Cryptography in RFID and Its Applications in China

Jiansuo Zhou

CEC Huada Electronic Design Co., Ltd.

RFID Crypto Workgroup

Oct. 24, 2012

Are you using RFID?

Is it secure?

Do you want to use secure RFID?

Contents

- RFID system and security
- Why crypto in RFID is needed in China?
- RFID crypto standard system
- RFID crypto applications
- Introduction to RFID crypto workgroup

Contents

- **RFID system and security**
- Why crypto in RFID is needed in China?
- RFID crypto standard system
- RFID crypto applications
- Introduction to RFID crypto workgroup

RFID system and security

RFID Applications

- Asset management
- Item tracking
- Authenticity verification
- Access control
- Supply chain management
- Anti-counterfeiting

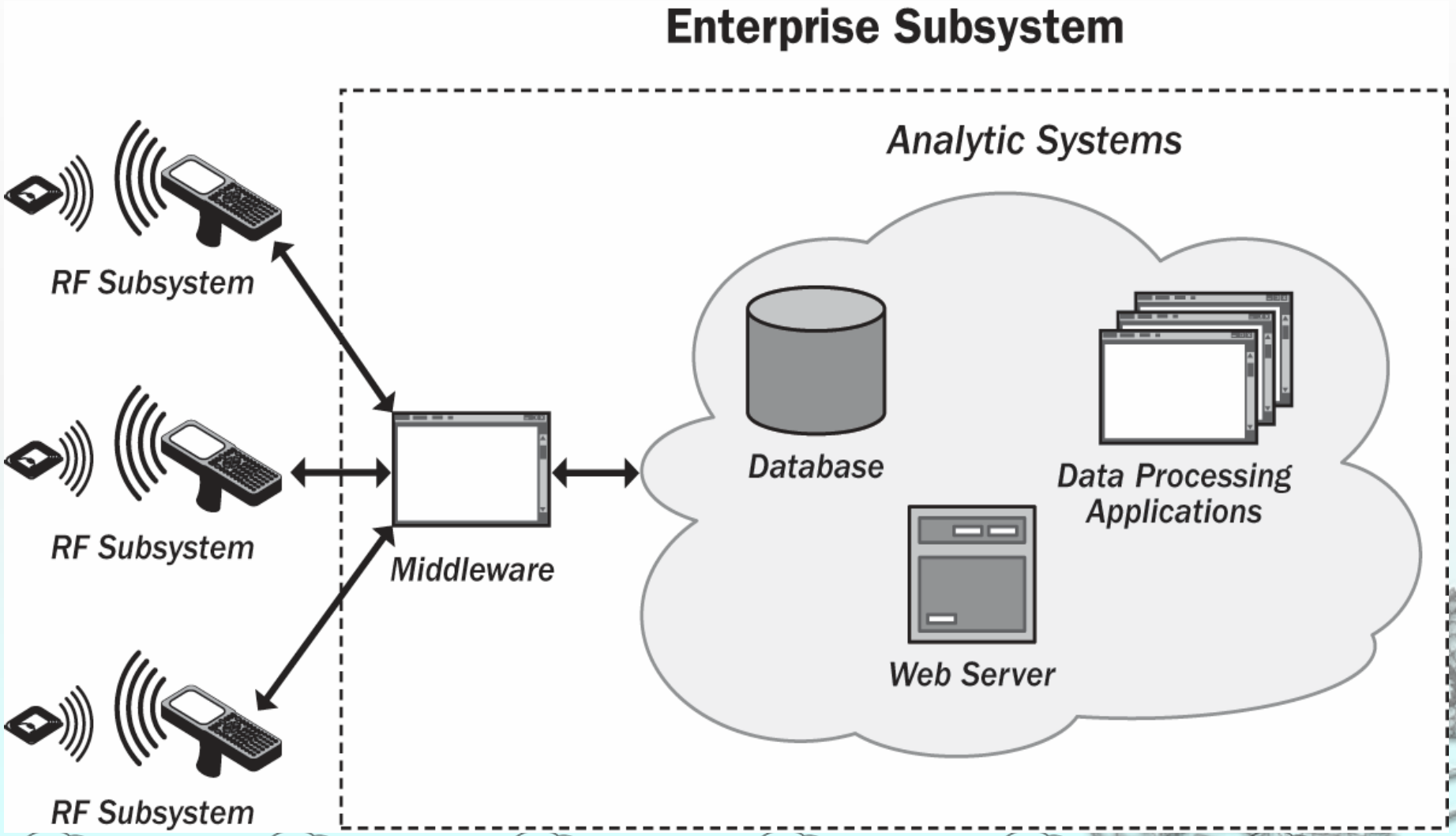
ISO18000

- **-2: 125~135KHz**
- **-3: 13.56MHz**
- **-4: 2.45GHz**
- **-5: 5.8GHz**
- **-6: 860-960MHz**
- **-7: 433.92MHz**

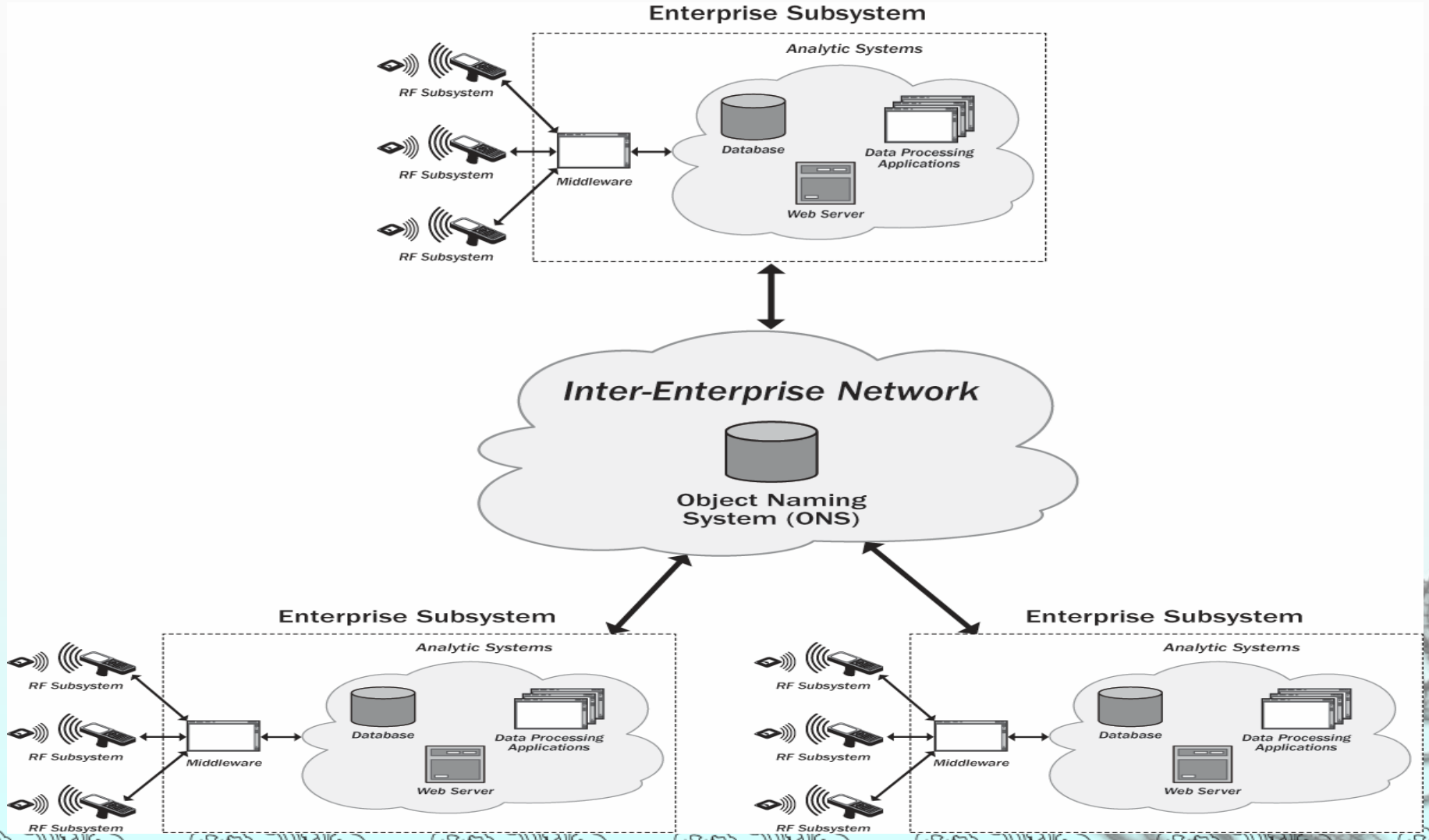
ISO14443

ABI Research: 70.5 Billion US$ in 2017, 20% rising annually, including tag, reader, SW and service.

RFID system and security



RFID system and security



RFID system and security

- **Security technology for RFID**

Authentication and data integrity

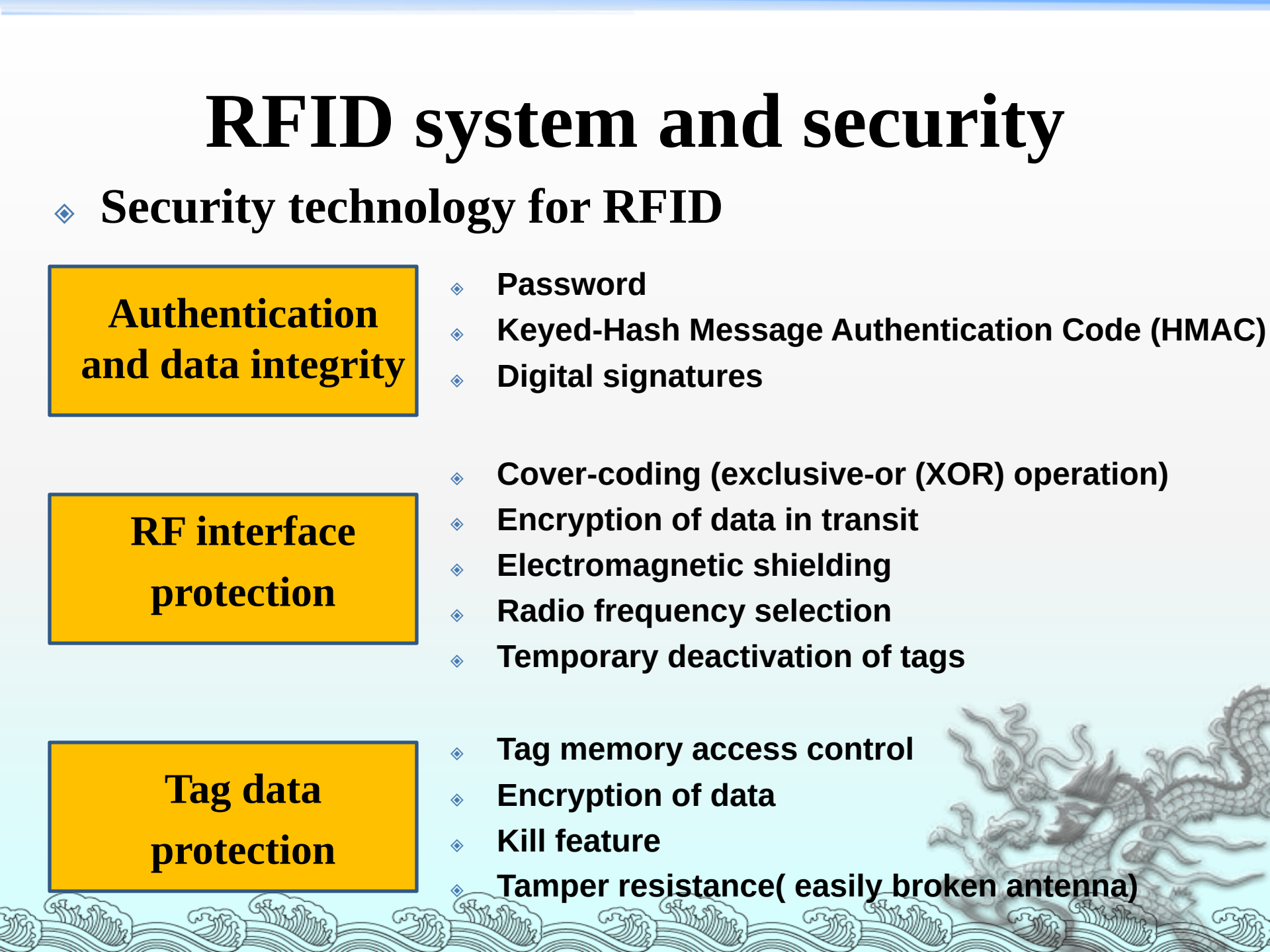
- Password
- Keyed-Hash Message Authentication Code (HMAC)
- Digital signatures

RF interface protection

- Cover-coding (exclusive-or (XOR) operation)
- Encryption of data in transit
- Electromagnetic shielding
- Radio frequency selection
- Temporary deactivation of tags

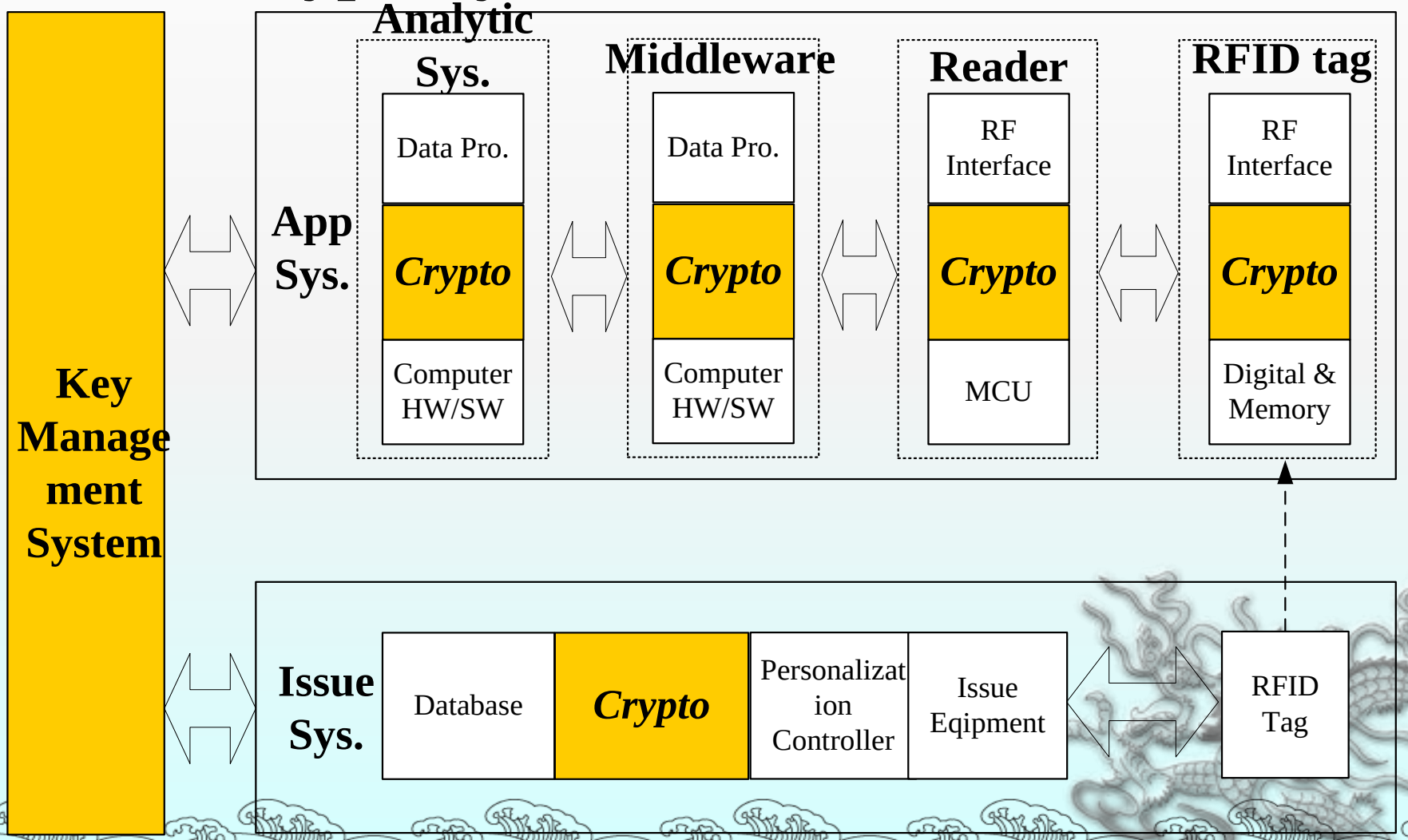
Tag data protection

- Tag memory access control
- Encryption of data
- Kill feature
- Tamper resistance(easily broken antenna)



RFID system and security

- RFID crypto system



Contents

- RFID system and security
- **Why crypto in RFID is needed in China?**
- RFID crypto standard system
- RFID crypto applications
- Introduction to RFID crypto workgroup

Why crypto in RFID is needed in China?

- **Anti-counterfeiting**

Anti-counterfeiting market: 120 Billion US$ annually in China, for medicine, food, cigarette and white liquor.

Why crypto in RFID is needed in China?

- Animal product tracking

Why crypto in RFID is needed in China?

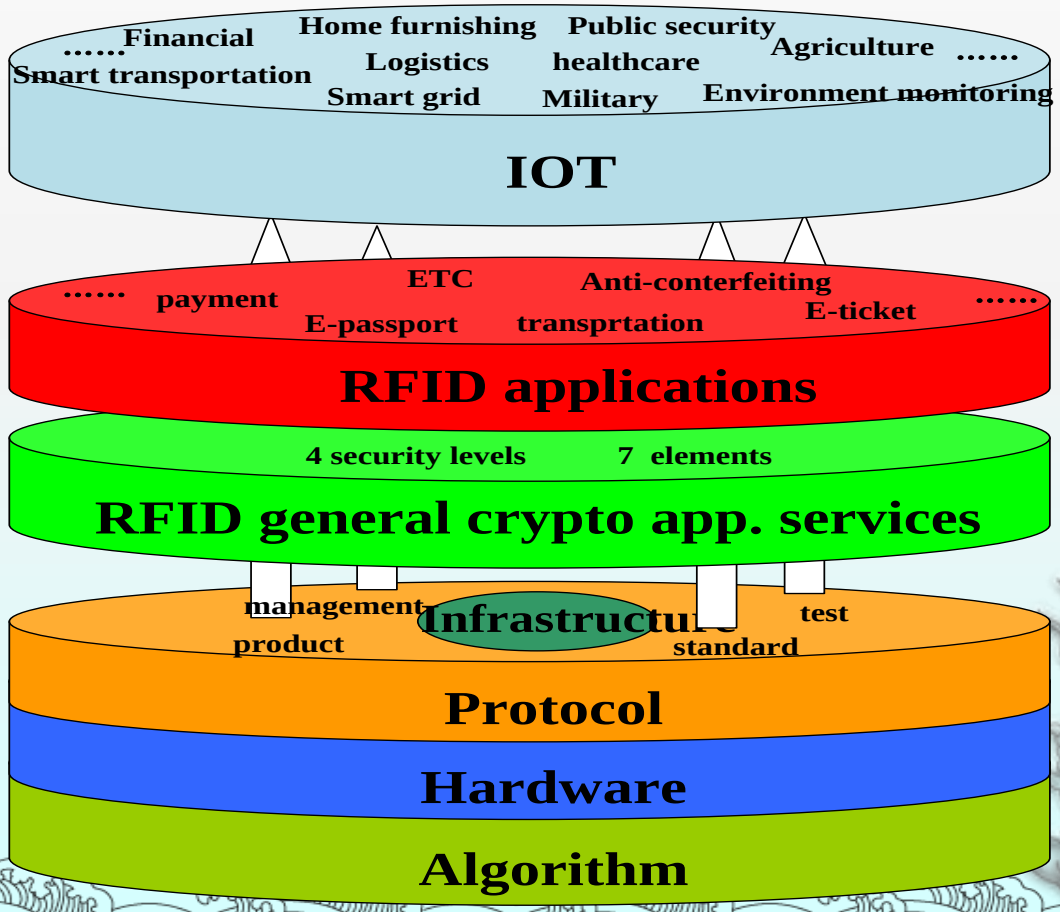
- Standard made by Ministry of Commerce
  - 2012
  - bottled white liquor anti-counterfeiting based on RFID
    - 1. Application data coding
    - 2. Tags technique requirements
    - 3. Readers technique requirements
    - 4. Inquires service process

Contents

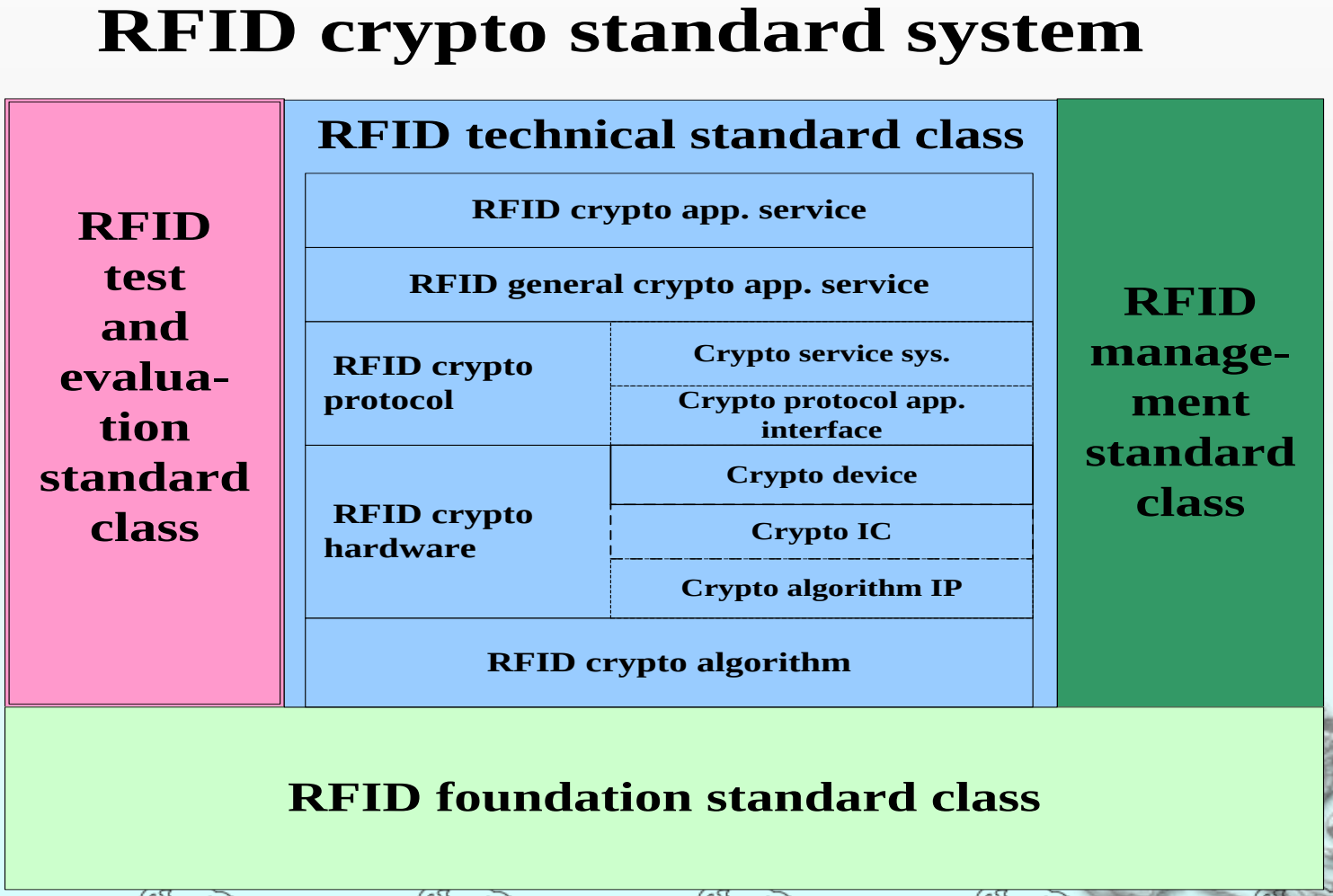
- RFID system and security
- Why crypto in RFID is needed in China?
- **RFID crypto standard system**
- RFID crypto applications
- Introduction to RFID crypto workgroup

RFID crypto standard system

- RFID crypto application technical system

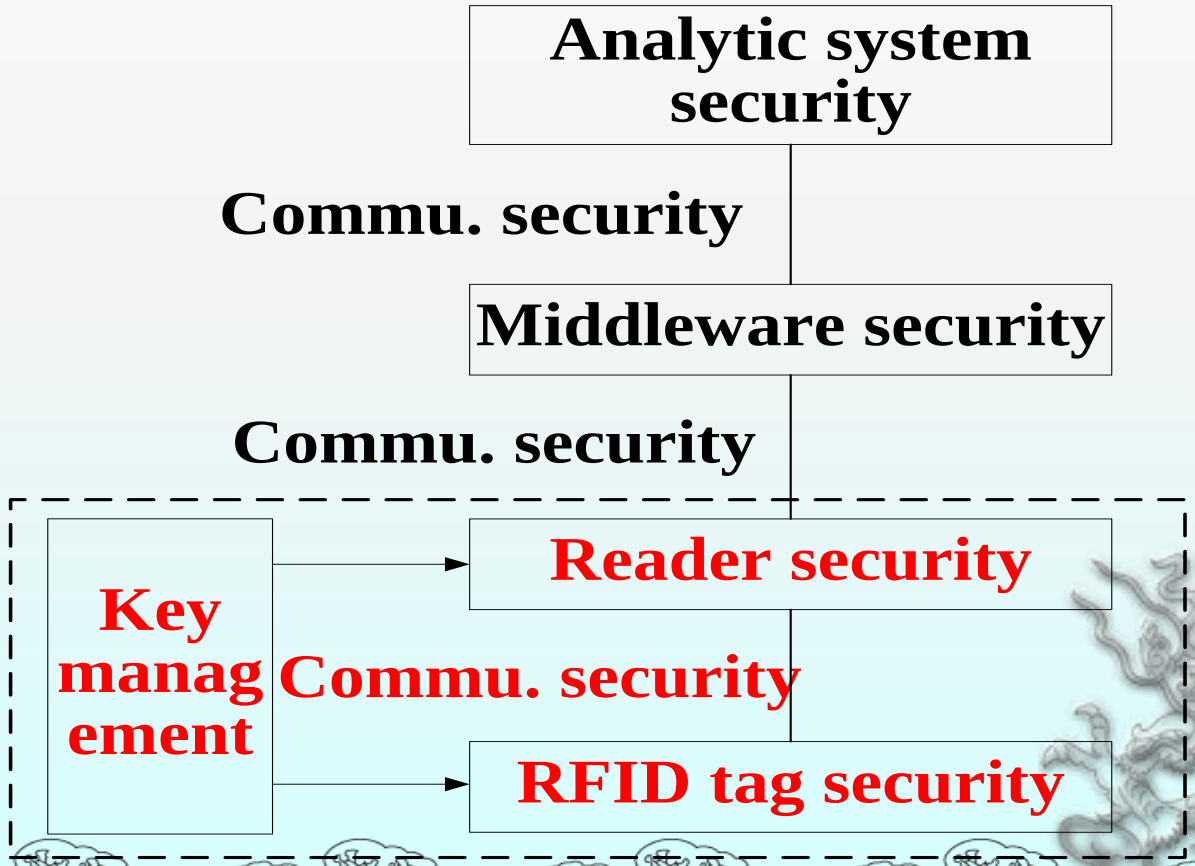


RFID crypto standard system



RFID crypto standard system

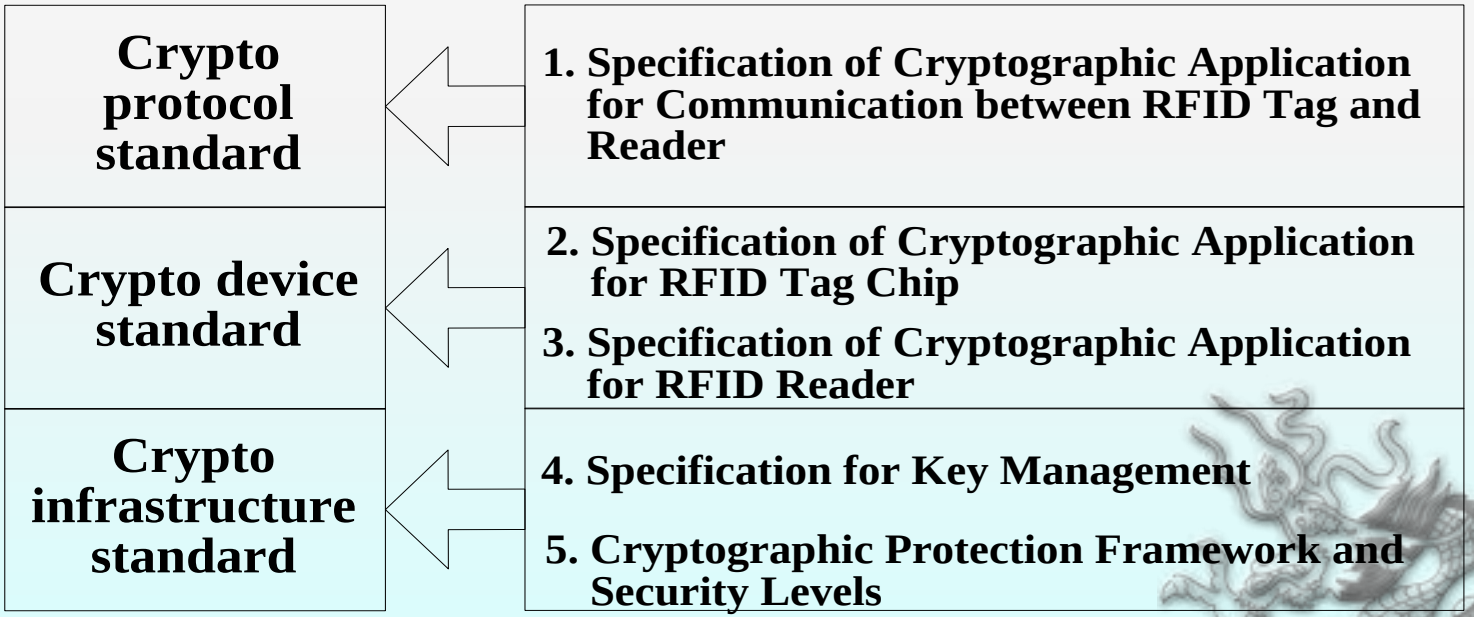
- RFID crypto workgroup focuses those standards



RFID crypto standard system

- **RFID crypto workgroup made those standards**

Specifications of Cryptographic Application for RFID Systems



RFID crypto standard system

- **Security elements and security levels for RFID system**

Elements\levels	Level 1	Level 2	Level 3	Level 4
Confidentiality			√	√
Integrity			√	√
Non-repudiation			△	√
Identity authentication	△	√	√	√
Access control		√	√	√
Audit				√
Crypto algorithm		√	√	√

Contents

- RFID system and security
- Why crypto in RFID is needed in China?
- RFID crypto standard system
- **RFID crypto applications**
- Introduction to RFID crypto workgroup

RFID crypto applications—algorithms

Type	algorithm	name	Key length	Block length	Clock	Logic gates	App. Eva.
symmetric	block	AES	128bit	128bit	1032	3.4K	Yes
		DES like	56bit	64bit	144	2.3K	Yes
		Hummingbird	64~256bit			1.023K	Yes
		present	80bit		32	1K~1.8K	Yes
	stream	Trivium64	64bit	——	1	5.5K	No
asymmetric		ECC/RSA		——		10K~30K	No
		IBC		——		大于100K	No
others	Hash	SHA-1	160bit	——	1228	8.1K	No
		Tav-128	128bit	——	1568	2.578K	Yes

■And Chinese commercial crypto algorithms are also be used.

RFID crypto applications

- **HF Products (13.56MHz)**

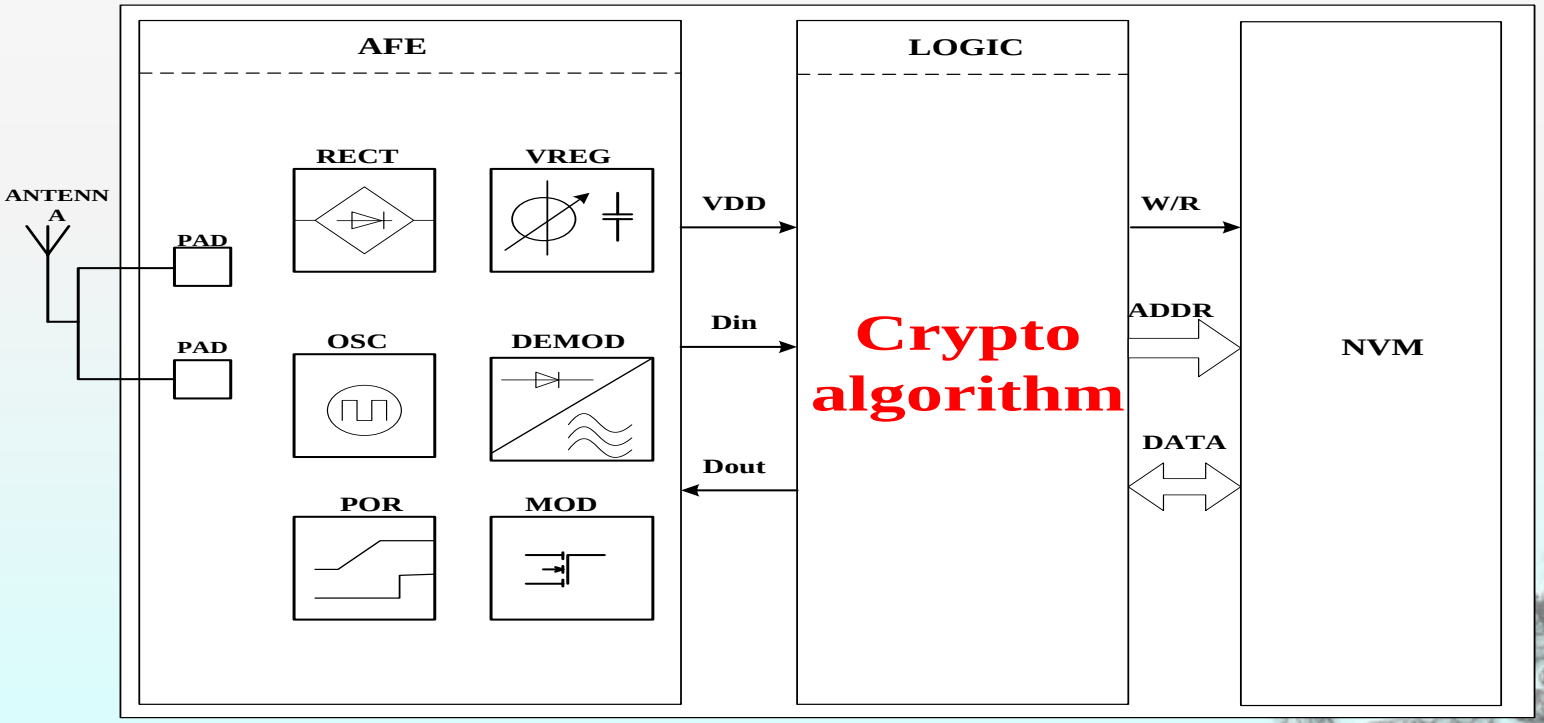
No.	Product	Certificate	Crypto
1	System	SXH2010058	128b symmetric
2	Reader	SXH2009051	128b symmetric/HASH/PKI
3	Reader	SXH2010100	128b symmetric/HASH/PKI
4	Tag IC	SXH2009087	128b symmetric
5	Tag IC	SXH2010028	128b symmetric
6	Tag IC	SXH2010039	128b symmetric
7	Tag IC	SXH2009021	128b symmetric
8	Tag IC	SXH2011016	128b symmetric
9	Tag IC	——	64b symmetric

RFID crypto applications

- UHF Products （800/900MHz)
  - Tag IC with 128b symmetric algorithm
  - Reader SAM
  - Key management system

RFID crypto applications

- The 1st UHF tag IC with symmetric crypto algorithm with ultra low power design, ~uW



RFID crypto applications

Contents

- RFID system and security
- Why crypto in RFID is needed in China?
- RFID crypto standard system
- RFID crypto applications
- **Introduction to RFID crypto workgroup**

Introduction to RFID crypto workgroup

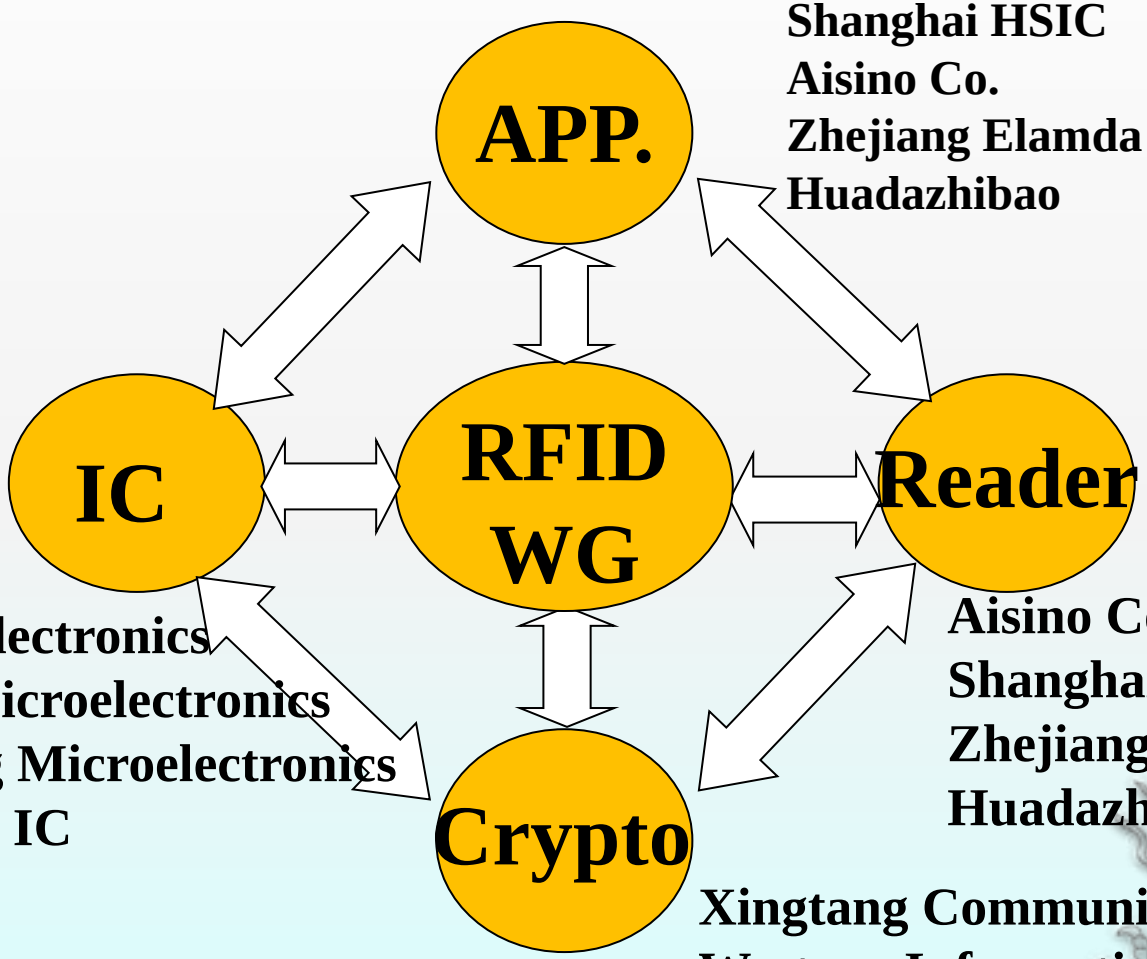
Cryptography Standardization Technical Committee

RFID Crypto Workgroup

11 members

Beijing CEC Huada Electronic Design Co., Ltd.
Xingtang Communication Technology Co., Ltd.
Shanghai Hsic Application System Co., Ltd.
Shanghai Fudan Microelectronics Group Company Limited
Tongfang Microelectronics Company
Fudan University
Aisino Corporation Inc.
Shanghai Huahong Integrated Circuit Co., Ltd.
Beijing Huadazhibao Electronic System Co., Ltd
Westone Information Industry Co., Ltd.
Zhejiang ELamda System Engineering Co., Ltd.

Introduction to RFID crypto workgroup



Shanghai HSIC
Aisino Co.
Zhejiang Elamda
Huadazhibao

Huada Electronics
Fudan Microelectronics
Tongfang Microelectronics
Huahong IC

Aisino Co.
Shanghai HSIC
Zhejiang Elamda
Huadazhibao

Xingtang Communication
Westone Information
Fudan University

We are working for RFID crypto application, you are welcome to join us.

Thanks