Document : ISO/IEC WAPI N 33

Date : 2005-08-18

TITLE :	WAPI and Cipher issue - CNB contribution for the Beijing meeting, 8-12 August
SOURCE :	CNB
REQUESTED ACTION :	For information
DISTRIBUTION :	

WAPI and Cipher issue

Chinese National Body

Date: 2005-08-06

Notice: This document is prepared for presentation at the Beijing meeting August 8-12, 2005. It is the basis for discussion. The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

Foreword

This document makes some discussions on the cipher issue in WAPI.

Agenda

- The historical background of ISO's encryption policies
- The working range and key area of JTC1/SC27
- The common regulation of cipher algorithm in ISO9160-1988
- The description of cipher algorithm in ISO18033
- The disposition of cipher algorithm in WAPI

The historical background of ISO’s encryption policies (1)

- **encryption standardization is a political issue**

--Since the foundation of SC20 in 1984, it has been in charge of the international encryption standardization. As a standard with priority, the US algorithm DES was named as DEA-1. And the DEA-2 was the public-key algorithm RSA.

--DES was propelled to DIS in January,1985. But great change happened in the following year.

--In the summer of 1985, The US President announced that the US government would not support DES any more. And the NSA was appointed to design a new algorithm, but the detailed technology was nondisclosed. This made the public begin to doubt the security degree of DES.

--Some member NB originally oppose the international encryption standardization considered that which cipher algorithm to be adopted by a country was a sensitive issue, other countries had on right to intermeddle.

The historical background of ISO’s encryption policies (2)

--The divarication appeared in 1986□but majority still agreed to propel DES to IS, and submit it to TC97.

--In May□1986,TC97 annual meeting produced a resolution: the international encryption standardization was not a technical issue, but a political issue.

- ISO decides not to study encryption standardization

--In october,1986□ISO decided to withdraw this project, and withdraw the encryption standardization from the working range of SC20. Furthermore,ISO clearly wrote down that not to study encryption standardization

The working range and key area of JTC1/SC27 (1)

----JTC1/SC27 is in charge of Information technology-Security techniques

1. JTC 1/SC 27 Statement of Scope

Standardization of generic methods and techniques for IT security. This includes:

- **identification of generic requirements (including requirements methodology) for IT system security services,**
- **development of security techniques and mechanisms (including registration procedures and relationships of security components),**
- **development of security guidelines (e.g., interpretative documents, risk analysis), and**
- **development of management support documentation and standards (e.g., terminology and security evaluation criteria).**

Excluded is the embedding of mechanisms in applications.

The working range and key area of JTC1/SC27 (2)

Note*: that* ***the SC 27 Scope and Area of Work includes the standardization of cryptographic algorithms for integrity, authentication and non-repudiation services****. Furthermore it includes the standardization of cryptographic algorithms for confidentiality services for use in accordance with internationally accepted policies.*

The working range and key area of JTC1/SC27 (3)

2 Work Program Priorities

– Priorities of Working Group 1 include the timely revision of ISO/IEC 17799: *Code of practice for information security management* (project 1.27.37), successful completion of the multipart standard on *Network Security* (project 1.27.28), and work on the new multipart standard entitled *Management of information and communications technology (ICT) security (MICTS)* which will eventually replace ISO/IEC 13335: *Guidelines for the management of IT Security*, Parts 1, 2 and 3 (project 1.27.14).

The working range and key area of JTC1/SC27 (4)

– For Working Group 2, priorities for the next work period include the successful completion of the WG 2 projects mentioned in section 3.1. In addition, WG 2.s role in the cooperation with TC 68 is of strategic importance.

The working range and key area of JTC1/SC27 (5)

– Priority for Working Group 3 is to ensure the timely alignment of security evaluation related standards and projects (IS 15408: *Evaluation Criteria for IT Security*, IS 15292: *Protection Profile registration procedures*, ISO/IEC 18045: *Methodology for IT Security Evaluation*, and ISO/IEC 15446: *Guide for the production of Protection Profiles and Security Targets*). In order to achieve consistence between the different standards, the anticipated upcoming revision of 15408 will need to converge with the end results of the on-going projects. In context of project 19792: *A framework for security evaluation and testing of biometric technology*, a strong liaison with SC 37 is considered to be of vital importance.

The working range and key area of JTC1/SC27 (6)

Comment□

encryption technology is one of the Information technology-Security techniques, which is within the working range and key area of SC27. However, SC27 does not require a fixed cipher algorithm.

The common regulation of cipher algorithm in ISO 9160-1988

Source: ISO 9160-1988, title “Information processing-Data encipherment- Physical layer interoperability requirements”

common regulation:

When using this standard to cooperate the DEEs with each other, the cooperated DEEs are required to have:

a. same cipher algorithm□

b. same secret key value□

c. same IV length, IV configuration, same IV transfer sequence by bit.

This standard does not regulate determinate cipher algorithm□but requires any adopted cipher algorithm use a single bit or byte as process unit to fit the physical layer services.

In this standard, Annex B gives an example of encryption application, but does not give any requirement of cipher algorithm.

The description of cipher algorithm in ISO 18033 (1)

ISO18033-1~4 is a active international standard□regarding Information technology-Security techniques-Encryption algorithms.

– **<u>18033 allows option on ciphers</u>**

“1 Scope

This part of ISO/IEC 18033 specifies several asymmetric ciphers. These specifications prescribe functional interfaces and correct methods of use of such ciphers in general, as well as functionality and ciphertext format for several specific asymmetric ciphers (although conforming systems may choose to use alternative formats for storing and transmitting cipher-texts). ”

The description of cipher algorithm in ISO 18033 (2)

– **18033 objective is to promote their use, Not Mandatory**

“Introduction

ISO/IEC 18033 is a multi-part International Standard that specifies encryption systems (ciphers) for the purpose of data confidentiality. The inclusion of ciphers in ISO/IEC 18033 is intended to promote their use as reflecting the current ‘state of the art’ in encryption techniques. ”

The disposition of cipher algorithm in WAPI (1)

1 **ISO’s tradition in cipher algorithm specification□**

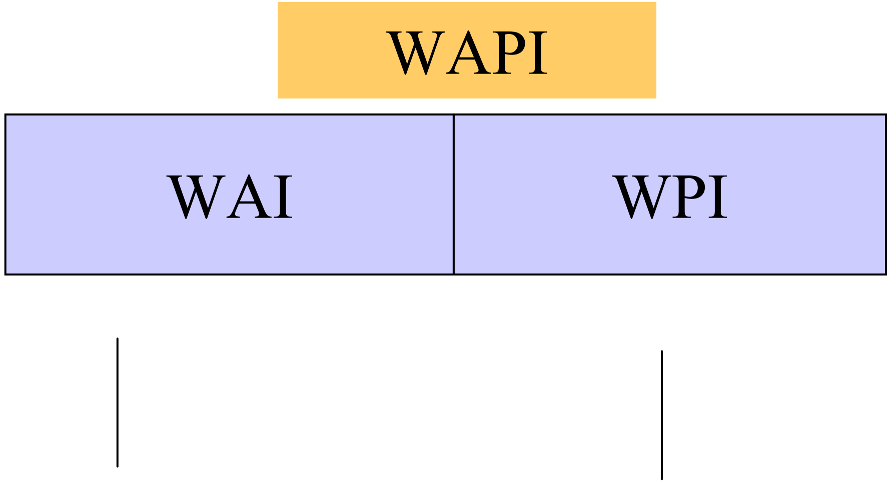
----ISO has no regulation of encryption standardization□

----ISO does not require a fixed cipher algorithm;

----ISO only require the description of the essential characters of cipher algorithm□

----Referring the specification of cipher algorithm in ISO9160□ WAPI proposal accord with the ISO’s tradition in cipher algorithm specification.

The disposition of cipher algorithm in WAPI (2)



WAPI

WAI

WPI

Each is a security protocol, which can use any secure algorithm.

Algorithms:

ECDSA
ECDH
SHA256

Algorithm

Optional --- SMS4, in China
--- Others, can choose from
AES, TWOFISH, SEED, etc.

The disposition of cipher algorithm in WAPI (3)

2 WAPI proposal:

----Respect the regulations regarding cipher algorithm of each country;

----Respect the attentions regarding information security of each country;

----Every country can choose the appropriate cipher algorithm according to the particular occasion and requirement.

3 In the algorithms adopted in WAPI:

----ECC related algorithms use ECDH and ECDSA ;

----HASH uses SHA-256□which is widely used by the international community□

----The choice and design of block cipher algorithm depends on the particular occasion and requirement in different countries and regions.

Conclusion

WAPI defines the interface of cipher algorithm according to the ISO’s common regulation of cipher algorithm