

TC260-PG-202511A

网络安全标准实践指南

——人工智能生成合成内容标识方法 文件
元数据隐式标识 安全防护技术指南

(V1.0-202508)



全国网络安全标准化技术委员会秘书处

2025 年 08 月

本文档可从以下网址获得：

www.tc260.org.cn/



全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC



前 言

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

本文件起草单位：中国科学院软件研究所、中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、浙江大学、华为技术有限公司、中央网信办数据与技术保障中心、北京抖音信息服务有限公司、北京快手科技有限公司、北京金山办公软件股份有限公司、阿里云计算有限公司、荣耀终端股份有限公司、北京小米移动软件有限公司、维沃移动通信有限公司、OPPO 广东移动通信有限公司、北京智谱华章科技股份有限公司、深圳市隐拓智安科技有限公司、中电信人工智能科技（北京）有限公司、北京零一万物科技有限公司。

本文件主要起草人：张严、郝春亮、许晓耕、王志伟、秦湛、杨子祺、胡子元、安红云、张树玲、杨敏、张立尧、熊安、郭建领、杜蕾、落红卫、谷晨、嵇程、张震、孙勇、王寒生、吕飞霄、郑天航、孙培尧、杜鹏、何林涛、王杰、徐曼、李根、龙江源、乔文斌、万嗣芳、万世隆、王海棠。



声 明

本《实践指南》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。



全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC



摘 要

为落实《人工智能生成合成内容标识办法》，根据强制性国家标准GB 45438—2025《网络安全技术 人工智能生成合成内容标识方法》的要求，本文件提供了人工智能生成合成内容文件元数据隐式标识安全防护的相关技术和安全防护信息的参考格式，指导文件元数据隐式标识的添加方实现文件元数据隐式标识的安全防护。





目 录

1 范围	2
2 规范性引用文件	2
3 术语和定义	2
4 缩略语	3
5 概述	3
6 安全防护目标	3
7 安全防护机制	4
7.1 使用数字签名技术的安全防护机制	4
7.2 绑定机制	6
8 安全防护信息	7
8.1 通用格式	7
8.2 绑定信息	8
8.3 非公开可验证安全防护信息	9
8.4 公开可验证安全防护信息	10
8.5 扩展信息	13
附录 A （资料性） 安全防护信息生成与验证示例	14





1 范围

本文件给出了人工智能生成合成内容标识中文件元数据隐式标识安全防护的相关技术和安全防护信息的参考格式。

本文件适用于文件元数据隐式标识的添加方实现文件元数据隐式标识的安全防护。

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 1988 信息技术 信息交换用七位编码字符集

GB 45438—2025 网络安全技术 人工智能生成合成内容标识方法

GB/T 25069—2022 信息安全技术 术语

3 术语和定义

GB 1988、GB 45438—2025、GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1 添加方 labeling entity



在内容文件元数据中添加文件元数据隐式标识的实体。

注：添加方包括初始添加文件元数据隐式标识的实体，以及对已有文件元数据隐式标识的内容进行增加和修改的实体。

3.2 绑定 binding

实现文件元数据隐式标识与人工智能生成合成内容关联的机制。

注：绑定机制所需信息可位于内容中（例如：在内容中写入数字水印）或文件元数据隐式标识中（例如：在文件元数据隐式标识中记录内容的杂凑值）。

4 缩略语

下列缩略语适用于本文件。

OID：对象标识符（Object Identifier）

URI：统一资源标识符（Uniform Resource Identifier）

5 概述

标识安全防护主要是通过对标识数据和文件内容数据使用数字签名等安全技术生成安全防护信息，并记录于文件元数据隐式标识中，从而实现内容传播过程中，对标识的真实性、完整性以及标识与文件关联性的验证。

6 安全防护目标

本文件给出的安全防护技术主要覆盖以下安全防护目标：

a) 标识真实性：确保文件元数据隐式标识是由真实的添加方实体生成的，而非伪造或仿冒；



b) 标识完整性：确保文件元数据隐式标识信息没有被篡改，并为标识与文件内容的关联性提供验证信息，避免由于内容被替换或修改导致的文件元数据隐式标识信息与文件的关联失效。

除本实践指南列举的安全防护技术外，标识添加方还可根据自身安全需求额外使用其他安全防护技术与机制。

7 安全防护机制

7.1 使用数字签名技术的安全防护机制

7.1.1 通用机制

使用数字签名技术的标识安全防护机制如下：

a) 在添加标识前，标识添加方生成用于标识防护的签名密钥，并通过数字证书等方式实现公钥与自身身份的关联，私钥由添加方秘密持有并安全存储，公钥公开发布；

b) 在完成标识中除预留字段1和预留字段2以外的其他内容的添加后，标识添加方将标识数据、内容的杂凑值以及其他需实施完整性保护的信息作为待签名数据，使用私钥进行签名，然后将签名值与用于验证签名的其他信息（例如：公钥值、数字证书、算法标识等）作为安全防护信息同时写入标识中，待签名数据的选取方式见7.1.2；

c) 在内容传播过程中，获取内容的实体可以从元数据隐式标识记录的安全防护信息中获取数字签名以及验证数字签名所需的公钥、



证书等信息，并结合根信任证书等对公钥或证书进行验证，然后再验证内容数据和标识数据的签名。

7.1.2 待签名数据的选取

在计算数字签名时，按照如下方法选取待签名数据：

a) 实现标识自身保护的待签名数据选取GB 45438附录E中规定的元数据标识字段，如果签名方是内容提供者，待签名数据从"Label"开始，到"value3"结束。如果签名方是内容传播者，待签名数据从"Label"开始，到"value6"结束。将选取的数据采用GB 1988给出的编码，作为消息输入签名算法。待签名数据选取示例参见附录A.1；

b) 实现标识与文件关联的保护待签名数据根据文件的类型，选取文件中记录内容信息部分的数据或根据内容信息生成的绑定数据，作为消息输入签名算法，典型文件类型的内容数据选取示例参见附录A.2。

7.1.3 签名的计算

在确定待签名数据后，选择如下方式之一计算签名：

a) 对7.1.2 a)中选取的标识数据进行签名，该方式仅保护标识自身的完整性，不受内容变化的影响，无法直接实现对内容替换等风险的发现；

注：可通过签名中包含的内容唯一编号使用后台留存日志检索与标识相对应的内容，或结合内容隐式标识等技术实现签名与内容信息的绑定。



b) 分别对多个待签名数据进行签名，并同时记录于标识中，该方式可通过对每个签名值进行验证来确认相应数据的完整性；

c) 将多个待签名以比特串方式进行连接，然后对连接后的数据进行签名，该方式具有较高的效率，但当其中一部分数据发生变化时，会导致整个签名验证的失败。

7.2 绑定机制

7.2.1 使用密码学杂凑函数的绑定机制

使用密码学杂凑函数的绑定机制如下：

a) 在添加标识时，标识添加方使用密码学杂凑函数计算出文件内容的杂凑值，并将编码后的特征值作为标识安全防护信息的一部分进行记录；

b) 当进行标识验证时，验证方可以对当前的文件内容使用相同的杂凑算法计算杂凑值，并与记录在标识中的杂凑值进行比较，如果相同，则说明文件与标识的关联有效。

7.2.2 使用其他内容杂凑函数的绑定机制

如果标识添加方希望所生成的绑定信息在内容发生一定程度的变化时仍然能够保留可验证性，可考虑在使用密码学杂凑函数的基础上额外使用内容指纹等内容杂凑技术用于标识与内容的绑定。在使用内容指纹时，建议评估所采用的技术对内容被有意篡改风险的抵御能力。基本方式如下：



a) 在添加标识时，标识添加方使用内容杂凑算法计算出特征值，将编码后的特征值作为标识安全防护信息的一部分进行记录；

注：常见的内容杂凑技术包括ISCC数据描述符（详见ISO 24138）、SIFT图像描述符等。

b) 当进行标识验证时，验证方可以对当前的内容（可能经过了编码、压缩、格式转换、裁剪等处理）使用相同的杂凑算法计算特征值，并计算两次特征值的相似度，然后判定文件与标识的关联是否有效。

8 安全防护信息

8.1 通用格式

标识添加方使用GB 45438—2025附录E中规定的文件元数据隐式标识预留字段1和预留字段2作为记录安全防护信息的位置，记录安全防护信息的格式如下：

a) 使用标签为"SecurityData"的JSON对象来记录安全防护信息，在该数据对象中，使用b)至g)中定义的标签记录相应信息，其中"Type"和"Version"标签为必选，"Bindings"、"PrivSD"、"PubSD"、"Extension"标签为可选，在一份安全防护信息中，同名标签至多存在一个；

b) 使用"Type"标签来记录该安全防护信息遵循的规范，依据本文件产生的信息的标签值固定为"TC260PG"；

c) 使用"Version"标签来记录该安全防护信息遵循的规范版本，依据本文件产生的信息的标签值固定为1；



d) 使用标签为"Bindings"的数组对象来记录内容绑定信息，例如：内容的密码学杂凑值、内容指纹信息等，相关说明见8.2；

e) 使用标签为"PrivSD"的数组对象来记录非公开可验证的安全防护信息，例如：秘密特征码或使用对称密码算法加密的信息，相关说明见8.3；

f) 使用标签为"PubSD"的数组对象来记录公开可验证的安全防护信息，例如：数字签名、公钥和证书等，相关说明见8.4；

g) 使用标签为"Extension"的数组对象来记录其他扩展信息，相关说明见8.5；

h) 避免使用本文件已使用的字段用于实现其他功能，以防止解析时产生歧义。

在完成所有安全防护信息的字段填写并生成标签为"SecurityData"的JSON对象后，将JSON对象转化为符合GB 45438—2025 附录E要求的字符串，根据添加方的类型（内容生成方或传播方），记录在文件元数据隐式标识的预留字段1或预留字段2中。安全防护信息记录示例参见附录A.3。

8.2 绑定信息

绑定信息记录于标签为"Bindings"的数组中，数组中的每一个实体用于记录一个特定类型的绑定信息，"Bindings"实体中可以包含多个不同类型的绑定信息。

对于数组中的每一个实体，需包含以下信息：



a) 类型 (Type): 指明绑定的类型, 对于使用密码学杂凑函数的绑定方法, 使用"Type":"Hash", 对于使用内容指纹的绑定方法, 使用"Type":"Soft";

b) 绑定信息标识 (ID): 当"Bindings"数组中存在多个绑定信息时, 每个实体需包含本字段, 用于索引;

c) 算法标识 (AlgID): 指明使用的绑定方案算法, 当使用密码学杂凑函数时, 使用杂凑算法的OID值, 例如: 对于使用SM3杂凑函数的绑定方法, 使用"AlgID":"1.2.156.10197.1.401";

d) 值 (Value): 使用算法标识所指明的算法对文件内容数据进行运算和编码后生成的绑定信息, 采用十六进制字符编码;

e) 参数 (Params): 应记录杂凑算法所使用的参数, 对于使用SM3杂凑函数的绑定方法, 不使用此字段或字段值为"null";

f) 内容数据选取 (CntSel): 当使用密码学杂凑函数时, 指明内容数据的选取方式, 本文件建议的选取方式及对应的标签值见附录A.2。

8.3 非公开可验证安全防护信息

非公开可验证的安全防护信息记录于标签为"PrivSD"的数组中, 数组中的每一个实体用于记录一个特定类型的验证信息, "PrivSD"数组中可以包含多个不同类型的验证信息, 对于数组中的每个实体, 需包含以下信息:

a) 类型 (Type): 指明安全防护信息的类型, 使得标识添加方能通过该字段的值确定使用该信息进行验证的方法;



- b) 值 (Value): 具体的安全防护信息, 由内容生成方自行使用;
- c) 其他信息 (VerifyInfo): 其他需在标识中记录的, 用于支持验证的信息, 例如: 验证接口的地址。

8.4 公开可验证安全防护信息

8.4.1 通用信息

公开可验证的安全防护信息记录于标签为"PubSD"的数组中, 数组中的每一个实体用于记录一个特定类型的验证信息, "PubSD"数组中可以包含多个不同类型的验证信息, 对于数组中的每个实体, 需包含以下信息:

类型 (Type): 指明安全防护信息的类型, 使得内容生成方能通过该字段的值确定使用该信息进行验证的方法, 签名信息使用"Type":"DS", 公开密钥信息使用"Type":"PubKey", 外部验证链接信息使用"Type":"ExLink"。

8.4.2 数字签名信息

记录数字签名信息的"PubSD"实体中需包含以下信息:

- a) 类型 (Type): 使用"Type":"DS";
- b) 算法标识 (AlgID): 使用签名算法的OID值, 例如: 对于使用SM3withSM2签名算法的签名, 使用"AlgID":"1.2.156.10197.1.501";
- c) 参数 (Params): 签名算法所使用的其他参数, 对于SM3withSM2签名算法, 不使用此字段或字段值为"null";



d) 待签名数据 (TBSData): 用于确定待签名数据的信息, 需包含以下信息:

1) 类型 (Type): 待签名数据类型使用的值见表1;

2) 当Type的值为Md时, 使用7.1.2 a)中的方法确定待签名数据; 值为Cnt时, 需额外包含一个"CntSel"标签, 用于指明内容数据的选取方式, 详见A.2; 值为Bnd时, 需额外包含一个"ID"标签, 用于指明待签名的绑定数据的标识, 待签名数据为相应"Binding"实体的全部内容。

表1 待签名数据类型

类型	值	描述
内容	Cnt	以内容数据作为签名消息时, 使用本类型。
绑定信息	Bnd	以内容的绑定信息作为签名消息时, 使用本类型。
元数据	Md	以元数据作为签名消息时, 使用本类型。
其他信息	Etc	使用其他方法生成签名消息时, 使用本类型。



e) 密钥标识 (KeyID): 用于指定签名所使用密钥的标识, 与公开密钥信息中所确定的一个密钥信息实体的标识的值相同, 当不包含此字段时, 使用标识为0的密钥;

f) 签名值 (Signature): 使用算法标识指定的签名算法和密钥标识指定的密钥, 对待签名数据进行签名得到的值, 采用十六进制字符编码, 对于SM3withSM2签名算法, 编码后的结果为128个字符;

g) 签名时间 (Time): 生成签名的时间信息, 可使用YYYYMMDDHHMMSSZ格式的时间或经过签名的可信时间戳的编码, 时间戳的数据格式参见GB/T 20520。

8.4.3 公开密钥信息

当使用数字签名作为安全防护信息时, 记录公开密钥信息的"PubSD"实体中需包含以下信息:

- a) 类型 (Type): 使用"Type":"PubKey";
- b) 算法标识 (AlgID): 使用签名算法的OID值, 例如: 对于SM3withSM2签名算法的密钥, 使用"AlgID":"1.2.156.10197.1.501";
- c) 密钥标识 (KeyID): 本密钥的标识, 使用整数, 当不包含此字段时, 默认标识为0, 信息生成方需确保同一个"PubSD"实体中不包含多个标识相同的密钥, 在进行签名验证时, 对于标识相同的密钥, 除第一个外应被忽略;
- d) 密钥 (KeyValue): 密钥的值, 使用十六进制字符编码;



e) 证书 (Certificate): 用于实现密钥与身份绑定的证书信息, 当使用GB/T 20518中规定的X.509证书时, 使用该证书DER编码的BASE64编码值;

f) 其他验证信息 (VerifyInfo): 用于实现密钥与身份绑定的, 除数字证书以外的其他信息, 例如: 添加方可以将公开发布密钥或证书信息的url记录在此字段中。

8.4.4 外部公开验证信息

当使用外部公开可验证信息作为安全防护信息时, 相应的"PubSD"实体中需包含以下信息:

- a) 类型 (Type): 使用"Type":"ExLink";
- b) 值 (Value): 获取外部公开可验证信息的URI链接。

8.5 扩展信息

保留"Extensions"标签作为扩展信息记录, 本文件不给出扩展信息的具体用法。



附录 A

(资料性)

安全防护信息生成与验证示例

A. 1. 标识信息安全防护数据选取

本节给出一个使用数字签名对标识信息进行安全防护时待签名数据选取的示例：

a) 生成合成内容服务提供者依据GB 45438—2025附录E的格式生成包含如下内容的标识：

——value1的取值为1（该内容属于生成合成内容）；

——value2的取值为001091350100M000100Y4300000（生成合成内容服务提供者的编码）；

——value3的取值为pid20250101v123456（内容唯一编号）；

b) 根据7.2.3.1 a)中的规则，待签名数据为以下字符串经GB 1988给出的编码方法编码后得到的数据：

"Label": "1" ,

"ContentProducer": "001091350100M000100Y4300000" ,

"ProduceID": "pid20250101v123456"

A. 2. 内容信息安全防护数据选取



本节给出典型文件格式的内容进行签名或计算杂凑时数据选取的建议方案，以及使用相应方案时CntSel标签的值。

——对于JPEG类型的图片文件，建议选取从SOS标志开始至EOI标志前的全部数据，作为内容数据，该数据以0xFFDA为起始。详见IEC T.81。采用本方式选取的内容数据，CntSel标签的值设为“JPEG”。

——对于PNG类型的图片文件，建议选取IDAT块中包含的数据。采用本方式选取的内容数据，CntSel标签的值设为“PNG”。

——对于其他类型的文件，建议选取文件中除GB 45438—2025附录E中规定的文件元数据隐式标识以外的所有字节作为内容数据。采用本方式选取的内容数据，CntSel标签的值设为“DFT”。

A. 3. 安全防护信息记录示例

本节给出了一个采用8中记录格式对安全防护信息记录的示例。为便于阅读，增加了换行与缩进：

```
{  
  "SecurityData": {  
    "Type": "TC260PG",  
    "Version": 1,  
    "Bindings": [  
      {  
        "Type": "Hash",  
        "ID": "1",
```



```
"AlgID": "1.2.156.10197.1.401",  
  
"CntSel": "JPEG",  
  
"Value": "AC17BE26BC39BA26AC17B126AC17B526"  
  
},  
  
{  
  
  "Type": "Soft",  
  
  "ID": "2",  
  
  "Alg": "ISO24138",  
  
  "Value": "EAASS3POFKW7KDJ"  
  
}  
  
],  
  
"PrivSD": [  
  
  {  
  
    "Type": "SomeAppDefault",  
  
    "Value": "56A6CC3E144DA84"  
  
  }  
  
],  
  
"PubSD": [  
  
  {  
  
    "Type": "DS",  
  
    "AlgID": "1.2.156.10197.1.501",
```



```
"TBSDData": [  
    {"Type": "Bnd", "ID": "1"},  
    {"Type": "Md"}  
],  
"Signature":  
"AC17BE26AC17BE26AC17BE26AC17BE26AC17BE26AC17BE26  
AC17BE26AC17BE26AC17BE26AC17BE26AC17BE26AC17BE26A  
C17BE26AC17BE26AC17BE26AC17BE26"  
},  
{  
    "Type": "PubKey",  
    "AlgID": "1.2.156.10197.1.501",  
    "KeyValue":  
"AC17BE26AC17BE26AC17BE26AC17BE26AC17BE26AC17BE26  
AC17BE26AC17BE26AC17BE26AC17BE26AC17BE26AC17BE26A  
C17BE26AC17BE26AC17BE26AC17BE26"  
}  
]  
}  
}
```