New keyPurpose OIDs

draft-brockhaus-lamps-automation-keyusages-00
Hendrik Brockhaus, David Goltzsche

Hendrik Brockhaus

IETF 121 – LAMPS Working Group

New keyPurpose EKUs required in industrial automation use cases

New Draft:

- IEC published a framework to secure industrial automation and control systems throughout their lifecycle. This framework is utilized by many verticals and legislations
- The Europe's Rail Joint Undertaking project is standardizing a safe and secure system architecture alongside with system requirements based on IEC 62443 for Rail Automation
- Want to get four new keyPurpose OIDs registered in the "SMI Security for PKIX Extended Key Purpose" registry
  - id-kp-configSigning
  - id-kp-trustanchorSigning
  - id-kp-updateSigning
  - id-kp-safetyCommunication
- Adding new OIDs to this registry require a specification, preferably an RFC, see RFC 7299 and RFC 5226

Next Steps:

Details on the for requested keyPurpose OIDs

id-kp-configSigning

- May be used for verifying signatures of general-purpose configuration files of various formats (for example XML, YAML or JSON). Configuration files are used to configure hardware or software.

id-kp-trustanchorSigning

- May be used for verifying signatures of trust anchor configuration files of various formats (for example XML, YAML or JSON). Trust anchor configuration files are used to add or remove trust anchors to the trust store of a device.

id-kp-updateSigning

- May be used for verifying signatures of secure software or firmware update packages. Update packages are used to install software (including bootloader, firmware, safety-related applications and others) on systems.

id-kp-safetyCommunication

- May be used to authenticate a communication peer for safety-critical communication based on TLS or other protocols.
- There are various safety protocols and layers in industrial automation like RaSTA or PROFIsafe, they are safe but not secure. The security of such safety protocols is often achieved by transmitting them via standard security protocols like TLS or IPSEC.