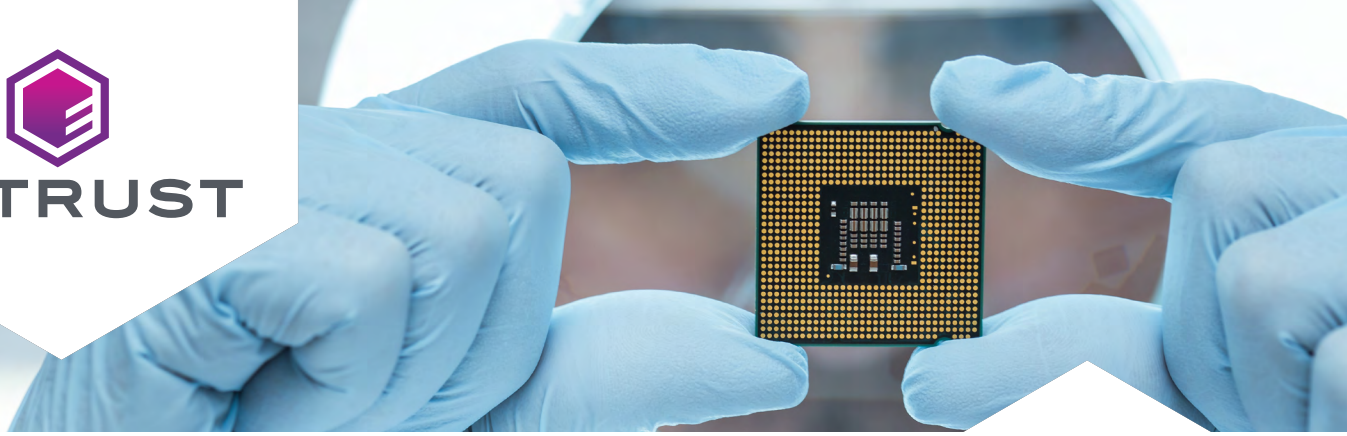

A Entrust fornece identidade raiz para microcontroladores SAM L11 prontos para IoT da Microchip

A Internet das Coisas (IoT) tornou-se um fenômeno imparável. Embora seja visto por muitos como um número altamente conservador, o IDC prevê que o número total de dispositivos IoT conectados excederá 40 bilhões em 2025.

No entanto, a proliferação explosiva de terminais relacionados à IoT - que variam de veículos autônomos a eletrodomésticos inteligentes e equipamentos de saúde a máquinas agrícolas - tem seus próprios desafios. Entre as mais críticas delas está a questão da segurança - garantir que cada dispositivo esteja protegido contra comprometimento.

NECESSIDADE DO NEGÓCIO

Anand Rangarajan, gerente de marketing de produto da Microchip Technology, elaborou: “O universo IoT atualmente não possui padrões difundidos de segurança. A enorme complexidade de incorporar medidas de segurança adequadas em seus produtos é uma proposta assustadora para muitos fabricantes.”

> **A integração da segurança de força industrial em um sistema embarcado é uma verdadeira virada de jogo para todo o mercado de IoT.**
>
> – Anand Rangarajan, gerente de marketing de produto da Microchip Technology

SAIBA MAIS EM ENTRUST.COM/HSM

Microchip

Reconhecida por sua inovação contínua e produtos que definem precedentes, a Microchip Technology, Inc. é um dos fornecedores líderes mundiais de soluções de microcontrolador, sinal misto, analógico e flash-IP. Um dos mais recentes microcontroladores da empresa, o SAM L11, recebeu o Prêmio de Inovação 2018 de Melhor Contribuição para a Segurança de IoT na ARM Techcon, abordando especificamente as necessidades de recursos, funcionalidade e segurança de nodes de IoT e terminais inteligentes, como dispositivos médicos, sensores, câmeras e carros.

Sediada em Chandler, Arizona, a Microchip é negociada publicamente na bolsa de valores Nasdaq. A empresa despachou bilhões de microcontroladores e microprocessadores para centenas de milhares de clientes em todo o mundo.

NECESSIDADES TECNOLÓGICAS

"Do ponto de vista do microcontrolador, o tipo de caso de uso que antecipamos para o SAM L11 determina algumas características de design muito exclusivas, como a necessidade de alto desempenho, mas baixo consumo de energia", descreveu Rangarajan.

SOLUÇÃO

No coração da arquitetura de segurança do SAM L11 está a raiz da função de confiança criada pela Microchip para permitir que uma chave exclusiva do dispositivo seja inserida durante a fabricação. A escolha da tecnologia para gerenciar e executar a tarefa crítica provou ser muito simples. "Temos um relacionamento de longa data com a Entrust (anteriormente nCipher) e selecionar seu módulo de segurança de hardware (HSM) para gerar as chaves individuais foi uma escolha clara para nós", observou Rangarajan.

O HSM Entrust nShield® é um dispositivo de segurança de hardware certificado que executa criptografia crítica, assinatura digital e funções de geração de chave. A plataforma de rede reforçada é altamente escalonável e utiliza uma arquitetura flexível única, capaz de atingir as taxas de transação criptográficas líderes do setor.

RESULTADOS

"Ter a capacidade de inserir uma chave exclusiva do HSM nShield em cada microcontrolador SAM L11 permite que os dispositivos sejam individualmente identificados, verificados e gerenciados remotamente. Isso é particularmente importante quando a confiança precisa ser restabelecida entre os dispositivos IoT e outros terminais endpoints", observou Rangarajan. "Os fabricantes agora podem tirar o máximo proveito da nuvem para fornecer conectividade segura e abrangente entre cada nó. É ideal para aplicativos como a segurança de sensores sem fio, criptografar dados de dispositivos médicos portáteis e até mesmo autenticação remota de sistemas conectados à nuvem."

Parte da proposta de valor muito atraente do microcontrolador Microchip SAM L11 é o resultado da parceria da empresa com a Trustonic, líder no mercado de segurança de dispositivos com mais de 1,5 bilhão de unidades protegidas implantadas em todo o mundo.

Um dos maiores avanços foi a criação da Trustonic de uma biblioteca de funções de segurança - incluindo autenticação, inicialização segura, detecção de adulteração, criptografia AES e SHA e armazenamento de chave seguro - que é incorporada a um kit de desenvolvimento de software.

Microchip

> **Selecionar o HSM Entrust nShield para gerar as chaves individuais foi uma escolha óbvia para nós.**
>
> – Anand Rangarajan, gerente de marketing de produto da Microchip Technology

"Os designers agora podem usar a estrutura de segurança modular para fazer chamadas API simples para acessar o conjunto muito sofisticado de recursos de segurança que criamos", comentou Rangarajan. "Não é mais necessária uma experiência profunda com protocolos em nível de chip. Isso acelera muito os prazos de desenvolvimento e reduz drasticamente a sobrecarga tradicionalmente associada à proteção de um dispositivo IoT."

A biblioteca de módulos de segurança é construída em cima do Kinibi-M, um ambiente operacional modular protegido por hardware projetado pela Trustonic para chipsets IoT de tamanho limitado. Embaixo do Kinibi-M, uma camada de abstração de hardware facilita a comunicação direta com o SAM L11, incluindo o gerenciamento do uso da chave criptografada gerada pelo Entrust nShield.

"Os desenvolvedores do Microchip do SAM L11 fizeram sua própria diligência para determinar se o HSM Entrust nShield era a escolha ideal para nós, mas separadamente, a Trustonic também recomendou que usássemos o HSM Entrust. Foi muito válido obter um endosso totalmente independente de nossa decisão", lembrou Rangarajan.

SIMPLIFICANDO A SEGURANÇA COM GAME-CHANGING CHIP

O SAM L11 é o primeiro microcontrolador da indústria a utilizar o processador Arm Cortex-M23 e a tecnologia de segurança embutida Arm TrustZone; fornecendo isolamento reforçado por hardware entre recursos confiáveis e não confiáveis. Rangarajan refletiu: "Apesar da sofisticação e dos recursos abrangentes da arquitetura de segurança, o uso do Kinibi-M ainda torna o desenvolvimento de aplicativos seguros mais simples com um firmware que está totalmente integrado aos recursos de segurança do SAM L11 e oferece exemplos de código para abordar casos de uso de IoT relevantes que podem se beneficiar a partir de um dispositivo como SAM L11."

A capacidade de fornecer aos desenvolvedores de dispositivos IoT uma Root-of-Trust (RoT) de classe mundial, utilizando chaves geradas por um HSM Entrust nShield®, está tendo um impacto global significativo. Rangarajan afirmou: "A abordagem que adotamos significa que agora podemos incorporar segurança em um pacote de alto desempenho com consumo de energia extremamente baixo. A integração da segurança de força industrial em um sistema embarcado é uma verdadeira virada de jogo para todo o mercado de IoT."

Microchip

TRANSFORMANDO A SEGURANÇA EM TODA A IoT

Necessidade do negócio

- Criar uma solução para proteger IoT nodes e endpoints
- Reduzir a complexidade e o custo de incorporação de segurança em dispositivos IoT
- Eliminar a necessidade de habilidades de programação especializadas em nível de chip

Necessidades tecnológicas

- Integrar recursos de segurança robustos em um microcontrolador rápido e com baixo consumo de energia
- Projetar pequenas dimensões para permitir o uso em aplicativos que usam muita memória
- Estabelecer root of trust

Solução

- HSM Entrust nShield

Resultados

- Lançamento do microcontrolador SAM L11 com recursos e desempenho líderes do setor
- O kit de desenvolvimento de software oferece acesso API simples a funções de segurança sofisticadas
- Tempo de colocação no mercado reduzido para fabricantes de dispositivos IoT
- Permite confiança para dispositivos IoT e os dados que eles produzem

SOBRE A ENTRUST

A Entrust mantém o mundo se movendo com segurança, permitindo identidades, pagamentos e proteção de dados confiáveis. Hoje, mais do que nunca, as pessoas exigem experiências seguras e contínuas, quer estejam cruzando fronteiras, fazendo uma compra, acessando serviços de governo eletrônico ou entrando em redes corporativas. A Entrust oferece uma gama incomparável de soluções de segurança digital e emissão de credenciais no centro de todas essas interações. Com mais de 2.500 colegas, uma rede de parceiros globais e clientes em mais de 150 países, não é de admirar que as organizações mais confiáveis do mundo confiem em nós.

Saiba mais em
entrust.com/HSM

ENTRUST

Entre em contato conosco:
HSMinfo@entrust.com