Coordination of Threat Analysis in ICT Ecosystems

Antonio Kung, CTO Trialog

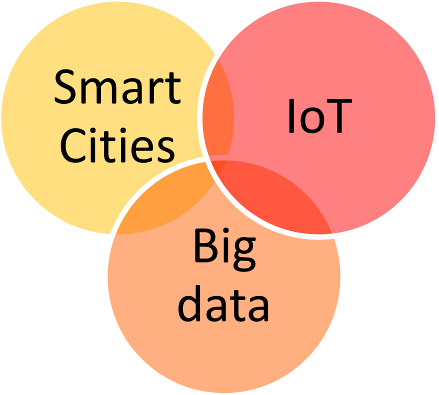
25 rue du Général Foy, 75008 Paris, France

www.trialog.com

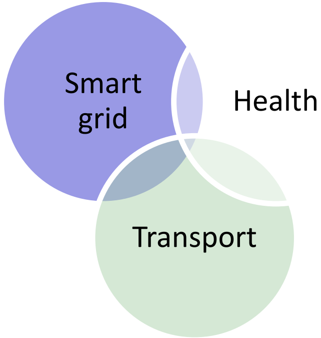
Speaker: Antonio Kung

- Engineering background
- Chair of citizen approach to data initiative
  - EIP-SCC: European Innovation Platform on Smart Cities and Communities
- Data protection / Privacy standards wiki for Ipen
  - Ipen.trialog.com
- ITU-T
  - SG17
    - Cybersecurity framework for intelligent transport system
  - FG-DPM
    - Security and privacy framework
- ISO/IEC
  - Projects
    - 27550 Privacy engineering
    - 27030 Security and privacy guidelines for the IoT
    - 27570 Privacy guidelines for smart cities
    - 20547-4 Big data Security and privacy
  - Study periods
    - Big data security and privacy processes
    - Big data implementation security
    - Framework privacy preference management (Joint ITU-ISO)

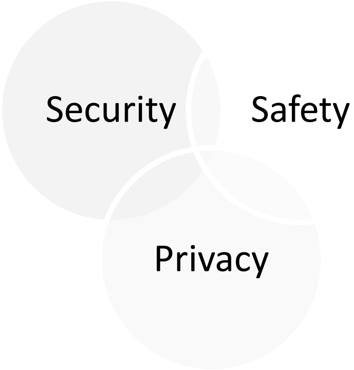
Ecosystems are complex



Ecosystems



Domains

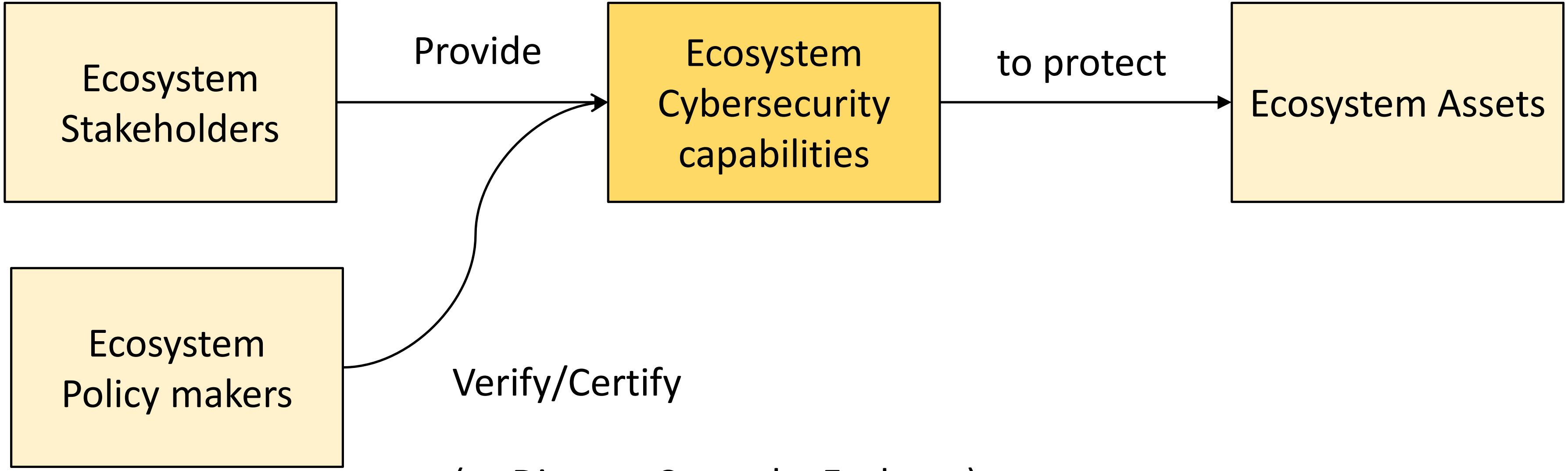


Concerns

Ecosystem Security and Data Protection Concerns

Stakeholder		**Legal Compliance Concern**	**Management Concern**	**System Lifecycle Concern**
Demand side	Policy maker	Compliance Check / Follow standards Transparency		
↓	**Operator**	Regulation for security Regulation for privacy	**Security and data protection risk analysis** Agreement with other operators	Security-by-design Privacy-by-Design
Supply side	**Supplier**	Operators Requirements		

Ecosystem Cybersecurity: What we Need



Ecosystem Stakeholders

Provide

Ecosystem Cybersecurity capabilities

to protect

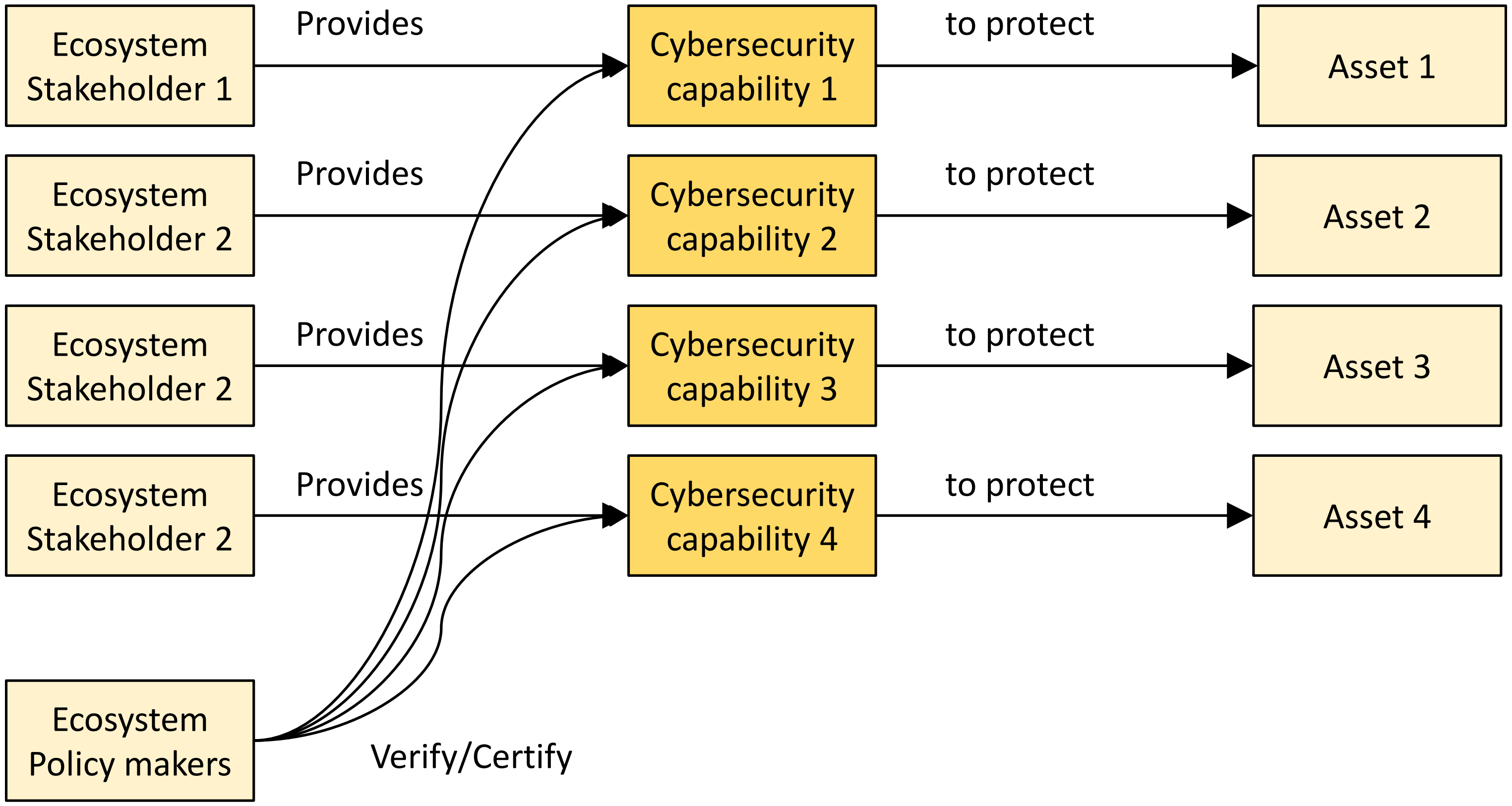
Ecosystem Assets

Ecosystem Policy makers

Verify/Certify

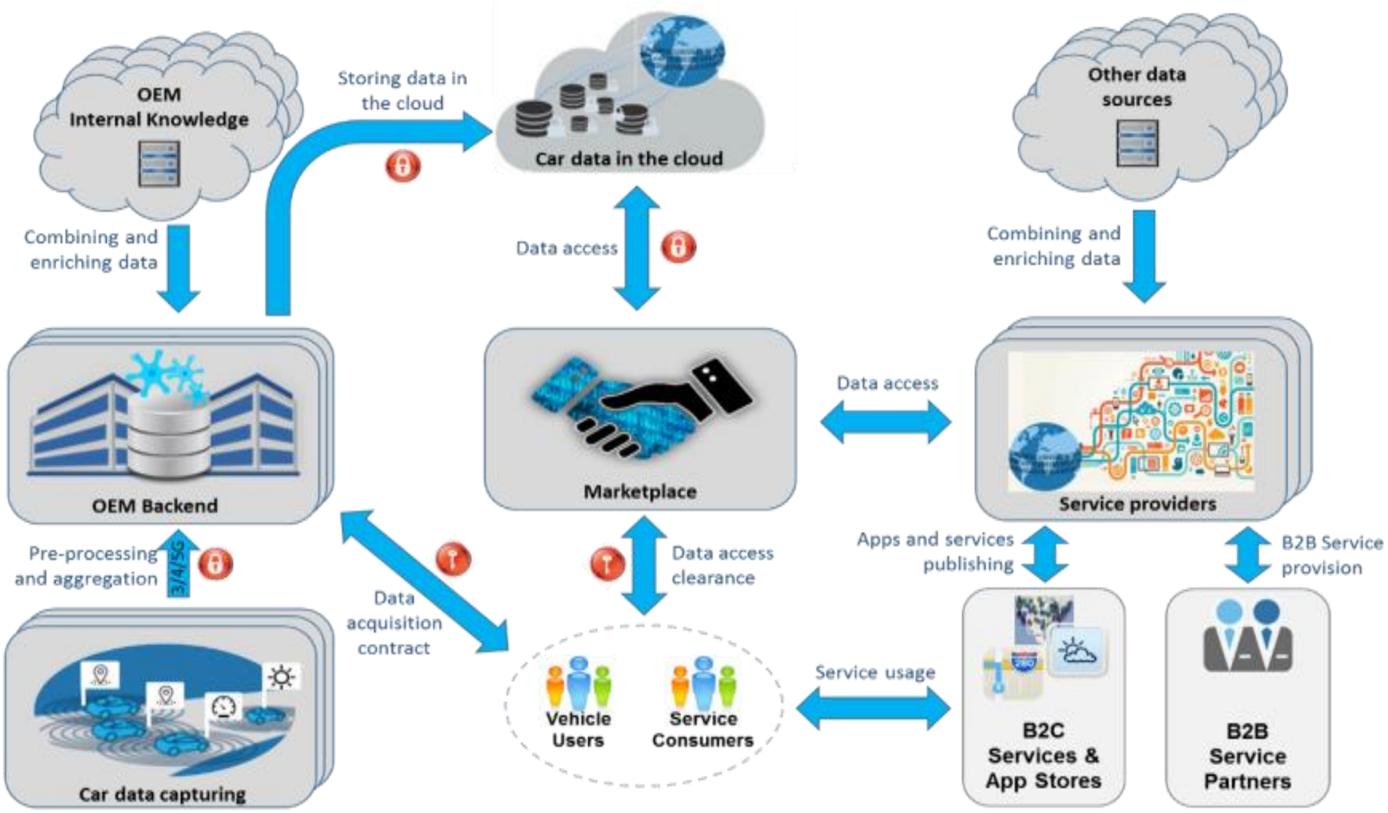
(or Direct – Control – Evaluate)

Ecosystem Cybersecurity: What we Have



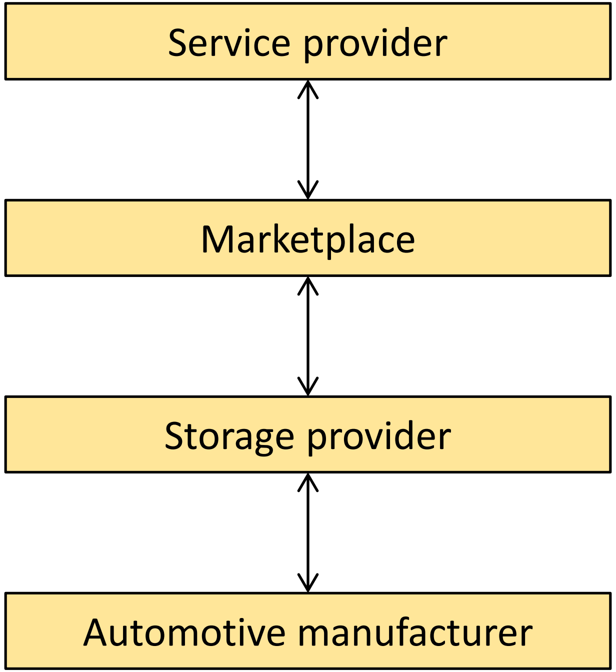
Example of Ecosystem: AutoMat

http://www.automat-project.eu



Example of Ecosystem: AutoMat

- Four types of stakeholders


Service provider

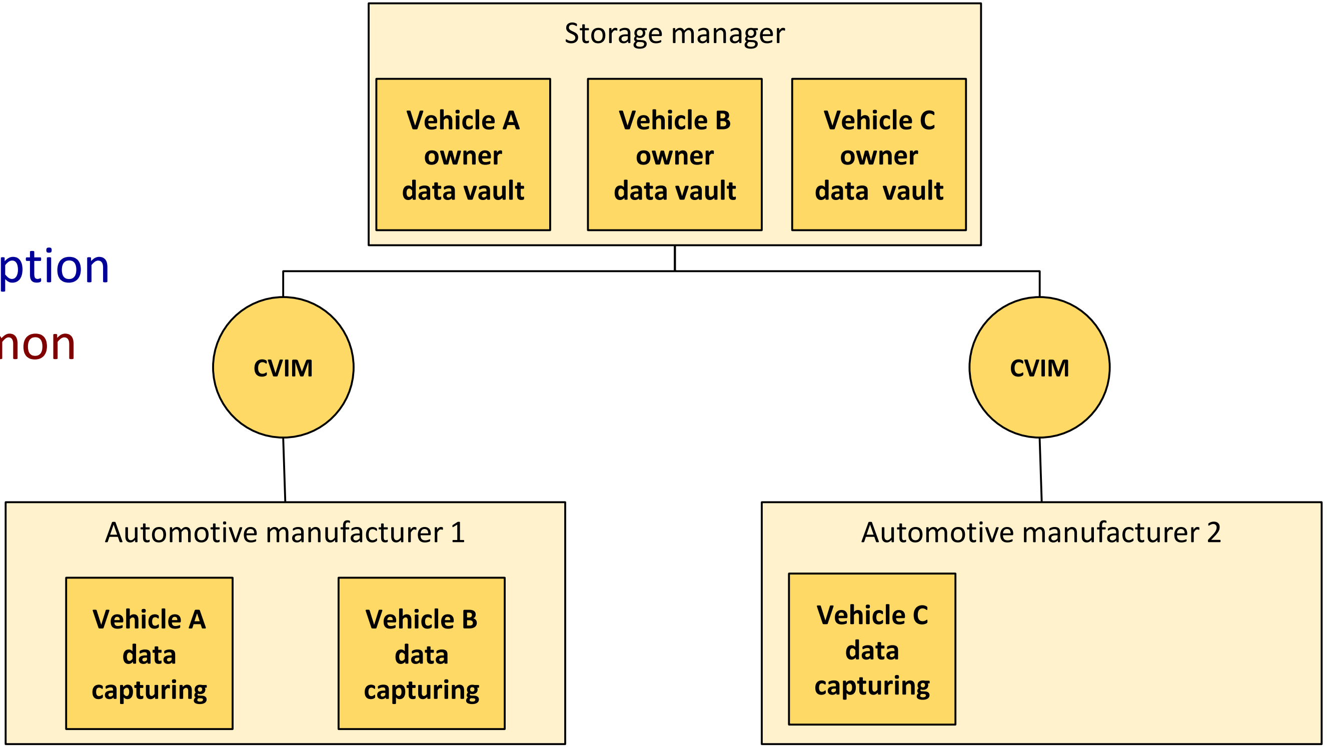
Marketplace

Storage provider

Automotive manufacturer

Ecosystem Design

- Personal data ecosystem
- Interoperability
  - Common description
    - CVIM (Common vehicle information model)



Storage manager

Vehicle A owner data vault

Vehicle B owner data vault

Vehicle C owner data vault

CVIM

CVIM

Automotive manufacturer 1

Vehicle A data capturing

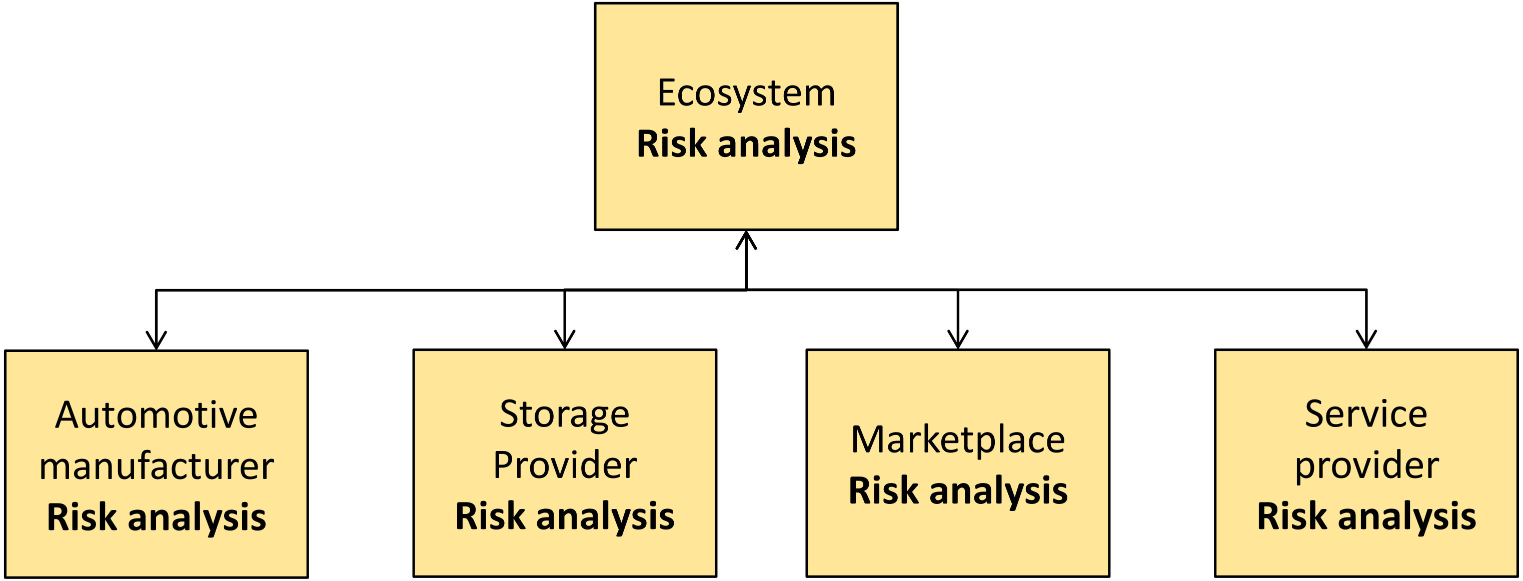
Vehicle B data capturing

Automotive manufacturer 2

Vehicle C data capturing

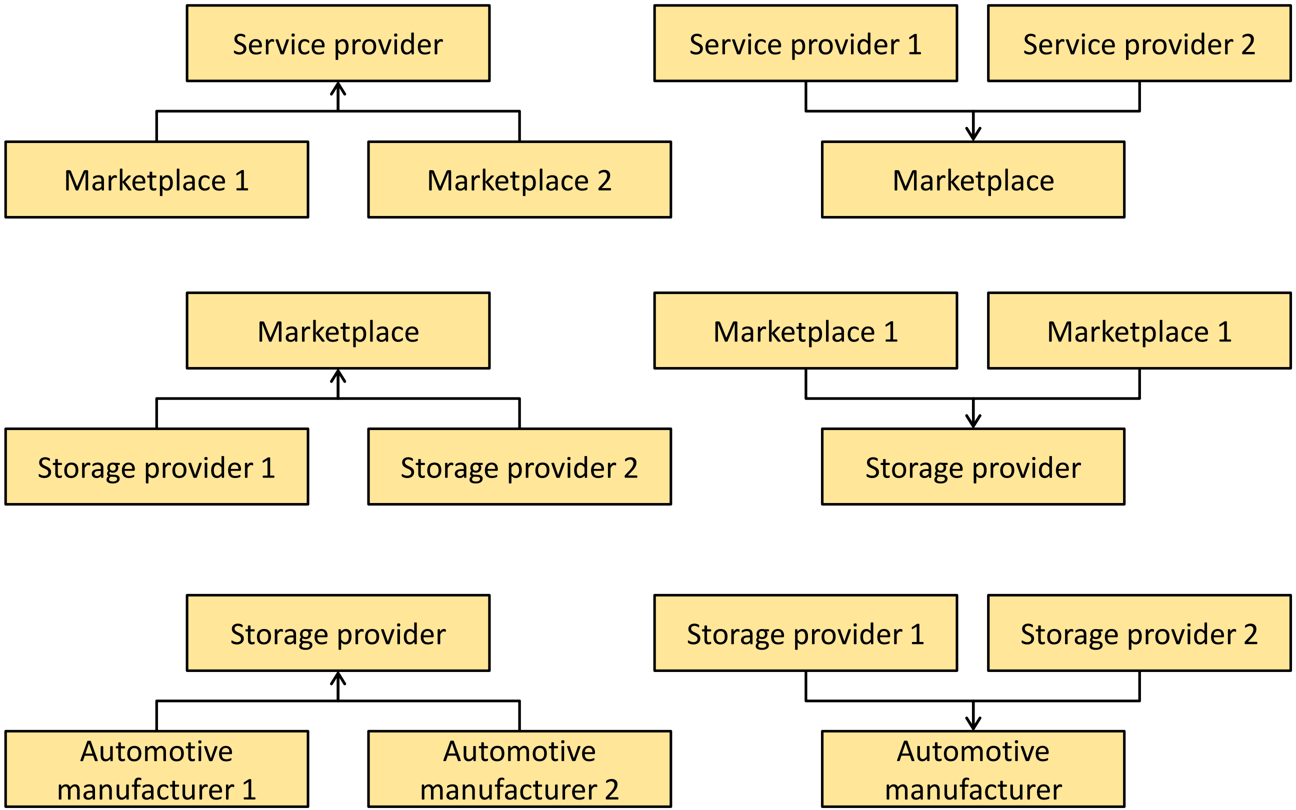
Ecosystem Risk Analysis

- Risk analysis includes
  - security risk analysis (e.g. ISO/IEC 27005)
  - privacy impact analysis (e.g. ISO/IEC 29134)



Ecosystem Interoperability

- Interoperability includes
  - Functional interoperability
  - Cybersecurity interoperability



Service provider

Marketplace 1

Marketplace 2

Service provider 1

Service provider 2

Marketplace

Marketplace

Storage provider 1

Storage provider 2

Marketplace 1

Marketplace 1

Storage provider

Storage provider

Automotive manufacturer 1

Automotive manufacturer 2

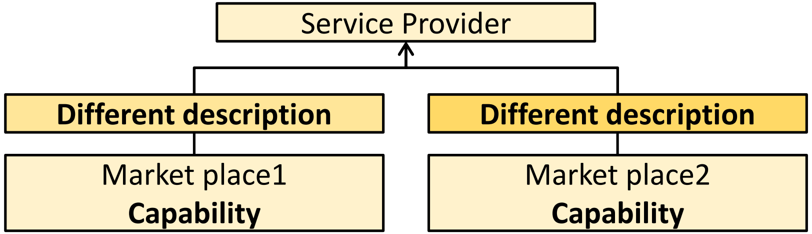
Storage provider 1

Storage provider 2

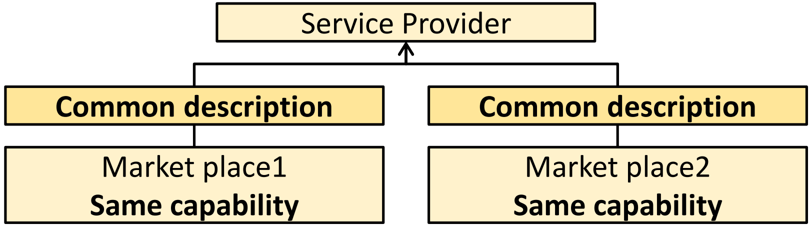
Automotive manufacturer

Different Types of Interoperability

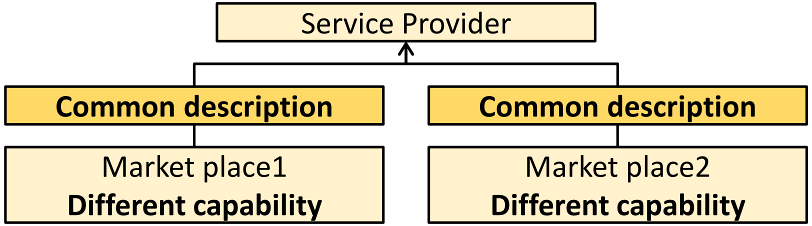
No interoperability



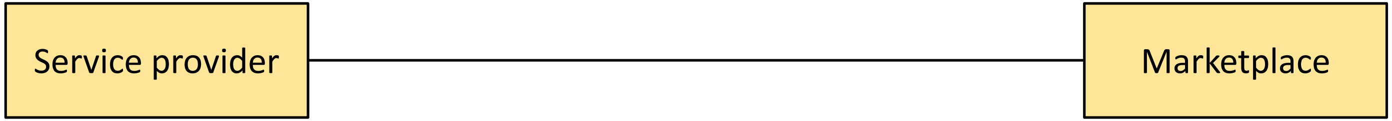
Interoperability of capabilities



Interoperability of descriptions



Need for **Consistent** Individual Cybersecurity Framework



Service provider

Marketplace

Service provider
Cybersecurity framework

- Capabilities
- Agreement

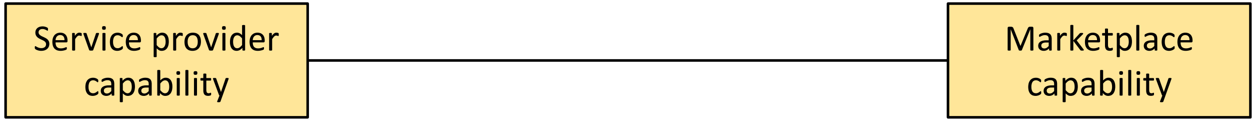
- Risks - Incidents - Consequences
- Measures

Marketplace
Cybersecurity framework

- Capabilities
- Agreement

- Risks - Incidents - Consequences
- Measures

Cybersecurity Capabilities



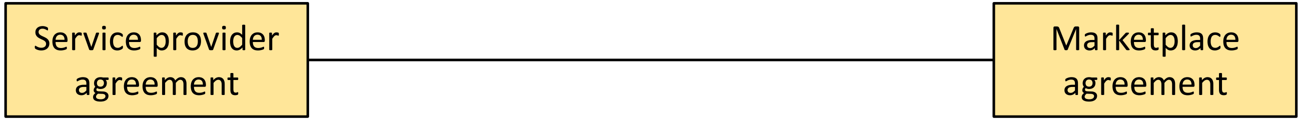
Service provider capability

Marketplace capability

Secure processing	Protect data processing
Transparency information	Provide information how data processing is protected
Data controller responsibility	Verifies whether service provider has data controller responsibility

Secure processing	Protect data pipeline and processing
Owner consent	Capability for vehicle owner to provide consent on personal data processing
Consent revocation	Capability for vehicle owner to withdraw from data pipeline
Transparency information	Capability to provide information on data processing chain
Secure connection to service providers	Capability to provide data to service provider securely
Secure connection to storage providers	Capability to retrieve data from storage manager securely
Data processor responsibility	Verifies whether marketplace has data processor responsibility

Agreement Cybersecurity Capabilities



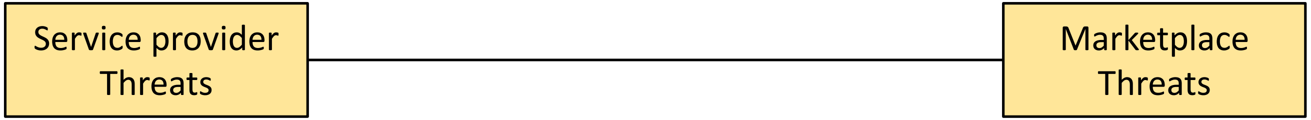
Service provider agreement

Marketplace agreement

Providing evidence of capability	provide evidence of cybersecurity compliance to marketplace
Getting evidence of capability	obtain evidence of marketplace cybersecurity compliance

Providing evidence of capability	provide evidence of cybersecurity compliance to service provider
Getting evidence of capability	obtain evidence of service provider cybersecurity compliance

Threats



STRIDE threat categories	
Spoofing	Spoofing marketplace
Tampering	Integrity and completeness of data obtained from marketplace
Information disclosure	Eavesdropping data during communication Eavesdropping metadata (e.g. log of interactions with marketplace) Incorrect management of data processing chain leading to leaks (e.g. incorrect deletion)
Denial Of Service	Massive access to marketplace
LINDDUN threat categories	
Linkability	Anonymisation not carried out correctly Attempt from external parties to re-identify vehicle owner by using other datasets New linkability threat not taken into account

STRIDE threat categories	
Spoofing	Spoofing storage provider Spoofing service provider
Tampering	Integrity and completeness of data provided to service provider
Repudiation	Service provider repudiation
Information disclosure	Eavesdropping data during communication Eavesdropping metadata (e.g. log of interactions with storage provider and with service provider) Incorrect management of data pipeline leading to leaks (e.g. incorrect deletion)
Denial Of Service	Massive access to marketplace by faked service providers
Elevation of privilege	Incorrect management of vehicle owner privacy rules (expressed in obtained metadata)
LINDDUN threat categories	
Linkability	Anonymisation not carried out correctly New linkability threat not taken into account

Incidents

Service provider Incidents

Incident	Description	Severity
Massive personal data breach	Public report of potential massive personal data leak because of improper operation at service provider level	Maximum
Massive denial of service	Service provider can no longer operate.	Significant

Marketplace Incidents

Incident	Description	Severity
Case of personal data breach	Public reporting that personal data vault has been accessed or that it has been processed against consent or privacy rules	Significant
Massive business data leak.	Public report of potential massive business data leak because of improper operation at marketplace level	Maximum
Massive personal data breach	Public report of potential massive personal data leak because of improper operation at marketplace level.	Maximum
Massive denial of service	Marketplace can no longer operate.	Significant

Measures

Service provider measures

ISO 27001 Categories of controls		Control
Information security policies	Management direction.	Data management policies
Human resource security	During employment	Internal cybersecurity preparedness
		External cybersecurity preparedness
Access control	System and application access control	Secure access to marketplace provider
Cryptography	Cryptographic controls	Anonymisation of data sets
Operation security	Operational procedures and responsibilities	Operation procedures for data processing
	Logging and monitoring	Logging capabilities
	Control of operational software	Operation procedures for transparency.
	Technical vulnerability management	**Plausibility check**
Communication security	Information transfer	Secure transmission of data
System acquisition, development and maintenance	Security in development and support processes	Secure data processing capabilities
		Cybersecurity monitoring capabilities
Information security incident management	Management of information security incidents and improvements	Alerting data processing chain
Information security aspects of business continuity management	Information security continuity	Assurance of service provider cybersecurity capabilities
		Periodic review of service provider cybersecurity capabilities
Compliance	Compliance with legal and contractual requirements	GDPR and cybersecurity compliance verification
	Information security reviews	Periodic review of interoperability

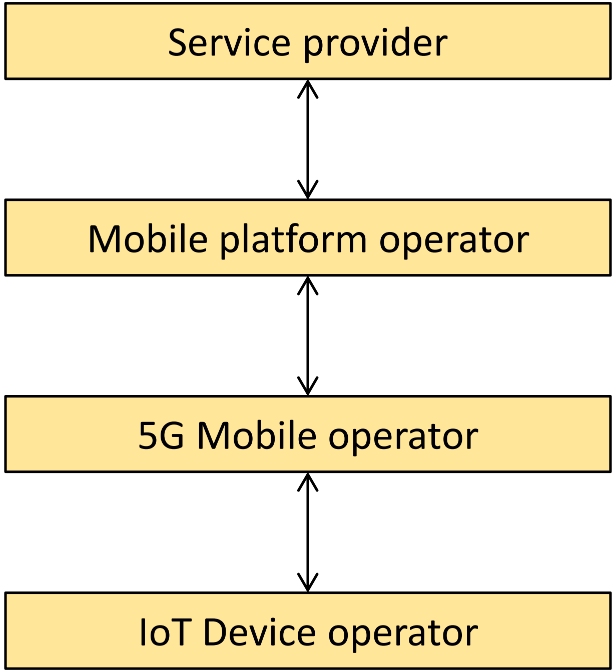
Marketplace Measures

ISO 27001 Categories of controls		Control
Information security policies	Management direction.	Data management policies
Human resource security	During employment	Internal cybersecurity preparedness
		External cybersecurity preparedness
Access control	Business requirements for access control	Requirements for service provider access
	System and application access control	Secure access from service provider
		Secure access to cloud storage provider
Cryptography	Cryptographic controls	**Confidentiality of personal data vaults**
		Anonymisation of data sets
Operation security	Operational procedures and responsibilities	Operation procedures for data search and processing
	Logging and monitoring	Logging capabilities
	Control of operational software	Operation procedures for transparency.
Communication security	Information transfer	Secure transmission of data
System acquisition, development and maintenance	Security in development and support processes	Secure data pipeline capabilities
		Cybersecurity monitoring capabilities
Information security incident management	Management of information security incidents and improvements	Alerting data processing chain
Information security aspects of business continuity management	Information security continuity	Assurance of cloud storage manager cybersecurity capabilities
		Periodic review of cloud storage manager cybersecurity capabilities
Compliance	Compliance with legal and contractual requirements	GDPR and cybersecurity compliance verification
	Information security reviews	Periodic review of interoperability

Conclusions

- Need for ecosystem design viewpoint
- Need for ecosystem risk analysis
- Need for interoperability of cybersecurity capabilities
- Need for Coordination of cybersecurity capabilities between different stakeholders of an ecosystem
- Ecosystem vision must be better explained at standardisation level

Example of 5G Ecosystem



www.trialog.com

Questions?