Alternative RPKI Repository Retrieval Mechanism

Terry Manderson
IETF72
ARRRM

• Details a mechanism and algorithm for a relying party to synchronize a local cache of RPKI objects against the collection of original publication points.
ARRRM

- Uses HTTP
- Provides for HTTPS
  - Integrity about what a relying party is fetching (and from whom)
- Identifies an efficient algorithm for synchronization and RPKI validation of a local cache from an RPKI Repository Server (RRS)
  - Protocol agnostic
- Relies upon the latest Manifest draft
ARRRM

- It provides
  - An additional fetch URI for the SIA field (remember SIA order is important)
  - An IETF based mechanism
  - An unambiguous algorithm for how relying parties should fetch and process objects from publication points
Thank you!

- And.. Should this be adopted as a WG item?