

# 公示材料

一、基本信息			
项目名称	中文	认证认可检验检测电子证书（报告）数字签名与在线验证及其平台建设研究	
	英文	Research on Digital Signature and Online Verification of Certification and Accreditation Inspection and Testing Electronic Certificate （ Report ） and Its Platform Establishment	
成果申报等级		<input checked="" type="checkbox"/> 一等奖 <input type="checkbox"/> 二等奖 <input type="checkbox"/> 三等奖	<input checked="" type="checkbox"/> 是否同意调级
主要完成人		周希昱、谭敏清、杨立远、冯洁、赵殷瑶、方洪海、张竑钧、侯建军	
主要完成单位		国家市场监督管理总局信息中心	
推荐单位(盖章)		国家市场监督管理总局信息中心	
奖项的主要项目来源		<input type="checkbox"/> 国家级 <input checked="" type="checkbox"/> 省部级 <input type="checkbox"/> 其他	
具体计划、基金的名称和编号：原国家认监委认证认可科技支撑计划项目（项目编号：2017RJWKJ09）			
成果的主要项目起止时间		起始： 2017-5	完成：2019-7
组织验收/鉴定单位		市场监管总局认可检测司	
成果登记号		G-2020-122	成果登记 时间    2020 年 12 月 31 日

## 二、奖项简介

本奖项对数字签名技术与认证认可检验检测电子证书（报告）的验证开展联合研究，完成了使用国际 RSA 和国密 SM2 两种算法实现双签双验的数字签名及验证技术的开发，提出电子证书（报告）在线验证平台技术方案并完成平台建设开发。

**主要技术内容：**基于检验检测认证机构所持有的 CA 证书，对 RSA 及 SM2 两种数字签名及验证算法、PDF 文件数字签名相关机制进行研究，开发对 PDF 格式认证认可检验检测电子证书（报告）使用 RSA 和 SM2 两种算法实现双签双验的数字签名及验证技术，提出在线验证平台技术方案与技术规范，建立认证认可检验检测电子证书（报告）数字签名与在线验证平台。

**技术指标：**1. 编制《认证认可检验检测电子证书（报告）数字签名在线验证平台技术方案》。2. 形成认证认可检验检测电子证书（报告）数字签名与在线验证技术规范草案。3. 建设“认证认可检验检测电子证书（报告）数字签名与在线验证平台”（<http://yz.cnca.cn/ver-ep/ve/v/pdfveri.jsp>）。

**主要创新点：**对 RSA 及 SM2 两种数字签名及验证算法进行研究，基于现行通用的 PDF 文档格式，开发了对同一份 PDF 文档实现 RSA 与 SM2 两种算法双签双验的技术（这是一个重大的技术应用创新），建立验证平台对认证认可检验检测电子证书（报告）进行数字签名在线验证，能够确认文档是否有数字签名、数字签名时间、文档签发者、签名时数字证书是否处于有效期及文档在流转过程中是否被篡改。

**授权知识产权情况：**本奖项成果共获得“检验检测认证证书与报告数字签名在线验证平台”等计算机软件著作权 5 项。

**取得的经济效益和社会效益：**本奖项成果独立于检验检测认证机构、企业与消费者，能够通过技术手段以客观、公正的方式，为各检验检测认证机构提供认证认可检验检测电子证书（报告）数字签名及作废服务，为企业和消费者提供认证认可检验检测电子证书（报告）验证服务，为行业主管部门提供针对电子证书（报告）进行监管的技术支撑手段，不断增强认证认可检验检测电子证书（报告）的采信能力。目前，已逐步推广到 300 多家检验检测认证机构使用，共接入 18 家 CA 机构，验证及作废文档共 1187134 份次。如果全国所有的检验检测认证证书（报告）都改为数字签名的电子文档，每年将可为认证认可检验检测机构节约书面报告印制、快递、保管等方面的成本支出约 68.4 亿元。

**推动市场监管技术进步情况：**平台的推广应用，极大地促进了认证认可检验检测电子证书（报告）的广泛使用，为支撑市场监管执法与根除“假证”发挥了积极的作用，为促进检验检测认证行业健康有序发展贡献了积极力量。