TLS: Using Identity as Raw Public Key

draft-wang-tls-raw-public-key-with-ibc

Haiguang Wang (wang.haiguang1@huawei.com)

Yanjiang Yang (yang.Yanjiang@huawei.com)

Xin Kang (kang.xin@huawei.com)

Zhaohui Cheng (chengzh@myibc.net)

IETF 104, March 2019, Prague

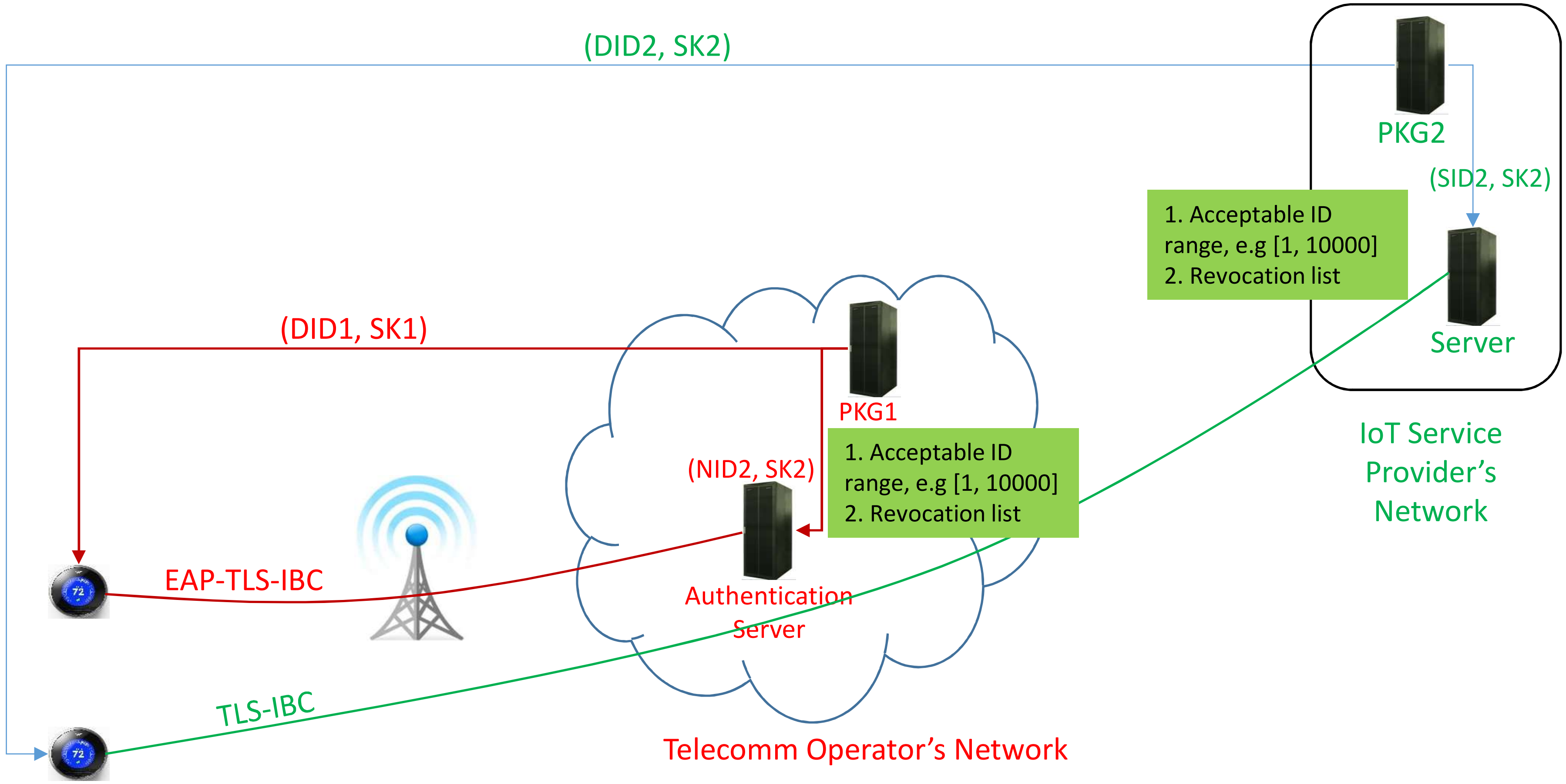
Motivation

- TLS 1.3 (RFC 8446) supports using the raw public key in the handshake protocol. The raw public key has following advantages over PKI certificates
  - ➢ Simple in authentication
  - ➢ Lightweight in communication comparing to a standard certificate.
- Issues with using the raw public key
  - ➢Need to maintain a binding list for public keys and their corresponding identifiers, which has to be provisioned to the server with out of band measures (as stated in the RFC 7250).
- Proposed Solution
  - ➢ Using Identity-based cryptography (IBC), i.e. the Identity-based Signature (IBS) to exempt server from provisioning of the binding between public keys and identifiers.

Usage Scenarios

Two potential usage scenarios:

1. Devices perform mutual authentication with network access server using EAP-TLS-IBC
2. Devices perform mutual authentication with service provider's server with TLS-IBC



Telecomm Operator's Network

IBC Standards

#C	Standard	SDO	Type	Description
1	IEEE P1363.3	IEEE	IBC	An cryptographic standard based on pairing including IBS/IBE/IBKA
2	RFC 5091	IETF	IBE	Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of BF and BB1 Cryptosystems
3	RFC 5408	IETF	IBE	Identity-Based Encryption Architecture and Supporting Data Structure
4	RFC 5409	IETF	IBE	Using Boneh-Franklin and Boneh-Boyen Identity-Based Encryption Algorithms with the Cryptography Message Syntax (CMS)
5	RFC 6507	IETF	IBS	Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)
6	RFC 6508	IETF	IBE	Using Identity-Based Encryption to exchange a shared secret from a Sender to a Receiver
7	RFC 6509	IETF	IBE + IBS	Provide a method of key exchange that uses Identity-based Public Key Cryptography (IDPKC) to establish a shared secret value and certificateless signatures to provide source authentication.
8	SM9	CCSE	IBC	An cryptographic standard based on pairing including IBS/IBE/IBKA
9	ISO/IEC 15946-5	ISO/IEC	ECC/IBC	Specify how to generate elliptic curve supporting pairing
10	ISO/IEC 11770-3 (2015)	ISO/IEC	IBKA	Including two ientity-based authenticated key agreement schemes
10	ISO/IEC 14888-3 (2018)	ISO/IEC	IBS	Including three identity-based signature schemes (ISO-IBS1, ISO-IBS2, ISO-ChineseIBS
11	ISO/IEC 18033-5 (2015)	ISO/IEC	IBE	Including three identity-based encryption schemes
12	Security of Mission Critical Push to Talk over LTE (3GPP TS 33.179)	3GPP	IBE+IBS	Apply IBE and IBS algorithm for secure SIP session key distribution and entity authentication over LTE

TLS-IBC： Using Identity as Raw Public Key

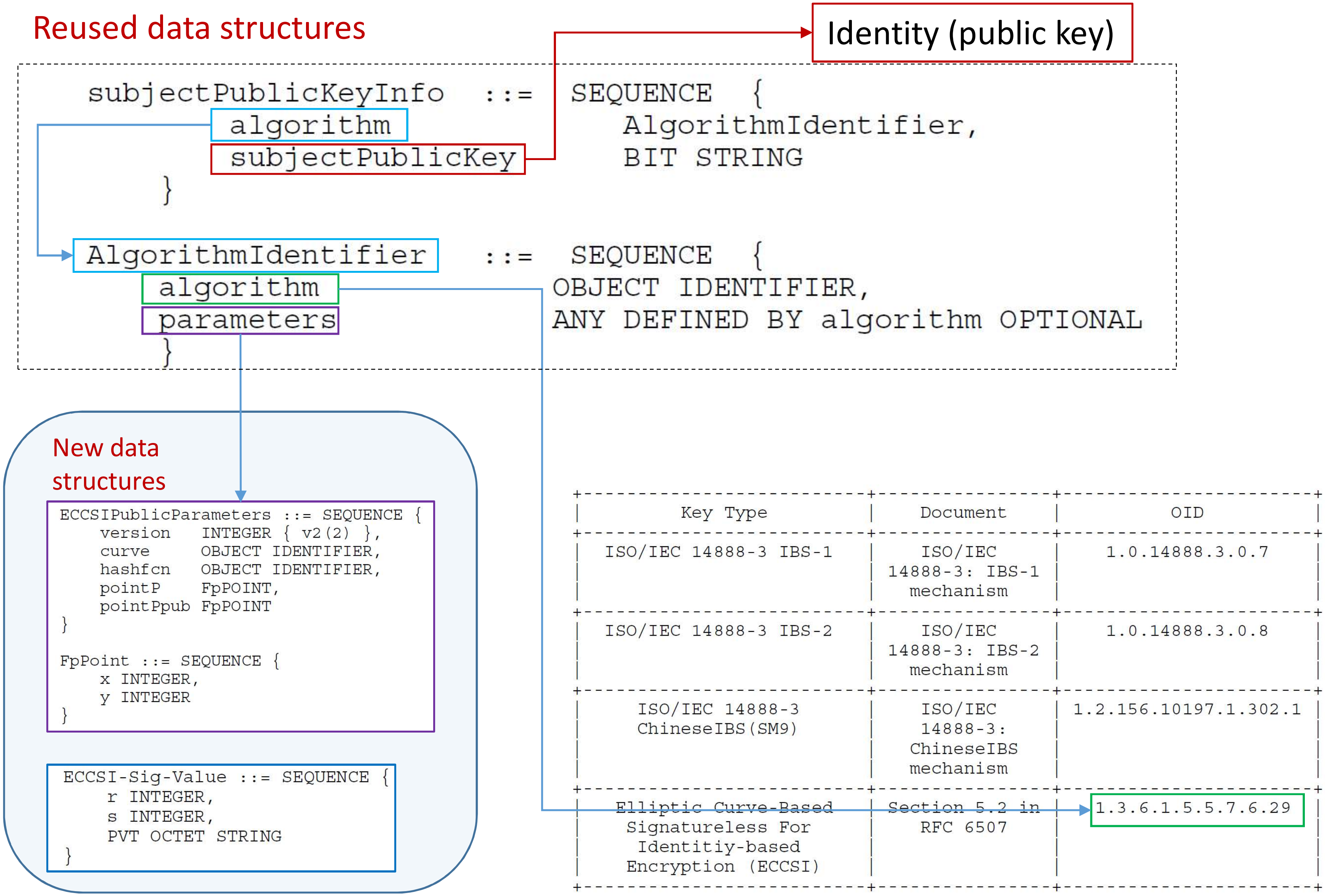
- Raw public key has been specified in the RFC 7250 and is included in the TLS 1.3 .
- Extend the TLS 1.3 to support IBS
  - ➢Using identity as the raw public key
  - ➢Using IBS signature algorithm in place of raw public key signature algorithms
- IBS algorithms to be supported
  - ✓ ECCSI: specified in RFC 6507, Elliptic Curve based
  - ✓ ISO-IBS1: ISO/IEC 14888-3, Bilinear Pairing based
  - ✓ ISO-IBS2: ISO/IEC 14888-3, Bilinear Pairing based
  - ✓ ISO-ChineseIBS: ISO/IEC 14888-3, Bilinear Pairing based
    - ❖ http://sca.hainan.gov.cn/dt/tzgg/201803/W020180327347630321953.pdf

Data Structure Extended

First of all, we need to extend the Signature Scheme to reserve some values for IBS.

```
enum {
...
/* IBS ECCSI signature algorithm */
eccsi_sha256 (TBD),
iso_ibs1 (TBD),
iso_ibs2 (TBD),
iso_chinese_ibs (TBD),
/* Reserved Code Points */
private_use (0xFE00..0xFFFF),
(0xFFFF)
} SignatureScheme;
```

Data Structure Reused/Newly defined (ECCSI)



Reused data structures

Identity (public key)

```
subjectPublicKeyInfo  ::=  SEQUENCE  {
     algorithm            AlgorithmIdentifier,
     subjectPublicKey     BIT STRING
}

AlgorithmIdentifier  ::=  SEQUENCE  {
     algorithm     OBJECT IDENTIFIER,
     parameters    ANY DEFINED BY algorithm OPTIONAL
}
```

New data structures

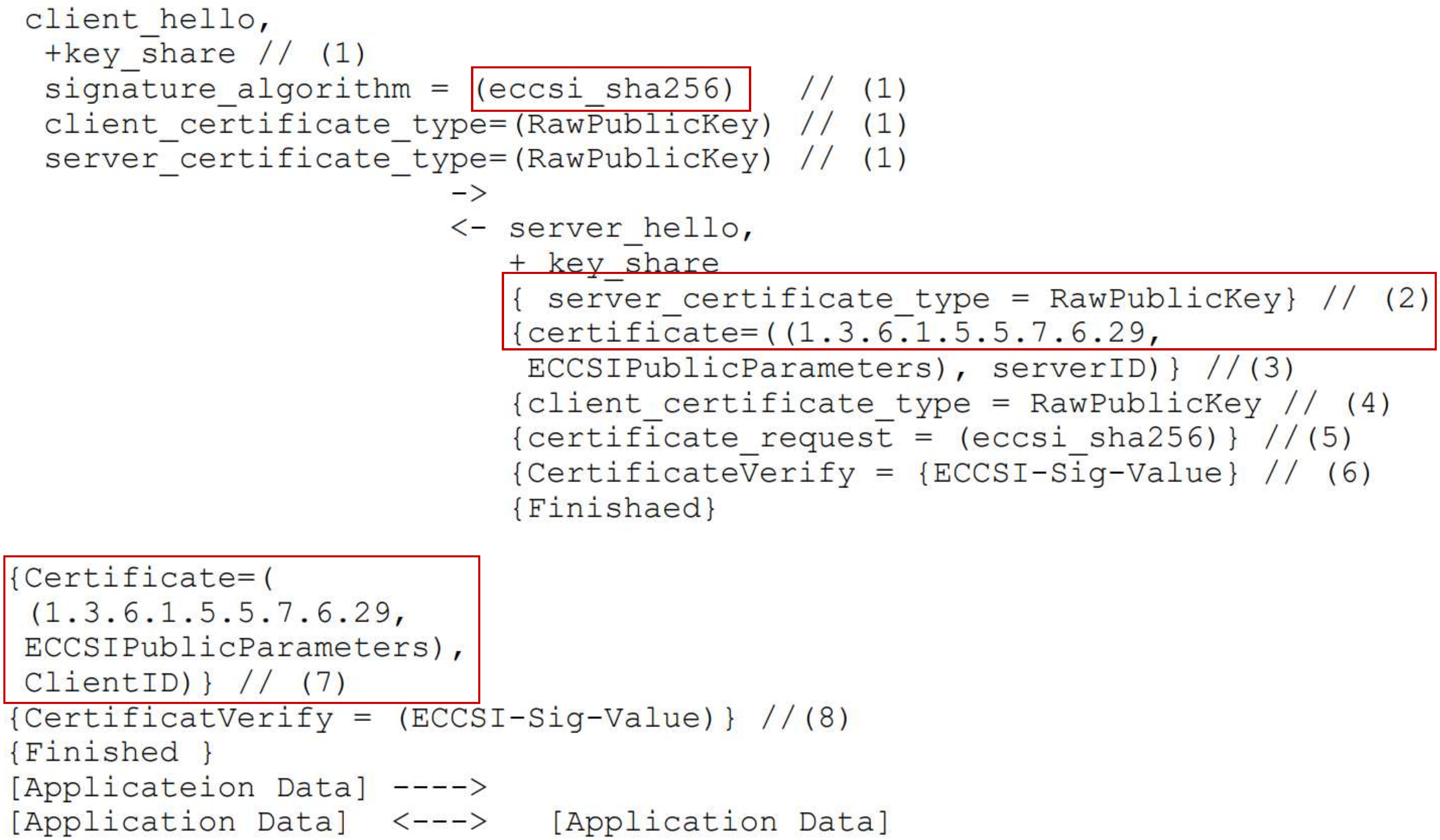
```
ECCSIPublicParameters ::= SEQUENCE {
    version   INTEGER { v2(2) },
    curve     OBJECT IDENTIFIER,
    hashfcn   OBJECT IDENTIFIER,
    pointP    FpPOINT,
    pointPpub FpPOINT
}

FpPoint ::= SEQUENCE {
    x INTEGER,
    y INTEGER
}
```

```
ECCSI-Sig-Value ::= SEQUENCE {
    r INTEGER,
    s INTEGER,
    PVT OCTET STRING
}
```

Key Type	Document	OID
ISO/IEC 14888-3 IBS-1	ISO/IEC 14888-3: IBS-1 mechanism	1.0.14888.3.0.7
ISO/IEC 14888-3 IBS-2	ISO/IEC 14888-3: IBS-2 mechanism	1.0.14888.3.0.8
ISO/IEC 14888-3 ChineseIBS(SM9)	ISO/IEC 14888-3: ChineseIBS mechanism	1.2.156.10197.1.302.1
Elliptic Curve-Based Signatureless For Identitiy-based Encryption (ECCSI)	Section 5.2 in RFC 6507	1.3.6.1.5.5.7.6.29

TLS-IBC: Handshake Protocols



```
 client_hello,
  +key_share // (1)
  signature_algorithm = (eccsi_sha256)   // (1)
  client_certificate_type=(RawPublicKey) // (1)
  server_certificate_type=(RawPublicKey) // (1)
                       ->
                       <- server_hello,
                          + key_share
                          { server_certificate_type = RawPublicKey} // (2)
                          {certificate=((1.3.6.1.5.5.7.6.29,
                           ECCSIPublicParameters), serverID)} //(3)
                          {client_certificate_type = RawPublicKey // (4)
                          {certificate_request = (eccsi_sha256)} //(5)
                          {CertificateVerify = {ECCSI-Sig-Value} // (6)
                          {Finishaed}

{Certificate=(
 (1.3.6.1.5.5.7.6.29,
 ECCSIPublicParameters),
 ClientID)} // (7)
{CertificatVerify = (ECCSI-Sig-Value)} //(8)
{Finished }
[Applicateion Data] ---->
[Application Data]  <--->   [Application Data]
```

Work in ITU-T SG-17

- ITU-T SG-17 now is developing “security framework for use of identity-based cryptography in support of IoT services over Telecom networks” . It covers the following topic:
  - ➢ An overview of IoT services over telecom networks.
  - ➢ Security Requirement when using IBC .
  - ➢ Generic Formulation and Supported IBC Algorithms
  - ➢ IBC key data definition
  - ➢ Key management operations
  - ➢ Authentication
  - ➢ Identity naming

Way Forward

We asked the WG group chairs to reserve following code points for us to use in the implementation and testing.

```
enum {
...
/* IBS ECCSI signature algorithm */
eccsi_sha256 (TBD),
iso_ibs1 (TBD),
iso_ibs2 (TBD),
iso_chinese_ibs (TBD),
/* Reserved Code Points */
private_use (0xFE00..0xFFFF),
(0xFFFF)
} SignatureScheme;
```

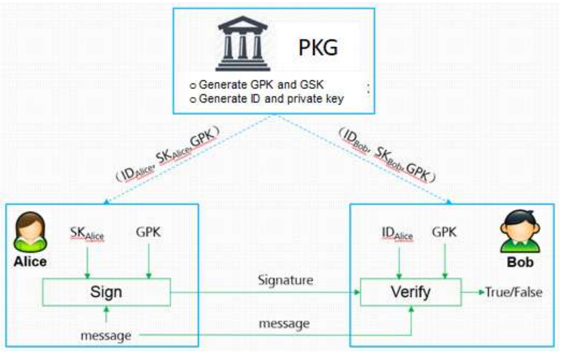
Questions

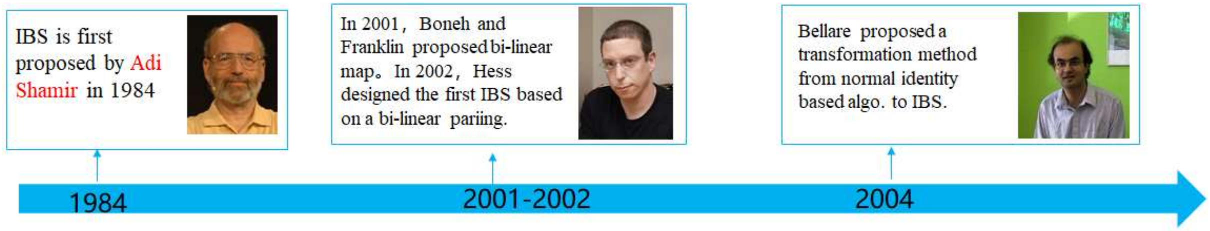
Identity-based Signature Scheme

- Identity-based Cryptography
  - using identity as public key
    - example: tom@xyz.com can be a public key
  - Identity-based encryption (IBE)/Identity-based Signature (IBS)

- Identity-based Signature (IBS)
  - Each user has own public and private key pairs, and its public key is its identity
  - User's private key is generated by PKG based on User's ID and PKG's Global Secret Key (GSK);
  - The signing and signature verification procedure do not involve the PKG；
    - ✓ To verify the signature, only the signature, message, id, and the Global Public Key (GPK) are needed.

ID-based Signature Framework





IBS is first proposed by Adi Shamir in 1984

In 2001，Boneh and Franklin proposed bi-linear map。In 2002，Hess designed the first IBS based on a bi-linear pariing.

Bellare proposed a transformation method from normal identity based algo. to IBS.