

## Pressmeddelande

Datum: 18 maj 2020

# IAR Systems möjliggör för företag att uppfylla säkerhetskrav i produkter baserade på NXP-processorer

**Den senaste versionen av säkerhetsverktyget C-Trust, ett tillägg till IAR Embedded Workbench, stödjer nu de populära processorerna K22, K24, K64, KV56 och KV58 från NXP, i tillägg till stödet som redan finns för NXP-processorer**

Stockholm, Sverige – 18 maj 2020 – IAR Systems meddelar att säkerhetsverktyget C-Trust nu har utökat stöd för NXP-processorer. Detta utökade stöd hjälper utvecklare av inbyggda system att implementera säkerhet i produkter och därmed kunna möta krav från nya lagar och förordningar kring säkerhet i IoT-produkter, både produkter som är i produktion samt för produkter som redan finns på marknaden. Dessutom kommer stöd för NXP's i.MX RT1064-processorer att läggas till i en kommande produktrelease av C-Trust, vilket kommer att ytterligare förenkla utveckling av säkra industri- och konsumentprodukter.

Sedan den 1 januari finns regler i både Kalifornien ([SB 237](#)) och Oregon ([HB 2395](#)) i USA som kräver att tillverkare av uppkopplade produkter säkerställer att de innehåller den säkerhet som behövs för att skydda produkten och dess information från obehörig användning. Detta krav gäller den som tillverkar utrustningen, vilket betyder att alla företag som säljer produkter till dessa stater måste uppfylla kravet. Liknande krav är på gång i Europa, där European Telecommunications Standards Institute (ETSI) har publicerat ett slutgiltigt utkast på standarden [EN 303 645](#) som definierar europeiska "best practices" för IoT-säkerhet för konsumenter. I Asien går länder framåt vad gäller cybersäkerhet och integritetslagar för IoT, till exempel har South Korean Internet & Security Agency (KISA) nyligen publicerat riktlinjer för [IoT Service Planning from Personal Information Perspective](#). C-Trust förenklar utveckling av produkter som är byggda på NXP-processorer som på sikt behöver möta de nya säkerhetskraven som kommer med dessa lagar och standarder.

C-Trust fungerar som en förlängning av utvecklingsverktyget IAR Embedded Workbench och gör det möjligt för utvecklare att enkelt bygga in säkerhet i sina applikationer, utan att behöva fördjupa sig i komplexa säkerhetsaspekter. Detta gör applikationen säkrare och skyddar mot IP-stöld, intrång, kopiering och överproduktion. Den senaste versionen av C-Trust lägger till stöd för NXP-processorerna

– mer –

K22, K24, K64, KV56 och KV58, i tillägg till existerande stöd för processorerna K65/66. Tack vare det uppdaterade processorstödet kan utvecklare som använder säkerhetsverktyget lägga till säkerhet i existerande produktdesigner för att kunna möta de utökade säkerhetskraven utan att behöva göra omfattande ändringar i designen.

"I takt med att fler och fler lagar och förordningar för säkerhet tillkommer världen över är det viktigt för oss att kunna hjälpa våra kunder i denna transformation", säger Stefan Skarin, VD, IAR Systems. "Genom att ta tillvara på vårt starka partnernetverk, till exempel med processorleverantörer som NXP, kan vi tillsammans möta de ökande säkerhetskraven och därmed i förlängningen skapa en mer säker och hållbar värld."

"Vi på NXP är glada att C-Trust nyligen fick stöd för processorfamiljen LPC55S6x och vi välkomnar nu utökningen av stödet med ytterligare processorer, eftersom det levererar en mer komplett produktportfölj som underlättar säkerhetsimplementation från generella applikationer hela vägen till applikationer med högre säkerhet", kommenterar Brendon Slade, director MCU ecosystem, NXP Semiconductors. "I takt med att marknadskraven utvecklas behöver företag ha möjlighet att snabbt kunna leverera den funktionalitet som krävs och möta slutkundens krav."

IAR Systems erbjuder också Security from Inception Suite, en helhetslösning som inkluderar omfattande programvara och tjänster som hjälper företag att anpassa säkerheten i inbyggda system. Mer teknisk information om IAR Systems kompletta säkerhetserbjudande och säkerhetsverktyget C-Trust finns på [www.iar.com/security](http://www.iar.com/security).

### Slut

*Editor's Note: IAR Systems, IAR Embedded Workbench, Embedded Trust, C-Trust, IAR Connect, C-SPY, C-RUN, C-STAT, IAR Visual State, IAR KickStart Kit, I-jet, I-jet Trace, I-scope, IAR Academy, IAR, and the logotype of IAR Systems are trademarks or registered trademarks owned by IAR Systems AB. All other product names are trademarks of their respective owners.*

### **Kontaktpersoner på IAR Systems Group AB**

Josefin Skarin, IR-kontakt, IAR Systems Group AB

Email: [josefin.skarin@iar.com](mailto:josefin.skarin@iar.com)

Stefan Skarin, VD och koncernchef, IAR Systems Group AB

Email: [stefan.skarin@iar.com](mailto:stefan.skarin@iar.com)

### **Om IAR Systems**

IAR Systems erbjuder programvara för programmering av processorer i inbyggda system. Programvaran gör det möjligt för företag världen över att skapa nutidens produkter och framtidens innovationer. Sedan 1983 har IAR Systems lösningar säkerställt kvalitet, tillförlitlighet och effektivitet i utveckling av över en miljon produkter, bland annat inom fordonsindustri, industriautomation, medicinteknik, konsumentelektronik och Internet of Things. Företaget har huvudkontor i Uppsala och sälj- och supportkontor över hela världen. Från och med 2018 är Secure Thingz, en leverantör av avancerade säkerhetslösningar för inbyggda system inom IoT, en del av IAR Systems. IAR Systems Group AB är noterat på NASDAQ OMX Stockholm, Mid Cap. Mer information finns på [www.iar.com](http://www.iar.com).