Definition of the Electronic-Key structure on an EKS Key

Contents

Components/modules used

EUCHNER

Description	Order no./item designation
EKM software	098578 / ANWPG ELECTRONIC KEY MANAGER, SINGLE 093322 / ANWPG ELECTRONIC KEY MANAGER
EKS Electronic-Key	077859 / EKS-A-K1RDWT32-EU 084735 / EKS-A-K1BKWT32-EU 091045 / EKS-A-K1BLWT32-EU 094839 / EKS-A-K1GNWT32-EU 094840 / EKS-A-K1YEWT32-EU

Tip: More information and downloads about the aforementioned EUCHNER products can be found at www.EUCHNER.de. Simply enter the order number in the search box.

Others

Description	Item
PC	Any Windows PC that meets the requirements in the EKM manual (093336)

Functional description

General

An Electronic-Key of the Electronic-Key-System EKS is a special industrial data carrier. It is supplied from the factory without data, except for a unique identifier (KeyID). A data structure must be created on the Electronic-Key before the EKS system is introduced. This structure must be the same for all machines and installations to be protected with an Electronic-Key. It is very difficult to change this structure later on, because it has to be changed in all machines and installations. Therefore, all conceivable access scenarios must be considered and reserves should always be created from the very beginning. Additions in the free ranges generally can be realized with relatively little effort.

Electronic-Key structure

The range from byte 0 to byte 115 on the Electronic-Key is freely available. An unchangeable KeyID is generally pre-programmed in bytes 116 to 124. This KeyID is different for each Electronic-Key and thereby makes every Electronic-Key unique.

Byte no.	Description	Type	Length	Explanation
0 - 115	-	-	-	Free range
116 - 123	KeyID	KeyID	8 bytes	The KeyID is a number that is permanently pre-programmed on the Electronic-Key by EUCHNER. This number is different for each Electronic-Key.

The Electronic-Key structure is also created in a database in the EKM and can be supplemented by additional data there.

Tip: EKS *Light* uses the data range from byte 110 on the Electronic-Key. If you plan to use a combination of EKS *Light* and EKS in a bus variant, leave the upper range from byte 110 free.

Basic considerations

To structure an Electronic-Key, it is best to begin with the largest unit that is to serve as the common unit for many applications. For most companies, this is surely an identifier that the Electronic-Key in question is a company Electronic-Key. This can be followed by an entire factory and then by a department, for example. However, it could be better in some circumstances to create an identifier across common tasks instead of across departments. This could be the work, for example. All welders would then be authorized to use the welding machines, and all lathe operators would have the rights to use the turning machines. Combinations of the various identifiers can also be used, of course. For example, only the lathe operators from department 1147 at the Leinfelden plant can work on certain machines, but not the lathe operators from department 4711.

It also must be borne in mind that one person could have several different authorizations on a single Electronic-Key. For example, one of the lathe operators from department 4711 can also perform welding work in department 4711, but the other one cannot. Consequently, the authorization for turning machines requires its own field and the authorization for welding applications requires a different one.

The next consideration to be made concerns how many of these “units” (departments and fields of activity, etc.) there are or how many units in total are to use the Electronic-Key. It is advisable to consider reserves as well. Thus, a word (16 bits) should be used instead of a byte (8 bits) if there are already 240 different units that have to be distinguished based on their numbers. In view of the total number, the reserve of only 15 units that can still be accommodated in a byte seems too small.

Another aspect to be considered is whether the data can be saved on the Electronic-Key as plain text or whether some type of encryption must be used. This is a very critical consideration, particularly in case of names and other personal data of Electronic-Key holders. One option offered by the EKM in this area is storage of the names in the database instead of on the Electronic-Key itself. These names can be made visible to only very few, authorized users. The EKM offers different access authorization levels to the database for this purpose. Access to the database can also be secured by an EKS Electronic-Key, of course. The unique KeyID can then serve as the identifier for the machines and installations. Only by conversion of the KeyID via the EKM database could it then be possible to determine the name or other data of the Electronic-Key holder if necessary. Such conversion can also be realized outside the EKM, of course.

A special data type offered by the EKM is the so-called KeyCRC. This is a checksum calculated over certain ranges of the Electronic-Key. The KeyID, i.e. the unique identifier, is generally included in the calculation of the KeyCRC. As a result, the checksum will differ for each Electronic-Key. The EKM writes this checksum to the assigned range of the Electronic-Key. For this purpose, it uses the definitions made when the database was created in the calculation. This naturally does not provide any protection on its own, because an Electronic-Key can be copied together with this checksum. However, since the calculation produces a different value for each Electronic-Key (due to the different KeyIDs), copy protection can function if the CRC is also calculated in the control system. If the calculation result differs from the value on the Electronic-Key, the control system will reject the Electronic-Key as invalid.

Instead of calculation, it is also possible to transfer all or some of the data from the database to the control systems by electronic means. The EKM provides the option of automatic file export in CSV format for this purpose. After export, the EKM can also prompt another program to process the data and thereby prepare them according to the desired restrictions and also transmit them directly to the control systems. This allows the CRC value to be stored in the control system, for example.

The export option described is also the key to another feature offered by the EKM. Electronic-Keys can be locked via the predefined “locked” field in the database. This field is used to lock lost Electronic-Keys. This field is not on the Electronic-Key itself, because an existing Electronic-Key typically does not have to be locked. It can simply be withdrawn or reprogrammed instead. Data transfer by means of a CSV file can also be used to transmit this locking code to the control systems automatically.

To help promote periodic training, EKM offers the option of writing a field of the type “date” on the Electronic-Key. This field can be monitored in a control system, and the Electronic-Key can become invalid automatically if the current date is newer than the date on the Electronic-Key. The date is updated only if the employee in question has taken a training course. Very many different date specifications can now become necessary if – for each authorization – an expiry date has to be stored in addition to the access level on the Electronic-Key. If this is necessary, the memory of the Electronic-Key will soon become too small. The only remedy in this case is to pursue a different approach or to store these data in the database itself.

Setting up the EKM software

Creating the database

The structure on the Electronic-Key can be stored in the EKM database. This informs the software about where to write the data. The same structure must be used in the control systems that are to evaluate the Electronic-Key. Here is a sample structure, which is also used for the other application examples. The application AP000169-2… describes how to create this database.

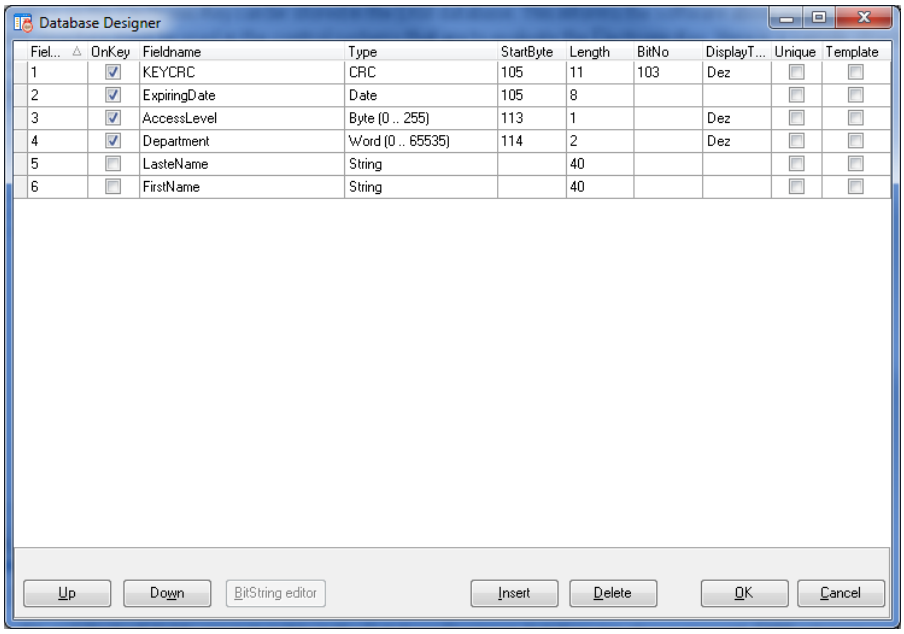

Figure 1

The “KeyID” and “locked” fields are not visible in the Database Designer, but they are always present. EKM autonomously creates them in the database, and it also creates the “KeyID” field on the Electronic-Key.

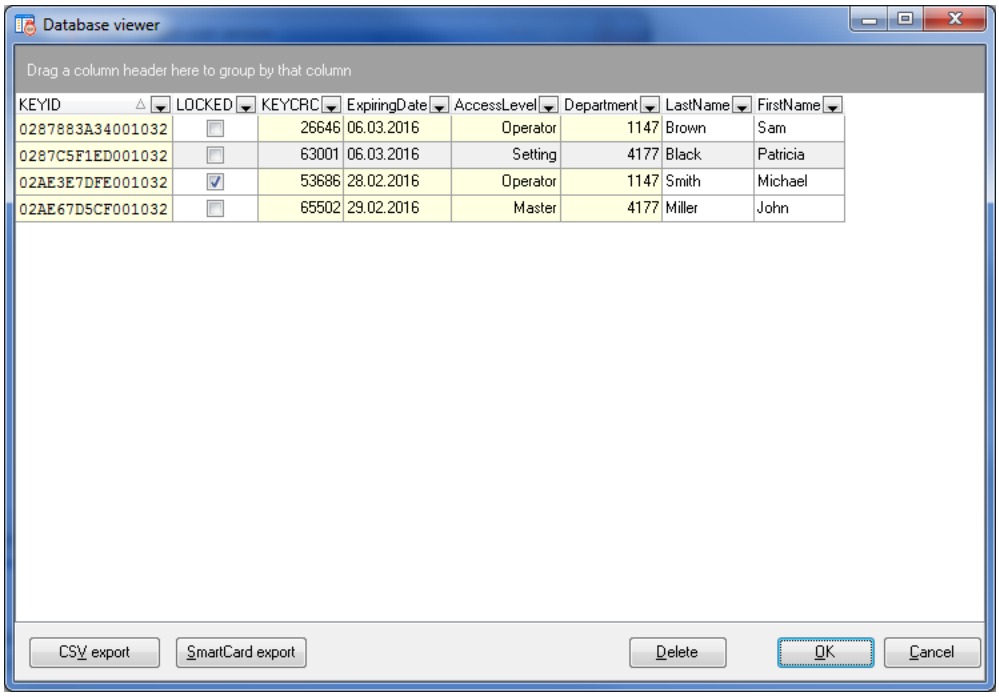

Figure 2

All fields and all Electronic-Keys are visible in the database viewer. The “locked” fields and the fields that are visible only in the database (but not on the Electronic-Key) can be changed here. In this example, the fields in question are the “first name” and “last name” fields.

Authorizations in the EKM

In very many cases, it is necessary not to display certain data fields for every employee. For example, the name typically falls under data privacy protection provisions and may be displayed only in certain, very specific circumstances. The EKM offers the option of using different authorizations for this purpose. These authorizations are administered via user groups. This allows the name to be displayed only to authorized persons, but not to the employee who assigns the authorization level, for example.

For this purpose, the EKM uses the option of assigning different EKM users to groups. These groups are given the authorization to see or change certain portions of the Electronic-Key or database content. Only the fields for which rights are assigned are then visible or editable. All other fields are not visible. It is important here to restrict the rights to view the entire database accordingly.

Figure 3 provides an example of what a screen for the users who administer the Electronic-Keys could look like. The menu item for the database viewer is missing in this case, because this right was not assigned.

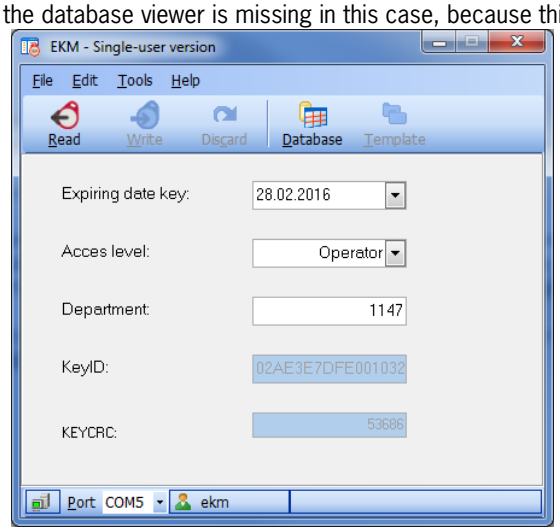

Figure 3

By contrast, a manager could view a screen like the one shown in Figure 4. The authorization level is unimportant here; the full name of the Electronic-Key holder is displayed instead.

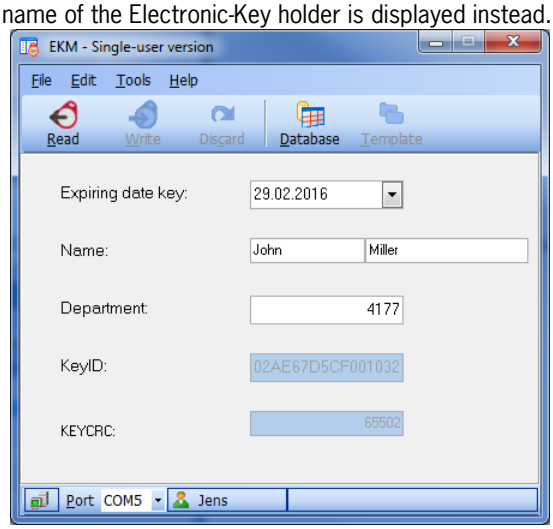

Figure 4

Both screens are excerpts from the same EKM application; only the logged-on user is different. The fields for the name and for the user rights were put in the same place in the layout.

Important note – please observe carefully!

This document is intended for a design engineer who possesses the requisite knowledge in safety engineering and knows the applicable standards, e.g. through training for qualification as a safety engineer. Only with the appropriate qualification is it possible to integrate the introduced example into a complete safety chain.

The example represents only part of a complete safety chain and does not fulfill any safety function on its own. In order to fulfill a safety function, the energy switch-off function for the hazard location and the software within the safety evaluation must also be considered, for example.

The introduced applications are only examples for solving certain safety tasks for protecting safety doors. The examples cannot be comprehensive due to the application-dependent and individual protection goals within a machine/installation.

If questions concerning this example remain open, please contact us directly.

In accordance with Machinery Directive 2006/42/EC, the design engineer of a machine or installation is obligated to perform a risk assessment and take measures to reduce the risk. When doing this, the engineer must comply with the applicable national and international standards. Standards generally represent the current state of the art. Therefore, the design engineer should continuously inform himself about changes in the standards and adapt his considerations to them. Relevant standards include EN ISO 13849 and EN 62061. This application must be regarded only as assistance for the considerations about safety measures.

The design engineer of a machine/installation is obligated to assess the safety technology itself. The examples must not be used for assessment, because only a small excerpt of a complete safety function was considered in terms of safety engineering here.

In order to be able to use the safety switch applications correctly on safety doors, it is indispensable to observe the standards EN ISO 13849-1, EN ISO 14119 and all relevant C-standards for the respective machine type. Under no circumstances does this document replace the engineer's own risk assessment, and it cannot serve as the basis for a fault assessment.

Particularly in case of fault exclusion, it must be noted that this can be performed only by the design engineer of a machine or installation and requires a reason. General fault exclusion is not possible. More information about fault exclusion can be found in EN ISO 13849-2.

Changes to products or within assemblies from third-party suppliers used in this example can lead to the function no longer being ensured or the safety assessment having to be adapted. In any event, the information in the operating instructions on the part of EUCHNER, as well as on the part of third-party suppliers, must be used as the basis before this application is integrated into an overall safety function. If contradictions should arise between the operating instructions and this document, please contact us directly.

Use of brand names and company names

All brand names and company names stated are the property of the related manufacturer. They are used only for the clear identification of compatible peripheral devices and operating environments in relation to our products.