Abstract

This short document outlines requirements for DTN key management. It may or may not grow to specify some DTN key management schemes.

Table of Contents

1. Introduction ............................................. 3
2. Key Management Requirements ............................. 4
3. Security Considerations ................................. 5
4. IANA Considerations .................................... 6
5. References ................................................ 7
   5.1. Normative References ................................. 7
   5.2. Informative References ............................... 7
Author’s Address ............................................. 8
Intellectual Property and Copyright Statements .............. 9
1. Introduction

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [1].

This document lists a set of putative requirements for key management for DTN protocols, in particular the bundle protocol [2] with the aim of assisting in the development of workable key management schemes for the bundle security protocol [3].


Depending on what happens, this document might grow to include the specification of some key management schemes.
2. Key Management Requirements

1. No single KM scheme will work for all DTNs therefore a set of schemes, or a framework, is REQUIRED.

2. All schemes MUST support some well-defined BSP ciphersuite(s).

3. At least one scheme SHOULD be defined for each of:
   1. Manual keying, i.e. pre-shared secrets or pre-installed public keys;
   2. Key transport & key agreement options.

4. Schemes SHOULD be able to use extension blocks to piggy-back KM information with application-data handling bundles.

5. Schemes MAY involve use of specific bundle payloads.

6. Some schemes MUST be defined using standard, well-known techniques (e.g. RSA key transport).

7. DTN node connectivity, computation and storage capabilities vary enormously, so some scheme for highly challenged nodes SHOULD be defined.
3. Security Considerations

This memo is entirely about security requirements. See above.
4. IANA Considerations

For now, there are none. If specific DTN key management schemes are defined that meet these requirements, then an IANA registry, or entries in an IANA registry, MAY be required.
5. References

5.1. Normative References


5.2. Informative References


Author’s Address

Stephen Farrell
Trinity College Dublin
Distributed Systems Group
Department of Computer Science
Trinity College
Dublin 2
Ireland

Phone: +353-1-608-1539
Email: stephen.farrell@cs.tcd.ie