Connected X Cyber Security

Video Recorder and Playback Security Requirements

Version 1.4

UNCONTROLLED COPY IF PRINTED

FORD CONFIDENTAL

1 Version History & Table of Contents

1.1 Table of Contents

1.2 Revision History:

Version	Revision Date	Description of Change	Affected Sections	Author
1.0	10-31-2019 🎃	Initial Draft	All	ssheahan
1.1	1-22-2020	Streaming Protocol Req Added	2.2.5	ssheahan
1.2	3-4-2020	Restructured the document to include specific requirements to VRS instead of the cascaded requirements from the Enhanced Dash Camera security spec.	See Description.	ssheahan
1.3	3-24-2020	Edits from Peer Review. Edits for Optional Video Encryption, Edits for key storage.	All	ssheahan
1.3.1	5-10-2021	2.1.13 Requirement change	2.1.13	Srapart1
1.4	5-27-2021	Edits from peer review. Edit for Optional video encryption Removed key rotation Removed unique X.509certificate per module Added symmetric and asymmetric key generation and storage	All	Srapart1

1.3 Reference Documents

Refer to the current version of the following reference documents for supporting cyber security requirements:

1) Operating Systems Security Spec
2) Key and Certificate management Spec - VDOC084140
3) Random Number Generator Requirement - RQT-001403-020666

2 Cyber Security Requirements

2.1 Functional Requirements

2.1.1

Video Stream Not Available Logging

The system shall detect if selected video streams to be recorded are unavailable or the stream is disrupted during recording and shall log this information into the metadata file associated with the video recordings.

Rationale			
Video unavailability needs to be detected as it impedes recording.			
Acceptance Criteria			**V&V Method**
• A log is generated when a selected video stream becomes unavailable.			DV Testing and Review
Notes			
			Scott Sheahan
Version	**Date**	**Author**	**Change**
1.4	11/4/2019	ssheahan	second version

2.1.2

Unencrypted Video Streaming Protocols

Unencrypted streaming protocols shall only be used after a threat analysis and approval from the cyber security team.

Rationale			
Unencrypted streaming protocols can be monitored over the network. Use of unencrypted streams should be approved by cyber security after a proper threat analysis.			
Acceptance Criteria			**V&V Method**
• Unencrypted streaming protocols are only used after a threat analysis and approval from the cyber security team.			DV Review
Notes			
			Scott Sheahan
Version	**Date**	**Author**	**Change**
1.4	1/22/2020	ssheahan	second version

2.1.3

Digital Signatures for Video Files and Metadata Files

The Video Recorder Service shall apply a digital signature to all files (video and metadata) such that the signature can be verified during playback within the vehicle, to ensure the files were not altered. The digital signature shall not interfere with playback outside of the vehicle. This digital signature shall consist of first generating a SHA-256 Hash of the file, then signing that hash using RSA 2048 with PSS padding

Rationale	
Signing assures data integrity, authenticity, and non-repudiation. This cryptographically ties a file to the Video Recorder Service that produced it.	
Acceptance Criteria	**V&V Method**
• All video and metadata files have a digital signature appended • Signed with RSA 2048 encrypted SHA 256 Hash of file using PSS Padding	DV Testing and Review
Notes	

Version	Date	Author	Change
1.4	3/4/2020	Srapart1	second Version

2.1.4 Video Recorder Service Command and Control

All command and control interactions with the Video Recorder Service shall take place over an authenticated channel using mTLS (bi-directional TLS).

Rationale	
Mutual TLS assures that both endpoints are authenticated and set up a session key for encrypted communications. The SOA Framework uses mTLS by default.	
Acceptance Criteria	**V&V Method**
• Packet captures of Ethernet data to Video Recorder will show TLS encryption. • TLS version 1.2 or greater	DV Testing and Review
Notes	

			Scott Sheahan
Version	**Date**	**Author**	**Change**
1.4	3/4/2020	ssheahan	second version

2.1.5 Video Recorder Service Asymmetric Key Provisioning

Each Video Recorder Service shall be provisioned with a unique two raw RSA 2048 private and public key Pairs. One key Pair is for Encrypting the Symmetric keys and another key pair is for digital signature.

Rationale	
Each public and private key pair needs to be unique to each camera system to provide nonrepudiation.	
Acceptance Criteria	**V&V Method**
• Every Video Recorder and Playback Service has a two unique RSA 2048 public and private key pairs.	DV Review
Notes	

Version	Date	Author	Change
1.4	5/18/2021	Srapart1	second Version

2.1.6 Signature Validation Prior to Processing Video/Meta Data Files

All video and metadata file digital signatures shall be verified with the public key associated for digital signature in VRP function. This process shall need the Public key to validate the file's digital signature. A file shall not be processed if the digital signature fails to be validated.

<table>
<tr><th colspan="4">Rationale</th></tr>
<tr><td colspan="4">Signature validation will ensure that the Video Recorder Service does not process malicious data and ensures that the VRP will only be able to process videos/files that have been produced by its own system.</td></tr>
<tr><th colspan="3">Acceptance Criteria</th><th>V&V Method</th></tr>
<tr><td colspan="3">• A test is done where a video and metadata file from another vehicle are attempted to be added to the system. The test must show that the VRP will reject processing these files.</td><td>DV Testing and Review</td></tr>
<tr><th colspan="4">Notes</th></tr>
<tr><td colspan="4"></td></tr>
<tr><th>Version</th><th>Date</th><th>Author</th><th>Change</th></tr>
<tr><td>1.4</td><td>5/18/2021</td><td>Srapart1</td><td>second version</td></tr>
</table>

2.1.7 Asymmetric Key Storage and Generation

All asymmetric public and private keys used in the VRP function shall meet the requirements in Key and certificate management spec

<table>
<tr><th colspan="4">Rationale</th></tr>
<tr><td colspan="4">Keys must not be available for copying or malicious use in the system. Secure storage of these keys is critical to cyber security.</td></tr>
<tr><th colspan="3">Acceptance Criteria</th><th>V&V Method</th></tr>
<tr><td colspan="3">• All Asymmetric keys used within VRP function should meet the key storage requirement Specification</td><td>DV Review</td></tr>
<tr><th colspan="4">Notes</th></tr>
<tr><td colspan="4">Key and Certificate Management Spec</td></tr>
<tr><th>Version</th><th>Date</th><th>Author</th><th>Change</th></tr>
<tr><td>1.4</td><td>5/18/2021</td><td>Srapart1</td><td>second version</td></tr>
</table>

2.1.8 Derived Symmetric key Generation, Storage and Deletion

Derived symmetric key to encrypt the video and associated metadata shall be derived by using a Random number generator satisfying RQT-001403 requirement, shall be stored in a secure area within application memory with read only access and shall be deleted from memory after a recording.

<table>
<tr><th colspan="4">Rationale</th></tr>
<tr><td colspan="4"></td></tr>
<tr><th colspan="3">Acceptance Criteria</th><th>V&V Method</th></tr>
<tr><td colspan="3">• Symmetric key should be derived by using a random number generator satisfying RQT-001403 requirement.
• New key should be generated per recording and previously used should be deleted from application's memory after a recording</td><td>DV Review</td></tr>
<tr><th colspan="4">Notes</th></tr>
<tr><td colspan="4"></td></tr>
<tr><th>Version</th><th>Date</th><th>Author</th><th>Change</th></tr>
<tr><td>1.4</td><td>5/18/2021</td><td>Srapart1</td><td>second version</td></tr>
</table>

2.1.9

Metadata File Encryption

All the PII (Personally Identifiable Information) in Metadata shall be encrypted and saved to the USB Drive using AES-128 with Counter Mode (CTR) of operation with a derived unique symmetric key per recording.

Rationale	
Metadata that contains PII needs to be encrypted.	
Acceptance Criteria	**V&V Method**
• All PII metadata needs to be encrypted using AES-128 with CTR mode of operation using derived unique symmetric key per recording	DV Testing and Review
Notes	

Version	**Date**	**Author**	**Change**
1.4	5/18/2021	Srapart1	second version

2.1.10

Video File Optional Encryption

Video file data shall be encrypted according to user selection and saved to the USB Drive. If selected to be encrypted, AES-128 with Counter Mode (CTR) shall be used with derived symmetric key per recording

Rationale	
Video files contain PII and can be optionally encrypted in persistent storage.	
Acceptance Criteria	**V&V Method**
• If user has selected to encrypt video files, they are encrypted with AES-256 with CTR mode of operation using a derived unique symmetric key per recording	DV Testing and Review
Notes	

			Scott Sheahan
Version	**Date**	**Author**	**Change**
1.4	5/18/2021	Srapart1	second version

2.1.11

Derived Symmetric Key Encryption

The derived symmetric key used to encrypt the video recordings and metadata shall be encrypted by using an Asymmetric RSA 2048 mode of encryption [RFC8017]

Rationale	
Derived symmetric key is used to encrypt the videos and needs to be encrypted by a Master Asymmetric key.	
Acceptance Criteria	**V&V Method**
• Derived symmetric key should be encrypted with as Master Asymmetric encryption key. RSA 2048 mode of encryption should be chosen.	DV Testing and Review
Notes	
RFC8017 - https://datatracker.ietf.org/doc/html/rfc8017	

Version	**Date**	**Author**	**Change**
1.4	5/18/2021	Srapart1	Initial version

2.1.12

Video Recorder Service Interface Disabled in Valet Mode

The Video Recorder Service HMI interface shall not be accessible while SYNC is in Valet Mode.

Rationale			
User will need to put vehicle in Valet Mode to block unauthorized viewing or deletion of videos from the Video Recorder Service.			
Acceptance Criteria			**V&V Method**
• The Video Recorder Service HMI interface is not accessible by the user while in Valet Mode.			DV Testing and Review
Notes			
			Scott Sheahan
Version	**Date**	**Author**	**Change**
1.4	3/4/2020	ssheahan	second version

2.1.13

Video Recorder Service Log Events

The following events shall be logged by the Video Recorder Service:

- Error state when video is commanded to be recorded and video data is not received
- Deletion of videos through SYNC HMI from USB flash storage
- USB insertion and extraction from system
- When video files are marked as read only to prevent deletion
- When video or metadata file signature check fails

Rationale			
Logs can be used for forensic purposed to verify events took place.			
Acceptance Criteria			**V&V Method**
• Each log event shall be tested and verified that it has been logged to a file.			DV Testing and Review
Notes			
			Scott Sheahan
Version	**Date**	**Author**	**Change**
1.4	3/4/2020	ssheahan	Second version