STS Association

STS 600-10-1

Edition 1.2

Feb 2022

Standard Transfer Specification – Key management – Functional and security requirements for hardware security modules

CONTENTS

Revision History

Edition	Clause	Date	Change details from previous edition
1.0			First edition
1.1	4.2	Oct 2019	Changed the security requirements approvals.
1.2	4.5	Feb 2022	Added requirement for declaration that HSM ID only allocated to a hardware device

STANDARD TRANSFER SPECIFICATION ASSOCIATION

_____

STANDARD TRANSFER SPECIFICATION –

Key management – Functional and security requirements for hardware security modules

FOREWORD

1) The Standard Transfer Specification Association (STSA) is a worldwide organization for standardization comprising all members of STSA. The object of STSA is to develop, maintain and promote international use of the Standard Transfer Specification (STS). To this end and in addition to other activities, STSA publishes Standards, Technical Specifications, Technical Reports, Codes of Practice and Guides (hereafter referred to as "STSA Publication(s)"). Their preparation is entrusted to technical working groups; any STSA member interested in the subject dealt with may participate in this preparatory work. STSA collaborates closely with the International Electrotechnical Commission (IEC) in accordance with conditions determined by agreement between the two organizations. As such STSA performs the role of Registration Authority of IEC 62055-41, IEC 62055-51 and IEC 62055-52 on behalf of IEC.
2) The formal decisions or agreements of STSA on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each working group has representation from all interested STSA members.
3) STSA Publications have the form of recommendations for international use and are accepted by STSA Board of Directors in that sense. While all reasonable efforts are made to ensure that the technical content of STSA Publications is accurate, STSA cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
5) STSA provides attestation of conformity. Independent testing bodies provide conformity assessment services and recommendations to STSA Board of Directors who provides conformance certificates and access to STSA marks of conformity.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to STSA or its directors, employees, servants or agents including individual experts and members of its technical working groups for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this STSA Publication or any other STSA Publications.
8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this STSA Publication may be the subject of patent rights. STSA shall not be held responsible for identifying any or all such patent rights.

Standard Transfer Specification STS 600-10-1 has been prepared by working group 8.

The text of this standard is based on the following documents:

CDV	Report on voting
STS 600-10-1 CDV	STS 600-10-1 CDV

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with STSA Directive STS 2100-1.

INTRODUCTION

The Standard Transfer Specification (STS) is a secure message protocol that allows information to be carried between point of sale (POS) equipment and payment meters and it caters for several message types such as credit, configuration control, display and test instructions. It further specifies devices and codes of practice that allows for the secure management (generation, storage, retrieval and transportation) of cryptographic keys used within the system.

This document specifies minimum requirements for hardware security modules (HSMs) and is intended for use by manufacturers of HSMs for the generation of tokens and the manufacturing of meters that comply with the STS. Additional proprietary specifications and operating modes may apply to HSMs other than those contained in this standard; please refer to the relevant manual supplied with the HSM for such additional commands and operating modes.

STANDARD TRANSFER SPECIFICATION –

Key management – Functional and security requirements for hardware security modules

1 Scope

This standard specifies the functional and security requirements for hardware security modules (HSMs) used in the production process of STS compliant prepayment meters (manufacturing module) and HSMs used in the production of STS compliant tokens (vending module).

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62051 - ELECTRICITY METERING – *Glossary of terms*

IEC 62055-41 - *ELECTRICITY METERING – PAYMENT SYSTEMS – Part 41: Standard Transfer Specification – Application layer protocol for one-way token carrier systems*

IEC 62055-51 - *ELECTRICITY METERING – PAYMENT SYSTEMS – Part 51: Standard Transfer Specification – Physical layer protocol for one-way numeric and magnetic card token carriers*

STS 600-4-2 - *STANDARD TRANSFER SPECIFICATION – Companion Specification – Key Management System*

STS 600-8-1 *Addendum to IEC 62055- 41: Key management - Legacy Security Module API for STS03V*

STS 600-8-2 *Addendum to IEC 62055- 41: Key management - Legacy Security Module API for STS03M*

STS 600-8-3 *Addendum to IEC 62055- 41: Key management - Legacy Security Module API for STS04A*

STS 600-8-4 *Addendum to IEC 62055- 41: Key management - Legacy Security Module API for STS05V*

STS 600-8-5 *Addendum to IEC 62055- 41: Key management - Legacy Security Module API for STS05M*

STS 600-8-6 *Standard Transfer Specification Key management - Hardware security module API*

Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) *Modular Security Requirements - Version 3.0, June 2016*

Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) *Modular Evaluation Vendor Questionnaire, V3.0 June 2016*

Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) *Modular Derived Test Requirements, V3.0, June 2016*

NOTE The PCI standards may be obtained from : www.pcisecuritystandards.org

3 Terms and definitions

3.1 Definitions

For the purposes of this standard, the terms and definitions given in IEC 62051, IEC 62055-41, IEC 62055-51, STS 600-8-6 and STS 600-4-2 shall apply.

3.2 Acronyms

API	Application Programming Interface
DCTK	Decoder Common Transfer Key
DDTK	Decoder Default Transfer Key
DITK	Decoder Initial Transfer Key
DUTK	Decoder Unique Transfer Key
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
KMC	Key Management Centre
PCI	Payment Card Industry
PTS	PIN Transaction Security
PUBKEY	Public Key of an asymmetrical key pair
STS	Standard Transfer Specification
STSA	STS Association

4 HSM requirements

4.1 Basic requirements

4.1.1 Key registers

The HSM shall support at least 25 supply group key registers in compliance with STS 600-4-2 and IEC 62055-41.

NOTE It is the intention of the STSA to consider a fewer number of supply group key registers in a future revision of this standard.

4.1.2 Transaction rate

The HSM shall support a transaction rate of at least 1 transaction per second.

4.1.3 HSM variants

The HSM shall implement only one of the variant types outlined below in Table 1.

Table 1 – HSM device variants

Module type	Reference
Manufacturing	4.4
Vending	4.4

The manufacturing module variant shall support all the key change functions as specified in 6.5 of IEC 62055-41.

The manufacturing module variant shall support the encryption and decryption of credit transfer tokens under DITK only and it shall not support same under DDTK, DUTK or DCTK.

The vending module variant shall support all the key change functions as specified in 6.5 of IEC 62055-41, except that it shall not support DITK to DUTK, DITK to DDTK or DITK to DCTK key changes.

The vending module variant shall support the encryption and decryption of credit transfer tokens under DUTK and DCTK and it shall not support same under DITK or DDTK.

The manufacturing and vending module variants shall support all other tokens in compliance with 4.3 and 4.4.

4.2 Security requirements

The HSM comprises hardware and application firmware that together implement the API and meet the functional requirements of this specification.

The HSM shall comply with the requirements given in the following PCI standards:

- Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) *Modular Security Requirements*;
- Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) *Modular Evaluation Vendor Questionnaire*;
- Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) *Modular Derived Test Requirements*.

NOTE 1 The Vendor Questionnaire document elaborates on the modular security requirements and guides the HSM Manufacturer to provide detailed answers on how their implementation meets the requirements

NOTE 2 The Derived Test Requirements document details how the modular security requirements criteria will be assessed, and guides the testing laboratory in its assessment.

The HSM shall comply with the following sections of the Vendor Questionnaire document as given in Table 2.

HSM compliance to the PCI standards shall be assessed by a PCI-recognized laboratory and the test report submitted to the STS Association. Based on this report, the STS Association shall grant or deny approval once it receives the letter of recommendation from an STSA approved test house for the conformance testing as specified in the relevant STS test specifications. All efforts are to be made to seek a listing on the PCI website. In the case that this is not possible, the decision to grant approval of the product will rest solely with the STS Association.

Table 2 – Vendor Questionnaire sections

Section	Name	Compliance
A1 to A5	Physical Security Requirements	mandatory
B1 to B4	Logical Security Requirements	mandatory
B4.1	Logical Security Requirements	optional (NOTE 1)
B5 to B14	Logical Security Requirements	mandatory
B15	Logical Security Requirements	optional
B16	Logical Security Requirements	mandatory
B17, B18	Logical Security Requirements	optional
B19	Logical Security Requirements	mandatory
B20	Logical Security Requirements	optional
C1	Policy and Procedures	mandatory
D	Key Loading Devices	optional
E	Remote Administration - Logical Security	optional

F	Devices with Message Authentication Functionality	optional
G	Devices with Key Generation Functionality	optional
H	Devices with Digital Signature Functionality	optional
I1 to I8 (NOTE 2)	Device Security Functionality During Manufacturing	mandatory
J1 to J5, J7, J8 (J6 is n/a)	Device security Requirements between Manufacturer and Point of Initial Deployment	mandatory
NOTE 1 “optional” indicates a requirement that is not necessary, but may be implemented by the HSM manufacturer at their discretion; the HSM manufacturer must answer this Modular Security Requirement evaluation according to the HSM implementation - ‘Yes’ or ‘No’ or ‘N/A’ as appropriate. The testing laboratory may still require the HSM manufacturer to explain or justify their answer (in particular an answer of ‘No’ or ‘N/A’ to any question in sections A, B, C, I, or J). NOTE 2 I6 refers - if an HSM is initialized as per the requirements of STS 600-4-2, and the HSM manufacturer publishes the $PUBKEY_{sm}$ in the prescribed manner, then a successful key agreement with the KMC confirms the authenticity of the HSM.		

4.3 Functional requirements

The HSM shall comply with the requirements as given in STS 600-4-2, IEC 62055-41 and IEC 62055-51.

4.4 Application Programming Interface (API)

The HSM shall comply with the requirements given in STS 600-8-6.

Several variants of the API are possible and the HSM may thus optionally also comply with one or more of the following interface specifications (in addition to STS 600-8-6):

- STS 600-8-1;
- STS 600-8-2;
- STS 600-8-3;
- STS 600-8-4;
- STS 600-8-5.

In the case where a single HSM supports more than one API implementation, each API implementation may optionally be identified by its own firmware identifier.

For the purposes of HSM certification, each firmware version shall be considered separately and a subsequent change in any one of the firmware versions shall require re-certification of the HSM together with the relevant changed firmware.

4.5 Manufacturing requirements

The manufacturer shall submit a letter to the STS Association containing the following statement:

[insert company name] confirms that they shall not publish to any Live KMC an association between a Public Key and a non-Certified SM (including a Virtual or software SM), and that records of the manufacturers Unique ID (ID_{man})that are allocated to an SMID will be available for inspection on request from the STS Association.

The purpose of the record inspection would be to confirm that for every Public Key received by a Live KMC, the associated private key is known exclusively to a single, Certified, hardware SM.

Note: for definitions of SMID and ID_{man} – see STS600-4-2.

4.6 Electrical and environmental requirements

Electrical and environmental requirements are not specified in this document. It is left to the HSM manufacturer to ensure that the product is suitable for the environment that it is deployed in.