

SAND-98-0253C
 SAND-98-0253C
 CONF-980209-

ATM Forum Technical Committee
 ATM Forum/98-xxxx

TITLE: Sandia's Straw Ballot Comments on the Security Version 1.0 Specification

SOURCES:

Thomas Tarman*
 Sandia National Laboratories
 P.O. Box 5800
 Albuquerque, NM 87185-0806
 USA
 Phone: +1-505-844-4975
 Fax: +1-505-844-2067
 Email: tdtarma@sandia.gov

Ann Hodges
 Sandia National Laboratories
 P.O. Box 5800
 Albuquerque, NM 87185-1138
 USA
 +1-505-844-6284
 +1-505-284-3850
 alhodge@sandia.gov

RECEIVED

FFR 10 1998

OSTI

DATE: February, 1998 (Anaheim)

DISTRIBUTION: Security

ABSTRACT:

This contribution provides Sandia's straw ballot comments for the Security Version 1.0 specification, STR-SECURITY-01.01.

NOTICE:

This contribution has been prepared to assist the ATM Forum. This proposal is made by the Sandia National Laboratories as a basis of discussion. This contribution should not be construed as a binding proposal on Sandia. Specifically, the author and his company reserve the right to amend or modify the statements contained herein.

1. Introduction

This contribution provides Sandia's comments to the ATM Forum Security 1.0 straw ballot specification, STR-SECURITY-01.01. These comments are organized as follows - major comments indicate technical defects in the specification which, if not resolved, may preclude Sandia's vote in favor of the specification. Minor comments are technical comments which, if left unresolved, will not preclude Sandia's favorable vote. Finally, editorial comments are also provided.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

MASTER

* This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy.

19980401 082

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

3. Minor Comments

Section 1 – Introduction

A statement that management plane security is not in this specification's scope is needed.

Suggested resolution: Add a sentence between paragraphs one and two stating that management plane security is outside the scope of this specification.

Section 1.5 – Specification Scope

In paragraph 3, more explanation is required distinguishing per-connection security from link security.

Suggested resolution: state that security services apply on individual virtual connections rather than physical links (which may carry many virtual connections).

Section 3.4.3 – Error Processing

The first sentence states that error processing is site specific. This requirement came from the observation that the desire to provide diagnostic information competes with the desire to withhold information which may be helpful to an attacker.

Suggested resolution: point to the error processing procedures in sections 5.1.4 and 5.1.5, and state that the use of error diagnostic information is site specific.

Section 5.0 – Support Services

In the fourth paragraph, there is no mention that the two-way exchange protocol can also be used to establish security services for the first leaf in a multipoint call.

Suggested resolution: append the following text to the first sentence of the fourth paragraph – “ or point-to-multipoint connection.”

Section 5.1.1.1 – Three-Way Security Message Exchange Protocol

Error processing is conspicuously absent in this section. Although error processing is described in more detail later in Section 5, it should be addressed here as well.

Suggested resolution: append a paragraph at the end of this section stating that if an error is encountered, the protocol shall cease, the connection shall be released, and an error code shall be returned. Also state that this protocol is described in detail in Section 5.1.5.3.

Section 5.1.1.2 – Two-Way Security Message Exchange Protocol

Again, error processing is conspicuously absent in this section. Although error processing is described in more detail later in Section 5, it should be addressed here as well.

Suggested resolution: append a paragraph at the end of this section stating that if an error is encountered, the protocol shall cease, the connection shall be released, and an error code shall be returned. Also state that this protocol is described in detail in Section 5.1.4.

Section 5.1.1.2 – Two-Way Security Message Exchange Protocol

Unlike the three-way security message exchange protocol, the two-way protocol does not provide for certificate exchange. We do not see a reason for this discrepancy.

Suggested resolution: modify the diagrams and text so that certificates are included in each of the flows in the two-way protocol.

M98003087



Report Number (14) SAND--98-0253C
CONF-980209--

Publ. Date (11) 199801
Sponsor Code (18) DOE/MA, XF
JC Category (19) UC-900, DOE/ER

DOE