ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0099—2020

开放式版式文档密码应用技术规范

Cryptography application technical specification of open fixed layout documents

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：中安网脉（北京）技术有限公司、北京数字认证股份有限公司、中国电子技术标准化研究院、北京电子科技学院、数安时代科技股份有限公司、北京数科网维技术有限责任公司、航天福昕软件（北京）有限公司、吉大正元信息技术股份有限公司、兴唐通信科技有限公司、成都卫士通信息产业股份有限公司。

本文件主要起草人：刘歆、王佳宁、王天顺、林雪焰、李海波、陈亚军、张永强、张立廷、田景成、朱亚飞、王少康、冯辉。

开放式版式文档密码应用技术规范

1 范围

本文件规范了采用密码技术对开放式版式文档进行签名、加密及完整性保护等相关内容。

本文件适用于指导开放式版式文档密码应用相关产品和系统的研发、使用和检测。

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 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 20520 信息安全技术 公钥基础设施 时间戳规范

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

GB/T 33190—2016 电子文件存储与交换格式 版式文档

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GB/T 38540—2020 信息安全技术 安全电子签章密码技术规范

3 术语和定义

GB/T 33190—2016、GB/T 38540—2020 界定的以及下列术语和定义适用于本文件。

3.1

版式 fixed layout

将文字、图形、图像等多种数字内容对象按照一定规则进行版面固化呈现的一种格式。

[来源：GB/T 33190—2016，3.1]

3.2

开放式版式文档 open fixed layout document

独立于软件、硬件、操作系统、输出设备的版式文档格式。

[来源：GB/T 33190—2016，3.2]

3.3

电子印章 electronic seal

一种由电子印章制作者数字签名的安全数据。

[来源：GB/T 38540—2020，3.1]

3.4

电子签章 electronic seal signature

使用电子印章签署电子文件的过程。

[来源：GB/T 38540—2020，3.2]

4 缩略语

下列缩略语适用于本文件。

CRL：证书吊销列表(Certificate Revocation List)

DER：可辨别编码规则(Distinguished Encoding Rules)

OFD：开放式版式文档(Open Fixed layout Document)

XML：可扩展标记语言(Extensible Markup Language)

5 密码应用机制

OFD是将文字、图形、图像等多种数字内容对象按照一定规则进行版面固化而呈现的电子文档格式，是我国制定的开放格式标准，也是国家电子文件管理的基础文件格式之一。

OFD采用“容器＋文档”的方式描述和存储数据，文档的内容由ZIP包内的多个文件共同决定，OFD存储逻辑结构如图1所示。

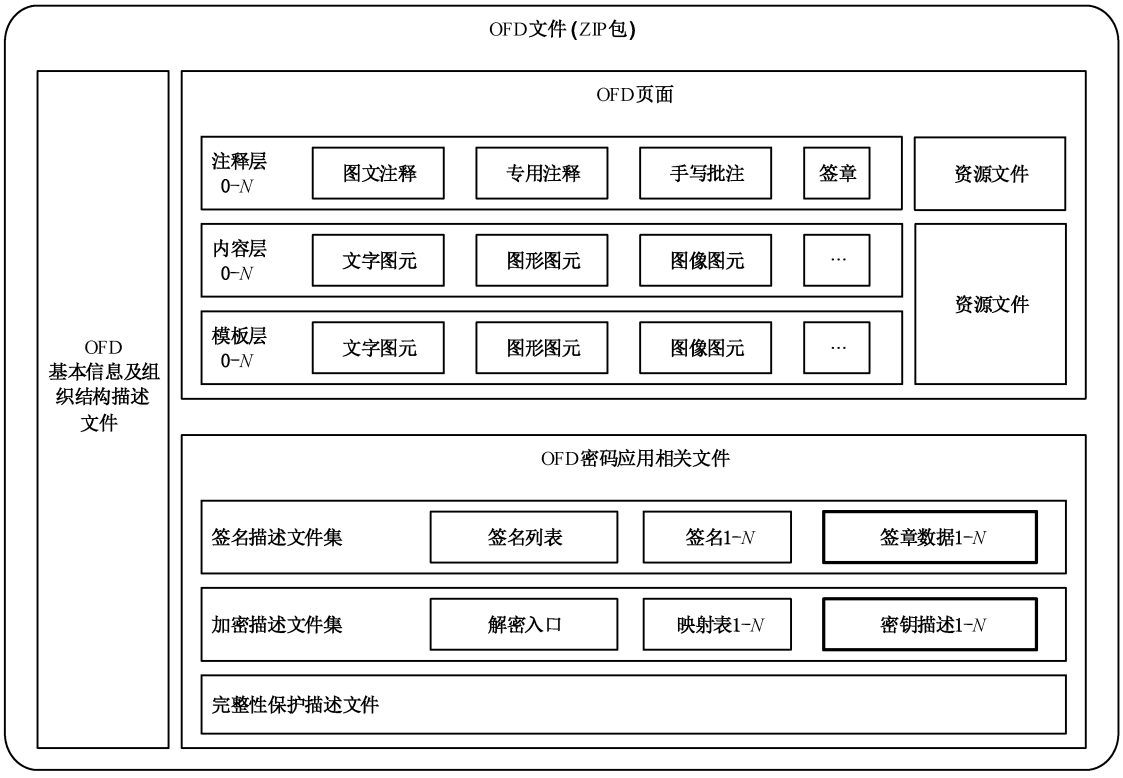

图1 OFD存储逻辑结构

OFD采用“容器(ZIP)＋文档(XML)”的文件存储结构，其ZIP包内主要包括OFD基本信息及组织结构描述文件、OFD页面和OFD密码应用相关文件等。

一个OFD文件内可能包含一个或多个文档，一个OFD文档有一个或多个OFD页面。页面内容可能由模板、内容和注释组成，分层组织。模板层与内容层主要包括文字、图形、图像及其他类型等图元内容，两类图层之间共享资源文件。注释可多层添加，主要包括常规图文注释、专用注释、手写签批和签章等内容，注释内容的资源文件独立。

OFD文档可进行多次签章、签名或加密，其信息采用对应的描述文件集进行记录。签名描述文件

集包括一个签名列表文件和若干组签名描述文件及其签章数据。加密描述文件集包括一个解密入口文件和若干组映射表及密钥描述文件。OFD 文件可包含完整性保护文件，用于防止在压缩包内夹带其他内容。

上述包内描述文件大都采用 XML 格式，部分资源本体文件和签章数据、密钥描述文件采用二进制格式描述。

OFD 的文件层次组织结构如图 2 所示。

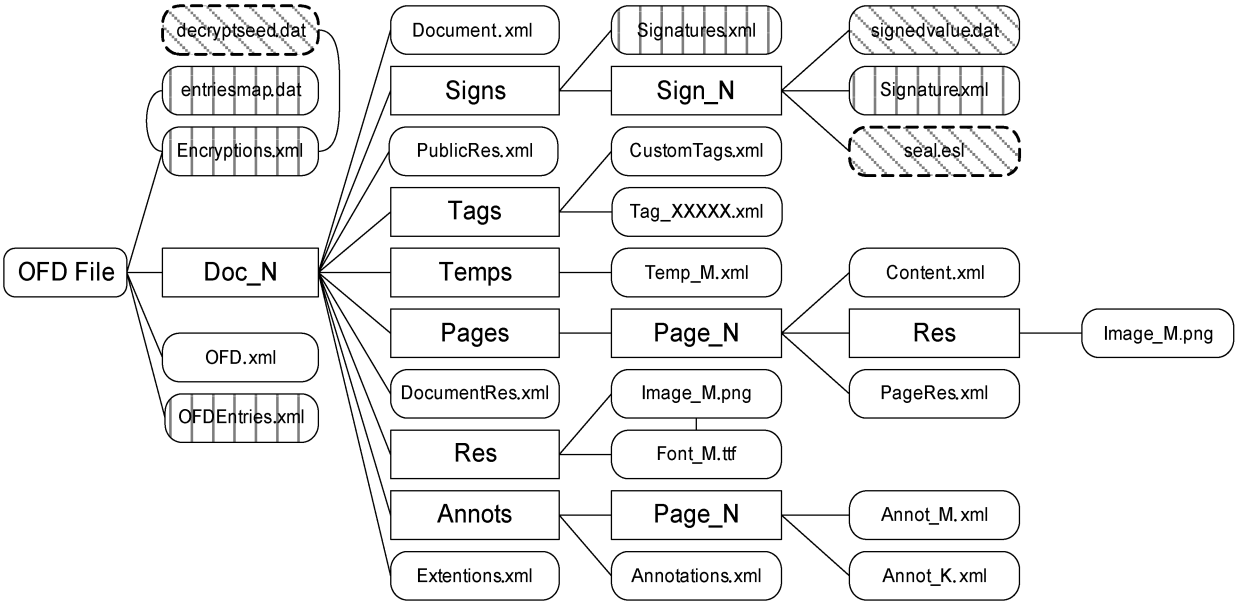

图 2　OFD 文件层次组织结构

其中，Signatures.xml、Signature.xml、Encryptions.xml、OFDEntries.xml、EntriesMap.xml（加密前）为 OFD 的密码应用描述文件，entriesmap.dat（加密后）、decryptseed.dat、signedvalue.dat 和 seal.dat（或.esl）为密码数据文件。

真实性和不可否认性保护时，可根据 OFD 签名协议针对 DOC_N 中 OFD 页面进行单次或多次签名，所有签名相关的内容都保存在签名文件夹 Signs 中。签名列表文件（Signatures.xml，见 GB/T 33190—2016 的 18.1）用于描述 Doc_N 中所有签名构成的签名列表。Sign_N 文件夹用于保存放每次签名生成的签名文件（Signature.xml，见 GB/T 33190—2016 的 18.2）和签名值数据（signedvalue.dat）。签名文件用于描述签名类型、签名保护范围、签名方案、签名值数据文件路径等内容。

机密性保护时，可根据 OFD 加密协议针对 OFD 中包含关键信息的描述文件或其他关键资源进行局部加密，或者对 OFD 文档涉及的所有包内文件进行整体加密。加密生成的解密入口文件（Encryptions.xml，将在 OFD 2.0 中增补）保存在 OFD 根目录下。解密入口文件用于描述加密操作简要信息、加密方案、明密文映射表（EntriesMap.xml 或 entriesmap.dat）和密钥描述数据（decryptseed.dat）文件路径等内容。

完整性保护时，可根据 OFD 完整性保护协议针对整个 ZIP 包进行保护，生成的完整性描述文件（OFDEntries.xml，将在 OFD 2.0 中增补）保存在 OFD 根目录下，描述支撑文件完整性的包内文件列表、签名方案、保存的签名值等内容。

上述三种密码应用相关文件共同作用，保证 OFD 在存储和传输过程中的机密性、完整性、真实性和不可否认性。

6 密码应用要求

OFD的密码应用的目标是保证文件的机密性、完整性、真实性和不可否认性。

OFD使用密码机制进行安全保护时，应保证各次的操作人对操作行为的不可否认，各层的独立成像效果和叠加后的成像效果真实有效，针对有机密性保护需求的内容应保证其机密性，同时还应保证OFD文件自身的完整性。

保证页面的机密性，应采用对关键信息描述文件进行加密的方式；保证页面及页面叠加效果的真实性和完整性，保证页面操作人对操作行为的不可否认，应采用操作者签名私钥对各页面所有描述文件进行数字签名的方式；保证OFD的完整性，应按OFD标准构建包内有效文件列表，并采用OFD文件操作者的签名私钥对该列表进行数字签名的方式。

7 密码应用协议

7.1 概述

OFD的安全性由签名、加密和完整性保护三个协议共同保证，分别保护文件的真实性和不可否认性、机密性、完整性。三个协议的入口及对象描述部分属于GB/T 33190的内容(附录)，协议中涉及到对数据进行摘要、加密等变换的机制和数据结构是本标准的内容。

在本标准中，对文档进行签名和加密运算时，使用的签名和加密方案标识及对应的相关内容见附录A。

7.2 OFD签名协议

7.2.1 协议描述

OFD签名协议用于保证OFD文档的真实性和签名人对签名行为的不可否认性。签名操作后将在OFD文件内形成新的签名文件和签名值数据，同时在签名列表中增加新形成的签名文件记录。

OFD签名存在两种类型：

a) 电子签章；

b) 数字签名。

OFD签名类型存储在签名列表文件(Signatures.xml)中各Signature节点的Type属性中。

7.2.2 数据格式要求

因OFD签名操作产生的签名文件和签名列表应符合GB/T 33190—2016中第18章的要求。为支持多种签名类型和自定义参数，签名文件应进行如附录B所示的扩展。

因OFD签名操作产生的签名值的数据格式要求如下：

a) 签名类型为电子签章时，签名值数据应遵循GB/T 38540—2020；

b) 签名类型为数字签名且签名算法使用SM2时，签名值数据应遵循GB/T 35275；

c) 签名类型为数字签名且签名算法为其他时，签名值数据应遵循该算法对应的数据值规范。

7.2.3 密码算法要求

OFD签名对密码算法的要求如下：

a) 签名算法使用SM2时，应遵循GB/T 32918(所有部分)和GB/T 35276；

b） 杂凑算法使用 SM3 时，应遵循 GB/T 32905。

7.2.4 数字证书要求

用于 OFD 签名的数字证书要求如下：

a） 证书中使用的算法应采用国家密码管理主管部门核准的算法；

b） 使用基于 SM2 算法的证书时，应遵循 GB/T 20518；

c） 使用其他算法的证书时，应符合国家密码标准和行业标准的要求。

7.2.5 时间戳要求

OFD 签名对时间戳的要求如下：

a） 签名值可包含时间戳；

b） 签名值包含时间戳时，则时间戳格式和使用应遵循 GB/T 20520。

7.2.6 签名流程

OFD 数字签名流程要求如下：

a） 确认参与签名的文件列表；

b） 根据签名方案，调用杂凑算法分别计算每个文件的杂凑值；

c） 见附录 B 所示的数据结构，组装签名文件；

d） 调用杂凑算法计算签名文件的杂凑值；

e） 根据签名方案，使用操作人签名私钥对杂凑值进行数字签名或电子签章；

f） 将签名值数据写入签名文件中。

7.2.7 验签流程

验证签名流程如下：

a） 根据签名文件中的签名方案，调用杂凑算法计算签名文件的杂凑值；

b） 根据签名文件中的签名方案，结合步骤 a）所得的杂凑值进行签名验证或签章验证，签章验证流程遵循 GB/T 38540；

c） 根据签名文件中的签名保护范围，逐个读取 OFD 文件包内的文件内容，计算杂凑值并与签名文件中的记录值做比对。

7.3 OFD 加密协议

7.3.1 协议描述

OFD 加密协议用于保障 OFD 文档中关键图形、图像、文字、印章等内容的机密性，其方案在 OFD2.0 规范中描述，见附录 C。每次加密操作后将在 OFD 文件内形成新的映射表和密钥描述文件，同时在解密入口文件中增加新形成的加密操作记录。

OFD 支持以下两种加密方式：

a） 口令加密；

b） 证书加密。

7.3.2 数据格式要求

OFD 采用“XML＋ZIP”的格式架构，文档的内容由 ZIP 包内的多个文件共同决定。可根据需要对不同的包内文件进行加密，实现文档局部或整体加密功能。

加密保护文件的数据结构和内容说明见附录C。

7.3.3 密码算法要求

OFD加密的算法要求如下：

a) 加密方案应符合国家密码管理主管部门的要求；
b) 加密算法采用SM2时，遵循GB/T 32918(所有部分)和GB/T 35276；
c) 加密算法采用SM4时，遵循GB/T 32907；
d) 加密算法采用其他算法时，应符合国家密码标准和行业标准的要求。

7.3.4 加密流程

根据加密方案进行文件加密。流程如下：

a) 生成用于ZIP包内文件加密的对称密钥；
b) 根据加密方案，使用步骤a)生成的文件加密对称密钥调用对称密码算法加密包内文件并写入ZIP包内；
c) 根据加密方案，对已经生成密文的明文文件进行处理，部分写入ZIP包；
d) 组装明密文映射表文件，根据加密方案对其进行加密后或直接写入ZIP包；
e) 组装加密入口文件，明文写入ZIP包；
f) 根据加密方案，对文件加密对称密钥进行密钥包装或非对称加密生成文件对称加密的包装密钥；
g) 如果电子文件访问者为多人，则重复7.3.4的步骤e)；
h) 组装密钥描述文件，并写入ZIP包。

7.3.5 解密流程

根据加密方案进行文件解密。流程如下：

a) 根据电子文件访问者身份从密钥描述文件的加密信息中获取文件对称加密的包装密钥；
b) 根据电子文件访问者身份，要求输入口令或读取用户私钥对文件对称加密的包装密钥进行解密，获取文件对称加密密钥；
c) 调用对称算法解密明密文映射表文件；
d) 根据文档解析流程，调用对称算法解密包内密文并用于OFD软件处理。

7.4 OFD完整性保护协议

7.4.1 协议描述

OFD完整性协议用于保证OFD文档自身的完整性。通过OFD完整性保护文件，可以检测OFD是否存在非法夹带。

7.4.2 数据格式要求

OFD的完整性保护信息使用XML文件描述。完整性保护文件中应记录OFD文件内与文档内容相关的所有包内文件。应对完整性保护文件实施带有时间戳的数字签名。

完整性保护文件的数据结构和内容说明见附录D。

7.4.3 密码算法要求

完整性保护要求如下：

a) 完整性保护使用的签名方案，应符合国家密码标准和行业标准的要求；
b) 签名算法采用 SM2 时，遵循 GB/T 32918(所有部分)和 GB/T 35275；
c) 杂凑算法采用 SM3 时，遵循 GB/T 32905；
d) 签名算法采用其他算法时，应符合国家密码标准和行业标准的要求；
e) 杂凑算法采用其他算法时，应符合国家密码标准和行业标准的要求。

7.4.4 数字证书要求

用于 OFD 签名的数字证书要求如下：

a) 证书中使用的算法应采用国家密码管理主管部门核准的算法；
b) 使用基于 SM2 算法的证书时，应遵循 GB/T 20518；
c) 使用基于其他算法的证书时，应符合国家密码标准和行业标准的要求。

7.4.5 生成流程

OFD 完整性保护签名流程如下：

a) 确认文件包内的所有文件；
b) 组装签名完整性保护文件；
c) 根据签名方案，计算完整性保护文件的杂凑值；
d) 根据签名方案，使用版式文件合成者的签名私钥对杂凑值进行数字签名；
e) 将数字签名结果写入签名值文件。

7.4.6 校验流程

OFD 完整性保护验证签名流程如下：

a) 读取完整性保护描述文件；
b) 根据签名方案，调用杂凑算法计算完整性保护文件的杂凑值；
c) 读取签名值文件，进行签名验证。

附 录 A
（规范性）
密码保护方案标识及保护方法

A.1 密码保护方案标识

OFD密码应用要求的密码保护方案的标识见表A.1。

表A.1 密码保护方案标识

对象标识符	对象标识符定义	备注
加密方案标识符		
1.1.1	采用口令方式加密(国密)	对称算法SM4,CBC模式。 CBC模式的初始向量IV值放入附录C密钥描述文件内,填充算法遵循PKCS#7,分块长度为16字节(8位)
1.1.2	采用证书方式加密(国密)	对称算法SM4,CBC模式。非对称算法SM2。 CBC模式的初始向量IV值放入附录C密钥描述文件内,填充算法遵循PKCS#7,分块长度为16字节(8位)
1.1.3～1.1.255	保留	
签名方案标识符		
1.2.1	采用证书进行数字签名	签名应遵循GB/T 35275 信息安全技术 SM2密码算法加密签名消息语法规范
1.2.2～1.2.255	保留	

A.2 口令加密方案

A.2.1 加密方案

加密方法如下：

a) 调用密码服务模块,产生文件加密对称密钥；
b) 采用对称算法,使用文件加密对称密钥加密原文件；
c) 将口令通过密钥派生函数生成加密文件加密对称密钥的密钥,使用密钥派生函数时,应遵循GB/T 32918；
d) 采用对称算法,使用步骤b)中运算结果作为加密密钥,对文件加密对称密钥进行加密,生成文件对称加密的包装密钥放入密钥描述文件。

A.2.2 解密方案

加密方法如下：

a) 将口令通过密钥派生函数生成解密文件加密对称密钥的密钥,使用密钥派生函数时,应遵循GB/T 32918；

b) 采用对称算法，以步骤 a)中运算结果作为解密密钥，解密文件对称加密的包装密钥，生成文件加密对称密钥；

c) 采用对称算法，使用文件加密对称密钥解密文件，获取原文。

A.3 证书加密方案

A.3.1 加密方案

加密方法如下：

a) 调用密码服务模块，产生文件加密对称密钥；

b) 采用对称密码算法，使用文件加密对称密钥，对原文件进行加密；

c) 采用非对称密码算法，使用电子文件访问者的公钥，对文件加密对称密钥进行加密，生成文件对称加密的包装密钥放入密钥描述文件。

A.3.2 解密方案

解密方法如下：

a) 采用非对称密码算法，使用电子文件访问者的加密私钥，对文件对称加密的包装密钥进行解密获取文件加密对称密钥；

b) 采用对称密码算法，使用文件加密对称密钥，对文件进行解密，获取原文。

A.4 签名方案

A.4.1 签名方案

签名方案如下：

a) 采用杂凑算法，计算包内文件杂凑值生成待签名域 Signature.xml(见图 2)；

b) 采用签名算法，使用签名者签名私钥对签名域进行数字签名。

A.4.2 验证签名方案

验证签名方案如下：

a) 采用杂凑算法，计算包内文件杂凑值生成待签名域 Signature.xml(见图 2)；

b) 采用签名算法，使用签名者签名公钥验证签名。

附 录 B
（资料性）
OFD 签名描述扩展方案

B.1 扩展说明

GB/T 33190—2016 虽然提供了扩展(Extension)机制支持临时性的特性扩展，但对照本标准规定的密码应用需求，仍存在以下不足：

a) 未提供直接机制支持签名叠加的功能；

b) 未提供直接机制记录密码组件的个性信息；

c) 未提供直接机制记录签名行为的个性信息。

建议对 GB/T 33190—2016 的第 18 章分别做 B.2 和 B.3 所示的扩展。

B.2 签名列表

一个 OFD 文档可多次签名(实际应用时对应联合发文和多人签批等情况)。按照 GB/T 33190，各个签名的入口信息应保存在签名列表文件(Signatures.xml)中。添加签名时，如果允许在本次签名后继续添加签名，则签名列表文件不应被包含到本次签名文件(Signature.xml)的保护文件列表(References)中。签名入口文件的描述结构见图 B.1。

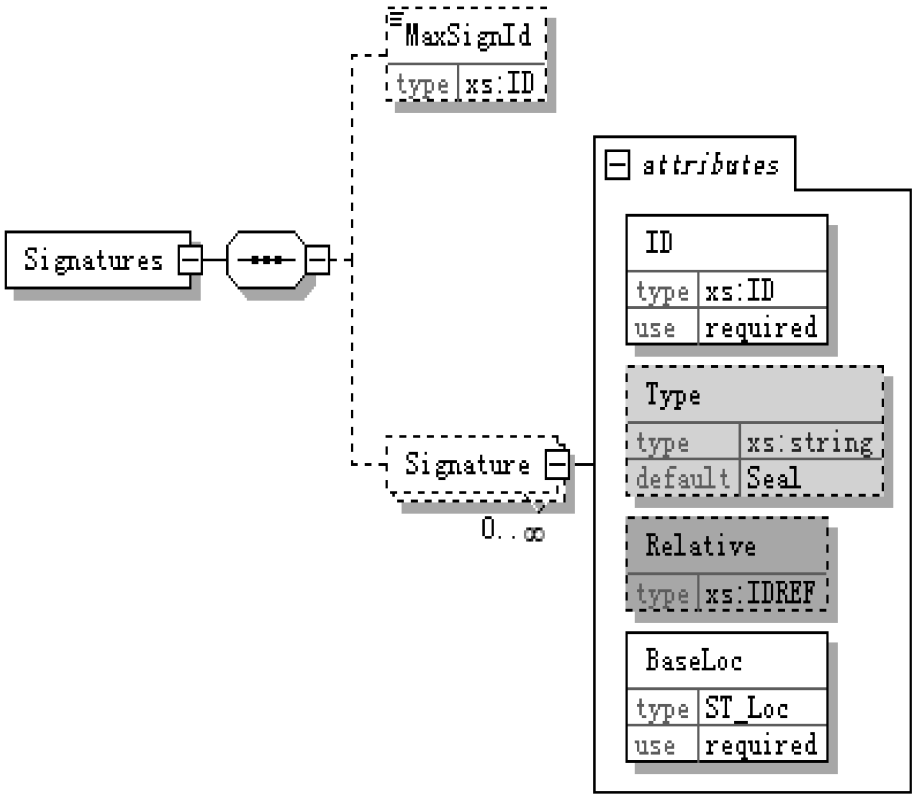

图 B.1 签名列表文件的描述结构

签名列表文件对应元素和属性说明见表 B.1。

表 B.1　签名列表文件元素和属性说明

名称	类型	说明	用法
Signatures		签名列表根结点	必选
-MaxSignId	xs:ID	安全标识的最大值，作用与文档入口文件 Document.xml 中的 MaxID 相同。 但未采用 ST_ID 类型，推荐使用“sNNN”的形式，NNN 从 1 开始	可选
-Signature		数字签名或安全签章在列表中的注册信息，一次签名或签章对应一个节点	可选
--ID	xs:ID	签名或签章的标识，应与指向文件中根节点标识一致	必选
--Type	xs:string	签名节点的类型	可选
--Relative	xs:IDREF	【2.0 版增加】 此签名基于的签名标识，一旦签名标注了该属性，则验证时应同时验证“基”签名	可选
--BaseLoc	ST_Loc	指向包内的签名描述文件	必选

B.3　签名文件

单个 OFD 数字签名信息采用 XML 文件描述，其数据结构如图 B.2 所示。

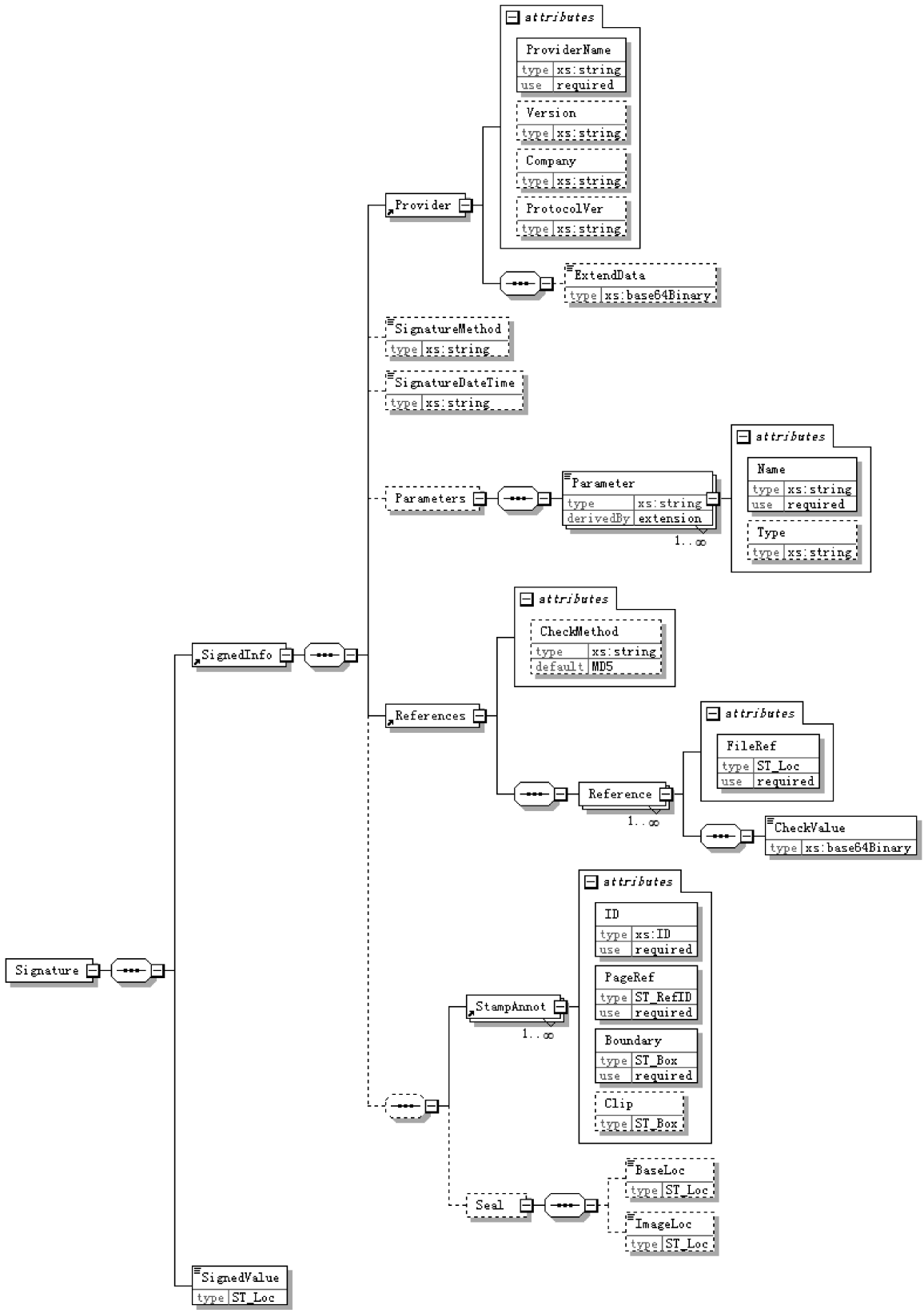

图 B.2　签名文件数据结构

签名描述文件的元素和属性说明见表 B.2。

表 B.2　签名文件元素和属性说明

名称	类型	说明	用法
Signature		签名描述文件的根节点	必选
-SignedInfo		签名信息，签名要保护的原文及本次签名相关的信息	必选
--Provider		记录本次签名的提供者信息	必选
---ProviderName	xs:string	创建签名时所用的签章组件的提供者	必选
---Company	xs:string	创建签名时所用的签章组件的制造商	可选
---Version	xs:string	创建签名时所用的签章组件的版本	可选
---ProtocolVer	xs:string	【2.0 版增加】 创建签名时所用的签章组件的接口协议版本	可选
---ExtendData	xs:base64Binary	【2.0 版增加】 创建签名时所用的签章组件的扩展信息	可选
--SignatureDateTime	xs:string	签名时间	必选
--SignatureMethod	xs:string	签名方案标识	必选
--Parameters		【2.0 版增加】 签名扩展属性集	可选
---Parameter	extend xs:string	【2.0 版增加】 签名扩展属性，记录一个属性的“键”(Name)和“值”，值在该节点的内容中记录	必选
----Name	xs:string	【2.0 版增加】 扩展属性的名称	必选
----Type	xs:string	【2.0 版增加】 扩展属性的值类型	可选
--References		本次签名所对应的保护文件列表	必选
---CheckMethod	xs:string	摘要方法，视应用场景的不同使用不同的摘要方法，用于各行业应用时，应使用符合该行业标准的算法	必选
---Reference		本次签名的摘要节点	必选
----FileRef	ST_Loc	本次签名文件路径	必选
----CheckValue	xs:base64Binary	对包内文件进行摘要计算，对所得的二进制摘要值进行 base64 编码所得结果	必选
--StampAnnot		签章关联的外观，如果一次签章存在多个外观(骑缝章)，该节点可出现多次	可选
---ID	xs:ID	签名或签章标识	必选
---PageRef	ST_RefID	引用外观注释所在的页面标识	必选
---Boundary	ST_Box	签章(完整)外观的外边框位置	必选

表 B.2（续）

名称	类型	说明	用法
---Clip	ST_Box	签章外观的裁剪设置	可选
--Seal		印章信息	可选
---BaseLoc	ST_Loc	印章数据存储位置	可选
---ImageLoc	ST_Box	【2.0 版增加】 印模图片存储位置	可选
-SignedValue	xs:string	存储数字签名文件对应的包内路径	必选

B.4 签名保护范围

GB/T 33190 允许对文档的不同内容分区进行签名保护，主要通过保护文件列表（References）中记录的包内文件来区分。

单次签名可保护的包内文件包括：

a） 主入口文件（OFD.xml）；

b） 文档根节点文件（主入口中 DocRoot 指向的文件，如 Document.xml）；

c） 文档描述文件（主入口中 DocInfo 指向的文件，以及文档根节点文件指向的文件，如公共资源列表文件 PublicRes.xml、大纲描述文件 Outline.xml、附件描述文件 Attachments.xml 等）；

d） 注释文件（从文档根节点文件派生的注释列表文件如 Annotations.xml 等及其引出的注释描述文件如 Annotation_N.xml）；

e） 内容文件（从文档根节点文件派生的页描述文件如 Content_N.xml 等及其引出的页资源列表文件如 PageRes.xml 等）；

f） 资源文件（各级资源列表文件中引出的字型 *.ttf、图像 *.jpg、音频、视频、矢量图像等文件）；

g） 已存在签名文件及签名值文件（Signature.xml 及 SignedValue.dat 等）；

h） 其他文档解析呈现必要的文件。

当次签名的签名文件和签名值文件均不应出现在保护文件列表中。

附 录 C
（资料性）
OFD 加密描述方案

C.1 总体说明

OFD 采用“xml＋zip”的格式架构，文档的呈现内容由 zip 包内的多个文件共同决定，这些文件的划分可以细分到图层和单次修改操作。基于这些特征，可根据需要对不同的包内文件进行加密，实现文档局部或整体加密的功能。

举例：如只对特定页（Page_N）的所有内容加密，则可将 Page_N 对应模板文件、页面内容文件和注释文件及其对应的资源文件列入待加密范围；如只对特定页面的注释内容进行加密，则可将该页的注释文件及资源文件列入待加密范围，该页对应模板文件和内容文件则维持不变。

包内文件加密后，原有的明文文件应删除或更换为非保密内容，并记录密文解密后的替换关系。在文件解密端（文档阅读器 OFD 阅读软件或其他文档处理程序）约定按照原有逻辑进行解析，并规约定一旦在替换关系中存在记录，解密端需使用密件解密后的内容取代对应明文。

在这种约定下，可以实现同一密件文档在不同的解密条件下呈现不同的内容。

C.2 密钥描述文件

密钥描述文件采用 XML 格式描述，存储了方案、算法和多人、多角色、多密码或证书等关键解密信息，其数据结构见图 C.1。

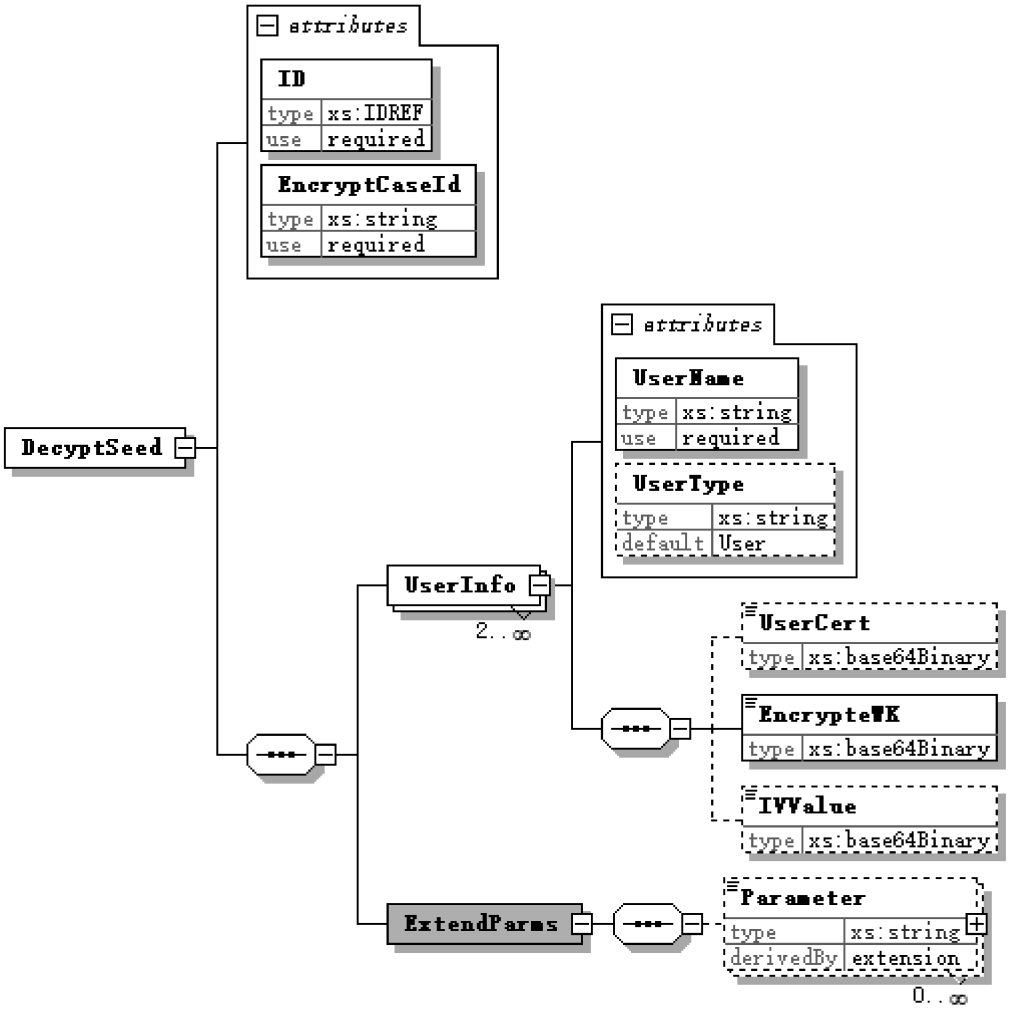

图 C.1　密钥描述文件数据结构

密钥描述文件的元素和属性说明见表 C.1。

表 C.1　密钥描述文件元素和属性说明

名称	类型	说明	用法
DecyptSeed		密钥描述文件的根节点	必选
-ID	xs:IDREF	加密操作标识，应与解密入口描述中的一致	必选
-EncryptCaseId	xs:string	加密保护方案标识，参见附录 A	必选
--UserInfo	xs:string	可解密该次操作的用户	必选
--UserName	xs:string	用户名称	必选
--UserType	xs:string	用户角色类型，当是文档管理员时取值为 Owner，普通用户是取值为 User，默认为 User	可选
--UserCert	xs:base64Binary	用户的加解密公钥证书，加密方案标识为 1.1.2 时必选	可选
--EncryptedWK	xs:base64Binary	文件对称加密的包装密钥	必选

表 C.1（续）

名称	类型	说明	用法
--IVValue	xs:base64Binary	初如化向量值，默认 16 个 0	可选
-ExtendParams	xs:string	扩展参数节点	必选
--Parameter	xs:string	扩展参数	可选
---Name	xs:string	扩展参数名称	必选
---Value	xs:string	扩展参数值	可选

根据加密类型的不同，文件对称加密的包装密钥的生成方式也不同。口令加密时，使用用户输入的口令作为基础，通过密钥派生函数派生出密钥，然后用该密钥对文件对称加密密钥进行加密，生成文件对称加密的包装密钥。使用密钥派生函数时，应遵循 GB/T 32918。证书加密时，使用用户的公钥证书对文件对称加密密钥进行非对称加密，生成文件对称加密的包装密钥。

C.3 解密入口

解密入口文件采用 XML 形式表示。文件以 Encryptions 为根节点，可包含多个加密信息（EncryptInfo）节点。每个加密信息节点的内容包含两部分，一部分为加密概要信息，另一部分为密钥描述文件和明密文映射表的位置，如图 C.2。

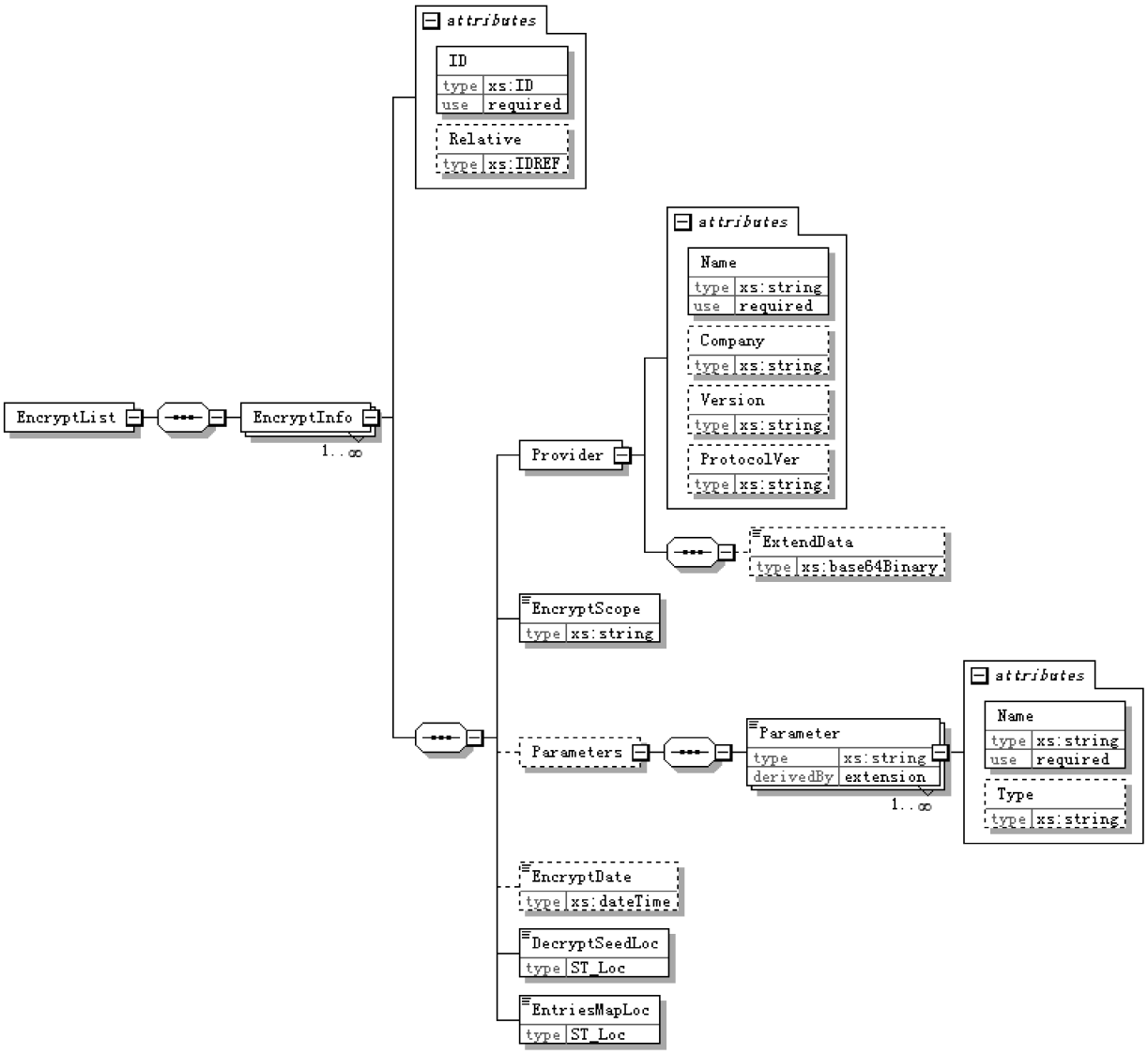

图 C.2　解密入口文件数据结构

OFD 文件可形成多重加密。多重加密时，图 C.2 中的 EncryptInfo 节点可出现多次，且前后两次加密可通过可选的 Relative 属性串联起来。

解密入口文件中元素和属性说明见表 C.2。

表 C.2　解密入口文件的元素和属性说明

名称	类型	说明	用法
Encryptions		解密入口根结点	必选
-EncryptInfo	CT_EncyptInfo	加密描述信息，多重加密形成多个加密操作记录	必选
--ID	xs:ID	加密操作标识	必选
--Relative	xs:IDREF	上一次加密操作标识	可选
-Provider		加解密组件的相关信息	必选
---Name	xs:string	加解密组件的名称	必选

表 C.2（续）

名称	类型	说明	用法
--Company	xs:string	加解密组件的公司名称	可选
---Version	xs:string	加解密组件的版本	必选
---ProtocolVer	xs:string	加解密组件的接口协议版本	可选
---ExtendData	xs:base64Binary	加解密组件的扩展信息	可选
--EncryptScope	xs:string	文档加密相关内容的描述(文档加密类型或范围)	必选
--EncryptDate	xs:dateTime	加密时间	可选
--Parameters		加密操作的附加描述集合	可选
---Parameter	xs:string	加密操作的附加描述(及其取值)	必选
----Name	xs:string	加密操作的附加描述项名称	必选
----Type	xs:string	加密操作的附加描述项取值类型	可选
--DecryptSeedLoc	ST_Loc	指向包内的二进制密钥描述文件,其中记录了解密所需的参数,例如密码算法标识、方案标识和其他参数等	必选
--EntriesMapLoc	ST_Loc	明密文映射表或其加密后的文件存储的路径	必选

解密输入文件的文件名固定为“Encryptions.xml”,应放置在 OFD 文件的根目录(与 OFD.xml 位置相同)。

C.4 明密映射表

未加密的明密文映射表文件的数据结构见图 C.3。

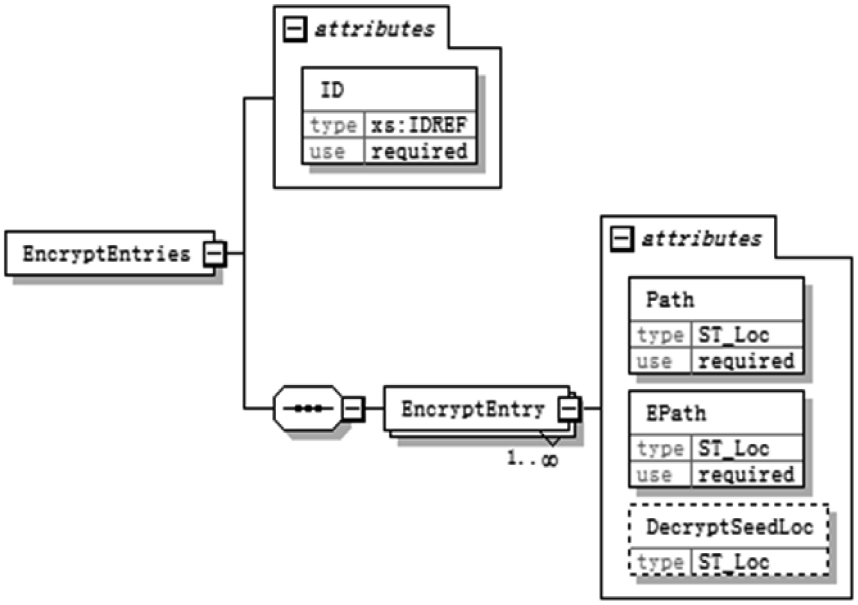

图 C.3 明密文映射表文件数据接口

未加密的明密文映射表文件中各元素及属性说明见表 C.3。

表 C.3　明密文映射表文件元素及属性说明

名称	类型	说明	用法
EncryptedEntries		根节点	必选
-ID	xs:ID	加密操作标识,应与解密入口描述中的一致	必选
-EncryptEntry		明密文对应关系	必选
--Path	ST_Loc	加密前包内文件的绝对路径	必选
--EPath	ST_Loc	加密后形成的包内密文的绝对路径	可选
--DecryptSeedLoc	ST_Loc	此项密文独有的密钥数据文件路径。 该属性不出现时,使用所属加密操作信息中定义的通用密钥数据	可选

加密后明密文对应文件的文件名建议为“entriesmap.dat”,根据入口文件进行寻址。

附 录 D
（资料性）
OFD 完整性保护方案

D.1 总体说明

OFD 是一个 ZIP 文件，从技术机制上可以包含各种文件。如果一个 OFD 文件包内的文件，其在按照“OFD.xml”“Encryptions.xml”及其衍生文件充分遍历后，仍未被任何其他文件引用，就属于“夹带文件”。夹带文件的存在对于 OFD 的安全性和完整性来说是一个威胁。应设计相应的机制支持快速检出夹带文件，保障 OFD 文件的完整性。

D.2 防夹带文件

为了支持防夹带机制，OFD 文件中需引入完整性保护描述文件，其数据结构如 D.1 所示。

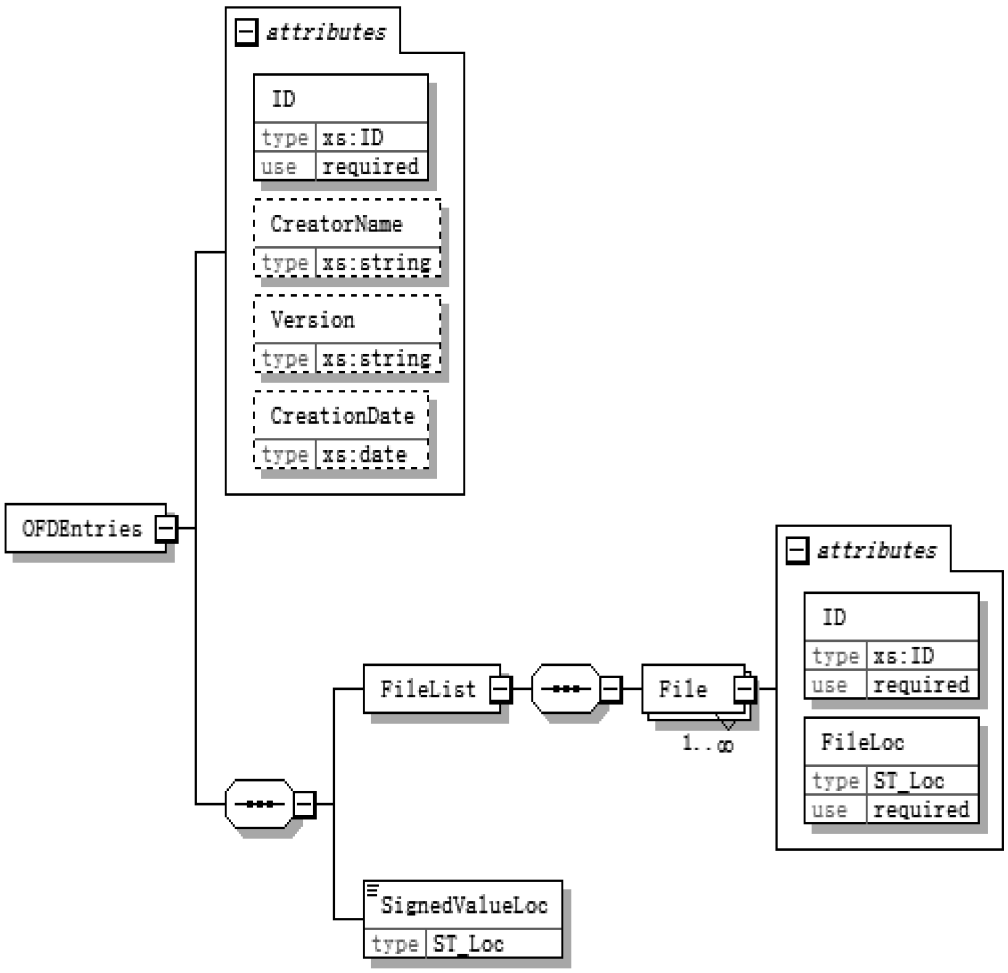

图 D.1 完整性保护描述文件数据结构

完整性保护描述文件中的元素及属性说明见表 D.1。

表 D.1　完整性保护描述文件元素和属性说明

名称	类型	说明	用法
DocEntries		根节点	必选
-ID	xs:ID	加密标识,应与解密入口描述中的一致	必选
-CreatorName	xs:string	明密文对应关系	可选
-Version	xs:string	加密前包内文件的绝对路径	可选
-CreationDate	xs:date	加密后形成的包内密文的绝对路径	可选
-FileList			必选
--File			必选
---ID	xs:ID	文件标识	必选
--FileLoc	ST_Loc	包内文件路径	必选
SignedValueLoc	ST_Loc	针对防夹带文件所在文件形成的签名值。 签名值应符合“GB/T 35275”标准	可选

放夹带文件的文件名固定为“OFDEntries.xml”,应放置在 OFD 文件的根目录(与 OFD.xml 位置相同)。

中华人民共和国密码
行业标准
开放式版式文档密码应用技术规范
GM/T 0099—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.75 字数 51 千字
2021年5月第一版 2021年5月第一次印刷
*
书号:155066·2-35849 定价 32.00 元

GM/T 0099-2020

码上扫一扫 正版服务到