Architecture

draft-moran-suit-architecture-03
Terminology

• **Manifest:**
  – The manifest contains meta-data about the firmware image.
  – The manifest is protected against modification and provides information about the author.

• **Firmware Image (or firmware):**
  – The firmware image is a binary that may contain the complete software of a device or a subset of it.
  – ... may consist of multiple images.
  – ... may consist of a differential update
Terminology

• **Author:**
  – The author is the entity that creates the firmware image, signs and/or encrypts it and attaches a manifest to it.

• **Device:**
  – The device is the recipient of the firmware image and the manifest.
  – The goal is to update the firmware of the device.

• **Untrusted Storage:**
  – Firmware images and manifests are stored on untrusted file servers or cloud storage infrastructure.
Terminology

• We had a discussion about the ITU-T terminology. Some terms can be mapped but for others there is no related concept since the ITU-T architecture is broader (e.g., tracker concept).
Requirements

- Agnostic to how firmware images are distributed
- Friendly to broadcast delivery
- Uses state-of-the-art security mechanisms
- Rollback attacks must be prevented.
- High reliability
- Operates with a small bootloader
- Small Parsers
- Minimal impact on existing firmware formats
- Robust permissions

Role of post-quantum secure signature mechanisms?

What should be stated as “state-of-the-art”? Relationship to bootloader.

Terminology and architecture does not really talk about bootloader.
Manifest with attached firmware

```
/------------\               /------------\
/Manifest with \               /Manifest with \
 |attached     |               |attached     |
\firmware image/               \firmware image/
\------------/  +-----------+  \------------/
+--------+                  |           |                 +--------+
|        |<................| Untrusted |<................|        |
| Device |                  | Storage   |                 | Author |
+--------+                  +-----------+                 +--------+
```
Independent retrieval of the firmware image

```
+--------+                  \
|        |<..............................................>|        |
| Device |                                             -- | Author |
|        |<-                                         ---  |        |
+--------+  --                                     ---    +--------+
-------+
    |
+--------+  -- +-----------+    --
|        |  -- |           |  --
| Firmware |       | Untrusted Storage |
|          |       |<-                |
+--------+       +--------+
```

7
Appendix

• Contains:
  – Threat Model
  – User Stories
  – Security Requirements
  – and Usability Requirements

• Made appendix easier to read with forward references.