3GPP TSG SA WG3 Security — S3#28 **S3-030255**
6 - 9 May 2003
Berlin, Germany

Title: **IEEE 802.11i Requirements**

Source: **Intel**

Agenda item: **7.11**
Document for: **[Discussion]**

IEEE 802.11i Requirements – Email Discussion Results

At the SA3#27, Intel was asked to lead the Email Discussion on the 802.11i Security Requirements. As there was virtually no discussion that took place on the list, the input material that was submitted for discussion is attached for informational purposes.

IEEE 802.11i Requirements Summary

The following requirements pertinent to 3GPP were identified in the the input material.

EAP Methods and Credentials

The IEEE 802.11i draft specification requires that one or more published, reviewed EAP methods are available which

- Support the following credentials: SIM and USIM
- Generate keying material
- Support mutual authentication
- Are resistant to dictionary attacks, and
- Provide protection against man-in-the-middle attacks.

It is desirable that the EAP methods have the following attributes

- Support fast resume
- Support end-user identity hiding

Key Strength Requirements

The EAP method must be capable of generating keying material with 128-bits of effective key strength. Key material must be at least 256 bits in length.

IEEE P802.11
Input to IETF EAP Working Group

Date: March 14th, 2003

Author: Dorothy Stanley
Agere Systems
2000 North Naperville Rd, Naperville, IL 60566
Phone: 1-630-979-1572
Fax:
e-Mail: dstanley@agere.com

Abstract

The IETF EAP working group has requested additional input on EAP method/credentials, and key strength requirements. This document contains the 802.11i response to the WG request.

Motion: Move to request Stuart Kerry, Chair of 802.11 to send the following letter to Harald Alvestrand, Chairman IETF, IESG.

From: Stuart Kerry, Chairman IEEE 802.11
To: Harald Alvestrand, Chairman IETF, IESG
Title: Input to IETF EAP Working Group on Methods and Key Strength
Purpose: For Information

Dear Harald,

We thank the IETF and the EAP WG for its ongoing work supporting the specification of EAP methods, EAP keying, and RADIUS keying attributes.

The purpose of this letter is to provide the EAP WG with additional input on (a) the EAP methods and credentials that are important to IEEE 802.11 wireless LAN deployments, and (b) IEEE 802.11i EAP Key Strength requirements.

EAP Methods and Credentials

Deployments of IEEE 802.11 WLANs today use several EAP methods, including EAP-TLS, EAP-TTLS, PEAP and EAP-SIM. These methods support authentication credentials that include digital certificates, usernames and passwords, secure tokens, and SIM secrets.

The IEEE 802.11i draft specification requires that one or more published, reviewed EAP methods are available which

- Support the following credentials: digital certificates, user-names and passwords, existing secure tokens, and mobile network credentials (GSM and UMTS secrets).
- Generate keying material
- Support mutual authentication
- Are resistant to dictionary attacks, and
- Provide protection against man-in-the-middle attacks.

It is desirable that the EAP methods have the following attributes

- Support fast resume
- Support end-user identity hiding
- Support for public/private key (without necessarily requiring certificates)
- Provide asymmetric credential support (password on one side, public/private key on the other), and
- Protect legacy credentials, such as passwords, from direct attack.

The current mandatory-to-implement EAP method is EAP-MD5. EAP-MD5 does not meet IEEE 802.11's requirements. We request that the mandatory to implement EAP methods be augmented to include one of the methods that IEEE 802.11 is able to use.

Key Strength Requirements

IEEE 802.11i RSN networks will use IEEE 802.1X and EAP methods to implement end user authentication, and require that these EAP methods provide keying material. The IEEE 802.11i requirement is that

> The EAP method must be capable of generating keying material with 128-bits of effective key strength. Key material must be at least 256 bits in length.

Please contact Stuart Kerry, IEEE 802.11 Working Group Chair and David Halasz, IEEE 802.11i Task Group Chair dhala@cisco.com with any questions, and to discuss IETF follow-up.

Stuart Kerry