面向SIM卡远程配置的国家商用密码算法技术要求

1 范围

本文件规定了面向消费电子设备的远程SIM配置在使用国家商用密码算法（以下简称国密算法，包括GB/T 32905、GB/T 32907、 GB/T 32918）时的技术要求，即在eUICC生态环境中加入国密算法后对于生态环境中各角色的技术要求。

本文件适用于支持国密算法的eUICC、CI、支持LPAd的设备、SM-DP+和SM-DS的开发。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32918（所有部分） 信息安全技术 SM2椭圆曲线公钥密码算法

GM/T 0056-2018 多应用载体密码应用接口规范

YD/T XXXX-202X 面向消费电子设备的远程SIM配置平台技术要求

YD/T YYYY-202X 面向消费电子设备的支持远程SIM配置的嵌入式通用集成电路卡（eUICC）技术要求

YD/T ZZZZ-202X 面向消费电子设备的支持远程SIM配置的终端技术要求

ISO/IEC 7816-4:2020 识别卡.集成电路卡.第4部分:组织、安全和交互命令(Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange)

GPC SPE 034 全球平台 智能卡技术规范 V2.3.1（GlobalPlatform Technology Card Specification Version 2.3.1）技术 卡规范

NIST SP 800 38B 分组密码操作模式建议：用于身份验证的CMAC模式（Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication）

3 术语和定义

下列术语和定义适用于本文件。

3.1

远程SIM配置 remote SIM provisioning

下载、安装、激活、去激活以及删除在eUICC上的profile。

3.1.1

运营签约数据文件 operational profile

运营商配置于 eUICC 上的数据以及应用的组合，应支持与相应运营商的签约以及允许建立移动网络的连接。应用也可包含于运营签约数据文件以提供非通信类的业务。

3.1.2

测试签约数据文件 test profile

配置于 eUICC 上的数据以及应用的组合，可为测试设备提供连接能力，用于设备以及 eUICC 的测试。测试签约数据文件不应存储任何运营商的凭证。

3.1.3

签约数据文件元数据 metadata of profile

有关用于本地签约数据文件管理目的的配置文件的信息。

3.1.4

签约数据文件包 profile package

使用可互操作的描述格式的个性化签约数据文件，传输到 eUICC 以加载和安装配置文件。

3.1.5

绑定签约数据文件包 bound profile package

已加密链接到特定 eUICC 的受保护的签约数据文件包。

3.1.6

签约数据文件策略规则 profile policy rule

定义在发生特定情况时对签约数据文件执行操作的资格或规则。

3.1.7

RSP 服务器 RSP server

签约管理发现服务器（SM-DS）或签约管理数据准备服务器（SM-DP+）。

3.1.8

激活码 activation code

由运营商/服务提供商向最终用户发布的信息，用于最终用户请求下载和安装签约数据文件。

3.1.9

激活码令牌 token of activation code

由运营商/服务提供商提供的激活码信息的一部分，用于引用订阅。

3.1.10

发行者安全域 issuer security domain

GPC SPE 034 定义的 UICC 上的安全域。

3.1.11

本地签约数据文件辅助管理 local profile assistant

设备或 eUICC 中提供本地签约数据文件下载（LPD），本地发现服务（LDS）和本地用户接口（LUI）功能的功能元素。当 LPA 位于设备中时，它们被称为 LPAd、LPDd、LUId、LDSd。当 LPA 位于 eUICC 中时，它们被称为 LPAe、LPDe、LUIe、LDSe。在使用 LPA、LPD、LDS 或 LUI 的情况下，它们应用于与其位置在设备中或 eUICC 中无关的元素。

3.1.12

签约数据文件所有者 profile owner

控制签约数据文件上执行操作的实体。除测试签约数据文件外通常是运营商。

3.1.13

设备 device

与eUICC配合使用连接到移动网络的用户设备,例如平板电脑/可穿戴设备/智能手机或手机。

4 缩略语

下列缩略语适用于本文件。

AID	应用标识	Application Identifier
APDU	应用协议数据单元	Application Protocol Data Unit
ASN.1	抽象语法记法一	Abstract Syntax Notation One
BPP	绑定签约数据文件分组	Bound Profile Package
CASD	控制授权安全域	Controlling Authority Security Domain
CERT.CI.SM2SIG	CI SM2SIG 公钥证书	Certificate of the CI for its Public SM2SIG Key
CERT.DPauth.SM2SIG	SM-DP+ 认证的 ESDSA 公钥证书	Certificate of the SM-DP+ for its Public SM2SIG key used for SM- DP+ authentication
CERT.DPpb.SM2SIG	SM-DP+ 签约数据文件绑定的 ESDSA 公钥证书	Certificate of the SM-DP+ for its Public SM2SIG key used for Profile Package Binding
CERT.EUICC.SM2SIG	eUICC SM2SIG 公钥证书	Certificate of the eUICC for its Public SM2SIG key
CERT.EUM.SM2SIG	EUM SM2SIG 公钥证书	Certificate of the EUM for its Public SM2SIG key

CERT.DP.TLS	SM-DP+安全 TLS 传输证书	Certificate of the SM-DP+ for securing TLS
CI	证书发行方	Certificate Issuer
CMAC	基于 MAC 的加密	Cipher-based MAC
CRL	证书吊销列表	Certificate Revocation List
CRT	控制参考模板	Control Reference Template
ECASD	eUICC 控制授权安全域	eUICC Controlling Authority Security Domain
EID	eUICC 标识	eUICC-ID
eUICC	嵌入式 UICC	Embedded UICC
EUM	eUICC 制造商	eUICC Manufacturer
FQDN	完全域名	Fully Qualified Domain Name
GSMA	GSM 协会	GSM Association
ICCID	集成电路卡标识	Integrated Circuit Card ID
ISD	发行者安全域	Issuer Security Domain
ISD-P	Profile 发行者安全域	Issuer Security Domain Profile
ISD-R	根发行者安全域	Issuer Security Domain Root
LDS	本地发现服务	Local Discovery Service
LDSd	当 LPA 在设备中的本地发现服务	Local Discovery Service when LPA is in the Device
LDSe	当 LPA 在 eUICC 中的本地发现服务	Local Discovery Service when LPA is in the eUICC
LPA	本地签约数据文件辅助管理	Local Profile Assistant
LPAd	当 LPA 在设备中的本地签约数据文件辅助管理	Local Profile Assistant when LPA is in the Device
LPAe	当LPA在eUICC中的本地签约数据文件辅助管理	Local Profile Assistant when LPA is in the eUICC
LPD	本地签约数据文件下载	Local Profile Download
LPDd	当 LPA 在设备中的本地签约数据文件下载	Local Profile Download when LPA is in the Device
LPDe	当LPA在eUICC中的本地签约数据文件下载	Local Profile Download when LPA is in the eUICC
LUI	本地用户接口	Local User Interface
LUId	当 LPA 在设备中的本地用户接口	Local User Interface when LPA is in the Device
LUIe	当 LPA 在 eUICC 中的本地用户接口	Local User Interface when LPA is in

		the eUICC
MAC	消息认证码	Message Authentication Code
OTA	空中下载技术	Over The Air
otPK.EUICC.SM2KEYEX	eUICC 密钥交换的一次性公钥	One-time Public Key of the eUICC for SM2 Keyexchange
otSK.EUICC.SM2KEYEX	eUICC 密钥交换的一次性私钥	One-time Private Key of the eUICC for SM2 Keyexchange
PKI	公钥基础设施	Public Key Infrastructure
PIR	签约数据文件安装结果	Profile Installation Result
PPK-ENC	消息加密/解密签约数据文件保护密钥	Profile Protection Key for message encryption/decryption
PPK-MAC	消息 MAC 生成/验证签约数据文件密钥	Profile Protection Key for message MAC generation/verification
PPP	受保护签约数据文件包	Protected Profile Package
PPR	签约数据文件策略规则	Profile Policy Rule
RAT	规则授权表	Rules Authorisation Table
RSP	远程 SIM 配置	Remote SIM Provisioning
SCP	安全通道协议	Secure Channel Protocol
SIM	用户识别模块	Subscriber Identity Module
S-ENC	消息加密/解密会话密钥	Session key for message encryption/decryption
SK.CI.SM2SIG	CI 签发证书私钥	Private key of the CI for signing certificates
SK.DPauth.SM2SIG	SM-DP+创建 SM-DP+认证签字私钥	Private Key of the of SM-DP+ for creating signatures for SM-DP+ authentication
SK.EUICC.SM2SIG	eUICC 创建签名私钥	Private key of the eUICC for creating signatures
SK.EUM.SM2SIG	EUM 创建签名私钥	Private key of the EUM for creating signatures
SM2SIG	椭圆曲线数字签名算法	Elliptic Curve cryptography Digital Signature Algorithm
SM2KEYEX	椭圆曲线密钥协商算法	Elliptic Curve cryptography Key Agreement algorithm
S-MAC	消息 MAC 生成/验证会话密钥	Session Key for message MAC generation/verification

SM-DP+	签约管理数据准备服务器（相比 SM-DP 功能增强）	Subscription Manager Data Preparation (Enhanced compared to the SM-DP)
SM-DS	签约管理发现服务器	Subscription Manager Discovery Server
SP	服务提供商	Service Provider
SVN	（GSMA SGP.22 中的）规范版本号（参考 SGP.21 的’eSVN’）	Specification Version Number (referred to as ’eSVN’ in SGP.21).
TLS	传输层安全协议	Transport Layer Security
TLV	标记-长度-数值	Tag-Length-Value
UICC	通用集成电路卡	Universal Integrated Circuit Card
UPP	非保护签约数据文件包	Unprotected Profile Package

5 系统框架

本章描述面向消费电子设备的远程 SIM 配置系统框架中加入国密算法支持功能后，各个角色及接口的相关变化。远程 SIM 配置系统框架（本地签约数据文件辅助管理 LPA 在设备中）如图 1 所示。

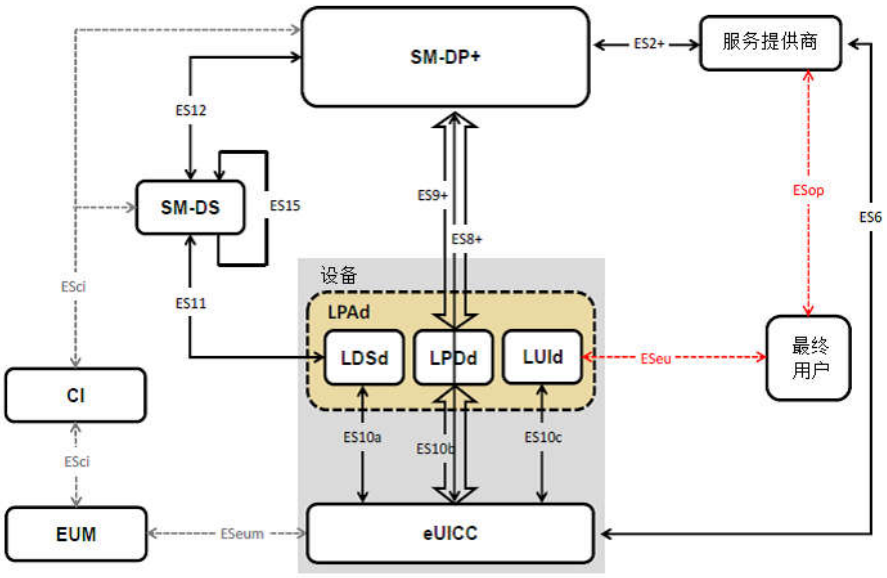

图 1 远程 SIM 配置系统（LPA 在设备中）

5.1 角色

各角色定义与 GSMA SGP.22 定义一致，系统加入国密算法后，各角色有如下变化：

CI 应具备签发 SM2（GB/T 32918-2016）国密证书能力。

SM-DS 应可存储 SM2 国密证书，具备 SM2 国密证书验证功能。

SM-DP+应可存储 SM2 国密证书，可以支持 SM2 密钥交换算法生成过程密钥，且能够使用 SM4 对称算法（GB/T 32907）进行 Profile 数据的封装，生成相应的 Protected Profile Package 和 Bound Profile Package。

EUM 应具备 SM2 国密密钥对生成能力，具备 SM2 证书签发能力。

eUICC 应可以存储 SM2 国密证书，支持 SM2 签名、SM2 验签、SM2 密钥交换算法以及 SM4 解密及 MAC 计算。

5.2 各角色技术要求

5.2.1 CI

CI 用于向 eUICC 系统中各个角色颁发证书，其中以下证书可以是 SM2 算法进行签名的证书：

- CI 证书 (CERT.CI. SM2SIG)
- EUM 证书(CERT.EUM. SM2SIG)
- SM-DP+ 证书 (CERT.DPauth. SM2SIG, CERT.DPpb. SM2SIG)
- SM-DS 证书 (CERT.DSauth. SM2SIG)

以下证书不使用SM2算法签名证书：

- SM-DS TLV 证书 (CERT.DS.TLS)
- SM-DP+ TLS 证书 (CERT.DP.TLS)

5.2.2 SM-DS

SM-DS 支持的功能应符合 YD/T XXXX-202X 的要求。

若 SM-DS 支持国密算法，还需要符合以下要求：

SM-DS 中应该存储 CI 颁发的 SM2 算法签名的证书 CERT.DSauth. SM2SIG。

ES11.InitiateAuthentication 中 serverSignature1 应使用 SK.DSauth.SM2SIG 通过 SM2 签名算法生成。serverCertificate 应使用 CERT.DSauth. SM2SIG。

ES11.AuthenticateClient 中对于 euiccSignature1 的验证过程应从相应的 SM2 证书 CERT.CI. SM2SIG、CERT.EUM. SM2SIG、CERT.EUICC.SM2SIG 中提取公钥，并使用 SM2 算法验证 euiccSignature1 的正确性。

5.2.3 SM-DP+

SM-DP+支持的功能应符合 YD/T XXXX-202X 的要求。

若 SM-DP+支持使用国密算法，还需要符合以下要求：

SM-DP+中应该存储 CI 颁发的 SM2 算法签名的证书 CERT.DPauth. SM2SIG，CERT.DPpb. SM2SIG。

ES9+.InitiateAuthentication 中 serverSignature1 应使用 SK.DPauth.SM2SIG 通过 SM2 签名算法生成。serverCertificate 应使用 CERT.DPauth. SM2SIG

ES9+.AuthenticateClient 中对于 euiccSignature1 的验证过程应从相应的 SM2 证书 CERT.CI. SM2SIG、CERT.EUM. SM2SIG、CERT.EUICC.SM2SIG 中提取公钥 PK.EUICC.SM2SIG，并使用 SM2 算法验证 euiccSignature1 的正确性。

ES9+. GetBoundProfilePackage 中对于 euiccSignature2 的验证过程应使用 PK.EUICC.SM2SIG 进行验证。

SM-DP+ 应生成 SM2 密钥对 otPK.DP. SM2KEYEX 和 otSK.DP. SM2KEYEX，并利用 otPK.eUICC.SM2KEYEX 生成过程密钥（S_ENC,S_MAC）和 MAC 初始向量（initial MAC chaining value）。

Profile Package Protection 生成过程应使用 SM4 算法，加密算法应使用 SM4 CBC 加密，MAC 算法应使用 SM4 进行 CMAC（NIST 800-38B） 算法计算。

ES9+. CancelSession 中 euiccCancelSessionSignature 应使用 PK.EUICC.SM2SIG 进行验证。

5.2.4 EUM

EUM 支持的功能应遵循 YD/T YYYY-202X 的要求。

若 EUM 支持国密算法，还应符合以下要求：

1)EUM 中应能够安全存储 SK.EUM. SM2SIG 和 CERT.EUM. SM2SIG。

2)EUM 应具备 SM2 密钥对生成能力，为每张 eUICC 卡生成密钥对，并使用 SK.EUM. SM2SIG 私钥，生成 eUICC 公钥证书 CERT.EUICC.SM2SIG。

5.2.5 设备

本文件不要求设备支持国密算法。

5.2.6 eUICC

eUICC 支持的功能应遵循 YD/T YYYY-202X。

若eUICC支持国密算法，还应符合以下要求：

a) ECASD 中应存储以下证书（表 1）及密钥（表 2）：

表1 ECASD证书

证书名称	证书含义	签名算法
CERT.CI.SM2SIG	CI的根证书	SM2
CERT.EUM.SM2SIG	EUM的证书	SM2
CERT.EUICC.SM2SIG	EUICC证书	SM2

表2 ECASD密钥

密钥名称	密钥含义	密钥算法
SK.EUICC.SM2SIG	eUICC用于生成签名数据的私钥	SM2

b) ES8+. InitialiseSecureChannel，eUICC 应使用 PK.DPbp.SM2SIG 进行 SM-DP+签名的验证。eUICC 应使用 otPK.DP. SM2KEYEX 和 otSK.EUICC. SM2KEYEX 生成过程密钥（S_ENC,S_MAC）和 MAC 初始向量（initial MAC chaining value）。

c) ES8+. ConfigureISDP， ES8+. StoreMetadata ，ES8+. ReplaceSessionKeys 过程中，数据完整性校验应使用 SM4 进行 CMAC 算法校验，数据解密应使用 SM4 CBC 解密。

d) ES8+. LoadProfileElements 过程中，使用 SK.EUICC.SM2SIG 生成 Profile Installation Result 中的 euiccSignPIR。

e) ES10b. PrepareDownload 过程中，使用 ECASD 服务，利用 CERT.CI.SM2SIG 验证 CERT.DPpb.SM2SIG 的有效性； smdpSignature2 使用 PK.DPpb.SM2SIG 进行验证； euiccSignature2 使用 SK.EUICC.SM2SIG 生成。

f) ES10b. LoadBoundProfilePackage 过程中，数据完整性校验应使用 SM4 进行 C_MAC 算法校验，数据解密应使用 SM4 CBC 解密。

g) ES10b. AuthenticateServer 过程中，使用 ECASD 服务，利用 CERT.CI.SM2SIG 验证 CERT.DPauth.SM2SIG 或者 CERT.DSauth.SM2SIG 的有效性； serverSignature1 使用 PK.DPauth.SM2SIG 进行验证； euiccSignature1 使用 SK.EUICC.SM2SIG 生成。

5.3 接口

接口定义应符合表 3 要求。

表3 远程SIM配置系统接口

接口	相关实体之间		描述
ES2+	运营商	SM-DP+	运营商通过本接口为eUICC定制Profile以及进行管理功能。 注：本接口不在本文件定义范围。
ES6	运营商	eUICC	运营商通过OTA服务对eUICC管理。
ES8+	SM-DP+	eUICC	本接口在SM-DP和eUICC间提供一个安全的点到点

接口	相关实体之间		描述
			的通道，实现ISD-P的执行和Profile的下载和安装。
ES9+	SM-DP+	LPD	用于SM-DP+和LPA（LPD）之间BPP和远程Profile管理命令的安全传输。
ES10a	LDSd	eUICC	用于 LDSd 和 LPA 服务之间处理 Profile 发现命令。
ES10b	LPDd	eUICC	用于LPDd和LPA服务之间传送BPP到eUICC。本接口不涉及Profile包解密
ES10c	LUId	eUICC	用于LUId和LPA服务之间用户的本地Profile管理。
ES11	LDS	SM-DS	用于LDS为各eUICC提取事件记录。
ES12	SM-DP+	SM-DS	本接口由SM-DP+通过SM-DS进行事件发布和注册。
ES15	SM-DS	SM-DS	本接口用于SM-DSs之间的交互。

5.4 Profile 的保护和数据传输

本条描述使用国密算法保护运营商的 Profile，然后将其下载到 eUICC 中。本条内容也适用于在系统内各个角色传输期间保护签约数据文件包的过程。

5.4.1 Profile 文件包类型概述

Profile 文件包类型应符合 YD/T XXXX-202X 5.9.1 的要求。

5.4.2 非保护签约数据文件包

非保护签约数据文件包(UPP)应符合 YD/T XXXX-202X 5.9.2 的要求。

5.4.3 受保护签约数据文件包

受保护签约数据文件包（PPP）是通过 SM-DP+生成的，其具有签约数据文件包保护功能。

PPP 应通过基于 SM4 的 SCP03t 进行保护。TLV 的加密命令和 MAC 应遵循 SGP.02 4.1.3.3 条的要求。在此步骤中，不考虑内部的 UPP 结构，而是将其看作一个独特的数据块。该数据块被分割成文件大小最大为 1020 字节的数据段（包括标签，长度字段和 MAC）。eUICC 应支持接收至少达到此文件大小的数据段。

注：每个数据段有 1020 个字节，其中只有 1008 个字节可用于有效承载数据（需要扣除掉占用 1 个字节的标签，3 个字节的长度字段和 8 个字节 MAC）。同时考虑到加密过程中必要的数据填充（16 字节长度的块加密和必要的“80”字节填充），实际上每个数据段只能包含 1007 字节的 PPP 数据块。

签约数据文件的保护应使用以下任一方式执行：

- 与 eUICC 签署密钥协议产生的会话密钥(S-ENC,S-MAC)。
- 或每个 Profile 的随机密钥（在本文档中表示为 PPK-ENC 和 PPK-MAC，在 SGP.02 中分别称为 S-ENC 和 S-MAC），由 SM-DP+生成。

如果 SM-DP+选择了随机密钥模式，用于 PPP 的第一段的初始 MAC 链接值与随机密钥(符合 YD/T YYYY-202X 的 9.3.4)一起提供，用于 ICV 计算的加密计数器被重置为初始状态(即 16 字节的值为“00…01”)。否则应使用 SGP.02 中定义的 MAC 链接方法（即使用前一个的 MAC 链接值）。

S-ENC，S-MAC，PPK-ENC 和 PPK-MAC 应为 128 比特长度。PPP 中的每个数据段由 SGP.02 中定义的标签“86”标识。

关于是否使用这个随机密钥集（PPK-ENC 和 PPK-MAC），是 SM-DP+的选择（根据运营商的协议）。

此模式允许在不具备 eUICC 信息知识的情况下提前执行 Profile 文件包保护。这样有助于提供更好的 SM-DP+可扩展性。eUICC 应能支持这两种模式。

在使用随机密钥模式的情况下，PPP 在此阶段不绑定到任何特定的 eUICC 或 ISD-P AID 值。

会话密钥和（如果使用的话）随机密钥只能在签约数据文件下载过程中使用。在流程结束时，应在 eUICC 上删除这些密钥信息。

签约数据文件创建过程不在本文件范围之内；运营商可以请求 SM-DP+预先创建多个签约数据文件。在这种情况下，SM-DP+必须批量创建签约数据文件，使用随机密钥模式保护它们，并存储生成的 PPP 供以后使用。

5.4.4 绑定的签约数据文件包

绑定的签约数据文件包（BPP）由具有签约数据文件包绑定功能的 SM-DP+生成。此操作的目的是将受保护的签约数据文件包链接到特定的 eUICC。这是在 eUICC 和 SM-DP+之间的密钥协议内完成的。

BPP 包含一系列 TLV 命令：

- 密钥协议的 TLV 命令是明确的；
- 一组基于 SM4 的 SCP03t 有效负载 TLV(标记为“87”)，其中包含用于 ConfigureISDP 的 TLV 命令；
- 一组基于 SM4 的 SCP03t 有效载荷 TLV(标记为“88”)，包含 StoreMetadata 的 TLV 命令；
- 一组可选的基于 SM4 的 SCP03t 有效负载 TLV(标记为“87”)，包含用于 Profile Protection Keys 的 TLV 命令；
- 随后是 PPP 的基于 SM4 的 SCP03t 有效负载 TLV（标记为“86”）。

每当收到标记为“86”，“87”或“88”的 TLV 时，ICV 计算的加密计数器都会递增。

绑定的签约数据文件包的数据结构如下：

```
BoundProfilePackage ::= [54] SEQUENCE { -- Tag 'BF36'
    initialiseSecureChannelRequest [35] InitialiseSecureChannelRequest, -- Tag 'BF23'
    firstSequenceOf87 [0] SEQUENCE OF [7] OCTET STRING, -- sequence of '87' TLVs
    sequenceOf88 [1] SEQUENCE OF [8] OCTET STRING, -- sequence of '88' TLVs
    secondSequenceOf87 [2] SEQUENCE OF [7] OCTET STRING OPTIONAL, -- sequence of '87' TLVs
    sequenceOf86 [3] SEQUENCE OF [6] OCTET STRING -- sequence of '86' TLVs
}
```

表 4 描述了“86”，“87”和“88”TLV 的各种序列：

表 4 TLV 的签约数据文件安装顺序

名称					
'A0'	Var.	‘87’标签第一序列			必选
		‘87’	Var.	SCP03t 字段包含 ConfigureISDP，由密钥协商（S-ENC，S-CMAC）产生的会话密钥保护； 内容：“ES8+.ConfigureISDP”函数的 TLV。	必选
'A1'	Var	‘88’标签序列			必选
		'88'	Var.	SCP03t 字段包含 StoreMetadata，通过密钥协商（S-CMAC）产生的会话密钥保护 MAC。	必选

名称					
				内容：“ES8+.StoreMetadata”函数的 TLV	
		'88'	Var.	如果一个“88”TLV 不能包含整个数据结构，则 SCP03t 字段包含 StoreMetadata 的剩余部分。	条件可选
'A2'	Var.	‘87’标签第二序列 如果无内容可为空			条件可选
		'87'	Var.	SCP03t 字段包含 Profile 保护密钥，由密钥协商（S-ENC，S-CMAC）产生的会话密钥保护。 内容：“ES8+.ReplaceSessionKeys”函数的 TLV	可选
'A3'	Var.	‘86’标签序列			必选
		'86'	Var.	SCP03t 有效载荷，使用签约数据文件保护密钥（PPK-ENC，PPK-MAC）或通过密钥协商（S-ENC，S-CMAC）产生的会话密钥保护字段 b1。	必选
		'86'	Var.	后续 SCP03t 有效载荷，字段 b2...bn	可选

5.4.4.1 InitialiseSecureChannel 块的描述

此文件块由 TLV 组成，用于与 eUICC 启动远程个性化的会话，其中包括密钥协议。

这些 TLV 是“ES8+.InitialiseSecureChannel”功能的一部分，并且不应被加密。通过签名保证完整性和真实性。

eUICC 执行此函数将生成基于 SM4 的 SCP03t 会话密钥，表示为 S-ENC、S-MAC 和初始的 MAC 链接值，SM-DP+将使用这些密钥来保护后续的 TLV。

5.4.4.2 ConfigureISDP 块的描述

该块包含一个用于 ISD-P 创建和配置的 TLV。TLV 是“ES8+.ConfigureISDP”功能的一部分，这个 TLV 应该使用基于 SM4 的 SCP03t 会话密钥进行加密和 MAC。

5.4.4.3 StoreMetadata 块的描述

此文件块包含一个或两个签约数据文件元数据的 TLV。这些 TLV 是“ES8+.StoreMetadata”功能的一部分，这些 TLV 只能用基于 SM4 的 SCP03t 会话密钥进行 MAC。

5.4.4.4 Profile Protection Keys 块的描述

“Profile Protection Keys”模块包含 “ES8+.ReplaceSessionKeys” 功能，替换由密钥协商产生的会话 S-ENC 和 S-MAC 密钥，用于保护 PPP，PPK-ENC 和 PPK_MAC 的密钥。

该功能由基于 SM4 的 SCP03t 用密钥协议生成的 S-ENC 和 S-MAC 密钥保护。该文件块是可选的，具体取决于 SM-DP+选择的模式。

5.4.5 分段绑定的签约数据文件包

分段绑定的签约数据文件包（SBPP）由 LPAd 生成，以使用本地接口 ES10b 将绑定签约数据文件包传送到 eUICC。

每个分段应根据绑定签约数据文件包的结构来构成：

- 绑定签约数据文件包 TLV 的标签和长度字段应加上初始化安全通道请求的 TLV；
- firstSequence0f87 TLV 的标签和长度字段应加上第一个标记为“87”的 TLV；
- 包含 sequence0f88 TLV 的标签和长度字段；
- 包含每一个“88”的 TLV；
- sequence0f87 TLV 的标签和长度字段应加上第一个标记为“87”的 TLV；
- 包含 sequence0f86 TLV 的标签和长度字段；
- 包含每一个“86”的 TLV 。

该列表中的每段最多 255 个字节，并在一个 APDU 中传输。比较大的 TLV 以第一个块的 255 个字节和最后一个比较短的块的形式发送。

5.4.6 签约数据文件安装结果

签约数据文件安装结果具体描述应符合 YD/T XXXX-202X 5.9.6，其中 eUICC 签名数据对象，使用数据对象 ProfileInstallationResultData（标记“BF 27”）上的 eUICC 私钥 SK.EUICC.SM2SIG。

5.4.6.1 签约数据文件安装结果错误

签约数据文件安装结果错误应符合 YD/T XXXX-202X 5.9.6.1 的要求。

5.5 安全概述

5.5.1 证书和密钥定义

面向消费电子设备的支持远程 SIM 配置的生态系统，如果支持国密算法，应支持表 5 中的证书。

表5 国密算法证书表

证书名称	证书含义	签名算法
CERT.CI.SM2SIG	CI的根证书	SM2
CERT.EUM.SM2SIG	EUM的证书	SM2
CERT.EUICC.SM2SIG	EUICC证书	SM2
CERT.DPauth.SM2SIG	SM-DP+用于与eUICC进行双向认证时的证书	SM2
CERT.DPpb.SM2SIG	SM-DP+用于生成PPP时使用的证书	SM2
CERT.DSauth.SM2SIG	SM-DS用于与eUICC进行双向认证时的证书	SM2

面向消费电子设备的支持远程 SIM 配置的生态系统，如果支持国密算法，应支持表 6 中的密钥。

表6 国密算法密钥表

密钥名称	密钥含义	密钥算法
PK.EUICC.SM2SIG	eUICC公钥，公钥包含在eUICC证书中	SM2
SK.EUICC.SM2SIG	eUICC用于生成签名数据的私钥	SM2
PK.DPauth.SM2SIG	认证SM-DP+签名的公钥	SM2

密钥名称	密钥含义	密钥算法
SK.DPauth.SM2SIG	SM-DP+私钥，生成供eUICC认证的SM-DP+签名。	SM2
PK.DPpb.SM2SIG	SM-DP+公钥，用于验证BPP中SM-DP+的签名。. 这个密钥包含在CERT.DPpb.SM2SIG中.	SM2
SK.DPpb.SM2SIG	SM-DP+私钥，用于生成 Profile 中的签名	SM2
PK.DSauth.SM2SIG	认证SM-DS签名的公钥	SM2
SK.DSauth.SM2SIG	SM-DS私钥，生成供eUICC认证的SM-DP+签名。	SM2
PK.EUM.SM2SIG	EUM公钥	SM2
SK.EUM.SM2SIG	EUM私钥	SM2
PK.CI.SM2SIG	CI公钥	SM2
SK.CI.SM2SIG	CI私钥	SM2
otPK.EUICC.SM2KEYEX	eUICC 用于密钥交换的一次性公钥.	SM2
otSK.EUICC.SM2KEYEX	eUICC 用于密钥交换的一次性私钥.	SM2
otPK.DP.SM2KEYEX	SM-DP+ 用于密钥交换的一次性公钥.	SM2
otSK.DP.SM2KEYEX	SM-DP+ 用于密钥交换的一次性私钥.	SM2

5.5.2 加密算法协商

加密算法协商中加入国密算法需求如表7所示。

表7 加密算法协商表

签名算法及曲线参数	密钥协商算法	PPP 使用的对称算法	签名算法所使用的 HASH 算法
ECDSA(1), NIST P-256	ECKA, NIST P-256, SHA-256	AES-CBC-128 AES-CMAC-128	As indicated in the CERT.XXauth.SIG
ECDSA (1), BrainpoolP256r1	ECKA , BrainpoolP256r1, SHA-256	AES-CBC-128 AES-CMAC-128	As indicated in the CERT.XXauth.SIG
ECDSA (1), FRP256V1	ECKA , FRP256V, SHA-256	AES-CBC-128 AES-CMAC-128	As indicated in the CERT.XXauth.SIG
SM2 Signature	SM2 KeyExchange	SM4	SM3（GB/T 32905）
注 1: ECDSA 参见《GlobalPlatform Card Specification Amendment E》 [8].			

6 流程

6.1 远程配置流程

6.1.1 签约数据下载初始化

应符合 YD/T XXXX-202X 第 6.1.1 条。

6.1.2 通用双向认证流程

本条描述在本文件中使用的通用双向鉴权流程，鉴权流程使用国密算法进行。

在本条中，使用以下符号：

- SM-XX 表示 SM-DP+或 SM-DS；
- CERT.XXauth.SM2SIG 表示 CERT.DPauth.SM2SIG 或 CERT.DSauth.SM2SIG；
- SK.XXauth.SM2SIG 表示 SK.DPauth.SM2SIG 或 SK.DSauth.SM2SIG；
- CERT.XX.TLS 表示 CERT.DP.TLS 或 CERT.DS.TLS；
- SK.XX.TLS 表示 SK.DP.TLS 或 SK.DS.TLS；
- ESXX 表示与 SM-DP+通信的 ES9+或与 SM-DS 通信的 ES11。

该过程意味着使用 CERT.XXauth.SM2SIG。遵循这种通用双向鉴权流程，如果使用 SM-XX 的其它证书，如 CERT.DPpb.SM2SIG，则这些证书应具有信任链可导向与 CERT.XXauth.SM2SIG 相同的根证书发行方证书。

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>SM-XX" as DP
participant "<b>LPAd" as LPA
participant "<b>eUICC" as E
LPA -> E : [1a] [ES10b.GetEUICCInfo]
E --> LPA : [1b] [euiccInfo1]
LPA -> E : [2] ES10b.GetEUICCChallenge
rnote over E #FFFFFF : [3] Generate euiccChallenge
E --> LPA : [4] eUICCChallenge
rnote over DP, LPA #FFFFFF : [5] Establish HTTPS connection
LPA -> DP : [6] ESXX.InitiateAuthentication \n (eUICCChallenge, euiccInfo1, SM-XX Address)
rnote over DP #FFFFFF
[7]
- [Check SM-XX Address]
- Check euiccInfo1
Endrnote

DP --> LPA : [error]
```

rnote over DP #FFFFFF
[8]
- Generate TransactionID
- Generate serverChallenge
- Build serverSigned1 = {TransactionID, euiccChallenge,
  serverChallenge, SM-XX Address}
- Compute serverSignature1 over serverSigned1
endrnote

DP --> LPA : [9] TransactionID, serverSigned1, serverSignature1,\neuiccCiPKIdToBeUsed, CERT.XXauth.SM2SIG
rnote over LPA #FFFFFF
[10]
[Perform contextual operation]
Check SM-XX Address
Generate ctxParams1
endrnote
LPA -> E : [11] ES10b.AuthenticateServer\n(serverSigned1, serverSignature1,\n euiccCiPKIdToBeUsed, CERT.XXauth.SM2SIG, ctxParams1)
rnote over E #FFFFFF
[12]
- Verify CERT.XXauth.SM2SIG
- Verify serverSignature1 over serverSigned1
- Verify serverSigned1
endrnote
E --> LPA : [error]
rnote over E #FFFFFF
[13]
- Generate euiccSigned1 = {TransactionID, serverChallenge,
  euiccInfo2, ctxParams1}
- Compute euiccSignature1 over euiccSigned1
endrnote
E --> LPA : [14] euiccSigned1, euiccSignature1\n CERT.EUICC.SM2SIG, CERT.EUM.SM2SIG
LPA -> DP : [15] ESXX.AuthenticateClient \n (euiccSigned1, euiccSignature1,\n CERT.EUICC.SM2SIG, CERT.EUM.SM2SIG)

rnote over DP #FFFFFF
[16]
- Verify CERT.EUM.SM2SIG
- Verify CERT.EUICC.SM2SIG
- Verify euiccSignature1 over euiccSigned1
- Verify euiccSigned1
endrnote

DP --> LPA : [error]

rnote over DP, E #FFFFFF : [17] Continue...

@enduml

通用双向鉴权流程如图 2 所示。

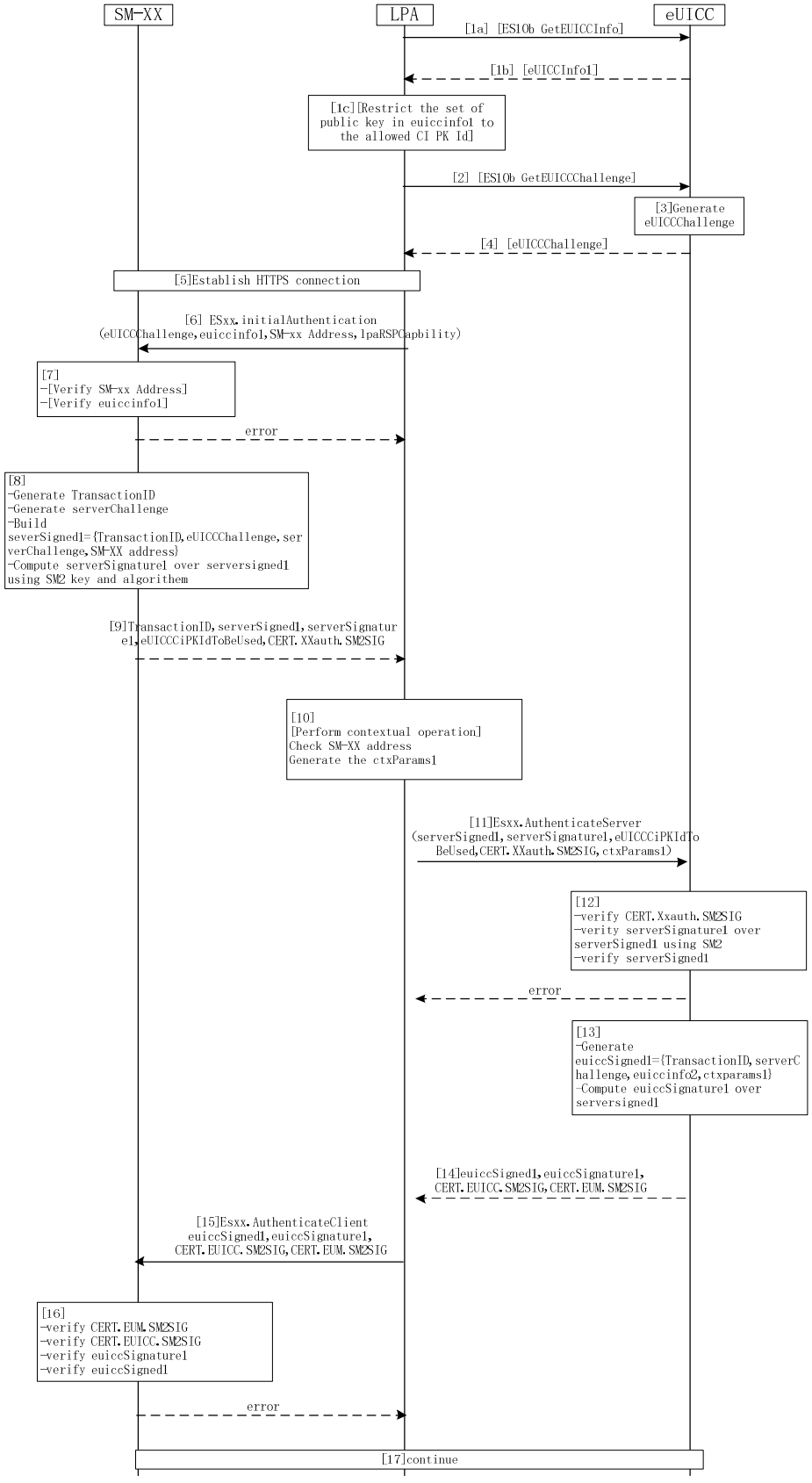
SM-XX
LPA
eUICC
[1a] [ES10b GetEUICCInfo]
[1b] [eUICCInfo1]
[1c][Restrict the set of public key in euiccinfo1 to the allowed CI PK Id]
[2] [ES10b GetEUICCChallenge]
[3]Generate eUICCChallenge
[4] [eUICCChallenge]
[5]Establish HTTPS connection
[6] ESxx.initialAuthentication (eUICCChallenge,euiccinfo1,SM-xx Address,lpaRSPCapbility)
[7]
-[Verify SM-xx Address]
-[Verify euiccinfo1]
error
[8]
-Generate TransactionID
-Generate serverChallenge
-Build severSigned1={TransactionID,eUICCChallenge,serverChallenge,SM-XX address}
-Compute serverSignature1 over serversigned1 using SM2 key and algorithem
[9]TransactionID,serverSigned1,serverSignature1,eUICCCiPKIdToBeUsed,CERT.XXauth.SM2SIG
[10]
[Perform contextual operation]
Check SM-XX address
Generate the ctxParams1
[11]Esxx.AuthenticateServer (serverSigned1,serverSignature1,eUICCCiPKIdToBeUsed,CERT.XXauth.SM2SIG,ctxParams1)
[12]
-verify CERT.Xxauth.SM2SIG
-verity serverSignature1 over serverSigned1 using SM2
-verify serverSigned1
error
[13]
-Generate euiccSigned1={TransactionID,serverChallenge,euiccinfo2,ctxparams1}
-Compute euiccSignature1 over serversigned1
[14]euiccSigned1,euiccSignature1, CERT.EUICC.SM2SIG,CERT.EUM.SM2SIG
[15]Esxx.AuthenticateClient euiccSigned1,euiccSignature1, CERT.EUICC.SM2SIG,CERT.EUM.SM2SIG
[16]
-verify CERT.EUM.SM2SIG
-verify CERT.EUICC.SM2SIG
-verify euiccSignature1
-verify euiccSigned1
error
[17]continue

图 2　通用双向鉴权流程

初始条件：

SM-XX 由下述数据配置：证书(CERT.XXauth.SM2SIG)、私钥(SK.XXauth.SM2SIG)、CI 证书(CERT.CI.SM2SIG)、TLS 证书(CERT.XX.TLS) 和 TLS 私钥 (SK.XX.TLS)。

eUICC 由下述数据配置：证书 (CERT.EUICC.SM2SIG)、私钥(SK.EUICC.SM2SIG)、EUM 证书(CERT.EUM.SM2SIG) 和 CI 公钥 (PK.CI.SM2SIG)。

步骤：

1) 可选地，LPA 可以通过调用“ES10b.GetEUICCInfo”函数接口从 eUICC 请求 eUICC 信息 euiccInfo1。如果 LPAd 尚未获取该信息，则需要该操作。
2) eUICC 将 euiccInfo1 返回给 LPAd。
3) LPAd 通过调用“ES10b.GetEUICCChallenge”函数接口，从 eUICC 请求 eUICC 挑战码。
4) eUICC 应生成一个 eUICC 的询问，随后由 SM-XX 签署，由 eUICC 进行 SM-XX 认证。
5) eUICC 将 eUICC 挑战码返回给 LPAd。
6) LPAd 以服务器验证模式与 SM-XX 建立新的 HTTPS 连接。TLS 会话建立将执行新的密钥交换（它不应重用上一会话密钥）。在此步骤中，LPAd 应验证 CERT.XX.TLS 是否符合有效性。如 CERT.XX.TLS 无效，流程将被终止。
7) LPAd 应调用“ESXX.InitiateAuthentication”功能（符合 YD/T ZZZZ-202X 12.1.1 和 12.3.1），其输入数据包括 euiccChallenge、euiccInfo1 和 SM-XX Address。euiccInfo1 包括 eUICCVerSupport(svn)euiccCiPKIdListForVerification 和 euiccCiPKIdListForSigning。SM-XX 是 LPAd 用于访问 SM-XX 的地址。SM-XX 地址的获取方式取决于通用调用的过程。
8) 根据服务器（即 SM-DS 或 SM-DP+），SM-XX 可以检查 LPAd 发送的 SM-XX 地址是否有效。如果 SM-XX 地址无效，则 SM-XX 应返回一个错误状态，程序应停止。

- SM-XX 将检查与 eUICC 凭证（euiccCiPKIdListForSigning）关联的 CI 公钥的列表。如果 SM-XX 不接受这些 CI 公共密钥中的任何一个，它将返回一个错误状态并且程序应该被停止。
- SM-XX 应检查接收到的 euiccInfo1 中包含的 CI 公钥标识符列表（euiccCi PKIdListForVerification）。如果无法提供由 eUICC 支持的 CI 公钥支持的 CERT.XXauth.SM2SIG，则应返回错误状态，并停止该流程。

9) SM-XX 应执行以下操作：

- 生成一个交易 ID，用于唯一标识 RSP 会话并关联属于同一个 RSP 会话的多个 ESXX 请求消息。
- 生成一个 SM-XX 挑战（serverChallenge），由 eUICC 稍后签署，用于 eUICC 认证。
- 在由 RSP 服务器支持的 euiccCiPKIdListForSigning 中提供的一个 CI 公钥中选择一个 CI 公钥，并在 euiccCiPKIdToBeUsed 中指明它。
- 生成包含 TransactionID，euiccChallenge，serverChallenge 和 SM-XX 地址的 serverSigned1 数据结构。
- 使用 SK.XXauth.SM2SIG 通过 serverSigned1 来计算 serverSignature1。

10) SM-XX 应将 TransactionID、serverSigned1、serverSignature1、euiccCiPKIdToBe Used 和 CERT.XXauth.SM2SIG 返回给 LPAd。
11) LPAd 应：

- （可选的）根据使用该调用过程的流程执行上下文操作。
- 验证 SM-XX 返回的 SM-XX 地址是否匹配 LPAd 在步骤 6）中提供的 SM-XX 地址。如果否，LPA 将通知用户，且流程终止。
- 生成要提供给 eUICC 的数据结构 ctxParams1，其包含在带符号数据中。

12) LPAd 应调用“ES10b.AuthenticateServer”功能，其输入数据包括上一步中可选地生成的

serverSigned1、serverSignature1、euiccCiPKIdToBeUsed、CERT.XXauth.SM2SIG 和 ctxParams1。

13）eUICC 应使用相关的 PK.CI.SM2SIG 验证 CERT.XXauth.SM2SIG。如果 eUICC 没有 PK.CI.SM2SIG，则 eUICC 应该返回相关的错误状态，并且应该停止流程。

14）eUICC 应该：

- 生成包含 TransactionID，serverChallenge，eUICCInfo2 和 ctxParams1 的 euiccSigned1 数据结构。
- 使用 SK.EUICC.SM2SIG 在 euiccSigned1 上计算 euiccSignature1。在生成 eicicSignature1 时，eUICC 应使用与从 SM-XX 收到的 euiccCiPKIdToBeUsed 参数相关的凭证。

15）eUICC 应将 euiccSigned1，euiccSignature1，CERT.EUICC.SM2SIG 和 CERT.EUM.SM2SIG 返回给 LPA。

16）LPAd 应调用“ESXX.AuthenticateClient”功能，其输入数据包括 euiccSigned1，euiccSignature1，CERT.EUICC.SM2SIG 和 CERT.EUM.SM2SIG。

17）在接受“ESXX.AuthenticateClient ”函数调用，SM-XX 应当：

- 通过验证两个交易 ID 匹配，将其与步骤 7）中处理的“ESXX.InitiateAuthentication”函数相关联。
- 确认 CERT.EUICC.SM2SIG 和 CERT.EUM.SM2SIG 的有效性。
- 使用 CERT.EUICC.SM2SIG 中包含的 PK.EUICC.SM2SIG 验证 euiccSignature1 是否通过 euiccSigned1 执行。
- 验证 euiccSigned1 中包含的 serverChallenge（服务器挑战）与步骤 7）中 SM-XX 生成的 serverChallenge（服务器挑战）匹配。验证 euiccInfo2 中包含的 SVN 与步骤 6）中传递的 SVN 相同。
- 如果验证失败，SM-XX 应返回一个相关的错误状态，程序应该停止。

18）该通用流程应根据使用它的流程的要求继续其它步骤。

6.1.2.1 签约数据下载和安装

本条描述签约数据文件下载和安装流程。

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>Operator" as OP
participant "<b>SM-DP+" as DP
participant "<b>LPAd" as LPA
participant "<b>eUICC" as E

rnote over LPA #FFFFFF : [1] (a) Get SM-DP+ Address, Parse Activation Code Token, [SM-DP+ OID] from AC, or\n (b) Get SM-DP+ Address and EventID from SM-DS, or\n (c) Get Default SM-DP+ Address from eUICC
```

rnote over DP, E #FFFFFF : [2] [Refer to Common mutual authentication procedure section 6.1.2]

rnote over DP #FFFFFF
[3]
- Look for Profile download pending order
- Eligibility Check using Device Info, euiccInfo2
endrnote

Group Opt.
DP -> OP : [4] ES2+.HandleDownloadProgressInfo(...)
OP --> DP : OK
end
DP --> LPA : [error]

rnote over DP #FFFFFF
[5]
- Build Profile Metadata
- Check if download retry
- Build smdpSigned2 = {TransactionID,
    Confirmation Code Required Flag, [bppEuiccOtpk]}
- Compute smdpSignature2 over smdpSigned2 and euiccSignature1
endrnote
DP -> LPA : [6] TransactionID, Profile Metadata, smdpSigned2, smdpSignature2, CERT.DPpb.SM2SIG

rnote over LPA #FFFFFF
[7a] Check if ProfileMetadata contains PPR(s)
endrnote

LPA -> E : [7b] [ES10b.GetRAT]
E --> LPA : [RAT]

LPA -> E : [7c] [ES10b.GetProfilesInfo]
E --> LPA : [ProfileInfoListOk]

rnote over LPA #FFFFFF
[8]
- [Check if PPR(s) is/are allowed against RAT.
Refer to section 2.9.2.3]
- [User Consent]
- [User Confirmation]
- [Prompt the End User to input Confirmation Code]

Endrnote

alt Download rejection
rnote over DP, E #FFFFFF：[Refer to Sub-procedure Profile Download and installation – Download rejection]

else Download confirmation
rnote over DP, E #FFFFFF：[Refer to Sub-procedure Profile Download and installation – End User confirmation]

else Download confirmation
rnote over DP, E #FFFFFF：[Refer to Sub-procedure Profile Download and installation – Download confirmation]

end

@enduml

签约数据文件下载和安装流程如图 3 所示。

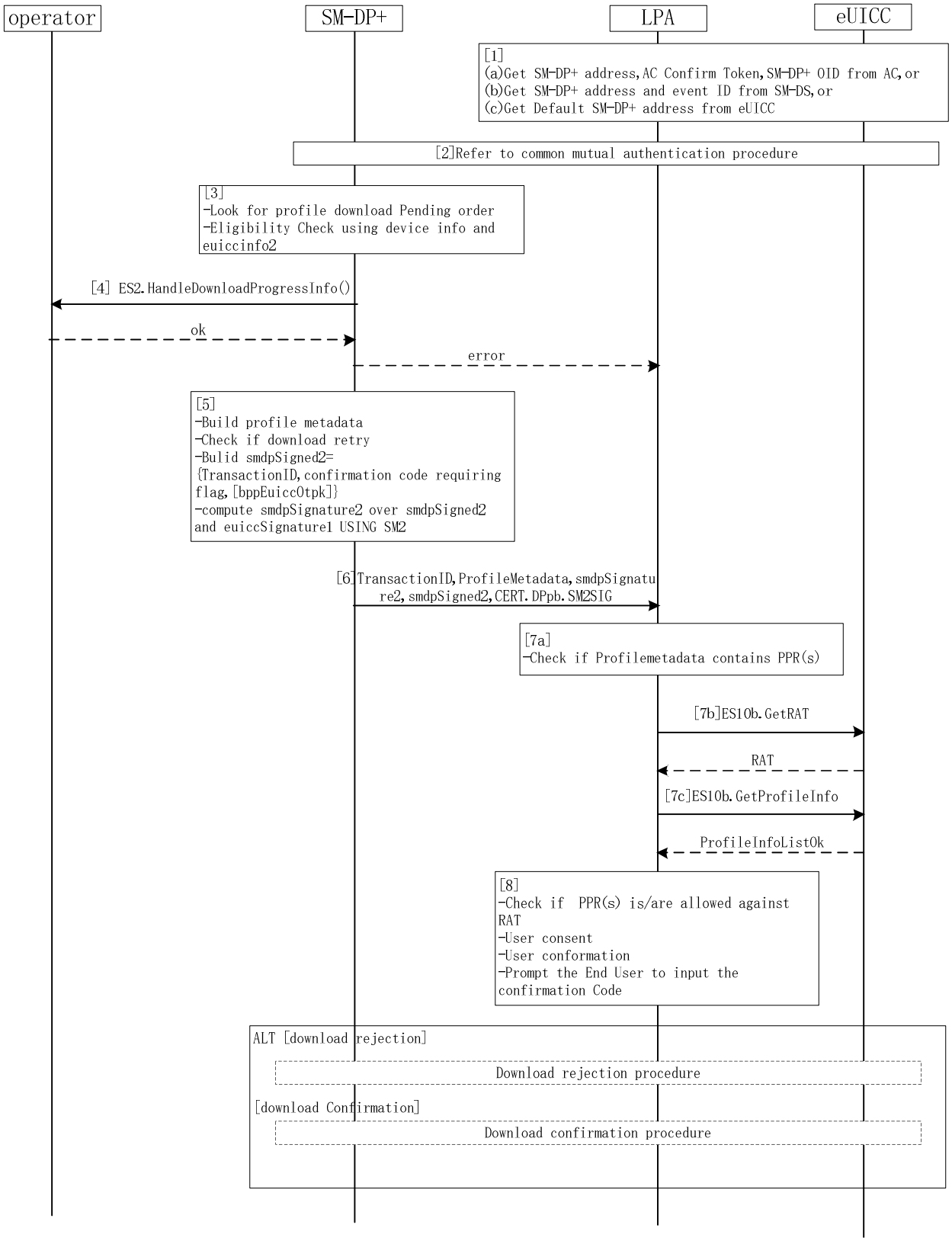

图 3　签约数据文件下载和安装流程

初始条件：

除 6.1.2 中定义的通用双向鉴权流程所需的初始条件之外，此过程需要根据步骤 1 中的选项执行以下初始条件：

如果此过程使用激活码（选项(a)）：

- 最终用户具有如 YD/T XXXX-202X 9.1 所述的激活码。
- 最终用户已经将激活码输入到 LPAd。根据设备能力，LPAd 可以通过手动输入和 QR 码扫描来支持激活码的输入。
- 如果此过程使用 SM-DS（选项(b)）：
- LPAd 已从 SM-DS 获取 SM-DP+ Address 和 EventID。
- 如果此过程使用默认 SM-DP+（选项(c)）：
- LPAd 已通过"ES10a.GetEuiccConfiguredAddresses"功能从 eUICC 中获取默认 SM-DP+地址。

此外，对于每个配置文件，SM-DP+将保留对下载该签约数据文件的尝试次数的计数和在下载该签约数据文件过程中输入确认码的尝试次数的计数。SM-DP+应分别限制下载尝试次数和确认码尝试次数。

一个预置的签约数据文件可以根据 GSMA SGP.21 义的用户 RSP 操作请求由 LPAd 启用。如果运营签约数据文件将被禁用且使用当前使能签约数据文件建立连接不成功，则该操作应含用户的同意。

最后，如果已经安装了使用 PPR1 组的签约数据文件，则发生在以下情况之下：最终用户已被告知此情况，并已同意下载，或者 LPA 可以在下载过程中任意时间点请求用户同意。

步骤：

1) （可选地，即对于选项（a））LPAd 解析激活码并找到 SM-DP+地址、激活码令牌和可选的 SM-DP+ OID。如果激活码的格式无效，则应停止流程，并由 LPAd 向最终用户提供错误消息。
2) 执行 6.1.2 定义的通用双向鉴权流程。当此流程用于签约数据文件下载和安装时，SM-XX 为 SM-DP+ ， CERT.XXauth.SM2SIG 、 PK.XXauth.SM2SIG 和 SK.XXauth.SM2SIG 分别为 CERT.DPauth.SM2SIG，PK.DPauth.SM2SIG 和 SK.DPauth.SM2SIG。ESXX 是 ES9+。

在步骤 10）的通用双向鉴权过程中，LPAd 应验证 SM-DP+返回的 CERT.DPauth.SM2SIG 中包含的 SM-DP+ OID 是否与 LPAd 已经从步骤 1)激活码中获得的 SM-DP+ OID 相同。如果比较失败，LPAd 将通知最终用户，并且流程终止。

在步骤 10）的通用双向鉴权过程中，LPAd 将创建 ctxParams1 数据对象，以将 MatchingID、Device Info 提供给 eUICC 进行签名。MatchingID 的值应设置如下：

- 如使用激活码，则 MatchingID 值应设置为激活码令牌。
- 如使用 SM-DS，则 MatchingID 值应设置为 EventID。
- 如使用默认 SM-DP+，则 MatchingID 值应设置为空字符串。

3) 在上述步骤 2）结束后，成功验证 eUICC 后，SM-DP+应：

- 确认提供了 MatchingID 的相关待定签约数据文件下载订单。
- 如果此签约数据文件下载订单已经链接到 EID，请验证它是否与经过身份验证的 eUICC 的 EID 相匹配。
- 确认与待处理的签约数据文件下载订单对应的签约数据文件处于“已下载”状态，或者在由于以前的安装失败而重试的情况下，处于“已下载”状态

如果这些验证中的任何一个失败，则 SM-DP+应返回相关的错误状态，并且程序应该停止。

SM-DP+应递增所标识的数据签约文件下载尝试次数。如果超过了最大尝试次数，SM-DP+应终止相应的数据签约文件下载命令，并通过调用“ES2+.HandleDownload ProgressInfo”（处理下载进度信息）函数来通知运营商，操作状态指示“失败”并显示相关的错误状态。程序将被停止。

否则，SM-DP+应根据设备信息和/或 eUICCInfo2 执行适当的资格检查。这些检查应包括检查 eUICC 是否可以安装一个签约数据文件。

4) （可选）根据与运营商达成一致的行为（本文件范围之外），SM-DP+应使用功能“ES2+.HandleDownloadProgressInfo”（处理下载进度信息）向运营商通知资格检查的结果。SM-DP+应提供 EID，ICCID，到达的点的标识（在这种情况下，应该是“资格检查”），达到这个点的时间戳，以及这个步骤的执行结果。

注：此通知步骤可以异步完成。

5) 如果资格检查失败，SM-DP+应：

- 在“错误”状态下设置与待处理的签约数据文件下载顺序对应的签约数据文件
- 向 LPAd 返回一个错误状态，程序应停止。
- 否则，SM-DP+应该：
- 确定签约数据文件是否已经绑定到 EID 从以前不成功的下载尝试。如果是这样，则 SM-DP+可以在 smdpSigned2 数据结构中包含前一个会话中获得的 otPK.eUICC.SM2KEYEX。
- 确定此待处理命令是否需要确认码。
- 生成包含交易 ID 和确认码必需标志的 smdpSigned2 数据结构。
- 使用 SK.DPpb.SM2SIG 通过 smdpSigned2 和 euiccSignature1 计算 smdpSignature2。

6) SM-DP+ 将 TransactionID 、 ProfileMetadata 、 smdpSigned2 、 smdpSignature2 和 CERT.DPpb.SM2SIG 返回给 LPAd。

7) 7a)在接收到 SM-DP+响应时，LPAd 会检查 ProfileMetadata 是否包含 PPR。

7b)如果 ProfileMetadata 包含 PPR 并且 LPAd 无规则授权表，则 LPAd 应通过调用“ES10b.GetRAT”功能从 eUICC 请求规则授权表。

7c）如果 ProfileMetadata 包含 PPR1，并且 LPAd 还没有已安装签约数据文件列表，则 LPAd 应通过调用“ES10b.GetProfilesInfo”列表从 eUICC 请求该信息。如果 ProfileMetadata 包含 PPR1 并安装了操作签约数据文件，则 LPAd 应按照原因代码“PPR 不允许”执行下文的“签约数据文件下载和安装-下载拒绝”子流程。

8) 如果 ProfileMetadata 包含 PPR，LPAd 将检查 PPR 是否允许。如果不允许一个或多个 PPR，则 LPAd 将继续按照原因代码“PPR 不允许”执行下文的“签约数据文件下载和安装-下载拒绝”子流程。如果任何 PPR 根据 RAT 需要额外用户同意，LPAd 应通过显示 PPR 的相关信息来请求用户同意。该信息应包括策略规则对用户的结果。该消息应以描述性和没有歧义的方式制定（例如，对于“非删除”签约数据文件策略规则：“您即将安装的配置文件只能根据您同意的服务提供商的条款进行删除。同意安装是/否？”）。

如果最终用户不同意签约数据文件策略规则，LPAd 将继续按照原因代码“用户拒绝”进行下文的“签约数据文件下载和安装 - 下载拒绝”子流程。

除非初始设备设置，应强制执行鉴权确认。

安装签约数据文件策略规则和签约数据文件下载的用户同意请求可能会组合到单独的提示中，因此需要最终用户的单个确认。无论是组合还是分离，这些都可以在 LPAd 下载 BPP 期间或之后执行，因为同样的签约数据文件元数据也可用。

如果在激活码令牌或 smdpSigned2 中设置了需要确认代码的标志，则 LPAd 应提示用户输入运营商提供的确认码。当提示时，LPAd 还可以显示 ProfileName 或包含在签约数据文件元数据中的任何相关信息，以帮助用户识别要在此 RSP 会话期间下载的签约数据文件。如果不需要确认码，LPAd 可以通过将 ProfileName 或包含在签约数据文件元数据中的任何相关信息显示给

最终用户来请求用户确认（例如简单的“是”或“否”或“稍后处理”），这些都可以在 LPAd 下载 BPP 期间或之后执行，因为同样的签约数据文件元数据也可用。

用户不同意下载签约数据文件的情况（例如，通过选择“否”或“稍后处理”），将在下文的子流程“签约数据文件下载和安装-下载拒绝”中进行说明。

如果最终用户在执行根据超时时间内没有响应 LPAd 提示，则 LPAd 将通过执行“签约数据文件下载和安装-下载拒绝”下文的子流程来取消签约数据文件下载，其原因是“超时”。

如果需要，LPAd 将按如下方式计算确认码的 HASH：

- HASH 确认码= SHA256（ SHA256（确认码）| TransactionID），其中'|'表示数据级联。

如果在上述步骤中没有拒绝签约数据文件下载，则应继续执行子流程“配置文件下载和安装-下载确认”

6.1.2.2 签约数据文件下载和安装-下载拒绝流程

该流程发生在签约数据文件下载的用户拒绝或超时等情况下：

- 对“ES9+.Authenticate Client”的响应之后
- 对“ES9+.GetBoundProfilePackage”的响应之后。

LPA可以提供额外的空间，最终用户将被提供这种可能性。

如果LPAd检测到"ES9+.Authenticate Client" 和 "ES9+.GetBoundProfilePackage"返回的签约数据文件Metadata不匹配，该过程也会发生。

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>Operator" as OP
participant "<b>SM-DP+" as DP
participant "<b> LPAd" as LPA
participant "<b>eUICC" as E

LPA -> E : [1] ES10b.CancelSession(TransactionID, reason)
rnote over E #FFFFFF
[2]
- Generate euiccCancelSessionSigned = {
    TransactionID, reason}
- Compute euiccCancelSessionSignature
    over euiccCancelSessionSigned
endrnote
E --> LPA : [3] euiccCancelSessionSigned, \neuiccCancelSessionSignature
```

```
LPA -> DP : [4] ES9+.CancelSession(TransactionID, \neuiccCancelSessionSigned, euiccCancelSessionSignature)

rnote over DP #FFFFFF
[5]
- Verify euiccCancelSessionSignature
- Get the reason
endrnote
DP --> LPA : [error]

Group Cond. Download rejection
rnote over DP #FFFFFF
[6]
- Terminate Download order
- [Delete Event, Refer to Event Deletion section 3.6.3]
endrnote

DP -> OP : [7] ES2+.HandleDownloadProgressInfo
OP --> DP : OK

end

DP --> LPA : OK

@enduml
```

签约数据文件下载和安装子过程（下载拒绝）如图4所示。

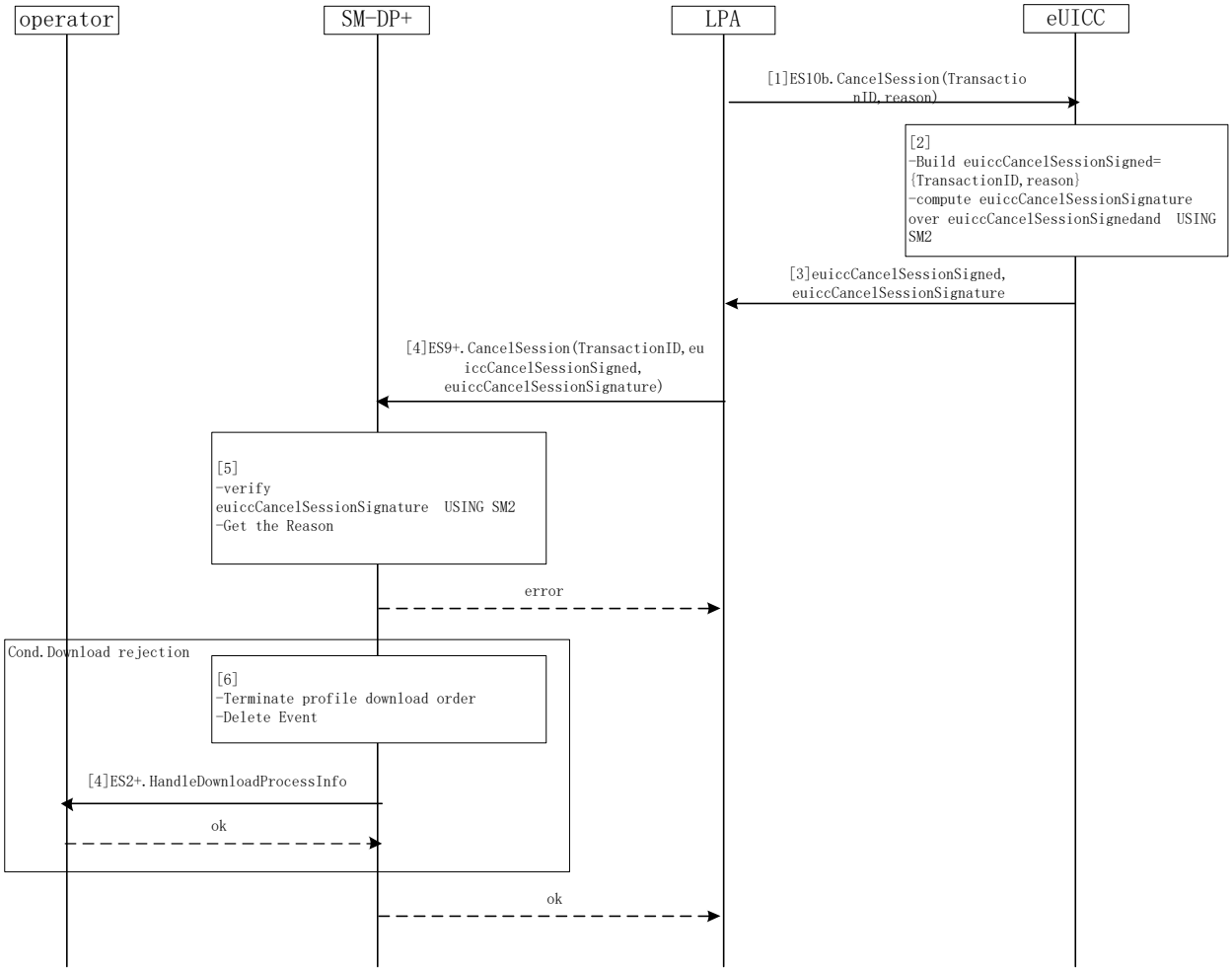

图 4　签约数据文件下载和安装子过程-下载拒绝

初始条件：

用户不同意下载签约数据文件（即选择“否”），或者根据规则授权表不允许ProfileMetadata中的PPR，或PPR1存在于ProfileMetadata中，并且操作签约数据文件已经安装在eUICC上。“ES9+.Authenticate Client”的响应中的ProfileMetadata和BPP中的Profile Metadata不匹配，或LPAd在BPP安装过程中发生错误。

步骤：

1) LPAd 应调用“ES10b.CancelSession”函数接口，其输入数据包括 TransactionID 和“用户拒绝”原因，“用户推迟”或 “超时”，“PPR 不允许”，“元数据不匹配”，“下载 BPP 执行错误”或“未定义原因”。
2) 接到这个函数调用后，eUICC 应该：
   a) 生成包含 TransactionID 和 LPAd 提供原因的 euiccCancelSessionSigned 数据对象。
   b) 使用相互认证过程中接收到的与 euiccCiPKIdToBeUsed 相对应的 SK.EUICC.SM2SIG，并通过 euiccCancelSessionSigned 计算 euiccCancelSession Signature。
3) eUICC 应返回 euiccCancelSessionSigned 和 euiccCancelSessionSignature 给 LPAd。
4) LPAd 应调用“ES9+.CancelSession”，其输入数据包括 TransactionID，euicc CancelSessionSigned 和 euiccCancelSessionSignature。

5) 接收到“ES9+.CancelSession”功能后，SM-DP+应：

- 检索由 TransactionID 标识的正在进行的 RSP 会话。如果 TransactionID 是未知的，SM-DP+应该返回一个功能执行状态“Failed”和相关的状态码。如果提供的值不正确，则 LPAd 可以使用不同的 TransactionID 重试此步骤。
- 使用与正在进行的 RSP 会话相关联的 PK.EUICC.SM2SIG 验证 euiccCancelSession Signature 是否通过 euiccCancelSessionSigned 签署。如果签名无效，则 SM-DP+应返回带有相关状态码的功能执行状态“失败”，程序应由 LPAd 停止。
- 验证收到的 smdpOid 是否与 SM-DP+相对应（即与在 Common Mutual Authentication Procedure 中使用的 CERT.DPauth.SM2SIG 中包含的值相同）。如果值不匹配，SM-DP+应该返回带有相关状态码的功能执行状态“失败”，程序应由 LPAd 停止。

如果 eUICCCancelSessionSigned 中包含的原因表示“最终用户推迟”或“超时”，则 SM-DP+应简单地返回功能执行状态“执行成功”，并将相应的签约数据文件下载命令保持在“已发布”状态，以便再次重试，程序应该停止。

如果 euiccCancelSessionSigned（eUICC 取消会议签名）中包含的原因指示任何其他条件，SM-DP+将执行以下步骤。

6) SM-DP+应将与正在进行的 RSP 会话关联的签约数据文件设置为“错误”状态（参见本文件的 6.1.7）；如果在选项（b）中执行该过程，则 SM-DP+应执行第 6.6.1 节中描述的 SM-DS 事件删除过程。

7) 根据给定的取消原因，SM-DP+应调用“ES2+.HandleDownloadProgressInfo”（处理下载进度信息）函数和相关的 notificationPointId（通知点 ID）集合以及状态码值为“Failed”的操作状态。取消会话原因码映射到状态码在 7.3.5 节给出。

SM-DP+应返回函数执行状态“Executed-Success”（成功执行）和程序应当停止返回。

6.1.2.3 签约数据文件下载和安装-下载确认流程

本条描述签约数据文件下载和安装-下载确认流程。

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>Operator" as OP
participant "<b>SM-DP+" as DP
participant "<b> LPAd" as LPA
participant "<b>eUICC" as E

LPA -> E : [1] ES10b.PrepareDownload \n (smdpSigned2, smdpSignature2, CERT.DPpb.SM2SIG,
```

[Hashed Confirmation Code])
rnote over E #FFFFFF
[2]
- Verify CERT.DPpb.SM2SIG
- Verify CERT.DPauth.SM2SIG and CERT.DPpb.SM2SIG have same owner
- Verify smdpSignature2 over smdpSigned2
- Verify smdpSigned2
Endrnote
E --> LPA: [error]
rnote over E #FFFFFF
[3]
- Generate one time SM2KEYEX key pair
    (otPK.EUICC.SM2KEYEX, otSK.EUICC.SM2KEYEX)
unless a valid otPK.EUICC.SM2KEYEX was provided
- Generate euiccSigned2=
    {TransactionID, otPK.EUICC.SM2KEYEX, [Hashed Confirmation Code]}
- Compute euiccSignature2 over euiccSigned2 and smdpSignature2
Endrnote
E -> LPA: [4] euiccSigned2, euiccSignature2
LPA -> DP : [5] ES9+.GetBoundProfilePackage \n (euiccSigned2, euiccSignature2)

rnote over DP #FFFFFF
[6]
- Verify euiccSignature2 over euiccSigned2
- Determine if Confirmation Code required
Endrnote
DP --> LPA : [error]

Group Cond. Confirmation Code handling
rnote over DP #FFFFFF
[7]
- [Verify Hashed Confirmation Code]
Endrnote
Group Cond. On CC error
DP -> OP : [8] ES2+.HandleDownloadProgressInfo
OP --> DP : OK
DP --> LPA : [error]
end

rnote over DP #FFFFFF
[9]
- [Generate one time SM2KEYEX key pair (otPK.DP.SM2KEYEX, otSK.DP.SM2KEYEX)]

- [Generate Session Keys]
- Generate Bound Profile Package
Endrnote

Group Opt.
DP -> OP : [10] ES2+.HandleDownloadProgressInfo(...)
OP --> DP : OK
end

DP --> LPA : [11] TransactionID, Bound Profile Package

rnote over LPA #FFFFFF
[12]
- [Verify Metadata]
- [Prompt/Display Profile Metadata to End User]
Endnote

alt
    rnote over OP, E #FFFFFF : [13] [Refer to Sub-procedure Profile Download and installation – Download rejection]
else
    rnote over OP, E #FFFFFF : [14] [Refer to Sub-procedure Profile Installation]
end
@enduml

签约数据文件下载和安装子过程（下载确认）如图 5 所示。

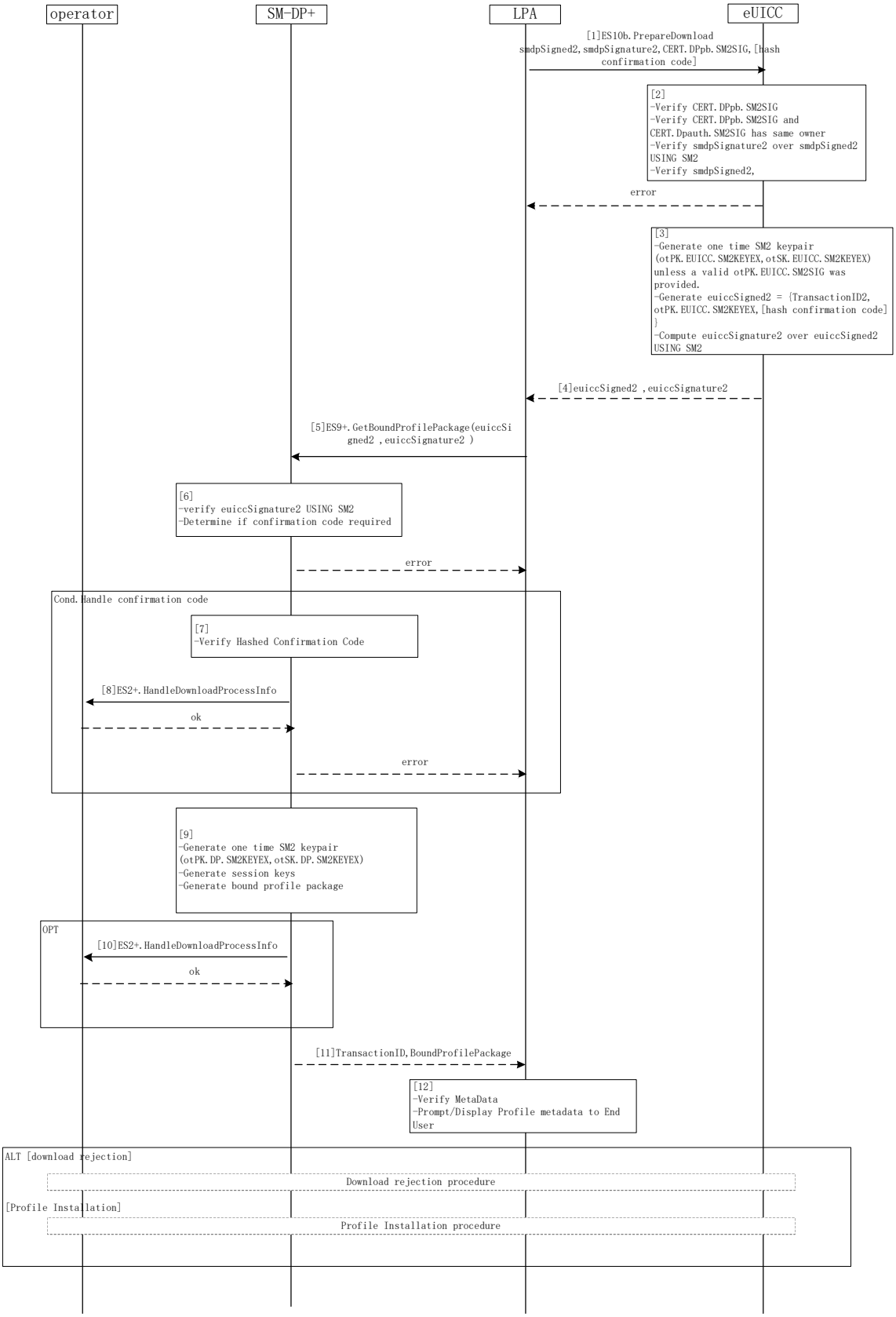

图 5　签约数据文件下载和安装子过程-下载确认

初始条件：

用户同意下载签约数据文件（即通过选择“是”）。

步骤：

1) LPAd 应调用"ES10b.PrepareDownload" 接口，其输入数据包括 wsmdpSigned2, smdpSignature2、CERT.DPpb.SM2SIG，还有可选的在签约数据文件下载和安装过程最终一步（符合 YD/T ZZZZ-202X 10.1.2.1）计算的确认码。
2) 在接收到“ES10b.PrepareDownload”（准备下载）功能时，eUICC 应该：
   a) 验证 CERT.DPpb.SM2SIG 是否有效。
   b) 确定 CERT.DPauth.SM2SIG 和 CERT.DPpb.SM2SIG 属于同一个实体（即相同的 subjectAltName 中的 OID 相同）。
   c) 使用 CERT.DPpb.SM2SIG 中包含的 PK.DPpb.SM2SIG 验证 smdpSignature2 是否通过 smdpSigned2 和 euiccSignature1 执行。
   d) 验证 smdpSigned2 中包含的 TransactionID 是否与正在进行的 RSP 会话的 TransactionID 匹配。
   e) 如果在 smdpSigned2 中设置了确认码必需标志，请验证 LPAd 是否提供 Hash 确认码。

   如果任何一个验证失败，eUICC 应返回一个相关的错误状态，程序应该停止。
3) 否则，eUICC 应：
   a) 如果在 smdpSigned2 中提供了 bppEuiccOtpk，并且它对应于此 SM-DP+的存储的一次性密钥对（otPK.EUICC.SM2KEYEX，otSK.EUICC.SM2KEYEX），则 eUICC 应使用此密钥对进行 RSP 会话。否则，应使用 CERT.DPpb.SM2SIG 的关键参数值生成一个新的一次性密钥对（otPK.EUICC.SM2KEYEX，otSK.EUICC.SM2KEYEX）。
   b) 生成包含 TransactionID，otPK.EUICC.SM2KEYEX 和可选的 Hash 确认码的 euiccSigned2 数据结构。
   c) 通过 euiccSigned2 和 smdpSignature2 并调用 SK.EUICC.SM2SIG 计算 euicc Signature2。生成 euiccSignature2 时，eUICC 将使用与 AuthenticateServer（验证服务器）响应中相同的私钥。
4) eUICC 应返回 euiccSigned2 和 euiccSignature2 到 LPAd。
5) LPAd 应调用 "ES9+.GetBoundProfilePackage" 接口，其输入数据包括 euiccSigned2、euiccSignature2。
6) 在接收到“ES9+.GetBoundProfilePackage”（获得绑定签约数据文件包）功能时，SM-DP+应使用与由交易 ID 标识的 RSP 会话相关联的 PK.EUICC.SM2SIG 验证通过 euiccSigned2 和 smdpsignature2 执行的 euiccSignature2。

   如果需要确认码，则 SM-DP+应继续执行步骤 7.否则，SM-DP+应继续执行步骤 9。
7) 如果需要验证码验证，则 SM-DP+应：
   - 通过“ES2.ConfirmOrder”检索为此订单存储的散列确认码，并将期望的 Hash 值计算为：预期的 Hash 值= SHA256（存储的散列确认码| 交易 ID）。
   - 验证收到的 Hash 确认码与预期的散列值匹配。

- 如果确认码验证失败，SM-DP+应递增签约数据文件的确认码尝试次数。如果超过最大重试次数，则 SM-DP+应将签约数据文件下载顺序对应的签约数据文件设置为“错误”状态（参见 YD/T XXXX-202X 的 6.1.7）并执行步骤 8。

8) （视情况而定）SM-DP+应通过调用“ES2+.HandleDownloadProgressInfo”（相应的标识点为“确认码检查”）和操作状态（执行状态=“失败” 与相关的状态码值）。

如果步骤 6）或 7）中的任何验证失败，则 SM-DP+应将错误状态返回给 LPAd，并且程序应该停止。除非已超过确认码条目的最大重试次数，否则 LPAd 可以通过重新启动签约数据文件下载和安装过程来重试。

9) 否则，SM-DP+应执行以下操作：

- 如果存在可重用的 BPP，并且 eUICC 返回了相应的 otPK.EUICC.SM2KEYEX，则只需要重新计算 InitialiseSecureChannel（初始化安全通道）的签名，并且可以跳过下一步。
- 如果可重复使用的 BPP 存在且 eUICC 返回了不同的 otPK.EUICC.SM2KEYEX，则 SM-DP+应向 LPAd 返回一个错误并终止该过程，或按照《面向消费电子设备的支持远程 SIM 配置的终端技术要求》 的 12.1.2 节所述重新绑定 PPP。
- 如果签约数据文件未链接到目标 eUICC 的 EID，则 SM-DP+应在此步骤将签约数据文件链接到 EID。
- 使用 CERT.DPpb.SM2SIG 的关键参数值指示的曲线生成一次性 SM2KEYEX 密钥对（otPK.DP.SM2KEYEX，otSK.DP.SM2KEYEX）。
- 根据 YD/T XXXX-202X 附录 D（对应 sgp.22 的附录 G）使用 CRT，otPK.eUCC.SM2KEYEX 和 otSK.DP.SM2KEYEX 生成会话密钥。
- 根据 YD/T XXXX-202X5.9.4 中给出的说明准备绑定签约数据文件包，包括可选的签约数据文件保护密钥（PPK）。

10) （可选步骤）根据与运营商达成一致的行为（本文件范围之外），SM-DP+应通知运营商使用功能“ES2+.HandleDownloadProgressInfo”（处理下载程序信息）下载了签约数据文件。SM-DP+应提供 EID，ICCID，到达点的标识（在这种情况下，应为“BPP 下载”），达到此点的时间戳，以及此步骤的执行结果。注意：此通知步骤可以异步完成。

11) SM-DP+将 TransactionID 和 BPP 响应返回到 LPAd，并将签约数据文件下载顺序设置为“已下载”状态。

12) 在 SM-DP+响应接收时，LPAd 可以使用 BPP 中包含的签约数据文件 Metadata 执行额外流程：

- 如果 LPAd 之前使用由“ES9+.AuthenticateClient”返回的签约数据文件元数据，则
    - LPAd 将验证 PPR 没有更改。如果验证失败，LPAd 应以原因码“PPR 不允许”执行“签约数据文件下载和安装-下载拒绝”子流程。
    - LPAd 应验证在之前的步骤中使用的所有其它签约数据文件 Metadata 元素（如签约数据文件名称，图标等）没有更改，如果此验证失败应终止该流程。若验证失败，LPAd 可以通知用户，并提供给用户推迟或拒绝签约数据文件安装的操作。或者，

LPAd 可以以原因码“Metadata 不匹配”执行“签约数据文件下载和安装-下载拒绝”子流程。

- 如果 LPA 之前没有收到关于签约数据文件 Metadata 和任何签约数据文件策略规则的用户许可，则

  LPAd 可以显示签约数据文件 Metadata 的任何相关部分，以帮助最终用户在该流程中识别要安装的签约数据文件。基于该信息，LPAd 可以提供最终用户推迟或拒绝签约数据文件安装的操作。如果用户在超时时间内未响应 LPAd 提示，则 LPAd 将通过执行“签约数据文件下载和安装-下载拒绝”子流程，以”Timeout” 原因来取消签约数据文件下载。

13) 如果最终用户延迟或拒绝签约数据文件安装，应执行 YD/T XXXX-202X6.1.4 中定义的“签约数据文件下载和安装-下载拒绝”子流程。
14) 否则应执行后续签约数据文件安装子流程。

6.1.2.4 签约数据文件安装流程

本条描述签约数据文件安装流程。

```
@startuml
hide footbox
skinparam sequenceMessageAlign center
skinparam sequenceArrowFontSize 11
skinparam noteFontSize 11
skinparam monochrome true
skinparam lifelinestrategy solid

participant "<b>Operator" as OP
participant "<b>SM-DP+" as DP
participant "<b> LPAd" as LPA
participant "<b>eUICC" as E

LPA -> E : [1] ES10b.LoadBoundProfilePackage x N\n(ES8+.InitialiseSecureChannel)

rnote over E #FFFFFF
[2]
- Verify InitialiseSecureChannel data
- Generate Session Keys
endnote
E --> LPA : Response APDU x N
LPA -> E : [3] ES10b.LoadBoundProfilePackage x N\n(ES8+.ConfigureISDP)
E --> LPA : Response APDU x N
LPA -> E : [4] ES10b.LoadBoundProfilePackage x N\n(ES8+.StoreMetadata)
E --> LPA : Response APDU x N
```

```
Group Cond. ES8+.StoreMetadata contains PPR(s)
rnote over E #FFFFFF
[4a] Verify PPR(s) against RAT. Refer to section 2.9.3.1
endrnote
end

LPA -> E : [5] [ES10b.LoadBoundProfilePackage x N]\n(ES8+.ReplaceSessionKeys)
E --> LPA : [Response APDU x N]
LPA -> E : [6] ES10b.LoadBoundProfilePackage x N\n(ES8+.LoadProfileElements)
E --> LPA : Response APDU x N \n(ProfileInstallationResult)


LPA -> DP : [7] ES9+.HandleNotification(ProfileInstallationResult)
DP --> LPA : OK

rnote over DP #FFFFFF
[8] [Terminate Download order]
endrnote

DP -> OP : [9] [ES2+.HandleDownloadProgressInfo]
OP --> DP : OK

rnote over DP #FFFFFF
[10] [Delete Event, Refer to Event Deletion section 3.6.3]
endrnote

LPA -> E : [11] ES10b.RemoveNotificationFromList

rnote over E #FFFFFF
[12] Delete Notification
endrnote

E --> LPA : OK

@enduml
```

签约数据文件安装子流程如图 6 所示。

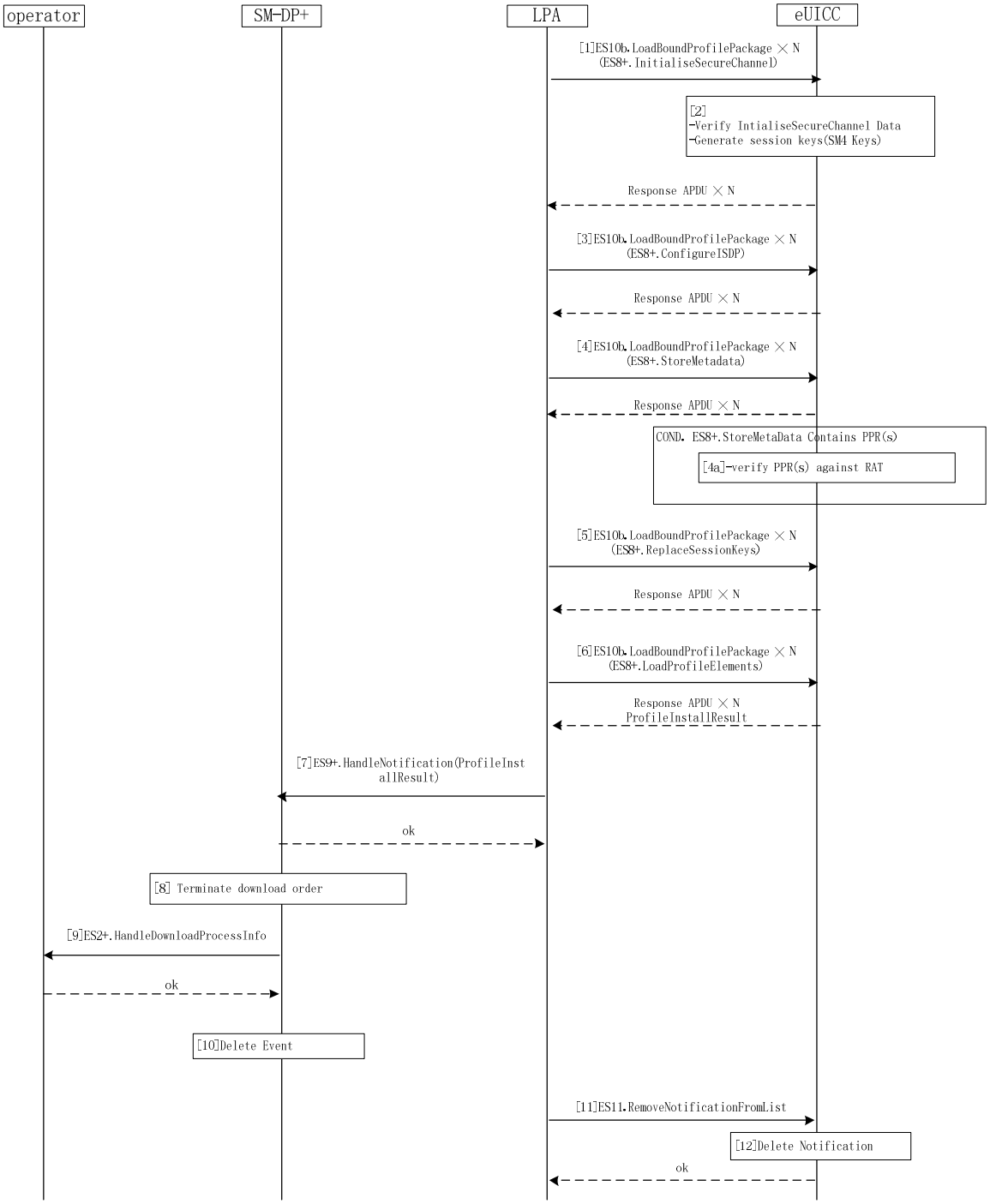

图 6　签约数据文件安装子流程

在该子流程中，LPAd根据YD/T XXXX-202X 5.9.5描述生成SBPP，并使用“ES10b.LoadBoundProfilePackage”命令序列将其发送到eUICC。如果LPAd无法执行分段（例如，由于BPP结构中的错误），或者如果任何“ES10b.LoadBoundProfilePackage”的调用返回除“90 00”或“91 XX”之外的状态字，LPAd应以原因码“下载BPP执行错误”执行子流程“签约数据文件下载和安装-下载拒绝”。