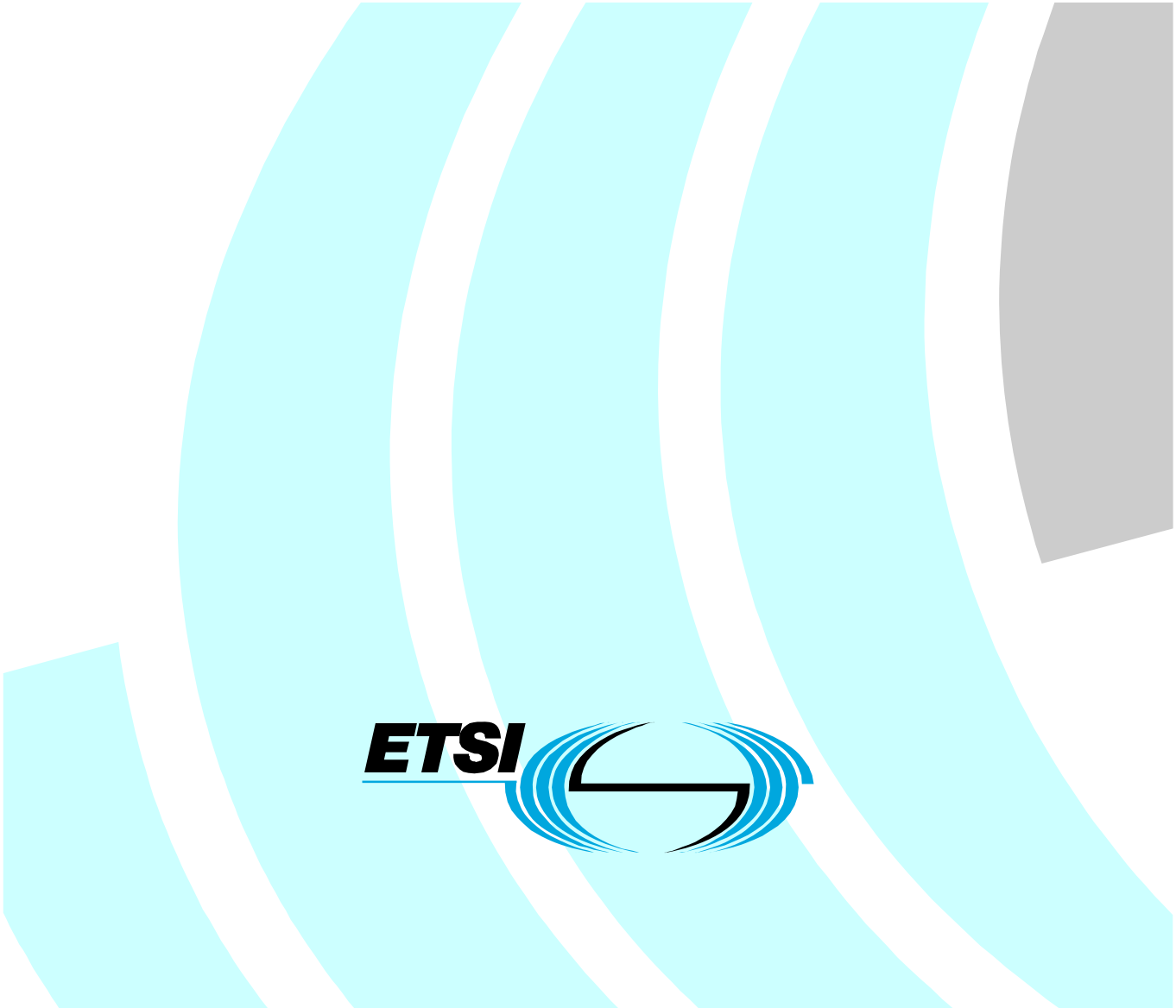
ETSI TS 103 162 V1.1.1 (2010-10)

Technical Specification

**Access, Terminals, Transmission and Multiplexing (ATTM);
Integrated Broadband Cable and Television Networks;
K-LAD Functional Specification**



Reference
DTS/ATTM-003012

Keywords
CA, cable

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Access, Terminals, Transmission and Multiplexing (ATTM).

1 Scope

The present document defines the key ladder and cryptographic requirements for security functionality to be embedded within a television receiver's chipset (e.g. SOC). The use of a standard key ladder ensures that any television receiving device may receive television content from any television distribution network regardless of the network security solution in use.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ISO/IEC 13818-1 (2007): Information technology - Generic coding of moving pictures and associated audio information: Systems".

[2] ETSI ETR 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems".

[3] ETSI TS 102 825-5: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 5: CPCM Security Toolbox".

[4] ISO/IEC 18033-3 (2005): Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers.

[5] FIPS-197 (AES): "Specification for the Advanced Encryption Standard Federal Information Processing Standards (FIPS)" Publication 197, November 26, 2001.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] DVB-CSA - DVB BlueBook A125 (2008)/(Document a125_CSA3_dTR101289.v1.2.1): "Support for use of the DVB Scrambling Algorithm version 3 within digital broadcasting systems".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Authentication key (A): a 16-byte key derived from K2 that is used by the challenge-response mechanism

NOTE: **A** can be used either to authenticate the sink device through a traditional challenge-response, or used by the sink device to authenticate messages from the source device by deriving a key for a CBC-MAC or similar symmetric message authentication algorithm.

control word: key used to descramble the video, either 8 or 16 bytes

Dk(Y): used to denote the data Y decrypted with key K

Ek(Y): used to denote the data Y encrypted with key K

ESCK: encrypted secret chipset key which is the value physically stored in the chipset's OTP

NOTE: It has to be at least as large as the SCK. The ESCK would be typically uneditable and unreadable after manufacture.

Key 1 (K1): 16-byte key used to decrypt the CW

Key 2 (K2): 16-byte key used to decrypt K1

Key Ladder Root Key, or Root Key (K3): 16-byte private key used by each compliant chipset at the root of the key ladder, it is used to decrypt K2

NOTE: In chipsets that implement an extended key ladder with n levels, the root key at the highest level of the key ladder will be denoted by Kn.

PID: Packet ID of a component elementary stream within a program carried in an MPEG-2 transport stream

public ID: 8-byte Public Identifier of the sink device chipset, including elements indicating the manufacturer and model as well as a globally unique identifier for the chipset instance within that model

SCK: secret chipset key which is unique to each compliant chipset

NOTE: It has to be at least 16-bytes. In initial chipset deployments that lack the root key derivation mechanism, the SCK may also serve as the key ladder root key K3. In this case the SCK shall be exactly 16 bytes.

vendor ID: value of at least 8 bits that will be used to identify CA vendors, network operators, and other entities using a compliant chipset

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard
CPU	Central Processing Unit
CW	Control Word
DES	Data Encryption Security
DVB-CSA2	Digital Video Broadcasting-Common Scrambling Algorithm
ILA	Industry Licensing Authority
MPEG	Motion Picture Equipment Group
OTP	One Time Programmable memory
SOC	System On Chip
SCK	Secret Chipset Key
STB	Set Top Box
TDES	Triple DES

4 Introduction

4.1 Overview

The present document is a specification for enabling and securing the delivery of content descrambling keys from a source device to a sink device.

The basis of the present document is a three-step key ladder and challenge-response authentication scheme in which the base key derivation inputs are protected within the one time programmable memory (OTP) of the sink device's hardware (e.g. chipset). The key ladder is used primarily for the delivery of content descrambling keys while the challenge-response mechanism is used for checking the integrity and authenticity of sink devices as well as messages arriving from an compliant source device.

The present document is intended for chipset manufacturers who choose to implement the key ladder functionality in their chipsets.

This key ladder specification is designed to support the dynamic substitution and replacement of either sink or source device in a manner that maintains the security and integrity of the underlying content distribution network. The specification enables the portability of sink devices between content distribution networks by permitting the field upgradeability of sink devices to work with previously unknown source devices. The specification also enhances the capability of networks to upgrade their source devices without disrupting the capabilities of already fielded sink devices.

While the source device is expected to be a key management system such as a traditional Conditional Access System or Digital Rights Management solution deployed by a content distribution network, and the sink device is expected to be a secure content consumption device such as a STB or television, the present document is not limited to only supporting these particular types of devices.

The present document is derived from an existing technical solution already deployed in existing hardware systems and is designed to be backwards compatible with these existing implementations.

The key derivation component of the present document enables cross-network portability by allowing network specific inputs to be securely reprogrammed in the field. The modification of one of these system inputs may occur 'on the fly', and is sufficient to enable a sink device to function securely on a new network, using a new 'root' key for the key ladder.

The present document does not specify how content arrives to the sink device descrambler, only that the sink device's descrambler shall recognize the scrambling algorithm utilized by the content's network distribution system.

The present document does not specify conformance and robustness rules for chipset hardware nor interoperability or certification requirements. Such rules are beyond the scope of the current specification and are expected to be the responsibility of an Industry Licensing Authority (ILA).

It is recognized that effective and safe implementation and deployment of content security systems based on the mechanisms described in the present document will require a complete security infrastructure that can deal with business, security, intellectual property , documentation and trusted information distribution issues. The description of such an infrastructure and the organizations which will administer it (i.e. an ILA) is outside of the scope of the present document.

As the present document is expected to be implemented in the chipset hardware of a sink devices, a universal separable security specification would also require that the sink device's hardware implement all standardized scrambling algorithms that it might ever encounter. To ensure universal portability of compliant sink device hardware between networks, a finite set of scrambling algorithms shall be implemented in these devices. Use of additional scrambling algorithms is permitted, but is not defined in the present document.

4.2 Descrambling Algorithm Requirements

The present document defines the key ladder, authentication mechanism, and cryptographic requirements of a compliant chipset implementation.

Except where explicitly noted, the following requirements are specific to Version 1 of the present document. To be backwards compatible, future versions of the present document shall support these initial requirements but may also support additional future requirements, such as DVB-CSA3 [i.1].

A compliant chipset shall include an MPEG-2 transport processor as defined by [1].

A compliant chipset shall include an MPEG-2 transport stream component descrambler utilizing an open, standard descrambling algorithm.

At a minimum, Version 1 requires support for two content descrambling algorithms (transport stream ciphers):

- DVB CSA2 [2];
- AES 128 Bit Cipher optimized for handling MPEG2 TS [3]) used in CBC mode only:
  - Chaining Mode is set to CBC and is therefore not required to implement RCBC chaining mode.

The authentication mechanism and the key ladder structure protecting the descrambling key within the descrambler of the transport processor chipset shall utilize two standardized block ciphers:

- TDES (Triple-DES as specified in [4]); and
- AES (as specified in [5]).

5 Functional Diagram

Figure 1 presents the functional design of the Version 1 key ladder embedded within the transport processor/descrambler chipset of the sink device, and depicts the key ladder's relationship with the drivers and dependent applications executed by the Main CPU, the content descrambler, and the other sink device functions. Figure 1 does not represent the chipset's actual hardware architecture.

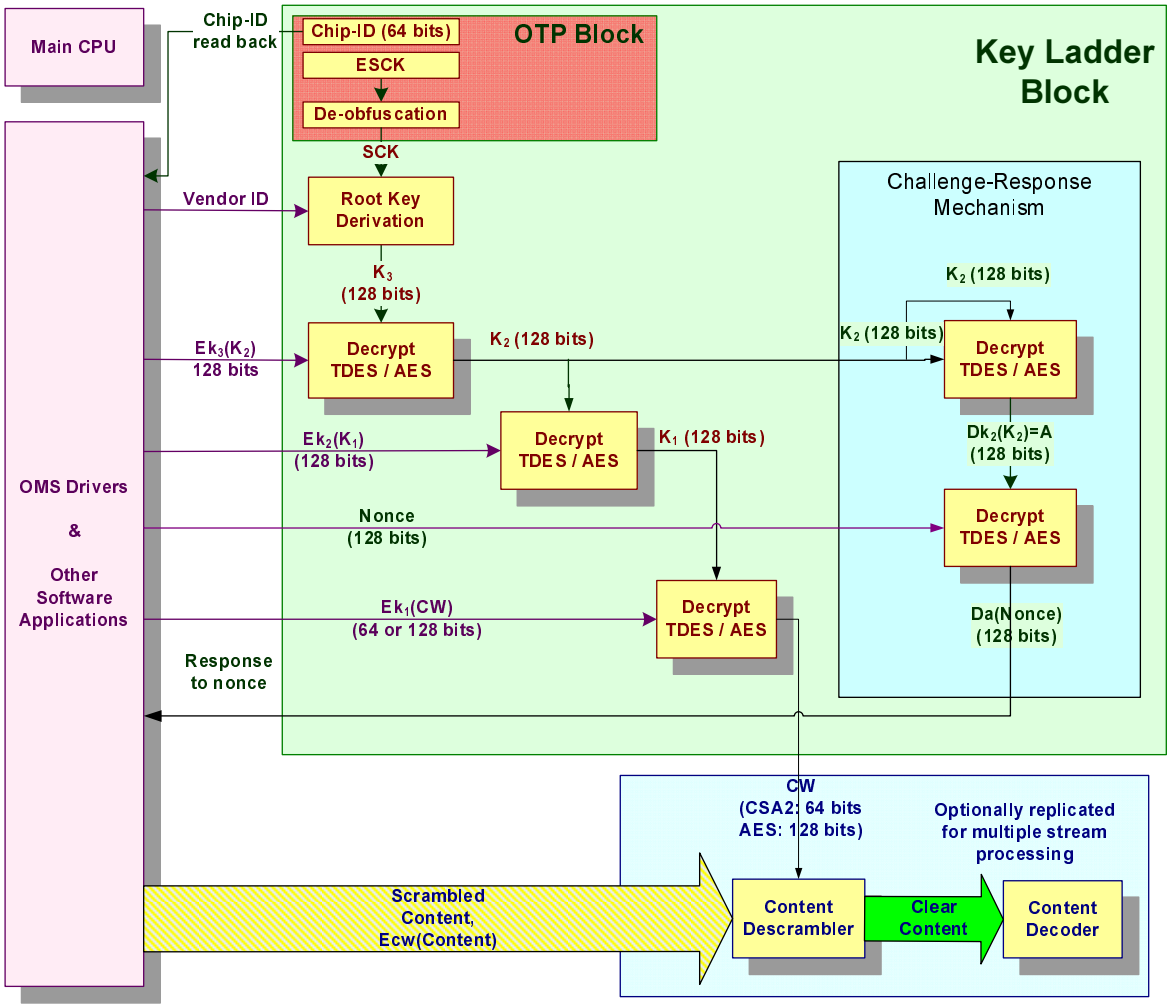


Figure 1: Key Ladder Functional Diagram

The following points are to be taken into consideration:

The chipset shall be capable of performing the key ladder operations in Figure 1 using both TDES and AES decryption - drivers will specify which algorithm to use for a given operation. In the case where the key ladder implements TDES and the content decryption is DVB-CSA2, the input **Ek1**(**CW**) to the last step in the key ladder is only 64 bits. In all other cases, **Ek1**(**CW**) is 128 bits.

The designation in Figure 1 of **Ecw**(**Content**) refers to encryption of content using AES or DVB CSA2 algorithms with C**W** serving as the key.

The **CW** is directed to the relevant register based on stream input, PID, and control word parity (odd/even).

In Figure 1, TDES parity checking of the key shall be suppressed in all TDES components.

The components in yellow in Figure 1 shall all be in a single silicon chip. The interface from applications that run on the CPU, even if the CPU is located on the same silicon as the key ladder, are permitted to input and output data only according to the interfaces that appear in the diagram. The main CPU shall have absolutely no read/write access to the registers that store **ESCK**, **SCK**, **Kn**,…,**K3, K2, K1 and A.** There shall be write, but no read, access to **CW**.

Table 1 describes the various options available depending on the key ladder and content descrambling algorithms employed.

Table 1: Key Ladder / Content Descrambling Algorithms

	DVB CSA2 Descrambling	AES Descrambling
TDES	64-bit CW	128-bit CW
AES	64-bit clear CW 128-bit encrypted CW	128-bit CW

6 Functional Requirements

6.1 Key Ladder Functions

6.1.1 CA Key Ladder

1. Each compliant chipset shall have a unique pair:

   a. A unique 64-bit CPU readable identification number (**Public-ID**).

   b. A unique secret 128-bit key (**SCK**).

2. Each compliant chipset shall have a mechanism for securely deriving an operator-specific 16-byte **K3** to serve as the root key of the key ladder. See clause Root Key Derivations below for further details.

   The format and values for the Public ID as well as for the **SCK** will be dictated by a Trusted Authority. The establishment of this administrative function is beyond the scope of the present document.

3. Each compliant chipset shall use the following sequence for decrypting video content:

   a. It shall receive the **Vendor ID** value and use this to derive a root key **K3** from the **SCK**.

   b. It shall receive **Ek3**(**K2**), decrypt this value using **K3** resulting in **K2** (128 bits).

   c. It shall receive **Ek2**(**K1**)**,** decrypt this value using **K2** resulting in **K1** (128 bits).

   d. It shall receive **EK1**(**CW**), decrypt this value using **K1** resulting in **CW** (64 bits for DVB CSA2; 128 bits for AES).

4. The compliant chipset shall be configurable as to whether or not the software may use clear control words. If clear control words are allowed, the compliant chipset shall allow the software to switch back and forth freely, without reset between clear control words and control words from the key ladder.

   If the compliant chipset supports descrambling of multiple streams simultaneously, then it shall be possible to use clear and encrypted control words simultaneously. Forbidding the use of clear control words will be configurable, one-time, in the form of on-chip OTP both by the chipset vendor as well as software programmable at the time of device (e.g. STB) manufacturing.

6.1.2 Challenge Response

The compliant chipset shall support a specific cryptographic challenge/response.

The specifics of the challenge/response modes are described in the four following points:

1. The compliant chipset shall receive the **Vendor ID**, **Ek3(K2**), and a 128-bit **nonce** via the driver API interface.

2. The compliant chipset shall produce a 128-bit key denoted **A** from **K2** by decrypting **K2** with itself to produce **Dk2(K2).**

3. The value nonce shall be decrypted using **A** to produce **Da(nonce).**

4. **Da(nonce)** shall be returned as the response to the CPU via the driver API interface.

6.1.3 Key Ladder Ciphers

The chipset shall support performing all decryptions in the key ladder and challenge-response mechanism using both:

- AES-128; and
- Triple DES (TDES).

The selection of which cipher to use will be controlled by the driver API interface. Only AES-128 or TDES will be used for a root key to **CW** derivation chain. However, the chipset does not need to enforce this.

"TDES", as used in the present document means two-key Triple DES. If the two keys are A and B, then the decryption function should be $\mathbf{D}_A(\mathbf{E}_B(\mathbf{D}_A(x)))$. When decrypting more than 64 bits (the block size of TDES), the cipher shall be used in ECB mode. The key parity bits shall be ignored.

NOTE: Some legacy chipsets currently only support TDES. All future chipsets must support both TDES and AES.

6.1.4 CW Alignment

When the **CW** is only 64 bits, the value of the **CW** will reside in the 64 left-most (highest) bits of the decrypted **Ek1(CW).** This is true whether the key ladder is operating in AES or TDES mode.

6.2 Time Constraints

The time from loading the entire key ladder (loading **Vendor ID, Ekn(Kn-1), …, Ek3(K2), Ek2(K1), Ek1(CW))** to the beginning of decryption of video shall be less than 1 ms.

6.3 Driver API

The drivers executing within the main CPU of the sink device are not specified in the present document because they are platform and industry-specific. The specific driver API may be obtained from the Trusted Authority upon request.

6.4 Secret Chipset Key Obfuscation

The value physically stored in the OTP shall not be **SCK** itself. Rather, it should be the result of performing an **invertible** secret function on the **ESCK**, the value physically stored in the chipset's OTP. Where feasible, this function should be different in every chipset model.

An ILA could provide a secret function upon request.

The function should have an input of at least 128 bits, be invertible, and produce close to 2^128 possible output values. In order to be effective as an obfuscation measure, the secret function shall be implemented in hardware.

The obfuscation shall be implemented such that during the chipset serialization process, the chipset receives the **ESCK** from the serializing entity and burns this value to OTP.

An ILA would need to be able to calculate the obfuscation function.

7 Root Key Derivations

7.1 Introduction

In this clause, the word 'vendor' may refer to either a network operator, device manufacturer, CA provider, or other entity that may wish to utilize the compliant chipset.

In order to facilitate future improvements and to increase portability of compliant chipsets between multiple networks, compliant chipsets shall contain a cryptographic mechanism for deriving vendor-specific secret keys from a combination of the chipset's OTP secret(s), secret functions, and field-programmable inputs received via software. The derived secret will then serve as the root key in the key-ladder and authentication mechanisms.

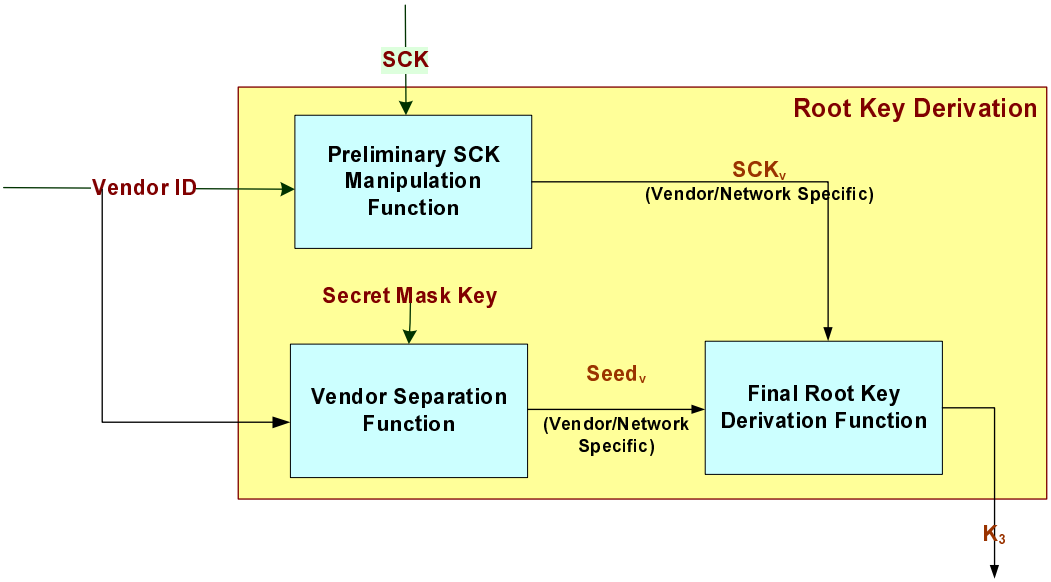


Figure 2: Root Key Derivation Functionality

Figure 2 "Root Key Derivation Functionality" represents an abstraction of the root key derivation mechanism and illustrates the separation of knowledge of secrets it affords. All boxes in the diagram are assumed to be cryptographically strong functions and for illustrative purposes may be thought of as one-way functions.

The process for calculating the root keys of a set of chips is as follows. For a given model chip, a vendor would obtain a list of (**Chip-ID, SCK_V**) pairs from the ILA, and a single **$Seed_V$** from the chip manufacturer corresponding to the provided **Vendor ID**. The **Vendor ID**s would be a known public constant that would serve to identify a given vendor. The vendor could then produce their own set of (**Chip-ID, K3**) pairs.

In this scenario, the ILA has knowledge of the **SCK** and the **Preliminary SCK Manipulation Function**, and **SCK_V** the chip manufacturer knows (at least) the **Vendor Separation Secret Function and $Seed_V$**, while the vendor knows **SCK_V**, **$Seed_V$**, and the Final Root Key Derivation Function. Note that only the vendor would have sufficient knowledge to compute **K_3**.

An ILA should act as the source for a complete Root Key Derivation mechanism.

7.2 Functional Requirements

1. The compliant chipset shall contain a Preliminary **SCK Manipulation Function** that accepts as inputs the 16-byte **SCK** and a **Vendor ID** of at least 8-bits via software. The output shall be 16-bytes and shall be denoted **SCK_V**.

2. The compliant chipset shall contain a **Vendor Separation Function** that accepts as inputs a secret mask key consisting of at least 16-bytes of secret gate-level data and at least 8-bits of **Vendor ID** data via software. The output shall be 16-bytes and shall be denoted **$Seed_V$**.

3. The compliant chipset shall contain a **Final Root Key Derivation Function** that accepts as inputs the **SCK_V**, **$Seed_V$**, and optionally, additional inputs from software. The output shall be the key ladder root key, typically **K_3**.

NOTE: A compliant chipset may use distinct Final Root Key Derivation functions for producing distinct Triple DES and AES root keys.

4. The root key derivation mechanism shall not preclude other security modules on the chipset from accessing vendor-independent chipset secrets.

8 Extensions

8.1 Introduction

This clause describes various extensions to the basic functionality described above which compliant chipset vendors may implement.

8.2 Additional Key Levels

The key ladder described above is referred to as a three-level key ladder composed of three **Ki = Dki-1(EKi)** operations. The compliant chipset vendor is permitted to build a ladder with more than three levels as long as the time constraints of Clause 6.2 Time Constraints, and certain security requirements detailed below are met.

In such a system, the root key of the n-level key ladder is denoted by **Kn**.

While a key ladder with more than three levels is permissible, a key ladder with a variable number of levels, but each time starting from the same key level is NOT permitted. Imagine for example a chipset supporting a key ladder that supported either three or four levels. That means that a chain of encrypted keys meant to be used with a four-level key ladder, could be applied to a three-level key ladder. The result is that the value intended as **K1** could be used as a control word. If an available content descrambling scheme is compatible with the key ladder decryption function, then the **CW** meant to be protected by a four-level key ladder becomes exposed by using the chipset as a three-level key ladder.

A chipset using more than 3 levels in the key ladder shall always compute the authentication key **A** by decrypting **K2** with itself, and not by decrypting **Kn-1** with itself.

Any system designed around the capabilities of the present document must ensure that it will function properly with devices supporting more than 3 levels in the key ladder.

If it is necessary to support a variable number of levels, it may be possible to use the chipset's key derivation mechanism to provide a different root key for each length key ladder.

8.3 Additional Security Operations

It may be desirable for some chipsets to perform additional operations with keys or values derived from **SCK**, **Kn**, or other approved key ladder keys. Approval of such uses will be determined solely by Industry Licensing Authority (ILAs) and their specific security and robustness requirements.

In general, a safe approach to offering such capabilities in an ILA approved compliant chipset would be to use a secret entirely separate from the approved keys, or to use a single secret from which both the approved keys and the key for the additional functionality are securely derived. For example, a chipset could require any approved key to pass through a cryptographic one way function before being exported for use in an external context.

History

Document history		
V1.1.1	October 2010	Publication