

Microchip vereenvoudigt op hardware gebaseerde IoT-beveiliging met de eerste industriële vooraf geïnstalleerde oplossingen voor elke gewenste toepassing



Met een minimum bestelaantal van 10 stuks biedt Microchip's Trust Platform de opslag van op hardware gebaseerde beveiligingssleutels voor laag-, midden- en hoog-volume toepassingen.

Omdat het aantal en het soort connected apparaten sterk toeneemt, vormen zowel de marktfragmentatie als de kwetsbaarheid van de beveiliging binnen het Internet of Things (IoT) enorme uitdagingen voor ontwerpers. Op hardware gebaseerde beveiliging is de enige manier om beveiligingssleutels te beschermen tegen concrete aanvallen en pogingen daartoe op afstand. Diepgaande kennis van beveiliging, ontwikkelingstijd en kosten zijn gemoeid bij het configureren en beveiligen van elk apparaat. Met bedrijven die waar dan ook honderden tot miljoenen verbonden apparaten per jaar produceren en over de aardbol verspreiden, kan de schaal-

baarheid van de architectuur van de ingebouwde componenten een aanzienlijk struikelblok voor toepassingen opwerpen. Fabrikanten kunnen meestal alleen maar orders met hoog volume installeren en configureren, zodat bedrijven met kleine tot middelgrote orders genoeg moeten nemen met minder goed presterende componenten. Om toch de gehele massamarkt te kunnen bedienen, introduceert Microchip Technology Inc. nu de eerste vooraf geïnstalleerde oplossing van de industrie die voorziet in de opslag van beveiligingssleutels voor laag-, midden- en hoog-volume componenten waarbij gebruik wordt gemaakt van het ATECC608A beveiligingselement. Met **Microchip's Trust Platform voor de CryptoAuthentication™ serie** kunnen bedrijven van elke omvang eenvoudig beveiligingsverificatie implementeren.

Microchip's Trust Platform bestaat uit een drietraps aanbod, met bij aankomst vooraf geïnstalleerde, vooraf geconfigureerde of geheel door de klant te specificeren beveiligingselementen, zodat ontwerpers het platform kunnen kiezen dat het best aansluit op hun individuele ontwerp. Als eerste oplossing voor het leveren van klaar-voor-gebruik beveiligingsverificatie voor de massamarkt, voorziet de eerste trap – **Trust&GO** – in vooraf geïnstalleerde beveiligingselementen zonder enige tussenkomst bij een minimaal te bestellen aantal componenten van slechts 10 stuks. De identiteitsgegevens van de component zijn voorgeprogrammeerd en vergrendeld binnenin de ATECC608A voor automatische cloud of LoRaWAN™ verificatie. Parallel daaraan worden de overeenkomstige certificaten en openbare beveiligingssleutels geleverd in een "manifest"-bestand dat kan worden gedownload via Microchip's e-commerce online verkoopkanaal en de geselecteerde distributiepartners.

Naast de besparing van enkele maanden ontwikkeltijd vereenvoudigt deze oplossing bovendien de logistiek aanzienlijk, omdat het voor klanten uit de massamarkt gemakkelijk wordt om apparaten te beveiligen en te beheren zonder de overheadkosten van derden die diensten leveren of de instanties die certificaten leveren.

Met de mogelijkheid tot verificatie op elke openbare of privé cloud infrastructuur is Microchip's Trust Platform ook flexibel en klantspecifiek aan te passen. Voor klanten met specifieke eigen wensen voorziet het programma in de TrustFLEX en TrustCUSTOM platforms. De tweede trap van het programma, **TrustFLEX**, biedt de flexibiliteit om gebruik te maken van de certificaataanbieder naar keus van de klant, waarbij nog steeds kan worden geprofiteerd van vooraf geconfigureerde gebruiksomstandigheden. Tot deze gebruiksomstandigheden behoren basisveiligheidsmaatregelen, zoals transportlaagbeveiligings (transport layer security; TLS) geharde verificatie voor verbinding met elk willekeurig op IP gebaseerd netwerk met elke willekeurige certificatieketen, LoRaWAN verificatie, veilig opstarten, updates via de ether (over-the-air; OTA), IP beveiliging, beveiliging van de data van de gebruiker en omdraaien van beveiligingssleutels. Dit beperkt de tijd en complexiteit die het klantspecifiek maken van een component met zich meebrengt zonder dat er klantspecifieke onderdelennummers nodig zijn. Voor klanten die hun ontwerpen volledig klantspecifiek willen aanpassen is de derde trap van het programma – **TrustCUSTOM** – bedoeld met klantspecifieke configuratiemogelijkheden en vertrouwensdocumenten.

"De toename van succesvolle aanvallen op software gebaseerde beveiligingsoplossingen onderstreept de noodzaak voor bedrijven om het beste wat de industrie te bieden heeft ook toe te passen, waaronder het isoleren van de eigen beveiligingssleutels in beveiligingselementen," zegt Nuri Dagdeviren, vice president van Microchip's afdeling beveiligingsproducten. "Microchip's Trust Platform maakt het implementeren van op hardware gebaseerde beveiliging eenvoudig en betaalbaar voor bedrijven van elke omvang, met verwijdering van de obstakels die traditioneel kenmerkend zijn voor het configureren en programmeren van componenten."

Microchip heeft samengewerkt met Amazon Web Services (AWS) voor het realiseren van een recht-toe-recht-aan en vereenvoudigd instapproces rond het AWS IoT dienstenpakket voor

producten die zijn ontwikkeld met alle varianten van het Microchip Trust Platform.

De ATECC608A beschikt over een Common Criteria Joint Interpretation Library (JIL) met een "eersterangs" opslag van de beveiligingssleutel, hetgeen klanten garandeert dat de componenten beveiligingspraktijken implementeren die zich in de industrie hebben bewezen en met de opslag van beveiligingssleutels op het hoogste niveau. Met op hardware gebaseerde vertrouwensbasis (root of trust) opslag en versleutelings-tegemaatregelen, beveiligt de component tegen de breedste klasse van bekende fysieke aanvallen.

Microchip's beveiligde productieafdeling programmeert de beveiligingssleutels en garandeert dat ze nooit worden afgestaan aan derden, noch tijdens het programmeren, noch tijdens de levensduur van de component.

Ontwikkelhulpmiddelen

De ATECC608A kan worden gekoppeld met elke willekeurige microcontroller en microprocessor. Voor het snel opzetten van prototypen met beveiligde oplossingen kunnen ontwerpers gebruik maken van de Trust Platform Design Suite met onderstaande modules:

- Een begeleide "use case tool"
- Uitvoerbare Python-handleidingen die draaien op Jupyter notebooks
- C-codevoorbeelden voor elke "use case"
- Een "geheimen uitwisselend" hulpprogramma
- De Trust Platform hardware-ontwikkelpakketten

Prijzen en beschikbaarheid

Componenten uit Microchip's Trust Platform zijn vanaf vandaag beschikbaar uit serieproductie met de volgende minimale bestelaantallen (minimum order quantities; MOQ):

- Trust&GO voor TLS (ATECC608A-TNGTLSx-B): \$1,20 met een MOQ van 10 stuks*
 - Trust&GO voor TLS (ATECC608A-TNGTLSx-G): \$0,77 met een MOQ van 2000 stuks*
 - Trust&GO voor LoRaWAN (The Things Industries ATECC608A-TNGLORAx-B en Actility ATECC608A-TNGACTU-B): \$1,40 met een MOQ van 10 stuks*
 - TrustFLEX voor LoRaWAN willekeurige join servers (ATECC608A-TFLXLORAx): \$0,938 met een MOQ van 2000 stuks*
 - TrustFLEX (ATECC608A-TFLXTLSx): \$0,845 met een MOQ van 2000 stuks*
 - TrustCUSTOM (ATECC608A-TCSTMx): \$0,883 met een MOQ van 4000 stuks*
- *uDFN (x = U) of SO8 (x = S)

Ontwerphulpmiddelen in Microchip's Trust Platform zijn beschikbaar voor:

- CryptoAuth Trust Platform pakket: \$13
- ATECC608a Trust Platform pakket: \$14

Bezoek voor aanvullende informatie en voor het verkrijgen van de hier genoemde producten www.microchipdirect.com of neem contact op met een erkende Microchip-distributeur. ◀