Aspects of End-to-End Security for Open Telematics

Based on a presentation to the IST World Congress, San Francisco, Nov. 2005 by H.-J. Vögel, M. Smirnov, J. Kane, I. Kulp, A. Petrou

hans-joerg.voegel@bmw.de

BMW Group Forschung und Technik
Telematics. 
Definition.

Services delivered to the mobile user with a specific focus on, or a particular added value in an automobile environment.
Horizontal Telematics market evolution.
Horizontal Telematics market evolution.

Transparent networking resources provided by private telco operators.
Open telematics protocols allows „virtual“ per-OEM telematics on shared infrastructure.
Service Providers deliver services anywhere without having to re-develop service implementations.
Horizontal Telematics market evolution.

Further standardization will foster interoperability among first-tier suppliers.
Advanced telematics today.
Example: BMW Online.

www.bmw-connecteddrive.com
Advanced telematics tomorrow.

Example.
Aggregators, Customers, Service Providers.

Security challenges.
Multiple authentication credentials? 
Re-configuring user profiles?
Aggregators, Customers, Service Providers.

Security challenges.

Multiple authentication technologies?
Maintaining service personalization?
Aggregators, Customers, Service Providers. Security challenges.

![Diagram showing Single Sign-On?]
Aggregators, Customers, Service Providers. Security challenges.
Federation.
General approach.

Establishing a circle of trust between business partners for management of user identities and profiles across heterogeneous domains.
Security assertions.
Standardized, technology independent.

Destination site

Relying Party (RP)

Service Center

Policy Enforcement

Source site

Asserting party (AP)

SAML Authority

Authentication Authority

Authorization Authority

Attribute Authority

User

Credential

Portal

SAML Assertion

XML

SAML Assertion

XML

Verify Assertion

Users, Roles, Rights

Credential Store
Security assertions.
Standardized, technology independent.

Single Sign-On:
User authenticates once. Assertion automatically inserted in subsequent service requests.
Security assertions.
Standardized, technology independent.

Open interface: Service infrastructure readily builds on central user management and security.
Security assertions.
Standardized, technology independent.

Trust:
Only one set of credentials per user.
Centrally managed.
Federating services and aggregator portals. Open security solution.
Federating services and aggregator portals. Open security solution.

Service Providers integrate their services into multiple portals without changing their security interface.
Federating services and aggregator portals. Open security solution.

Aggregator is free in choice of credential technology. Adding services to portal portfolio is facilitated by open interface.
Experimental experience.
Early field trial setup.
Next steps.
Cross-OEM trials at european scale.

www.gstforum.org
Conclusions.

• Technical consolidation in telematics happens slowly.
• Open interfaces help setting up new services in fragmented business environment.
• Federation approaches greatly reduce the technical effort of securely integrating services into aggregator portals.
• Federation reduces the entry burden for new service providers, as they can build on aggregator user management platform.
• SAML has been evaluated and successfully trialed as viable federation technology in telematics environments.
• European project GST takes experimentation to the next level – see www.gstforum.org
Thank you for your attention.

hans-joerg.voegel@bmw.de

BMW Group
Research and Technology

Chair Security Working Group

www.car-2-car.org