sematicon
INDUSTRIAL IT SECURITY

designed
developed
made
in Germany

se.SAM™

sematicon.**S**ecurity and **A**uthentication **M**odules

Kryptographie-Werkzeuge und Sicherheitslösungen für Industrie und Elektronikentwicklung

sematicon

Das Unternehmen

Die **sematicon AG** ist ein Münchner Unternehmen mit Fokus auf Informationssicherheit und Kryptographie in Industrie, Elektronik sowie der IIoT-Welt.

Wir verbinden jahrzehntelange Erfahrung aus diesen Bereichen und eröffnen neue Horizonte, um dabei mit einem Dogma der IT-Branche zu brechen: **Sicherheit muss nicht immer kompliziert sein**. Benutzerfreundlichkeit und Systemsicherheit stehen bei uns an erster Stelle und schließen einander eben nicht aus.

Mit unserem spezialisierten und hoch motivierten Team stellen wir uns den aktuellen Herausforderungen der **Industrie 4.0**. Die von uns entwickelten Lösungen erlauben es, sicher auf Industrieanlagen zuzugreifen sowie die **Integrität**, **Authentizität** und **Sicherheit** der digitalen Daten und Prozesse zu gewährleisten. Unsere innovativen Lösungen sind bisher **einmalig am Markt**.

Daher sind wir Ihr zuverlässiger Partner bei allen Fragen zur sicheren Industrie 4.0„**Made in Germany**“.

IT-Sicherheit und die Kluft zwischen IT und Industrie

Die **digitale Transformation** bietet enorme neue Möglichkeiten der Vernetzung und Digitalisierung. Gleichzeitig entstehen dadurch komplexe **Anforderungen**, wie die **Vertraulichkeit**, **Echtheit** und **Verfügbarkeit** der nun digital vorliegenden Daten und Prozesse sicherzustellen. Um diesen Herausforderungen zu begegnen, bedarf es dem Einsatz starker Kryptographie-Verfahren.

In der IT-Welt hat sich die Kryptographie flächendeckend etabliert. Dies liegt meist daran, dass der Zugang zu vielen der Teils komplexen Algorithmen durch graphische Werkzeuge und digitale Assistenten enorm vereinfacht wurde. Jedoch lassen sich diese bewährten Verfahren und Werkzeuge nicht einfach in der Industrie und Elektronik-Entwicklung nutzen.

Grund dafür sind die abweichenden Anforderungen, wie etwa **veraltete Anlagen**, **knappe Ressourcen**, **kalkulierbare Reaktionszeiten**, **Update-Zyklen**, **Lieferbarkeit**, **Laufzeiten** oder fehlende **graphische Betriebssysteme**. Nichtsdestotrotz müssen industrielle oder elektronische Geräte und Maschinen in moderne IT-Systeme oder ins Internet eingebunden werden, was die bewährten Standards fordert.

sematicon bietet hier entsprechende **Lösungen** und Werkzeuge an, die im Einklang mit der Industrie durch neuartige Ansätze entwickelt wurden. Unsere praxisbezogenen Tools machen Kryptographie für jedermann **plattformunabhängig** nutzbar und **schließen so erfolgreich die Kluft zwischen IT und Industrie**.

sematicon

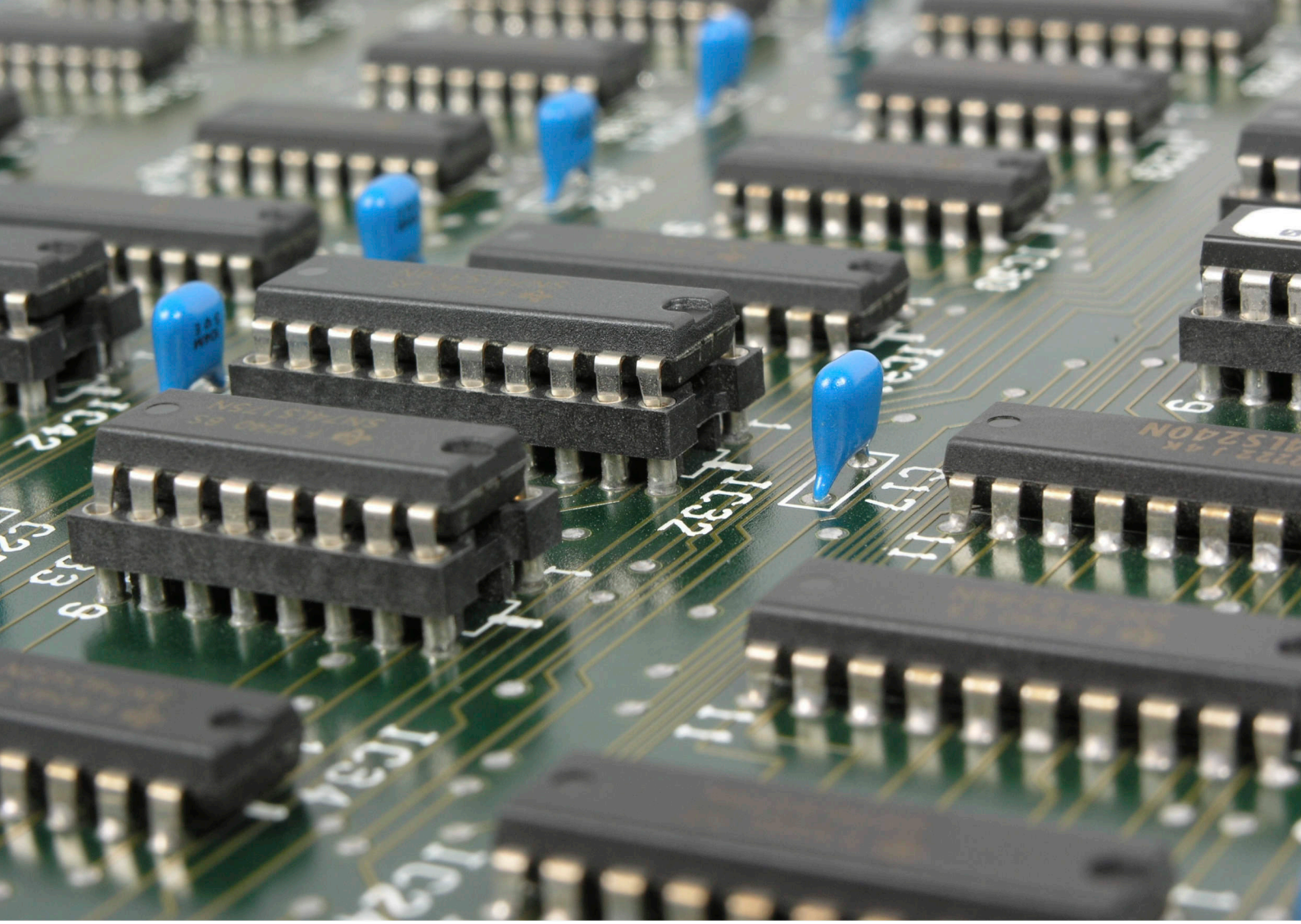
Weniger ist oft mehr

Von der IT lernen, aber nicht kopieren

Beim Gedanken an die Sicherheit von **intelligenten Geräten** wird oft versucht, durch klassische IT-Ansätze mit **Kanonen auf Spatzen** zu schießen. Viel zu oft wird dabei Sicherheit mit Vertraulichkeit gleichgesetzt, was in einer exzessiven Nutzung von Verschlüsselung mündet, die oftmals **nicht notwendig** ist. Ebenso schweift der Gedanke gerne in Richtung einer PKI-Lösung (Public Key Infrastructure), wenn es um die Authentizität bzw. Echtheit von Daten geht. PKI-Systeme sind aber aufwendig, komplex und meist auch teuer hinsichtlich der Installation und des Betriebs. Es fallen **hohe Kosten** für die PKI-Software, die Bereitstellung von Servern und zusätzlicher Hardware an. Auch ist das spätere **Management** der Geräte und deren Zertifikate oftmals eine **große Herausforderung**.

Es haben sich über die Jahre für zahlreiche Anwendungsfälle entsprechende IT-Standards etabliert. Viele Verfahren sehen dabei in der IT einfach aus, weil die **richtigen Werkzeuge** verfügbar sind, welche die Komplexität abstrahieren. Klassische IT-Ansätze eignen sich aber oftmals nicht direkt für den Einsatz im Industrie- oder (I)IoT-Umfeld, weil die notwendige IT-Basis für diese Werkzeuge fehlt.

Dennoch wird versucht, die Verfahren und Techniken meist unreflektiert zu übernehmen. Deshalb **scheitern** viele Sicherheitsprojekte bereits vor dem Start oder während der Projektphase aufgrund der hohen Komplexität oder der Kosten. Der **Fehler** liegt auf der Hand: Es wird versucht von der **IT zu kopieren** ohne **Alternativen** zu beleuchten.



Es muss nicht immer komplex sein

Natürlich können die Lösungsvorschläge aus der IT durch die Verwendung von Werkzeugen anwenderfreundlich gestaltet werden. Für den Einsatz im Umfeld der Industrie und Elektronik gibt es derartige Tools meist jedoch nicht. Die Entwicklung von Alternativen hierfür ist oft mit den geringeren Hardware-Ressourcen in der Industrie bzw. der Elektrotechnik oder Elektronik gar nicht machbar.

Dabei sind die Werkzeuge nur ein Teil der Wahrheit. Was viele nicht wissen: Die Welt der **Kryptographie** bietet eine Vielzahl an sicheren Algorithmen, die **alternative** Lösungsansätze ermöglichen. Durch Ihren Einsatz lassen sich viele der Anwendungsfälle mit teils **einfacheren** Methoden lösen, ohne die Kompatibilität zur IT zu gefährden.

Dabei sind allgemein einige Punkte zu beachten:

1) Standardisierte Krypto-Verfahren nutzen, um Sicherheit und Kompatibilität zu gewährleisten

2) Schlüssel und Geheimnisse immer isolieren, um das unterschätzte Risiko durch gemeinsame Ressourcen zu minimieren

3) Kryptographie nicht in Software abbilden, um die Leistung zu erhöhen und den Verlust der Schlüssel durch „Seitenkanalangriffe“ zu verhindern

4) Anforderungen und Schutzziele müssen klar definiert sein (siehe z.B. IEC-62443)

5) Risiken bei der Fertigung müssen zwingend in Betracht gezogen werden

sematicon

Was leistet se.SAM™?

Wozu benötige ich die **se.SAM™** Produktfamilie?

Kryptographie-Lösungen gibt es viele am Markt. Diese sind meist ausschließlich für den Einsatz im Office- bzw. IT-Umfeld geeignet.

Die **se.SAM™** Produktfamilie unterscheidet sich hier deutlich. Sie wurde für den Einsatz von Kunden aus den Bereichen der **Industrie und Elektronik** entwickelt und zeichnet sich durch eine besonders **einfache Handhabung** aus.

So wurden beispielsweise klassische IT-Schnittstellen (**PKCS#11**) durch **Industrie-Schnittstellen** ersetzt. Diese sind leicht integrierbar, besonders **benutzerfreundlich** und verfügen über eine schnell zu erlernende Befehlsstruktur. Neben unseren **schlüsselfertigen Hardwarelösungen** haben wir mit unserer **se.SAM™ Library** auch eine Software-Bibliothek im Programm. Damit können „**Secure Elements**" Dritter unter Anwendung derselben einfachen **se.SAM™** Syntax direkt eingebunden werden.

Die Befehlsstruktur bildet unsere flexiblen „**Krypto-Bausteine**" ab. Entsprechend eines Baukastensystems lassen sich so vielfältige Anwendungsfälle bedarfsgerecht zusammenstellen und integrieren.

Zu jeder Zeit wird sichergestellt, dass Kryptographie ausschließlich im **isolierten** „Secure Element" angewendet wird - **unabhängig** von der eingesetzten Hardware oder eines Herstellers.

Der Vorteil liegt auf der Hand: grenzenlose Flexibilität.

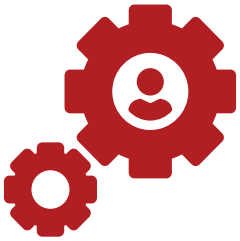
Schutz von geistigem Eigentum

Durch den Einsatz unserer Lösungen wird die Anwendung von Kryptographie zum Kinderspiel. Ihr Produkt lässt sich durch Sicherstellung von Signatur und Verschlüsselung vor **Manipulation** und geistigem **Diebstahl** schützen. Egal ob „**Secure Boot**“, das Management von **Lizenzen** oder **Sicherheit in der Produktion** - Sie sind stets gerüstet.

Authentizität von Software und Daten

Geht es darum, die **Unveränderlichkeit** von Daten und Software zu verifizieren, bietet **se.SAM™** eine sichere **Alternative zu klassischen IT-Ansätzen** wie beispielsweise kostspieligen PKI-Infrastrukturen. Durch den Einsatz unserer flexiblen Krypto-Bausteine können wir bedarfsgerecht auf Ihre Anforderungen reagieren.

Flexible Aus- und Nachrüstung von Systemen



Kryptographie muss **in Hardware abgebildet** werden, um den **Schutz** der Schlüssel und somit die Sicherheit zu **gewährleisten**. Viele Anlagen oder Maschinen stellen dabei eine besondere Herausforderung dar. Hierfür bietet **se.SAM™** durch die Unterstützung einer Vielzahl von Umgebungen, Betriebssystemen und Hardware-Architekturen eine **flexibel und kostengünstig** einsetzbare Lösung für die Aus- und Nachrüstung.

Internationale Standards und Richtlinien

Durch die Risiken, welche durch die Vernetzung intelligenter Geräte entstehen, bekommen **Richtlinien** wie die **IEC-62443** im industriellen IT-Umfeld immer mehr Gewicht. In einigen Branchen wird die Einhaltung bereits heute gefordert. Der Einsatz von Kryptographie spielt hierbei eine einscheidende Rolle. **se.SAM™** unterstützt Sie bei der **einfachen Umsetzung**.

Robuste und umweltbeständige Technik

Bei der Entwicklung, Komponentenauswahl und Fertigung unserer Systeme spielt die Qualität eine entscheidende Rolle. Wir stellen verlässliche Hardware „**Made in Germany**“ her. Durch **Klima- und elektromagnetische Resistenz** können wir den harten Bedingungen im **Außenbereich**, **Schaltschrank** sowie im **Office** und **IT-Bereich** problemlos gerecht werden.

Sicherheit bei Produktion und Wartung

Unser **se.SAM™** Portfolio bietet **schlüsselfertige Lösungen** für die **sichere Produktion**. Mit unseren speziellen **se.SAM™ Sicherheitsmodulen** haben Sie sogar die **produzierte Stückzahl** im Blick. Somit lassen sich **Überproduktionen**, speziell bei der Fertigung in **externen Fabriken**, verhindern. Sicheres **Firmware-Management** decken Sie ebenfalls ab, wenn es um **Updates** oder **Wartungsfälle** bei Ihren Kunden geht.

sematicon

Unsere Produktfamilie

Die **se.SAM™** Produktfamilie

se.SAM™ P210 für Systeme mit PCI-Express Mini-Steckplatz. Erweitern Sie Ihren Industrie-PC oder Ihr IoT Gateway um einen unabhängigen und sicheren Schlüsselspeicher mit Kryptographie-Werkzeugen

se.SAM™ P220 mit integrierter Echtzeituhr für dynamisches und automatisches Key Management. Dies erlaubt die Offline-Synchronisation von Schlüsseln und eröffnet somit zusätzliche Möglichkeiten.

se.SAM™ U-Serie für Anlagen mit USB-Anschluss und besonderen physikalischen Anforderungen. Vermeiden Sie Grauware mit der speziellen „Secure Manufacturing"-Funktion.

se.SAM™ N-Serie für den Einsatz im Netzwerk. Erlaubt den sicheren Betrieb einer PKI und unterstützt durch den Einsatz verschiedener Industrie-Protokolle das Krypto-Projekt im Rechenzentrum.

se.SAM™ Embedded für den Einsatz direkt auf der Platine. Erlaubt den einfachen und transparenten Einsatz von Kryptographie in Ihren Projekten. Eine sichere, vorkonfigurierte Lieferung der Hardware ist möglich.

Hohe Umweltbeständigkeit

Die Hardware ist wasserdicht, stoßfest und temperaturtolerant, was den Einsatz im Innen- und Außenbereich problemlos ermöglicht.*

Hohe elektromagnetische Störfestigkeit

se.SAM™ ist für den IT- und Industriebereich zertifiziert. Damit ist die Hardware für den Anlagen- oder Schaltschrankeinbau bestens geeignet.

Schlüsselfertige Lösung mit flexibler Schnittstelle

Unsere Krypto-Bausteine lassen sich ohne Software oder Treiber flexibel über die meisten Betriebssysteme und Architekturen hinweg einsetzen.

Langfristige Verfügbarkeit

Die Lieferbarkeit unserer **se.SAM™** Produkte ist über viele Jahre hinweg gesichert. Das reduziert Kosten und vermeidet Rezertifizierungsprozesse.

Umfangreiche Unterlagen und Dienstleistungsangebote

Neben einer umfangreichen Dokumentation in Deutsch und Englisch bieten wir weiterführende Schulungen und Dienstleistungen an.

*Nicht in allen Versionen der **se.SAM™** Hardware verfügbar. Bitte gesondert anfragen.

sematicon

Die Krypto - Bausteine

Flexibel - der **se.SAM™** Werkzeugkasten

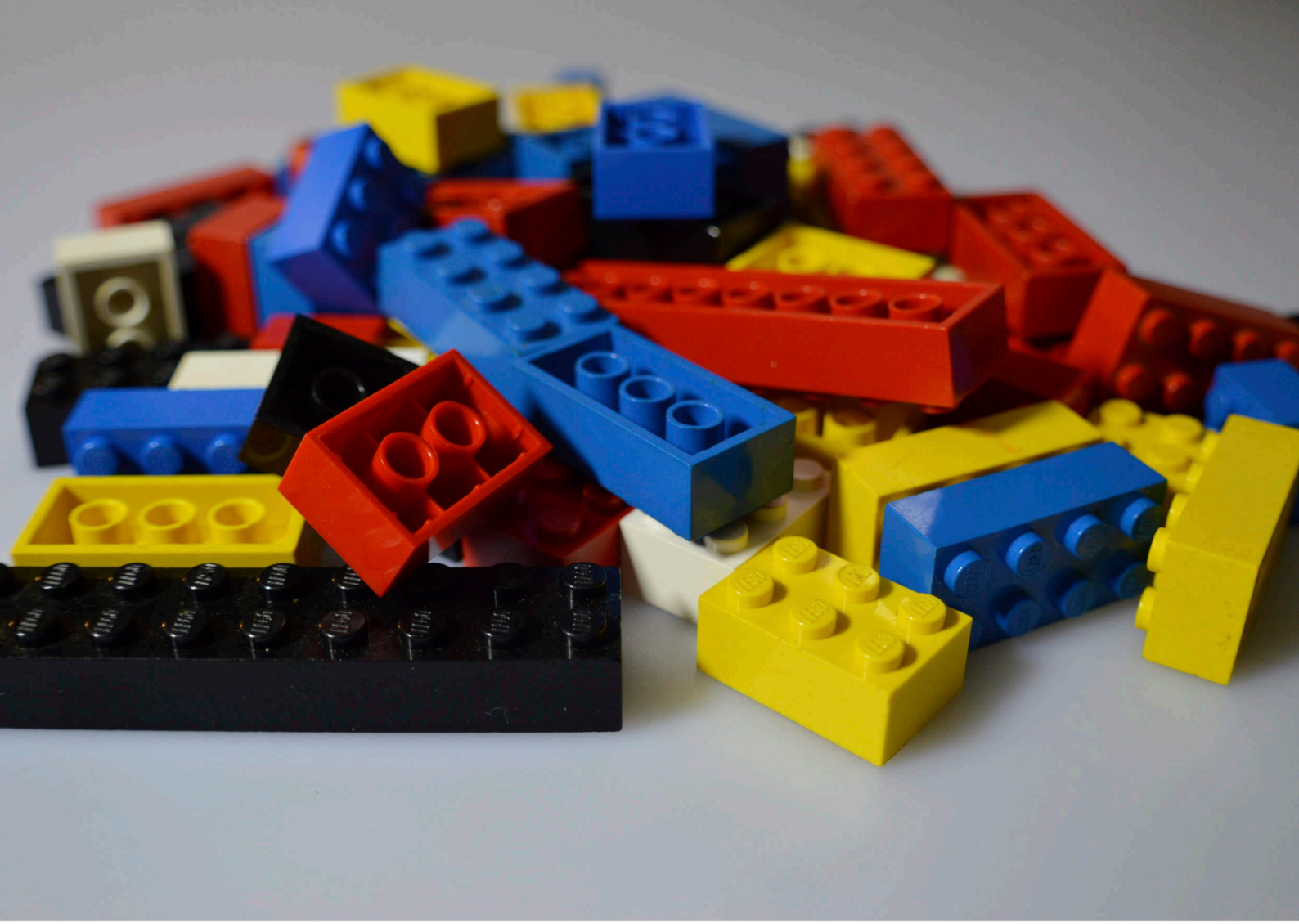
Die Basis der **se.SAM™** Produkte bilden unsere **Krypto-Bausteine**. Dabei handelt es sich um Algorithmen, die auf modernen kryptographischen Standards basieren. Wie mit einem Baukasten lassen sich diese **flexibel** und **bedarfsgerecht** kombinieren, um verschiedensten Anwendungsfällen Rechnung zu tragen.

Die Bausteine werden durch die unterschiedlichen Befehle repräsentiert, die über die gesamte Produktfamilie hinweg **einheitlich** sind. Die Befehle sind einfach zu erlernen und bleiben dank unseres **HCI** (Human Command Interface) **lesbar und verständlich**.

Mit den Bausteinen werden neben den klassischen symmetrischen und asymmetrischen Algorithmen auch Befehle für den sicheren Schlüsselaustausch, für Zufallszahlen oder Hash-Funktionen bereitgestellt. Aufgrund der **IT-Standardkonformität** ist der Austausch auch mit IT-Lösungen eventueller dritter Hersteller **kompatibel**. Damit eigenen sich die **se.SAM™** Produkte auch für die Kommunikation mit einem **Rechenzentrum** oder einem **Cloud-System**.

Begleitet wird das Set aus Bausteinen (Befehlen) durch eine **umfassende Dokumentation,** welche in deutscher und englischer Sprache verfügbar ist.

Zusätzlich bieten wir die Möglichkeit, in ausgewählten Kursen der **sematicon** academy den Umgang mit Kryptographie und unseren Bausteinen in praxisnahen Szenarien zu erlernen.




provkey
import
salt
pepper
derive
exchkey
verify
sign
hash
aes-ebc
aes-cbc
aes-ctr
hmac
encrypt
decrypt
se.SAM

sematicon

Kryptographie für Entwickler

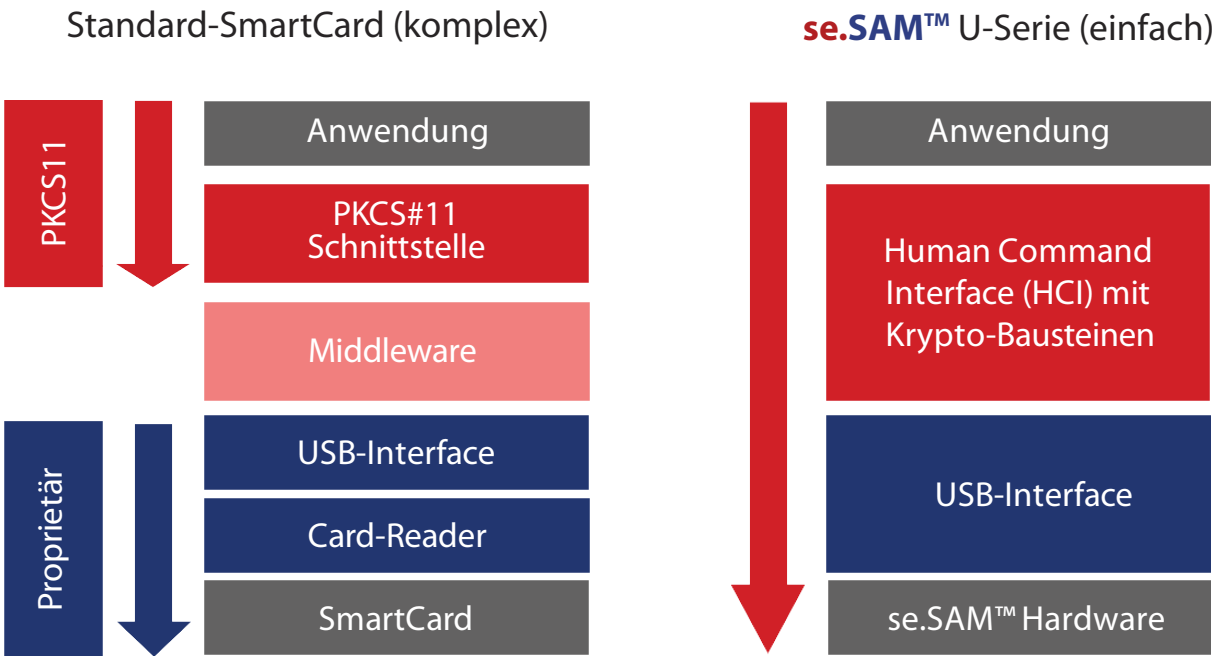
Zugriff auf **se.SAM™** ohne Softwareinstallation

Klassische SmartCards und Sicherheits-USB-Token werden normalerweise über die umfangreiche und komplexe IT-Standard-Schnittstelle **PKCS#11** angesprochen. Für den Betrieb ist daher eine sogenannte **Middleware** notwendig. Dabei handelt es sich um proprietäre Programme, welche die Nutzung der SmartCard erst ermöglichen. Diese Middleware - im weitesten Sinne ein Gerätetreiber - muss für jedes System extra zur Verfügung gestellt und installiert werden. Daraus ergeben sich Herausforderungen im Hinblick auf die Kompatibilität und Abhängigkeiten der Middleware von den verwendeten Betriebssystemen bzw. der Hardware.

Im Gegensatz dazu wird für den Zugriff auf die **se.SAM™** Hardware-Lösungen im einfachsten Fall nur ein USB-Anschluss benötigt. Das **HCI** (Human Command Interface) wird über eine virtuelle serielle Schnittstelle (COM) zur Verfügung gestellt. Nahezu alle Betriebssysteme bringen dafür bereits **integrierte Treiber** mit, wodurch die Installation zusätzlicher Middleware und Treiber unnötig wird. So wird das System **nicht** zusätzlich mit fremder Software **belastet** und komplett „**Plug & Play**“ betrieben. Ein weiterer Vorteil besteht auch darin, dass **se.SAM™** über die Standardbibliotheken in den gängigen **Programmiersprachen** nutzbar ist.

Durch unseren **einzigartigen Ansatz** ist somit eine einfache Handhabung unabhängig von Betriebssystem oder Hardware-Architektur möglich.

Beispiel: Zugriff auf die **se.SAM™** U-Serie



sematicon

Kryptographie im Terminal

Zugriff auf **se.SAM™** über die serielle Konsole

Das serielle Interface ist einfach und robust aufgebaut und erlaubt Zugriff auf externe Peripheriegeräte. Die serielle Schnittstelle (**RS232** oder **UART**) hat Einzug in fast alle Architekturen und Systeme vom PC, Industrierechner bis hin zum 8-bit-Prozessor gehalten. Damit ist diese Schnittstelle seit vielen Jahrzehnten eine verlässliche Konstante und Industriestandard.

Die **se.SAM™** Produktreihe nutzt genau deshalb diese **Standardschnittstelle**. Sie ermöglicht damit die Nutzung der Krypto-Funktionen des Moduls **ohne zusätzliche Software** durch **direkte Eingabe** der Befehle (Krypto-Bausteine). Mit einer **automatischen Anpassung** der Baudrate und Konfiguration der Schnittstellenparameter, je nach eingesetztem System, ist der **Einsatz** und der **Betrieb** völlig **problemlos**.

Auch bei der USB-Variante wird das Gerät als **serielle Schnittstelle** im System eingebunden. Der Vorteil ist, dass die notwendigen **Treiber** bereits Teil des jeweiligen Betriebssystems sind und deshalb **nicht zusätzlich installiert** werden müssen.

Im Gegensatz zu einem PKCS#11-Sicherheitsmodul muss nicht erst ein Programm für den Zugriff entwickelt werden. Es kann mit jedem beliebigen Terminal-Programm über die **serielle Konsole** auf das Modul zugegriffen werden. Die Befehle bzw. die **Krypto-Bausteine** können damit **unkompliziert evaluiert** werden: durch einfaches **Eintippen**.

GtkTerm - /dev/ttyACM0 115200-8-N-1

File Edit Log Configuration Control signals View Help

```
getrandom(100)
99E6
2FF731742017583883EAAFF7BC920029BC49D12A454649B1AEEB4546886F925A80FE3FC599
F24F3A3F4607C8137D25234D7DD2204984873CF9259307F39B9A62EAE5593571AF4673FA39
4A03DE75682B674D6C4B61E98D7AA1F1EF6163B7734457A737A8
6A9F
generatekeypair(1)
D5DE
5C2C1F4804D9359D37B5DD8BEB1CF085DEF61A671EAAA2BCAE33CA6331154F14CA8E61FB4E
B4B22337DC21F038FB42B0275FC61EF4A72B582A0022C354C5A4F0
52F5
hash(Hallo Welt)
BF80
2D2DA19605A34E037DBE82173F98A992A530A5FDD53DAD882F570D4BA204EF30
FC7F
sign(1,2D2DA19605A34E037DBE82173F98A992A530A5FDD53DAD882F570D4BA204EF30)
2B7F
41B66400B7BBBCC481DC9767C44AB404EA8AC71AA2A799687FE517BAF45AD3CA4115CA2033
1ED574EBC079AB57995AAE60FEA16656E260C091896082A281A3B9
CB0D
```

/dev/ttyACM0 115200-8-N-1 DTR RTS CTS CD DSR RI

sematicon

Kryptographie im Workflow

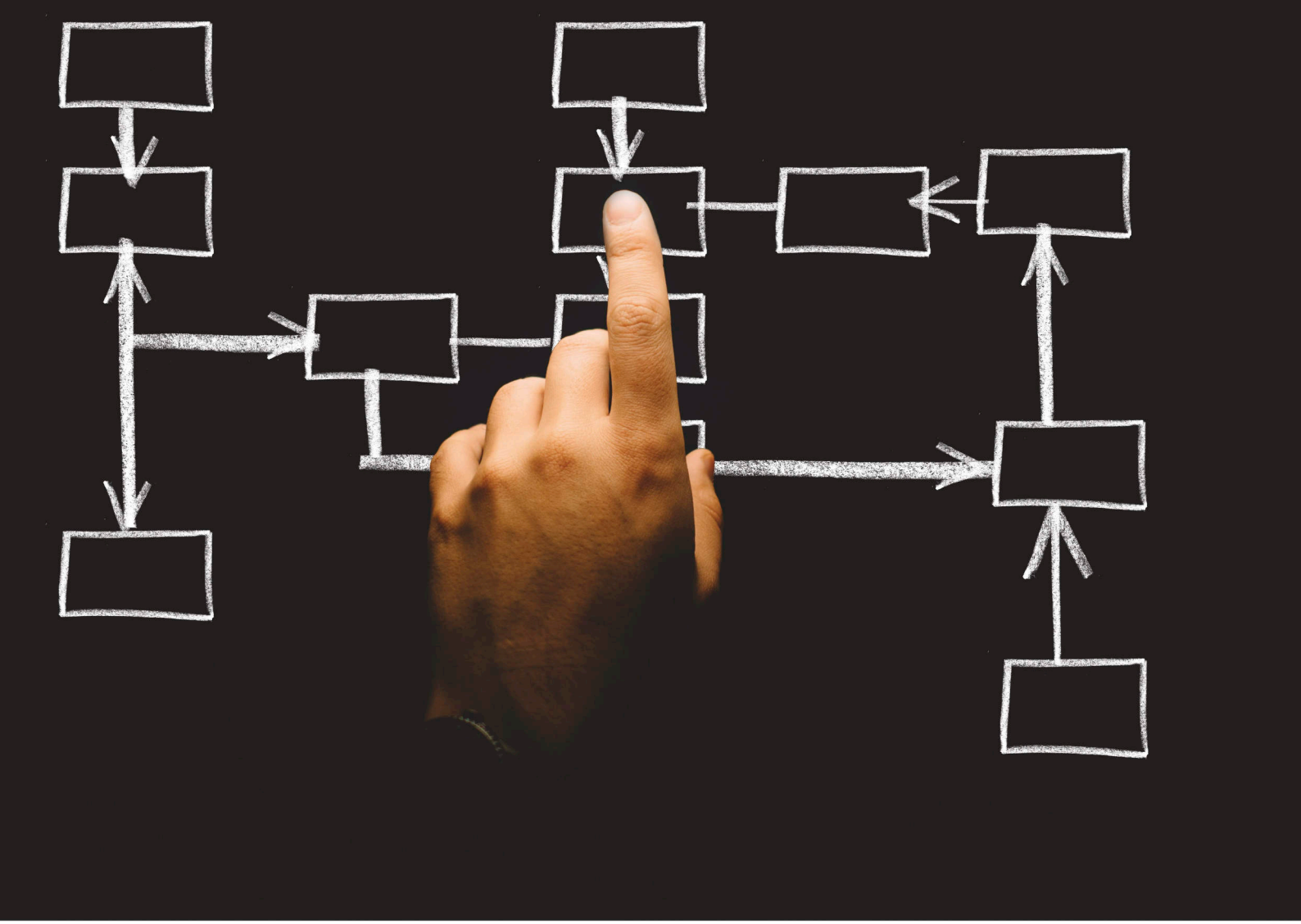
Direkte Integration von **se.SAM™** in Node-RED

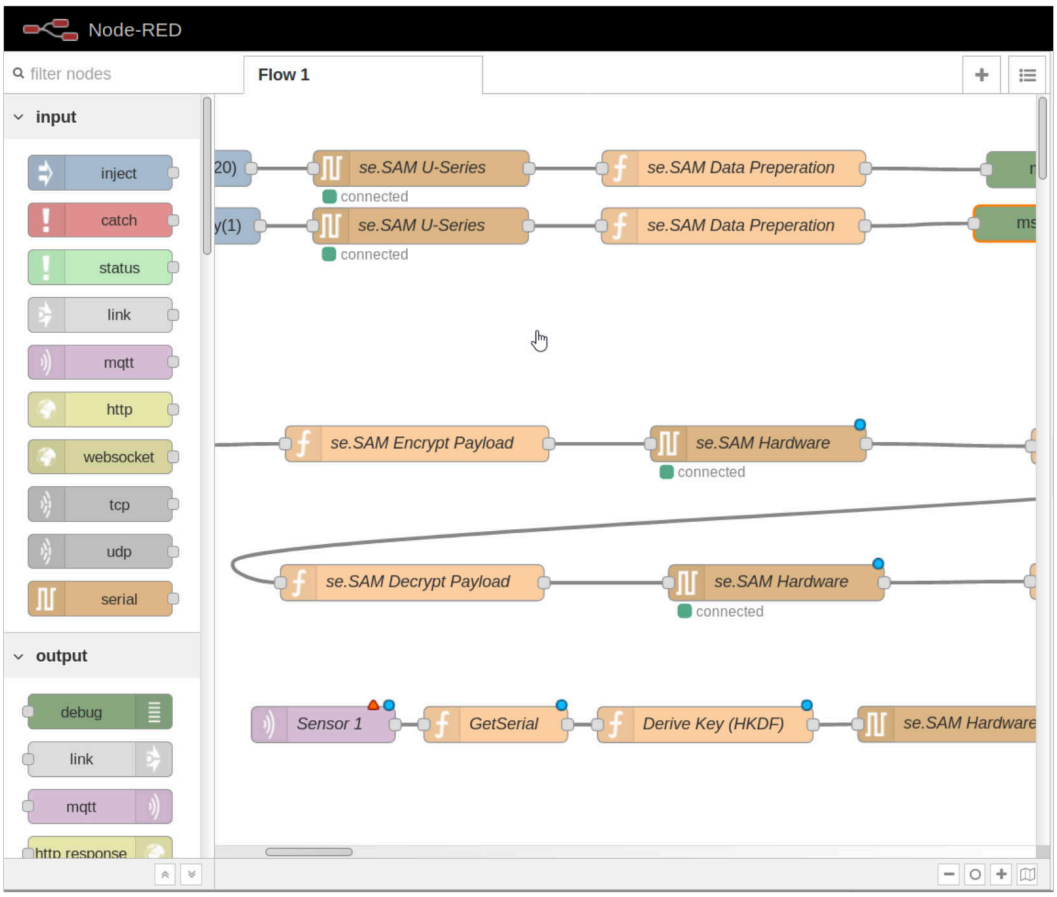
Node-RED ist ein Tool zur einfachen Programmierung von Prozessabläufen (Workflows) mittels einer grafischen Oberfläche. In der (I)IoT-Welt gilt es als weit verbreiteter Standard. Die freie Software unterstützt dabei, mit Daten von unterschiedlichsten industriellen Sensoren oder Aktoren zu interagieren. Die Besonderheit ist das einfache Baukastenprinzip mit den sogenannten „Nodes".

se.SAM™ integriert sich nahtlos in Node-RED - durch den Einsatz der „Serial Node" aus dem Bestand von Node-RED. Die **se.SAM™** Krypto-Bausteine werden in einer **se.SAM™** Application-Note (AN) als frei editierbare „**Funktions-Nodes**" zur Verfügung gestellt. Diese lassen sich dann grafisch zu komplexeren Anwendungen und Abläufen verbinden. Anhand der zahlreichen Möglichkeiten, die **se.SAM™** bietet, können so in **kürzester Zeit** die **Workflows** mit Kryptographie ausgestattet werden.

Diese **kryptographischen Funktionen** werden dabei **vollständig in Hardware** verarbeitet. Eine **Isolation** zwischen Schlüsselmaterial und Anwendung ist somit jederzeit gewährleistet. Es ist ausgeschlossen, dass Schlüssel das System verlassen oder Teil der Datensicherung werden.

Für den Betrieb ist es unerheblich, ob **se.SAM™** im **IoT-Gateway** verbaut ist (E-Serie) oder ob ein **Bestandssystem** mittels USB-Modul (U-Serie) **aus- oder nachgerüstet** werden soll.




Node-RED
filter nodes
Flow 1
input
inject
catch
status
link
mqtt
http
websocket
tcp
udp
serial
output
debug
link
mqtt
http response
se.SAM U-Series
connected
se.SAM Data Preperation
se.SAM U-Series
connected
se.SAM Data Preperation
se.SAM Encrypt Payload
se.SAM Hardware
connected
se.SAM Decrypt Payload
se.SAM Hardware
connected
Sensor 1
GetSerial
Derive Key (HKDF)
se.SAM Hardware

sematicon

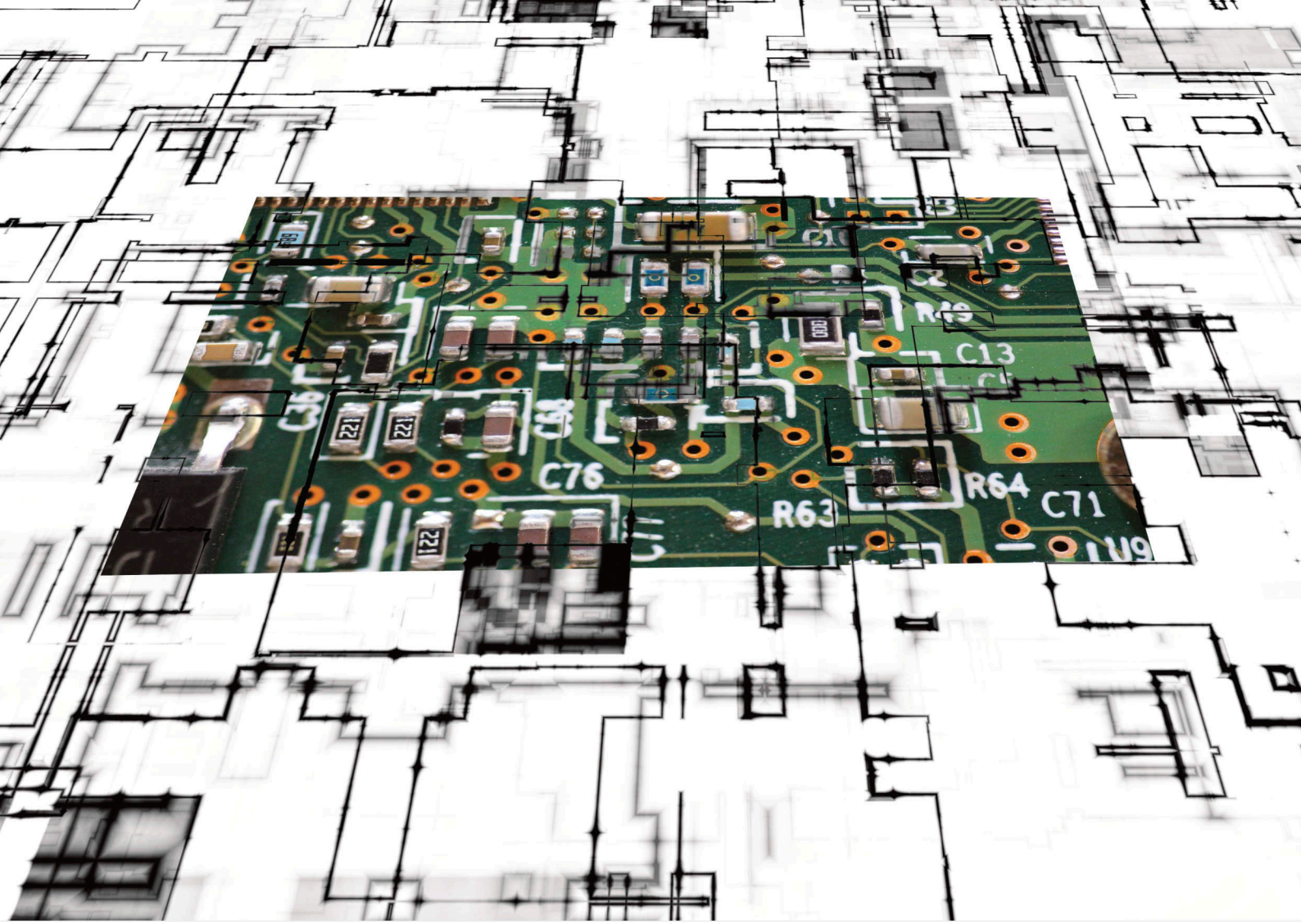
Kryptographie für Elektroniker

Die se.SAM™ Library für Secure Elements

Oftmals spielt der verfügbare **Platz** auf der Platine eine entscheidende Rolle beim Design neuer Hardware-Lösungen. In einigen Fällen macht es daher Sinn, platzsparende, sogenannte „Secure Elements“ (ICs) **direkt auf der Leiterplatte** zu verbauen, um das Schlüsselmaterial abzusichern. Es gibt eine Vielzahl solcher Chips am Markt. Wir helfen gerne bei der **Auswahl**, **Provisionierung** und **Integration** des richtigen Chips für Ihre Anwendungen.

Die **Secure Elements** besitzen oft ein **komplexes Interface**. Für das Verständnis der zugehörigen Dokumentation ist meistens tiefgründiges Wissen über die Kryptographie und die eingesetzten Algorithmen nötig. Häufig müssen auch Operationen für bestimmte Funktionalitäten kombiniert werden, was die **Komplexität** zusätzlich erhöht. Bibliotheken zu diesen Secure Elements sind - sofern vorhanden - meist nur für eine bestimmte Plattform verfügbar.

Wir stellen unseren Kunden mit der **se.SAM™ Library** im Gegensatz dazu die umfangreiche Funktionalität unserer **Krypto-Bausteine plattformunabhängig** zur Verfügung. Somit können Secure Elements einfach und **benutzerfreundlich** ins Projekt eingebunden werden. Voraussetzung ist, dass die jeweiligen Chips über die erforderliche Hardware-Ausstattung für den Einsatz der **se.SAM™ Library** verfügen. Es müssen, je nach Chip, lediglich die Funktionen für den Einsatz an der richtigen Schnittstelle ergänzt werden. Im Falle eines Secure Elements-Wechsels ist eine **Anpassung** der Einstellungen der **se.SAM™ Library** ausreichend.



Auswahl des Secure Elements

Wir beraten Sie bei der Auswahl des richtigen Secure Elements. Natürlich unterstützen wir auch bei der Provisionierung (Konfiguration ab Werk) und Konzeptionierung.

Source-Code-Lizenz mit Dokumentation

Die **se.SAM™ Library** wird als Source-Code geliefert und ist nicht vorkompiliert. Dies ermöglicht volle Code-Einsicht und Transparenz über die verwendeten Funktionen.

Optimiert auf Größe und Geschwindigkeit

Die **se.SAM™ Library** ist optimiert auf minimale Größe und maximale Geschwindigkeit. Dadurch eignet sich der Einsatz auch in leistungsschwachen 8-bit-Systemen.

Plattformunabhängig und flexibel

Die **se.SAM™ Library** unterstützt alle gängigen Prozessoren und ist plattformunabhängig einsetzbar. Abhängigkeiten zu Bibliotheken Dritter gibt es nicht.

Kurze Einarbeitungszeit und Dienstleistungsangebot

Auf Basis der **se.SAM™** Krypto-Bausteine stellt die **se.SAM™ Library** eine kurze Einarbeitungszeit sicher und wird optional durch Schulungen, Consulting und Entwickler-Support begleitet.

Wir sind das Münchner Unternehmen mit dem Fokus auf IT-Sicherheit und Kryptographie im industriellen Umfeld.

Wir bieten Unterstützung an zu den Themen:

Sicheres Management von Industrieanlagen

Verschlüsselte, nachvollziehbare und sichere Verbindung auf kritischen Mikroprozessor-, Industrie- und Steuerungsanlagen

Kryptographie für IoT, IIoT und Embedded Systeme

Konzeption, Unterstützung und Begleitung bei der Entwicklung sicherer IIoT, IoT und Embedded Systeme

Training und Consulting

Dienstleistungen rund um das Thema Zertifikate (PKI), Kryptographie, Verschlüsselung und sichere Schlüssel-Aufbewahrung (HSM)

sematicon AG
Schatzbogen 56
81829 München
Deutschland

Telefon: +49 (89) 413 293 - 000
Fax: +49 (89) 413 293 - 199

E-Mail: sales@sematicon.com
Internet: www.sematicon.com

sematicon
INDUSTRIAL IT SECURITY

V3.0 DE 2020