Architecture for Delay-Tolerant Key Administration

IETF 101 DTN Working Group
March 23, 2018

Scott Burleigh (Scott.Burleigh@jpl.nasa.gov)

David Horres (David.C.Horres@jpl.nasa.gov)

Kapali Viswanathan (kapaleeswaran.viswanathan@boeing.com)

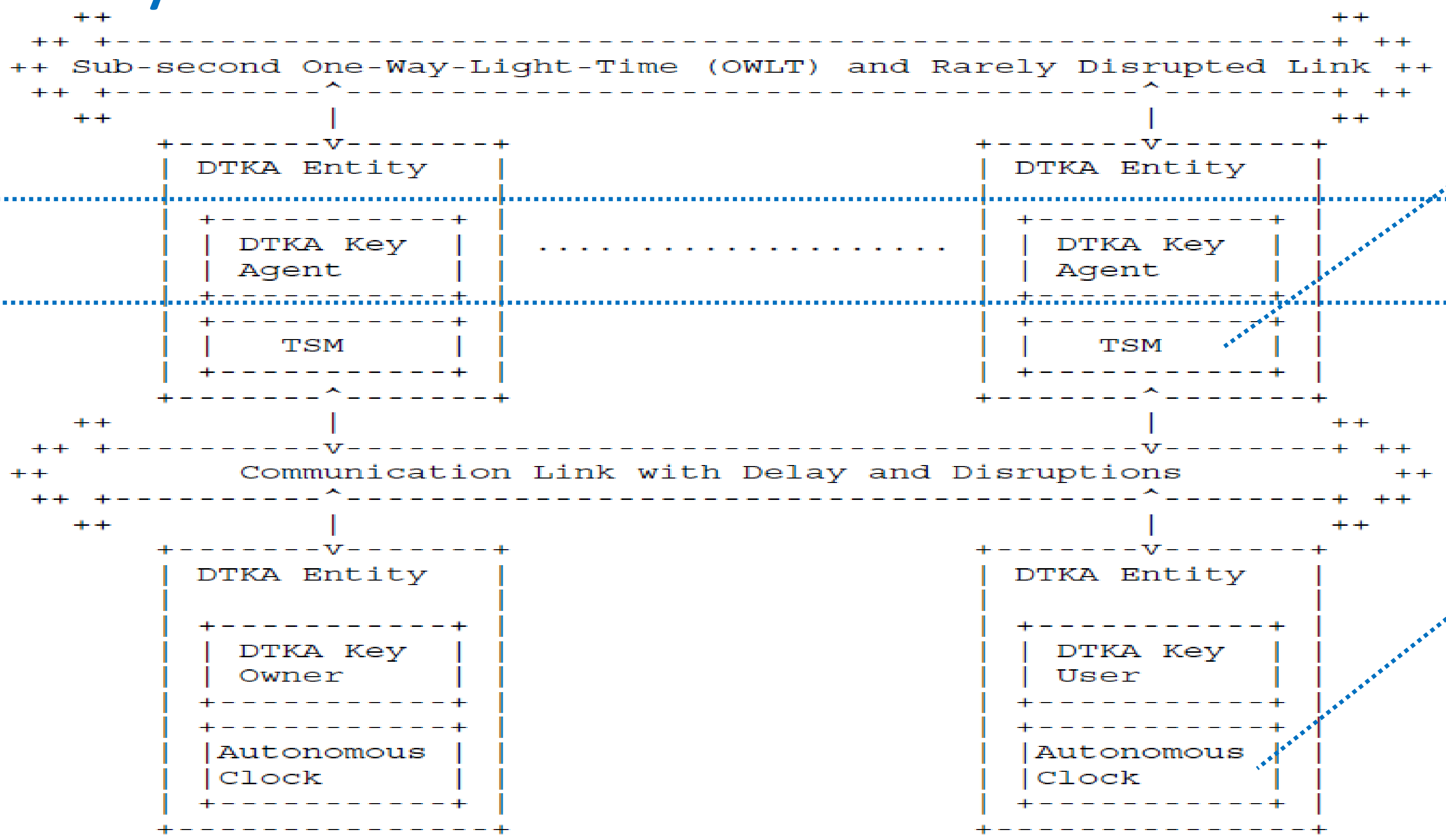
Michael W. Benson (michael.w.benson@boeing.com)

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

Recap: Motivation

- On-demand & interactive communication cannot be assumed in DTN
- SSL and Online Certificate Status Protocol (OCSP) require on-demand & interactive communication
- A DTN-friendly public-key distribution and revocation protocol suite is needed

Recap: System Architecture



```
   ++                                                           ++
 ++ +-----------------------------------------------------------+ ++
++ Sub-second One-Way-Light-Time (OWLT) and Rarely Disrupted Link ++
 ++ +-----------^--------------------------------------^--------+ ++
   ++           |                                      |        ++
        +-------v-------+                      +-------v-------+
        | DTKA Entity   |                      | DTKA Entity   |
        |               |                      |               |
        | +-----------+ |                      | +-----------+ |
        | | DTKA Key  | | . . . . . . . . . .  | | DTKA Key  | |
        | | Agent     | |                      | | Agent     | |
        | +-----------+ |                      | +-----------+ |
        | +-----------+ |                      | +-----------+ |
        | |   TSM     | |                      | |   TSM     | |
        | +-----------+ |                      | +-----------+ |
        +-------^-------+                      +-------^-------+
   ++           |                                      |        ++
 ++ +-----------v--------------------------------------v--------+ ++
++         Communication Link with Delay and Disruptions           ++
 ++ +-----------^--------------------------------------^--------+ ++
   ++           |                                      |        ++
        +-------v-------+                      +-------v-------+
        | DTKA Entity   |                      | DTKA Entity   |
        |               |                      |               |
        | +-----------+ |                      | +-----------+ |
        | | DTKA Key  | |                      | | DTKA Key  | |
        | | Owner     | |                      | | User      | |
        | +-----------+ |                      | +-----------+ |
        | +-----------+ |                      | +-----------+ |
        | |Autonomous | |                      | |Autonomous | |
        | |Clock      | |                      | |Clock      | |
        | +-----------+ |                      | +-----------+ |
        +---------------+                      +---------------+
```

Figure 2: DTKA System Interconnections

Key Authority for the Application Domain

A "Time Synchronization Mechanism" like the Network Time Protocol (NTP)

Allowed drift in the order of seconds.

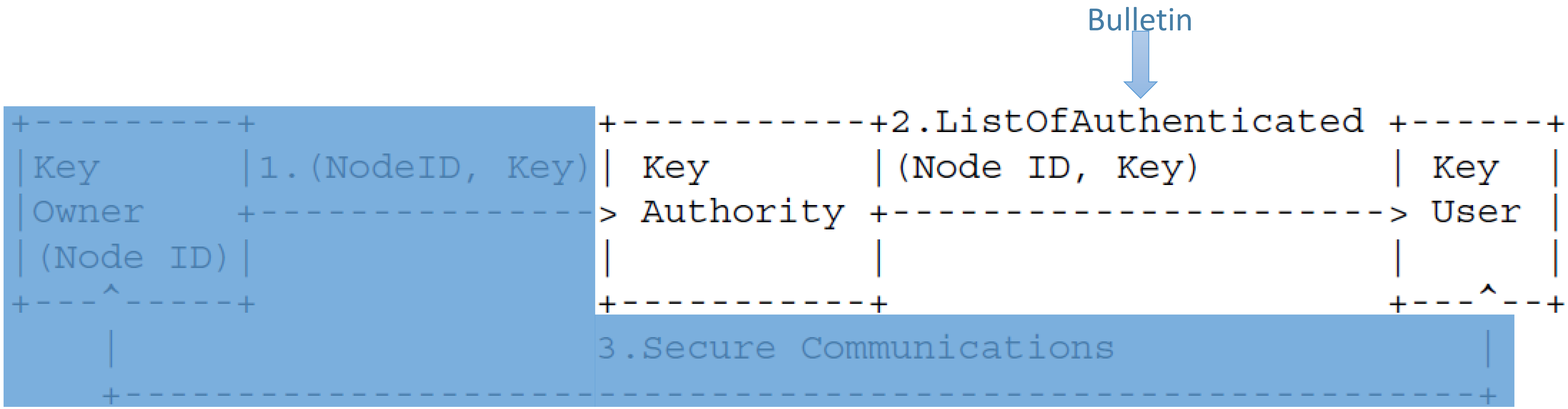
UTC offsets may be present

System Security Configuration:

- Public key of each DTKA Key Agent is securely configured into every Agent, Owner and User in the application domain
- Trust Model Number configuration (New in this version)

https://tools.ietf.org/html/draft-burleigh-dtnwg-dtka-01

Recap: Bulletin authentication



Bulletin

```
+----------+                +------------+2.ListOfAuthenticated +-------+
|Key       |1.(NodeID, Key)| Key        |(Node ID, Key)          | Key   |
|Owner     +----------------> Authority  +-----------------------> User  |
|(Node ID) |                |            |                        |       |
+---^------+                +------------+                        +---^---+
    |                       3.Secure Communications                   |
    +-----------------------------------------------------------------+
```

Figure 1: Abstract Data-Flow-Diagram for DTKA

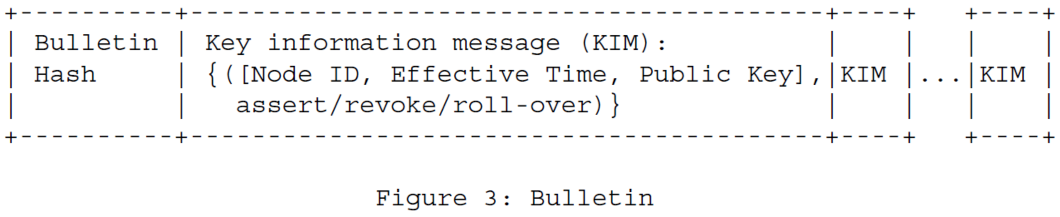
https://tools.ietf.org/html/draft-burleigh-dtnwg-dtka-01

Feedbacks from IETF 100 presentation

- Feedback 1
  - What if bulletins were missed by key users? How will they know? How can they initiate actions to synchronize?
- Feedback 2
  - Can there be different trust models for accepting keys and revoking keys?
- Feedback 3
  - Should consensus mechanism for Key Agents be part of the draft?

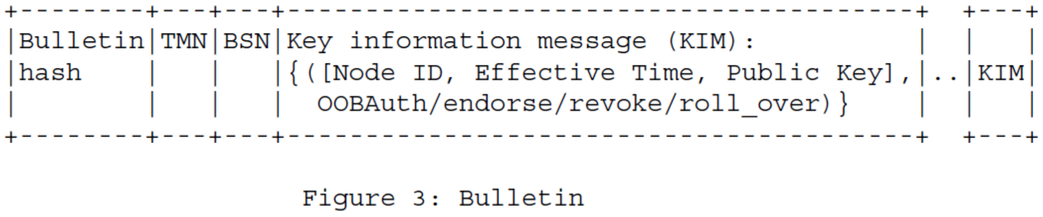
Feedback 1: Loss of bulletins

Version 00



```
+----------+----------------------------------------+----+   +----+
| Bulletin | Key information message (KIM):          |    |   |    |
| Hash     | {([Node ID, Effective Time, Public Key],|KIM |...|KIM |
|          |   assert/revoke/roll-over)}             |    |   |    |
+----------+----------------------------------------+----+   +----+

                       Figure 3: Bulletin
```

Version 01



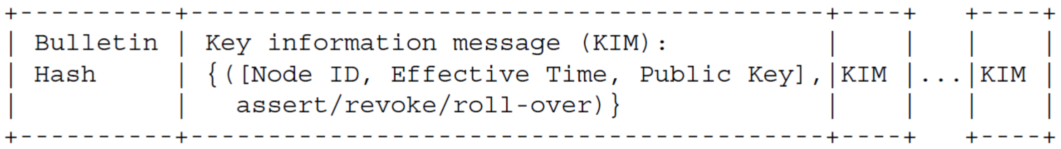
```
+--------+---+---+---------------------------------------+   +---+
|Bulletin|TMN|BSN|Key information message (KIM):         |   |   |
|hash    |   |   |{([Node ID, Effective Time, Public Key],|..|KIM|
|        |   |   |  OOBAuth/endorse/revoke/roll_over)}    |   |   |
+--------+---+---+---------------------------------------+   +---+

                       Figure 3: Bulletin
```

- Introduced a new field in the bulletin called BSN
  - BSN = Bundle Serial Number
- It is a monotonously increasing number
- Receivers store a finite history of successfully received BSNs
  - History will help receivers identify non-receipt of bulletins
- Mechanisms described to request Key Agents for bulletins that were not received

https://tools.ietf.org/html/draft-burleigh-dtnwg-dtka-01

Feedback 2: Allowing multiple trust models

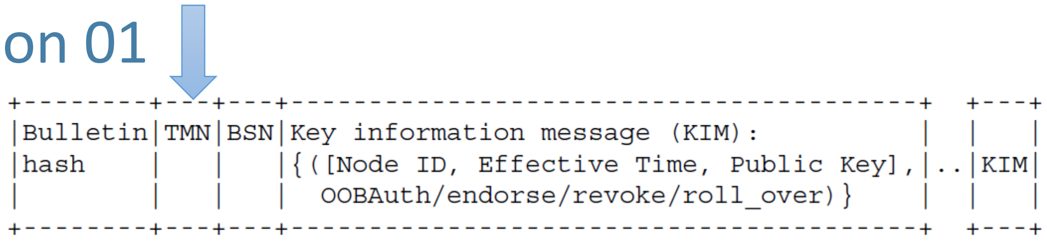
Version 00



```
+----------+--------------------------------------+----+   +----+
| Bulletin | Key information message (KIM):       |    |   |    |
| Hash     | {([Node ID, Effective Time, Public Key],|KIM |...|KIM |
|          |   assert/revoke/roll-over)}           |    |   |    |
+----------+--------------------------------------+----+   +----+
```

Figure 3: Bulletin

Version 01



```
+--------+---+---+---------------------------------------+  +---+
|Bulletin|TMN|BSN|Key information message (KIM):        |  |   |
|hash    |   |   |{([Node ID, Effective Time, Public Key],|..|KIM|
|        |   |   | OOBAuth/endorse/revoke/roll_over)}    |  |   |
+--------+---+---+---------------------------------------+  +---+
```

Figure 3: Bulletin

- Introduced a new field in the bulletin called TMN
  - TMN = Trust Model Number
- Defined by the DTKA Key Agents (Key Authority)
  - Defines allowed trust configurations for bulletins in the Key Authority’s domain
    - Example: t-out-of-n for registration and 2-out-of-n for revocation
- Definitions loaded securely into every DTKA Entity during bootstrapping
- Bulletin hash has TMN an input

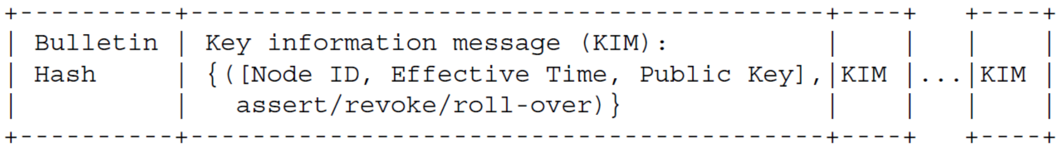
https://tools.ietf.org/html/draft-burleigh-dtnwg-dtka-01

Feedback 3: DTKA-KA consensus mechanism

- Should consensus mechanism for Key Agents be part of the draft?
  - DTKA Key Agents need to agree on the bit-map of the bulletin that they shall authenticate to all DTKA Entities
  - The consensus mechanism for this agreement is a matter of implementation
  - Left out of this Internet Draft

Proactive update

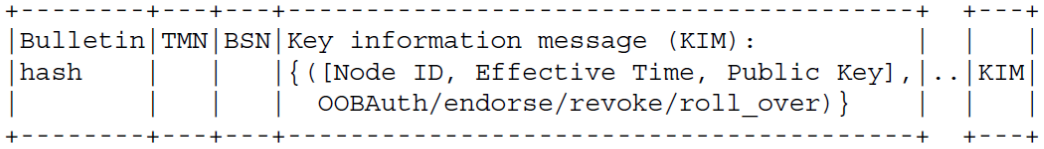
Version 00



```
+----------+-----------------------------------------+-----+   +-----+
| Bulletin | Key information message (KIM):          |     |   |     |
| Hash     | {([Node ID, Effective Time, Public Key],|KIM  |...|KIM  |
|          |   assert/revoke/roll-over)}             |     |   |     |
+----------+-----------------------------------------+-----+   +-----+
```

Figure 3: Bulletin

Version 01



```
+--------+---+---+----------------------------------------+  +---+
|Bulletin|TMN|BSN|Key information message (KIM):          |  |   |
|hash    |   |   |{([Node ID, Effective Time, Public Key],|..|KIM|
|        |   |   |  OOBAuth/endorse/revoke/roll_over)}    |  |   |
+--------+---+---+----------------------------------------+  +---+
```

Figure 3: Bulletin

- Key Information Message Types
  - No change
    - revoke, roll over
  - Name change
    - assert → OOBAuth (Out-of-band authentication)
  - New type
    - endorse
      - Key owner performs OOBAuth with an authenticated Trusted Third Party (TTP)
      - On behalf of Key Owner, TTP authenticates Key Owner’s key to DTKA Key Agents

Thank you!