Keys

MAO-DOC-HOW-004 v1.1

Contents

Introduction

This guide names all the keys used by the MULTOS security mechanism and describes their use. The actual processes are explained in detail in other documents, namely *Enablement*, *Guide to Loading and Deleting Applications* and *Guide to Generating Application Load Units*.

The keys are described in the order they are used in the lifecycle of a MULTOS device. For asymmetric keys the following name extensions are used:

_SK : The secret / private half of the key
_PK : The public half of the key
_PK_C : A certified public key

Table of Keys

Full name	Mnemonic	Type	Source & Usage
MULTOS Injection Security Application Base Key	MISA_Base	Symmetric	KMA generated base keys which are derived from master keys. These keys are diversified during wafer production to inject each chip with a unique transport key (TKV, see below).
Transport Key (Variable)	TKV	Symmetric	Unique key injected during wafer manufacture. Used to encrypt enablement data (MSMs). All chips are therefore individually locked at manufacture and DO NOT require a key rotation step later on. It also guarantees that only genuine MULTOS chips can be enabled.
Transport Key (Fixed)	TKF	Symmetric	Injected during manufacture. Used by the Check Data command.
MULTOS Device Key	MKD	Asymmetric	Randomly generated by the KMA MKD_SK and MKD_PK_C are loaded to the chip as part of the enablement data. The use of MKD allows chips to be authenticated and applications to remain confidential. MKD_PK is used during Application Load Unit (ALU) generation to encrypt the Key Translation Unit (KTU). MKD_SK is used by the chip to decipher the KTU when loading applications. MKD_PK_C is output by the card at the beginning of application loading (see TKCK).
Transport Key	TKCK	Asymmetric	Generated by the KMA. This key is different for

Certifying Key			each implementer and product line. The KMA uses TKCK_SK to sign MKD_PKs during enablement data generation. TKCK_PK can be used during ALU generation to validate the authenticity of a chip (and recover its key) by deciphering MKD_PK_C.
Data Encryption Key	DEK	Symmetric	Randomly generated by the ALU generator. Used to encipher sections of the application. It is included as part of the KTU, which is secured by the chip's key (MKD).
Application Provider's Key	APP	Asymmetric	Generated by the application provider or personaliser. The use of APP makes it possible to check the authenticity and integrity of an application. APP_PK must be signed by the KMA as part of an Application Load Certificate (ALC). APP_SK is used during ALU generation to sign the ALU.
Hash Modulus	HASH_MOD	Asymmetric	Generated by the KMA. This key is different for each implementer and product line and forms part of the Legacy cryptographic scheme. In the Enhanced cryptographic scheme it is not used. The public part of the key is used to seed a hash generation algorithm (AHASH) that uses the RSA co-processor for secure hash generation. AHASH may be used for hash generation when signing ALUs and for checksums in enablement data. HASH_MOD is included as part of the chip's mask and is referred to as a "ROM Key". The secret part of the key is not used.
Key Certifying Key	KCK	Asymmetric	Generated by the KMA. This key is different for each implementer and product line. KCK_SK is used to sign APP_PKs in ALCs and therefore guarantees the authenticity of applications.

			KCK_PK is included as part of the chip's mask (a "ROM Key") and is used by the chip to verify ALCs during application loading.

Key Map