SIPE'07

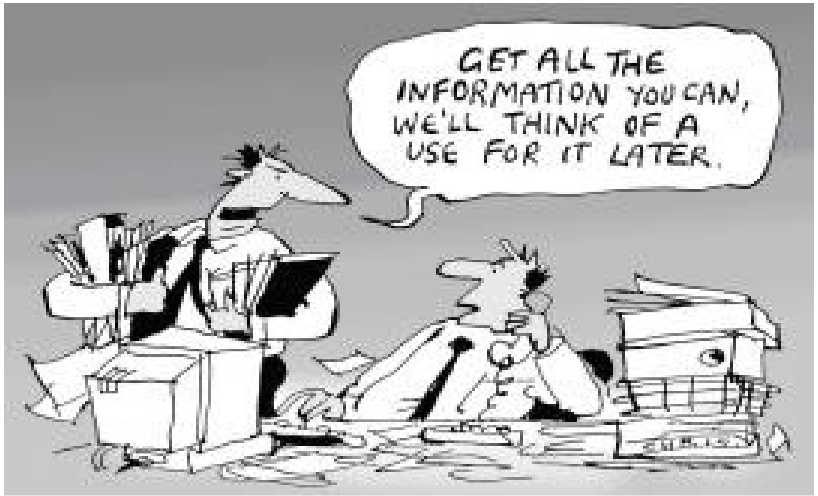
Privacy-Aware Service Integration

Pierre Parrend, Stéphane Frénot
pierre.parrend@insa-lyon.fr
Lab. CITI, 21, Avenue J. Capelle
69621 Vileurbanne Cedex, France

Sebastian Höhn
sebastian.hoehn@iig.uni-freiburg.de
Dept. of Telematics
University Freiburg (Germany)

Context

- Pervasive Systems
  - Personnalized Services Everywhere
  - Useful when combined together
- Data handling in Pervasive Systems


GET ALL THE INFORMATION YOU CAN, WE'LL THINK OF A USE FOR IT LATER.

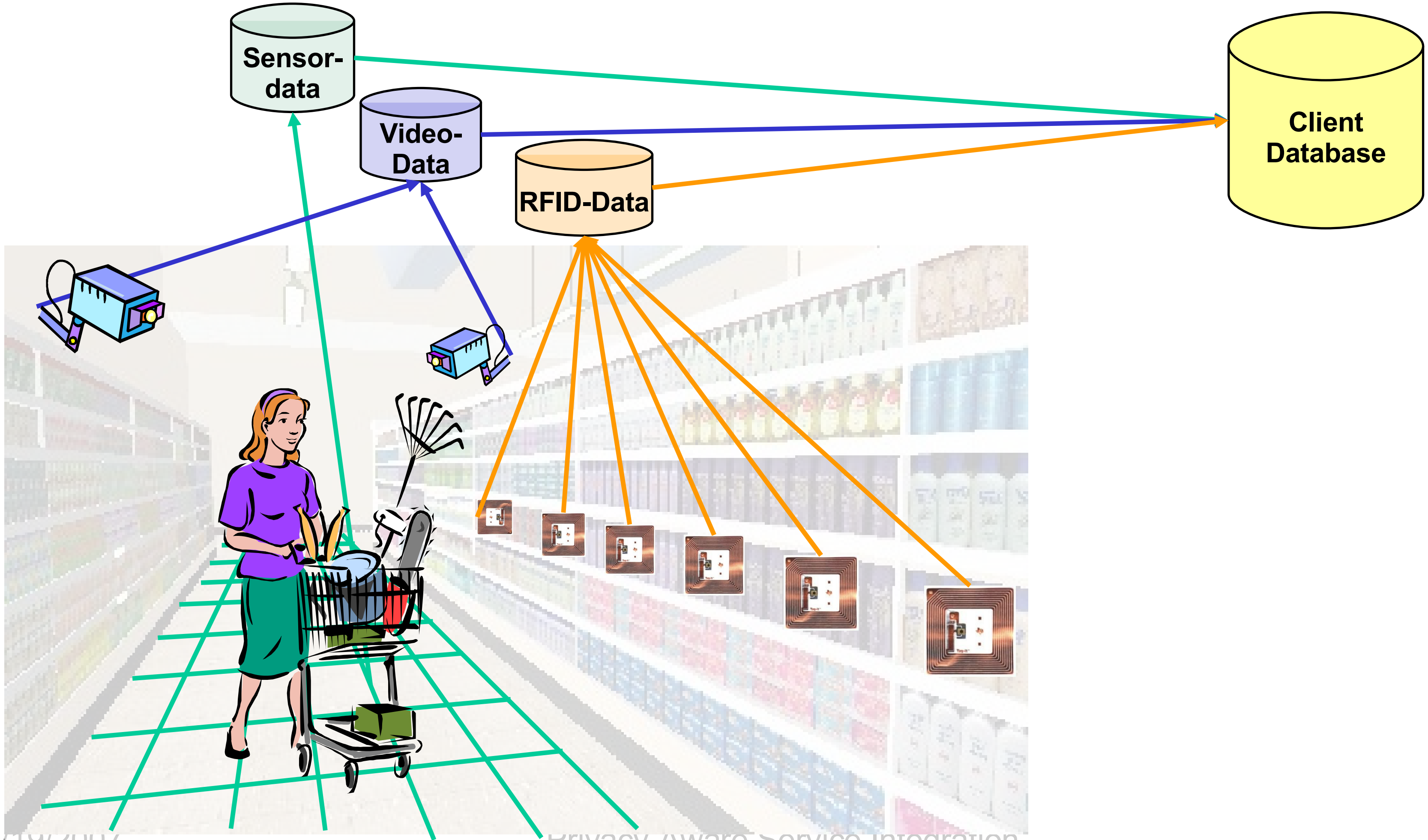
SIPE'07

A Framework for Privacy Aware Service Integration

- A vision of Pervasive Services
- Secure Architecture for Pervasive Service Provisioning
- Privacy Model
- System Requirements

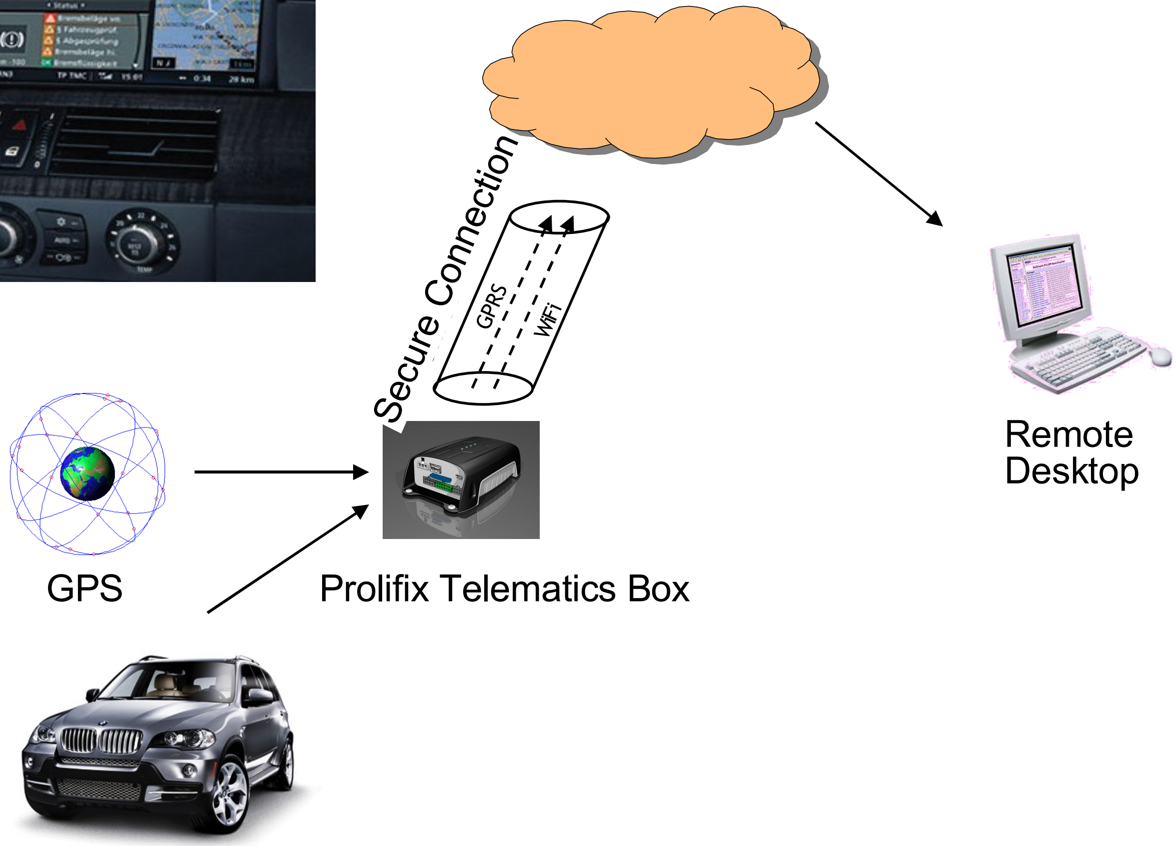
A Vision of Pervasive Services

- Use Case I: Intelligent supermarket



A Vision of Pervasive Services

- Use Case II: On-board Desktop



Secure Connection

GPRS

WiFi

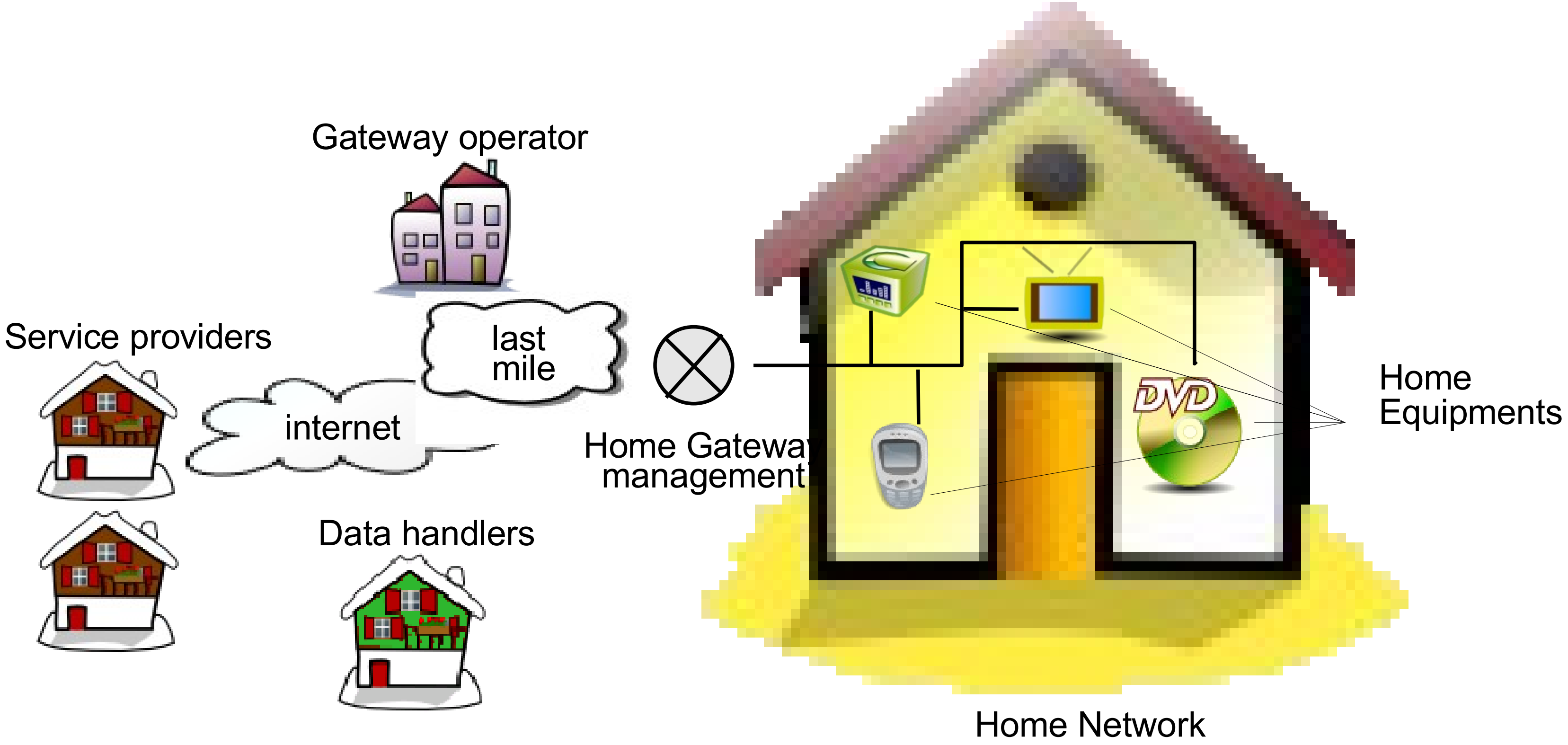
Remote Desktop

GPS

Prolifix Telematics Box

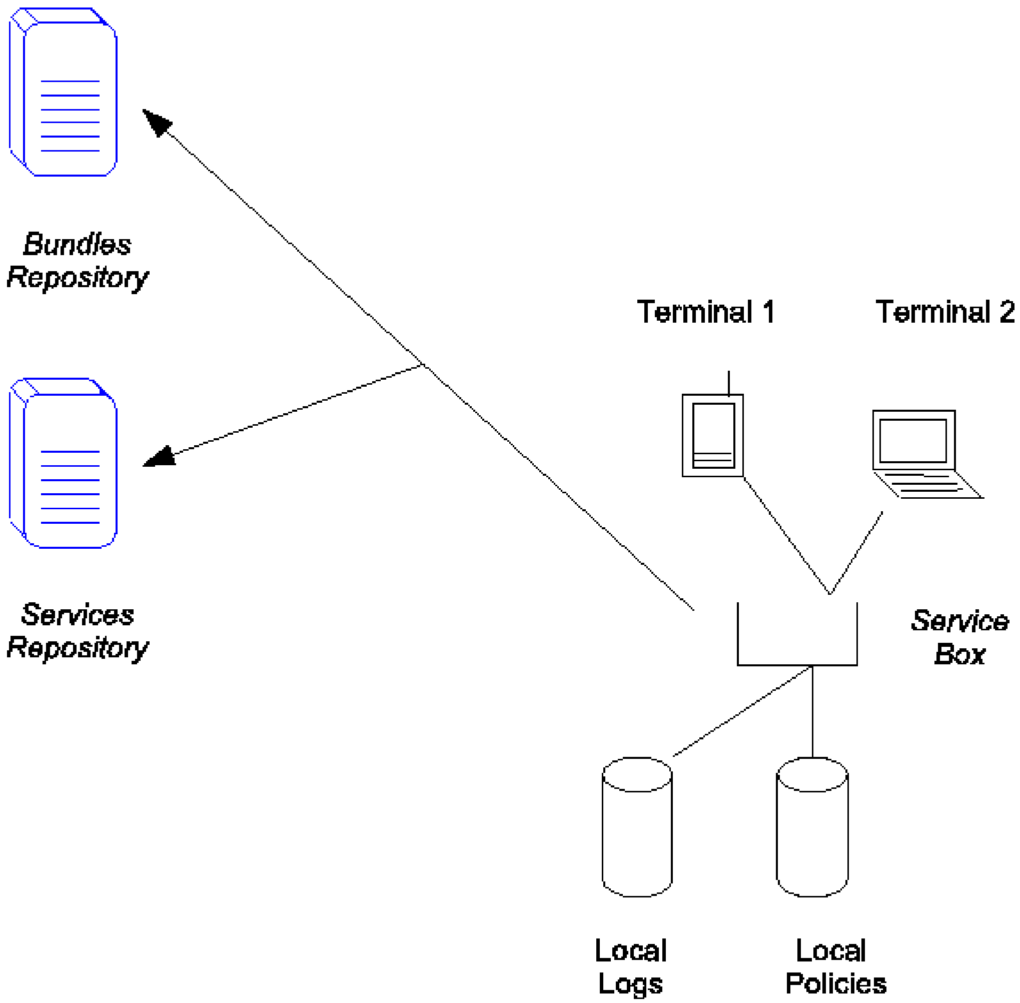
A Vision of Pervasive Services

- Use Case III: Smart Home



A Vision of Pervasive Services

- Architectural Overview



A Vision of Pervasive Services

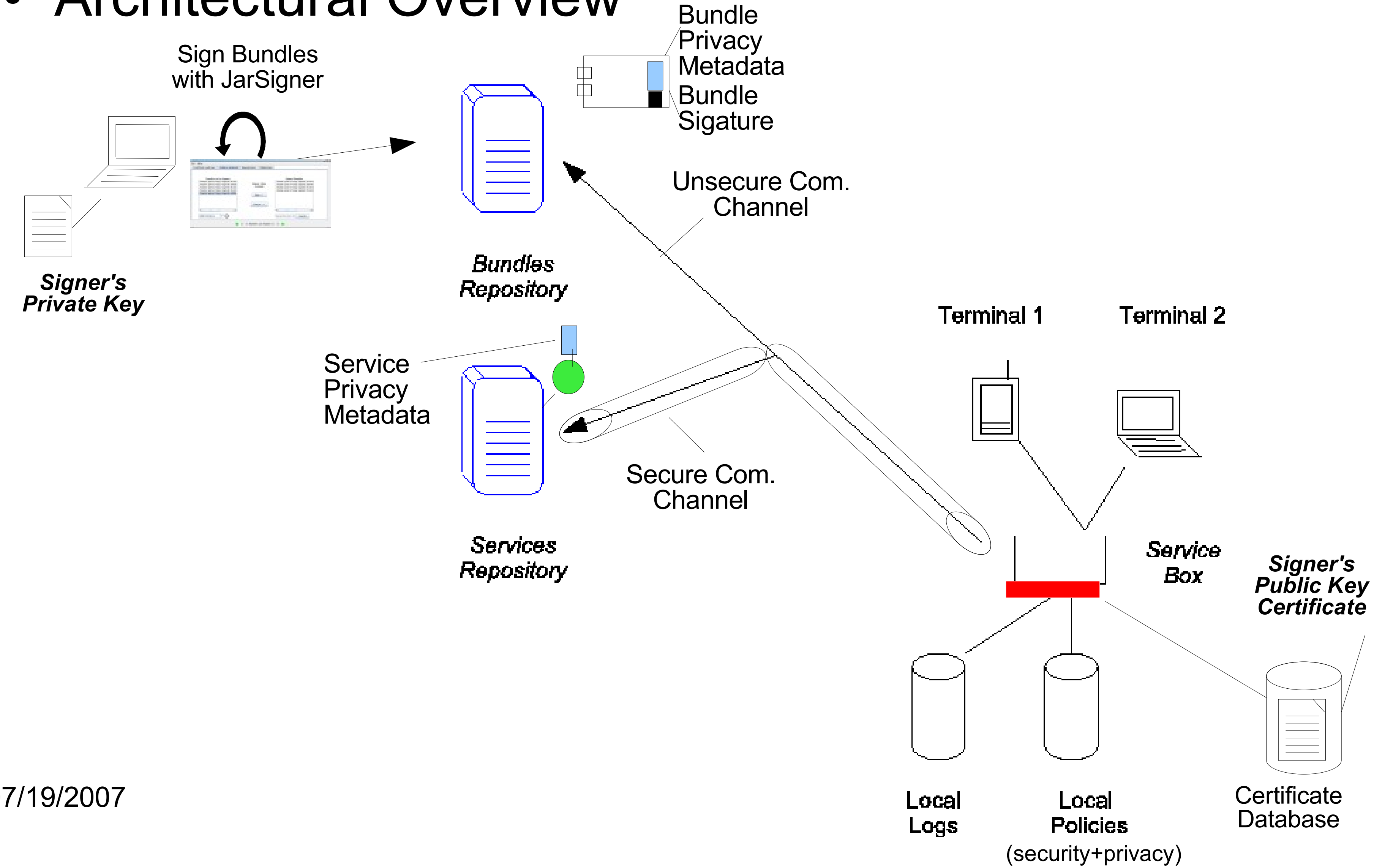
- Requirements for Privacy Aware Pervasive Services
  - No external Data Misuse – Secure Architecture
  - No internal Data Misuse – Privacy-friendly Services

Summary

- A vision of Pervasive Services
- Secure Architecture for Pervasive Service Provisioning
- Privacy Model
- System Requirements

Secure Architecture for pervasive Service Provisionning

- Architectural Overview



Sign Bundles with JarSigner

Signer's Private Key

Bundles Repository

Bundle Privacy Metadata

Bundle Sigature

Unsecure Com. Channel

Service Privacy Metadata

Services Repository

Secure Com. Channel

Terminal 1

Terminal 2

Service Box

Signer's Public Key Certificate

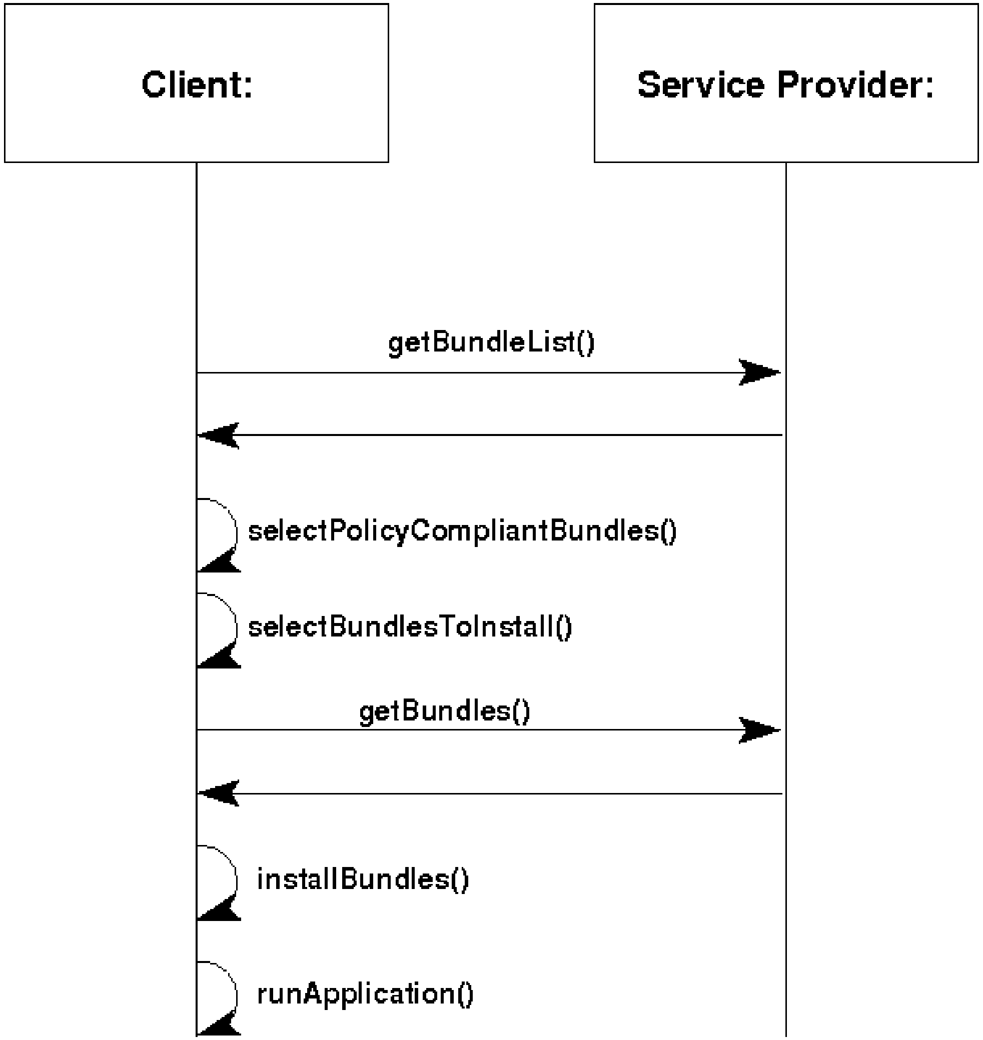
Local Logs

Local Policies (security+privacy)

Certificate Database

Secure Architecture for pervasive Service Provisionning

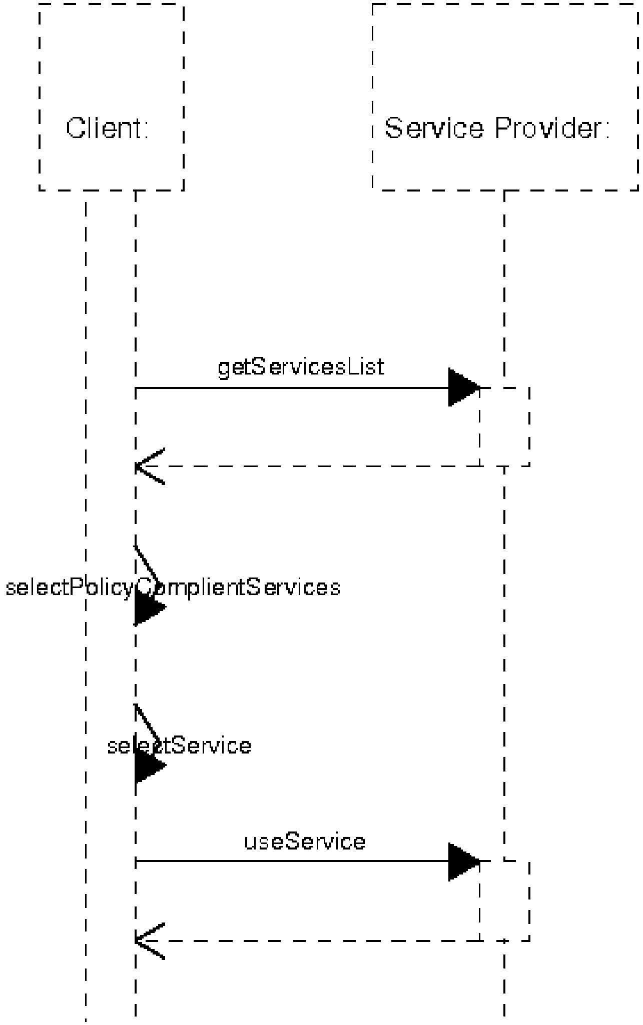
- Discovery Protocol for Bundles



Secure Architecture for pervasive Service Provisionning

SIPE'07

- Discovery Protocol for Services



Secure Architecture for pervasive Service Provisionning

- Security Analysis
  - Bundle Deployment
    - Bundle Digital Signature
    - Integrity, Authentification of the Publisher
    - No confidentiality
    - Client Side Control
  - Service Use
    - Secure Communication Channel, as SSH
    - Integrity, Authentication and Confidentiality must be checked at the server side AND at the client side

Summary

SIPE'07

- A vision of Pervasive Services
- Secure Architecture for Pervasive Service Provisioning
- Privacy Model
- System Requirements

SIPE'07

Privacy Model

- Formal Foundations
  - Missing Semantics:
    - Attributes and associations to individuals
    - The context in which they are processed and evaluated
  - Requirements (for practical applicability)
    - Handling of non-static spreading of information
    - Distributed modeling
    - Information gathering through data-mining

Privacy Model

- Formal Foundations
  - Users Id – the users
  - Actions Act_i – the services
  - Attributes A – the data that is gathered about a user by a service
  - Production Rules: to identify data mining risks
    - $R_p \subseteq Set(A_{available}) \times Set(A_{deduced})$

Privacy Model

Building blocks for implementation

- Services and actions
- Users
- Data Attributes
- Administrative Domains

Definition of Privacy-Aware Partial Policy

- Well-defined set of actions
- Data attributes
- Administrative Domains and their trust-level

Summary

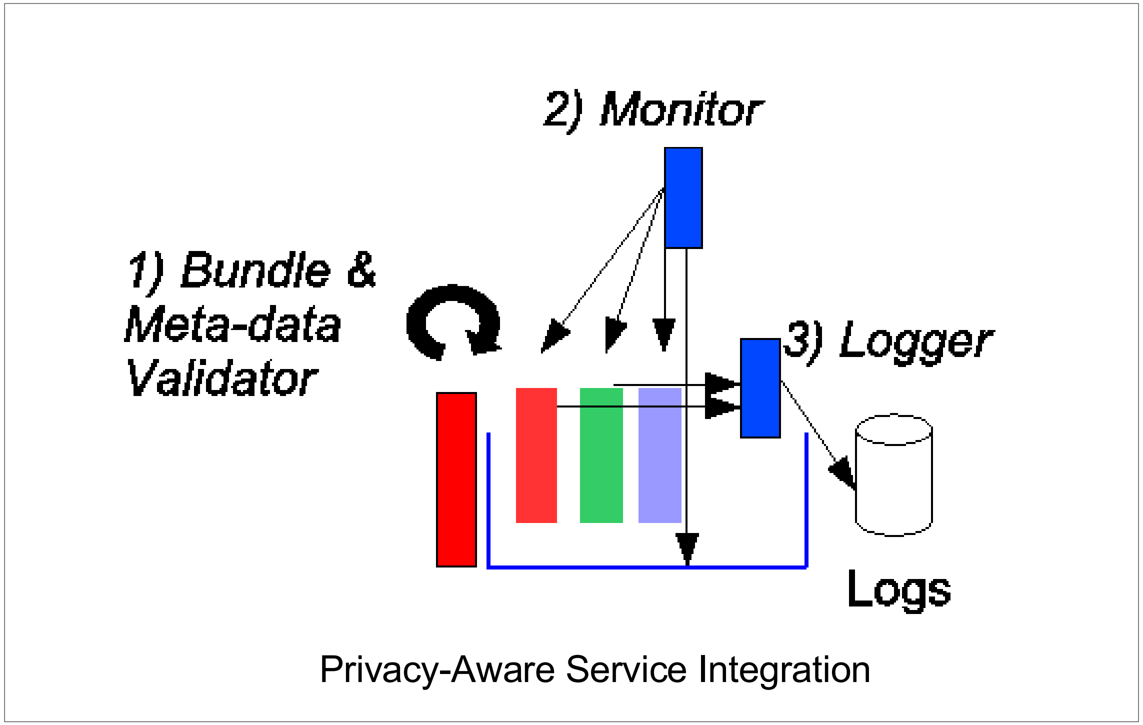
- A vision of Pervasive Services
- Secure Architecture for Pervasive Service Provisioning
- Privacy Model
- System Requirements

System Requirements

- Remote Service Implementation
  - Openness and Transparency
    - Users can observe the fulfilment of privacy policies
    - Technically unaware people can rely on others
    - like Open-Source approach
  - Enforcement rather difficult (according to Hilty, 2005)
    - Enforceable obligations
    - Observable obligation
    - Other obligations
  - Human actions are required
    - Service certification – before release
    - Service audit – during runtime, and in case of court trial

System Requirements

- User Platform
  - 3 steps-control: validation during installation, monitoring, and logging
  - Sandboxing: Java Permissions, Virtual OSGi for multi-provider support



System Requirements

- Isolation between Bundles for Privacy policy enforcement
  - Services are bound to a privacy profile
    - which bundles are allowed to access it
    - which bundles it is allowed to access
    - specific rights (see services/use service)
  - Through OSGi Services only (no package-level access)
  - All Services provided by a given bundle must share the same privacy profile
  - OSGi Service Permission not sufficient
    - Do not take the privacy meta-data into account

System Requirements

- Isolation between Bundles for Privacy policy enforcement
  - OSGi Context must be modified to allow access to authorized services only: definition of 'RestrictedContext', which contains a policy driven filter that can not be modified by the bundles (better performance)
    - OR
  - Service Conditionnal Permissions must be extended to take the privacy model into account (slight extension of the current specification)

Conclusions

- Contribution
  - Framework for privacy aware service integration
  - Privacy meta-data part of the bundle/service meta-data
    - Privacy aware service integration can be performed as other types of service integration
  - System requirements
- To be done
  - Integration of the model with the use cases

CITI

INRIA RHÔNE-ALPES

IIG

SIPE'07

Questions ?

© Cartoonbank.com

"Would you like to purchase a videotape of your transaction?"

GOOD AFTERNOON MR. HENFENNEL! HEMORRHOID CREAM AISLE SIX!
Beep!
TOO MUCH INFORMATION IN MY MEDICAL I.D. CHIP.
DON'T FORGET MOUTHWASH. I FIGURED THAT ONE OUT BY MYSELF.
TOLES
©2004 THE WASHINGTON POST