Car Connectivity Consortium

MirrorLink®

DAP Audit Requirements and Certificate Management

Version 1.1.6
(CCC-TS-035)

VERSION HISTORY

Version	Date	Comment
1.1.0	24 October 2012	Approved Version
1.1.1	05 March 2013	Approved Errata Version
1.1.2	05 November 2013	Approved Errata Version
1.1.3	18 March 2013	Approved Errata Version
1.1.4	17 June 2014	Approved Errata Version
1.1.5	17 September 2014	Approved Errata Version
1.1.6	18 March 2015	Approved Errata Version

LIST OF CONTRIBUTORS

Brakensiek, Jörg (Editor)	Microsoft Corporation
Ewing, Alan	Nokia Corporation
Kostiainen, Kari	Nokia Corporation
Pichon, Ed	E-Qualus (for CCC)

LEGAL NOTICE

The copyright in this Specification is owned by the Car Connectivity Consortium LLC (“CCC LLC”). Use of this Specification and any related intellectual property (collectively, the “Specification”), is governed by these license terms and the CCC LLC Limited Liability Company Agreement (the “Agreement”).

Use of the Specification by anyone who is not a member of CCC LLC (each such person or party, a “Member”) is prohibited. The legal rights and obligations of each Member are governed by the Agreement and their applicable Membership Agreement, including without limitation those contained in Article 10 of the LLC Agreement.

CCC LLC hereby grants each Member a right to use and to make verbatim copies of the Specification for the purposes of implementing the technologies specified in the Specification to their products (“Implementing Products”) under the terms of the Agreement (the “Purpose”). Members are not permitted to make available or distribute this Specification or any copies thereof to non-Members other than to their Affiliates (as defined in the Agreement) and subcontractors but only to the extent that such Affiliates and subcontractors have a need to know for carrying out the Purpose and provided that such Affiliates and subcontractors accept confidentiality obligations similar to those contained in the Agreement. Each Member shall be responsible for the observance and proper performance by such of its Affiliates and subcontractors of the terms and conditions of this Legal Notice and the Agreement. No other license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

Any use of the Specification not in compliance with the terms of this Legal Notice, the Agreement and Membership Agreement is prohibited and any such prohibited use may result in termination of the applicable Membership Agreement and other liability permitted by the applicable Agreement or by applicable law to CCC LLC or any of its members for patent, copyright and/or trademark infringement.

THE SPECIFICATION IS PROVIDED “AS IS” WITH NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AND COMPLIANCE WITH APPLICABLE LAWS.

Each Member hereby acknowledges that its Implementing Products may be subject to various regulatory controls under the laws and regulations of various jurisdictions worldwide. Such laws and regulatory controls may govern, among other things, the combination, operation, use, implementation and distribution of Implementing Products. Examples of such laws and regulatory controls include, but are not limited to, road safety regulations, telecommunications regulations, technology transfer controls and health and safety regulations. Each Member is solely responsible for the compliance by their Implementing Products with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for their Implementing Products related to such regulations within the applicable jurisdictions.

Each Member acknowledges that nothing in the Specification provides any information or assistance in connection with securing such compliance, authorizations or licenses**.**

NOTHING IN THE SPECIFICATION CREATES ANY WARRANTIES, EITHER EXPRESS OR IMPLIED, REGARDING SUCH LAWS OR REGULATIONS. ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF ANY INTELLECTUAL PROPERTYRIGHTS OR FOR NONCOMPLIANCE WITH LAWS, RELATING TO USE OF THE SPECIFICATION IS EXPRESSLY DISCLAIMED. BY USE OF THE SPECIFICATION, EACH MEMBER EXPRESSLY WAIVES ANY CLAIM AGAINST CCC LLC AND ITS MEMBERS RELATED TO USE OF THE SPECIFICATION.

CCC LLC reserve the right to adopt any changes or alterations to the Specification as it deems necessary or appropriate.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

TERMS AND ABBREVIATIONS

ACMS	Application Certification Management System
BT	Bluetooth
CA	Certification Authority
CCC	Car Connectivity Consortium
CTS	Conformance Test System
DAP	Device Attestation Protocol
ML	MirrorLink
OCSP	Online Certificate Status Protocol
OS	Operating System
PK	Public Key
RFB	Remote Framebuffer
SK	Secure Key
UPnP	Universal Plug and Play
USB	Universal Serial Bus
VNC	Virtual Network Computing

MirrorLink is a registered trademark of Car Connectivity Consortium LLC

Bluetooth is a registered trademark of Bluetooth SIG Inc.

RFB and VNC are registered trademarks of RealVNC Ltd.

UPnP is a registered trademark of UPnP Forum.

Other names or abbreviations used in this document may be trademarks of their respective owners.

1 ABOUT

This document specifies the requirements for security audits of MirrorLink client and server devices and device manufacturers in support of the Device Attestation Protocol (DAP) component of the MirrorLink specifications. These audits are intended to ensure that the DAP system will not be compromised by the leak of a secret key in the DAP authentication chain, and to limit the damage caused by a leak.

The specification lists a series of requirements, either explicitly or within the text, which are mandatory elements for a compliant solutions. Recommendations are given, to ensure optimal usage and to provide suitable performance. All recommendations are optional.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are following the notation as described in RFC 2119 [1].

1. MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
2. MUST NOT: This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
3. SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
5. MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

2 DAP Certification Architecture

The Device Attestation Protocol (DAP) establishes a trust chain between any MirrorLink Server device and any MirrorLink Client device using X.509 certificates as specified [2]. The DAP certification architecture is based on a single, centralized root-of-trust, which is the CCC Certification Authority (CCC CA). The CCC CA can sign MirrorLink Server device manufacturer certificates. The CCC CA's public key is installed into every MirrorLink Client device.

Every MirrorLink Server manufacturer MUST run their own intermediate-CA to issue device certificates and sign them with the manufacturer key. A MirrorLink Server manufacturer MUST receive only one CCC signed manufacturer certificate per named corporate entity. The MirrorLink Server manufacturer MAY issue sub-certificates that can in turn generate device certificates to allow for better integration with their existing manufacturer systems.

The DAP Certification Architecture is shown in the following figure.

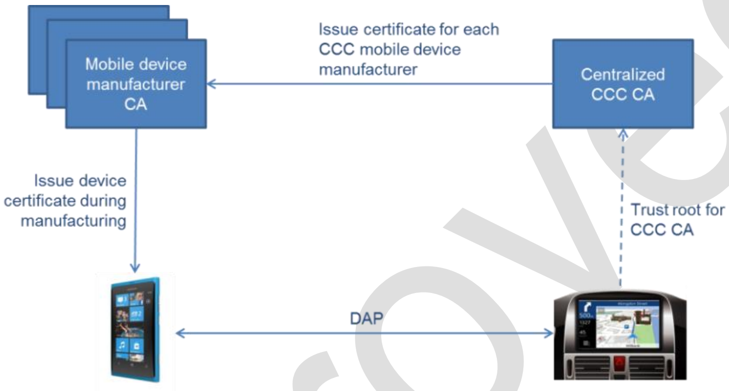
Mobile device manufacturer CA
Issue certificate for each CCC mobile device manufacturer
Centralized CCC CA
Issue device certificate during manufacturing
Trust root for CCC CA
DAP

Figure 1: DAP Certification Architecture

MirrorLink uses standard X.509 certificates for establishing trust relationships between the different involved entities. X.509 uses key pairs SK_A/PK_A, whereas SK_A defines the private key and PK_A the Public key. The certificate is used from the issuer, to sign a key or attribute of a subject, using the issuer's private key. Therefore the certificate $Cert_A = Sig(SK_B, PK_A)$ means that the certificate issuer B has signed the Public key PK_A of A with the Private key SK_B (of issuer). The Public key PK_B is available from the root certificate of the issuer. Note: The root certificate of the issuer might be in term signed from a different CA.

The entire end-to-end trust chain is therefore built on a series of X.509 certificates, as shown in the following figure.

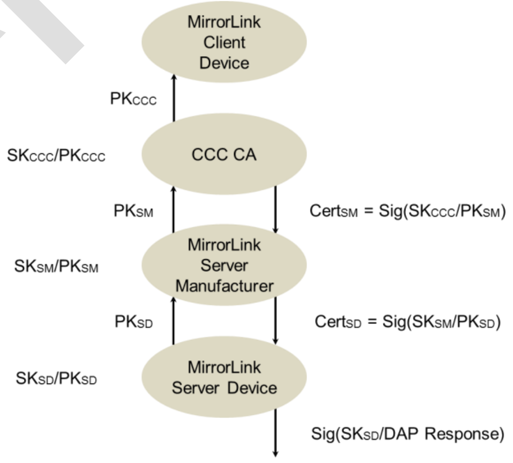

Figure 2: DAP Trust Chain

The public key is provided to the signing entity, which returns it back signed within the certificate. Note that the private root key is never exposed to anybody. Its public key though is widely shared to validate that the trust chain points to this trust root.

As soon as any of the private keys of the trust chain leaks, the chain is broken, as certificates can be easily copied and installed on any other device.

3 DAP CERTIFICATE MANAGEMENT

In DAP device certification, one of the biggest challenges is the fact that some certified device keys may leak. Essentially, if even one key leaks it can be copied to an unlimited number of fake devices that can then perform faked DAP protocol runs. To prevent key leakage, mobile device manufacturers will either deploy software/OS-based protection mechanisms for the certified device keys in their devices or use hardware protection mechanisms. For keys protected by hardware protection mechanisms, key leakage is unlikely.

There are two well-known ways to handle key leaks, if they appear:

1. issue short-lived device certificates, or
2. deploy online certificate revocation system.

In any revocation system, the verifier of the certificate (i.e., the MirrorLink Client in our case) should contact an online service for fetching the latest certificate revocation list (CRL) or checking the revocation status of given certificates using OCSP.

Doing such online checks is difficult with MirrorLink Clients that have no connectivity, and in addition, the current version of DAP protocol provides no support for revocation checks. In principle, it is possible to utilize the connectivity of the mobile device for certificate revocation checks, but that requires updates to DAP protocol. That also requires CCC to establish an online revocation system for device certs.

Thus, for MirrorLink possible key leakage will be handled with an expiration date for manufacturer and device certificates dependent on the risk for key leakage.

- Long-lived certificates have an expiration date of up to **10 years** after the signing date.
- Short-lived certificates have an expiration date of up to **1 year** after the signing date.

Manufacturer certificates MUST NOT have an expiration date beyond the expiration date of the certifying CCC root certificate. Device certificates MUST NOT have an expiration date beyond the expiration date of the certifying manufacturer certificate.

Device and manufacturer certificates MUST use the "Not Before" validity field, containing the date and time of the signature. MirrorLink Client devices, which do not have access to date and/or time information MUST NOT validate the validity period of the certificates.

CCC Root, manufacturer and device certificates MUST use RSA key signing algorithms.

3.1 Renew DAP Certificates

When a manufacturer certificate expires, the MirrorLink server manufacturer is expected to renew the manufacturer certificate from the CCC root Certification Authority (CA), and to issue the renewed manufacturer certificate to all corresponding fielded devices. Manufacturer Certificates for devices, which device key has leaked, MUST NOT be renewed.

The device manufacturer SHOULD obtain new manufacturer certificates prior to expiration of the old ones to avoid shortened device certificate lifetimes. The CCC root certification authority MUST allow for overlapping periods.

Short-lived Manufacturer Certificates

CCC MUST allow the device manufacturer to renew their manufacturer 1 year prior the current one expires. CCC MUST issue a new manufacturer certificate with an up to 1 + 1 year life time.

Long-lived Manufacturer Certificates

CCC MUST allow the device manufacturer to renew their manufacturer 10 years prior the current one expires. CCC MUST issue a new manufacturer certificate with an up to 10 + 2 years life time.

This overlapping manufacturer certificate's validity period is shown for a short-lived manufacturer certificates in Figure 3 and for long-lived manufacturer certificates in Figure 4.

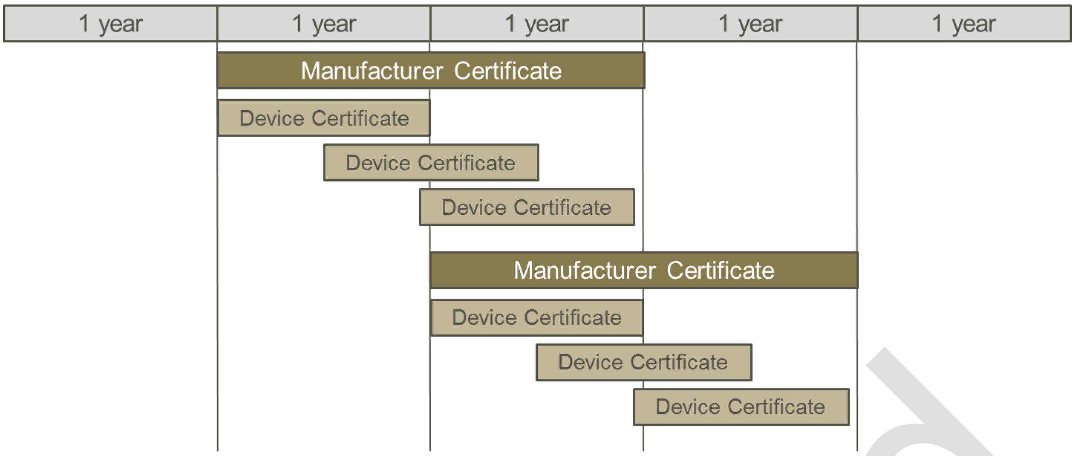

Figure 3: Overlapping Manufacturer Certificate Validity, while signing Device Certificates (short-lived)

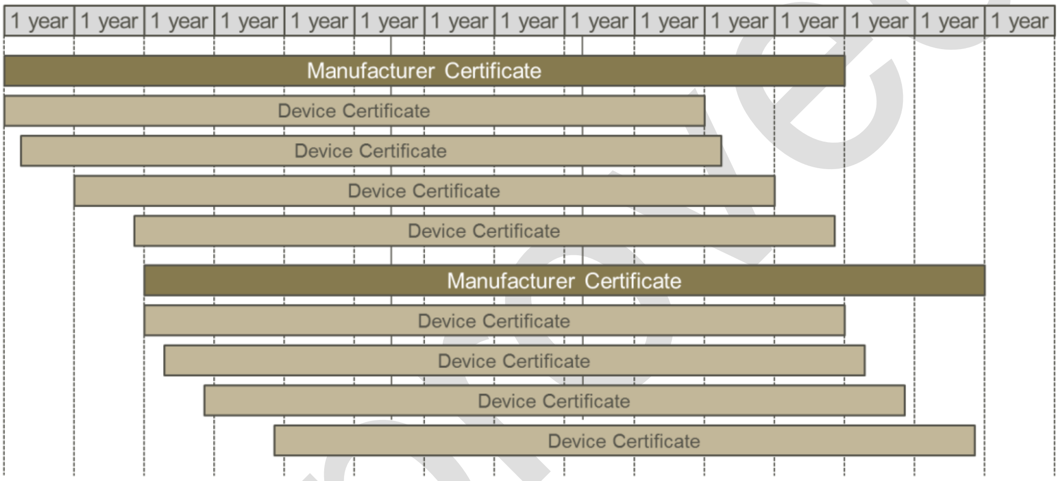

Figure 4: Overlapping Manufacturer Certificate Validity, while signing Device Certificates (long-lived)

When a device certificate expires, the MirrorLink server manufacturer is expected to issue a renewed device certificate to all corresponding fielded devices. Device Certificates for devices, which device key has leaked, MUST NOT be renewed.

3.2 Leakage of DAP Private Device Keys

If the CCC notices key leaks and fake devices using leaked keys, there will be a window of time in which misuse is possible. Once the device certificate of leaked key expires this certificate MUST NOT be renewed, and the CCC has a way of recovering from the incident.

The MirrorLink Server manufacture SHOULD issue unique device certificates per device. The MirrorLink Server manufacturer MAY issue the same device certificate to a batch of devices. If a device key from one device, out of a batch of devices, leaks, the MirrorLink Server manufacturer MUST NOT update device certificates of any device within the same batch. Other devices of the same manufacturer, outside the batch, remain operational, when their device certificates get renewed. If a server manufacturer misbehaves (e.g. renews certificates for leaked keys or issues device certificates with too long expiry times), CCC MAY decide not to renew the manufacturer certificate. Manufacturer and Device certificates SHOULD expire the same time, so that they can be renewed together.

If the private device key leaks, the server manufacturer MUST inform CCC about the key leakage, MUST NOT renew the device certificate, make improvement plan for security which to present to CCC and audited, issue new device (and manufacturer) certificates (only in case the underlying problem has been fixed). Issue an update to server or server's key store. CCC MUST keep this information SECRET.

3.3 Changes to MirrorLink Server Manufacturer Names

In case the name of a MirrorLink Server manufacturer's corporate entity, which is named within the CCC signed manufacturer certificate, changes, CCC will issue a new signed manufacturer certificate on request from the MirrorLink Server manufacturer.

The MirrorLink Server manufacturer MUST only undergo a new MirrorLink Sever manufacturer audit, prior received the newly signed certificate, in case the new corporate entity is applying any change to the processes or tools, audited in the original manufacturer audit.

It is the responsibility of the MirrorLink Server manufacturer to provide evidence (e.g. in written statements), that supports why no new audit is necessary.

It is the responsibility of CCC's Device Certification Body to decide whether a full, a partial or no audit will be necessary.

4 MIRRORLINK SERVER MANUFACTURER AUDIT

A MirrorLink Server device manufacturer is subject to the MirrorLink Manufacturer Audit when DAP functionality is implemented into any of their MirrorLink enabled devices. MirrorLink server manufacturers MUST be periodically audited to ensure that they are taking adequate measures to maintain the validity and security of the DAP system.

In case the MirrorLink server manufacturer is not using the same DAP certificate management process across different devices or device families, each DAP certificate management process MUST be audited individually or via an Engineering Change Order (ECO) process.

Changes to the DAP certificate management process MUST be audited within 6 month, using an Engineering Change Order (ECO) process.

4.1 Risks

The primary risk to the DAP system from the server manufacturers comes in two forms:

1. Leakage of private keys for the server manufacturer or server device. If either key is leaked, it can be copied into unlimited number of fake devices. If fake measurement or signatures can be generated, then only one device is affected.
2. Issuing of invalid device certificates. If a manufacturer's intermediate-certificate is issued to a non-trusted party, that certificate could be used to generate invalid device certificates for an unlimited number of fake devices.

4.2 Audit Objectives

The purpose of the Server Manufacturer Audit is to ensure that the server manufacturer has implemented adequate security processes to:

- Protect generated private keys and prevent them from being exposed.
- Generate key pairs in a secure, non-predictable manner.
- Control issuing of manufacturer's intermediate-certificates to prevent them from being issued to non-trusted party.

The following aspects MUST be included in the Audit:

Aspect	Audit Analysis
Device Key Generation	• Protection against private key leakage • Secure key-pair generation • Validation of expiration periods • Validation of device certificate recipients
Intermediate-Certificate Generation	• Protection against private key leakage • Secure key-pair generation • Validation of intermediate-certificate recipients
Device Certificate Management	• Mechanism to renew device certificates • Identification of leaked keys • Mechanism to replace leaked device certificates • Issue of batch device certificates • Validation of device certificate recipients

Table 1: MirrorLink Server Manufacturer – Audit Aspects

The Audit MUST follow common practices.

4.3 Audit Verdicts

The audit will provide one of the following verdicts:

Verdict	Consequence
FAILED	• MirrorLink Server manufacturer MUST discontinue use of manufacturer certificate granted by CCC's certificate authority. • MirrorLink Server manufacturer MUST exclude DAP support from their PICS for any device they manufacture. • MirrorLink Server manufacturer MUST NOT issue Device Certificates for any devices they manufacture.
PASSED	• MirrorLink Server manufacturer MAY obtain a manufacturer certificate from the CCC's certificate authority. • MirrorLink Server manufacturer MAY include DAP support from their PICS for any device they manufacture. • MirrorLink Server manufacture MAY issue Device Certificates for any devices they manufacture. • No new audit required for 24 months.
CONDITIONAL	• MirrorLink Server manufacturer MAY obtain a manufacturer certificate from the CCC's certificate authority. • MirrorLink Server manufacturer MAY include DAP support from their PICS for any device they manufacture. • MirrorLink Server manufacture MAY issue Device Certificates for any devices they manufacture. • New audit is required within 6 months.

Table 2: MirrorLink Server Manufacturer – Audit Verdicts

The auditing company SHOULD provide a recommendation for date of the next audit and the expiration date of the manufacturer certificate.

4.4 Use of Contractors

A MirrorLink Server device manufactures MAY use contractors, outsourcing or externally hosted systems to manage the server manufacturer related mechanisms.

A MirrorLink Server device manufacturer MUST control and ensure the security of the end-to-end delivery of the keys to their devices.

If the MirrorLink Server device manufacturer cannot show complete control over the key pair generation, distribution and signing, contractors MAY be subject to an additional audit, requested by the CCC Device Certification Body.

Contractors MUST distribute private keys or conduct certificate signing only to the extent required from the DAP process. The MirrorLink Server device manufactures MUST keep track of provided private keys and conducted certificate signing.

5 MIRRORLINK SERVER AUDIT

All MirrorLink Server devices, implementing DAP functionality, are subject to the MirrorLink Server Audit. Each MirrorLink server device seeking certification MUST provide an audit report to the certification body, documenting that the device implements adequate measures to maintain the validity and security of the DAP system.

A MirrorLink Server device MUST NOT pass DAP related MirrorLink Device Certification, if either the MirrorLink Server Manufacturer or the MirrorLink Server Device Audit is not successfully completed (allowed Audit Verdicts: PASSED or CONDITIONAL.

MirrorLink Building Blocks MAY NOT need to pass any DAP related audits, if the audit will be done as part of final product certification. A MirrorLink Server Building Block MUST only use DAP certificates (very short lived, for testing purpose), pointing to the CCC root, if the manufacturer has successfully passed the DAP Manufacturer Audit.

Changes to the implementation of the DAP functionality on the MirrorLink Server MUST be audited again, using an Engineering Change Order (ECO) process.

Any MirrorLink Server Device, not passing the DAP Audit, SHOULD NOT be granted MirrorLink Device Certification.

5.1 Background

The MirrorLink Client will trust the MirrorLink Server device that is operating the MirrorLink stack as specified and that it provides correct and valid information. Device Attestation Protocol (DAP) is used to establish a basic trust relationship between the MirrorLink Client device and the MirrorLink Server device, using an attestation model.

The basic idea behind the attestation model is based on a trusted software component (the Attestation Service), which measures other software components on the MirrorLink Server device and reports signed measurements or properties to the attestation verifier, i.e. the MirrorLink Client device.

In addition, certificates are used to control the operation of applications within a MirrorLink session, and must be signed by the CCC's root Certificate authority. These certificates are distributed using the Application Certification Management System (ACMS) via HTTP Get responses, and their revocation status is checked via OCSP query. The OCSP query includes a random nonce provided by the MirrorLink server device.

5.2 Risks

The two types of attackers can be distinguished with respect to MirrorLink Attestation Service.

1. **Remote attackers** that try to attack the system over the network. Such attackers can try to trick the user into installing malicious applications that may utilize software vulnerabilities in the mobile device OS and system libraries. The malicious code can then try to generate fake measurements or fake attestation signatures on this device, or extract the device key.
2. **Physical attackers** that have physical access to the device. Such attackers can try to read/extract the device key from a mobile device and then copy it into fake devices. Further physical attacks can be divided into
    a. *Simple physical attacks*, like reading device key from flash memory when device is turned off.
    b. *Sophisticated physical attacks*, like determining key bits from power consumption of the device ("side-channel attacks") or extracting the entire key by physically dismantling CPU core without destroying it.

Preventing device key extraction is more important than preventing generation of fake measurements or fake signatures. If one key is leaked, it can be copied into unlimited number of fake devices. If fake measurement or signatures can be generated, then only one device is affected.

Consumer electronic device can provide protection against device key leakage against remote attackers and simply physical attacks. Typical consumer electronic devices do not provide protection against sophisticated physical attacks.

In addition, MirrorLink Server devices must validate applications certificates provided by the ACMS. This validation includes verifying that the trust chain is based on the known CCC trust root. The CCC trust root, does not constitute any secrets, i.e. leakage of the CCC trust root, does not create any harm. But any attacker, being able to override the CCC trust root, can redirect the trust chain.

5.3 Audit Objectives

The purpose of this audit is to analyze how the MirrorLink DAP Server implements the following aspects of the DAP protocol

- Generation of DAP responses
- Measurement of MirrorLink components
- Protection of MirrorLink components
- Protection of Private keys

The following aspects MUST be included in the Audit:

Aspect	Audit Analysis
Measurement of MirrorLink Device (Attestation Service Integrity)	• Mechanism to protect Operating System boot o No protection – Any OS version can be booted o Signing – only signed OS images can boot (e.g. secure boot) • Protection of the boot signature verification key o SW based security mechanism o HW based security mechanism
Measurement of individual MirrorLink Server Protocol Components • TerminalMode:VNC-Server • TerminalMode:UPnP-Server • TerminalMode:RTP-Server • TerminalMode:RTP-Client • MirrorLink:CDB-Endpoint	• Mechanism for component measurement and validation o Verification that component is protected by the operating system o Verification that any port the component is using, is protected by the operating system o Verification that component or group of components has a valid identifier, which has been assigned by a (centralized) trusted authority (e.g. an entity within the device manufacturer) or that component is part of a trusted authority. o Calculation of a hash value over the attested component
Component specific session keys	• Protection against private key leakage o SW based security mechanism o HW based security mechanism
Signing DAP responses	• Protection against private key leakage o SW based security mechanism o HW based security mechanism • Mechanism for access control to ensure that only genuine Attestation Service is allowed to sign data with the device key o Verification that calling component is protected by the operating system o Verification that calling component identifier is assigned by a centralized trusted authority or that component is part of a trusted authority.

Aspect	Audit Analysis
	○ Calculation of a hash value over the calling component.
MirrorLink Stack Runtime Integrity	• Protection against port hijacking ○ Verification that port is protected by the operating system • Protection against un-authorized component replacement ○ Verification that component is protected by the operating system
IMEI Protection	• Protection against fake IMEI number for MirrorLink server devices, which can be used for development devices. ○ SW based security mechanism ○ HW based security mechanism
Creation of OCSP requests	• Mechanism to create a random nonce
ACMS Root Certificate Key	• Mechanism to protect the CCC root certificate key

Table 3: MirrorLink Server Device – Audit Aspects

5.4 Audit Verdicts

The audit will provide one of the following verdicts:

Verdict	Consequence
FAILED	• MirrorLink Server manufacturer MUST exclude DAP support from their PICS for the device. • By failing the audit the MirrorLink Server MUST not be provided with a DAP Manufacturer Certificate • MirrorLink Server manufacturer MUST NOT issue Device Certificates for the device
PASSED	• MirrorLink Server manufacturer MAY include DAP support from their PICS for the device. • MirrorLink Server manufacture MAY issue Device Certificates for the device. • No new audit required.
CONDITIONAL	• MirrorLink Server manufacturer MAY include DAP support from their PICS for the device. • MirrorLink Server manufacturer MAY issue Device Certificates for the device. • New audit is required within 6 months.

Table 4: MirrorLink Server Device – Audit Verdicts

The auditing company MAY provide a recommendation for the validity period.

The MirrorLink Server device MUST pass all of the following conditions in order to receive long-lived up to 10-year device certificates.

- Attestation service integrity:
  - Only manufacturer signed OS image can be booted
  - HW security is used to protect the integrity of this signature verification key.
- Measurement of ML components:
  - Measurement component integrity protected by OS
  - Port allocation protected by OS

  - Components have identifiers assigned by trusted authority OR are part of a trusted authority OR app identities can be verified with calculated binary hashes
- Components specific keys
  - None
- Signing DAP responses
  - DAP private key HW protected
  - DAP signing HW protected
  - DAP signing access control by OS

If any of the above conditions is not fulfilled, the MirrorLink server device can only use up to 1-year short-lived device certificates.

A MirrorLink Server device MUST NOT be used as a development device for MirrorLink certified applications if the MirrorLink Server device fails the IMEI related audit and does not provide HW based security mechanisms for IMEI protection.

5.5 Testing Considerations

In order to perform developmental testing of their devices, MirrorLink Server manufacturers need the ability to install legitimate device certificates in devices during development. For the purposes of testing, MirrorLink Server manufacturers are allowed to issue a small number (≤100) of device certificates with an expiration of ≤3 months from the date of signing before successful completion of their Server Device Audit. MirrorLink Server manufacturers must still have a PASSED/CONDITIONAL result for their Server Manufacturer Audit in order to receive a Manufacturer Certificate.

6 MirrorLink Client Audit

All MirrorLink Client devices, implementing DAP functionality, are subject to the MirrorLink Client Audit. Each MirrorLink client device seeking certification shall provide an audit report to the certification body, documenting that the device implements adequate measures to maintain the validity and security of the DAP system.

A MirrorLink Client device MUST NOT pass DAP related MirrorLink Device Certification, if the MirrorLink Client Device Audit is not successfully completed (allowed Audit Verdicts: PASSED or CONDITIONAL).

MirrorLink Building Blocks MAY NOT need to pass any DAP related audits, if the audit will be done as part of final product certification.

6.1 Risks

The DAP client is responsible for validating the MirrorLink Server's DAP responses. This validation includes verifying that the trust chain is based on the known CCC trust root. The trust root, does not constitute any secrets, i.e. leakage of the trust root, does not create any harm. But any attacker, being able to override the trust root, can redirect the trust chain.

6.2 Audit Objectives

The purpose of this audit is to analyze how the MirrorLink DAP Client implements the following aspects of the DAP protocol

- Validation of trust chain

The following aspects MUST be included in the Audit:

Aspect	Audit Analysis
Creation of DAP requests	• Mechanism to create a random nonce
Validation of trust chain	• Mechanism for trust chain validation • Protection against overriding CCC trust root • Integrity of the validation process
Integrity of the public root key	• Mechanism to protect the public root key o Note: For the purposes of performing conformance testing, the CCC root certificate key must be changed to the CTS root certificate key. Changing this value MUST NOT be user-accessible.
Integrity of the MirrorLink Stack	• Integrity of the MirrorLink Client stack

Table 5: MirrorLink Client Device – Audit Aspects

6.3 Audit Verdicts

The audit will provide one of the following verdicts:

Verdict	Consequence
FAILED	• MirrorLink Client manufacturer MUST exclude DAP support from their PICS.
PASSED	• MirrorLink Client manufacturer MAY include DAP support from their PICS. • No new audit required

CONDITIONAL	• MirrorLink Client manufacturer MAY include DAP support from their PICS. • New audit is required within 6 months.

Table 6: MirrorLink Client Device – Audit Verdicts

The auditing company MAY provide a recommendation for the date of the next audit.

7 REFERENCES

[1] IETF, RFC 2119, “Keys words for use in RFCs to Indicate Requirement Levels”, March 1997. http://www.ietf.org/rfc/rfc2119.txt

[2] IETF, RFB 2459, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, January 1999, http://www.ietf.org/rfc/rfc2459.txt

[3] Car Connectivity Consortium, “MirrorLink - Device Attestation Protocol”, Version 1.1, CCC-TS-014

[4] Car Connectivity Consortium, “MirrorLink – Application Certificate Handling”, Version 1.1, CCC-TS-036