CEN/TC 33/WG 4 "Building hardware"
WG Secretariat: **SIS**
Convenor: **Lidén Inge Mr**

Draft for Vote - TS MKS Data Security July 2021

Document type	Related content	Document date	Expected action
Project / Draft		2021-07-19	**INFO**

Description

Dear members of CEN/TC 33/WG 4,

The draft for CEN/TS *Building Hardware — Masterkey System Data Protection — Guidance* has now been sent to the secretariat of CEN/TC 33 to be sent out for voting.

Best regards,

The secretariat of CEN/TC 33/WG 4 Building hardware

Åse Lyngstad, Secretary Support

CEN/TC 33

Date: 2021-07-14

prTS XXXXX: XXXX

Secretariat: AFNOR

Building Hardware — Masterkey System Data Protection — Guidance

Baubeschläge — Haupt-Element — Ergänzendes Element

Quincaillerie pour le bâtiment — Élément central — Élément complémentaire

ICS: 91.190

CCMC will prepare and attach the official title page.

Contents

Page

European foreword 3
Introduction 4
1 Scope 5
2 Normative references 5
3 Terms and definitions 5
4 Characteristics and Requirements 6
4.1 Planning and ordering of Master Key Systems 6
4.2 Transmission of Master Key Systems Lock Charts 6
4.3 General Data Handling Requirements 6
4.4 Calculation of Master Key Systems 6
4.5 Manufacturing of Master Key Systems 7
4.6 Preparation of Keys belonging to Master Key Systems 7
4.7 Shipment of Master Key System Cylinders and Keys 7
4.8 Installation of Master Key Systems 7
4.9 Management of Master Key System related Data during Systems' lifetime 7
5 Verification 8
5.1 Planning and ordering of Master Key Systems 8
5.2 Transmission of Master Key Systems Lock Charts 8
5.3 General Data Handling Requirements 8
5.4 Calculation of Master Key Systems 9
5.5 Manufacturing of Master Key Systems 9
5.6 Preparation of Keys belonging to Master Key Systems 9
5.7 Shipment of Master Key System Cylinders and Keys 9
5.8 Installation of Master Key Systems 9
5.9 Management of Master Key System related Data during Systems' lifetime 9
Bibliography 10

European foreword

This document (prTS XXXX:XXXX) has been prepared by Technical Committee CEN/TC 33 "'Doors, windows, shutters, building hardware and curtain walling", the secretariat of which is held by AFNOR.

This document is currently submitted to the CEN Enquiry.

No European Standard or Technical Specification is superseded.

Introduction

TS XXXX:XXXX Technical Specification for Masterkey System Data Protection has been prepared to provide guidance for the handling of data that is used in the design, manufacture, supply, installation and maintenance of master key systems, constructed from mechanical cylinder locks. This document provides guidance to working methods and aims to promote this as best practice.

This document has two main sections: Section 4.0 Requirements and Classification containing the process of handling data from design through to system maintenance and Section 5.0 Verification providing methods of best practice to ensure compliance with this specification.

It is recommended that any company claiming compliance with this technical specification, carries out 3rd party certification of the processes used for masterkey systems that are provided in accordance with this document. The process of supplying a masterkey system may be provided by multiple parties within the supply chain, therefore it is important that manufacturers and suppliers clearly indicate to which areas of this technical standard they claim compliance.

1 Scope

This document specifies requirements and procedures to achieve and maintain protection of data and sensitive information related to mechanical Master Key Systems and other mechanical key systems where customer or application related data is being processed throughout the process of planning, production, installation, and maintenance.

The requirements and test methods for mechanical cylinder locks is covered by EN 1303.

Reference shall be made to EN 1303 and Annexes relating to Master Key Systems (MKS).

Requirements relating to the information security of key based and non-key based electronic cylinders are covered by EN ISO/IEC 27001.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

EN 1303:2015 *Building Hardware – Cylinders for Locks – Requirements and Test Methods*

3 Terms and definitions

For the purposes of this document, the following terms and definitions and the terms and definitions given in EN 1303:2015 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1

Master Key System

MKS

combination of lock cylinders and related keys with different codings and/or profiles which are in functional relation

3.2

MKS/cylinder manufacturer

company who is owning the design of the cylinders and supplies either the assembled cylinders or components for assembly of cylinders

4 Characteristics & Requirements

4.1 Planning and ordering of Master Key Systems

Data to calculate and produce a Master Key System always must be provided without personal data/information related to the individual key holders. Therefore, key plans, org charts or any other documents/information provided to plan a system shall always be created without showing any personal data (e.g. name, function, employee no., etc.).

Key marking shall avoid any obvious reference to its function, the location of the door and/or key holder.

Suitable processes and security arrangements shall be established to ensure that orders for Master Key System keys and cylinders can be placed by authorized persons only.

4.2 Transmission of Master Key Systems lock charts

Electronic transmission of lock charts shall use state of the art encrypted communication such as:

- MKS manufacturers' planning and ordering software with data encryption
- Third party planning and ordering software with data encryption (software shall meet data protection and functional requirements as specified by MKS manufacturer)
- E-mail systems with encryption function enabled
- In cases where hard copy lock charts are required transfer shall be via registered mail or trackable courier service.

4.3 General data handling requirements

Access management for secure server rooms and/or secure archives with paper files and/or security cards or other media used for identification shall be in place.

Storage of electronic data shall be in a secure file system or secure database environment.

Daily backup files shall be created and protected.

A matrix of roles and access permissions shall be defined and continuously reviewed to maintain security procedures.

Persons with access to MKS calculation software and/or data shall be security screened/checked (e.g. criminal record) and be conversant with data protection requirements.

4.4 Calculation of Master Key Systems

Calculation of MKS shall be done using a calculation software tool which is either provided by the cylinder manufacturer (design owner) or third-party calculation software that has been approved by the cylinder manufacturer.

MKS calculations shall be in full accordance with the specific rules defined by the cylinder manufacturers.

4.5 Manufacturing of Master Key Systems

Access to production/assembly area shall be restricted to authorised persons only.

Access to assembly related paperwork or data shall be restricted to authorised persons only. After use, the assembly related paperwork or data shall be destroyed / deleted or stored in a secure environment.

Test keys and incorrectly produced keys shall be destroyed or kept in a secure environment without direct reference to the location at which the MKS is installed.

The MKS manufacturing data set shall not provide any reference to the location at which the MKS is installed.

4.6 Preparation of keys belonging to Master Key Systems

Access to key cutting machines shall be controlled and limited to authorised persons only.

Key blanks shall be stored in a secure and access-controlled environment.

Records about key blank inventory, covering cut keys, miss-cut keys and disposed keys shall be kept.

4.7 Shipment of Master Key System cylinders and keys

Security cards or other media used for identification as well as master keys shall be sent in sealed tamper-proof and non-transparent envelopes/enclosures.

It shall be agreed between the manufacturer and the customer whether the security card or other media used for identification and/or the master keys shall be included in MKS shipments or sent separately.

Shipment of MKS, either complete or in part (cylinders and/or keys), shall always be made by registered mail or trackable courier service.

4.8 Installation of Master Key Systems

A hand-over audit shall be conducted to ensure that all parts supplied and installed match with the order. The installer shall ensure that only authorised persons have access to cylinders and keys during installation.

It shall be ensured that keys are not left in the doors after installation of cylinders.

Information about maintenance and service requirements shall be provided to end-users in order to maintain the quality and security performance of the system.

Hand-over of security cards or other media used for identification, master keys and regular keys shall be signed off by end-users' authorised persons.

4.9 Management of Master Key System related data during system's lifetime

For an MKS produced and installed all information in relation to system changes and/or extensions, replacement cylinders, re-codings, deleted cylinders, additional keys, deleted keys, system compromises as well as any other relevant information shall be recorded.

The individual MKS log shall include information about persons involved in the different activities and the documentation of any activities described above.

The purpose of security cards is to identify the MKS and to authorise re-ordering of cylinders and keys or key copies. Manufacturers and distributors shall keep records of card issuance, including new system cards, additional cards, replacement cards and lost cards.

5 Verification

5.1 Planning and ordering of Master Key Systems

- No personal data related to end users/key holders (e.g. name, function, employee number) shall be included in any key plans, org charts or other physical or electronic documents related to a Master Key System.

- No obvious reference to the function of the key, the location of the door and/or key holders is allowed on the key.

- Proof of access restriction to authorized personnel to planning and ordering tools.

5.2 Transmission of Master Key System lock charts

- Planning tools shall use 128 Bit AES or similar encryption technology or higher for transmission of data. Third party planning and ordering tools shall be approved by the MKS manufacturer. E-mails or other electronic files containing MKS related data shall be transmitted with encryption function enabled.
- MKS related printed documents shall be transferred via registered mail or trackable courier service only.

5.3 General data handling requirements

- Physical access management for server rooms and archives shall be in place
- Storage of electronic data shall be in a secure file system or secure database environment, requiring a security protocol for access
- Backup files shall be stored on secure servers or storage media requiring a security protocol for access.
- An up-to-date list of persons with access to MKS related data and their access rights shall be available.
- Where local laws allow, records of security checks (e.g. criminal records) of persons with access to MKS related data shall be maintained and available.

5.4 Calculation of Master Key Systems

- Calculation tools in use shall be provided by MKS manufacturer or in case third party software is in use, shall be approved by the MKS manufacturer.

5.5 Manufacturing of Master Key Systems

- Production/assembly areas shall be restricted to authorized persons. Physical access control systems shall be in place. A list of authorized persons will be available.
- Access to planning/assembly related paperwork shall be restricted to authorized persons. Paperwork shall be destroyed after use or stored in a secure access-controlled area.
- A procedure for the destruction of test keys and incorrectly produced keys shall be available. Alternatively, such keys shall be stored in a secure, access-controlled environment without direct reference to the Master Key System or location of the system's installation.
- Manufacturing documentation of individual Master Key Systems shall be free from any reference to the user and location where the Master Key System is installed.

5.6 Preparation of keys belonging to Master Key Systems

- Access to key cutting machines shall be restricted to authorized persons. Physical access control systems shall be in place with a list of authorized persons to be maintained.
- Key blanks shall be stored in a secure and access-controlled environment with access restricted to authorized persons. Physical access control systems shall be in place with a list of authorized persons to be maintained.
- Records about key blank inventory, covering cut keys, incorrectly produced keys and disposed keys shall be available and stored in a secure and access-controlled environment with access restricted to authorized persons. Physical access control systems shall be in place with a list of authorized persons to be maintained.

5.7 Shipment of Master Key System cylinders and keys

- Security cards or other media used for identification as well as master keys shall be sent in sealed tamper-proof and non-transparent envelopes/enclosures.
- The preferred shipment method of security cards, other identification media and master keys including whether they are sent with MKS cylinders or sent on a separate shipment shall be documented and available.
- Documentation of shipments showing that MKS cylinders and keys, security cards, identification media and master keys were sent with registered mail, or a trackable courier service shall be available.

5.8 Installation of Master Key Systems

- Hand-over documentation signed-off by the customer, listing all cylinders, keys, security cards and other system authentication media, maintenance, service requirements and relevant documentation (in line with the MKS order) which were supplied to the customer's authorized persons shall be available.
- It shall be confirmed that Master Key Systems (cylinders, keys, key cards, installation plans etc.) have been stored in an area restricted to authorized persons before installation on site.
- An installation log which includes the delivery and installer of the MKS including cylinders and keys at the installation site shall be available.
- It shall be confirmed that any MKS related documentation is stored in a physical access-controlled environment with access restricted to authorized persons only. A list of authorized persons and an access log shall be available.

5.9 Management of Master Key System related data during system's lifetime

- Complete documentation for any active Master Key System shall be available at the company maintaining that system. The documentation includes information about changes/extensions to the structure of the system, replacement cylinders, re-codings, deleted cylinders, additional keys, deleted keys, lost keys, known system compromises and any other MKS data relevant information.
- A system maintenance log shall be kept which includes information about persons involved in the different activities.
- All documentation related to the maintenance of an active Master Key System shall be stored in a secure physical access-controlled environment with access to authorized persons only.

Bibliography

<std>[1] EN ISO/IEC 27001:2013 *Information technology — Security techniques — Information security management systems — Requirements*

</std>