ERICSSON

Configuring Key Chains

SYSTEM ADMINISTRATOR GUIDE

70/1543-CRA 119 1170/1-V1 Uen D

Copyright

© Ericsson AB 2009–2011. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

SmartEdge	is a registered trademark of Telefonaktiebolaget LM Ericsson.
NetOp	is a trademark of Telefonaktiebolaget LM Ericsson.

Contents

1 Overview

This document provides an overview of the SmartEdge routerSM family of systems key chain feature and describes the tasks used to configure, monitor, and administer key chains. This document also provides a configuration example of key chains.

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the **`Product Overview`** folder of this Customer Product Information library.

Key chains allow you to control authentication keys used by various protocols in the system. The SmartEdge router supports the use of key chains with Mobile IP services and the Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Virtual Router Redundancy Protocol (VRRP) routing protocols. Enabling key chains for a protocol is part of the configuration process for the protocol. For information about configuring Mobile IP services, see *Configuring Mobile IP for a Foreign Agent*. For information about configuring the above-mentioned routing protocols, see *Configuring OSPF*, *Configuring IS-IS*, or *Configuring VRRP*.

2 Configuration and Operations Tasks

Note: In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the *Command List*.

To configure key chains, perform the tasks described in the following sections.

2.1 Configure a Key Chain Name and Description (Optional)

To configure a key chain name and description, perform the task described in Table 1.

Table 1 Configure a Key Chain Name and Description (Optional)

Task	Root Command	Notes
Configure a key chain name and description.	*key-chain description*	Enter this command in context configuration mode. The description is displayed in the output of the **`show configuration`** and **`show key-chain`** commands.

2.2 Configure a Key Chain Name and ID

To configure a key chain name and ID, perform the task described in Table 2.

Table 2 Configure a Key Chain Name and ID

Task	Root Command	Notes
Configure a key chain name and ID, and access key chain configuration mode.	*key-chain*	Enter this command in context configuration mode.

2.3 Configure a Security Parameter Index

To configure a security parameter index (SPI) for a key chain, perform the task described in Table 3.

Table 3 Configure an SPI for a Key Chain

Task	Root Command	Notes
Configure an SPI for a key chain.	*key-chain*	Enter this command in key chain configuration mode.

2.4 Configure a Key String

To configure a key string (a password), perform the task described in Table 4.

Table 4 Configure a Key String

Task	Root Command	Notes
Configure a key string.	*key-string*	Enter this command in key chain configuration mode.

2.5 Limit the Lifespan of a Key

To limit the lifespan of a key, perform one or more of the tasks described in Table 5; enter all commands in key chain configuration mode.

Table 5 Limit the Lifespan of a Key

Task	Root Command	Notes
Specify a date and time at which to start sending the key, and optionally, a time at which to stop sending the key.	*send-lifetime*	If you do not issue the **`send-lifetime`** command, the key is sent starting immediately and continues to be sent indefinitely.
Specify a date and time at which to start accepting the key, and optionally, a time at which to stop accepting the key.	*accept-lifetime*	If you do not issue the **`accept-lifetime`** command, the key is accepted starting immediately and continues to be accepted indefinitely.

2.6 Enable Key Chain Authentication with Routing Protocols

To enable key chain authentication with OSPF, IS-IS, or VRRP, perform the task described in Table 6.

Table 6 Enable Key Chain Authentication with Routing Protocols

Task	Root Command	Notes
Enable key chain authentication with routing protocols.	*authentication*	Enter this command in OSPF interface, IS-IS router, IS-IS interface, or VRRP configuration mode, depending on the routing protocol being configured.

For information about configuring routing protocols and the **`authentication`** command (in any of the modes listed in Table 6), see *Configuring OSPF*, *Configuring IS-IS*, or *Configuring VRRP*.

2.7 Enable Key Chain Authentication with Mobile IP

To enable key chain authentication for Mobile IP services, perform the task described in Table 7.

Table 7 Enable Key Chain Authentication for Mobile IP Services

Task	Root Command	Notes
Enable key chain authentication for Mobile IP services.	*authentication*	Enter this command in foreign agent (FA) or home agent (HA) peer configuration mode.

For information about configuring Mobile IP services and the **`authentication`** command (in FA configuration mode), see *Configuring Mobile IP for a Foreign Agent*.

2.8 Operations Tasks

To monitor and troubleshoot key chain features, perform the key chain operations tasks described in Table 8. Enter the **`debug`** command in exec mode; enter the **`show`** command in any mode.

Table 8 Key Chain Operations Tasks

Task	Root Command
Enable the generation of key chain debug messages.	*debug key-chain*
Display information about one or all key chains configured in the system.	*show key-chain*

3 Configuration Examples

The following example configures a rollover period on February 2, 2002 from 12:00 a.m. to 2:00 a.m. During this period, both keys will be accepted. Starting at 1:00 a.m., the new key will be sent:

```
[local]Redback(config-ctx)#key-chain ospf-keychain key-id 1
[local]Redback(config-key-chain)#key-string redback
[local]Redback(config-key-chain)#accept-lifetime 2001:02:02:00:00:00 2001:02:02:02:00:00
[local]Redback(config-key-chain)#send-lifetime 2001:02:02:01:00:00 2002:02:02:01:00:00
[local]Redback(config-key-chain)#key-chain ospf-keychain key-id 2
[local]Redback(config-key-chain)#key-string se800
[local]Redback(config-key-chain)#accept-lifetime 2002:02:02:00:00:00 2003:02:02:02:00:00
[local]Redback(config-key-chain)#send-lifetime 2002:02:02:01:00:00 2003:02:02:01:00:00
[local]Redback(config-key-chain)#exit
[local]Redback(config-ctx)#router ospf 1
[local]Redback(config-ospf)#area 0
[local]Redback(config-ospf-area)#interface fa4/1
[local]Redback(config-ospf-if)#authentication md5 ospf-keychain
```