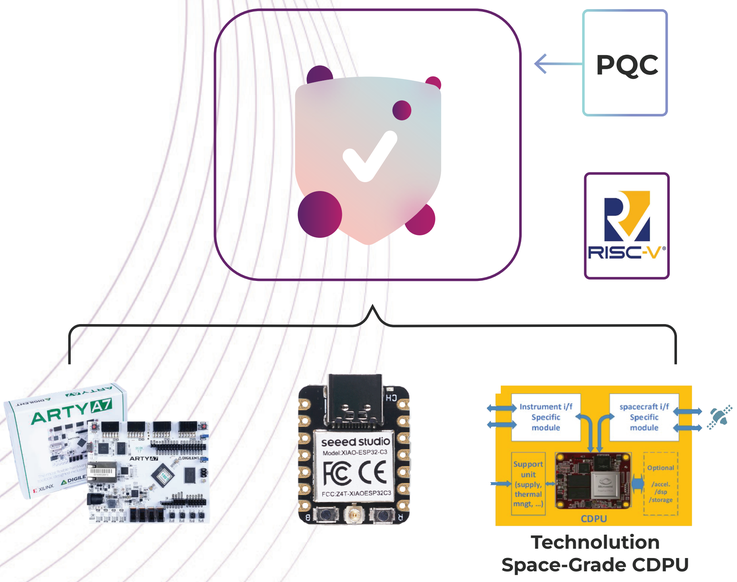
Building a RISC-V Bootloader for the Satellite Industry

Protect. Renew. Empower.

WE ARE LOOKING FOR PARTNERS TO TEST AND INTEGRATE OUR BOOTLOADER IN FULL, OR OUR SECURITY LIBRARY STANDALONE

Irdeto's RISC-V Bootloader Characteristics

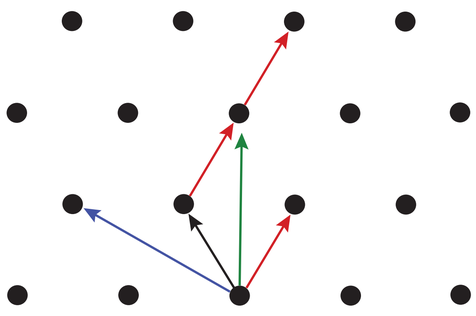
- Reliable and efficient, implemented in **both ROM and RAM**.
- Using **no external library dependency,** ensuring lightweight and portable design.
- **Small memory footprint**, optimizing resource use.
- **Predictable execution time**, enhancing stability (except for faultinjection countermeasures).
- Implements key services: 1, 3, 5, 6, 9, 20, and 128.
- **Minimal HAL** (Hardware Abstraction Layer) simplifies deployment on new chips.
- **Supports crypto agility** at runtime for adaptability.
- Going through an **independent code reviews process** (e.g. Riscure)
- **Comprehensive and reliable test suite.**



Technolution Space-Grade CDPU

WE HAVE CHOSEN FALCON, A PQC ALGORITHM, FOR SIGNATURE VERIFICATION

- FALCON Security is based on Lattices
- Hardware optimizations can be done with standard RISC-V ISA
  - **F Extension (Single-Precision Floating-Point)**
  - **D Extension (Double-Precision Floating-Point)**
  - Used in FFT/Gaussian sampling
- Reusable for other lattice base crypto: KEM/Kyber



NB : We plan to add other schemas in the future

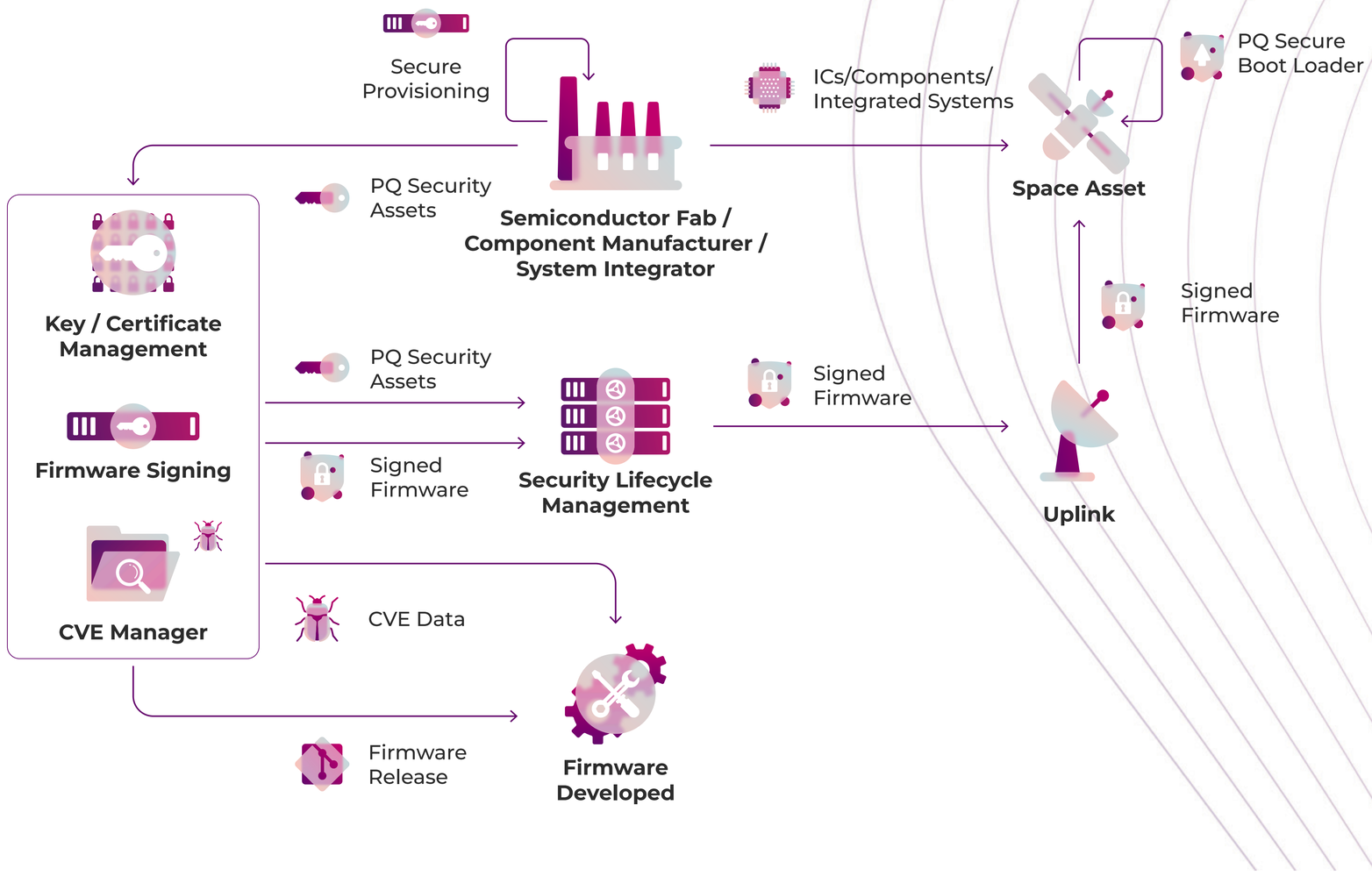
Scheme	Public Key Size	Private Key Size	Signature Size	Security Level
Falcon-512	897 bytes	1,280 bytes	666 bytes	NIST LEVEL 1
Falcon-1024	1,793 bytes	2,304 bytes	1,280 bytes	NIST LEVEL 5
Dilithium-2	1,312 bytes	2,528 bytes	2,420 bytes	NIST LEVEL 1
Dilithium-3	1,952 bytes	4,000 bytes	3,293 bytes	NIST LEVEL 3
Dilithium-5	2,592 bytes	4,864 bytes	4,459 bytes	NIST LEVEL 5
SPHINCS+-128s	32 bytes	64 bytes	80,80 bytes	NIST LEVEL 1
SPHINCS+-128f	32 bytes	64 bytes	17,088 bytes	NIST LEVEL 1
SPHINCS+-192s	48 bytes	96 bytes	16,976 bytes	NIST LEVEL 3
SPHINCS+-192f	48 bytes	96 bytes	35,664 bytes	NIST LEVEL 3
SPHINCS+-256s	64 bytes	128 bytes	29,792 bytes	NIST LEVEL 5
SPHINCS+-256f	64 bytes	128 bytes	49,216 bytes	NIST LEVEL 5

OUR LOADING PROTOCOL ADHERES TO THE PUS-C (ECSS) STANDARD

ECSS

SAVOIR IMA
space avionics open interface architecture

THE BOOTLOADER IS ONE KEY COMPONENT WITHIN IRDETO'S FULL SECURITY LIFECYCLE INFRASTRUCTURE



OUR EXPERTISE

PROVEN RELIABILITY
Robust bootloader (ROM/RAM) with flawless performance for over a decade.

WIDE DEPLOYMENT
Successfully deployed in millions of Set-Top Boxes (STBs).

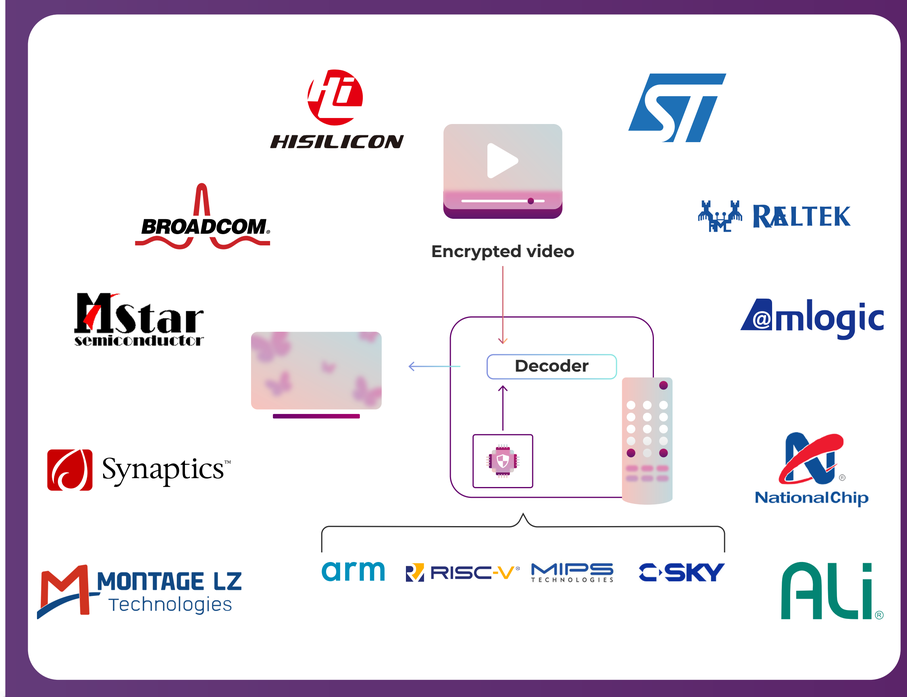
COMPREHENSIVE TESTING
Equipped with a robust test suite ensuring thorough validation of software and hardware.

ADVANCED SECURITY
Resilient against fault injection and side-channel attacks, ensuring secure operations.

SEAMLESS INTEGRATION
API providing streamlined hardware access for loaded applications.

EFFICIENT OTA UPDATES
Supports Over-the-Air updates via a proprietary protocol.

OPTIMIZED PERFORMANCE
Enables loading of RAM-based applications for video decoding.



WHY IS SECURE BOOTLOADING SO IMPORTANT?

PREVENT UNAUTHORIZED CODE EXECUTION
- Ensures only trusted firmware and software are loaded
- Blocks malicious or tampered code from running

PROTECT AGAINST CYBER THREATS
- Defends against malware, rootkits and unauthorized modifications
- Strengthens overall system security from the ground up

ENSURE DEVICE INTEGRITY
- Verifies firmware authenticity using cryptographic signatures
- Prevents unauthorized rollback to vulnerable versions

COMPLIANCE WITH SECURITY STANDARDS
- Meets industry regulations

BUILDS USER TRUST
- Provides assurance that the device operates safely and as intended
- Enhances reliability and brand reputation

CONTACT US