

ETSI TS 103 544-14 V1.3.1 (2019-10)



**Publicly Available Specification (PAS);
Intelligent Transport Systems (ITS);
MirrorLink®;
Part 14: Application 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-036 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-98-14

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

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

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	7
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	7
3.3 Abbreviations	7
4 Application Certification Concept.....	8
5 Application Certificate Structure.....	9
5.1 X.509 Certificate	9
5.1.1 Application Certificate.....	9
5.1.2 Intermediate Certificate	9
5.1.3 Root Certificate.....	10
5.2 MirrorLink Extension.....	10
5.2.1 Extension Header	10
5.2.2 CCC-MirrorLink Extension Value	10
5.2.3 Certificate Signing Entities	12
5.2.4 MirrorLink Server Platform Identifier	13
5.2.4.1 Registered MirrorLink Server Platform Identifier	13
5.2.4.2 Proprietary MirrorLink Server Platform Identifier.....	13
5.2.5 MirrorLink Server Runtime Identifier	14
5.2.6 Application identifier.....	14
5.2.7 Mapping of Locales	14
6 Application Certificate Life Cycle	15
6.1 General	15
6.2 Certificate Retrieval and Validation.....	15
6.2.1 Certificate Retrieval.....	15
6.2.2 Certificate Validation.....	17
6.2.3 Testing Considerations	19
6.3 Certificate Revocation Checks	19
6.3.1 Revocation Protocol.....	19
6.3.2 Certificate Valid.....	22
6.3.3 Certificate Revoked	22
6.3.4 Certificate Updated	23
6.3.5 Unchecked Certificates	23
6.3.6 Testing Consideration.....	24
6.4 Query and Grace Periods.....	24
6.4.1 Query Period.....	24
6.4.2 Grace Period	25
6.4.3 Period Update	26
7 Handling of Applications with a Certificate distributed by CCC.....	27
7.1 Application Installation	27
7.2 Application Filtering	27
7.3 Updating UPnP Application Server Services	29
7.3.1 Eventing.....	29
7.3.2 A_ARG_TYPE_AppList.....	29
7.3.3 A_ARG_TYPE_CertifiedAppList.....	29
7.3.4 A_ARG_TYPE_AppCertificateInfo.....	30

Annex A (normative):	XSD MirrorLink Extension Value	31
Annex B (informative):	OCSP Request & Response Example.....	34
Annex C (informative):	Application Certificate Example	36
Annex D (informative):	Authors and Contributors.....	38
History		39

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/f57fe828-2436-4753-a913-770abd9c08b1/etsi-ts-103-544-14-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 14 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.

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.

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 <http://tools.ietf.org/html/rfc6960>.

[3] ETSI TS 103 544-16 (V1.3.1): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 16: Application Developer Certificates".

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

[5] ETSI TS 103 544-15 (V1.3.1): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 15: Application Programming Interface (API) Level 1 & 2".

[6] ETSI TS 103 544-22 (V1.3.1): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 22: Android Specific Specifications enabling AIDL-based MirrorLink® Applications".

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
API	Application Programming Interface
CA	Certificate Authority
CCC	Car Connectivity Consortium
CN	Common Name
CRL	Certificate Revocation List
CTS	Conformance Test System
DAP	Device Attestation Protocol
DER	Distinguished Encoding Rules
HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Numbers Authority
LLC	Logical Link Control
NR	Non-Restricted
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
PC	Personal Computer
PMD	Process Management Document
RFB	Remote Framebuffer
RSA	Rivest-Shamir-Adleman
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Universal Resource Locator
UTF	Unicode Transformation Format
UUID	Universally Unique Identifier
VNC	Virtual Network Computing
WP	Windows Phone

XML eXtensible Markup Language
XSD XML Schema Definition

4 Application Certification Concept

MirrorLink distinguishes three main categories of applications:

- 1) A **MirrorLink-Aware Application** describes an application that implements software interfaces, which can be used via MirrorLink. A MirrorLink-Aware Application does not have MirrorLink or CCC Member certification, as described below.
- 2) A **MirrorLink-Certified Application** describes the certification status of a MirrorLink-Aware Application, which is additionally fulfilling CCC application certification criteria. This category comes in two sub-categories:
 - a) A **MirrorLink Base-Certified Application** is fulfilling CCC application certification criteria for basic MirrorLink Client and Server interoperability, usability and reliability.
 - b) A **MirrorLink Drive-Certified Application** is a MirrorLink Base-Certified Application, which is additionally approved by the CCC for use in a MirrorLink Client and Server system by a driver, while the vehicle is in motion.
- 3) A **Member-certified Application** describes the certification status of a MirrorLink-Aware Application, which is additionally fulfilling CCC Member application certification criteria. This category comes in two sub-categories:
 - a) A **Member Base-Certified Application** is fulfilling the CCC Member's certification criteria for basic MirrorLink Server and CCC Member's MirrorLink Client interoperability, usability and reliability.
 - b) A **Member Drive-Certified Application** is a Member Base-Certified Application and is approved by the CCC Member for use in a MirrorLink Server and CCC Member's MirrorLink Client system by a driver, while the vehicle is in motion.

Certified applications will have an Application Certificate containing information about the application, relevant for allowing it in drive or non-drive mode (App Info), along with information (App ID) how the application can be securely identified on the MirrorLink Server device.

As shown in Figure 1, an application is downloaded from any application store and installed on the MirrorLink Server device. The application may come with a self-signed application certificate, which provides necessary information for the application advertisements as a MirrorLink-Aware Application.

In addition, the MirrorLink Server will retrieve the Application's associated MirrorLink or Member Certificate from the Application Certificate Management System (ACMS). The application identification information is used to securely link the application certificate to the downloaded and installed application. The MirrorLink Server device will be able to validate with the ACMS, whether the available application certificate is still valid.

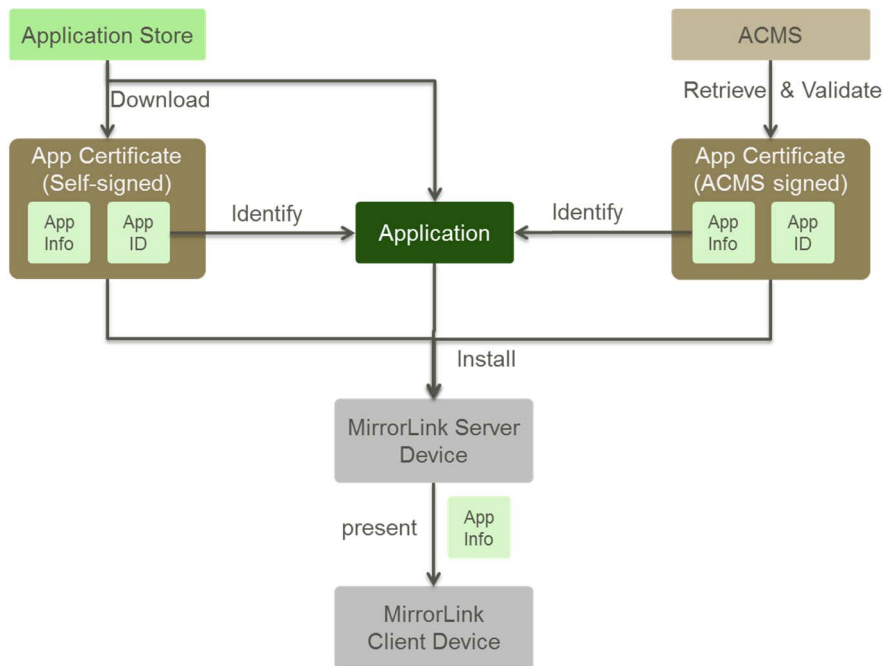


Figure 1: Application Certification Architecture (MirrorLink Server View)

The MirrorLink Server device will take the application information out of the validated application certificate and present the information to the MirrorLink Client devices.

Within the present document, we use the term **restricted** mode, to refer to the condition, when driver distraction rules have to be followed (e.g. while driving). The term **non-restricted** mode is used to refer to the condition, when driver distraction rules have not to be followed (e.g. while being parked).

5 Application Certificate Structure

5.1 X.509 Certificate

5.1.1 Application Certificate

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

MirrorLink uses long-lived Application Certificates. The signing Certification Authority should set an expiration date of 10 years from the date of signing, but it shall not be longer than the expiration date of the signing root or intermediate certificate.

Application Certificates shall use 2 048-bit RSA keys with SHA-256 or SHA-512 signature algorithms.

5.1.2 Intermediate Certificate

Hierarchy of certification authorities (CAs) may be used for application certification. 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 application certificate.

The Intermediate certificate, which 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

An Intermediate Certificate should have an expiration date of 20 years from the date of signing, but it shall not be longer than the expiration date of the signing root certificate.

Any Intermediate Certificate shall use 4 096-bit RSA keys with SHA-512 signature algorithms.

5.1.3 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.

5.2 MirrorLink Extension

5.2.1 Extension Header

The X.509v3 [1] extension header shall have the following format. The CCC-MirrorLink Extension Id is provided from IANA. The identifier shall be provided without any "<>" delimiter. Its value is outside the scope of the present document:

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

The CCC-MirrorLink-OCSP extensions for *queryPeriod*, *driveGrace* and *baseGrace* are defined later on clause 6.4.3.

5.2.2 CCC-MirrorLink Extension Value

The DER encoded XML shall follow the format in Table 1. Detailed description of the elements can be found in the definitions of *A_ARG_TYPE_AppList* and *A_ARG_TYPE_AppCertificateInfo* in [4].

Table 1: MirrorLink Extension Header extnValue XML

Element	Description	Parent	Availability
certificate	MirrorLink Application Certificate.	-	Required
version	Version of the certificate. NOTE: This version corresponds to the Certificate Version, mainly the structure of this XML. It does not correspond to the MirrorLink specification version.	certificate	Optional
majorVersion	Major Version (it shall be 1). Type: Unsigned integer. Default: 1.	version	Optional
minorVersion	Minor Version. Type: Unsigned integer. Default: 0.	version	Optional
appIdentifier	Platform specific application identifier (defined in Annex B).	certificate	Required
appListEntry	Application entry for the UPnP Application Server Service <i>A_ARG_TYPE_AppList</i> listing.	certificate	Required
name	Application name.	appListEntry	Required

Element	Description	Parent	Availability
providerName	Name of the application provider.	appListEntry	Optional
providerURL	URL of the application provider's website.	appListEntry	Optional
description	Text description of application.	appListEntry	Optional
iconList	List of available application icons.	appListEntry	Platform specific
icon*	Describes an application icon. The MirrorLink server shall include an icon for all applications with <protocolID> = VNC.	iconList	Platform specific
mimetype	Type of icon image (A_ARG_TYPE_String)	icon	Required
width	Width of icon (A_ARG_TYPE_INT).	icon	Required
height	Height of icon (A_ARG_TYPE_INT).	icon	Required
depth	Color depth of icon. (A_ARG_TYPE_INT).	icon	Required
url	URL where icon is available within the install package (platform specific). (A_ARG_TYPE_URI).	icon	Required
applInfo	Information about the listed application.	appListEntry	Optional
appCategory	Application category.	applInfo	Optional
displayInfo	Information about display content.	appListEntry	Optional
contentCategory	Visual content categories used.	displayInfo	Optional
orientation	Display orientations supported.	displayInfo	Optional
audioInfo	Information about audio content.	appListEntry	Optional
audioType	Audio type.	audioInfo	Optional
contentCategory	Audio content categories used.	audioInfo	Optional
appCertInfoEntry	Application entry for the UPnP Application Server Service A_ARG_TYPE_AppCertificateInfo listing.	certificate	Required
appUUID	UUID of the application. The UUID shall be unique across all mobile device platform variants and application versions.	appCertInfoEntry	Optional
entity*	Certifying entity.	appCertInfoEntry	Optional
name	Entity name. Unique identifier of the entity certifying the application. Allowed values are specified in Table 2.	entity	Required
targetList	Target.	entity	Optional
target*	Target name. Entry is undefined in case of the CCC entity and shall be ignored from the MirrorLink Client. Otherwise the format is OEM specific. The OEM may use this entry to implement a white and/or black list of supported targets.	targetList	Required
restricted	List of locales for restricted use.	entity	Required
nonRestricted	List of locales for non-restricted use.	entity	Required
serviceList	List of used data services.	entity	Required
service*	Service name.	serviceList	Required
properties	Application properties. Contains an UTF-8 XML representation of certified application properties. The XML representation is out-of-scope of the present document.	appCertInfoEntry	Optional