

DTN Research Group	S. Farrell	
Internet-Draft	Trinity College Dublin	
Intended status: Informational	June 19, 2007	
Expires: December 21, 2007		

[TOC](#)

DTN Key Management Requirements

draft-farrell-dtnrg-km-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on December 21, 2007.

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
- [2.](#) Key Management Requirements
- [3.](#) Security Considerations
- [4.](#) IANA Considerations
- [5.](#) References
 - [5.1.](#) Normative References
 - [5.2.](#) Informative References
- [§](#) Author's Address

1. Introduction

[TOC](#)

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 [\[refs.RFC2119\]](#) (Bradner, S. and J. Reynolds, "Key words for use in RFCs to Indicate Requirement Levels," October 1997.).

This document lists a set of putative requirements for key management for DTN protocols, in particular the bundle protocol [\[refs.DTNBP\]](#) (Scott, K. and S. Burleigh, "Bundle Protocol Specification," April 2007.) with the aim of assisting in the development of workable key management schemes for the bundle security protocol [\[refs.DTNBPsec\]](#) (Symington, S. and S. Farrell, "Bundle Security Protocol Specification," .).

Readers should also consult the DTN Architecture RFC [\[RFC4838\]](#) (Cerf, V., Burleigh, S., Hooke, A., Torgerson, L., Durst, R., Scott, K., Fall, K., and H. Weiss, "Delay-Tolerant Networking Architecture," April 2007.) and the DTN Security Overview and Motivations document [\[refs.DTNsecOver\]](#) (Farrell, S., Symington, S., and H. Weiss, "Delay-Tolerant Network Security Overview," October 2006.) which contains an overview of the current work on DTN security.

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

2. Key Management Requirements

[TOC](#)

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

4. Schemes MAY involve use of specific bundle payloads.
5. Some schemes MUST be defined using standard, well-known techniques (e.g. RSA key transport).
6. DTN node connectivity, computation and storage capabilities vary enormously, so some scheme for highly challenged nodes SHOULD be defined.

3. Security Considerations

[TOC](#)

This memo is entirely about security requirements. See above.

4. IANA Considerations

[TOC](#)

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

[TOC](#)

5.1. Normative References

[TOC](#)

[refs.RFC2119]	Bradner, S. and J. Reynolds , " Key words for use in RFCs to Indicate Requirement Levels ," RFC 2119, October 1997.
----------------	---

5.2. Informative References

[TOC](#)

[RFC4838]	Cerf, V., Burleigh, S., Hooke, A., Torgerson, L., Durst, R., Scott, K., Fall, K., and H. Weiss, "Delay-Tolerant Networking Architecture," RFC 4838 , April 2007.
[refs.DTNBP]	Scott, K. and S. Burleigh, "Bundle Protocol Specification," draft-irtf-dtnrg-bundle-spec-09.txt , April 2007.

[refs.DTNBPsec]	Symington, S. and S. Farrell , "Bundle Security Protocol Specification."
[refs.DTNsecOver]	Farrell, S., Symington, S. , and H. Weiss, "Delay-Tolerant Network Security Overview," draft-irtf-dtnrg-sec-overview-02.txt , October 2006.

Author's Address

[TOC](#)

	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

Full Copyright Statement

[TOC](#)

Copyright © The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of

such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.