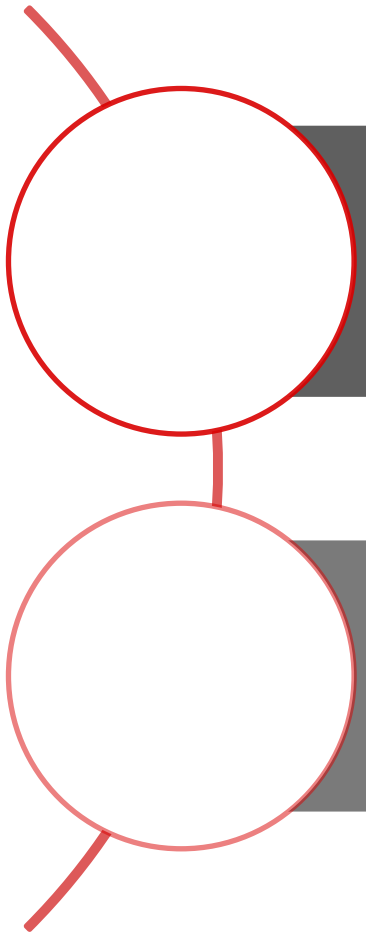
Chinese Commercial Cryptographic Scheme VS. ISO/IEC 19790

Di Li (di.li@atsec.com), atsec China

Agenda



Overview of Chinese Commercial Cryptographic Scheme

Comparison Between ISO/IEC 19790 and Chinese Scheme

OVERVIEW OF CHINESE COMMERCIAL CRYPTOGRAPHIC SCHEME

OSCCA and Commercial Cryptography

- What is “Commercial Cryptography” in China?
  - “Commercial Cryptography” is a set of algorithms and standards used in the commercial area, e.g. banks, telecommunications, third party payment gateways, enterprises, etc. …
  - In this area, only “Commercial Cryptography” certified products can be used.

- Issued and regulated by the Office of the State Commercial Cryptographic Administration (OSCCA)
  - Department of State Cryptography Administration (SCA)
- Products shall be tested by CST labs:
  - Only 2 domestic labs accredited by OSCCA
  - **NO** 3rd party testing lab accreditation mechanism.

OSCCA Certified Product List

- Only OSCCA certified products are allowed to be sold or used in China:
  - Used commercially, no state secrets involved
  - Used for encryption, protection, or security certification of information
  - As its core function, e.g. Hardware Security Module (HSM), smart card chip, Trusted Platform Module (TPM) chip, USB token ...
  - Implements Commercial Cryptographic algorithms (no limitation on standard algorithm)
  - No foreign encryption products can be legally sold or used in China

Published OSCCA Algorithms

- Published: SM2, SM3, SM4, SM9, ZUC
  - Open source portal: http://gmssl.org/

- GM/T 0003: SM2 (published in 2010):
  - Elliptic Curve Cryptography (ECC) based asymmetric algorithm, public key 512 bits and private key 256 bits (GM/T 0003.1)
  - Digital signature generation and verification (GM/T 0003.2)
  - Key establishment (together with SM3 and a KDF function defined in GM/T 0003.3)
  - Public key encryption (GM/T 0003.4)
  - Accepted by ISO standard: ISO/IEC 14888-3

Published OSCCA Algorithms

- GM/T 0004-2012: SM3 (published in 2010):
  - Hash functions
  - Max input: 2^64 bits
  - Output: 256 bits
  - Accepted by ISO standard: ISO/IEC 10118-3

- GM/T 0002-2012: SM4 (published in 2012):
  - Block cipher symmetric algorithm
  - Block size: 128 bits
  - Key length: 128 bits
  - Accepted by ISO standard: ISO/IEC 18033-3

Published OSCCA Algorithms

- GM/T 0044-2016: SM9 (published in 2016):
  - Identity-Based Asymmetric Cryptography Algorithm (GM/T 0044.1)
  - Digital signature generation and verification (GM/T 0044.2)
  - Key establishment and key wrapping (GM/T 0044.3)
  - Public key encryption (GM/T 0044.4)
  - ECC based asymmetric algorithm, similar to SM2
  - Public key is bind to user’s identity information
  - Accepted by ISO standard: ISO/IEC 14888-3

Published OSCCA Algorithms

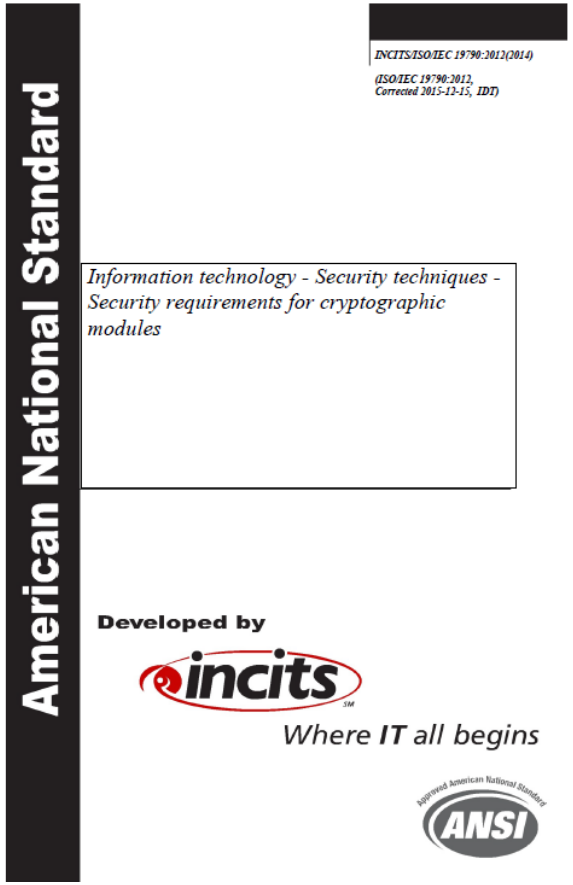
- GM/T 0001-2012: ZUC (published in 2012):
  - Stream cipher algorithm
  - Message encryption / decryption (GM/T 0001.2)
  - Message authentication check (GM/T 0001.3)
  - Key length: 128 bits
  - IV length: 128 bits
  - Proposal stage by ISO standard: ISO/IEC18033-4

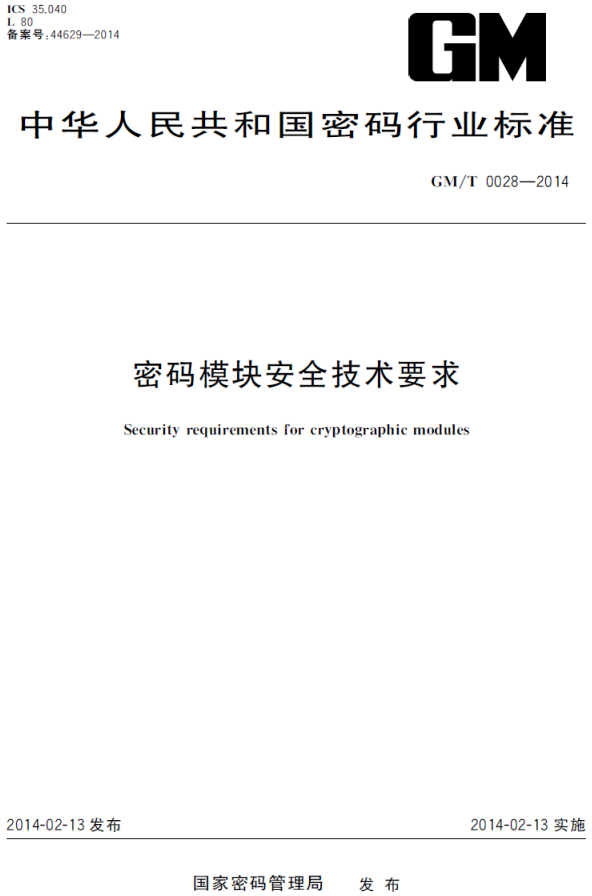
Published OSCCA Standards

- GM/T 0028-2014: Cryptographic Module Security Requirements
  - Not equivalent translation to ISO/IEC 19790: 2012 (no correction)
  - Updated version: GB/T 37092-2018 Information security technology—Security requirements for cryptographic modules

- GM/T 0039-2015: Cryptographic Module Security Testing Requirements
  - Not equivalent translation to ISO/IEC 24759: 2014

- Other published standards with GM/T (OSCCA standards) or GB/T (national standards), referenced in the annexes of the GM/T 0028





DIFFERENCES BETWEEN ISO/IEC 19790 AND GM/T 0028

Implementation Schedule of ISO/IEC 19790 in U.S.

Date	Action
March 22, 2019	FIPS 140-3 Approved
Mid-2019	Drafts of SP 800-140x available for public comment
September 22, 2019	FIPS 140-3 Effective Date •Publication of SP 800-140x documents •ISO Document request application available
March 22, 2020	CMVP program updates completed: •Update Pearson competency test •Implementation Guidance updates •Resolve applications Changes
September 22, 2020	FIPS 140-3 Testing Begins
September 22, 2021	FIPS 140-2 Testing Ends

Current Status of GM/T 0028

- **Published and implemented as Industrial Standard:**
  - February 13, 2014
  - Current referenced by OSCCA

- **Adopted as National Standard: GB/T 37092-2018**
  - Published on December 28, 2018
  - Implemented on July 1, 2019
  - Not referenced by OSCCA

- **First certified module on April 4, 2019: SJK1926, HSM card, L3.**
  - http://www.oscca.gov.cn/app-zxfw/xzspsx/symmcp.jsp?channel_code=c100135

Same Parts

- **Module types:**
  - Software, firmware, hardware, software-hybrid, firmware hybrid
- **Embodiments:**
  - Single chip, multi-chip embedded, multi-chip standalone
- **Security levels:**
  - Security level 1 to security level 4
- **Security requirements:**
  - 12 security requirements

1. General requirements
2. CM Specifications
3. CM Interfaces
4. Roles, services, and authentication
5. Software/firmware security
6. Operational environment
7. Physical security
8. Non-invasive security
9. SSP management
10. Self-tests
11. Life-cycle assurance
12. Mitigation of other attacks

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.1 General:**
  - 19790: The security requirements cover areas related to the design and implementation of a cryptographic module
  - 0028: The security requirements cover areas related to the design, implementation, **operation and decommission** of a cryptographic module

- **7.2.2 Types of cryptographic modules:**
  - 19790: For software modules executing in a modifiable environment, the physical security requirements found in 7.7 are optional and the applicable non-invasive security requirements in 7.8 shall apply
  - 0028: For software modules executing in a modifiable environment, the physical security requirements found in 7.7 and the non-invasive security requirements in 7.8 **are optional**.

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.2.2 Types of cryptographic modules:**
  - 19790: For hybrid modules, all applicable requirements of 7.5, 7.6, 7.7 and 7.8 shall apply
  - 0028: For hybrid modules, **software and firmware components** shall apply for all applicable requirements of 7.5, 7.6; **hardware components** shall apply for all applicable requirements of 7.7 and 7.8.

- **7.2.4.1 Modes of operations general requirements:**
  - 19790: A non-approved cryptographic algorithm or non-approved generated key may be used to obfuscate data or CSPs but the result is considered unprotected plaintext and provides no security relevant functionality until protected with an approved cryptographic algorithm
  - 0028: ~~**until protected with an approved cryptographic algorithm**~~

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.2.4.3 Degraded operation:**
  - 19790: A cryptographic module may be designed to support degraded functionality if the module enters the error state.
  - 0028: **NO degraded operation is allowed. (Please also note all the other requirements relate to degraded operation, e.g. 7.4.3.1)**

- **7.3.3 Definition of interfaces:**
  - 19790: The cryptographic module shall distinguish between data, control information, and power for input, and data, control information, status information, and power for output.
  - 0028: ~~**power for output**~~

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.3.4 Trusted channel for security level 3:**
  - 19790: the physical ports used for the trusted channel shall be physically separated from all other ports or the logical interfaces used for the trusted channel shall be logically separated from all other interfaces
  - 0028:
    - the physical ports used for the trusted channel shall be physically separated from all other ports
    - **and**
    - the logical interfaces used for the trusted channel shall be logically separated from all other interfaces

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.4.3.2 Bypass capability &**
- **7.4.3.3 Self-Initiated cryptographic output capability:**
  - 19790: No extra requirements for security level 4.
  - 0028: **For security level 4, two independent internal actions shall be performed by two independent operators to activate the capability.**

- **7.5 Software/Firmware security (security level 1):**
  - 19790: The expected referenced output of the integrity technique mechanism may be considered data and itself not subject to the integrity technique.
  - 0028: **NO such statement.**

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.5 Software/Firmware security (security level 1):**
  - 19790: A cryptographic mechanism using an approved integrity technique or an error detection code (EDC) shall be applied to all software and firmware components within the hardware module's defined cryptographic boundary or within disjoint hardware components of the hybrid module.
  - 0028: A cryptographic mechanism using an approved integrity technique **~~or an error detection code (EDC)~~** shall be applied to all software and firmware components within the hardware module's defined cryptographic boundary **~~or within disjoint hardware components of the hybrid module~~**.

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.5 Software/Firmware security (security level 1):**
  - 19790: If the software or firmware that is loaded is associated, bound, modifies or is an executable requisite of the validated module, then the software/firmware load test is applicable and shall be performed by the validated module with the following exceptions…
  - 0028: If the software or firmware that is loaded is associated, bound, modifies or is an executable requisite of the validated module, then the software/firmware load test is applicable and shall be performed by the validated module ~~**with the following exceptions.**~~ **NO exceptions are accepted.**

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.5 Software/Firmware security (security level 2, 3, and 4):**
  - 19790: For software and firmware modules and the software or firmware component of a hybrid module for Security Level 2 (except for the software and firmware components within a disjoint hardware component of a hybrid module): An approved digital signature or keyed message authentication code shall be applied to all software and firmware within the module's defined cryptographic boundary.
  - 0028: An approved digital signature or keyed message authentication code shall be applied to all software and firmware within the module's defined cryptographic boundary. **NO exception statement regarding the software and firmware components within a disjoint hardware component of a hybrid module.**

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.6.3 Operating system requirements for modifiable operational environments:**
  - 19790: No statement of modifiable operational environments under security level 3 and security level 4.
  - 0028: Clearly state **“This standard provides no requirements for modifiable operational environments under security level 3 and security level 4, thus modifiable operational environment cannot be certified under security level 3 and security level 4”.**

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.7.4.3 Environmental failure testing procedures:**
  - 19790: From a temperature within the normal operating temperature range to the highest (i.e. hottest) temperature that either (1) shuts down or goes into an error state or (2) zeroises all unprotected SSPs.
  - 0028: From a temperature within the normal operating temperature range to the highest (i.e. hottest) temperature that either (1) shuts down ~~**or goes into an error state**~~ or (2) zeroises all unprotected SSPs

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.8 Non-invasive security:**
  - 19790: This subclause is not applicable if the cryptographic module does not implement non-invasive attack mitigation techniques to protect the module's unprotected SSPs from non-invasive attacks referenced in Annex F.
  - 0028: ~~**This subclause is not applicable if the cryptographic module does not implement non-invasive attack mitigation techniques to protect the module's unprotected SSPs from non-invasive attacks referenced in Annex F.**~~ **Which means this chapter is always applicable.**

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.8 Non-invasive security at security level 3 and security level 4:**
  - 19790: The cryptographic module shall be tested to meet the approved non-invasive attack mitigation test metrics for Security Level 3 or Security Level 4 as referenced in Annex F.
  - 0028: **For Security Level 3, beside the above requirements, documents shall provide the proof of the effectiveness for each mitigation method, as well as the testing methods. For Security Level 4, the cryptographic module shall be tested to meet the requirements of national relevant departments regarding the mitigation of non-invasive security.**

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.9.1 SSP management general requirements:**
  - 19790: CSPs encrypted or obfuscated using non-approved security functions are considered unprotected plaintext within the scope of this International Standard.
  - 0028: CSPs encrypted ~~**or obfuscated**~~ using non-approved security functions are considered unprotected plaintext within the scope of this standard**.**

- **7.9.2 Random bit generators:**
  - 19790: No extra requirements on the length of entropy.
  - 0028: **No matter whether the entropy is collected internally or externally, the min-entropy shall be no less than 256 bits for any of the CSPs. If the entropy is collected internally, detailed design of random bit generator shall be provided.**

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.9.7 SSP zeroization:**
  - 19790: SSPs need not meet these zeroization requirements if they are used exclusively to reveal plaintext data to processes that are authentication proxies (e.g. a CSP that is a module initialization key).
  - 0028: **~~SSPs need not meet these zeroization requirements if they are used exclusively to reveal plaintext data to processes that are authentication proxies (e.g. a CSP that is a module initialization key).~~ Which means ALL unprotected SSPs shall be zeroized.**

Differences Between GM/T 0028 and ISO/IEC 19790

- **7.10.1 Self-test general requirements:**
  - 19790: All self-tests identified in underlying algorithmic standards (Annexes C through E) shall be implemented as applicable within the cryptographic module. All self-tests identified in addition or in lieu of those specified in the underlying algorithmic standards (Annexes C through E) shall be implemented as referenced in Annexes C through E for each approved security function, SSP establishment method and authentication mechanism.
  - 0028: All self-tests identified in underlying algorithmic standards (Annexes C through E) shall be implemented as applicable within the cryptographic module. ~~**All self-tests identified in addition or in lieu of those specified in the underlying algorithmic standards (Annexes C through E) shall be implemented as referenced in Annexes C through E for each approved security function, SSP establishment method and authentication mechanism.**~~

Annex C Approved Security Functions

	ISO/IEC 19790	GM/T 0028
Block ciphers	ISO/IEC 18033-3	GM/T 0002-2012: SM4 Algorithm GB/T 17964-2008: Modes of Block Cipher
Stream ciphers	ISO/IEC 18033-4	GM/T 0001-2012: ZUC Algorithm
Asymmetric algorithms and techniques	ISO/IEC 9796-2 ISO/IEC 9796-3 ISO/IEC 14888 ISO/IEC 15946 ISO/IEC 18033-2	GM/T 0003-2012: SM2 Algorithm GM/T 0009-2012: SM2 Usage Specification GM/T 0010-2012: SM2 Encrypted Signature Message Syntax Specification GM/T 0015-2012: SM2 Digital Certificate Format Specification
Message authentication codes	ISO/IEC 9797-2	Meet the requirements of OSCCA regarding message authentication code.

Annex C Approved Security Functions

	ISO/IEC 19790	GM/T 0028
Hash functions	ISO/IEC 10118-2 ISO/IEC 10118-3 ISO/IEC 10118-4	GM/T 0004-2014: SM3 Algorithm
Entity authentication	ISO/IEC 9798-2 ISO/IEC 9798-3 ISO/IEC 9798-4 ISO/IEC 9798-5 ISO/IEC 9798-6	GB/T 15843.2-2008: Mechanisms using symmetric encipherment algorithms GB/T 15843.3-2008: Mechanisms using digital signature techniques GB/T 15843.4-2008: Mechanisms using a cryptographic check function GB/T 15843.5-2008: Mechanisms using zero knowledge techniques

Annex C Approved Security Functions

	ISO/IEC 19790	GM/T 0028
Key management	ISO/IEC 11770-2 ISO/IEC 11770-3 ISO/IEC 11770-4	Meet the requirements of OSCCA regarding key management.
Random bit generation	ISO/IEC 18031	1. Meet the requirements of OSCCA regarding random bit generation; 2. Conformant to GM/T 0005-2012 Randomness Testing Specification; 3. Random Bit Generator shall be certified by OSCCA

Annex D Approved SSP Generation and Establishment Methods

	ISO/IEC 19790	GM/T 0028
Sensitive security parameter generation	(Blank in the standard)	Meet the requirements of OSCCA regarding SSP generation.
Sensitive security parameter establishment methods	ISO/IEC 11770-2 ISO/IEC 11770-3	GM/T 0003.3-2012: SM2 Key Establishment Protocol

Annex E Approved Authentication Mechanisms

	ISO/IEC 19790	GM/T 0028
Authentication mechanisms	No approved mechanisms defined at this time.	GB/T 15843.2-2008: Mechanisms using symmetric encipherment algorithms GB/T 15843.3-2008: Mechanisms using digital signature techniques GB/T 15843.4-2008: Mechanisms using a cryptographic check function GB/T 15843.5-2008: Mechanisms using zero knowledge techniques

Annex F Approved Non-Invasive Attack Mitigation Test Metrics

	ISO/IEC 19790	GM/T 0028
Non-invasive attack mitigation test metrics	No approved non-invasive attack mitigation test metrics defined at this time.	Power analysis (including SPA and DPA) attack. Timing analysis attack. Electro-magnet leakage attack. Test metrics requirements: acquire less than 8-bits key for SPA, 1st order DPA, 2nd order DPA, SEMA, 1st order DEMA, 2nd order DEMA, and timing attack.

Thanks!

Please visit our website at www.atsec.com