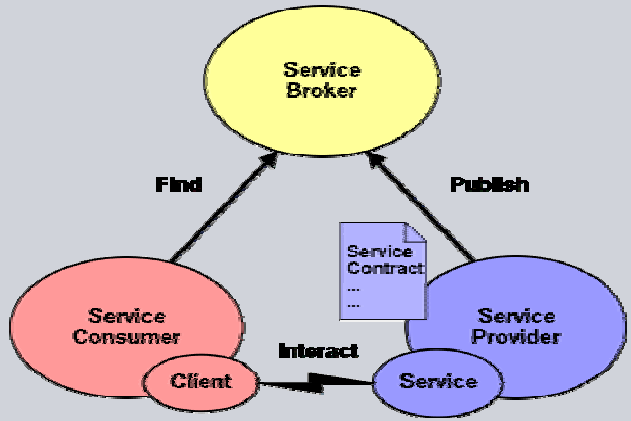
SIEMENS

AVANTSSAR – an overview with examples

avantssar.eu



Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures

EU FP7-2007-ICT-1, ICT-1.1.4, Strep project no. 216471

Jan 2008 - Dec 2010, 590 PMs, 6M€ budget, 3.8M€ EC contribution

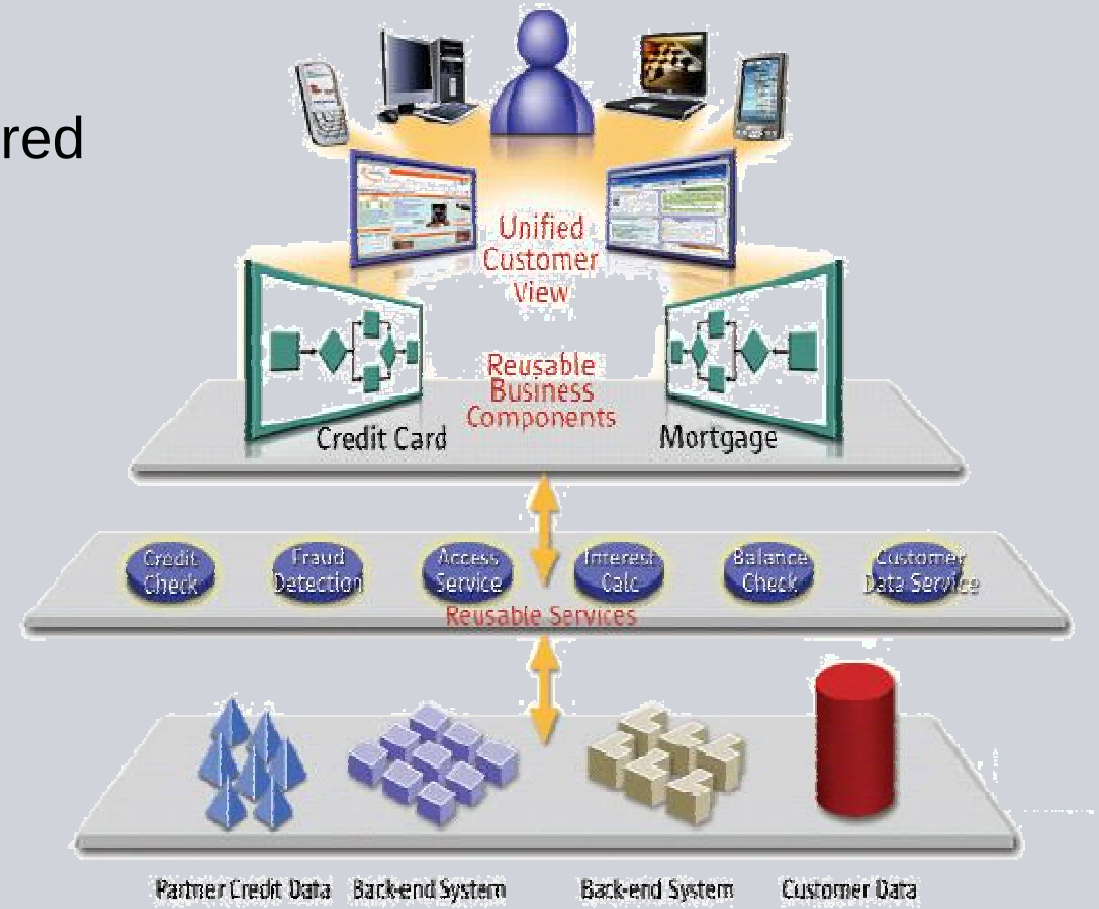
Presented at GI FoMSESS Annual Meeting, Berlin, Germany, 2010-04-27

AVANTSSAR project motivation

ICT paradigm shift: from components to services, composed and reconfigured dynamically in a demand-driven way.

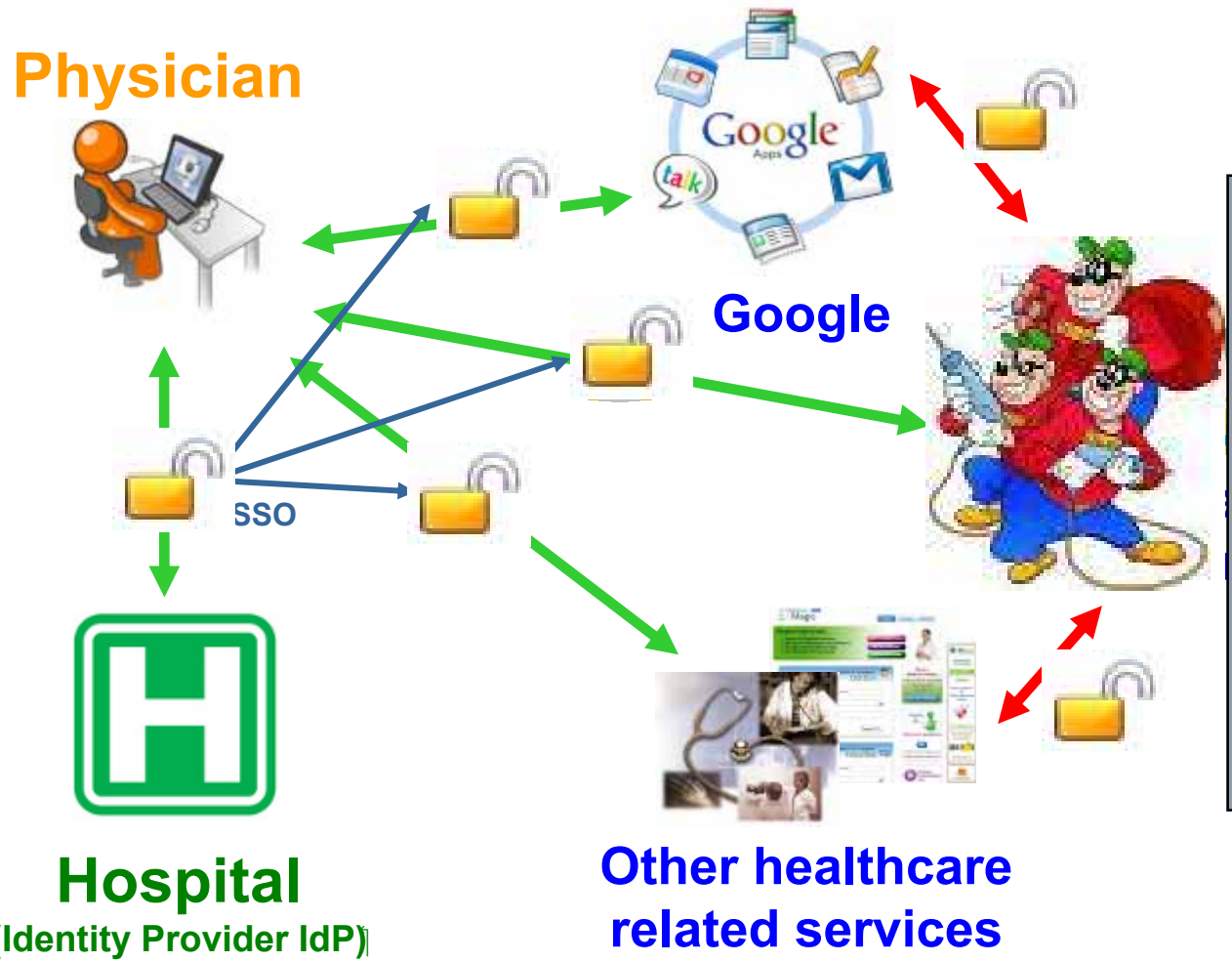
Trustworthy service may interact with others causing novel trust and security problems.

For the composition of individual services into service-oriented architectures, validation is dramatically needed.



SIEMENS

Example 1: Google SAML-based Single Sign-On (SSO)



A malicious service provider can access the data of the physician located at all other services connected via Google SSO

Example 1: Google SAML SSO protocol flaw

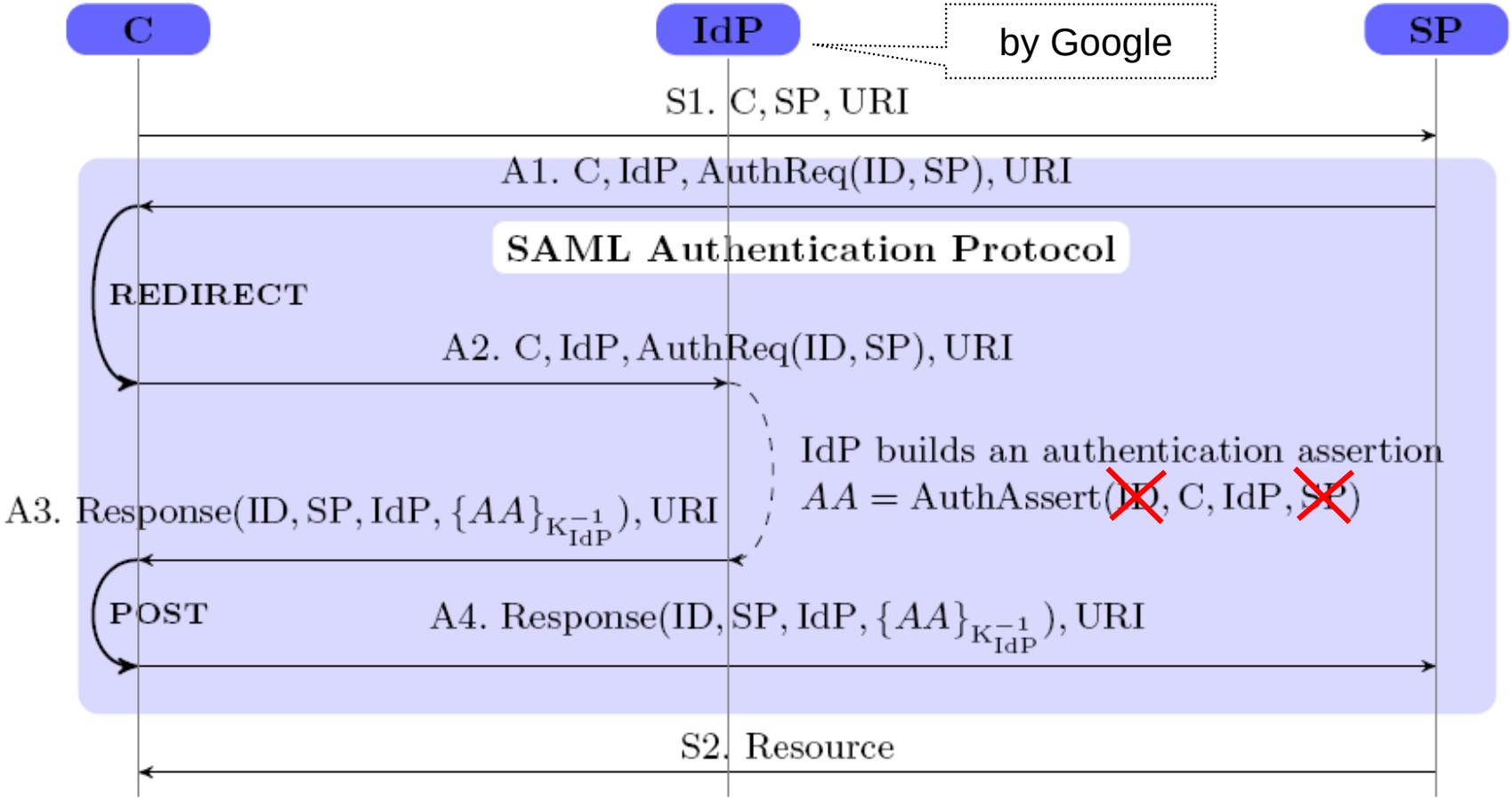


Fig. 1. SP-Initiated SSO with Redirect/POST Bindings

AVANTSSAR consortium

SIEMENS

Industry

SAP Research France, Sophia Antipolis

Siemens Corporate Technology, München

IBM Zürich Research Labs (part time)

OpenTrust, Paris

Academia

Università di Verona

Università di Genova

ETH Zürich

INRIA Lorraine

UPS-IRIT Toulouse

IEAT Timisoara

Expertise

Service-oriented enterprise architectures

Security solutions

Standardization and industry migration

Security engineering

Formal methods

Automated security validation

AVANTSSAR main objectives and principles

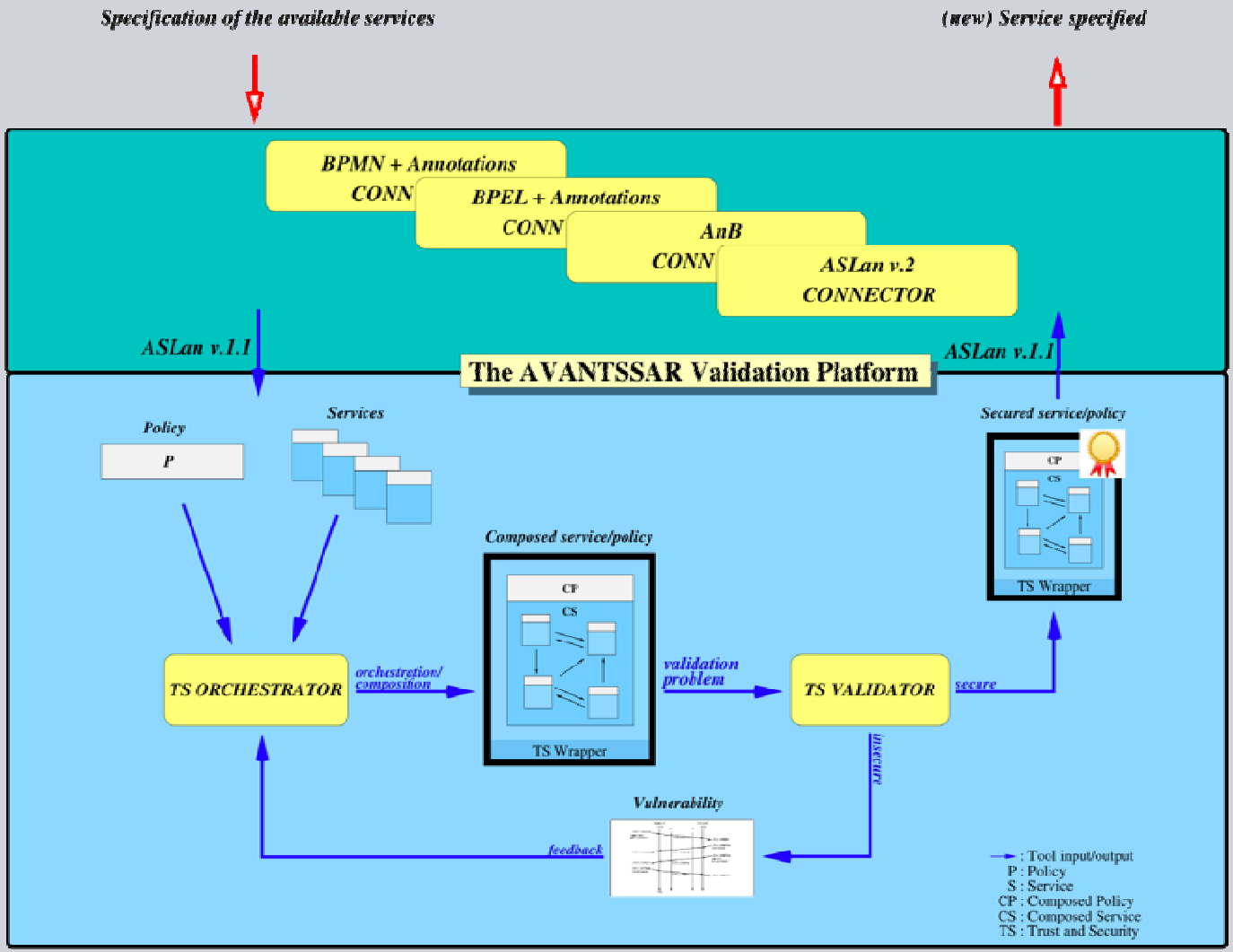
AVANTSSAR product: Platform for formal specification and automated validation of trust and security of SOAs

- Formal language for specifying trust and security properties of services, their policies, and their composition into service-oriented architectures
- Automated toolset supporting the above
- Library of validated industry-relevant case studies

Migration of platform to industry and standardization organizations

- Speed up development of new service infrastructures
- Enhance their security and robustness
- Increase public acceptance of SOA-based systems

AVANTSSAR project results and innovation



SIEMENS

Example 2: Electronic Car Registration policies

local policy

RegOffCA can say
who is RegOffHead
who is RegOffEmpl

certificate

Peter is RegOffEmpl
of CarRegOffice
(signed by RegOffCA)

ACL

anybody,
get empty forms
RegOffHead, write
RegOffEmpl, read
RegOffEmpl, write,
if *his* RegOffHead
says so

CentrRep

write(..)

Peter

Melinda

RegOffCA

certificate

Melinda is RegOffHead
of CarRegOffice
(signed by RegOffCA)

certificate

Peter can write
CentrRep
(signed by Melinda)

Question:

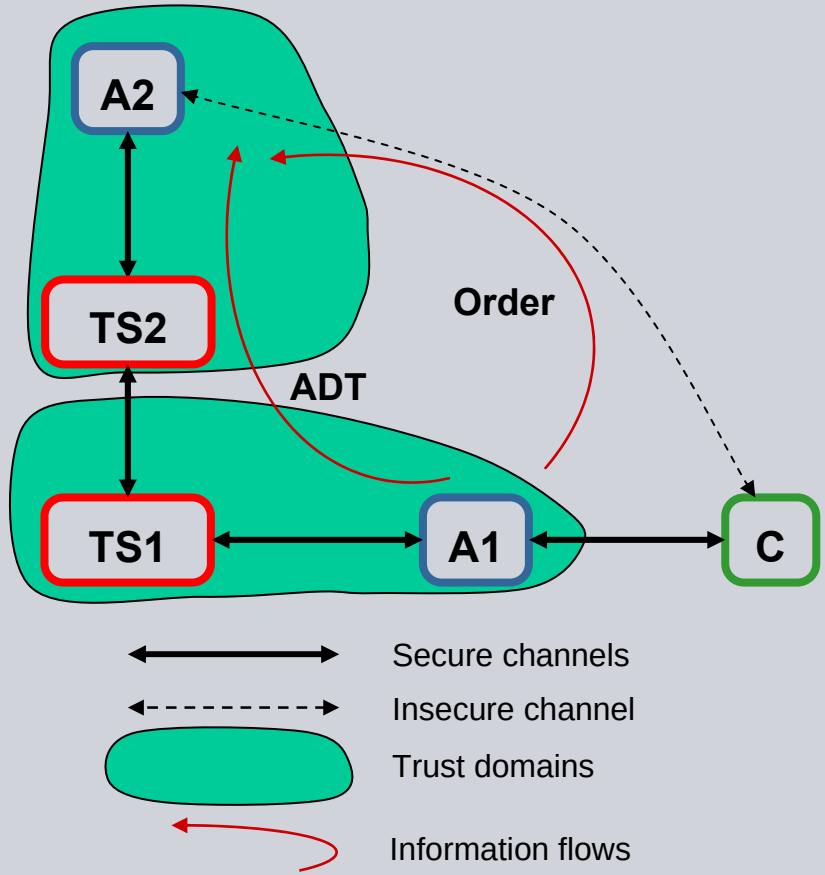
May Peter write to CentrRep?

Example 3: Process Task Delegation (PTD)

Authorization and trust management via token passing

- There are three roles in the protocol (**C, A, TS)** and potentially several instances for each role
- The *client* **C** (or *user*) uses the system for SSO, authorization and trust management
- Each *application* **A** is in one domain, each domain has exactly one active *token server* **TS**
- **A1** uses the system to pass to **A2** some **Order** and an **ADT (Authorization Decision Token)**
  - **Order** contains:
    - workflow task information
    - application data
    - information about the client **C** and his current activity

    to be delivered securely (integrity and confidentiality)
  - **ADT** is mainly authorization *attributes* and *decisions*
    - sent via **TS1** and **TS2**, who may weaken it
    - must remain unaltered, apart from weakening by **TS**
    - must remain confidential among intended parties
- **C**, **A1**, and **A2** must be authenticated among each other



Security prerequisites:

- PKI is used for **A** and **TS**, username & pwd for **C**
- **TS** enforces a strict time-out

Example 3: ASLan++ model of A2

```
entity A2 (Actor: agent, TS2: agent) {    % Applicaton2, connected with TokenServer2
  symbols
    C0,C,A1: agent;
    CryptedOrder, Order, Order0, Details, Results, TaskHandle, ADT, HMAC: message;
    SKey: symmetric_key;
  body { while (true) {
    select {
      % A2 receives (via some C0) a package from some A1. This package includes encrypted and
      % hashed information. A2 needs the corresponding key and the Authorization Decision Token.
      on (?C0 -> Actor: (?A1.Actor.?TaskHandle.?CryptedOrder).?HMAC): {
        % A2 contacts its own ticket server (TS2) and requests the secret key SKey and the ADT.
        Actor *->* TS2: TaskHandle;
      }
        % A2 receives from A1 the SKey and checks if the decrypted data corresponds to the hashed data
      on (TS2 *->* Actor: (?ADT.?SKey).TaskHandle  & CryptedOrder = scrypt(SKey,?,?Details.?C)
          & HMAC = hmac(SKey, A1.Actor.TaskHandle.CryptedOrder)): {
        % A2 does the task requested by A1, then sends to A1 via C the results encrypted with the secret key.
        Results := fresh();  % in general, the result depends on Details etc.
        Actor -> C: Actor.C.A1. scrypt(SKey,Results);
   }}}
  goals
    authentic_C_A2_Details: C  *-> Actor: Details;
    secret_Order: secret (Order, {Actor, A1});
}
```


AVANTSSAR current status

SIEMENS

WP2: ASLan++ supports the formal specification of trust and security related aspects of SOAs, and of static service and policy composition

WP3: Techniques for: satisfiability check of policies, model checking of SOAs w.r.t. policies, different attacker models, compositional reasoning, abstraction

WP4: Deploy first prototype of **AVANTSSAR Platform**

WP5: Formalization of **industry-relevant problem cases** as ASLan++ specifications and their validation

WP6: Ongoing dissemination and migration into scientific community and industry

AVANTSSAR impact: industry migration

Services need to be securely combined according to evolving trust and security requirements and policies.

A rigorous demonstration that a composed SOA meets the security requirements and enforces the application policy will:

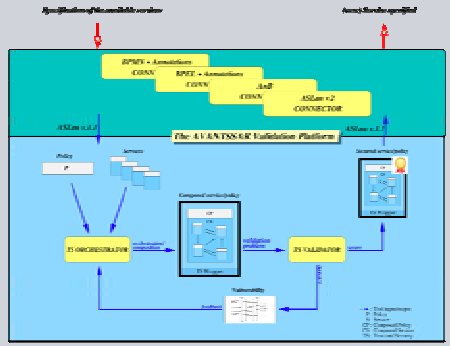
- significantly increase customers' confidence
- enable customers to fully exploit the benefits of service orientation

Integration of AVANTSSAR Platform in industrial development environment

The AVANTSSAR Platform will advance the security of industrial vendors' service offerings: validated, provable, traceable.

AVANTSSAR will thus strengthen the competitive advantage of the products of the industrial partners.

eBusiness



Portals

SW Dist

Health care

