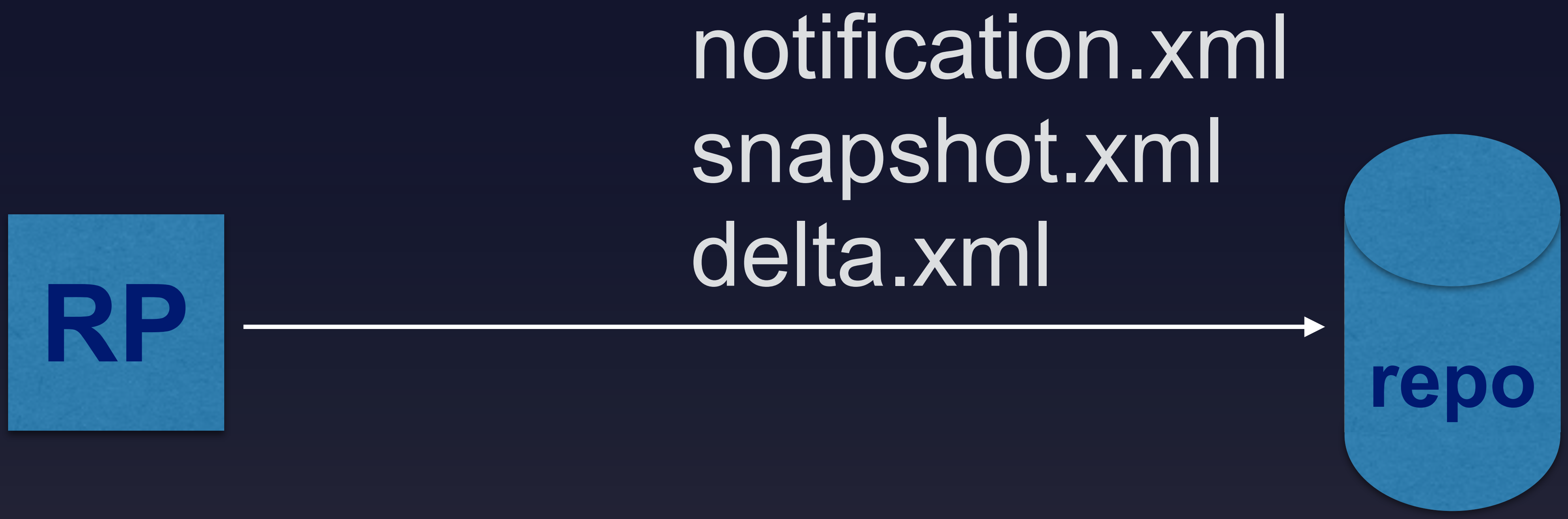
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RRDP-03

HTTPs.. and done?

HTTPS



notification.xml	Attacker can replay or withhold HTTPS check helps detect
snapshot.xml delta.xml	Signed RPKI Objects Can be validated regardless of source. We have semantics to find the latest valid objects in cache.

HTTPS

It is RECOMMENDED that Relying Parties and Publication Servers follow the Best Current Practices outlined in [RFC7525] on the use of HTTP over TLS (https).

Note that a Man-in-the-Middle (MITM) cannot produce validly signed RPKI data, but they can perform withhold or replay attacks targeting an RP, and keep the RP from learning about changes in the RPKI. Because of this RPs SHOULD do TLS certificate and host name validation when they fetch from an RRDP Publication Server

However, such validation issues are often due to configuration errors, or a lack of a common TLS trust anchor. In these cases it would be better that the RP retrieves the signed RPKI data regardless, and performs validation on it.

Therefore RPs SHOULD log any TLS certificate or host name validation issues they find, so that an operator can investigate the cause. But the RP SHOULD continue to retrieve the data. The RP MAY choose to log this issue only when fetching the notification update file, but not when it subsequently fetches snapshot or delta files from the same host.

Furthermore the RP MAY provide a way for operators to accept untrusted connections for a given host, after the cause has been identified.

Last call?

- HTTPS in TAL in this spec

- Two interoperable implementations
- We believe it works