PARSEC: An opensource collaborative project
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
Service Architecture

Cloud-native delivery/orchestration

Application

Client Library

Listener

PARSEC Service

Provider

TPM

HSM

TEE

Trusted App

Wire protocol based on PSA Crypto API

Platform-Agnostic

IPC
Application Identity and Multi-Tenancy

Application
  Container
  Container

Application
  Container
  Container
  Container

Identity Provider

PARSEC
  Brokering, Access Control, Keystore Partitioning

Root of Trust and Crypto Services in HW/TEE
### What is available today? What’s next?

<table>
<thead>
<tr>
<th>Client Libraries</th>
<th>PSA API Coverage</th>
<th>Back-End Support</th>
<th>Environments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rust</td>
<td>Key Management</td>
<td>TPM 2.0</td>
<td>Linux/Containerized</td>
</tr>
<tr>
<td>C</td>
<td>Sign/Verify</td>
<td>PKCS#11</td>
<td>Single-Tenant</td>
</tr>
<tr>
<td>Go</td>
<td>Asymmetric Crypto</td>
<td>Mbed TLS</td>
<td>Multi-Tenant</td>
</tr>
<tr>
<td>Python</td>
<td>Symmetric Crypto</td>
<td>PSA in TZ</td>
<td>Virtualized</td>
</tr>
<tr>
<td>Java</td>
<td>HMAC</td>
<td>Custom...</td>
<td>Windows</td>
</tr>
<tr>
<td>Other...</td>
<td>KDF/Agreement</td>
<td></td>
<td>RTOS...</td>
</tr>
<tr>
<td></td>
<td>RNG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AEAD</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
References

GitHub

https://github.com/parallaxsecond

https://parallaxsecond.github.io/parssec-book

Slack

#parssec on https://dockercommunity.slack.com

Bi-weekly community call (see GitHub)

Note: “parssec” was already being used as an organization name in GitHub, which is why the expanded “parallaxsecond” term was selected instead.