Project	IEEE 802.16 Broadband Wireless Access Working Group <**http://IEEE 802.org/16**>
Title	Hybrid authentication hierarchy in MMR Control Plane for the relay network
Date Submitted	2007-01-08
Source(s)	Sheng Sun; Guo-Qiang Wang; Hang Zhang; Peiying Zhu; Wen Tong; Mo-han Fong 3500 Carling Avenue Ottawa, Ontario K2H 8E9	Voice: 1-613-763-1315 [mailto:wentong@nortel.com] [mailto:pyzhu@nortel.com] [mailto:shengs@nortel.com]
Re:	A response to a Call for Technical Proposal, http://wirelessman.org/relay/docs/80216j-06_034.pdf
Abstract	Security elements and mechanisms for .16j MMR control plane
Purpose	To incorporate the proposed text into the P802.16j Baseline Document (IEEE 802.16j-06/026r1)
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://IEEE 802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://IEEE 802.org/16/ipr/patents/notices>.

Hybrid authentication hierarchy in MMR Control Plane for the relay network

Sheng Sun; Guo-qiang Wang; Hang Zhang;
Peiying Zhu; Wen Tong; Mo-han Fong
Nortel

1 Introduction

This contribution aims to introduce the security mechanisms into the .16j MMR control plane to protect the confidentiality and integrity of the transmission of the MMR control messages. The encryption key distribution and management model are laid on the security principles of PKMv2 required with respect to the IEEE 802.16-2004 and IEEE 802.16e-2005.
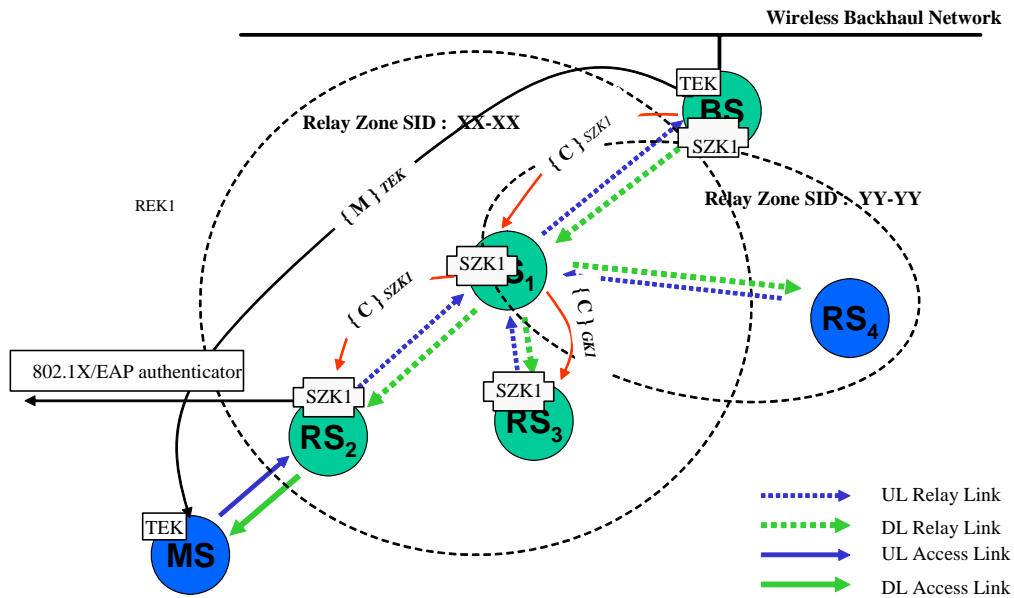

Figure 1   RRPS overview

1.1 RRPS (Robust Relay Path Security)

1.1.1 RRPS overview
Robust Relay Path Security (RRPS) service is used to permit efficient establishment of transmission between the Base Station (BS) and Relay Stations (RS) in a .16j MMR network.

Today's .16e network security services provide the minimum security protection to the control planes messages (Sec 7.1.1 of IEEE 802.16e-2005) in the Access link. The multi-hop based MMR relay network needs more complicated security model in order to satisfy both of the security objective and the performance objective. In other words, the security mechanism in the .16j MMR network should impose very minimum overhead onto the control plane. Another metric of the security model required for .16j network is the fast link/path establishment and the fast re-association in the case of link failure or the handover operations.

RRPS is the security framework comprising the following security elements

Hybrid Association/Authentication Model

Encryption Keys and Keys distribution

The operation of RRPS relies on the BS which centralizes the authentication for the RSs within its Security Zone identified by the SZID (Security Zone ID). Each RS within the security zone becomes the Delegated Authenticator (DA) when it gets authenticated from its anchored authenticator as illustrated in the following diagram.
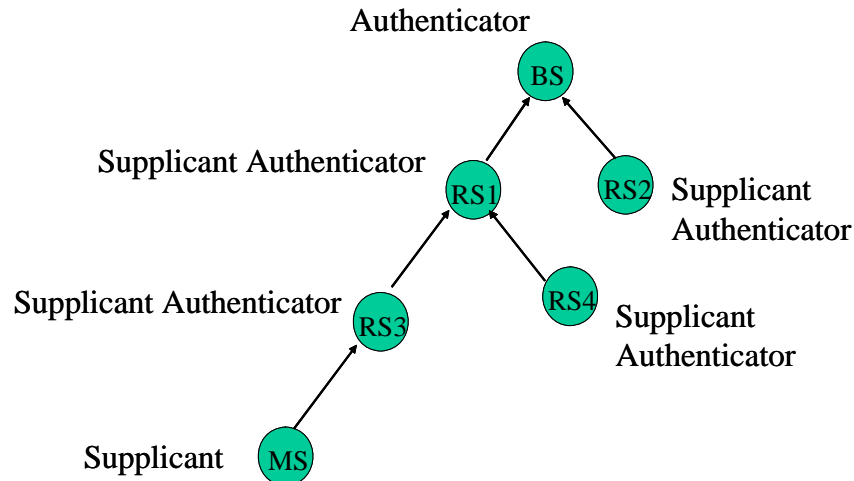
Figure 2   Authentication Hierarcy

This authentication hierarchy distributes the authenticator function to the perimeter of the security zone. Any RS assumes the authenticator role implements the full PKMv2 authentication function. The distributed authentication model virtually extends the BS's authentication function as closer to the .16e/d access link as possible, which brings the following characteristics:

   - Basic uses IEEE 802.16e-2005 PKMv2

   - Many relay operations are associated with paths, and these operations populate the same information to all RS along a given path

-   MMR cell could be decomposed as security zones

-   In each zone, the RSs share the same group key for path-oriented operations

-   Group key is managed and distributed by BS

-   Per Group SA associated HMAC/CMAC is used to authenticate the sender

-   Group-cast signaling messages are defined to support path operations

-   Greatly reduce the signaling overhead, especially in RS handover case

RRPS requires information to be exchanged during a RS's initial security association with a Authenticator, Subsequent security associations to other Authenticators within the same security zone may utilize the PKMv2 key hierarchy that is established during Initial RRPS Authentication.

Note: How to define security zone is out of scope of this contribution.

1.1.3 Link Establishment

The Initial RRPS Authentication mechanism permits an RS to enable the becoming of the Delegated Authenticator (DA) when establishing security for subsequent links. The DA here involves the process of authentication and key exchange to become the trustworthy authenticator within a specific security zone.

A MMR-BS first announces its policy as the root of the security zone which is identified by the Security Zone ID (SZID), the SZID is randomly computed by the MMR-BS involving the CID and MAC address of the MMR-BS and other parameters. A RS1 bootstraps itself by 802.16 UL/DL sync association with the BS. Then RS1 requests the EAP authentication or be requested by the MMR-BS depending on the EAP mode they negotiate. The MSK is distributed by the backend AAA (Radius) server as per PKMv2 as illustrated in Figure

Phase I: RS 1 Association and Authentication Bootstrap (802.16-2005)
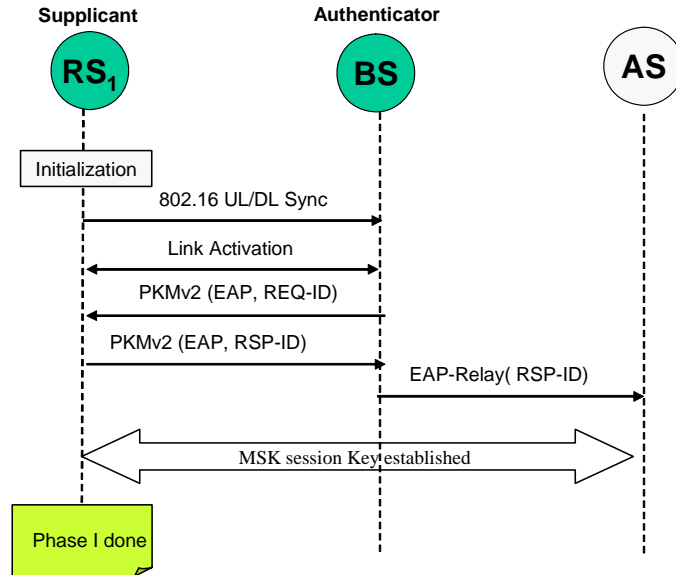
Figure 3   RRPS Security Link Establishment Phase I

Then the MMR-BS generates the SZK and distributes it to the RS1 through the SZ Key exchange method. Up to this point, the RS1 becomes the Delegated Authenticator (DA) with the full set of authentication function. The SZ key exchange method could reuse the TEK exchange method specified in PKMv2

Phase II: RS1 becomes the delegated authenticator

Security Zone:
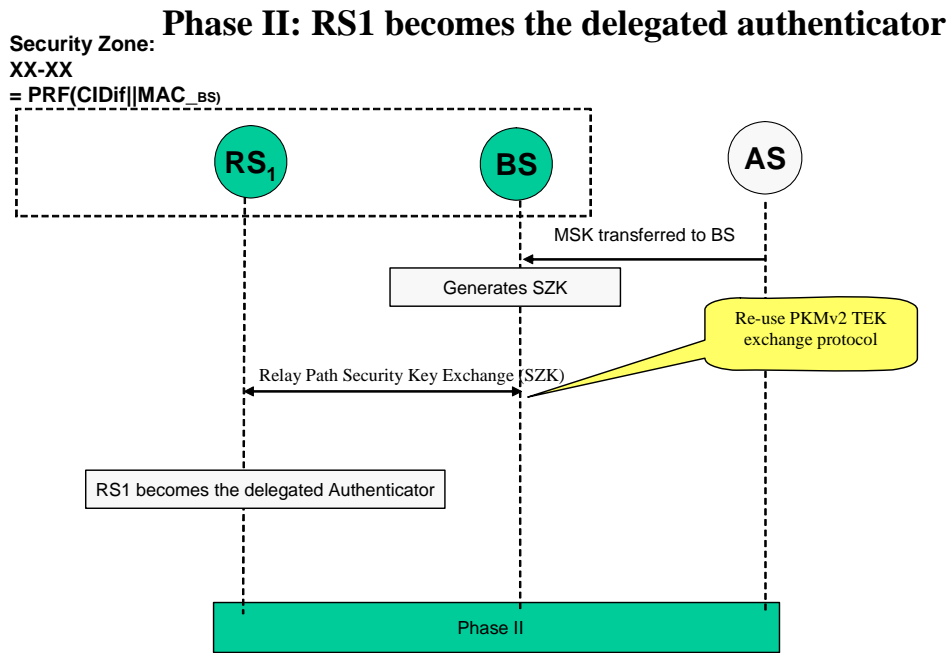**XX-XX**
= PRF(CIDif||MAC_BS)

Figure 4   RRPS Security Link Establishment Phase II

Another RS goes through the same handshake and EAP authentication process to become the DA within the security zone. However, RS2 handshakes with the RS1's DA instead of the MMR-BS.
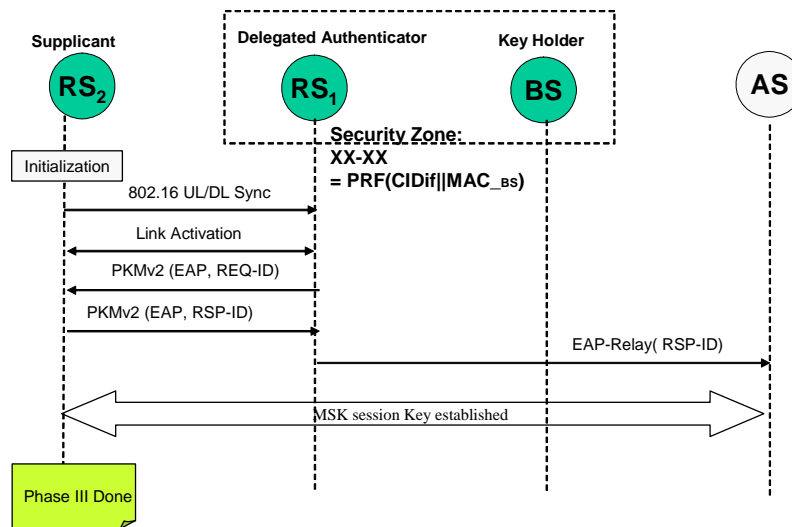
Phase III: RS 2 Authentication Bootstrap

Figure 5   RRPS Security Link Establishment Phase III

Then BS sends the SZK (Security Zone Key) to the RS2 and RS2 inherently becomes the DA.
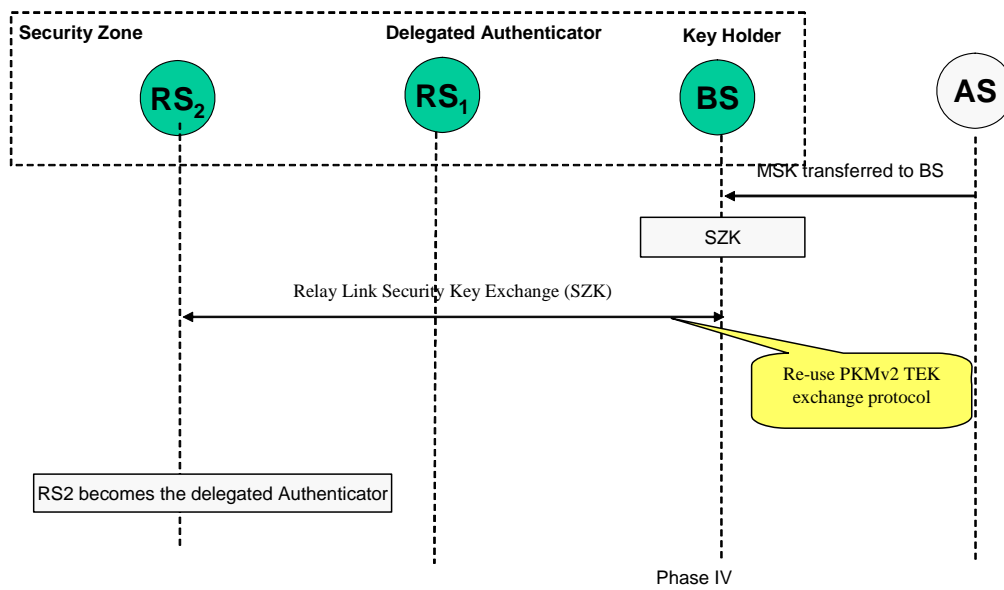
Phase IV: RS2 becomes the delegated authenticator

Figure 6   RRPS Security Link Establishment Phase IV

2. Proposed text changes

++++++++++++ start text proposal ++++++++++++++++++++++++++++++++++
[Insert the followings after the end of section 7.1]

The Security Architecture for .16j relay network has two components to follow

An authentication protocol for the effective authentication purpose across the wireless relay network. The protocol defines the hierarchy of the relay authentication model, i.e the Root Authenticator (RA) and the Delegated Authenticator (DA) etc. Associated with the Authentication Model, a new conceptual security zone is also defined which can be dynamically composed and decomposed.
The encryption/signature key derivation structure. So as to secure the control message transmitted over the open air, the security protocol defines the security zone key which is shared by all the Relay Stations (RS) for the delivery of the control messages.

    The encryption key distribution and management model are laid on the security principles of PKMv2 required with respect to the IEEE 802.16-2004 and IEEE 802.16e-2005.

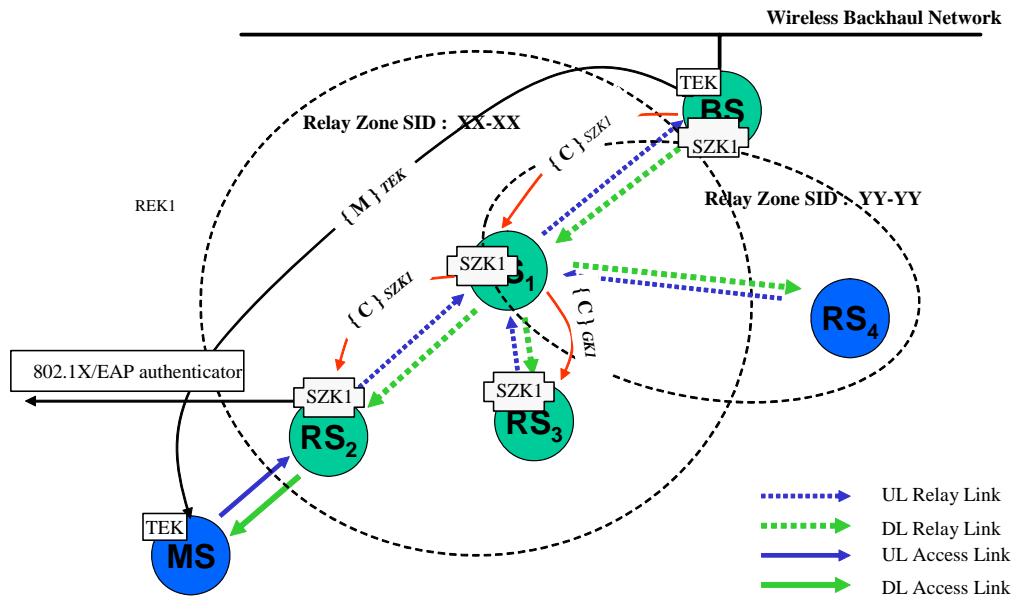# Robust Relay Path Security Protocol (RRPS)

Figure X   RRPS overview

Robust Relay Path Security (RRPS) service is used to permit efficient establishment of transmission between the Base Station (BS) and Relay Stations (RS) in a .16j MMR network.

Today's .16e network security services provide the minimum security protection to the control planes messages (Sec 7.1.1 of IEEE 802.16e-2005) in the Access link. The multi-hop based MMR relay network needs more complicated security model in order to satisfy both of the security objective and the performance objective. In other words, the security mechanism in the .16j MMR network should impose very minimum overhead onto the control plane. Another metric of the security model required for .16j network is the fast link/path establishment and the fast re-association in the case of link failure or the handover operations.

RRPS is the security framework comprising the following security elements

Hybrid Association/Authentication Model

Encryption Keys and Keys distribution

The operation of RRPS relies on the BS which centralizes the authentication for the RSs within its Security Zone identified by the SZID (Security Zone ID). Each RS within the security zone becomes the Delegated Authenticator (DA) when it gets authenticated from its anchored authenticator as illustrated in the following diagram.
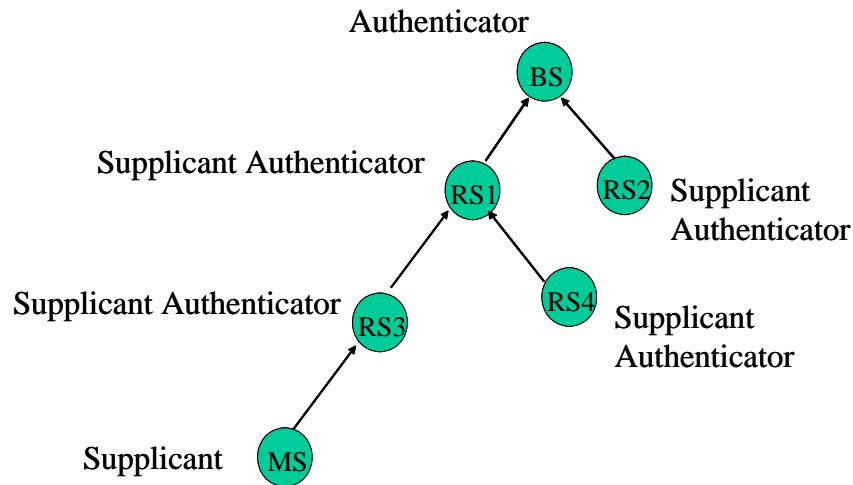
Authenticator

Figure Y   Authentication Hierarcy

This authentication hierarchy distributes the authenticator function to the perimeter of the security zone. Any RS assumes the authenticator role implements the full PKMv2 authentication function. The distributed authentication model virtually extends the BS's authentication function as closer to the .16e/d access link as possible, which brings the following characteristics:

   - Basic uses IEEE 802.16e-2005 PKMv2

   - Many relay operations are associated with paths, and these operations populate the same information to all RS along a given path

-    MMR cell could be decomposed as security zones

-    In each zone, the RSs share the same group key for path-oriented operations

-    Group key is managed and distributed by BS

-    Per Group SA associated HMAC/CMAC is used to authenticate the sender

-    Group-cast signaling messages are defined to support path operations

-    Greatly reduce the signaling overhead, especially in RS handover case

RRPS requires information to be exchanged during a RS's initial security association with a Authenticator, Subsequent security associations to other Authenticators within the same security zone may utilize the PKMv2 key hierarchy that is established during Initial RRPS Authentication.

Note: How to define security zone is out of scope of this contribution.

[Insert the followings after the end of section 7.2]

The Initial RRPS Authentication mechanism permits an RS to enable the becoming of the Delegated Authenticator (DA) when establishing security for subsequent links. The DA here involves the process of authentication and key exchange to become the trustworthy authenticator within a specific security zone.

A MMR-BS first announces its policy as the root of the security zone which is identified by the Security Zone ID (SZID), the SZID is randomly computed by the MMR-BS involving the CID and MAC address of the MMR-BS and other parameters. A RS1 bootstraps itself by 802.16 UL/DL sync association with the BS. Then RS1

requests the EAP authentication or be requested by the MMR-BS depending on the EAP mode they negotiate. The MSK is distributed by the backend AAA (Radius) server as per PKMv2 as illustrated in Figure

**Phase I: RS 1 Association and Authentication Bootstrap
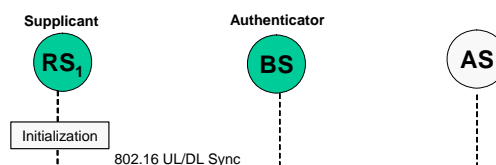(802.16-2005)**

Figure Z   RRPS Security Link Establishment Phase I

Then the MMR-BS generates the SZK and distributes it to the RS1 through the SZ Key exchange method. Up to this point, the RS1 becomes the Delegated Authenticator (DA) with the full set of authentication function. The SZ key exchange method could reuse the TEK exchange method specified in PKMv2

Phase II: RS1 becomes the delegated authenticator

Security Zone:
XX-XX
= PRF(CIDif||MAC_BS)

RS$_1$ BS   AS

MSK transferred to BS

Generates SZK

Re-use PKMv2 TEK exchange protocol

Relay Path Security Key Exchange (SZK)

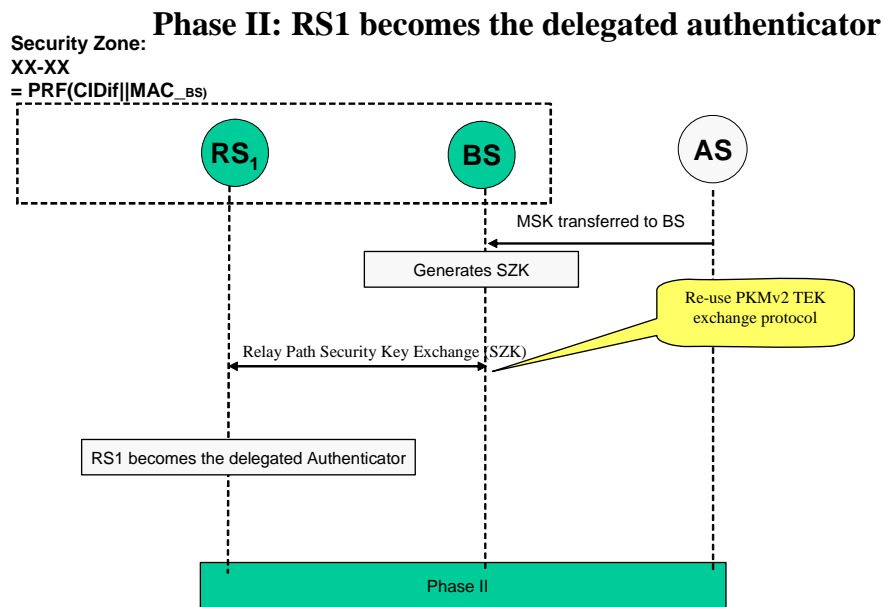RS1 becomes the delegated Authenticator

Phase II

Figure U   RRPS Security Link Establishment Phase II

Another RS goes through the same handshake and EAP authentication process to become the DA within the security zone. However, RS2 handshakes with the RS1's DA instead of the MMR-BS.
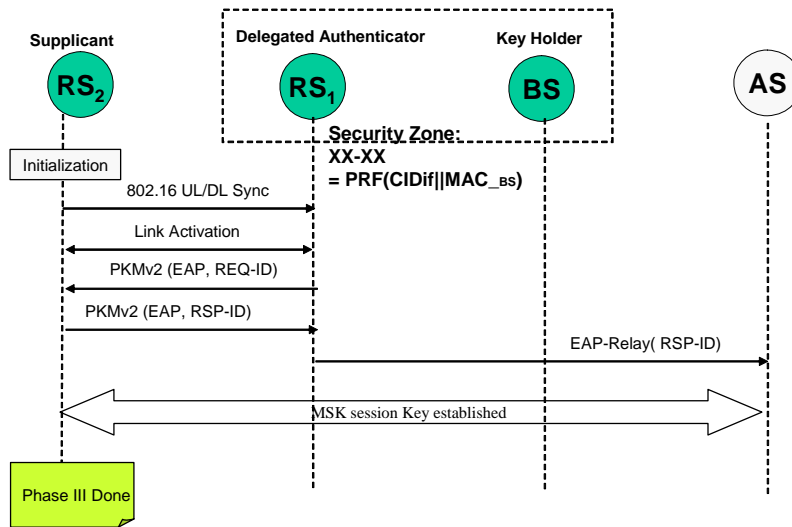
Phase III: RS 2 Authentication Bootstrap

Figure V   RRPS Security Link Establishment Phase III

Then BS sends the SZK (Security Zone Key) to the RS2 and RS2 inherently becomes the DA.
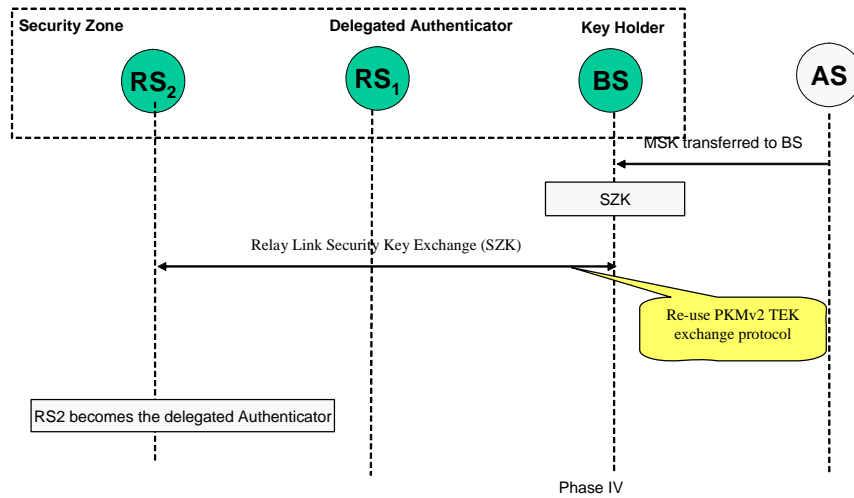
Phase IV: RS2 becomes the delegated authenticator

Figure W   RRPS Security Link Establishment Phase IV

+++++++++++++++++++ *End of text proposal* +++++++++++++++++++