SEPIOR™

Transact With Trust™

MPC-Based Key Management

Using threshold trust to address different threat models

Jakob Pagter

CTO, Co-founder Sepior

Introduction to Sepior

- Founded 2014 in Denmark
  - Spinout from University of Aarhus, world-renowned cryptographers
  - Groundbreaking research in Multiparty Computation (MPC), essential patents & applications
  - Proven leadership team based in CA and Denmark
  - Well funded, grants from EU & Denmark, Series A

- World-leader in Threshold Cryptography
  - Distributed cryptographic key management using MPC
  - License cryptographic libraries, SDKs, and platforms to solution integrators and service providers
  - Co-founders of the MPC Alliance

MPC ALLIANCE

I/O models (NISTIR 8214A)

- "Threshold modes" focus on how input and output sent to/from client
- No explicit focus on
  - Who control the components
  - How is the client structured
- These perspectives are often an important focus of the practitioner using a Threshold Security Module and map to the threat model and security policies underlying the practical application

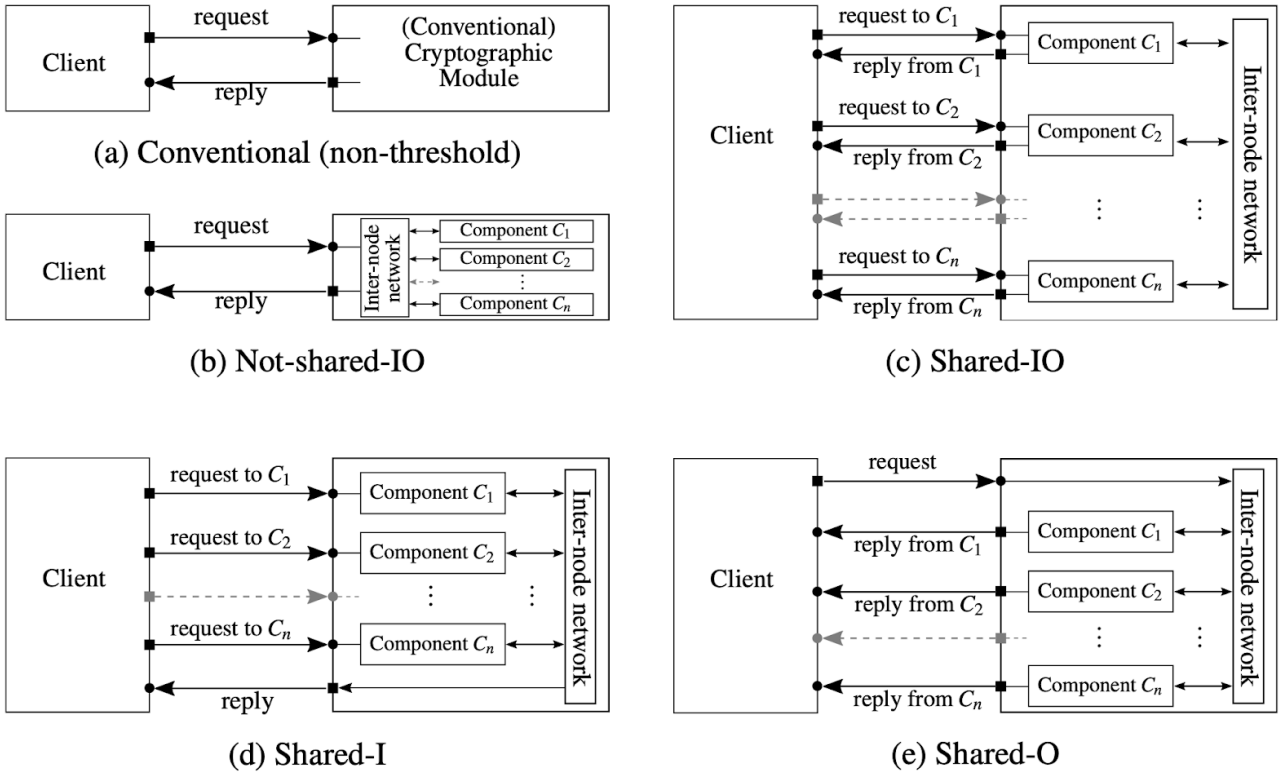
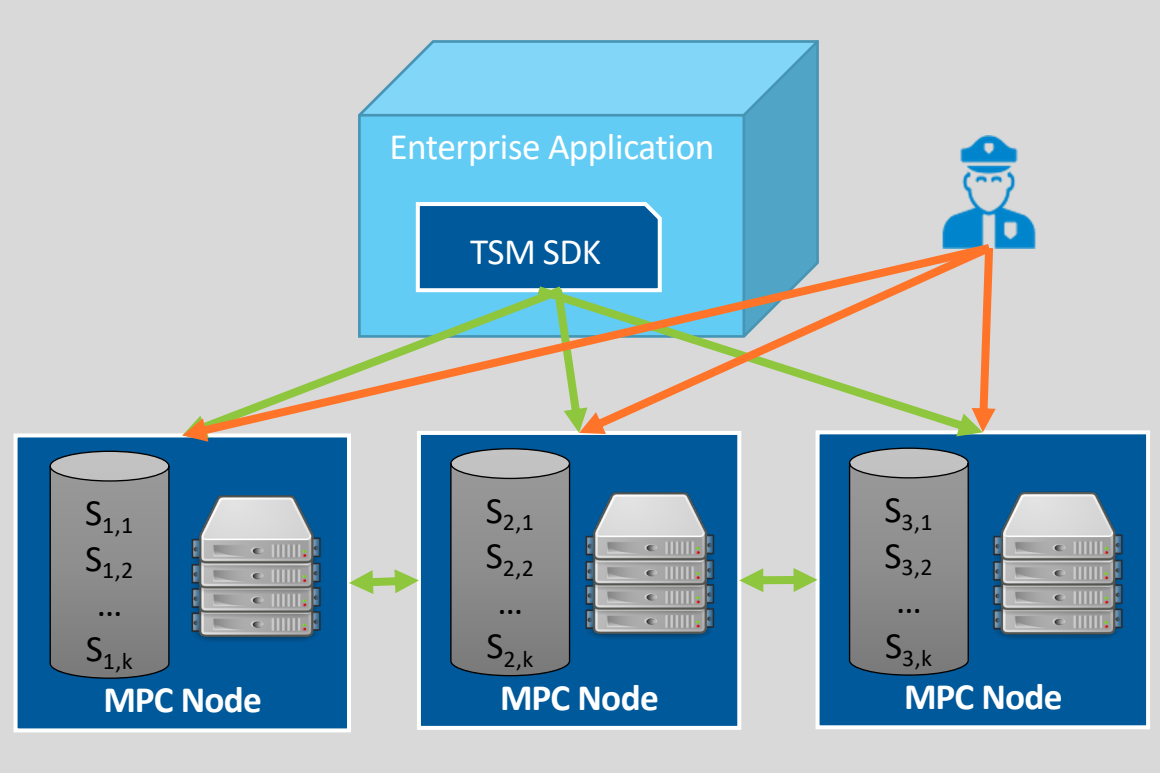


Figure 2. Several threshold interfaces (and one non-threshold case)

From NISTIR 8214A

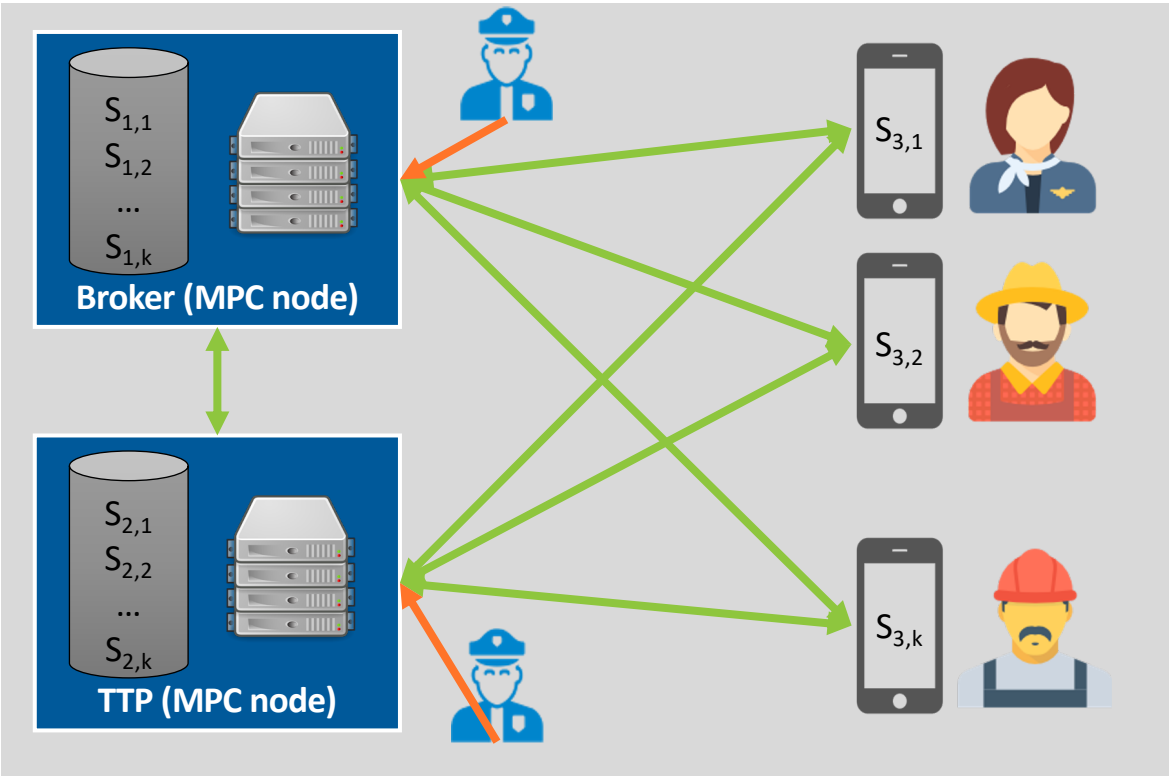
Two examples

Threshold Security Module (TSM)



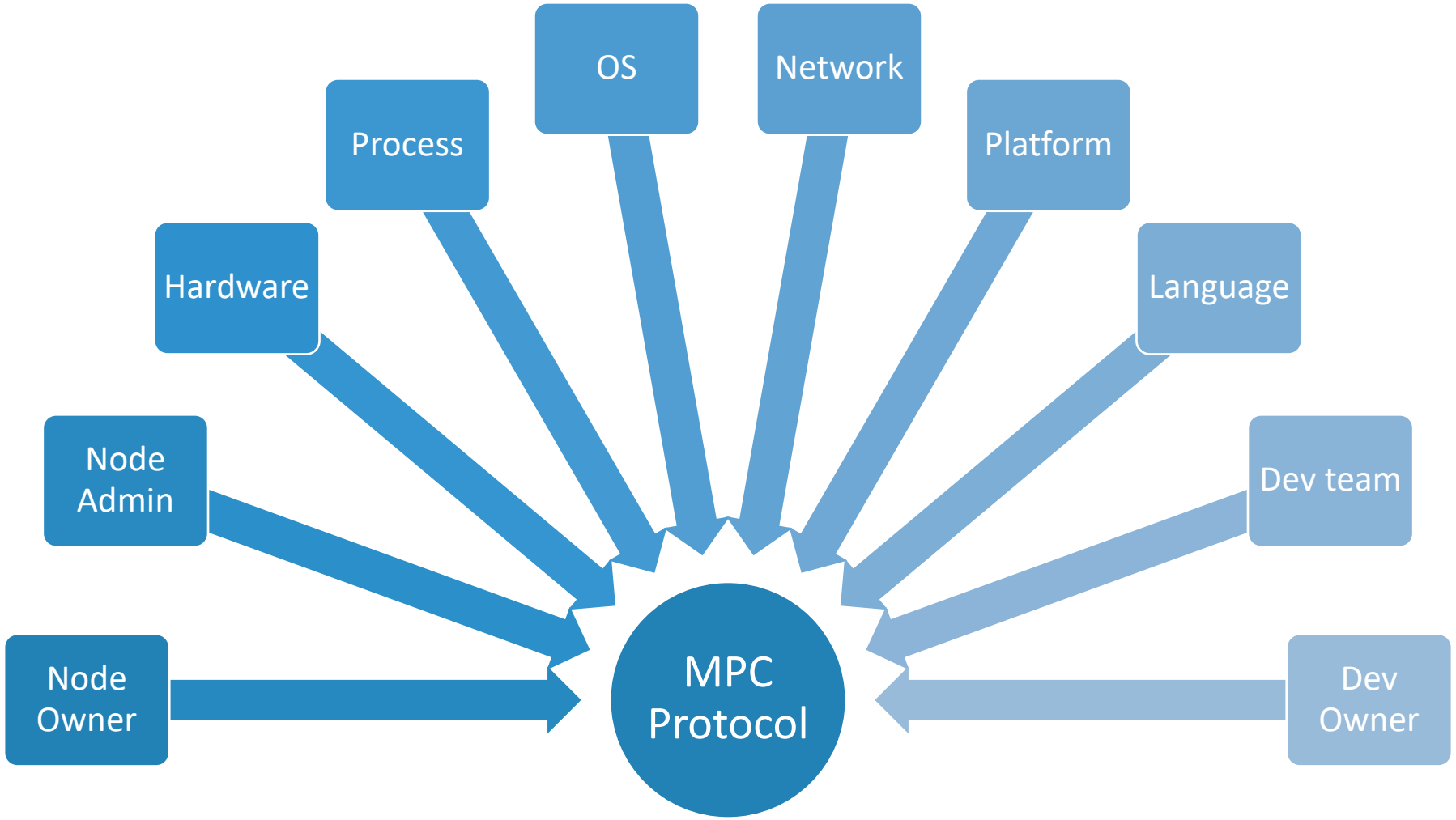
(Simplified) threat model: intrusion across enterprise perimeter

Policy-ruled end-user wallet



(Simplified) threat model: mutual distrust between end-user and wallet service

Taxonomy building blocks



SEPIOR™

Transact With Trust™

THANK YOU!