

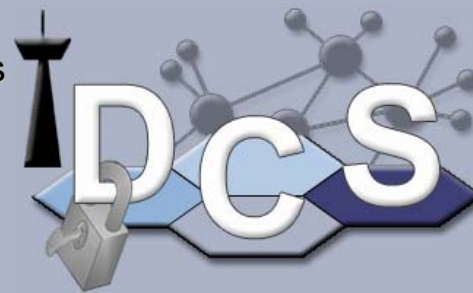
Summary

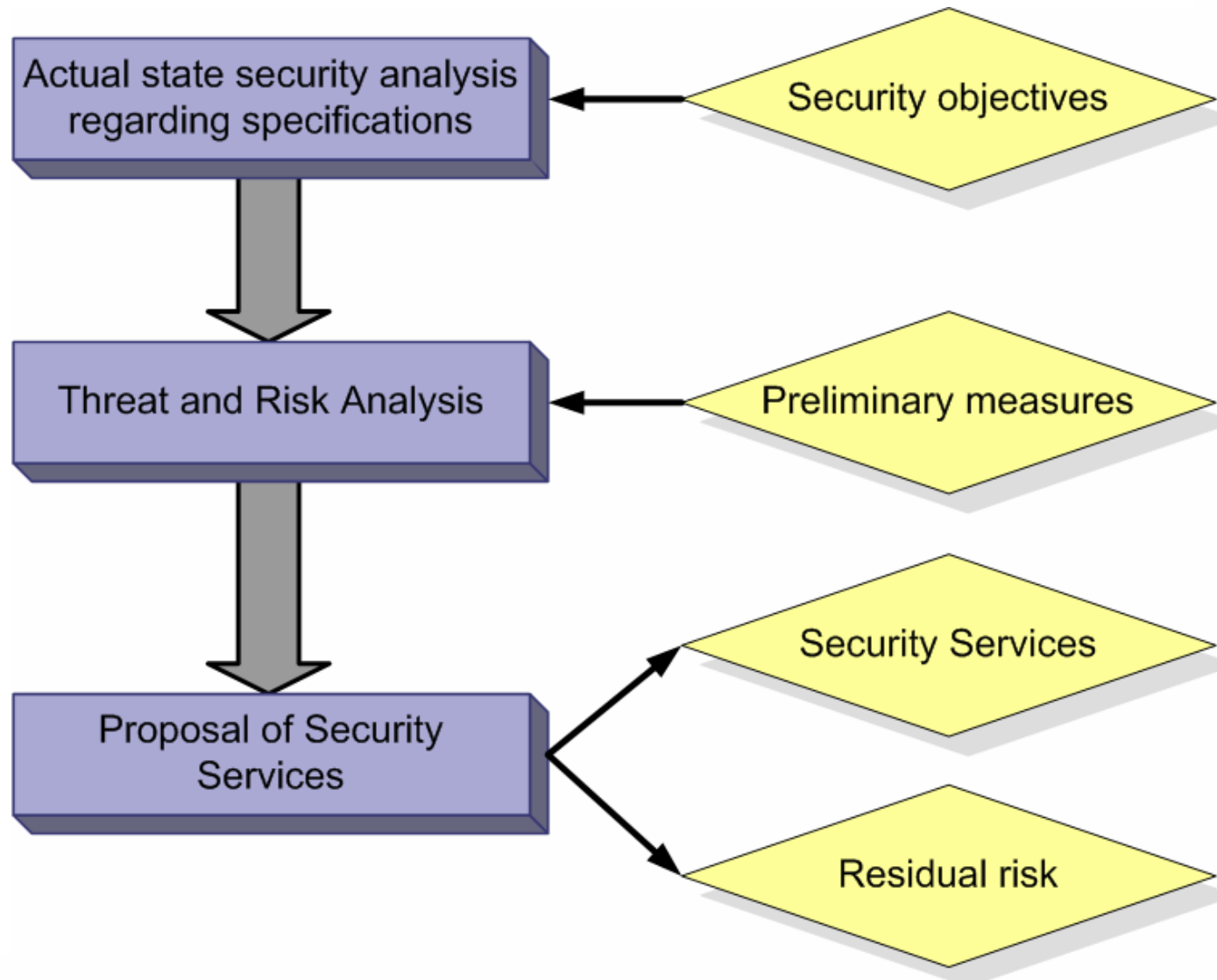
TPEG Security Analysis

The Analysis was performed by order of the Federal Office for Information Security (BSI) in Germany

University of Siegen

Institute for Data Communications Systems
Univ.-Prof. Dr. Christoph Ruland
Hölderlinstraße 3
D-57076 Siegen
<http://www.dcs.uni-siegen.de>





- Normative references
 - ISO 14819 Part 1-3, 6
Traffic and Traveller Information (TTI) – TTI Messages via traffic message coding
 - ISO/TS 18234 Part 1-6
Traffic and Travel Information (TTI) – TTI via Transport Protocol Experts Group (TPEG) data-streams
 - ISO/TS 24530 Part 1-4
Traffic and Travel Information (TTI) – TTI via Transport Protocol Experts Group (TPEG) Extensible Markup Language (XML)
- Cross references
 - RTTI WG
 - Communications WG

□ Confidentiality

- No encryption mechanism designated in the technical specification.
- The metadata of service frame 01 for conventional data provide a field of 1 byte length called "encryption indicator", which signals if or if not an encryption and/or compression is applied to all data of the component multiplex of the conventional data service frame.

□ Data Integrity

- No mechanisms to ensure data integrity are defined.
- A service provider may integrate data integrity services into the encryption function by its own.
- For transmission errors (but not malicious modifications) CRC is used for headers inside a transport frame. (TPEG assumes an error correcting bearer)

- ❑ The documents ISO/TS 24530 Part 1-4 provide knowledge, data types and document type definitions (DTD) to convert the binary TPEG format into an XML representation.
- ❑ tpegML is an application layer protocol
- ❑ Only used as an exchange format between Content and Service Provider and not between different Content Providers, because tpegML does not consider special metadata concerning the information source etc.

- ❑ For TPEG in XML (tpegML) there are no security services intended in the corresponding technical specifications.

□ Confidentiality

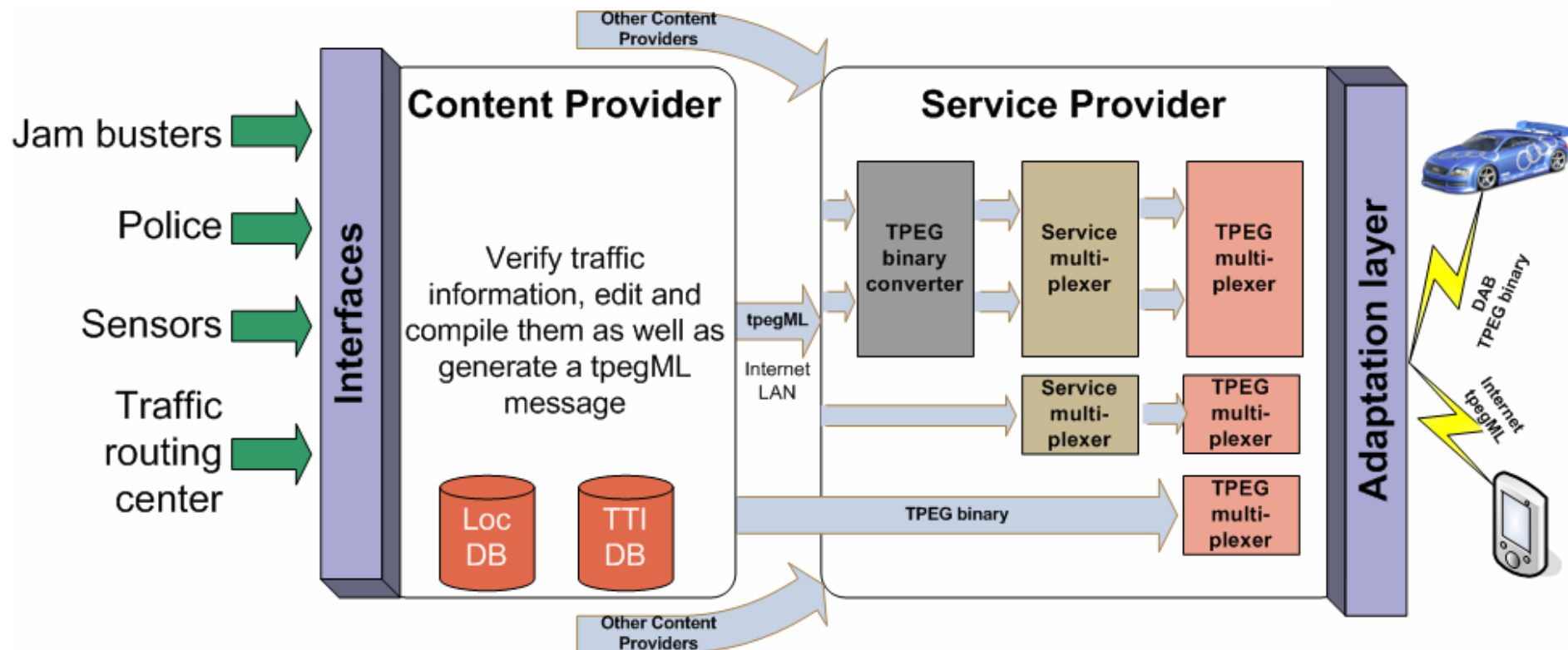
- ISO/TS 14819-6 describes the encryption and conditional access.
- 16 bits long Location element is encrypted in each RDS-TMC message to render the message virtually useless without decryption.
- Light symmetric encryption and easy to break by frequency analysis
- Reason: Only little RDS capacity and no required hardware changes
- Encryption is performed by the service provider

□ Data Integrity

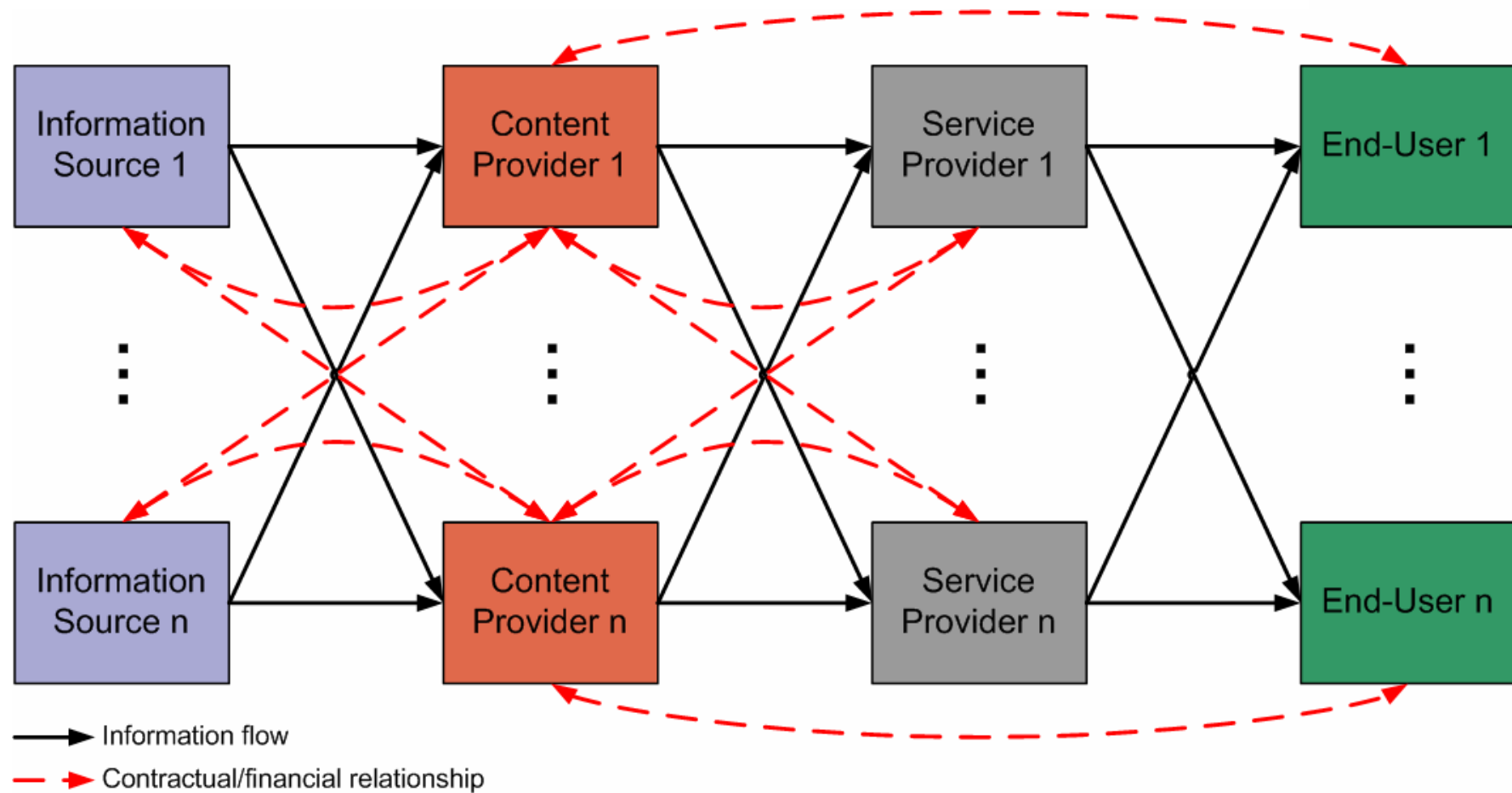
- To ensure the integrity of messages, ALERT-C requires a periodical transmission or message repetition.
- Each group "shall be sent at least twice in succession, before the next group is sent".
- The ALERT-C protocol requires the receipt of at least two identical RDS-TMC groups, before the data can be accepted as valid
- Optional: Additional use of the RDS error correction

- Not addressed regarding TPEG and RDS-TMC
 - Authorisation
 - Authentication of data origin
 - Availability
 - Non-Repudiation
 - Audit and Accountability
 - Privacy, Anonymity and Pseudonymity

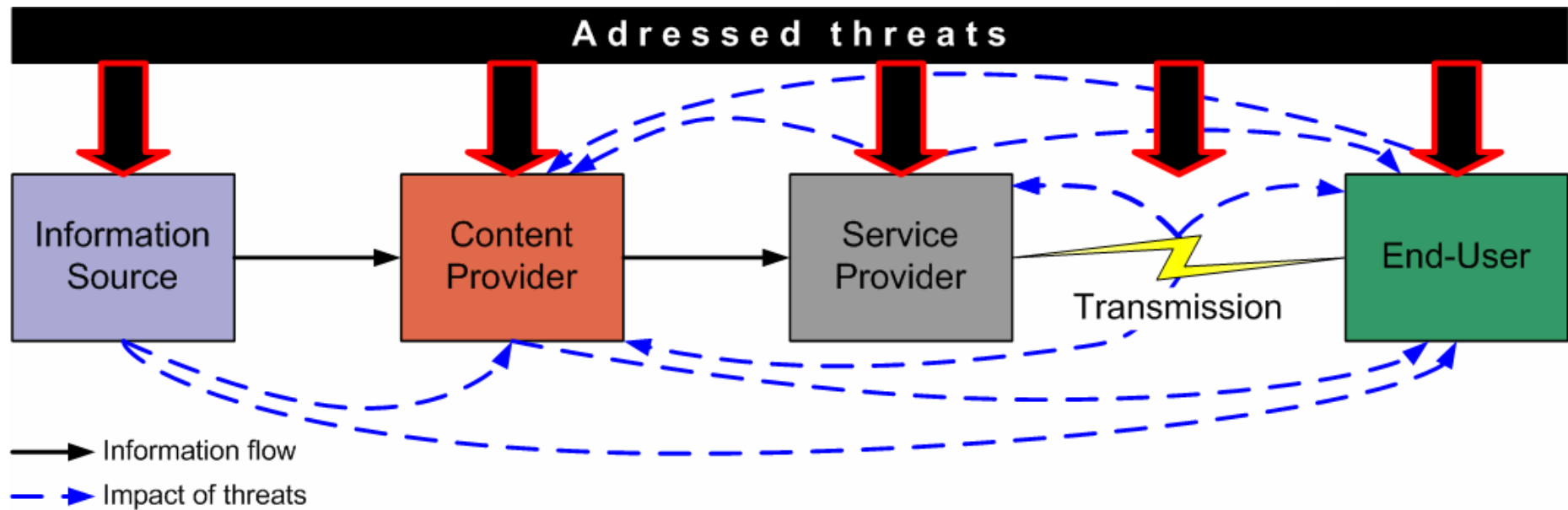
□ Model of the TPEG environment and role allocation



□ Assumed simplified TPEG business model



- Simplified TPEG scenario and attack locations



- Analysis of potential threat situations, possible consequences, identification of affected components and possible attackers as well as their motivation
- The structure of the threat analysis follows the catalogues of threats of the Federal Office for Information Security (BSI) in Germany.
- Risk evaluation is provided (used ratings low, medium, high)
 - Necessary effort to execute an attack
 - Likelihood of the occurrence of threats
 - Severity of consequential damages of an successful attack
 - Risk is calculated depending on likelihood and severity of threats
- Threats rated "medium" or "high" have to be prevented by explicitly defined measures
- "Low" rated threats offer as being accepted as residual risk

Threat	Impact	Attacked component	Attacker (effort)	Likelihood	Severity	Risk
Force majeure						
Natural disasters	Partial failure of the system	All		L	L-H	L-M
Loss of personnel	Disruption of service, loss of knowledge	CP, SP, Manufacturer		M	L-M	L-M
Failure of IT system	Failure of the system	All		L	L-M	L-M
Transmission error	Undetected errors, lost data	Transmission		H	L	M
Technical failure						
Disruption of support networks	Dysfunction and disruption of parts of or the whole system	All		M	L-M	L-M
Disruption of comm. Networks	Impairment or disruption of the transmission and the service	(Wireless) transmission		M	L	L
Insecure cryptographic / signature algorithms	Loss of confidentiality, authenticity, integrity and non-repudiation, no falsification of forgeries, financial damage	SP		L	M	L
Failure of the device	Services are no longer receivable for this specific end-user	Device		L	L	L

Threat	Impact	Attacked component	Attacker (effort)	Likelihood	Severity	Risk
<i>Deliberate attacks</i>						
Sabotage	Failure of the system, loss of data and confidentiality	CP, SP, device (OEM)	External, Internal (high)	L	L-H	L-M
Eavesdropping / Espionage	Commercial damage, charge fraud, unauthorised access and loss of confidentiality	Transmission (all for espionage)	External (also Internal for espionage) (low)	H	H	H
Traffic analysis	Loss of confidentiality	Transmission	External (med)	M	L	L
Manipulation of transmitted information	Loss of data integrity and availability of information, unreadable messages, no authenticity verification possible, influence on behaviour of device and/or user	Transmission	External (med)	M	H	H
Unauthorised use of IT systems	Loss of integrity, availability, confidentiality and authenticity of messages as well as authorisation of the system	CP, SP	External, Internal (medium-high)	L-M	H	M-H
Abuse of end-user rights	Financial damage, loss of confidentiality	Device (OEM) (PIN, passwd)	External, Internal (low-medium)	H	M	H

Threat	Impact	Attacked component	Attacker (effort)	Likelihood	Severity	Risk
<i>Deliberate attacks</i>						
Device manipulation	Financial damage, loss of confidentiality	Device	Internal (medium)	M	H	H
Masquerading	Forgery of identities, deceit of participants, hijacking of existing connections, impersonation as an authorised party, loss of authenticity and integrity	All	External (medium)	M	H	H
Repudiation of messages	Civil dispute	Transmission	External, Internal (low)	L	M	L
Denial-of-Service	Financial damage, loss of availability	All, mainly Transmission	External, Internal (med)	M	M	M
Hoaxes	Misleading information, Denial-of-Service, loss of confidence	Information Source, CP	External, Internal (low)	M	M	M
Compromising of cryptographic keys	Malicious actions, loss of confidentiality, financial damage	CP, SP, device (OEM), transmission of keys	External, Internal (medium)	M	H	H

□ Confidentiality

- The transmission of TPEG data for closed user groups has to be confidential.

Two modes of encryption:

- Without encryption: The application and data is freely available to everybody (public broadcast services).
- With encryption: The application and data is encrypted and can be only decoded by components of a closed user group.

□ Data Integrity

- Application conventional data and metadata (origin etc.) has to be of integrity to all components
 - This data must not be separated from the TPEG message
- Mechanisms to detect software, firmware and hardware manipulations of all parties of the system.

- Authorisation
 - Especially the devices should provide mechanisms for access control that only authorised persons are able to use TPEG services.
- Authentication of data origin
 - The device has to verify the authenticity of TPEG messages (origin).
 - The content of TPEG messages has to be authentic
- Availability
 - A broad coverage of TPEG (bearer) has to be available
 - Assure transmissions of events in a specified time frame
 - Backup mechanisms and emergency plans for special situations

- Non-Repudiation
 - Optional / Residual Risk: It must not be possible that a Content or Service Provider is able to neglect sending a TPEG message.
- Audit and Accountability
 - Logging mechanisms for all TPEG related actions
 - Logging mechanisms for hardware, software and firmware updates
 - Intrusion Detection for unauthorised / fraudulent actions
- Privacy / Anonymity / Pseudonymity
 - Personal data concerning contractual issues have to be treated confidential regarding the relevant privacy laws and restrictions of the country.
 - TPEG uses a broadcast medium (unidirectional)
 - No user tracking and user profiles can be created

- ❑ Security issues did not play an essential role when defining the specifications of TPEG
- ❑ No lessons learned regarding RDS-TMC security experiences
- ❑ Assumption: TPEG scenario and business model
- ❑ Threat and risk analysis
 - Hardware security
 - Especially threats regarding missing authentication and confidentiality are rated with the highest risk
- ❑ Proposal of Security Services
 - Focus on the main threats and security requirements
 - Establish an acceptable level of security (with acceptable residual risks)
 - Most important: Establishment of authentic TPEG messages to verify that a TPEG message comes from a trustworthy sender
 - The second most important: Encryption to enable closed user group services

- Requirements for additional Security Services and more detailed research
- Engagement in standardisation regarding Security Services
- Cooperation with RTTI WG
- Cooperation with Communications WG

