COIN Security
draft-urien-coin-sec-00.txt

Pascal.Urien@Telecom-Paris.fr

About COIN

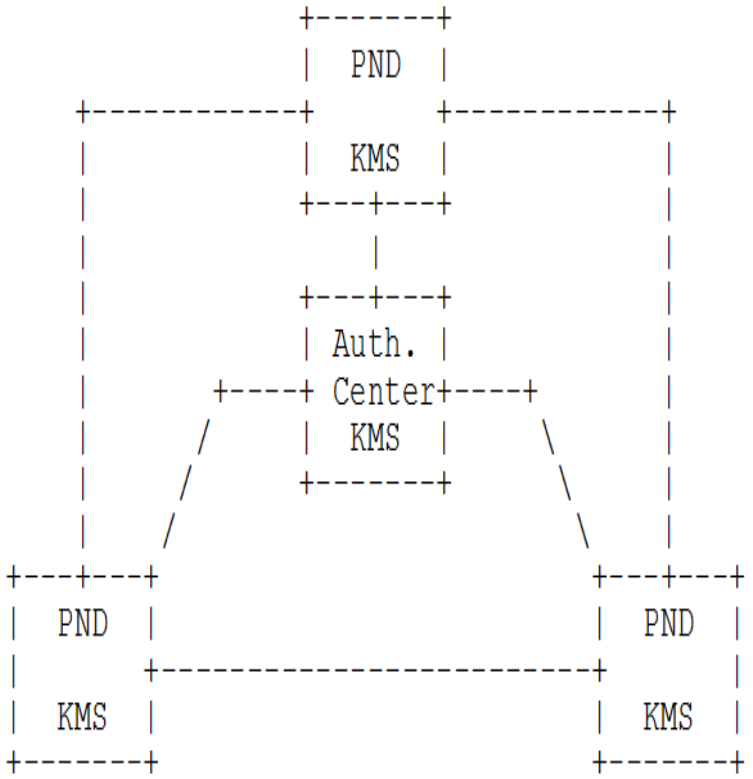
- Computing in the Network (COIN) is a concept that aims at deploying and using programs, based on computing resources hosted in Programmable Network Devices (PNDs).
  - Such infrastructures could be integrated in edge computing or 5G slicing.
- A program works with several PNDs exchanging data over secure communications.
- In that context there is a need for security
  - for intrinsic COIN needs
  - for programs running in COIN systems

Intrinsic COIN Security

- COIN should rely on fully encrypted communications, what implies authentication and keying mechanisms based on symmetric or asymmetric secrets.
- Some research items for COIN security are the following:
  - 1) Security Architecture
  - 2) PND security model
  - 3) Key Management System
  - 4) Authentication Center

Intrinsic COIN Security

- PND could include a Key Management System (KMS) in order to provide these security features.
- If COIN services rely on centralized architecture an Authentication Center (AC) should provide KMS functionalities.
- PND processors can also include a physical entity with isolated (for example Trusted Execution Environment, TEE) or tamper resistant computing resources (sometimes refers as integrated secure element iSE).
- A classical approach in cloud computing relies on the deployment of Hardware Secure Module (HSM) in data centers, typically performing offload or KMS operations, i.e. computing cryptographic procedures in a trusted environment.



Program Security

- Programs could have security requirements. For example the generation of blockchain transactions implies secure key storage and trusted signature.
- Some research items for program security are the following:
  - 1) Secure program deployment
  - 2) Attestation and secure cryptographic provisioning
  - 3) Level of security & trust
  - 4) Scalability & Performances
- The IoSE draft introduces on-demand secure computing resources, identified by Uniform Resources Identifier (URI), and could be a use case for COIN