TA Architectures

Stefan Santesson

Microsoft

stefans@microsoft.com

The Trust Anchor store

Local device or host

Local TA Mgmt App	Application

API

TA Store

OS
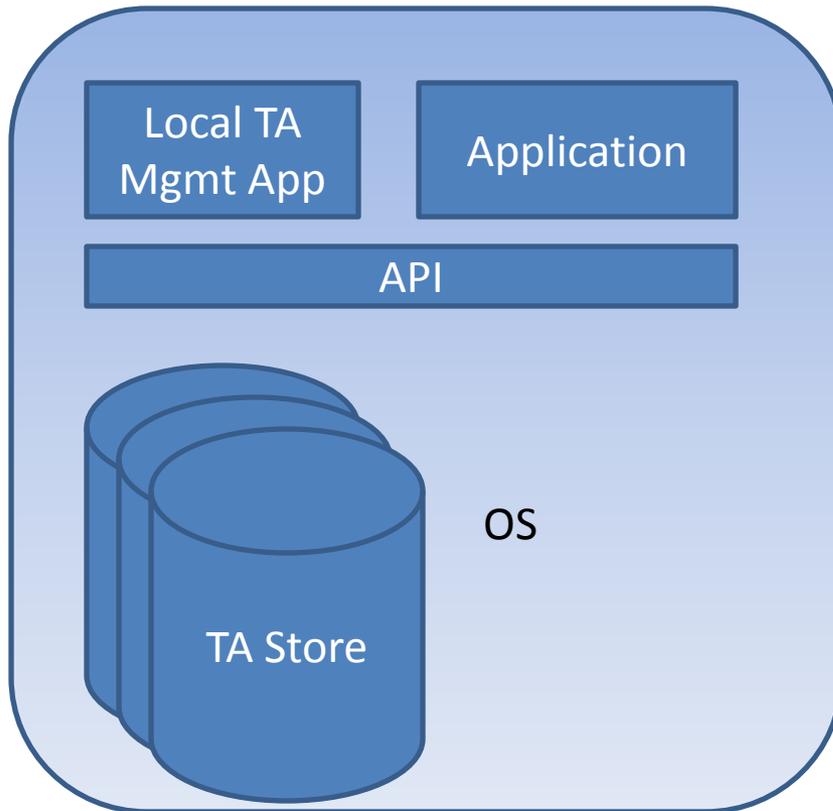
TA Management Protocol
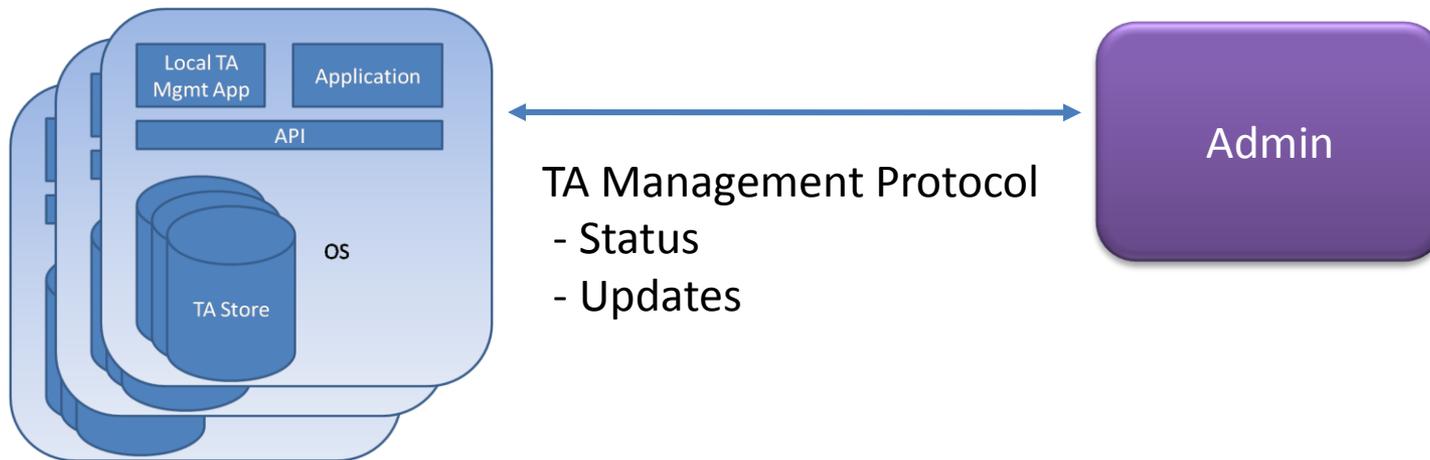
TA Management - Directory
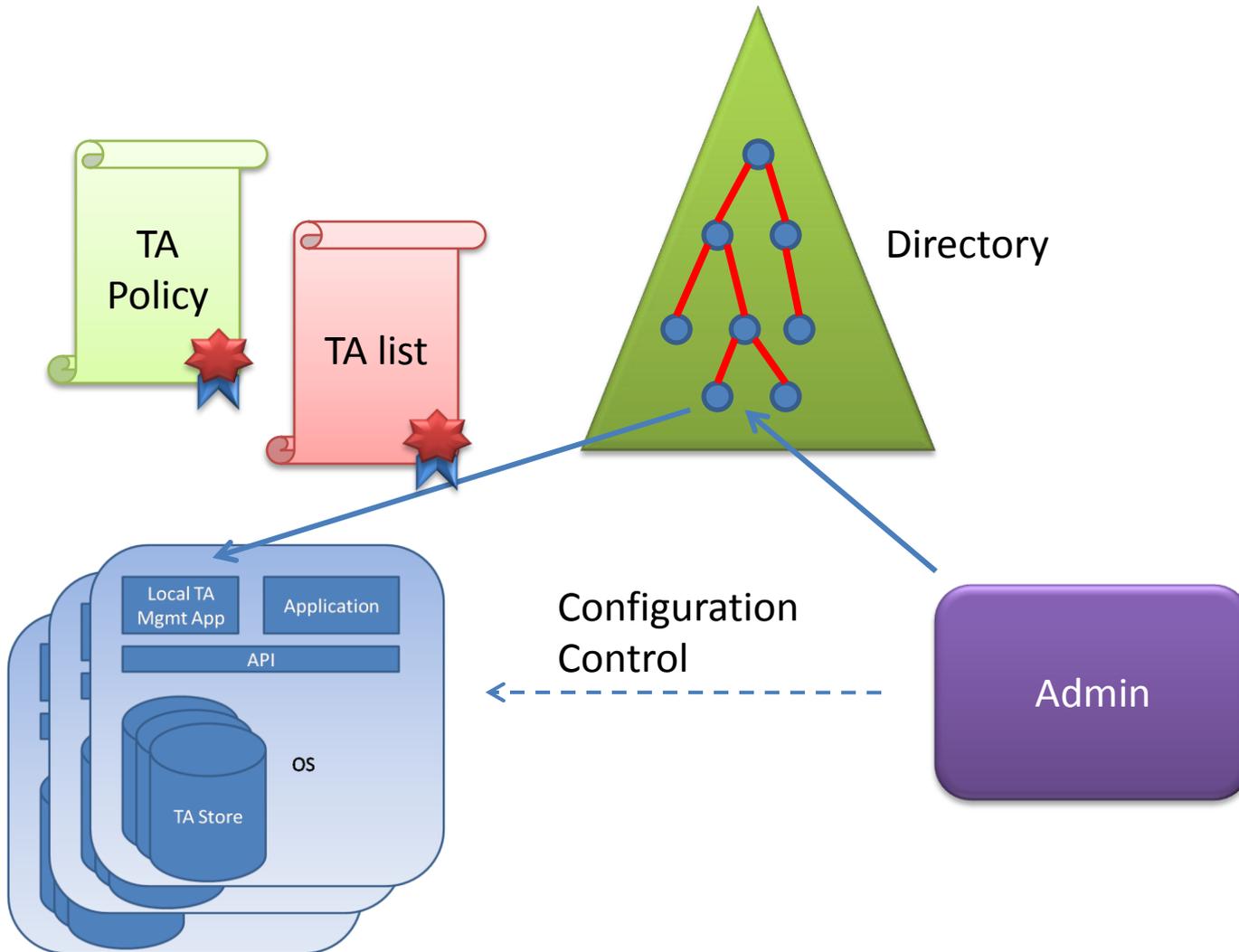
Problem statement

- Still requirements document more than problem statement
- Some requirements are not applicable to the directory based environment
  - E.g. A trust anchor manager must be able to authenticate which device produced a report listing the contents of a trust anchor store.
- Problem statement is still very protocol oriented

Common need

- A format for storing and protecting trust anchor information
  - Public Key
  - Name (Issuer name in issued certs=
  - Parameters (policy, constraints etc…)
- The rest is more or less redundant for a directory based (or repository based) solution

What do we need?

- The directory based approach is implemented and works and can be built on existing protocols, standards and infrastructures

- Problem statement should clearly describe the two approaches and identify where a protocol is needed/desired and why

- Start work on the TA information format separately?