

MOBILITY APPLICATIONS FOR SOFTWARE-DEFINED VEHICLES

White Paper



**An approach based on verifiable
credentials**

Authors

Albert Kos, Torsten Stange, Peter Lang

Continental Automotive Technologies GmbH
Research & Advanced Engineering

Research & Advanced Engineering (R&A) is responsible for research and predevelopment activities within Continental Automotive. Its vision: to research and evaluate innovative technologies and solutions for the mobility ecosystems of tomorrow. In doing so, R&A anticipates customer requirements and market trends, fosters partnerships, and thus gains a strategic advantage. R&A connects across business areas and industries by leveraging our core competencies and expanding our mobility markets. We deliver inventions and innovations through research and advanced technology, thereby accelerating market entry.

Acknowledgments

We would like to thank Sebastian Böttigheimer, Fabian Faller, Markus Fischer, Dr. Viktor Kress and Ilona Tzudnowski for their support in creating this white paper.

Disclaimer

This white paper serves exclusively for general information purposes. It has been carefully prepared to provide accurate and up-to-date information. However, no guarantee can be given for the correctness, completeness or up-to-dateness of the content. The information contained herein does not constitute legal, financial, technical or any other form of professional advice and should not be regarded as such.

Use of the information provided in this white paper is at own risk. The publisher accepts no liability for any loss or damage arising directly or indirectly from the use of the content.

All trademarks, trade names and logos mentioned in this document are the property of their respective owners. The reproduction or distribution of this white paper, in part or in whole, is not permitted without the express permission of the publisher.

Contents

Executive Summary	5
1. The Mobility of Tomorrow	
1.1 The vehicle as part of the cloud ecosystem	7
1.2 Multimodal mobility	7
1.3 Data-driven applications	8
1.4 Improvement of advanced driver assistance systems	8
2. Challenges in the Integration of Mobility Applications	
2.1 Open, data-driven ecosystems	10
2.2 Decentralized management of identities and data	10
2.3 Relationships between OEMs, users and service providers	11
2.4 Integration of third-party software in the vehicle	12
3. A Sovereign and Trustworthy Digital Ecosystem of the Future	
3.1 Gaia-X federation and trust framework	14
3.2 Identity management and verifiable credentials	15
3.3 Trust models and business models	17
3.4 Provision of services, data flow and communication	19
3.5 Cloud-native and mixed-criticality applications	21
4. AGEDA Framework Authorization and Identity Management	
4.1 Gaia-X compliance and SSI	24
4.2 Software components and features	24
4.3 AGEDA plugins and their implementation	26
4.4 Integration into the Gaia-X infrastructure	28
4.5 AGEDA toolchain and digital twin services	31
Conclusion and Outlook	33

Executive Summary

This white paper envisions vehicles as a versatile platform for executing software solutions, moving beyond their role as a mere means of transport. The aim is to open up the possibility of implementing innovative applications directly in the vehicle and offering users added value through **personalized mobility solutions**. At the same time, the requirements for security, data protection and integrity of the functions provided need to be ensured.

Mobility applications are increasingly becoming a central component in meeting the mobility requirements of tomorrow. It is necessary to create a framework that ensures both the seamless integration of new applications and compliance with strict security and data protection standards. Our research shows that so-called **verifiable credentials** (VCs) are a promising approach for ensuring security and privacy when using vehicles as an execution platform for mobility applications.

This white paper is based on the findings of the **GAIA-X 4 AGEDA project**. The aim of this project is to analyze the requirements for the vehicle as part of the cloud ecosystem, to develop a suitable framework and to demonstrate its effectiveness through use cases. The necessary fundamentals are explained to facilitate understanding. The key aspects, such as how the use of VCs is an effective way of ensuring secure and flexible access to vehicle data and functions, are explained in more detail. The advantages and necessity of establishing the framework developed in the project and its underlying concepts as an essential part of a modern vehicle architecture in the software-defined vehicle (SDV) are highlighted.

The proposed solution demonstrates the benefits of VCs as a forward-looking technology for the execution of in-vehicle mobility applications. The **AGEDA framework** serves as a proof of concept (PoC) to realize the full potential of these applications and lay the foundation for innovative in-vehicle services with a secure, scalable architecture.

The mobility of tomorrow is connected, personalized, flexible and multimodal. Here, mobility applications are playing an increasingly important role. They provide access to a wide range of services that can make journeys more pleasant, safer and more efficient.



1. The Mobility of Tomorrow

1.1 The vehicle as part of the cloud ecosystem

One prerequisite for the use of mobility services is the integration of vehicles into the cloud ecosystem. This enables vehicles to communicate with other vehicles, the traffic infrastructure and mobile devices in order to exchange real-time data and adapt the journey to the individual needs of the user. In addition, vehicles can serve as mobile sensors in order to collect traffic information in real time and optimize traffic. Increasing connectivity requires secure and reliable communication between vehicles and cloud services to guarantee the confidentiality, integrity and availability of data.

1.2 Multimodal mobility

Flexibility and independence are the most important factors for people when choosing their means of transportation. Multimodal mobility services could provide a solution here. This is because they connect various mobility services with each other, making it easier to combine different modes of transportation [such as car, bicycle, bus, train and taxi] on a single route.¹ Mobility applications serve as central platforms for booking, paying for and combining the various means of transport to offer users a smooth travel experience.

¹Source: German Federal Ministry for Digital and Transport (BMDV):
[BMDV – Mobility as a service: flexible travel from A to B with multimodal mobility services](#)

1.3 Data-driven applications

The introduction of data-driven applications in the field of mobility may require significant changes in business processes and culture. These applications rely heavily on data and its analysis to provide functions and services.

It is essential that the data collected is accurate, complete and consistent. The protection of sensitive data and compliance with legal regulations such as the General Data Protection Regulation (GDPR) are top priorities in this context.

1.4 Improvement of advanced driver assistance systems

Another important aspect is the continuous improvement of safety in the vehicle. Advanced driver assistance systems (ADAS) use real-time data and sensors to detect potential hazards and warn the driver in a timely manner.

These systems are increasingly intervening in driving operations by, for example, adjusting the speed, keeping the vehicle in lane or braking automatically. In the long term, these technologies aim to enable fully automated driving, in which the vehicle can take over all driving functions.² Mobility applications play a crucial role in providing advanced driver assistance systems with real-time data and services – for example by providing warnings about danger spots previously reported by other vehicles.

²Source: Continental Automotive Technologies GmbH: [Mobility Study 2020 | From Driver to Passenger](#)



The integration of mobility applications in vehicles, the necessary connection to an open ecosystem and the decentralized management of identities and data, however, also raise questions.

2. Challenges in the Integration of Mobility Applications

2.1 Open, data-driven ecosystems

Services offered in an open ecosystem must comply with the principles for the processing of personal data. Data must come from trustworthy sources and be processed for clearly defined purposes. In addition, data as a digital commodity needs to be securely managed within the supply chain in order to ensure its integrity and security. Strict compliance with these requirements is a fundamental prerequisite for opening up vehicles as a platform for mobility applications.

2.2 Decentralized management of identities and data

The changed requirements for data protection and privacy place new demands on identity management. Users want to retain control over their data and decide which data they share with a provider. Centralized identity management systems are outdated and do not meet the requirements for data protection and data security. SSI [self-sovereign identity] is intended to solve the challenges and problems of existing digital identity management systems and is regarded as the next step in the development of digital identities.³

³Source: Fraunhofer Institute for Applied Information Technology FIT: [Self-Sovereign Identity White Paper, 2021](#)

Centralized or federated identity management systems are often easier to implement, but they also have disadvantages. As a central weak point, they are vulnerable to attacks. Moreover, they are often not user-friendly and require a high level of trust between the parties. SSI better meets the requirements because its architecture focuses on user empowerment, security and privacy.

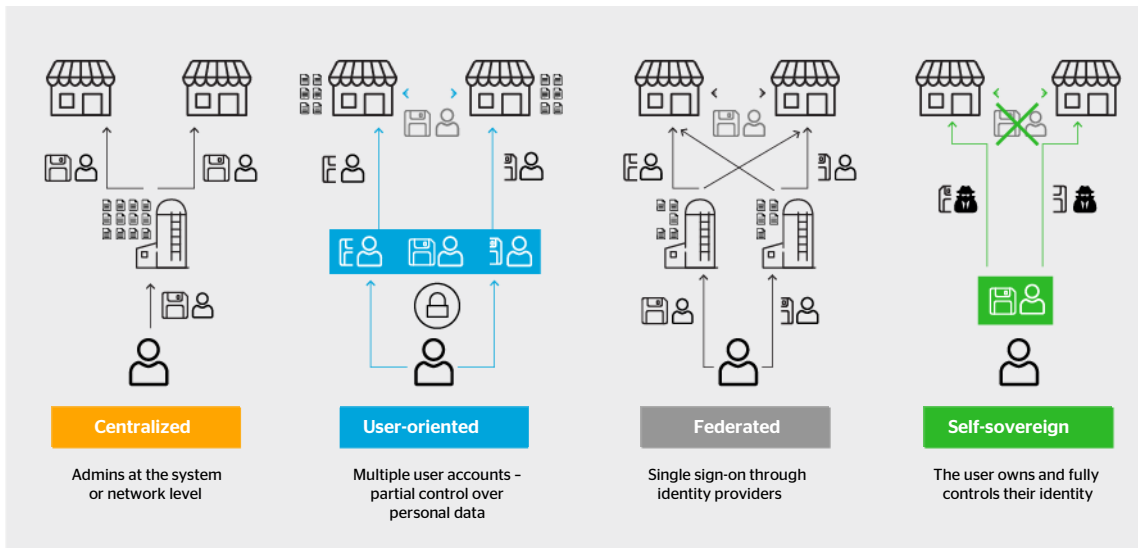


Figure 1: Comparison of different identity management systems⁴

2.3 Relationships between OEMs, users and service providers

Who owns which data and what is it used for? Here, it is important to understand who the actors are and how they relate to one another. The relationships between vehicle manufacturers (original equipment manufacturers, or OEMs), users and service providers are complex and require a clear understanding of roles. The mobility service provider must take into account the various roles and responsibilities of OEMs, vehicle owners and vehicle users to make sure that all legal and contractual obligations are met and smooth operations are ensured.

⁴Source: Fraunhofer Institute for Applied Information Technology FIT: [Self-Sovereign Identity White Paper, 2021](#)

- › *OEMs*: Bear responsibility for safety, emissions and technical standards, are liable for errors and must comply with strict standards.
- › *Vehicle owners*: Responsible for maintenance, insurance and legal use
- › *Service providers*: Responsible for the provision of mobility services, compliance with data protection regulations and the security of user data

The role of the supplier, such as Continental, lies in the provision of technical components (e.g. the AGEDA framework), systems or services that are necessary for the functionality and further development of vehicles and mobility solutions. Suppliers act as trusted partners to OEMs and other actors in the value chain.

2.4 Integration of third-party software in the vehicle

The integration of third-party software (here: mobility applications) in the vehicle requires strict compliance with safety and data protection guidelines. In addition to the General Data Protection Regulation (GDPR), industry-specific standards also have to be observed. The most important standards include:

- › ISO 26262 (Functional safety)
- › ISO 21448 (Safety of the intended functionality)
- › ISO/SAE 21434 (Cybersecurity)
- › ISO/IEC 27001 (Information security)
- › ISO 15504 (Software process assessment)
- › ISO 14229 (Diagnostic systems)

The challenges identified require technological solutions that are scalable, secure and adaptable.

The integration of mobility applications into the vehicle requires a secure and user-centered framework that guarantees the privacy and security of users.



3. A Sovereign and Trustworthy Digital Ecosystem of the Future

3.1 Gaia-X federation and trust framework

Gaia-X is a European initiative aimed at creating a secure, trustworthy and sovereign data infrastructure in Europe. Federations are a central component of Gaia-X, as they promote collaboration between various participants while allowing the respective owners to retain control over data and services.

The trust framework in Gaia-X is a set of rules that defines the minimum requirements for being part of the Gaia-X ecosystem. It forms the basis for functional and trusting cooperation within the federation. These rules can be extended and adapted by the federation.

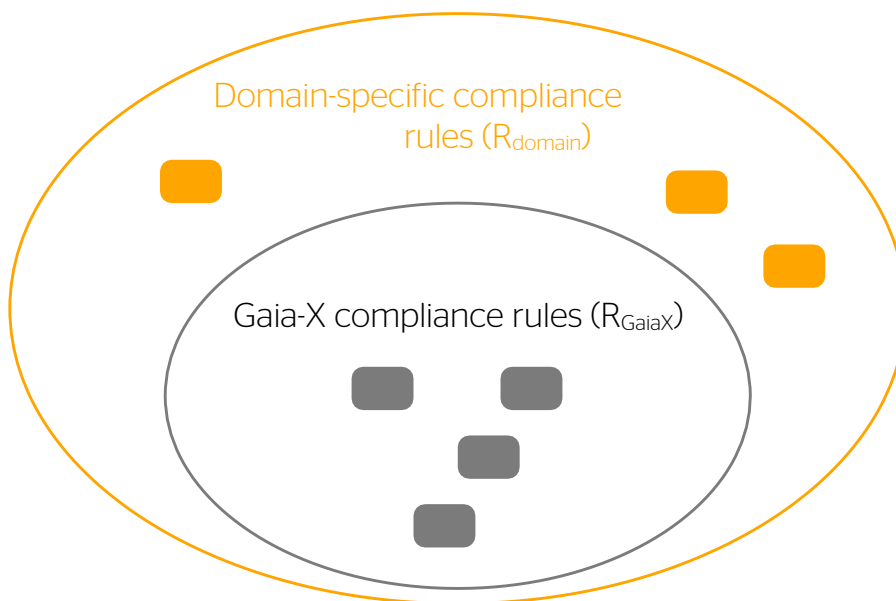


Figure 2: Trust framework scope

The Gaia-X Digital Clearing House (GXDCH) serves as the audit and verification body for compliance with the rules and requirements. It enables participants to automatically check and confirm their compliance with the Gaia-X rules. The rules for compliance with security and data protection guidelines are defined by the Gaia-X Policy Rules Committee.

3.2 Identity management and verifiable credentials

The components of SSI include standards such as decentralized identifier (DID) and specifications such as the VC Data Model, which ensure interoperability and security.

VCs are standardized by the W3C consortium with the goal of building digital trust in order to align user privacy with the benefits of digital certificates. VCs enable a verifiable digital exchange of credentials and attribute attestations via any communication channel[...].⁵

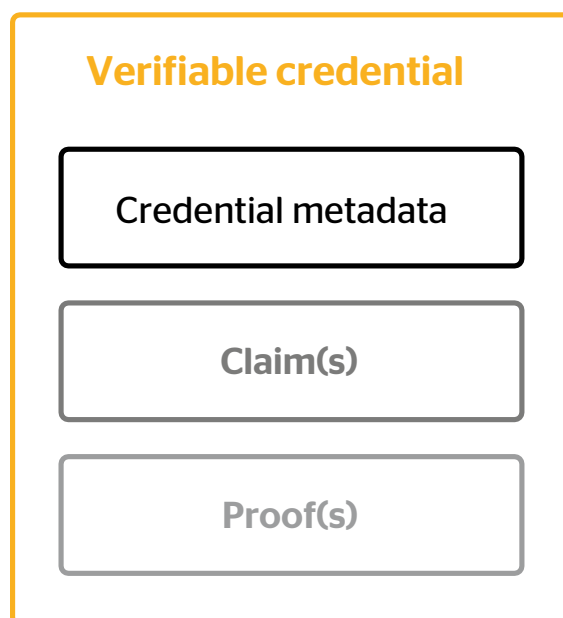


Figure 3: Main components of a VC within the W3C Verifiable Credentials Data Model 2.0

⁵Source: Fraunhofer Institute for Applied Information Technology FIT: [Self-Sovereign Identity White Paper, 2021](#)

VCS enable a decentralized, user-centric approach for the secure and data protection-compliant exchange of identities. Users retain control over their data without having to rely on central parties. VCs consist of cryptographically signed claims that are issued by a trusted party (issuer), managed by the holder and can be selectively presented to a verifier. Known as the triangle of trust, this model clearly separates the roles and reduces dependencies on central authorities. The VCs contain information about the identity of the parties involved, the certification requirements and the access rights to resources. Through the issuance and verification of VCs, the trust relationship between the actors is ensured. The following VC issuers are used within the framework of AGEDA:

- › *OEM*: Creates VCs for the certification of service providers and the use of end devices
- › *Service provider*: Creates VCs for the provision of mobility applications

Zero-knowledge proofs (ZKPs) enhance data protection by allowing specific attributes, such as age, to be verified without disclosing unnecessary information like the exact date of birth. The AGEDA framework leverages these technologies to provide a secure and user-centric platform that ensures both the protection of sensitive data and minimization of data disclosure.

3.3 Trust models and business models

Thanks to the dynamic structure of VCs, multiple wallets (i.e. an application that enables a person or organization to use digital credentials [claims]) and different authorization levels can be managed. The introduction of a well-designed role model allows precise control of access rights.

Role-based user perspective

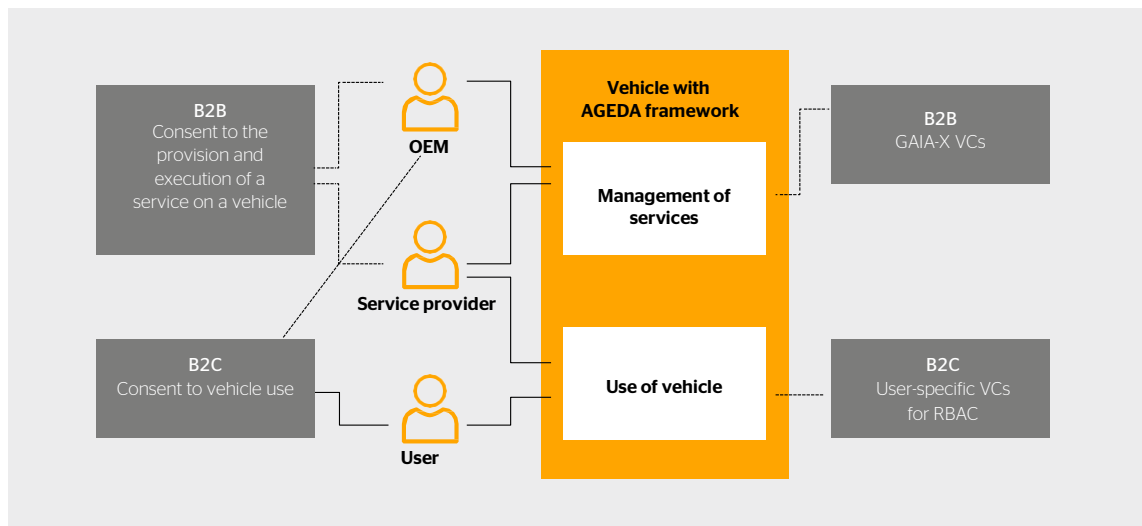


Figure 4: AGEDA roles and their relationships from the user perspective

- › **OEM**: Is responsible for the integration and operation of mobility applications in the vehicle; it can certify service providers according to their requirements and give the user the opportunity to make use of service offerings
- › **Vehicle user**: Can grant, restrict or withdraw consent for the use of a service in the vehicle; if necessary, the user can identify their data and its usage
- › **Service provider**: Provides services for the vehicle; it can register with the GXDCH and create a service VC that contains the authorizations for using the service in the vehicle

The OEM can extend the role model by defining user groups (e.g. mechanics, drivers). This facilitates participation in a Gaia-X federation without compromising the security of the overall system.

Trust models and business models can be derived from the roles and relationships shown in Figure 4.

The AGEDA framework supports the following models:

- › *B2B*: The service provider links its policies (e.g. compliance requirements) directly with Gaia-X-compliant service VCs, thereby ensuring a high level of security and traceability.
- › *B2C*: Users connect their digital wallet to the AGEDA framework; through user-defined VCs and ZKPs, they can grant their consent in a granular manner, while at the same time meeting the requirements for data protection and privacy

B2C VCs are individually designed to cater to the specific usage scenarios and preferences of users. The AGEDA framework manages the identities and their access rights, for example to certain vehicle functions or digital services. This allows services to be provided flexibly for different vehicle users or deactivated if required.

3.4 Provision of services, data flow and communication

A key objective of the AGEDA framework is to facilitate the integration of mobility services into the vehicle.

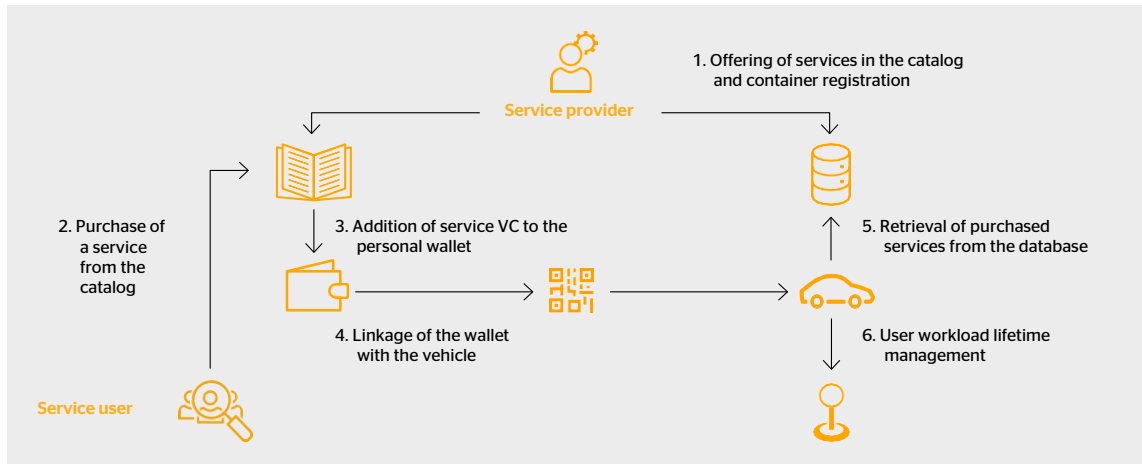


Figure 5: Provision of services

From the perspective of a service provider, the process of service provision can be reduced to two steps:

1. Provision of the application as a container image in a container registry
2. Publication of the service offering as a VC in a service catalog

The OEM can check the VC, test the application and activate it for the user. The user can check the VC and give their consent for use of the mobility application in the vehicle.

To lower the participation barriers for service providers, the concept of freedom from interference is applied, in which a system or a component within a system can function without external interference or impairment. This results in the following advantages when providing services:

- › *Reduction of participation barriers*: Suppliers of non-safety-relevant software benefit from simplified requirements, as they do not need to undergo a complete hazard and risk analysis (failure modes, effects and diagnostic analysis, or FMEDA).
- › *Safety guarantee through isolation*: Errors or security vulnerabilities in non-safety-critical software do not affect safety-relevant functions in the vehicle
- › *Flexibility for OEMs*: A wider range of software and services can be integrated without jeopardizing the functional safety of the vehicle


The AGEDA framework handles the verification of the VC and controls and manages communication as well as an application's access to the vehicle's resources (sensors, actuators and runtime environment). For this purpose, the VCs contain parameters that allow an application to be specifically configured, parameterized and executed in the vehicle. They are comparable to Helm charts, which contain a collection of configuration files and templates that enable the easy deployment, management and version control of a complex Kubernetes application.

3.5 Cloud-native and mixed-criticality applications

By integrating the vehicle into the cloud ecosystem, the system boundaries are expanded and new demands are placed on the system. To ensure the integrity of the system, container technologies (cloud-native) are used in addition to VCs. Containers are standardized units of software that contain all the necessary libraries, dependencies and configurations, and enable the isolation of applications and the provision of services in a consistent environment. The applications are executed in containers that are isolated through the use of different runtime environments. The AGEDA framework supports the execution of mixed-critical applications by prioritizing (orchestrating) and isolating applications.

By using cloud-native technologies, a hexagonal architecture can be implemented that enables loose coupling to the technical implementation while simultaneously providing high cohesion with respect to the vehicle domain and the relevant user requirements. The core of a hexagonal architecture consists of the application itself, which is connected to the outside world through ports (interfaces) and adapters (implementations). This allows external dependencies such as databases or user interfaces to be easily exchanged without affecting the core logic of the application.

Use of the AGEDA framework ensures that only tested and approved applications are installed and executed in the vehicle context.



The AGEDA framework allows the OEM to manage the identities and access rights of service providers and users.

4. AGEDA Framework Authorization and Identity Management

The OEM registers its vehicles by representing the identity of the vehicles in its domain through a DID. The service provider can verify the identity of the vehicles and determine whether they are under the control of the OEM.

To enable traceability of who is behind the identities, Gaia-X exclusively uses the did:web method and requires participants (e.g. the OEM) to provide an EV-SSL or eIDAS certificate, the public part of which is published via the did:web method. The participant's private key remains in a wallet, which is managed by the AGEDA framework.

The DID document serves to disclose the public keys with which VCs or verifiable presentations (digital credentials that are issued by a trusted source and can be checked by a third party) can be verified, for example in the form of JSON Web Keys (JWKs). However, it does not replace a conventional SSL/TLS certificate: the latter protects HTTPS traffic, while the DID document makes domain ownership verifiable.

To prove that an AGEDA instance is managed by the OEM, the OEM, as the service user, must provide the public key of the AGEDA instance under its own domain (e.g. <https://einOEM.de/.well-known/some-vehicle-did.json>). This allows the AGEDA framework to manage the identities of the vehicles and delegate access to the container database provided by the service provider to the AGEDA instance.

4.1 Gaia-X compliance and SSI

The basis for Gaia-X compliance is provided by the Gaia-X architecture document. A key element for compliance is the GXDCH. This ensures that the participants of a federation can trust one another and follow defined ontologies for interoperability. Thanks to the modular structure of the AGEDA framework, other VC and DID methods can be used by replacing the Gaia-X connector with a suitable component.

To ensure seamless integration of novel SSI technologies with existing authorization systems such as OAuth2.0, a credential offering based on OIDC4VC is used within the AGEDA framework to coordinate user workload access to vehicle resources.

The AGEDA framework is treated as a public client of the service provider and, by proving the identity of the OEM, gains access to mobility services that comply with the OCI distribution specification.

4.2 Software components and features

The AGEDA framework manages the entire life cycle of a mobility application, from deployment to updating or deactivation in the vehicle. The features required for this purpose can be summarized as follows:

- › Control of data flows between actors and networks using VCs
- › Cloud-native processes for the integration and development of mobility applications in the vehicle
- › Abstract representation of vehicle sensors and actuators and their representation as a digital twin

To implement these features, the AGEDA framework is divided into three main components: Gaia-X connector, edge enabler and platform services.

The main tasks of the individual components are:

- › *Gaia-X connector*: Management of identities and access rights by VCs (B2B/B2C)
- › *Edge enabler*: Orchestration (cloud-native applications) and node management
- › *Platform services*: Abstraction of vehicle components such as actuators, sensors, execution and storage units, the networks between the computing units, as well as the provision of system services that span across a number of services.

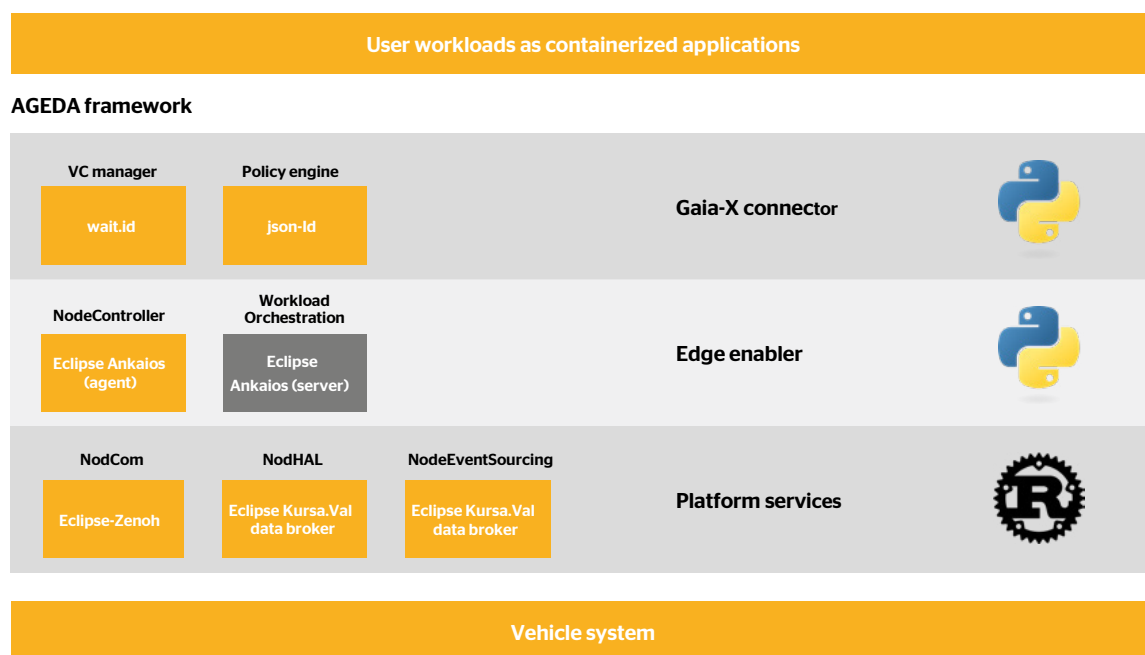


Figure 6: AGEDA framework – main components

4.3 AGEDA plugins and their implementation

Thanks to the innovative plugin concept of the AGEDA framework, the individual components can be flexibly extended and adapted. Plugins implement specific functions of the AGEDA components and can be divided into the following categories:

Gaia-X connector plugins

- › *VC manager*: Manages the user's VCs issued by the OEM and service provider
- › *Policy engine*: Ensures compliance with the defined access rights

Edge enabler plugins

- › *Workload orchestration*: Orchestrates the user workloads and ensures that they are only executed under the defined conditions
- › *NodeController*: Manages and monitors individual nodes in the vehicle and ensures that the user workloads are executed on the appropriate nodes

Platform services plugins

- › *NodeCom*: Coordinates communication between the vehicle nodes and monitors the status and functionality of the AGEDA framework
- › *NodeHAL*: Provides the hardware abstraction layer for the vehicle nodes
- › *NodeEventSourcing*: Saves events that occur on the vehicle nodes and enables traceability (audit trail)

The AGEDA plugins are designed to be flexible and can be replaced by components with similar functions to enable integration into other systems and ensure interoperability.

Plugin	Implementation
VC manager	wait.id
Workload orchestration	Ankaaios client
NodeHAL	kuksa.val
NodeEventSourcing	duckdb
NodeCom	Zenoh
NodeController	Ankaaios agent

Table 1: Overview of AGEDA plugins and their implementation

4.4 Integration into the Gaia-X infrastructure

The Gaia-X specification is recommended as an entry point for understanding the Gaia-X infrastructure. Gaia-X-compliant credentials provide the necessary elements of trust for creating ecosystems that operate according to a jointly defined governance. The Gaia-X credentials ensure that the rules agreed between the participants are verified and can be validated at any time.

The central point of contact for automatically checking compliance with the Gaia-X rules is the GXDCH. This clearing house ensures that the Gaia-X rules are adhered to and that participants receive the necessary compliance level credentials.

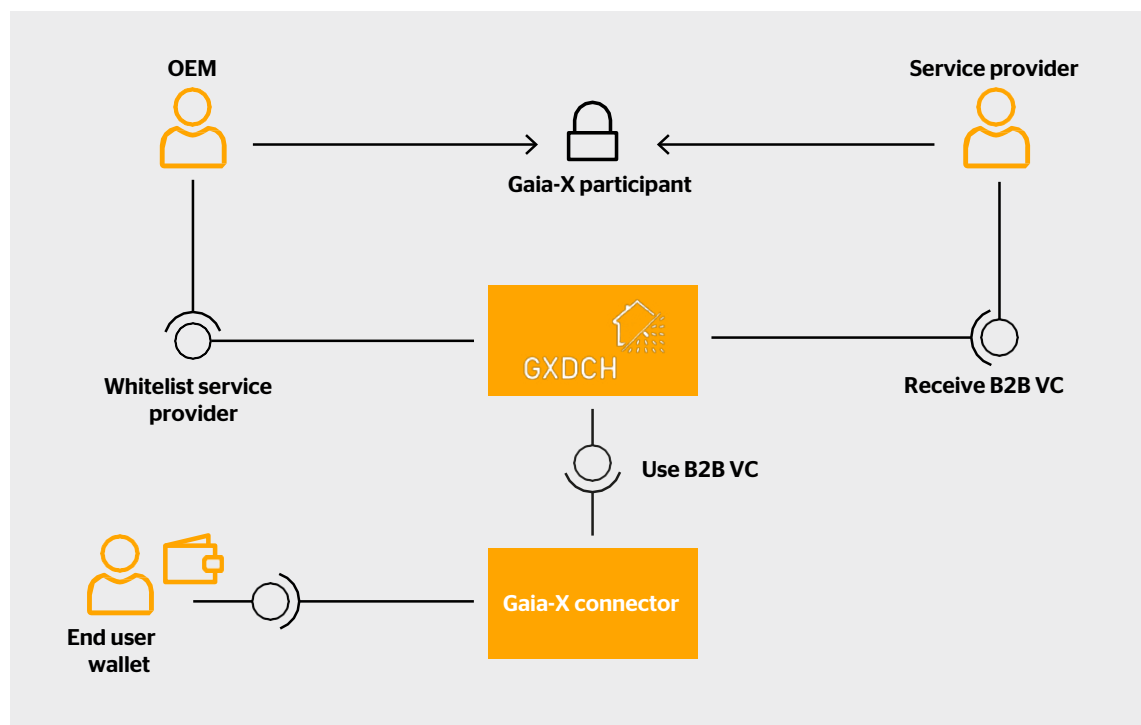


Figure 7: Internal processes for managing credentials between OEM, service provider and user

Based on GXDCH version v2 Loire, a clearing house can be self-hosted or used as a service. However, to obtain a compliance label, an official clearing house must be used. The main components are:

- › *Registry*: Used by the compliance service; but can be used directly to validate VCs
- › *Compliance services*: Implementation of the Gaia-X compliance criteria
- › *Notary*: Registers a company using vatID, leiCode or EORI
- › *Credential Event Service (CES)*: Enables VCs to be distributed within the federation

All offerings from Gaia-X providers are referred to as services. These can consist of various types of physical or virtual resources. A service description that follows the Gaia-X scheme and whose information is validated by the Gaia-X Compliance Service becomes a Gaia-X Service Offering Credential.

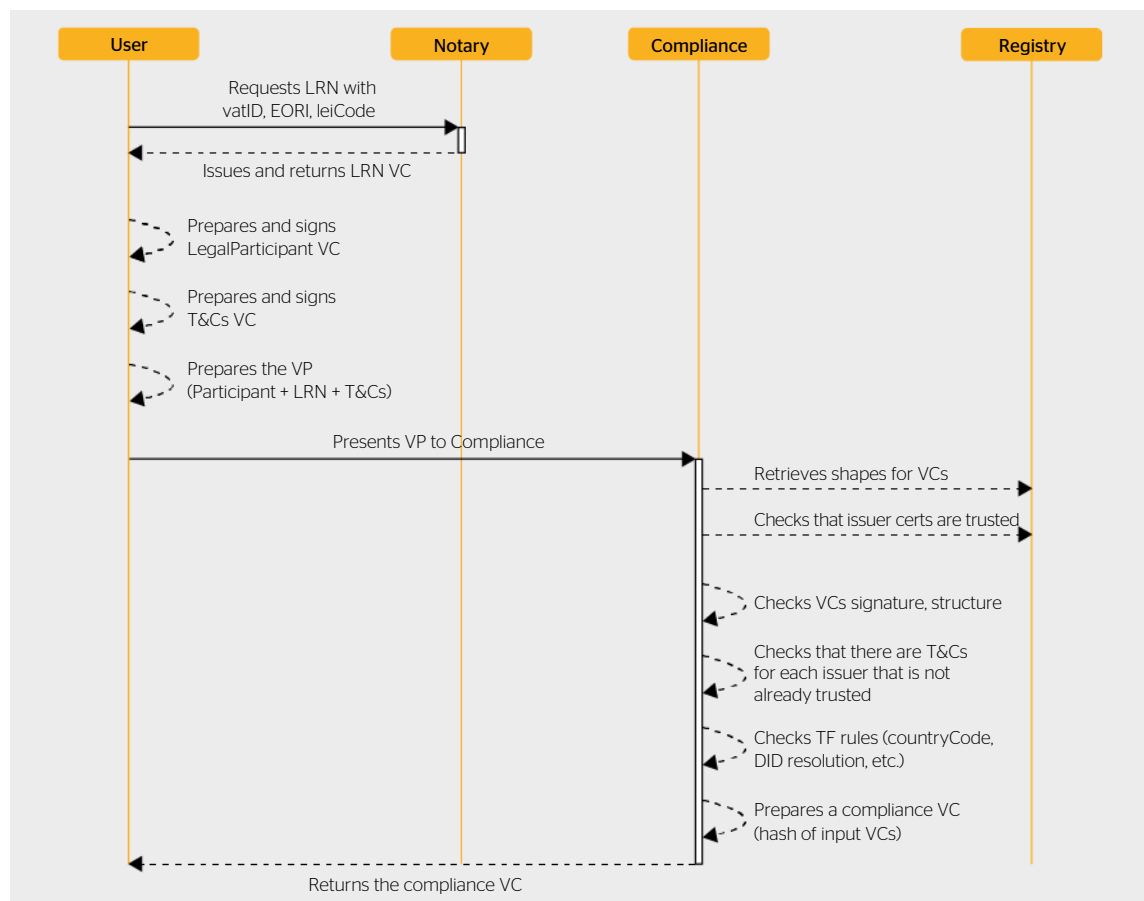


Figure 10: Gaia-X Compliance API

The service offering for the AGEDA framework is a container image which is provided in a container registry, e.g. JFrog container registry. An AGEDA service offering contains the following Gaia-X-compliant information as the subject of a B2B VC:

- › The identity of the service provider
- › URL to the container image
- › The certification requirements (optional)
- › Access rights to the sensors and actuators (optional)
- › Vehicle status conditions under which the application may be executed (optional)

In order for the AGEDA framework to be integrated into the Gaia-X infrastructure, a VC has attributes that are validated by the Gaia-X Compliance Service. Using the Gaia-X ontology, the declaration must contain either a resolvable identifier or a contact form for requesting further information that refers to the legally binding action offered by the provider.

The ontology, shapes and schemas are automatically updated by the Gaia-X Service Characteristics Working Group CI. The trusted issuers and any revocation lists are managed by an InterPlanetary File System (IPFS) pinning service.

This service is not intended to be used by parties other than the Gaia-X AISBL (Association Internationale Sans But Lucratif).

Although the service itself is hosted centrally, the artifacts are not hosted centrally (due to the nature of the IPFS hashtable). Each participant can decide to use their own IPFS to distribute the files.

4.5 AGEDA toolchain and digital twin services

The AGEDA framework supports the service provider right from the development stage. The provider can develop and test their application in a virtual environment before the application is adapted to and transferred onto a vehicle. The AGEDA framework provides tools that support the development, provision and operation of in-vehicle applications:

- › *Workbench*: DevOps pipeline, DevContainer and container registry for the development and deployment of applications
- › *Service catalog*: Service provider's service offering database as VC in the service catalog
- › *Digital twin services*: Enable the development and testing of applications in a virtual environment before they are transferred to the vehicle

The digital twin of the vehicle is a virtual representation of the physical vehicle that contains all relevant data and functions. A virtual hardware platform is provided that allows the target software to be tested in a bit-identical manner. In addition, a virtual environment is made available in which the software can be tested under realistic driving conditions, with either synthetic or real data supplied for that purpose.

This approach enables software testing in the initial phases of the development process, allowing issues to be identified and resolved at an early stage. This allows the service provider to develop the software faster and more cost-effectively. Moreover, the OEM can validate and approve the software early on in the development process.

To meet the demands of tomorrow's mobility, it is necessary to develop new technologies for vehicles and the associated ecosystem while taking existing standards and regulations into account.



Conclusion and Outlook

This white paper makes a concrete contribution by examining the possibilities and the necessity of establishing mobility applications as an essential part of vehicles with modern SDV architectures. It demonstrates how the proposed framework for the secure management and exchange of data using verifiable credentials (VCs) is structured within a mobile ecosystem and how it can be practically implemented. The roles and the resulting relationship between the actors enable a trustworthy business relationship between OEM, service provider and user.

Despite the numerous advantages, there are also some open issues and risks that need to be considered when implementing and using the framework. This includes acceptance by vehicle manufacturers, integration into existing systems, scalability and the security of the system. Although the framework offers high security standards, there may still be concerns regarding security and data protection, especially when processing sensitive vehicle and user data. User acceptance of the framework is also an important factor. They need to understand and accept the new technologies and processes.

Through the continuous development of the framework as well as partnerships with OEMs and service providers, these challenges can be overcome and a substantial contribution made to the mobility of tomorrow.

Continental Automotive Technologies GmbH

Guerickestraße 7

60488 Frankfurt am Main, Germany

Phone: +49 69 7603-01

E-mail: info.automotive@continental-corporation.com

Legal notice:

All rights reserved

© 2025 Continental Automotive Technologies GmbH, Frankfurt