Public Key Distribution Network (PKDN) for DTN Security Key Management

IETF95 DTN Working Group Meeting


April 4, 2016

Kapali Viswanathan (kapaleeswaran.viswanathan@boeing.com)
Fred L. Templin (fred.l.templin@boeing.com)
Overview

• PKDN Overview
• PKDN Entities and Functions
• PKDN & DTN Key Management Requirements
• Changes Since Last Version
PKDN Overview

- Certificate revocation manager certifies one or more validators.
- Sender chooses a validator either by configuration or by discovery. Current PoC implements choice by configuration.

CRL = Certificate Revocation List
Delta-CRL = Additions to CRL
PKDN Layering

Sender
Bundle Protocol

Receiver
Bundle Protocol

Validator
Bundle Protocol

Certificate Revocation Manager
Bundle Protocol

Certificate Revocation Manager
Bundle Protocol

Validator
Bundle Protocol

Delay Tolerant Network Cloud (Interconnected Bundle Protocol Routers)
PKDN Event Propagation

Role of PKDN:
• Association performed by arbitrary external software (e.g. X.509 PKI software)
• PKDN references key uniquely as: (key-fingerprint, expiry-timestamp)

Role of PKDN:
• Provides an in-band mechanism to exchange validated certificates

Role of PKDN:
• Propagates public key revocation events to a network of validators using multicast communication
• Notifies public-key revocation events to interested endpoints
Overview

• PKDN Overview

• PKDN Entities and Functions
• PKDN & DTN Key Management Requirements
• Changes Since Last Version
Revocation event subscription

Delay Tolerant Networking

Sender

Certificate revocation Manager

Validator

Subscribe

Publish (Delta-CRL)

Receiver

Public key certificate

Validated public key certificate

Revocation status

Validated public key certificate

Public key certificate

Revocation status

CRL = Certificate Revocation List
Delta-CRL = Additions to CRL
Delay Tolerant Networking

Revocation event & status propagation

CRL = Certificate Revocation List
Delta-CRL = Additions to CRL
Session management and secure communication

- Delay Tolerant Networking
- Certificate revocation Manager
  - Subscribe
  - Publish (Delta-CRL)
- Validator
  - Public key certificate
  - Validated public key certificate
  - Revocation status
- Sender
  - Validated public key certificate
  - Revocation status
- Receiver
  - Validated public key certificate
  - Revocation status

CRL = Certificate Revocation List
Delta-CRL = Additions to CRL
Overview

• PKDN Overview
• PKDN Entities and Functions
☐ • PKDN & DTN Key Management Requirements
  • Changes Since Last Version
PKDN & DTN Key Management Requirements

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

REQ1: Must Provide Keys When Needed
• Receivers receive validated sender certificates encapsulated with initial message bundles

REQ2: Must Be Trustworthy
• Certificates are signed by trusted authorities
• Certificate revocations are signed by trusted authorities

REQ3: No Single Point of Failure
• Multiple CRMs are allowed
• Path redundancy from CRMs to Validators strengthen REQ3

REQ4: Multiple Points of Authority
• Multiple certificate and certificate revocation authorities can co-exist

REQ5: No Veto
• Validators, Senders, and Receivers can be configured to validate certificates and certificate revocations issued by multiple authorities
PKDN & DTN Key Management Requirements

REQ6: Must Bind Public Key with DTN Node Identity
• Realized using standard public key certificate structures (certificates minimally include address, public key, and expiry date)

REQ7: Must Support Secure Bootstrapping
• All PKDN entities must have root public key and root revocation public key manually installed

REQ8: Must Support Revocation
• Validators 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
Overview

• PKDN Overview
• PKDN Entities and Functions
• PKDN & DTN Key Management Requirements
• Changes Since Last Version
Changes Since Last Version

• Draft title changed from ‘draft-viswanathan-dtnwg-pkdn-00’ to align document to DTN Working Group

• Now using unicast Certificate Revocations for interested parties instead of DTN-wide CRL multicast

• PKDN Validators remember the certificates of interest to individual receivers for a limited time period

• Senders must send fresh certificates through a PKDN validator before validator interest memory expiration