

eID服务标准

HB-╳╳-╳╳╳-╳╳╳╳

eID应用服务机构技术规范

版本号：1.0.0

╳╳╳╳-╳╳-╳╳实施

╳╳╳╳-╳╳-╳╳发布

公安部第三研究所 发布

目　　录

[前言 I](#_Toc422413253)

[1 范围 1](#_Toc422413254)

[2 规范性引用文件 1](#_Toc422413255)

[3 术语、定义和缩略语 1](#_Toc422413256)

[4 概述 2](#_Toc422413257)

[5 系统结构 2](#_Toc422413258)

[6 技术实现流程 3](#_Toc422413259)

[6.1 eID运营机构验证方式 3](#_Toc422413260)

[6.1.1 实名认证 3](#_Toc422413261)

[6.1.2 HMAC实名认证 4](#_Toc422413262)

[6.1.3 签名认证 5](#_Toc422413263)

[6.1.4 HMAC签名验证 6](#_Toc422413264)

[6.2 eID应用服务机构验证方式 6](#_Toc422413265)

[7 eID应用服务机构管理 7](#_Toc422413266)

[7.1 申请/审核/开通 7](#_Toc422413267)

[7.2 暂停/恢复 7](#_Toc422413268)

[7.3 终止服务 8](#_Toc422413269)

[8 应用接入管理 8](#_Toc422413270)

[8.1 申请/审核/开通 8](#_Toc422413271)

[8.2 暂停/恢复 9](#_Toc422413272)

[8.3 密钥更换 9](#_Toc422413273)

[9 接口要求 9](#_Toc422413274)

[9.1 AP－eID应用服务机构 9](#_Toc422413275)

[9.1.1 实名认证 9](#_Toc422413276)

[9.1.2 HMAC实名认证 9](#_Toc422413277)

[9.1.3 签名验证 10](#_Toc422413278)

[9.1.4 HMAC验证 10](#_Toc422413279)

[9.2 eID应用服务机构－eID运营机构 10](#_Toc422413280)

[9.2.1 PKI实名认证 10](#_Toc422413281)

[9.2.2 HMAC实名认证 10](#_Toc422413282)

[9.2.3 签名验证 10](#_Toc422413283)

[9.2.4 HMAC验证 11](#_Toc422413284)

[9.2.5 提交AP注册信息 11](#_Toc422413285)

[9.2.6 AP状态变更通知（暂停／恢复／终止） 11](#_Toc422413286)

[9.2.7 AP密钥更换 11](#_Toc422413287)

[10 密钥管理 12](#_Toc422413288)

[11 安全要求 12](#_Toc422413289)

[12 编制历史 12](#_Toc422413290)

前言

本标准的目的。

本标准包括的主要内容，或修订的主要内容。

本标准是eID系列标准之一，该系列标准的结构、名称或预计的名称如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 标准编号 | 标准名称 |
| 例 |  |  |
| [1] | HB-X-XXX-2015 | eID服务术语表 |
| [2] | HB-X-XXX-2015 | eID服务业务规范 |
| [3] | HB-X-XXX-2015 | IDSP基础服务技术规范 |
| [4] | HB-X-XXX-2015 | AP与IDSP接口规范 |
| [5] |  | IDSP与eID中心接口规范 |
| [6] |  | IDSP与eID验证设备接口规范 |
| [7] | …… | …… |

本标准的附录     为标准性附录，附录     为资料性附录。

本标准由eID中心     号文件印发。

本标准由eID中心     提出，eID中心归口。

本标准起草单位：

本标准主要起草人：

# 范围

本标准规定了     ，供使用；适用于     。

规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。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标准，然而，鼓励根据本标准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标准。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 标准编号 | 标准名称 | 发布单位 |
| 例： |  |  |  |
| [1] |  |  |  |
| [2] |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

术语、定义和缩略语

下列术语、定义和缩略语适用于本标准：

1. eID中心: 权威eID颁发机构。
2. eID网络身份服务提供机构：简称IDSP，是指提供eID网络身份服务的机构,，包括eID运营机构和eID应用服务机构。
3. eID运营机构：Operating institution，简称OP，指的是向eID应用服务机构提供eID网络身份基础服务的机构。
4. eID应用服务机构：Application service institution，简称AS，指的是向互联网应用提供基于eID增值服务的机构。
5. 应用提供机构: Application provider，简称AP，基于eID的互联网应用服务。
6. eID专用验证设备：eID device，部署在eID运营机构的提供特定服务的设备。
7. eID标识：eidcode，是根据公民个人身份信息加密处理后得到的字符编码，长度为48字节，与公民个人身份具有可验证的唯一性对应关系。
8. eID应用标识：appeidcode， eID用户在具体应用上的唯一标识码。
9. eID载体标识：简称idcarrier，加载eID的载体唯一标识符。
10. 应用注册码：简称regcode，AP在注册时经eID中心生成的授权码，该码仅eID device能识别，用于生成appeidcode
11. 安全因子：security factor，报文通信中，用于生成加密密钥和签名密钥的8字节随机数。

概述

标准eID服务包括：

* 实名认证
* HMAC实名认证
* 签名验证
* HMAC验证
* PKI实名登录
* HMAC实名登录

系统结构

eID服务所涉及的三方包括：

* AP
* eID应用服务机构
* eID运营机构

三者之间的关系如下图所示。

eID运营机构

AP

eID应用服务机构

eID应用服务机构是面向AP提供eID服务的窗口。 AP将eID认证服务请求发送给eID应用服务机构，eID应用服务机构将其转发至eID运营机构，由eID运营机构完成对eID认证服务请求的验证，并将验证结果返回给eID应用服务机构，eID应用服务机构再将其返回给AP。

eID应用服务机构自建自建IT系统，对AP进行接入管理，接收来自AP的eID认证服务请求，并将其转发至eID运营机构进行验证。

技术实现流程

## PKI身份识别



流程描述：

1. AP发起实名认证请求，携带用户身份信息、原文、签名、签名类型、CertID、appid；
2. eID应用服务机构验证AP合法性，包括验证appid、appkey的准确性；并转发给eID运营机构实名认证请求，携带用户身份信息、原文、签名、CertID、appid、asid；
3. eID运营机构验证eID应用服务机构合法性。
4. eID运营机构验证用户身份，验证通过后生成appeidcode；
5. eID运营机构将验证结果反馈给eID应用服务机构，返回appeidcode；
6. eID应用服务机构将验证结果及appeidcode反馈给AP。

## HMAC身份识别



流程描述：

1. AP发起HMAC实名认证请求，携带用户身份信息、原文、HMAC签名值、签名类型、、idcarrier、appid；
2. eID应用服务机构验证AP合法性，包括验证appid、appkey的准确性；并转发HMAC实名认证请求，携带用户身份信息、原文、HMAC签名值、签名类型、idcarrier、asid；
3. eID运营机构验证eID应用服务机构合法性；
4. eID运营机构进行HMAC实名认证；
5. eID运营机构生成appeidcode；
6. eID运营机构将验证结果反馈给eID应用服务机构，返回appeidcode；
7. eID应用服务机构反馈验证结果及appeidcode给AP。

## PKI签名验证



流程描述：

1. AP发起签名验证请求，携带原文、签名、CertID、appid；
2. eID应用服务机构验证AP合法性，包括验证appid、appkey的准确性，并转发签名验证请求，携带原文、签名、CertID、appid，asid；
3. eID运营机构验证eID应用服务机构合法性；
4. eID运营机构验证签名；
5. eID运营机构生成appeidcode；
6. eID运营机构反馈给eID应用服务机构验证结果，返回appeidcode；
7. eID应用服务机构给AP返回验证结果，返回appeidcode。

## HMAC签名验证



流程描述：

1. AP发起HMAC验证请求，携带原文、HMAC、idcarrier、appid；
2. eID应用服务机构验证AP合法性，并转发AP验证请求，携带原文、HMAC、idcarrier、appid、asid；
3. eID运营机构验证eID应用服务机构合法性；
4. eID运营机构验证HMAC签名；
5. eID运营机构生成appeidcode；
6. eID运营机构返回验证结果，返回appeidcode；
7. eID应用服务机构返回验证结果，返回appeidcode。

## PKI实名登录



流程描述：

1. AP发起PKI实名登陆请求，携带原文、签名、CertID、appid；
2. eID应用服务机构验证AP合法性，包括验证appid、appkey的准确性，并转发签名验证请求，携带原文、签名、CertID、appid，asid；
3. eID运营机构验证eID应用服务机构合法性；
4. eID运营机构验证签名；
5. eID运营机构生成appeidcode；
6. eID运营机构反馈给身份信息索引值H2及appeidcode；
7. eID应用服务机构给AP返回身份信息索引值H2及appeidcode。

## HMAC实名登录

流程描述：

1. AP发起HMAC登陆请求，携带原文、HMAC、idcarrier、appid；
2. eID应用服务机构验证AP合法性，并转发AP验证请求，携带原文、HMAC、idcarrier、appid、asid；
3. eID运营机构验证eID应用服务机构合法性；
4. eID运营机构验证HMAC签名；
5. eID运营机构生成appeidcode；
6. eID运营机构反馈给身份信息索引值H2及appeidcode；
7. eID应用服务机构给AP返回身份信息索引值H2及appeidcode。

应用接入管理

AP若要使用eID相关服务，需要到eID应用服务机构提出申请，提交相关申请材料，eID应用服务机构审核通过后，提交到eID运营机构复审，通过后eID运营机构将资料提交到eID中心进行终审，终审通过后，eID运营机构为其开通服务，eID应用服务机构为AP办理系统对接。

## 应用注册



1. AP向eID应用服务机构提出申请，在eID应用服务机构的注册业务提交业务申请信息，并按要求提交纸质材料；
2. eID应用服务机构的业务人员审核申请材料，对于具有独立法人资格的客户，需确认其法人资格；对于不具独立法人资格的客户，需审核其组织机构代码证。
3. 审核通过后，eID应用管理机构提交AP注册信息到eID运营机构。
4. eID运营机构将提交AP注册信息到eID中心进行最终审核；
5. eID中心收到请求并审核通过后，生成appid、appkey分散因子，返回给eID运营机构，运营机构返回给eID应用服务机构。
6. eID应用服务机构存储appid/appkey\_foctor，并根据appkey\_foctor计算得出appkey。
7. eID应用服务机构为该AP开通eID服务；
8. eID应用服务机构向AP管理员返回服务开通消息，并以密文的方式发放给AP appid和appkey。

## 应用注册信息更新



1. AP向eID应用服务机构提出注册信息更新申请， eID应用服务机构的业务人员审核注册信息变更申请材料；
2. 审核通过后，eID应用管理机构提交AP注册信息更新资料到eID运营机构；
3. eID运营机构将提交AP注册信息更新资料到eID中心进行最终审核；
4. eID中心收到请求并审核通过后，给eID运营机构返回更新成功。
5. eID运营机构给eID应用服务机构返回更新成功。

## 应用服务状态同步



1、AP提交变更服务状态申请；

2、eID应用服务机构变更AP的服务状态；并同步到eID运营机构。

3、eID运营机构将服务状态提交到eID中心。

4、eID运营机构将eID中心成功的消息返回给eID应用服务机构。

5、eID应用服务机构想AP返回成功。

## 应用密钥变更



1、AP提交秘钥变更申请，选择秘钥类型；

2、eID应用服务机构秘钥变更申请及秘钥类型到eID运营机构。

3、eID运营机构将秘钥变更申请提交到eID中心。

4、eID中心生成新的appkey\_factor，并返回给eID运营运营机构。

5、eID运营机构接收新appkey\_factor，并返回给eID应用服务机构。

6、eID应用服务机构存储新appkey\_factor，并生成新的appkey。

7、eID应用服务机构以密文的方式将新appkey返回给AP。

8、在新密钥未正式启用前，新旧密钥同时并行，AS申请时输入旧密失效天数，AS、OP在失效天数到期后自动失效；但AS管理员可以立即对旧密进行失效。

接口要求

## AP－eID应用服务机构

### PKI身份识别

* 请求方：AP，响应方：eID应用服务机构
* 请求参数：用户身份信息、原文、签名、签名类型、CertID、idcarrier(可选)、appid
* 返回参数：认证结果、appeidcode
* eID应用服务机构的处理逻辑：

1. 接收AP的请求，转发给eID运营机构；
2. 接收eID运营机构的验证结果，转发给AP。

### HMAC身份识别

* 请求方：AP，响应方：eID应用服务机构
* 请求参数：用户身份信息、原文、HMAC、HMAC算法、CertID（可选）、idcarrier、appid
* 返回参数：认证结果、appeidcode
* eID应用服务机构的处理逻辑：
  1. 接收AP的请求，转发给eID运营机构；
  2. 接收eID运营机构的验证结果，转发给AP。

### PKI签名验证

* 请求方：AP，响应方：eID应用服务机构
* 请求参数：原文、签名、签名类型、CertID、idcarrier（可选）、appid
* 返回参数：验证结果、appeidcode
* eID应用服务机构的处理逻辑：
  1. 接收AP的请求，转发给eID运营机构；
  2. 接收eID运营机构的验证结果，转发给AP。

### HMAC签名验证

* 请求方：AP，响应方：eID应用服务机构
* 请求参数：原文、HMAC、HMAC算法、CertID（可选）、idcarrier、appid
* 返回参数：认证结果、appeidcode
* eID应用服务机构的处理逻辑：
  1. 接收AP的请求，转发给eID运营机构；
  2. 接收eID运营机构的验证结果，转发给AP。

### PKI实名登陆

* 请求方：AP，响应方：eID应用服务机构
* 请求参数：用户身份信息、原文、签名、签名类型、CertID、idcarrier(可选)、appid
* 返回参数：H2、appeidcode
* eID应用服务机构的处理逻辑：
  1. 接收AP的请求，转发给eID运营机构；
  2. 接收eID运营机构的返回结果，转发给AP。

### HMAC实名登陆

* 请求方：AP，响应方：eID应用服务机构
* 请求参数：用户身份信息、原文、签名、签名类型、CertID(可选)、idcarrier、appid
* 返回参数：H2、appeidcode
* eID应用服务机构的处理逻辑：
  1. 接收AP的请求，转发给eID运营机构；
  2. 接收eID运营机构的返回结果，转发给AP。

## eID应用服务机构－eID运营机构

### PKI身份识别

* 请求方：eID应用服务机构，响应方：eID运营机构
* 请求参数：用户身份信息、原文、签名、签名算法、CertID、idcarrier(可选)、应用服务机构id
* 返回参数：认证结果、appeidcode
* eID应用服务机构的处理逻辑：
  1. 接收AP的请求，转发给eID运营机构；
  2. 接收eID运营机构的验证结果，转发给AP。

### HMAC身份识别

* 请求方：eID应用服务机构，响应方：eID运营机构
* 请求参数：用户身份信息（可选）、原文、HMAC、HMAC算法、CertID（可选）、idcarrier、应用服务机构id
* 返回参数：认证结果、eidcode
* eID应用服务机构的处理逻辑：
  1. 接收AP的请求，转发给eID运营机构；
  2. 接收eID运营机构的验证结果，转发给AP。

### PKI签名验证

* 请求方：eID应用服务机构，响应方：eID运营机构
* 请求参数：原文、签名、签名算法、CertID、idcarrier(可选)、应用服务机构id
* 返回参数：验证结果、appeidcode
* eID应用服务机构的处理逻辑：
  1. 接收AP的请求，转发给eID运营机构；
  2. 接收eID运营机构的验证结果，转发给AP。

### HMAC签名验证

* 请求方：eID应用服务机构，响应方：eID运营机构
* 请求参数：原文、HMAC、HMAC算法、CertID（可选）、idcarrier、应用服务机构id
* 返回参数：认证结果、appeidcode
* eID应用服务机构的处理逻辑：
  1. 接收AP的请求，转发给eID运营机构；
  2. 接收eID运营机构的验证结果，转发给AP。

### 提交AP注册信息

* 请求方：eID应用服务机构，响应方：eID运营机构
* 请求参数：AP注册信息（名称，……）、应用服务机构id
* 返回参数：appid，appkey\_factor
* eID应用服务机构的处理逻辑：

1. 提交AP注册信息；
2. 存储eID运营机构返回的appid、appkey分散因子，根据appkey分散因子计算appkey，并将appid、appkey以密文方式返回给AP。

### 提交AP注册信息更新

* 请求方：eID应用服务机构，响应方：eID运营机构
* 请求参数：AP变更信息（名称，……）、应用服务机构id
* 返回参数：extension
* eID应用服务机构的处理逻辑：  
  1. 提交AP变更信息；

2. 接收eID运营机构返回成功消息。

### AP服务状态同步

* 请求方：eID应用服务机构，响应方：eID运营机构
* 请求参数：服务信息（服务类型，服务状态）、应用服务机构id
* 返回参数：extension
* eID应用服务机构的处理逻辑：  
  1. 提交AP服务状态；

2. 接收eID运营机构返回成功消息。

### AP密钥变更

* 请求方：eID应用服务机构，响应方：eID运营机构
* 请求参数：appid、应用服务机构id
* 返回参数：appid，appkey\_factor
* eID运营机构的处理逻辑：

1. 向eID中心申请密钥变更；
2. 根据eID中心返回的新appkey分散因子，存储，然后返回给eID应用服务机构；
3. eID应用服务机构根据新appkey分散因子生成appkey
4. eID应用服务机构将新appkey以密文方式返回给AP

密钥管理



采用三级密钥体系。eID运营机构保存根密钥（rk1）；eID应用服务机构保存二级根密钥rk2，用于生成appkey，并保护eID应用服务机构与eID运营机构之间的消息完整性；AP保存appkey，用于保护AP与eID应用服务机构之间的消息完整性。

eID应用服务机构需配置加密设备保存rk2，rk2的生成和导入应由eID运营机构以安全的方式完成。

对每个AP，将为其分配一个appkey，该密钥由eID中心生成分散因子，返回给eID应用服务机构，eID应用服务机构计算生成appkey，并以保密的形式发放给AP。

安全要求

eID应用服务机构若需保存用户敏感信息，需达到eID产业联盟制定的相关安全要求。

编制历史

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 版本号 | 更新时间 | 主要内容或重大修改 | 编制人 | 技术审核人 | 部门审核人 |
| 例： |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |