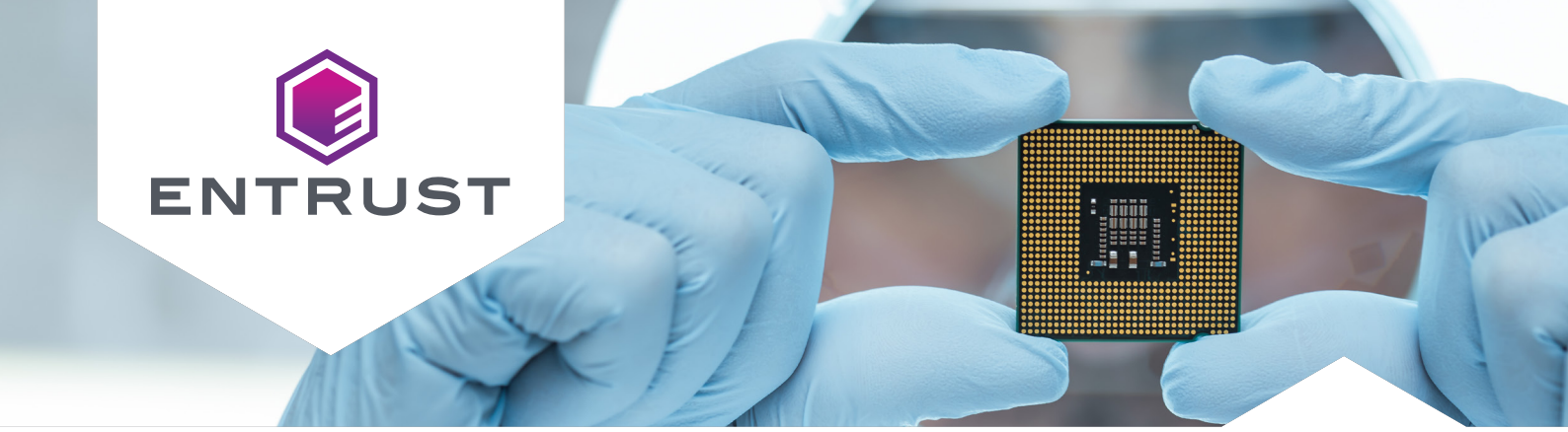

Entrust fornisce l'identità di root per i microcontrollori SAM L11 di Microchip per applicazioni IoT

L'Internet of Things (IoT) è diventato un fenomeno inarrestabile. IDC prevede che il numero totale di dispositivi IoT connessi supererà i 40 miliardi entro il 2025, sebbene siano in molti a ritenere che questa stima sia decisamente prudente.

Dai veicoli autonomi agli elettrodomestici intelligenti, passando per le apparecchiature sanitarie e le macchine agricole, l'impressionante diffusione degli endpoint IoT porta con sé alcune sfide specifiche. Tra i problemi più urgenti spicca quello della sicurezza, ovvero come garantire la protezione dei dispositivi.

OBIETTIVI COMMERCIALI

Anand Rangarajan, Product Marketing Manager di Microchip Technology, ha spiegato: "L'universo IoT manca di standard di sicurezza dettagliati. Incorporare misure di sicurezza adeguate nei prodotti è un'operazione complessa che scoraggia molti produttori."

> **« L'integrazione della sicurezza di livello industriale in un sistema embedded è un vero punto di svolta per il mercato dell'IoT. »**
>
> – Anand Rangarajan, Product Marketing Manager, Microchip Technology

SCOPRI DI PIÙ SU ENTRUST.COM/HSM

Microchip

Conosciuta per l'innovazione continua e lo sviluppo di prodotti leader del settore, Microchip Technology, Inc. è uno dei principali fornitori al mondo di soluzioni a segnale misto, analogiche, Flash-IP e per microcontrollori. Uno dei nuovi microcontrollori dell'azienda, il SAM L11, ha ricevuto un Innovation Award come miglior contributo alla sicurezza IoT nell'ambito del convegno ARM Techcon del 2018. Il prodotto risponde in modo specifico alle esigenze in termini di caratteristiche, funzionalità e sicurezza dei nodi IoT e degli smart endpoint, tra cui i dispositivi medici, i sensori, le videocamere e le automobili.

Quotata al Nasdaq, Microchip ha sede a Chandler, in Arizona, e ha prodotto miliardi di microcontrollori e microprocessori per centinaia di migliaia di clienti in tutto il mondo.

OBIETTIVI TECNICI

"Dal punto di vista della progettazione, il tipo di caso d'uso che prevediamo per il SAM L11 impone caratteristiche uniche, come la necessità di garantire prestazioni elevate con un basso consumo energetico," ha commentato Rangarajan.

LA SOLUZIONE

Al cuore dell'architettura di sicurezza del SAM L11 risiede una funzione "root of trust" ideata da Microchip per consentire l'inserimento di una chiave univoca per ciascun dispositivo durante la produzione. Individuare la tecnologia per la gestione e l'esecuzione di questa attività così delicata non è stato affatto complesso. "Collaboriamo da tempo con Entrust (in passato nCipher) e i loro hardware security module (HSM) sono stati una scelta naturale per consentire alla nostra azienda di generare chiavi univoche," ha affermato Rangarajan.

Gli HSM nShield® di Entrust sono appliance hardware di sicurezza, certificate per l'esecuzione di attività sensibili come la crittografia, l'emissione di firme digitali e la creazione di chiavi. Sicura e altamente scalabile, la piattaforma collegata alla rete utilizza un'architettura straordinariamente flessibile in grado di raggiungere volumi molto elevati di transazioni crittografiche.

I RISULTATI

"L'inserimento di una chiave univoca proveniente dall'HSM nShield in ogni microcontrollore SAM L11 consente di identificare, verificare e gestire separatamente i dispositivi da remoto. L'importanza di questo aspetto emerge, in particolare, quando è necessario ristabilire la fiducia tra i dispositivi IoT e gli altri endpoint connessi," ha osservato Rangarajan. "I produttori possono ora sfruttare appieno i vantaggi del cloud per fornire una connettività solida e sicura tra ciascun nodo. Questo processo è ideale per applicazioni come la protezione dei sensori wireless, la crittografia dei dati di dispositivi medici portatili e persino l'autenticazione remota dei sistemi connessi al cloud."

L'interessante proposta di valore offerta dal microcontrollore SAM L11 di Microchip è, in parte, il risultato della partnership dell'azienda con Trustonic, leader nel mercato della sicurezza dei dispositivi che vanta oltre 1,5 miliardi di unità protette distribuite in tutto il mondo.

Una delle svolte dall'impatto maggiore è stata la creazione, da parte di Trustonic, di una libreria di funzioni di sicurezza, tra cui autenticazione, avvio sicuro, rilevamento di eventuali manomissioni, crittografia AES e SHA e archiviazione sicura delle chiavi, inclusa in un kit di sviluppo software.

Microchip

> **Gli HSM nShield di Entrust sono stati una scelta naturale per consentire alla nostra azienda di generare chiavi univoche.**
>
> – Anand Rangarajan, Product Marketing Manager, Microchip Technology

"Gli sviluppatori possono ora effettuare semplici chiamate API per accedere al set molto avanzato di funzionalità di sicurezza che abbiamo creato," ha commentato Rangarajan. "Non è più necessaria un'esperienza approfondita con i protocolli a livello di chip. Questo accelera sostanzialmente i tempi di sviluppo e riduce in modo drastico i costi associati alla sicurezza dei dispositivi IoT."

La libreria di moduli di sicurezza è creata su Kinibi-M, un ambiente operativo modulare protetto da hardware, progettato da Trustonic per chipset IoT di dimensioni ridotte. Alla base di Kinibi-M, un livello di astrazione hardware facilita la comunicazione diretta con il microcontrollore SAM L11, inclusa la gestione dell'uso della chiave generata dall'HSM nShield di Entrust.

"I nostri sviluppatori hanno fatto svariate ricerche prima di stabilire che gli HSM nShield di Entrust fossero la scelta migliore per Microchip. In parallelo, anche Trustonic è giunta alla medesima conclusione. Ricevere l'approvazione della nostra scelta ha rappresentato un'ulteriore conferma della sua validità, soprattutto perché ottenuta in modo del tutto indipendente," ricorda Rangarajan.

SEMPLIFICARE LA SICUREZZA CON UN CHIP RIVOLUZIONARIO

Il SAM L11 è il primo microcontrollore del settore a utilizzare il processore Arm Cortex-M23 e la tecnologia di sicurezza incorporata Arm TrustZone, introducendo un isolamento hardware tra risorse affidabili e non. A questo proposito, Rangarajan ha affermato: "Nonostante le ampie e avanzate capacità di sicurezza dell'architettura, Kinibi-M semplifica lo sviluppo di applicazioni sicure grazie a un firmware che si integra perfettamente con le funzionalità di sicurezza del SAM L11. Offre inoltre esempi di codice adatti a casi d'uso IoT pertinenti, che potrebbero trarre vantaggio da un dispositivo come questo."

La possibilità di utilizzare le chiavi generate da un HSM nShield di Entrust per offrire agli sviluppatori di dispositivi IoT una solida root of trust sta avendo un impatto significativo a livello mondiale. Su questo tema, Rangarajan ha commentato: "Questo approccio ci ha consentito di includere la sicurezza in un pacchetto ad alte prestazioni, caratterizzato da un consumo energetico molto basso. L'integrazione della sicurezza di livello industriale in un sistema embedded è un vero punto di svolta per il mercato dell'IoT."

Microchip

RIVOLUZIONARE LA SICUREZZA DELL'IoT

Obiettivi commerciali

- Sviluppo di una soluzione per proteggere i nodi e gli endpoint IoT
- Riduzione della complessità e dei costi legati all'introduzione di misure di sicurezza nei dispositivi IoT
- Eliminazione della necessità di esperienza di programmazione a livello di chip

Obiettivi tecnici

- Integrazione di funzionalità di sicurezza efficaci in un microcontrollore rapido e a basso consumo
- Progettazione di un ingombro ridotto per consentire l'uso del dispositivo per applicazioni a uso intensivo di memoria
- Introduzione di una root of trust

La soluzione

- HSM nShield di Entrust

I risultati

- Lancio del microcontrollore SAM L11 con caratteristiche e prestazioni leader del settore
- Creazione di un kit di sviluppo software per un accesso semplice a funzioni di sicurezza avanzate tramite API
- Riduzione del time-to-market per i produttori di dispositivi IoT
- Garanzia di fiducia per i dispositivi IoT e i dati prodotti

INFORMAZIONI SU ENTRUST

Entrust permette al mondo di continuare ad avanzare in sicurezza attraverso sistemi di identificazione, pagamento e protezione dei dati ad alta affidabilità. Oggi più che mai, le persone si aspettano esperienze sicure e ottimizzate, che si tratti di attraversare le frontiere tra Stati, effettuare un acquisto, accedere ai servizi elettronici della pubblica amministrazione o collegarsi a una rete aziendale. Entrust offre un'ineguagliabile gamma di soluzioni di sicurezza digitale ed emissione di credenziali, il vero fondamento di tutte queste interazioni. Con oltre 2.500 colleghi, una rete di partner globali e clienti in più di 150 Paesi, non sorprende che le organizzazioni più fidate al mondo scelgano noi.

Scopri di più su
entrust.com/HSM

ENTRUST

Per contattarci:
HSMinfo@entrust.com