

Preconfigured Binding Management Keys for Mobile IPv6
<[draft-ietf-mip6-precfgKbm-00.txt](#)>

Status of This Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#).

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>.

Abstract

A mobile node and a correspondent node may preconfigure a Binding Management Key for authorizing Binding Updates.

Perkins

Expires 5 October 2004

[Page i]

1. Preconfiguring a Binding Management Key (Kbm)

A mobile node and a correspondent node may preconfigure a Binding Management Key (Kbm) for authorizing binding management messages, especially Binding Update and Binding Acknowledgement messages. The key **MUST** be the same length as that configured using inputs from Mobile IPv6 [1] return routability. The key is associated to the mobile node's home address.

Replay protection for Binding Update messages using the preconfigured Kbm depends upon the value of the sequence number field in the Binding Update. If the correspondent node does not maintain information about the recently used values of that field, then there may be an opportunity for a malicious node to replay old Binding Update messages and fool the correspondent node into routing towards an old care-of address. For this reason, a correspondent node that uses a preconfigured Kbm also **MUST** keep track of the most recent value of the Sequence Number field of Binding Update messages using the preconfigured Kbm value.

When a Binding Update is to be authenticated using such a preconfigured binding key (Kbm), the Binding Authorization Data suboption **MUST** be present. The Nonce Indices option **SHOULD NOT** be present. If it is present, the nonce indices supplied **MAY** be ignored and are not included as part of the calculation for the authentication data, which is to be carried exactly as specified in [1].

2. Applicability Statement

Preconfigured keys between a mobile node and a correspondent node are useful in several specific scenarios:

- mobile node and correspondent node are administered within the same domain, and the correspondent node has good reason to trust the actions of the mobile node
- the correspondent node has some guarantee that the mobile node will behave properly (perhaps by contractual agreement)

- the method of assignment for keys between the correspondent node and mobile node results in a stronger security association than what can be provided by the Return Routability procedure.
- diagnostic procedures
- software development and testing

Generally speaking, the required level of trust that the correspondent node needs for enabling a preconfigured Kbm with a

mobile node is more often found within relatively small, closed groups of users who are personally familiar with each other, or who have some external basis for establishing trustworthy interactions.

3. Security Considerations

A correspondent node and a mobile node MAY use a preconfigured binding management key (Kbm) to manage the authentication requirements for binding cache management messages. Such keys must be handled carefully to avoid inadvertent exposure to the threats outlined in [2].

A mobile node MUST use a different binding management key (Kbm) for each node in its Binding Update List. This ensures that the sender of a Binding Update can always be uniquely determined. This is necessary, as this authorization method does not provide any guarantee that the given care-of address is legitimate. For the same reason, this method SHOULD only be applied between nodes that are under the same administration. The return routability procedure is RECOMMENDED for all general use and MUST be the default, unless the user explicitly overrides this by entering a key for a particular peer.

Replay protection for the Binding Authorization Data option authentication mechanism is provided by the Sequence Number field of the Binding Update. This method of providing replay protection fails when the Binding Update sequence numbers cycle through the 16 bit counter (i.e., not more than 65,536 distinct uses of Kbm), or if the sequence numbers are not protected against reboots. If the mobile node were to move every hour, 24 hours a day, every day of the year, this would require changing keys every 7 years. Even if the mobile node were to move every minute, this would provide protection for over a month. Given typical mobility patterns, there is little danger of replay problems; nodes for which problems might arise are expected to use methods other than manual configuration for Kbm anyway. When the sequence number field rolls over, the parties SHOULD configure another value for Kbm.

If a correspondent node does NOT keep track of the Sequence Number for Binding Update messages from a particular mobile node, then the correspondent node could be fooled into accepting an old value for the mobile node's care-of address. In the unlikely event that this

address was reallocated to another IPv6 node in the meantime, that IPv6 node would then be vulnerable to unwanted traffic emanating from the correspondent node. In order to circumvent this possibility, correspondent nodes are mandated to keep track of the most recent Sequence Number value in a Binding Update message from the mobile node.

There is no upper bound on the lifetime defined for the preconfigured Kbm. As noted, the key is very, very likely to be quite secure over the lifetime of the security association and usefulness of applications between a mobile node and correspondent node that fit the terms specified in [section 2](#).

[4](#). IANA Considerations

No new protocol numbers are required.

[5](#). Acknowledgement

Thanks are due to everyone who reviewed the discussion of issue #146.

References

- [1] D. Johnson, C. Perkins, and J. Arkko. Mobility support in IPv6 (work in progress). Internet Draft, Internet Engineering Task Force, May 2003.
- [2] P. Nikander, T. Aura, J. Arkko, G. Montenegro, and E. Nordmark. Mobile IP version 6 Route Optimization Security Design Background. Internet Draft, Internet Engineering Task Force, June 2003.

The first citation is normative, and the second citation is informative only.

Perkins

Expires 5 October 2004

[Page 3]

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be

revoked by the Internet Society or its successors or assignees. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

Author's Address

Questions about this document can also be directed to the author:

Charles E. Perkins
Nokia Research Center
313 Fairchild Drive
Mountain View, CA 94043
USA

Phone: +1 650 625-2986
Fax: +1 650 625-2502
E-mail: charles.perkins@nokia.com

Perkins

Expires 5 October 2004

[Page 5]