3GPP TSG SA WG3 (Security) #16 **S3-000731**

Sophia Antipolis, France, 28 - 30 November 2000

Agenda Item: 10.7

Source: Mitsubishi Electric, NTT DoCoMo

Title: Encryption Algorithms for MAP Security

Document for: Discussion and Decision

1 Introduction

Ericsson has presented a preliminary analysis of the suitable algorithms to be used for MAP Application Layer Security and proposed encryption and MAC algorithms in Tdoc S3-000674.

This proposal recommends to include two more encryption algorithms, **MISTY1** and **Camellia**.

2 Candidate Algorithms

2.1 MISTY1

MISTY1 is a 64-bit block cipher with a 128-bit key and **IPR free**. KASUMI is a variant algorithm of MISTY1. Recently MISTY1 has become an **RFC** of **IETF**.

On the other hand, MISTY1 has been proposed to ISO standard encryption algorithms[1], NESSIE project[2] and CRYPTOREC project[3]. MISTY1 is a strong candidate for all of them.

2.2 Camellia

Camellia is a block cipher with a variable block length (128, 192 or 256 bits) and key length (128, 192, or 256 bits), i.e. has the **same interface as AES**. Camellia has been jointly developed by NTT (the parent company of NTT DoCoMo) and Mitsubishi Electric including the designer of MISTY1 and KASUMI. Camellia is **IPR free** and an **Internet Draft** on **IETF** has been published.

Camellia also has been proposed to ISO standard encryption algorithms, NESSIE project and CRYPTOREC project. Camellia is a strong candidate for all of them.

For more details of Camellia, refer to http://www.security.melco.co.jp .

3 Recommendation

Mitsubishi Electric and NTT DoCoMo propose MISTY1 and Camellia as (optional) encryption algorithms for MAP Security.

---

1 ISO/IEC 18033: Encryption Algorithms. Standardisation will be completed in 2002.

2 European encryption standards including block cipher, stream cipher, public key cipher, hash function, etc. Standardisation will be completed in 2002.

3 Encryption standards for Japanese government including block cipher, stream cipher, public key cipher, hash function, etc. The result of evaluations will be published in March 2001.

The following table lists the algorithms currently recommended to be supported in MAP Security implementations:

Encryption Algorithms	MAC Algorithms
AES-Rijndael (Mandatory)	SHA-1 (Mandatory)
Twofish (Optional)	MD5 (Optional)
Blowfish (Optional)	
MISTY1 (Optional)	
Camellia (Optional)	