Delay Tolerant Network (DTN) Security Key Management Design Alternatives

DTN Interim Working Group Meeting

January 18, 2016

Fred L. Templin (fred.l.templin@boeing.com)

Kapali Viswanathan (kapaleeswaran.viswanathan@boeing.com)

https://datatracker.ietf.org/doc/draft-viswanathan-dtnwg-pkdn

https://datatracker.ietf.org/doc/draft-templin-dtnskmreq

Problem: How to make public keys / revocations available in a timely manner in DTNs?

1. Request-response
   - Receiver requests revocation information
   - Trusted authority responds with requested information
2. Publish-subscribe
   - Receiver requests revocation information once
   - Trusted authority sends periodic updates for requested information
3. Blacklist broadcast
   - Trusted authority periodically broadcasts revocation information
4. Whitelist broadcast
   - Trusted authority periodically broadcasts valid public-key information
5. Publish with proxy subscribe (PKDN)
   - Sender routes certificate through trusted authority to receiver
   - Trusted authority verifies validity of certificate and sends periodic updates

PKDN Characterization

Public Key Distribution Network (PKDN) uses publish with proxy subscribe

PKDN is an overlay on top of DTN

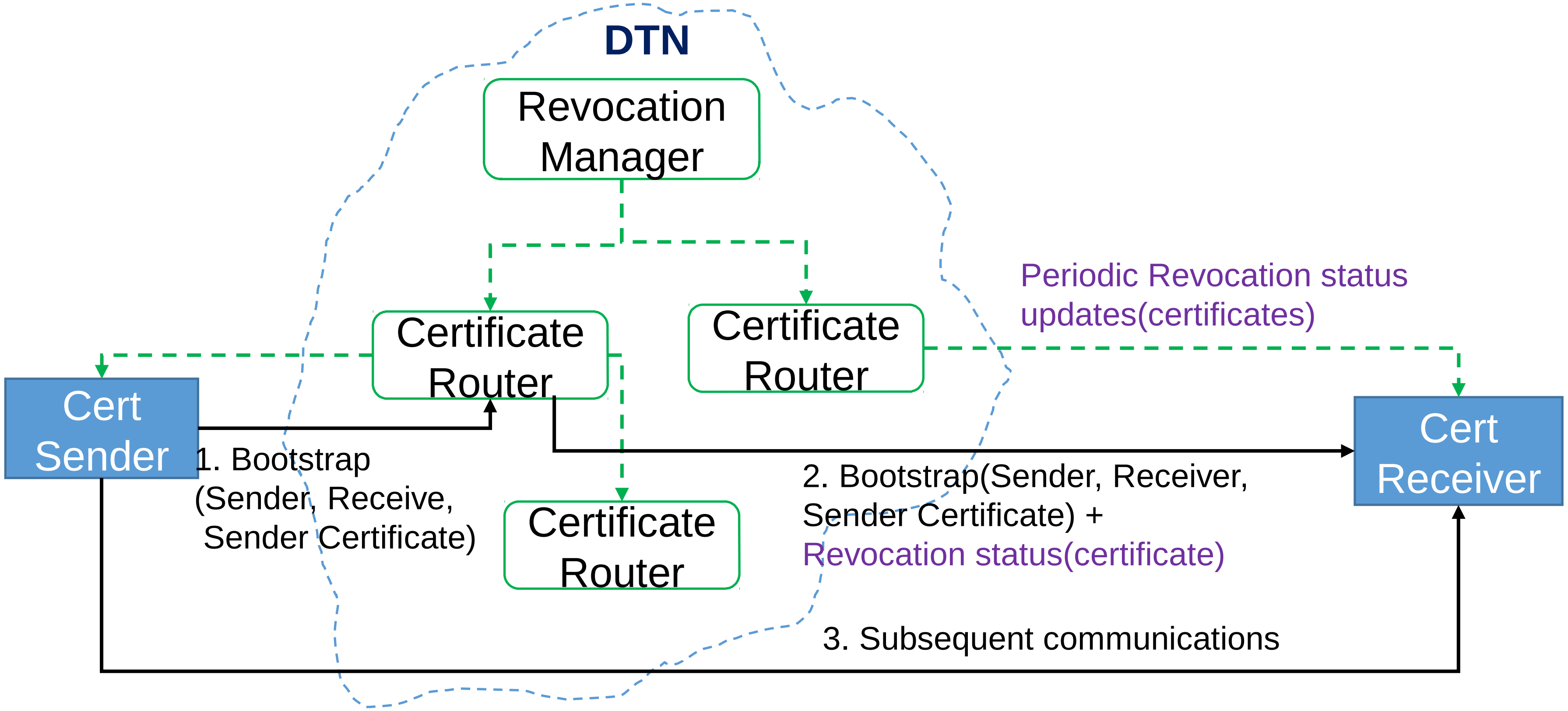
- It does not use any other communication channel other than DTN

PKDN has four architectural entities

- **PKDN Sender** for sending a node’s certificate to a PKDN receiver
- **PKDN Router** for validating certificates from PKDN Senders
  - A network of PKDN Routers results in a distribution network
  - Redundancy in distribution network ensures that all nodes in the network will eventually receive revocation information
  - Router discovery through manual configuration or dynamic discovery
- **PKDN Receiver** for receiving validated certificates and revocation information from PKDN Routers
- **Certificate Revocation Manager (CRM)** for injecting authenticated revocation information into the distribution network formed for PKDN Routers

Technical update: PKDN Solution

- Publish-Subscribe network for delta CRL distribution
  - Revocation Manager is the root of trust
    - Creates and sends authentic delta CRLs
  - Routers subscribe either to Revocation Manager or to other routers
  - End-users subscribe to their respective
- Forwarding as a mechanism for trust establishment


DTN
Revocation Manager
Certificate Router
Certificate Router
Certificate Router
Cert Sender
Cert Receiver
Periodic Revocation status updates(certificates)
1. Bootstrap (Sender, Receive, Sender Certificate)
2. Bootstrap(Sender, Receiver, Sender Certificate) + Revocation status(certificate)
3. Subsequent communications

PKDN Router Functions

Routing

- Receive and validate certificates from PKDN Senders
- Forward valid certificates to PKDN Receivers

Cache synchronization

- Receive certificate revocation updates from CRM to maintain a consistent local Certificate Revocation List
- Forward certificate revocation updates to other PKDN Routers

Revocation update dissemination

- Send periodic certificate revocation updates to PKDN Receivers

PKDN vis-à-vis DTN Key Management Requirements

REQ1: Must Provide Keys When Needed

- Receivers receive validated sender certificates encapsulated with initial message bundles
- Senders can access validated certificates of receivers either from PKDN Routers or from receivers or through manual configuration

REQ2: Must Be Trustworthy

- Certificates are signed by trusted authorities
- Certificate revocation are signed by trusted authorities

REQ3: No Single Point of Failure

- Path redundancy in distribution network formed by PKDN Routers avoid single points of failures

REQ4: Multiple Points of Authority

- Multiple certificate and certificate revocation authorities can be allowed for a single PKDN instance

REQ5: No Veto

- PKDN Routers, Senders, and Receivers can validate certificates and certificate revocation issued by multiple authorities

PKDN vis-à-vis DTN Key Management Requirements

REQ6: Must Bind Public Key with DTN Node Identity

- Realized using standard public key certificate structures (certificate includes name plus public key)

REQ7: Must Support Secure Bootstrapping

- Realized using standard public key certificate structures (all DTN nodes must have root public key installed)

REQ8: Must Support Revocation

- PKDN Routers and CRM achieve this property

REQ9: Revocations Must Be Delay Tolerant

- Achieved by designing PKDN as a strict overlay on top of DTN, and by using **event-driven semantics**

Candidate Multicast Key Management Design (draft-templin-dtnskmreq)

- **Delay-Tolerant Key Administration (DTKA)**
- Distributed Key Authorities (KAs)
- Every KA multicasts authenticated key management bulletins
- A minimum number of KA bulletins are needed to recreate authorized key updates for that point in time
- Design Constraints
  - All nodes in the DTN need to receive bulletins in timely manner
  - Bulletins contain current and future node-key association for all DTN nodes
  - All DTN nodes maintain a local data-base of valid keys at that point in time

http://ipnsig.org/wp-content/uploads/2015/05/IPNSIG-DTN-Security-Key-Management.pdf

PKDN vis-à-vis Multicast Key Management

DTKA

- Whitelist broadcast (bulletin w/ future public keys)
- Time-based synchronization (sender must send cryptographic bundles only after receiver receives key bulletins with sender’s key)
- Mechanism identical for sender to have receiver’s key and for receiver to have sender’s key.
- Key revocation is implicit (revoked keys are not included in the future bulletins)
- Requires time-bound consistency of node-key association on all DTN nodes.

PKDN

- publish-with-proxy-subscribe unicast
- **Event-based synchronization** (sender encapsulates its public-key certificate in the cryptographic bundle for the receiver)
- Provides mechanism for receiver to have sender’s key. Can support multiple additional mechanisms for sender to have receiver’s key.
- Key revocation is explicit (key certification and revocation are issued separately potentially by separate authorities.)
- Requires *eventual* consistency of Certificate Revocation List (CRL) on all PKDN Routers. Requires delta-CRL to *eventually* reach all DTN nodes.