ETSI TS 103 544-4 V1.3.1 (2019-10)

Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 4: Device Attestation Protocol (DAP)

CAUTION

The present document has been submitted to ETSI as a PAS produced by CCC and approved by the ETSI Technical Committee Intelligent Transport Systems (ITS).

Reference

RTS/ITS-98-4

Keywords

interface, ITS, PAS, smartphone

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

The present document is part 4 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.1].

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document is part of the MirrorLink® specification which specifies an interface for enabling remote user interaction of a mobile device via another device. The present document is written having a vehicle head-unit to interact with the mobile device in mind, but it will similarly apply for other devices, which provide a color display, audio input/output and user input mechanisms.

The term "device attestation" in this context refers to the MirrorLink client verifying that the MirrorLink server is from a compliant manufacturer and running approved software. The attestation will be based on standard X.509 certificates [2] and attestation mechanisms defined by Trusted Computing Group®.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] W3C Recommendation 11 April 2013: "XML Signature Syntax and Processing Version 1.1".

NOTE: Available at http://www.w3.org/TR/xmldsig-core/.

[2] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate", May 2008.

NOTE: Available at http://tools.ietf.org/html/rfc5280.

[3] IETF RFC 3279: "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002.

NOTE: Available at http://tools.ietf.org/html/rfc3279.

[4] Trusted Platform Module (TPM) specifications, Version 1.2.

NOTE: Available at http://www.trustedcomputinggroup.org/resources/tpm-main-specification.

[5] TCG Mobile Trusted Module Specification, Version 1.0, April 2010.

NOTE: Available at https://trustedcomputinggroup.org/resource/mobile-phone-work-group-mobile-trusted-module-specification/.

[6] Recommendation ITU-T X.690 (08/2015): "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[7] ETSI TS 103 544-12 (V1.3.1): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 12: UPnP Server Device".

[8] ETSI TS 103 544-9 (V1.3.1): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 9: UPnP Application Server Service".

[9] ETSI TS 103 544-10 (V1.3.1): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 10: UPnP Client Profile Service".

[10] ETSI TS 103 544-2 (V1.3.1): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 2: Virtual Network Computing (VNC) based Display and Control".

[11] ETSI TS 103 544-3 (V1.3.1): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 3: Audio".

[12] Trusted Computing Group, "Credentials Profiles Specification 1.1", May 2007.

NOTE: Available at http://www.trustedcomputinggroup.org/resources/infrastructure-work-group-tcg-credential-profiles-specification.

[13] ETSI TS 103 544-5 (V1.3.1): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 5: Common Data Bus (CDB)".

[14] ETSI TS 103 544-17 (V1.3.1): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 17: MirrorLink over Wi-Fi Display (WFD)".

[15] ETSI TS 103 544-21 (V1.3.1): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 21: High Speed Media Link (HSML)".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 103 544-1 (V1.3.1): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 1: Connectivity".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

pointer event: touch screen action in which the user touches the screen with one (virtual) finger only at a single location

touch event: touch screen action in which the user touches the screen with two or more separate fingers at different locations

NOTE: Touch events are used to describe more complex touch action, like pinch-open or pinch-close.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

PK_A	Public key of device A.
PK_{CCC}	Public key of the CCC root CA.
PK_{CTS}	Public key of the CTS root CA (for testing purpose).
PK_{CTSD}	Public key of the CTS Device (for testing purpose).
PK_{CTSM}	Public key of the CTS Manufacturer CA (for testing purpose).
PK_{SD}	Public key of a Server Device.

PK_{SM}	Public key of a Server Manufacturer CA.
SK_A	Private key of device A.
SK_B	Private key of device B.
SK_{CCC}	Private key of the CCC root CA.
SK_{CTS}	Private key of the CTS root CA (for testing purpose).
SK_{CTSD}	Private key of the CTS Device (for testing purpose).
SK_{CTSM}	Private key of the CTS Manufacturer CA (for testing purpose).
SK_{SD}	Private key of a Server Device.
SK_{SM}	Private key of a Server Manufacturer CA.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASN.1	Abstract Syntax Notation One
CA	Certification Authority
CCC	Car Connectivity Consortium
CDB	Common Data Bus
CTS	Conformance Test System
DAP	Device Attestation Protocol
DER	Distinguished Encoding Rules
HSML	High-Spead Media Link
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
ML	MirrorLink
MTM	Mobile Trusted Module
OID	Object IDentifier
OS	Operating System
PCR	Platform Configuration Register
PKCS	Public Key Cryptography Standards
RFB	Remote Framebuffer
RSA	Rivest-Shamir-Adleman
RTP	Real-time Transport Protocol
SHA	Secure Hash Algorithm
SOAP	Simple Object Access Protocol
TCP	Transmission Control Protocol
TPM	Trusted Platform Module
UDP	User Datagram Protocol
UINT	Unsigned INTeger
UPnP	Universal Plug and Play
URL	Universal Resource Locator
VNC	Virtual Network Computing
WFD	Wi-Fi Display
XML	eXtensible Markup Language
XSD	XML Schema Definition

4 Managing a DAP Session

4.1 Bindings

4.1.1 TCP Binding

4.1.1.1 Identifying DAP Server

The identification of the DAP server is described in [8].

4.1.1.2 Device Attestation Launch

The DAP server start-up is facilitated via the UPnP *TmApplicationServer*:1 service *LaunchApplication* action, as defined in [8]. The *LaunchApplication* action shall return with a URL to the DAP server.

If the returned URL is already used from any established DAP session, this session will continue without any change.

Otherwise a new DAP session shall be established, given the following steps:

a) DAP server shall listen for the DAP client to make TCP connection at the provided URL for at least 10 s.

b) DAP client shall make a TCP connection to the provided URL.

c) DAP server and client shall start DAP according to the steps defined in Clause 5.

4.1.2 Intentionally Terminating the DAP Session

The DAP server shall not intentionally terminate a DAP session.

The DAP client shall intentionally terminate a DAP session, using the following steps:

1) UPnP Control Point uses TmApplicationServer:1 service's *TerminateApplication* SOAP action to send termination request.

2) DAP client shall disconnect the TCP connection.

3) DAP server should disconnect the TCP connection on detection of the client TCP disconnect or 5 s after responding to the *TerminateApplication* SOAP action, whichever comes first.

The DAP client shall wait for any outstanding Device Attestation Response messages, for at least 10 s, prior to terminating the DAP session. The DAP Server shall provide a DAP response to any DAP request within 10 s.

4.1.3 Unintentionally Terminating the DAP Session

Unintentional termination of the DAP session may happen at any time due to error conditions. In the case of unintentional termination of the DAP session, the respective DAP server or client shall disconnect the TCP connection. The respective counterpart should disconnect as well.

If the MirrorLink Client decides to re-establish the DAP session, it shall follow the steps given in clause 4.1.1.2.

To avoid the DAP server or client being in a TCP TIME-WAIT time-out loop as a result of an unintentional active disconnect, the TCP socket should be established using the SO_REUSEADDR option (or similar platform specific variant), allowing the operating system to reuse a port address, even it is currently in the TIME-WAIT state or the DAP server should use a different, unaffected port number.

4.2 Other Bindings

Besides TCP/IP, it will be possible to run MirrorLink Device Attestation Protocol on top of other protocols like Bluetooth RFCOMM, but how to discover and establish connection for such configuration is outside the scope of the present document.

4.3 Testing Considerations

If the MirrorLink Client is in a dedicated testing state (as part of the MirrorLink Certification), it shall launch a new DAP session (either initiated automatically or manually from the user), whenever the DAP server has unintentionally terminated the DAP session.

The MirrorLink Client shall have a mechanism to allow a test engineer to launch a DAP session (either automatically or manually).

For DAP testing purposes, the MirrorLink Client shall use a CTS root certificate to validate responses from the CTS Server. This CTS root certificate shall be decoupled from the regular CCC root certificate used during production.

The CTS root certificate shall be accepted from the MirrorLink Client in test setup only. The CTS public key (DER encoded) and the 32-byte SHA-256 hash of the CTS public key (Base64 encoded) are provided separately.

The DAP trust chain, for testing purposes is shown in Figure 1.

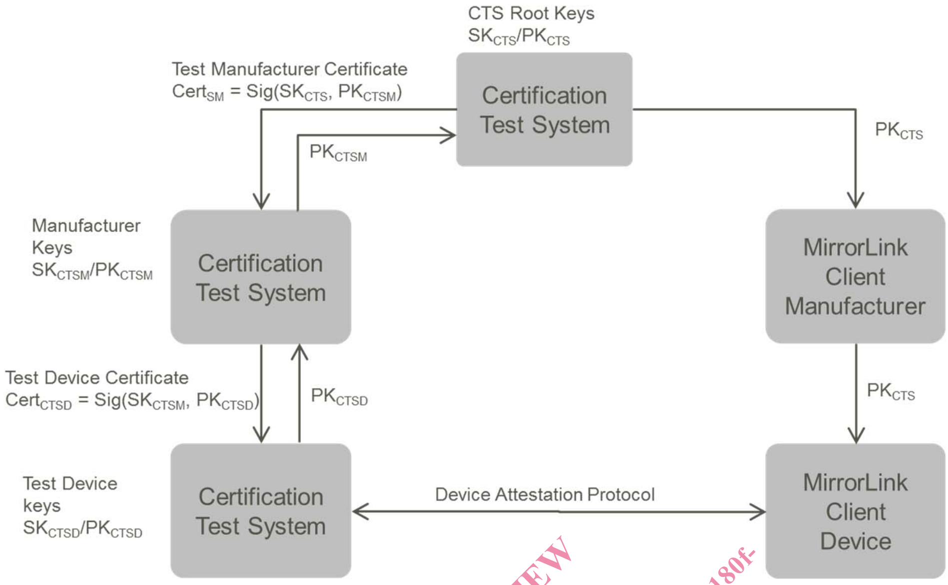

Figure 1: Device Attestation Certification Infrastructure - Testing Only

The MirrorLink Client shall not accept and request the CTS root certificate outside DAP testing and certification.

For testing MirrorLink Servers, the CTS shall only accept legitimate certificates signed by the CCC's Root Certificate.

5 Device Attestation Protocol

The prerequisite of successful Device Attestation Protocol run is that the MirrorLink server has a X.509 device certificate (with Extended Key Usage *tcg-kp-AIKCertificate* OID 2.23.133.8.3 as specified in clause 3.5 of [12]) for its device key pair from the server device manufacturer. The MirrorLink Client shall not expect other X.509 certificate extensions, mandated e.g. in clause 3.4 or 3.5 of [12]. Additionally, the server shall have one X.509 manufacturer certificate signed from the CCC DAP management system. The server device's private key(s) shall be stored securely. The secure storage is manufacturer specific and may use:

1) hardware-based Mobile Trusted Module (MTM) [5] implementation or equivalent;

2) storage on OS, which integrity has been verified with hardware-assisted secure boot process; or

3) storage on OS alone.

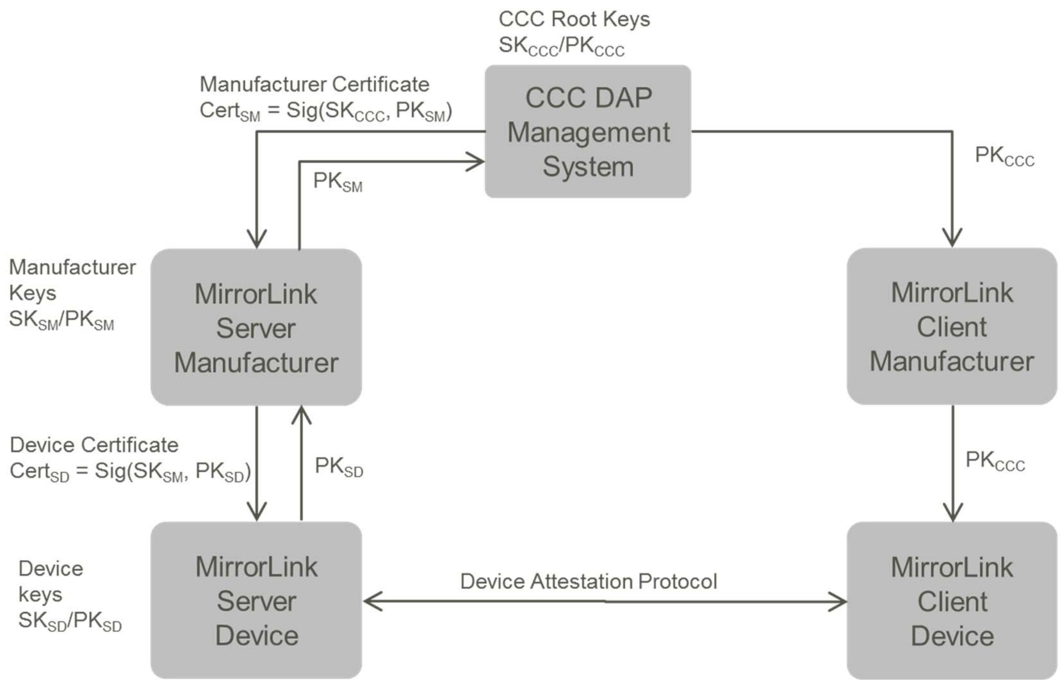

Figure 2: Device Attestation Certification Infrastructure

MirrorLink assumes pre-established trust relationships and security associations between the MirrorLink server device manufacturers and MirrorLink client device manufacturers via a central CCC controlled DAP Management System which extends to both client and server devices. This is achieved using a standard X.509 certificate chain.

The key pair SK_A/PK_A, as shown in Figure 2 consists of the private key SK_A and the public key PK_A. The certificate $Cert_A = Sig(SK_B, PK_A)$ is an X.509 public key certificate with subject public key PK_A and signed with private key SK_B (i.e. the certificate issuer is B).

After the MirrorLink Server device manufacturers have been certified from the central CCC DAP management system ($Cert_{SM} = Sig(SK_{CCC}, PK_{SM})$), they can certify individual devices they produce ($Cert_{SD} = Sig(SK_{SM}, PK_{SD})$). Again, MirrorLink specifies using standard X.509 certificates. This certification will typically take place during device manufacturing time, but some device manufacturers may have proprietary mechanisms and the device cert may be bootstrapped during first boot. This operation is done only once per each device.

Using the device certificate, the MirrorLink Server device can authenticate/attest itself to the MirrorLink Client device. For this MirrorLink specifies using Device Attestation Protocol (DAP). This process (DAP) will be run for each connection from a MirrorLink Server device to the MirrorLink Client device. Both the device and the manufacturer certificates are included in the DAP message exchange. Using this chain of certificates, the MirrorLink Client device can verify at runtime that the MirrorLink Server device is a genuine/compliant device from an authorized MirrorLink Server device manufacturer. The MirrorLink Client shall have the public key PK_{CCC} available, to be able to validate the MirrorLink Server device manufacturer certificate.

An overview of device and software attestation protocol is shown in Figure 3 below. The protocol is two-flow protocol: MirrorLink client sends *attestationRequest* message and MirrorLink server replies with *attestationResponse* message. Both of these messages are XML formatted.