

Definition der Schlüsselstruktur auf einem EKS-Schlüssel



Inhalt

Verwendete Bauteile / Module	2
EUCHNER	2
Andere.....	2
Funktionsbeschreibung	2
Allgemein	2
Schlüsselstruktur	2
Grundüberlegungen	3
Einrichten EKM Software	4
Datenbank anlegen	4
Berechtigungen im EKM.....	5
Wichtiger Hinweis – Bitte unbedingt sorgfältig beachten!.....	6

Verwendete Bauteile / Module

EUCHNER

Beschreibung	Best.-Nr. / Artikelbezeichnung
EKM Software	098578 / ANWPG ELECTRONIC KEY MANAGER EINZEL 093322 / ANWPG ELECTRONIC KEY MANAGER
EKS Schlüssel	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

Tipp: Weitere Informationen und Downloads zu den o.g. EUCHNER-Produkten finden Sie unter www.EUCHNER.de. Geben Sie einfach die Bestellnummer in die Suche ein.

Andere

Beschreibung	Artikel
PC	Beliebiger Windows PC entsprechend den Voraussetzungen im EKM Handbuch (093336)

Funktionsbeschreibung

Allgemein

Ein elektronischer Schlüssel des Electronic Key Systems EKS ist ein spezieller industrietauglicher Datenträger, der ab Werk keine Daten außer einer eindeutigen Kennzeichnung (KeyID) enthält. Vor Einführung des EKS Systems muss auf dem Schlüssel eine Datenstruktur geschaffen werden, die für alle Maschinen und Anlagen, die mit einem Schlüssel gesichert werden sollen, gleich ist. Da diese Struktur später nur mit großem Aufwand geändert werden kann, denn es muss in allen Maschinen und Anlagen geändert werden, müssen von Anfang an denkbare Zugangsszenarien bedacht werden und es sollten immer Reserven geschaffen werden. Ergänzungen in freien Bereichen lassen sich typisch mit relativ wenig Aufwand umsetzen.

Schlüsselstruktur

Auf dem Schlüssel steht der Bereich von Byte 0 bis Byte 115 zur freien Verfügung. In den Bytes 116 bis 124 ist generell eine KeyID bereits vorprogrammiert, die nicht geändert werden kann. Diese KeyID ist bei jedem Schlüssel individuell unterschiedlich und macht damit jeden Schlüssel zu einem Unikat.

Bytenr.	Beschreibung	Typ	Länge	Erläuterung
0 - 115	-	-	-	Freier Bereich
116 - 123	KeyID	KeyID	8 Byte	Die KeyID ist eine von EUCHNER fest programmierte Nummer auf dem Schlüssel. Diese Nummer ist bei jedem Schlüssel unterschiedlich.

Die Schlüsselstruktur wird auch in der Datenbank im EKM angelegt und kann hier um weitere Daten ergänzt werden.

Tipp: EKS *Light* nutzt den Datenbereich ab Byte 110 auf dem Schlüssel. Wenn Sie vorhaben, gemischt mit EKS *Light* und EKS in einer Busvariante zu arbeiten, lassen Sie den oberen Bereich ab Byte 110 frei.

Grundüberlegungen

Um einen Schlüssel zu strukturieren, geht man am besten so vor, dass man mit der größten Einheit beginnt, die als gemeinsame Einheit für viele Anwendungen dienen soll. Dies ist bei vielen Firmen sicherlich eine Kennung, dass es sich um einen Firmenschlüssel handelt. Anschließend kann bspw. ein ganzes Werk kommen und danach eine Abteilung. Unter Umständen ist es aber besser, über gemeinsame Aufgaben statt über Abteilungen hinweg eine Kennung anzulegen. Dies könnte z.B. die Tätigkeit sein. Dann hätten alle Schweißer die Berechtigung Schweißgeräte zu nutzen und alle Dreher die Berechtigung für die Drehmaschinen. Natürlich können auch Kombinationen aus den verschiedenen Kennungen verwendet werden. Beispielsweise dürfen nur Dreher der Abteilung 1147 im Werk Leinfeld an bestimmten Maschinen arbeiten, nicht dagegen die Dreher aus der Abteilung 4711.

Es muss auch bedacht werden, dass unter Umständen eine Person mit einem einzigen Schlüssel mehrere unterschiedliche Berechtigungen haben kann. Bspw. kann einer der Dreher der Abteilung 4711 auch Schweißaufgaben in der Abteilung 4711 übernehmen, der andere jedoch nicht. Daraus folgt dann, dass die Berechtigung für Drehmaschinen ein eigenes Feld benötigt und die für Schweißanwendungen ein anderes.

Die nächste Überlegung, die angestellt werden muss, ist die, wie viele verschiedene dieser „Einheiten“ (Abteilungen, Tätigkeitsfelder usw.) es gibt bzw. wie viele Einheiten insgesamt den Schlüssel nutzen sollen. Dabei ist es gut, Reserven mit zu bedenken. So sollte ein Word (16 Bit) anstelle eines Bytes (8 Bit) verwendet werden, wenn bereits 240 verschiedene Einheiten, die durch ihre Nummer unterschieden werden sollen, vorhanden sind. Die Reserve von nur 15 Einheiten, die in einem Byte noch untergebracht werden können, erscheint angesichts der Gesamtzahl zu gering.

Ein weiterer Aspekt ist, ob die Daten in Klartext auf dem Schlüssel stehen dürfen, oder ob eine Art Verschlüsselung genutzt werden muss. Insbesondere bei Namen und anderen persönlichen Daten von Schlüsselbesitzern, wird dies sehr kritisch gesehen. Eine Möglichkeit, die EKM hier anbietet, ist die, dass Namen in der Datenbank hinterlegt werden, aber nicht auf dem Schlüssel selbst. Diese Namen können für nur sehr wenig Berechtigte sichtbar gemacht werden. EKM bietet hierzu unterschiedliche Zugangsberechtigungen für die Datenbank an. Der Zugang zur Datenbank kann natürlich auch über EKS-Schlüssel gesichert werden. Als Kennung für die Maschinen und Anlagen kann dann die eindeutige KeyID dienen. Erst durch Umschlüsselung der KeyID über die EKM Datenbank könnte dann im Bedarfsfall der Name oder weitere Daten des Schlüsselbesitzers ermittelt werden. Natürlich kann eine solche Umschlüsselung auch außerhalb von EKM realisiert werden.

Einen besonderen Datentyp, den EKM anbietet ist die sogenannte KeyCRC. Hierbei handelt es sich um eine Prüfsumme, die über bestimmte Bereiche des Schlüssels berechnet wird. Generell wird dabei die KeyID, also die eindeutige Kennung, in die Berechnung der KeyCRC mit einbezogen. Das führt dann dazu, dass die Prüfsumme für jeden Schlüssel unterschiedlich wird. EKM schreibt diese Prüfsumme auf den zugewiesenen Bereich des Schlüssels. Es nutzt dazu die Definitionen, die in der Datenbankanlage gemacht wurden, um diese zu berechnen. Das alleine bietet natürlich noch keinen Schutz, denn ein Schlüssel kann mitsamt dieser Prüfsumme kopiert werden. Da jedoch die Berechnung für jeden Schlüssel einen anderen Wert ergibt (durch die unterschiedliche KeyID), kann der Kopierschutz greifen, wenn die Berechnung der CRC auch in der Steuerung erfolgt. Die Steuerung weist im Fall, dass die Berechnung einen anderen Wert ergibt als auf dem Schlüssel steht, den Schlüssel als ungültig zurück.

Anstelle der Berechnung besteht auch die Möglichkeit, die Daten ganz oder teilweise aus der Datenbank auf elektronischem Weg an die Steuerungen zu übertragen. Hierzu ist in EKM die Möglichkeit eines automatischen Dateixports im CSV Format vorgesehen. Zudem kann EKM im Anschluss an den Export auch gleich ein beliebiges Programm anstoßen, die Daten weiter zu verarbeiten und somit entsprechend den gewünschten Einschränkungen aufzubereiten und auch direkt an die Steuerungen zu übertragen. Damit kann dann bspw. der Wert der CRC in der Steuerung hinterlegt werden.

Die beschriebene Exportmöglichkeit ist auch der Schlüssel für ein weiteres Feature, das EKM bietet. Schlüssel können über das vordefinierte Feld „locked“ in der Datenbank gesperrt werden. Das Feld wird genutzt, um verloren gegangene Schlüssel zu sperren. Dieses Feld steht nicht auf dem Schlüssel selbst, da ein vorhandener Schlüssel ja typischerweise nicht gesperrt werden muss, er kann einfach eingezogen oder umprogrammiert werden. Um nun dieses Sperrkennzeichen automatisch an die Steuerungen zu übertragen, kann ebenfalls die Übertragung der Daten mittels CSV Datei genutzt werden.

Zur Unterstützung eines regelmäßigen Schulungswesens bietet EKM die Möglichkeit, ein Feld vom Typ Datum auf den Schlüssel zu schreiben. Dieses Feld kann in einer Steuerung überwacht werden und der Schlüssel kann automatisch ungültig werden, wenn das aktuelle Datum neuer als das auf dem Schlüssel ist. Das Datum wird nur erneuert, wenn der betreffende Mitarbeiter eine Schulung erhalten hat. Es können nun sehr viele verschiedene Datumsangaben notwendig sein, wenn für jede einzelne Berechtigung neben der Zugriffsstufe auch noch ein Verfallsdatum auf dem Schlüssel stehen muss. Falls das notwendig wird, ist der Speicher des Schlüssels schnell zu klein. Dann hilft es nur, entweder ein anderes Konzept zu verfolgen oder aber diese Daten in der Datenbank selbst zu führen.

Einrichten EKM Software

Datenbank anlegen

In der EKM Datenbank kann die Struktur auf dem Schlüssel hinterlegt werden. Dadurch weiß die Software, an welche Stelle die Daten zu schreiben sind. Dieselbe Struktur muss in den Steuerungen genutzt werden, die den Schlüssel auswerten sollen. Hier eine Beispielstruktur, die auch für die weiteren Applikationsbeispiele verwendet wird. In der Applikation AP000169-2... finden Sie eine Beschreibung, wie diese Datenbank angelegt wird.

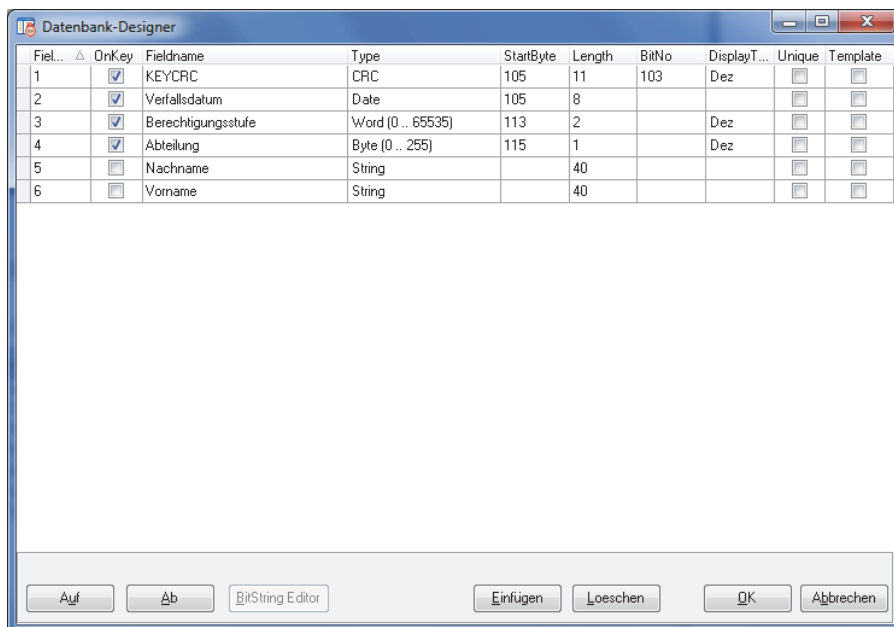


Bild 1

Im Datenbank Designer sind die Felder KeyID sowie „locked“ nicht sichtbar, jedoch immer vorhanden. Diese legt EKM in der Datenbank bzw. das Feld KeyID auch auf dem Schlüssel selbständig an.

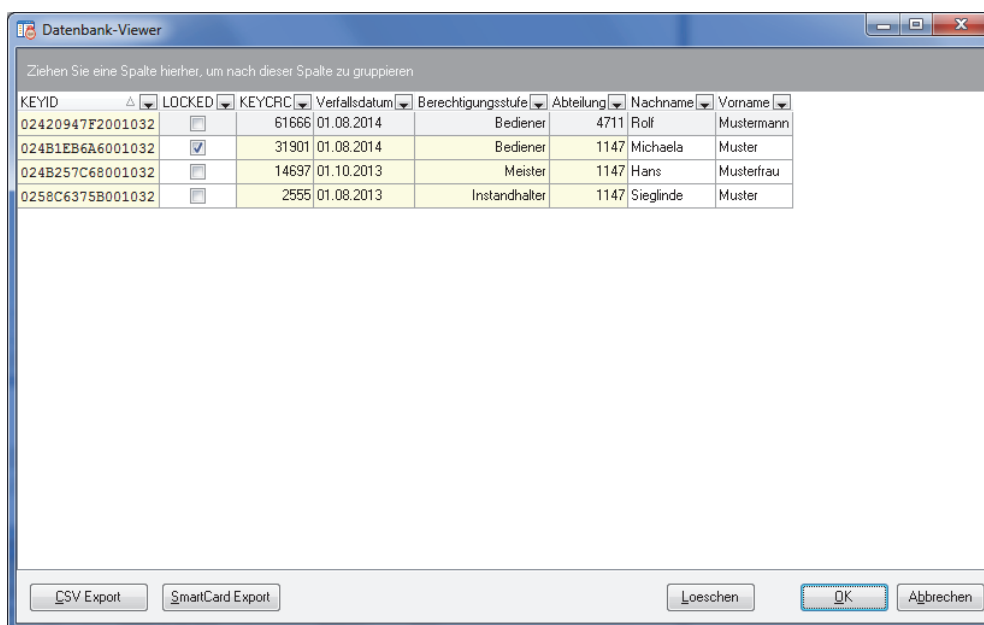


Bild 2

Im Datenbank Viewer sind alle Felder und alle Schlüssel sichtbar. Die Felder „locked“ und auch die Felder, die nur in der Datenbank, aber nicht auf dem Schlüssel sind, können hier geändert werden. Das sind in diesem Beispiel die Felder Vorname und Nachname.

Berechtigungen im EKM

Sehr oft ist es notwendig, bestimmte Datenfelder nicht für jeden Mitarbeiter anzuzeigen. Beispielsweise fällt der Name typischerweise unter Datenschutzbestimmungen und darf nur unter ganz bestimmten Umständen angezeigt werden. Hierzu bietet EKM die Möglichkeit unterschiedliche Berechtigungen zu nutzen. Diese Berechtigungen werden über Benutzergruppen verwaltet. Auf diese Weise ist es möglich, dass der Name nur von befugten Personen sichtbar gemacht werden kann, bspw. nicht aber von dem Mitarbeiter, der die Berechtigungsstufe vergibt.

EKM verwendet hierzu die Möglichkeit, dass die verschiedenen Nutzer von EKM in Gruppen eingeteilt werden. Diese Gruppen bekommen die Rechte, bestimmte Teile des Schlüssel- bzw. Datenbankinhalts zu sehen oder zu ändern. Nur die Felder, zu denen die Rechte vergeben werden, sind dann auch sichtbar bzw. änderbar. Alle anderen Felder sind nicht sichtbar. Wichtig ist dabei, dass auch die Rechte, die gesamte Datenbank zu sehen, entsprechend eingeschränkt werden.

Eine Maske für die Benutzer, die die Schlüssel verwalten sollen, könnte entsprechend Bild 3 gestaltet sein. Der Menüpunkt für den Datenbankviewer fehlt hier, da das Recht nicht zugeteilt wurde.

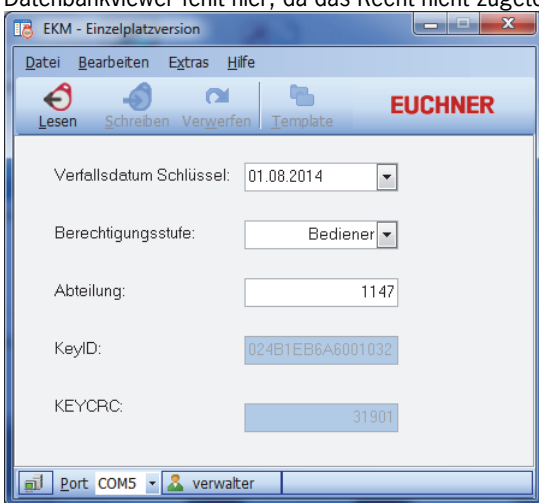


Bild 3

Dagegen kann ein Bild für jemanden mit Personalverantwortung wie in Bild 4 gezeigt aussehen. Die Berechtigungsstufe interessiert hier nicht, dafür wird jedoch der vollständige Name des Schlüsselbesitzers angezeigt.

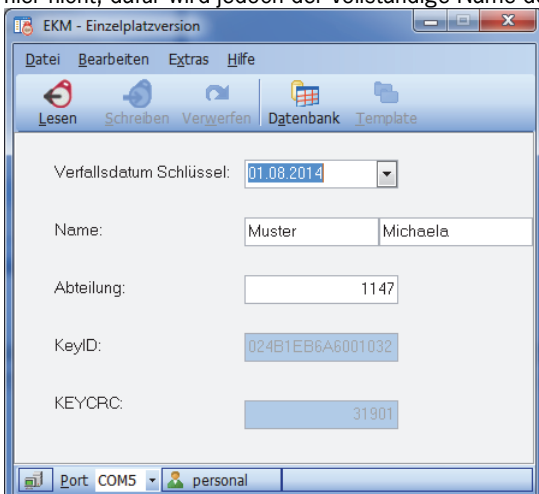


Bild 4

Beide Bilder sind Auszüge aus derselben EKM Anwendung, nur der angemeldete Nutzer ist unterschiedlich. Die Felder für Name und Benutzerrechte sind an derselben Stelle im Layout platziert worden.

Wichtiger Hinweis – Bitte unbedingt sorgfältig beachten!

Dieses Dokument richtet sich an einen Konstrukteur, der die entsprechenden Kenntnisse in der Sicherheitstechnik hat und die Kenntnis der einschlägigen Normen besitzt, z. B. durch eine Ausbildung zum Sicherheitsingenieur. Nur mit entsprechender Qualifikation kann das vorgestellte Beispiel in eine vollständige Sicherheitskette integriert werden.

Das Beispiel stellt nur einen Ausschnitt aus einer vollständigen Sicherheitskette dar und erfüllt für sich allein genommen keine Sicherheitsfunktion. Zur Erfüllung einer Sicherheitsfunktion muss beispielsweise zusätzlich die Abschaltung der Energie der Gefährdungsstelle sowie auch die Software innerhalb der Sicherheitsauswertung betrachtet werden.

Die vorgestellten Applikationen stellen lediglich Beispiele zur Lösung bestimmter Sicherheitsaufgaben zur Absicherung von Schutztüren dar. Bedingt durch applikationsabhängige und individuelle Schutzziele innerhalb einer Maschine/Anlage können die Beispiele nicht erschöpfend sein.

Falls Fragen zu diesem Beispiel offen bleiben, wenden Sie sich bitte direkt an uns.

Nach der Maschinenrichtlinie 2006/42/EG ist der Konstrukteur einer Maschine bzw. Anlage verpflichtet, eine Risikobeurteilung durchzuführen und Maßnahmen zur Minderung des Risikos zu ergreifen. Er muss sich hierbei an die einschlägigen nationalen und internationalen Sicherheitsnormen halten. Normen stellen in der Regel den aktuellen Stand der Technik dar. Der Konstrukteur sollte sich daher laufend über Änderungen in den Normen informieren und seine Überlegungen darauf abstimmen, relevant sind u.a. die EN ISO 13849 und EN 62061. Diese Applikation ist immer nur als Unterstützung für die Überlegungen zu Sicherheitsmaßnahmen zu sehen.

Der Konstrukteur einer Maschine/Anlage ist verpflichtet die Sicherheitstechnik selbst zu beurteilen. Die Beispiele dürfen nicht zu einer Beurteilung herangezogen werden, da hier nur ein kleiner Ausschnitt einer vollständigen Sicherheitsfunktion sicherheitstechnisch betrachtet wurde.

Um die Applikationen der Sicherheitsschalter an Schutztüren richtig einsetzen zu können, ist es unerlässlich, dass die Normen EN ISO 13849-1, EN ISO 14119 und alle relevanten C-Normen für den jeweiligen Maschinentyp beachtet werden. Dieses Dokument ersetzt keinesfalls eine eigene Risikoanalyse und kann auch nicht als Basis für eine Fehlerbeurteilung herangezogen werden.

Insbesondere bei einem Fehlerausschluss ist zu beachten, dass dieser nur vom Konstrukteur einer Maschine bzw. Anlage durchgeführt werden kann und dass hierzu eine Begründung notwendig ist. Ein genereller Fehlerausschluss ist nicht möglich. Nähere Auskünfte zum Fehlerausschluss gibt die EN ISO 13849-2.

Änderungen an Produkten oder innerhalb der Baugruppen von dritten Anbietern, die in diesem Beispiel verwendet werden, können dazu führen, dass die Funktion nicht mehr gewährleistet ist oder die sicherheitstechnische Beurteilung angepasst werden muss. In jedem Fall sind die Angaben in den Betriebsanleitungen sowohl seitens EUCHNER, als auch seitens der dritten Anbieter zugrunde zu legen, bevor diese Applikation in eine gesamte Sicherheitsfunktion integriert wird. Sollten hierbei Widersprüche zwischen Betriebsanleitungen und diesem Dokument auftreten, setzen Sie sich bitte mit uns direkt in Verbindung.

Verwendung von Marken- und Firmennamen

Alle aufgeführten Marken- und Firmennamen sind Eigentum des jeweiligen Herstellers. Deren Verwendung dient ausschließlich zur eindeutigen Identifikation kompatibler Peripheriegeräte und Betriebsumgebungen im Zusammenhang mit unseren Produkten.