3GPP TSG SA WG3 Security – S3#24 **S3-020368**

14 - 17 May 2002

Helsinki, Finland

Source: **SSH Communications Security Corp.**

Title: **COPS usage for IPSec policy management in NDS/IP**

Document for: **Discussion**

Agenda Item: **6.2**

1 Introduction

In S3#21bis the contribution S3z020013 / N4-020418 [1] concerning the usage of COPS [2,3] protocol for MAP SA management was presented. The principle the contribution presented was approved by CN4 on April 9, 2002 in Ft. Lauderdale meeting.

Since COPS is already deployed in rel-5 networks, this contribution suggests reutilising the existing COPS framework for IPSec policy management.

2 Technical rationales for usage of COPS in IPSec policy management

This Chapter describes technical rationales for adopting COPS also for IPSec policy management.

2.1 Existing standards

COPS protocol (RFC 2748) and the Usage of COPS for policy provisioning (RFC 3084) are both IETF RFCs that have received the RFC status several years ago (RFC 2748 in 2000 and RFC 3084 in 2001).

The standards required for IPSec policy management, but is still an IETF draft, are

1. IPSec Policy Information Base (PIB) [4]

   IPSec PIB is expected to go to IP Security Policy (IPSP) WG last call within the near future. However, since IPSP WG is not gathering in the 54th IETF meeting in Yokohama, the draft can still be updated according to the functionalities that NDS/AF requires, but are not covered with IPSec PIB.

2. Framework Policy Information Base [6]

   Also the framework PIB is expected to go to the WG last within the near future.

2.2 Deployed framework

As described in [1], the COPS policy management framework is already deployed within rel-5 schedule for MAP SA management. Since the COPS model is designed to be extensible so that other kinds of policy clients may be supported, the protocol can be used for MAPSec SA as well as IPSec policy management.

2.3 Existing reference implementations

COPS framework is also widely deployed in Internet and open source client implementations are available, like [5].

2.4 Simplifies policy management architecture

NDS/MAP, NDS/IP and NDS/AF form complex security architecture to 3GPP rel-5+ networks. Management of security is hard (badly configured architecture easily ends up to security holes) and managing complex security architecture is even harder. If also the management system is complex (composing of numerous different policy management protocols), configurations resulting in a security breach are expected to increase. Therefore the management architecture should be kept as simple as possible and the existing management architecture should be utilized as much as possible to avoid the introduction of additional complexity.

3 Proposal

The above rationales clearly give several benefits for reutilising COPS for the policy management with rel-6 schedule, so SA3 are asked to take the usage of COPS as the working assumption for rel-6 NDS/IP IPSec policy management and to suggest this principle to CN4.

Reference

[1] 3GPP S3z020013, “Proposed additions to 33.200 about COPS usage in Ze interface for Local Security Association and Policy Distribution“, February 2002.
<http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_21b_adhocs_NDS_MAP_IMS/Docs/PDF/S3z020013.pdf>

[2] IETF RFC 2748, “The COPS (Common Open Policy Service) protocol“, January 2000

[3] IETF RFC 3084: “COPS Usage for Policy Proviosing“, March 2001

[4] IETF draft: IPsec Policy Information Base, February 2002
< draft-ietf-ipsp-ipsecpib-04.txt >

[5] Intel® COPS Client Software Development Kit
< http://www.intel.com/ial/cops/download.htm >

[6] IETF draft, "Framework Policy Information Base", November 2001
< draft-ietf-rap-frameworkpib-06.txt >