Changes since v05

• Two major changes
  • Removed delegation chains
    • Moved to cose wg: draft-tschofenig-cose-cwt-chain-00
    • This is a generic approach to delegation of authority
  • Added candidate verification
    • Enables several new use cases
Trust change between Fetch & Install

• Trust domain transitions sometimes required between stages
  • Fetch => client
  • Install => installer app
• Enables e.g. staging areas smaller than active firmware
  • Decompress into active area
  • Highly relevant to flash & energy constrained devices
    • E.g. LoRa requires 10x energy to receive byte as write to flash
• Important for differential updates as well
Candidate Verification

• After a trust domain transition, authenticity verification is required
  • E.g. reboot into installer introduces new vulnerabilities
    • TOCTOU
      • no guarantee that flash has not changed between client check and installer boot
    • Privilege escalation
      • Client can write arbitrary content to staging flash & installer will consume it
  • Mitigation is re-verification
    • Installer verifies at time of use and verifies authority of signer to install
Candidate Verification Sequence

- Compares each component to expected digest
- No fetch/copy/swap permitted—verify only
- Needs to occur before install
- Proposal:
  - Current installation key is 17
  - 19 => Candidate Verification
  - 20 => Installation
  - Ensures that current implementations detect that installation has moved
  - Opens a space for future expansion