# OPTIGA™ Trust M

## Product Version: V1

## 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 M 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
**4 Infineon Productive certificates** ..... **8**
4.1 PKI hierarchy for Productive Certificates ..... 8
4.2 Productive CA certificate ..... 9
**Revision History** ..... **11**

# 1 Abbreviations

**Table 1 Abbreviations**

| Abbreviation | Definition |
|---|---|
| CA | Certificate Authority |
| PKI | Public Key Infrastructure |
| NIST | National Institute of Standards and Technology |

# 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 M 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 M Test certificates is as given below.

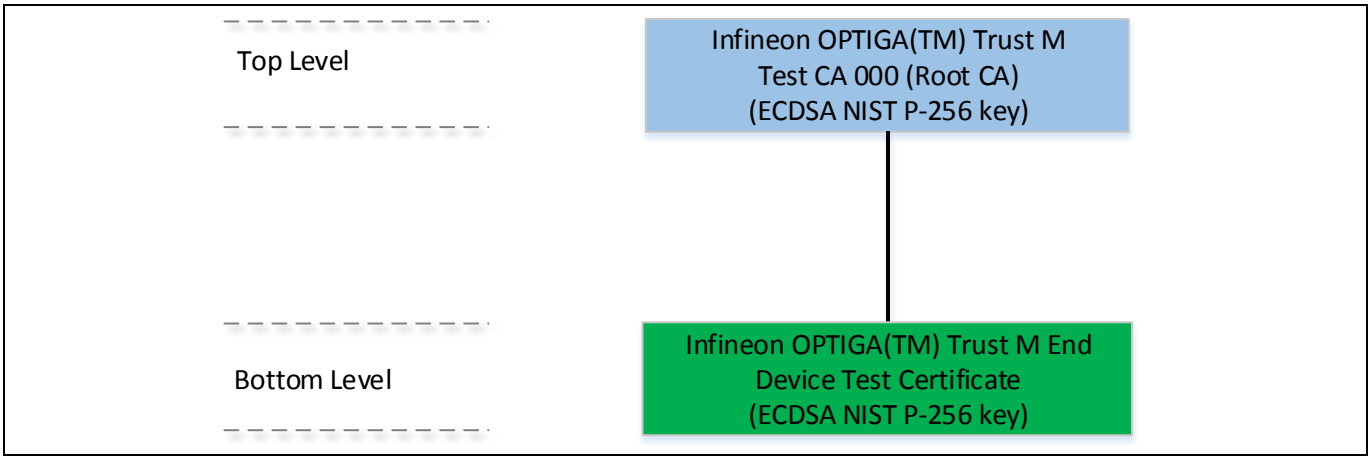


**Figure 1 PKI Hierarchy – Test Certificates**

## 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<br>FB E1 CA 1A 90 F5 20 64 30 0A 06 08 2A 86 48 CE<br>3D 04 03 02 30 77 31 0B 30 09 06 03 55 04 06 13<br>02 44 45 31 21 30 1F 06 03 55 04 0A 0C 18 49 6E<br>66 69 6E 65 6F 6E 20 54 65 63 68 6E 6F 6C 6F 67<br>69 65 73 20 41 47 31 13 30 11 06 03 55 04 0B 0C<br>0A 4F 50 54 49 47 41 28 54 4D 29 31 30 30 2E 06<br>03 55 04 03 0C 27 49 6E 66 69 6E 65 6F 6E 20 4F<br>50 54 49 47 41 28 54 4D 29 20 54 72 75 73 74 20<br>4D 20 54 65 73 74 20 43 41 20 30 30 30 30 1E 17<br>0D 31 38 30 36 31 35 31 34 32 39 35 33 5A 17 0D<br>34 33 30 36 30 39 31 34 32 39 35 33 5A 30 77 31<br>0B 30 09 06 03 55 04 06 13 02 44 45 31 21 30 1F<br>06 03 55 04 0A 0C 18 49 6E 66 69 6E 65 6F 6E 20<br>54 65 63 68 6E 6F 6C 6F 67 69 65 73 20 41 47 31<br>13 30 11 06 03 55 04 0B 0C 0A 4F 50 54 49 47 41<br>28 54 4D 29 31 30 30 2E 06 03 55 04 03 0C 27 49<br>6E 66 69 6E 65 6F 6E 20 4F 50 54 49 47 41 28 54<br>4D 29 20 54 72 75 73 74 20 4D 20 54 65 73 74 20<br>43 41 20 30 30 30 30 59 30 13 06 07 2A 86 48 CE<br>3D 02 01 06 08 2A 86 48 CE 3D 03 01 07 03 42 00<br>04 1B 51 FD AC 28 A5 BD 0B 39 57 41 A7 00 6E 23<br>64 F8 D3 C4 08 C7 5C A0 80 5E 35 F6 6E 9F 10 1F<br>25 8C 56 F6 21 33 D5 D9 45 2E 5F A7 70 29 EC F9<br>99 B3 4A 73 A5 9B 98 AA 96 F8 0A 35 37 0A 88 8E<br>67 A3 7A 30 78 30 12 06 03 55 1D 13 01 01 FF 04<br>08 30 06 01 01 FF 02 01 00 30 0B 06 03 55 1D 0F<br>04 04 03 02 02 04 30 1D 06 03 55 1D 0E 04 16 04<br>14 53 1B 46 32 F2 BA 1B EC 35 23 B0 C6 84 E2 BC<br>7F 11 DA A2 2E 30 1F 06 03 55 1D 23 04 18 30 16<br>80 14 53 1B 46 32 F2 BA 1B EC 35 23 B0 C6 84 E2<br>BC 7F 11 DA A2 2E 30 15 06 03 55 1D 20 04 0E 30<br>0C 30 0A 06 08 2A 82 14 00 44 01 14 01 30 0A 06<br>08 2A 86 48 CE 3D 04 03 02 03 48 00 30 45 02 20<br>1B B3 72 A2 3E 36 85 CF 21 A3 E2 95 4F 67 0C 44<br>69 45 70 D8 A8 8E 2F 76 B0 5C 0F 5F 27 F2 EB F1<br>02 21 00 AD F0 D3 E1 8B F2 E2 5F 45 98 48 0C B6<br>43 18 2F A3 8F E0 8A 6E F3 DD 2A F1 EF 7C 27 6A<br>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 | ECDSA NIST P-256 |
| Public Key | 04<br>1B 51 FD AC 28 A5 BD 0B 39 57 41 A7 00 6E 23 64<br>F8 D3 C4 08 C7 5C A0 80 5E 35 F6 6E 9F 10 1F 25<br>8C 56 F6 21 33 D5 D9 45 2E 5F A7 70 29 EC F9 99<br>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 M 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<br>00 01 30 0A 06 08 2A 86 48 CE 3D 04 03 02 30 77<br>31 0B 30 09 06 03 55 04 06 13 02 44 45 31 21 30<br>1F 06 03 55 04 0A 0C 18 49 6E 66 69 6E 65 6F 6E<br>20 54 65 63 68 6E 6F 6C 6F 67 69 65 73 20 41 47<br>31 13 30 11 06 03 55 04 0B 0C 0A 4F 50 54 49 47<br>41 28 54 4D 29 31 30 30 2E 06 03 55 04 03 0C 27<br>49 6E 66 69 6E 65 6F 6E 20 4F 50 54 49 47 41 28<br>54 4D 29 20 54 72 75 73 74 20 4D 20 54 65 73 74<br>20 43 41 20 30 30 30 30 1E 17 0D 31 38 30 39 32<br>34 31 34 32 39 35 33 5A 17 0D 33 38 30 39 32 34<br>31 34 32 39 35 33 5A 30 1C 31 1A 30 18 06 03 55<br>04 03 0C 11 49 6E 66 69 6E 65 6F 6E 20 49 6F 54<br>20 4E 6F 64 65 30 59 30 13 06 07 2A 86 48 CE 3D<br>02 01 06 08 2A 86 48 CE 3D 03 01 07 03 42 00 04<br>5D F7 36 9A 8B 47 E8 61 A6 94 5C 9D EC 18 EF 4A<br>6F BE 55 1C 78 23 74 A6 06 29 D4 65 9B 81 C2 5D<br>9F F5 1F 70 8A 4D 3F 19 36 70 C3 10 51 DD 67 12<br>DC F2 B6 2A 8A 70 53 92 13 95 2D 05 D2 90 38 07<br>A3 58 30 56 30 0C 06 03 55 1D 13 01 01 FF 04 02<br>30 00 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02<br>07 80 30 1F 06 03 55 1D 23 04 18 30 16 80 14 53<br>1B 46 32 F2 BA 1B EC 35 23 B0 C6 84 E2 BC 7F 11<br>DA A2 2E 30 15 06 03 55 1D 20 04 0E 30 0C 30 0A<br>06 08 2A 82 14 00 44 01 14 01 30 0A 06 08 2A 86<br>48 CE 3D 04 03 02 03 49 00 30 46 02 21 00 A6 BF<br>28 A3 EF AE 18 3A DE 0A 0B 49 32 1D A2 C2 E0 CF<br>AF 4E D6 F2 FF 80 57 1E 4E 50 EF C3 0D 5D 02 21<br>00 F6 B9 E4 74 07 91 B4 2C 99 4B 45 C8 07 F3 1D<br>BE BF 7B 54 73 3B 0E 63 E6 0C 11 0E 09 11 13 43<br>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 | ECDSA NIST P-256 |
| Public Key | 04<br>5D F7 36 9A 8B 47 E8 61 A6 94 5C 9D EC 18 EF 4A<br>6F BE 55 1C 78 23 74 A6 06 29 D4 65 9B 81 C2 5D<br>9F F5 1F 70 8A 4D 3F 19 36 70 C3 10 51 DD 67 12<br>DC F2 B6 2A 8A 70 53 92 13 95 2D 05 D2 90 38 07 |

# 4 Infineon Productive certificates

## 4.1 PKI hierarchy for Productive Certificates

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

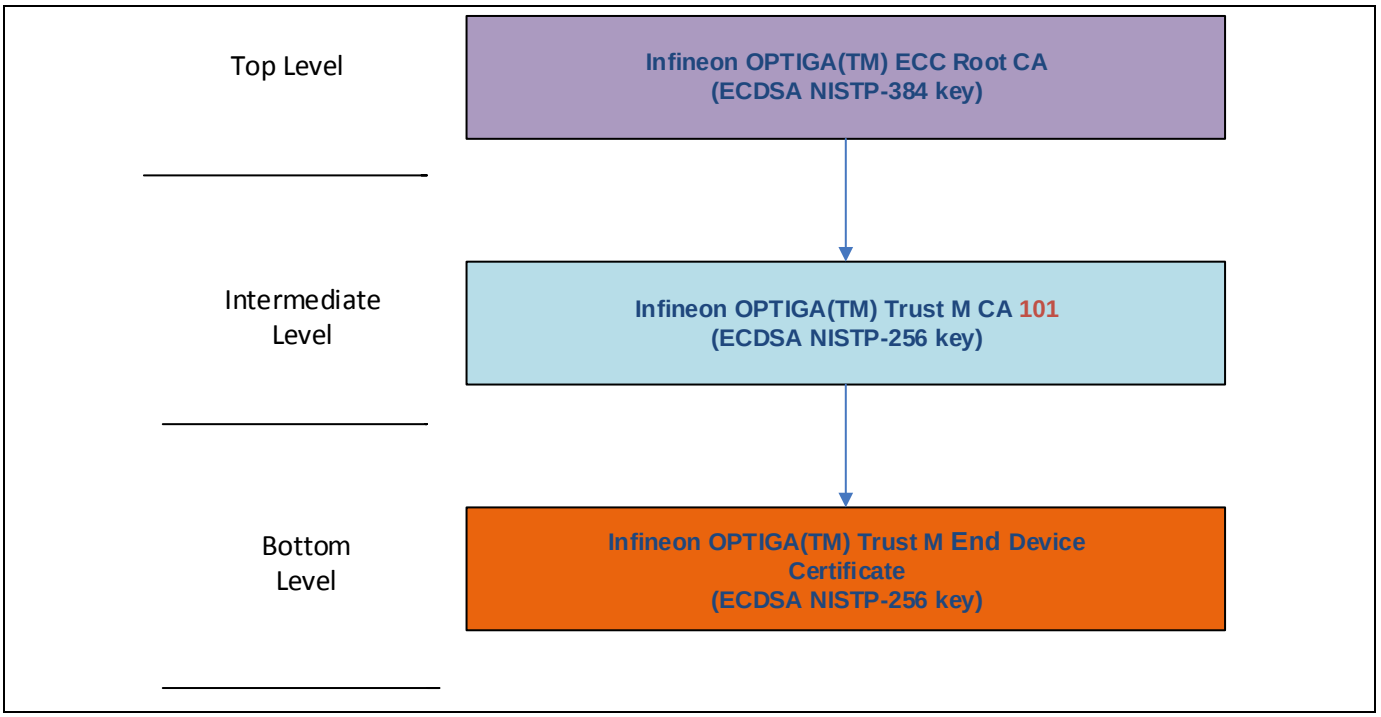


**Figure 2 PKI Hierarchy**

## 4.2 Productive CA certificate

The Infineon OPTIGA(TM) Trust M CA 101 is of intermediate level which is issued by Infineon OPTIGA(TM) ECC Root CA.

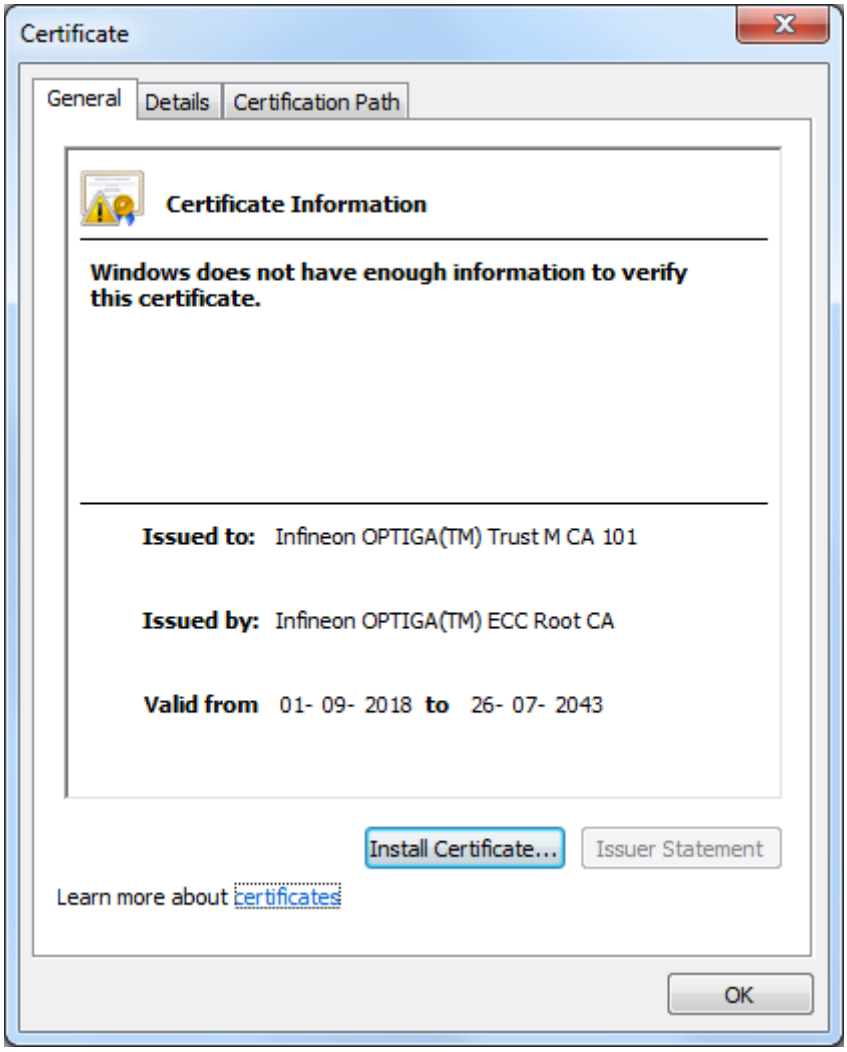


**Figure 3 Infineon intermediate CA details**

The details of the OPTIGA(TM) Trust M CA 101 intermediate CA certificate are given below:

**Table 4 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 14<br>D1 6F 3B 30 0A 06 08 2A 86 48 CE 3D 04 03 03 30<br>77 31 0B 30 09 06 03 55 04 06 13 02 44 45 31 21<br>30 1F 06 03 55 04 0A 0C 18 49 6E 66 69 6E 65 6F<br>6E 20 54 65 63 68 6E 6F 6C 6F 67 69 65 73 20 41<br>47 31 1B 30 19 06 03 55 04 0B 0C 12 4F 50 54 49<br>47 41 28 54 4D 29 20 44 65 76 69 63 65 73 31 28<br>30 26 06 03 55 04 03 0C 1F 49 6E 66 69 6E 65 6F<br>6E 20 4F 50 54 49 47 41 28 54 4D 29 20 45 43 43<br>20 52 6F 6F 74 20 43 41 30 1E 17 0D 31 38 30 39<br>30 31 31 34 34 36 34 30 5A 17 0D 34 33 30 37 32<br>35 32 33 35 39 35 39 5A 30 72 31 0B 30 09 06 03<br>55 04 06 13 02 44 45 31 21 30 1F 06 03 55 04 0A<br>0C 18 49 6E 66 69 6E 65 6F 6E 20 54 65 63 68 6E<br>6F 6C 6F 67 69 65 73 20 41 47 31 13 30 11 06 03<br>55 04 0B 0C 0A 4F 50 54 49 47 41 28 54 4D 29 31<br>2B 30 29 06 03 55 04 03 0C 22 49 6E 66 69 6E 65<br>6F 6E 20 4F 50 54 49 47 41 28 54 4D 29 20 54 72<br>75 73 74 20 4D 20 43 41 20 31 30 31 30 59 30 13<br>06 07 2A 86 48 CE 3D 02 01 06 08 2A 86 48 CE 3D<br>03 01 07 03 42 00 04 97 33 77 34 AD 74 23 A1 4B<br>F4 0F D4 EE 1D 27 AF 8E D0 5A E8 79 70 C7 4D FE<br>29 88 9B 49 9A D2 D0 1E A2 49 AE 79 10 F0 52 C5<br>9D 85 51 4A 82 15 E2 D6 3E 47 30 CD FB 5C C1 53<br>BB CC 00 A7 E6 40 8B A3 7D 30 7B 30 1D 06 03 55<br>1D 0E 04 16 04 14 3C 30 8C 5C D5 8A E8 A3 5D 32<br>80 E4 54 83 B2 FF CD 86 4D 23 30 0E 06 03 55 1D<br>0F 01 01 FF 04 04 03 02 00 04 30 12 06 03 55 1D<br>13 01 01 FF 04 08 30 06 01 01 FF 02 01 00 30 15<br>06 03 55 1D 20 04 0E 30 0C 30 0A 06 08 2A 82 14<br>00 44 01 14 01 30 1F 06 03 55 1D 23 04 18 30 16<br>80 14 B4 18 85 C8 4A 4A C5 12 7A F2 40 39 DE C4<br>F5 8B 1E 7E 4A D1 30 0A 06 08 2A 86 48 CE 3D 04<br>03 03 03 68 00 30 65 02 31 00 9E 7C D9 E9 82 63<br>7B BC 51 65 66 A9 C5 BA 30 EC A5 0A 0C 3B 98 1D<br>C7 24 4A 3D FE 5D D3 00 48 98 EE 92 38 03 AE B5<br>5A FA 25 4D 73 4C 8A 4C 7B 83 02 30 73 58 F0 FE<br>F3 BA 8E 33 78 4C 33 FF 37 EA 6F 35 72 B3 56 90<br>32 B5 CE 3E 6A D1 AC 47 79 42 01 B1 AC 37 AD E2<br>53 D8 76 B2 93 58 B9 1A 53 11 76 CD |
| SHA1 Thumbprint | 8e ee dc 75 fb 9d e6 57 b7 99 27 e8 d2 6d 51 c2 e7 32 a9 86 |
| Sign and Hash Algorithm | SHA384 ECDSA |
| Public Key parameters | ECDSA NIST P-256 |
| Public Key | 04<br>97 33 77 34 AD 74 23 A1 4B F4 0F D4 EE 1D 27 AF<br>8E D0 5A E8 79 70 C7 4D FE 29 88 9B 49 9A D2 D0<br>1E A2 49 AE 79 10 F0 52 C5 9D 85 51 4A 82 15 E2<br>D6 3E 47 30 CD FB 5C C1 53 BB CC 00 A7 E6 40 8B |

# 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,<br>Infineon test end entity certificate updated. |
| Page 7 | Revision 1.2,<br>Infineon test end entity certificate updated common subject name to Infineon IoT Node. |
| Page 5 | Revision 1.30,<br>Note for not using test certificate for final product added. |
| Page 8,9,10 | Revision 1.40,<br>Added productive certificate details |
| All | Revision 1.50,<br>Product Naming changed to TrustM |

**Trademarks of Infineon Technologies AG**
µHVIC™, µIPM™, µPFC™, AU-ConvertIR™, AURIX™, C166™, CanPAK™, CIPOS™, CIPURSE™, CoolDP™, CoolGaN™, COOLiR™, CoolMOS™, CoolSET™, CoolSiC™, DAVE™, DI-POL™, DirectFET™, DrBlade™, EasyPIM™, EconoBRIDGE™, EconoDUAL™, EconoPACK™, EconoPIM™, EiceDRIVER™, eupec™, FCOS™, GaNpowIR™, HEXFET™, HITFET™, HybridPACK™, iMOTION™, IRAM™, ISOFACE™, IsoPACK™, LEDrivIR™, LITIX™, MIPAQ™, ModSTACK™, my-d™, NovalithIC™, OPTIGA™, OptiMOS™, ORIGA™, PowIRaudio™, PowIRStage™, PrimePACK™, PrimeSTACK™, PROFET™, PRO-SIL™, RASIC™, REAL3™, SmartLEWIS™, SOLID FLASH™, SPOC™, StrongIRFET™, SupIRBuck™, TEMPFET™, TRENCHSTOP™, TriCore™, UHVIC™, XHP™, XMC™

Trademarks updated November 2015

**Other Trademarks**
All referenced product or service names and trademarks are the property of their respective owners.

**Edition 2019-07-12**

**Published by**

**Infineon Technologies AG**

**81726 Munich, Germany**

**© 2019 Infineon Technologies AG.**
**All Rights Reserved.**

**Do you have a question about this document?**

**Email:**
**DSSCustomerService@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.