The Equipment & Tool Institute
Serving the Automotive Repair Industry since 1947

Secure Vehicle Communication Tool Authentication Resolutions

June 13, 2018[1]

Background

Representatives from the companies who are full members of the Equipment and Tool Institute ("Institute") which design, manufacture, and sell external test equipment for service and diagnosis of vehicles have convened discussion on the emerging topic of secure vehicle communication tool authentication. During this discussion a collection of resolutions which describe authentication principles have been defined and organized. Therefore, presented in this document are resolutions adopted by the Institute's full member body on the topic of tester authentication.

Executive Overview

Addressing the need for diagnostic equipment to maintain a connection to the vehicle for diagnostic purposes, and to communicate its requirements to industry, the Institute's member body has adopted resolutions that surround its definition of secure vehicle communication tool authentication.

A total of five categories of resolutions have been authored, which are presented in the list below[2]:

1. Business: covers tool volume, install base, tool registration
2. End User and Customer: covers technician, business owner, and customer registration
3. End-User Privacy: covers technician and business owner privacy and commercial fees
4. Marketplace: covers certificate authority, tool company to vehicle manufacturer server connection, digital certificates, and multiple tool support
5. Product: covers tool authentication process, certificate type and coverage, industry recommended practice, tool requirement, ECU requirement, and revocation strategy

Summary

Institute membership acknowledges that vehicle security is of paramount concern to vehicle manufacturers, as design of electronic control unit and datalink communication networks now may include requirement from the cybersecurity community. The Institute also acknowledges that a majority of vehicles in operation are diagnosed and serviced in an aftermarket repair center. By preparing these resolutions, the Institute is transparently sharing its requirement for diagnostic products to be included in the discussion with vehicle manufacturer electronic system and cybersecurity designers to ensure they can continue to provide diagnostic products to the aftermarket service centers which in turn can then continue to service the complex vehicles of today and in the future.

[1] Document content updated to version 18 on November 13, 2018

[2] For complete detail on each resolution per category, please refer to the section with heading titled "Presentation of Resolutions"

Secure Vehicle Communication Tool Authentication Resolutions
June 13, 2018

Definitions Used in this Document

- Customer – the vehicle owner
- End-User – the service technician and business owner
- Tool – a device which is developed and marketed by a Tool manufacturer. Performs diagnostic, service, and maintenance functions. May also be known as Tester, OBD Scanner, Scan Tool, Dongle, or External Test Equipment.
- Vehicle Manufacturer – a design and manufacturing company who offers for sale vehicles that are ground based

Presentation of Resolutions

1) The Institute's member body adopts the following secure vehicle communication Tool authentication resolutions in the category of <u>Business</u>.
   a) Tool volume by maker shall not be divulged to a Vehicle Manufacturer or designated third party vendor
   b) Tool type by maker shall not be divulged to an Vehicle Manufacturer or designated third party vendor
   c) Tool manufacturer shall not be required to register their installed base of Tools

2) The Institute's member body adopts the following secure vehicle communication Tool authentication resolutions in the category of <u>End User and Customer</u>.
   a) End user information shall not be provided to a Vehicle Manufacturer or designated third party vendor
   b) Customer information shall not be provided to a Vehicle Manufacturer or designated third party vendor

3) The Institute's member body adopts the following secure vehicle communication Tool authentication resolutions in the category of <u>End-User Privacy</u>. Tool manufacturer customers and Tool End-Users are not the same entity. In the best interest in securing end-user privacy:
   a) End User information shall not be provided to an Vehicle Manufacturer or designated third party vendor
   b) End Users shall not be required to pay any fee directly to an Vehicle Manufacturer or designated third party vendor for any part of a Tool developed by a Tool manufacturer

4) The Institute's member body adopts the following secure vehicle communication Tool authentication resolutions in the category of Marketplace
   a) A Vehicle Manufacturer shall deploy one certificate authority process for use by Tools in a global marketplace
   b) Tool shall connect to a Tool Manufacturer server to facilitate Tool authentication
   c) A secure Tool digital certificate server shall be managed and/or operated by an independent third party vendor not owned or partially owned by any vehicle manufacturer, and one which is recognized and endorsed by aftermarket trade associations
   d) A secure Tool digital certificate server shall be available 99.99% of the time
   e) A secure Tool digital certificate server shall perform proxy tasks with Vehicle Manufacturer digital certificate server for performing Tool authentication functionality
   f) Any authentication interface must support multiple Tool hardware and software solutions and not be so complex as to effectively force a single vendor supplied solution

5) The Institute's member body adopts the following secure vehicle communication Tool authentication resolutions in the category of Product
   a) A digital certificate which authenticates Tool shall not be required for basic diagnostic functions (e.g. SAE J1979)
   b) A digital certificate which authenticates Tool shall be active for an off-line use case
   c) A digital certificate which authenticates Tool shall be time based
   d) A digital certificate which authenticates Tool shall be obtained in advance with wide vehicle application scope to perform diagnostic and/or reprogramming functions
   e) Tool shall not be required to have a 100% on-line connection in order to facilitate being operated in an off-line environment, such as a test drive, roadside repair, or other use case
   f) The vehicle application scope of a digital certificate shall cover all vehicle makes or all vehicle models from a particular Vehicle Manufacturer
   g) To facilitate Tools being operated in an off-line enabled environment, a Tool may obtain a digital certificate with a time period greater than or equal to 30 days
   h) Any certificate authority process must allow Tools using commercially available operating systems which are available on today's diagnostic tester market to function with a Vehicle Manufacturer's Tool authentication process
   i) Any certificate authority process must allow Tools available in today's diagnostic tester market that are not using an operating system (e.g. microcontroller with small memory capacity) to function with a Vehicle Manufacturer's Tool authentication process
   j) Tools with varying operating systems (e.g. not Windows or Android) shall be allowed to function properly with a tester authentication system, and shall do so without requiring Vehicle Manufacturer or 3rd party designated software to be installed on the Tool to acquire diagnostic data from vehicle systems with OBD
   k) Tools which execute non-Windows operating system (e.g. included but not limited to Android, iOS, proprietary OS) shall be accommodated in a Tool authentication process

l) A Tool shall not be required to use a Vehicle Manufacturer defined hardware security solution to support any Tool authentication process

m) All diagnostic-related ECUs shall follow SAE J3138 recommended practice for determining what intrusive and non-intrusive diagnostic messages need Tool authentication and those that do not

n) A Tool shall be designed to interact with diagnostic-related ECUs that follow SAE J3138 recommended practices for deciding what diagnostic messages need Tool authentication and those that do not

o) To facilitate Tool operation in a permanent or semi-permanent use case, security certificates shall be available for installation during or after Tool production

p) All diagnostic services shall be accessed directly from a connector on the vehicle and not only through any Vehicle Manufacturer or third party portal

q) Communication messages which contain diagnostic data shall not be encrypted at the vehicle diagnostic connector

r) Authentication interface must be based on open standards and not be tied to a specific vendor or vendor’s software

s) A Tool shall be capable of supporting an authentication methodology revocation use case

t) Minimum capability for a Tool, which supports an authentication process, shall include microprocessor, flash memory, and asymmetric encryption functionality

u) An intrusion detection system devised by a Vehicle Manufacturer for any level of vehicle cybersecurity (e.g. API, ECU, datalink, or other) shall include compliance to Tool requirements defined by the secure vehicle communication tool authentication resolutions