

# 团 体 标 准

T/WAPIA 035.3—2020/ISO/IEC 9798-3:2019  
代替T/WAPIA 035—2016

## 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

IT security techniques—Entity authentication—Part 3: Mechanisms  
using digital signature techniques

(ISO/IEC 9798-3:2019, IDT)

2020-12-09 发布

2020-12-09 实施

中关村无线网络安全产业联盟发布

## 目 次

版权声明 .....	II
前言 .....	III
引言 .....	IV
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 符号与缩略语 .....	2
4.1 符号 .....	2
4.2 缩略语 .....	3
5 概述 .....	3
5.1 时变参数 .....	3
5.2 权标 .....	3
5.3 Text 字段的用法 .....	3
6 要求 .....	3
7 不引入在线可信第三方的机制 .....	4
7.1 单向鉴别 .....	4
7.2 双向鉴别 .....	5
8 引入在线可信第三方的机制 .....	9
8.1 概述 .....	9
8.2 单向鉴别 .....	9
8.3 双向鉴别 .....	11
附录 A（规范性） .....	17
A.1 形式定义 .....	17
A.2 后续客体标识符的使用 .....	17
附录 B（资料性） .....	18
B.1 安全属性 .....	18
B.2 机制的比较和选择 .....	18
附录 C（资料性） .....	20
参考文献 .....	21

## 版权声明

本文件版权归WAPI产业联盟（中关村无线网络安全产业联盟）©所有。

本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

联系WAPI产业联盟标准化部（lmbz@wapia.org）可获取本文件授权相关信息。

**WAPI Alliance**  
产 | 业 | 联 | 盟

©WAPIA产业联盟（中关村无线网络安全产业联盟）版权所有。