

Criptografia Pós-Quântica (PQC)

Estratégias de implementação em sistemas embarcados



A Leading Provider of Smart, Connected and Secure Embedded Control Solutions



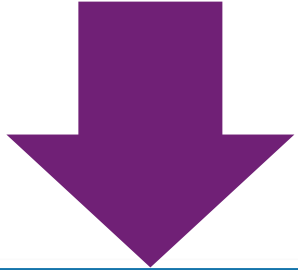
SMART | CONNECTED | SECURE

Rogério Moreira
Outubro 2026

Conteúdo



Conteúdo



Parte 1

Considerações gerais
sobre PQC



Parte 2

Portfolio de
produtos Microchip
para Criptografia
clássica e PQC

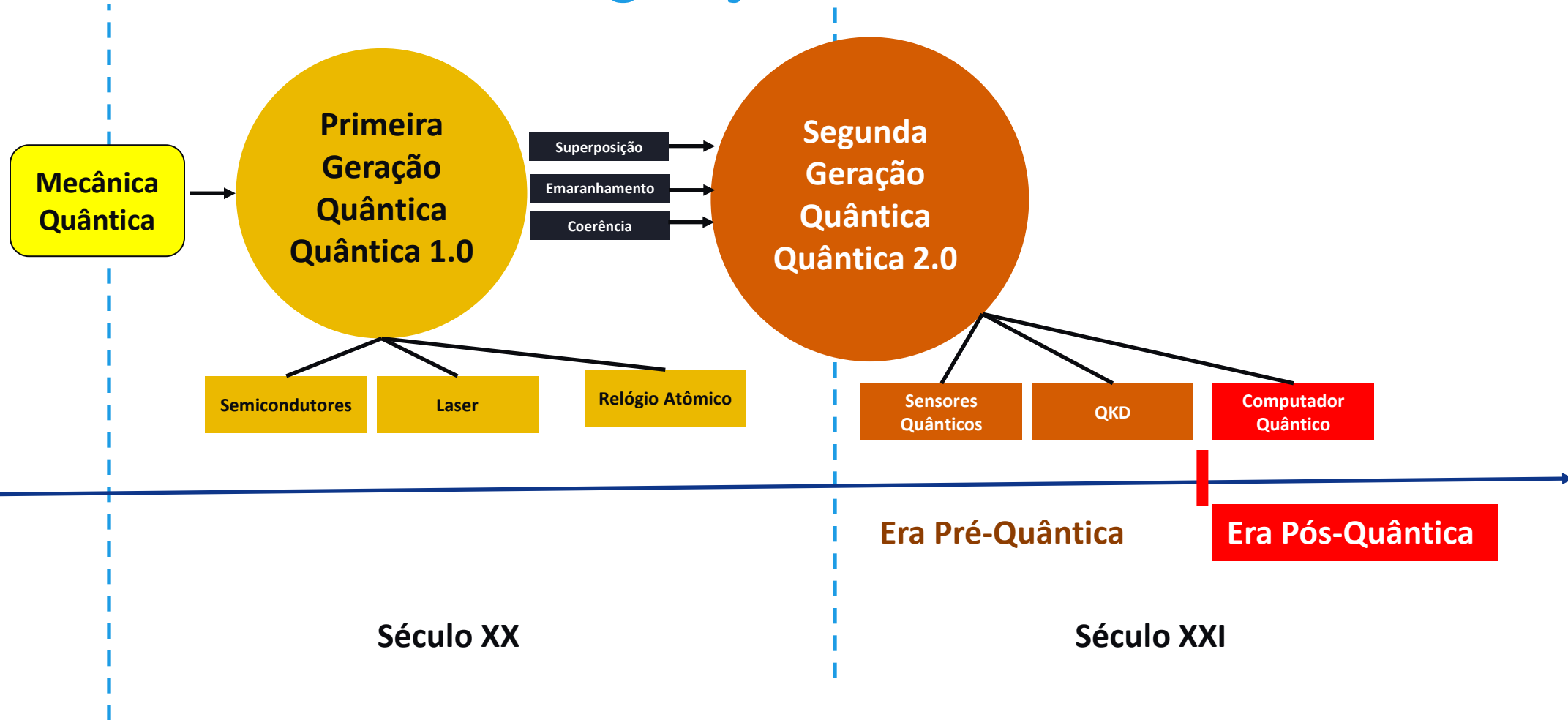


Parte 3

Estratégias de
Implementação PQC

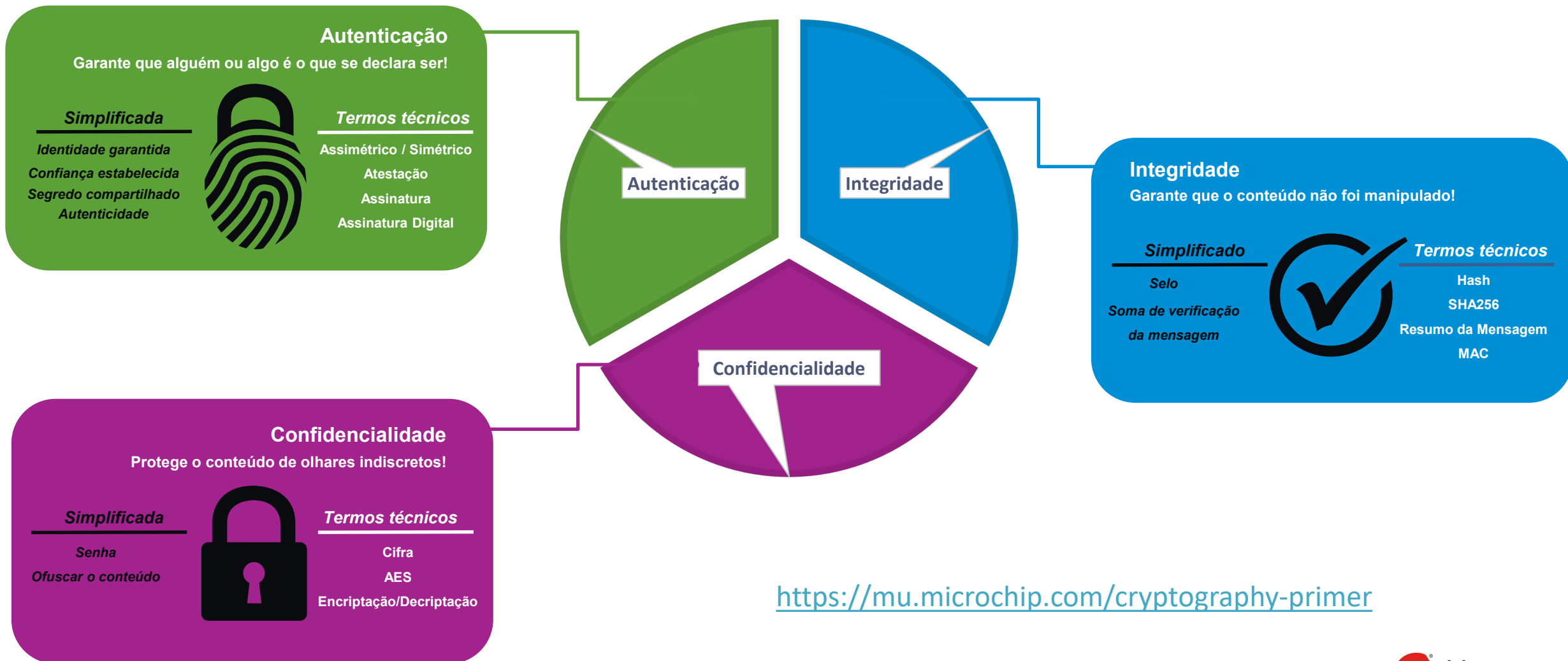
Tecnologias quânticas

Duas gerações



Segurança de Sistemas de Informação

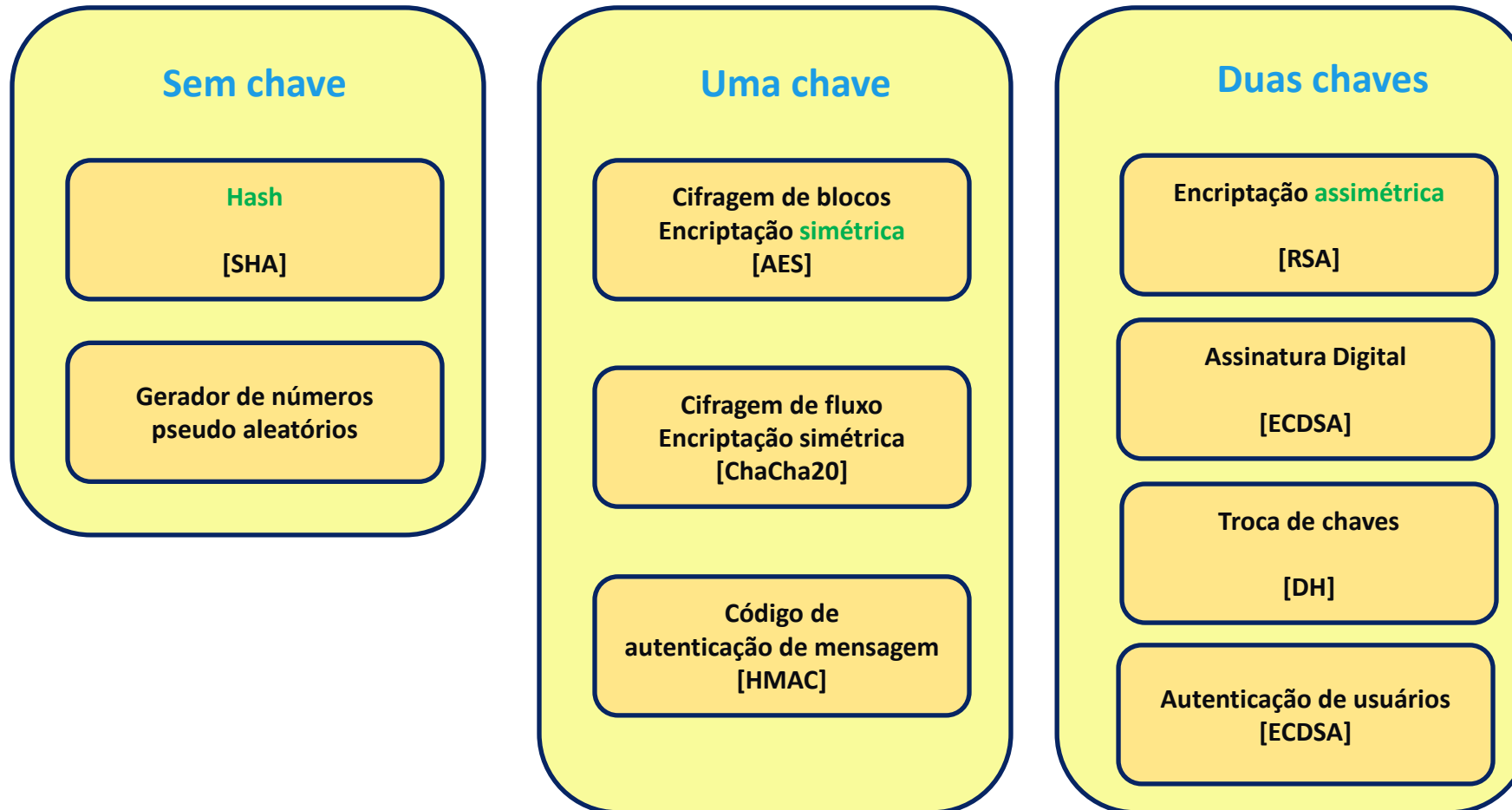
Sistemas seguros baseiam-se em três fundamentos.



<https://mu.microchip.com/cryptography-primer>

Criptografia

Algoritmos básicos



Criptografia

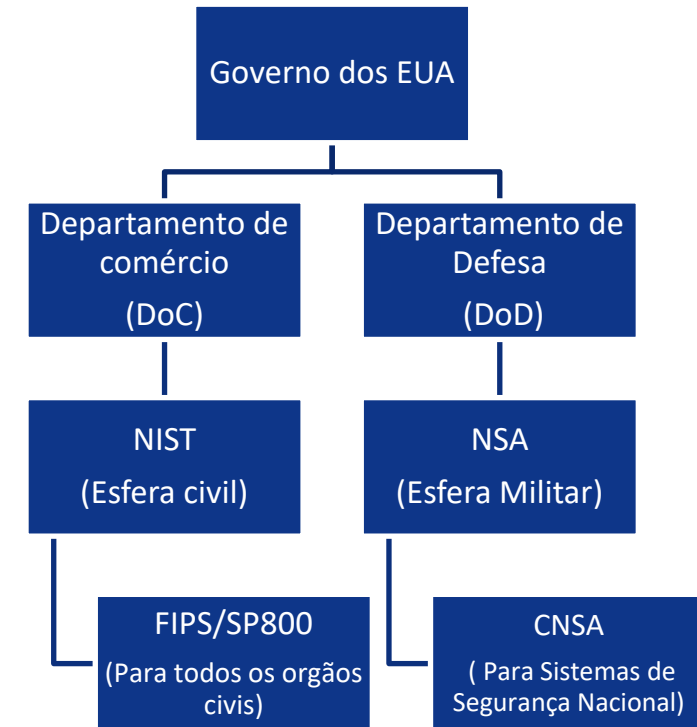
	Sem Chave	Uma Chave	Duas Chaves
Autenticação	Não se aplica	AES	ECDSA
Integridade	SHA-384	HMAC-SHA384	RSA
Confidencialidade	Não se aplica	AES	RSA

Obs.:Lista não exaustiva , só citando alguns exemplos.

CNSA Suite 1.0

(★ 2015)

Função criptográfica	Algoritmos aprovados	Especificação	Parâmetros mínimos /Tamanho de chave
Hash	SHA	FIPS Pub 180-4	SHA-384
Criptografia simétrica	AES	FIPS Pub 197	256-bit keys (FIPS 197)
Assinatura digital	ECDSA	FIPS Pub 186-4	Curve P-384
	RSA		Min. módulo de 3072-bit
Trocas de chaves	ECDH	NIST SP 800-56A	Curve P-384
	DH	IETF RFC 3526	Min. módulo de 3072-bit
	RSA	NIST SP 800-56B rev 1	Min. módulo de 3072-bit



Criptografia clássica

Força dos algoritmos usando computação clássica

Algoritmo e Tamanho da Chave	Bits de Segurança Reais	Espaço de Chaves (Combinações)	Tempo Estimado para Quebra (Computação Clássica)	Status de Segurança Atual
DES (56 bits)	56 bits	$2^{56} \approx 7.2 \times 10^{16}$	Segundos a poucas horas	Totalmente obsoleto. Quebrado nos anos 90.
3DES (168 bits)	112 bits	$2^{112} \approx 5.1 \times 10^{33}$	~1 bilhão de anos	Obsoleto/Legado. Vulnerável a ataques de colisão (Sweet32) e descontinuado pelo NIST.
RSA-1024	~80 bits	$2^{80} \approx 1.2 \times 10^{24}$	Meses a poucos anos (via fatoração GNFS)	Inseguro. Banido para novos usos por agências de segurança.
ECC-256	128 bits	$2^{128} \approx 3.4 \times 10^{38}$	~ 10^{18} anos (Trilhões de vezes a idade do universo)	Seguro contra computadores clássicos.
AES-128	128 bits	$2^{128} \approx 3.4 \times 10^{38}$	~ 10^{18} anos (Trilhões de vezes a idade do universo)	Altamente seguro. Padrão comercial global.
RSA-2048	~112 bits	$2^{112} \approx 5.1 \times 10^{33}$	~1 bilhão de anos (via fatoração GNFS)	Seguro a curto prazo. Sendo gradualmente substituído.
AES-256	256 bits	$2^{256} \approx 1.1 \times 10^{77}$	incalculável (> 10^{50} anos. Exige mais energia do que o Sol produzirá)	Imbatível por força bruta. Nível militar/governamental.

**Então por que usar a
Criptografia Pós-Quântica (PQC)?**

Algoritmo de Shor (1994)



O Computador Quântico

quebra

- RSA
- ECC

pode ser paralelizado

Algoritmo de Grover (1996)



O Computador Quântico

enfraquece levemente

- AES
- SHA
- HMAC

não pode ser paralelizado

Criptografia clássica

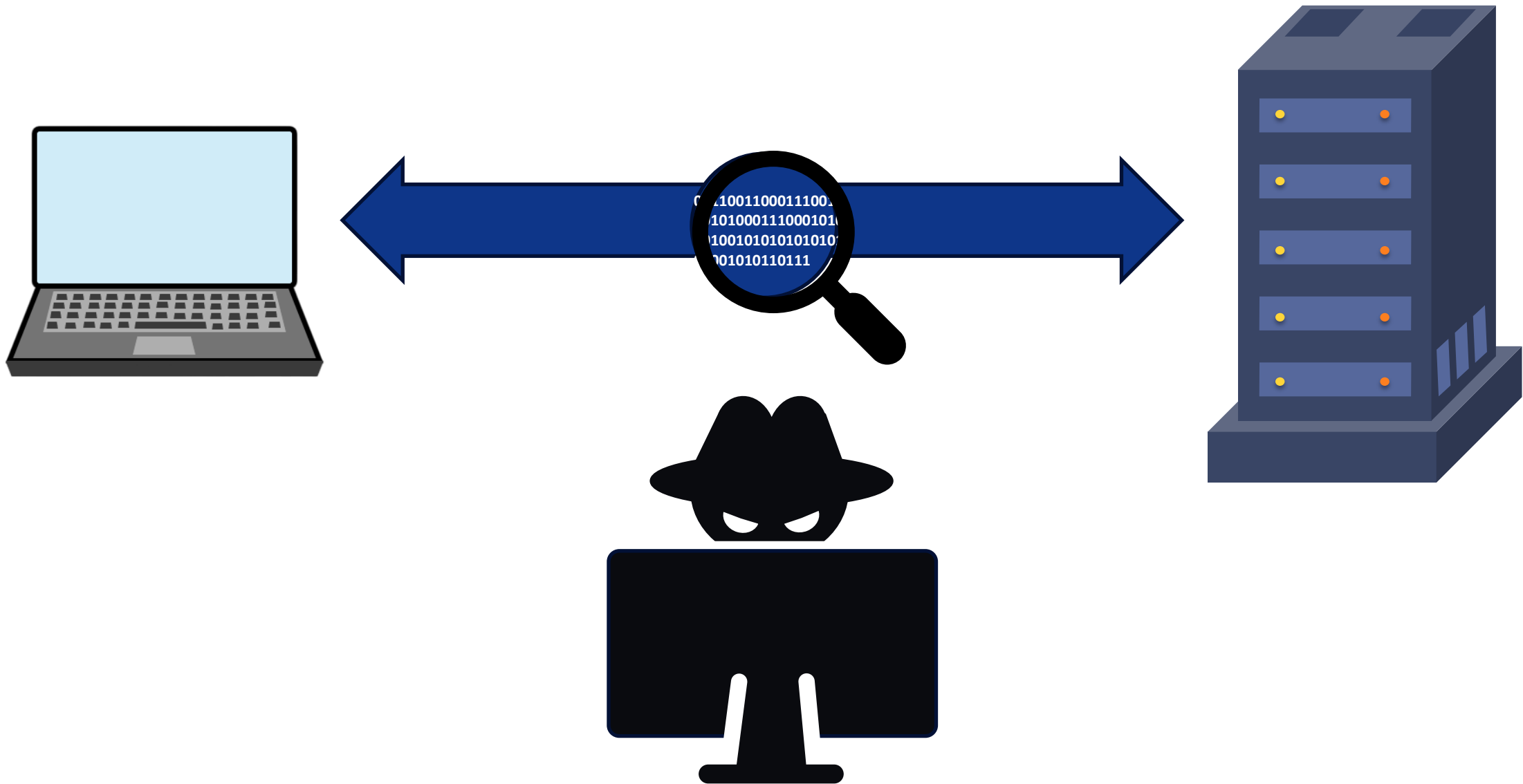
Força dos algoritmos usando computação quântica

Algoritmo	Segurança clássica	Segurança contra ataque quântico	Situação	O que acontece na matemática?
DES	56 bits	28 bits	Já quebrado (mesmo sem quântico)	Chave curta demais: já é vulnerável a computadores convencionais.
RSA-2048	~112 bits	~0 bits	Quebrado	O Algoritmo de Shor resolve a fatoração de inteiros em tempo polinomial.
ECC-256	128 bits	~0 bits	Quebrado	O Algoritmo de Shor também resolve o logaritmo discreto em curvas elípticas.
AES-128	128 bits	64 bits	Enfraquecido	O Algoritmo de Grover reduz pela metade os bits de segurança (de 2^{128} para 2^{64} operações).
AES-256	256 bits	128 bits	Seguro	Mesmo com o Grover, restam 2^{128} operações: continua inviável de quebrar.

CNSA Suite 1.0

(★ 2015 - †2033)

Função criptográfica	Algoritmos aprovados	Especificação	Parâmetros mínimos /Tamanho de chave
Hash	SHA	FIPS Pub 180-4	SHA-384
Criptografia simétrica	AES	FIPS Pub 197	256-bit keys (FIPS 197)
Assinatura digital	ECDSA	FIPS Pub 186-4	Curve P-384
	RSA		Min. módulo de 3072-bit
Trocas de chaves	ECDH	NIST SP 800-56A	Curve P-384
	DH	IETF RFC 3526	Min. módulo de 3072-bit
	RSA	NIST SP 800-56B rev 1	Min. módulo de 3072-bit



Harvest Now/Decrypt Later

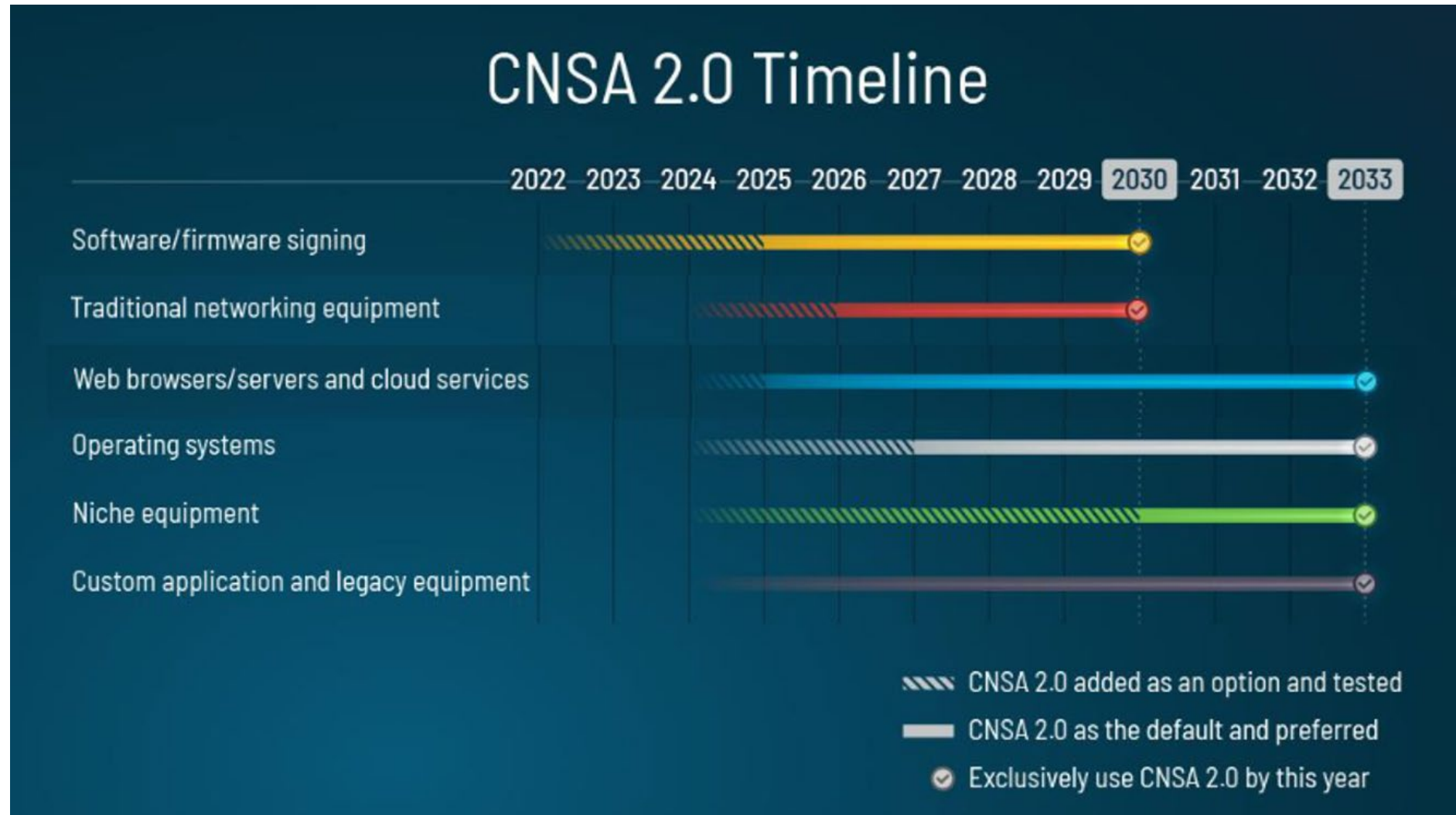
CNSA 2.0

(★ 2027 - †tbd)

Função criptográfica	Algoritmos aprovados	Especificação	Parâmetros mínimos /Tamanho de chave
Hash	SHA	FIPS Pub 180-4	SHA-384 ou SHA-512
Criptografia simétrica	AES	FIPS Pub 197	Chave com 256 bits
Assinatura digital	ML-DSA-87 (Module-Lattice-Based Digital Signature Algorithm, nome antigo: CRYSTALS-Dilithium)	FIPS 204	
Trocas de chaves	ML-KEM-1024 (Module-Lattice-Based Key Encapsulation Mechanism, nome antigo: CRYSTALS-Kyber)	FIPS 203	
Assinatura de software e firmware	LMS (Leighton-Micali Signature)	NIST SP 800-208	SHA-256/192
	XMSS (Extended Merkle Signature Scheme)		

De CNSA Suite 1.0 para 2.0

Cronograma de mudança



Por que migrar agora para o CNSA 2.0

Commercial National Security Algorithm Suite 2.0 (NSA)

Set/2022

NSA anuncia o CNSA 2.0 em substituição ao CNSA 1.0

Ago/2024

NIST finaliza FIPS 203 e FIPS 204, após processo de 7 anos

NSS

Obrigatório para todos os Sistemas de Segurança Nacional

O que muda

- Toda a criptografia de chave pública vulnerável à computação quântica
- Troca de chaves (ECDH/DH) e assinaturas (RSA/ECDSA)
- Base: NIST FIPS 203, FIPS 204 e SP 800-208

O que permanece

- AES-256 (criptografia simétrica)
- SHA-384 / SHA-512 (hashing)
- Foco da migração: somente a camada de chave pública

Os novos algoritmos

O que substitui o quê em sistemas embarcados

ML-KEM-1024

FIPS 203

Encapsulamento de chaves

- Substitui ECDH e DH
- Reticulados (Module-LWE)
- Níveis 512 / 768 / 1024

*Chave pública ML-KEM-768: ~1.184 bytes
(~37× X25519)*

ML-DSA-87

FIPS 204

Assinaturas digitais

- Substitui RSA e ECDSA
- Reticulados (Module-LWE)
- Níveis 44 / 65 / 87

Assinatura ML-DSA-87: 4.627 bytes (vs. 64 bytes Ed25519)

LMS / XMSS

NIST SP 800-208

Assinatura de firmware e software

- Baseados em hash, com estado
- Raízes de confiança de longa duração
- NSA prefere LMS SHA-256/192

Segurança depende apenas da função de hash

Atenção: SLH-DSA (SPHINCS+, FIPS 205) é padrão NIST, mas não é aprovado para NSS sob o CNSA 2.0.

O que muda na implementação

O custo real está no tamanho, não na CPU

chaves públicas maiores que as clássicas

25–50×

assinaturas maiores que as clássicas

40–80×

ML-KEM-512 no Cortex-M0+
(17× mais rápido que ECDH-P256)

35,7 ms

Planeje antes de implantar

- TLS ClientHello com ML-KEM-768 costuma ocupar dois pacotes
- Fragmentação de protocolo e MTU
- Largura de banda, memória e cadeias de certificados
- Cache e armazenamento de sessões

Agilidade criptográfica e CBOM

Arquitetura que sobrevive a qualquer algoritmo específico

Agilidade criptográfica

Trocar algoritmos, chaves e protocolos sem reprojeter o sistema.

- Pilares: modularidade, camadas de abstração, políticas, observabilidade
- **NIST CSWP 39 (dez/2025)**: de termo da moda a prática de projeto
- Em embarcados, as escolhas são feitas cedo: planeje desde o início
- FIPS 140-3

CBOM

Lista de Materiais Criptográficos

- Inventário de algoritmos, chaves, protocolos e certificados
- Complementa a SBOM
- Primeiro passo de qualquer migração: não se migra o que não se vê
- **OWASP Cyclone DX / ECMA-424**

Esta não será a última migração. Prepare-se também para a próxima.

Plano de ação de migração

Seis passos para começar hoje

1

Inventário

Crie a CBOM e mapeie todo uso de RSA, ECDH, ECDSA e DH

2

Priorização

Dados de longa duração e raízes de confiança do firmware (risco HNDL)

3

Piloto

TLS híbrido em fluxos não críticos; meça o impacto em tamanho e latência

4

Arquitetura

Abstrações de agilidade criptográfica antes de trocar algoritmos

5

Firmware

Gestão de estado LMS/XMSS e infraestrutura de assinatura com HSM

6

Padrões

Validação FIPS 140-3, prazos do CNSA 2.0 e drafts híbridos da IETF

Conteúdo



Parte 1

Considerações gerais
sobre PQC



Parte 2

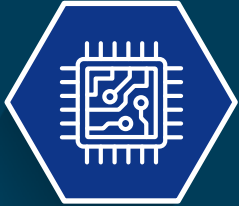
Portfolio de
produtos Microchip
para Criptografia
clássica e PQC



Parte 3

Estratégias de
Implementação
PQC

Portfolio de produtos da Microchip



Processors

8-, 16- & 32-Bit Microcontrollers
Digital Signal Controllers
32- & 64-bit Microprocessors
FPGAs and PLDs



Connectivity

CAN, CAN2 and CAN FD
Bluetooth®, Wi-Fi®, Zigbee®
Ethernet, Optical Networking
RF Modules & Microwave Solutions



Touch

MaxTouch® Touchscreen Controllers
GestIC® Air Gesture Controllers
Proximity Touchscreens
MCUs with Capacitive Touch



Sensor & Motor Drive

Current/Voltage/Power Monitor ICS
CO/Smoke Detector Horn Driver ICS
Motor Drivers, Temperature
Sensors, Inductive Position Sensors



Security Products

Authentication ICs
Root of Trust Controllers
MCUs w/ Integrated Security
Secure FPGAs and SoC FPGAs



Interface & Connectivity

Ethernet Switches, PHYs, Controllers
Power-over-Ethernet (PoE)
LIN Bus Networking
Line Circuits and Drivers
PCIe® Switches
USB Hubs, Switches and Transceivers
USB-C Power Delivery Controllers



Analog & Mixed Signal

Op Amps, INAs & PGAs
DACs & ADCs
AC/DC Power & Energy Devices
Current/Voltage/Power Monitors
Digital Potentiometers
Voltage References, Comparators



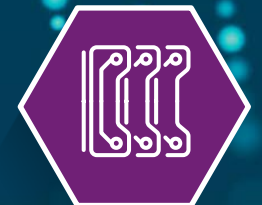
Power Management

Silicon Carbide Products
MOSFETs
LDOs and Battery Management
DC-DC Switching Converters
Voltage Supervisors & References
Battery Chargers Gate Drivers
AC-DC Power Converters
Electromechanical Voltage Relays



Clock & Timing

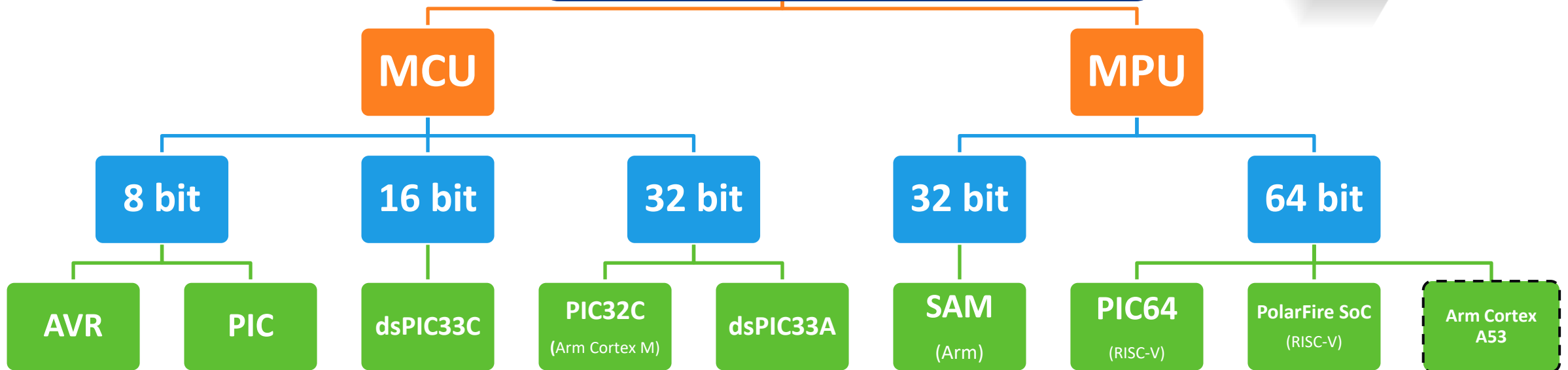
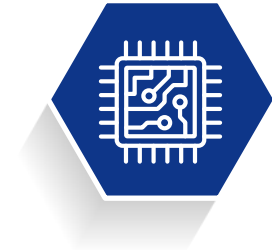
Atomic Clocks
GNSS Disciplined Oscillators
Clock Generators and Buffers
Oscillators
Real-Time Clocks
Jitter Attenuators
PCIe™ Timers
High Performance Timing Systems



Memory & Storage

Serial EERAM & Serial EEPROM
Serial & Parallel FLASH Memory
Serial SRAM & Serial NVSRAM
Adaptec Host Bus Adaptor
Adaptec® SmartRAID RAID Adaptors
Smart IOC I/O Controllers
SXP SAS Expanders

Processadores



Diferenciais tecnológicos dos processadores



Ultra-Low Power

Fast Wake-up
Power Gating
Intelligent Peripherals
SleepWalking™
Event System



Touch

Ultra-low power
Buttons, wheels,
sliders & touchpad
Level Sensing
Gestures
Hands-Off Detection
Independent Hardware



Motor Control

Visual Design Tools
Multi-motor support
Fast Analog
MATLAB/Simulink
based model support
Wide range of
algorithms and demos



Security

Scalable Solutions
Secure Boot
Secure Key Storage
HW Crypto
Acceleration
Hardware Security Modules
(HSM)
Factory Provisioning



Functional Safety

IEC 60730, IEC 61508,
and ISO 26262
Certified Hardware &
Software Libraries
Complete Safety
Collateral
Hardware Safety
Features



Graphics

Segment LCD
2D Accelerators
Visual Design Tools
Design Simulator
Professional Demos
RTOS & Linux Support



Connectivity

Gigabit Ethernet
High-speed USB
CAN-FD
Bluetooth
Wi-Fi
ZigBee
Power Line
Communication (PLC)

Key Markets: Medical, Appliance, Automotive, Industrial, Smart Home IoT, Smart Energy, Consumer

PIC32C MCU (Arm 32 bit)

Entry Level ARM (Arm Cortex M0+ & M23)

Up to 72MHz
512KB Flash
128KB RAM
HSM-Lite
2x CAN-FD
Full Speed USB
100-pins

PIC32CM

Entry Level Families

Arm Cortex M0+, M23
Up to 100 DMIPS

Mid Range ARM (Arm Cortex M4 & M33)

Up to 120MHz
2MB Flash
256KB RAM
HSM Options
2x CAN-FD
2x FS/HS Speed USB
10/100 Ethernet
144-pins

PIC32CK
PIC32CX

Mid Range Families

Arm Cortex M4F, M33
100 - 200 DMIPS

High End ARM (Arm Cortex M7)

Up to 300MHz
8MB Flash
1MB RAM
HSM Options
6x CAN-FD
2x HS USB
GB Ethernet
208 pins

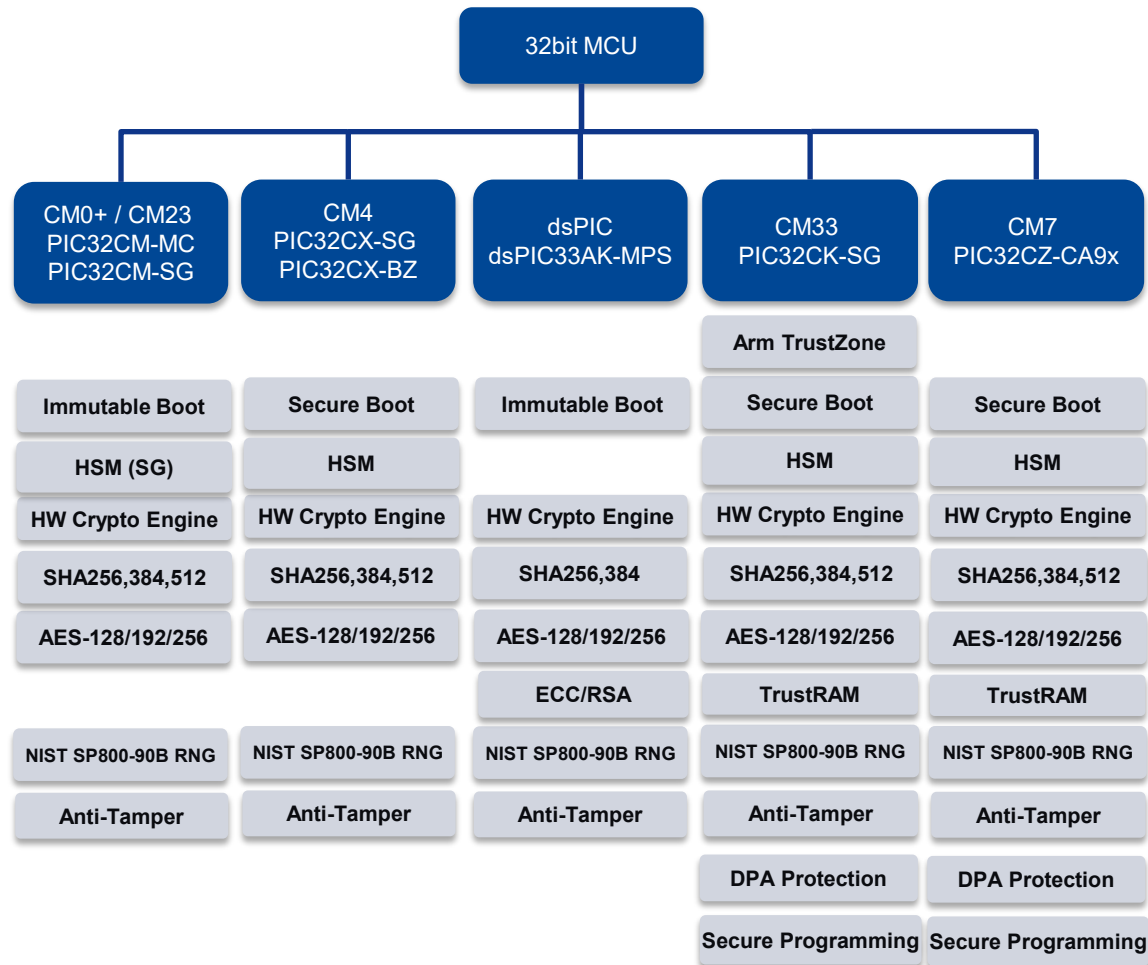
PIC32CZ

High End Families

Arm Cortex M7
300- 600 DMIPS

MCU 32 bit

Funcionalidades para criptografia



MPUs Microchip 32-bit

Entry Level, Low-Power ARM9, Cortex-A5 and A7 up to 1GHz

SAM9X60

Up to 600MHz
Secure Boot
LCD
2D HW Accel
I2S, Class D
Dual Ethernet
QSPI
AEC-Q100

System in Package
D6K - 64Mb SDRAM
D5M - 512Mb DDR2
D1G - 1Gb DDR2

System On Module

SAM9X7x Series

Up to 800MHz
DDR3L support
MIPI DSI/CSI
LVDS
CAN-FD
Giga Ethernet
Octal SPI
PUF
AEC-Q100

System in Package
D5M - 512Mb DDR2
D1G - 1Gb DDR3L
D2G - 2Gb DDR3L

System On Module
In Development

SAMA5D2 Series

Up to 500MHz
DDR3 support
PCI security
10/100 Ethernet
Up to 128 I/O
CAN, USB, QSPI
AEC-Q100

System in Package
D1M - 128Mb DDR2
D5M - 512Mb DDR2
D1G - 1Gb DDR2
LD1G - 1Gb LPDDR2
LD2G - 2Gb LPDDR2

System on Module

SAMA5D3 Series

Up to 536MHz
10/100 Ethernet
Giga Ethernet
Up to 160 I/O
CAN, USB

Connectivity



SAMA5D4 Series

Up to 600MHz
720p Video
Decoder
Dual 10/100
Ethernet
Advanced Security
Up to 152 I/O
USB

Video



SAMA7G54

Up to 1GHz
533MHz DDR3
MIPI Camera
10/100 Ethernet
Giga Ethernet
Audio
6x CAN-FD
QSPI, Octal SPI
Up to 136 I/O
AEC-Q100

System in Package
D1G - 1Gb DDR3L
D2G - 2Gb DDR3L
D4G - 4Gb DDR3L

System On Module
In Development

SAMA7D65

Up to 1GHz
533MHz DDR3
MIPI DSI, LVDS
2D GPU
Dual Giga
Ethernet w/ TSN
PUF, Audio, I3C
5x CAN-FD
QSPI, Octal SPI
Up to 142 I/O
AEC-Q100

System in Package
D5M - 512Mb DDR2
D1G - 1Gb DDR3L
D2G - 2Gb DDR3L
D4G - 4Gb DDR3L

System On Module
In Development

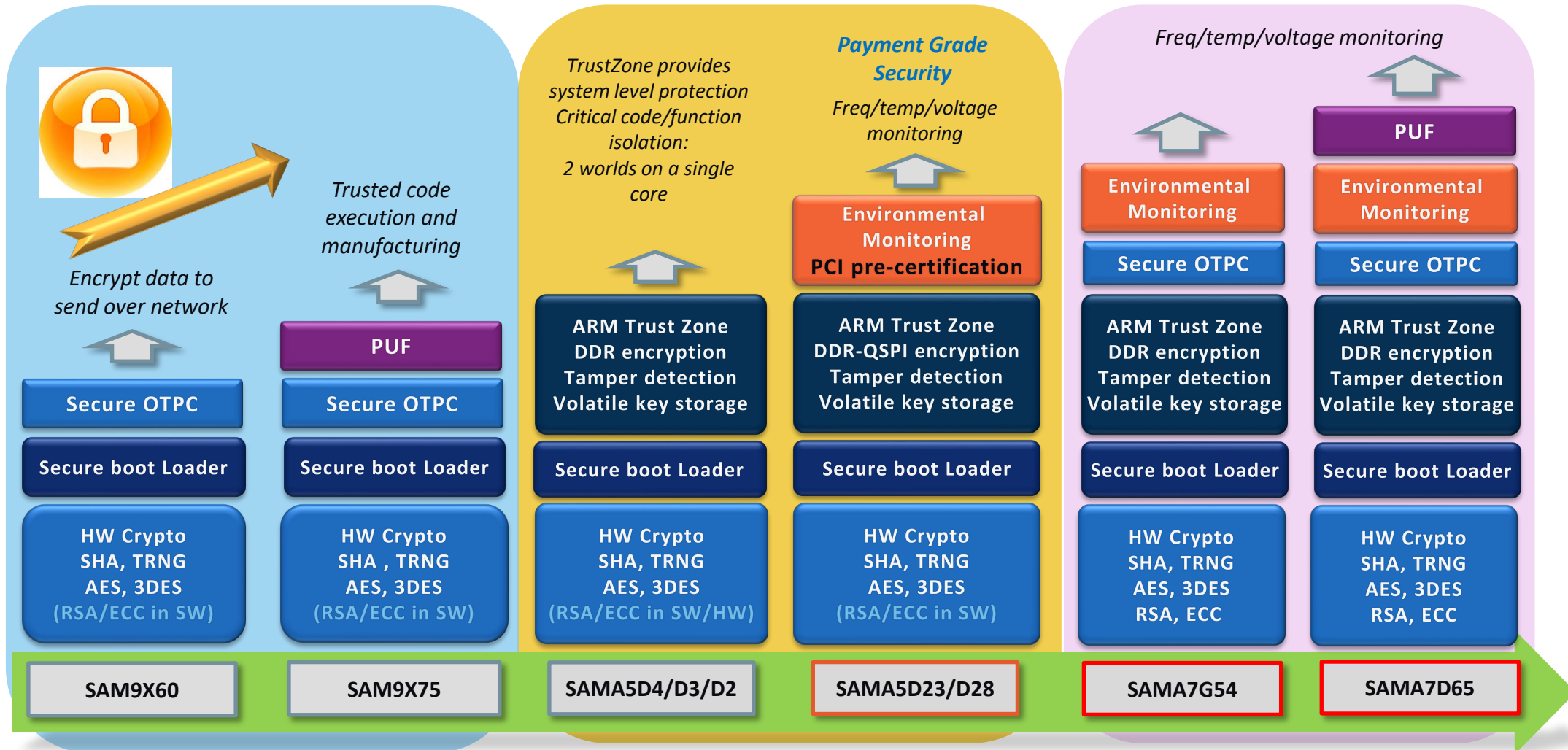
Entry Level: ARM9
Up to 800 MHz / 880 DMIPS

Arm Cortex A5
Up to 600 MHz / 940 DMIPS

Arm Cortex A7
1 GHz / 1900 DMIPS

MPU 32 bit

Funcionalidades para criptografia



PIC64™



Flexible and Scalable Compute



Diverse End Markets

Industrial



Automotive



Consumer



Defense



Aviation



Communications



Scalable Radiation Performance



Rad-Hard



Rad-Tolerant



Engineering Model

Multiple Mission Profiles

Satellites



Spacecraft



Rovers/Landers

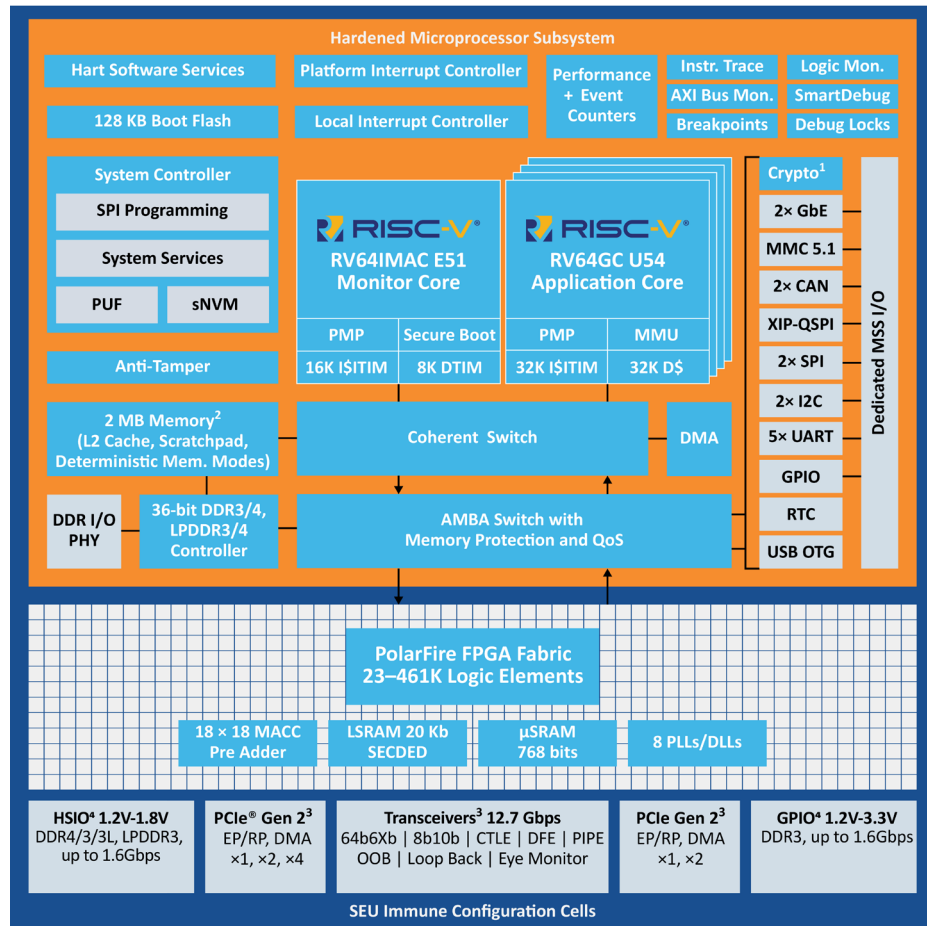


Microchip 64-bit Processing Solutions

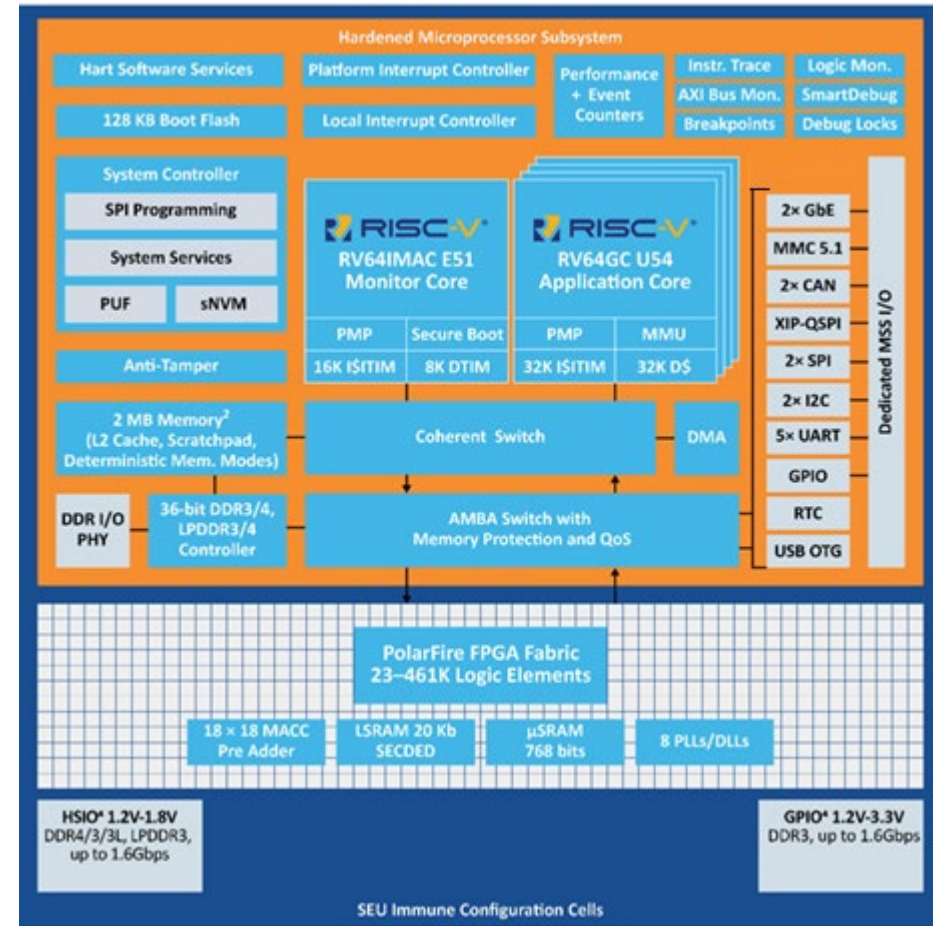
	PIC64[™] GX		PIC64[™] HX	PIC64[™] HPSC
Product	GX1000	GX1100	HX1000	HPSC1000
64-bit Application CPUs	4x RISC-V (U54)	4x RISC-V (U54)	8x RISC-V X280	8x RISC-V X280
64-bit Application CPUs DMIPs	5k	5k	26k	26k
Processing Modes	SMP and AMP	SMP and AMP	SMP, AMP, Virtualization, DCLS	SMP, AMP, Virtualization, DCLS
Real Time Optimizations	Yes	Yes	Yes	Yes
Virtualization	No	No	Yes	Yes
AI / Vector Processing	No	Yes	Yes – 2 TOPS	Yes – 2 TOPS
System Controller / Monitor	Yes – 64-bit RISC-V	Yes – 64-bit RISC-V	Yes – 64-bit RISC-V	Yes – 64-bit RISC-V
Video Features	Yes	ML, H.264, DSI-2	No	No
Ethernet Interfaces	2x GbE	2x GbE	Switch: 16x Up to 10GbE Non-Switch: 4x Up to 10GbE	Switch: 16x Up to 10GbE Non-Switch: 4x Up to 10GbE
TSN Ethernet Switch	No	No	Yes	Yes
PCIe / CXL	x1/ x4 Gen 2 Host	x1/ x4 Gen 2 Host	2 x1/ x4 / x8 Gen 3 Interfaces 2x CXL2.0	2 x1/ x4 / x8 Gen 3 Interfaces 2x CXL2.0
Secure Boot	Yes	Yes	Yes – with Post Quantum	Yes – with Post Quantum
User Crypto Acceleration	Yes	Yes	Yes – with Post Quantum	Yes – with Post Quantum
Qualification	Ext Commercial / Industrial	Ext Commercial / Industrial	Industrial + Auto/Hi-Rel	Radiation-Hardened / Tolerant

FPGA PolarFire

PolarFire SoC FPGA



PolarFire Core SoC FPGA



Security and Computing Group (SCG)

Unidade de negócios dedicada a segurança



Conteúdo



Estratégias de implementação

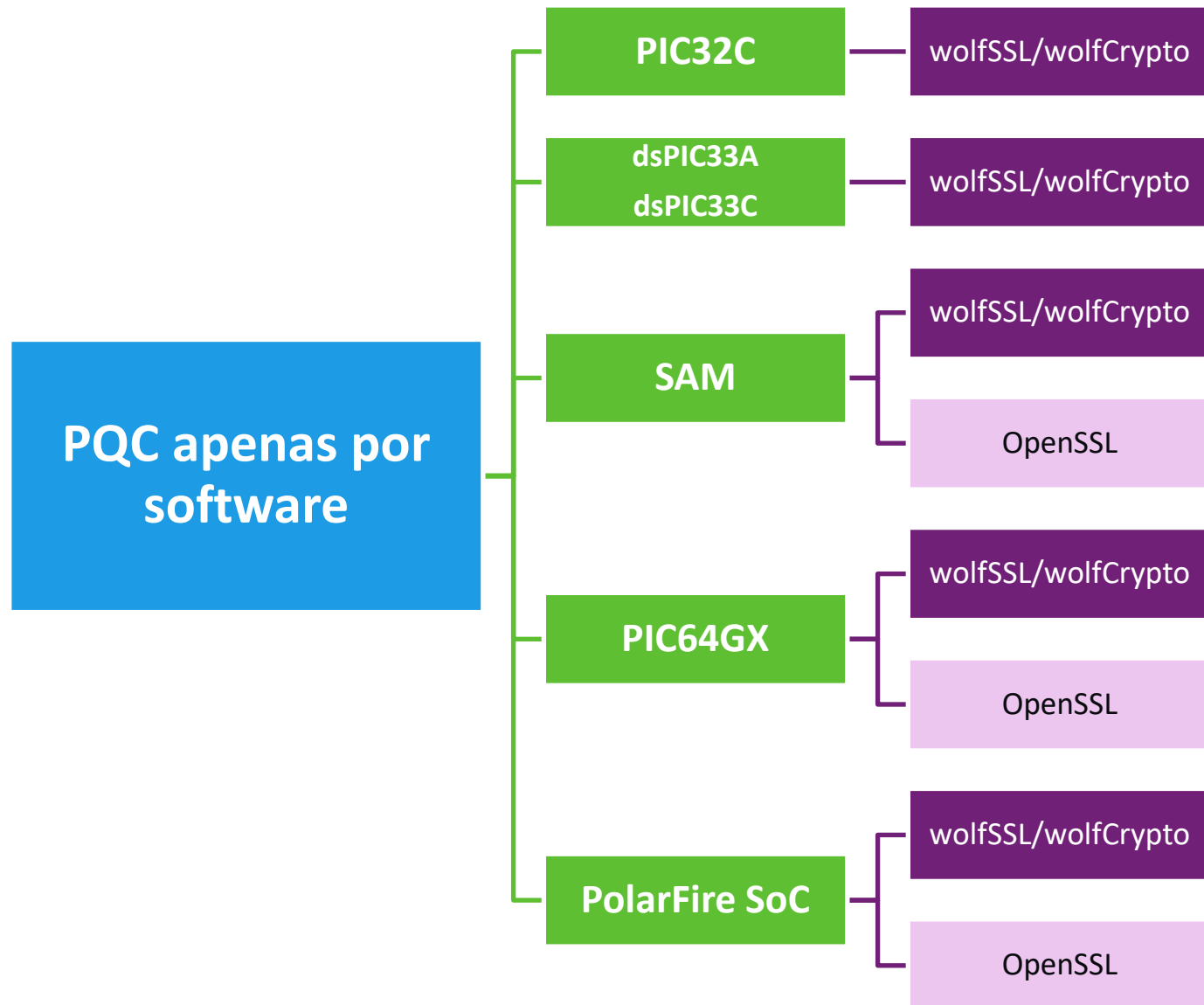
PQC apenas por software

PQC acelerada por hardware

PQC por
hardware dedicado
c/ Root of Trust

PQC
acelerada por FPGA

Migração híbrida
(Criptografia clássica+PQC)



wolfSSL / wolfCrypt: cobertura PQC

Os algoritmos do CNSA 2.0 em uma biblioteca para embarcados

Algoritmo	Padrão	Uso	No wolfCrypt
ML-KEM 512/768/1024	FIPS 203	Troca de chaves (TLS/DTLS 1.3)	Puro ou híbrido com ECDH
ML-DSA 44/65/87	FIPS 204	Assinaturas e certificados X.509	Assinatura e verificação
LMS	SP 800-208 · RFC 8554	Firmware e secure boot	Todos os parâmetros da RFC 8554
XMSS	SP 800-208 · RFC 8391	Firmware e secure boot	Parâmetros SHA-256 do SP 800-208

Algoritmos PQC do wolfCrypt validados no NIST CAVP (certificado #A8437)

TLS 1.3 híbrido com wolfSSL

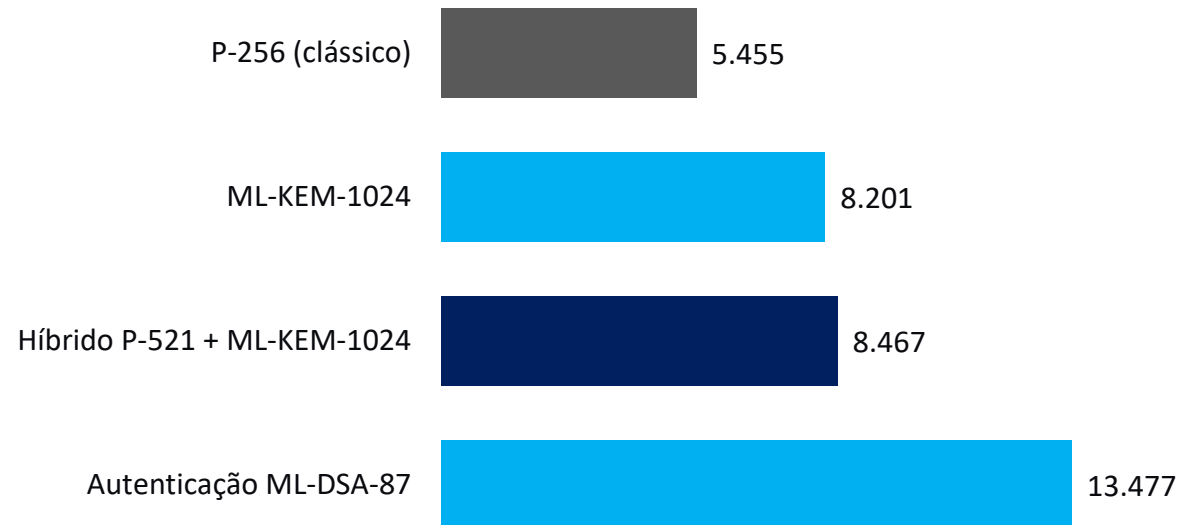
Grupos padronizados e o custo real no handshake

Grupos híbridos padrão

- X25519MLKEM768
- SecP256r1MLKEM768
- **SecP384r1MLKEM1024** — nível do CNSA 2.0
- ML-KEM puro 512/768/1024 também disponível
- Funciona em TLS 1.3 e DTLS 1.3

`--enable-mlkem` (híbridos já inclusos)

Bytes trocados no handshake TLS 1.3 (autenticação mútua)



Anti-downgrade: configure `wolfSSL_UseKeyShare()` e `wolfSSL_set_groups()` só com grupos PQC. Anunciar grupos clássicos permite cair para um algoritmo vulnerável.

wolfSSL em microcontroladores

Footprint adequado e assinatura de firmware com estado

~31 KB

TLS 1.3 mínimo (PSK + X25519) no
Cortex-M33

~13 KB

verificação de certificado ML-DSA-65

+1,3 KB

memória estática: operação sem heap

Perfil tiny TLS 1.3

- --enable-tinytls13=cert,mldsa
- ML-DSA só verificação: ideal para o dispositivo
- Grupo híbrido escolhido pela aplicação

LMS: estado sob controle

- Callbacks persistem a chave a cada assinatura
- wc_LmsKey_SigsLeft(): assinaturas restantes
- Winternitz maior: assinatura menor, mais lenta

Comparação de estratégias de implementação de criptografia

Biblioteca de Software x Hardware dedicado

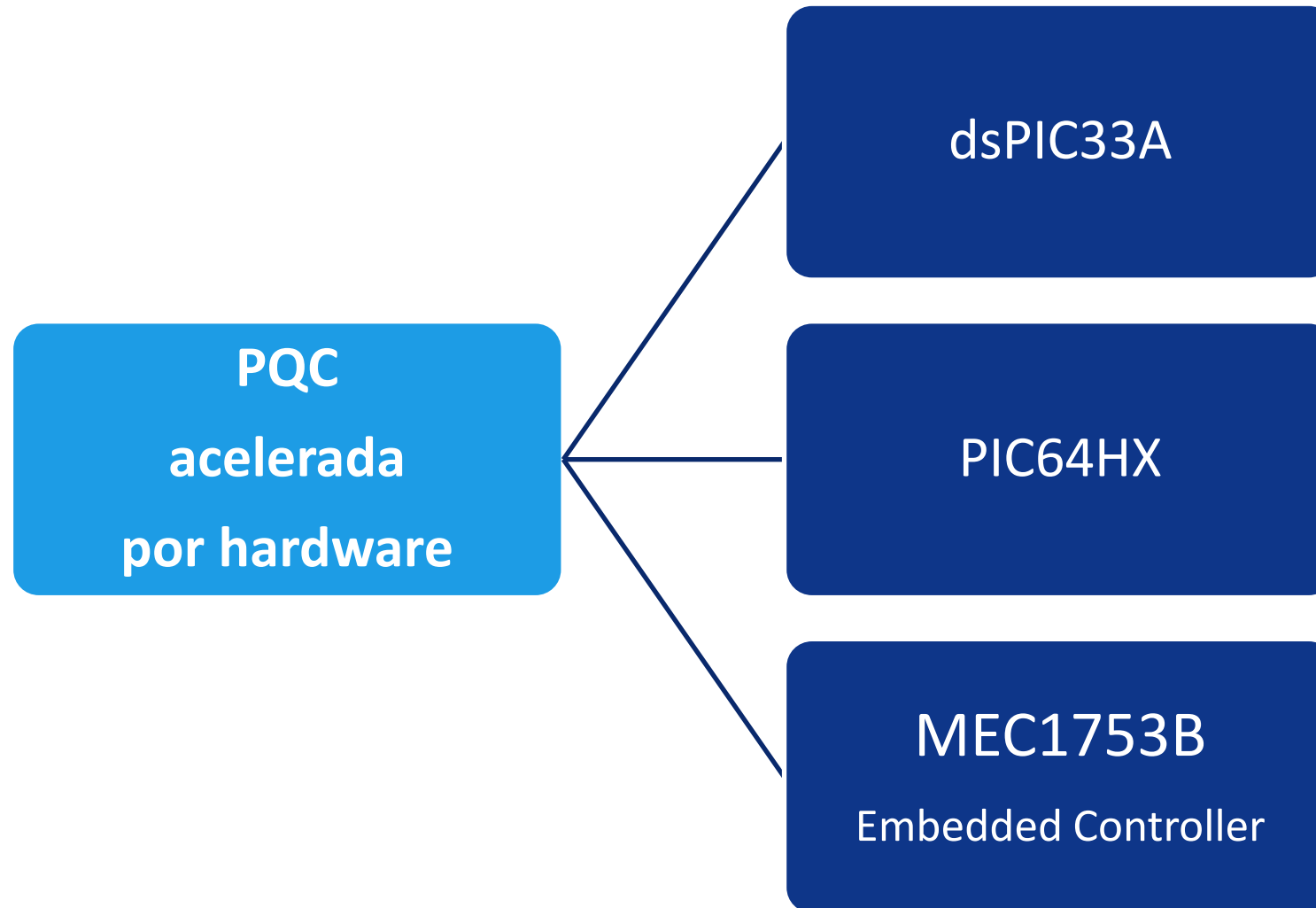
Abordagem	Pontos Fortes (Vantagens)	Pontos Fracos (Desvantagens)
Biblioteca de Software	• Baixo custo de implementação e sem gastos com novos componentes físicos. • Alta flexibilidade para atualizações, correções de bugs e troca de algoritmos. • Fácil escalabilidade e rápida distribuição em múltiplos sistemas.	• Menor desempenho (consome ciclos de processamento da CPU principal). • Maior vulnerabilidade a ataques de malware, vazamento de memória e falhas do sistema operacional.
Hardware Dedicado (ex: HSM, TPM, Smart Cards)	• Desempenho máximo com processamento isolado e aceleradores criptográficos. • Segurança física robusta contra adulteração (tamper-resistant) e extração de chaves. • Isolamento total das chaves privadas em relação ao sistema operacional.	• Alto custo de aquisição, manutenção e substituição dos dispositivos. • Baixa flexibilidade, sendo difícil atualizar o hardware caso surjam novas vulnerabilidades ou padrões. • Complexidade de integração física e lógica.

Comparação wolfSSL com OpenSSL

Característica	<u>wolfSSL</u>	<u>OpenSSL</u>
Foco Principal	Dispositivos embarcados, IoT e sistemas com recursos restritos (RAM/Flash).	Servidores web, desktops e sistemas operacionais de propósito geral (Linux/Windows).
Tamanho do Código	Muito compacto (geralmente entre 20 kB e 100 kB, altamente modular).	Grande (vários megabytes, difícil de enxugar para chips pequenos).
Consumo de Memória	Otimizado para usar o mínimo de RAM possível (usa alocação estática).	Consumo de RAM considerável, baseado em alocação dinâmica intensa.
Licenciamento	Duplo: GPLv2 (código aberto) ou Comercial (paga, para produtos proprietários).	Apache License 2.0 (permissiva, gratuita tanto para código aberto quanto comercial).
Portabilidade	Roda nativamente em "bare-metal" (sem SO) e RTOS (FreeRTOS, Zephyr, ThreadX).	Depende fortemente de uma API de sistema operacional completa (POSIX/Windows).
Suporte a Hardware	Integração nativa com aceleradores criptográficos de MCUs	Suporte focado em instruções de CPUs de grande porte (como Intel AES-NI ou ARMv8 Crypto).

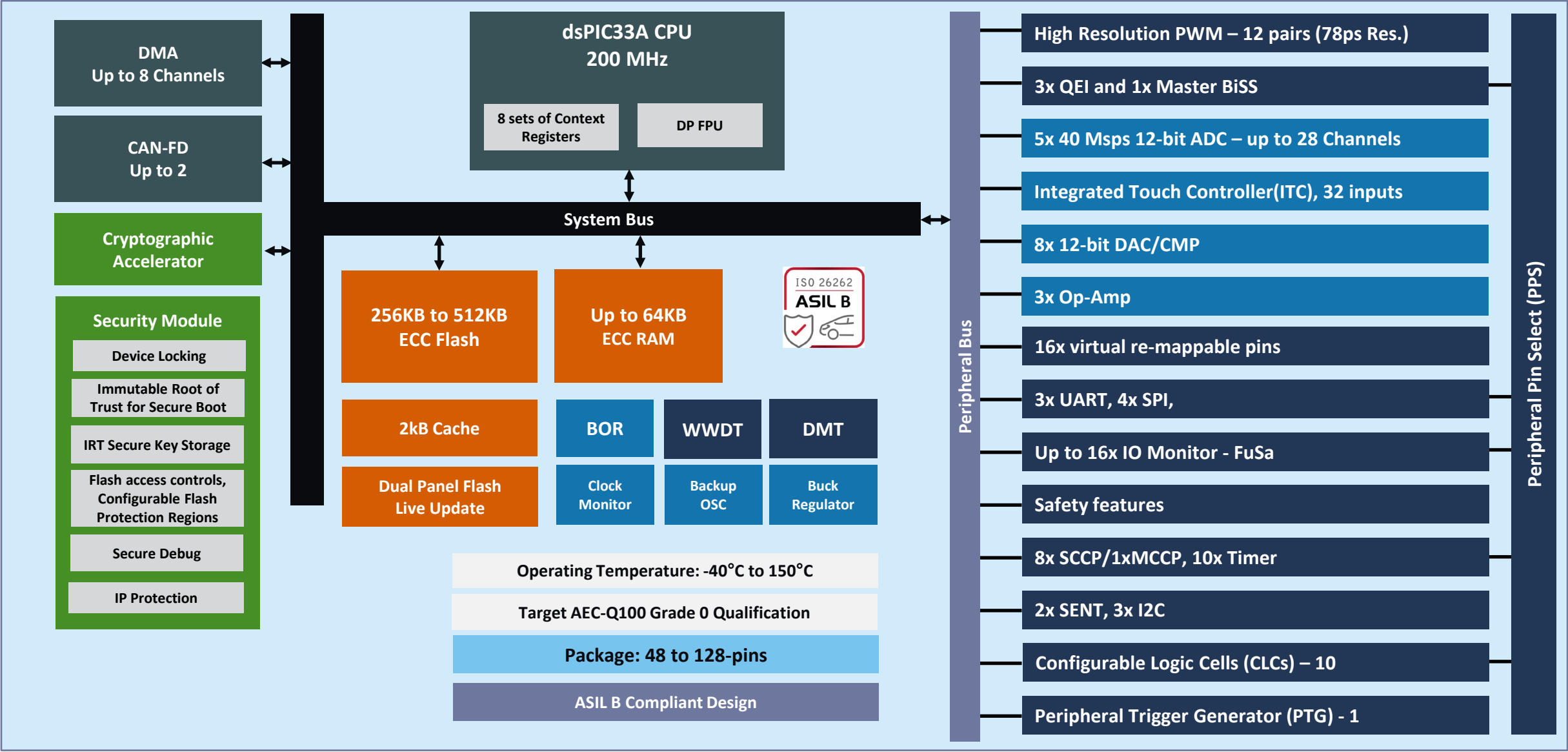
PQC – Estratégias de implementação

PQC acelerada por hardware



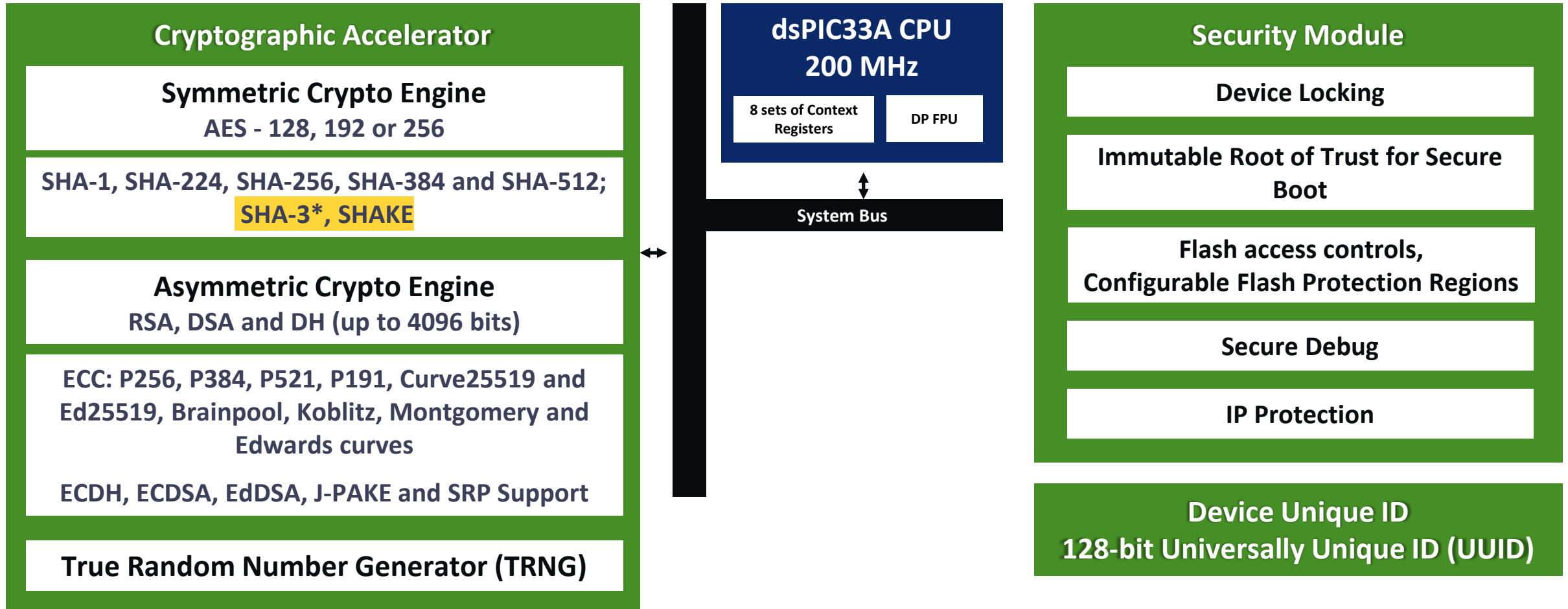
dsPIC33AK512/256MPS Family Block Diagram

Released



Security Features

dsPIC33A Security Features



SHA-256, SHA-3, SHAKE engine speeds up PQC algorithms

* SHA-3 and SHAKE is available on dsPIC33AK256MPS3xx and newer devices

dsPIC33 Post-Quantum Crypto (PQC) Support

Available Now

In Progress

Beta / EA Available

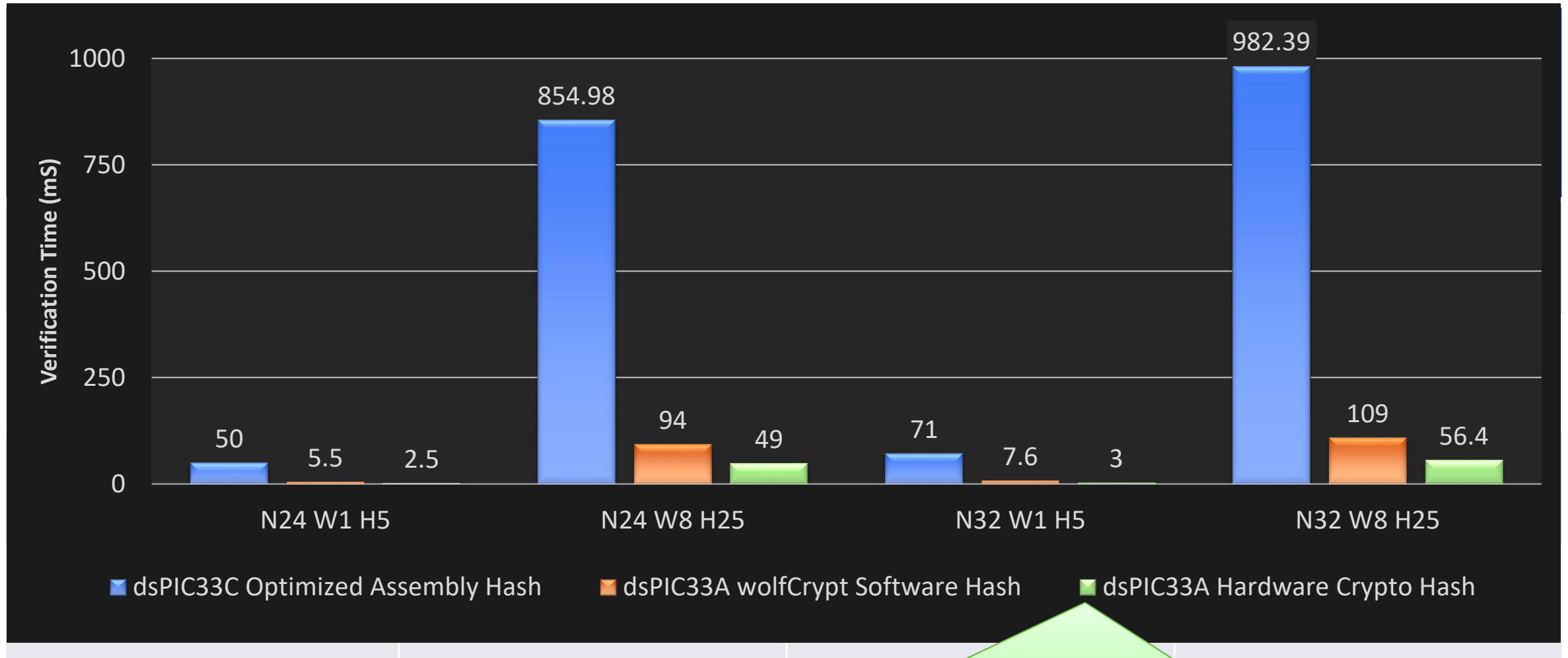
- PQC algorithm support
- Enable secure boot applications

Quantum Algorithms		dsPIC33C - Optimized Assembly Hash	dsPIC33A - wolfCrypt Software Hash	dsPIC33A - Hardware Crypto Accelerator for Hash	Parameters Details
Key Verification	LMS	✓	✓	✓	Hash: SHA256_192 (N24), SHA256 (N32) Width: 1, 2, 4, 8 Height: 5, 10, 15, 20, 25
	ML-DSA	✓	✓	✓	ML-DSA-44 (Category 2) ML-DSA-65 (Category 3) ML-DSA-87 (Category 5)
Key Exchange Decapsulation	ML-KEM		✓	✓	ML-KEM-512 (Category 1) ML-KEM-768 (Category 3) ML-KEM-1024 (Category 5)
Key Generation	ML-DSA				

Post Quantum Cryptography Library and Example Projects: [Link](#)

Benchmark of LMS – Key Verification

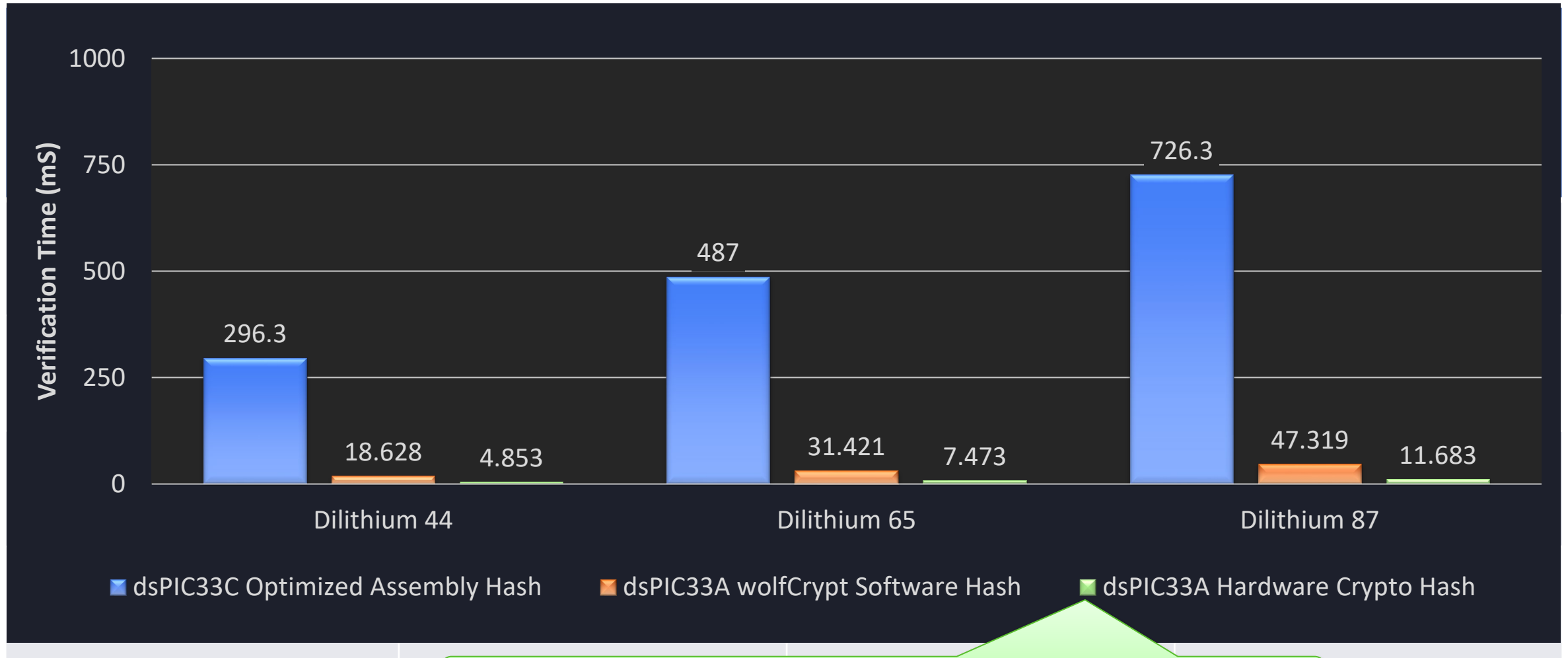
Hardware Crypto Accelerator Speeds up PQC Algorithms



Hardware Crypto Accelerator Speeds up PQC Algorithms

Benchmark of ML-DSA - Key Verification

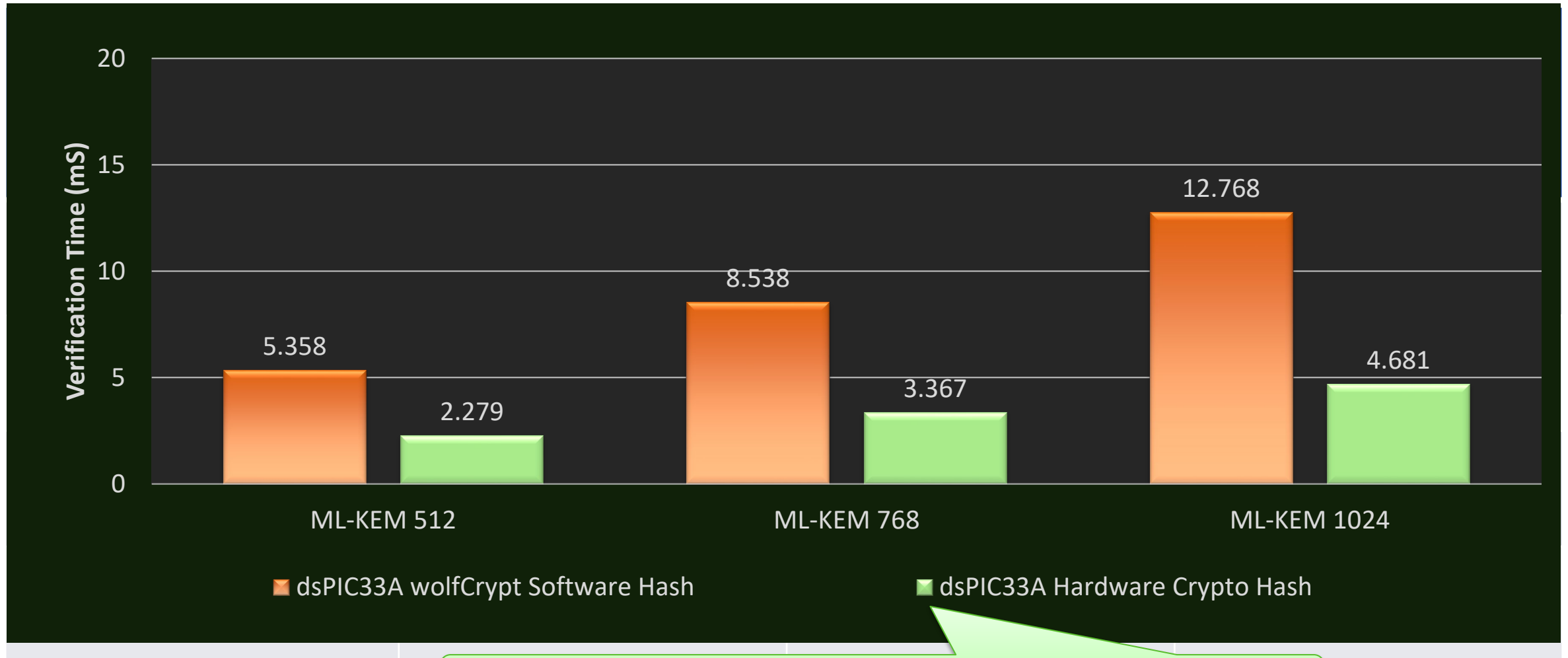
Hardware Crypto Accelerator Speeds up PQC Algorithms



Hardware Crypto Accelerator Speeds up PQC Algorithms

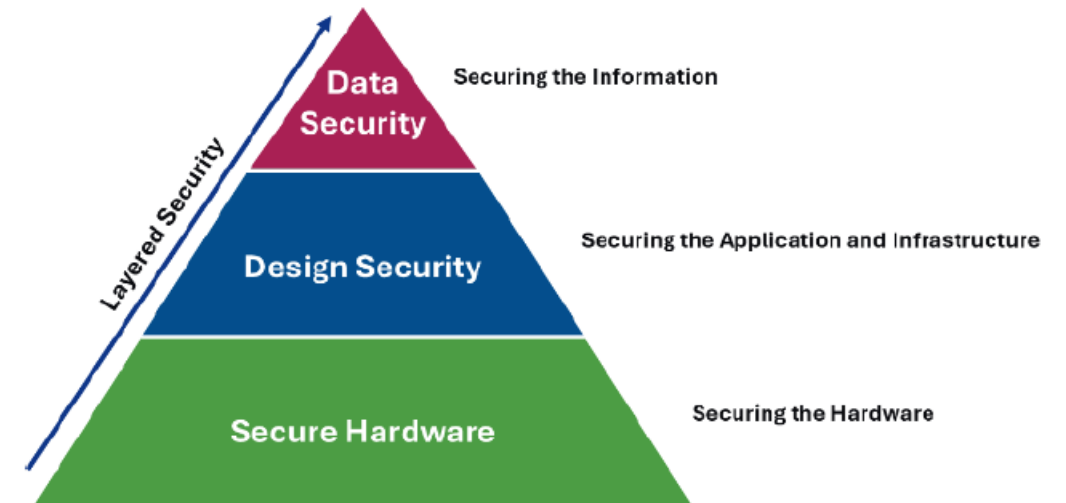
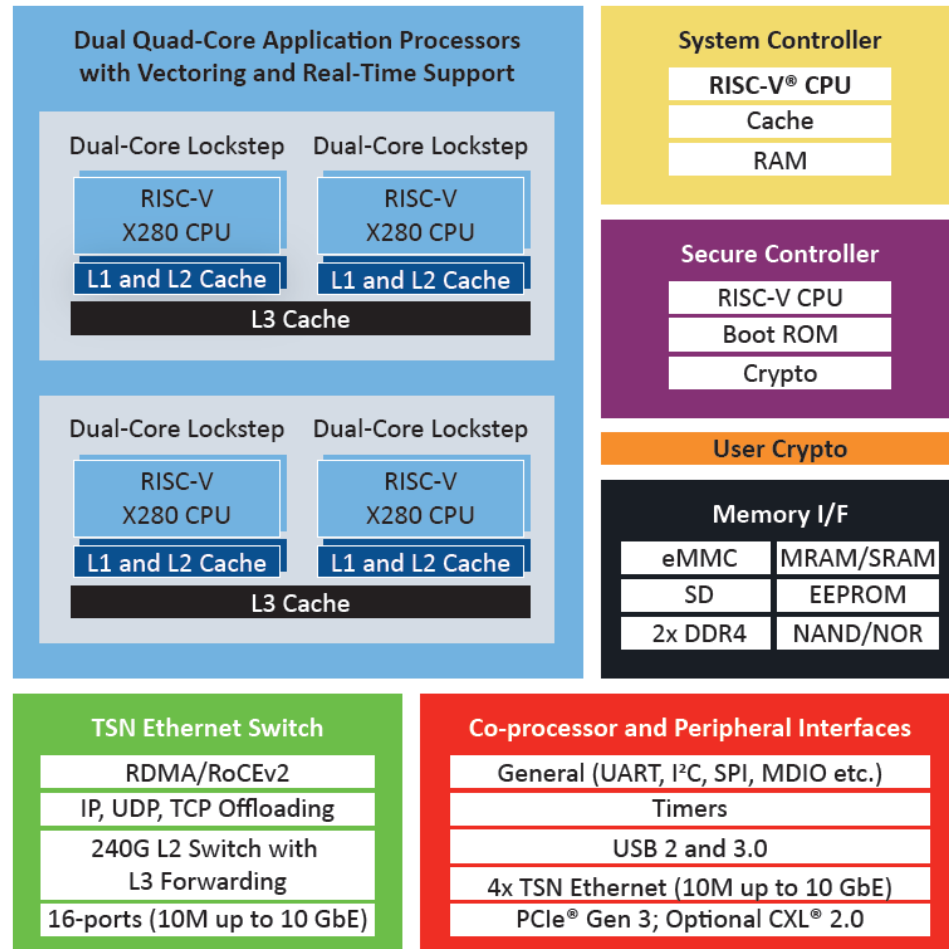
Benchmark of ML-KEM - Decapsulation

Hardware Crypto Accelerator Speeds up PQC Algorithms



PIC64HX

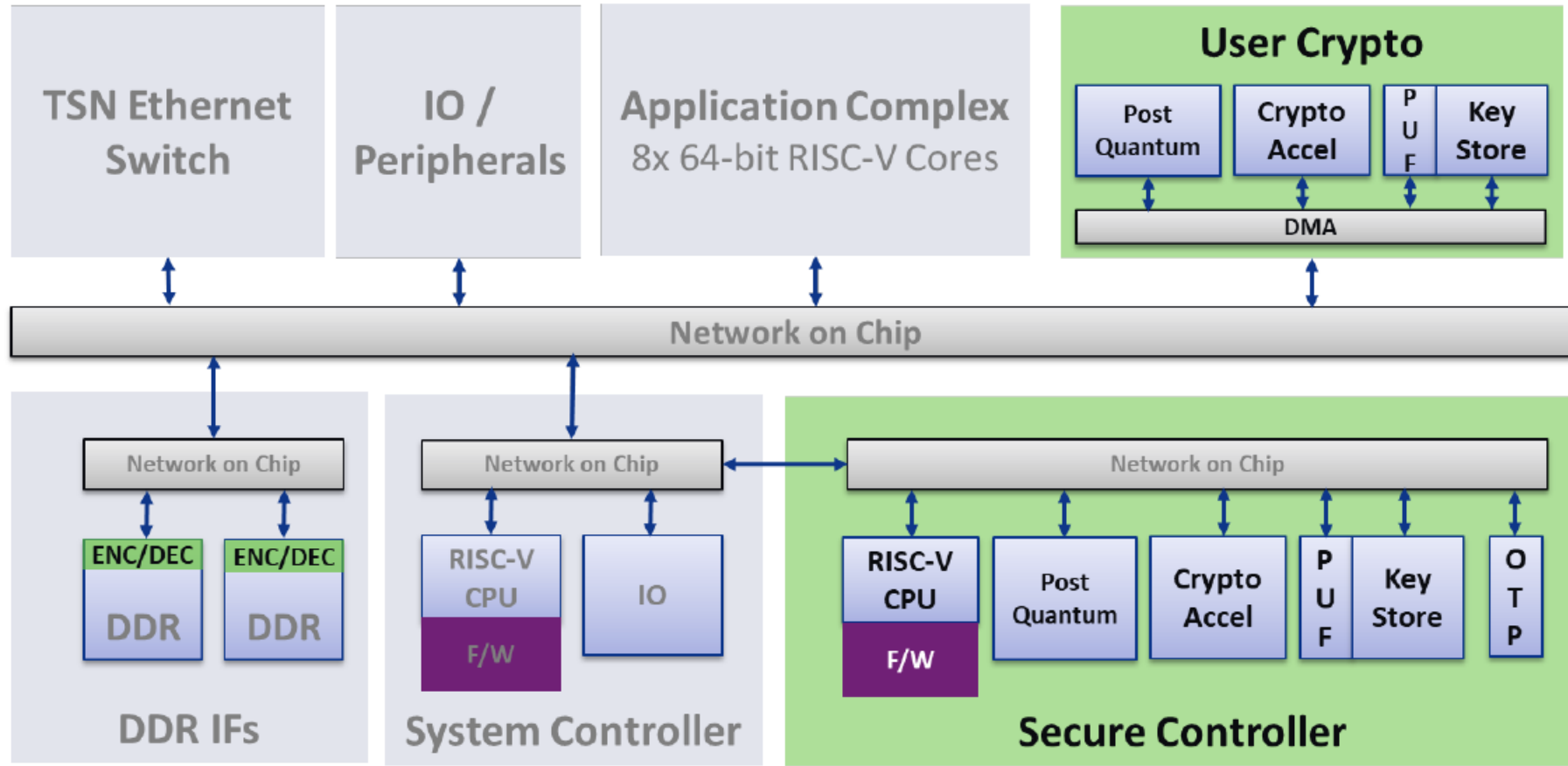
Diagrama de blocos



Abordagem de segurança em camadas

PIC64HX

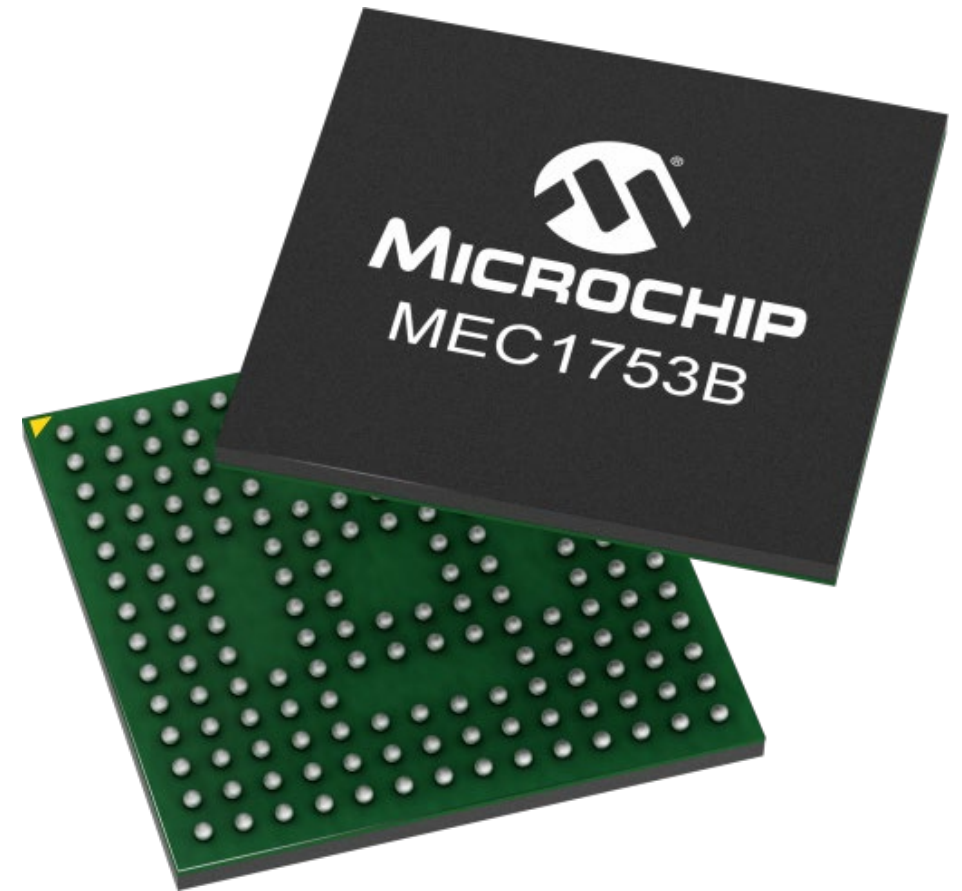
Diagrama de blocos com destaque às características de segurança



MEC1753B – Embedded Controller

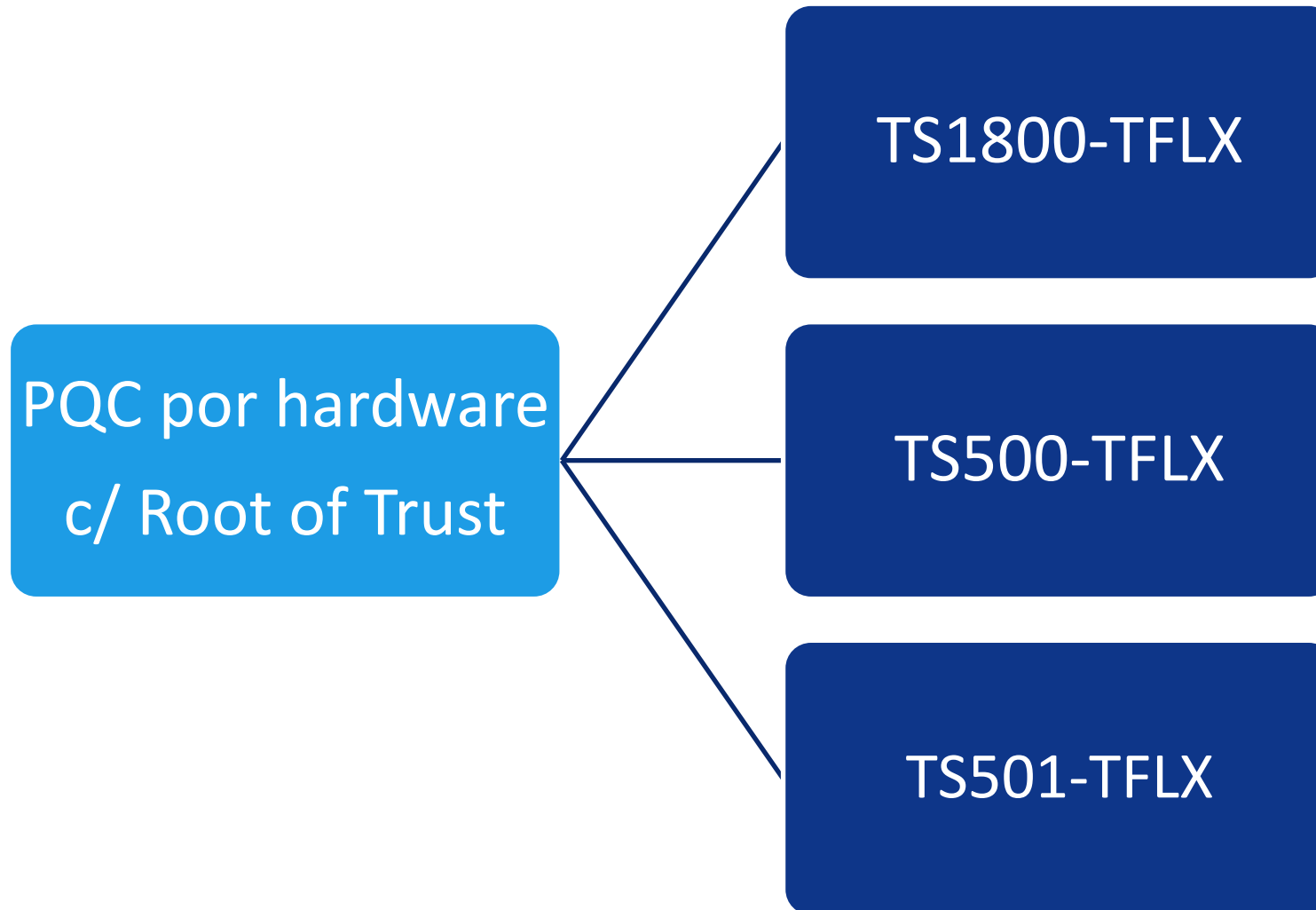
PQC acelerada por hardware

- Boot ROM Secure Boot Loader
- ❖ **Module-Lattice-Based Digital Signature Algorithms (ML-DSA)**
- ❖ **Merkle stateful hash-based Leighton-Micali Signature (LMS)**
- ❖ **Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) standardized by NIST**
- Hardware Root of Trust (RoT) using Secure Boot and Immutable code
- Supports 2 Code Images in external SPI Flash (Primary and Fall back image)
- Authenticates SPI Flash image before loading
- Support AES-256 Encrypted SPI Flash images
- Multi purpose AES Crypto Engine 128 bits and 256 bits
- ECDSA and **EC_KCDSA**
- SHA-1, SHA-256 to SHA-512
- RSA keys length of 1024 to 4096 bits
- ECC Prime Field keys up to 571 bits
- ECC Binary Field keys up to 571 bits
- Microcoded support for standard public key algorithms
- True Random Number Generator
- **ARM® Cortex-M4F Embedded Processor**



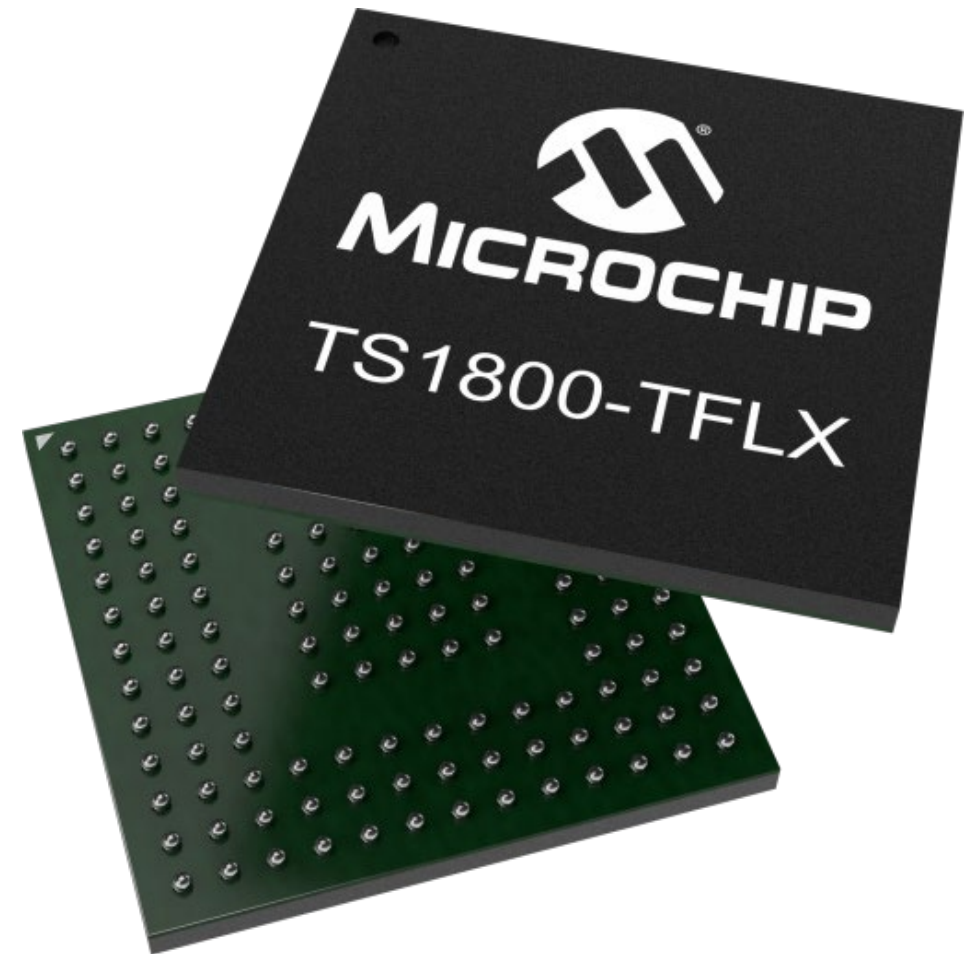
PQC – Estratégias de implementação

PQC por hardware dedicado c/ Root-of-Trust



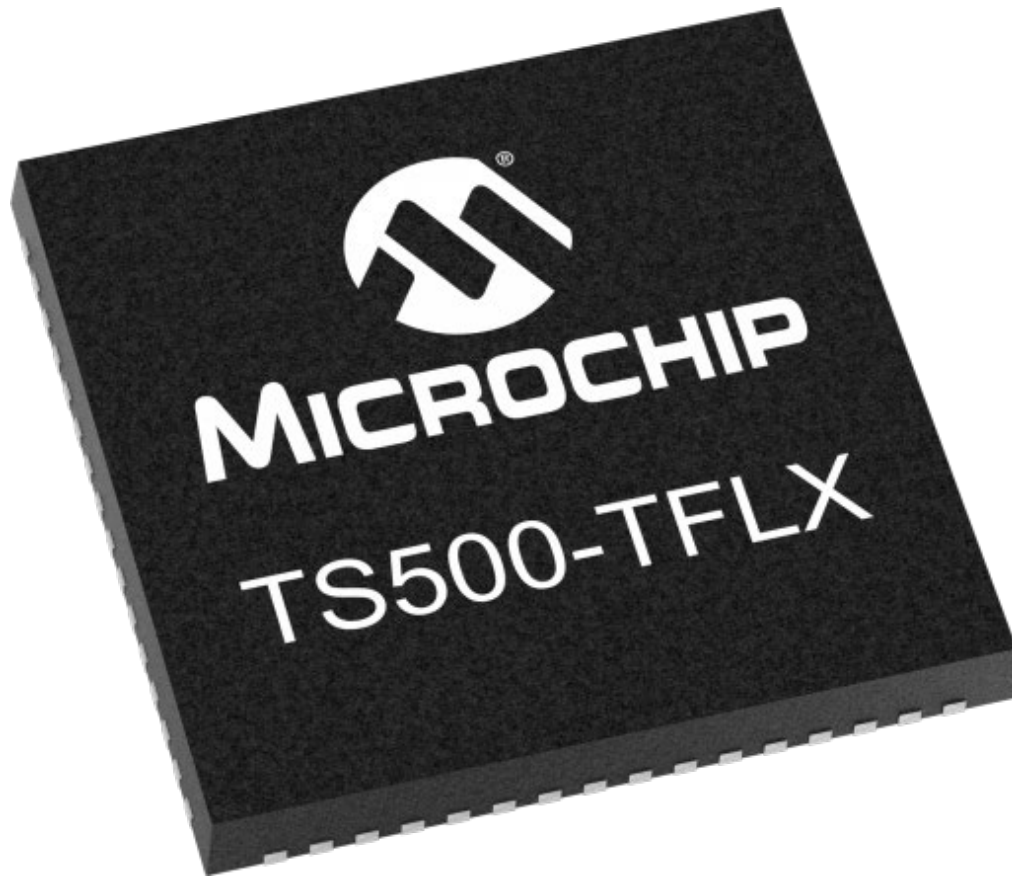
PQC por hardware dedicado c/ Root-of-Trust

- ❑ Raiz de confiança de plataforma externa , de alto desempenho para sistemas complexos de múltiplos componentes
- ❑ **Criptografia híbrida (pós-quântica e clássica).**
- ❑ Projetado para atender aos requisitos do **NIST SP 800-193** (Platform Firmware Resiliency Guidelines) e do **Open Compute Project (OCP).**
- ❑ Processador Arm® Cortex® M4F de alto desempenho com clock de até 192 MHz.
- ❑ USB 2.0 para atualizações rápidas de firmware.
- ❑ Suporte a QSPI/SPI multicanal.
- ❑ Recursos integrados de inicialização segura (secure boot), atualizações seguras, proteção contra reversão (rollback), recuperação de emergência e gerenciamento de ciclo de vida.



ICs TrustFLEX TS500 e TS501 — Raiz de Confiança (Root of Trust)

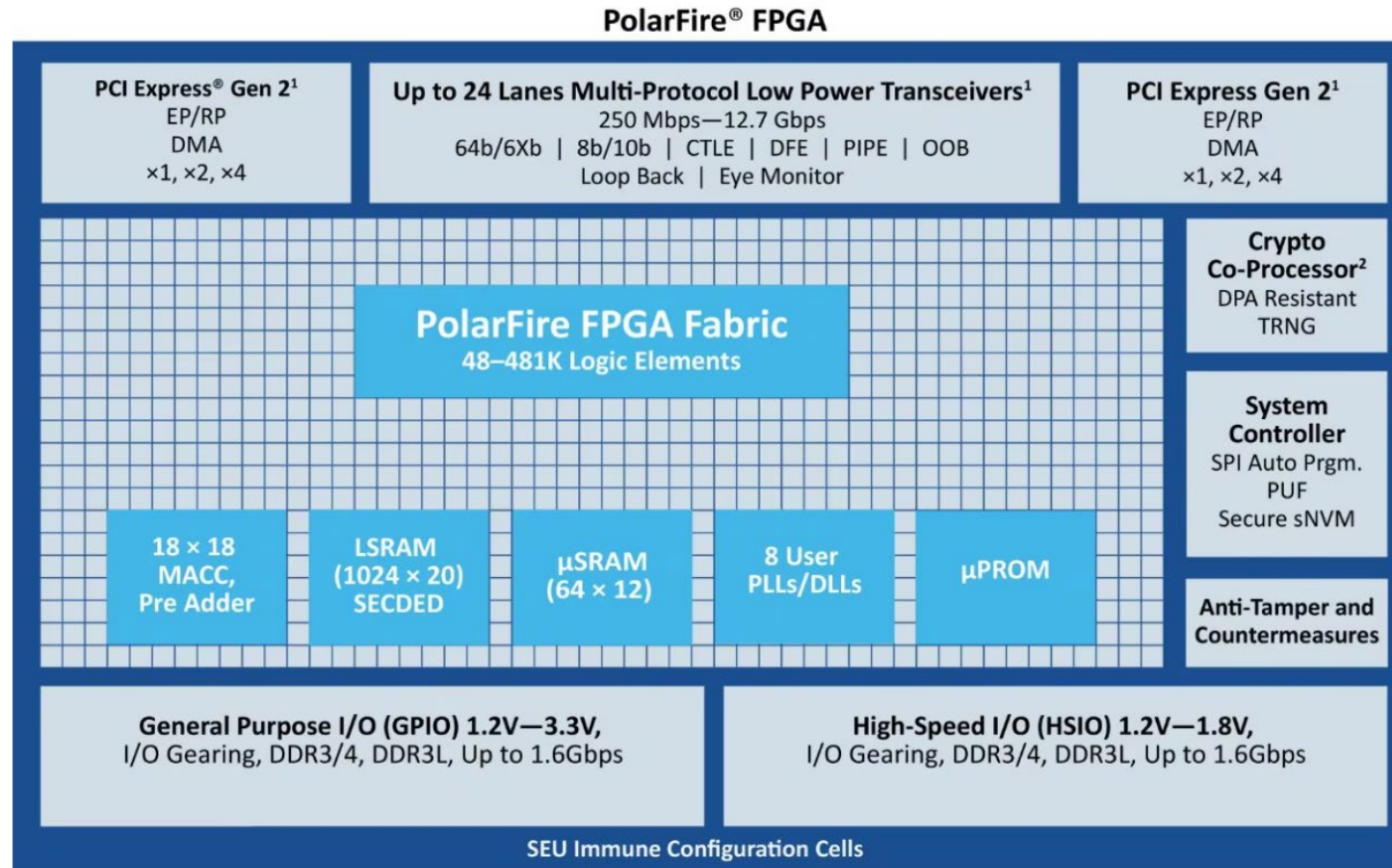
PQC por hardware dedicado c/ Root-of-Trust



- ❑ Inicialização segura (secure boot) baseada em hardware com autenticação pronta em PQC.
- ❑ Conexão em linha (inline) entre o System on Chip (SoC) e a memória Flash SPI, mantendo o sistema em estado de reset até que a verificação seja bem-sucedida.
- ❑ Opções de criptografia híbrida (PQC e clássica) para migração da inicialização segura.
- ❑ Projetados para suportar a norma NIST SP 800-193 de Resiliência de Firmware de Plataforma.
- ❑ TS500: Firmware armazenado em memória Flash SPI externa.
- ❑ TS501: Memória Flash SPI interna integrada para projetos simplificados.
- ❑ Compatíveis com sistemas baseados em x86 e Arm®.

PQC – Estratégias de implementação

PQC acelerada por FPGA



Notes:

1. PCIe® and Transceivers **not available** in PolarFire Core devices
2. DPA-Safe Crypto Co-Processor supported in S devices
3. PolarFire Core devices are available in STD speed only. Refer to STD speed I/O specs for core devices.

PQC – Estratégias de implementação

PQC acelerada por FPGA

Parceiro	Foco principal	Suporte ao algoritmo PQC	Valor único de hardware/segurança	Principais requisitos de conformidade/certificações	Otimização/Footprint	Plataforma FPGA da Microchip
PQSecure	Codesign HW/SW	ML-KEM/DSA (Rede); Hash	Desempenho de hardware de 90 a 99,99%; Proteção DPA de primeira ordem	Validação do NIST CAVP ; Contramedidas opcionais da DPA	Versões de ponta vs. versões básicas; Descarregamento da CPU	FPGAs PolarFire e FPGAs SoC
PQShield	Bibliotecas SW certificáveis	ML-KEM/DSA, SLH-DSA (Finalistas do NIST)	Otimizado para IoT (RAM 6 a 11 vezes menor); Execução em tempo constante	Certificado FIPS 140-3 CMVP ; Certificado CAVP	Ocupa pouco espaço de memória (<16 KB)	FPGAs PolarFire e FPGAs SoC
Xipherra	Lógica RTL pura	ML-KEM/DSA (em conformidade com FIPS 203/204)	Sem componentes de CPU/software; Proteção contra SCA baseado em temporização	Algoritmos PQC padronizados pelo NIST	Otimizado para configurações compactas, equilibradas ou de alta velocidade; uso mínimo de recursos.	FPGAs PolarFire e FPGA SoC
CAST	Acelerador de hardware	KiviPQC-Box (ML-KEM e ML-DSA, FIPS 203/204)	Descarregamento de hardware para cálculos de PQC; Reforçado contra SCA baseado em temporização	Em conformidade com as normas NIST FIPS 203 e FIPS 204.	Disponível nas versões Tiny (ex.: 6.143 LUTs) e Fast.	FPGAs PolarFire
Rambus	Propriedade intelectual de silício	ML-KEM, ML-DSA (NIST); XMSS/LMS (Stateful Hash)	Contramedidas DPA/SCA (Reforçadas); Motor Programável à Prova de Ataques Quânticos	Projetos em conformidade com FIPS 140-3 ; prontos para CNSA 2.0 e ISO 26262.	Núcleos IP configuráveis (IoT para Data Center); Criptografia de memória embutida	FPGAs PolarFire (com licença DPA)

Migração híbrida (Criptografia clássica+PQC)

A chave de sessão depende dos dois segredos



Cenário	Clássico	PQC	Chave
Hoje	seguro	seguro	Segura
Computador quântico	quebrado	seguro	Segura
Falha no ML-KEM	seguro	quebrado	Segura
Os dois quebrados	quebrado	quebrado	Exposta

O atacante precisa quebrar os DOIS: a segurança é a do algoritmo mais forte.



MICROCHIP



SMART | CONNECTED | SECURE

APÊNDICE

Segurança da Informação



NIST standard FIPS 199 apud Stallings (2020)

Segurança da Informação

```
graph LR; A((Segurança da Informação)) --> B(Confidencialidade); A --> C(Integridade); A --> D(Disponibilidade); B --> E[Garantia que a informação seja acessada apenas por quem tem autorização.]; C --> F[Garantia que a informação não seja alterada ou destruída indevidamente, mantendo-a autêntica e confiável.]; D --> G[Garantia do acesso oportuno e confiável para uso da informação.];
```

Confidencialidade

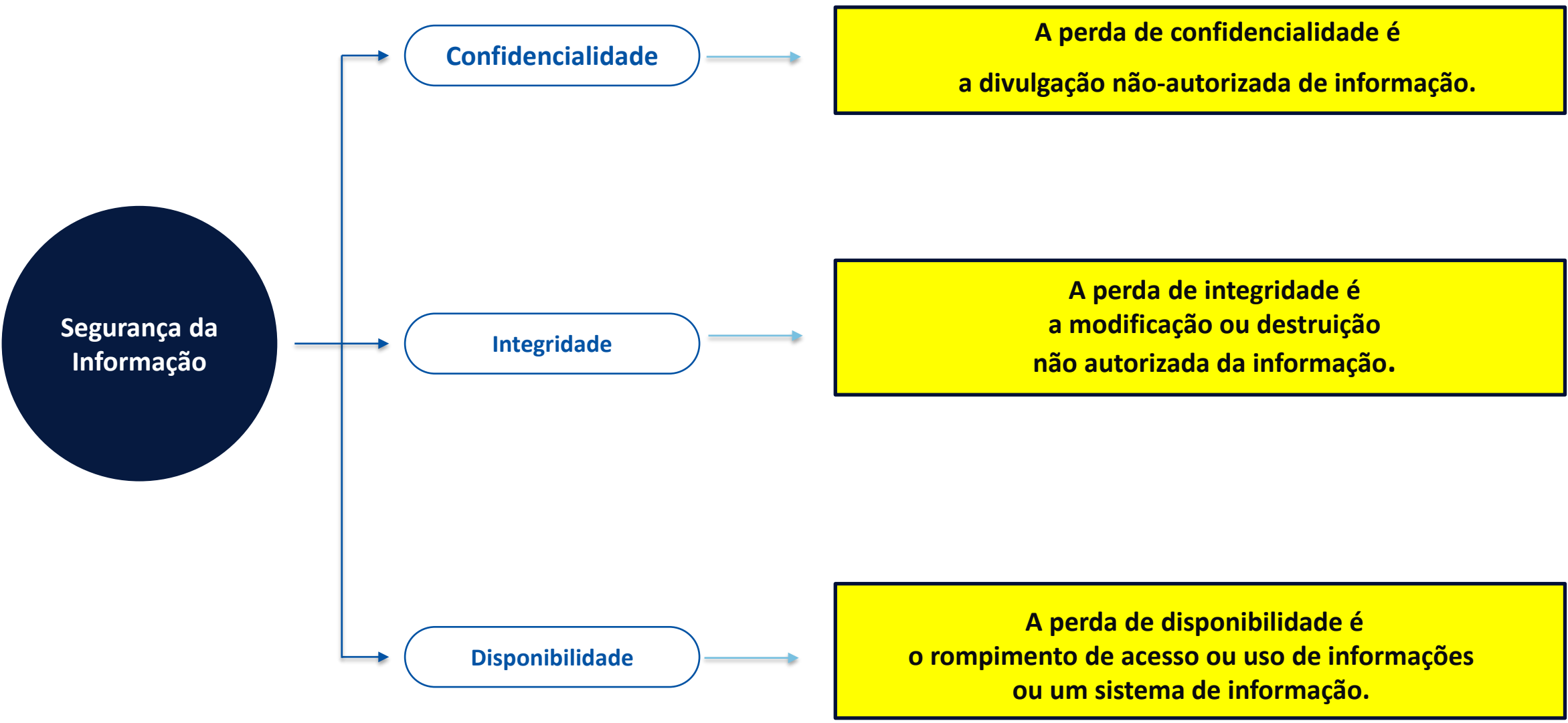
Garantia que a informação seja acessada apenas por quem tem autorização.

Integridade

Garantia que a informação não seja alterada ou destruída indevidamente, mantendo-a autêntica e confiável."

Disponibilidade

Garantia do acesso oportuno e confiável para uso da informação.



Ataques

Ataques Passivos

Liberação de
conteúdo de
mensagens

Análise de tráfego

Ataques Ativos

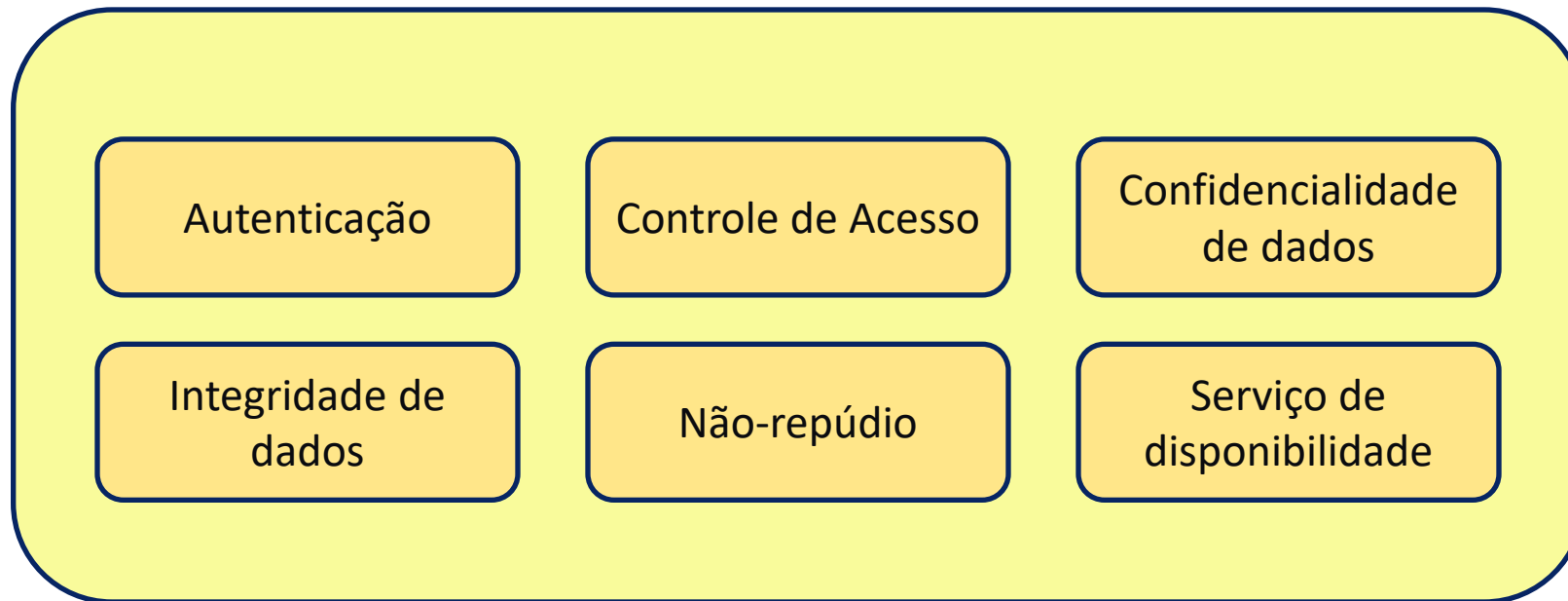
Repetição

Modificação de
dados

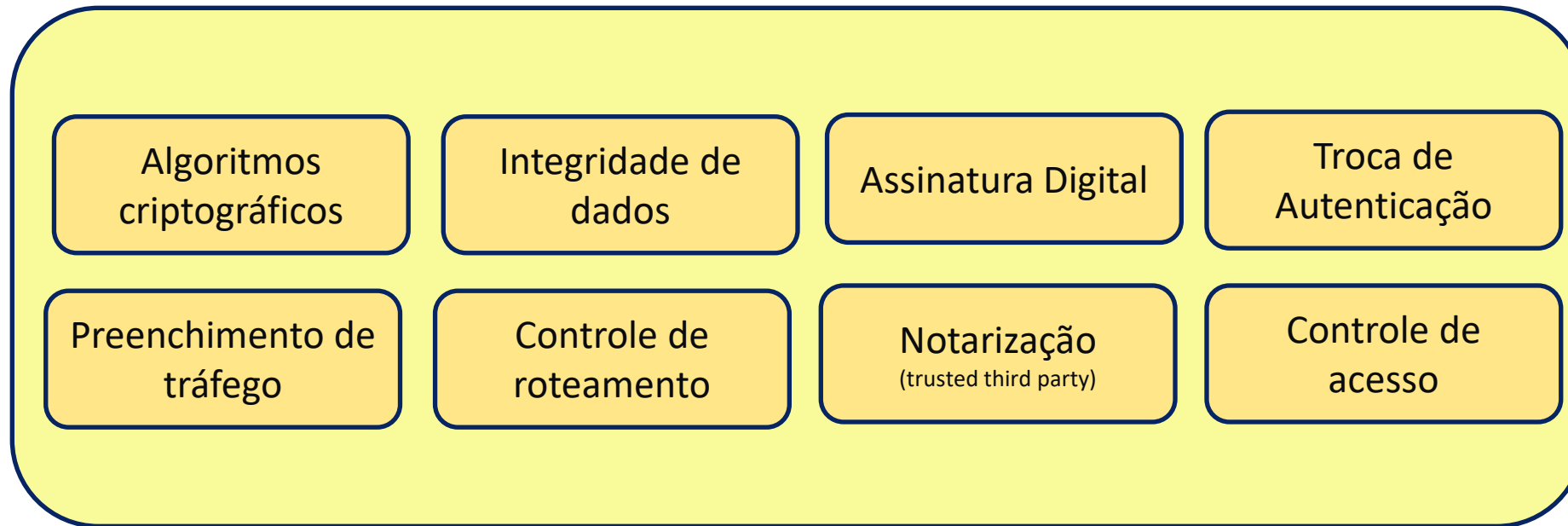
Disfarce

Negação de serviço

Serviços de Segurança



Mecanismos de Segurança



Criptografia

