ISO SC 27 – ETSI Security Workshop
Session 1: Security Mechanisms

ISO/IEC JTC 1/SC 27/WG 2

26 April 2013

Takeshi Chikazawa
SC 27/WG 2 Convenor
t-chika@ipa.go.jp

WG 2 Mission

- SC 27/WG 2 "**Cryptography and Security Mechanisms**"
- The Terms of Reference:
    - o Identify the need and requirements for these techniques and mechanisms in IT systems and applications; and
    - o Develop terminology, general models and standards for these techniques and mechanisms for use in security services.

WG 2 Mission

- The scope covers both cryptographic and non-cryptographic techniques and mechanisms including;
  - **Confidentiality**;
  - **Entity authentication**;
  - **Non-repudiation**;
  - **Key management**; and
  - **Data integrity** such as
    - Message authentication,
    - Hash-functions, and
    - Digital signatures.

WG 2 Standards

Standard	Title	Status	Abstract
ISO/IEC 18033-1	**Encryption algorithms** Part 1: General	1st ed. 2005 Under revision	ISO/IEC 18033 specifies asymmetric ciphers (including identity-based ciphers) and symmetric ciphers (block ciphers and stream ciphers).
-2	Part 2: Asymmetric ciphers	1st ed. 2006	
-3	Part 3: Block ciphers	2nd ed. 2010	
-4	Part 4: Stream ciphers	2nd ed. 2011	
-5	Part 4: Identity-based ciphers	Under development	
ISO/IEC 29192-1	**Lightweight cryptography** Part 1: General	1st ed. 2012	ISO/IEC 29192specifies symmetric ciphers (block ciphers and stream ciphers) and mechanisms using asymmetric techniques (authentication, key exchange and identity-based signature) which are suitable for lightweight cryptographic applications.
-2	Part 2: Block ciphers	1st ed. 2012	
-3	Part 3: Stream ciphers	1st ed. 2012	
-4	Part 4: Mechanisms using asymmetric techniques	Under development	
ISO/IEC 19772	**Authenticated encryption**	1st ed. 2009	ISO/IEC 19772 specifies methods for authenticated encryption, i.e., defined ways of processing a data string for data confidentiality, data integrity and data origin authentication.
ISO/IEC 29150	**Signcryption**	1st ed. 2011	ISO/IEC 29150 specifies mechanisms for signcryption that employ public key cryptographic techniques requiring both the originator and the recipient of protected data to their own public and private key pairs.
ISO/IEC 10116	**Modes of operation for an n-bit block cipher algorithm**	3rd ed. 2006	ISO/IEC 10116 specifies modes of operation for a block cipher algorithm, i.e., ECB, CBC, OFB, CFB and CTR.
ISO/IEC 10118-1	**Hash-functions** Part 1: General	2nd ed. 2000 Under revision	ISO/IEC 10118 specifies some kinds of hash-functions which map arbitrary strings of bits to a given range.
-2	Part 2: Hash-functions using an n-bit block cipher	3rd ed. 2010	
-3	Part 3: Dedicated hash-functions	3rd ed. 2006 (+Amd1)	
-4	Part 4: Hash-functions using modular arithmetic	1st ed. 1998	
ISO/IEC 15946-1	**Cryptographic techniques based on elliptic curves** Part 1: General	2nd ed. 2008	ISO/IEC 15946 describes the mathematical background and general techniques in addition to the elliptic curve generation techniques.
-5	Part 5: Elliptic curve generation	1st ed. 2009	

WG 2 Standards

Standard	Title	Status	Abstract
ISO/IEC 9796-2	**Digital signature schemes giving message recovery** Part 2: Integer factorization based mechanisms	3rd ed. 2010	ISO/IEC 9796-2 specifies digital signature mechanisms giving partial or total message recovery aiming at reducing storage and transmission overhead.
-3	Part 3: Discrete logarithm based mechanisms	2nd ed. 2006	
ISO/IEC 14888-1	**Digital signatures with appendix** Part 1: General	2nd ed. 2008	ISO/IEC 14888 specifies digital signature mechanisms with appendix.
-2	Part 2: Integer factorization based mechanisms	2nd ed. 2008	
-3	Part 3: Discrete logarithm based mechanisms	2nd ed. 2006 (+Amd2)	
ISO/IEC 20008-1	**Anonymous digital signatures** Part 1: General	Under development	ISO/IEC 20008 specifies anonymous digital signature mechanisms, in which a verifier makes use of a group public key to verify a digital signature.
-2	Part 2: Mechanisms using a group public key	Under development	
ISO/IEC 18370-1	**Blind digital signatures** Part 1: General	Under development	ISO/IEC 18370 specifies blind digital signature mechanisms which allow a recipient to obtain a signature without giving signer any information about the actual message or resulting signature.
-2	Part 2: Discrete logarithm based mechanisms	Under development	
ISO/IEC 9798-1	**Entity authentication** Part 1: General	3rd ed. 2010	ISO/IEC 9798 specifies several kinds of entity authentication mechanisms that an entity to be authenticated proves its identity by showing its knowledge of a secret.
-2	Part 2: Mechanisms using symmetric encipherment algorithms	3rd ed. 2008	
-3	Part 3: Mechanisms using digital signature techniques	2nd ed. 1998 (+Amd1)	
-4	Part 4: Mechanisms using cryptographic check function	2nd ed. 1999	
-5	Part 5: Mechanisms using zero knowledge techniques	3rd ed. 2009	
-6	Part 6: Mechanisms using manual data transfer	2nd ed. 2010	
ISO/IEC 20009-1	**Anonymous entity authentication** Part 1: General	Under development	ISO/IEC 20009 specifies anonymous entity authentication mechanisms in which a verifier makes use of a group signature scheme to authenticate the entity with which it is communicating, without knowing this entity's identity.
-2	Part 2: Mechanisms based on signatures using a group public key	Under development	
-3	Part 3: Mechanisms based on blind signatures	Under development	

WG 2 Standards

Standard	Title	Status	Abstract
ISO/IEC 9797-1	**Message authentication codes (MACs)** Part 1: Mechanisms using a block cipher	2nd ed. 2011	ISO/IEC 9797 specifies message authentication code (MAC) algorithms, which are data integrity mechanisms that compute a short string.
-2	Part 2: Mechanisms using a dedicated hash-function	2nd ed. 2011	
-3	Part 3: Mechanisms using a universal hash-function	1st ed. 2011	
ISO/IEC 7064	**Check character systems**	1st ed. 2003	ISO/IEC 7064 specifies a set of check character systems capable of protecting strings against errors.
ISO/IEC 11770-1	**Key management** Part 1: Framework	2nd ed. 2010	ISO/IEC 11770 describes general models on which key management mechanisms are based, defines the basic concepts of key management, and defines several kinds of key establishment mechanisms .
-2	Part 2: Mechanisms using symmetric techniques	2nd ed. 2008	
-3	Part 3: Mechanisms using asymmetric techniques	2nd ed. 2008 Under revision	
-4	Part 4: Mechanisms based on weak secrets	1st ed. 2006	
-5	Part 5: Group key management	1st ed. 2011	
ISO/IEC 13888-1	**Non-repudiation** Part 1: General	3rd ed. 2009	ISO/IEC 13888 specifies for the provision of non-repudiation services. The goal of the non-repudiation service is to generate, collect, maintain, make available and validate evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. The event or act on can be the generation of a message, sending of a message, receipt of a message, submission of a message transport of a message.
-2	Part 2: Mechanisms using symmetric techniques	2nd ed. 2010	
-3	Part 3: Mechanisms using asymmetric techniques	2nd ed. 2009	
ISO/IEC 18014-1	**Time-stamping services** Part 1: Framework	2nd ed. 2008	ISO/IEC 18014 defines time-stamping services that are provided using time-stamp tokens between the participating entities in addition to the traceability of time sources.
-2	Part 2: Mechanisms producing independent tokens	2nd ed. 2009	
-3	Part 3: Mechanisms producing linked tokens	2nd ed. 2009	
-4	Part 4: Traceability of time sources	Under development	
ISO/IEC 18031	**Random bit generation**	2nd ed. 2011	ISO/IEC 18031 specifies a conceptual model for a random bit generator for cryptographic purposes, together with the elements of this model.
ISO/IEC 18032	**Prime number generation**	1st ed. 2005	ISO/IEC 18032 presents methods for generating prime numbers as required in cryptographic protocols and algorithms.

Current topics

- Lightweighy cryptography
- Key derivation
- Study periods

Lightweight cryptography

- Part 1: General
- Part 2: Block ciphers
  - Present
  - CLEFIA
- Part 3: Stream ciphers
  - Enocoro-128v2, -80
  - Trivium

Lightweight cryptography

- Part 4: Mechanisms using asymmetric techniques (to be published soon)
  - cryptoGPS
  - ALIKE
  - IBS
- Part 5: Hash-functions (agreed to start the development)

Key derivation

- SC 27 has developed a multi-part standard "Key management," but no part for key derivation techniques.
- A liaison statement from ETSI triggered to study this techniques.
- WG 2 agreed to start a development work for key derivation at its meeting this week.
- Techniques using MAC functions and hash functions will de described.

Study Periods

- Homomorphic encyption algorithms
- Secret sharing
- Broadcast encryption

Collaboration with ETSI

- SC 27/WG 2 welcomes the experts participation and contribution from ETSI.

Thank you!