# Intel Compute Card lieferbar

**Intels Compute Card ist nur 0,5 cm dick, so breit wie eine Scheckkarte und 1 cm länger.**

Intels 5 Millimeter flache Mini-PCs mit Apollo-Lake- und Core-Y-Prozessoren für Embedded Systems sind nun erhältlich, jedenfalls Varianten mit Celeron N3455 (CD1C64GK, 165 Euro), Pentium N4200 (CD1P64GK, 210 Euro) und Core m3-7Y30 (CD1M3128MK, 370 Euro). Die Version mit Core i5-7Y75 (CD1IV128MK, 550 Euro) ist noch nicht lieferbar. Die Kärtchen mit 5,5 und 9,5 Zentimeter langen Kanten – ebenso breit, aber 1 cm länger als eine Scheckkarte – passen in ein 120 Euro teures Dock mit Lüfter (DK132EPJ) und arbeiten dann wie ein PC.

Die teuerste Compute Card hat 8 GByte RAM, alle anderen 4 GByte. Die beiden billigsten kommen mit je 64 GByte eMMC-Flash, in den anderen stecken 128-GByte-SSDs. WLAN und Bluetooth haben alle, USB 3.0, HDMI 1.4 und DisplayPort 1.2 sind ähnlich wie bei USB Typ C zugänglich, aber nur über einen speziellen Flachstecker. *(ciw@ct.de)*

# Robuste MicroSD-Karten

Speziell für Überwachungskameras und Bodycams hat Micron eine Baureihe von „Industrial MicroSD“-Karten aufgelegt, zunächst mit 32 und 64 GByte Kapazität. Sie sind für kontinuierliche Video-Aufzeichnung über drei Jahre spezifiziert. Die 32-GByte-Karte soll dabei 4 MBit/s verdauen, die 64-GByte-Karte das Doppelte. 2018 folgen MicroSD-Karten mit 128 und 256 GByte Kapazität. Micron verwendet dabei 3D-NAND-Flash mit 64 Lagen.

Die Karten LSDMI32GBJWW und LSDMI64GBJWW vertragen –25 bis +85 Grad Celsius und entsprechen den „Class 10“-Vorgaben, schreiben also mit bis zu 10 MByte/s. Die Firmware des Controllers ist für kontinuierliches Schreiben optimiert, um Frame Drops zu vermeiden. Preise nannte Micron bisher nicht.

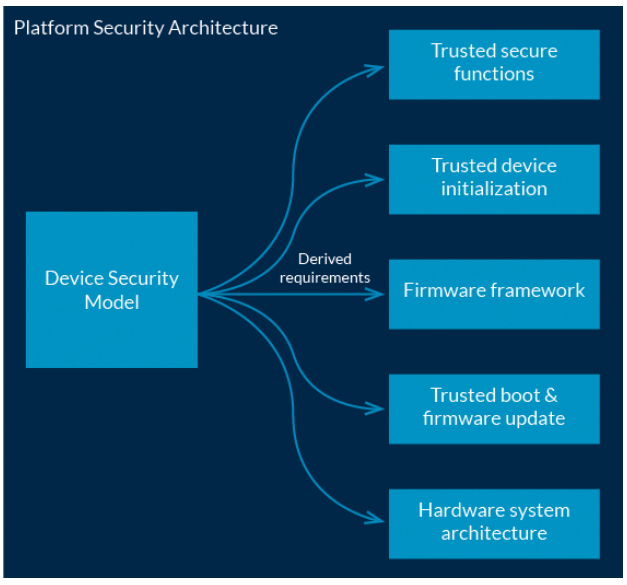
Robuste MicroSD-Karten für Embedded Systems und Kameras gibt es auch von anderen Firmen, darunter Transcend und Swissbit. Letztere hat auch Karten mit spezieller Firmware, etwa mit einem Leseschutz: Dadurch lassen sich gespeicherte Aufnahmen etwa einer Bodycam nur mit Passwort auslesen oder löschen. *(ciw@ct.de)*

# ARM trommelt für IoT-Sicherheit

Der britische Prozessorentwickler ARM gibt Designern und Programmierern von Embedded Systems Hilfestellung für sichere und vertrauenswürdige Produkte. Die Platform Security Architecture (PSA) ist eine Kombination aus Bedrohungsanalysen (Threat Models), Leitfäden, Hardware-Funktionsblöcken und passender Software. Sie soll es erleichtern, IoT-Geräte robuster gegen Attacken zu machen und somit einerseits Folgekosten zu senken, aber auch die Akzeptanz für IoT zu steigern – ARM möchte erreichen, dass es 2035 rund 1 Billion vernetzte Geräte gibt. Zum Scheitern dieses ambitionierten Plans könnten weiter zunehmende Probleme durch Sicherheitslücken oder unzuverlässige Funktionen beitragen. ARM versucht also auch aus ganz eigennützigen Gründen, die Situation zu verbessern.

2018 will ARM erste PSA-Spezifikationen veröffentlichen. Die Anleitungen zielen auf einfachere Controller mit Mikrocontroller-Kernen aus der Baureihe Cortex-M. Den meisten davon fehlt die TrustZone-Erweiterung der Cortex-A-Kerne, denn sie wäre für viele typische Einsatzgebiete von Cortex-M-Typen auch zu kompliziert und letztlich zu teuer. PSA soll auch bei ganz einfachen Geräten mit minimalistischen Echtzeitbetriebssystemen (RTOS) die Trennung unkritischen Codes von geschützter Firmware, Passwörtern sowie digitalen Signaturen und Schlüsseln ermöglichen.

ARM will eine Open-Source-Implementierung eines Secure Processing Environment (SPE) liefern, welches sich nach Spezifikationen wie Common Criteria EAL zertifizieren lässt. Wenn Chipentwickler stärkeren Schutz wünschen, können sie den Cortex-M künftig mit einer TrustZone CryptoCell kombinieren oder auch einem TrustZone CryptoIsland, welches ähnlich widerstandsfähig wie eine SmartCard sein soll. Bei Cortex-M23 und Cortex-M33 mit der Architektur ARMv8-M hat ARM hingegen bereits TrustZone integriert. *(ciw@ct.de)*




**ARMs Platform Security Architecture härtet IoT-Geräte gegen Angriffe.**