OPTIGA™ Trust M configurations

Configuration guide

About this document

Scope and purpose

This document compares the configurations of the following OPTIGA™ Trust M variants:

1. OPTIGA™ Trust M V1
2. OPTIGA™ Trust M V3
3. OPTIGA™ Trust M Express
4. OPTIGA™ Trust M MTR

Intended audience

This document is primarily intended for solution providers and system integrators.

Table of contents

List of tables

1 Introduction

The OPTIGA™ Trust M chip is programmed and provisioned in a secure and certified Infineon factory, with a variety of personalization options available.

OPTIGA™ Trust M V1 and OPTIGA™ Trust M V3 chips provide a standard configuration (unless otherwise specified), which indicates that data objects and keys objects will have default data as per *OPTIGA™ Trust M, Solution Reference Manual* [1] and a default PKI setup. An ECC NIST P-256 end device certificate and the corresponding private key are provisioned in the certificate object 0xE0E0 and 0xE0F0, respectively, in the default PKI setup.

The OPTIGA™ Trust M Express chip is identical to the OPTIGA™ Trust M V3 chip, however it is provisioned and configured with all of the features required to securely connect the device to the cloud (AWS, Azure).

CIRRENT™ Cloud ID supports OPTIGA™ Trust M Express. The device certificates and secrets provisioned in the chip can be downloaded from CIRRENT™ Cloud ID.

The OPTIGA™ Trust M MTR chip is identical to the OPTIGA™ Trust M V3 chip, however it is provisioned and configured in a way to enable the late-stage provisioning of Matter related credentials. Additionally, it has all the features required to securely connect the device to the cloud (AWS, Azure). Kudelski IoT hosts a Matter certified Product Attestation Authority (PAA), which will be used to set up a Matter PKI (PAI) for the customer and in turn generate Device Attestation Certificates (DAC). These credentials can be downloaded from Kudelski keySTREAM.

2 OPTIGA™ Trust M configurations

Table 1 compares the OPTIGA™ Trust M variants in terms of configurations.

Table 1 Comparison of OPTIGA™ Trust M configurations

Object ID - description		OPTIGA™ Trust M V1	OPTIGA™ Trust M V3	OPTIGA™ Trust M Express	OPTIGA™ Trust M MTR
0xE0E0 – Certificate	Validity	20 years	20 years	20 years	20 years
	Intermediate CA certificate CN	Infineon OPTIGA™ Trust M CA 101	Infineon OPTIGA™ Trust M CA 300	Infineon OPTIGA™ Trust M CA 306	Infineon OPTIGA™ Trust M CA 306
	Root CA certificate CN	Infineon OPTIGA™ ECC Root CA	Infineon OPTIGA™ ECC Root CA 2	Infineon OPTIGA™ ECC Root CA 2	Infineon OPTIGA™ ECC Root CA 2
	Read AC	ALW	ALW	ALW	ALW
	Change AC	NEV	NEV	Conf(0xE140) && Auto(0xF1D0)	(LcsO < operational) || (Conf(0xE140) && Auto(0xF1D0))
	Execute AC	ALW	ALW	ALW	ALW
	Life cycle state (LcsO)	Creation	Creation	Operational	Initialization
0xE0F0 - Private key	Value	Chip unique key. Corresponding public key certificate is stored in 0xE0E0	Chip unique key. Corresponding public key certificate is stored in 0xE0E0	Chip unique key. Corresponding public key certificate is stored in 0xE0E0	Chip unique key. Corresponding public key certificate is stored in 0xE0E0
	Key algorithm	ECC P-256	ECC P-256	ECC P-256	ECC P-256
	Read AC	NEV	NEV	NEV	NEV
	Change AC	NEV	NEV	Conf(0xE140) && Auto(0xF1D0)	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	ALW	ALW	ALW	ALW
	Life cycle state (LcsO)	Creation	Creation	Operational	Operational
0xE0E1 - Certificate	Validity	This data object contains default value	This data object contains default value	20 years	20 years
	Intermediate CA certificate CN			Infineon OPTIGA™ Trust M CA 306	Infineon OPTIGA™ Trust M CA 306
	Root CA certificate CN			Infineon OPTIGA™ ECC Root CA 2	Infineon OPTIGA™ ECC Root CA 2
	Read AC	ALW	ALW	Conf(0xE140)	ALW

(table continues...)

Table 1 (continued) Comparison of OPTIGA™ Trust M configurations

Object ID - description		OPTIGA™ Trust M V1	OPTIGA™ Trust M V3	OPTIGA™ Trust M Express	OPTIGA™ Trust M MTR
	Change AC	LcsO < operational	LcsO < operational	Conf(0xE140) && Auto(0xF1D0)	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	ALW	ALW	Conf(0xE140)	ALW
	Life cycle state (LcsO)	Creation	Creation	Operational	Operational
0xE0F1 - Private key	Value	Default	Default	Chip unique key. Corresponding public key certificate is stored in 0xE0E1	Chip unique key. Corresponding public key certificate is stored in 0xE0E1
	Key algorithm	Not configured	Not configured	NIST P-256	ECC P-256
	Read AC	NEV	NEV	NEV	NEV
	Change AC	LcsO < operational	LcsO < operational	Conf(0xE140) && Auto(0xF1D0)	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	ALW	ALW	Conf(0xE140)	ALW
	Life cycle state (LcsO)	Creation	Creation	Operational	Operational
0xE0E2 - Certificate	Validity	This data object contains default value	This data object contains default value	20 years	20 years
	Intermediate CA certificate CN			Infineon OPTIGA™ Trust M CA 309	Infineon OPTIGA™ Trust M CA 309
	Root CA certificate CN			Infineon OPTIGA™ RSA Root CA 2	Infineon OPTIGA™ RSA Root CA 2
	Read AC	ALW	ALW	ALW	ALW
	Change AC	LcsO < operational	LcsO < operational	Conf(0xE140) && Auto(0xF1D0)	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	ALW	ALW	ALW	ALW
	Life cycle state (LcsO)	Creation	Creation	Operational	Operational
0xE0FC - Private key	Value	Default	Default	Chip unique key. Corresponding public key certificate is stored in 0xE0E2	Chip unique key. Corresponding public key certificate is stored in 0xE0FC
	Key algorithm	Not configured	Not configured	RSA 2048	RSA 2048
	Read AC	NEV	NEV	NEV	NEV

(table continues...)

Table 1 (continued) Comparison of OPTIGA™ Trust M configurations

Object ID - description		OPTIGA™ Trust M V1	OPTIGA™ Trust M V3	OPTIGA™ Trust M Express	OPTIGA™ Trust M MTR
	Change AC	LcsO < operational	LcsO < operational	Conf(0xE140) && Auto(0xF1D0)	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	ALW	ALW	ALW	ALW
	Life cycle state (LcsO)	Creation	Creation	Operational	Operational
0xE140 - Platform binding secret	Value	Default	Default	Chip unique value	Chip unique value
	Read AC	LcsO < operational	LcsO < operational	NEV	NEV
	Change AC	LcsO < operational || Conf(0xE140)	LcsO < operational || Conf(0xE140)	Conf(0xE140) && Auto(0xF1D0)	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	ALW	ALW	ALW	ALW
	Life cycle state (LcsO)	Creation	Creation	Operational	Operational
0xF1D0 – Arbitrary data	Value	Default	Default	Chip unique value	Chip unique value
	Read AC	ALW	ALW	NEV	NEV
	Change AC	LcsO < operational	LcsO < operational	Conf(0xE140) && Auto(0xF1D0)	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	NEV	NEV	Conf(0xE140)	Conf(0xE140)
	Life cycle state (LcsO)	Creation	Creation	Operational	Operational
	Object type	Not configured	Not configured	AUTOREF	AUTOREF

***Note**: For default values, refer to OPTIGA™ Trust M, Solution Reference Manual [1].*

The following ACs are used in Table 1:

- **ALW** - the action is ***always*** possible. It can be performed without any restrictions
- **NEV** - the action is ***never*** possible. It can only be performed internally
- **LcsO(X)** - the action is only possible in case the data object-specific lifecycle status meets the condition given by X
- **Auto(X)** - the action is only possible in case the authorization of the external entity was successfully performed using the authorization reference secret
- **Conf(X)** - the action is only possible in case the data involved (to be read/written) are confidentiality protected with key given by X. This enforces the shielded connection during the operations to enable the restricted usage (only with the known host)

2.1 OPTIGA™ Trust M MTR: Late-Stage Provisioning Configuration

The OPTIGA™ Trust M MTR is not in its final state upon delivery to the customer. Some of the data objects must be customized (the so-called "late stage provisioning") by the OEM to fit the Matter use case. In the following table, we show one of the possible final configurations after "late-stage provisioning":

Table 2 **OPTIGA™ Trust M MTR configurations after late-stage provisioning**

Object ID - description		OPTIGA™ Trust M MTR (OEM)
0xE0E0 – Certificate	Validity	20 years
	Intermediate CA certificate CN	Matter OEM-Specific PAI (located in 0xE0E8)
	Root CA certificate CN	Kudelski Root PAA
	Read AC	ALW
	Change AC	(LcsO < operational) || (Conf(0xE140) && Auto(0xF1D0))
	Execute AC	ALW
	Life cycle state (LcsO)	Operational
0xE0F0 – Private key	Value	Chip unique key. Corresponding public key certificate is stored in 0xE0E0
	Key algorithm	ECC P-256
	Read AC	NEV
	Change AC	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	ALW
	Life cycle state (LcsO)	Operational
0xE0E1 – Certificate	Validity	20 years
	Intermediate CA certificate CN	Infineon OPTIGA™ Trust M CA 306
	Root CA certificate CN	Infineon OPTIGA™ ECC Root CA 2
	Read AC	ALW
	Change AC	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	ALW
	Life cycle state (LcsO)	Operational
0xE0F1 – Private key	Value	Chip unique key. Corresponding public key certificate is stored in 0xE0E1
	Key algorithm	ECC P-256
	Read AC	NEV
	Change AC	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	ALW
	Life cycle state (LcsO)	Operational

(table continues...)

Table 2 (continued) OPTIGA™ Trust M MTR configurations after late-stage provisioning

Object ID - description		OPTIGA™ Trust M MTR (OEM)
0xE0E2 – Certificate	Validity	20 years
	Intermediate CA certificate CN	Infineon OPTIGA™ Trust M CA 309
	Root CA certificate CN	Infineon OPTIGA™ RSA Root CA 2
	Read AC	ALW
	Change AC	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	ALW
	Life cycle state (LcsO)	Operational
0xE0FC – Private key	Value	Chip unique key. Corresponding public key certificate is stored in 0xE0FC
	Key algorithm	RSA 2048
	Read AC	NEV
	Change AC	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	ALW
	Life cycle state (LcsO)	Operational
0xE140 – Platform binding secret	Value	Chip unique value
	Read AC	NEV
	Change AC	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	ALW
	Life cycle state (LcsO)	Operational
0xF1D0 – Arbitrary data	Value	Chip unique value
	Read AC	NEV
	Change AC	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	Conf(0xE140)
	Life cycle state (LcsO)	Operational
	Object type	AUTOREF
0xE0E8 – Certificate	Validity	20 years
	Intermediate CA certificate CN	n/a
	Root CA certificate CN	Kudelski Root PAA
	Read AC	ALW
	Change AC	Conf(0xE140) && Auto(0xF1D0)
	Execute AC	ALW
	Life cycle state (LcsO)	Operational

3 Access condition

This section describes the access condition "Conf(0xE140) && Auto(0xF1D0)."

When Conf(0xE140) && Auto(0xF1D0) is specified as the access condition for change (write) access type, the following conditions must be met for the successful execution of change operation:

- **Conf(0xE140)** - the shielded connection must be established between Host MCU and OPTIGA™ Trust M already using the specified pre-shared secret (0xE140) known as “platform binding secret” and the command is sent with protection (encrypted). For more information on shielded connection refer to *OPTIGA™ Trust M, Solution Reference Manual* [1]
- **Auto(0xF1D0)** - the authorization of the external entity must be successfully performed by using the authorization reference secret as specified by the secret OID (0xF1D0). For detailed description, refer to authorization reference sub-section of Appendix section in *OPTIGA™ Trust M, Solution Reference Manual* [1]

References

Infineon

[1] Infineon Technologies AG: *OPTIGA™ Trust M, Solution Reference Manual* (Revision 3.60); 2023-12-04

[2] Infineon Technologies AG: *OPTIGA™ Trust M Cloud ID, User Guide* (Revision 1.2); 2022-11-09

Glossary

AC

access condition (AC)

CA

certificate authority (CA)

CN

common name (CN)

ECC

elliptic curve cryptography (ECC)

RSA

Rivest Shamir Adleman (RSA)
An asymmetric cryptographic algorithm in which the encryption key is public and differs from the decryption key, which is kept secret (private).

Revision history

Reference	Description
Revision 2.2, 2024-01-17	
Chapter 1	Fix typography
Revision 2.1, 2023-12-04 (Internal revision)	
Chapter 1	Minor changes
Revision 2.0, 2023-11-14 (Internal revision)	
All	Added OPTIGA™ Trust M MTR configurations
Revision 1.2, 2022-11-09	
All	Layout change
Revision 1.1, 2022-10-20	
All	Editorial changes
Revision 1.0, 2022-10-11	
All	Initial release

Trademarks

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

Edition 2024-01-17

Published by

Infineon Technologies AG

81726 Munich, Germany

© 2024 Infineon Technologies AG

All Rights Reserved.

Do you have a question about any aspect of this document?

Email:
CSSCustomerService@infineon.com

Document reference
IFX-gxd1663743760933

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.

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.