ICS 35.110
M 11

YD

中华人民共和国通信行业标准

YD/T 3150-2016

网络电子身份标识 eID 验证服务接口技术要求

Technical requirements for eID verification service interface

2016-07-11 发布　　2016-10-01 实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本标准属于网络电子身份标识eID相关服务与应用接口系列标准之一，该系列标准包括：

——《网络电子身份标识eID桌面应用接口技术要求》

——《网络电子身份标识eID移动应用接口技术要求》

——《网络电子身份标识eID验证服务接口技术要求》

——《网络电子身份标识eID桌面应用接口测试方法》

——《网络电子身份标识eID移动应用接口测试方法》

——《网络电子身份标识eID验证服务接口测试方法》

本标准依据GB/T 1.1-2009给出的规则起草。

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。

本标准由中国通信标准化协会提出并归口。

本标准由公安部第三研究所、中国科学院软件研究所、北京中电华大电子设计有限责任公司、国防科学技术大学计算机学院、北京邮电大学、中国科学院信息工程研究所等单位起草。

本标准主要起草人：邹　翔、杨明慧、汪志鹏、倪力舜、黄　俊、高志刚、兰　天、李树栋、落红卫、高　峰、柳　扬、全　拥、邓　璐、许　晋、周　薇、戴　娇。

引　言

本标准旨在规范第三方应用后台与eID服务平台交互参数的命名，统一交互方式，方便第三方应用接入，降低维护成本。

网络电子身份标识eID验证服务接口技术要求

1 范围

本标准规范了通过访问eID验证服务接口来实现第三方应用后台与eID服务平台进行交互的技术要求，主要内容包括第三方应用与eID服务平台的注册、eID桌面验证服务接口、eID移动验证服务接口以及数据交互中的签名机制。

本标准适用于第三方应用后台与eID服务平台的交互接口，并可供eID的其他应用接口参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GM/T 0005-2012 随机性检测规范

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

网络电子身份标识 Electronic Identity

用于在互联网上在线识别公民身份的电子标识，承载于智能安全芯片上，基于密码技术实现与公民真实身份的校验一一对应。

3.1.2

eID标识码 eID_code

eID的组成元素之一，长度为48字节，由公民真实身份信息和随机数经过eID服务平台生成和管理，本身不含公民身份信息。

3.1.3

eID第三方应用 eID Third-Party Applications

由非eID载体持有人及非eID服务平台提供的、在客户端PC上或移动终端设备上的应用（如政府eService、电子商务eService），与eID卡一起提供某项事务的执行。

3.1.4

eID服务平台 eID Service Platform

提供eID的生成、存储、使用及维护等全生命周期业务处理相关服务的系统。

3.1.5

eID身份验证 eID Authentication

通过将所提交的eID身份声明与事先证明的信息进行比较来确认声明的eID身份是正确的过程。

3.1.6

eID身份注册　eID Registration

通过为实体的身份赋予唯一的eID标识码，提供一组作为声明的身份和/或权利的证据的数据，并签发eID载体，保证其真实性。

3.1.7

eID移动应用　eID Mobile Applications

通过eID移动客户端提供的第三方应用。

3.1.8

eID验证服务　eID Authentication Service

由eID服务平台提供给各第三方应用的身份识别及验证服务。

3.1.9

eID桌面应用　eID Personal Computer Application

通过eID桌面客户端提供的第三方应用。

3.2　缩略词

下列缩略语适用于本文件。

DSA	Digital Signature Algorithm	DSA数字签名算法
eID	electronic Identity	网络电子身份标识
PIN	Personal Identification Number	个人识别码
SDK	Software Development Kit	软件开发工具包
SM2		椭圆曲线公钥密码算法

4　eID 验证服务流程

eID验证服务是由eID服务平台提供给各第三方应用的一个后台认证服务。

当第三方应用需要使用eID验证服务来验证网络用户的访问请求时，第三方应用应完成相应的eID加密或签名运算，将结果封装成符合eID验证服务接口技术要求的形式，再传输给eID服务平台。eID服务平台在完成eID验证功能后，将验证结果按照eID验证服务接口技术要求的形式返回给第三方应用。第三方应用在每次验证服务请求时，验证服务都会返回一个随机数作为本次验证服务的挑战，随机数的产生遵循GM/T 0005-2012。eID验证服务的概要流程如图1所示。

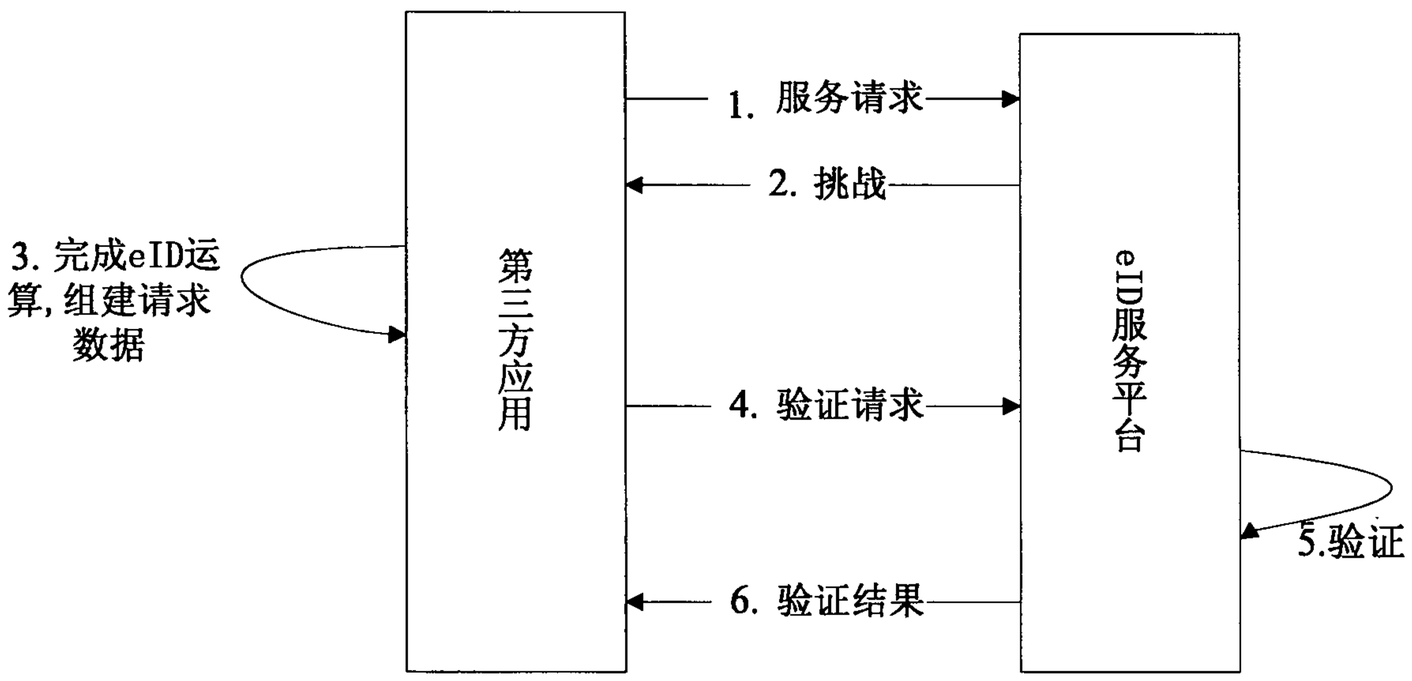

图1　eID 验证服务的流程

第一步，第三方应用根据需要向eID服务平台发送服务请求。

第二步，eID服务平台返回一个随机数作为本次验证服务的挑战。

第三步，第三方应用完成相应的eID运算，将待传输数据按照本标准中6.2节或7.2节的格式要求组建。

第四步，第三方应用将组建完成的数据作为验证请求，发送给eID服务平台。

第五步，eID服务平台在本地执行相关的验证服务。

第六步，eID服务平台返回相应的验证结果按照本标准中6.3节或7.3节的格式给第三方应用。

第三方应用接入eID验证服务前，需首先在eID服务平台进行注册，相关注册要求参照本标准的5.2节，eID服务平台对注册请求返回结果请参照本标准的5.3节。根据应用的不同，eID验证服务接口分为eID桌面验证服务接口和eID移动验证服务接口。

5 注册要求

5.1 概述

第三方应用接入eID验证服务前，需首先在eID服务平台进行注册，获得对应的应用标识与共享密钥，以保证后续流程与通讯以及正确对第三方应用与用户进行验证与授权。只有通过注册的应用系统，才能与eID验证服务接口建立合法的通信连接。eID验证服务将用应用注册信息，对每次应用访问进行安全访问审核。

5.2 注册请求参数

5.2.1 第三方应用信息

参数名称：app_info

参数类型：Char(50)

参数说明：待注册的第三方应用信息，为必选项。

5.2.2 第三方应用名称

参数名称：app_name

参数类型：Char(50)

参数说明：待注册的第三方应用名称，为必选项。

5.2.3 机构名称

参数名称：cmp_name

参数类型：Char(50)

参数说明：待注册的第三方应用所属机构名称，为必选项。

5.2.4 域名

参数名称：domain_name

参数类型：Char(80)

参数说明：待注册的第三方应用的域名，为必选项。

5.2.5 IP 地址

参数名称：ip_addr

参数类型：Char(15)

参数说明：待注册的第三方应用的IP地址，为必选项。

5.2.6 公钥证书

参数名称：sign_cert

参数类型：Char(100)

参数说明：待注册的第三方应用的数字签名证书，可空，为必选项。

5.2.7 应用类型

参数名称：app_type

参数类型：Char(5)

参数说明：待注册的第三方应用的类型，为必选项。

5.2.8 签名算法

参数名称：sign_type

参数类型：Char(2)

参数说明：DSA、RSA、MD5三个值可选,用2、1、0表示；为必选项。

5.2.9 结果返回地址

参数名称：return_url

参数类型：Char（255）

参数说明：返回结果的URL地址,可空，为必选项。

5.3 eID 服务平台返回参数

5.3.1 第三方应用信息

参数名称：app_info

参数类型：Char(50)

参数说明：待注册的第三方应用信息，为必选项。

5.3.2 第三方应用名称

参数名称：app_name

参数类型：Char(50)

参数说明：待注册的第三方应用名称，为必选项。

5.3.3 机构名称

参数名称：cmp_name

参数类型：Char(50)

参数说明：待注册的第三方应用所属机构名称，为必选项。

5.3.4 域名

参数名称：domain_name

参数类型：Char(80)

参数说明：待注册的第三方应用的域名，为必选项。

5.3.5 IP 地址

参数名称：ip_addr

参数类型：Char(15)

参数说明：待注册的第三方应用的IP地址，为必选项。

5.3.6 公钥证书

参数名称：sign_cert

参数类型：Char(100)

参数说明：待注册的第三方应用的数字签名证书，可空，为必选项。

5.3.7 应用类型

参数名称：app_type

参数类型：Char(5)

参数说明：待注册的第三方应用的类型，为必选项。

5.3.8 签名算法

参数名称：sign_type

参数类型：Char(2)

参数说明：DSA、RSA、MD5三个值可选,用2、1、0表示；为必选项。

5.3.9 结果返回地址

参数名称：return_url

参数类型：Char（255）

参数说明：返回结果的URL地址，可空，为必选项。

5.3.10 第三方应用标识

参数名称：app_id

参数类型：Char(39)

参数说明：注册在eID服务平台的唯一的应用号，前两位为标识位，默认为DF，公安应用前两位为GA，由eID服务平台颁发。为必选项。

5.3.11 共享密钥

参数名称：app_key

参数类型：Char（100）

参数说明：由eID服务平台产生，为必选项。

5.3.12 服务器 URL

参数名称：server_url

参数类型：Char（255）

参数说明：请求服务的地址，为必选项。

5.3.13 服务器公钥证书

参数名称：server_cert

参数类型：Char(100)

参数说明：第三方应用对返回结果验签所需的证书文件，可空，为必选项。

6 eID 桌面验证服务接口

6.1 简介

eID桌面验证服务接口为eID桌面应用中第三方应用与eID服务平台的交互提供交互协议与数据传输格式要求。数据的传输包含第三方应用发往eID服务平台的请求参数与eID服务平台返回给第三方应用的返回参数。

6.2 第三方应用请求参数

6.2.1 第三方应用 ID

参数名称：app_id

参数类型：Char(39)

参数说明：注册在eID服务平台的唯一的应用号，前两位为标识位，默认为DF，公安应用前两位为GA（注册返回信息中获取），为必选项。

6.2.2 签名方式

参数名称：sign_type

参数类型：Char(2)

参数说明：DSA、RSA、MD5三个值可选，用2、1、0表示，为必选项。

6.2.3 签名

参数名称：sign

参数类型：Char(100)

参数说明：见附录A 签名机制（现默认RSA），为必选项。

6.2.4 结果返回 URL

参数名称：return_url

参数类型：Char(255)

参数说明：结果返回第三方应用路径，为必选项。

6.2.5 业务流水号

参数名称：biz_sequence_id

参数类型：Char(64)

参数说明：应用针对本次请求的唯一标识串码，为必选项。

6.2.6 请求时间

参数名称：apply_time

参数类型：Char(19)

参数说明：时间，格式为yyyy-mm-dd hh:mm:ss；为必选项。

6.2.7 业务类型

参数名称：biz_type

参数类型：Char(2)

参数说明：为必选项。业务类型包括：1）桌面账号绑定；2）桌面账号找回；3）移动一键账号绑定；4）移动一键账号找回；5）桌面安全登录；6）移动一键安全登录；7）移动实名认证；8）后台实名认证。

6.2.8 安全等级

参数名称：security_class

参数类型：Char(1)

参数说明：业务对应用的安全等级，为必选项。

6.2.9 eID 用户信息

参数名称：eid_user_info

参数类型：Char

参数说明：在支付业务中，通过eID支付终端SDK签名函数获得的用户信息。可选项。

6.2.10 eID 签名值

参数名称：eid_sign_info

参数类型 ：Char

参数说明：实名认证中，通过eID支付终端SDK签名函数获得的签名结果，为必选项。

6.2.11 签名算法 ID

参数名称：sign_algorithm_id

参数类型：Char(4)

参数说明：用户用eID设备签名的算法ID，为必选项。

6.2.12 待签信息原文

参数名称：data_to_sign

参数类型：Char(2000)

参数说明：用户发起的交易原文明文。为可选项。

6.2.13 eID 属性信息

可选项。待定。

6.2.14 消息扩展

参数名称：extension

参数类型：Char(200)

参数说明：为后续应用提供一些扩展服务，为必选项。

6.3 eID 服务平台返回参数

6.3.1 返回结果

参数名称：result

参数类型：Char(5)

参数说明：业务处理结果，为必选项。

6.3.2 签名方式

参数名称：sign_type

参数类型：Char(2)

参数说明：SM2、SM3、DSA、RSA、MD5五个值可选，用4、3、2、1、0表示。为必选项。

6.3.3 签名

参数名称：sign

参数类型：Char(100)

参数说明：见附录A 签名机制（现默认RSA），为必选项。

6.3.4 业务流水号

参数名称：biz_sequence_id

参数类型：Char(64)

参数说明：针对本次请求及应答的唯一标识串码，为必选项。

6.3.5 返回时间

参数名称：result_time

参数类型：Char(19)

参数说明：时间，格式为yyyy-mm-dd hh:mm:ss，为必选项。

6.3.6 eID 标识码

参数名称：eID_code

参数类型：Char(80)

参数说明：用户登录的eID标识码，为必选项。

6.3.7 用户账户

参数名称：user_account

参数类型：Char(80)

参数说明：用户在第三方应用注册的账号，为必选项。

6.3.8 消息扩展

参数名称：extension

参数类型：Char(200)

参数说明：无，为必选项。

7 eID 移动验证服务接口

7.1 简介

eID移动验证服务接口为eID移动应用中第三方应用与eID服务平台的交互提供交互协议与数据传输格式要求。数据的传输包含第三方应用发往eID服务平台的请求参数与eID服务平台返回给第三方应用的返回参数。

7.2 第三方应用请求参数

7.2.1 第三方应用 ID

参数名称：app_id

参数类型：Char(39)

参数说明：注册在eID服务平台的唯一的应用号，前两位为标识位，默认为DF，公安应用前两位为GA（注册返回信息中获取），为必选项。

7.2.2 签名方式

参数名称：sign_type

参数类型：Char(2)

参数说明：DSA、RSA、MD5三个值可选，用2、1、0表示；为必选项

7.2.3 签名

参数名称：sign

参数类型：Char(100)

参数说明：见附录A 签名机制（现默认RSA）；为必选项。

7.2.4 结果返回 URL

参数名称：return_url

参数类型：Char(255)

参数说明：结果返回第三方应用路径，为可选项。

7.2.5 业务流水号

参数名称：biz_sequence_id

参数类型：Char(64)

参数说明：应用针对本次请求的唯一标识串码；为必选项。

7.2.6 请求时间

参数名称：apply_time

参数类型：Char(19)

参数说明：时间，格式为yyyy-mm-dd hh:mm:ss；为必选项。

7.2.7 手机号

参数名称：user_phone

参数类型：Char(15)

参数说明：手机号，为必选项。

7.2.8 业务类型

参数名称：biz_type

参数类型：Char(2)

参数说明：为必选项。业务类型包括：1）桌面账号绑定；2）桌面账号找回；3）移动一键账号绑定；4）移动一键账号找回；5）桌面安全登录；6）移动一键安全登录；7）移动实名认证；8）后台实名认证。

7.2.9 安全等级

参数名称：security_class

参数类型：Char(1)

参数说明：业务对应用的安全等级，为必选项。

7.2.10 消息扩展

参数名称：extension

参数类型：Char(200)

参数说明：无，为必选项。

7.3 eID 服务平台返回参数

7.3.1 结果

参数名称：result

参数类型：Char(5)

参数说明：业务处理结果，为必选项。

7.3.2 签名方式

参数名称：sign_type

参数类型：Char(2)

参数说明：DSA、RSA、MD5三个值可选，用2、1、0表示，为必选项。

7.3.3 签名

参数名称：sign

参数类型：Char(100)

参数说明：见附录A 签名机制（现默认RSA），为必选项。

7.3.4 业务流水号

参数名称：biz_sequence_id

参数类型：Char(64)

参数说明：针对本次请求及应答的唯一标识串码，为必选项。

7.3.5 返回时间

参数名称：result_time

参数类型：Char(19)

参数说明：时间，格式为yyyy-mm-dd hh:mm:ss；为必选项。

7.3.6 eID 标识码

参数名称：eID_code

参数类型：Char(80)

参数说明：用户登录的eID标识码，为必选项。

7.3.7 消息扩展

参数名称：extension

参数类型：Char(200)

参数说明：无，为必选项。

附　录　A
（资料性附录）
签名机制

A.1　需要参与签名的参数

在第三方应用与eID服务平台请求及返回的参数中，除去sign、sign_type两个参数外，其他需要使用到的参数皆为需签名参数。

A.2　生成待签名字符串

例如对于如下的参数数组：

string[] parameters = {

"app_id = 1234567890",

"return_url = http://www.test.com/verify/return_url.asp",

" biz_sequence_id = 12345678901234567890123456789012345678901234567890123456789012345678901234",

"apply_time = 2013-01-01 10:10:10",

"cellphone = 12345678901"

};

对数组里的每一个值从a到z的顺序排序，若遇到相同首字母，则看第二个字母，以此类推。排序完成之后，再把所有数组值以“&”字符连接起来，如：

app_id=001234567890&apply_time=2013-01-01 10:10:10&biz_sequence_id=12345678901234567890123456789012345678901234567890123456789012345678901234&cellphone=12345678901&return_url=http://www.test.com/verify/return_url.asp

最后直接连接app_key后得到字符串为，设app_key=”app_key”：

app_id=1234567890&apply_time=2013-01-01 10:10:10&biz_sequence_id=12345678901234567890123456789012345678901234567890123456789012345678901234&cellphone=12345678901&return_url=http://www.test.com/verify/return_url.aspapp_key

此串字符串便是待签名字符串。

参 考 文 献

[1] GB/T 16649.1-2006 识别卡.带触点的集成电路卡.第1部分:

[2] GB/T 16649.3-2006 识别卡.带触点的集成电路卡.第3部分:电信号和传输协议

[3] GB/T 16649.4-2006 识别卡.带触点的集成电路卡.第4部分:用于交换的结构、安全和命令

[4] GB/T 16649.6-2001 识别卡.带触点的集成电路卡.第6部分:行业间数据元

中华人民共和国
通信行业标准
网络电子身份标识 eID 验证服务接口技术要求
YD/T 3150-2016
*
人民邮电出版社出版发行
北京市丰台区成寿寺路 11 号邮电出版大厦
邮政编码：100164
北京康利胶印厂印刷

*
开本：880×1230　1/16　　2016 年 10 月第 1 版
印张：1.25　　2016 年 10 月北京第 1 次印刷
字数：30 千字
15115・1176
定价：20 元
本书如有印装质量问题，请与本社联系　电话：(010)81055492