ATNP WG3
WP 1408

Aeronautical Telecommunication Network Panel (ATNP)
Applications and Upper Layer Work Group (WG3)

Bordeaux, France
29 September – 2 October, 1998

Selection of ATN cryptographic algorithm

Prepared by WG1SG2
Presented by Michael Bigelow Chair, WG1SG2

Summary

Currently, the responsibility for the selection of the cryptographic algorithm to be used in the ATN is assigned to WG3SG3. Considering the potential system implications of the selection, WG1SG2 has reconsidered that assignment and wishes to take that responsibility and undertake the attendant work.

Selection of ATN cryptographic algorithm

1 Introduction

During the division of work associated with the inclusion of security into the ATN, the responsibility for the selection of the cryptographic algorithm to be used in the ATN was allocated to WG3. WG1SG2 understands this has been delegated to WG3SG3 but that no work has been done on this to-date.

2 Problem statement

A necessary part of the establishment of the asymmetric (Public Key) cryptographic framework for the ATN is the selection of an appropriate algorithm. This algorithm has considerable potential effect on the operation of the ATN due to such things as processing overhead and signature length (and attendant communications overhead). WG1SG2 has reconsidered the proposal that this work be done by WG3 and is prepared to undertake the work on its own.

3 Recommendation

WG1SG2 requests that

1. WG1 consider the information provided above and coordinate with WG3 to inform them that WG1SG2 will be conducting the investigation and selection of the specific cryptographic algorithm to be used within ATN.

2. WG1 perform a call for input and recommendations on specific algorithms to be considered for use in the ATN based on the following text.

> WG1SG2 is conducting investigation into the most suitable algorithm for use in the ATN Public Key Infrastructure. WG1SG2 requests input in the form of working papers which evaluate various alternative algorithms and make recommendations. WG1SG2 has established the following as base criteria to be used for the selection of the Public Key Algorithm for use in the ATN.
>
> Criteria which must be met. (Required)
>
> 1. Anticipated useful life of at least 10 years.
> 2. Key length of at least 1024 bits
> 3. Implementable in software as well as hardware. Runs sufficiently fast in software.
> 4. A published algorithm (e.g. DES, IDEA, RSA)
> 5. Minimized message size overhead, as compared to alternative algorithms. The resultant overhead must be less than 128 bits with 32-64 bits preferred for air-ground applications.
> 6. Relatively fast, as compared to alternative algorithms. This should be less than 100ms to sign or verify.
>
> Criteria which are nice but not required.
>
> 1. Unencumbered by patent by year 2005.
> 2. Well known. In commercial use for two or more years. (Exposure to cracking attempts)