ICS 35.040
L 80
备案号：

中华人民共和国密码行业标准

GM/T XXXX—XXXX

基于 IBC 技术的身份鉴别协议规范

IBC technology Based Protocol Specifications of Identity Authentication

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

××××-××-××发布　　××××-××-××实施

国家密码管理局 发布

目　　次

前　言

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由国家密码管理局提出并归口。

本标准起草单位：上海信息安全工程技术研究中心、国家信息安全工程技术研究中心、无锡江南信息安全工程技术研究中心、西安工业大学。

本标准主要起草人：袁峰、郭晓雷、刘平、药乐、蒋楠、谢安明、胡春卉、杨恒亮、唐英、容晓峰、浦雨三、武勇、吕存志、王建。

引　　言

本规范是IBC（Identity-Based Cryptography）基于身份标识密码技术系列规范之一，本规范依托于《SM9基于双线性对椭圆曲线标识密码算法》规范，面向应用系统中基于IBC技术和SM9算法进行的身份认证时涉及到的鉴别需求。

本规范为相关身份鉴别给出了所需的密钥数据格式定义、认证协议流程和格式定义。

基于 IBC 技术的身份鉴别协议规范

1. 范围

本规范适用于采用IBC技术的实体鉴别机制。鉴于标识密码技术的特点，规定了两种单向认证的鉴别和一个双向认证的鉴别。

鉴别机制中采用诸如时间戳、序号或随机数等变化参数，防止先前有效的鉴别信息以后又被接收或者多次接收。

本规范还在附录中给出了利用IBC技术进行鉴别时需要访问PPS的基本流程和相关密码协议。

2. 规范性引用文件

下列文件中的条款通过本规范的引用而成为本规范的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本规范，然而，鼓励根据本规范达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本规范。

GM/T 0006-2012 密码应用标识规范

GM/T AAAA SM9基于双线性对椭圆曲线标识密码算法

GM/T BBBB SM9密码使用规范

3. 术语和定义

下列术语和定义适用于本规范。

3.1.

标识 identity

可唯一确定一个对象身份的信息，例如电子邮箱地址、手机号码、指纹数据等。

3.2.

SM9 密码算法 SM9 algorithm

一种采用双线性对的椭圆曲线公钥密码算法。

3.3.

公开参数服务 Public Parameter Service

用于发布基于身份标识密码技术中公开参数、私钥生成策略、用户标识信息和状态等数据的应用服务。

4. 符号和缩略语

下列缩略语适用于本规范。

IBC：基于身份标识的密码技术（Identity-Based Cryptography）

IRIs：国际资源标识符（Internationalized Resource Identifiers）

PKG：私钥生成（Private Key Generation）

PPS：公开参数服务（Public Parameter Service）

URI：统一资源标识符（Uniform Resource Identifier）

5. 标识结构

标识数据格式的ASN.1定义为：

```
IBCIdentityInfo ::= SEQUENCE {
        district            IA5String,
        serial              INTEGER,
        identityType        OBJECT IDENTIFIER,
        identityData        OCTET STRING,
        validity            ValidityPeriod,
        idExtensions        Extensions OPTION
}
```

district（区域）是一个 IA5 字符串，代表 IBC 加密信息的接收者能够恢复需要加密的 IBC 公共参数或者对身份进行加密的信息进行解密的 URI [URI] 或 IRI[IRI]即 PPS 的访问地址。

serial（序列串）一个整数，其定义了一个唯一的 IBC 公共参数集（在一个以上的参数集被一个单一 District 域使用的情况下）

identityType（身份类别）是一个对象标识符号 OID，定义身份数据域被编码的格式。

identityData（身份数据）八位串，身份的具体描述。

```
ValidityPeriod::= SEQUENCE {
     NotBefore                GeneralizedTime, -- 有效期起始时间
     notAfter                 GeneralizedTime OPTION -- 有效期终止时间
}
```

validity(有效期)时间类型，标识的有效期限，如果 notAfter 不填写，表示永久有效。

```
Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension
Extension  ::=  SEQUENCE  {
     extnID      OBJECT IDENTIFIER,
     critical    BOOLEAN DEFAULT FALSE,
     extnValue   OCTET STRING
}
```

extnID：表示一个扩展元素的 OID

critical：表示这个扩展元素是否极重要

extnValue：表示这个扩展元素的值，字符串类型。

6. 用户身份鉴别协议

6.1. 描述

用户身份鉴别过程包含了鉴别双方的流程和具体协议，在进行身份鉴别时各方都可以通过访问PPS获取相关认证体系的关键参数，例如IBC的公开参数；还可以通过访问PPS获取对方标识的相关信息，例如标识信息的状态，完整的标识数据等，如图8-1所示。

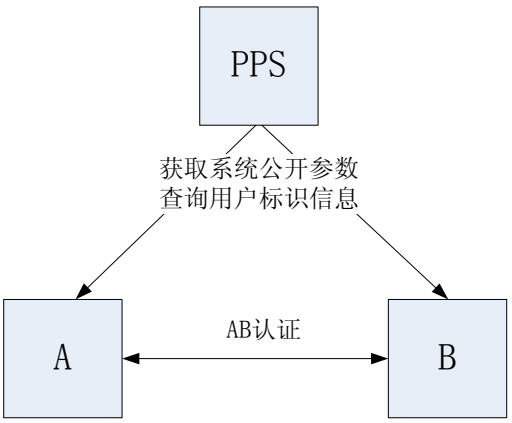

图 8-1

对PPS的查询协议具体内容见附录A公开参数查询协议部分。

6.2. 单向用户身份鉴别协议

6.2.1. 接收者认证发起者身份的鉴别协议

1) 非挑战应答方式

其特点是接收者B直接验证声明者A的身份，见图8-2。

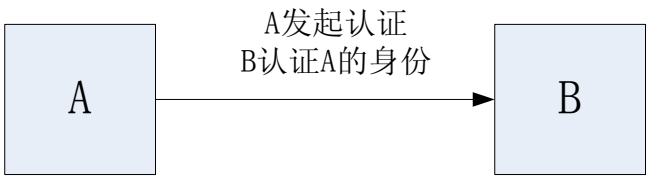

图 8-2

声明者A发起认证过程，由接收者B对其身份进行鉴别。提交的用于验证的数据记作令牌Token，其唯一性/时效性通过产生并验证时间戳或者顺序号进行控制。

具体内容如下：

A：A向B发送TokenAB,

A to B：$ID_A \| TokenAB$, 也可表示为{ ID_A, TokenAB }

声明者A发送给验证者B的令牌记作TokenAB

$TokenAB= ID_B \| t^A \| Text1 \| sign_A(ID_B \| t^A \| Text1)$,也可表示为，

$TokenAB=\{ID_B, t^A, Text1, sign_A(ID_B, t^A, Text1)\}$ 。

ID_B为验证者B的唯一性标识。

t^A为表示唯一性的时间戳或者由声明者产生的顺序号。

$sign_A$为声明者A的签名。

Text1为可选项，其他需要传递的信息。如果有信息需要加密传输，则应以数字信封方式进行封装。

请求被认证的格式如下：

```
RequestAuthenticated::=SEQUENCE{
        userIDA         IBCIdentityInfo,
        authToken       AuthToken
}
AuthToken::=SEQUENCE{
        userIDB         IBCIdentityInfo,
```

```
        verifier        Verifier,
        text1           OCTET STRING Option,
        userSignature   SM9Signature
}
Verifier::= CHOICE{
        generalTime         GeneralizedTime,
        serialNumber        INTEGER Option
}
```

SM9Signature的定义见GM/T BBBB。

B：验证A的认证信息

B接收A发来的含有TokenAB的消息后，进行认证鉴别，见图8-3。

具体内容如下：

a) B根据A的标识生成A的公钥，如果B没有生成A公钥的公共参数，应从公开参数服务系统PPS中获取；

b) 检验包含在令牌中的A的签名信息；

- 检验 TokenAB 中 ID_B标识段的值，是否等于实体 B 的标识符；
- 验证数字签名的正确性；
- 检验唯一性/时效性；
- 解析 Text1.

若任一验证结果不正确，则停止通联，且反馈：认证失败信息。

若验证正确，则完成认证鉴别。

2) 挑战应答方式

当采用挑战应答方式时t^A代表一个随机数，具体内容如下：

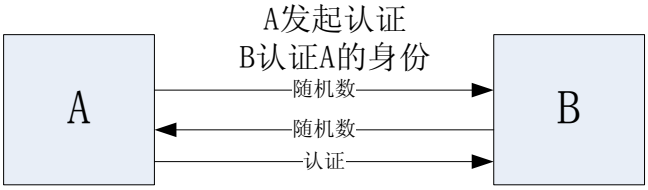

图8-3

A：A向B发送请求带着随机数t^A。

A to B：$ID_A \| t^A$

请求被认证的格式如下：

```
RequestHello::=SEQUENCE{
        userIDA         IBCIdentityInfo,
        randeom         INTGER
}
```

B：回复A一个随机数t^B。

B to A： t^B

请求被认证的格式如下：

```
ResponseHell        INTGER
```

A：A向B发送TokenAB。

A to B：$ID_A \| TokenAB$, 也可表示为{ ID_A, TokenAB }

TokenAB= $ID_B \| Text1 \| sign_A(ID_B \| H \| Text1)$

$H=Hash(t^A \| \Delta t^B)$，$\Delta t^B$是一个预约变化量。

请求被认证的格式如下：

```
RequestAuthenticated::=SEQUENCE{
        userIDA         IBCIdentityInfo,
        authTokenC      AuthTokenC
}
AuthTokenC::=SEQUENCE{
        userIDB         IBCIdentityInfo,
        text1           OCTET STRING Option,
        userSignature   SM9Signature
}
```

B：验证A的认证信息

B接收A发来的含有TokenAB的消息后，进行认证鉴别。

6.2.2. 声明者认证接收者身份的鉴别协议

其特点是声明者A要求接收者B向A证明自己的身份，要求获取B的签名并验证，见图8-4。

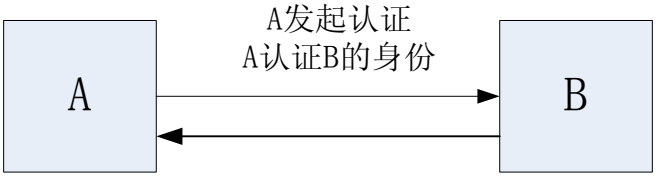

图 8-4

声明者A发起认证过程，接收者B回应A的要求并将自身的身份信息返回给A，由A对其身份进行鉴别。提交的用于验证的数据记作令牌Token，其唯一性/时效性通过产生并验证时间戳或者顺序号进行控制。

具体内容如下：

A：A向B发送获取验证B身份信息的要求。

A to B：$ID_A \| t^A \| Text1$, 也可表示为{ ID_A, t^A, Text1 }

ID_A为声明者B的唯一性标识。

t为表示唯一性的时间戳、由声明者产生的顺序号或者随机数。

Text1为可选项，其他需要传递的信息。

要求认证对方的格式如下：

```
RequireAuthentication::=SEQUENCE{
      userIDA         IBCIdentityInfo,
      verifier        Verifier,
      text            OCTET STRING Option
}
```

B：B向A返回确认其身份的信息。

B to A：$ID_B \| TokenBA$, 也可表示为{ ID_B, TokenBA }

接收者B发送给声明者A的令牌记作TokenBA

$TokenBA= ID_A \| t^A \| Text2 \| sign_B(ID_A \| \Delta t^A \| Text2)$,也可表示为，

$TokenBA=\{ID_A, t^A, Text2, sign_B(ID_A, \Delta t^A, Text2)\}$ 。

ID_A为声明者A的唯一性标识。

t^A为可选项，由于A对该值已知，B在向A返回时可以不再附带之。

Δt^A为表示唯一性的时间戳或者由声明者产生的顺序号、随机数的变化值，例如t^A+1。

$Sign_B$为接收者B的签名。

Text2为可选项，其他需要传递的信息。如果有信息需要加密传输，则应以数字信封方式进行封装。

回应的格式同RequestAuthenticated：

ResponseAuthentication RequestAuthenticated

A：验证B的认证信息

声明者A接收B发来的含有TokenAB的消息后，进行认证鉴别。

具体内容如下：

a）A根据B的标识生成B的公钥，如果A没有生成B公钥的公共参数，应从公开参数服务系统PPS中获取；

b）检验包含在令牌中的B的签名信息；

- 检验 TokenBA 中 ID_A标识段的值，是否等于实体 A 的标识符；
- 验证数字签名的正确性；
- 检验唯一性/时效性；
- 解析 Text2.

若任一验证结果不正确，则停止通联，且反馈：认证失败信息。

若验证正确，则完成认证鉴别。

6.3. 双向用户身份鉴别协议

其特点是接收者B验证声明者A的身份，接收者B也向A证明自己的身份，见图8-5。

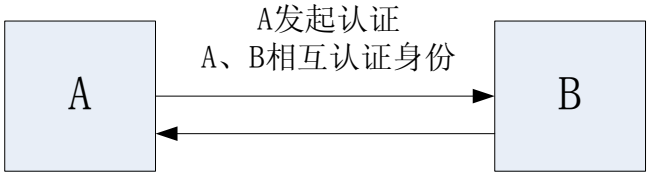

图 8-5

A签名，将签名值发给B

B直接验证

B签名，将签名值发给A

A直接验证

声明者A发起认证过程，先由接收者B对其身份进行鉴别。接收者B在将自身的身份信息返回给A，由A对其身份进行鉴别。提交的用于验证的数据记作令牌Token，其唯一性/时效性通过产生并验证时间戳或者顺序号进行控制。

具体内容如下：

A：A向B发送TokenAB,

A to B：$ID_A \| TokenAB$, 也可表示为{ ID_A, TokenAB }

声明者A发送给验证者B的令牌记作TokenAB

$TokenAB= ID_B \| t^A \| Text1 \| sign_A(ID_B \| t^A \| Text1)$,也可表示为，

$TokenAB=\{ID_B, t^A, Text1, sign_A(ID_B, t^A, Text1)\}$ 。

t为表示唯一性的时间戳或者由声明者产生的顺序号、随机数。

$sign_A$为声明者A的签名。

ID_B为验证者B的唯一性标识。

Text1为可选项，其他需要传递的信息。如果有信息需要加密传输，则应以数字信封方式进行封装。

采用RequireAuthentication定义。

B：验证A的认证信息

B接收A发来的含有TokenAB的消息后，进行认证鉴别。

具体内容如下：

a) B根据A的标识生成A的公钥，如果B没有生成A公钥的公共参数，应从公开参数服务系统PPS中获取；

b) 检验包含在令牌中的A的签名信息；

- 检验 TokenAB 中 ID_B标识段的值，是否等于实体 B 的标识符；
- 验证数字签名的正确性；
- 检验唯一性/时效性；
- 解析 Text1.

若任一验证结果不正确，则停止通联，且反馈：认证失败信息。

若验证正确，则完成认证鉴别。

B：B向A返回确认其身份的信息。

B to A：$ID_B \| TokenBA$, 也可表示为{ ID_B, TokenBA }

接收者B发送给声明者A的令牌记作TokenBA

$TokenBA= ID_A \| t^A \| Text2 \| sign_B(ID_A \| \Delta t^A \| Text2)$,也可表示为，

$TokenBA=\{ID_A, t^A, Text2, sign_B(ID_A, \Delta t^A, Text2)\}$ 。

ID_A为声明者A的唯一性标识。

t^A为可选项，由于A对该值已知，B在向A返回时可以不再附带之。

Δt^A为表示唯一性的时间戳或者由声明者产生的顺序号、随机数的变化值，例如t^A+1。

$Sign_B$为接收者B的签名。

Text2为可选项，其他需要传递的信息。如果有信息需要加密传输，则应以数字信封方式进行封装。

采用RequestAuthenticated定义。

A：验证B的认证信息

声明者A接收B发来的含有TokenAB的消息后，进行认证鉴别。

具体内容如下：

a) A根据B的标识生成B的公钥，如果A没有生成B公钥的公共参数，应从公开参数服务系统PPS中获取；

b) 检验包含在令牌中的B的签名信息；

- 检验 TokenBA 中 ID_A标识段的值，是否等于实体 A 的标识符；
- 验证数字签名的正确性,验证签名时要按照 TokenBA 的验证包按照 $ID_A \| \Delta t^A \|$ Text2 的格式进行组织；
- 检验唯一性/时效性；
- 解析 Text2.

若任一验证结果不正确，则停止通联，且反馈：认证失败信息。

若验证正确，则完成认证鉴别。

附 录 A
（规范性附录）
公共参数查询协议

A.1 描述

本附录定义了与公开参数服务系统（PPS）进行信息查询的相关协议，协议格式基于XML格式规范进行编写。

A.2 获取PPS服务信息

用于获取PPS支持的IBC密钥管理基础设施或者IBC密钥管理系统的数量和类型。

```
PPSInfoRequest::= SEQUENCE {
    version             INTEGER { v1(1) },
    id                  ibcIdentityInfo
    time                GeneralizedTime
}
```

version版本号项，本文中定义为1。
id标识项，为查询者的身份标识。
time时间项，返回的时间，采用格林威治格式。

A.3 获取PPS服务信息应答

用于PPS基本信息的回复。

```
PPSInfoResponse::= SEQUENCE{
  responseCode            INTEGER,
  ppsInfo             PPSInfo,
  signInfo                IbcSignInfo
}
IbcSignInfo::= SEQUENCE {
  signData                IbcSignData,
  algorithm               OBJECT IDENTIFIER
}

PPSInfo::= SEQUENCE {
  version             INTEGER {v1(1)},
  id                  ibcIdentityInfo
  responseKgsItem ::= SET OFKgsInfo,
```

```
  time                    GeneralizedTime,
  algorithm               OBJECT IDENTIFIER
}
KgsInfo ::=SEQUENCE{
  kgsName             OCTET STRING,
  kgsIDInfo           ibcIdentityInfo
  algorithm               OBJECT IDENTIFIER
}
```

PPSInfoResponse:表示PPS的应答信息。

responseCode：表示应答的返回码 0标识正确其他标识错误。

PPSInfo：表示PPS的相关信息。

version版本号项，本文中定义为1。

id标识项，为PPS的身份标识。

responseKgsItem返回密钥生成服务器信息的集合，代表该PPS中支持那些密钥生成服务器。

KgsInfo密钥生成服务器信息项，如果查询成功将返回kgsName、kgsIDInfo项。

kgsName密钥生成服务器名称项，PPS所服务的密钥生成服务器或IBC系统（仅限支持一组主密钥）的名称。

kgsIDInfo密钥生成服务器标识项，PPS所服务的密钥生成服务器或IBC系统（仅限支持一组主密钥）的ID标识。

algorithmKgs支持的算法标识

time时间项，返回的时间，采用格林威治格式。

IbcSignInfo：签名信息

signData签名项，PPS的签名信息，内容包括PPSInfo。

algorithm签名用的算法标识

A.4 公开参数信息查询

用于向PPS查询IBC系统公开参数的请求。

```
PublicParameterRequest::= SEQUENCE {
  version             INTEGER {v1(1)},
  id                  ibcIdentityInfo,
  kgsIDInfo           ibcIdentityInfo,
  time                    GeneralizedTime
}
```

version版本号项，本文中定义为1。

id标识项，为查询者的身份标识。

kgsIDInfo 查询条件，查询密钥生成服务器的标识信息，以PPS基本信息之一作为获取PPS中某组公开参数的查询条件。

time时间项，查询时间，采用格林威治格式。

A.5 公开参数信息查询应答

用于PPS对公开参数查询的回复。

```
PublicParameterResponse::= SEQUENCE{
  responseCode            INTEGER,
  publicParameter     PublicParameter,
  signInfoIbc         SignInfo
}
IbcSignInfo::= SEQUENCE {
  signData                IbcSignData,
  algorithm           OBJECT IDENTIFIER
}

PublicParameter::= SEQUENCE {
  version             INTEGER {v1(1)},
  parameter           IBCSysParams,
  id                  ibcIdentityInfo,
  time                    GeneralizedTime,
  algorithm               OBJECT IDENTIFIER
}
```

PublicParameterResponse 公共参数应答信息。
responseCode：表示应答的返回码 0标识正确其他标识错误。
publicParameter：是公共参数信息。
version版本号项，本文中定义为1。
parameter公开参数项。如果查询成功将返回公开参数内容IBCSysParams；
id标识项，为PPS的身份标识。
time时间项，返回的时间，采用格林威治格式。
algorithm算法标识项，表示该kgs支持的算法。
IbcSignInfo：签名信息。
signData签名项，PPS的签名信息，内容包括PublicParameter。
algorithm签名用的算法标识。

A.6 用户标识查询

用于向PPS查询用户的标识参数的请求。

```
ibcUserInfoRequest ::= SEQUENCE {
  version             INTEGER { v1(1) },
  id                  OCTET STRING,
  time                    GeneralizedTime
}
```

version版本号项，本文中定义为1。

Id用户ID标识项，被查询的用户标识。
time时间项，查询时间，采用格林威治格式。

A.7 用户标识查询应答

应答内容包括：正确＋有效标识，无效＋有效标识，无效

```
IbcUserInfoResponse::= SEQUENCE{
  responseCode            INTEGER,
  ibcUserInfo         IbcUserInfo,
  signInfo                IbcSignInfo
}
IbcSignInfo::= SEQUENCE {
  algorithm           OBJECT IDENTIFIER,
  signData                IbcSignData
}


IbcUserInfo ::= SEQUENCE {
  version             INTEGER { v1(1) },
userInfo ::= SET OFUserInfo,
  time                    GeneralizedTime,
}

UserInfo::=SEQUENCE{
  userStatusCode      INTEGER,
  userIDInfo          ibcIdentityInfo,
  publishTime         GeneralizedTime,
}
```

IbcUserInfoResponse 用户信息查询应答
responseCode，表示应答的返回码 0标识正确其他标识错误。
ibcUserInfo，ibc 用户信息。
version版本号项，本文中定义为1。
userInfo，用户基本信息的集合。
userStatusCode标识状态项，表示当前用户标识信息的状态。
userIDInfo，表示用户标识信息。
publishTime，用户信息的发布时间。
time时间项，返回的时间，采用格林威治格式。
algorithm签名用的算法标识。
IbcSignInfo，签名信息。
signData签名项，PPS的签名信息，内容包括IbcUserInfo。

A.8 IBC公共参数结构

```
IBCSysParams ::= SEQUENCE {
    version                 INTEGER { v2(2) },
    districtName            IA5String,
    districtSerial          INTEGER,
    validity                Validity,
    ibcPublicParameters     IBCPublicParameters,
    ibcIdentityType         OBJECT IDENTIFIER,
    ibcParamExtensions      IBCParamExtensions OPTIONAL
}
```

version 版本域确定了 IBCSysParams 格式的版本。本文中提及的格式，必须设置为 2。

districtName 域是一个必须以 URI 或者 IRI 编码的 IA5 字符串

districtSerial 域是一个代表了可用的唯一 IBC 公共参数(对于以 districtName 定义的 URI 或 IRI）设置的整数。如果为 districtName 公布一个新的参数，那么 districtSerial 的数值必须大于之前使用的 districtSerial 数值。

validity 有效域确定了一个具体 IBCSysParams 范例的寿命，并按照以下内容确定：

notBefore 与 notAfter 的数值必须以格林威治时间表示，并包含秒（如：时间表示为 YYYYMMDDHHMMSSZ），即使是秒数为零，同时还用表示为最近的秒数。客户必须确认它使用的 IBC 公共参数的日期处于 IBC 公共参数的 notBefore 时间与 notAfter 时间之间，于此同时，如果日期没有处于这一区间时，不能使用用于 IBC 加密操作的参数。

当 ibcPublicParameters, ibcIdentityType 或者 ibcParamExtensions 的数值改变了一个区域时，IBC 公共参数必须重新生成与公布。客户必须在应用程序配置间隔内重新找回 IBC 公共参数，以确保参数的版本为最新。

IBCPublicParameters 域是一个包含了公共参数（对应于 PKG 支持的 IBC 算法式）的结构。其定义如下：

```
IBCPublicParameters ::= SEQUENCE (1..MAX) OF IBCPublicParameter
IBCPublicParameter   ::= SEQUENCE {
    ibcAlgorithm            OBJECT IDENTIFIER,
    publicParameterData     OCTET STRING
}
```

ibcAlgorithm OID 确定了 IBC 算法式。两个 IBC 算法式的 OID 以及他们的 publicParameterData 结构。

publicParameterData 是一个 DER 编码结构，其包含了真实的加密参数。其具体结构取决于算法式。

ibcIdentityType 域是一个确定了在这一区域使用的身份类型的 OID。对于每一个 OID、所需要以及选择性的域都应为依赖于应用程序而存在的。

IBCParamExtensions 域是一组用于确定特定操作所需额外参数的一组扩展。定义如下：

```
IBCParamExtensions ::= SEQUENCE OF IBCParamExtension

IBCParamExtension ::= SEQUENCE {
    ibcParamExtensionOID        OBJECT IDENTIFIER,
    ibcParamExtensionValue      OCTET STRING
}
```

ibcParamExtensionValue 的八位字符串内容由具体的 ibcParamExtensionOID 确定。一个

域的 IBCParamExtensions 可能包含任何数量的扩展（包括零在内）。一个实际应用的扩展实例如下：它为电子邮件系统用户提供了一个 URI，在这里加密的信息可以被解密，同时对用户可见。另一个实例如下：它提供了商标信息以使得银行可以为处于不同业务部门的客户提供不同的用户界面。

```
ibcParamExt OBJECT IDENTIFIER ::= {
    ibcs ibcs3(3) parameter-extensions(2)
}
```

参考文献

[1] GB/T 15843.1-2008 信息技术 安全技术 实体鉴别 第3部分:采用数字签名技术的机制

[2] GB/T 16262.1-2006 信息技术 抽象语法记法一（ASN.1)：基本记法规范(ISO/IEC 8824-1:2002，IDT)

[3] RFC5408 IETF Identity-Based Encryption Architecture and Supporting Data Structures January 2009

[4] RFC5409 IETF Using the Boneh-Franklin and Boneh-Boyen Identity-Based Encryption January 2009