ESSA White Paper

Introduction to prEN 17646:2021

General Requirements of the New Standard for Distributed Systems
(Issue 0.1, 9th of July 2021)

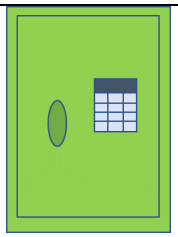
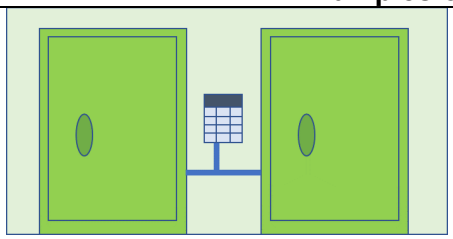
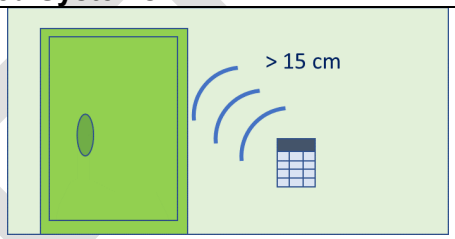
Caution: This ESSA-White Paper is based on a preliminary standard. The official standard is planned to be published in August 2022. Until then requirements will change.

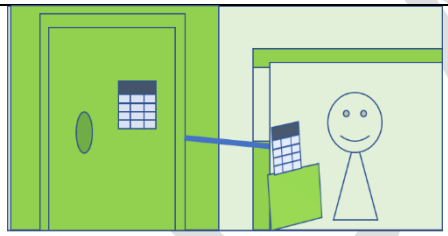
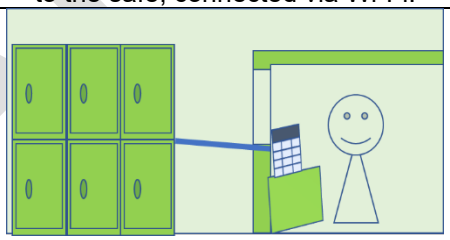
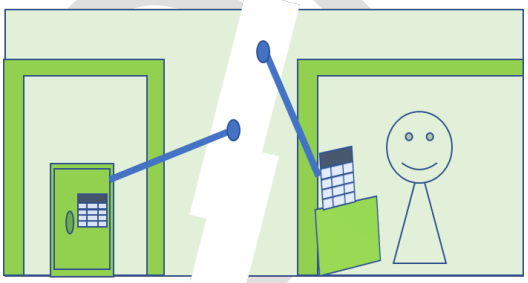
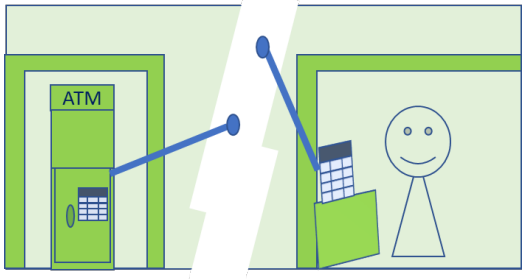
For ease of reading, no distinction is made in this document between the male and female form. If terms are listed only in male or female form, they refer equally to all genders.

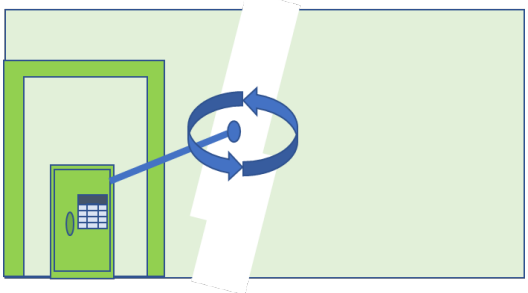
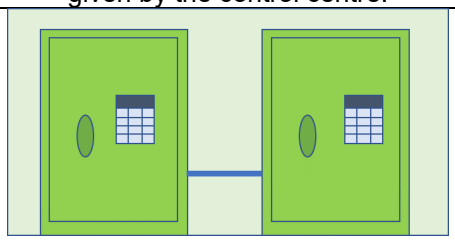
Content

1. Introduction

On 18 March 2021 the prEN 17646:2021 was published by CEN. It gives requirements on electronic safe locks, which have a connection to a system which is active outside of the safe ("Distributed System"). Examples are shown in the figures below:

<table>
<tr><th colspan="2">Not a Distributed System</th></tr>
<tr><td colspan="2"> 
Standard safe without any connection to the outside world.</td></tr>
<tr><th colspan="2">Examples of Distributed Systems</th></tr>
<tr><td> 
Two safes in one room, controlled by one input unit.</td><td> 

One safe controlled by an input unit not attached to the safe, connected via Wi-Fi.</td></tr>
<tr><td> 
Strongroom with a control room in which permission is given to open the door via separate input unit.</td><td> 
Weapon room in a police station. Access only permitted with additional permission from a control room.</td></tr>
<tr><td> 
Safe in bank A controlled in bank B.</td><td> 

ATM where access for the cash in transit company is only possible after permission is given by the control centre.</td></tr>
<tr><td> 
Safe with an update function via internet.</td><td> 
Safes connected to another. In case users change their code on one safe, the user code is automatically changed on the other safes.</td></tr>
</table>

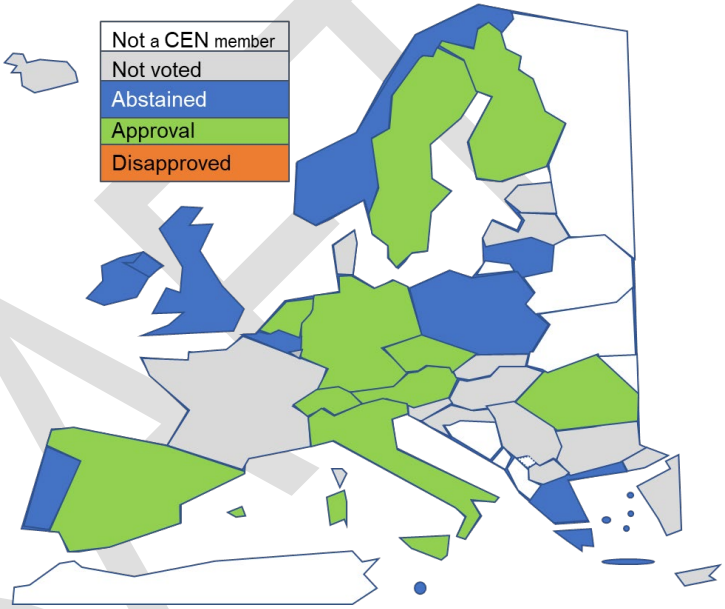
All of these examples (the components of a Distributed System are listed in clause 4) need security measures to prevent unauthorized access. The security requirements are set in the prEN 17646:2021.

On the basis of this document, ESSA members can inform themselves on this current standardization project and know which requirements future products according to the EN 17646:2022 **may** be tested to, when the standard is published in August 2022. Until August 2022 the requirements shown in this White Paper **will**, however, **change**. The validity of this White Paper is therefore only for the preliminary version of the standard.

This White Paper simplifies the requirements so that they are understandable to the general public and only shows a small percentage of the requirements in the document. Designers of a system should therefore purchase the prEN 17646:2021 or EN 17646:2022 for further reading.

2. Voting process

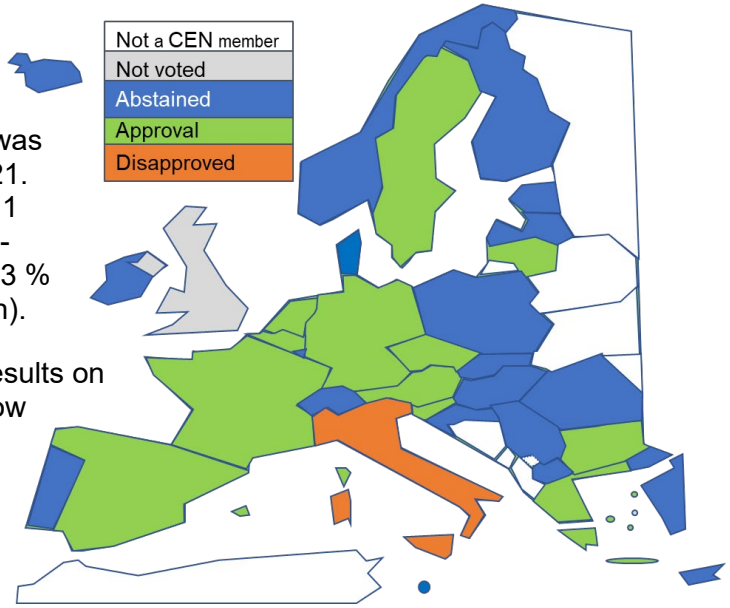
The voting procedure of European Standards has several steps. As a first step a "Work Item Vote" is held. Aim is to know whether a Standard on a certain topic should be created. For the EN 17646 this vote was held between 16 January and 16 March 2019. As 10 countries voted in favour and no country against, the Work Item was initiated.



The map on the right shows the voting results on the Work Item vote.

After the Work Item is created a Working Group (in this case the CEN/TC 263/ WG 3) creates requirements and discusses the standard until a majority of the participants assume that Europe would accept it.

The standard is then sent to CEN for translation and is given to the CEN members for voting. The voting procedure is quite complex on the one hand at least 55 % of the voting countries must accept the standard, in addition 65 % of the voting population must vote in favour.



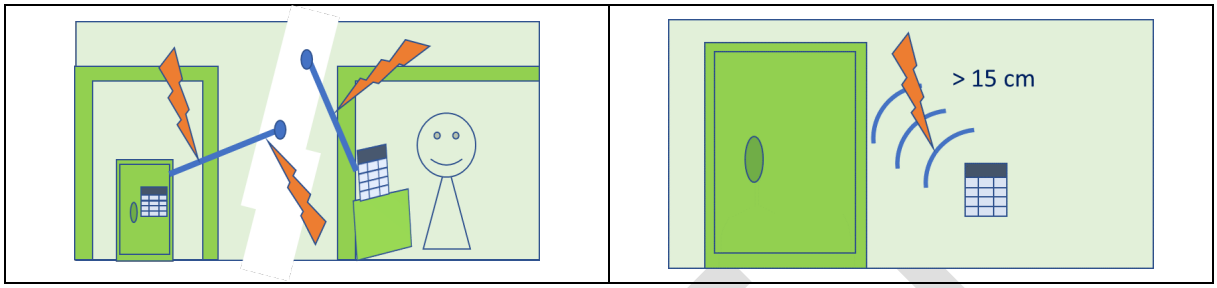
For the prEN 17646 this "CEN Enquiry" was held between 18 March and 10 June 2021. As 12 countries voted in favour and only 1 country against, the outcome of the CEN-Enquiry was positive (approval rating 92.3 % of members and 82.2 % of the population).

The map on the right shows the voting results on the CEN-Enquiry. The Working Group now has the task to discuss each received comment and write an update proposal. This proposal will then again be sent to CEN for the "Formal Vote". This vote is planned to take part in Spring 2022.

3. How the Standard protects against attacks

3.1. Secure communication

In contrast to a traditional safe lock, the communication between input unit and locking device does not exclusively take place inside of the secure storage unit (safe, secure cabinet, deposit system, ATM safe, strongroom etc.). This means that for Distributed Systems the communication which takes place outside of the unit could be attackable via special sniffing tools.



To prevent such sniffing tools from reading the communication between the safe and the input unit, it is important that information, which is sent via the Distributed System is not readable. This is achieved by encrypting the information before sending it to the safe. The safe afterwards decrypts the information and performs the tasks, which the authorized person at the input unit commands.

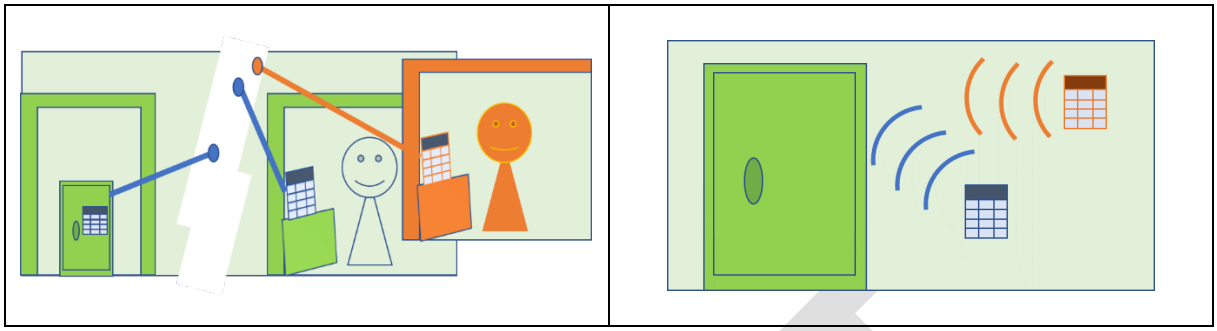
A sniffer can now only "sniff" not understandable information, which is therefore not directly usable for an attacker.

For this the prEN 17646 requires state of the art encryption modules which are approved by institutes such as the American NIST or the German BSI.

EN 1300 Comparison 1 Requirements on encryption	Distributed Systems of EN 1300 also require an encryption, however, with three main differences to the current prEN 17646: • The EN 1300 only required that "security relevant information" must be encrypted, in contrast the prEN 17646 requires that **any** information sent outside of the secure storage unit must be encrypted. • The EN 1300 gave a specific reference to which encryption algorithm shall be used (Triple DES or AES 128). The prEN 17646 only accepts algorithms which are currently approved by NIST, BSI etc. Currently AES 128 is accepted by both bodies. Therefore, there is currently no difference regarding to the AES requirement, but there may be a difference in the future. • In the EN 1300 it was possible for the manufacturer to create the encryption software themself or use any IT component, which can perform an encryption according to the standard. According to prEN 17646 the software and/**or** IT components must be approved by NIST or BSI.

3.2. Authenticity

In a Distributed System the safe lock does not need to be directly attached to the safe. Therefore, it must be prevented that a burglar simulates an authorized opening by using an own input unit, which the burglar connects to the network.



To prevent such attacks, the prEN 17646 requires that the components authenticate another beforehand, to prove that the incoming data is from a trusted source.

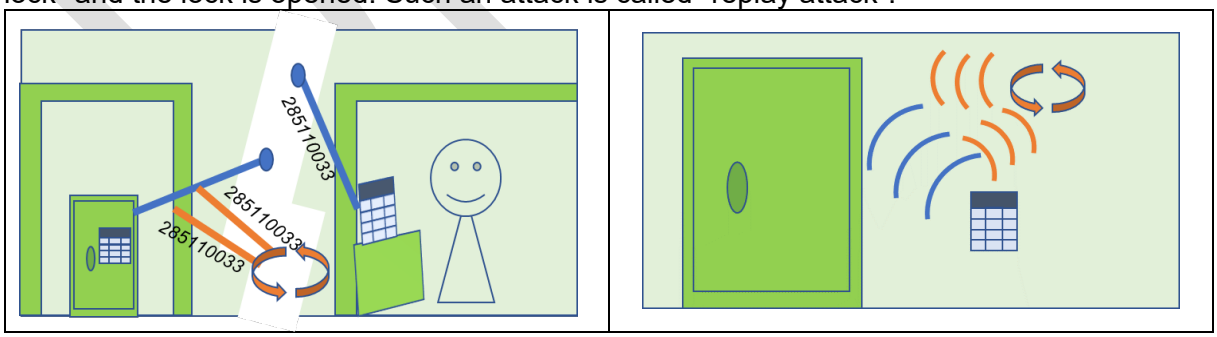
It is required that the authentication methods correspond to the state of the art.

EN 1300 Comparison 2 Authentication	Distributed systems of EN 1300 also require authentication, however, it only requires that the components must use authentication, it did not refer to "state of the art".

3.3. Integrity

Due to encryption, it may not be possible to understand the data which is sent encrypted to the safe. However, this does not mean, that the communication cannot be attacked.

Example:
The command "open the lock" is encrypted to 285110033 and sent to the lock. A sniffing tool could read and store 285110033 without knowing the content behind it. One hour later the sniffing tool could send 285110033 to the lock. The lock decrypts 285110033 to "open the lock" and the lock is opened. Such an attack is called "replay attack".

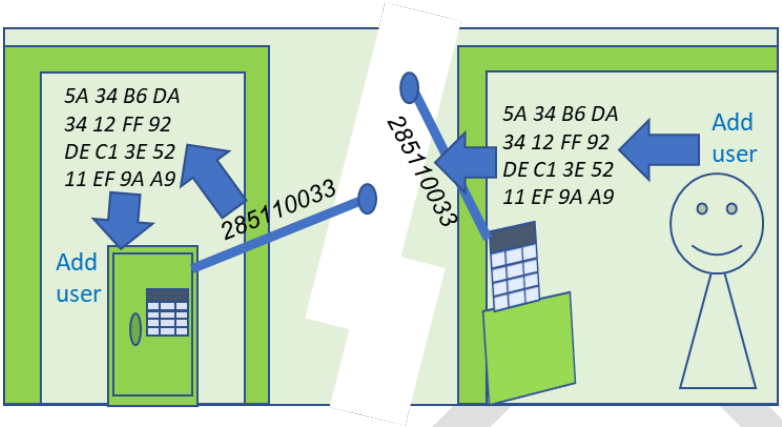


To prevent "replay attacks" and other integrity specific methods, the prEN 17646 requires using integrity mechanisms. It is required that the integrity methods correspond to the state of the art and prevent modification, deletion, addition or repeated input.

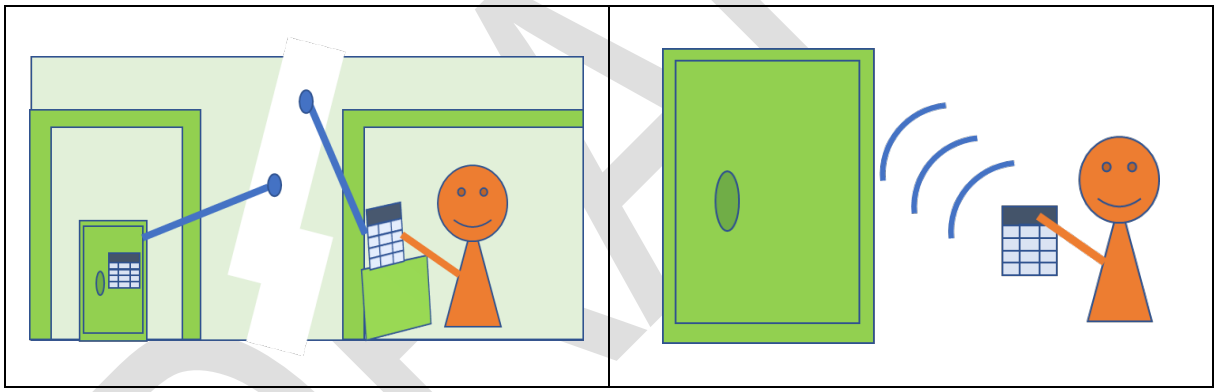
EN 1300 Comparison 3 Integrity	Where the prEN 17646 only states that the mechanisms shall be state of the art, the EN 1300 also gave a few examples on which mechanisms could be used (for instance MAC algorithms). The EN 1300 does not explicitly require that the integrity measures shall prevent replay attacks, but indirectly the paragraph could be read as such.

3.4. Protection of the cryptographic key

To encrypt information, it is necessary to use a "cryptographic key" which changes the information from readable to not readable and also from not readable to readable. This cryptographic key is usually a code in HEX format, for a 128 Bit encryption for instance: *5A 34 B6 DA 34 12 FF 92 DE C1 3E 52 11 EF 9A A9*.



If an attacker would be able to get access to this cryptographic key or a former employee would still know the cryptographic key, the information could be decrypted by an unauthorized person.



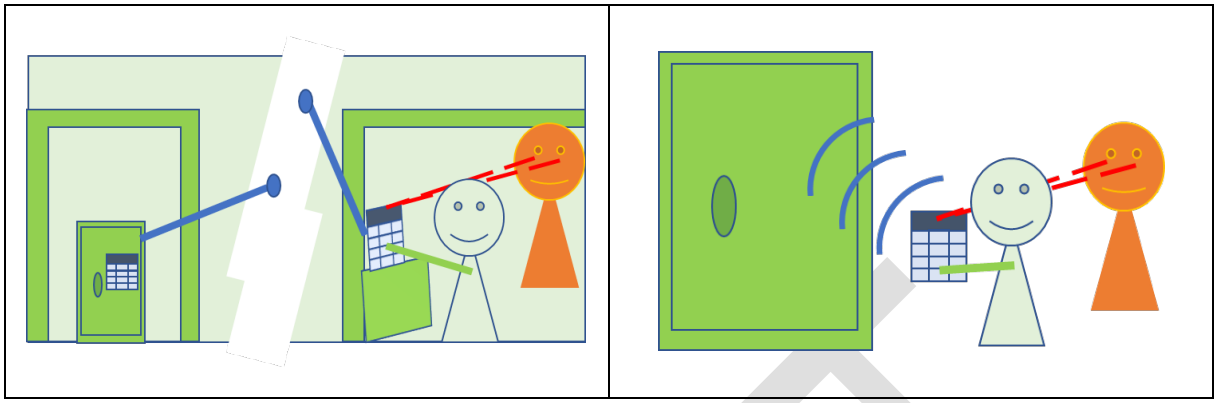
To prevent such attacks, the prEN 17646 requires the cryptographic key to be stored in such a way that it is not readable. In case of an access of authorized users to the key for class C and D a two-factor authentication is required in addition (two different coding means must be entered to get access to the key).

To prevent former employees using the cryptographic keys in the future it is required that it must be possible to change the cryptographic key in the system. Changing the cryptographic key regularly also improves the overall security of the system, as it hampers brute forces attacks on the key, cryptanalysis etc.

EN 1300 Comparison 4 Cryptographic key	The requirements are nearly identical to the EN 1300 but are written more precisely in the prEN 17646. Furthermore, a two-factor authentication was not required to read the cryptographic key for the classes C and D in the EN 1300. However, the EN 1300 has higher requirements for protecting the key inside of a remote input unit (using physical security level 3 of FIPS PUB 140-2:2002).

3.5. Code Spying

A rather simple method of attacking a system is spying the code information when this information is entered ("shoulder surfing").

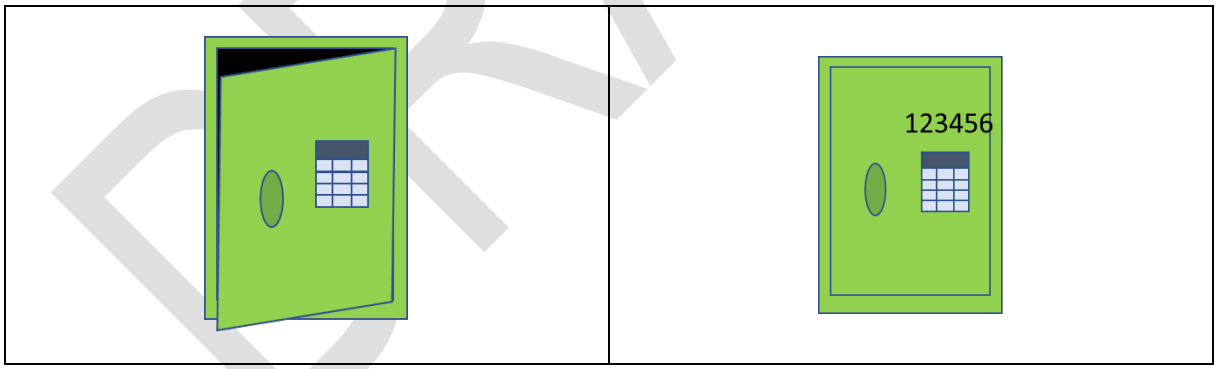


prEN 17646 therefore requires that in an angle of 30° around the screen as well as the keyboard the information on a distributed input unit is not readable.

EN 1300 Comparison 5 Spying resistance	The EN 1300 also requires that for **distributed** input units the information shall not be readable for **all** the classes, however, with these two differences: • The EN 1300 does not directly state that it shall be from the screen **and** the keyboard. • The EN 1300 requires a screen protection to the right and left but not to the top and bottom.

3.6. Security issues regarding usage

Sometimes not the IT-security is the weak point of a system, but the user.



prEN 17646 therefore requires that in case the lock did not close correctly (for instance due to a jammed boltwork) the input unit shall give an indication, that the lock is still unlocked.

In addition, if user codes are automatically generated by the system these shall not be simply guessable.

EN 1300 Comparison 6 User errors	**Closure of the lock** In the EN 1300 for classes A, B and C it is sufficient, if the locked status can be checked in other ways, for instance by turning a handle. For classes D the same requirement as in prEN 17646 is required. **Simple Codes** Simple code usage is also not permitted in EN 1300. The application "generation of codes" was, however, not directly stated.

3.7. Internal fraud

In case of internal fraud it is important to have audit entries, which indicate what tasks the users performed on the system or when which user opened a safe. For this the prEN 17646 requires that the last 9000 events are stored.

EN 1300 Comparison 7 Auditing	The EN 1300 requires audit entries only for class B (last 10 openings + last firmware updates), C (last 50 openings + 3 last firmware updates) and D (last 500 openings+ 5 last firmware updates), where the prEN 17646 requires to have 9000 events for **all** classes for each locking device. The EN 1300 concentrates on the storage of opening events, the prEN 17646 requires that also other events, like configuration events, setting of time delays etc. must be stored including the time the event was initiated by which user.

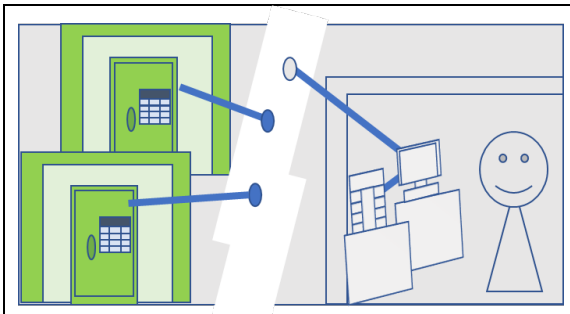
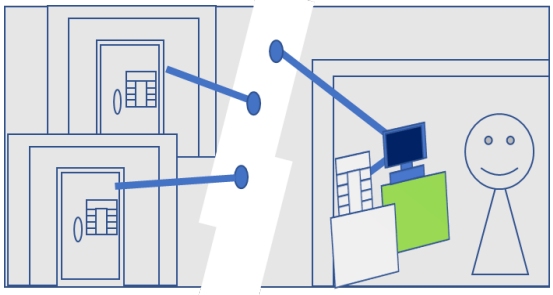
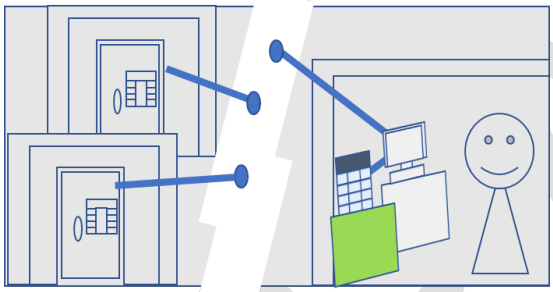
3.8. Firmware updates

As in normal locks, no security measure is perfect. Now and then new tools and attack methods are implemented, which could not be foreseen when designing a system. The prEN 17646 therefore requires that the locks used in a Distributed System must be updatable.

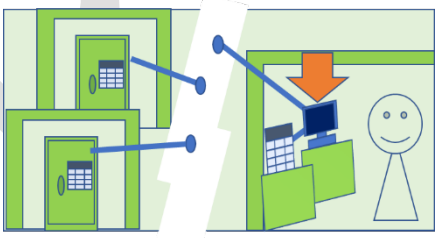
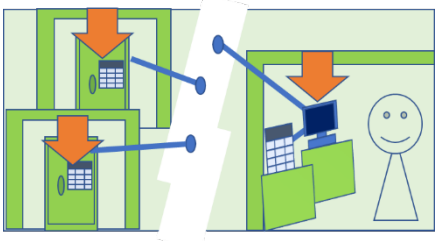
EN 1300 Comparison 8 Firmware	EN 1300 also includes requirements on how firmware updates shall be performed. However, the firmware update functionality is only an option in the EN 1300 and not a must.

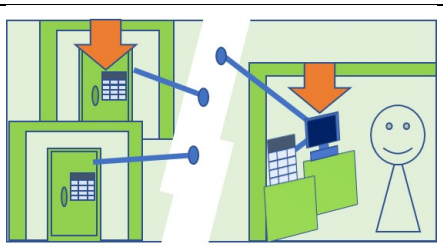
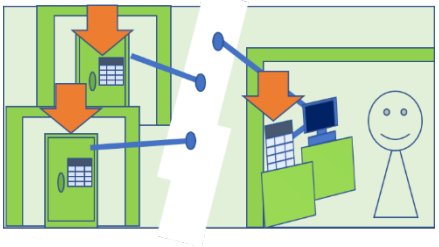
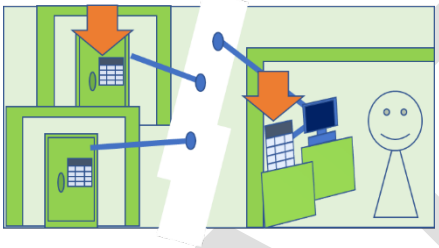
4. Which function is permitted where?

A Distributed System can be differentiated in three main components:

	Different secure storage units, which are connected to a Distributed System.
	A data processing unit DPU (for instance a PC) via which functions of the secure storage unit may be controlled or set.
	As PCs may be hackable, in addition, "remote input units" are required, where the code is entered.

Depending on the function, the prEN 17646 requires that certain tasks may be initiated from the DPU for all the secure storage units, where other need additional actions at different components:

What is permitted?	**Figure**	**Permitted for:**
All function may be performed on the DPU without any other actions.		• Checking audit entries • Changing holiday times • Setting an opening delay • Configuration tasks • etc.
May be initiated at the DPU but must be confirmed **in addition** on **every** secure storage unit by a deliberate action.		• Authentication of components • Configuring hardware during initial commissioning • Modifying after initial commissioning • Resetting the system to the condition as supplied

May be initiated at the DPU but must be confirmed **in addition** on **one single** secure storage unit for all other secure storage units.		• Activating new users • Initiating firmware updates
Code must be entered on a "remote input unit" but must be confirmed **in addition** on **every** secure storage unit.		• Opening the lock
Code must be entered on a "remote input unit" but must be confirmed **in addition** on **one single** secure storage unit for all other secure storage units.		• Changing the user code

About the author
This White Paper was written by the CEN/TC 263/WG 3 secretary Falko Adomat.

Falko Adomat organises the European standardization meetings for high security locks ("CEN/TC 263/WG 3) and was part of the Working Group creating the requirements for cryptography in the EN 1300 as well as the prEN 17646.

White Paper of the European Security Systems Association (ESSA) e. V.

Issue 0.1, 9th of July 2021

5. Bibliography

[1] CEN (2021, 04) prEN 17646:2021. *Secure storage units – Classification for high security locks according to their resistance to unauthorized opening – Distributed Systems*

[2] CEN (2018,12) EN 1300:2018. *Secure storage units – Classification for high security locks according to their resistance to unauthorized opening*

[3] NIST (2002,03) FIPS PUB 140-2:2002. *Security Requirements for Cryptographic Modules.*

6. Version history

Version 0.1 (9rh of July 2021)
Draft version, which was distributed to the ESSA members for review.