ETSI TS 103 544-16 V1.3.1 (2019-10)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/8d...-5fed-4b2d-bbe6-af3b1b02d45a/etsi-ts-103-544-16-v1.3.1-2019-10

Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 16: Application Developer Certificates

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).

CCC is owner of the copyright of the document CCC-TS-044 and/or had all relevant rights and had assigned said rights to ETSI on an "as is basis". Consequently, to the fullest extent permitted by law, ETSI disclaims all warranties whether express, implied, statutory or otherwise including but not limited to merchantability, non-infringement of any intellectual property rights of third parties. No warranty is given about the accuracy and the completeness of the content of the present document.

Reference

RTS/ITS-98-16

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

iTeh STANDARD PREVIEW (standards.iteh.ai) Full standard: https://standards.iteh.ai/catalog/standards/sist/...ecf7-5fcd-4b24-...b1b02.../etsi-ts-103-544-16-v1.3.1-2019-10

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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

©ETSI 2019.
© Car Connectivity Consortium 2011-2019.
All rights reserved.

ETSI logo is a Trade Mark of ETSI registered for the benefit of its Members.
MirrorLink® is a registered trademark of Car Connectivity Consortium LLC.
RFB® and VNC® are registered trademarks of RealVNC Ltd.
UPnP® is a registered trademark of Open Connectivity Foundation, Inc.
Other names or abbreviations used in the present document may be trademarks of their respective owners.
DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
oneM2M™ logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners.
GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/8ab6ecf7-5fed-4b2d-bbe6-af3a1b7dd45a/etsi-ts-103-544-16-v1.3.1-2019-10

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 16 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.1].

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/adb6ecf7-5fed-4b0d-bbe6-a63b1902d45a/etsi-ts-103-544-16-v1.3.1-2019-10

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 colour display, audio input/output and user input mechanisms.

MirrorLink provides the ability to run certified applications on MirrorLink server devices that can be launched from the MirrorLink Client device. In order to improve safety and ensure a quality user experience, an application certification program is implemented that will control which applications can be used with MirrorLink in drive on in non-drive situations. Application developers will be able to use specific application development certificates, which simplifies the development of applications on the one side, but which will be usable only on a small set of MirrorLink Server devices - as well as a potentially restricted set of MirrorLink Client devices.

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

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

[2] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", June 2013.

NOTE: Available at https://tools.ietf.org/html/rfc6960.

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

[4] ETSI TS 103 544-14 (V1.3.1): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 14: Application Certificates".

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI standard:
https://standards.iteh.ai/catalog/standards/sist/82b6ecf7-5fe4-4b2d-bbea-af3b502d4ae/etsi-ts-103-544-16-v1.3.1-2019-10

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

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

ACMS	Application Certification Management System
AIA	Authority Information Access
CA	Certificate Authority
CN	Common Name
CTS	Conformance Test System
DAP	Device Attestation Protocol
DER	Distinguished Encoding Rules
HTTP	HyperText Transfer Protocol
OCPS	Online Certificate Status Protocol
OCSP	Online Certificate Status Protocol
RFB	Remote Framebuffer
RSA	Rivest-Shamir-Adleman
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Universal Resource Locator
UUID	Universally Unique IDentifier
VNC	Virtual Network Computing
XML	eXtensible Markup Language

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/8db6ecf7-5fed-4b63-be6-af3b1b02145a/etsi-ts-103-544-16-v1.3.1-2019-10

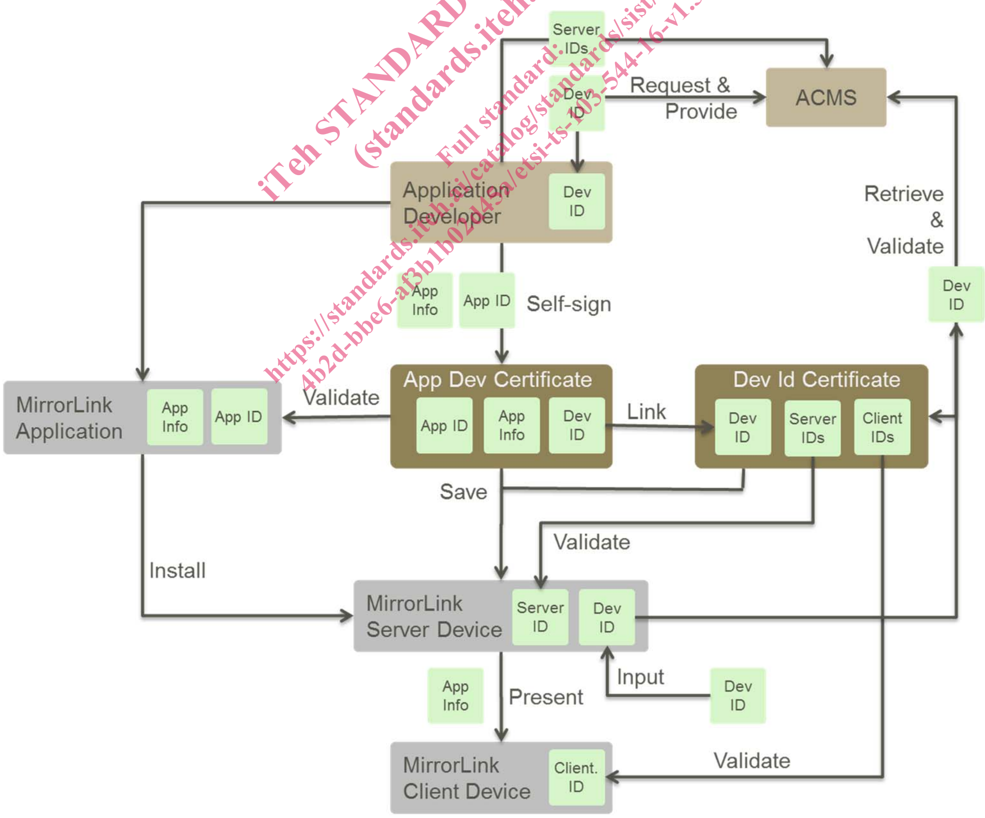
4 Developer Application Concept

MirrorLink provides the ability to run certified applications on MirrorLink server devices that can be launched from the MirrorLink client device. In order to improve safety and ensure a quality user experience, an application certification program is implemented that will control which applications can be used with MirrorLink in drive on in non-drive situations. Application developers will be able to use specific application development certificates, which simplifies the development of applications on the one side, but which will be usable only on a small set of MirrorLink Server devices - as well as a potentially restricted set of MirrorLink Client devices.

Each application under development, which can be uniquely identified by a platform specific application identifier (App ID), will come with an Application Development Certificate (App Dev Certificate), which contains the App ID; necessary application information, provided to the MirrorLink Client (App Info); and the Developer ID (Dev ID). The Application Development Certificate is self-signed by either the application developer or the MirrorLink Server's software development kit.

The MirrorLink Server will use the information from the App Development Certificate to validate the MirrorLink Application, and to link it to the Developer Identifier Certificate (Dev ID Certificate). The Dev ID Certificate contains a unique Developer Identifier (Dev ID), and one or more Server Device Identifiers (Server Device IDs) for which the Dev ID Certificate is valid. An optional list of Client Device Identifiers (Client Device IDs) defines a black list of client devices, for which the Dev ID Certificate is not valid.

As shown in Figure 1, the App Dev and the Dev ID Certificates are stored on the MirrorLink Server Device. It is the responsibility of the MirrorLink Server to check, whether the Dev ID Certificate has not been revoked and whether it is valid for the MirrorLink Server and Client combination. In case the App Dev Certificate is valid, the corresponding MirrorLink application will be presented to the MirrorLink Client Device as an application coming with a certificate distributed by CCC.



iTeh STANDARD PREVIEW (standards.iteh.ai)
Full standard:

Figure 1: Application Developer Certification Architecture (MirrorLink Server View)

A MirrorLink Client will not see the difference from any regular non-development version, besides a different signing entity name and an additional X.509 v3 extension as specified in [1].

Support for development applications as described above may be restricted to specific MirrorLink Server Developer devices; those shall be made available to application developers. Therefore, a regular MirrorLink Server device may NOT be able to run development applications as certified applications.

5 Application Developer Certificate Structure

5.1 Application Development Certificate

5.1.1 General

MirrorLink Application Development Certificates shall be a public key X.509 version 3 certificate as specified in [1].

The certificate is a self-signed certificate. The signing authority shall not set an expiration date of longer than 1 month from the date of signing.

Application Development Certificate shall use 2048-bit RSA keys with SHA-256 or SHA-512 signature algorithms.

5.1.2 Extension Header

The X.509 extension header shall have the following format:

```
X509v3 extensions:
CCC-MirrorLink-Developer-Id Extension:
        extnId:    1.3.6.1.4.1.41577.3.1
        critical:  no
        extnValue: DER:OCTET STRING
   CCC-MirrorLink Extension:
        extnId:    1.3.6.1.4.1.41577.2.1
        critical:  no
        extnValue: DER:<DER encoded XML, as specified below>
```

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/8db6ecf7-5fed-42cb-be6-12b1b02d45a/etsi-ts-103-544-16-v1.3.1-2019-10

5.1.3 Extension Values

5.1.3.1 CCC-MirrorLink-Developer-Id

Developer Id, as provided from the Application Certification Management System (ACMS), shall be formatted as a character string of up to 40 alphanumeric characters (`'a'-'z', '0'-'9'`).

5.1.3.2 CCC-MirrorLink Extension Value

The DER encoded XML of the application information, as specified in [4].

The Signing Entity Name of application development certificates shall be `"DEVELOPER"`.

5.2 Developer Identification Certificate

5.2.1 General

The MirrorLink Dev ID Certificate shall be a public key X.509 version 3 certificate as specified in [1].

The certificate shall be signed by the CCC's Root Certificate. A hierarchy of Certification Authorities (CAs) may be used for Dev ID certificates. In case intermediate CAs are used, the entire certificate chain up to the root CA shall be provided to the MirrorLink Server together with the Dev ID certificate. Any intermediate certificate shall not have an expiration date of more than 1 year from the date of signing.

The Intermediate certificate, which is signed by the CCC root CA, shall have a Common Name (CN) in the issuer information, identical to "ACMS CA"; otherwise the certificate shall not be accepted. A valid example issuer information is given below:

```
Issuer: O=Car Connectivity Consortium, CN=ACMS CA
```

Any intermediate certificate shall use 4096-bit RSA keys with SHA-512 signature algorithms.

5.2.2 Extension Header

The X.509 extension header shall have the following format:

```
X509v3 extensions:
    CCC-MirrorLink-Developer-Id Extension:
        extnId:    1.3.6.1.4.1.41577.3.1
        critical:  no
        extnValue: DER:OCTET STRING
    CCC-MirrorLink-Developer-Server-Ids Extension:
        extnId:    1.3.6.1.4.1.41577.3.2
        critical:  no
        extnValue: DER:OCTET STRING
    CCC-MirrorLink-Client-Manufacturer-Ids Extension:
        extnId:    1.3.6.1.4.1.41577.3.3
        critical:  no
        extnValue: DER:OCTET STRING
```

5.2.3 Extension Values

5.2.3.1 CCC-MirrorLink-Developer-Id

Developer Id, as provided from the Application Certification Management System (ACMS), shall be formatted as a character string of up to 40 alphanumeric characters (‘a’-‘z’, ‘0’-‘9’).

5.2.3.2 CCC-MirrorLink-Developer-Server-Ids

A comma-delimited list of Server Ids, for which the Dev ID certificate is valid; each entry shall be formatted as a string (UTF-8).

Server IDs are the IMEI/IMEISV number or version 5 UUID derived from an equivalent unique identifier of the MirrorLink Server devices on which development applications can be used, as defined in the platform specific specification.

5.2.3.3 CCC-MirrorLink-Client-Manufacturer-Ids

Comma-separated list of MirrorLink Client manufacturer ids, for which the Dev ID certificate is not valid (black list). Each entry shall be formatted as a string (UTF-8).

Each list entry represents a manufacturer name, and shall match the manufacturer name (as provided from the UPnP Client Profile service [5]) or the *AppCertFilter*'s entity name (as used in the UPnP Application Server service [3]).

5.3 Root Certificate

The signing certification authority's Root Certificate, a hash of it or a hash of its public key shall be stored in the MirrorLink Server. Access to the certificate's public key shall be read-only.

Expiration date of the root certificate shall be 20 years from the date of signing.

Root certificate shall use 4 096-bit RSA keys with SHA-512 signature algorithms. The root certificate shall be identical to the DAP root certificate.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/8db6ecf7-5fed-4b2d-bead-f3b1b0285a/etsi-ts-103-544-16-v1.3.1-2019-10

6 Developer Identification Certificate Life Cycle

6.1 Certificate Retrieval and Validation

6.1.1 Certificate Retrieval

The MirrorLink Server shall use HTTP-GET to obtain the MirrorLink Dev ID certificate from the Application Certification Management System using the following URL:

```
http://acms.carconnectivity.org:80
```

The following GET command shall be used to obtain the application certificate:

```
GET /obtainDeveloperCertificate.html?
certificateVersion=1.0&
developerID=<Developer Identifier>&
serverID=<Server Identifier>
HTTP/1.1<CR><LF>
Host: acms.carconnectivity.org:80<CR><LF>
<CR><LF>
```

The provided *serverID* shall uniquely identify a particular MirrorLink Server device. The MirrorLink Server shall use the IMEI/IMEISV number (or equivalent unique identifier) of the MirrorLink Server device for *serverID*. Devices without an IMEI/IMEISV number shall not be used for Application development at this time.

The MirrorLink Server shall retrieve the Dev ID Certificate before it can use any self-signed application development certificates. The MirrorLink Server shall not retrieve the Dev ID Certificate, unless the device is going to be used for MirrorLink application development.

The ACMS's HTTP Server shall return the Dev ID certificate and the entire chain of intermediate certificates, Base 64 encoded. Blank lines separate the certificates, starting from the certificate signed directly by the CCC root CA.

Otherwise it shall provide one of the following error codes:

iTeh STANDARD PREVIEW (standards.iteh.ai)

Table 1: Certificate Retrieval Error Codes

HTTP Error Code	CCC Error Code	Description
1xx	N/A	MirrorLink Server shall handle the HTTP response in compliance with the HTTP protocol (implementation specific).
200	N/A	MirrorLink Server shall validate the received application certificate, in accordance with clause 6.1.2.
2xx	N/A	MirrorLink Server shall handle the HTTP response in compliance with the HTTP protocol (implementation specific).
3xx	N/A	MirrorLink Server shall handle the HTTP response in compliance with the HTTP protocol (implementation specific).
400	N/A	Bad request - The request cannot be fulfilled due to bad syntax (e.g. missing, empty or wrongly formatted parameter). The MirrorLink Server shall not retry the request.
4xx	N/A	MirrorLink Server shall not retry the request
500	800	No certificate available for the given parameter. The MirrorLink Server should retry the request.
500	801	Certification Database currently offline. The MirrorLink Server shall retry between 1 h and 24 h after the last HTTP-Get attempt.
500	8xx	Reserved for future use. The MirrorLink Server should retry the request.
500	900	Certificate has been revoked. The MirrorLink Server shall not retry the request.