AN12976

Wi-Fi Alliance Derivative Certification Process

Rev. 6 — 13 December 2023   **Application note**

Document information

Information	Content
Keywords	Wi-Fi Alliance (WFA), certificate qualification, certification process, derivative
Abstract	Overview of Wi-Fi Alliance certification program and step-by-step procedure of the Wi-Fi derivative certification process

1 About this document

1.1 Purpose and scope

This document presents the overall Wi-Fi Alliance derivative certification process with the steps to follow for the derivative certification of your products.

1.2 References

Table 1. Reference documents

Document type	Description
Overview	Wi-Fi Alliance - *Wi-Fi _CERTIFIED_Derivative_Certifications_Overview_v3.2_0.pdf*
Policy	Wi-Fi Alliance - *Wi-Fi_Alliance_Derivative_Certifications_Policy_v4.2.pdf*

AN12976

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Application note

Rev. 6 — 13 December 2023

2 / 17

2 Wi-Fi certification program

2.1 Overview

Wi-Fi CERTIFIED™ is an internationally recognized logo of approval for products indicating that they meet the industry agreed standard for interoperability, security, quality and a range of application specific protocols. It ensures the product delivers best user experience.

The Wi-Fi certification program assures tested and proven interoperability among Wi-Fi devices. This certification gives confidence that Wi-Fi product bearing Wi-Fi Certified logo have passed rigorous interoperability requirements.

Authorized Test Labs(ATL) certification is important and most of the time it is the last milestone before the product launch.

For more information, refer to https://www.wi-fi.org/.

2.2 Certificate qualification

2.2.1 88W9098 (LBEE5ZZ1XL)

- STA | WiFi6 11ax
- STA | Wi-Fi CERTIFIED ac
- STA | Wi-Fi CERTIFIED n
- STA | PMF
- STA | VU
- STA | FFD
- STA | Security Improvement
- STA | WPA-SAE R3
- STA | Agile Multiband (MBO)

2.2.2 IW612 (LBES5PL2EL)

- STA | WiFi6 11ax
- STA | Wi-Fi CERTIFIED ac
- STA | Wi-Fi CERTIFIED n
- STA | PMF
- STA | VU
- STA | FFD
- STA | Security Improvement
- STA | WPA-SAE R3
- STA | Agile Multiband (MBO)

2.3 Roles and responsibilities

Wi-Fi Alliance

- Owner of the certification program
- Maintain policies and requirements
- Review ATLs results
- Final authority for the approval of Wi-Fi CERTIFIED products

Authorized Test Labs (ATL)

- Operate as independent testing facilities
- Submit results to WFA
- Help in getting the approval for ASD

WFA members

- Membership is needed to those who wish to obtain certification of products
- Only members can submit products to ATLs and choose any ATL

2.4 Certification process

Figure 1. Certification process
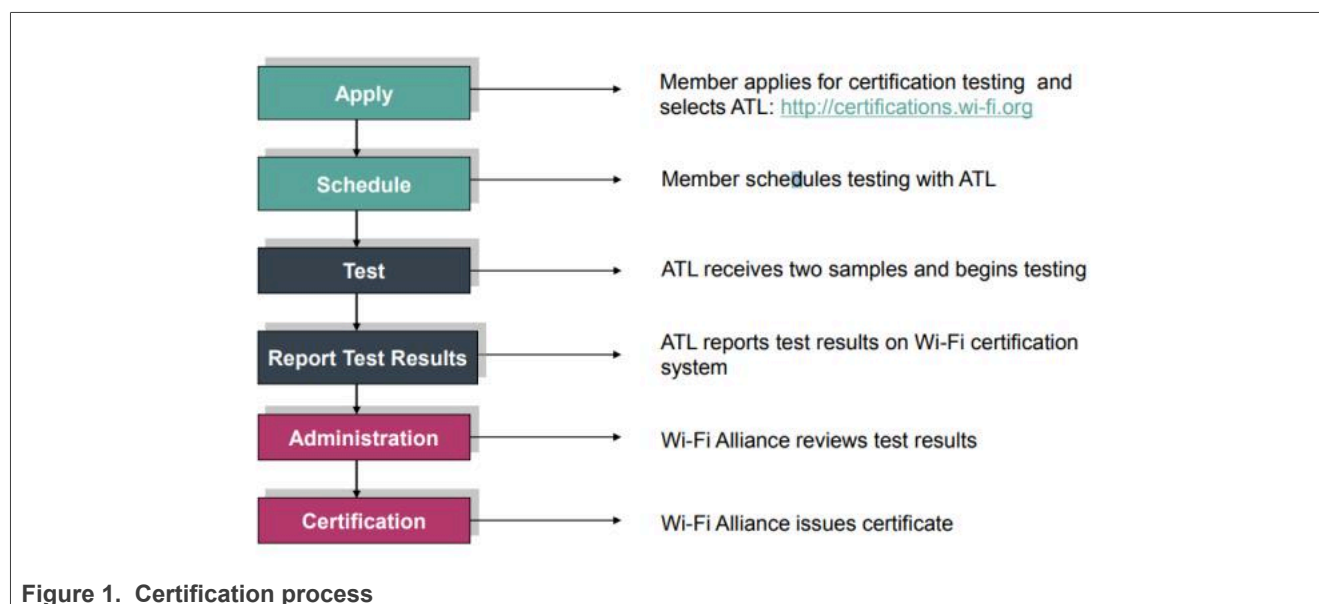
Note: When applying for a derivative certification, some steps of the certification process are skipped as you provide a reference to an already certified product. The process is explained in the following section.

Rev. 6 — 13 December 2023

3 Derivative certification

3.1 Overview

A derivative certification is a cost-effective way to utilize test results of a Wi-Fi CERTIFIED source product that has undergone ATL testing and Wi-Fi certification.

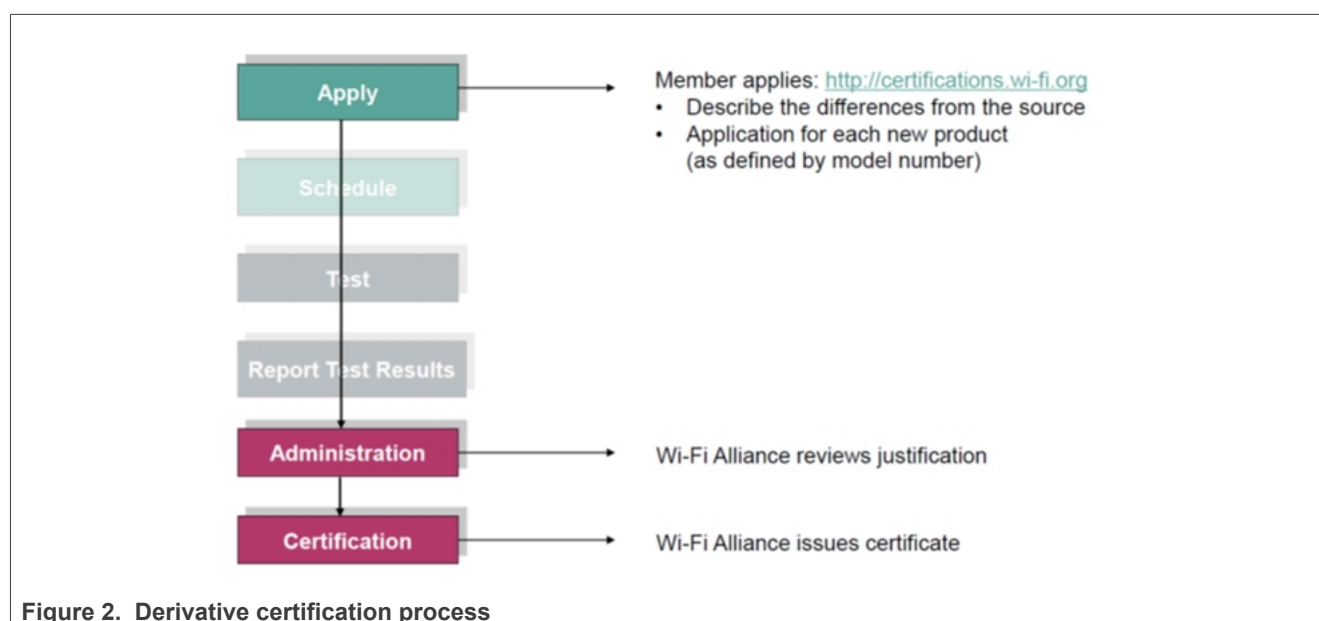Multiple derivative certifications can be created from the same source product.

The new product must have the same chipset, operating system (OS), and firmware as tested in the Wi-Fi CERTIFIED source product.

The new product must operate in the same manner as the Wi-Fi CERTIFIED source product.

Any changes in the new product MUST NOT affect the wireless functionality.

A derivative certification cannot be designated as a source, and as a result, a derivative certification cannot be used to create another derivative.

3.2 Derivative certification process

Figure 2. Derivative certification process

Please refer to Section 4 "Step by step procedure".

AN12976

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Application note

Rev. 6 — 13 December 2023

5 / 17

4 Step by step procedure

4.1 Log on and start a new application

Log on to www.wi-fi.org site as a member. The site opens on the **Applications** page. Click on the **New Application** tab.
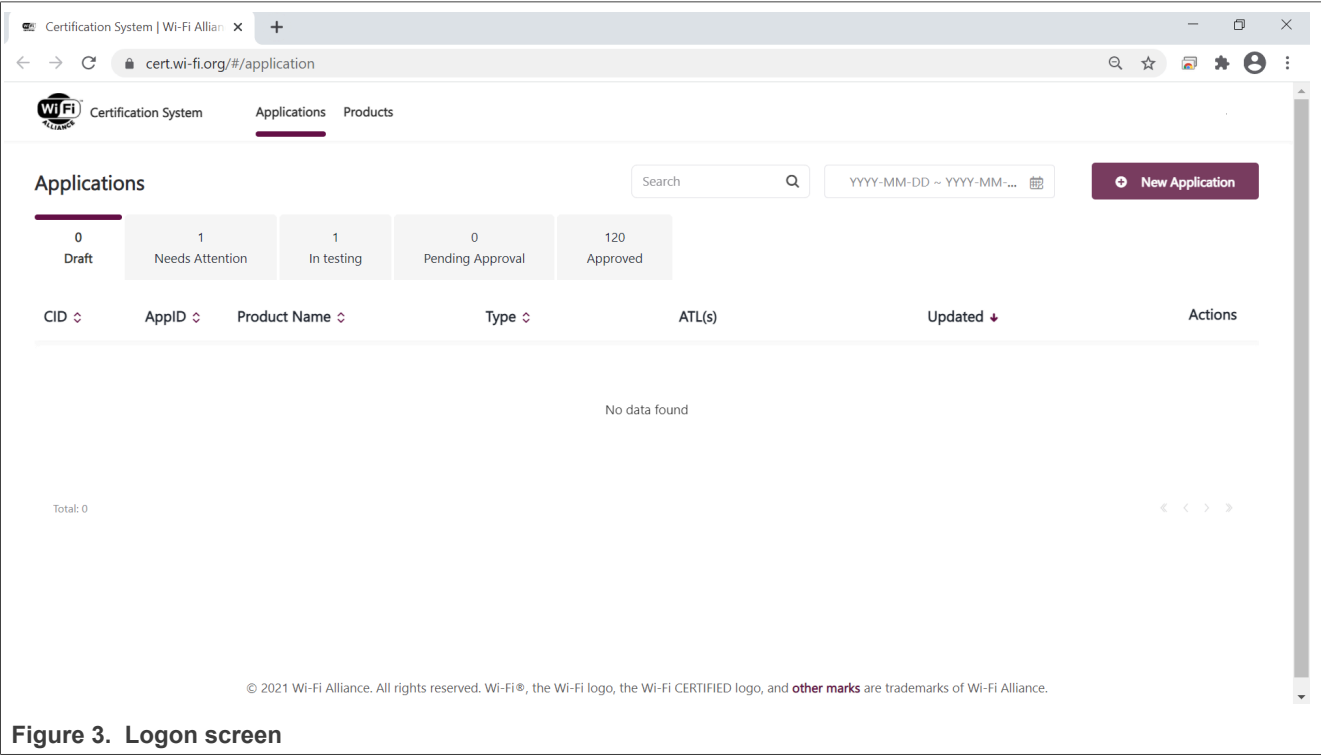
Figure 3. Logon screen

AN12976

Application note

All information provided in this document is subject to legal disclaimers.

Rev. 6 — 13 December 2023

© 2023 NXP B.V. All rights reserved.

6 / 17

On the New Application page, go to **Please select the certification type**, and select the third item on the list: **A derivative of Existing Product**.
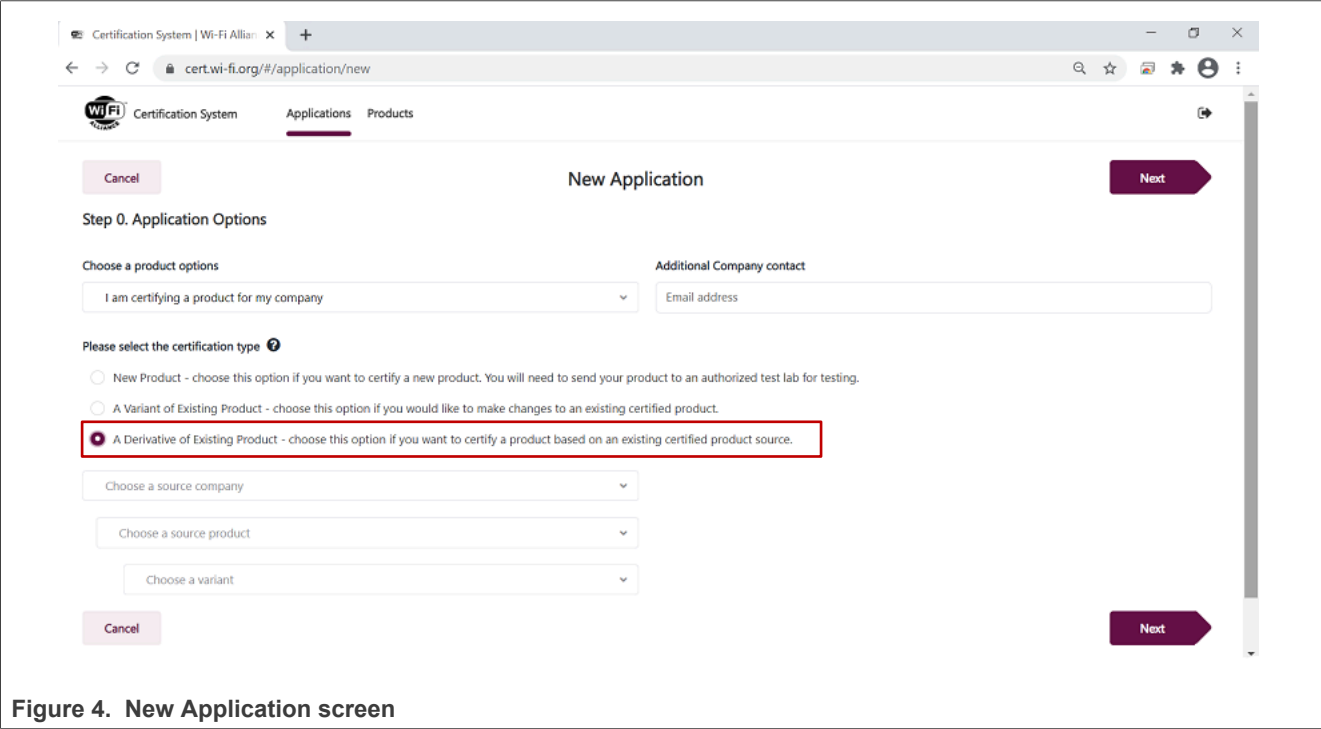
Figure 4. New Application screen

- Click on the icon on the right of the first field to open the list and select **NXP Semiconductors** as the source company.
- Click on the icon on the right of the second field and select the CID for your product and operating system. Figure 5 shows the CID for 88W8987-based wireless module and Linux OS.
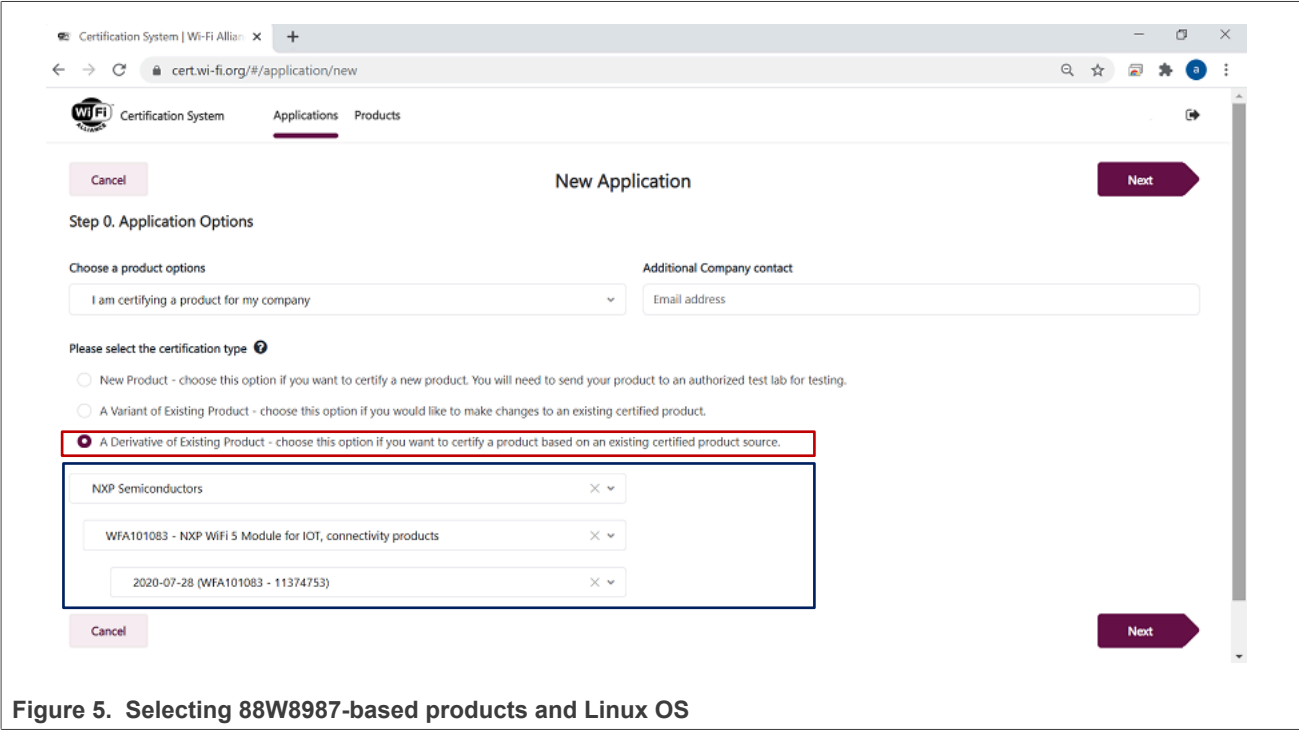

Figure 5. Selecting 88W8987-based products and Linux OS

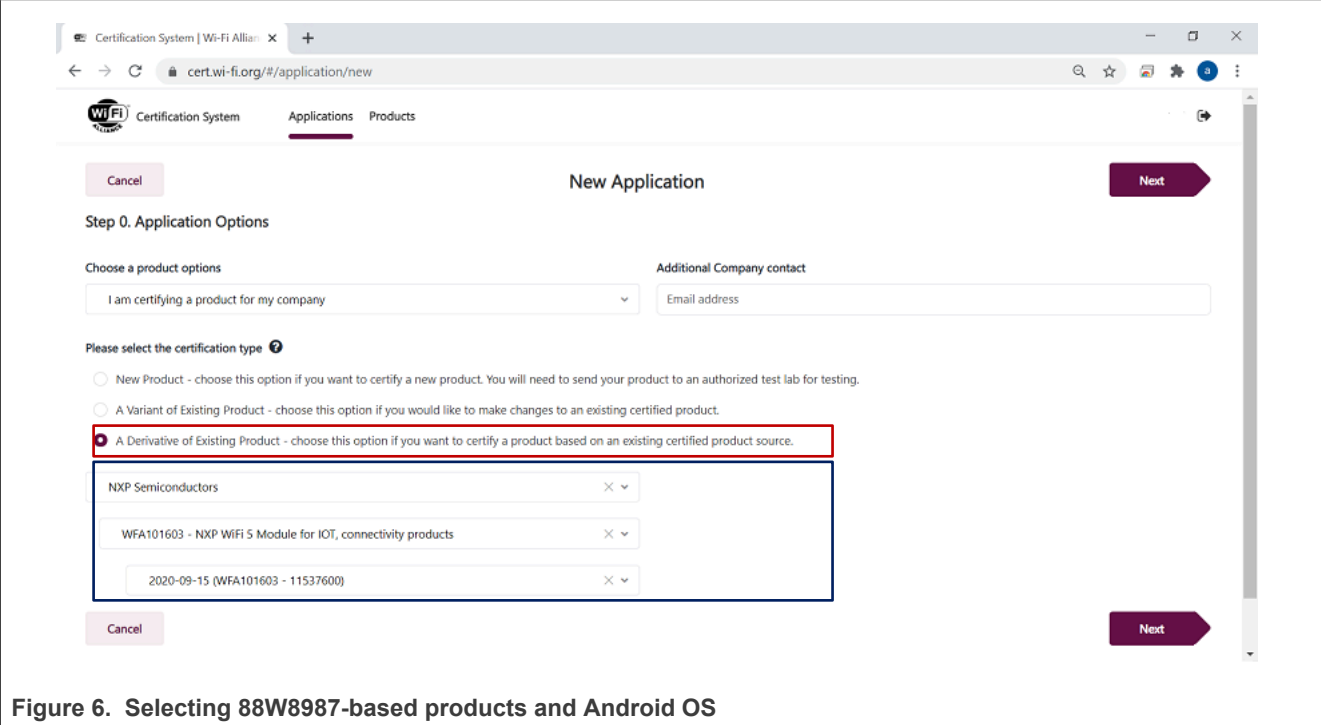Figure 6 shows the CID for 88W8987-based wireless module and Android OS.

Figure 6. Selecting 88W8987-based products and Android OS

- Click on **Next**

AN12976
Application note

All information provided in this document is subject to legal disclaimers.

Rev. 6 — 13 December 2023

© 2023 NXP B.V. All rights reserved.

9 / 17

4.2 Capture the product information

The next **New Application** page is for **Step 1. Product Information**.

Caution: Make sure to capture the exact information about your product as the Wi-Fi components cannot be modified once you have submitted the application.

- Capture the **Product Name** and **Variant Name**
- Capture the **Model Number** and **Product URL**
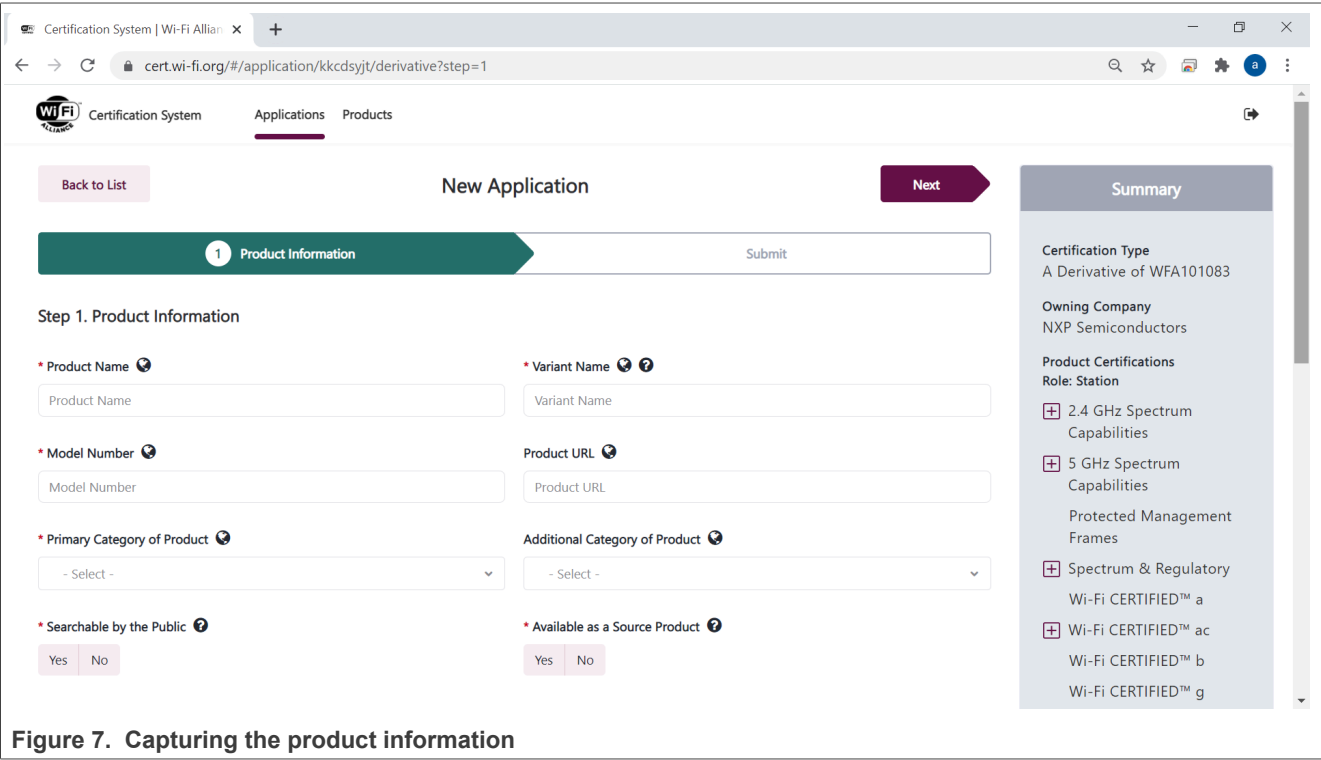- Click on the icon to view the list of **Primary Category of Product** and select the category for your product

Figure 7. Capturing the product information

- Verify the Wi-Fi component details.
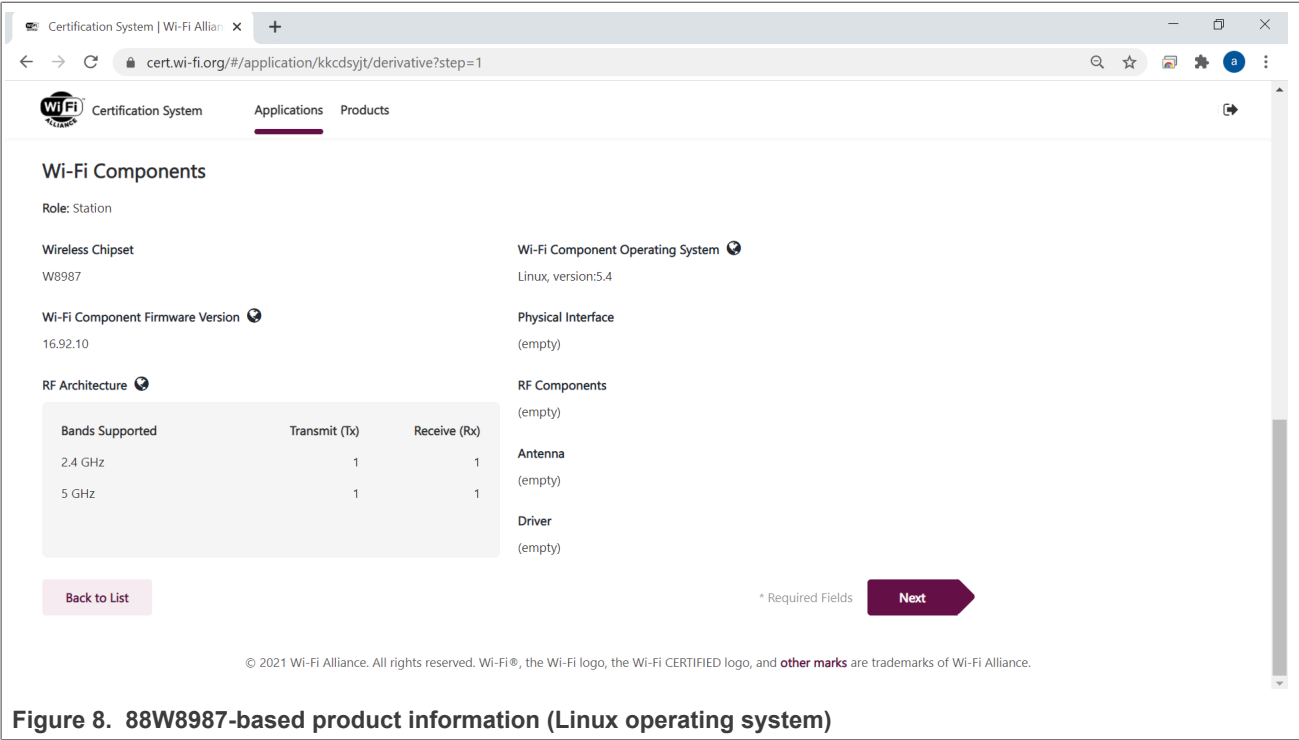 Figure 8 shows the Wi-Fi component details for a product based on 88W8987-based product and Linux OS.

AN12976

Application note

All information provided in this document is subject to legal disclaimers.

Rev. 6 — 13 December 2023

© 2023 NXP B.V. All rights reserved.

10 / 17

Figure 8. 88W8987-based product information (Linux operating system)

[Figure 9](#) shows the Wi-Fi component details for a product based on 88W8987-based product and Android OS.
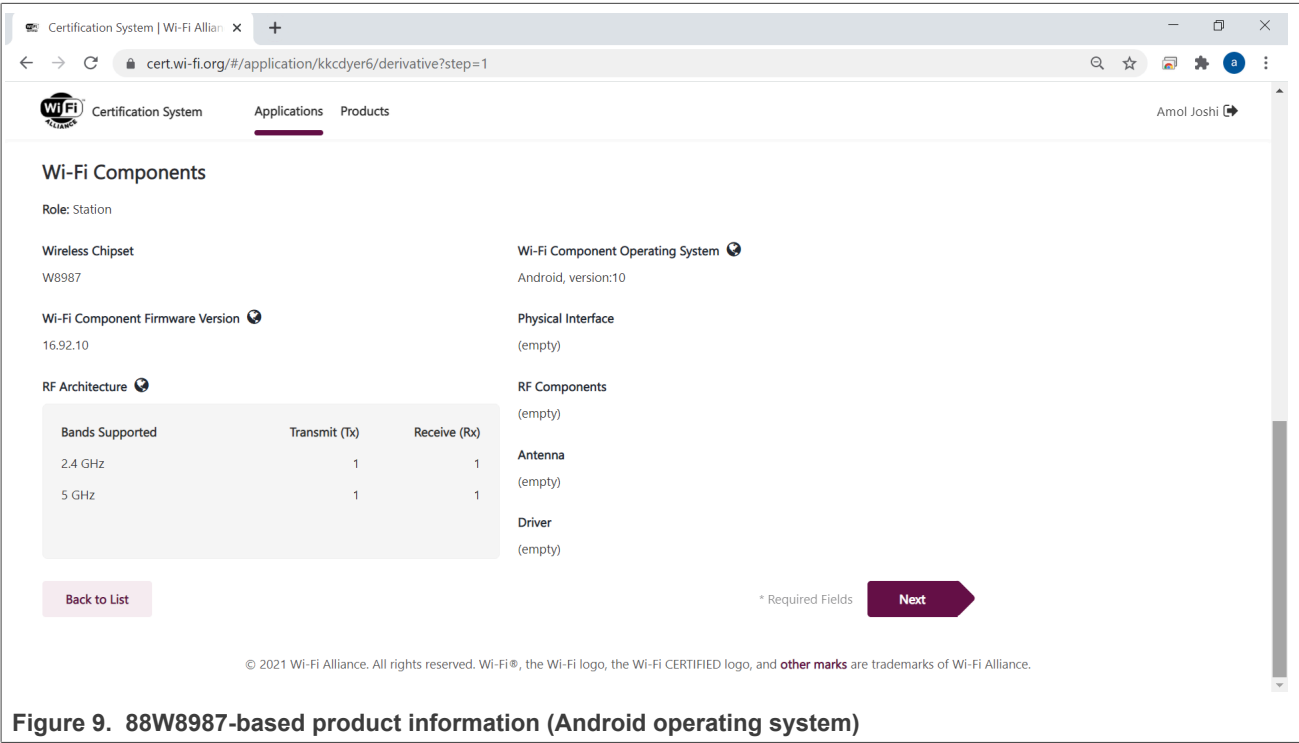

Figure 9. 88W8987-based product information (Android operating system)

- Click on **Next Step**

4.3 Submit the application

The last **New Application** page is for **Step 2. Submit**.

• Capture optional information such as the PO number and/or CTIA number
• Go to the **Wi-Fi Alliance Terms and Agreements** section on the page
• Check the two boxes to confirm you acknowledge *Wi-Fi Alliance Certification Terms and Conditions* and that you agree to the *Wi-Fi Alliance Certification Mark License Agreement*
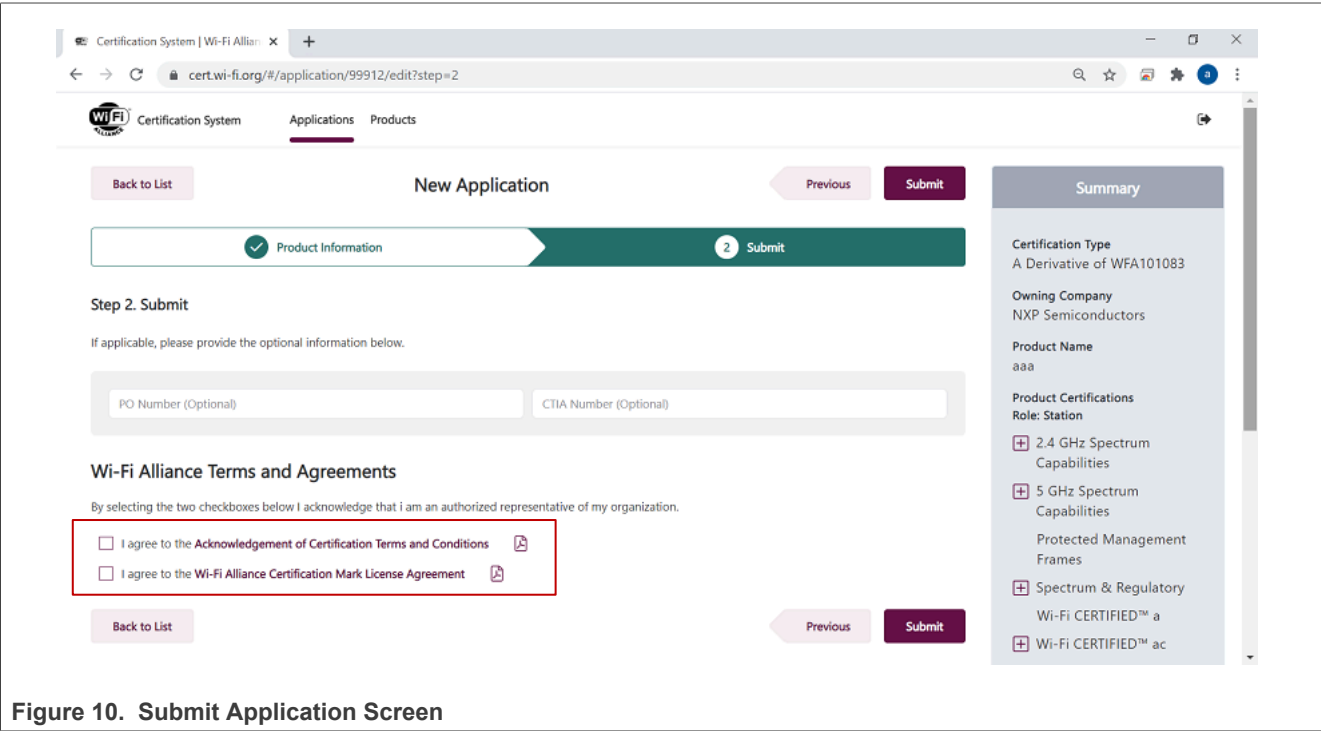• Click on **Submit**

Figure 10. Submit Application Screen

5 Obligations and outcomes for derivative certifications

- A member holding the source certification shall be informed of all approved derivative certifications.
- The member holding the source certification and the member holding the derivative certification shall both be accountable for addressing interoperability concerns.
- If interoperability concerns are found with a Derivative Certification and/or Source Certification then both certifications shall be subject to additional verification.
- If identified interoperability concern has not been resolved, the associated certifications shall be revoked.
- If information provided in the certification application(s) is found to be inaccurate, the associated certifications shall be revoked.
- If a Source Certification is revoked, all Derivative Certifications based on that Source Certification shall be revoked.
- A Member holding a Source Certification or a Derivative Certification shall be responsible for responding to Wi-Fi Alliance requests for information in support of these activities.

6 Acronyms and abbreviations

Table 2. Acronyms and abbreviations

Terms	Definition
ATL	Authorized Test Labs
CID	Certification Identification Number
CTIA	Cellular Telecommunications and Internet Association

7 Revision history

Revision history

Document ID	Date	Description
AN12976 v.6	13 December 2023	Updates in Section 2.2 "Certificate qualification": • Removed the section *88W8801 (LBWA0ZZ2DS)* • Removed the section *88W8987 (AW-CM358MA)* • Section 2.2.1 "88W9098 (LBEE5ZZ1XL)": added. • Section 2.2.2 "IW612 (LBES5PL2EL)": added.
AN12976 v.5	29 September 2022	• Added the section *88W8801 (LBWA0ZZ2DS)*
AN12976 v.4	14 December 2021	• Section *88W8987 (AW-CM358MA)*: updated • Section 4.1 "Log on and start a new application": updated the figures • Figure 10 "Submit Application Screen": updated
AN12976 v.3	29 January 2021	• Section 1 "About this document": updated • Section 4 "Step by step procedure": updated per the latest certification system from Wi-Fi Alliance
AN12976 v.2	6 November 2020	• Section 4.1 "Log on and start a new application": added the screen capture showing the CID option for 88W8987-based products and Android operating system • Section 4.2 "Capture the product information": added the screen capture showing 88W8987 product information with Android operating system
AN12976 v.1	30 September 2020	Initial version

AN12976

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Application note

Rev. 6 — 13 December 2023

14 / 17

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Figures

Contents