

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: December 05, 2014

M. Richardson  
SSW  
June 03, 2014

**table of contents for security architecture  
draft-richardson-6tisch-table-of-contents-00**

Abstract

This is a template for a security architecture.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on December 05, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	security requirements . . . . .	<a href="#">2</a>
<a href="#">1.1.</a>	thread model . . . . .	<a href="#">2</a>
<a href="#">1.2.</a>	implementation cost . . . . .	<a href="#">2</a>
<a href="#">1.3.</a>	denial of service . . . . .	<a href="#">2</a>
<a href="#">2.</a>	protocol requirements/constraints/assumptions . . . . .	<a href="#">2</a>
<a href="#">2.1.</a>	inline/offline . . . . .	<a href="#">2</a>
<a href="#">3.</a>	time sequence diagram . . . . .	<a href="#">3</a>
<a href="#">3.1.</a>	explanation of each step . . . . .	<a href="#">3</a>
<a href="#">3.2.</a>	size of each packet . . . . .	<a href="#">3</a>
<a href="#">4.</a>	resulting security properties obtained from this process . .	<a href="#">3</a>
<a href="#">5.</a>	deployment scenarios underlying protocol requirements . . . .	<a href="#">3</a>
<a href="#">6.</a>	device identification . . . . .	<a href="#">3</a>
<a href="#">6.1.</a>	PCE/Proxy vs Node identification . . . . .	<a href="#">3</a>
<a href="#">6.2.</a>	Time source authentication / time validation . . . . .	<a href="#">3</a>
<a href="#">6.3.</a>	description of certificate contents . . . . .	<a href="#">3</a>
<a href="#">6.4.</a>	privacy aspects . . . . .	<a href="#">3</a>
<a href="#">7.</a>	slotframes to be used during join . . . . .	<a href="#">3</a>
<a href="#">8.</a>	configuration aspects . . . . .	<a href="#">3</a>
<a href="#">9.</a>	authorization aspects . . . . .	<a href="#">3</a>
<a href="#">9.1.</a>	how to determine a proxy/PCE from a end node . . . . .	<a href="#">3</a>
<a href="#">9.2.</a>	security considerations . . . . .	<a href="#">3</a>
<a href="#">10.</a>	security architecture . . . . .	<a href="#">4</a>
<a href="#">11.</a>	Posture Maintenance . . . . .	<a href="#">4</a>
<a href="#">12.</a>	Security Considerations . . . . .	<a href="#">4</a>
<a href="#">13.</a>	Other Related Protocols . . . . .	<a href="#">4</a>
<a href="#">14.</a>	IANA Considerations . . . . .	<a href="#">4</a>
<a href="#">15.</a>	Acknowledgements . . . . .	<a href="#">4</a>
<a href="#">16.</a>	Normative references . . . . .	<a href="#">4</a>
	Author's Address . . . . .	<a href="#">4</a>

**[1.](#) security requirements****[1.1.](#) thread model****[1.2.](#) implementation cost**

(storage of security material, computational cost)

**[1.3.](#) denial of service**

other communication impacts of security protocol mechanics

**[2.](#) protocol requirements/constraints/assumptions****[2.1.](#) inline/offline**



dependencies on centralized or external functionality, inline and offline

### **3. time sequence diagram**

#### **3.1. explanation of each step**

#### **3.2. size of each packet**

and number of frames needed to contain it.

### **4. resulting security properties obtained from this process**

### **5. deployment scenarios underlying protocol requirements**

### **6. device identification**

#### **6.1. PCE/Proxy vs Node identification**

#### **6.2. Time source authentication / time validation**

Note: RPL Root authentication is a chartered item

#### **6.3. description of certificate contents**

#### **6.4. privacy aspects**

### **7. slotframes to be used during join**

how is this communicated in the (extended) beacon.

### **8. configuration aspects**

(allocation of slotframes after join, network statistics, neighboetc.)

### **9. authorization aspects**

lifecycle (key management, trust management)

#### **9.1. how to determine a proxy/PCE from a end node**

#### **9.2. security considerations**

what prevents a node from transmitting when it is not their turn  
(part one: jamming)

can a node successfully communicate with a peer at a time when not supposed to, may be tied to link layer security, or will it be policed by receiver?

## **10. security architecture**

security architecture and fit of e.g. join protocol and provisioning into this

## **11. Posture Maintenance**

(SACM related work)

## **12. Security Considerations**

## **13. Other Related Protocols**

## **14. IANA Considerations**

## **15. Acknowledgements**

## **16. Normative references**

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

### Author's Address

Michael C. Richardson  
Sandelman Software Works  
470 Dawson Avenue  
Ottawa, ON K1Z 5V7  
CA

Email: [mcr+ietf@sandelman.ca](mailto:mcr+ietf@sandelman.ca)  
URI: <http://www.sandelman.ca/>