ETSI TS 103 544-14 V1.3.0 (2017-10)

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).

Reference

DTS/ITS-88-14

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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 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 3281: "An Internet Attribute Certificate Profile for Authorization", April 2002.

NOTE: Available at http://www.ietf.org/rfc/rfc3281.txt.

[2] IETF RFC 2459: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January 1999.

NOTE: Available at http://www.ietf.org/rfc/rfc2459.txt.

[3] 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.

[4] ETSI TS 103 544-16 (V1.3.0): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 16: Application Developer Certificates".

[5] ETSI TS 103 544-9 (V1.3.0): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 9: UPnP Application Server Service".

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 (V1.3.0): "Publicly Available Specification (PAS); Intelligent Transport Systems (ITS); MirrorLink®; Part 1: Connectivity".

3 Abbreviations

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

ACMS	Application Certification Management System
BT	Bluetooth
CCC	Car Connectivity Consortium
ML	MirrorLink
OCSP	Online Certificate Status Protocol
RFB	Remote Framebuffer
UPnP	Universal Plug and Play
USB	Universal Serial Bus
VNC	Virtual Network Computing

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 in 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.

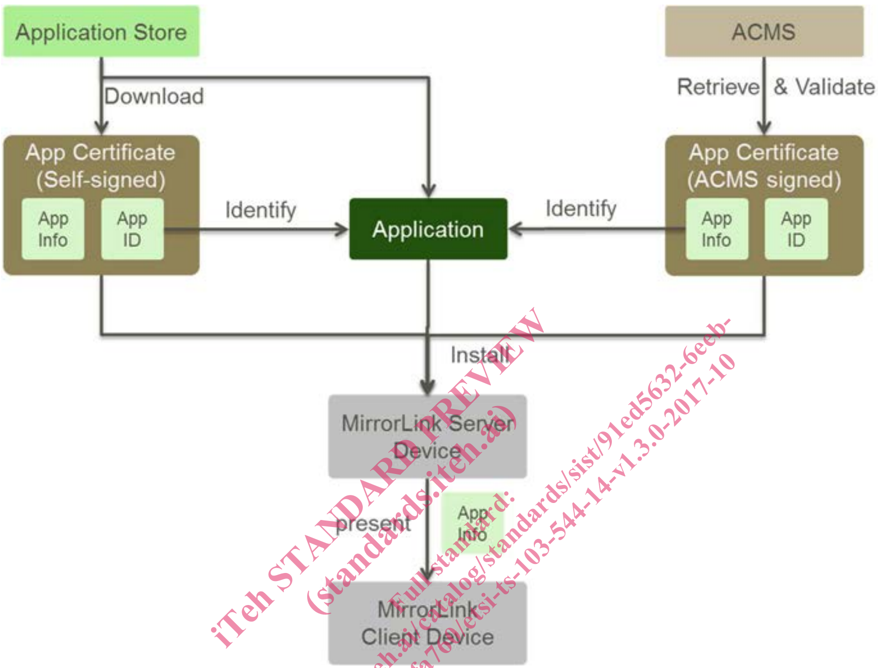

Figure 1: Application Certification Architecture (MirrorLink Server View)

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 2048-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 4096-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 4096-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.509 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 below. Detailed description of the elements can be found in Table 1.

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

Element	Description	Parent	Availability
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 A_ARG_TYPE_AppList listing	certificate	Required
name	Application name	appListEntry	Required
provider Name	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
appInfo	Information about the listed application	appListEntry	Optional
appCategory	Application category	appInfo	Optional
displayInfo	Information about display content	appListEntry	Optional
content Category	Visual content categories used	displayInfo	Optional
audioInfo	Information about audio content	appListEntry	Optional
audioType	Audio type	audioInfo	Optional
content Category	Audio content categories used	audioInfo	Optional
appCert InfoEntry	Application entry for the UPnP Application Server Srevice 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.	appCert InfoEntry	Optional
entity*	Certifying entity	appCert InfoEntry	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
non Restricted	List of locales for non-restricted use	entity	Required

Element	Description	Parent	Availability
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.	appCert InfoEntry	Optional
server Properties	MirrorLink Server Properties	certificate	Required
platform	Platform supported from application A separate certificate is provided for each platform/runtime.	server Properties	Required
platformID	Platform identifier, as defined in Table 3.	platform	Required
blacklisted Platform Versions	Comma separated list of black-listed platform versions. Version information is platform specific. Version information shall be complete. An empty version tag indicates that the application certificate is not dependent on a specific version of the host OS in question.	platform	Required
runtimeID	Runtime identifier, as defined in Table 4	platform	Required
blacklisted RuntimeVersions	Comma separated list of black-listed runtime versions. Version information is runtime specific. Version information shall be complete. An empty version tag indicates that the application certificate is not dependent on a specific runtime version.	platform	Required

Elements marked with a (*) can have multiple instances.

In case the entity is missing from the Application Certificate, the application shall be treated as a MirrorLink-Aware application.

5.2.3 Certificate Signing Entities

The following entity names are currently registered with CCC. The MirrorLink Client shall ignore any unknown entries.

Table 2: Certificate Signing Entities

Entity Name	Description
CCC	Car Connectivity Consortium The application follows application guidelines, as specified from CCC, for the certified regions.
DEVELOPER	MirrorLink Developer Application The application is a developer self-signed MirrorLink aware application, as specified in [4]. The application need not follow any application guidelines, as specified from the CCC.
ACMS	MirrorLink Aware Application The application is a self-signed MirrorLink aware application. The MirrorLink Server shall check with the ACMS for a CCC or Member-signed certificate.
<Empty String> OR Tag missing OR Unknown entity name	MirrorLink Aware Application The application is a self-signed MirrorLink aware application. The MirrorLink Server shall not check with the ACMS for a CCC or Member-signed certificate.