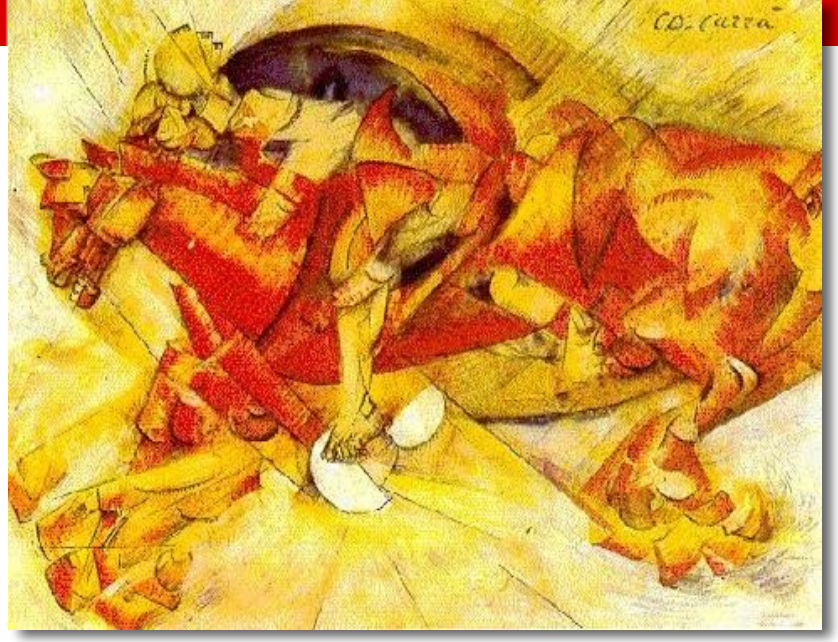
the information security provider



Introduction to the Commercial Cryptography Scheme in China

atsec China

Di Li
di.li@atsec.com
+86 138 1022 0119

Yan Liu
yan@atsec.com
+86 139 1072 6424

18 May 2016

Disclaimer

atsec China is an independent lab specializing in IT security evaluations.

The authors do not represent any Chinese government agency or Chinese government-controlled lab. All information used for this presentation is publicly available on the Internet, despite the fact that most of them are in Chinese.

Agenda

- **Background on commercial cryptography in China**
- **Product certification list**
- **Published algorithms and standards**
- **Certification scheme**
- **Conclusions**

What is “Commercial Cryptography”?

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.
  - Constituted by the Chinese Academy of Science (CAS)
  - Issued and regulated by the Office of the State Commercial Cryptography Administration (OSCCA)
    - Established in 1999
    - Testing lab setup in 2005

OSCCA Certified Product List

Certified product list (1509 items):

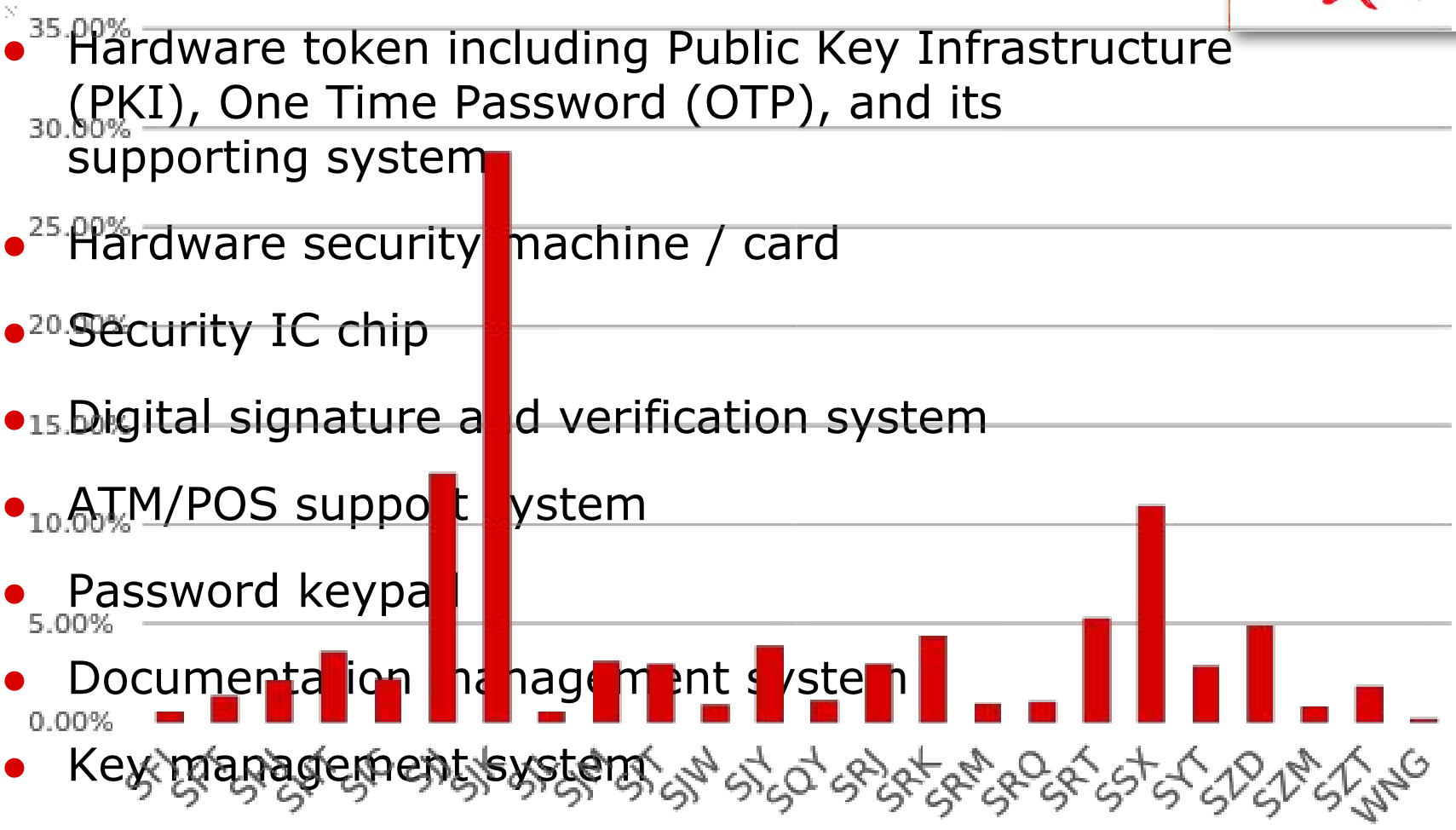
Until 2016-02-29

http://www.oscca.gov.cn/News/201603/News_1321.htm

Sequence No.	Product Model	Product Name	Vendor Name	Validation Date	Certificate No.
1505	SJJ1603	移动安全智能终端	郑州信大捷安信息技术股份有限公司	2016-02-23	SXH2016049
1506	SHT1614	移动通信服务平台	郑州信大捷安信息技术股份有限公司	2016-02-23	SXH2016050
1507	SSX1611	安全芯片	北京中电华大电子设计有限责任公司	2016-02-23	SXH2016053
1508	SRJ1601	数字签名终端	北京握奇智能科技有限公司	2016-02-23	SXH2016055
1509	SJK1612	TF密码卡	北京数盾信息科技有限公司	2016-02-23	SXH2016057

Certified Products and Its Use

- Hardware token including Public Key Infrastructure (PKI), One Time Password (OTP), and its supporting system
- Hardware security machine / card
- Security IC chip
- Digital signature and verification system
- ATM/POS support system
- Password keypad
- Documentation management system
- Key management system



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)
  - Lawfully, no foreign encryption products are allowed to be sold or used in China
  - Software or firmware products are not affected

How many “Commercial Cryptographic Algorithms and Standards” are there?

Published Algorithms

- Published: **SM2, SM3, SM4, SM9, ZUC**
- GM/T 0003.1: **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)
  - Competitor of **ECDSA P-256**

Published Algorithms

- GM/T 0004.1-2012: **SM3** (published in 2010):
  - Hash functions
  - Max input: 2^64 bits
  - Output: 256 bits
  - Competitor of **SHA-256**

- GM/T 0002-2012: **SM4** (published in 2012):
  - Block cipher symmetric algorithm
  - Block size: 128 bits
  - Key length: 128 bits
  - Competitor of **AES-128**

Published Algorithms

- GM/T 0044-2016: **SM9** (published in 2016):
  - Identity-Based Asymmetric Cryptography Algorithm
  - 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

Published Algorithms

- GM/T 0001.1-2012: **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

- SM2, SM3 and SM4 have been adopted in TPM2.0 of the Trust Computing Group (TCG) standard.
- ZUC has been adopted by 3GPP (3rd Generation Partnership Project) to be used in 3GPP LTE (128-EEA3 and 128-EIA3).

Published Standards

- GM/T 0005-2012: Randomness Test Specification
- GM/T 0008-2012: Cryptography Test Criteria for Security IC
- GM/T 0011-2012: Trusted Computing Functionality and Interface Specification
- GM/T 0014-2012: Digital Certificate Authentication System Cryptography Protocol Specification
- GM/T 0021-2012: One Time Password Application

Published Standards

- GM/T 0022-2014: IPSEC VPN Technology Specification
- GM/T 0027-2014: Technique Requirements for Smart Token
- GM/T 0030-2014: Specifications for Host Cryptographic Server
- GM/T 0045-2016: Specifications for Financial Data Encryption
- GM/T 0039-2015 : Security Requirements for Cryptographic Modules

Comparison with FIPS 140-2

- Security Requirements for Cryptographic Modules
  - Same:
  - 4 security levels
  - Single chip, Multichip embedded, and Multichip standalone
  - 10 security requirements

Comparison with FIPS 140-2

- Security Requirements for Cryptographic Modules
  - Different:
  - No IG, DTR to support the standard
  - No software/firmware module defined
  - Annex C: SM4 and SM1 as symmetric algorithms, SM2 as asymmetric algorithm, SM3 as hash function, ZUC as stream cipher, ISO/IEC 9797-2 as MAC, GM/T 0005-2012: Randomness Test Specification as RNG specification
  - Annex D: SM2 part 3, ISO/IEC 11770-2 and ISO/IEC 11770-3 as key establishment scheme.
  - Annex E: Best practices for software development
  - Annex F: Samples of mitigation of other attacks

How many roles in the scheme?

OSCCA and Vendor

- OSCCA
  - Certification body: Issues the product certificates
  - Testing lab: Tests products according to the standard
  - Market developer and supervisor: Develops new markets and monitors the sale status of certified products

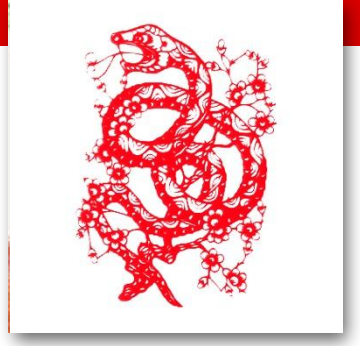
- Vendor
  - Designs and develop product
  - Manufactures the product
  - Sells the product and reports the annual sales progress

How can I certify myself as a vendor?

Application Procedure

- If you only want to sell cryptographic products in China:
  - Apply for sales permission only
  - Product must be certified and listed in the website
  - Time frame: 1 month or even less
- If you want to sell YOUR OWN cryptographic products in China:
  - Manufacturer permission
  - Sales permission
  - Product certification
  - Time frame: around 6 months depending on the vendor's condition and the product type

Procedure – Manufacturer Permission



- Has the capability to design the security product
- Has a factory / facility to manufacture the security product
- Has the equipment, a process and an assurance system for manufacturing the security product
- Complies with national laws, regulations, and policy requirements
- NO foreigner is allowed to be involved in the design and development of the cryptographic product
- Re-validation every 3 years

Procedure – Sales permission

Sequence No.	Vendor Name	First Validation Date	Latest Validation Date	Expiration Date	Sales Permission No.
489	上海倍胜信息科技有限公司		2014-10-31	2017-10-30	国密局销字 SXS2214号
490	上海金雅拓智能卡技术有限公司	2014-08-04	2014-10-31	2017-10-30	国密局销字 SXS2215号
491	西藏珂尔信息技术有限公司		2014-10-31	2017-10-30	国密局销字 SXS2216号
492	深圳市科曼信息技术有限公司		2014-10-31	2017-10-30	国密局销字 SXS2217号
680	深圳市捷顺科技实业股份有限公司		2015-06-04	2018-06-03	国密局销字 SXS2406号
681	捷德（中国）信息科技有限公司	2006-03-01	2015-06-04	2018-06-03	国密局销字 SXS2407号
682	北京汉邦高科数字技术股份有限公司	2012-06-28	2015-06-28	2018-06-27	国密局销字 SXS2408号

Procedure - Product certification

- To apply a product must be manufactured by a certified manufacturer
- Must pass the security examination held by OSCCA
- Implements Commercial Cryptography Algorithms
- Complies with Commercial Cryptography standards or protocols
- Complies with national laws, regulations and policy requirements
- Re-validation every 5 years

How is the product certified?

How a Product Can be Certified

- Different approaches:
  - IC product: the design shall:
    - Be validated according to "Cryptography Test Criteria for Security IC" and "Security Requirements for Cryptographic Modules"
    - Pass the algorithm test
    - For a Security Level 2 IC product, anti-DPA/SPA is recommended (test under draft standard)
    - Entropy analysis is mandatory required by "Randomness Test Specification" including 15 tests
  - Other product: USE CERTIFIED IC PRODUCT INSIDE
    - No common chip is allowed

How a Product Can be Certified

- Documentation check:
  - Application form
  - Technical summary report
  - Security design report
  - Guidance to the end user
  - Test procedure
  - Other materials required by OSCCA
- Application materials shall be submitted through branch office in vendor registered city, and then forwarded to OSCCA
- Comments will be given by OSCCA within 21 days of submission

How a Product Can be Certified

- Vendor modifies documentation and / or design, then resubmits
- When OSCCA is satisfied with the modifications, they will inform the vendor to bring the product for onsite examination
  - Product presentation
  - Functional demonstration
  - Security design explanation
  - By experienced experts group, 8 ~ 10 people, at least half outside OSCCA
- Normally it takes 4 days to get the result

Conclusions, Now and in the Future

Current Situation

- New procurement in important industries (e.g. banking) must use certified products (HSMs, POSes, VPNs)
- In 2013, China Union Pay published the PBOC3.0 which added the support of Commercial Cryptography Algorithms.
- Since 2015, new procurement of smart cards are recommended to use certified ICs. (More than 10 banks are testing internally (Incl. ICBC), one main commercial bank has issued 20K cards with certified IC.)
- Maybe the biggest market: USB token for e-banking and smart card

Current Situation

- Lack of information can be found before submitting the application
- Fewer choices of algorithms
- The algorithm standards are published, but common IC with software implementation will not be certified
- No third party labs are involved, only OSCCA can perform the evaluation

Questions?

Please visit our website at
www.atsec.com / www.atsec.cn