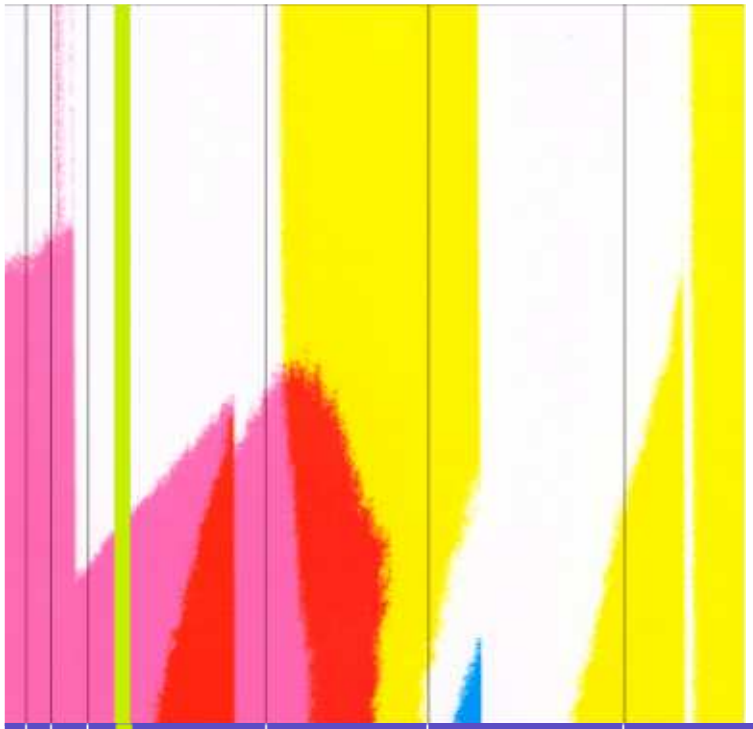


PRIAM
Architecture Meeting

25-26/10/2007

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA
RHÔNE-ALPES

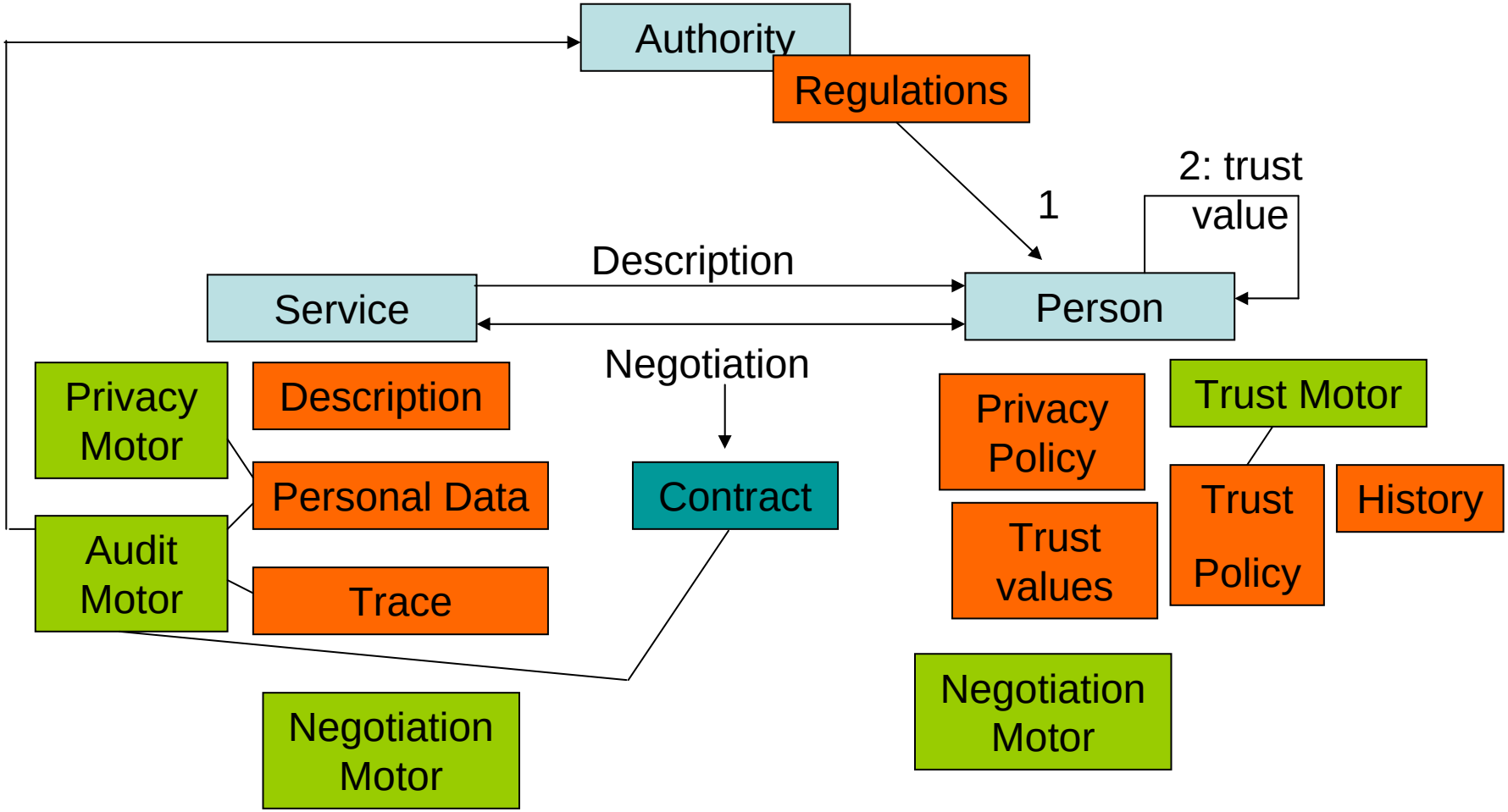
Plan

1. Architecture Principles
2. Functional Architecture
3. Technical Architecture
4. Partners' Contributions
5. Technical Choices
6. Scenario
7. Architecture Paper Plan
8. Next Workshop Meeting

Architecture Principles

- Distributed Architecture
  - Peer-to-peer support
  - Central server support
- Service-Oriented Architecture
  - Service-to-service communications
  - Service Trust
  - Service Negotiation
- Hardware Constraints
  - Wireless Communications
  - Resource-constrained Devices
  - Trusted Platform Module
- Formal Model
  - Model Checking
  - I/O Logging

Functional Architecture



Functional Architecture

- Authority Regulations
  - Law rules
    - Conservation, destruction time limit
    - Use of data
    - …

(State of the Art

- Privacy versus Regulation

cf. Discretionary v Mandatory in BLP

)

Functional Architecture

- Person Privacy Policy (Composable)
  - Complete Anonymization
  - Non-divulgation to 3rd party
  - Time-limited Data Holding
  - Notification of Use Policy
  - Confidence-rated Policy
  - Service-class Use Policy (Non-commercial e.g.)
  - Exclusive Use Policy (To avoid cross-referencing)
  - No Privacy Policy
  - …

- Privacy Language to define to build the Regulation and the Service Description (Privacy Policy)
  - Variables: mapping of law rule to functional definition (personal->IP, …)
  - Operators: storage (variable, time), destruction (variable)

Functional Architecture

- Service Negotiation Motor
  - Description ↗↘ (+,-)
  - Privacy Policy ↗↘ (Boolean logic, fuzzy-preference-modal operator)

  - Goal: description evolution to reach a contract

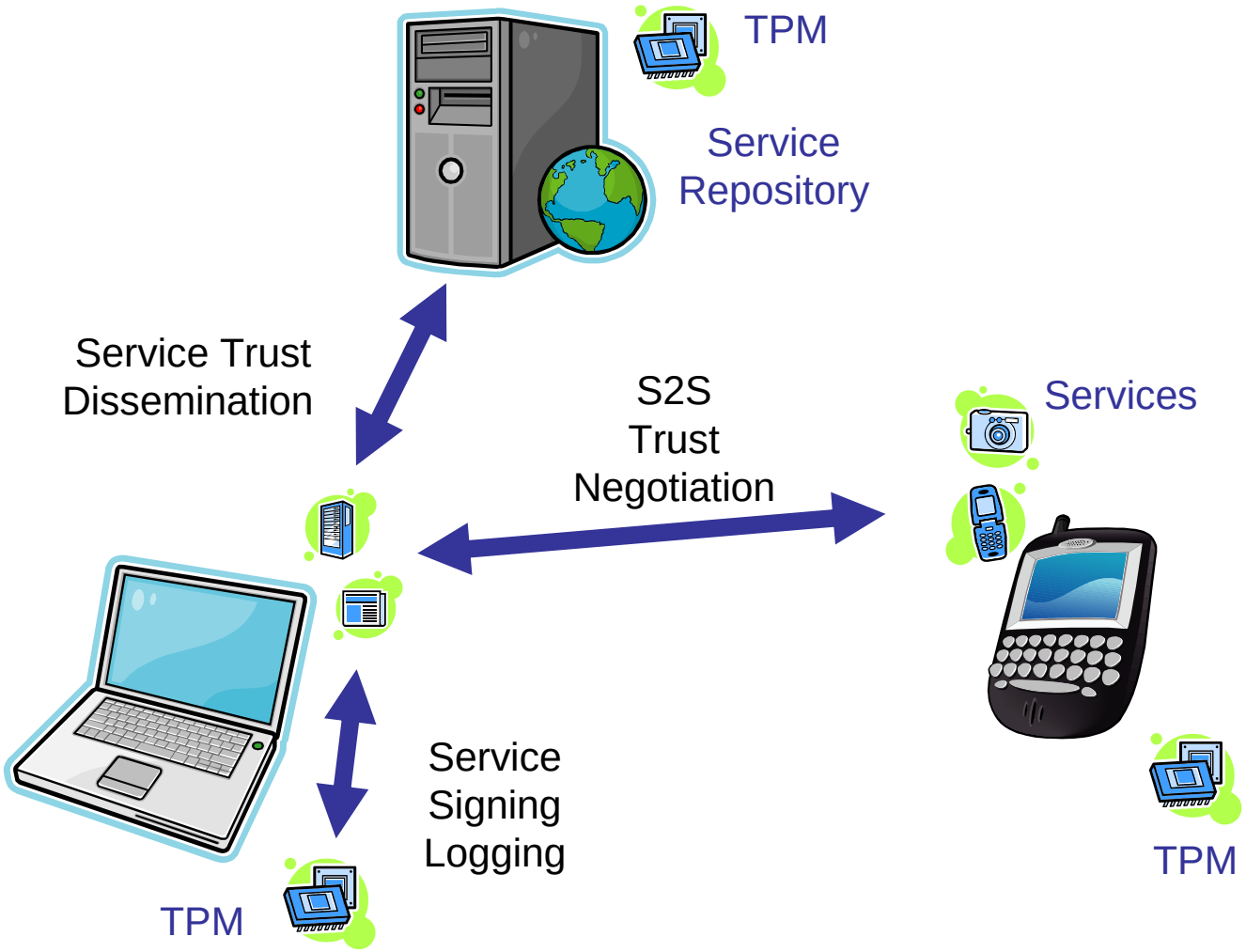
Functional Architecture

- Service Audit Motor
  - Mandated by the Authority
  - Contract Respect Checking
    - Inputs: Trace, Personal Data, Obligations, Contracts
    - Contracts respect Regulations
    - Trace respects Contracts
    - Outputs: All regulations and traces not respected
  - PRIAM-compliant System
- Service Audit Motor
  - Rules: to check conformance between contract (express by the privacy language) and the trace (technically expressed)
- Service Trace
  - I/O on Services (Description, Contract, Personal Data)

Open Issues

- Service Audit Interpretor ?
  - To (eventually) reuse Audit results into the Trust calculation (matching level)
- Model Checking
  - Checking of the Audit ?
  - How to express the policies ? P3P, XML ?

Technical Architecture



Partners' Contributions

1. Service-Oriented Architecture – INRIA ARES
   - Service Model, S2S Negotiation (Frédéric)
   - Service Trust, Dissemination (Marine, Frédéric)
2. Device and Trusted Platform Module – INRIA ACES
   - Service Signing (Ciarán)
   - Cryptography level (Marine)
3. Formal Model – INRIA Pop Art, University of Twenty
   - Logging decision/legal aspect (Daniel)
   - Logging Service (Frédéric)
   - Model Checking (Marnix, Sandro)

Technical Choices

1. Service-Oriented Architecture – INRIA ARES
   - Service Model (Frédéric)
     - Java/OSGi Services vs C#(or else)/.net WebServices
   - S2S Trust Negotiation (Frédéric)
     - Model published in 4th Workshop for Ubiquitous Networking and Enablers to Context-Aware Services" held at UCS2007, Akihabra, Tokyo
   - Service Trust Dissemination (Marine)
     - Linear Dissemination Model

   - On-going work (Frédéric, Marine)
     - S2S Trust Negotiation, code refactoring to fit the new service model
     - Service Trust Dissemination, implementation to do
     - All parts planed to be submitted to Joint iTrust and PST Conferences on Privacy, Trust Management and Security 2008, Trondheim, Norway

Technical Choices

2. Device and Trusted Platform Module – INRIA ACES
   - Service Signing (Ciarán)
     - PRIAM-compliant checking (all parts of the system)
     - TPM not use to compromise privacy (no backdoor)
   - Cryptography level (Marine)
     - SHA-1, random generator, RSA to sign contracts

Technical Choices

3. Formal Model – INRIA Pop Art, University of Twenty
   - Legal aspect (Daniel)
     - To fill
   - Logging Service (Frédéric)
     - Apache Logging Service
     - Fits with both Service Model: log4j for Java, log4net for the Microsoft .NET framework and a log viewer and analysis tool: Chainsaw
   - Model Checking (Marnix, Sandro, Daniel)
     - Checking of the Audit ?
     - To fill

Technical Details

1. Service-Oriented Architecture – INRIA ARES
   - Service Trust Dissemination (Marine)
     - Linear Dissemination Model

Associated Trust level

- A service requester asks the registry for a given service, it receives the description of the service and the associated trust rate
- It computes its own trust note according
  - its own history : $T^{i}_{R}(P_1)$
  - the trust rate provided: $M_{T'_i}(P_1)$

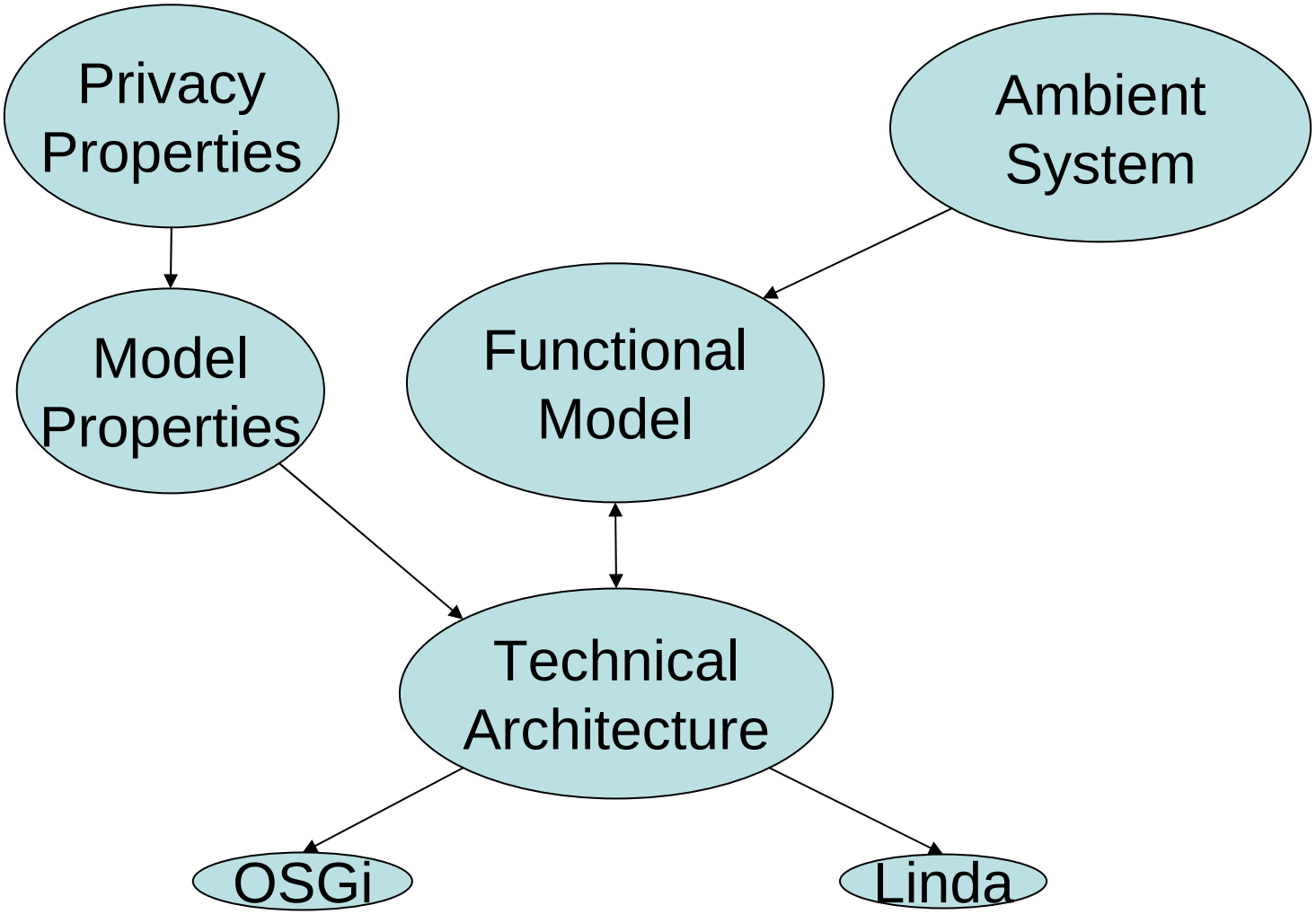
$$Note_R(T'_i, P_1) = \delta_{registry}\, M_{T'_i}(P_1) + (1 - \delta_{registry})\, T^{i}_{R}(P_1)$$

$\delta_{registry}$ depends if the service requester R trusts the corresponding registry

Scenario

- E-commerce
  - Fridge: Food Inventory Service
  - PDA: Shopping List Service
  - Shop: Navigation Service, Advertisement Service, E-Payment Service
  - Bank: Account Service

Paper Collaboration Plan



Next Workshop Program

- Thematic:
  - PRIAM Architecture talk
  - ARES Trust talk
  - ACES QoSecurity
  - HP TPM talk