ATM Forum
Technical Committee

Addendum to Sec 1.1
Secure CBR Traffic in a Policed Network

AF-0189.000

July 2002

The information in this publication is believed to be accurate as of its publication date. Such information is subject to change without notice and The ATM Forum is not responsible for any errors. The ATM Forum does not assume any responsibility to update or correct any information in this publication. Notwithstanding anything to the contrary, neither The ATM Forum nor the publisher make any representation or warranty, expressed or implied, concerning the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind shall be assumed by The ATM Forum or the publisher as a result of reliance upon any information contained in this publication.

The receipt or any use of this document or its contents does not in any way create by implication or otherwise:

- Any express or implied license or right to or under any ATM Forum member company's patent, copyright, trademark or trade secret rights which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor
- Any warranty or representation that any ATM Forum member companies will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor
- Any form of relationship between any ATM Forum member companies and the recipient or user of this document.

Implementation or use of specific ATM standards or recommendations and ATM Forum specifications will be voluntary, and no company shall agree or be obliged to implement them by virtue of participation in The ATM Forum.

The ATM Forum is a non-profit international organization accelerating industry cooperation on ATM technology. The ATM Forum does not, expressly or otherwise, endorse or promote any specific products or services.

NOTE: The user's attention is called to the possibility that implementation of the ATM interoperability specification contained herein may require use of an invention covered by patent rights held by ATM Forum Member companies or others. By publication of this ATM interoperability specification, no position is taken by The ATM Forum with respect to validity of any patent claims or of any patent rights related thereto or the ability to obtain the license to use such rights. ATM Forum Member companies agree to grant licenses under the relevant patents they own on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. For additional information contact:

The ATM Forum
Worldwide Headquarters
572 B Ruger Street
San Francisco, CA 94129-0920
Tel: +1.415.561.6275
Fax: +1.415.561.6120

Table of Contents

1 INTRODUCTION........ 1

1.1 PURPOSE........ 1
1.2 REFERENCES........ 1
1.3 ABBREVIATIONS AND ACRONYMS........ 1

2 NORMATIVE NOTES FOR SECURE CBR TRAFFIC IN A POLICED NETWORK........ 2

2.1 SEPARATE POLICING FULLY SUPPORTED........ 2
2.2 SEPARATE POLICING NOT FULLY SUPPORTED........ 2

List of Figures

None
Blank Page

List of Tables

None
Blank Page

1 INTRODUCTION

As described in ATM Forum's Security 1.1 Specification [1], cryptographic synchronization for confidentiality algorithms using counter mode and all Key Update operations are maintained though the use of User OAM (Operation and Maintenance) cells. Without taking care during call establishment of a Constant Bit Rate (CBR) connection, however, a User OAM cell introduced by the security device on behalf of the users will likely cause a non-compliant cell to be detected and policed. Either the User OAM cell or the subsequent data cell will be lost depending on where the cell is inserted with respect to the traffic flow. This data loss may result in undecipherable user traffic until the next synchronization cell is successfully passed.

Starting in User-Network Interface Signaling Specification (UNI) 4.1 [2], and Private Network to Network Interface (PNNI) 1.1 [3], support for the OAM Traffic Descriptor Information Element (IE) was introduced to facilitate separate policing of user and OAM traffic. This supports a robust implementation of ATM Security in a CBR environment. The OAM Traffic Descriptor IE was developed to allow up to an additional 1% of the requested user traffic to be dedicated to User OAM cells. This allows the UNI or PNNI interfaces to identify and to police separately the user data and the User OAM cell.

1.1 Purpose

This addendum is intended to give guidance to the developers of ATM Security devices to understand how to use the OAM Traffic Descriptor IE. Guidance is also provided for supporting security synchronization on CBR connections through networks that do not fully support separate policing of F5 OAM cells. It is assumed that the reader has a working knowledge of [1].

1.2 References

[1] ATM Forum Technical Committee, "ATM Security Specification," Version 1.1 af-sec-0100.002, March 2001

[2] ATM Forum Technical Committee, "ATM User-Network Interface Signaling Specification," Version 4.1 af-sig-0061.001, April 2002

[3] ATM Forum Technical Committee, "Private Network-Network Interface Specification," Version 1.1 af-pnni-0055.002

[4] Telecommunication Standardization Sector of the International Telecommunication Union (ITU), "B-ISDN Application Protocols for Access Signaling, Recommendation Q.2931," February 1995

1.3 Abbreviations and Acronyms

AAL	ATM Adaptation Layer
ATM	Asynchronous Transfer Mode
CBC	Cipher Block Chaining
CBR	Constant Bit Rate
IE	Information Element
ITU	International Telecommunication Union
OAM	Operation and Maintenance
PNNI	Private Network to Network Interface
PVC	Permanent Virtual Channel
SA	Security Agent
SKE	Session Key Exchange
UNI	User to Network Interface
VBR	Variable Bit Rate

2 Normative Notes for Secure CBR Traffic in a Policed Network

2.1 Separate Policing Fully Supported

Where separate policing of OAM and User traffic is supported throughout the network,the OAM Traffic Descriptor IE may be used as described below:

- The initiating Security Agent (SA) should look for the presence of the OAM Traffic Descriptor IE. If the IE is not present, the SA should generate the IE and append it to the SETUP message. If the IE is present, in support of nesting, the initiating SA should verify the values and pass the IE. The values shall be set as follows:
    1. The Shaping Indicator shall be set to '0 0' (no user specified requirement on shaping by the network, if shaping is applied by the network),
    2. The Compliance Indicator shall be set to '0' (the use of end-to-end OAM F5 flow is optional),
    3. The User-network fault management indicator may have any valid value
    4. The Forward end-to-end OAM flow indicator shall be set to a value other than '0 0 0' (0% of the forward cell rate specified by the ATM traffic descriptor information element),
    5. Backward end-to-end OAM flow indicator shall be set to a value other than '0 0 0' (0% of the backward cell rate specified by the ATM traffic descriptor information element).
- In order to accommodate nesting, the responding SA shall verify the presence of the IE and pass it on unmodified.
- If the OAM Traffic Descriptor IE in the CONNECT message is missing (e.g., the end user did not include the IE in the CONNECT message), the responding SA must insert the OAM Traffic Descriptor IE in the CONNECT message.
- The SA that originally inserted the IE into the SETUP message shall remove the IE from the corresponding CONNECT message.
- If PVCs are being used, the OAM bandwidth requirement shall be configured at provisioning.

If the OAM Traffic Descriptor IE is being used for both security OAM cells and another F5 OAM application, then it is indeterminable by the originator whether this other F5 OAM application is supported end-to-end. This case is beyond the scope of this document.

2.2 Separate Policing Not Fully Supported

In environments where separate policing of the User OAM cells from the user traffic is not supported (e.g. where the OAM Traffic Descriptor IE is not supported or where earlier versions of UNI and PNNI may be encountered) there are four mechanisms known to maintain synchronization on the link. Each, however, has limitations and should be tried only after establishing that separate policing is not fully supported.

- Shaping: A shaping element inserted between the SA and the policing switch can be configured to make the combined user and OAM traffic conform to the CBR contract. The SA needs to determine whether the current contract is sufficient to support both user and OAM traffic and if not adjust the contract accordingly. Note that this introduces both cell delay and cell delay variation to the user's data.
- Increased Traffic Rate: If the user's contracted bandwidth is sufficiently higher than the user's required bandwidth, then any OAM insertions may be within the tolerances of the policing function. This, however, is dependent on each vendor's implementation of the policing function and cannot be guaranteed. Note that in determining the additional bandwidth required, one must consider both the bandwidth needed for the inserted OAM cells and the cell delay variation specified in the contract. This may require at least twice the bandwidth of the user's traffic.
- Use AAL5: If AAL5 traffic can be exclusively used, then cryptographic synchronization for counter mode is also maintained through the use of the End Of Message indication within the cell header. The Linear Feedback Shift Register processing (Sec 1.1 Section 6.4.6.1.2 [1]) in AAL5 is reset on the receipt of the End Of Message. Thus

AAL5 traffic should introduce less resynchronization OAM traffic. This, however, does not solve the case of Session Key Exchange (SKE where OAM cells are still required. Failure or incorrect use of SKE would also result in loss of synchronization or reuse of old key stream.

- Change Traffic Type to VBR: Because switches anticipate bursting within VBR traffic, changing the user's traffic contract request to VBR, with the appropriate traffic parameters, may accommodate OAM cell insertion. If the security device changes the contract request, then the data originator loses control over the choice of traffic type. In addition, both cell delay and cell delay variation will be increased throughout the network.
- Use Electronic CodeBook (ECB) or Cipher Block Chaining (CBC): ECB and CBC modes of encryption do not use resynchronization cells. While this eliminates the need for synchronization cells, SKE still requires OAM cells. As mentioned above, failure or incorrect use of SKE would also result in loss of synchronization or reuse of old key stream. In addition, neither of these solutions scales to high data rates.