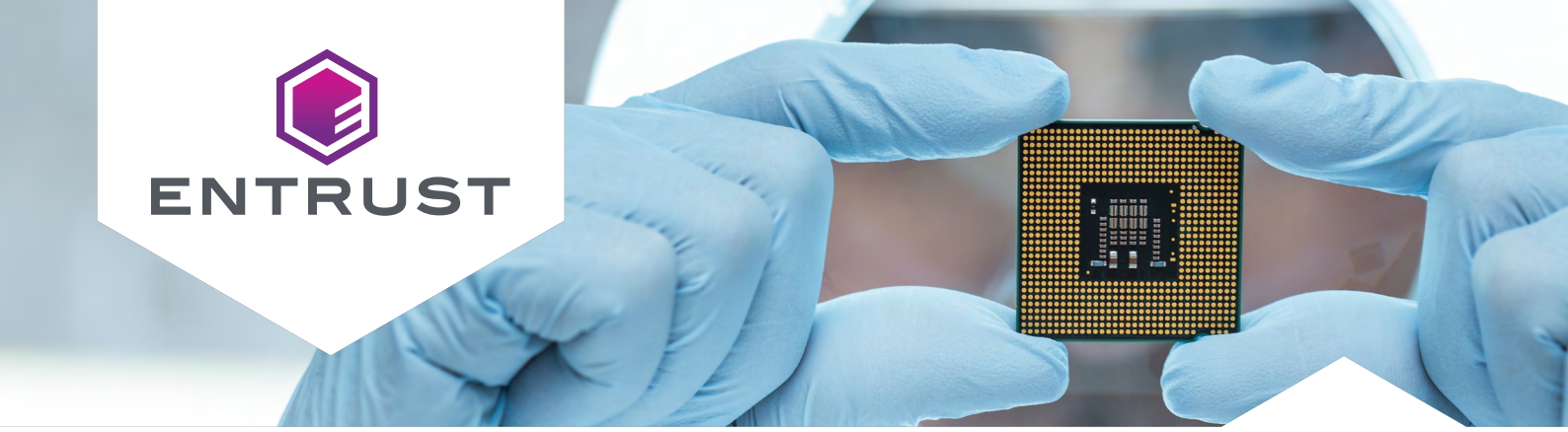

# Entrust stellt primäre Identitäten für die IoT-fähigen SAM L11 Mikrocontroller von Microchip bereit

Der Siegeszug des Internet of Things (IoT) ist nicht mehr zu stoppen. Die IDC sieht für das Jahr 2025 insgesamt mehr als 40 Milliarden verbundenen IoT-Geräten voraus – eine Zahl, die von vielen noch als zurückhaltend betrachtet wird.

Allerdings bringt die explosionsartige Verbreitung von IoT-Endgeräten – von selbstfahrenden Autos über intelligente Haushalts- und Medizingeräte bis hin zu Landwirtschaftsmaschinen – ihre ganz eigenen Herausforderungen mit sich. Einen besonderen Stellenwert hat hier das Thema Sicherheit: Jedes einzelne Gerät muss zuverlässig vor Gefahren geschützt werden.

## GESCHÄFTLICHE ANFORDERUNGEN

Anand Rangarajan, Product Marketing Manager bei Microchip Technology, führt aus: „Im IoT-Universum fehlen derzeit einheitliche Sicherheitsstandards. Viele Hersteller lassen sich von der schier zu komplex erscheinenden Aufgabe entmutigen, geeignete Sicherheitsmaßnahmen in ihre Produkte einbauen zu müssen."

> **Die Integration branchentauglicher Sicherheit in ein eingebettetes System ist wegweisend für den gesamten IoT-Markt.**
>
> – Anand Rangarajan, Product Marketing Manager bei Microchip Technology

**WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM**

# Microchip

Microchip Technology, Inc. ist für seine stetigen Innovationen und wegweisenden Produkte bekannt. Das Unternehmen ist einer der weltweit führenden Anbieter von Mikrocontrollern sowie Mixed-Signal-, analogen und Flash-IP-Lösungen. SAM L11, einer der neusten Mikrocontroller des Unternehmens, wurde 2018 auf der ARM Techcon mit dem *Innovation Award for Best Contribution to IoT* Security ausgezeichnet. Er ist speziell auf die Besonderheiten, Funktionen und Sicherheitsanforderungen von IOT-Knoten und smarten Endgeräten wie medizinische Geräte, Sensoren, Kameras und Autos zugeschnitten.

Microchip hat seinen Sitz in Chandler, Arizona, und ist an der Nasdaq notiert. Das Unternehmen hat Milliarden Mikrocontroller und Mikroprozessoren an hunderttausende Kunden in der ganzen Welt geliefert.

## TECHNISCHE ANFORDERUNGEN

„Da es sich um einen Mikrocontroller handelt, verlangt der für den SAM L11 vorgesehene Anwendungsfall im Hinblick auf die Konstruktion einige Besonderheiten, wie z. B. hohe Leistung bei niedrigem Stromverbrauch“, erläutert Rangarajan.

## LÖSUNG

Das Herzstück der Sicherheitsarchitektur des SAM L11 ist eine von Microchip entwickelte Vertrauensankerfunktion, mit der jedes einzelne Gerät während der Fertigung mit einem individuellen Schlüssel versehen werden kann. Die Auswahl der richtigen Technologie für die Verwaltung und Ausführung dieser wichtigen Funktion erwies sich als sehr einfach. „Wir arbeiten seit vielen Jahren mit Entrust (früher nCipher) zusammen, Daher fiel uns die Entscheidung für ihre Hardware-Sicherheitsmodule (HSM) zur Erstellung individueller Schlüssel nicht schwer“, so Rangarajan.

Der nShield®-HSM von Entrust ist ein zertifiziertes Hardware-Sicherheitsmodul, das kritische Verschlüsselung ausführt sowie digitale Signaturen und Schlüssel erstellt. Die robuste vernetzte Plattform ist in hohem Maße skalierbar und nutzt eine einzigartige, flexible Architektur, die branchenführende kryptographische Transaktionsraten ermöglicht.

## ERGEBNISSE

„Mithilfe der nShield HSM können wir jeden einzelnen SAM-L11-Mikrocontroller mit einem individuellen Schlüssel versehen. So ist es möglich, dass die Geräte einzeln identifiziert, geprüft und verwaltet werden. Das ist insbesondere dann wichtig, wenn das Vertrauen zwischen IoT-Geräten und sonstigen verbundenen Endgeräten wiederhergestellt werden soll“, bemerkt Rangarajan. „Hersteller profitieren somit in hohem Maße von der Cloud und können eine sichere, einheitliche Verbindung zwischen den einzelnen Knoten herstellen. Das ist ideal für Anwendungen wie die Sicherung von Funksensoren, die Verschlüsselung der Daten tragbarer medizinischer Geräte und die Remote-Authentifizierung von mit der Cloud verbundenen Systemen.“

Das äußerst attraktive Leistungsversprechen des Mikrocontrollers SAM L11 von Microchip ist unter anderem in der Partnerschaft des Unternehmens mit Trustonic begründet, einem führenden Anbieter auf dem Markt für Gerätesicherheit mit über 1,5 Milliarden geschützten Gerätebereitstellungen weltweit.

Trustonic hat eine Bibliothek mit Sicherheitsfunktionen wie Authentifizierung, sicheres Starten, Manipulationserkennung, AES- und SHA-Verschlüsselung und sichere Schlüsselspeicherung entwickelt, die in ein Softwareentwicklungskit integriert ist – ein großer Durchbruch.

# Microchip

> **Die Entscheidung für die nShield HSM von Entrust zur Erstellung einzelner Schlüssel fiel uns nicht schwer.**
>
> – Anand Rangarajan, Product Marketing Manager bei Microchip Technology

„Entwickler könne nun das modulare Sicherheitspaket für einfache API-Anrufe nutzen, um auf diese von uns entwickelten, äußerst ausgereiften Sicherheitsfunktionen zuzugreifen“, führt Rangarajan aus. „Eine tiefergehende Fachkenntnis der Protokolle auf Chipebene ist nicht länger erforderlich. Dadurch wird der für die Entwicklung benötigte Zeitrahmen deutlich verkürzt und der traditionell mit der Sicherung von IoT-Geräten verbundene Aufwand drastisch reduziert.“

Die Bibliothek mit Sicherheitsmodulen ist auf Kinibi-M aufgebaut, einer durch Hardware gesicherten Betriebsumgebung, die von Trustonic speziell für IoT-Chipsets mit Größenbeschränkungen entwickelt wurde. Eine Hardwareabstraktionsschicht unter Kinibi-M ermöglicht die direkte Kombination mit dem SAM L11 einschließlich der Verwaltung der Nutzung des verschlüsselten, vom nShield HSM von Entrust erstellten Schlüssels.

„Die Entwickler des SAM L11 von Microchip haben mit der ihnen eigenen Sorgfalt alles dafür getan, um den nShield HSM zur optimalen Lösung für uns zu machen. Aber unabhängig davon hat uns auch Trustonic empfohlen, den HSM von Entrust zu nutzen. Deren vollkommen unabhängige Befürwortung unserer Entscheidung war für uns eine Bestätigung“, erinnert sich Rangarajan.

## EINFACHE SICHERHEIT DANK EINEM WEGWEISENDEN CHIP

Der SAM L11 ist branchenweit der erste Mikrocontroller, der den Arm Cortex-M23-Prozessor und die in die Arm TrustZone eingebettete Sicherheitstechnologie nutzt. Er bietet hardware-gestützte Isolation von vertrauenswürdigen und nicht vertrauenswürdigen Ressourcen. Rangarajan führt aus: „Trotz der differenzierten und umfangreichen Möglichkeiten der Sicherheitsarchitektur vereinfacht die Nutzung von Kinibi-M eine sichere Anwendungsentwicklung. Verantwortlich hierfür ist eine Firmware, die vollständig mit den Sicherheitsfunktionen des SAM L11 integriert ist. Außerdem werden so Codebeispiele für entsprechende IoT-Anwendungsfälle bereitgestellt, die von einem Gerät wie dem SAM L11 profitieren können.“

Die Möglichkeit, Entwicklern von IoT-Geräten durch die Verwendung von Schlüsseln, die von einem nShield®-HSM von Entrust erstellt wurden, einen erstklassigen Vertrauensanker bereitzustellen, fand weltweit Anklang. Rangarajan erklärt: „Dank dieser Herangehensweise sind wir nun in der Lage, ein sicheres Hochleistungspaket mit extrem niedrigem Stromverbrauch anzubieten. Die Integration branchentauglicher Sicherheit in ein eingebettetes System ist wegweisend für den gesamten IoT-Markt.”

# Microchip

## NEUGESTALTUNG DER SICHERHEIT IM GESAMTEN IoT

### Geschäftliche Anforderungen

- Entwicklung einer Lösung zur Sicherung von IoT-Knoten und Endgeräten
- Reduzierung des Aufwands und der Kosten des Einbaus von Sicherheitstechnologie in IoT-Geräte
- Weniger Fachkenntnissen für die Programmierung auf Chipebene erforderlich

### Technische Anforderungen

- Integration robuster Sicherheitsfunktionen in schnelle, stromsparende Mikrocontroller
- Entwicklung eines kompakten Designs mit geringen Abmessungen, um die Verwendung mit speicherintensiven Anwendungen zu ermöglichen
- Bereitstellung eines Vertrauensankers

### Lösung

- nShield HSM von Entrust

### Resultat

- Veröffentlichung des Mikrocontrollers SAM L11 mit branchenführender Funktionalität und Leistung
- Ein Softwareentwicklungskit ermöglicht einfachen API-Zugriff auf ausgereifte Sicherheitsfunktionen
- Kürzere Produkteinführungszeit für Hersteller von IoT-Geräten
- Baut Vertrauen in IoT-Geräte und die von diesen erzeugten Daten auf

### ÜBER ENTRUST

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Weitere Informationen auf
**entrust.com/HSM**

ENTRUST

**Kontakt:**
**HSMinfo@entrust.com**