



Daric Security MCU

CR7SE01

ARM M7 MCU and integrated Secure Element
TSMC 22nm ULL Process Node

Data Sheet – Advanced Information

Features

- **Powerful ARM M7 CPU**
 - 800MHz CPU/400MHz AXI
 - FPU, double precision
 - MPU, 16 entries
 - Icache 16kB, Dcache 16kB
 - iTCM 256kB, dTCM 64kB
- **RISC-V CPU**
 - 400MHz CPU
 - MMU
 - Icache 16kB, Dcache 16kB
- **Large high-speed memory system**
 - 4MByte embedded NVM
 - RRAM robust against physical attack, aging, & environment
 - 2MByte main SRAM
 - Separate buffer RAM for I/O
 - 2x QSPI for off-chip memory
- **Flexible I/O set**
 - I2S, I2C
 - Q/SPIM, SPIs
 - Camera IF
 - SD Host
 - UART
 - USB2.0
 - QSPI Flash controller
 - Aux ADC/PWM DAC
 - GPIO/GPINT
- **Embedded Cryptographic Engine**
 - Isolated from CPU bus
 - Asymmetric cryptography
 - ECDSA, Schnorr, EdDSA and ECDH (secp256k1, P-256/384, ed25519, Curve25519)
 - RSA, up to 8192 bit
 - Symmetric cryptography
 - AES
 - Homomorphic Encryption
- **Paillier cryptosystem**
- **Hashes**
 - SHA2, SHA3/Keccak, RIPEMD160, BLAKE2/3
- **Authentication codes**
 - HMAC 256/512
- **High Speed TRNG**
- **Monotonic counters**
- **Logical security**
 - Boot / lifecycle protection
 - Test mode sealing / debug mode sealing
 - Crypto engine isolated from CPU
 - Detailed memory protection/privilege
- **Physical Countermeasures**
 - Active mesh
 - Glue cell network
 - Voltage glitch detection
 - Chip decap sensing
 - Thermal attack
 - Memory fault detection
 - False injection detection
 - Side channel protection, clock jitter, power balancing
 - Redundant key registers
 - Puzzle routing
 - Secret zeroization
- **Integrated PMU**
 - Operation from single supply
- **Software Development Kit**
- **Optional packages**
 - 188BGA 8mm X 8mm for MCU+SE function
 - 71 Ball WLCSP for limited function
 - KGD
- **Operational temperature**
 - -20C to 85C ambient



1 Description

Daric is a novel integrated general purpose Microcontroller Unit (MCU) and Secure Element (SE), all under a common umbrella of logical countermeasures (LCMs) and physical countermeasures (PCMs). The entire chip has the physical security of a typical SE, but unlike standalone SE chips, also has the computing power of a powerful general purpose MCU. By using novel RRAM and 22nm ULL technology, speed, power, memory size, and security are all markedly enhanced. Key Features include:

Integrated MCU and SE

- Integrating both functions on a single die reduces cost, power, and area, and enhances security.
- Shielded MCU can secure important functions outside of SE, such as user display and input, which otherwise are typically executed in a general purpose MCU outside of the shield of PCMs.
- Most advanced MCU in M-series (M7) with advanced features such as cache, TCM, floating point unit, AXI bus fabric.
- Alternate boot mode into RiscV system with MMU (separate SKU option).

Code and NV data are stored in Resistive RAM, with many advantages over legacy floating gate flash.

- Not readable by simple physical attack such as passive voltage contrast or electron microscopy.
- Long retention (does not leak charge continuously).
- Robust against magnetic fields and high energy particles.
- High memory density enabling larger code/data space than comparable MCUs.
- Integrated with small 22nm ULL process (which floating gate cannot be).

The advanced 22nm ULL process has many advantages in the context of secure MCU:

- Low cost, power, size
- High speed operation (800MHz)
- Higher memory sizes due to high NVM and SRAM density
- Small feature size is naturally more resistant to physical attack, FIB, probe, and inspection.
- Countermeasures are also more effective due to high feature density and lower emissions.

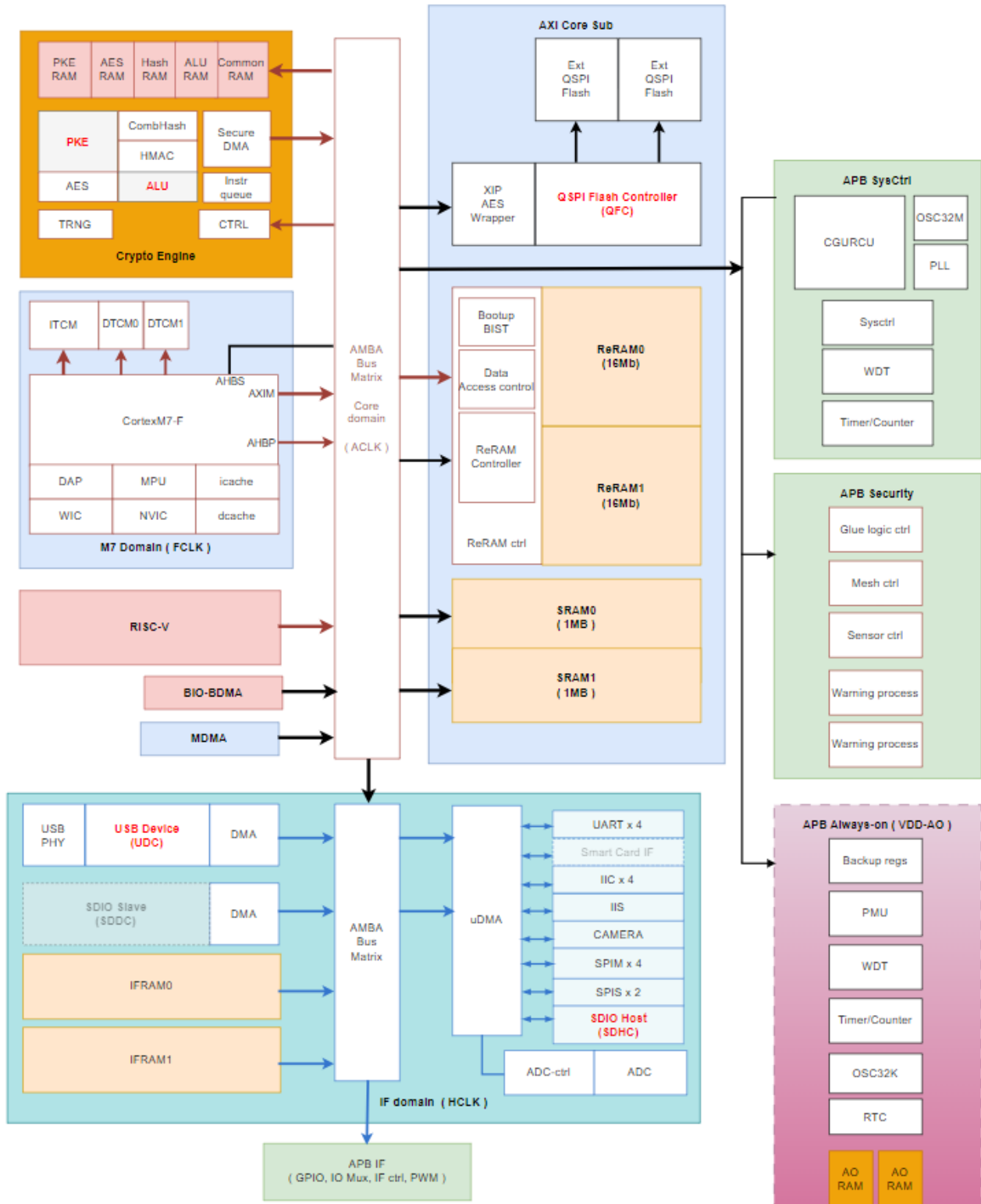
Advanced Cryptographic Architecture

- Support for modern curves and functions with known performance and security advantages
- High throughput and low latency
- Atomic functions may be chained together directly in SE
 - Has the system isolation and simplicity of a direct hardware SE
- Alternately, the MCU may access atomic functions
 - Thus entire chip, including MCU, may be used as a flexible, physically shielded, “super SE” for cryptographic innovation

Open Development

- Supported with devkit and open development tools
- Open source strategy unlike typical banking/payment SE's

2 Block Diagram



3 Revision History

Rev. #	Date	Changes
.1	June 14, 2022	Initial draft
.2	Feb 11, 2023	Updated Crypto Features, RiscV Option
3	March 11, 2025	Overhauled to reflect latest architecture, features and performance

©2025 Cromium Labs, Inc., all rights reserved. Pico™ is a trademark of Cromium Labs, Inc. All other brand or product names are trademarks of their respective holders. No license, express or implied, by estoppel or otherwise, is granted to any intellectual property rights that are disclosed by this document.

Disclaimers

The information provided herein (the "Disclosure") is provided solely for the evaluation and use of Cromium Labs, Inc. products. To the maximum extent permitted by applicable law: (1) The Disclosure is made available "AS IS" and with all faults, CRAMIUM LABS, INC. HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR ANY PARTICULAR PURPOSE; and (2) CRAMIUM LABS, INC. SHALL NOT BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE DISCLOSURE FOR ANY LOSS OR DAMAGE OF ANY KIND OR NATURE RELATED TO, ARISING UNDER, OR IN CONNECTION WITH, THE DISCLOSURE (INCLUDING YOUR USE OF THE DISCLOSURE), INCLUDING FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL LOSS OR DAMAGE (INCLUDING LOSS OF DATA, PROFITS, GOODWILL, OR ANY TYPE OF LOSS OR DAMAGE SUFFERED AS A RESULT OF ANY ACTION BROUGHT BY A THIRD PARTY) EVEN IF SUCH DAMAGE OR LOSS WAS REASONABLY FORESEEABLE OR CRAMIUM INC. HAD BEEN ADVISED OF THE POSSIBILITY OF THE SAME. Cromium Labs, Inc. products are not designed for or intended to be used for fail-safe performance, for medical use, for transportation, for energy production, for military use or for other critical applications. Cromium Labs, Inc. may change the Disclosure at any time and assumes no obligation to correct any errors contained in the Disclosure or to provide notification of updates to the Disclosure.