OPTIGA™ Trust M1

Keys and Certificates

About this document

Scope and purpose

The scope of this document is to provide the certificates to be considered while integrating the OPTIGA™ Trust M1 solution.

Intended audience

This document addresses the audience: Customers, solution providers and system integrators.

Table of Contents

About this document **1**
Table of Contents **2**
1 Abbreviations **3**
2 References **4**
3 Infineon Test Certificates **5**
3.1 PKI Hierarchy for Test Certificates 5
3.2 Infineon Test CA Certificate 6
3.3 Infineon End Device Test Certificate 7
Revision History **8**

1 Abbreviations

Table 1 Abbreviations

Abbreviation	Definition
CA	Certificate Authority
PKI	Public Key Infrastructure

2 References

None

3 Infineon Test Certificates

The Infineon test certificates include the Infineon Test CA certificate and Infineon End Device Test certificate as shown in PKI hierarchy.

Note: Engineering Samples come with Test Certificates in Security Chip and Test CA on local host platform. These are not meant to be used for final product. Please use productive samples and productive CA for final product rollout.

The Infineon End Device Certificate is in default loaded in OPTIGA™ Trust M1 security chip Engineering samples. The Infineon Test CA is to be integrated to respective Host platform to perform device authentication.

3.1 PKI Hierarchy for Test Certificates

The PKI hierarchy of the OPTIGA™ Trust M1 Test certificates is as given below.

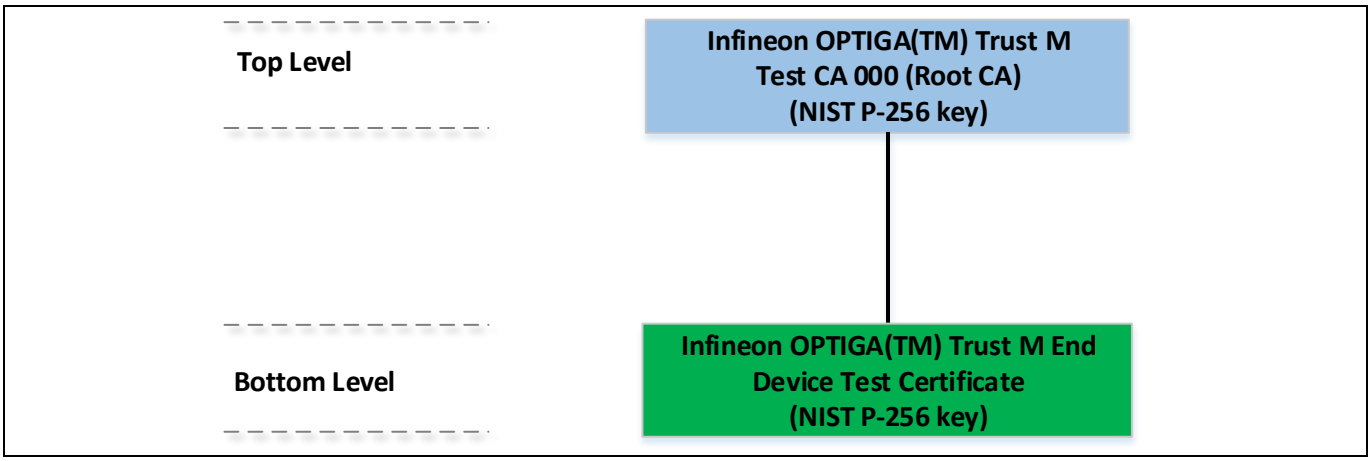

Figure 1 PKI Hierarchy – Test Certificates

3.2 Infineon Test CA Certificate

The details of the Infineon Test CA are given below.

Table 2 Infineon Test CA Certificate

Type of Data	Data in Hex
Certificate Data	30 82 02 5F 30 82 02 05 A0 03 02 01 02 02 09 00 FB E1 CA 1A 90 F5 20 64 30 0A 06 08 2A 86 48 CE 3D 04 03 02 30 77 31 0B 30 09 06 03 55 04 06 13 02 44 45 31 21 30 1F 06 03 55 04 0A 0C 18 49 6E 66 69 6E 65 6F 6E 20 54 65 63 68 6E 6F 6C 6F 67 69 65 73 20 41 47 31 13 30 11 06 03 55 04 0B 0C 0A 4F 50 54 49 47 41 28 54 4D 29 31 30 30 2E 06 03 55 04 03 0C 27 49 6E 66 69 6E 65 6F 6E 20 4F 50 54 49 47 41 28 54 4D 29 20 54 72 75 73 74 20 4D 20 54 65 73 74 20 43 41 20 30 30 30 30 1E 17 0D 31 38 30 36 31 35 31 34 32 39 35 33 5A 17 0D 34 33 30 36 30 39 31 34 32 39 35 33 5A 30 77 31 0B 30 09 06 03 55 04 06 13 02 44 45 31 21 30 1F 06 03 55 04 0A 0C 18 49 6E 66 69 6E 65 6F 6E 20 54 65 63 68 6E 6F 6C 6F 67 69 65 73 20 41 47 31 13 30 11 06 03 55 04 0B 0C 0A 4F 50 54 49 47 41 28 54 4D 29 31 30 30 2E 06 03 55 04 03 0C 27 49 6E 66 69 6E 65 6F 6E 20 4F 50 54 49 47 41 28 54 4D 29 20 54 72 75 73 74 20 4D 20 54 65 73 74 20 43 41 20 30 30 30 30 59 30 13 06 07 2A 86 48 CE 3D 02 01 06 08 2A 86 48 CE 3D 03 01 07 03 42 00 04 1B 51 FD AC 28 A5 BD 0B 39 57 41 A7 00 6E 23 64 F8 D3 C4 08 C7 5C A0 80 5E 35 F6 6E 9F 10 1F 25 8C 56 F6 21 33 D5 D9 45 2E 5F A7 70 29 EC F9 99 B3 4A 73 A5 9B 98 AA 96 F8 0A 35 37 0A 88 8E 67 A3 7A 30 78 30 12 06 03 55 1D 13 01 01 FF 04 08 30 06 01 01 FF 02 01 00 30 0B 06 03 55 1D 0F 04 04 03 02 02 04 30 1D 06 03 55 1D 0E 04 16 04 14 53 1B 46 32 F2 BA 1B EC 35 23 B0 C6 84 E2 BC 7F 11 DA A2 2E 30 1F 06 03 55 1D 23 04 18 30 16 80 14 53 1B 46 32 F2 BA 1B EC 35 23 B0 C6 84 E2 BC 7F 11 DA A2 2E 30 15 06 03 55 1D 20 04 0E 30 0C 30 0A 06 08 2A 82 14 00 44 01 14 01 30 0A 06 08 2A 86 48 CE 3D 04 03 02 03 48 00 30 45 02 20 1B B3 72 A2 3E 36 85 CF 21 A3 E2 95 4F 67 0C 44 69 45 70 D8 A8 8E 2F 76 B0 5C 0F 5F 27 F2 EB F1 02 21 00 AD F0 D3 E1 8B F2 E2 5F 45 98 48 0C B6 43 18 2F A3 8F E0 8A 6E F3 DD 2A F1 EF 7C 27 6A 44 B6 0F
SHA1 Thumbprint	b5 11 84 30 f2 94 05 b3 03 84 08 94 7b e1 ce 50 19 e1 6b de
Sign and Hash Algorithm	SHA256 ECDSA
Public Key parameters	NIST P-256
Public Key	04 1B 51 FD AC 28 A5 BD 0B 39 57 41 A7 00 6E 23 64 F8 D3 C4 08 C7 5C A0 80 5E 35 F6 6E 9F 10 1F 25 8C 56 F6 21 33 D5 D9 45 2E 5F A7 70 29 EC F9 99 B3 4A 73 A5 9B 98 AA 96 F8 0A 35 37 0A 88 8E 67

3.3 Infineon End Device Test Certificate

The details of the Infineon End Device Test certificate are given in the below.

Note: The Infineon end device certificate will be different in the OPTIGA™ Trust M1 samples if personalized for the unique keys and certificates.

Table 3 Infineon End Device Test Certificate

Certificate Field	Data in Hex
Certificate Data (In Hex)	30 82 01 DD 30 82 01 82 A0 03 02 01 02 02 03 10 00 01 30 0A 06 08 2A 86 48 CE 3D 04 03 02 30 77 31 0B 30 09 06 03 55 04 06 13 02 44 45 31 21 30 1F 06 03 55 04 0A 0C 18 49 6E 66 69 6E 65 6F 6E 20 54 65 63 68 6E 6F 6C 6F 67 69 65 73 20 41 47 31 13 30 11 06 03 55 04 0B 0C 0A 4F 50 54 49 47 41 28 54 4D 29 31 30 30 2E 06 03 55 04 03 0C 27 49 6E 66 69 6E 65 6F 6E 20 4F 50 54 49 47 41 28 54 4D 29 20 54 72 75 73 74 20 4D 20 54 65 73 74 20 43 41 20 30 30 30 30 1E 17 0D 31 38 30 39 32 34 31 34 32 39 35 33 5A 17 0D 33 38 30 39 32 34 31 34 32 39 35 33 5A 30 1C 31 1A 30 18 06 03 55 04 03 0C 11 49 6E 66 69 6E 65 6F 6E 20 49 6F 54 20 4E 6F 64 65 30 59 30 13 06 07 2A 86 48 CE 3D 02 01 06 08 2A 86 48 CE 3D 03 01 07 03 42 00 04 5D F7 36 9A 8B 47 E8 61 A6 94 5C 9D EC 18 EF 4A 6F BE 55 1C 78 23 74 A6 06 29 D4 65 9B 81 C2 5D 9F F5 1F 70 8A 4D 3F 19 36 70 C3 10 51 DD 67 12 DC F2 B6 2A 8A 70 53 92 13 95 2D 05 D2 90 38 07 A3 58 30 56 30 0C 06 03 55 1D 13 01 01 FF 04 02 30 00 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02 07 80 30 1F 06 03 55 1D 23 04 18 30 16 80 14 53 1B 46 32 F2 BA 1B EC 35 23 B0 C6 84 E2 BC 7F 11 DA A2 2E 30 15 06 03 55 1D 20 04 0E 30 0C 30 0A 06 08 2A 82 14 00 44 01 14 01 30 0A 06 08 2A 86 48 CE 3D 04 03 02 03 49 00 30 46 02 21 00 A6 BF 28 A3 EF AE 18 3A DE 0A 0B 49 32 1D A2 C2 E0 CF AF 4E D6 F2 FF 80 57 1E 4E 50 EF C3 0D 5D 02 21 00 F6 B9 E4 74 07 91 B4 2C 99 4B 45 C8 07 F3 1D BE BF 7B 54 73 3B 0E 63 E6 0C 11 0E 09 11 13 43 19
SHA1 Thumbprint	2d e9 11 cc 92 1f b3 ca 43 3a 20 3a 7a 47 4d 3b fa 93 39 45
Sign and Hash Algorithm	SHA256 ECDSA
Public Key parameters	NIST P-256
Public Key	04 5D F7 36 9A 8B 47 E8 61 A6 94 5C 9D EC 18 EF 4A 6F BE 55 1C 78 23 74 A6 06 29 D4 65 9B 81 C2 5D 9F F5 1F 70 8A 4D 3F 19 36 70 C3 10 51 DD 67 12 DC F2 B6 2A 8A 70 53 92 13 95 2D 05 D2 90 38 07

Revision History

Major changes since the last revision

Page or Reference	Description of change
All	Revision 1.0, Initial version
Page 7	Revision 1.1, Infineon test end entity certificate updated.
Page 7	Revision 1.2, Infineon test end entity certificate updated common subject name to Infineon IoT Node.
Page 5	Revision 1.30 , Note for not using test certificate for final product added.

Edition 2019-03-07

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email: erratum@infineon.com

Document reference

IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”) .

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.