ICS 35.040
L80

中华人民共和国国家标准

GB/T XXXXX.3—XXXX

信息安全技术 公民网络电子身份标识安全技术要求 第3部分：验证服务协议

Information security techniques—Security technical requirements for eID—Part 3: Verification service protocol

（征求意见稿）

（本稿完成日期：2017年6月）

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。

XXXX－XX－XX 发布　　XXXX－XX－XX

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

GB/T XXXXX《公民网络电子身份标识安全技术要求》分为三个部分：

——第 1 部分：读写机具安全技术要求

——第 2 部分：载体安全技术要求

——第 3 部分：验证服务协议

本部分为GB/T XXXXX的第3部分。

本部分依据GB/T 1.1-2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

本部分由全国信息安全标准化技术委员会提出并归口。

本部分主要起草单位：中国科学院软件研究所、公安部第三研究所、国防科学技术大学、商用密码检测中心。

本部分主要起草人：张立武、张严、杨明慧、邹翔、冯登国、胡传平、张振峰、汪志鹏、倪力舜、黄俊、高志刚、夏丽娟、余丹萍。

公民网络电子身份标识安全技术要求
第 3 部分：验证服务协议

1 范围

本部分规定了公民网络电子身份标识验证过程的参与方、网络电子身份标识验证服务接口的调用方式、消息格式和编码处理规则。本部分适用于网络电子身份标识验证服务及使用该服务的应用与系统的设计和开发。

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。

GB 13000-2010 信息技术 通用多八位编码字符集（UCS）

GB/T 25069-2010 信息安全技术 术语

GB/T 26231-2010 信息技术 开放系统互连 OID的国家编号体系和注册规程

IETF RFC 4648-2006 The Base16, Base32, and Base64 Data Encodings

3 术语

GB/T 25069-2010界定的以及下列术语适用于本文件。

3.1

网络电子身份 cyber electronic identity

用于网络在线识别个人身份的电子标识，也称网络电子身份标识，包括公民网络电子身份标识和普通网络电子身份标识。

3.2

普通网络电子身份标识 common cyber electronic identity

由证书认证机构颁发的用于网络在线识别个人身份的网络电子身份，通过嵌入公民网络电子身份标识码与公民网络电子身份标识建立关联关系。由一对非对称密钥和含有其中公钥及相关信息的数字证书组成。

3.3

公民网络电子身份标识 citizen cyber electronic identity；eID

由国家主管部门颁发，与个人真实身份具有一一对应关系，用于在线识别公民真实身份的网络电子身份。由一对非对称密钥和含有其公钥及相关信息的数字证书组成。

3.4

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。

3.5

eID 身份验证 eID verification

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。

3.6

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。

3.7

eID 移动应用 eID mobile application

在移动客户端上运行的 eID 应用。

3.8

eID 验证服务 eID authentication service

由 eID 服务平台提供给各应用的进行身份识别及验证的服务。

3.9

eID 桌面应用 eID desktop application

通过桌面客户端运行的 eID 应用。

4 缩略语

下列缩略语适用于本文件。

AP:应用服务提供商（Application Provider）

eID: 公民网络电子身份标识（citizen cyber Electronic IDentity）

HTTPS: 安全超文本传输协议（Hypertext Transfer Protocol over Secure Socket Layer）

OID: 对象标识符（Object Identifier）

PIN: 个人识别码（Personal Identification Number）

SDK: 软件开发工具包（Software Development Kit）

5 概述

eID系统的eID身份验证包含三个参与者：eID服务平台，应用服务提供商和持有eID的用户。

当应用服务提供商需要使用eID验证服务来验证网络用户的访问请求时，应用服务提供商应完成相应的eID加密或签名运算，将结果按照本部分所述封装成符合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应用服务提供商。应用服务提供商在每次发送验证服务请求时，验证服务都会返回一个随机数作为本次验证服务的挑战。上述流程如图1所示，具体步骤如下：

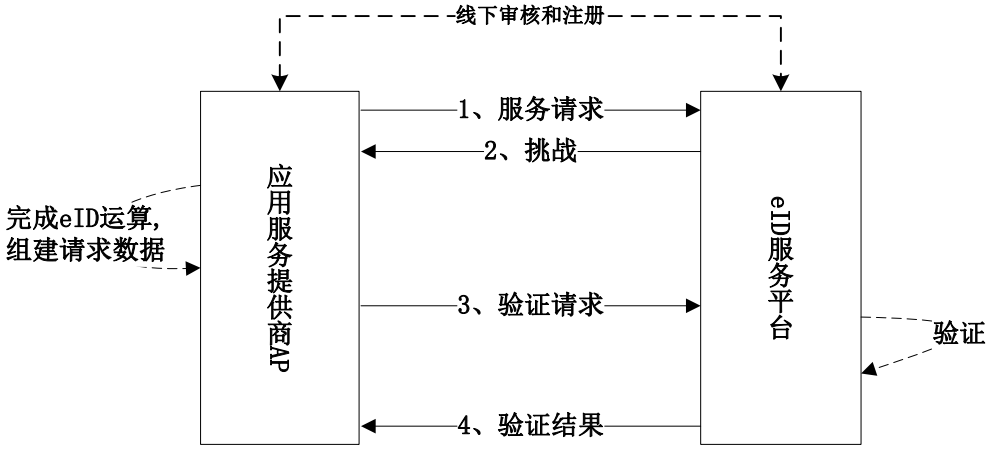

图1　eID 身份验证步骤

1）　应用服务提供商根据需要向 eID 服务平台发送服务请求。
2）　eID 服务平台返回一个随机数作为本次验证服务的挑战。
3）　应用服务提供商完成相应的 eID 运算,将待传输数据按照本部分中 8.2 节或 9.2 节所规定的格式要求组建。并将组建完成的数据作为验证请求，发送给 eID 服务平台。
4）　eID 服务平台在本地执行相关的验证服务后，按照本部分中 8.3 节或 9.3 节的格式返回相应的验证结果应用服务提供商。

AP在接入eID验证服务前，应首先在eID服务平台中进行注册，并获得对应的应用标识与共享密钥。以保证后续流程的执行，并使得eID服务平台可以对应用服务提供商AP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验证服务将使用应用注册信息对每次应用访问进行安全访问审核。例如：应用服务提供商AP提交ICP备案号，营业执照副本，税务登记证，组织机构代码证等材料给eID服务平台，来完成注册前的审核。相关注册要求见7.2节，eID服务平台对注册请求返回结果见7.3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。

6　公民网络电子身份标识验证服务接口处理规则

6.1　消息编码与处理规则

6.1.1　参数类型

本部分使用如下参数类型：

——Char：表示 GB 13000-2010 中所规定的字符集中的一个字符，本部分中所使用的字符类型参数仅包含可见字符，此外，本部分使用‘，’字符作为分隔符，因此参数的值不能包含‘，’字符。

——Byte：表示 8 比特长的单个字节。

——Char(X)表示长度固定为 X 个 Char 类型字符的参数。

——Char(A..B)表示长度为 A 至 B 个 Char 类型字符的参数。

——Byte(0..A)表示可为空且长度至多为 A 个 Byte 类型字节的参数。

6.1.2 参数编码规则

本部分所规定的接口应采用HTTPS信道进行传输。消息发送方（AP和eID平台）应按照以下步骤生成并发送请求参数：

1) 消息发送方将所有参数类型为 Byte()的参数的值按照 IETF RFC 4648-2006 中所述 Base64 编码规则进行编码，将其转化为 Char()类型。
2) 消息发送方将所有参数按照如下格式组装成 Char()类型的字符串：

{

“*参数标识 1*”:“*参数值 1*”,

“*参数标识 2*”:“*参数值 2*”,

…

“*参数标识 N*”:“*参数值 N*”,

}

其中名称/值对的名称应与本部分所规定的参数标识严格一致，各参数标识间无顺序。在组装时，应忽略所有的不可见字符，具体的请求参数示例见附录 B。

若某参数值为空，则在生成的字符串中，该参数的参数标识保留，参数值设为空（长度为 0 的字符串）。

3) 消息发送方将组装好的数据放入 http body 域中，并新增下列内容

HEAD：“idsp-protocol-version=2.0.0”

用来描述本协议内容的版本号。

4) 消息发送方使用 ISO/IEC 10646:2014 中规定的 UTF-8 编码格式对上述字符串进行编码，然后用 POST 方式将消息发送到请求地址。

6.2 参数解析要求

收到消息后，消息接收方应按照6.1节规定的对组装好的参数进行解析，获取各名称对应的参数值。对于使用本部分的消息接收方，在对收到的参数进行解析时应遵循以下要求：

1) 消息接收方按照 6.1 节规定的格式对收到的消息进行解析，即确定消息字符串的首字符与尾字符分别为‘*{*’与‘*}*’ 否则当成本次请求失败进行处理。
2) 使用‘，’作为分隔符将消息字符串分割成若干名称/值对。
3) 获取相应的名称/值对后，搜索第一个 ‘:’作为分隔符，将名称/值对解析为名称和值两部分。
4) 确定名称和值均以‘“’与‘”’作为起始与结束，否则当成本次请求失败进行处理。
5) 将名称的内容与本部分 7 至 9 章规定的各参数的参数标识相同的名称/值对进行处理。如果收到的消息不符合 6.1 节规定的数据格式，消息接收方应当成本次请求失败进行处理。
6) 在解析消息时，消息接收方应忽略名称未在本部分 7 至 9 章参数标识中出现的名称/值对。
7) 在解析消息时，如果存在多个名称相同的名称/值对，且格式符合本部分的规定，则消息接收方可根据需要当成本次请求失败进行处理或仅接收最后出现的名称/值对中的值。
8) 在解析消息时，消息接收方应确认收到的数据中值的长度符合本部分 7 至 9 章所规定的消息长度，否则当成本次请求失败进行处理。
9) 如果收到的数据中未包含一个或多个必选的参数所对应的名称/值对，或该参数的值不符合本部分定义的参数类型，消息接收方应当成本次请求失败进行处理。

各接口的请求与返回消息示例见附录 B。

6.3 接口调用方式

eID服务平台提供的接口调用方式分为异步调用和同步调用两种。

1) 当 AP 通过异步调用方式调用接口时，需要在请求消息中通过 return_url 参数发送一个供 eID 服务平台使用的结果返回地址。eID 服务平台会在收到 AP 发送的消息后返回确认消息，其内容为：*{“received”:”true”}*，表示请求已接收到，如果 AP 在预先定义的超时时间

后未收到 eID 服务平台的同步返回结果，应当成本次请求失败进行处理，不可以将相同的信息进行重复发送。超时时间可根据网络与应用实际情况制定。

随后，eID 服务平台会通过参数中 return_url 中包含的结果返回将业务处理结果返回给 AP，AP 在接收到 eID 服务平台的处理结果之后，需要向 eID 服务平台返回确认消息，其内容为：*{"received":"true"}*，表示已接收到结果。如果 eID 服务平台在超时时间内未收到 AP 的接收确认，eID 服务平台应根据策略按一定间隔重复发送直到达到最大重试次数或收到 AP 的接收确认。因此，AP 有可能会收到多次相同的处理结果数据，AP 应自行处理此逻辑，避免异常。

2) 当 AP 通过同步调用方式调用接口时，eID 服务平台会保持会话，待处理完所有业务以后，按照 7 至 9 节中的定义直接返回相关参数。如果 AP 在超时时间内未收到 eID 服务平台的同步返回结果,应当成本次请求失败进行处理。超时时间可根据网络与应用实际情况制定。

6.4 签名参数生成

当第三方应用与eID服务平台需要生成signature参数时，应按照以下步骤进行处理：

1) 生成消息中除去 signature 和 sign_type 两个参数外的其他所有需要使用到的参数,将这些参数作为需签名参数。
2) 对需签名参数数组里的每一个名称/值对按名称从 a 到 z 的顺序排序，若首字母相同，则依照第二个字母进行排序，以此类推。排序完成之后，将字符串中的所有‘&’字符改为“\&”进行转义，之后再把所有数组值以‘&’字符连接起来。
3) 直接在步骤 2)中得到的字符串后连接“app_key=”和 app_key 的值后得到最终的待签名字符串。
4) 使用 sign_type 中规定的签名算法对步骤 3)中的到的待签名字符串进行签名，所得的签名作为 signature 参数的值。

本节所规定的签名参数的生成示例见附录 A。

7 注册接口参数

7.1 输入参数

7.1.1 应用服务提供商信息

参数标识：app_info
参数类型：Char(1..50)
参数说明：待注册的应用服务提供商信息，为必选项。

7.1.2 应用服务提供商名称

参数标识：app_name
参数类型：Char(1..50)
参数说明：待注册的应用服务提供商名称，为必选项。

7.1.3 机构名称

参数标识：app_org
参数类型：Char(1..50)
参数说明：待注册的应用服务提供商所属机构名称，为必选项。

7.1.4 域名

参数标识：app_domain
参数类型：Char(1..80)
参数说明：待注册的应用服务提供商的域名，为必选项。

7.1.5 IP 地址

参数标识：ip_addr
参数类型：Char(1..15)
参数说明：待注册的应用服务提供商的IP地址，为必选项。

7.1.6 结果返回地址

参数标识：return_url
参数类型：Char（1..255）
参数说明：返回结果的URL地址,可空，为必选项。

7.2 返回参数

7.2.1 应用服务提供商信息

参数标识：app_info
参数类型：Char(1..50)
参数说明：待注册的应用服务提供商信息，为必选项。

7.2.2 应用服务提供商名称

参数标识：app_name
参数类型：Char(1..50)
参数说明：待注册的应用服务提供商名称，为必选项。

7.2.3 机构名称

参数标识：app_org
参数类型：Char(1..50)
参数说明：待注册的应用服务提供商所属机构名称，为必选项。

7.2.4 域名

参数标识：app_domain
参数类型：Char(1..80)
参数说明：待注册的应用服务提供商的域名，为必选项。

7.2.5 IP 地址

参数标识：ip_addr
参数类型：Char(1..15)
参数说明：待注册的应用服务提供商的IP地址，为必选项。

7.2.6 结果返回地址

参数标识：return_url
参数类型：Char（1..255）
参数说明：返回结果的URL地址，可空，为必选项。

7.2.7 应用服务提供商标识

参数标识：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。

7.2.8 共享密钥

参数标识：app_key
参数类型：Byte（1..100）
参数说明：由eID服务平台产生，为必选项。

7.2.9 服务器 URL

参数标识：server_url
参数类型：Char（1..255）
参数说明：请求服务的地址，为必选项。

7.2.10 服务器公钥证书

参数标识：server_cert
参数类型：Byte(1..10000)
参数说明：应用服务提供商对返回结果验签所需的证书文件，可空，为必选项。

8 eID 验证服务接口

8.1 概述

eID验证服务接口包含eID桌面验证服务接口和eID移动验证服务接口，分别为eID桌面应用与eID移动应用中的应用服务提供商与eID服务平台的交互提供交互协议与数据传输格式要求。数据的传输包含应用服务提供商发往eID服务平台的请求参数与eID服务平台返回给应用服务提供商的返回参数。

8.2 应用服务提供商请求参数

8.2.1 应用服务提供商 ID

参数标识：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，为必选项。

8.2.2 签名方式

参数标识：sign_type
参数类型：Char(1..100)
参数说明：签名使用的算法对应的OID，为必选项。

8.2.3 签名值

参数标识：signature
参数类型：Byte(1..2000)
参数说明：使用sign_type中所规定的签名算法对需要参与签名的参数进行签名得到的值，为必选项，具体规则见6.4节。

8.2.4 结果返回 URL

参数标识：return_url
参数类型：Char(1..255)
参数说明：结果返回应用服务提供商路径，为必选项。

8.2.5 业务流水号

参数标识：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。

8.2.6 请求时间

参数标识：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。

8.2.7 业务类型

参数标识：biz_type
参数类型：Char(2)
参数说明：为必选项。具体值的含义如下：
——“01”：桌面帐号绑定；
——“02”：桌面帐号找回；
——“03”：移动一键帐号绑定；
——“04”：移动一键帐号找回；
——“05”：桌面安全登录；
——“06”：移动一键安全登录；
——“07”：移动实名认证；
——“08”：后台实名认证

8.2.8 安全等级

参数标识：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。

8.2.9 eID 用户信息

参数标识：eid_user_info
参数类型：Char(1..100)
参数说明：仅在eID桌面应用中使用。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。

8.2.10 eID 签名值

参数标识： eid_sign_info
参数类型 ：Byte(1..2000)
参数说明：仅在eID桌面应用中使用。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。

8.2.11 签名算法 ID

参数标识：sign_algorithm_id
参数类型：Char(1..100)

参数说明：仅在eID桌面应用中使用。用户用eID设备签名使用的算法对应的OID，为必选项。

8.2.12 待签信息原文

参数标识：data_to_sign
参数类型：Char(1..2000)
参数说明：仅在eID桌面应用中使用。用户发起的交易原文明文，为可选项。

8.2.13 eID 属性信息

可选项。保留。

8.2.14 消息扩展

参数标识：extension
参数类型：Char(1..200)
参数说明：为后续应用提供一些扩展服务，为必选项。

8.2.15 手机号码

参数标识：user_phone
参数类型：Char(1..15)
参数说明：仅在eID移动应用中使用。当前应用运行平台对应的手机号码，为必选项。

8.3 eID 服务平台返回参数

8.3.1 返回结果

参数标识：result
参数类型：Char(5)
参数说明：业务处理结果，为必选项。

8.3.2 签名方式

参数标识：sign_type
参数类型：Char(2)
参数说明：签名使用的算法对应的OID，为必选项。

8.3.3 签名值

参数标识：signature
参数类型：Byte(1..2000)
参数说明：使用sign_type中所规定的签名算法对需要参与签名的参数进行签名得到的值，为必选项，具体格式见6.4节。

8.3.4 业务流水号

参数标识：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。

8.3.5 返回时间

参数标识：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。

8.3.6 eID 标识码

参数标识： eID_code
参数类型：Char(1..80)
参数说明：用户登录的eID标识码，为必选项。

8.3.7 用户账户

参数标识：user_account
参数类型：Char(1..80)
参数说明：仅在eID桌面应用中使用。用户在应用服务提供商注册的账号，为必选项。

8.3.8 消息扩展

参数标识：extension
参数类型：Char(1..200)
参数说明：无，为必选项。

附 录 A
（资料性附录）
签名参数生成示例

A.1 待签名字符串生成方法示例

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"
};

则根据6章步骤2）规则所生成的字符串如下：

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

之后，根据6章步骤3）规则的描述，直接连接app_key后得到最终的待签名字符串如下（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

此字符串便是最终的待签名字符串。

附 录 B
（资料性附录）
请求与返回消息示例

B.1 概述

本附录描述了7至9章所述各请求与返回消息的示例，供应用参考，在应用时，应根据实际情况生成相应的参数内容。

B.2 注册请求与返回消息示例

B.2.1 注册请求消息示例

如7.2节所示注册请求消息示例如下。

```
{
    "app_info": "eid_service_example",
    "app_name": "example_sp",
    "app_org": "example_org",
    "app_domain": "http://www.eid-service.cn",
    "ip_addr": "1.2.3.4",
    "sign_cert": "CERT=0123456789ABCDEF",
    "app_type": "DF",
    "sign_type": "2",
    "return_url": "http://www.eid-service.cn/return_url"
}
```

B.2.2 注册返回消息示例

如7.3节所示注册返回消息示例如下。

```
{
    "app_info": "eid_service_example",
    "app_name": "example_sp",
    "app_org": "example_org",
    "app_domain": "http://www.eid-service.cn",
    "ip_addr": "1.2.3.4",
    "sign_cert": " CERT=0123456789ABCDEF",
    "app_type": "DF",
    "sign_type": "1.2.156.10197.1.501",
    "return_url": "http://www.eid-service.cn/return_url",
    "app_id": "DF12345678901234567890123456789012345678901234567",
    "app_key": "0123456789ABCDEF0123456789ABCDEF ",
    "server_url": " http://www.eid.cn/server_url ",
    "server_cert": "CERT= ABCDEF 0123456789"
}
```

B.3 桌面验证请求与返回消息示例

B.3.1 桌面验证请求消息示例

如8.2节所示桌面验证请求消息示例如下。

```
{
    "app_id": " DF12345678901234567890123456789012345678901234567",
    "sign_type": "1.2.156.10197.1.501",
    "signature": "0123456789ABCDEF",
    "return_url": " http://www.eid-service.cn/return_url ",
    "biz_sequence_id": "00123456789",
    "apply_time": "2013-01-01 10:10:10",
    "biz_type": "1",
    "security_class": "1",
    "eid_user_info": "userinfo",
    "eid_sign_info": "0123456789ABCDEF ",
    "sign_algorithm_id": "1",
    "data_to_sign": "data",
    "extension": "some_extension"
}
```

B.3.2 桌面验证返回消息示例

如8.3节所示桌面验证请求消息示例如下。

```
{
    "result": "1",
    "sign_type": "1.2.156.10197.1.501",
    "signature": "0123456789ABCDEF",
    "biz_sequence_id": "00123456789",
    "return_time": "2013-01-01 11:11:11",
    "eID_code": "0123456789ABCDEF ",
    "user_account": "alice",
    "extension": "some_extension "
}
```

B.4 移动验证请求与返回消息示例

B.4.1 移动验证请求消息示例

如9.2节所示移动验证请求消息示例如下，在应用时，应根据实际情况生成相应的参数内容。

```
{
    "app_id": " DF12345678901234567890123456789012345678901234567",
    "sign_type": "1.2.156.10197.1.501",
    "signature": "0123456789ABCDEF ",
    "return_url": " http://www.eid-service.cn/return_url ",
    "biz_sequence_id": "00123456789",
    "apply_time": "2013-01-01 10:10:10",
    "user_phone": "13012345678",
```

```
    "biz_type": "1",
    "security_class": "1",
    "extension": "some_extension "
}
```


B.4.2 移动验证返回消息示例

如9.3节所示移动验证请求消息示例如下，在应用时，应根据实际情况生成相应的参数内容。


```
{
    "result": "1",
    "sign_type": "1.2.156.10197.1.501",
    "signature": "0123456789ABCDEF ",
    "biz_sequence_id": "00123456789",
    "return_time": "2013-01-01 11:11:11",
    "eID_code": "0123456789ABCDEF",
    "extension": "some_extension "
}
```

参 考 文 献

[1] ECMA-404《The JSON Data Interchange Format》1st Edition，Oct 2013.ECMA-International.