

# Requirement specification for Remote Vehicle Interaction

© 2016 Jaguar Land Rover.

This document is licensed under the Creative Commons Attribution 4.0 International (CC BY 4.0).

See: <https://creativecommons.org/licenses/by/4.0/> for detailsClick here for details

## Revisions

### Changes

- |     |                          |
|-----|--------------------------|
| 0,1 | Initial template.        |
| 1   | Requirements for RVI 1.0 |

[HLD]

RVI High-Level Design Document, 15-456-POC-RVI-HLD\_RevB

## Requirement

## P Description

### RVI-GEN

#### General Requirements

- |           |   |
|-----------|---|
| RVI-GEN-1 | M RVI shall connect a vehicle to an internet-based server         |
| RVI-GEN-2 | M RVI shall connect a mobile phone to a vehicle                   |
| RVI-GEN-3 | M RVI shall support multiple data links                           |
| RVI-GEN-4 | M RVI shall support the communication protocol specified by [HLD] |
| RVI-GEN-5 | M RVI shall support communication link failure and recovery       |

### RVI-SVC

#### Service Name

- |            |  |
|------------|--|
| RVI-SVC-1  | M Service Names conform to MQTT Topic Name Specification                   |
| RVI-SVC-2  | M Service Names starting with '\$' are treated as Internal Service Names   |
| RVI-SVC-3  | M Internal Service Names cannot be addressed from outside the Service Edge |
| RVI-SVC-4  | M Service Names consist of at least 4 levels                               |
| RVI-SVC-5  | M Uuid part must be unique to [domain]/[type]                              |
| RVI-SVC-6  | M Domain part must conform to RFC1035                                      |
| RVI-SVC-7  | M Matching of Service Names is case-insensitive                            |
| RVI-SVC-8  | M Domain part must not begin with '/'                                      |
| RVI-SVC-9  | M Service Names must not be longer than 2048 bytes                         |
| RVI-SVC-10 | M Service Names must not contain the bytes '+', '#' or null                |

RVI-SVC-11	M	The '+' character used in service patterns signals wildcard matching of a single topic level
RVI-SVC-12	M	The '#' character may only follow a '/' at the end of service patterns, and matches the remainder of the pattern
RVI-SVC-13	M	Topic levels must be at least one character long
RVI-SVC-14	M	Service Names must be system-wide unique
RVI-SVC-15	M	Service Names beginning

#### **RVI-DLINK-DISC**

RVI-DLINK-DISC-1  
RVI-DLINK-DISC-2  
RVI-DLINK-DISC-3  
RVI-DLINK-DISC-4

#### **Data link discovery**

- O Two RVI nodes on the same LAN/WLAN shall be able to discover each other
- O Discovery shall be done using UDP/IP multicast
- O RVI shall be able to detect when a network link becomes available and trigger discovery
- O RVI should support inactivity timers on active connections, disconnecting idle connections

#### **RVI-TLS**

RVI-TLS-1  
RVI-TLS-2  
RVI-TLS-3  
RVI-TLS-4  
RVI-TLS-5  
RVI-TLS-6  
RVI-TLS-7  
RVI-TLS-8  
RVI-TLS-9

#### **RVI TLS**

- M RVI shall support TLS 2.0
- M Each RVI node shall have a unique private/public key pair
- M Each RVI node shall have a copy of the Root Server Public Key
- M RVI shall support server-side certificates.
- M RVI shall support cached validation
- M RVI shall upgrade all TCP connections to TLS
- M RVI shall validate the X.509 certificate of the peer node
- O RVI shall support partial-chain validation
- M RVI shall reject any connection attempt that cannot be validated

#### **RVI-AUTHEN**

RVI-AUTHEN-1  
RVI-AUTHEN-2  
RVI-AUTHEN-3  
RVI-AUTHEN-4

#### **Authentication**

- M The connecting RVI node (client) shall authenticate itself
- M The authentication shall be sent as an X.509 certificate
- M The X.509 certificate shall be signed by a root server.
- M The connected RVI node (server) shall authenticate itself

#### **RVI-AUTHOR**

#### **Authorization**

RVI-AUTHOR-1	M	The connecting RVI node (client) shall authorize itself
RVI-AUTHOR-2	M	The connected RVI node (server) shall authorize itself
RVI-AUTHOR-3	M	The authorization ("auth") message shall contain the same Public Key as the key used for the TLS handshake
RVI-AUTHOR-4	M	The auth message shall indicate a protocol version supported by the current node
RVI-AUTHOR-5	M	RVI shall reject the connection if the offered protocol version is not supported
RVI-AUTHOR-6	M	Each credential shall be sent as a JSON Web Token (JWT)
RVI-AUTHOR-7	M	The JWT signing shall use the 'RS256' algorithm
RVI-AUTHOR-8	M	RVI shall verify the JWT signature using the Root Server Public Key
RVI-AUTHOR-9	M	RVI shall reject any JWT that cannot be verified using the Root Server Public Key
RVI-AUTHOR-10	M	The JWT shall have a format and content specified by [RVI HLD]
RVI-AUTHOR-11	M	The conencted RVI node (server) shall authorize itself

#### **RVI-SVC\_DISC**

RVI-SVC_DISC-1	M	RVI nodes shall announce services to connected nodes that are authorized to invoke said services
RVI-SVC_DISC-2	M	RVI nodes shall not announce services for which they are not authorized to receive invocations
RVI-SVC_DISC-3	M	RVI nodes shall not announce services that the receiving node is not authorized to invoke
RVI-SVC_DISC-4	M	RVI nodes shall prepend their own node ID to the service announcement "route" list
RVI-SVC_DISC-5	O	RVI nodes may support relaying service announcements
RVI-SVC_DISC-5	M	RVI may only relay service announcements to other nodes authorized to invoke the announced services
RVI-SVC_DISC-6	M	RVI shall not relay an announcement if the announcement "route" list length equals or exceeds the "hops" count
RVI-SVC_DISC-7	M	RVI shall ignore announcements whose "route" list length exceeds the "hops" count

#### **Service Discovery**

#### **RVI-SVC\_INVOC**

RVI-SVC_INVOC-1	M	RVI shall support service invocations to active services
RVI-SVC_INVOC-2	M	RVI shall validate service invocations against the "right_to_invoke" lists for the calling node
RVI-SVC_INVOC-3	M	RVI shall validate service invocations against the "right_to_receive" lists for the receiving node
RVI-SVC_INVOC-4	M	RVI shall ignore any service invocation that does not pass validation
RVI-SVC_INVOC-5	M	Service invocations shall include a timeout value on Unix time (ms) format
RVI-SVC_INVOC-6	O	RVI may support a "synch" option in service invocations, requesting a synchronous (round-trip) RPC
RVI-SVC_INVOC-7	M	If "synch" supported, originating node shall create a unique, ephemeral Internal Service Point as "reply_to"
RVI-SVC_INVOC-8	M	RVI shall buffer service invocations that cannot immediately be routed
RVI-SVC_INVOC-9	M	RVI shall process invocations with the same "channel" value in the same order as they arrived
RVI-SVC_INVOC-10	M	Invocations that are fragmented on delivery shall hold up succeeding messages with same "channel" id
RVI-SVC_INVOC-11	M	RVI shall discard invocations if their specified timeout is triggered
RVI-SVC_INVOC-12	M	RVI shall notify the caller immediately if invocation fails, provided that "synch" is requested

#### **Service Invocation**

**STORE\_FWD**

STORE\_FWD-1

STORE\_FWD-2

**Store and forward**

RVI may store buffered messages persistently

Buffered messages shall be delivered as soon as a connection to the destination node becomes available

**PROV\_SVC**

PROV\_SVC-1

PROV\_SVC-2

PROV\_SVC-3

**Provisioning services**

- M RVI shall support adding and removing credentials
- M RVI shall support replacing the public/private key pair
- M RVI shall support migration of the root public key

**Author**

Magnus Feuer

Ulf Wiger

**Notes**

Exception: Internal Service Names start with '\$'





