# Uptane: Informal Visualizations

# Data Types

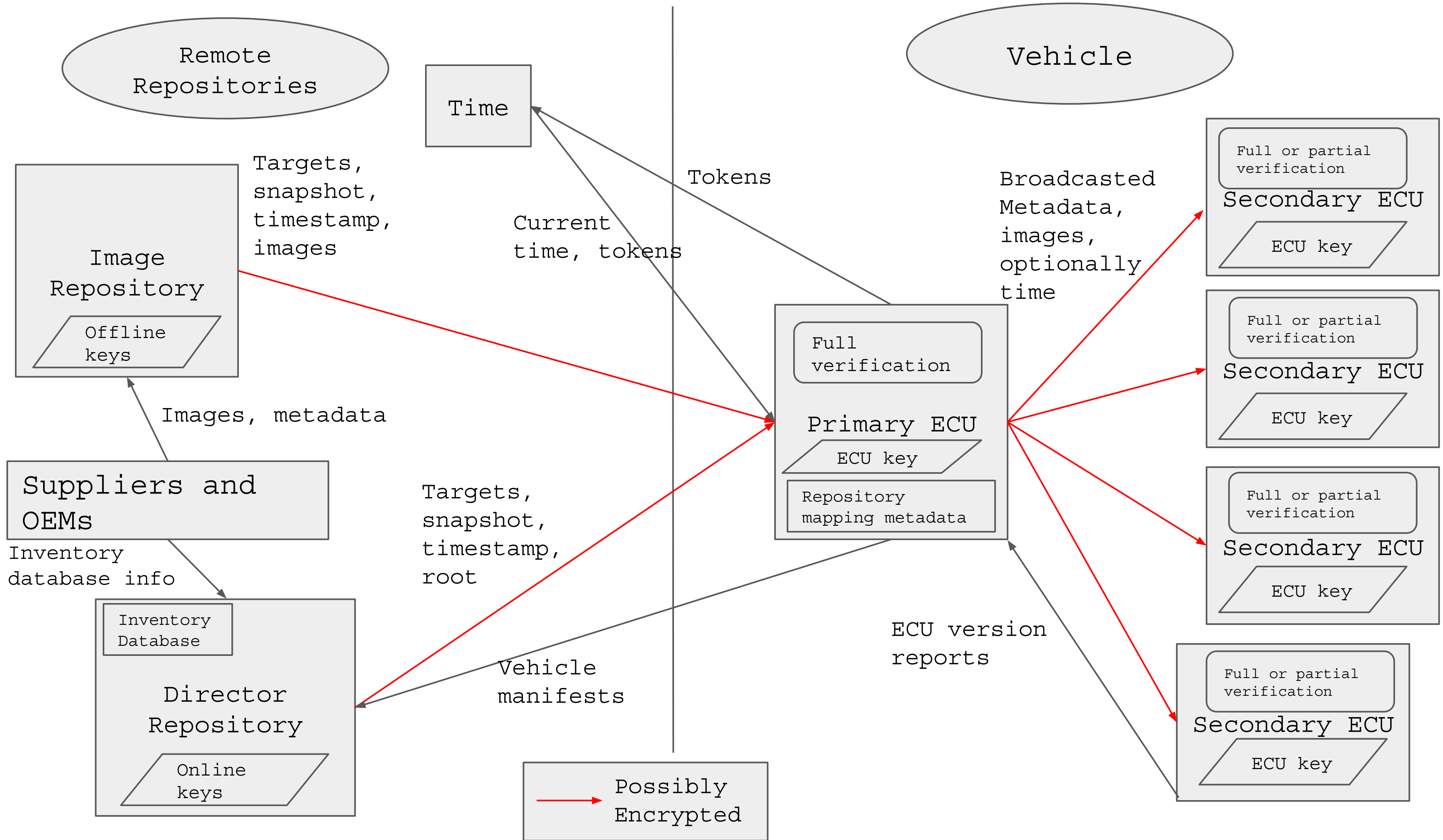
- Common metadata structure
  - Payload (see below)
  - List of signatures and associated public key IDs
- Root metadata
  - List of public keys for 4 metadata types
  - Mapping of roles to public keys and threshold of signatures
- Timestamp metadata
  - Filenames
  - Hashes
  - File sizes
  - Optionally
    - Other image info
    - Delegations metadata
- Targets metadata
  - Filename
  - Size (bytes)
  - Hash(es) of image file
  - Hash function(s)
  - Custom Image metadata (optional)
- Snapshot metadata
  - Filename of targets metadata file
  - Version number of targets metadata file
- Delegations metadata
  - List of public keys
  - List of delegations
    - List of filenames
    - Optional list of hardware IDs
    - Terminating?
    - List of Roles
      - Name
      - Key IDs
      - Threshold number of keys
- Repository mapping metadata
  - List of repo names and URLs
  - List of mappings from image paths to repos (who needs to sign what)
- Custom image metadata (if encrypted)
  - Filename, hash, file size
  - Encryption method
  - ECU ID (Director)

# Data Types Cont.

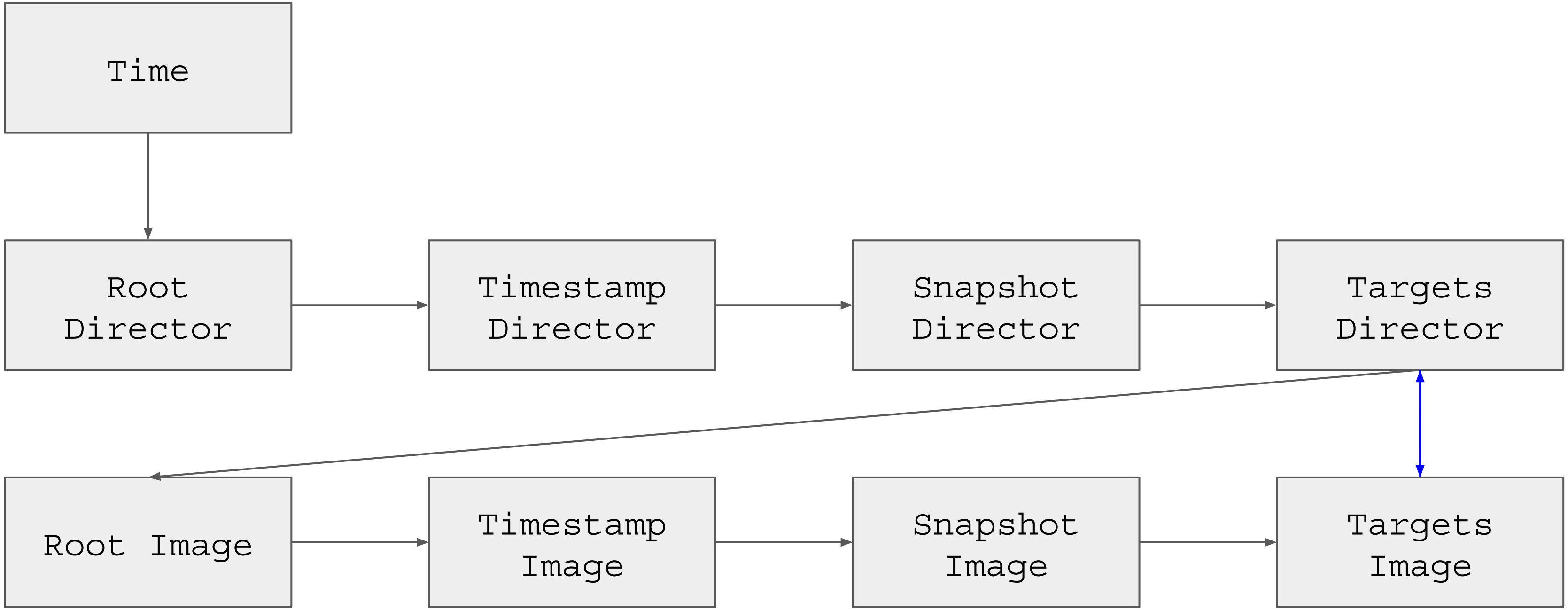
- Inventory database entry
    - Vehicle ID for each vehicle
    - For each ECU:
        - ID
        - Associated vehicle ID
        - ECU key
        - ECU key ID
        - Primary or Secondary?
- Vehicle manifest
    - Signatures (public key ID, signing method, hash of payload, hash function, signature of hash)
    - Payload
        - Vehicle ID
        - Primary ECU ID
        - List of ECU version reports
- ECU version report
    - Signatures (public key ID, signing method, hash of payload, hash function, signature of hash)
    - Payload
        - ECU ID
        - Current image filename
        - Current image hash
        - Current image length
        - Record of any detected security attacks
        - Time of report generation
        - Counter that increments for each update cycle

# Data Types Cont.

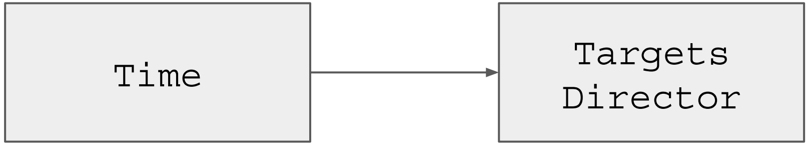
- ECU
    - Metadata
    - ECU key
    - Repository mapping metadata
- Director Repository
    - Inventory Database
    - Metadata
- Image Repository
    - Images
    - Metadata


Remote Repositories
Time
Vehicle
Targets, snapshot, timestamp, images
Tokens
Current time, tokens
Broadcasted Metadata, images, optionally time
Full or partial verification
Secondary ECU
ECU key
Image Repository
Offline keys
Full verification
Primary ECU
ECU key
Repository mapping metadata
Full or partial verification
Secondary ECU
ECU key
Images, metadata
Suppliers and OEMs
Inventory database info
Targets, snapshot, timestamp, root
Full or partial verification
Secondary ECU
ECU key
Inventory Database
Director Repository
Online keys
Vehicle manifests
ECU version reports
Full or partial verification
Secondary ECU
ECU key
Possibly Encrypted

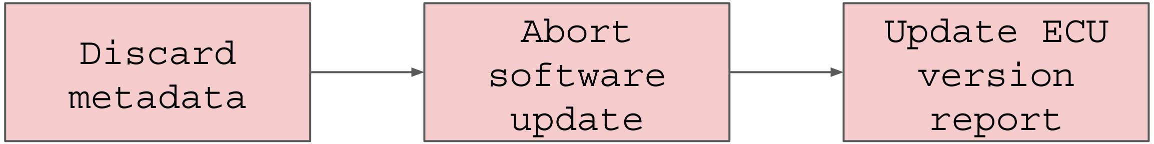
# Full Verification



# Partial Verification



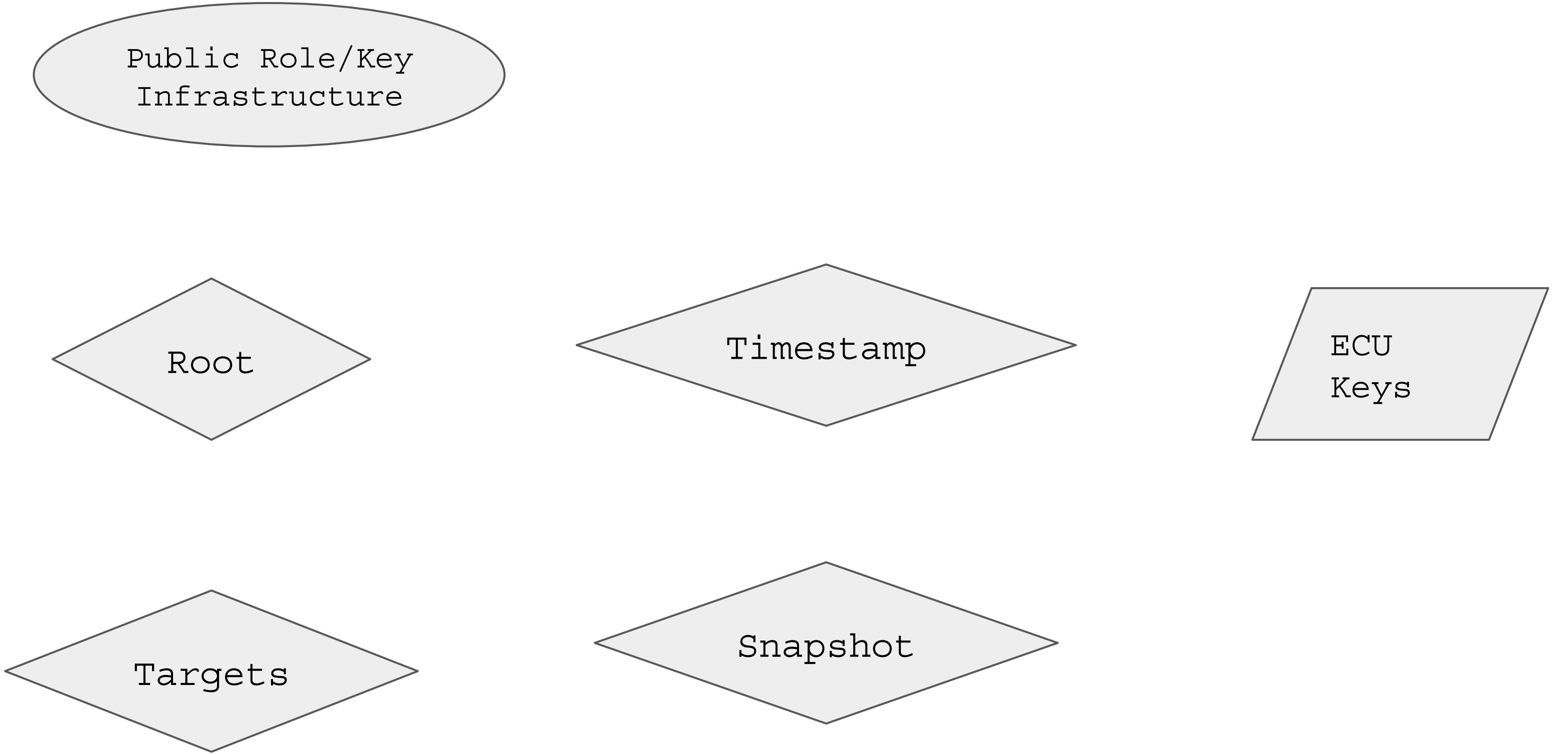
# Verification Failure



Discard metadata

Abort software update

Update ECU version report



Public Role/Key Infrastructure

Root

Timestamp

ECU Keys

Targets

Snapshot

# Questions/Notes

1. How do we model Uptane’s optional features (MAY, SHOULD, RECOMMENDED, OPTIONAL)?
2. How do we model Uptane’s features that have multiple possible implementations-- e.g., asymmetric or symmetric encryption
3. What types of metadata are associated with each arrow in the first diagram?
4. Digitally signed vs encrypted-- which messages are which, or both
5. Do both repositories have images? Who sends images to primary ECU?
6. Why do ECUs need metadata at original construction to verify Director and Image repos?
7. Does the director store vehicle version manifests?
8. Why do primary and secondary ECUs both do verification?
    a. ECUs and their connections can be compromised
9. What triggers messages to be sent?
10. When is root metadata set?
11. How do we determine encrypted, integrity-protected, replay-protected, etc.?

# Questions/Notes

- What do secondary ECUs send to primary ECUs
- Which messages are encrypted, integrity protected, etc.
- Image vs metadata verification
- Wildcard path?
- Does the primary decrypt images before sending to secondaries?
- Primary sends metadata and images to secondaries-- same message? Different messages?