10900-B Stonelake Boulevard, Suite 126 • Austin, TX 78759 USA
Phone: +1-512-498-WIFI (+1-512-498-9434) | Fax: +1-512-498-9435
www.wi-fi.org

Exhibit C-2

Wi-Fi Alliance Cover Sheet for All Documents Sent

Liaison Transmittance of Information
Name of External Organization: Car Connectivity Consortium
Date: 9/23/14
Title of Document Sent: Best Practices Document for Wi-Fi CERTIFIED Miracast™ Devices
Source Group within the Wi-Fi Alliance: Wi-Fi Display MTG
Requested Action(s): Information Only

The documents sent may only be used for the purposes of the liaison communication pursuant to the terms of the Liaison Agreement between the Wi-Fi Alliance and the organization noted above.

You acknowledge and agree that (i) the Wi-Fi Alliance has not conducted an independent intellectual property rights review of the documents and the information contained therein, and makes no representations or warranties regarding third party intellectual property rights, including without limitation patents, copyrights or trade secret rights; and (ii) the documents may contain inventions for which you and your members must obtain licenses from third parties before making, using or selling the inventions.

The input of the documents and information from the Wi-Fi Alliance in no way obligates the Wi-Fi Alliance nor its members to any of the membership policies, including but not limited to the intellectual property rights policy, of your organization.

YOUR USE OF THE DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS IS AT YOUR SOLE RISK. THE DOCUMENTS ARE PROVIDED ON AN "AS IS" "AS AVAILABLE" AND "WITH ALL FAULTS" BASIS. THE WI-FI ALLIANCE DISCLAIMS ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES OF ANY KIND, INCLUDING ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

TO THE FULL EXTENT PERMITTED BY LAW, THE WI-FI ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES (INCLUDING, WITHOUT LIMITATION, LOSS OF BUSINESS, REVENUE, PROFITS, GOODWILL, USE, DATA, OR OTHER ECONOMIC ADVANTAGE) ARISING OUT OF OR IN CONNECTION WITH THE USE OF THESE DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

_ Public _X_ Confidential

If the confidentiality box is selected, this liaison receipt of information is intended to be confidential pursuant to the agreement between the Wi-Fi Alliance and organization noted above. Neither party should make this communication available to non-members.

Best Practices Document for
Wi-Fi CERTIFIED Miracast™ Devices

Version 1.0

WI-FI ALLIANCE PROPRIETARY – SUBJECT TO CHANGE WITHOUT NOTICE

This document may be used with the permission of Wi-Fi Alliance under the terms set forth herein. By your use of the document, you are agreeing to these terms. Unless this document is clearly designated as an approved specification, this document is a work in process and is not an approved Wi-Fi Alliance specification. This document is subject to revision or removal at any time without notice. Information contained in this document may be used at your sole risk. Wi-Fi Alliance assumes no responsibility for errors or omissions in this document. This copyright permission does not constitute an endorsement of the products or services. Wi-Fi Alliance trademarks and certification marks may not be used unless specifically allowed by Wi-Fi Alliance.

Wi-Fi Alliance has not conducted an independent intellectual property rights ("IPR") review of this document and the information contained herein, and makes no representations or warranties regarding IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions.

Wi-Fi Alliance owns the copyright in this document and reserves all rights therein. A user of this document may duplicate and distribute copies of the document in connection with the authorized uses described herein, provided any duplication in whole or in part includes the copyright notice and the disclaimer text set forth herein. Unless prior written permission has been received from Wi-Fi Alliance, any other use of this document and all other duplication and distribution of this document are prohibited. Unauthorized use, duplication, or distribution is an infringement of Wi-Fi Alliance's copyright.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY WI-FI ALLIANCE AND WI-FI ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS DOCUMENT AND ANY INFORMATION CONTAINED IN THIS DOCUMENT.

Revision History

Version	Date	Remarks
1.0.	September 2014	Initial release

Table of Contents

1. Introduction

1.1. Purpose

The purpose of this document is to provide additional technical guidance and recommended best practices for the implementation of Wi-Fi CERTIFIED Miracast™ devices. Although the guidelines mentioned in this document are not mandatory for Miracast certification, their use will contribute towards enhancing the end-user experience with Miracast devices.

1.2. Scope

This document contains clarifications, guidelines, and recommendations for Miracast Source and Sink devices. These recommendations are not normative, and they do not supersede the generic protocol specification.

1.3. Related Documents

	Document	Date	Location
[1]	Wi-Fi Display Technical Specification v1.1	May 2014	Wi-Fi Alliance Website (www.wi-fi.org)
[2]	Wi-Fi Alliance Brand Styleguide	April 2014	Wi-Fi Alliance Website (www.wi-fi.org)
[3]	HDCP 2.2 IIA Compliance Test Specification	January 2014	DCP Website (www.digital-cp.com)

2. List of Acronyms and Definitions

AKE	Authenticated Key Exchange
Constricted content	Content where the quality has decreased in order to provide non-authorized viewers a lower resolution/lower quality version.
HDCP	High-bandwidth Digital Content Protection
HDCP revision mismatch	Discrepancy between what the content provider allows and what the device supports. For example, a new movie might require a higher HDCP version than is supported on the device
HDCP2	HDCP2 refers to HDCP IIA Specifications Rev.2.0, 2.1, 2.2, 2.2 Errata and future HDCP2 revisions.
LED	Light Emitting Diode
SKE	Session Key Exchange

3. Best Practices for HDCP Implementations

Section 3 applies only to Miracast devices that support HDCP2.

3.1. User Experience Issues

Consumers have frequently reported an inconsistent or unsatisfactory experience when attempting to stream protected content with their Miracast devices. Examples of common complaints are:

- Lack of error messages
- Inconsistent error messages
- Incorrect error messages
- Inconsistent behavior when protected content cannot be shown

3.2. Successful HDCP2 Authentication

The HDCP2 authentication protocol is described in the HDCP 2.2 IIA Compliance Test Specification [3]. As described in this specification, the HDCP2 authentication protocol includes four stages:

- Authenticated Key Exchange (AKE)
- Locality Check
- Session Key Exchange (SKE)
- Authentication with Repeaters (if repeater is present)

In this Miracast best practices document, "successful HDCP2 authentication" means that an HDCP2-capable Miracast source (with an HDCP Transmitter) successfully completed all the required stages in the HDCP2 authentication protocol.

Since an HDCP2 source may retry all or some of the stages of the authentication protocol, "HDCP2 authentication failure" should only be concluded after all the retry efforts fail.

For a given Miracast session, the following recommendations (Sections 3.3 and 3.4) stand true only if HDCP2 authentication does not succeed at the first attempt or during subsequent retries. If the first attempt at HDCP2 authentication succeeds, but subsequent attempts fail, Section 4.7 (Link Content Protection Setup) of [1] shall be followed. At this point, the end user can be informed of the failure via error messages as outlined in Sections 3.3.3, 3.3.4, and 3.4.2 of this document.

3.3. Recommended behavior for HDCP2-capable Miracast Source

The following recommendations should be taken as a group. All of these recommendations should be implemented on any Miracast Source capable of HDCP2.

3.3.1. Keep Miracast session alive

An HDCP2-capable Miracast source should not tear down the Miracast session when an HDCP2 error happens. Examples of HDCP2 errors are:

- HDCP2 authentication failure
- When the HDCP2-capable device playback of protected content is not possible

Keeping the Miracast session alive, despite HDCP2 errors, allows the Miracast source the flexibility needed to handle protected content playback problems in order to minimize user confusion.

3.3.2. Send constricted content if possible

In the case where the playback of protected content is not possible but constricted protected content is allowed (based on content rules and other rules that apply), it is recommended that the Miracast source proceed with constricted content playback if the capability exists.

3.3.3. Alert user regarding problem with protected content playback

An HDCP2-capable Miracast source should show an error message to the user to indicate that playback of protected content is not possible when playback of protected content is required but the Miracast source determines that it cannot send encrypted content to the sink.

A Miracast source may determine that it cannot send encrypted content due to various reasons for example:

- HDCP2 authentication failure
- Miracast sink not supporting HDCP2
- HDCP2 revision mismatches

3.3.4. Error messages for HDCP2 Capable Miracast Source

An HDCP2-capable Miracast source may not be able to determine the root cause of the HDCP2 problem reliably. An HDCP2-capable Miracast source should not indicate to the user the root cause of the protected content playback problem, unless the root cause can be determined with certainty. For example, an HDCP2-capable Miracast source should not indicate whether the problem is on the source or sink side or due to HDCP2 revision mismatches.

An error message should simply inform the user that the playback of protected content is not possible based on the current source and sink combination.

An HDCP2-capable Miracast source with a local display should show an error message on its local screen.

If the HDCP2-capable Miracast Source is a headless device, an error code in the form of audio and/or visual stimulus (beeping and/or flashing LEDs) should be given to the end user. A user-manual or similar document should establish the association between the audio/video stimulus and the HDCP2 incompatibility to the user.

In addition, the HDCP2-capable Miracast source (headless or not) should display an error message on the screen of the Miracast sink if it is not sending constricted content in place of the protected content.

When receiving constricted content a Miracast sink may display a periodic error message.

3.4. Recommended behavior for HDCP2-capable Miracast Sink

The HDCP2 authentication protocol does not ensure that an HDCP2-capable Miracast sink will reliably detect HDCP2 related problems. As a result, the sink should not make any decisions related to connectivity in order to address HDCP2 problems.

The following recommendations should be taken as a group. All of these recommendations should be implemented on any Miracast Sink capable of HDCP2.

3.4.1. Keep Miracast session alive

An HDCP2-capable Miracast sink should not terminate a Miracast session because of HDCP2 related problems.

Keeping the Miracast session despite HCDP2 errors allows the Miracast source flexibility needed to handle protected content playback problems in order to minimize user confusion.

3.4.2. Do NOT show error messages related to HDCP2

Since an HDCP2-capable Miracast sink cannot detect HDCP2 problems reliably, it should not show any error messages to the user (related to HDCP2 problems) other than error messages received from the source.

3.4.3. Support both HDCP2 encrypted and unencrypted content

After successful HDCP2 authentication, an HDCP2-capable Miracast source may send content using HDCP2 encryption. It may also send unencrypted content that does not require content protection. In this scenario, an HDCP2-capable Miracast sink should display both HDCP2 encrypted and/or unencrypted content as chosen by the source.

4. Appendix: Error Messages

List of Potential Error Messages displayed by either Source or Sink:

> The combination of Wi-Fi CERTIFIED Miracast™ devices you are currently using does not support the streaming of protected content when used together.