ICS 35.040
CCS L 80

中华人民共和国密码行业标准

GM/T 0087—2020

浏览器密码应用接口规范

Browser cryptography API specification

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：北京海泰方圆科技股份有限公司、无锡江南信息安全工程技术中心、格尔软件股份有限公司、成都卫士通信息产业股份有限公司、吉大正元信息技术股份有限公司。

本文件主要起草人：柳增寿、蒋红宇、徐明翼、郑强、罗俊、赵丽丽。

浏览器密码应用接口规范

1 范围

本文件定义了浏览器执行网页中的密码操作的 JavaScript API，包括加密、解密、杂凑、签名、签名验证和随机数生成等操作。

本文件定义的 API 适用于浏览器中用户或服务的认证、文档或代码的签名、通信的机密性与完整性保证等。

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 32918（所有部分） 信息安全技术 SM2 椭圆曲线公钥密码算法

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

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

字典

一种使用键-值对作为元素的集合。

3.1.2

承诺

一种 JavaScript 范式，承诺（promise）代表一个任务结果。通过本范式可以实现浏览器脚本程序的异步功能。

3.2 缩略语

下列缩略语适用于本文件。

IDL 接口描述语言（Interface Description Language）

4 概述

本文件用于为网络应用中浏览器 JavaScript 脚本提供密码操作能力。网络应用可以让用户利用浏览器内置密码能力在浏览器端来保护其身份数据和隐私数据。直接使用 JavaScript 实现密码功能的方式会导致安全缺陷和性能问题。因此有必要在浏览器上原生实现密码功能，并向 JavaScript 程序提供