA)

- Outsourcing of services
- Enforcement of business policies and legal regulations
- Administrative domains have goals and trust requirements
- Long term goal is an open service market
- You need to trust the domains!



Slide 44/55

Example of Trust Goals and Decision Support

- Goals of end-users
 - Privacy (legal and social)
 - Reliability of service
- Goals of service providers
 - Contractual issues (legal)
- Validation based on an user survey
- Given a service composition, how to choose the more trustworthy entities with respect to the policy enforcement?

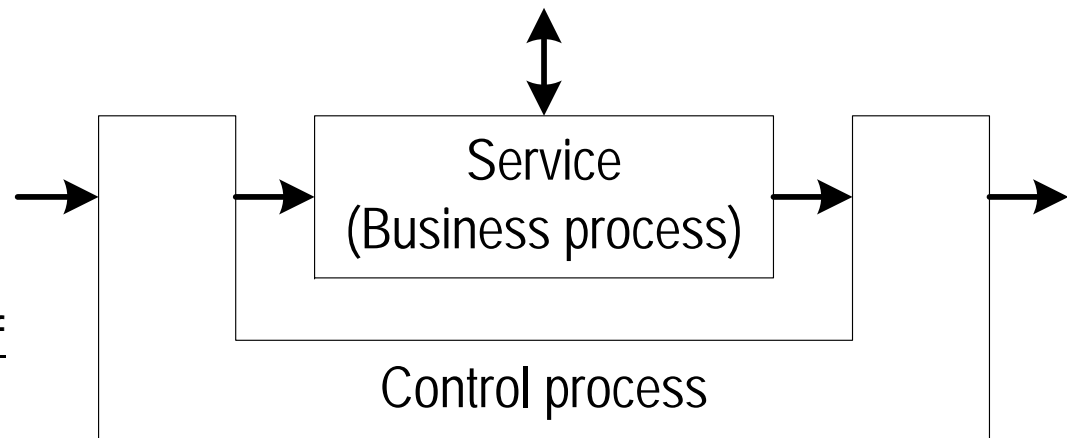
Slide 45/55

Trust and Policy Management in SOAs

Policies are enforced by a control process

Key assurance and security indicators

To verify the integrity of the control process in other administrative domains we need trusted computing!



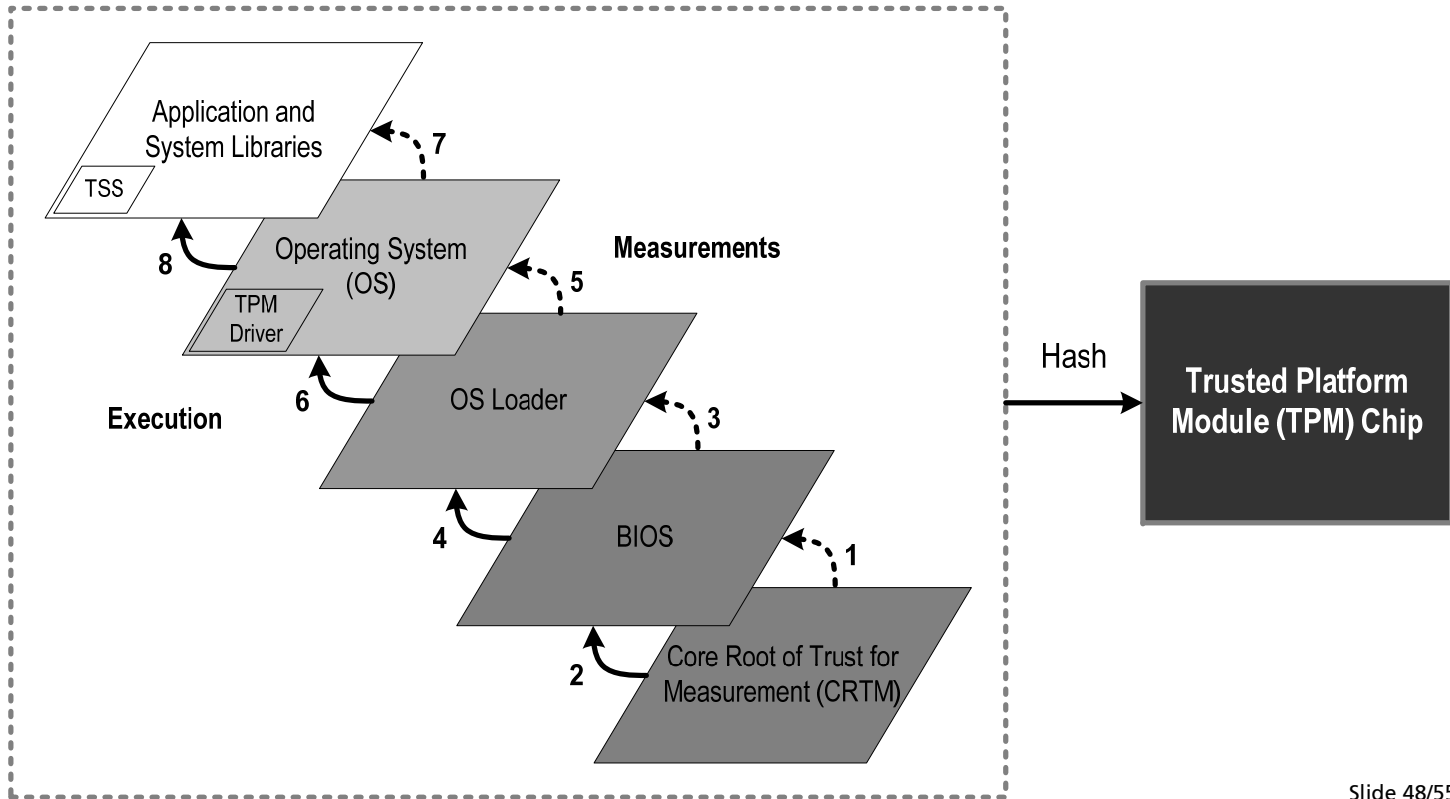
Slide 46/55

Chain of Trust

- Starts in the BIOS
- Sequence:
 - Hash of code is made
 - Hash is stored in the TPM chip
 - Control is passed to the hashed code
 - Hashing is cumulative, influenced by previous hashes
- Hashed values can be checked to see if the right configuration/code has been executed/loaded (attestation)



Slide 47/55

Chain of Trust – The Booting Process



Slide 48/55

Roots of Trust

- Core Root of Trust
 - for Measurement (RTM): BIOS or CPU
 - for Storage (RTS) 
 - for Reporting (RTR) 
- TPM chip protects RTS and RTR

Slide 49/55

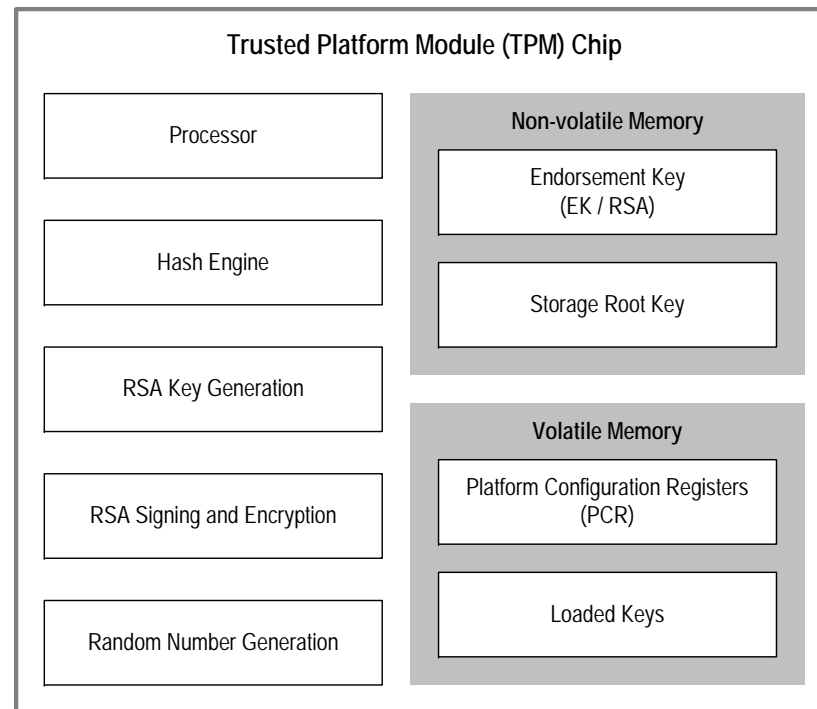
Key Trusted Platform Module (TPM) Functionalities

- Root of trust for storage and reporting
- Protection of key material: endorsement key
- System authentication
- Communication of the system's security status (attestation)
- Random number generation
- File sealing
- Secure saving of configuration changes in the Platform Configuration Registers (PCR)

Slide 50/55

Trusted Platform Module (TPM) Chip

- Passive, no influence in program execution
- Combination with OS maybe problematic
- It is not a cryptographic accelerator



Slide 51/55

Remote Attestation

- Allows detection of changes in the system properties to be detected at a distance by authorized parties
- System properties can be related to hardware or software components
- System properties measurements are stored in the PCR
- TPM signs a set of PCRs that should be interpreted by interested party (Key certification?)
- Discouraged in favor of Direct Anonymous Attestation (DAA) – Endorsement Key is unique

Slide 52/55

Preliminary Results

- Policy enforcement mechanism running in a OpenBSD virtual machine
- Using:
 - TPM emulator
 - Systrace framework for system calls interposition
- Policies specified for system calls executed by the users' processes

Slide 53/55

Conclusions (end of part 3)

- Trust management model supports decisions and risk analysis
- Practical use of Trusted Computing Platform to support concrete trust metrics for policy enforcement
- Has to be customized according to the stakeholder goals
- Integrity attestation is not enough, we need semantic/behavior attestation too
- Usage control and trust management patterns for SOA
 - Goals/tasks
 - Trust beliefs/metrics
 - Decision and risk analysis

Slide 54/55

Wrap-up and Discussion

- Contact information:
Ricardo Neisse
Ricardo.Neisse@iese.fraunhofer.de
<http://wwwhome.cs.utwente.nl/~neisser/>
- For further information you can check my thesis and our publications in my website

Slide 55/55
