FCA

FIAT CHRYSLER AUTOMOBILES

FCA Authenticated (secure) Diagnostics

Jim Savich

Network & Diagnostics

1/19/2016

FCA Authenticated (secure) Diagnostics

Secure Diagnostics three main components

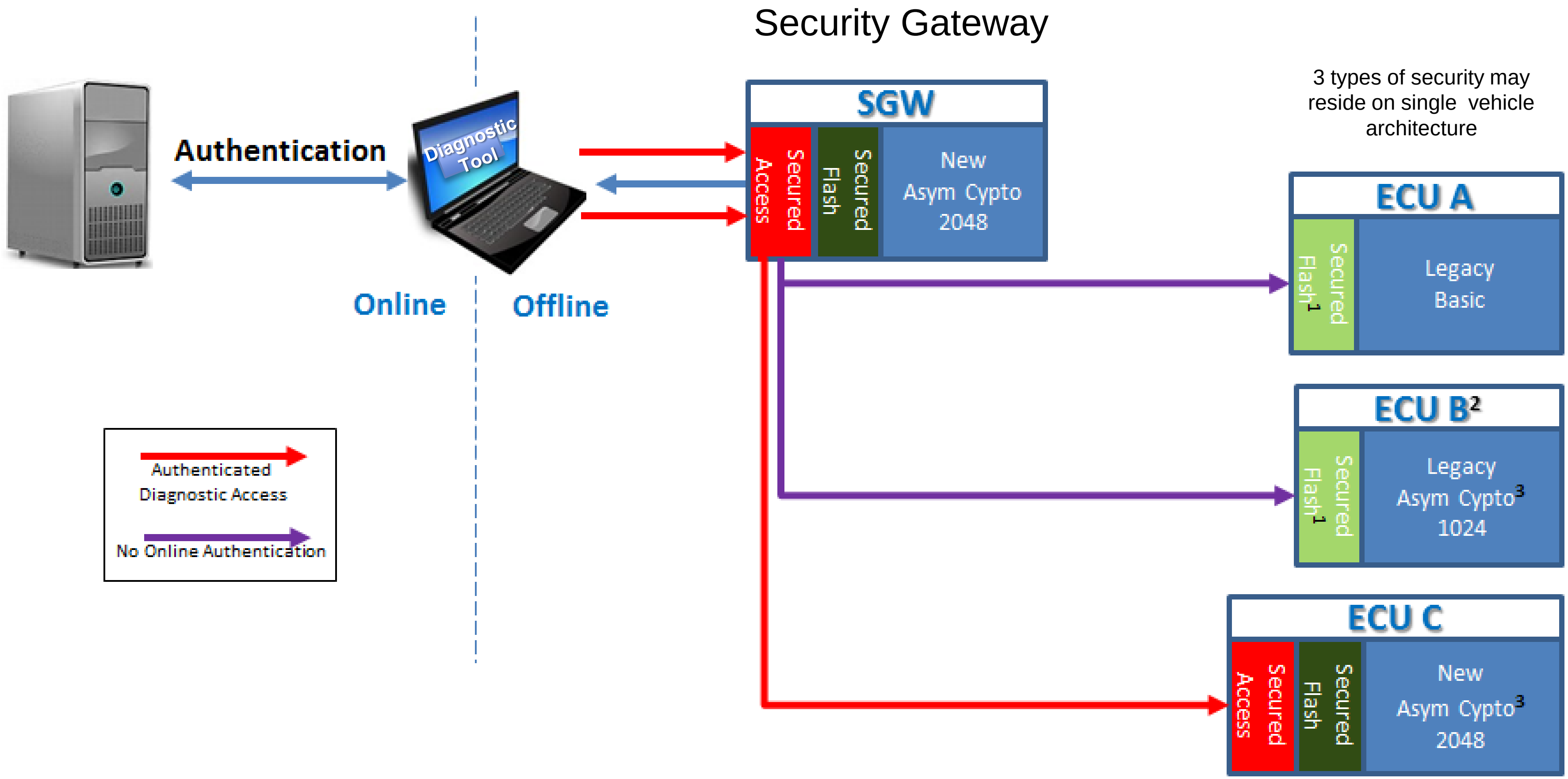
1. Tester Authentication

2. Rights Management

3. Secure Communication

FCA Authenticated (secure) Diagnostics

Topology includes SGW as firewall

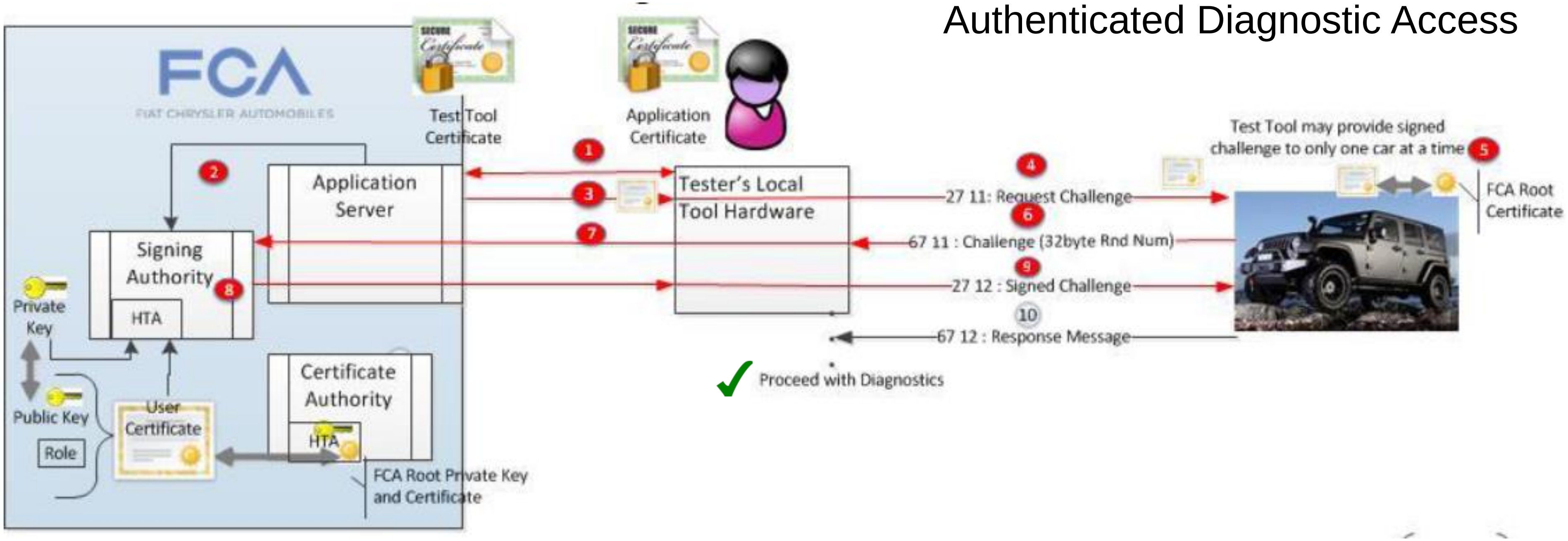


Firewall for hard & remote (i.e. LTE Modem, wifi, etc) connections

1. Traditional Seed/Key security
2. Asymmetric Cryptography - Legacy
3. Asym Cypto = Asymmetric Cryptography referred to Level 4 access

FCA Authenticated (secure) Diagnostics

Authenticated Diagnostic Access



1. Mutual TLS authentication between Manufacturing or Aftersales Workshops Application Server (from now on called just the server) and the Test Tool client (intended as physical device) through proper application and test tool certificates to establish a secure session. Afterward user/password credentials are sent to the server over the established secure channel to "profile" the tester with proper rights and privileges.

2. The appropriate application server will retrieve or create the identified User Certificate, which includes the authorized role for that user along with the Signing Authority Public Key, from the certificate Authority

3. The Test Tool receives the user certificate from the server to be used for starting challenge/request process with ECU

4. The Test Tool forwards the user certificate as part of the Security Access Authenticated Diagnostics Access request to the ECU.

5. ECU verifies the user certificate to be part of the Trust Chain with the FCA root certificate installed on board. (Transparent to Test Tool)

6. ECU replies to Test Tool with the requested challenge.

7. Test Tool forwards the challenge to the Application server over the secured channel.

8. The Application server submits the challenge to the FCA Authenticated Diagnostics Access Signing Authority to have it signed with private key associated with the user certificate.

9. Test Tool receives the response from its server to relays it to the ECU.

10. The signature of the response is verified with the User Certificate, then the Authenticated Diagnostic Access Response (i.e. encrypted challenge which is then decrypted using the public key associated with the user certificate) is compared with the expected one (in this case the original random challenge). Test Tool gets reply (passed/failed check) from ECU.

At this stage the date and time is set on the ECU .

FCA Authenticated (secure) Diagnostics

Diagnostic Service 0x27 used to authenticate. Sub-function 11/12 defined as Challenge (Req/Send)

TABLE 3: Request Message Definition – Security Access

Byte no.	Parameter name	Message Usage	Data Value (Hex)
0	Security Access Request Service ID	M	27
1	Request Challenge (Sub Function)	M	11

TABLE 4: Response Message Definition – Security Access

Byte no.	Parameter name	Message Usage	Data Value (Hex)
0	Security Access Response Service ID	M	67
1	Security Access Mode – Request Challenge	M	11
2	Random Number High Byte	M	00-FF
	. .	M	00-FF
5	Low Byte	M	00-FF

TABLE 5: Request Message Definition – Security Access

Byte no.	Parameter name	Message Usage	Data Value (Hex)
0	Security Access Request Service ID	M	27
1	Send Challenge (Sub Function)	M	12
2 : 1001	Security Key Key - High Byte Key - Low Byte	M : M	00-FF : 00-FF

TABLE 6: Response Message Definition – Security Access

Byte no.	Parameter name	Message Usage	Data Value (Hex)
0	Security Access Response Service ID	M	67
1	Security Access Mode - Challenge	M	12

UDS Service $84 Secured Data Transmission - Not Used

TABLE 7: Negative Response Message Definition – Security Access

Byte no.	Parameter name	Message Usage	Data Value (Hex)
0	Negative Response	M	7F
1	Security Access	M	27
2	Negative Response Code	M	00-FF
	Sub-Function Not Supported		12
	Incorrect Message Length – Invalid Format		13
	Request Sequence Error		24
	Invalid Key		35
	Required Time Delay Not Expired		37
	Sub-Function Not Supported in Active Session		7E
	Revoked Certificate		tbd
	Invalid Response		tbd

FCA Authenticated (secure) Diagnostics

Rights Management

The diagnostic application of the ECU shall, before each diagnostic service, check whether the access of the test tool to a given service is allowed.
The decision is based on filter of roles that is pre-stored on ECU per each service provided by the ECU. When a service request is received by the ECU, the current active role, set by authentication process, is checked with the list of allowed roles for that service.

Engineering [role 0]
This role aligns with existing Engineering audience

Service / After-Sales [role 1]
This role aligns with existing Service audience

Manufacturing [role 2]
This role aligns with existing Manufacturing audience

Supplier [role 3]
This role will be given to replace existing supplier sessions. The SGW will not permit diagnostic access via the OBD port using a supplier role.

After-Market [role 4]
This role will be given to aftermarket tools and users. By right to repair, this will be treated the same as the service / after-sales roles.

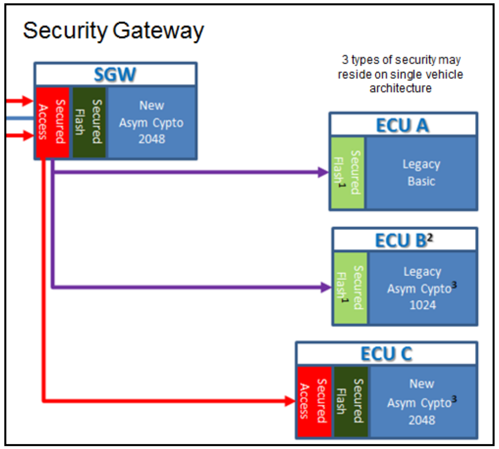
On-Board Tool [role 5]
This role will be given to ECUs that request elevated diagnostics.

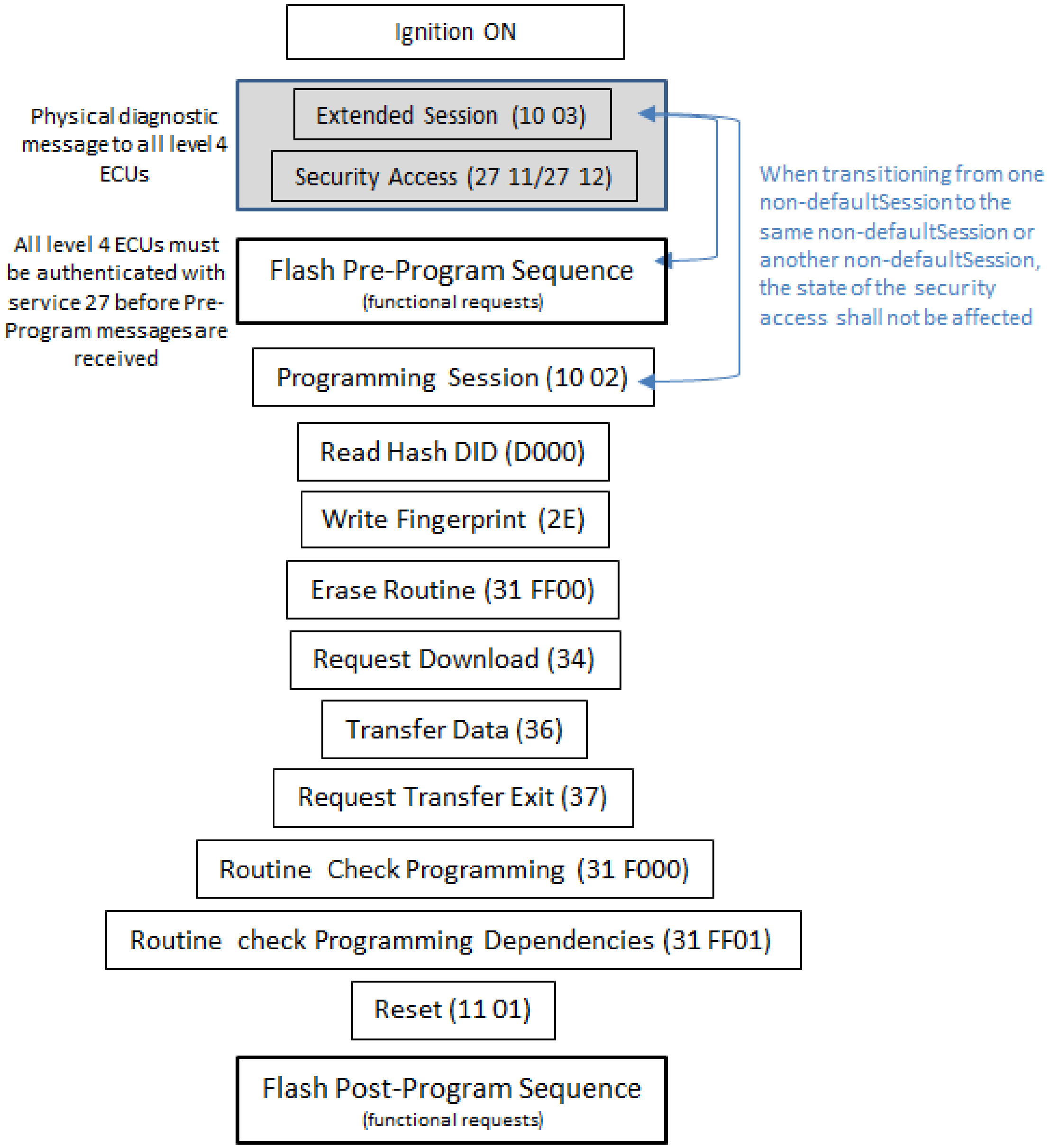
FCA Authenticated (secure) Diagnostics

FIAT CHRYSLER AUTOMOBILES

Flash Sequence

(ECU C = Level 4 ECU)





Ignition ON

Physical diagnostic message to all level 4 ECUs

Extended Session (10 03)

Security Access (27 11/27 12)

All level 4 ECUs must be authenticated with service 27 before Pre-Program messages are received

Flash Pre-Program Sequence
(functional requests)

Programming Session (10 02)

When transitioning from one non-defaultSession to the same non-defaultSession or another non-defaultSession, the state of the security access shall not be affected

Read Hash DID (D000)

Write Fingerprint (2E)

Erase Routine (31 FF00)

Request Download (34)

Transfer Data (36)

Request Transfer Exit (37)

Routine Check Programming (31 F000)

Routine check Programming Dependencies (31 FF01)

Reset (11 01)

Flash Post-Program Sequence
(functional requests)

Backup