PARSEC

PARSEC – Platform Abstraction for Security

A Lightning Talk Overview for

EDGE X FOUNDRY™

Paul Howard

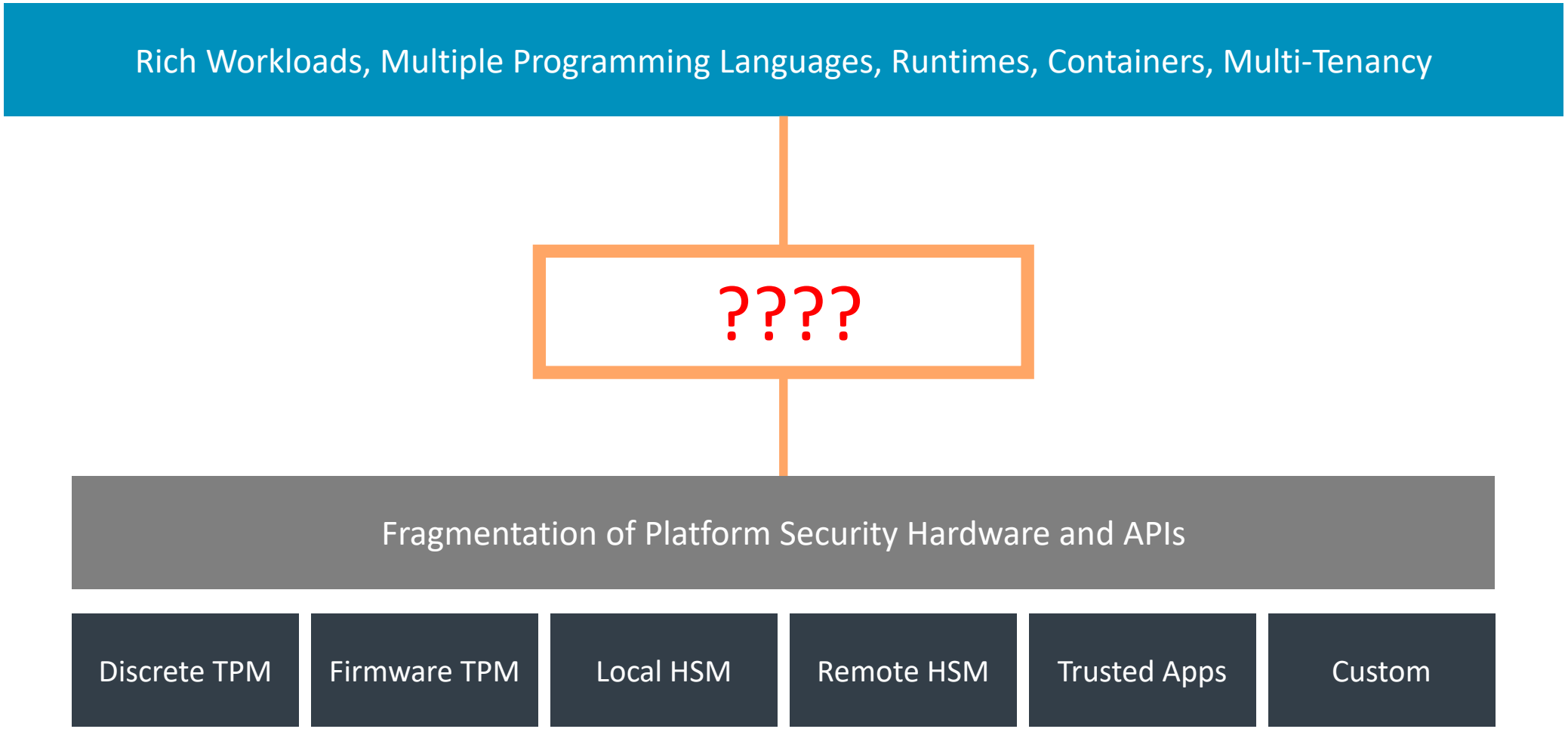
- Principal System Solutions Architect at **Arm**
- Joined Arm in November 2018
- Based in Cambridge, UK
- Software Engineering background
- **@paulhowardarm** on GitHub
- **https://www.linkedin.com/in/paulhoward4**
- **mailto:paul.howard@arm.com**
- **Slack**: EdgeX, LF, Docker Community
- Tech lead for PARSEC at Arm

PARSEC

PARSEC: A Collaborative Open-Source Project

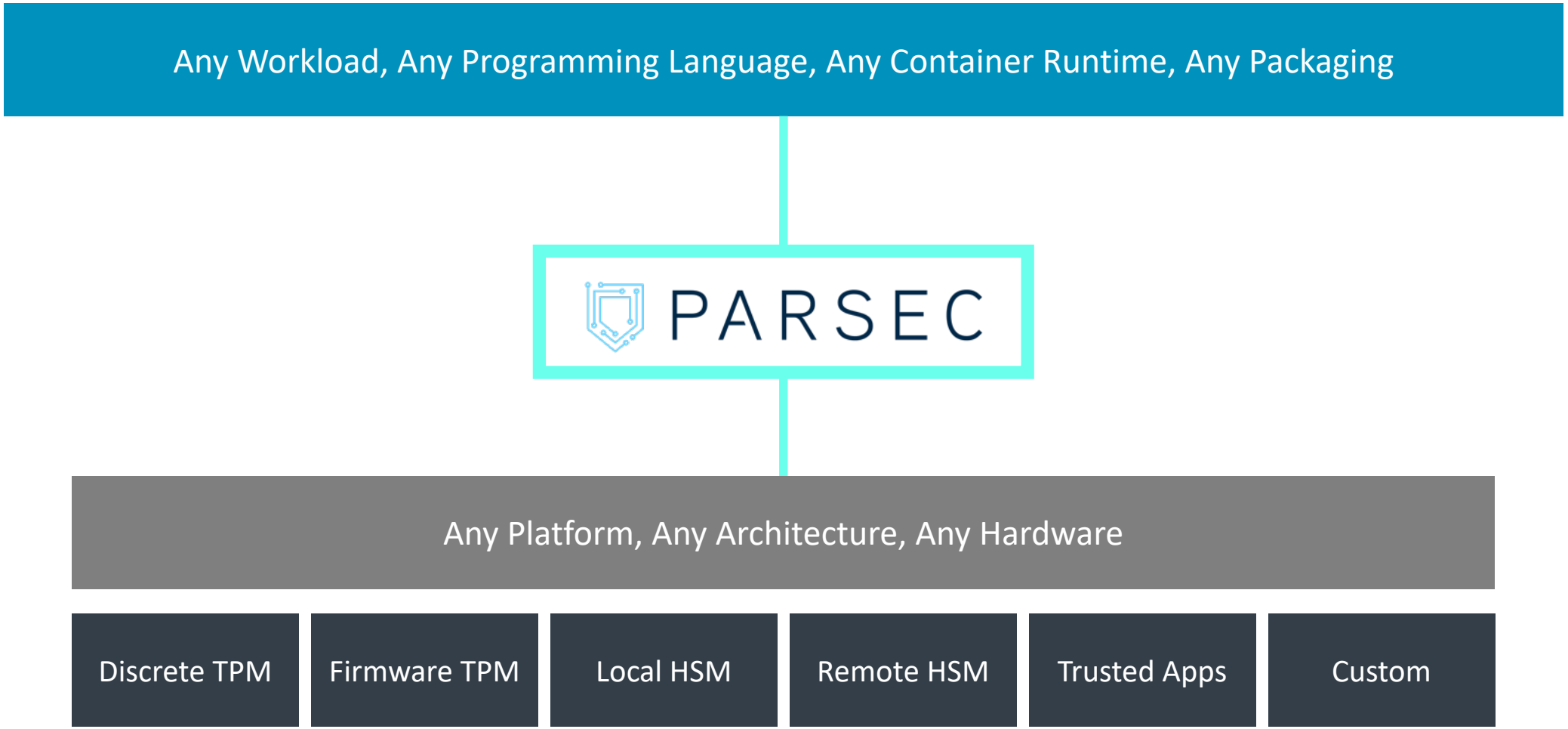
PARSEC

Edge as a Rich Compute Platform – Fragmentation Challenges



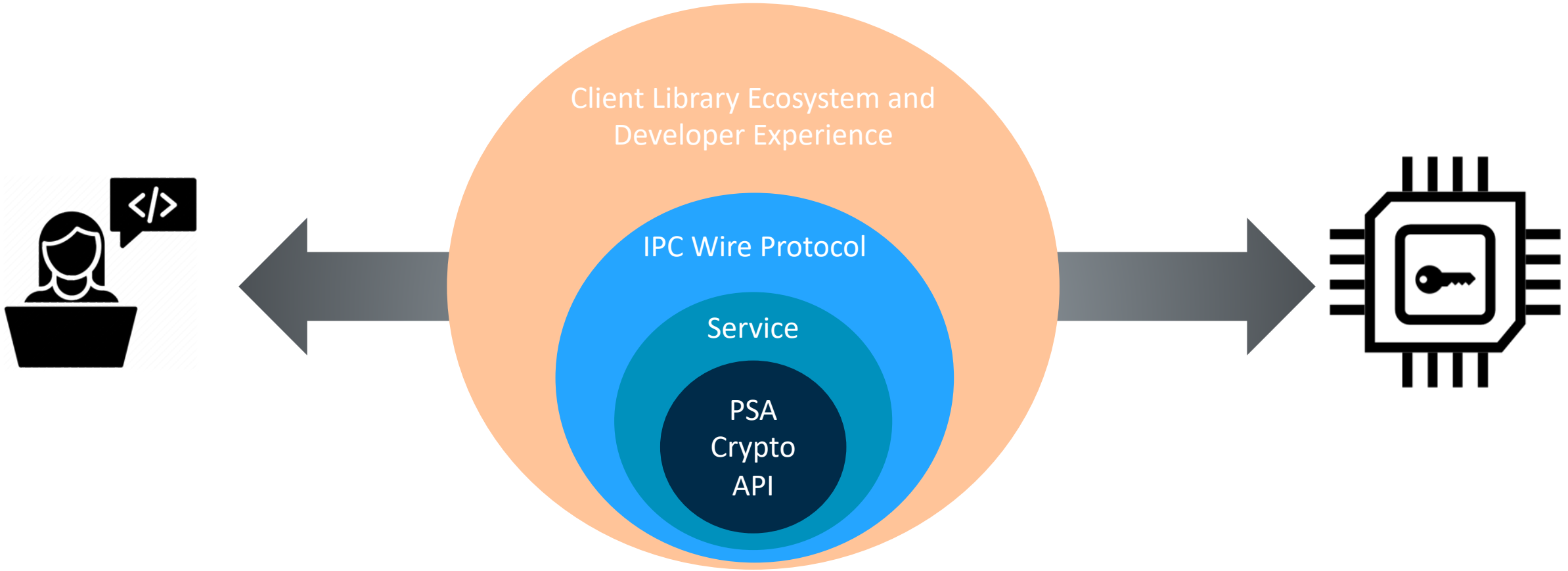
PARSEC

PARSEC: A Platform Abstraction For Security



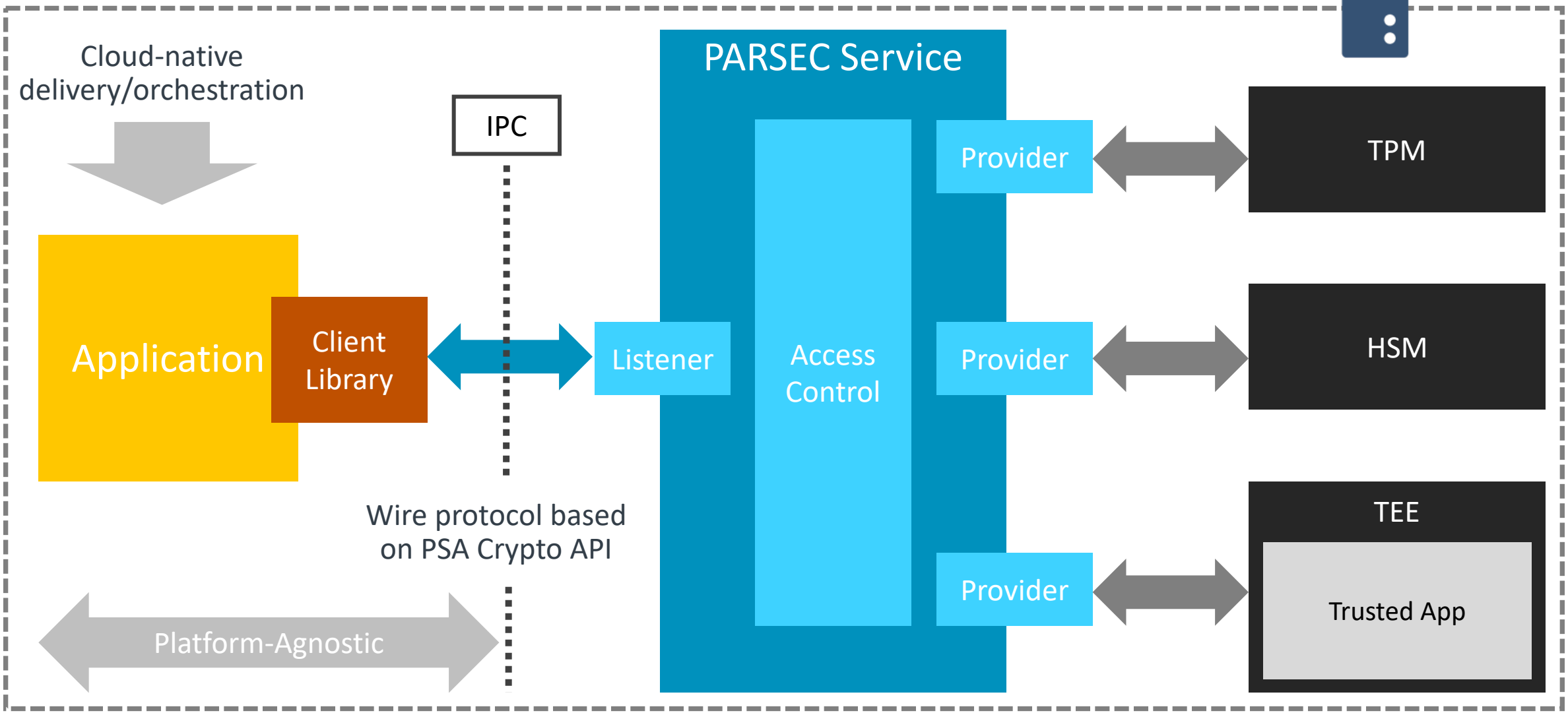
PARSEC

Conceptual View



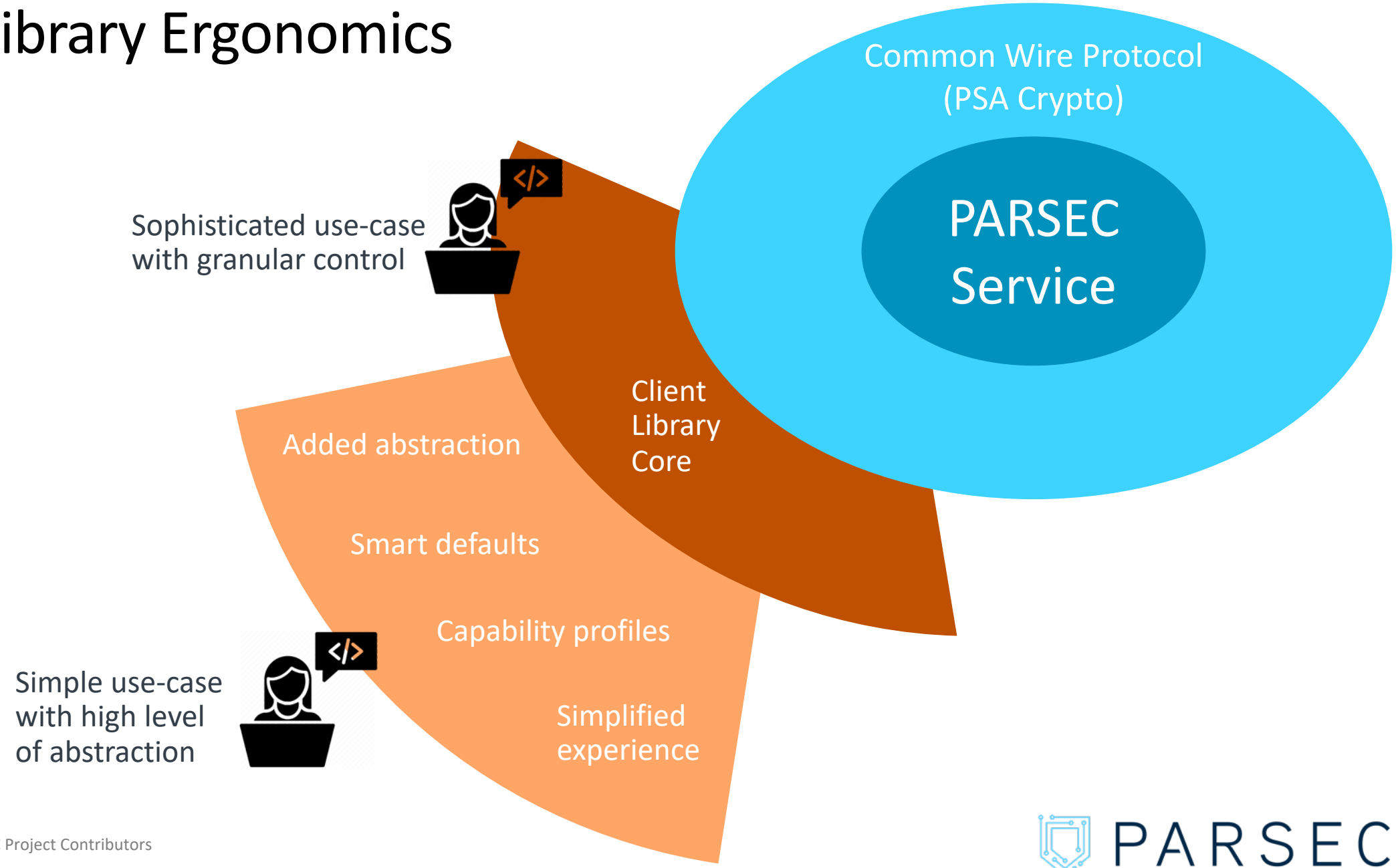
PARSEC

Service Architecture



PARSEC

Client Library Ergonomics



PARSEC

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

PARSEC Status

- Public open source as of Oct 2019 under Apache 2 license
- Available primitives based on portable RoT (eg. mTLS bootstrap) use case:
  - Provisioning asymmetric key pairs (RSA)
  - Importing/exporting public keys
  - Asymmetric sign and verify operations
- Available back-end integrations today:
  - Mbed Crypto (software only – for evaluation)
  - PKCS#11 standard (for HSMs, also connects to secure object library on NXP LS1046a)
  - TPM 2.0
- Current engineering focus on making existing pieces deployable in production
- Rust and C libraries available soon; Golang client some time later
- Seeking open governance (ideally CNCF)
- Seeking partnerships, integration opportunities and contribution opportunities

PARSEC

EdgeX Integration Opportunities

- Part of portable HW root-of-trust design? (It was mentioned yesterday)
- Source of entropy (by abstracting over available HWRNG)
- Source of IKM for Vault master key workflows?
- Anywhere where HW security needs to be driven abstractly
- Suggestions please! ☺

References

https://github.com/parallaxsecond

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

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

Bi-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