SSF 1075

NORM FOR

DISTRIBUTION, STORAGE AND USE OF DIGITAL KEYS

CLASSIFICATION, DEMANDS AND EVALUATION

MARCH 2020

SSF 1075 Edition 2

SSF
Stöldskyddsföreningen

SSF (the Swedish Theft Prevention Association) is a non-profit association. The aim of the association is to promote safety and security for individuals and property through crime prevention measures, and to help shape opinions and disseminate information with regard to crime prevention. (Excerpt from SSF's by-laws § 1 and § 2. Laid down on May 13, 2011)

SSF, the Swedish Theft Prevention Association, develops and specifies noms for testing and classification within areas considered relevant to the aims of the association.

A list of current SSF norms can be found on the SSF website at www.stoldskyddsforeningen.se

INNEHÅLL

Foreword

SSF's regulations specify properties that are considered to be of importance for functionality and reliability. The aim of the regulations is to stipulate quality and security levels that can be applied generally, both when specifying demands and in conjunction with the procurement of burglar-resistant products or structures.

The regulations refer to, or wherever possible are based on, national and international standards and other applicable technical specifications or international standards.

Application is voluntary unless agreed otherwise.

In addition to the demands specified in the standards and regulations, compliance with laws and official regulations is assumed.

Stockholm, Mars 2020.

Changes in relation to SSF 1075 Edition 1:

- Definitions for AES and MAC added
- General change of cryptographic key length in table 2, 4 and 6 ≥200 bits to ≥ 128 bits and ≥100 bits to ≥128 bits
- changes of demands for integrity checking 16-bits CRC to 16 respective 64 bits in table 2 and 6
- text changed in table 2
- Informative Annex B added – Examples of classification and connection between different SSF norms

This norm, SSF 1075 Edition 2, applies from 2020-04-06 and replaces SSF 1075 Edition 1 which is withdrawn on 2020-10-06.

1 Scope

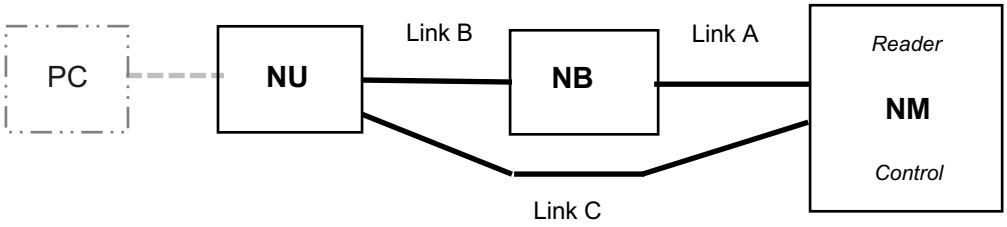
This standard describes systems for the distribution and storage of digital keys for authorizing lock operation.

This standard includes classification, demands and evaluation methods for components and/or systems.

Compliance with other regulations is required, in addition to the demands in this standard.

Statutes or regulations take precedence in the event of any conflict.

Basic system model:



Figur 1: Basic model.

NU = Key issuer
NB = Key carrier
NM = Key recipient (reading and evaluation device)

Note. Systems can be divided into more units than are shown in the illustration, and the demands for each part must be applied

Annex C provides two examples of application.

2 References

These regulations contain dated or undated references to regulations in other publications. These normative references can be found in the body copy.
The publications are listed below. With regard to dated references to publications that have subsequently been amended or supplemented, such amendments and supplements are only valid if they have been inserted into these regulations. For undated references, the latest edition of the publication applies.

SSF 3522 edition 2	*Burglar resistant fixed mounted lock units – Classification, demands and testing*
SSF 3523 edition 1	*Digital locking device – Classification, requirements and test methods*
SSF 200 edition 5	*Rules for burglar resistance - Buildings and premises*