



INTERNATIONAL TELECOMMUNICATION UNION

**TELECOMMUNICATION  
STANDARDIZATION SECTOR**

STUDY PERIOD 2017-2020

**SG17 – LS 42**

**Original: English**

**Question(s):** 6/17

Geneva, 29 August – 6 September 2017

**Ref: TD 790 Rev.1 (PLEN/17)**

**Source:** ITU-T Study Group 17

**Title:** LS/o on ' Security Requirements and Framework of Using Identity-Based Cryptography Mechanisms in Internet of Things ' [to 3GPP SA3, ETSI TC CYBER, GSMA FASG, IRTF CFRG, IETF Security Area, ISO/IEC JTC 1/SC 27/WG 2]

**LIAISON STATEMENT**

**For action to:** -

**For comment to:** 3GPP SA3, ETSI TC CYBER, GSMA FASG, IRTF CFRG, IETF Security Area, ISO/IEC JTC 1/SC 27/WG 2

**For information to:** -

**Approval:** ITU-T SG17 meeting (Geneva, 6 September 2017)

**Deadline:** 28 February 2018

**Contact:** Jonghyun Baek  
Rapporteur of ITU-T Q6/17  
Republic of Korea

Tel: +82 2 405 6540  
Fax: + 82 2 405 5219  
E-mail: [jhbaek@kisa.or.kr](mailto:jhbaek@kisa.or.kr)

**Contact:** Yu Jiang  
China Telecom (China)  
People's Republic of China

Tel: +86 18918585305  
Email: [jiangyu@sttri.com.cn](mailto:jiangyu@sttri.com.cn)

**Contact:** Haiguang Wang  
Huawei Technologies Co. LTD (China)  
People's Republic of China

Tel: +65 91398518  
Email: [wang.haiguang1@huawei.com](mailto:wang.haiguang1@huawei.com)

ITU-T Study Group 17 thanks you for your continuous collaboration with Q6/17.

In SG17 meeting on 29 August – 6 September 2017, we adopted a new work item (X.ibr-iot) on *Security Requirements and Framework of Using Identity-Based Cryptography Mechanisms in Internet of Things*. This item will study the following aspects of using identity-based cryptography in IoT networks:

- Identity Management
- Key Management Architecture
- Key Management Operations
- Authentication

**Scope** (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability):

The scope of this recommendation will focus on the security requirements of management operations including device identifying, private key issuing, public parameter lookup etc. and the framework of using IBC in IoT in a single operator model. All IoT devices connect to a single telecom operator and all identity-based private keys are generated by KGC controlled by the operator. The trust across multiple KGCs might be studied in the future, but not in this recommendation.

**Summary** (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work):

Internet of Things has gained tremendous momentum in recent years. With the practical deployment of NB-IoT, it is predicted that billions of devices will be connected in the coming years. Security of IoT is one of the foremost concerns due to the ubiquitous nature of the devices coupled with the increasing sensitivity of user data. Recent high profile security breaches of IoT devices highlight the significance of the issue.

IoT devices are characterized by the constraint of resources such as commutation and communication capabilities. Thus the nature of IoT devices brings new challenges to satisfy the security requirements in an IoT system. Particularly easy-deployment, lightweight management operations and distributed authority are among the key factors when considering security solutions for IoT.

Authentication, access control, and data confidentiality are the essential services required for securing IoT. Both symmetric-key and public-key cryptography mechanics can be exploited for providing such services.

The symmetric-key based security solution is relatively simple but does not fit well the peer-to-peer scenarios such as the M2M applications in IoT without an online service playing as a trust broker and without IoT devices pre-sharing a secret pairwise. Cross-system secure communication is also complicated without exposing user secret to peer parties.

The traditional certificate-based public key cryptography solution involves heavyweight key management operations including certificate issuing, querying, and revocation. Such systems face great difficulty to keep up with the pace of device increment of IoT at the same time maintaining decent performance.

Identity-based cryptography technology is another type of public-key technology which uses an entity's identity as a public key. As one of the essential features of IoT, everything has a unique identifier. Using such identifiers as public keys, no certificates are required. Consequently, IBC security solution utilizes simpler key management, enables distributed authorities controlling their own devices and scales well to both the high number of endpoints and the diversity of the devices.

The concept of Identity-based cryptography was first proposed by Adi Shamir in 1984, together with the first concrete Identity-based signature scheme, while concrete Identity-based encryption schemes were only realized in year 2000 by Saki, Boneh and Franklin based on bi-linear pairing technology. Since then, more than 10 standards have been developed by various standard development bodies such as ISO [1][2][3], IEEE [4], CCSE [5] and IETF [6][7][8][9][10][11][12] etc.

Although there are more than 10 standards have been developed, majority of them are developed for the crypto algorithms, encryption and signature methods [1] [2][3][4][5][6][8][9][10], and only a few of them are developed for key management, such as key distribution [7] and key exchange [11][12].

IBC-based public key technologies have been used in a number of applications such as email encryption [13], multimedia security [14], payment, and IoT authentication [15] etc. However, majority of usages are still in small scale. Some proprietary protocols in key distribution and revocation need to be used when using the IBC public key. The standardization paces of IBC in IETF is rather slow. The reason is because that at the moment, most of devices on the internet are powerful in computing power and rich in transmission bandwidth. PKI-based certificate can satisfy their requirement. On the hand, IoT devices are constraint in computing power and transmission bandwidth. They need light weight cryptography protocol more urgently. Another concern of using IBC over internet is the key escrow issue, i.e., the private key of user is known to the key generation centre. However, for IoT networks, this may not be an issue since it is normal for network operators to know the devices' network access credentials. For example, the current 4G networks, the credentials of devices are known to the operators.

IBC-based public key is started being used for device authentication in IoT networks. However, no security framework has been defined for using IBC public key in IoT networks yet. And some part of protocols are still missing. For example, how to ensure the uniqueness of identifiers, what protocol shall be used for authentication, key distribution and revocation. All these factors may prevent the IBC public key technologies from being used for large scale IoT networks.

This contribution analyses security requirements of various management operations of using IBC in IoT including device identifying, private key issuing, public parameter lookup etc. and presents a security framework based on federated IBC authorities including system components in a single authority.

Our scope is that all IoT devices connect to a single telecom operator and all identity-based private keys are generated by KGC controlled by the operator. The trust across multiple KGCs might be studied in the future, but not in this recommendation.

### References

- [1] ISO/IEC 15946-5:2009 Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 5: Elliptic curve generation.
- [2] ISO/IEC 14888-3:2016 [Preview](#) Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms
- [3] ISO/IEC 18033-5:2015 [Preview](#) Information technology -- Security techniques -- Encryption algorithms -- Part 5: Identity-based ciphers
- [4] IEEE P1363.3 Standard for Identity-based 3 Public-key Cryptography Using 4 Pairings
- [5] GM/T 0044-2016 SM9 Identity-based Cryptography Algorithm
- [6] IETF RFC 5091, X. Boyen et. al., Identity-Based Cryptography Standard (IBCS) #1:Supersingular Curve Implementations of the BF and BB1 Cryptosystems
- [7] IETF RFC 5408, G. Appenzeller et. al., Identity-Based Encryption Architecture and Supporting Data Structures
- [8] IETF RFC 5409, L. Martin et. al., Using the Boneh-Franklin and Boneh-Boyer Identity-Based Encryption Algorithms with the Cryptographic Message Syntax (CMS)
- [9] IETF RFC 6507, M. Groves, Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)
- [10] IETF RFC 6508, M. Groves, Sakai-Kasahara Key Encryption (SAKKE)
- [11] IETF RFC 6509, M. Groves, MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)
- [12] IETF RFC 6539, IBAKE: Identity-Based Authenticated Key Exchange
- [13] HP: Using IBE with FPE for securing payment transactions, email protection, [http://h41111.www4.hp.com/event/uk/en/software-protect roadshow/Brendan%20Rizzo%20-%20Roadshow%20Protect%20EMEA2015%20-%20Voltage%20-%20with%20videos-v4.pdf](http://h41111.www4.hp.com/event/uk/en/software-protect%20roadshow/Brendan%20Rizzo%20-%20Roadshow%20Protect%20EMEA2015%20-%20Voltage%20-%20with%20videos-v4.pdf)
- [14] Secure Voice at Official, <https://www.ncsc.gov.uk/guidance/secure-voice-official>
- [15] Vanadium: Privacy, Discovery, and Authentication for the Internet of Things, <http://iot.stanford.edu/pubs/PrivateloT.pdf>

ITU-T SG17 would welcome comments and documents relevant to this subject.