中国电池ID
China Battery ID

数字身份设计概要 V1.0

China BatteryID Solution Schema-Corporate Digital Identity V1.0

汽车工业节能与绿色发展评价中心
Energy-saving and Green-development Assessment Center for Automobile Industrial

CNTARC 中汽中心 | 数据
中 汽 数 据 有 限 公 司

一、背景

众所周知，随着数字化转型的不断深入，互联网与实体经济的加速融合，数字经济时代已悄然来临。2023 年 2 月，由中共中央、国务院印发的《数字中国建设整体布局规划》明确指出，建设数字中国是构筑国家竞争新优势的有力支持，而数字信任成为了构建可靠、安全、高效数字生态系统的关键要素。其中，数字身份作为实体进入到数字空间的第一道闸口，既是构建数字信任架构的前提，也是实体在数字空间内进行数据交互等各项活动的信任支撑。

国际标准化组织 ISO 将身份定义为一组与实体关联的属性。基于身份可被赋予不同的权力和义务。因此，身份既是一种标识，也是一种共识。在物理世界中，身份证可以看作是身份的象征，它不仅是公民身份的证明，也是公民合法合规参与各项社会活动的重要工具。在数字空间中，为参与各种数字化活动，也需拥有一个在线身份，来实现物理世界到数字世界的映射。这个在线身份，即为数字身份，它将真实身份信息浓缩为数字标识代码，任一实体对应唯一标识，并关联特定数字属性，来开展相关数字活动。

二、基于标识的密码系统概述

基于标识的密码系统（Identity-Based Cryptography，简称 IBC）的概念最初由 Shamir 在 1984 年提出，其核心思想是系统中不需要证书，使用用户的标识作为公钥。直到 2000 年以后，D. Boneh 和 M. Franklin 以及 R. Sakai、K. Ohgishi 和 M. Kasahara 两个团队独立提出用椭圆曲线配对构造标识公钥密码，引发了标识密码的新发展。

IBC 是一种非对称的公钥密码体系，是在基于传统的公钥基础设施基础（Public Key Infrastructure， 简称 PKI）上发展而来，主要简化了大量数字证书的交换问题，使安全应用更加易于部署和使用。与传统的公钥密码体系（如 RSA 和 ECC）不同，IBC 系统中的公钥是用户的身份标识，例如姓名、IP 地址、电子邮箱地址、手机号码等。用户的私钥由密钥生成中心（Key Generate Center, 简称 KGC）根据系统主密钥和用户标识计算得出，而公钥则由用户标识唯一确定，从而用户不需要第三方来保证公钥的真实性。

IBC 包括基于标识的加密算法 IBE（Identity-Based Encryption）和基于标识的签名算法 IBS(Identity-Based Signature) 以及基于标识的密钥协商算法

IBKA(Identity-Based Key Agreement)。这些算法可以用于数据加密、数字签名、数据完整性机制、数字信封、用户识别、用户认证等多种安全需求。IBC 具有以下技术特点：

- 无需证书：IBC 系统中，用户的标识直接作为公钥，省去了数字证书的颁发和验证过程，降低了系统的复杂性和成本。
- 易于管理：由于不需要证书，IBC 系统简化了密钥管理过程，减少了管理证书和密钥基础设施的复杂性和成本。
- 安全性：IBC 系统的安全性依赖于椭圆曲线离散对数问题的困难性，目前尚未出现针对椭圆曲线密码的有效破解方法。

三、SM9 算法概述

国密 SM9 加密算法是一种基于椭圆曲线密码学（ECC）的公钥密码体制，由中国密码学家于 2016 年提出，它是一种 IBC 算法。该算法旨在提供高效、安全的数字签名、密钥协商和加密服务，因此广泛应用于数字身份识别、电子认证等信息安全领域。SM9 算法自提出以来，已发布了以下标准：

- 国家标准《信息安全技术 SM9 标识密码算法 第 1 部分：总则》（GB/T 38635.1-2020）：这项标准由全国网络安全标准化技术委员会归口，主管部门为国家标准委。该标准发布于 2020 年 4 月 28 日，并从 2020 年 11 月 1 日起实施。
- 国家标准《信息安全技术 SM9 标识密码算法 第 2 部分：算法》（GB/T 38635.2-2020）：与第一部分一同发布，代表 SM9 算法正式成为国家标准。
- 国际标准 ISO/IEC 11770-3：《信息安全密钥管理 第 3 部分：使用非对称技术的机制》：SM9 密钥协商协议作为该国际标准 2021 版的一部分正式发布。
- 国际标准 ISO/IEC 18033-5:2015/AMD1:2021《信息技术安全技术 加密算法 第 5 部分:基于标识的密码补篇 1:SM9》：SM9 标识加密算法作为国际标准发布，这是继 SM9 数字签名算法成为 ISO/IEC 国际标准后发布的第二项 SM9 算法标准。
- 密码行业标准 GM/T 0080-2020《SM9 密码算法使用规范》：该标准于 2020 年 12 月 28 日发布，并于 2021 年 7 月 1 日实施，由国家密码管理局发布。

请联系service@batteryid.com.cn

获取《数字身份设计概要 V1.0》全文