CLOUD NATIVE
COMPUTING FOUNDATION

PARSEC

CLOUD NATIVE
SANDBOX

Sandbox Projects | Incubating Projects | Graduated Projects

EARLY STAGE

Marc Meunier marc.meunier@arm.com

SW Ecosystem Development Team

Overview

March 2021

PARSEC: A Platform Abstraction For Security

Any Workload, Any Programming Language, Any Container Runtime, Any Packaging

PARSEC

Any Platform, Any Architecture, Any Hardware

| Discrete TPM | Firmware TPM | Local HSM | Remote HSM | Trusted Apps | Custom |

PARSEC

Why Parsec?

Cloud

Edge

Endpoint

- Rich Workloads

- Multi-Tenant

- Cloud-Native Development
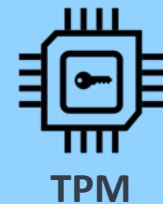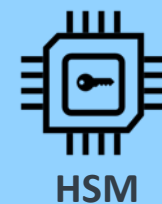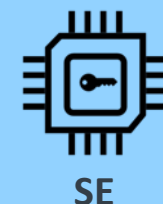
- Threat Landscape

- Variety of Platforms

- Device-specific RoT

TPM   HSM   SE
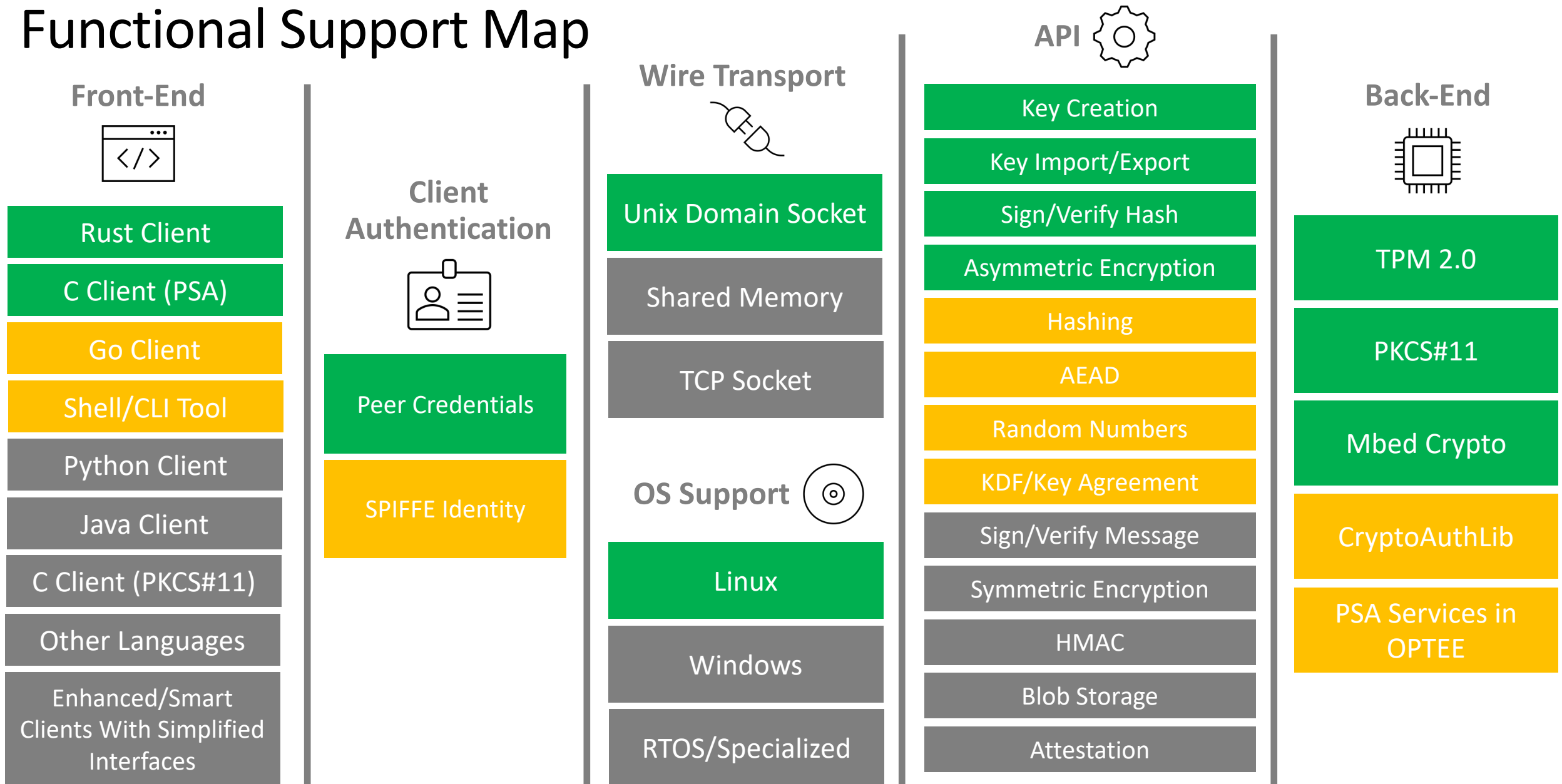
PARSEC

PARSEC: An opensource collaborative project

PARSEC Value Proposition

- **Abstraction** – a common API that is truly agnostic and based on modern cryptographic principles

- **Mediation** – security as a microservice, brokering access to the hardware and providing isolated key stores in a multi-tenant environment

- **Ergonomics** – a client library ecosystem that brings the API to the fingertips of developers in any programming language: "easy to consume, hard to get wrong"

- **Openness** – an open-source project inviting contributions to enhance the ecosystem both within the service and among its client libraries

CLOUD NATIVE SANDBOX

Sandbox Projects | Incubating Projects | Graduated Projects

EARLY STAGE

PARSEC

Functional Support Map

Front-End

- Rust Client
- C Client (PSA)
- Go Client
- Shell/CLI Tool
- Python Client
- Java Client
- C Client (PKCS#11)
- Other Languages
- Enhanced/Smart Clients With Simplified Interfaces

Client Authentication

- Peer Credentials
- SPIFFE Identity

Wire Transport

- Unix Domain Socket
- Shared Memory
- TCP Socket

OS Support

- Linux
- Windows
- RTOS/Specialized

API

- Key Creation
- Key Import/Export
- Sign/Verify Hash
- Asymmetric Encryption
- Hashing
- AEAD
- Random Numbers
- KDF/Key Agreement
- Sign/Verify Message
- Symmetric Encryption
- HMAC
- Blob Storage
- Attestation

Back-End

- TPM 2.0
- PKCS#11
- Mbed Crypto
- CryptoAuthLib
- PSA Services in OPTEE

🟩 *Available*   🟧 *Incomplete or partial support*   ⬜ *Not yet implemented*

PARSEC

Where to find us

GitHub https://github.com/parallaxsecond

📖 https://parallaxsecond.github.io/parsec-book

slack **#parsec** on CNCF https://cloud-native.slack.com

Weekly community call (see GitHub)

Note: "**parsec**" was already being used as an organization name in GitHub, which is why the expanded "**parallaxsecond**" term was selected instead.

PARSEC