SAND95-0666C
Revised

ATM Forum Technical Committee
ATM Forum/95-0461R1

****

TITLE: Proposed DSS-Specific Fields for the Generic Authentication Information Element

****

SOURCE: Thomas D. Tarman
Sandia National Laboratories*
P.O. Box 5800
Albuquerque, NM 87185-0777
Phone: (505)844-4975
Fax: (505)844-9641
E-mail: tdtarma@sandia.gov

* This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000

****

DATE: August 6, 1995

****

DISTRIBUTION: Security Ad-Hoc WG, PLEN, SIG

****

ABSTRACT:

This contribution proposes the format of the "Algorithm-Specific Information" and "Signature" fields within the "Proposed Generic Authentication Information Element" for authentication IEs based on the Digital Signature Standard (DSS). These fields are designed to allow various levels of authentication "strength" (or robustness), and many of these fields may be omitted in systems that optimize authentication performance by sharing common (public) Digital Signature Algorithm (DSA) parameters. This allows users and site security officers to design their authenticated signaling according to site security and performance requirements.

****

Notice:

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

****

I. Introduction

This contribution proposes the "Algorithm-Specific Information" and "Signature" fields for a Generic Authentication Information Element [1] which uses the Digital Signature Standard (DSS). The Digital Signature Standard, which was developed by the United States National Institute of Standards and Technology (NIST), uses the Digital Signature Algorithm (DSA) to ensure the integrity and authenticity of electronic transactions. The DSA uses a hash value of the message (computed using the Secure Hash Algorithm), the signer's private key, and a cryptographic algorithm to generate the digital signature. When used with the Generic Authentication Information Element, the integrity and authenticity of signaling messages can be validated with confidence by another party.

II. Requirements

Currently, the DSS specifies that the DSA modulus be 512 bits in length [3]. However, several cryptanalysts have criticized this specification on the basis that this modulus, and associated parameters, are not large enough [2]. Conversely, for some applications, a 512 bit modulus may be too large. To support various levels of robustness (i.e. cryptographic strength), the DSS fields must meet the following requirement:

1. DSS-specific parameters and signature values should be variable length

The DSA uses a number of public parameters to generate and validate signatures. To minimize the time required to generate and validate signatures, these parameters, as well as the hash function identification, may be distributed beforehand to entities that are involved in these processes. Therefore, as an optimization, the following is also required:

2. Public DSA parameters may be omitted from the Authentication IE

III. DSS-Specific Information

The following diagram shows the DSS-specific format of the "Algorithm-Specific Information" field of the Generic Authentication IE. Each of these fields are optional (see requirement 2).

```
|-----------------------------------------------|
|  8  |  7  |  6  |  5  |  4  |  3  |  2  |  1  |
|===============================================|
|               P Parameter ID *                |
|-----------------------------------------------|
|                  P Length *                   |
|-----------------------------------------------|
|                      P *                      |
|                       .                       |
|                       .                       |
|                       .                       |
|-----------------------------------------------|
|               Q Parameter ID *                |
|-----------------------------------------------|
|                  Q Length *                   |
|-----------------------------------------------|
|                      Q *                      |
|                       .                       |
|                       .                       |
|                       .                       |
|-----------------------------------------------|
|               G Parameter ID *                |
|-----------------------------------------------|
|                  G Length *                   |
|-----------------------------------------------|
|                      G *                      |
|                       .                       |
|                       .                       |
|                       .                       |
|-----------------------------------------------|
|               Y Parameter ID *                |
|-----------------------------------------------|
|                  Y Length *                   |
|-----------------------------------------------|
|                      Y *                      |
|                       .                       |
|                       .                       |
|                       .                       |
|-----------------------------------------------|
```

* Optional parameter

IV. DSS Information Fields

A. P Parameter ID

This field identifies the following parameter as the P parameter. The P parameter is a public parameter which is the prime modulus used by DSA [3].

B. P Length

This field contains the length of the P (see requirement 1).

C. P

This field contains the P parameter described above.

D. Q Parameter ID

This field identifies the following parameter as the Q parameter. The Q parameter is a public parameter which is the prime divisor used by the DSA [3].

E. Q Length

This field contains the length of the Q (see requirement 1).

F. Q

This field contains the Q parameter described above.

G. G Parameter ID

This field identifies the following parameter as the G parameter. The G parameter is a public parameter used by the DSA [3].

H. G Length

This field contains the length of the G (see requirement 1).

I. G

This field contains the G parameter described above.

J. Y Parameter ID

This field identifies the following parameter as the Y parameter, or the "public key" [3].

K. Y Length

This field contains the length of the Y (see requirement 1).

L. Y

This field contains the public key described above.

V. DSS Signature

The following diagram shows the DSS-specific format of the "Signature" field of the Generic Authentication IE. All of these fields are required.

```
|-----------------------------------------------|
|  8  |  7  |  6  |  5  |  4  |  3  |  2  |  1  |
|===============================================|
|                R Parameter ID                 |
|-----------------------------------------------|
|                   R Length                    |
|-----------------------------------------------|
|                      R                        |
|                      .                        |
|                      .                        |
|                      .                        |
|-----------------------------------------------|
|                S Parameter ID                 |
|-----------------------------------------------|
|                   S Length                    |
|-----------------------------------------------|
|                      S                        |
|                      .                        |
|                      .                        |
|                      .                        |
|-----------------------------------------------|
```

VI. DSS Signature Fields

A. R Parameter ID

This field identifies the following parameter as the R parameter, one of two components of the DSS digital signature [3].

B. R Length

This field contains the length of the R parameter (see requirement 1).

C. R

This field contains the digital signature component described above.

D. S Parameter ID

This field identifies the following parameter as the S parameter, the second component of the DSS digital signature [3].

E. S Length

This field contains the length of the S (see requirement 1).

F. S

This field contains the digital signature component described above.

VII. Performance Issues

The DSA algorithm is slow, particularly for signature validation. However, prior information can be used to optimize its signature generation and validation performance. The greatest performance improvement can be realized when all authenticating entities in an ATM network use common values of the P, Q, and G parameters. This allows a one-time initialization to be used over all subsequent signature generation/validation operations.

If, by chance, another authenticating entity uses different values of P, Q, and G, then the entity which validates the signature will need to initialize another signature generator/validator with these values. This optimization still allows generation and validation of signatures with different parameters, however, this will slow authentication operations considerably.

VIII. Summary

This contribution describes the proposed contents of the "Algorithm-Specific Information" and "Signature" fields of the "Proposed Generic Authentication Information Element" defined in [1]. Variable-length fields are specified here to allow DSA parameters to be sized according to the user's desired level of authentication "strength". Since many of the "public" parameters may be omitted in systems that share these parameters (for optimization purposes), many of the DSA parameters listed here may be omitted from authenticated signaling messages as well.

IX. References

[1] Tom Tarman, Sandia National Laboratories, A Proposed Generic Authentication Information Element, ATM Forum/95-0460R1, August 6, 1995.

[2] Schneier, *Applied Cryptography*, John Wiley and Sons, Inc., 1994.

[3] NIST, *Digital Signature Standard (DSS)*, FIPS PUB 186, May 19, 1994.

[4] The ATM Forum Technical Committee, *User-Network Interface (UNI) Specification*, Version 3.1, September, 1994.

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.