AUTOMAT CYBER SECURITY

Overview of the Cyber Security and Privacy framework in the context of CVIM

MOTIVATION AND PROBLEM SPACE

AutoMat CVIM Motivation

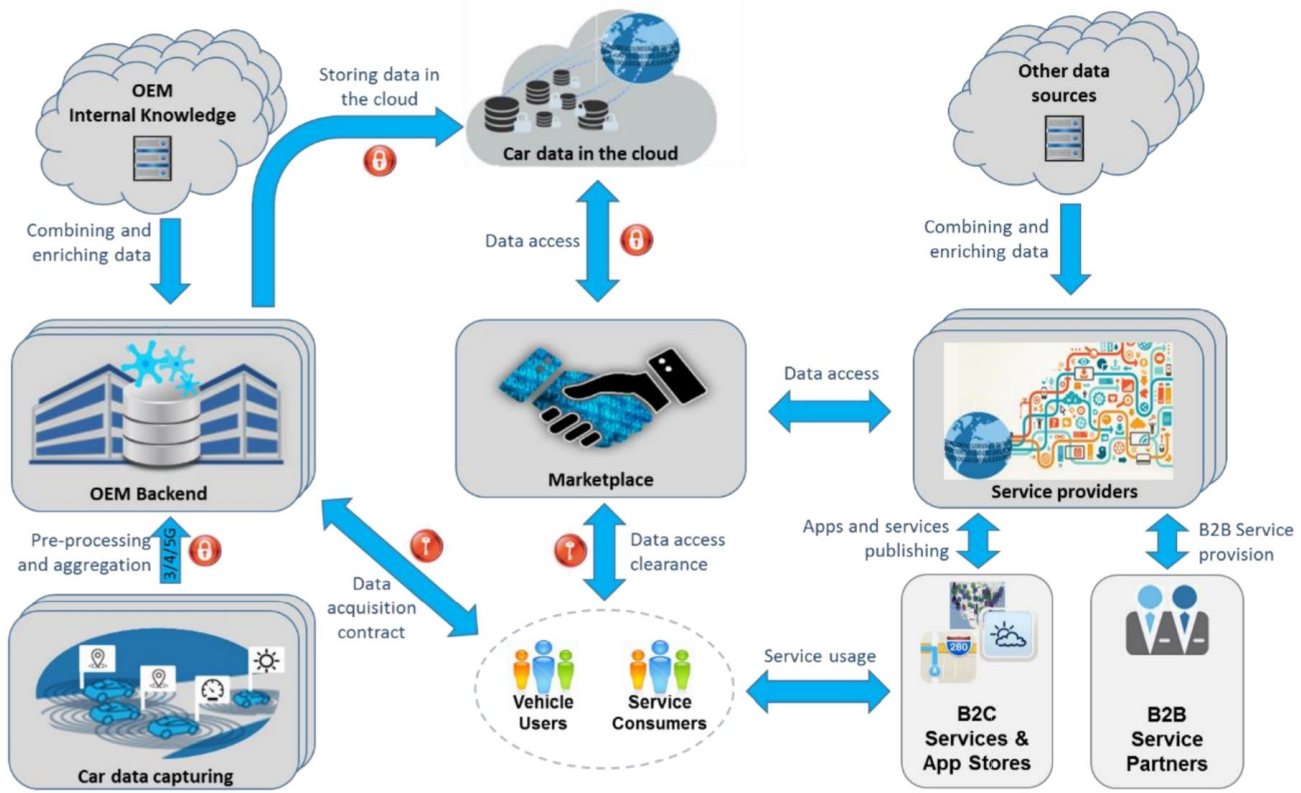
Huge amount of data produced by vehicles that open unexplored possibilities – both business and technical. This requires **big data approach** to handling and managing this data

Problem Area

Not able to establish open service ecosystem like in other industries – e.g. mobile industry

DATA CHARACTERISTICS

- Vehicle data
- Generated by different OEMs
- Owned by users
- Pre-processed by OEMs
- Stored in data vaults by Cloud Storage Providers
- Brokered by Data Marketplace
- Used by Service Providers
- Audited by users



CONTENTS OF THE FRAMEWORK

- Concepts and approaches that address each stakeholder's responsibilities
- Establishing security guidelines for each component of the AutoMat public ecosystem
- Answering to the needs for:
  - Ethics and legal support
  - Process for design compliant with security and privacy guidelines
  - Security and privacy component description
  - Security and privacy capability description at user level

STAKEHOLDERS

Major Stakeholders, Responsibilities and Relationships

STAKEHOLDERS

OEM

- Obtains data collection consent
- Operates OEM backend for data collection and pre-processing

Cloud Storage Provider

- Enforces user-based data access (CRUD operations, controlled by users)
- Establishes and maintains data vaults

Marketplace Operator

- Obtains data sharing consent
- Publishes offers by service providers for data access

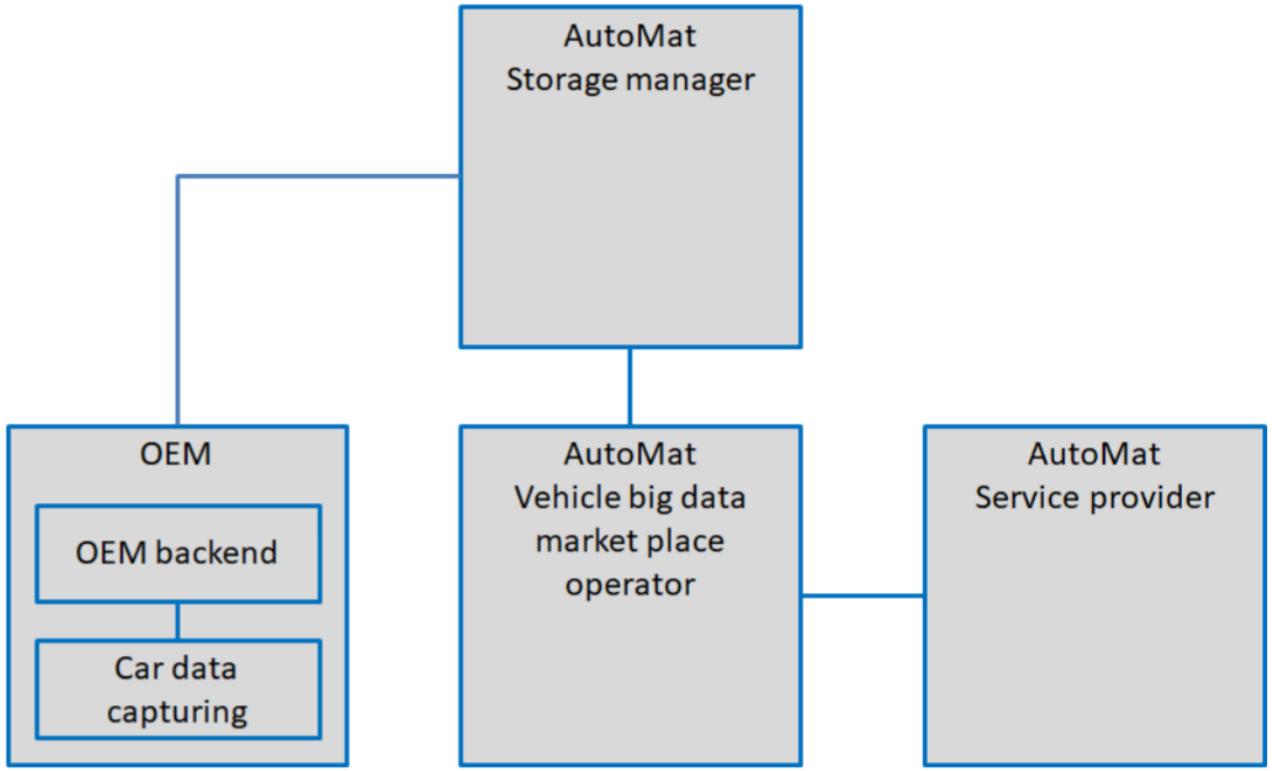
STAKEHOLDERS

Service Provider

- Utilizes data marketplace for data retrieval
- Enriches data

User

- Provides consents for data access and sharing
- Uses data marketplace for data auditing



METADATA – SOURCE FOR DATA PROTECTION POLICY DEFINITION

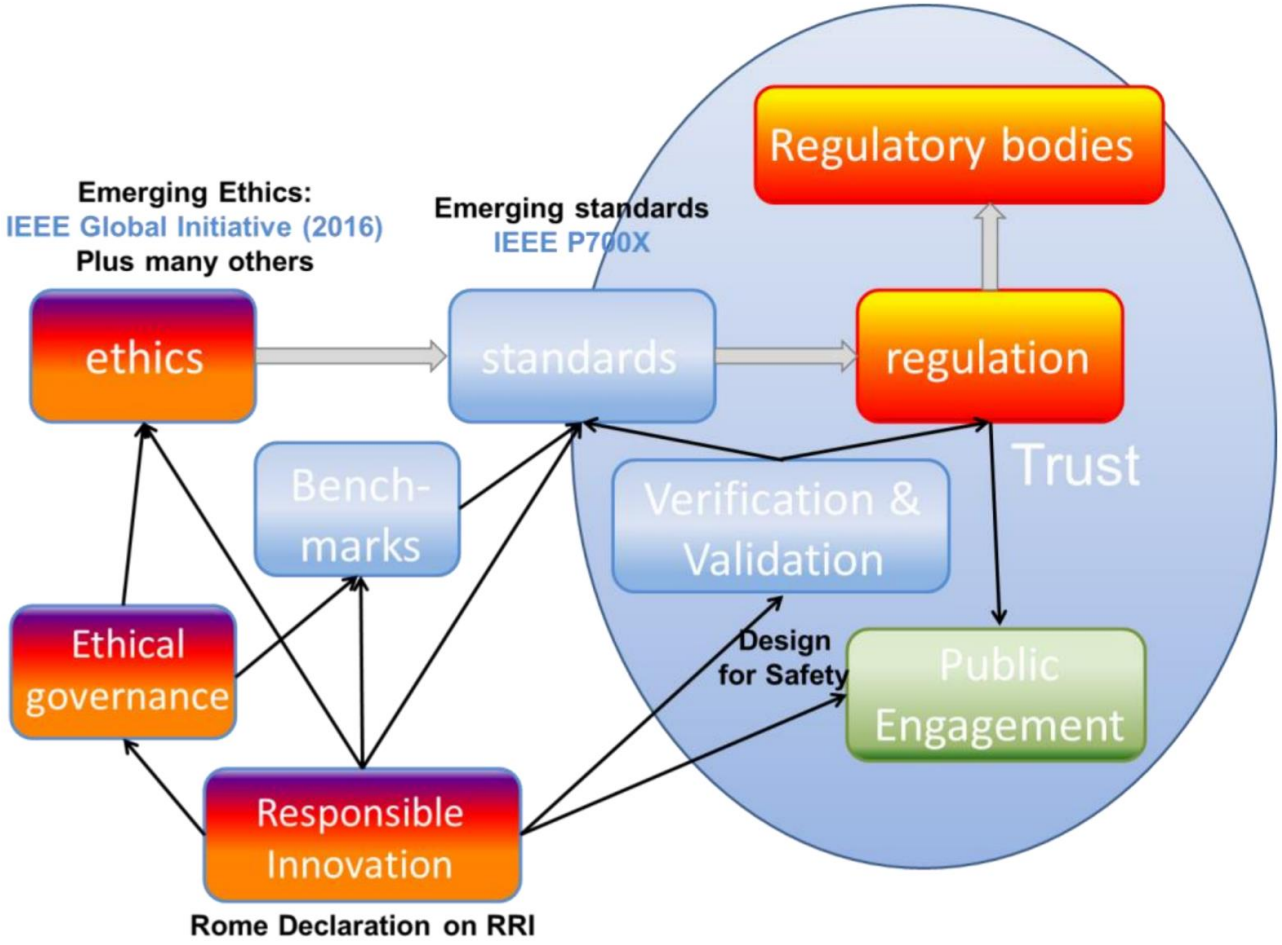
CVIM establishes of set of **metadata** pertaining to the data records that is used to enforce data protection policy:

- **Copyright stakeholders** - list of stakeholders with ownership rights
- **Data privacy level** - public, shared, private
- **Data stakeholders** - list of stakeholders with control capacity - controller, processor
- **Privacy veto rights** - policy parameters - consent, format jurisdiction, OEM / personal storage

ETHICAL AND LEGAL ASPECTS

MAIN OBJECTIVE

Turning ethics principles into **public trust** through **standardization** and **regulations** on the basis of **public engagement**



EMERGING STANDARDS – IEEE P700X

Adoption of **emerging standards** – IEEE P700X – concerned with definition of what is ethical governance including:

- Code of conduct
- Ethics training
- Ethical risk assessment
- Transparency

- **Applicable legislation**
  - Regulation 2016/679 (GDPR)
  - Directives around the European Strategy on Cooperative Intelligent Transport Systems (C-ITS)

SECURITY AND PRIVACY-BY-DESIGN PROCESS

SECURITY AND PRIVACY ATTRIBUTES

Security Protection Attributes	Privacy Protection Attributes
Confidentiality	Unlinkability
Integrity	Transparency
Availability	Intervenability

ISO/IEC 27000

ISO/IEC 27550

RISK ANALYSIS PROCESS

COMPLIANCE WITH THREAT, VULNERABILITY AND RISK ANALYSIS – TVRA

- Identification of target of evaluation
- Identification of objectives
- Identification of functional security requirements
- Systematic inventory of assets
- Systematic identification of vulnerabilities
- Calculation of the likelihood of the attack and its impact
- Establishment of risks
- Security and privacy counter- measure identification
- Countermeasure cost-benefit analysis
- Specification of detailed requirements

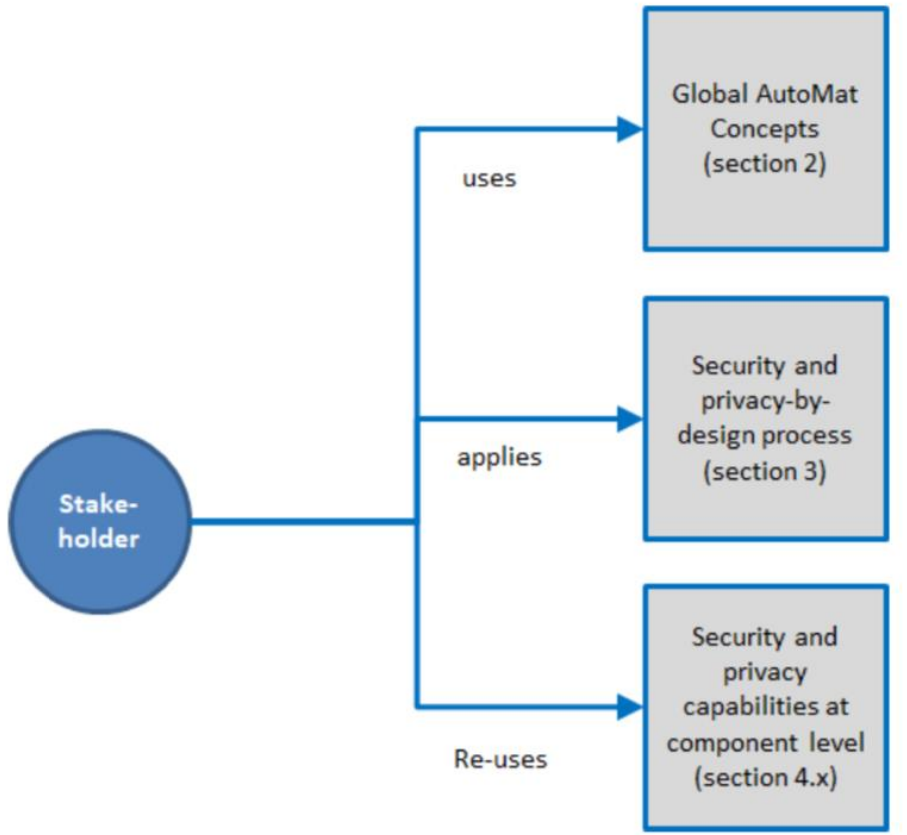
https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/04.02.03_60/ts_10216501v040203p.pdf

SECURITY AND PRIVACY AT COMPONENT LEVEL

Description of security and privacy analysis for each of the framework components – OEM (including in-vehicle and proprietary backend), Cloud Storage Provider, Marketplace, Service Provider

Each framework component analysis can be used independently. They have common secuirity and privacy items that are repeated among the comoinent descriptions for completeness

Each stakholder is responsible for implementing their own security and privacy model that is compliant with the global AutoMat concepts, applies the security and privacy design process and re-uses the component design and privacy capabilities



CONTENT OF THE SECURITY AND PRIVACY COMPONENT CAPABILITIES

- Characterization of the modules of the component – actors, use cases, architectural entities
- Typical business and contractual cybersecurity capabilities
- Typical cybersecurity threats
  - Threat modelling using STRIDE categorization
  - Threat modelling using LINDDUN categorization
- Typical breaches and impact for the component including threat-to-breach matrix (what threats can cause which breach)
- Typical measures to mitigate identified threats – categorization and contribution to identified threats

Threat	Property	Description
Spoofing	Authentication	The identity of users is established (or you're willing to accept anonymous users).
Tampering	Integrity	Data and system resources are only changed in appropriate ways by appropriate people.
Repudiation	Nonrepudiation	Users can't perform an action and later deny performing it.
Information disclosure	Confidentiality	Data is only available to the people intended to access it.
Denial Of Service	Availability	Systems are ready when needed and perform acceptably.
Elevation of privilege	Authorization	Users are explicitly allowed or denied access to resources.

STRIDE
PROPOSED BY MICROSOFT

Threat	Property		Description
Linkability	Hard privacy	Unlinkability	Hiding the link between two or more actions, identities, and pieces of information.
Identifiability		Anonymity	Hiding the link between an identity and an action or a piece of information
Non-repudiation		Plausible deniability	Ability to deny having performed an action that other parties can neither confirm nor contradict
Detectability		Undetectability and unobservability	Hiding the user's activities
Disclosure of information	Security	Confidentiality	Hiding the data content or controlled release of data content
Unawareness	Soft Privacy	Content awareness	User's consciousness regarding his own data
Non-compliance		Policy and consent compliance	Data controller to inform the data subject to the system's privacy policy, or allow the data subject to specify consents in compliance with legislation

LINDDUN
PROPOSED BY KU LEUVEN