OPTIGA™ Trust X1

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 X1 solution.

Intended audience

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

Table of Contents

1 Abbreviations

Table 1 Abbreviations

Abbreviation	Definition
CA	Certificate Authority
DTLS	Datagram Transport Layer Security
PKI	Public Key Infrastructure

2 References

None

3 Infineon Productive certificates

3.1 PKI hierarchy for Productive Certificates

The PKI hierarchy of the OPTIGA™ Trust X1 certificates is as given below:

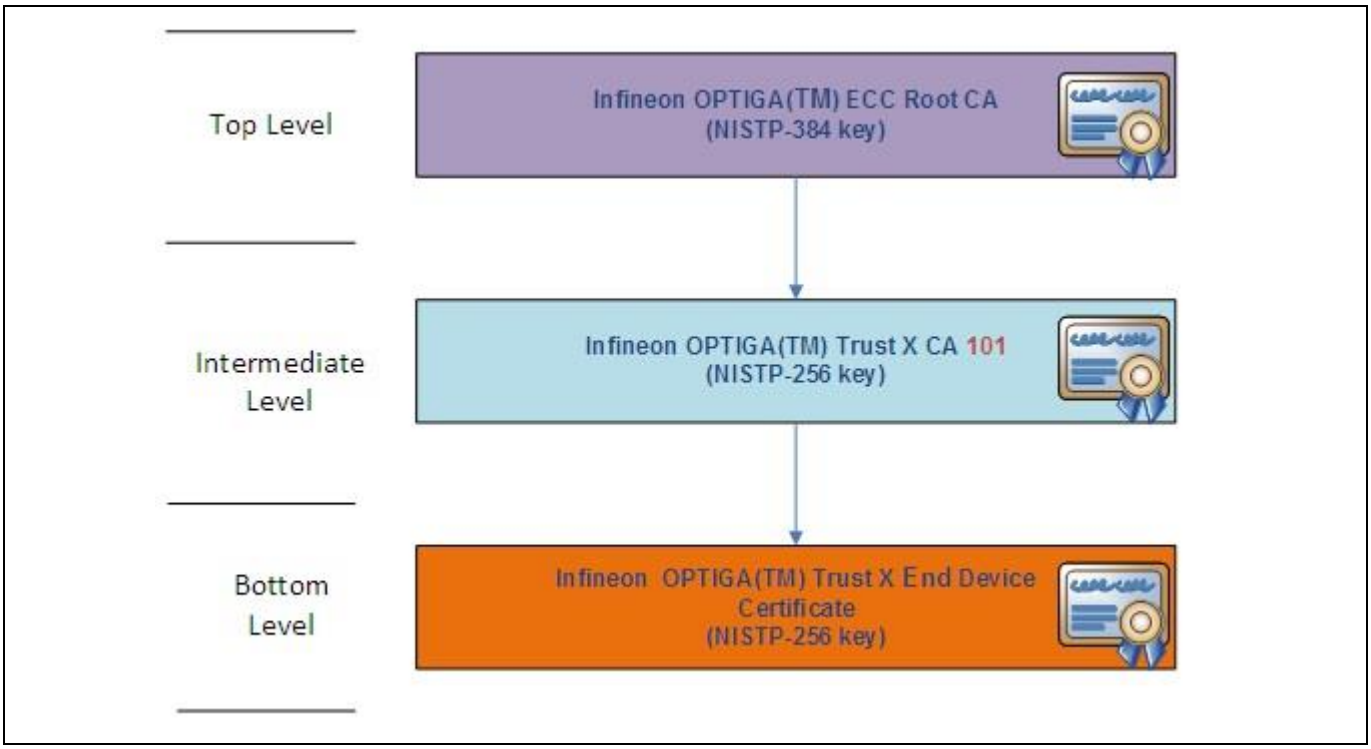

Figure 1 PKI Hierarchy

3.2 Productive CA certificate

The Infineon OPTIGA(TM) Trust X CA is of intermediate level which is issued by Infineon OPTIGA(TM) ECC Root CA.

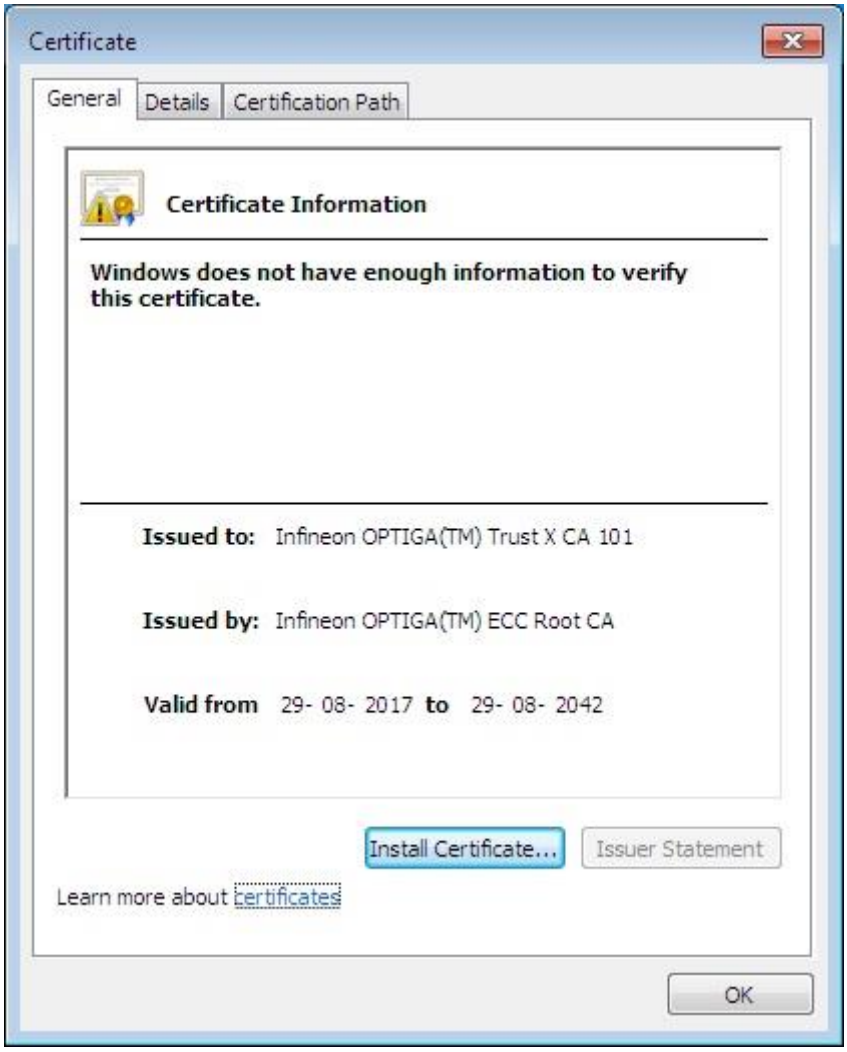

Figure 2 Infineon intermediate CA details

The details of the OPTIGA(TM) Trust X CA intermediate CA certificate are given below:

Table 2 Infineon Intermediate CA certificate

Type of Data	Data in Hex
Certificate Data	30 82 02 78 30 82 01 FE A0 03 02 01 02 02 04 6A DB DD D6 30 0A 06 08 2A 86 48 CE 3D 04 03 03 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 1B 30 19 06 03 55 04 0B 0C 12 4F 50 54 49 47 41 28 54 4D 29 20 44 65 76 69 63 65 73 31 28 30 26 06 03 55 04 03 0C 1F 49 6E 66 69 6E 65 6F 6E 20 4F 50 54 49 47 41 28 54 4D 29 20 45 43 43 20 52 6F 6F 74 20 43 41 30 1E 17 0D 31 37 30 38 32 39 31 36 32 37 30 38 5A 17 0D 34 32 30 38 32 39 31 36 32 37 30 38 5A 30 72 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 2B 30 29 06 03 55 04 03 0C 22 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 58 20 43 41 20 31 30 31 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 60 D7 9D 39 60 FB 10 D4 28 89 09 56 4F FD A8 47 E2 22 FD 8D 3A 24 07 7B 38 0D C3 70 4E 37 42 08 1B 33 C6 EC 47 D0 A8 FB CF AD 3F DC 7C 6E CD 94 7A 4C 1E 90 63 D0 7F E4 20 A7 AB 14 D5 92 B6 C0 A3 7D 30 7B 30 1D 06 03 55 1D 0E 04 16 04 14 CA 05 33 D7 4F C4 7F 09 49 FB DB 12 25 DF D7 97 9D 41 1E 15 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02 00 04 30 12 06 03 55 1D 13 01 01 FF 04 08 30 06 01 01 FF 02 01 00 30 15 06 03 55 1D 20 04 0E 30 0C 30 0A 06 08 2A 82 14 00 44 01 14 01 30 1F 06 03 55 1D 23 04 18 30 16 80 14 B4 18 85 C8 4A 4A C5 12 7A F2 40 39 DE C4 F5 8B 1E 7E 4A D1 30 0A 06 08 2A 86 48 CE 3D 04 03 03 03 68 00 30 65 02 31 00 D2 21 49 C3 46 70 4B 16 85 9E F2 92 6D 0C D2 B8 74 4F DD 12 61 78 45 9B 54 31 D2 9D 50 4A DD 5C FE F7 54 12 B8 03 C2 11 21 95 53 FC 30 39 00 D6 02 30 13 62 98 1F E7 64 4C 89 EF F0 E7 83 EB 71 5C A1 AE 47 F7 E7 FB 7E 70 A8 DF 28 04 14 42 47 66 70 62 22 1D BF F3 E6 B3 5E 23 CB 29 32 DE EA B5 8E
SHA1 Thumbprint	51 c7 c9 24 b2 b3 b8 2b e8 71 b9 2b b0 95 03 fb de 39 36 95
Sign and Hash Algorithm	SHA384 ECDSA
Public Key parameters	NIST P-256
Public Key	04 60 D7 9D 39 60 FB 10 D4 28 89 09 56 4F FD A8 47 E2 22 FD 8D 3A 24 07 7B 38 0D C3 70 4E 37 42 08 1B 33 C6 EC 47 D0 A8 FB CF AD 3F DC 7C 6E CD 94 7A 4C 1E 90 63 D0 7F E4 20 A7 AB 14 D5 92 B6 C0

4 Infineon Test Certificates

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

The Infineon End Device Certificate is in default loaded in OPTIGA™ Trust X1 security chip Engineering samples. The Infineon Test CA is to be integrated to respective Host platform to perform device authentication.

4.1 PKI Hierarchy for Test Certificates

The PKI hierarchy of the OPTIGA™ Trust X1 Test ceritificates is as given below.

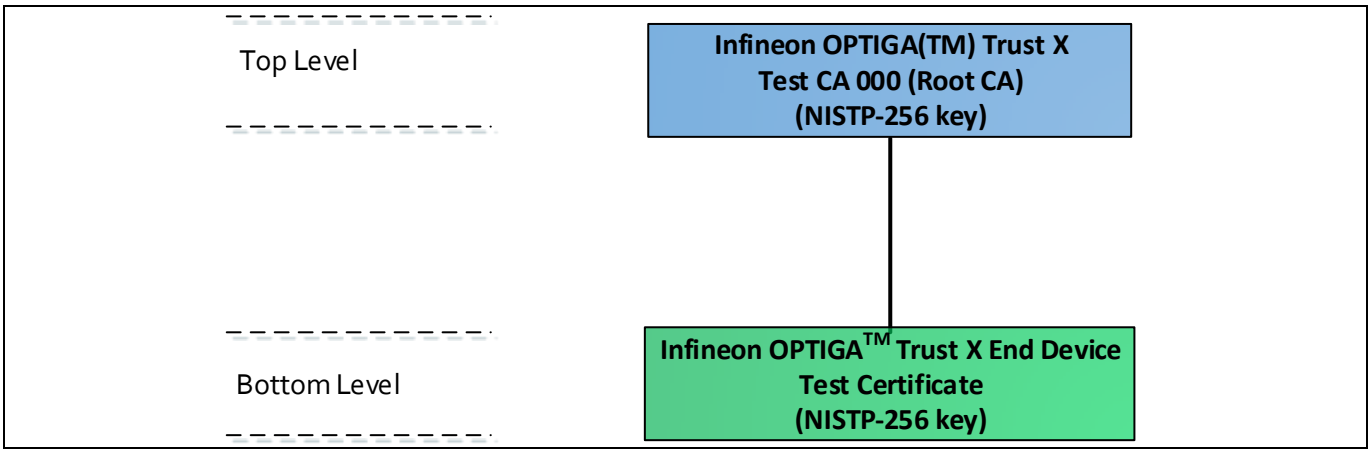

Figure 3 PKI Hierarchy – Test Certificates

4.2 Infineon Test CA Certificate

The details of the Infineon Test CA are given below.

Table 3 Infineon Test CA Certificate

Type of Data	Data in Hex
Certificate Data	30 82 02 62 30 82 02 08 A0 03 02 01 02 02 09 00 C6 40 14 6A 1D DA FE 46 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 58 20 54 65 73 74 20 43 41 20 30 30 30 30 1E 17 0D 31 36 30 35 31 30 32 30 31 38 33 30 5A 17 0D 34 31 30 35 30 34 32 30 31 38 33 30 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 58 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 94 89 2F 09 EA 4E CA BC 6A 4E F2 06 36 26 E0 5D E0 D5 F9 77 EA C3 B2 70 AC E2 19 00 F5 DB 56 E7 37 BB BE 46 E4 49 76 38 25 B5 F8 94 74 9E 1A B6 5A F1 29 D7 3A B6 9B 80 AC C5 E1 C3 10 F2 16 C6 A3 7D 30 7B 30 1D 06 03 55 1D 0E 04 16 04 14 42 E3 5D 56 E5 6C 8E 8D 02 71 8C 9E F2 33 C9 47 3B 82 53 6C 30 1F 06 03 55 1D 23 04 18 30 16 80 14 42 E3 5D 56 E5 6C 8E 8D 02 71 8C 9E F2 33 C9 47 3B 82 53 6C 30 12 06 03 55 1D 13 01 01 FF 04 08 30 06 01 01 FF 02 01 00 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02 02 04 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 21 00 F5 F3 2B 5B 93 09 92 90 2C A4 5F 74 56 C1 24 BB 2B 9C E4 4F C7 F0 F1 6C 3F 5F 81 53 9F 09 77 98 02 20 51 B0 82 77 85 06 77 DE EF 3D 49 21 B7 92 1D 87 B5 C2 92 6D 91 07 9D 02 EA 63 1C A8 E9 91 25 A6
SHA1 Thumbprint	6A 00 75 D0 AB B7 F2 A1 95 39 1F 42 E8 5F EA 31 E2 B0 4A 07
Sign and Hash Algorithm	SHA256 ECDSA
Public Key parameters	NIST P-256
Public Key	04 94 89 2F 09 EA 4E CA BC 6A 4E F2 06 36 26 E0 5D E0 D5 F9 77 EA C3 B2 70 AC E2 19 00 F5 DB 56 E7 37 BB BE 46 E4 49 76 38 25 B5 F8 94 74 9E 1A B6 5A F1 29 D7 3A B6 9B 80 AC C5 E1 C3 10 F2 16 C6

4.3 Infineon End Device Test Certificate

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

Table 4 Infineon End Device Test Certificate

Certificate Field	Data in Hex
Certificate Data (In Hex)	30 82 01 C0 30 82 01 67 A0 03 02 01 02 02 04 01 02 03 0A 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 58 20 54 65 73 74 20 43 41 20 30 30 30 30 1E 17 0D 31 36 30 35 31 30 32 30 31 39 30 31 5A 17 0D 33 36 30 35 30 35 32 30 31 39 30 31 5A 30 00 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 A0 28 0E 73 9F 32 7A 8E 81 3B 5A 15 45 56 64 97 43 DC 22 A6 03 63 84 6D 08 72 DD BD 38 8B 7C C2 AA 62 25 13 0F 0F 0F D5 73 D6 5B FE 07 66 77 0F A3 A9 C6 31 5D 80 D3 76 14 32 15 67 6B 6C 18 61 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 15 06 03 55 1D 20 04 0E 30 0C 30 0A 06 08 2A 82 14 00 44 01 14 01 30 1F 06 03 55 1D 23 04 18 30 16 80 14 42 E3 5D 56 E5 6C 8E 8D 02 71 8C 9E F2 33 C9 47 3B 82 53 6C 30 0A 06 08 2A 86 48 CE 3D 04 03 02 03 47 00 30 44 02 20 1D 9C 64 5D ED AF C8 3B 16 58 A6 F1 D1 81 C4 52 52 CD 43 C0 2A 4D 70 A7 B1 17 64 24 84 0F 39 95 02 20 43 12 B7 B0 1D 61 28 2B 2F 6F 63 40 ED B0 B0 D0 81 31 50 6B A4 72 F3 A9 09 7C 2D E3 28 FA 6D 99
SHA1 Thumbprint	9F EF 52 20 7C C8 C1 D9 F3 F9 C6 22 9A 49 A2 5D AF 3D 89 B6
Sign and Hash Algorithm	SHA256 ECDSA
Public Key parameters	NIST P-256
Public Key	04 A0 28 0E 73 9F 32 7A 8E 81 3B 5A 15 45 56 64 97 43 DC 22 A6 03 63 84 6D 08 72 DD BD 38 8B 7C C2 AA 62 25 13 0F 0F 0F D5 73 D6 5B FE 07 66 77 0F A3 A9 C6 31 5D 80 D3 76 14 32 15 67 6B 6C 18 61

5 Infineon Test Server Certificates

The Infineon test server certificates are intended to use for the demonstration of the Mutual Authentication (DTLS Client) and Encrypted Communication (OPTIGA™ Trust X1 and Server) use cases. The PKI hierarchy of the test server certificates is as shown below.

5.1 PKI Hierarchy for Test Server Certificates

The PKI hierarchy of the OPTIGA™ Trust X1 Test server ceritificates is as given below.

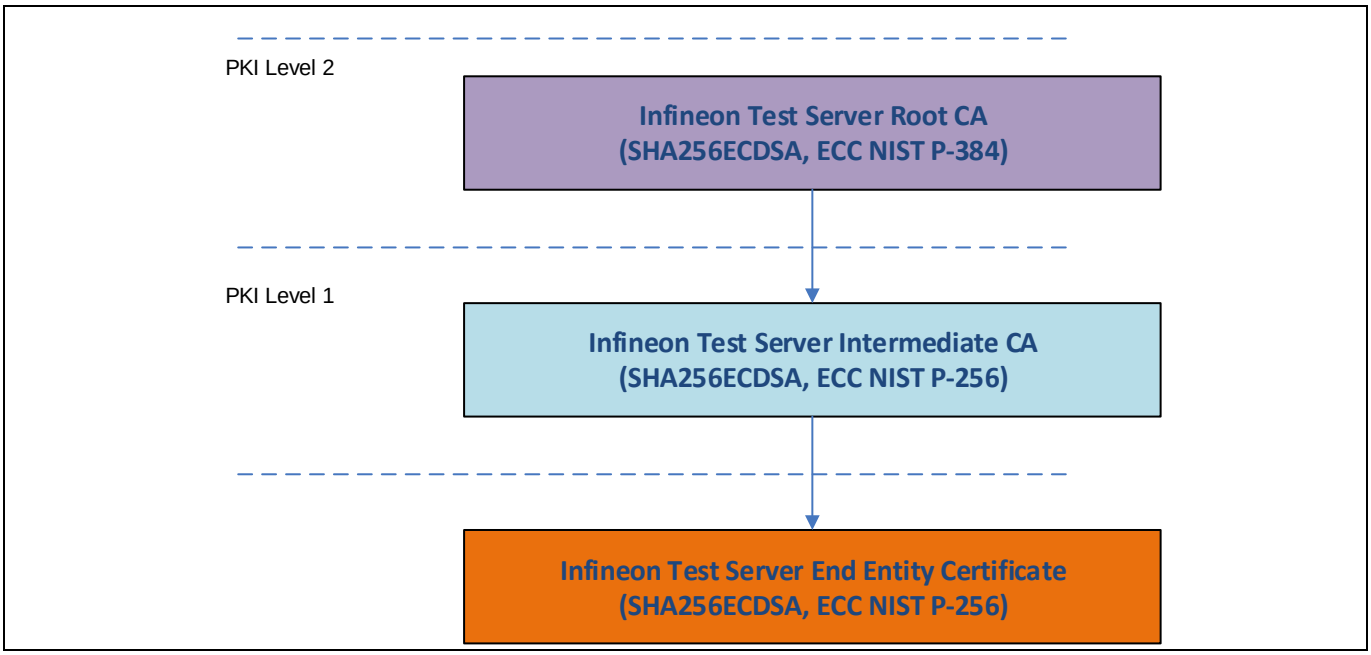

Figure 4 PKI Hierarchy – Test Server Certificates

The Infineon Test Server Root CA certificate (Trust Anchor) is in default loaded in OPTIGA™ Trust X1 security chip samples unless requested to load a different certificate(Customer specific) during the production.

5.2 Infineon Test Server Root CA Certificate

The details of the Infineon Test Server Root CA certificate are given below.

Table 5 Infineon Test Server Root CA Certificate

Type of Data	Data in Hex
Certificate Data	30 82 02 7E 30 82 02 05 A0 03 02 01 02 02 09 00 9B 0C 24 B4 5E 7D E3 73 30 0A 06 08 2A 86 48 CE 3D 04 03 02 30 74 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 1B 30 19 06 03 55 04 0B 0C 12 4F 50 54 49 47 41 28 54 4D 29 20 54 72 75 73 74 20 58 31 25 30 23 06 03 55 04 03 0C 1C 49 6E 66 69 6E 65 6F 6E 20 54 65 73 74 20 53 65 72 76 65 72 20 52 6F 6F 74 20 43 41 30 1E 17 0D 31 36 31 30 31 34 30 33 35 38 33 36 5A 17 0D 34 31 31 30 30 38 30 33 35 38 33 36 5A 30 74 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 1B 30 19 06 03 55 04 0B 0C 12 4F 50 54 49 47 41 28 54 4D 29 20 54 72 75 73 74 20 58 31 25 30 23 06 03 55 04 03 0C 1C 49 6E 66 69 6E 65 6F 6E 20 54 65 73 74 20 53 65 72 76 65 72 20 52 6F 6F 74 20 43 41 30 76 30 10 06 07 2A 86 48 CE 3D 02 01 06 05 2B 81 04 00 22 03 62 00 04 7B 2E E6 FB BD 6F 40 0F 41 9F E5 F0 8C 97 21 B0 07 B5 BB D2 B8 5A 14 3B 75 54 7E EA FE F2 8D 5A B8 54 E0 C8 AD ED F1 D5 8B 97 BA 02 3E D9 25 E0 00 86 17 35 E6 E6 D9 12 0F 8A 21 1C 62 FA CE F6 9E B1 F8 8C A3 DC 52 04 83 EB A0 B3 FA B0 CA 02 30 B1 FE 53 4E AD FB E0 88 05 86 4E 5E 67 EB 7B A3 63 30 61 30 1D 06 03 55 1D 0E 04 16 04 14 91 4A 4B 07 58 B2 C6 4B 37 FD 91 62 D8 8A 17 28 AA 94 18 62 30 1F 06 03 55 1D 23 04 18 30 16 80 14 91 4A 4B 07 58 B2 C6 4B 37 FD 91 62 D8 8A 17 28 AA 94 18 62 30 0F 06 03 55 1D 13 01 01 FF 04 05 30 03 01 01 FF 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02 02 04 30 0A 06 08 2A 86 48 CE 3D 04 03 02 03 67 00 30 64 02 30 20 1C 7A 21 50 50 C9 15 1C C5 14 8D 46 5C A6 D3 81 CE 57 06 1A AE 39 10 27 51 42 EF CD 64 75 99 DE 0D 3D 01 47 69 FC 93 6D 99 C7 F0 F8 8C AA D1 02 30 68 C3 27 D9 0F 52 AD 3A A8 DB F8 53 11 1D F1 30 6B 39 F3 3F EF 65 61 BE C4 DD 19 11 1E 83 F9 E8 3F 41 97 45 FC 61 E0 06 D0 E6 F7 5C 9F E2 57 C2
SHA1 Thumbprint	23 C1 8D CC 67 00 56 2D F3 DB 73 3A B4 13 22 92 DB 3D E6 C1
Sign and Hash Algorithm	SHA256 ECDSA
Public Key parameters	NIST P-384
Public Key	04 7B 2E E6 FB BD 6F 40 0F 41 9F E5 F0 8C 97 21 B0 07 B5 BB D2 B8 5A 14 3B 75 54 7E EA FE F2 8D 5A B8 54 E0 C8 AD ED F1 D5 8B 97 BA 02 3E D9 25 E0 00 86 17 35 E6 E6 D9 12 0F 8A 21 1C 62 FA CE F6 9E B1 F8 8C A3 DC 52 04 83 EB A0 B3 FA B0 CA 02 30 B1 FE 53 4E AD FB E0 88 05 86 4E 5E 67 EB 7B

5.3 Infineon Test Server Intermediate CA Certificate

The details of the Infineon Test Server Intermediate CA certificate are given in the below.

Table 6 Infineon Test Server Intermediate CA Certificate

Certificate Field	Data in Hex
Certificate Data (In Hex)	30 82 02 1A 30 82 01 9F A0 03 02 01 02 02 05 00 D6 D3 16 52 30 0A 06 08 2A 86 48 CE 3D 04 03 02 30 74 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 1B 30 19 06 03 55 04 0B 0C 12 4F 50 54 49 47 41 28 54 4D 29 20 54 72 75 73 74 20 58 31 25 30 23 06 03 55 04 03 0C 1C 49 6E 66 69 6E 65 6F 6E 20 54 65 73 74 20 53 65 72 76 65 72 20 52 6F 6F 74 20 43 41 30 1E 17 0D 31 36 31 30 31 34 30 38 31 30 32 30 5A 17 0D 33 31 31 30 31 31 30 38 31 30 32 30 5A 30 2F 31 2D 30 2B 06 03 55 04 03 0C 24 49 6E 66 69 6E 65 6F 6E 20 54 65 73 74 20 53 65 72 76 65 72 20 49 6E 74 65 72 6D 65 64 69 61 74 65 20 43 41 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 EE F4 63 2E 96 1C 43 FA AB F8 61 61 9E BE 86 0E F8 12 08 47 30 5B 81 83 BF 6D 2D 71 92 F4 C9 B6 EB F9 95 18 E1 01 37 D6 60 CE C5 40 CB C8 68 93 81 5A B8 B5 27 21 47 DD DB 13 56 A9 2A 44 82 48 A3 63 30 61 30 1D 06 03 55 1D 0E 04 16 04 14 D4 3F AA DD 49 BF A4 2B CF 7C D5 21 D3 9E 91 37 8F BB E3 09 30 1F 06 03 55 1D 23 04 18 30 16 80 14 91 4A 4B 07 58 B2 C6 4B 37 FD 91 62 D8 8A 17 28 AA 94 18 62 30 0F 06 03 55 1D 13 01 01 FF 04 05 30 03 01 01 FF 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02 02 04 30 0A 06 08 2A 86 48 CE 3D 04 03 02 03 69 00 30 66 02 31 00 EE 82 01 8F 95 12 D3 A2 8B B5 EB 7A BC C7 12 23 DD 86 56 DA 22 23 AD 6E 4B 70 8D 44 A9 21 4E 3F 45 24 F6 36 3C 75 D0 2D 44 29 64 C6 54 70 2C 57 02 31 00 FC 57 40 DB 83 33 19 42 3F 63 39 10 F1 22 6C D7 6E A2 79 FD 09 F9 9D 6C 46 4F 78 9E 82 08 1F 0B 10 CE 38 73 52 20 71 82 50 91 78 E0 21 ED 5D 70
SHA1 Thumbprint	8E 2C 70 EC 7C 32 EA 58 A7 BB D7 7A 6C 7C FA EF 14 08 05 09
Sign and Hash Algorithm	SHA256 ECDSA
Public Key parameters	NIST P-256
Public Key	04 EE F4 63 2E 96 1C 43 FA AB F8 61 61 9E BE 86 0E F8 12 08 47 30 5B 81 83 BF 6D 2D 71 92 F4 C9 B6 EB F9 95 18 E1 01 37 D6 60 CE C5 40 CB C8 68 93 81 5A B8 B5 27 21 47 DD DB 13 56 A9 2A 44 82 48

5.4 Infineon Test Server End Entity Certificate

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

Table 7 Infineon Test Server End Entity Certificate

Certificate Field	Data in Hex
Certificate Data (In Hex)	30 82 02 3A 30 82 01 E0 A0 03 02 01 02 02 04 17 5F EE 8F 30 0A 06 08 2A 86 48 CE 3D 04 03 02 30 2F 31 2D 30 2B 06 03 55 04 03 0C 24 49 6E 66 69 6E 65 6F 6E 20 54 65 73 74 20 53 65 72 76 65 72 20 49 6E 74 65 72 6D 65 64 69 61 74 65 20 43 41 30 1E 17 0D 31 36 31 30 31 34 30 38 31 33 31 37 5A 17 0D 32 34 31 30 31 32 30 38 31 33 31 37 5A 30 36 31 34 30 32 06 03 55 04 03 0C 2B 49 6E 66 69 6E 65 6F 6E 20 54 65 73 74 20 53 65 72 76 65 72 20 45 6E 64 20 45 6E 74 69 74 79 20 43 65 72 74 69 66 69 63 61 74 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 BA 0D FE 24 CC AC F8 CD 35 25 F3 67 83 18 7B 5A C2 1A C6 36 49 01 68 38 4E A1 7C 3C 0C CF C8 A8 D1 92 96 B8 55 BB 74 26 CB C0 66 A8 5C C4 63 13 0A EB B2 D3 F1 44 DD 41 AF 55 16 08 2A 59 CA E4 A3 81 E2 30 81 DF 30 09 06 03 55 1D 13 04 02 30 00 30 1D 06 03 55 1D 0E 04 16 04 14 FF A3 62 68 A0 6F 99 81 7B DE 43 EC 66 15 33 16 48 CB 23 30 30 81 A2 06 03 55 1D 23 04 81 9A 30 81 97 80 14 D4 3F AA DD 49 BF A4 2B CF 7C D5 21 D3 9E 91 37 8F BB E3 09 A1 78 A4 76 30 74 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 1B 30 19 06 03 55 04 0B 0C 12 4F 50 54 49 47 41 28 54 4D 29 20 54 72 75 73 74 20 58 31 25 30 23 06 03 55 04 03 0C 1C 49 6E 66 69 6E 65 6F 6E 20 54 65 73 74 20 53 65 72 76 65 72 20 52 6F 6F 74 20 43 41 82 05 00 D6 D3 16 52 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02 07 80 30 0A 06 08 2A 86 48 CE 3D 04 03 02 03 48 00 30 45 02 20 0B 9A 86 02 21 44 CD 7D E5 19 CB 40 85 4E 90 91 4C 22 D9 CE 0A 94 D8 95 A8 24 55 43 0E BB 24 9C 02 21 00 F5 91 1A 3D B1 64 06 4E 22 0C F3 32 84 C9 92 3F 6F 58 FD FD EE E9 58 0B FE FC 54 58 8F 2E 0B BC
SHA1 Thumbprint	ED 97 A3 62 81 0B AB 80 7B AF 11 C8 35 3F 1F B2 17 9A 0B E4
Sign and Hash Algorithm	SHA256 ECDSA
Public Key parameters	NIST P-256
Public Key	04 BA 0D FE 24 CC AC F8 CD 35 25 F3 67 83 18 7B 5A C2 1A C6 36 49 01 68 38 4E A1 7C 3C 0C CF C8 A8 D1 92 96 B8 55 BB 74 26 CB C0 66 A8 5C C4 63 13 0A EB B2 D3 F1 44 DD 41 AF 55 16 08 2A 59 CA E4

The private key of the corresponding public key for above mentioned certificate is given below.

29 0A 43 99 C3 61 51 AA 4F FA 5E C1 95 DB B8 CE
EE 77 95 5A F6 52 7A 29 3E 56 B6 77 38 B8 E3 FE

Revision History

Major changes since the last revision

Page or Reference	Description of change
All	Revision 1.0, Initial version
Section 3.1	Revision 1.1, Updated the PKI Hierarchy for Test certificates
Section 3	Revision 1.2, Added productive certificate details

Edition 2017-10-06

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.