Maritime Connectivity Platform

Identity Management and Security in MCP

Michael Kirkedal Thomsen
IFI, University of Oslo & DIKU, University of Cph

MCP Identity Management & Security Seminar
IALA HQ, Sep 24 2022

Outline

Identity Management and Security in MCP

What is MCP

What is MCP **NOT**

MCP is not one stand-alone system.

Example: The Internet is not the servers that runs webpages

- We create the foundation for others to run it
- We provide the needed documents and standard for interoperability

Design Principles

What are our guiding principles when designing the MCP?

- Decentralisation
  - Centralised system does not scale and are more vulnerable to errors and malicious attacks.
- Diversity
  - Monotone systems can result in single point of failures
  - Policy in different countries can have both positive and negative effects
- Security using known principles
  - We should not invent new
  - Smarter people have already done the work
- Separation of concerns
  - We need different components to handle different effects.

Trust!?!?

Phil Zimmermann on Web of Trust for PGP

As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys.

- The world is not based on absolute truths
- We have confidence in the system based on trust we build
- Trust is a product of multiple sources
- Trust must be an explicit property

The Maritime Identity Register

The Maritime Identity Register (MIR)

A central component if the Maritime Identity Register [1]

What does the MIR give?

- Tokenisation of real things
  - Identifiers with MRNs

[MCC IDsec2,]

- Providing cryptographic identities
  - Public/private key-pairs and certificates

[MCC IDSec3,]

[1] Oliver Haagh will detail this more in the afternoon

The Decentral nature of MIRs

There should be more than one MIR instance.

- Each MIR is responsible for its own MRN domain
- Working independently
- Vetting procedure

[MCC, Gen5]

- Trust to identities given by identity service provider

Currently: Navelink, KRISO.[2]
Comming: Fintrafic, MarineFields/Bergman Marine.

[2] Mikael Olofson in a moment

Extending Trust

Identity Management and Security in MCP

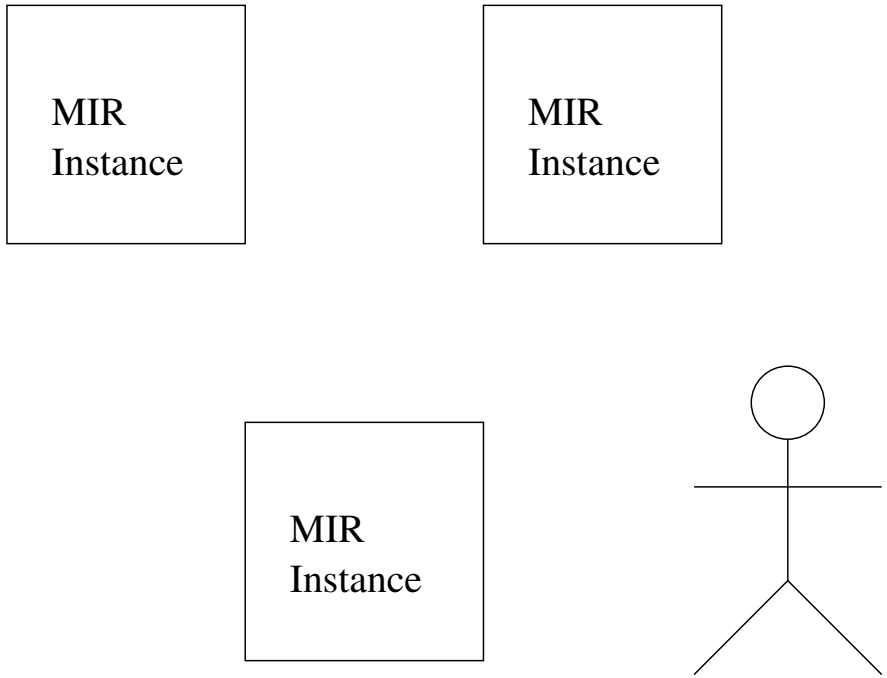
The Maritime Identity Register

Extending Trust

Conclusion

Overall MCP IDSec architecture

The decentral MIRs gives what is common by conventional Certificate Authorities.



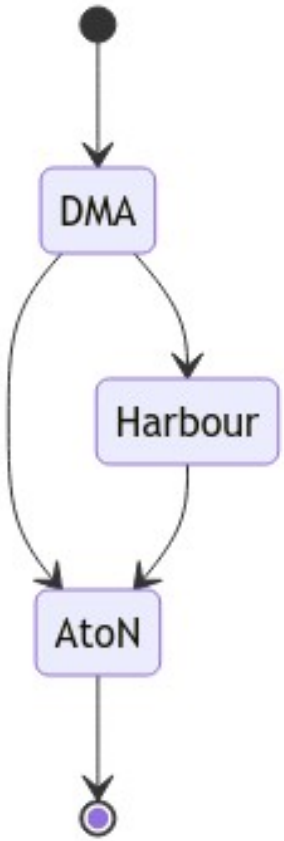
Check that certificates are valid.

The Trust System

Define an “order” on certificates.

- Keys/certificates are associates with a term/property
- Define a simple structure that defines the relationships
- “Proves” for these structures are distributed via decentral systems

Example



Conclusion

Identity Management and Security in MCP

The Maritime Identity Register

Extending Trust

Conclusion

Conclusion

- MCP provides vetting though the MIRs
- Identifiers are besed on MRNs
- Identities can be associated with certificates
- Trust system can give structured relationship between multiple actors
- Decentralisation is used for security, reliabillity and diversity

Thank You

Questions

?

Bibliography I

MCC, M. C. P. C. (Gen5).

Vetting procedure for mcp instance providers.
MCP Gen5, version 1.1.

MCC IDsec2, M. C. P. C.

Mcc identity management and security: Identity management.
MCP IDsec2, version 1.0.

MCC IDSec3, M. C. P. C.

Mcc identity management and security: Public key infrastructure (pki).
MCP IDsec3, version 1.02.

UiO : Department of Informatics
University of Oslo

Michael Kirkedal Thomsen

Identity Management and Security in MCP