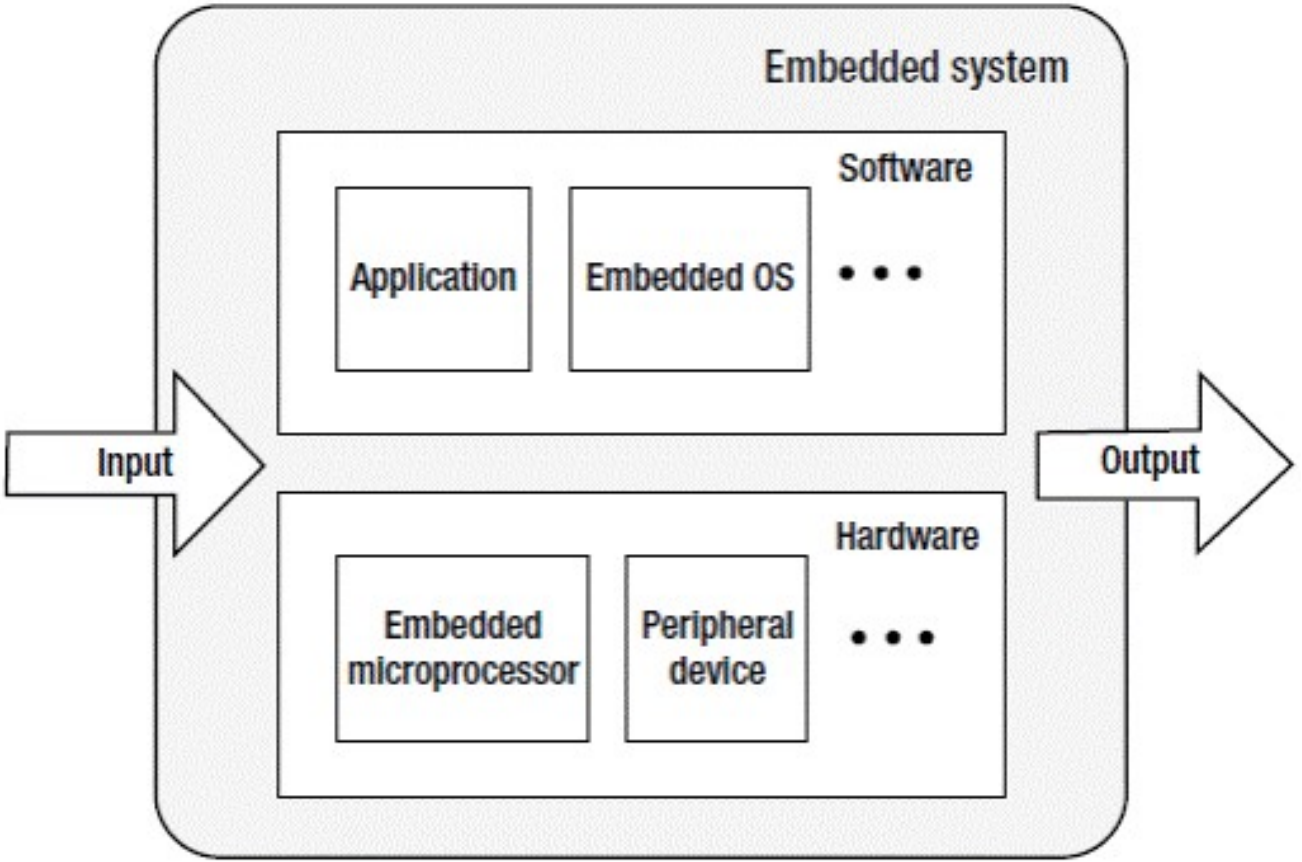
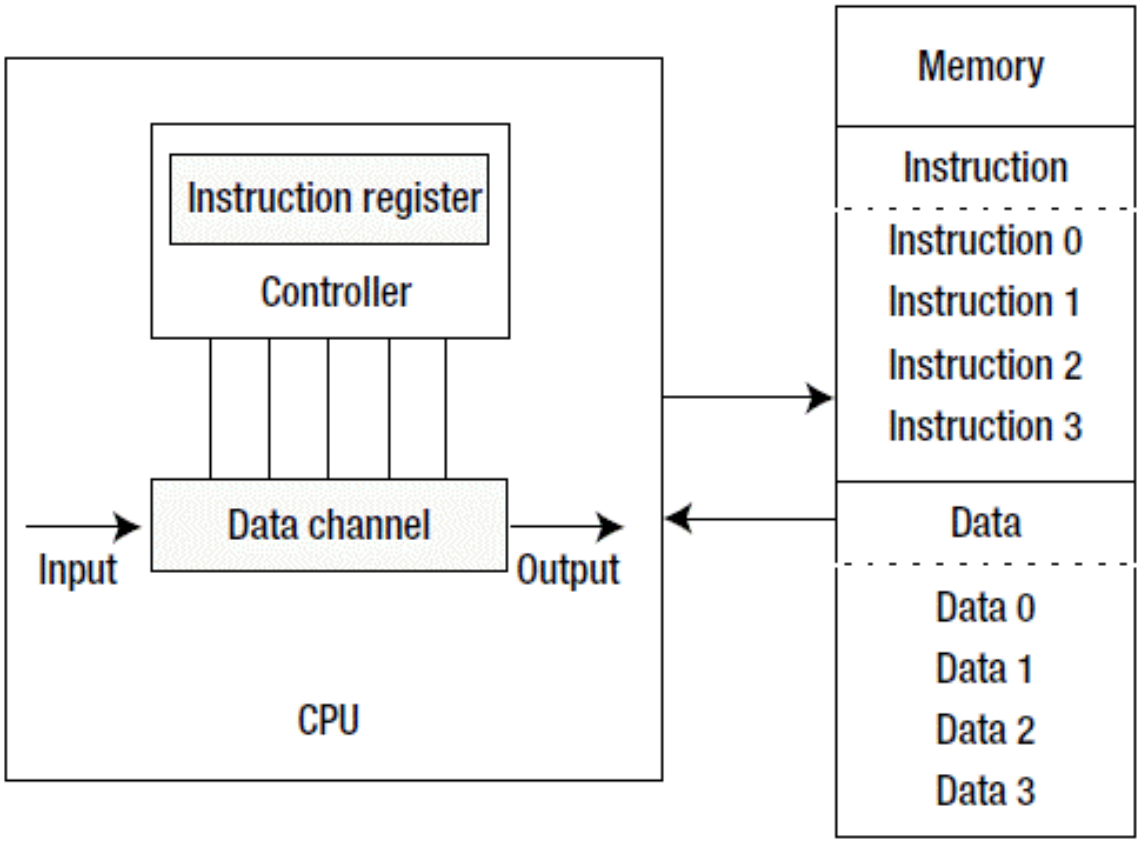
Architektura systemów wbudowanych

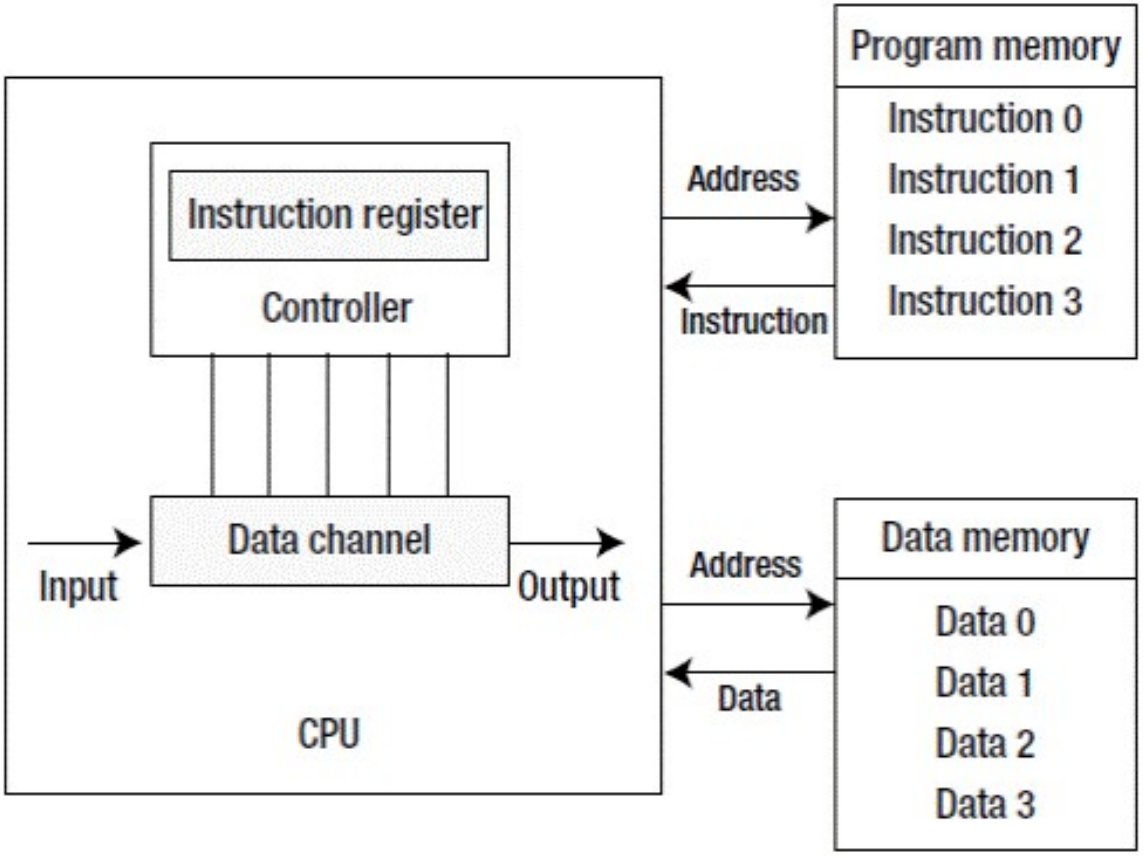
Architektura systemu wbudowanego – ogólnie



Architektura Von Neumann’a



Architektura Harvardzka



Różnice pomiędzy architekturami Von Neumann’a a Harvardzką

Von Neumann	Harvard
Pamięć współdzielona jest pomiędzy program i dane	Dedykowane rodzaje pamięci dla programu i danych
Procesor wczytuje dane w jednym cyklu i program w następnym cyklu zegara. Potrzebuje więc 2 cyklów do wykonania większości operacji.	Procesor wczytuje dane i program w jednym cyklu zegara bo operacje przebiegają na oddzielnych szynach.
Rozwiązania systemowe o większej prędkości	Wolniejsze rozwiązania systemowe.
Prostszy projekt systemu	Bardziej skomplikowany projekt systemu.

Systemy CISC i RISC

- CISC – Complex Instruction Set Computer – instrukcje są skomplikowane i o różnej długości instrukcji i danych
- RISC – Reduced Instruction Set Computer – instrukcje są proste o standardowej długości rozkazów i danych

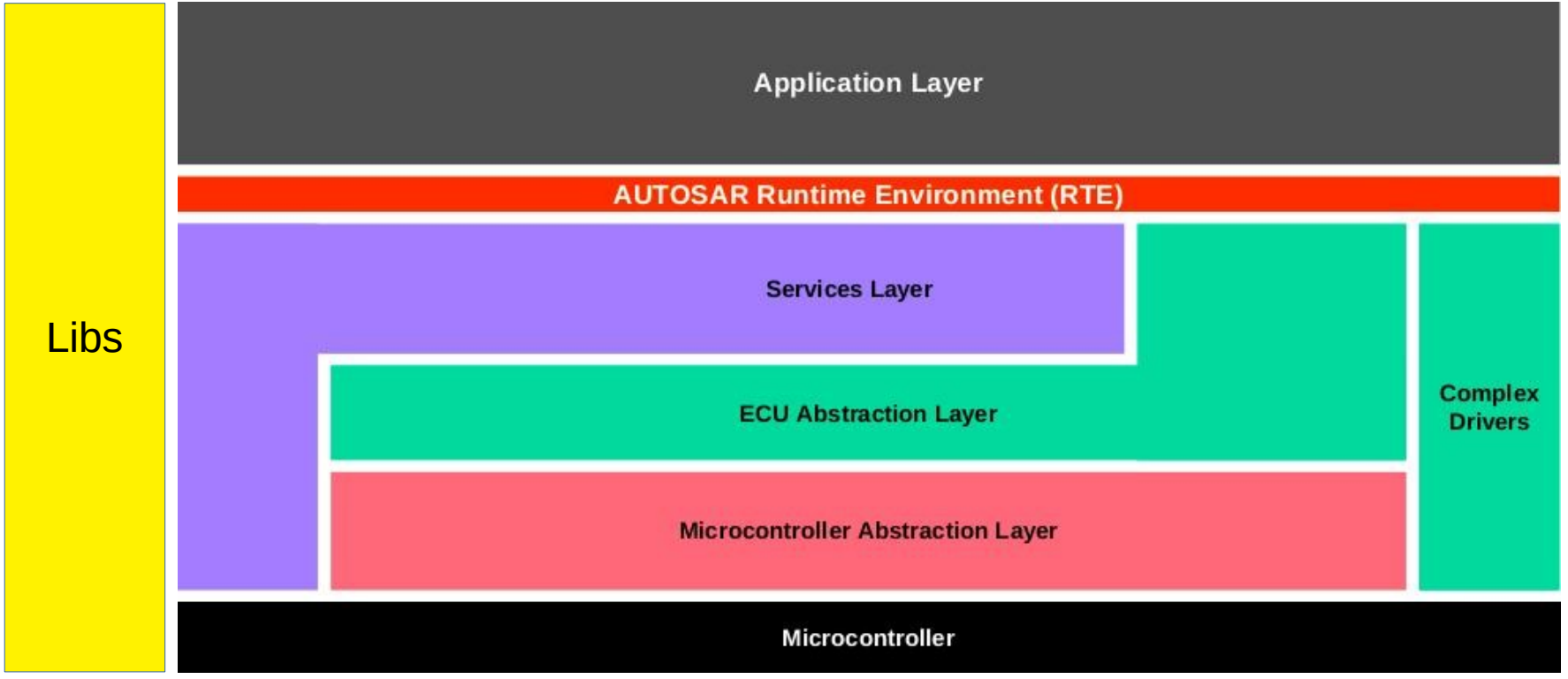
CISC vs RISC

CISC	RISC
Duży zbiór instrukcji, łatwiejsze programowanie niskopoziomowe	Mały zbiór instrukcji, kompilator potrzebuje wielu do wykonania operacji
Prostsza architektura kompilatora	Złożona architektura kompilatora
Dużo trybów adresowania, złożone instrukcje, (z reguły) brak ortogonalności	Mała ilość trybów adresowania, prosty format instrukcji, częściej występuje ortogonalność
Instrukcje zmiennej długości	Instrukcje stałej długości
Wysoka częstotliwość taktowania systemu	Niska częstotliwość taktowania systemu
Skupienie na własnościach sprzętowych	Skupienie na warstwie oprogramowania
Ogromny podsystem kontroli pracy procesora, wymagany mikroporogram	Prosty blok kontroli, wszystkie instrukcje wykonuje bezpośrednio sprzęt
Powolne wykonanie, wymagane pobranie, dekodowanie i dalsze etapy..	Szybkie wykonanie, wszystkie instrukcje bezpośrednio wykonane w warstwie

Konsekwencje dla bezpieczeństwa

- Architektura Von Neumann umożliwia łatwiejszą zmianę zawartości programu (dane i program w jednej przestrzeni)
- Architektura Harwardzka może uniemożliwiać dostanie się do przestrzeni adresowej programu poprzez konsekwentne wydzielenie przestrzeni adresowych
- Oprogramowanie projektowane z uwzględnieniem aspektów bezpieczeństwa, nie powinno używać dynamicznego gospodarowania wektorami przerwań czy auto-modyfikacji programu
- …

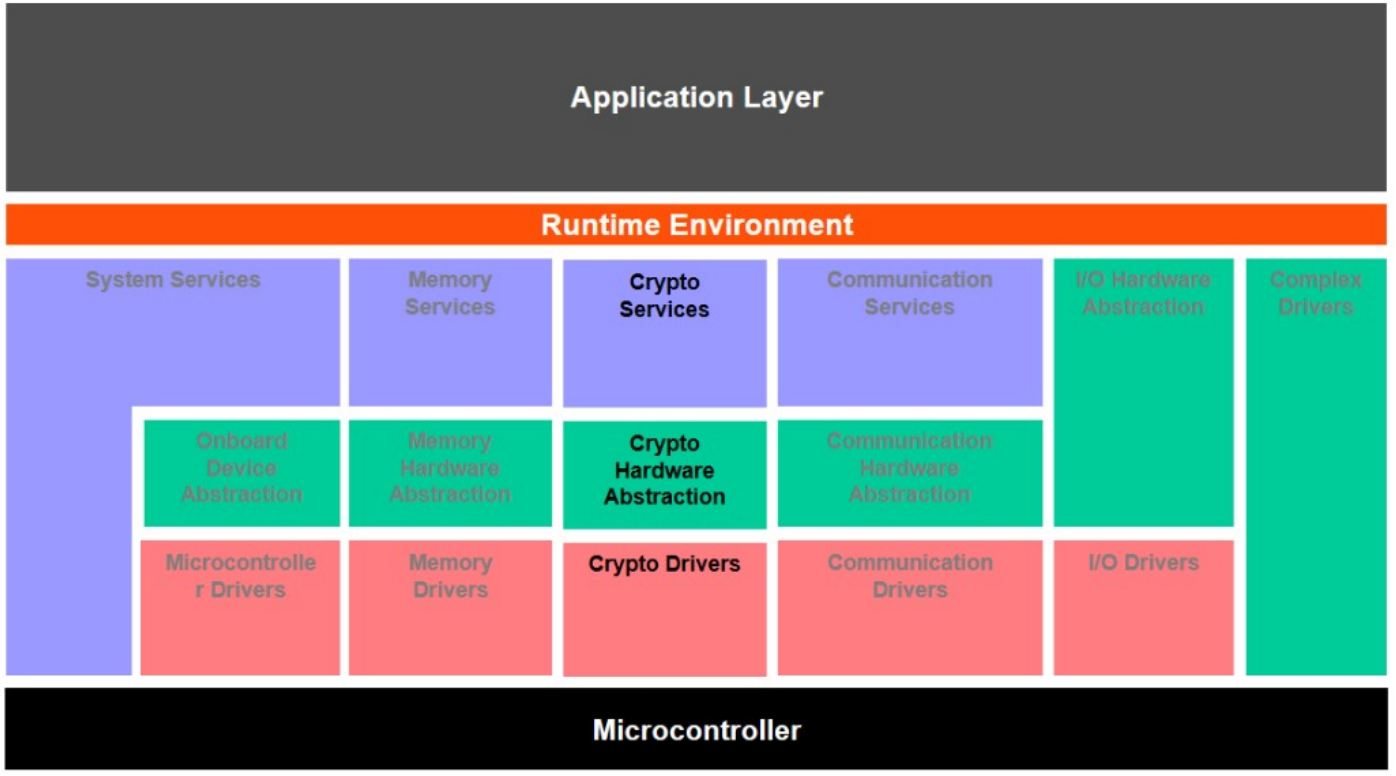
Architektura Classic ECU w AUTOSAR

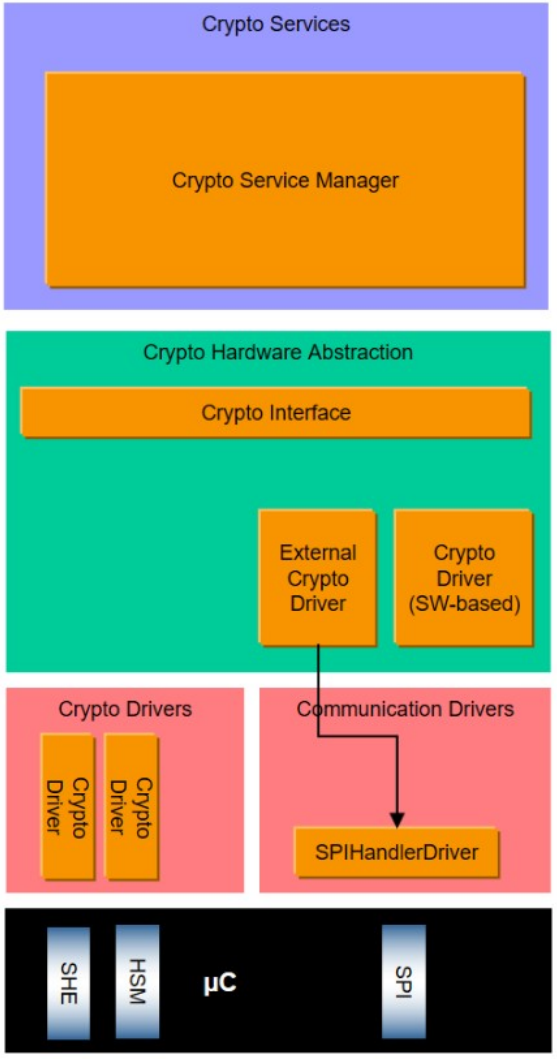


AUTOSAR - warstwy

- Micro-controller Abstraction Layer (MCAL) – sterowniki niskiego poziomu, agregujące elementy mikrokontrolera i zapewniające separację od sprzętu
- ECU Abstracion Layer (ang. ECU – Electronic Control Unit) – warstwa abstrakcji sprzętu poza samym MCU ale występującego w ramach ECU
- Services Layer – warstwa zapewnienia poprawnej pracy dla BSW (ang. Basic SoftWare). Serwisy udostępniające w standaryzowany sposób właściwości platformy sprzętowej
- RTE – (ang. RunTime Environment) – warstwa pozwalająca na osadzenie re-używalnych komponentów AUTOSAR. Zapewnia obsługę Virtual Function Bus w całości architektury
- CCD (ang. Component Device Driver) – zapewnia szybszą obsługę specyficznych właściwości platformy, bez pośrednictwa warstw serwisowych
- Libraries – warstwa bibliotek

AUTOSAR – Crypto Service Manager

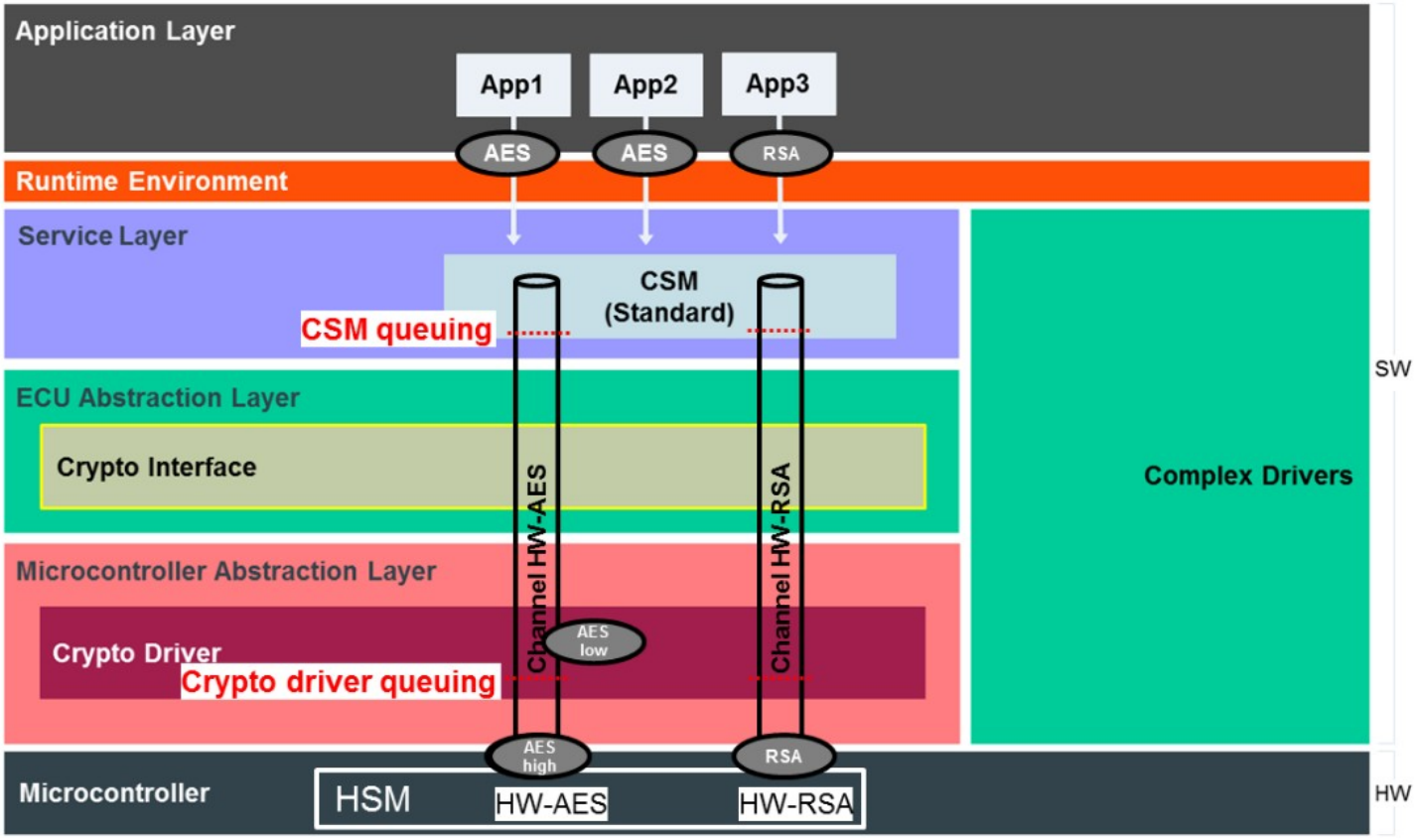




Serwisy modułu Crypto Service Manager

- Moduł Crypto Service Manager zadania:
  - Szyfrowanie – blokowe i wspierane przez sprzęt
  - Zarządzanie kluczem – identyfikacja i szyfrowanie
- Serwis wspiera operacje synchroniczne i asynchroniczne
- Zlecenia gromadzone są w kolejkach priorytetowych
- Zlecenia posiadają status (START, UPDATE, FINISH)

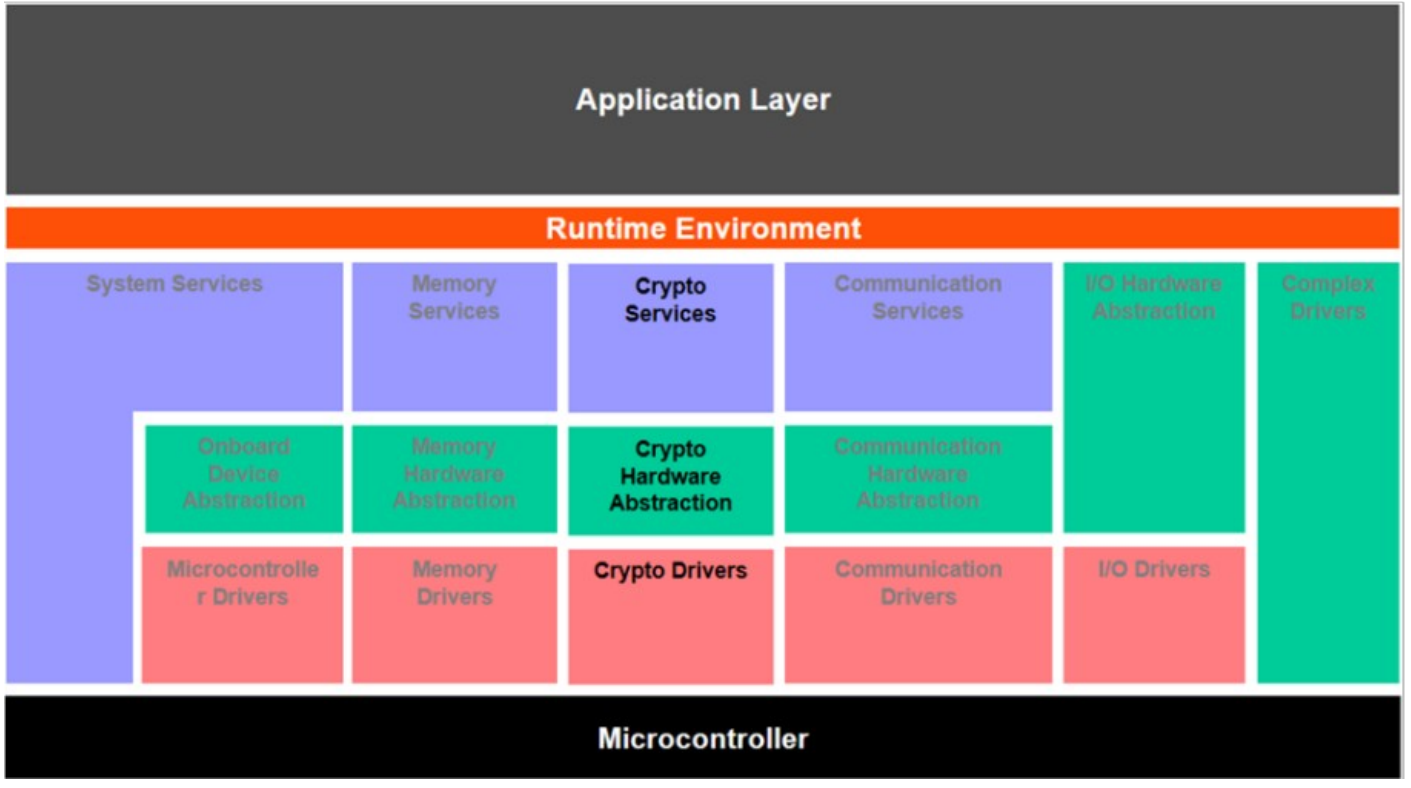
Kolejka Crypto Service

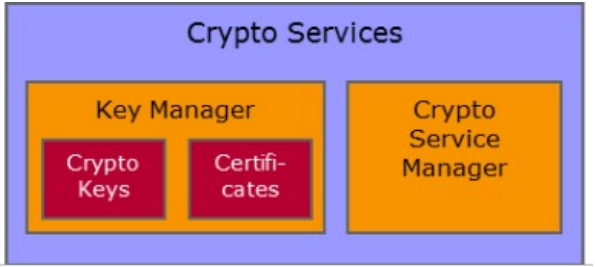


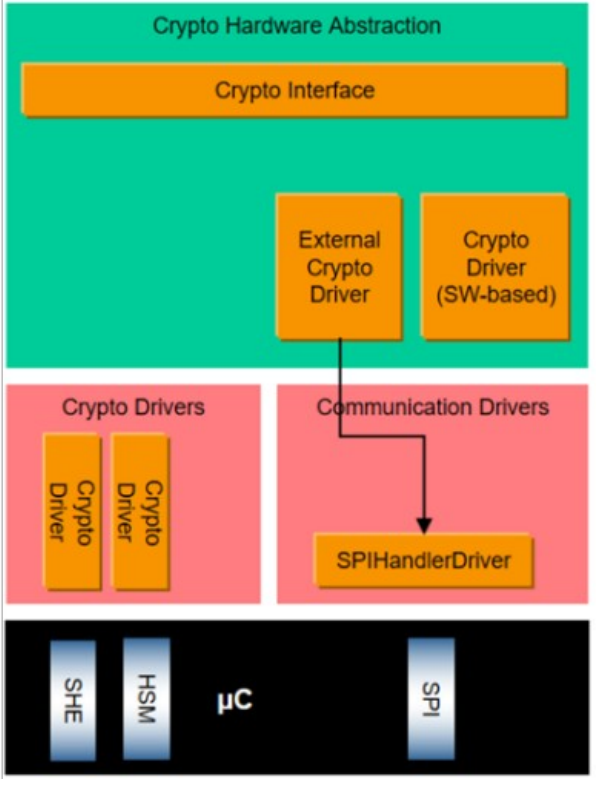
Rekomendowane algorytmy

- Generowanie liczb losowych:
  - DRNG – Deterministic
  - TRNG – True
- Szyfrowanie symetryczne:
  - AES - 128 i 256 bitów w trybie ECB, CBC, CTR, GCM, OFB, XTS
  - PRESENT – 128 bitów w trybach jw.
- Szyfrowanie asymetryczne:
  - RSA – 1024, 2048, 3072, 4096 bitów klucza
  - Curve25519/Ed25519
- Funkcja skrótu (Hash):
  - SHA-2 – 224, 256, 384, 512 bitów
  - SHA-3 – j.w.
  - BLAKE – jw.
  - RIPEMD-160
- MAC – (ang. Message Authentication Code):
  - CMAC
  - GMAC
  - HMAC

Zarządzanie kluczami







Moduł certyfikatów

- Pod-moduł certyfikatów, może przechowywać hierarchię certyfikatów w:
  - CSM – samym zarządcy Crypto
  - NVM – pamięci nieulotnej platformy
- Operacje na pamięci NVM bywają szybsze stąd klucze pośrednie mogą być umieszczone w niej w celu przyśpieszenia operacji
- Zaleca się wykonanie parsowania certyfikatu jako operację w tle.