Technical Solutions to Support Automotive Right to Repair

Technical Feasibility for Right to Repair

Questions Raised about Right to Repair:

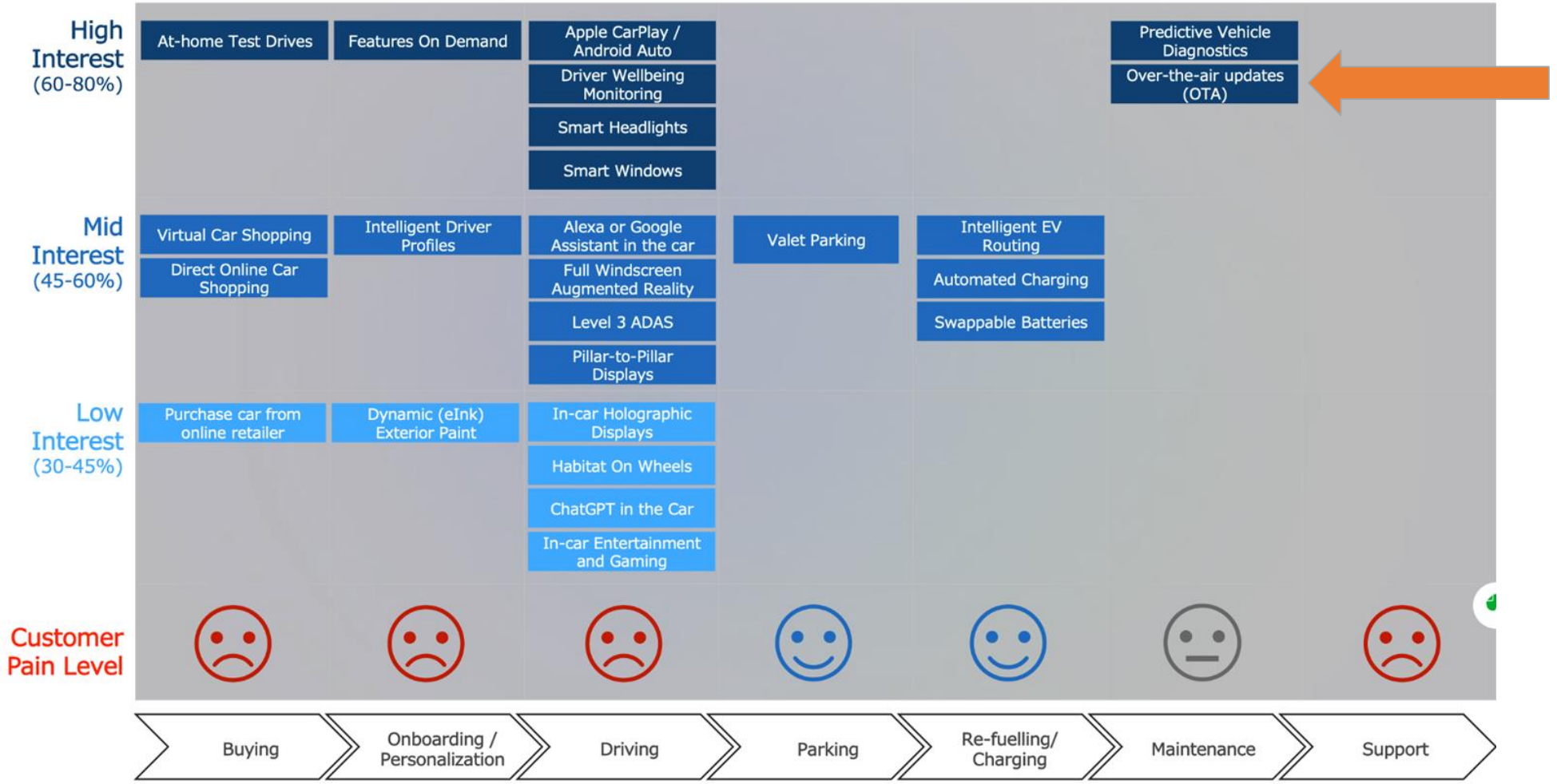
- Is Right to Repair technically feasible?
- Can it be deployed with existing technology?
- Can it be implemented safely over long-distance (cellular) connections?
- Does it require OEMs to remove critical safety features?

Why is Bluetooth-only not a viable option?

- OEMs are already rolling out and marketing remote diagnostics that drive customers directly to their dealer network and preferred partners (see this example from BMW)
- Independent repair shops require the same level of remote diagnostic capability
- Capabilities performed remotely can be limited

autocare™ ASSOCIATION
Independence drives us.

Value Proposition for Drivers



Source: SBD Automotive (https://www.sbdautomotive.com/)

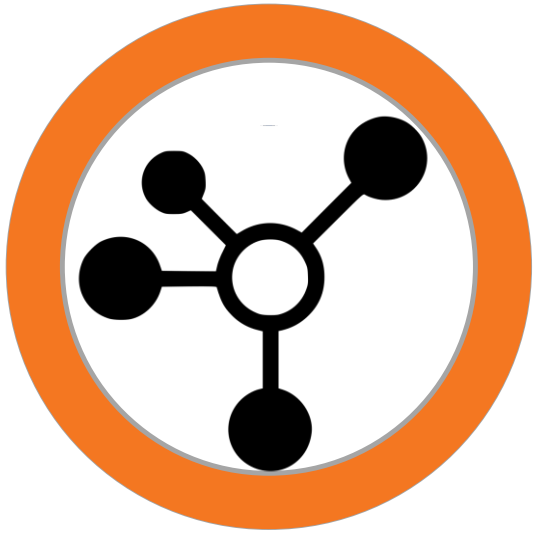
autocare™ ASSOCIATION
Independence drives us.

Massachusetts Ballot Question and Legislation

- ***Access*** to vehicle on-board diagnostic systems shall be ***standardized and not require any authorization by the manufacturer***, directly or indirectly, unless the authorization system is standardized across all makes and models and is administered by an entity unaffiliated with a manufacturer.
- Requires vehicles with a telematics system to be equipped with ***standardized and open access platform*** capable of securely ***communicating all vehicle mechanical data***, upon the authorization of the vehicle owner, ***directly from the motor vehicle*** to an independent repair facility or a new car dealer.
- ***Access*** by independent repair facility is ***limited to the time to complete the repair*** or for a period of time agreed to by the vehicle owner for the purposes of maintaining, diagnosing and repairing the motor vehicle.
- Access ***shall include the ability to send commands*** to in-vehicle components if needed for purposes of maintenance, diagnostics and repair.

autocare™ ASSOCIATION
Independence drives us.

Requirements for Secure Deployment



1

Shared Trust Model

- Reliable, repeatable, secure method to establish trust among tools, vehicles, and users

2

Registration portal

- Interactive portal to manage ownership, declare intent, and authorize data access

3

Connected Tools

- Diagnostic and repair tools that can be authorized to operate over a remote connection

4

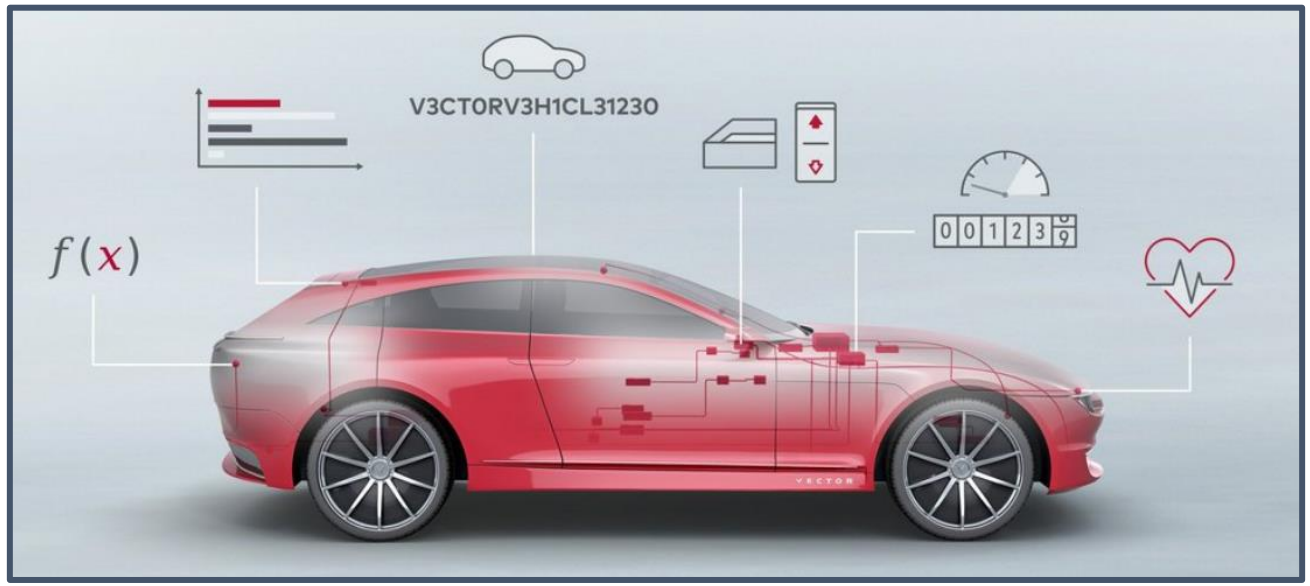
Data Channel

- Reliable, secure, bi-directional data connection that can support remote diagnostics and repairs when nearby

Compliant Protocol: SOVD

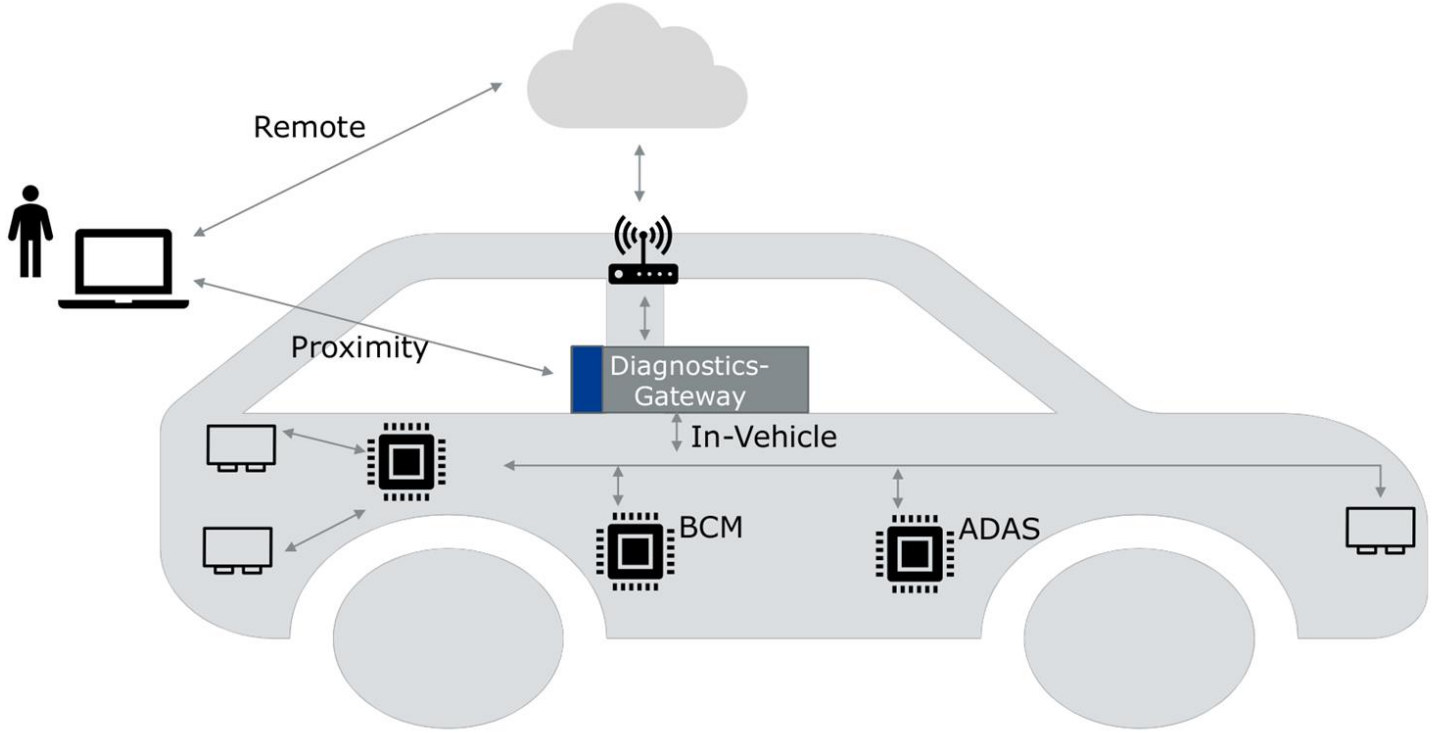
Service Oriented Vehicle Diagnostics

- Uses broadly adopted web interface standards
- Supports direct access to vehicle data and independent user authentication
- Portable to any vehicle with a High Performance Computer (HPC) and cellular network connectivity
- Created by and endorsed by ASAM OEM members



SOVD Properties

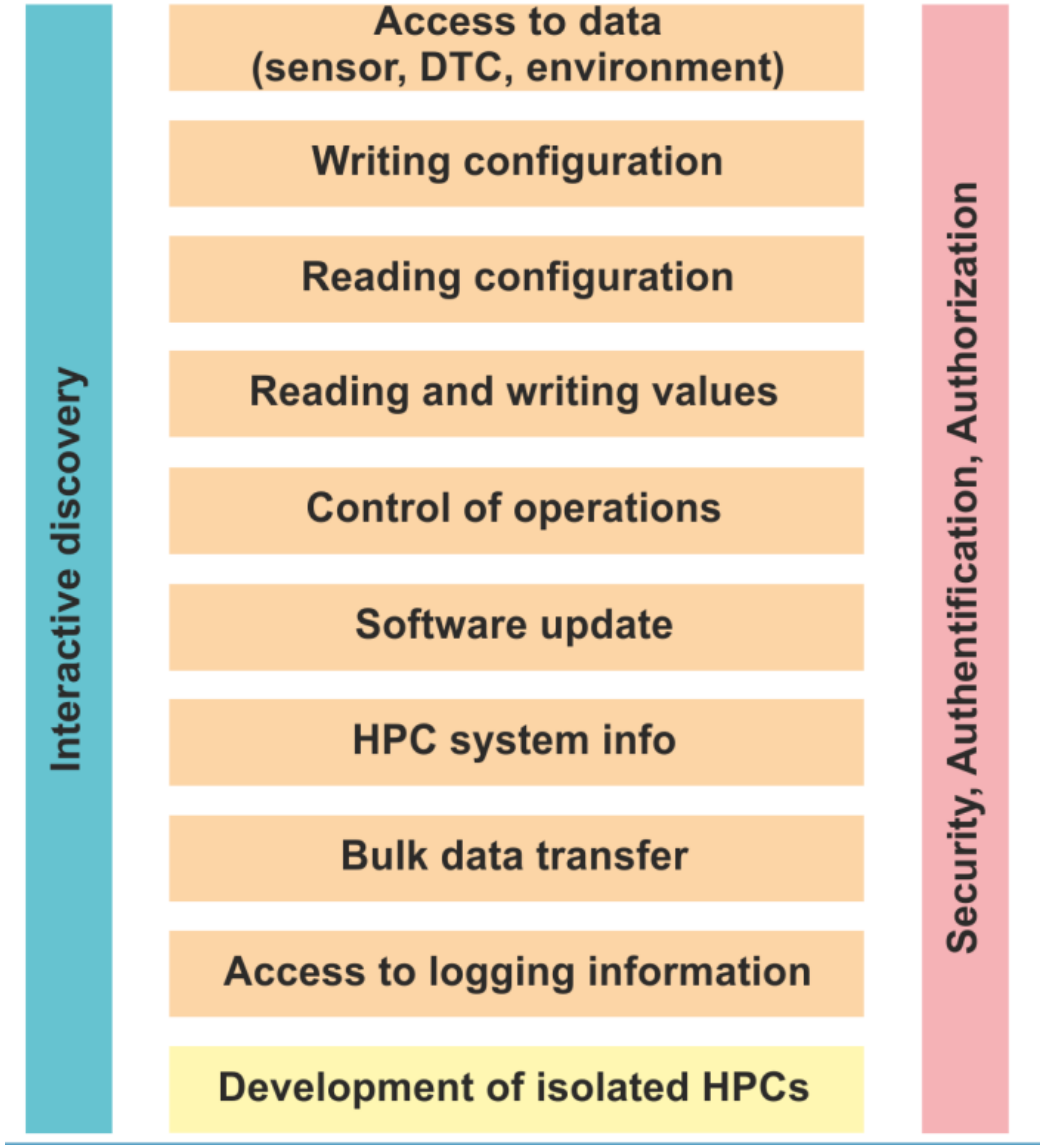
- Modern API for vehicle diagnostics
- Designed by OEM and Tier-1 technical experts
- Remote, Proximity and In-vehicle Use Cases
- State-of-the-art IT-technologies (HTTP, REST, JSON, OAuth)
- Computation is encapsulated, and a stateless access is possible
- Client Implementation requires no OEM-specific stack
- Supports direct to vehicle connections
- Enables remote commands



The SOVD Gateway requires a High Performance Computer (HPC) module - most modern cars with OEM telematics already meet this requirement

autocare™ ASSOCIATION
Independence drives us.

SOVD Supports Complex Operations



- The REST API definition can be extended over time to offer new features.
- Discovery of vehicle capabilities will allow tools to adapt to different vehicle features.
- Legacy module data and vehicle specific messages are “wrapped” in a modern API

autocare™ ASSOCIATION
Independence drives us.

SOVD Maturity

- Version 1.0 API specification published in 2022
- Existing standard is sufficient to meet the requirements of the MA ballot initiative
- Tier-1 Suppliers have already demonstrated and marketed compatible HPC modules
- Ongoing work will further define standard message and data types
  - ISO/AWI 17978 work has started

ISO/AWI 17978-1

Road vehicles

Service-oriented vehicle diagnostics (SOVD)

DATASHEET

Title	Service-Oriented Vehicle Diagnostics
Domain	Diagnostics
Current Version	1.0.0
Release Date	30 Jun 2022
Application Areas	• Diagnostic communication to HPCs and ECUs (remote, proximity, in-vehicle) • Software updates • Logging • Upload / download of bulk data and parameter data • Diagnostics without external description file
Specification Content	• API • OpenAPI definition (yaml files)

Developed by OEM Members of ASAM

- BMW AG
- Daimler AG
- Volkswagen AG
- Audi AG
- Porsche AG
- Ford Motor Company
- General Motors
- Honda R&D
- Toyota Motor Corporation
- Volvo Cars
- Renault
- Jaguar Land Rover Limited
- Scania CV AB
- MAN Truck & Bus SE
- Hyundai Motor Company
- KIA Corporation

ASAM

Association for Standardisation of Automation and Measuring systems

autocare™ ASSOCIATION
Independence drives us.

SOVD Implements OAuth2 Authorization

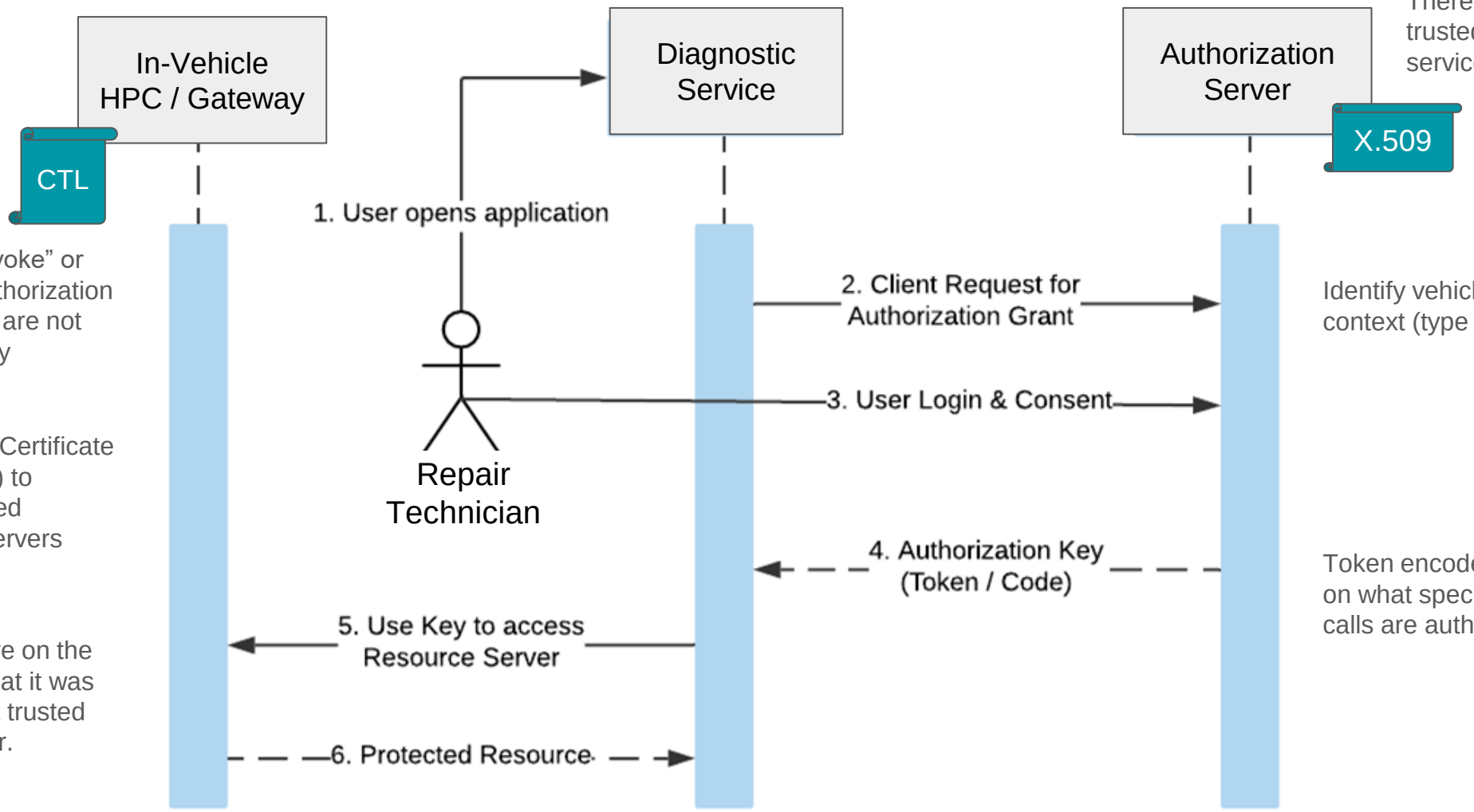
- **Simplified Authorization**: It involves obtaining an access token from an authorization server, which can then be used to access resources on the user's behalf.
- **Enhanced Security**: OAuth 2.0 incorporates strong security measures like HTTPS and short-lived access tokens to protect user data and prevent unauthorized access.
- **Greater Flexibility**: OAuth 2.0 offers a wider range of grant types, such as authorization code, client credentials, and password, to accommodate different use cases and application types. This allows for more granular control over the level of access granted to third-party applications.
- **Improved Scalability**: The token-based approach of OAuth 2.0 is suitable for large-scale deployments and high-traffic applications where handling numerous user credentials might not be feasible.
- **Wide Adoption**: OAuth 2.0 has gained widespread adoption across various platforms and APIs. This provides developers with a more consistent and standardized approach to authorization, simplifying integration and maintenance.

autocare™ ASSOCIATION
Independence drives us.

SOVD Implements OAuth2 Authorization

1. **Scopes:** This is the primary method for fine-grained control in OAuth. Scopes are strings that define the specific resources or actions that an access token grants access to. For example, a "read_status" scope might allow a tool to access basic information, while a "write_values" scope would allow it to create or edit parameters.
2. **Permissions:** Some OAuth 2.0 implementations allow for defining even more granular permissions within scopes. These permissions can be specific actions or attributes associated with a resource, allowing even finer control over access. For example, within a "write_values" scope, you might have separate permissions for accessing specific module types or constraints on vehicle location.
3. **Claims:** Claims are data assertions included in the access token itself. These claims can provide additional information about the user, such as their role, group membership, or specific attributes. This information can be used by the resource server to make finer-grained authorization decisions based on specific user characteristics or context. For example, a claim about a technician's association with a shop may allow them to inherit permissions associated with the shop.
4. **Resource servers:** While not part of the OAuth specification itself, resource servers play a crucial role in fine-grained access control. They are responsible for validating access tokens and enforcing authorization rules based on the requested scopes, permissions, claims, and any other relevant factors. By implementing custom authorization logic on the resource server, you can achieve a high level of control over who can access what data and under what conditions.

OAuth 2.0 Abstract Flow for SOVD



There can be multiple trusted authorization services

OEM may “revoke” or remove an authorization service if they are not following policy

Identify vehicle and context (type of repair)

Vehicles use a Certificate Trust List (CTL) to recognize trusted authorization servers

Token encodes details on what specific API calls are authorized

A valid signature on the token proves that it was authorized by a trusted service provider.

autocare™ ASSOCIATION
Independence drives us.

Sequence of Steps in Authentication

1. **Signature Verification:** The car first verifies the token signature. This ensures the token hasn't been tampered with during transmission. (recommend X.509 certs)
2. **Token Validation:** Next, the car validates the token itself. This involves decoding the token and extracting its claims, such as issuer, subject, expiration time, and scopes.
3. **Issuer validation:** The car confirms that the issuer (authentication portal) matches a registered and trusted authorization server.
4. **Audience validation:** The car checks if it's listed as the intended recipient for the token.
5. **Expiration validation:** The car ensures the token hasn't expired.
6. **Scope validation:** The car verifies if the requested service module falls within the granted scopes of the token.
7. **Additional checks (optional):**
    a. Nonce validation: This involves verifying a unique identifier included in the token to prevent replay attacks.
    b. Claims validation: The car will check specific claims about the user or context to make more granular authorization decisions.
8. **Access granted or denied:** Based on the successful completion of all these checks, the resource server either grants access to the requested resource or denies it with an appropriate error message.

autocare™ ASSOCIATION
Independence drives us.

Protect Car Owners from Attacks

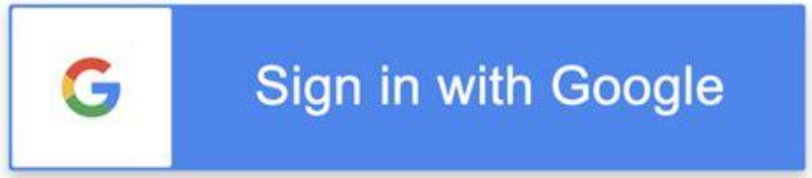
- The introduction of SOVD and independent shops does not prevent OEMs from monitoring access and activity in their fleet
  - An OEM can run intrusion detection and flag malicious activity
  - An OEM can “revoke” an authorization service if they are not following policy
- In-vehicle systems continue to apply safety rules
  - Some diagnostic tests require that the vehicle be stopped or parked
  - Some updates or write operations require specific conditions
- In-vehicle network segmentation and access controls can still be applied as long as they do not interfere with normal repair operations

autocare™ ASSOCIATION
Independence drives us.

Many Options for Authentication Service

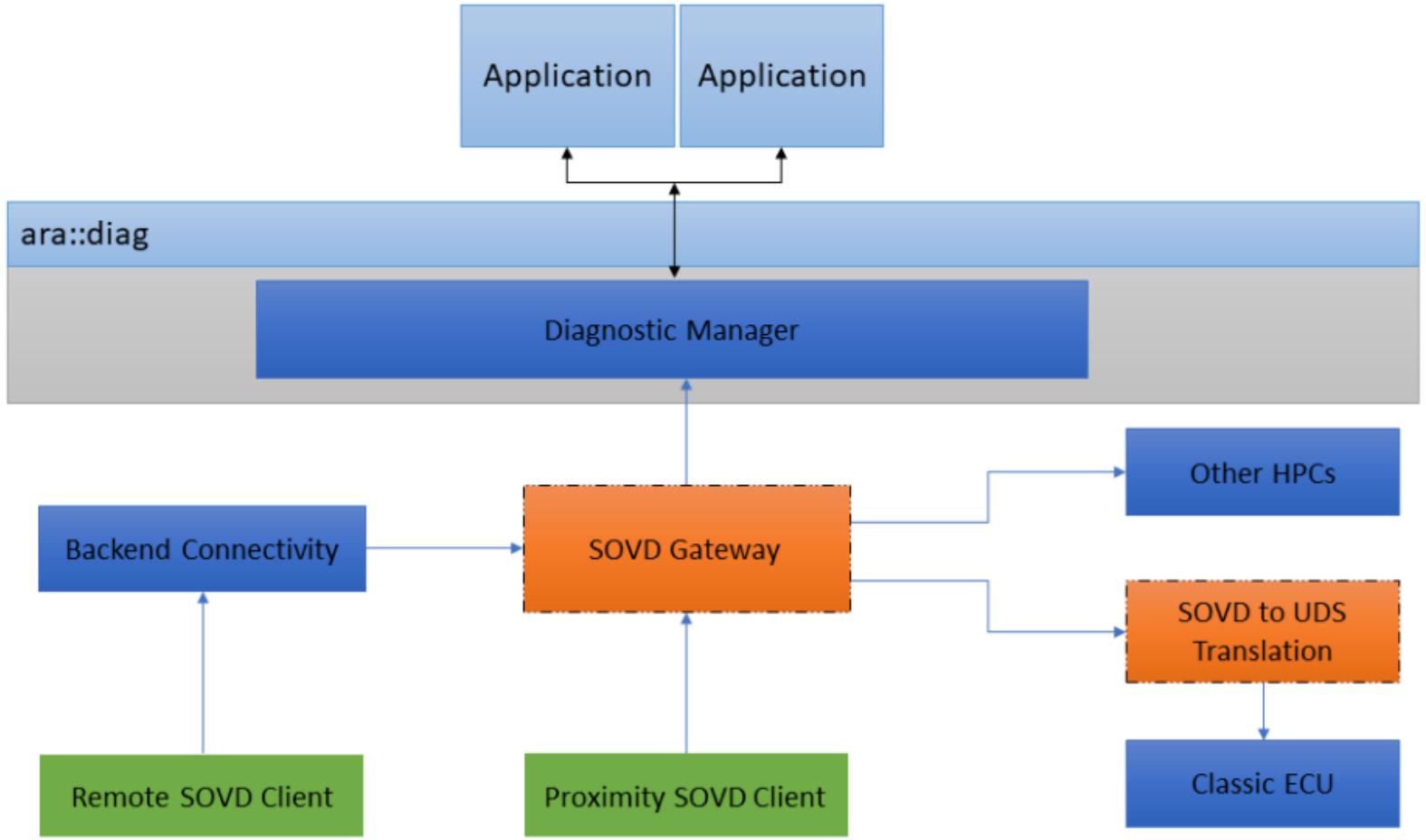
- OAuth2 is a widely used authentication service, supported by major cloud vendors
- A service like AutoAuth is uniquely suited as it already has vetted accounts and credentials for shops, shop tools, and technicians.
- Car owners can use an existing online account to prove their identity, no need to remember an additional username and password

AUTOAUTH®
AUTO AUTHENTICATION AUTHORITY



autocare™
ASSOCIATION
Independence drives us.

SOVD Reference Architecture



- SOVD Support UDS translation and encapsulation
- This allows legacy ECUs and legacy tools to work without a universal data model
- Tools can use existing methods to lookup UDS message content (as they do today)

The SOVD Gateway can wrap UDS (Unified Diagnostic Services) messages in a modern API - this enables early adoption

autocare™ ASSOCIATION
Independence drives us.

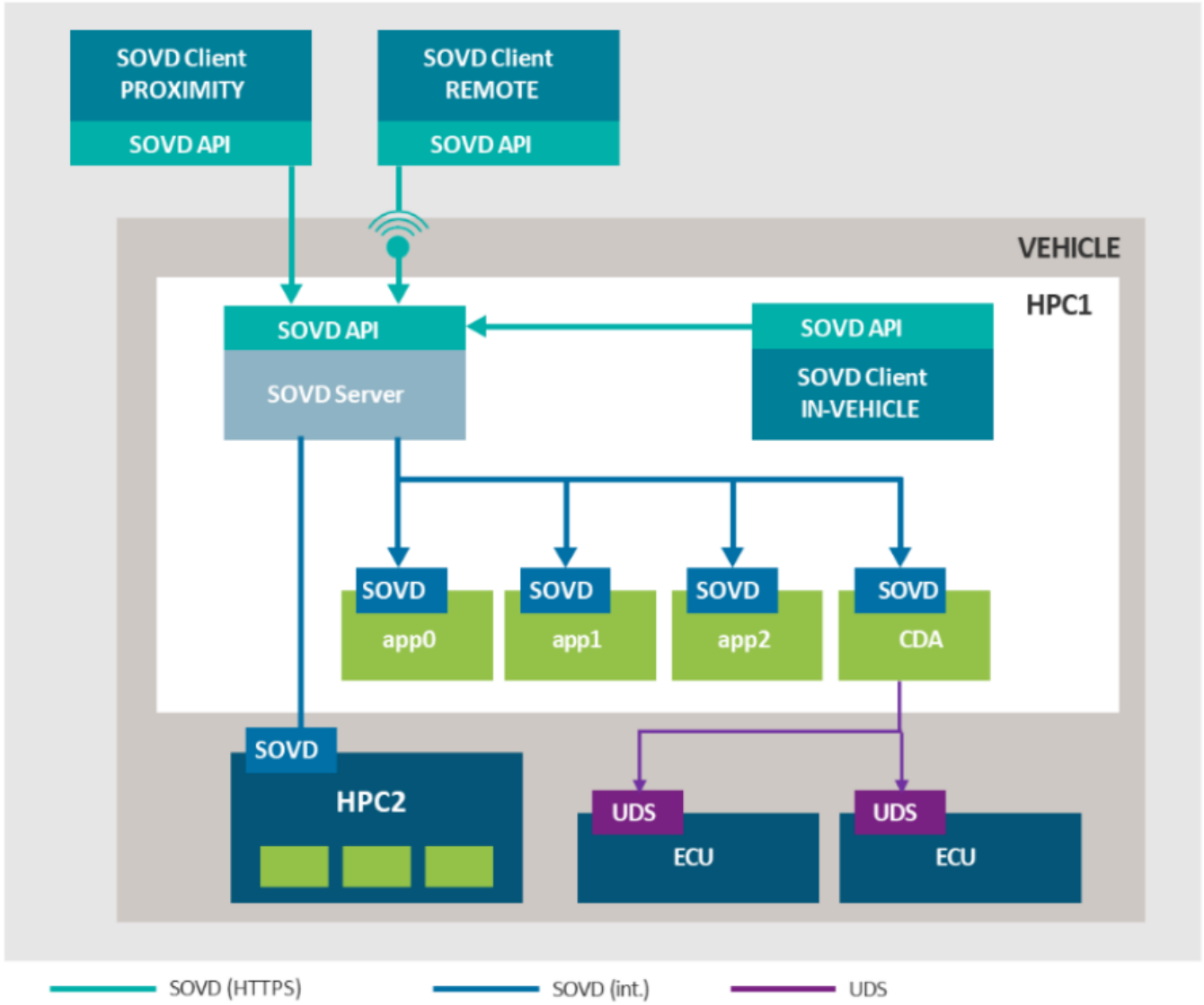
Several Leading Tool and Platform Vendors are Early Adopters

- DSA
- Softing
- KPIT
- Siemens
- Vector
- RA Consulting
- Tata consultancy
- Luxoft

https://www.vector.com/int/en/products/solutions/diagnostic-standards/sovd-service-oriented-vehicle-diagnostics/

autocare™ ASSOCIATION
Independence drives us.

SOVD Support Local and Cellular Connections



- Remote client can take advantage of OEM's existing cellular connection to the vehicle.
- A local (proximity) client can support near-field communications (WiFi or BlueTooth)
- Vehicle can enforce policy to allow read-only diagnostics when remote
- API calls from the tool to the car flow through an end-to-end tunnel (SSL)

autocare™ ASSOCIATION
Independence drives us.

Summary

- SOVD is an established diagnostic protocol created by OEMs
- This protocol can fully support current Right to Repair requirements
  - **Trust Model:** OAuth2 supports fine-grain access control with time limits
  - **Registration Portal:** Several existing services can be updated to issue OAuth2 tokens
  - **Connected Tools:** SOVD can wrap legacy data already managed by modern tools
  - **Data Channel:** REST + SSL can be used on Cellular, WiFi, or Bluetooth connections
- SOVD can safely enable remote diagnostics and proximity (nearby) repairs

autocare™ ASSOCIATION
Independence drives us.

autocare™
ASSOCIATION

Independence drives us.

www.autocare.org