



# **Daidalos Security - Innovation and Implementation**

## **Security in (M&W) Heterogeneous Networks**

**23rd September 2004, Brussels**

**Presented by  
Jim Clarke**





# Daidalos technical context

Within the context of IPv6 and mobile IP, the technical goals of Daidalos are to:

- Design, prototype and validate the necessary infrastructure and components for efficient distribution of services over diverse network technologies beyond 3G,
- Integrate complementary network technologies to provide pervasive and user-centred access to these services,
- Develop an optimized signalling system for communication and management support in these networks,
- Demonstrate the results of the work through strong focus on user-centered and scenario-based development of technology.





# Challenges

- ▶ Heterogeneous networks
- ▶ Network independence of services
- ▶ Ambitious service integration goals
- ▶ Broadcast service security
- ▶ Use of open standard protocols and technologies
- ▶ Interworking between service provider's security domains
- ▶ Optimum maximisation of usability and security
- ▶ Integration with Mobile IP
- ▶ Security embedded throughout the project
- ▶ Balance the service provider's and the user's needs



# Key areas of innovation in Daidalos security



- ▶ Vertical integration
  - Single sign-on
  - Bundling of application and network services
- ▶ Privacy and anonymity
  - Virtual ID protects real identity
  - Registration ID for billing etc.
- ▶ Simple user and service provider model.
  - Simple service registration
  - Broadcast and point-to-point services



# Daidalos work-package structure – the security effort

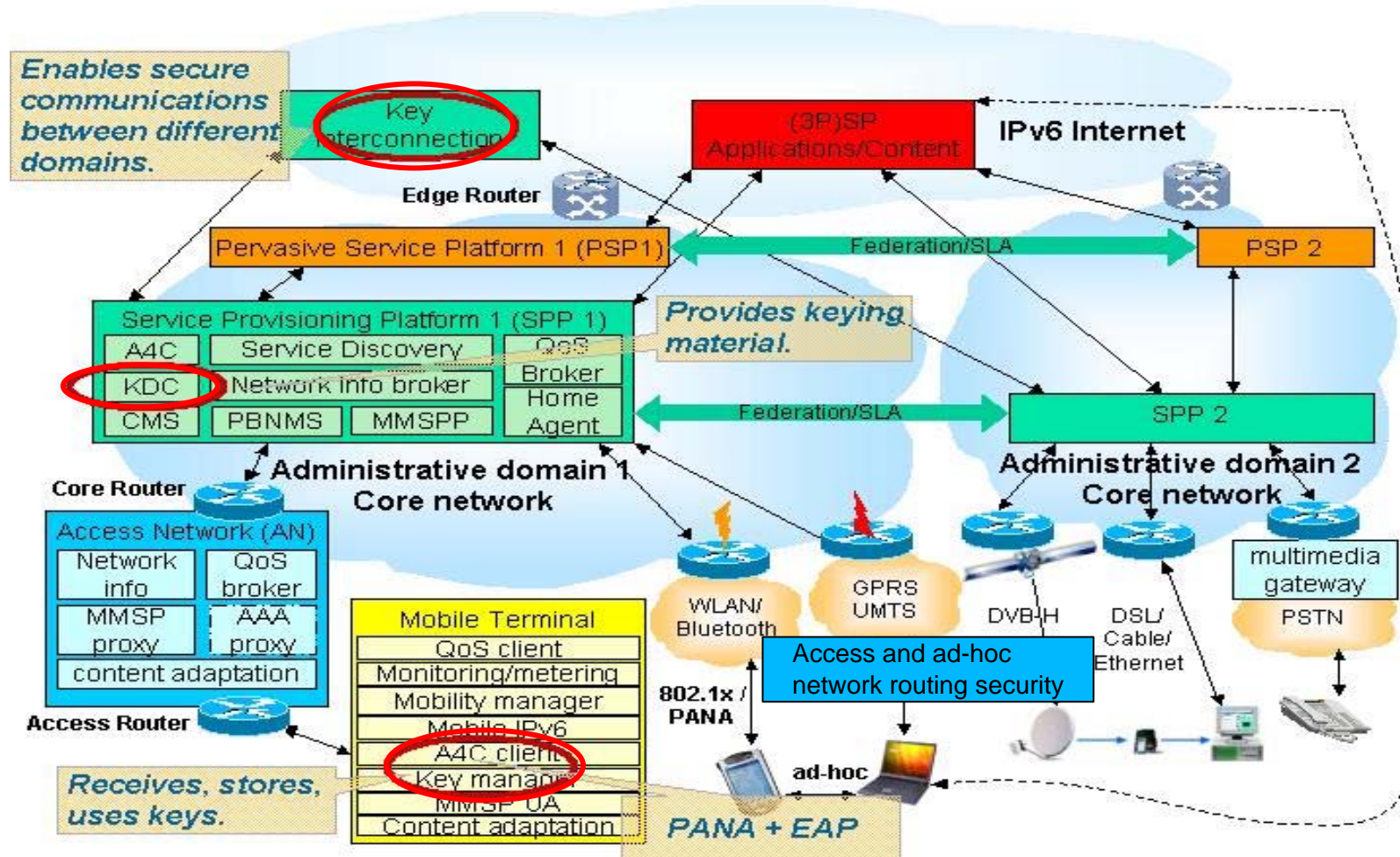


- ▶ WP1 Global architecture - Security is central to each of the work packages and is co-ordinated by a Vertical Security Team
- ▶ WP2 Network integration – Access network & link layer security and common cryptographic library
- ▶ WP3 Service and Network management – Network security & security portions of the Service Provisioning Platform
- ▶ WP4 Pervasive systems – Privacy Policy and Pervasive Service Security
- ▶ WP5 Integration System evaluation - ensures integration into the scenario use cases





# Daidalos Security Architecture



# WP2 Network integration - Security focus

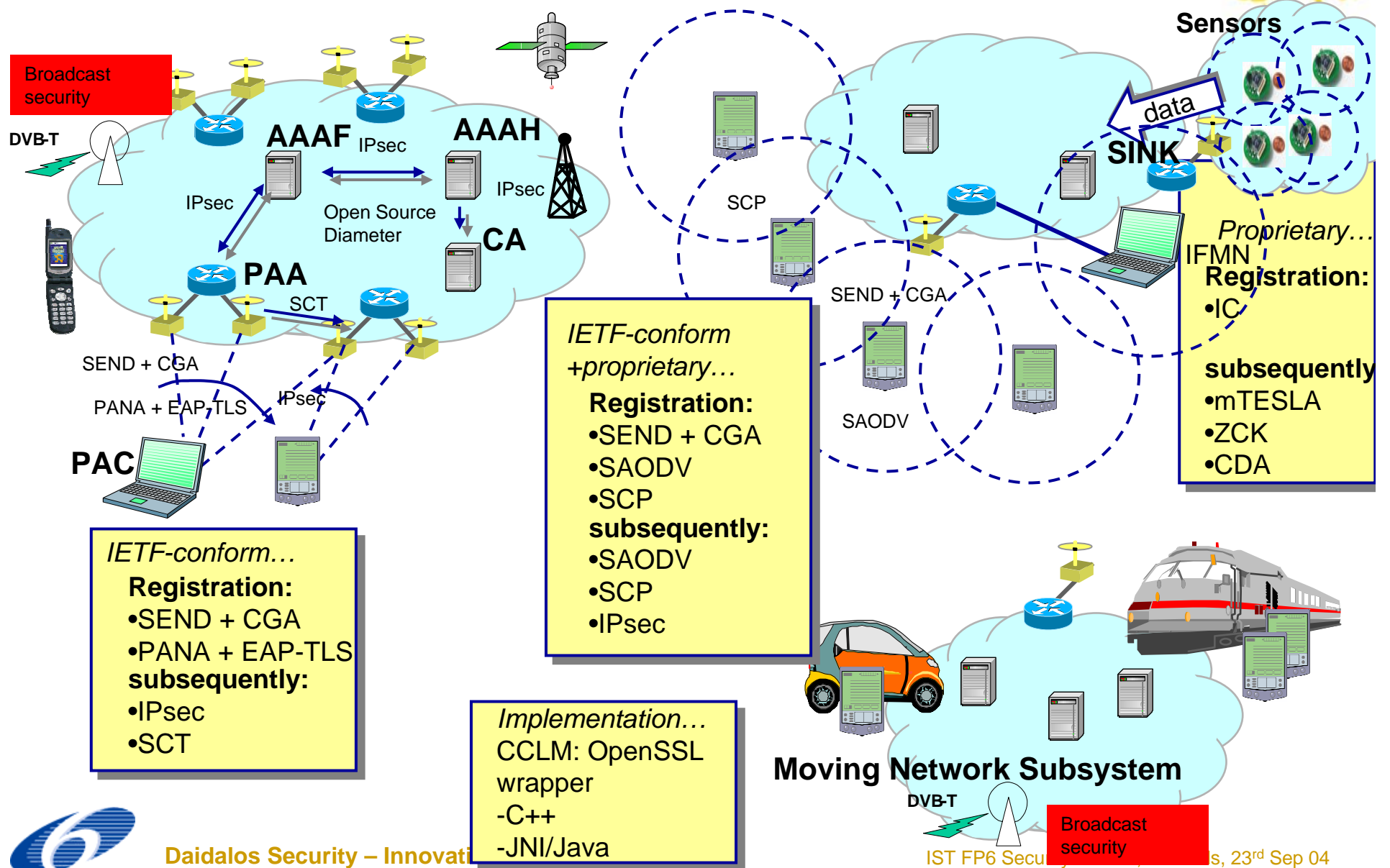


- ▶ Securing the (ad hoc) edge network against routing attacks and address spoofing
- ▶ Ensuring that QoS signalling is outside the encryption envelope.
- ▶ Secure Neighbour Discover Protocol IETF draft
- ▶ Secure AODV IETF draft
- ▶ Secure Charging Protocol IETF draft
- ▶ IPv6 header to expose QoS signalling to the Access Router
- ▶ Providing a optimised common cryptographic library interface to to WP3 and WP4 for use in the mobile terminal
- ▶ Perfect forward secrecy for smart-dust sensor networks





# WP2 Security architecture view





# WP2 Security architecture view

|                |   |
|----------------|---|
| <b>SEND</b>    | <b>Secure Neighbor Discovery</b>  |
| <b>SCT</b>     | <b>Security Context Transfer</b>  |
| <b>CGA</b>     | <b>Cryptographically Generated Addresses (more generic Secure IP Acquisition)</b> |
| <b>EAP/TLS</b> | <b>Extensible Authentication Protocol TLS</b>                                     |
| <b>SCP</b>     | <b>Secure Charging Protocol</b>   |
| <b>mTESLA</b>  | <b>(Micro) Time Efficient Stream Loss-tolerant Authentication</b>                 |
| <b>CDA</b>     | <b>Concealed Data Aggregation</b>   |
| <b>ZCK</b>     | <b>Zero Common Knowledge Authentication</b>                                       |
| <b>SAODV</b>   | <b>Secure AODV</b>  |
| <b>PANA</b>    | <b>Protocol for Carrying Authentication for Network Access</b>                    |
| <b>CCLM</b>    | <b>Common Cryptographic Library Module</b>  |
| <b>IC</b>      | <b>Identity Certified Authentication</b>  |





# WP2 security implementation

- ▶ GNU C + Java on Linux 2.6 kernel with MiPL 2.0 addition.
- ▶ Mobile terminals – iPAQs running Familiar Linux.
- ▶ Optimise crypto for iPAQ CPU – use of elliptic curve asymmetric algorithms
- ▶ Provision of a general library for use on the mobile terminal and within the network
- ▶ User mode daemons preferred but some kernel modification is necessary
- ▶ Common crypto shared library
  - C/C++ interface
  - Java interface via JNI
- ▶ Sensor network uses the Tiny OS and Zigbee environments



# WP3 Service and network - security focus



- ▶ **Security service provision platform**
  - Mutual authentication of users and services
  - End to end encryption using IPSec/IKE
  - Certificate and key lifecycle management
  - Provision of security services to WP4 pervasive services and applications via the WP2 common crypto library
  
- ▶ **Network authentication**
  - Generalisation of the PANA protocol
  - Core A4C infrastructure based on Diameter / EAP
  
- ▶ **Base identity management**
  - Certificated SAML assertions
  
- ▶ **Inter-security domain federation**
  - SAML authentication messaging
  - Bridge certification authorities
  
- ▶ **Broadcast security services**





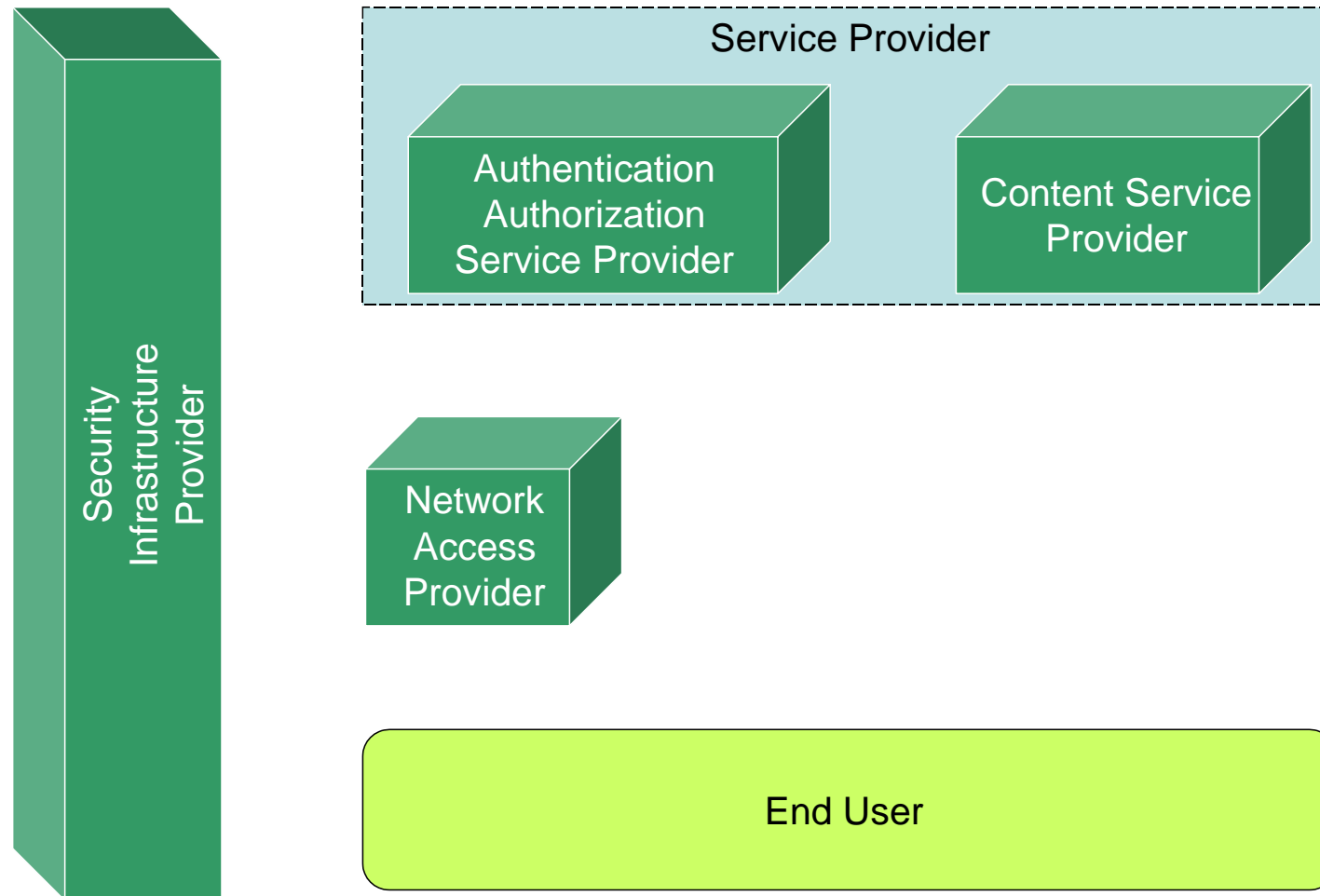
# WP3 Security focus cont'd

- ▶ **Security service provision platform**
  - Mutual authentication of users and services
  - End to end encryption using IPSec/IKE
  - Certificate and key lifecycle management
  - Provision of security services to WP4 pervasive services and applications via the WP2 common crypto library
  
- ▶ **Network authentication**
  - Generalisation of the PANA protocol
  - Core A4C infrastructure based on Diameter / EAP
  
- ▶ **Base identity management**
  - Certificated SAML assertions
  
- ▶ **Inter-security domain federation**
  - SAML authentication messaging
  - Bridge certification authorities
  
- ▶ **Broadcast security services**

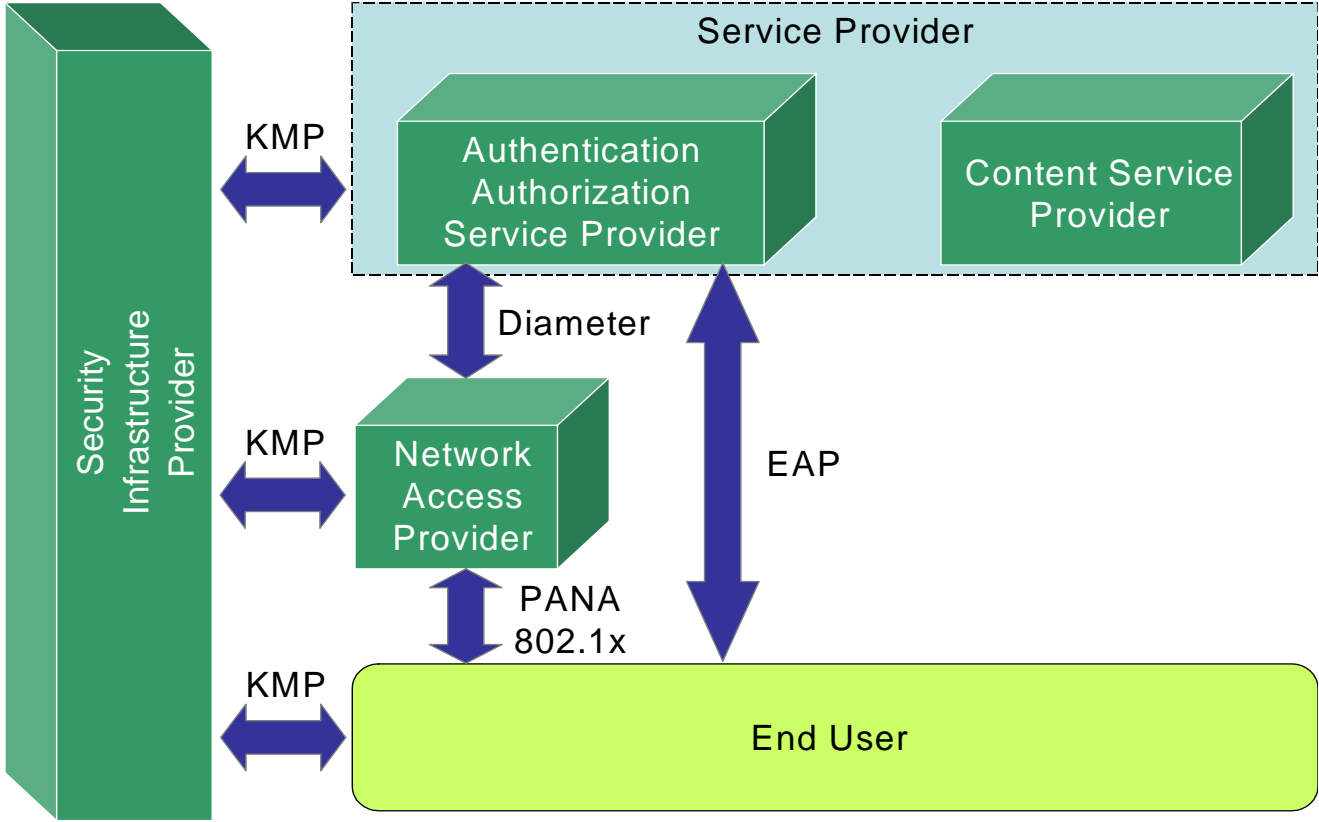




# WP3 System Components

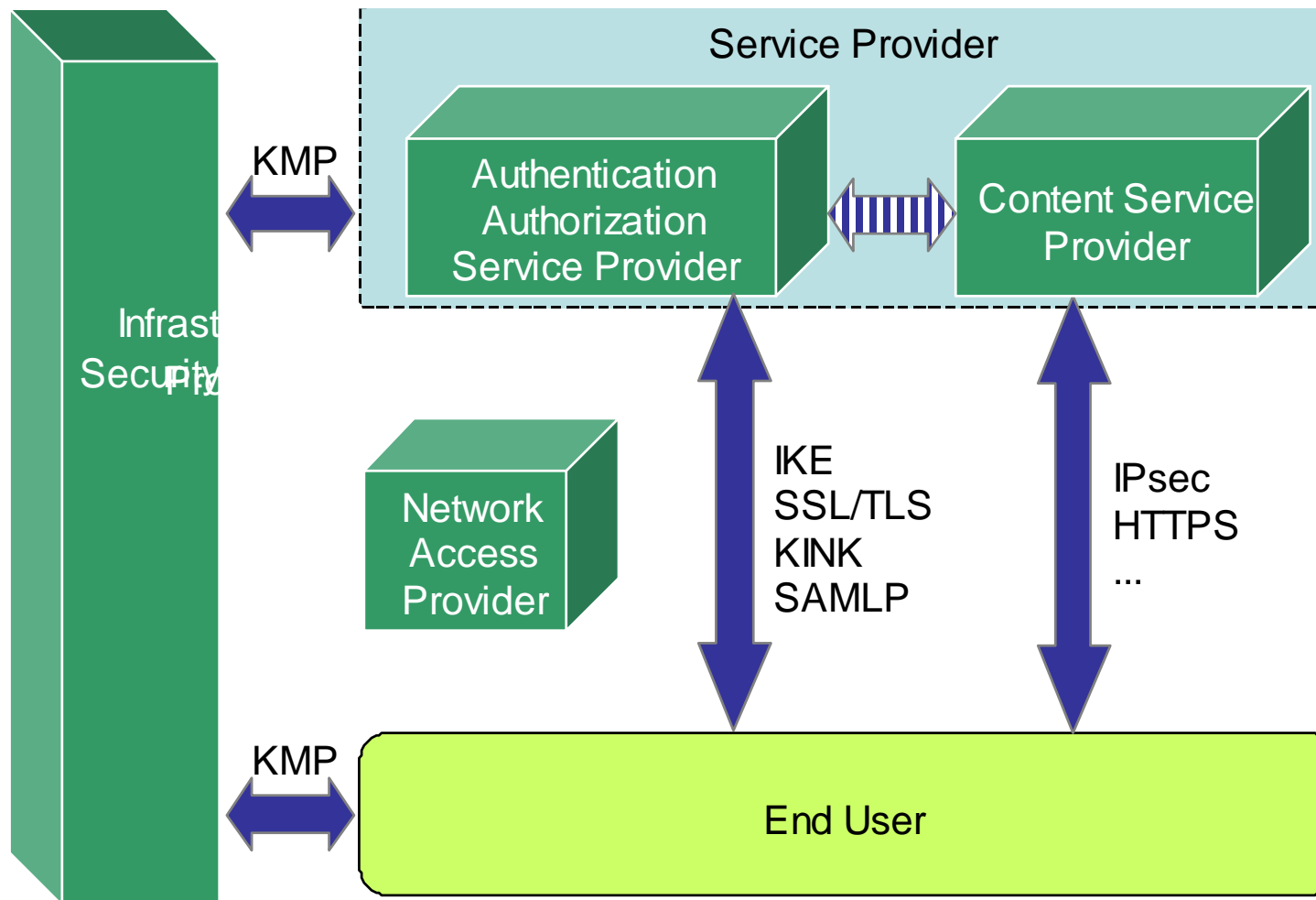


# WP3 security components/protocols





# WP3 Service components/protocols





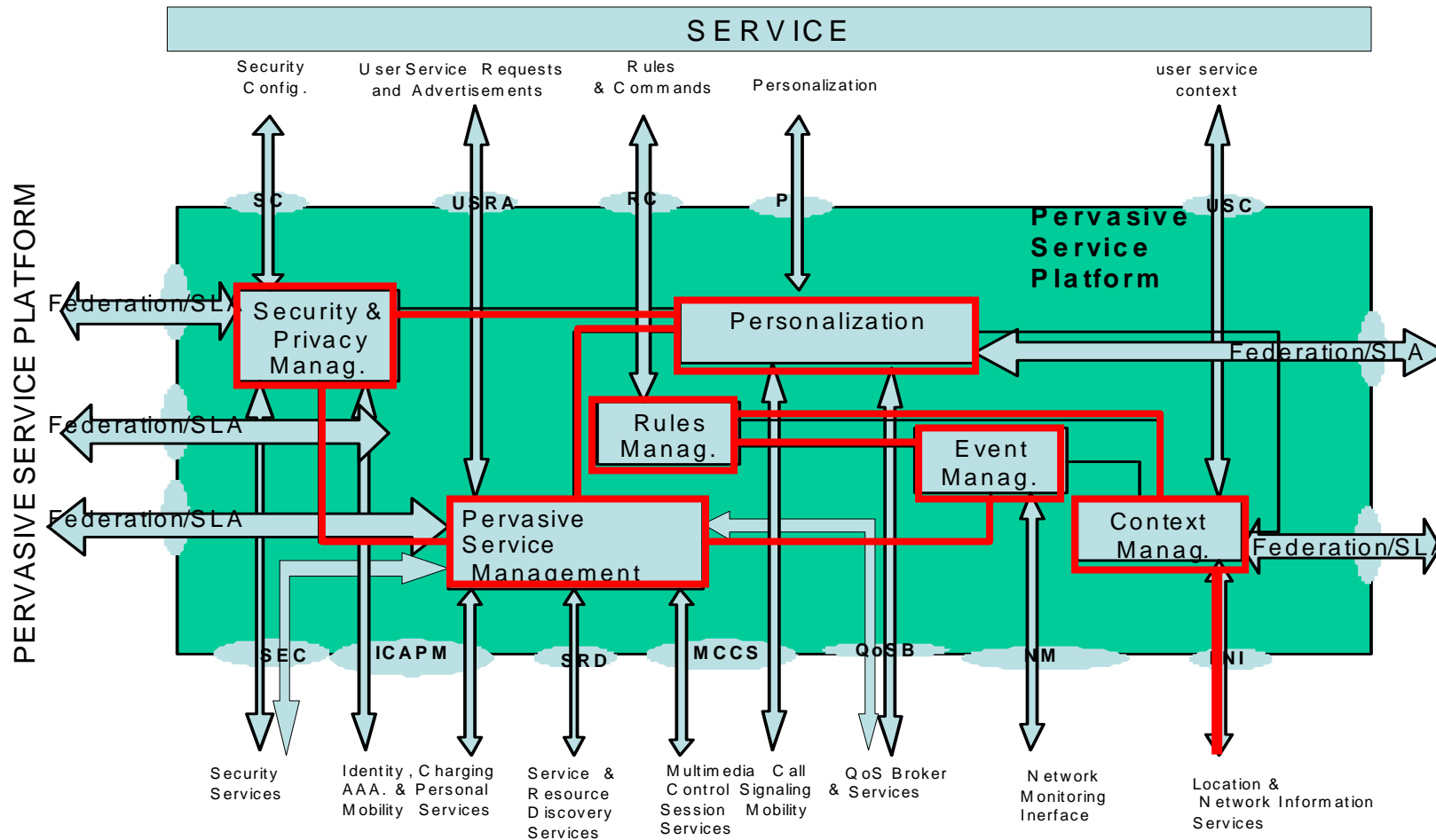
# WP3 implementation

- ▶ C/C++ modules calling the Common Crypto Library
- ▶ OpenDiameter / EAP
- ▶ SAML for security assertions
- ▶ Certificates verifying SAML assertions





# WP4 software architecture



# WP4 Security & Privacy Manager (SPM)

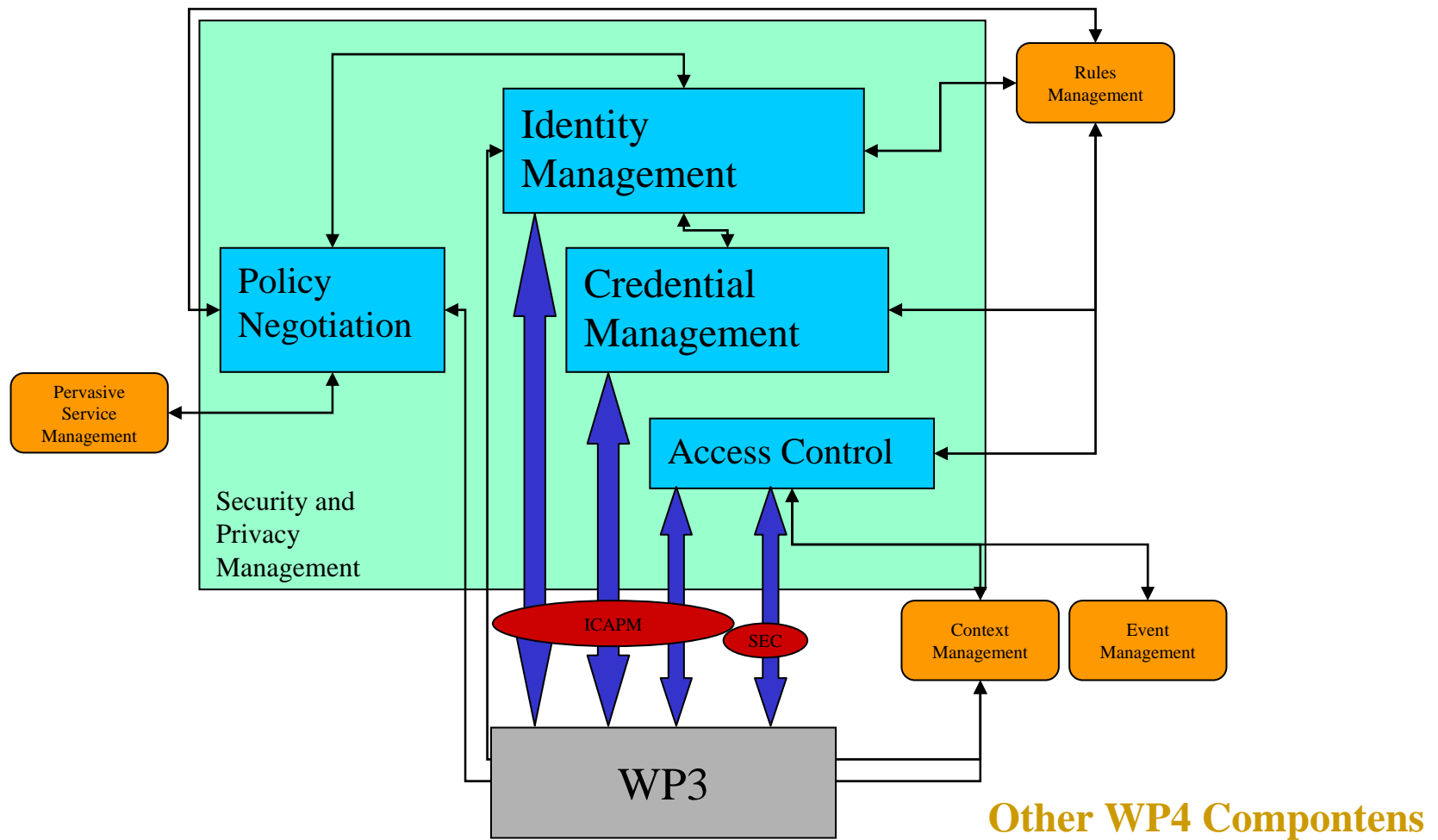


- ▶ „Everything is a service and is composed dynamically“
- ▶ Requirements: Multidimensional dynamics
  - User changes location
  - User changes identities
  - User changes devices
  - User changes services
  - User composes new services
- ▶ Legacy security approach
  - Static contracts
  - Static trust and security relationships
  - Static configurations (very slow!)
  - Configurations bound to device
- ▶ Must be much more dynamic!





# WP4 SPM architecture





# WP4 Identity Certificates

## „Identity“ Certificates

- ▶ Non-repudiation must be assured
- ▶ VIDs-identifier must be able to sign in a non-repudiable way
  - Certification of pub. key to VID-identifier by TTP (CA)
  - TTP must know RegID, which can pay for VID's signed actions
- ▶ Link to WP3
  - WP4 ID-Mgmt „orders“ new VID by WP3 ID-Mgmt
  - WP3 ID-Mgmt registers VID-identifier at CA
  - A4C stores link VID <-> RegID





# WP4 Identity Certificates (cont'd)

## Attribute Certificates

- ▶ SAML assertions
- ▶ Statements about access rights or authentication status
  - Signed by „issuer“





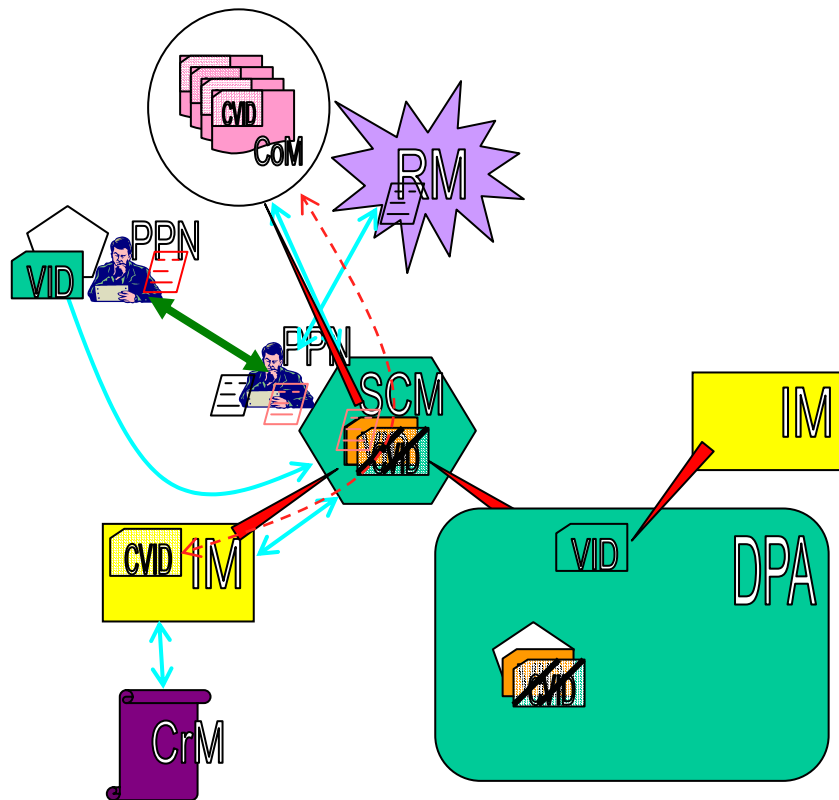
# WP4 Actors in security architecture

- ▶ Daidalos Personal Assistant (DPA) – represents a user
- ▶ Event Management (EM)
- ▶ Service Composition Management (SCM)
- ▶ Identity Management (IM)
- ▶ Privacy Policy Negotiation (PPN)
- ▶ Rules Management (RM)
- ▶ Context Management (CoM)
- ▶ Credential Management (CrM)
- ▶ Access Control (AC) – is distributed between parties and alas not presented in diagrams; it is used in any relation requiring a sort of access to private or secure data.





# Typical WP4 process flow

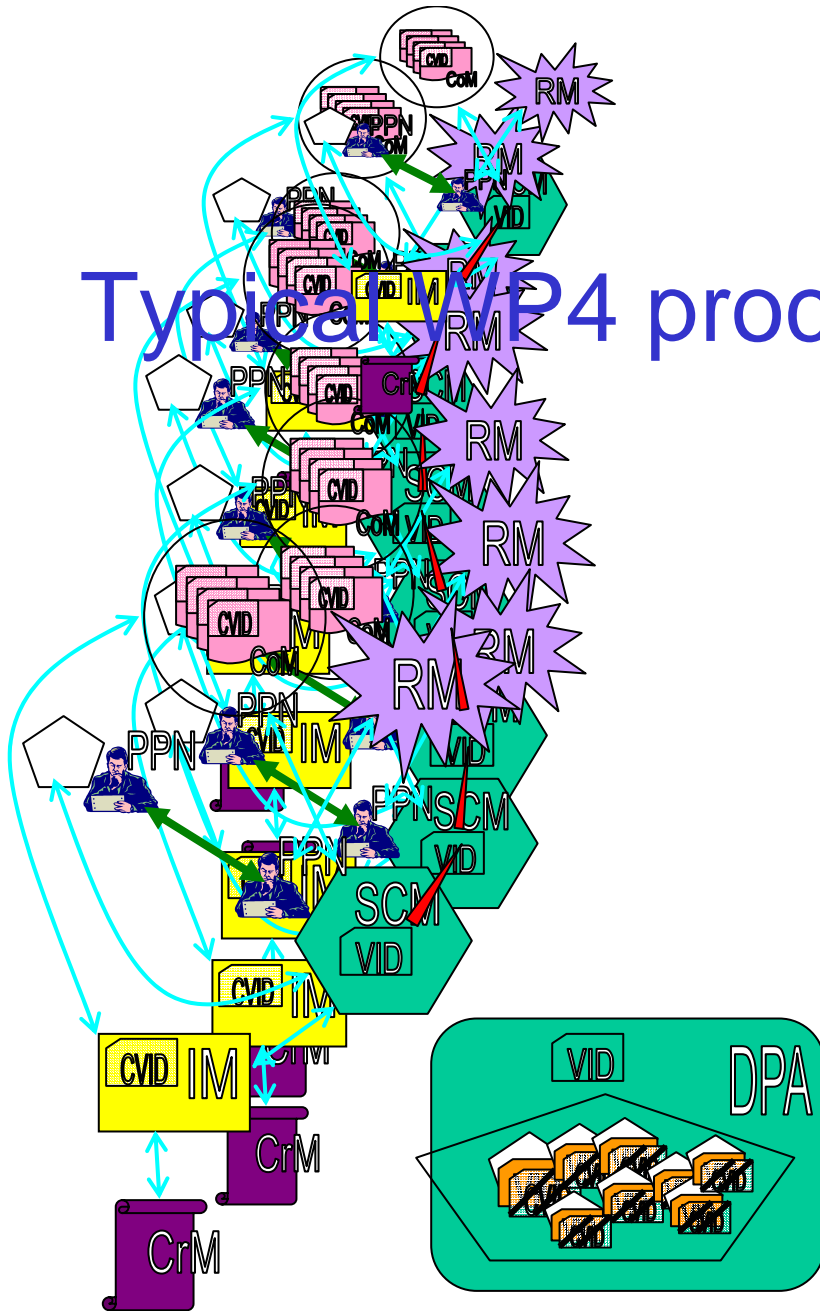


- User acquires a default VID.
- User initiates service composition on her/his DPA, providing a default VID.
- A service is queried.
- Eventually negotiation is required, user's policy acquired from Rules Management,
- negotiation performed,
- and a common agreed intersection policy derived,
- upon which a new VID is fixed (including negotiated credentials);
- but the service needs some context information,
- referred to by relevant data from common agreed intersection policy,
- so encrypted Context VID is supplied,
- and the service set with this composite VID.





# Typical WP4 process flow

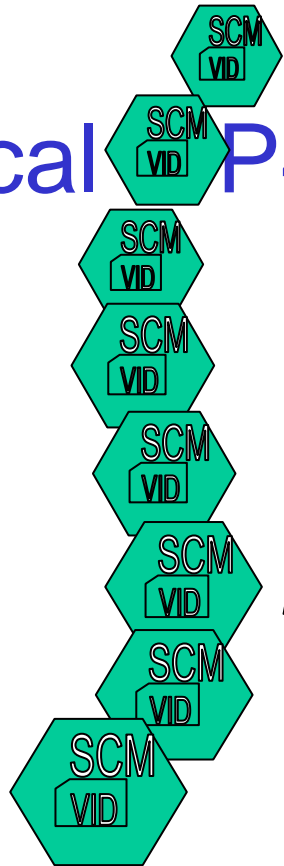


- But this service needs another service,
- which is established performing the same relations.
- And the new service needs another service,
- and this one another,
- and this one another,
- and this one another,
- and this one another,
- and this one another,
- until a composite service established.





# Typical P4 process flow



And there we have a nice backbone.





# WP4 security focus

- ▶ Privacy, A4C and identity management for pervasive services.
- ▶ Providing the higher-level layer of the Service Provisioning Platform (SPP) facing 3<sup>rd</sup> party service providers.
- ▶ User interface to define user preferences
- ▶ Policy management and negotiation component
- ▶ Access control to services (including services)
- ▶ ID and credential management for service providers



# WP4 implementation environment



- ▶ Components intended for use in the mobile terminal and service provider platforms
  - Challenge will be to fit everything into the PDA mobile terminal
- ▶ Spiral iteration of UML designs and Java components
- ▶ Extensive usage of the crypto interface library for efficiency



# WP5 and WP1 – security integration



- ▶ WP1 vertical security team
  - Includes representatives of all work packages
  - Ensures there is not duplication of function in the integrated project.
  
- ▶ WP5 integration security team
  - Integrated demonstration of Daidalos components
  - Ensure compliance with the overall scenarios



## Contributors to presentation



| Name                      | Organisation                             |
|---------------------------|--|
| Stephen Butler            | LAKE Communications                      |
| Jim Clarke                | LAKE Communications                      |
| Kajetan Dolinar           | SETCCE                                   |
| Igor Orazem               | SETCCE                                   |
| Antonio F. Gómez Skarmeta | Uni Murcia                               |
| Parijat Mishra            | Institute for Infocomm Research          |
| Christian Hauser          | University of Stuttgart                  |
| Martin Neubauer           | University of Stuttgart                  |
| Jose Gonzales             | Telefonica I+D (TID)                     |
| Migel Neves               | Instituto Telecomunicações - Aveiro      |
| Diogo Nuno Pereira Gomes  | Instituto Telecomunicações - Aveiro      |
| João Girão                | NEC                                      |
| Telemaco Melia            | NEC                                      |
| Dirk Westhoff             | NEC                                      |
| Ian Martin                | HW Communications                        |
| Ioannis Katsaros          | Lancaster University                     |
| Bahram Honary             | Lancaster University                     |
| Czeslaw Jedrzejek         | ITTI                                     |
| Miguel Ponce de Leon      | Waterford Institute of Technology - TSSG |
| John Ronan                | Waterford Institute of Technology - TSSG |





- ▶ For further information on Security elements of DAIDALOS, please contact:
  - [dirk.westhoff@netlab.nec.de](mailto:dirk.westhoff@netlab.nec.de) (WP1)
  - [stephen.butler@lakecommunications.com](mailto:stephen.butler@lakecommunications.com) and [joao.girao@netlab.nec.de](mailto:joao.girao@netlab.nec.de) (WP2)
  - [skarmeta@dif.um.es](mailto:skarmeta@dif.um.es) (WP3)
  - [hauser@ikr.uni-stuttgart.de](mailto:hauser@ikr.uni-stuttgart.de) (WP4)
  - [jim.clarke@lakecommunications.com](mailto:jim.clarke@lakecommunications.com) (WP5)

