ICMC 2019 PKCS #11 Interop Demonstration Event

Tony Cox

Jun 2019

Rationale

- Requirement to show testing value
  - Participants
  - Industry expectations
  - Spec & Profile development
- Commitment to members

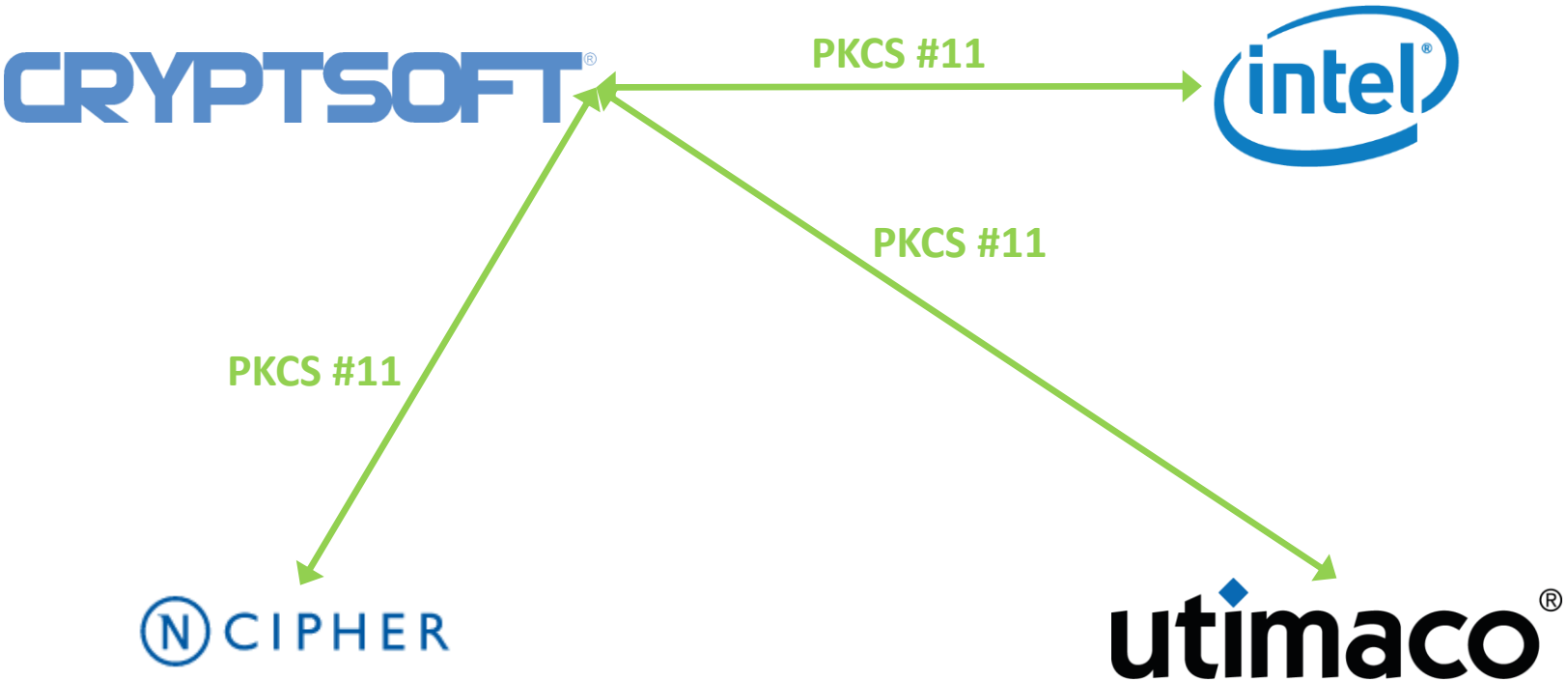
Event Overview

- Relatively painless setup
- 2 full days (in between speaking sessions)
- ~400 attendees at event
- Most booth visitors were knowledgeable about PKCS #11

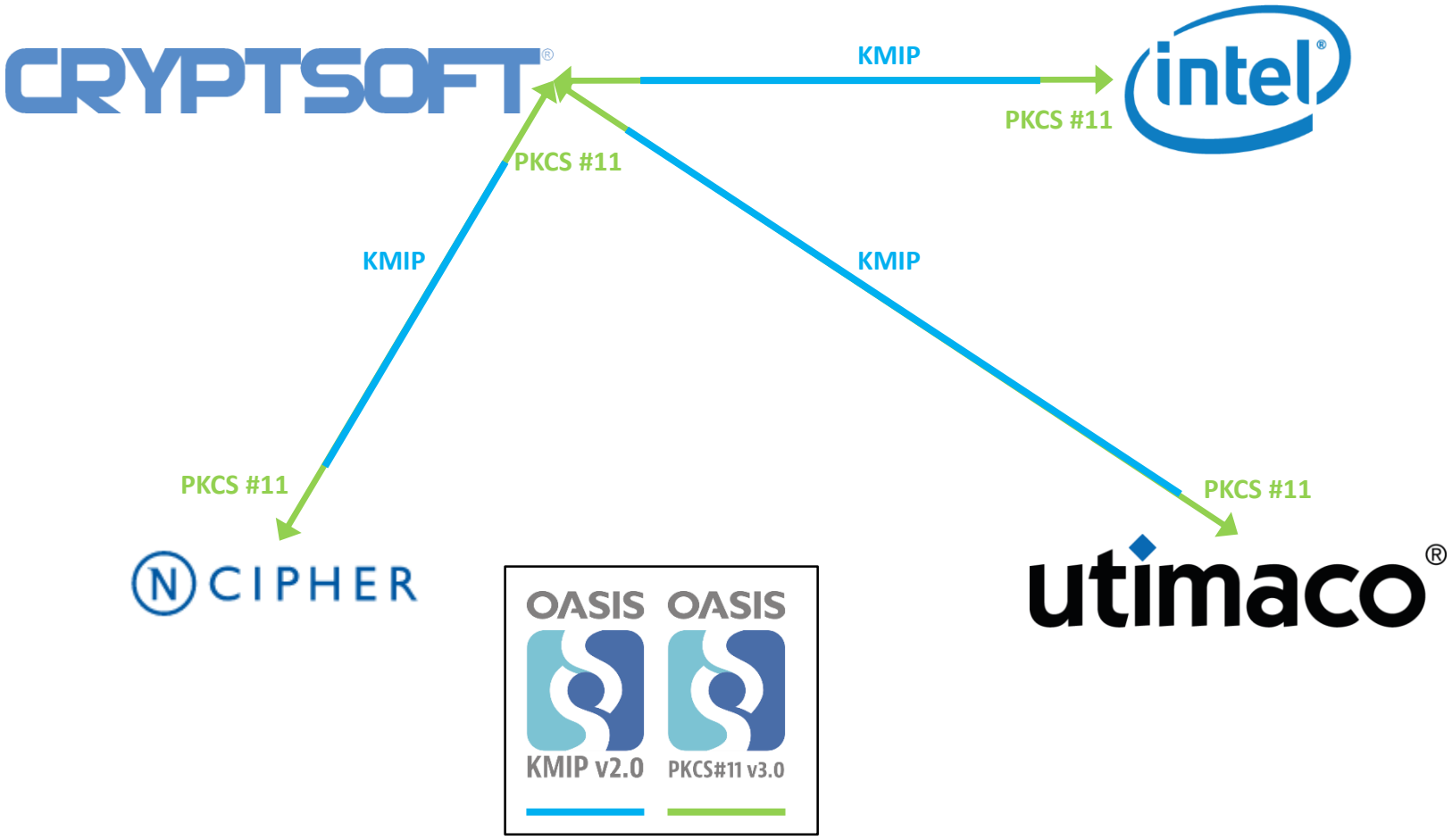
What we actually demonstrated

- A range of operations:
  - C_GenerateKey
  - C_GenerateRandom
  - C_Encrypt/C_Decrypt
  - C_GetMechanismList
  - C_GetInfo
  - C_FindObjects
- All operations performed without needing to install vendor-specific PKCS#11 drivers/APIs on consumer systems
- All operations were serialised and transmitted via a standardised network protocol (KMIP)
- Vendors were able to see actual PKCS #11 interactions between vendors

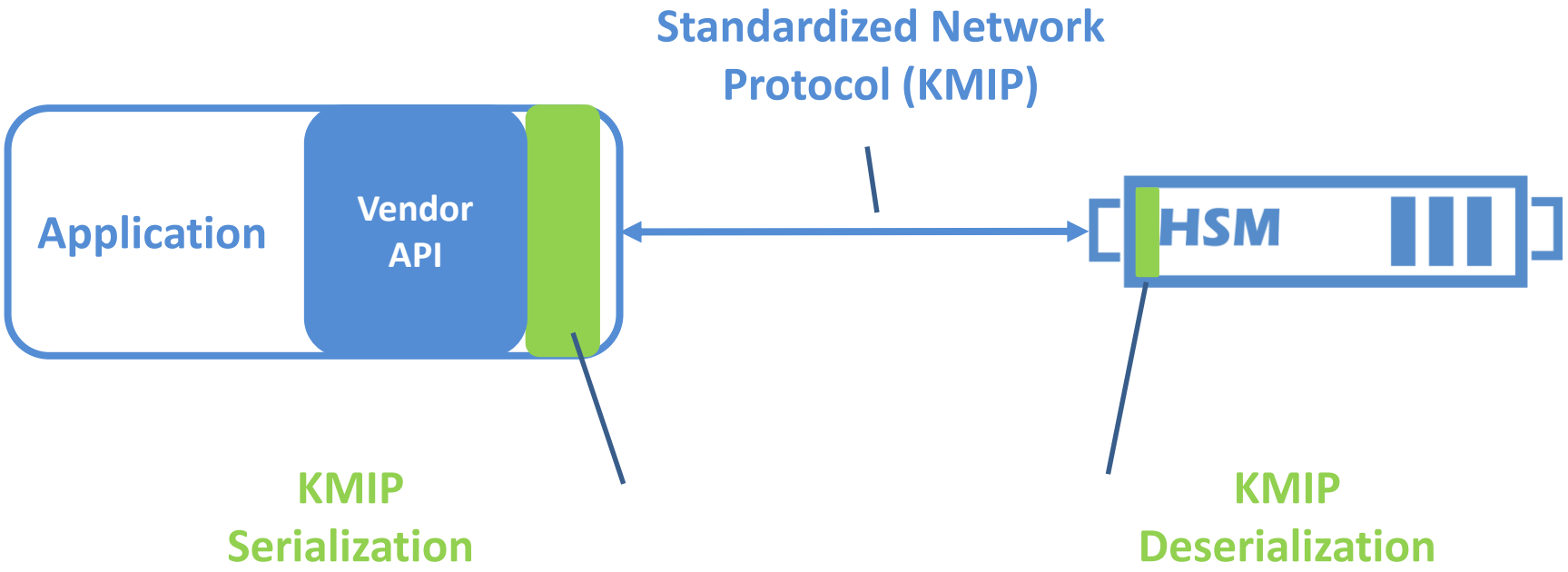
PKCS #11 Demonstration



PKCS #11 Demonstration



PKCS #11 Demonstration



Where to from here?

- All participants stated interest in attending an interop at ICMC2020 using a further-developed version of what was used this year
- Stated interest in overlapping with KMIP
- Stated interest in XML-based testing to prepare for the event and eliminate some teething issues during setup.
- Stated interest in conformance testing metrics