CLOUDNATIVE SECURITYCON

NORTH AMERICA 2023

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Taming Attestation for the Cloud-Native World With Parsec

Paul Howard, Principal System Solutions Architect, Arm

Who Am I?

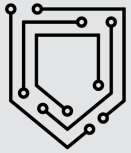
CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Paul Howard
Principal System Solutions Architect at **Arm**
paul.howard@arm.com
https://slack.cncf.io/
https://www.linkedin.com/in/paulhoward4/

@paulhowardarm

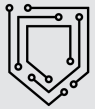
This Session

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023



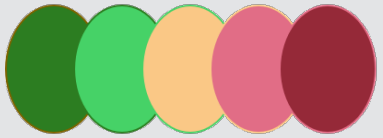
PARSEC

Context And Introduction



PARSEC

VERAISON



Attestation Evidence And Verification

TLS

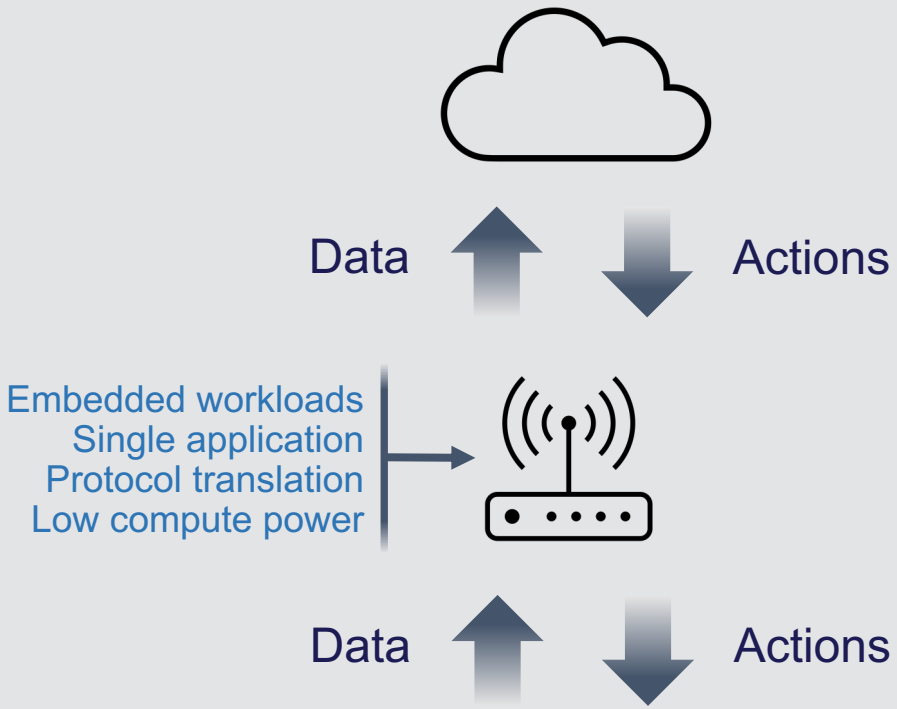
SPIRE

Applications Of Attestation

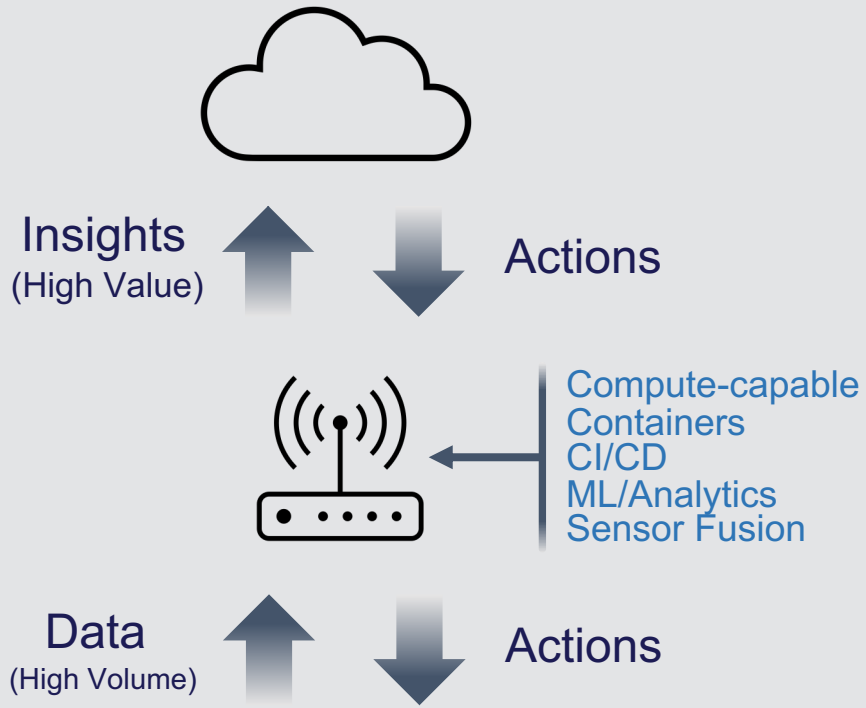
The Cloud-Native Edge

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Gateway Model



Cloud-Native Edge Model



Cloud-Native Edge Security

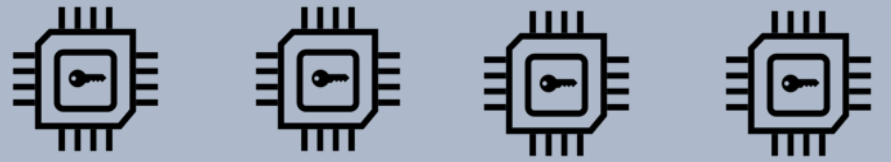
Cloud-Like Development

- Rich Workloads in High-Level Languages
- Multi-Tenancy
- CI/CD
- Containers/Orchestration

Edge

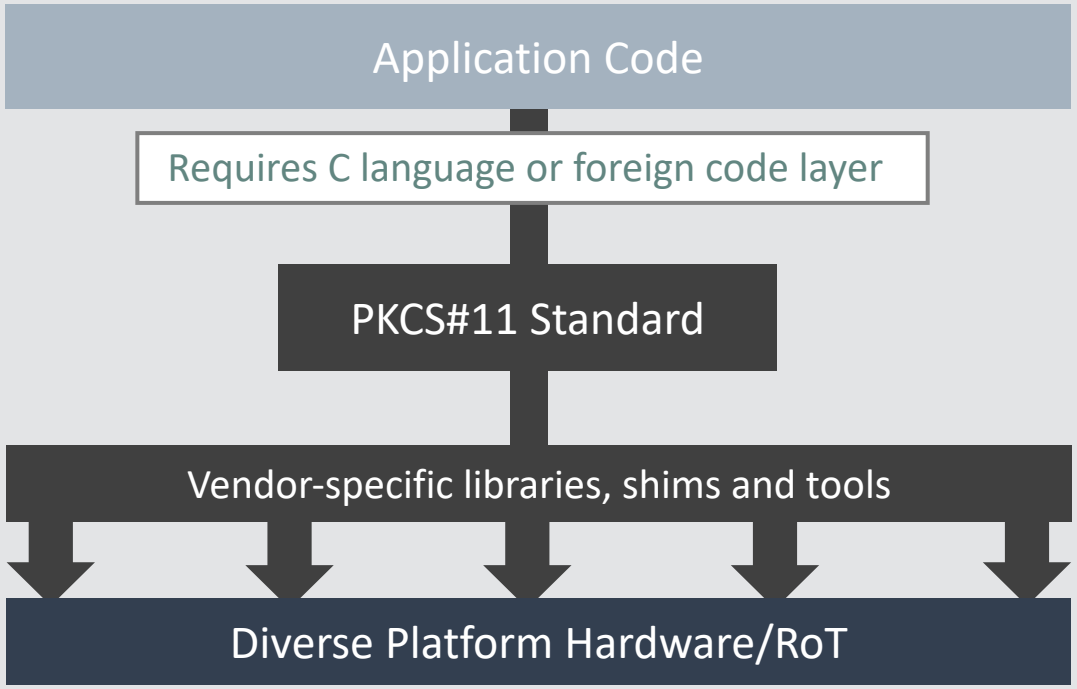
IoT-Like Security

- Tamper-Prone Environments
- Platform Diversity
- Hardware-Backed Security
- Low-Level, Device-Specific APIs
  (requiring specialist, non-portable engineering)



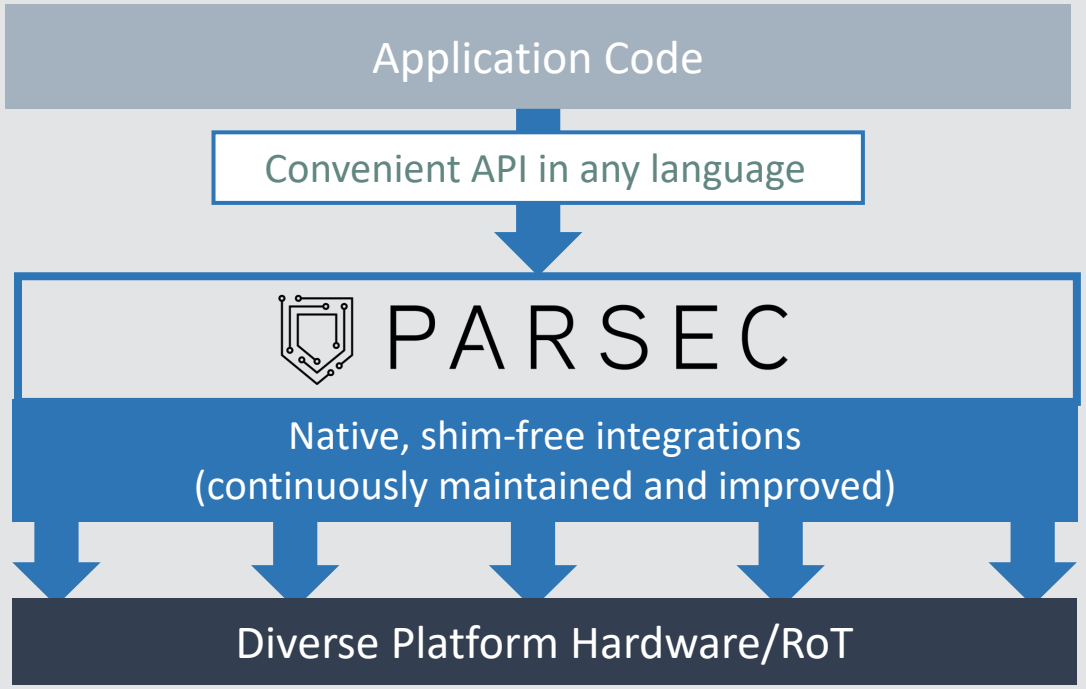
Parsec Simplifies Hardware Security

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023



The Legacy World

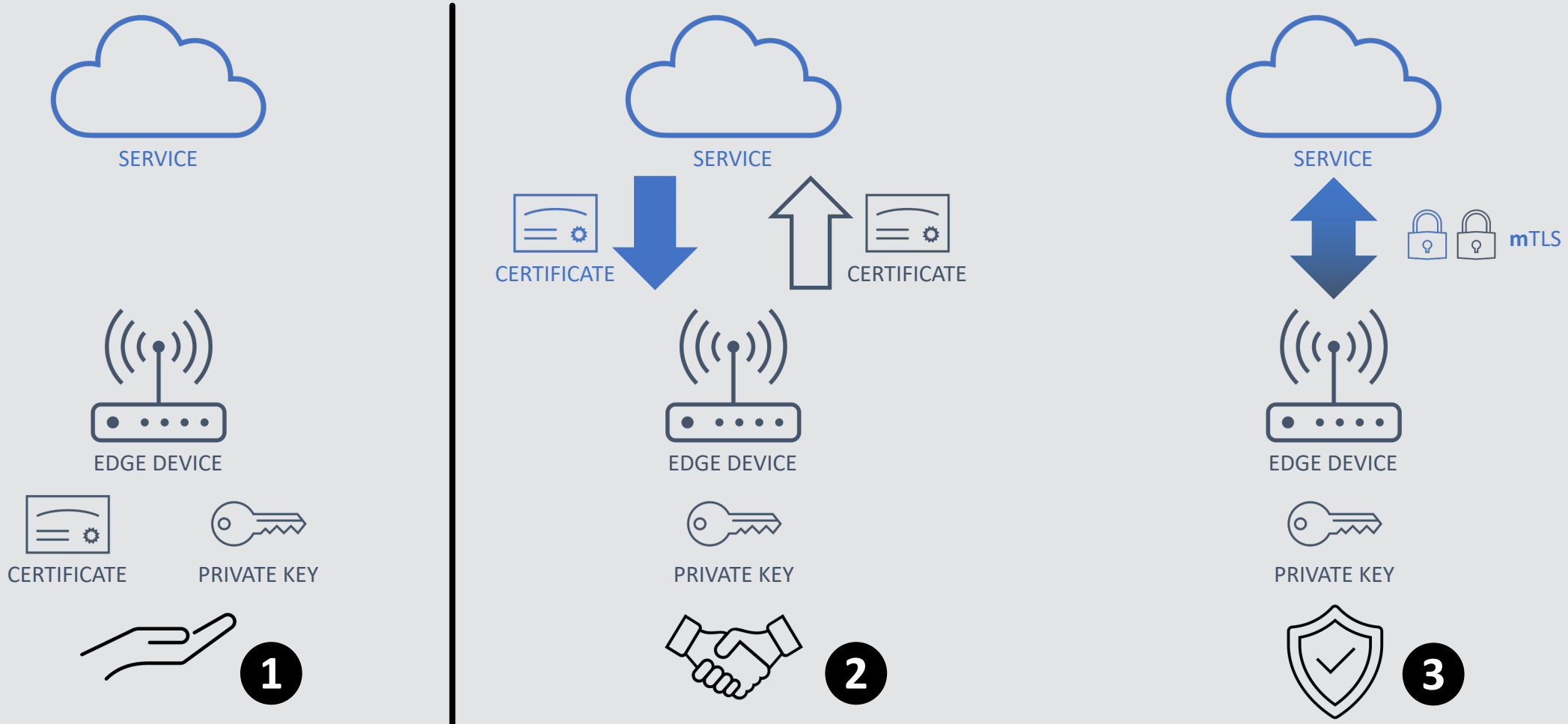
The historical prevalence of the PKCS#11 standard has led to a variety of libraries and shims. Application code needs to directly link and be tested against various libraries on different platforms.



The Parsec World

The Parsec microservice runs as part of the platform, meaning that application code has only a single component to interact with. Parsec handles the variety of integrations needed for different platforms and is maintained by an expert community.

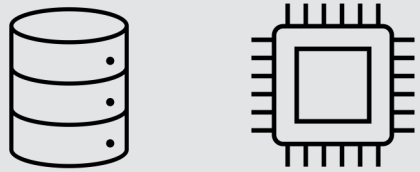
Use Case: Onboarding



Provision

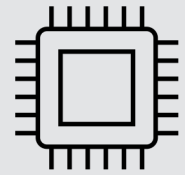
Register

The Private Key is Not Enough

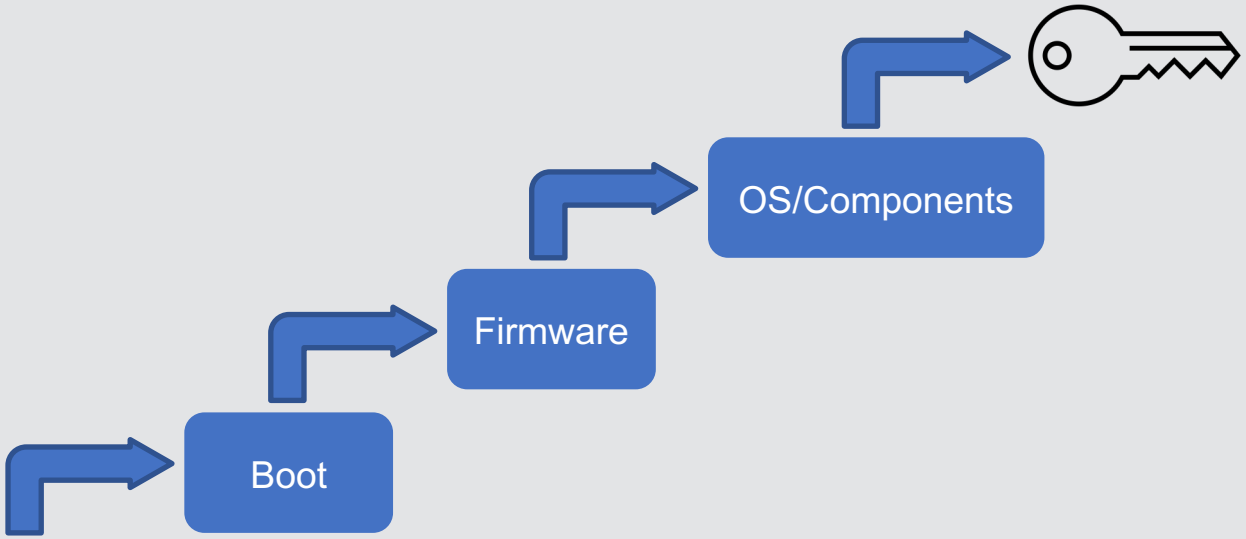


?

Private Key Owned by Unverified Platform

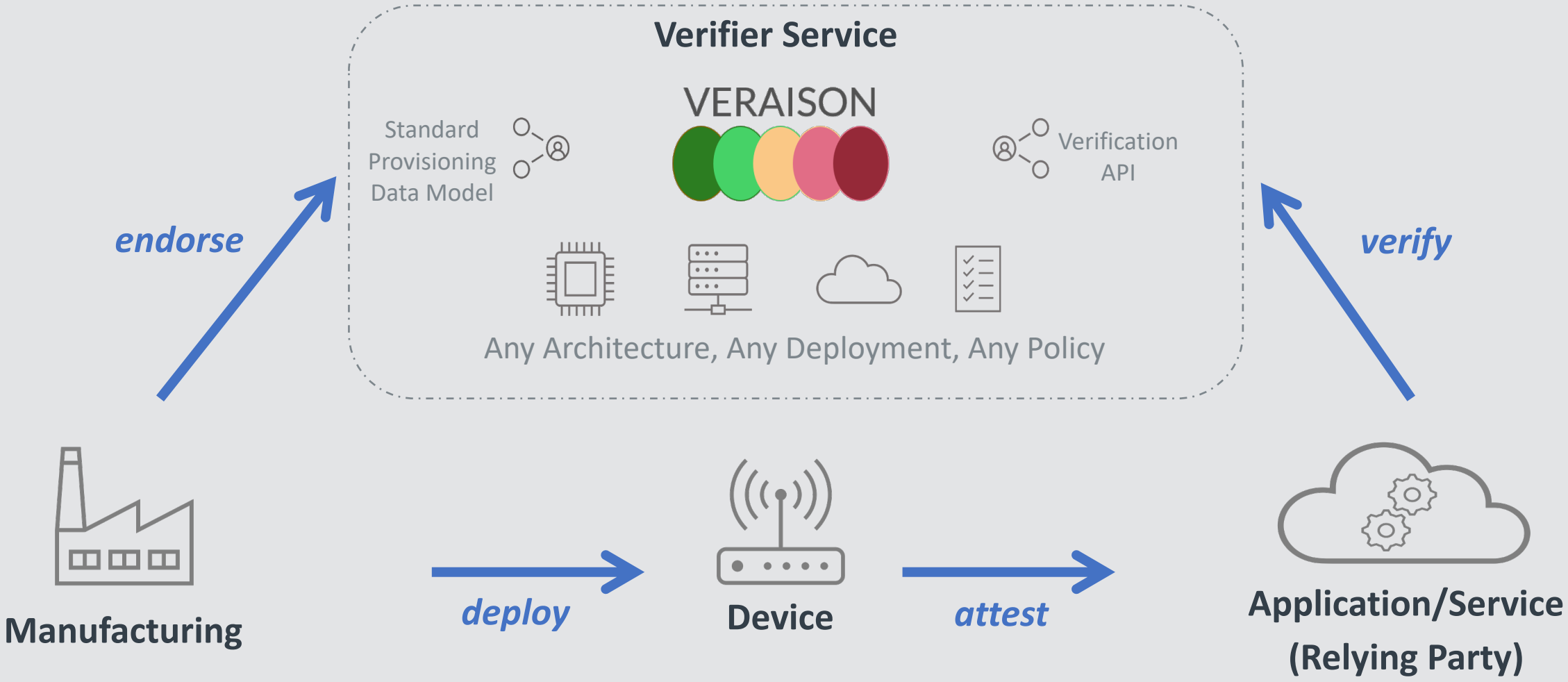


Root of Trust



Private Key Owned by Measured/Verified Platform

Endorse, Attest, Verify



Platform-Agnostic Evidence and Verification

Relying Party (Platform-Agnostic)

RATS Conceptual Messages Wrapper (Common Encapsulation)
https://datatracker.ietf.org/doc/draft-ftbs-rats-msg-wrap/01/

PARSEC

EVIDENCE

RESULTS

VERAISON

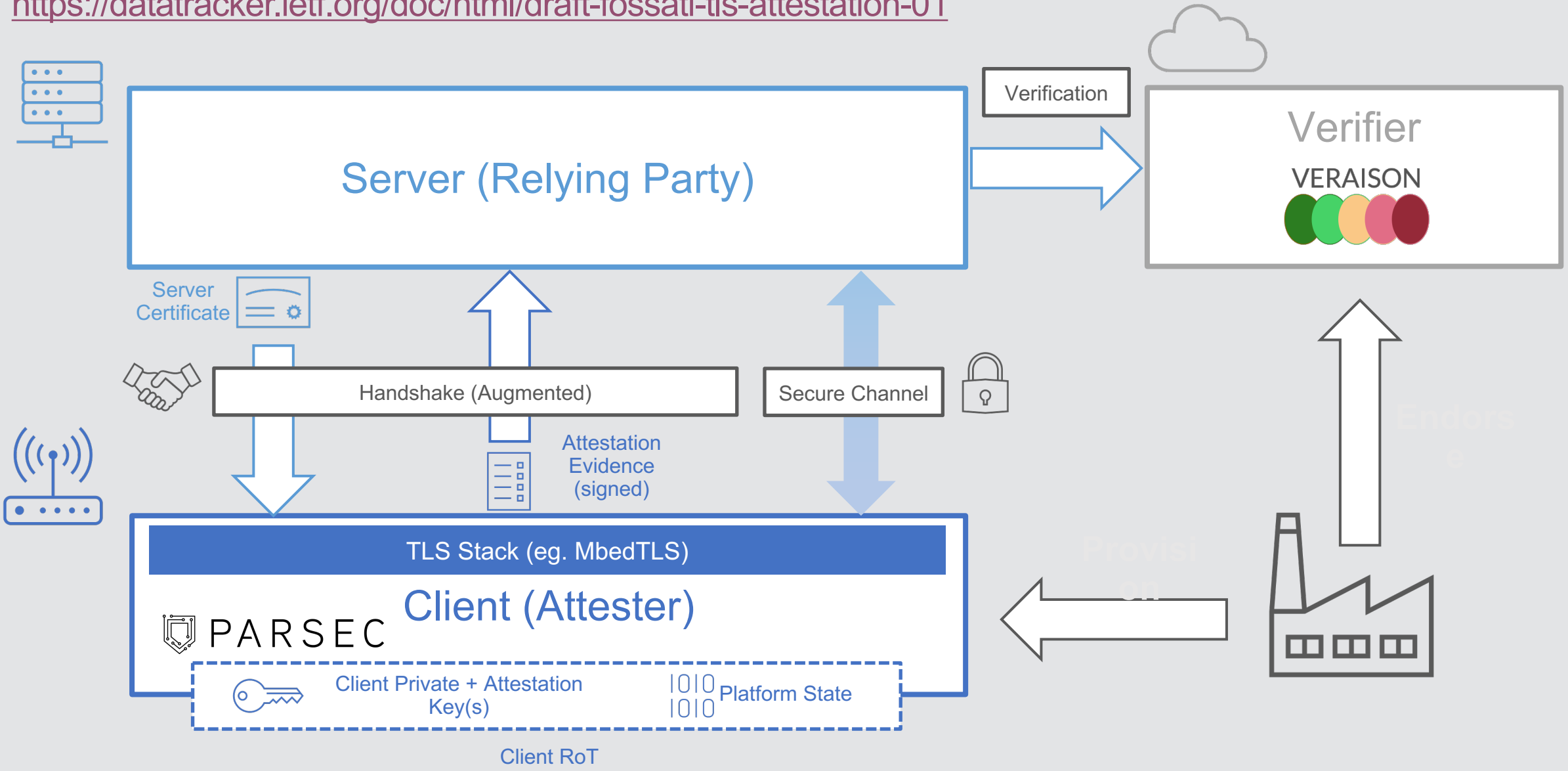
Verifier Service (Platform-Agnostic)

Trusted Platform Module (TPM)			PSA Root of Trust		
TPM 2.0 Cert/Quote Structures			Entity Attestation Token (EAT)		
TPM Components			Trusted Services (Isolated)		
Crypto	Hierarchies	PCRs	Crypto	Secure Storage	Attestation

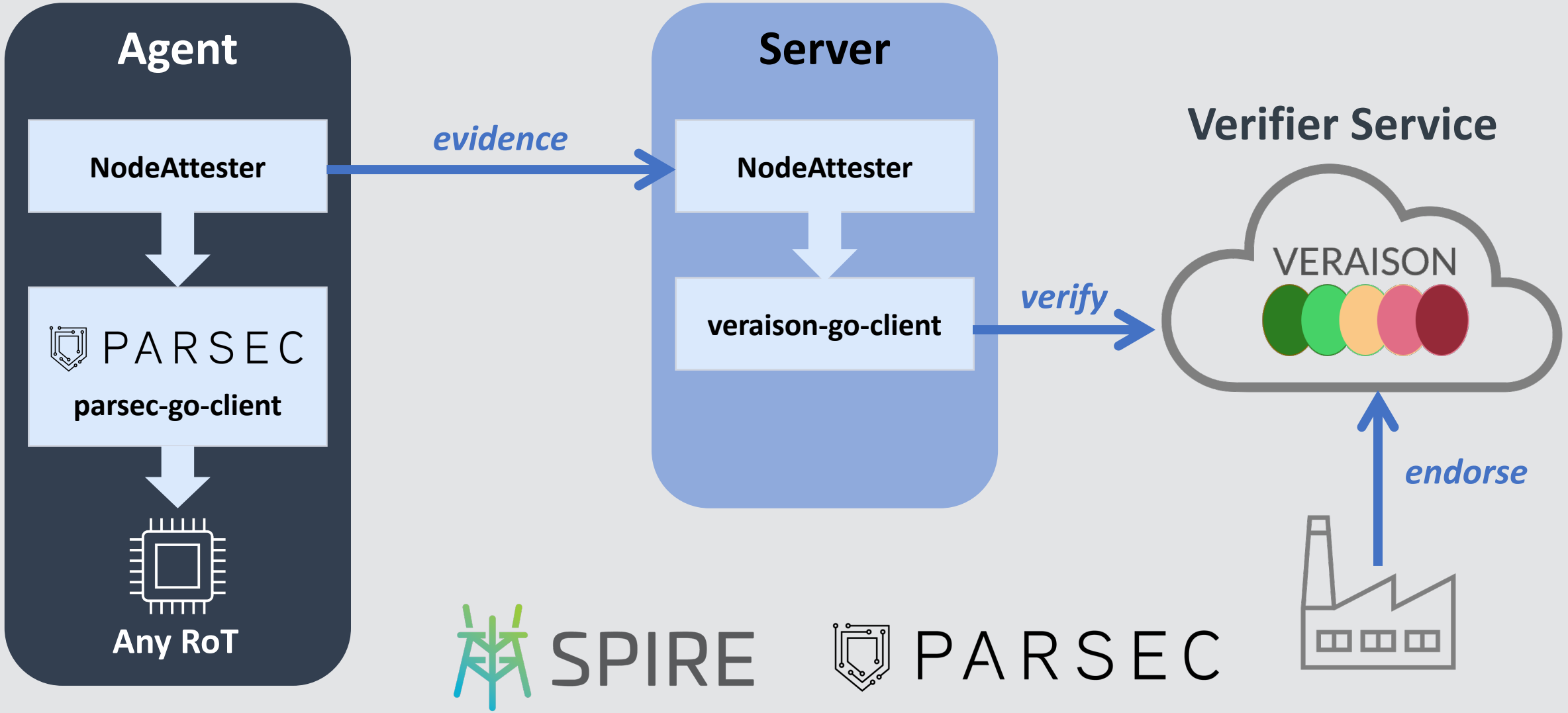
psacertified™
https://www.psacertified.org

Attested TLS

https://datatracker.ietf.org/doc/html/draft-fossati-tls-attestation-01



SPIRE Node Attestation



Learn More and Get Involved!

PARSEC

https://github.com/parallaxsecond/parsec

https://parsec.community

VERAISON

https://github.com/veraison

Attested
TLS

https://datatracker.ietf.org/doc/html/draft-fossati-tls-attestation-02

https://github.com/CCC-Attestation/attested-tls-poc

Thank You!

Q&A