GM/Y 5013-2024

电子合同服务平台密码应用技术研究

密码行业标准化技术委员会
CRYPTOGRAPHY STANDARDIZATION TECHNICAL COMMITTEE

2024 年 12 月

摘 要

信息安全是国家安全的关键环节，为降低敏感信息泄露和信息系统遭受攻击的风险，本项目通过对国内电子合同服务平台的调研，分析国内主流电子合同平台的功能和密码技术使用情况，重点研究电子合同服务平台的技术框架，从电子合同面临的问题、平台功能架构、业务流程等层面分析信息安全需求与挑战；针对电子合同服务平台现有密码技术应用情况以及电子合同相关标准、密码行业标准，本研究报告从业务角度、安全角度、部署角度对电子合同中的密码技术框架进行了梳理和分析，并提出了相应的技术路线和标准化建议，为构建安全可靠的电子合同服务平台提供指引。

关键词：电子合同，数字签名，时间戳

目 录

摘 要..... I
目 录..... II
前 言..... IV
电子合同服务平台密码应用技术研究..... 1
1.概述..... 1
1.1 背景..... 1
1.1.1 政策背景..... 1
1.1.2 技术背景..... 1
1.1.3 必要性..... 2
1.2 研究目标..... 3
2.研究范围..... 4
2.1 电子合同服务平台的内涵..... 4
2.2 电子合同与智能合约的区别..... 4
2.3 电子合同与电子保单的关系..... 5
2.4 电子合同服务平台的应用外延..... 5
3.电子合同服务平台发展现状..... 6
3.1 国外电子合同服务平台现状..... 6
3.1.1 市场状况描述..... 6
3.1.2 国内外电子合同应用的差异..... 6
3.1.3 小结..... 7
3.2 国内电子合同服务平台现状..... 7
3.2.1 市场状况调研..... 7
3.2.2 应用情况调研..... 8
3.2.3 技术情况调研..... 11
3.2.4 主要的电子合同产品和平台..... 11
4. 法律法规和标准化现状..... 17
4.1 国外法律法规/标准化组织的相关研究..... 17
4.1.1 法律法规..... 17
4.1.2ISO/IEC 相关标准..... 18
4.1.3 美国国家标准化研究院（NIST）相关标准..... 19
4.1.4 欧洲电信标准化协会（ETSI）相关标准..... 19
4.2 国内法律法规/标准化组织的相关研究..... 20
4.2.1 电子合同服务平台建设层面..... 20
4.2.2 服务平台使用的密码技术层面..... 23
4.2.3 小结..... 25
4.3 发展趋势..... 25
5.密码应用技术研究..... 26
5.1 需求分析..... 26
5.1.1 电子合同面临的问题..... 26
5.1.2 电子合同服务平台的基本框架..... 28

5.1.3 密码技术需求 29
5.2 电子合同服务平台密码技术框架 32
5.2.1 技术框架-业务角度 32
5.2.2 技术框架-安全角度 33
5.2.3 技术框架-部署角度 35
5.2.4 小结 36
5.3 电子合同服务平台密码应用技术实现 37
5.3.1 业务流程的技术路线 37
5.3.2 电子合同常用的密码技术 40
5.3.3 主要研究的密码技术 44
5.3.4 其他关键技术研究 53
6.标准化研究 55
6.1 标准体系 55
6.2 标准化建议 55
6.2.1 标准化的目的 55
6.2.2 标准化思路 55
6.3 其他标准建议 58
7.总结 59
参考文献 60

前 言

本项目属于密标委标准体系中的“密码应用类标准”，通过综合运用现有的密码基础类标准（如 SM 系列密码算法）、密码设备类标准（如密码机、智能密码钥匙等）、基础设施类标准（如证书认证系统等），满足信息安全与管理的需求与技术挑战。

对于密标委正在制定的《基于云的电子签名服务技术要求》，本项目与该规范为相辅相成的关系，在电子合同服务平台中允许使用云签名技术，也可能形成完全融合的一体化建设方案。

本项目起草单位：数安时代科技股份有限公司（简称：GDCA，原广东数字证书认证中心有限公司）、北京信安世纪科技股份有限公司、暨南大学、北京数字认证股份有限公司、飞天诚信科技股份有限公司、江西金格科技股份有限公司、格尔软件股份有限公司、信睿吉科技（北京）有限公司、亚数信息科技（上海）有限公司、吉大正元信息技术股份有限公司、三未信安科技股份有限公司。

本项目主要起草人：周蔚林、汪宗斌、谭武征、张永强、朱鹏飞、刘磊、李兴勤、易其朋、陈满祥、魏一才、田景成、高志权、牛海超、赵丽丽、吴林枫、杜志强、黄金波、修磊、王春兰、肖强、沈传案。

电子合同服务平台密码应用技术研究

1.概述

1.1 背景

1.1.1 政策背景

随着互联网技术的快速发展，我国企业信息化推进步入深水区，无论互联网企业还是传统企业都基本实现了数字化办公，传统的纸质合同因成本高，效率低，已然成为企业现阶段数字化办公的掣肘之一，越来越多的企业选择电子合同。电子合同本质上仍属于合同的范畴，只是区别于传统的签约形式和文件载体。电子合同与纸质合同一样属于书面形式的合同，受法律承认和保护。《中华人民共和国合同法》（简称“《合同法》”）第十条和第十一条明确规定，当事人订立合同，有书面形式、口头形式和其他形式；书面形式是指合同书、信件和数据电文（包括电报、电传、传真、电子数据交换和电子邮件）等可以有形地表现所载内容的形式。在 2018 年 8 月颁布的《中华人民共和国电子商务法》第四十八条规定，电子商务当事人使用自动信息系统订立或者履行合同的行为对使用该系统的当事人具有法律效力。《中华人民共和国电子签名法》（简称“《电子签名法》”）第十四条规定：“可靠的电子签名与手写签名或者盖章具有同等的法律效力”，认可了可靠电子签名的合法效力；《最高人民法院关于适用（中华人民共和国民事诉讼法）的解释》认可了电子数据作为法定证据种类的合法地位；2020 年 1 月 1 日起正式施行的《中华人民共和国密码法》，标志着我国在密码的应用和管理等方面有了专门性的法律保障，大力推进了电子签名、电子合同的发展。此外，国家还颁布了《中华人民共和国民法典》、《电子商务协议》、《电子商务第三方交易平台服务规范》、《网络商品交易及有关服务行为管理暂行办法》等相关法律法规，为电子合同的法律效力提供保障。

2015 年 2 月国家商用密码管理办公室发布公告称：根据要求，全国第三方电子认证服务机构针对电子认证服务系统和密钥管理系统公钥算法的升级改造完毕，已经全面支持 SM 系列密码算法，同时各电子认证服务机构正在积极推动 SM 系列密码算法的应用服务改造，淘汰有安全风险以及低强度的密码算法和产品。虽然在 SSL VPN、数字证书认证系统、密钥管理系统、金融数据加密机、签名验签服务器、智能密码钥匙、智能 IC 卡、PCI 密码卡等产品上改造完毕，但是目前的信息系统整体架构中还有操作系统、数据库、中间件、浏览器、网络设备、负载均衡设备、芯片等软硬件，由于复杂的原因无法完全把密码模块升级为 SM 系列密码算法模块，导致整个信息系统还存在安全薄弱环节。

1.1.2 技术背景

电子签名是利用技术手段确保主体缔约行为与合同内容唯一性、真实性的一种方式，它是最早也是最广泛应用于电子合同领域的技术。在我国乃至世界多个国家和地区，有关电子签名的立法开启了电子商务、信息经济立法的先河。从《电

子签名法》颁布至今十多年的社会各界的实践状况来看，电子签名技术应用受到了来自外部及自身的局限，影响了电子签名在电子合同领域的应用。其中，电子签名自身的原因就在于其技术属性过强，偏离了日益发展的互联网应用所具有的简单、便捷、快速迭代等特点，而外部原因则有法律制度缺乏系统性、标准缺乏统一性以及市场替代解决方案的冲击等多方面因素。即便如此，电子签名技术依然是支撑电子合同应用与发展的重要配套服务，在今后的发展方面，立法和标准需要往系统性、统一性方向靠近，而开放电子签名技术服务市场、鼓励创新则是突破其自身局限的重要出路。当然，电子签名并不是唯一的确认电子合同真实性的手段，无论是在技术层面还是在市场应用层面，其它替代性方式的出现大大丰富了电子合同配套服务的形式，这些替代性手段充分适应了市场需求并具有一定的创新性，在立法上应当认可并鼓励。

电子合同服务平台的出现解决了传统的纸质合同签署流程繁琐，易出错等问题，以及合同电子化过程中身份难以鉴别，数据安全性差，发生纠纷时难以鉴定等问题，为用户提供了便捷、安全、合法的在线签约服务。

随着 2015 年《国务院关于积极推进“互联网+”行动的指导意见》的发布，互联网+广泛地应用到各行各业，为电子合同提供了足够宽广的应用场景，云计算平台也为电子合同带来了新的承载方式，区块链的不可篡改性也为电子合同服务平台注入了新的活力。

1.1.3 必要性

密码产业发展机遇前所未有。全球的网络安全产业刚刚起步，投资与创业机会将聚焦网络安全领域，未来可能催生万亿级别的大市场（资料显示：2016 年全球网络安全市场已超过 6000 亿人民币，Gartner 的数据是 906 亿美元）。目前，我国网络安全投入还很不够，仅占整个 IT 产业比重的 1%至 2%，低于世界 5%至 10%的平均水平，更低于欧美国家 8%至 12%的水平，相比于西方发达国家，我国尚有 8 倍的增长空间，这既是短板也是市场。按照国家有关部署，金融和重要领域正在强化密码应用，大量网络和信息系统涉及密码保障系统的新建或改造，市场空间很大。可以说，密码应用将会带动更多安全投入，拓展更大安全市场空间。谁投入早，创新多，谁成为网络安全行业龙头的可能就更大。对此，产业单位要有更加积极的认识。

但如何推进密码深入广泛应用，提升网络空间安全保障能力，我们面临着严峻的挑战，特别是在密码使用方面，还存在使用密码意识不强，密码应用缺乏规划，密码使用不够规范，以及服务保障、风险控制和应急处置能力不足等问题。可以说，问题突出，隐患很大，必须构建科学完善的密码安全保障体系。

电子合同服务在国内外应用广泛，近几年来，国内电子合同服务的厂家百花齐放，已经形成相对稳定的产业生态圈。特别是近两年第三方电子签名市场规模增长势头明显，发展潜力巨大。其中，使用者集中于类似互联网金融等领域的企业，互联网相关业务发生频率高，同时对合同签订流程的完整性要求较严。然而，市面上的电子合同服务产品种类多，产品安全性能参差不齐。

《“十四五”国家信息化规划》提出，打造市场化法治化国际化营商环境，提升电子文件管理和应用水平，深化电子证照、电子合同、电子发票、电子会计凭证等在政务服务、财税金融、社会管理、民生服务等重要领域的有序有效应用。推进涉企政务事项的全程网上办理，大力推进公共资源全流程电子化交易，构建覆盖全国、透明规范、互联互通、智慧监管的公共资源交易体系。电子合同服务

平台是重点行业的关键信息基础设施，密码技术在安全电子合同服务中的规范化应用，能够开拓电子合同服务的应用市场，拓展电子合同服务在各个行业中的应用范围。

1.2 研究目标

本项目通过对国内电子合同服务平台的调研，明确电子合同服务平台的概念内涵和外延，确定本标准研究报告的范围，着重分析国内主流电子合同平台的功能和密码技术使用情况，重点研究电子合同服务平台的技术框架，从电子合同面临的问题、电子合同平台功能架构、业务流程等层面分析信息安全需求与挑战，针对电子合同服务现有密码技术应用情况，从业务角度、安全角度、平台部署角度对电子合同中的密码技术框架进行了分析，并提出了相应的技术路线和标准化建议，为构建安全可靠的第三方电子合同服务平台提供指引。

2. 研究范围

2.1 电子合同服务平台的内涵

根据 GB/T 36298-2018《电子合同订立流程规范》的定义，电子合同是指平等主体的自然人、法人、其他组织之间以数据电文为载体，并利用电子通信手段设立、变更、终止民事权利义务关系的协议。《合同法》第十条：当事人订立合同，有书面形式、口头形式和其他形式。第十一条：“书面形式是指合同书、信件以及数据电文(包括电报、电传、传真、电子数据交换和电子邮件)等可以有形地表现所载内容的形式”。因此电子合同属于合同的一种表现形式，而电子合同服务平台是以电子签名为法律及底层技术基础、云计算为交付及服务技术基础、互联网为场景基础，通过公众平台网站、API/SDK 等方式提供电子签名、电子合同产品及相关配套服务的云端电子合同服务平台。结合《电子签名法》与《合同法》的相关规定，有效的电子合同应当具备以下条件： 1）数据电文原件，能够可靠地保持内容完整、防篡改，满足法律规定的原件形式及文件保存要求；2）电子签名，能够标识签署人、签署时间，防篡改，满足法律规定的有效电子签名要求；3）身份经过第三方有效认证，满足法律规定的认证要求。但是，由于普通个人或企业用户实现上述条件过程繁琐且成本高，与电子化签署提速降本的初衷相悖，因此，普通用户只需选择可靠的第三方电子合同订立系统即可签署有效的电子合同。这也符合商务部在 GB/T 36298-2018《电子合同在线订立流程规范》的规定：“通过第三方（电子合同服务提供商）的电子合同订立系统中订立电子合同，才能保证其过程的公正性和结果的有效性”。同时该规范也对第三方电子合同服务平台做了定义：“第三方电子合同服务平台为独立于合同缔约人，具备身份认证、谈判磋商、电子签名、合同存储与调用等功能，能实现电子合同在线订立及处理的信息系统”。因此本研究报告对电子合同服务平台的研究重点放在第三方电子合同服务平台上。

2.2 电子合同与智能合约的区别

根据《中国区块链技术和产业发展论坛标准 CBD-Forum-001-2017》，智能合约（smart contract）定义为“以数字形式定义的能够自动执行条款的合约”，“注：在区块链技术领域，智能合约是指基于预定事件触发、不可篡改、自动执行的计算机程序。”而《合同法》对合同的定义为“本法所称合同是平等主体的自然人、法人、其他组织之间设立、变更、终止民事权利义务关系的协议。”对于“合约”而言，是由参与各方签署生效后，再由参与各方各自按照约定执行；而“智能合约”存在本身就意味着其已经在执行过程中了，约定内容在“智能合约”诞生之前已经商定好了。“智能合约”更像以程序“if-then”的基本逻辑中的一个触发条件，一旦条件触发就自行执行程序的下一步。所以“智能合约”本质上是一个脚本程序，以程序“if-then”的基本逻辑为基础来运行。这种脚本程序之所以叫“智能合约”，是因为其编写目的是为了实现事先商定好的合约内容的。反过来看，只有能够通过编程实现的合约内容才能成为“智能合约”的实现对象，这就注定了“智能合约”的实现对象是非常有限的，因为不是所有的人类活动都能够通过编程实现的。

对于“合约”而言，在执行过程中，参与各方都有违反合约的可能，“智能合约”则没有这种“人性风险”，“智能合约”一旦设定好，只有作为“钥匙”的脚本满足“锁”的“开启条件”时，才会执行。“合约”的执行是参与各方进行的人类活动，而“智能合约”的执行其实是执行一段程序，对虚拟价值进行处分。对于“合约”而言，环境条件的改变可能会导致合约需要用补充协议、变更协议的形式加以调整。“智能合约”则不具备这种灵活性。“智能合约”更适合在稳定的环境中进行大量重复性运作的应用场景。“合约”的使用广泛渗透在人类活动的层层面面，其双方只要合意达成一致即可成立的特性，使得“合约”具备最大限度的灵活性，从而方便的应用在各个场景。“智能合约”是以程序为基础的虚拟世界当中的特有产物，是在特定应用环境内反映了某种合约关系的程序，按照“if-then”的基本逻辑运行，适用于特定的场景，其功能较为单一，执行较为简单，适用于在稳定的环境中进行大量重复性运作的应用场景。“智能合约”相对于“合约”，就跟“机器人”相对于“人类”类似，前者缺乏灵活性，但在稳定环境、单一功能、大量重复性运作的应用场景中能发挥替代后者的威力。

因此,鉴于“智能合约”在法律性质、履行机制及责任归属等方面与传统法律概念中的“合约”和“公证”存在本质区别，本研究报告暂不将其直接视作电子合同的等效形式，亦不将基于“智能合约”的区块链平台纳入电子合同服务平台的核心主体进行深入研究。然而，我们充分认识到区块链技术，特别是智能合约的不可篡改性和透明性对于电子合同证据保存的价值。依据 GB/T 36320-2018《第三方电子合同服务平台功能建设规范》中关于“电子合同归档与存储”的规定，本研究将探讨如何有效地将区块链技术作为增强型存证手段，将其纳入电子合同服务平台的功能外延，以提升合同数据的完整性和司法证明力。

2.3 电子合同与电子保单的关系

根据《中华人民共和国保险法》，保险单（简称：保单）是保险人与被保险人订立保险合同的正式书面证明。保险单必须完整地记载保险合同双方当事人的权利义务及责任。保险单记载的内容是合同双方履行的依据。保险单是保险合同成立的证明。电子保单是指保险公司借助遵循 PKI 体系的数字签名软件和企业数字证书为客户签发的具有保险公司电子签名的电子化保单。GM/T 0070-2019《电子保单密码应用技术要求》也对电子保单做了定义：保险公司为投保人签发的具有保险公司数字签名的电子化保险合同凭证，法律效力等同于纸质保险单证。因此电子保单与电子客票类似属于电子合同的一个特殊应用场景，属于电子合同的范畴。本研究将在现有第三方电子合同服务平台功能建设规范、电子保单密码应用技术要求等的基础上，在电子合同的范畴内对平台的密码应用技术的要求做深入的梳理、完善，形成第三方电子合同服务平台密码应用规范。

2.4 电子合同服务平台的应用外延

本项目的研究范围不限于对电子合同的处理，还可以进一步扩充为“第三方电子文档签署服务系统”、“第三方电子证据存证平台”、“第三方电子证据取证平台”（例如《电子合同取证流程规范》）等。

3.电子合同服务平台发展现状

3.1 国外电子合同服务平台现状

3.1.1 市场状况描述

来自国家工业和信息化部门的官方数据显示，在国际方面，2019 年 10 月，上市一年半的美国电子签约服务商 DocuSign 总市值已经突破 118 亿美元，与刚上市时的 60 亿美元相比，涨幅接近 100%。目前 DocuSign 在全球有超过 50 万个付费客户和数亿用户，获得 800 个联邦、州和地方政府机构、FedRAMP 的授权。

2019 年 5 月 3 日，欧盟公布了其关于电子商务未来规则和义务的拟议案，其中关于通过互联网签订的电子合同问题，欧盟的提议是：WTO 成员国必须允许通过电子手段签订合同，并且其法律制度既不应为使用电子合同制造障碍，也不应导致合同被剥夺。

可见，电子合同的合法性已获得美国及欧盟国家的普遍认可，且具有一定量的应用市场。

3.1.2 国内外电子合同应用的差异

3.1.2.1 中外法律差异

在国外（例如美国），电子签名的效力，重点集中在查证签名人的意图，而不是签名的形式和规则，这主要是因为国外的信用体系完善，网络环境相对安全，违法成本较高，签名人对安全的顾虑不像国内一样强烈。

就国内来说，签署电子合同前要确认签署各方身份真实有效，签署行为符合签署人的意愿，签署后合同不被篡改，这样的电子合同才是合法有效的。在国内会经常出现盗用公章、私刻公章的情况，如果使用国外电子签名就很难厘清了。所以，国外的电子签名产品很难进入国内市场。

另外，法律适用范围也不同。在国外，所有的签署场景都可以使用电子合同。而我国的《电子签名法》明确规定了以下几种场景不可以使用电子合同：涉及婚姻、收养、继承等人身关系的；涉及停止供水、供热、供气等公用事业服务；法律、行政法规规定的不适用电子文书的其他情形。

3.1.2.2 认证流程差异

在国外，用户可以通过邮箱申请使用电子签名服务。他们的账户通常需要绑定特定的 IP 地址以确保安全性。每次签署文件后，系统会自动生成并存储发送记录。所有操作包括查看、打印、签名等，都会被准确记录并加上时间戳。这些记录最终会存储在数字证书中，以确保数据的完整性和可追溯性。而在国内，基本上所有的第三方电子合同平台都需要接入 CA 机构的数字证书，以保证签署人的身份无误。数字证书是保证电子合同合法合规的标配，只有使用《电子签名法》认可的可靠的电子签名，才具备与手写签名或者盖章具有同等的法律效力，而由国家认可的 CA 机构所签发的数字证书可提供相应的可靠的电子签名保障。

国内外认证流程之所以有区别，主要还是由于国外信用体系完善，契约精神较好。目前，国内个人签署电子合同需要使用真实的手机号进行平台注册，并通过验证身份证、银行卡，以及人脸识别来完成个人实名认证。国内企业则需要通

过验证营业执照、法人身份证、授权代表人身份证，以及对公转账等完成实名认证。

3.1.2.3 产品模式差异

国外没有公章，只有电子签名，无论是个人还是企业，在合同上只需要签署合法的电子签名即可。但在国内，公章都是在重大决策、重大合同等正式场合下使用的不可或缺的工具，因此在国内的电子合同产品应用中，既有电子签名也有电子印章，所以国外的电子签名产品无法满足我国电子合同签署的业务需要。

3.1.2.4 技术服务差异

国外的电子合同发展较早，受限于 IT 技术，企业成本投入较高，比如国外的 Docusign 服务器是自建的。而国内赶上了 IT 技术大发展的时代，私有云、公有云、SaaS 等几种模式，满足了用户的使用条件，降低了企业用户的使用门槛，同时也减少了使用成本，缩短了部署时间。

3.1.3 小结

由于国内外电子合同在法律适用、认证流程（功能）、产品模式及技术服务等多个方面存在较大差异，国外的电子签署平台技术和市场发展虽有一定的参考价值，但其借鉴性和可比性较为有限。因此，本研究报告将主要聚焦于国内电子合同服务平台的现状和需求，深入分析其在密码技术应用中的实践经验和规范要求。通过对国内平台的调研，为后续制定符合我国法律和技术要求的相关标准提供参考，因此不再对国外电子签署平台进行深入研究。

3.2 国内电子合同服务平台现状

3.2.1 市场状况调研

公开数据表明，过去几年国内电子合同市场仍处于发展的起步阶段，整个行业的渗透率还非常低（不到 5%），几大平台的营收合计仅在亿元级别。

图 3-1　国内电子合同市场规模及年复合增长率图

2017 年以来，电子合同已在慢慢渗透各行各业，特别是在相关政策的引导下，电子合同在互联网金融、旅游、保险、长租、电子商务等行业已成为合规“标

配”，电子合同的渗透率已经在逐年提升，应用领域已扩大至互联网金融、供应链、电子商务、旅游、保险、银行、长租等行业。未来电子合同将会向更多行业渗透，达到数十亿元乃至上百亿的市场规模，能普遍适用全行业任何签约场景的云端产品/服务。

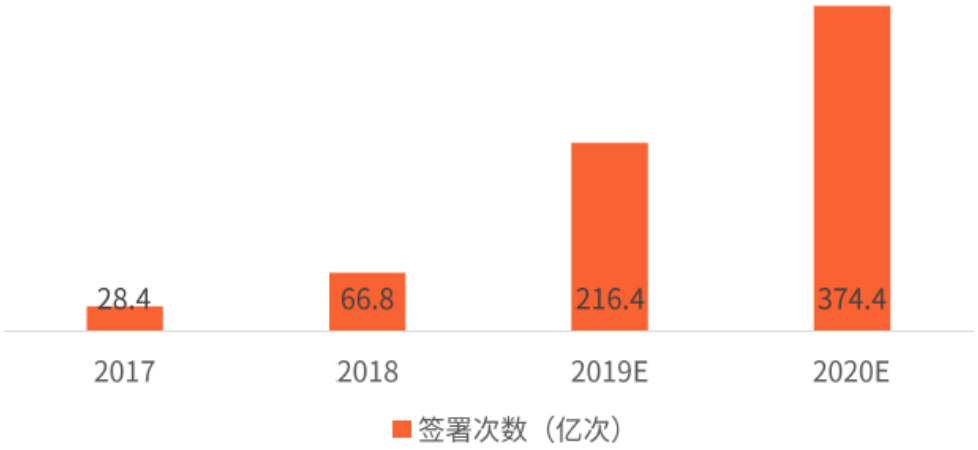

图 3-2　2017-2020 国内电子合同签署次数规模及预测图

来自国家工业和信息化部门的官方数据显示，国内方面：2018 年，中国互联网和相关服务业保持平稳较快增长，其中互联网业务收入保持较高增速，中国规模以上互联网和相关服务企业（简称互联网企业）完成业务收入 9562 亿元，比上年增长 20.3%。2018 年中国电子合同签署次数达 66.8 亿次，预计 2019 年电子签名行业仍将保持快速的增长，签署总量规模有望突破 200 亿次。

3.2.2 应用情况调研

随着互联网经济的发展，中国电子商务的快速发展，加上“互联网+”概念的普及，电子合同的需求日益剧增，电子合同在国内应用广泛，电子合同服务的厂家百花齐放，已经形成相对稳定的产业生态圈。从国内主流的电子合同厂商应用情况看，当前电子合同的应用主要集中在互联网金融、电子商务、旅游、保险、银行、大型供应链、房地产、物流等行业。

1)　金融行业

金融机构应用第三方电子合同的核心原因是政策引导。针对金融机构对电子合同的应用，政策的指引主要涵盖两个方面：

- 国家政策对互联网金融和传统金融机构互联网业务的合规性要求：电子合同成为理财、贷款等业务中重要且必要的一环；
- 政策倡导下，传统金融机构对云计算等新技术的实践应用。

综上，现阶段电子合同市场在政策的引导下，帮助金融机构确立了先发优势，也极大地促进了其对电子签名及电子合同的认知，其对电子合同的核心需求也更多的集中在从前期 CA 认证到中期合同签订、流转、存储再到后期司法鉴定、公正、仲裁等全流程生态服务。

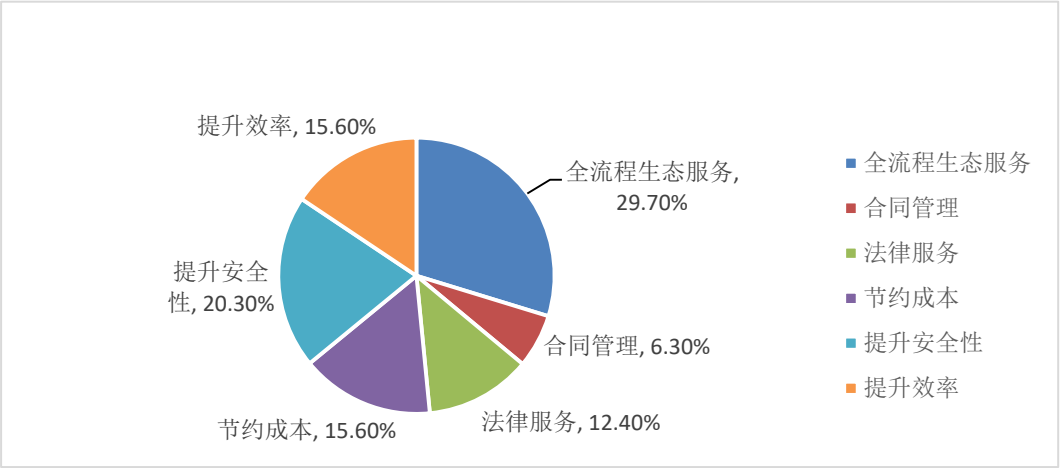

图 3-3　金融机构对电子合同的核心需求

在面对金融行业多个细分领域时，电子合同厂商针对性的提供了差异化解决方案，但现阶段各类型解决方案的核心应用集中在对签约流程的行业个性化配置，工具属性比较突出。

2)　电子商务行业

电子商务作为现阶段国内发展迅速且日益成熟的行业，在电子合同的实践中依然处于摸索尝试阶段：

- 电子商务企业应用电子合同显得较为“被动”，实践的初衷集中在尝试和跟随，同时也包括基于互联网交易闭环完善的被动导入，企业并没有有效掌握电子合同的能力和优势，对电子合同的认知水平存在不足；
- 电子商务行业发展日趋成熟，各企业的商业模式不一，对于电子合同的需求十分分散，并没有形成一个统一的明确的核心需求点，企业依然处于摸索尝试阶段。

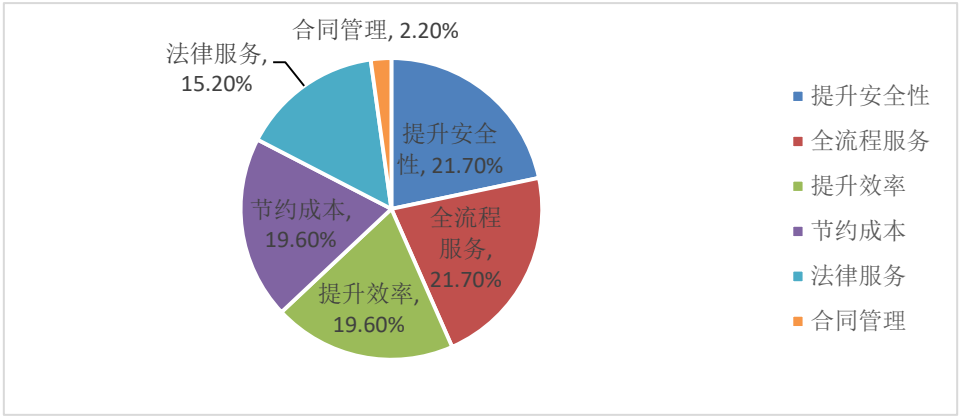

图 3-4　电子商务企业对电子合同的需求点较分散

电子合同在电子商务行业中的应用依附于交易订单的形成，而电商企业会经常面临订单高并发的局面，因此对企业而言，优质的负载能力有助于保障交易流程（包括合同订立）在订单高并发时期顺利完成。

B2B 电子商务已经从 1.0 信息撮合时代进入 2.0 线上交易时代。随着技术发展和网络环境的成熟，越来越多的大宗商品交易选择上线完成交易，合同作为其中重要的一环，安全性和规范性自然成为企业用户的重要关注点，而国家的认证

资质及企业的运营能力则成为企业衡量安全性和规范性的重要标准。

此外，相较于其他行业，电子商务企业应用电子合同时需要 IT 技术人员进行更多的后台操作，因此 IT 技术人员的操作复杂对电子商务企业的持续应用产生了消极影响。

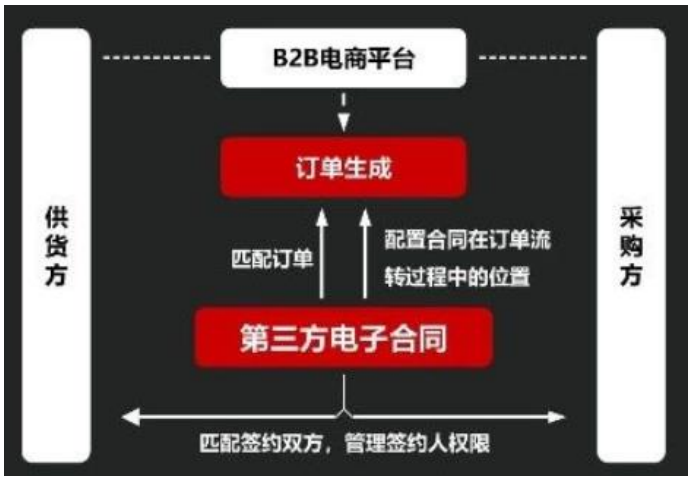

图 3-5　IT 技术人员的后台配置内容

3)　物流行业

《人民日报》报道称，2016 年中国快递业务量规模已经稳居世界首位，全年业务量完成 313.5 亿件，业务收入突破了 4000 亿元。我国快递业已经连续六年保持 50%左右的高速增长，在全球每年约 700 亿件的快递量中，中国占了 40%。

《2020-2026 年中国物流产业竞争现状及未来发展趋势报告》，2018 年社会物流总额达到 283 万亿元，快递业务量突破 500 亿件，稳居世界第一，实现了跨越式发展，走出了一条中国特色的物流发展道路。

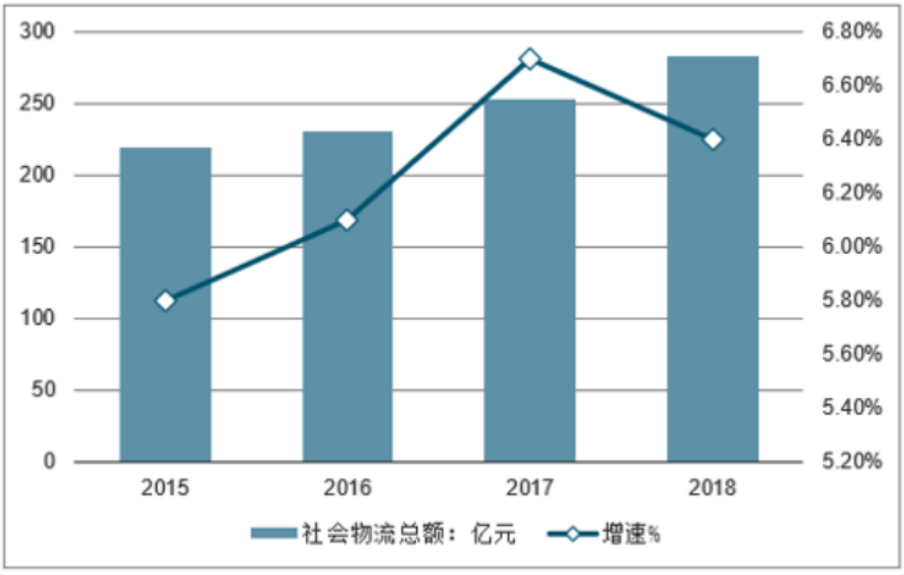

图 3-6　2016-2018 年我国社会物流总额及增长情况

随着物流行业的高速发展，其背后衍生出的物流成本管控和合同单据管理困难已经成为了物流行业目前急于解决的重要问题。而物流电子合同的出现，成为了物流行业稳步发展的一大新助力。

交通运输部关于修改《道路货物运输及站场管理规定》的决定（中华人民共和国交通运输部令 2019 年第 17 号），道路货物运输经营者和货物托运人应当按照《合同法》的要求，订立道路货物运输合同。鼓励道路货物运输经营者采用电子合同、电子运单等信息化技术，提升运输管理水平。

在物流行业的电子合同签署应用中，由于其监管难、取证慢、取证难，因此物流电子合同的安全可靠需确保各方主体身份的真实性和有效性，以第三方权威机构认证各参与方的真实身份，以合法第三方 CA 机构为认证的各参与方颁发数字证书，结合数字签名、时间戳技术，保障电子单据的交接及确保签收行为的真实、有效性，以“电子认证+电子签名+电子存证（区块链存证/第三方存证）”技术相结合，通过电子认证技术实现对业务的监管，通过电子签名技术保障业务数据的真实、有效性，通过电子存证固化原始电子数据。

3.2.3 技术情况调研

2018 年 9 月 7 日，《最高人民法院关于互联网法院审理案件若干问题的规定》指出，当事人提交的电子数据，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认。

结合《最高人民法院关于互联网法院审理案件若干问题的规定》，目前国内电子合同应用，主要基于非对称加密算法 RSA 进行电子合同签署来固化证据，同时通过可信时间戳、区块链等技术加强证据的可信度，而国内目前一方面有 OFD 版式文件，同时国家密码主管部门也在主推 SM2 算法，因此电子合同的加密技术应当把 SM 系列密码算法也囊括在内。

为满足用户多维度的签署需求，目前电子合同服务平台基本都可以提供公有云签署、API/SDK 签、私有云签三种应用。在签署层提供 PC、APP、小程序、H5 签署，在接入层提供 API/SDK 接入方式；在应用层提供身份认证、合同签署、合同管理、司法支持四大应用模块。

公有云提供电子签约系统、APP、小程序、H5 多种方式签署合同，无需对接，即签即走，简单易用，安全有效，且相互之间数据全面互通。

私有云提供产品本地部署包与 API 接口服务，由用户根据需求全程在自己服务器内调用合同发起、合同签署、合同下载、合同验证等功能。签署后的合同保存至用户本地服务器，接口采用标准 http/https 协议，跨语言、跨平台的同时，能够满足 PC 端、APP、小程序、H5 端接口调用，并提供可选第三方服务，如：身份认证、数字证书、时间戳、电子存证、短信、云存储等服务。

3.2.4 主要的电子合同产品和平台

3.2.4.1 信睿吉签

信睿吉签区块链电子合同采用盲可验证加密签名（RSA-BVES）、身份验证、智能合约、区块链等技术，在 CA 提供证书的基础上，为用户提供了一个无中心的可信第三方合同签存平台，可以有效抗抵赖抗捏造、保护隐私，为用户能够公平安全地签存合同进行有力的保障。

该平台产品采用的盲可验证加密签名技术（RSA-BVES），可避免区块链上的结点获取到合同相关的信息造成合同信息泄露，整个过程实现了对合同信息的盲化达到隐私保护的目的，同时，对签署后的 PDF 电子合同进行加密存储。而区块链上的链码可以验证 RSA-BVLES 签名是否有效，最终合同签署双方又可以从对方

RSA-BVES 签名提取一个普通的 RSA 签名，实现了交换签名的目的。产品主要由合同签署模块、区块链模块、加密模块组成，其业务功能如下图所示：

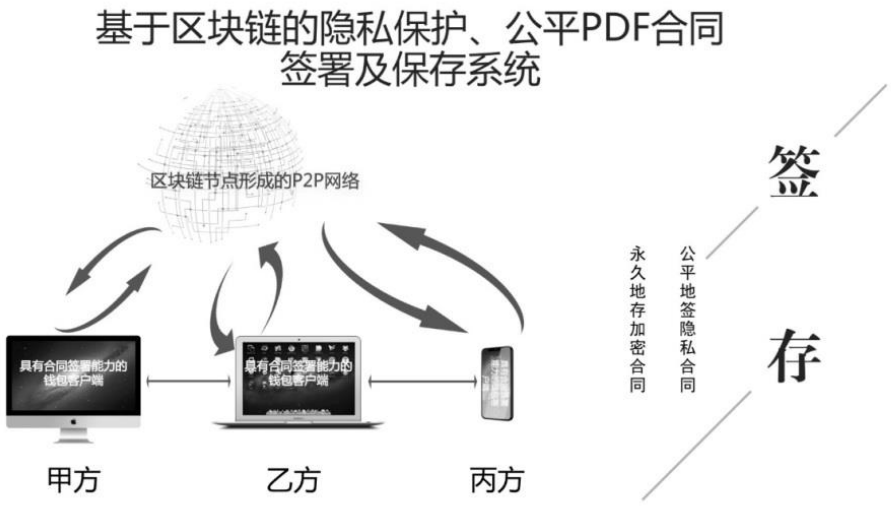

图 3-7　信睿吉签区块链电子合同业务功能图

目前，信睿吉签区块链电子合同，主要应用在房地产领域。

3.2.4.2 金格信签

金格信签是一款基于 PKI 技术体系，采用公钥加密技术结合数字签名技术、时间戳技术、实名认证技术、数据安全认证等技术的电子合同签署服务平台，可以支持 RSA 算法或者 SM2 算法进行签章，同时 OFD 格式签章按照 OES 接口标准和《安全电子签章密码应用技术规范》开发，系统设计符合 GB/T 38540-2020《信息安全技术 安全电子签章密码技术规范》系统安全可靠，适用于政府、企业和软件开发商应用集成。该产品以物联网和云计算为依托，整合行业资源，通过公有云 SaaS 平台以及专属私有云部署等多种方式，为政府、企业及个人用户提供实名认证、电子合同签署、电子签章、电子存证、合同验真及法律服务等全场景、全生态、全流程的电子合同。其产品功能图如下：

图 3-8　金格信签功能架构图

金格信签为基础性电子合同服务平台，系统包含服务端管理端，也需提供SDK、API 集成与小程序、APP 等方式签署，可以方便的与其他业务系统进行集成，服务端应该为管理员提供组织机构管理、证书管理、印章管理、系统管理、安全控制、以及合同的统计审计等功能。

金格信签目前应用行业遍布地产、电子商务、物流、信托、银行、企业集团等众多行业。

3.2.4.3 签吧

签吧是一款采用了 CA 认证、数字签名、时间戳、密钥托管、身份验证、访问控制、电子表单、中间件等技术的第三方在线签约服务平台。该产品主要面向大型企业及上下游供应商或经销商、科研机构、事业单位等，解决传统的纸质合同签署过程中成本高、效率低、容易出错，以及合同电子化过程中身份难以鉴别，数据安全差，发生纠纷时难以鉴定等问题。该产品由签吧平台代理、WEB 服务平台、PDF 处理平台、通知服务平台、存证平台、认证与证书平台、文件服务平台、密钥托管服务器等八大子系统组成。其各子系统负责：

1) 签吧平台代理：负责统一处理所有向签吧发起的请求，起安全控制和服务转发作用；
2) WEB 服务平台：负责处理 WEB 相关的请求与服务；
3) PDF 处理平台：提供 PDF 文档的各种服务；
4) 通知服务平台：负责短息、邮件等通知消息的处理；
5) 存证平台：负责对文档的全生命周期和各种用户操作保存电子证据；
6) 认证与证书平台：负责实名认证和证书处理；
7) 文件服务平台：负责对文档进行保存并加密；
8) 密钥托管服务器（可选）：部署在客户企业的内部网络，使用户可以管理自己公司内部的密钥。

图 3-9　产品功能框架图

签吧目前应用的行业主要有：公共金融交易中心、医药行业、大型超市及上下游供应商或经销商、房地产企业。

在密码技术应用方面，签吧支持用户使用硬件密码模块或软件密码模块生成并持有密钥对，由 CA 对用户的身份进行认证，为其持有的密钥对签发数字证书。客户端用户对电子合同的签名使用了 PDF 签名技术，该技术对 PDF 格式的电子合同文档、用户签名外观图片、签名时间戳等进行消息摘要计算，使用用户所持有的数字证书对消息摘要结果进行签名，并将签名合成到 PDF 文档中。签名后的电子合同文档，通过 SSL 通道在网络上传输，SSL 技术保证了网络上传输的数据被签名和加密。如果电子合同文档需要在服务平台上存储，服务平台提供文档加密存储的服务，使用硬件密码模块中的密钥对电子合同文档加密后存储，只有获得授权的用户才能对电子合同文档进行解密。

3.2.4.4 信手书电子合同服务平台

信手书电子合同服务平台提供完整的从实名身份鉴别、数字证书颁发、合同签署服务、数据存证保全到司法举证服务的全流程闭环交付的电子合同服务。

信手书电子合同服务平台的总体框架如下图所示，平台集成数字证书服务、数字签名和有效性验证功能为一体，采用手写签署方式实现可靠、可视化、可感知的电子签名，免去数字证书或电子签章介质的交互成本，真正实现“所见即所签、所签即所得、所得即可验”。除了便捷与高效率，信手书电子合同服务平台

保证网上身份的真实、签署数据的完整、网上系统的安全、个人数据的隐私，不仅仅在人与人、企业与企业之间建立信任关系，同时也在所关联的数据、代码和服务平台建立数字化信任。

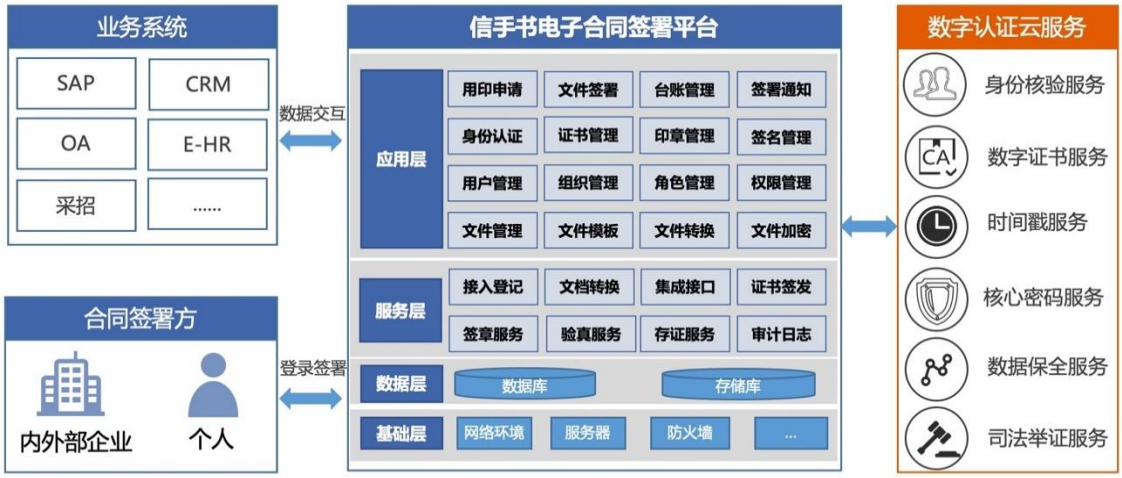

图 3-10　信手书电子合同服务平台框架图

信手书电子合同服务平台在电子合同签署的流程中，身份认证、合同文件数据、网上数据传输等环节中应用了大量密码学算法和技术原理，不仅为用户提供高安全级加密防护，还确保了在电子合同管理的各环节有效阻断任何未授权的操作行为。信手书电子合同服务平台应用的密码技术及信息安全保障措施具体包括：

1) 提供完善的合同生命周期管理服务，包括文件生成、合同发起、印章管理、模板管理、合同流转、查询统计、合同验真、消息送达、台账管理、日志审计等；
2) 采用多种身份核查方式，结合生物识别手段，实现了对合同签约人身份的实时在线核验，保证了电子合同签约主体身份的真实性、可靠性，同时对用户身份信息进行不可逆脱敏处理，保证用户隐私；
3) 采用手机签名、UKEY 签名、手写签名、短信签名、批量签名等多种可靠电子签名方式，对业务签署的时间、地点、签名人身份信息、签署行为证明素材、手写轨迹以及电子合同内容等关键数据进行安全采集、签名认证、证据固化，从而确认当事人身份和签署行为，满足《电子签名法》对可靠电子签名的要求，保障电子合同的法律效力；
4) 采用密码技术提供数据加密来确保电子合同文件存储的安全，在平台中为用户提供细粒度的文档权限管控，同时提供文档哈希存证与保全；
5) 基于 SSL 双向通讯认证及传输链路加密，确保电子合同文件的数据传输安全，防止恶意窃听及篡改合同文件；
6) 将签署事件过程中产生的关键证据封装成存证数据包，并加盖时间戳固化，保存于本地，与此同时将存证数据包加密处理后上传至云保全平台进行证据保全；
7) 在合同管理的各阶段采用密码技术确保操作行为留痕可追溯，保障电子合同的业务信息安全。

信手书电子合同服务平台目前应用的行业主要有政府、金融、卫生、交通、企业、教育、房地产等多个行业。

3.2.4.5 法大大电子合同服务平台

法大大电子合同服务平台是一款采用了“实名认证、电子签名、第三方取时、区块链存证技术”等技术的电子合同签署平台。平台产品支持平台部署、系统集成部署和本地部署，签署渠道支持 PC、APP 部署，支持微信签署。

在合同签署及管理方面，支持用户上传合同，并支持用户自行添加附件，其签署顺序支持无序签、顺序签和单独签，支持用户撤销签署。签名方式支持用户使用系统章和手绘签名。

在实名认证方面，支持企业认证，对于个人用户，法大大支持身份证、银行卡、支付宝认证，其签署认证方式支持人脸识别、短信认证、银行卡验证、身份证验证、公安部 eID 认证和使用签署密码认证。

在防篡改方面，使用数据加密技术、可信时间戳服务，对电子文件的存储和传输采用国际标准 PDF 格式，并采用国际通用哈希值技术固化原始电子文件数据。

法大大从电子合同签署、托管、出证到纠纷解决的全流程闭环法律服务：

1) 提供电子合同签署、电子签章、合同在线编辑、合同管理、存证出证等服务，满足用户对电子合同的基本需求；
2) 整合提供司法鉴定、网络仲裁和律师服务；
3) 提供 500 多个商用合同供用户免费下载使用，涉及各行各业，用户可快速生成自己的专属合同；
4) 联合中国广州仲裁委员会上线国内首个“一站式”网络仲裁服务系统，为合同纠纷提供高效和合规的解决方案。

法大大作为电子合同领域的主流厂商，是少数能将区块链技术应用到电子合同存储及数据防篡改方面的平台。目前该产品主要的应用行业有：金融、保险、第三方支付、旅游、房地产、医疗、物流、供应链、B2B、B2C 线上交易平台、人力资源管理等行业以及政府机构。

3.2.4.6 小结

结合上述电子合同服务平台来看，发现当前电子合同服务商的核心服务基本集中在提供电子签章、合同在线签署、合同管理、合同查验等功能。基本上均会采用实名认证、电子签名、时间戳等技术以保证电子合同签署过程的安全性、真实性、数据完整性以及不可否认性，确保签署的电子合同合法合规。此外，部分电子合同厂商除提供上述服务之外，还可提供第三方的法律服务（如：在线仲裁、存证出证、司法鉴定、技术证明、企业法律服务等）。少部分电子合同厂商目前已引入区块链技术，提供电子数据去中心化存证服务，实现证据固化，可以有效抗抵赖抗捏造、保护隐私，为用户公平安全地签存合同提供有力的保障。

4. 法律法规和标准化现状

4.1 国外法律法规/标准化组织的相关研究

4.1.1 法律法规

随着全球贸易和电子商务快速发展，各组织/国家也出台了相关的法律法规明确电子签名的定义、确立电子签名的法律效力。

1) 联合国《电子商务示范法》

规定了电子签名的“功能等同原则”法律效力。

2) 联合国《电子签名统一规则》

在“功能等同原则”的基础上进一步设定了一些判断电子签名是否可靠的条件，使得对电子签名效力的规定更科学、完善。

3) 联合国《电子签名示范法》

对电子签名做了明确定义：指在数据电文中以电子形式所含、所附或在逻辑上与数据电文有联系的数据，它可用于鉴别与数据电文相关的签名人和表明签名人认可数据电文所含信息。

4) 欧盟《关于内部市场与电子商务有关的若干法律问题的指令》

第 11 条也规定“各成员国须在其国内立法中规定，除非当事人均为专业人员且另有规定，在信息服务获取方应邀对信息服务供应商所作的要约通过技术手段，如点击键盘按键，来表示其承诺的情况下，自服务获取方通过电子手段收到服务供应商关于收悉服务获取方承诺的回执时合同成立。”

5) 欧盟《电子签名共同框架指令》

规定“以电子形式所附或在逻辑上与其他电子数据相关的数据，作为一种判别的方法”称电子签名，明确了电子签名的含义。

6) 美国《电子签名法案》

它使电子签名和传统方式的亲笔签名具有同等法律效力，被看作是美国迈向电子商务时代的一个重要标志。

7) 美国《统一电子交易法》

第 8 条第 1 款规定“如果当事人同意以电子手段进行交易，并且某一法律要求一方应以书面形式向另一方提供、发送或送达信息，那么若此信息依其情形是由在接收器接收信息时有接收保持信息能力的电子记录来提供、发送或送达的，则上述该法律的要求即被满足。”

8) 新加坡《电子商务法》

一方面规定了电子签名的一般效力，保持技术中立性，适用于以任何技术为基础的电子签名;另一方面，又对所谓“安全电子签名”做出了特别规定，并建立了配套认证机制。

除了上述组织和国家，还有法国、德国、英国等国家都有各自相应的法律法规，在对法律应该承认什么样的电子签名具有法律效力的问题上，联合国示范法和各国电子签名法采用了不同的立法模式，主要有以下三种：

第一，技术中立模式。这种模式以联合国电子商务示范法为代表，即规定只要符合一定的条件，电子签名就具有与传统手写签名同等的法律效力，而不限制达到规定条件的电子签名应该采用的技术。联合国电子商务示范法规定，如果法

律要求一个人签字，则对于一项数据电文而言，倘若情况如下(即满足了该项要求)：1.使用了一种方法，鉴定了该人的身份，并且表明该人认可了数据电文所含的信息;2.从所有各种情况看来,包括根据任何相关协议,所用方法是可靠的，对生成或传递数据电文的目的来说也是适当的。美国、澳大利亚、新西兰等国的电子签名法采用了这种技术中立的立法模式。

第二，技术特定模式。即法律只明确采用某种特定技术的电子签名的法律效力，对采用其他技术的电子签名的法律效力未做规定。如韩国电子署名法只承认数字签名为合法的电子签名。韩国电子署名法规定：与公认认证机关颁布的认证书所包含的电子署名检证键一致的电子署名生成键所生成的电子署名,可视为依法而定的署名或印章。此外德国、丹麦、马来西亚、印度以及我国香港地度等的电子签名法也都采用技术特定的立法模式。

第三，技术中立与技术特定的折衷模式。这种模式承认所有安全电子签名都具有与手写签名同等效力，同时以目前国际上比较公认的成熟技术为基础，推荐一定的安全条件和标准。新加坡电子签名法规定，如果一项法律规则要求签名，或规定某一文件未经签名会产生特定的法律后果,则采用电子签名的形式满足该法律规则。同时该法又规定，通过使用法定的安全程序，或当事人同意采用的合理安全的商业程序，如果能够证实一项签名在制作时符合下列条件，则该签名可以视为安全的数字签名：1.使用者唯一的签名；2.能证实使用者的身份；3.通过某种使用者可以唯一控制的方式或方法创设;4.和相关的电子记录以某种方式具有密切联系，一旦该记录被修改，则签名也随之失效。联合国电子签名示范法、菲律宾电子商务法、台湾电子签章法等也都采用了这种折衷式的立法模式。

4.1.2ISO/IEC 相关标准

ISO/IEC/JTC1/SC27/WG2 已经制定并发布了一系列基础和共性标准，涉及数字签名技术、时间戳、实体鉴别、消息鉴别码、抗抵赖、哈希函数，以及密码技术和密钥管理等领域，为电子签名技术及应用提供指导。

ISO/IEC 27000 系列标准是由国际标准化组织（ISO）及国际电工委员会（IEC）联合定制。ISO27001 标准（信息安全管理体系标准）最早于 1993 年由英国贸易工业部立项，是现今广泛应用于信息安全领域的管理体系标准。ISO27001:2005 已经成为世界上应用最广泛与典型的信息安全管理标准,旨在制定单个组织实施安全控制方面的要求，它涵盖了物理设备的控制以及 IT 安全方面,最新版本为 ISO27001:2013。信息安全管理系统是组织结构过程和整体管理架构的一部分，在涉及流程、信息系统、控制措施时都应考虑信息安全。信息安全管理对每个企业或者组织来说都是十分重要的,所以信息安全管理体系认证具有普遍的适用性，不受地域、产业类别和公司规模限制。若电子合同厂商通过了 ISO27001:2013 认证,代表着其电子合同服务平台的组织信息安全已建立起了一套科学有效的管理体系作为保障。

ISO/IEC 27018:2014（云端隐私数据保护标准认证）是面向云服务提供商的国际标准认证,此类云服务提供商依据其与客户签订的合同来处理个人可识别信息（PII），并且以使双方都能满足针对 PII 保护所使用的法规要求及合同义务的方式来进行服务运营，是目前国际上最权威、最严格的，同时也是最被广泛接受和应用的信息安全体系认证。ISO/IEC 27018:2014 针对适用于 PII 的 ISO27002 控制体系提供了实施指南，旨在满足现有 ISO27002 控制体系组合未能满足的公有云 PII 保护要求。若电子合同厂商通过 ISO27018 认证,可证明其电子合同服务

平台在保护企业数据、知识产权、文档和云端 IT 系统安全等方面达到了高标准的行业最佳实践。

4.1.3 美国国家标准化研究院（NIST）相关标准

NIST 隶属美国商务部，主要负责对物理、生物和工程方面进行基础和应用研究，并为美国甚至世界提供标准、标准参考数据及在相关领域的服务。

SP800 系列标准是 NIST 从风险管理的各个阶段、环节的需要为出发点而发布的一系列关于信息安全的指南，该系列文档作为针对信息安全技术和管理领域的实践参考指南，在国际安全界得到了广泛的认可和应用。NIST SP800 系列已经出版了大量与信息安全相关的文件，例如，SP800-26 和 SP800-30 分别描述了自评估指南和风险管理指南，SP800-34 信息技术系统应急计划指南，SP800-51 描述通用缺陷和暴露（CVE）缺陷命名方案的使用，SP800-53 和 SP800-60 描述了信息系统与安全目标及风险级别对应指南，SP800-56 提供了成对使用离散对数密码体制的密钥建立计划的建议，SP800-63-2 是电子认证指南，SP800-76-2 是个人身份验证的生物识别数据规范，SP800-89 给出了数字签名应用安全保障获取建议，SP800-102 则提供了数字签名实时性建议，SP800-118 提供了企业密码管理的参考指南，SP800-130 提供了密钥管理系统的设计框架的准则，SP800-164 是移动设备硬件层安全准则等。

其中，SP 800-131A 定义哪些密码算法有效，以及需要哪些密码算法参数值才能在特定的时间段内实现特定的安全强度。自 2014 年起，在处理或创建新数据时所需的最低安全强度为 112 位。按照实施安全数据管理准则的其他 NIST 标准，使用 80 位的安全强度来处理的现有数据应该会在大约 2031 年之前保持安全。

SP 800-144 是公有云中的安全和隐私指南，它描述了与公有云计算相关的安全和隐私方面的挑战，论述了公有云环境的威胁、技术风险和保护措施，并为规划出合理的信息技术解决方案提供了一些建议。

4.1.4 欧洲电信标准化协会（ETSI）相关标准

欧盟方面从事相关标准化工作的组织为“欧洲电信标准化协会”（ETSI）(European Telecommunications Standards Institute)。

2008 年 11 月，欧盟委员会发布促进电子签名和电子身份跨国应用的行动计划，在该计划中将原来十分复杂的标准结构进行了梳理，重新分类。重新梳理的文档分为 5 个类型，分别为：

1) 指导方针；
2) 政策及安全要求；
3) 技术规格；
4) 一致性的评估；
5) 测试的合规性和互操作性。

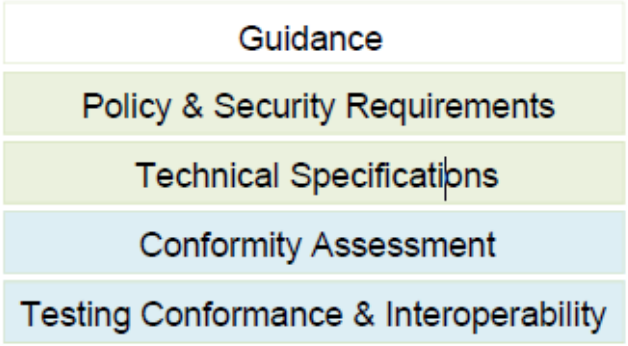

图 4-1　欧盟电子签名文档分类

（ETSI SR 001 604-2012）

相应的电子签名框架结构如下图所示：

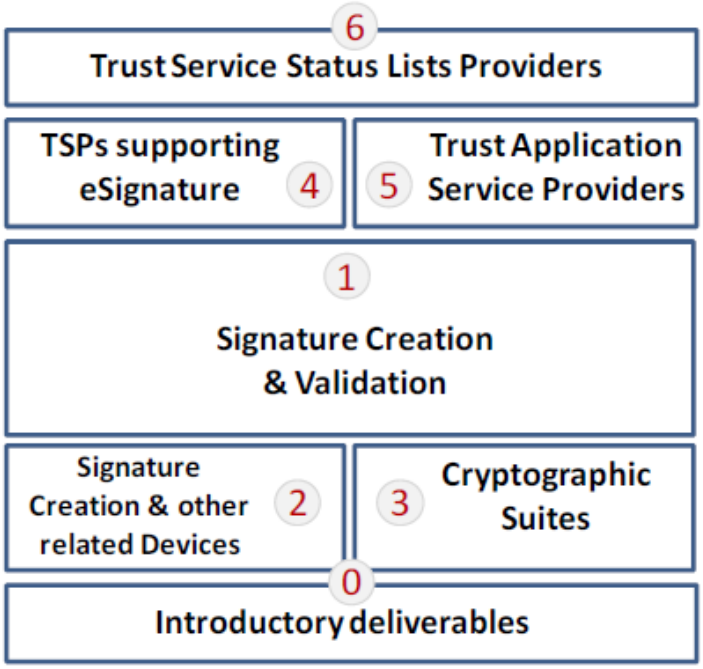

图 4-2　欧盟电子签名框架

（ETSI SR 001 604-2012）

4.2 国内法律法规/标准化组织的相关研究

4.2.1 电子合同服务平台建设层面

截至 2021 年 3 月，国内已经出台了若干与电子合同服务相关的法律法规及标准规范，包括：《中华人民共和国民法典》、《合同法》、《电子签名法》、《中华人民共和国密码法》、GB/T 36298-2018《电子合同订立流程规范》、GB/T 36319-2018《电子合同基础信息描述规范》、GB/T 36320-2018《第三方电子合同服务平台功能建设规范》、《电子合同取证流程规范》等。具体如表 4-1 所示：

表 4-1　电子合同服务相关法律法规及标准规范表

法律层面	《合同法》、《电子签名法》、《中华人民共和国密码法》、《中华人民共和国民法典》
国家标准	GB/T 19252-2003《电子商务协议》 GB/T 18769-2003《大宗商品电子交易规范》 GB/T 20520-2006《信息安全技术 公钥基础设施时间戳规范》 GB/T 25064-2010《信息安全技术 公钥基础设施 电子签名格式规范》 GB/T 36298-2018《电子合同订立流程规范》 GB/T 36319-2018《电子合同基础信息描述规范》 GB/T 36320-2018《第三方电子合同服务平台功能建设规范》 GB/T 39321-2020《电子合同取证流程规范》
涉及的相关行业标准	《电子商务模式规范》（SB/T 10518-2009） 《网络交易服务规范》（SB/T 10519-2009） 《互联网信息服务管理办法》（国务院令第 292 号） 《电子认证服务管理办法》（工业和信息化部令第 1 号） 《信息安全等级保护管理办法》（公通字[2007]43 号） 《信息系统密码应用基本要求》（GM/T 0054-2018） 《电子保单密码应用技术要求》（GM/T 0070-2019）
团体标准	《互联网金融个体网络借贷电子合同安全规范》

1)　《合同法》

该文件虽然没有直接给出电子合同的定义，但肯定了以数据电文为表现形式的合同的合法性。电子合同本质上还是合同，是合同的一种特殊表现，其特殊性在于以数据电文作为合同的表现形式，合同内容的记载方式实现了电子化。

2)　《电子签名法》

该文件进一步明确了：采用电子签名的方式订立的电子合同具有完备的法律效力。该文件针对“数据电文、电子签名”进行了进一步的法律定义，对什么样的数据电文是符合法律、法规要求的书面形式进行了详细定义，对什么样的签名是可靠的电子签名，及如何认证签名人身份进行了详细定义，完成了对电子合同的核心要素的法律覆盖，是电子合同得以广泛应用的法律基石。

3)　《中华人民共和国密码法》

密码法标志着我国在密码的应用和管理等方面有了专门性的法律保障，大力推进了电子签名、电子合同的发展。

4)　《中华人民共和国民法典》

民法典中明确给出了电子合同的定义：电子合同是可以随时调取查用的数据电文并明确电子合同的地位、成立时间、成立地点、交付时间，指出电子合同和纸质合同是处于同样的法律地位。

5)　GB/T 19252-2003《电子商务协议》

该标准规定了以契约形式管理电子商务的协议样本。该标准适用于企业与企业间的电子商务，也可用于企业与消费者间的电子商务，但由于本标准未考虑任何有关保护消费者的条款，而消费者保护法通常是强制性的，并在大多数情况下，一旦与消费者达成交易，消费者所在国和所在地的国家级和地方性的消费者保护法就会立即对其适用，因此，采用本标准与消费者订立合同关系的企业必须认识到要遵守国家和地方的消费者保护法。此外，如果该标准被用于与行政或官方机

构的电子商务，应进行适当修改。

6) GB/T 18769-2003《大宗商品电子交易规范》

该标准规定了大宗商品现货电子交易的参与方要求和电子交易的业务程序。该标准适用于现货领域的大宗商品电子交易活动，尤其是现货批发市场开展电子交易活动，不适用于期货交易。

7) GB/T 20520-2006《信息安全技术 公钥基础设施时间戳规范》

该标准规定了时间戳系统部件组成、时间戳的管理、时间戳的格式和时间戳系统安全管理等方面的要求。该标准适用于时间戳系统的设计和实现，时间戳系统的测试和产品采购亦可参照使用。

8) GB/T 25064-2010 《信息安全技术 公钥基础设施 电子签名格式规范》

该标准针对基于公钥密码学生成的数字签名类型的电子签名，定义了电子签名与验证的主要参与方、电子签名的类型、验证和仲裁要求。本标准还规范了电子签名的数据格式，包括基本数据格式、验证数据格式、签名策略格式等。该标准适用于电子签名产品的设计和实现，同时相关产品的测试、评估和采购亦可参照使用。

9) GB/T 36298-2018《电子合同订立流程规范》

该标准规定了电子合同订立的原则，电子合同的订立业务及业务流程，身份登记、身份认证、电子合同签署的业务流程及描述，电子合同查询、下载和验证的业务流程及描述，电子合同辅助业务流程以及扩展方法。

该标准适用于第三方电子合同服务平台的建设和开发，以及合同双方、三方或多方通过第三方平台签署电子合同的活动。以其他方式订立电子合同业务也可参照执行。

10) GB/T 36319-2018《电子合同基础信息描述规范》

该标准规定了电子合同基础信息的术语和定义、信息描述属性和方法、信息模型、摘要描述以及信息扩展方法。该标准适用于对电子合同基础信息的交换、查询、存储和管理等。

11) GB/T 36320-2018《第三方电子合同服务平台功能建设规范》

该标准规定了第三方电子合同服务平台的建设原则、功能框架以及功能基本要求。该标准适用于第三方电子合同服务平台功能的设计、开发、实施和维护。

12) GB/T 39321-2020《电子合同取证流程规范》

本标准规定了电子合同取证的原则、业务流程及描述，包括电子合同取证的申请、受理、提取、验证以及出证。本标准适用于第三方电子合同取证服务机构按照规范流程提供取证服务，以及委托方通过第三方服务机构申请取证的活动。

13) SB/T 10519-2009《网络交易服务规范》

该标准针对电子商务 B2B、B2C 和 C2C 模式的特点，规定了各模式中网络交易方、网络交易平台提供商、网络支付平台提供商和网络交易辅助服务提供商的行为服务规范。该标准适用于中国境内所有的网络交易服务行为。

14) 《互联网信息服务管理办法》（国务院令第 292 号）

该办法是为了规范互联网信息服务活动，促进互联网信息服务健康有序发展而颁发的。其中，互联网信息服务指通过互联网向上网用户提供信息的服务活动。在中华人民共和国境内从事互联网信息服务活动，必须遵守本办法。

15) 《电子认证服务管理办法》（工业和信息化部令第 1 号）

该办法规范了电子认证服务行为，对电子认证服务提供者实施监督管理。在中华人民共和国境内设立电子认证服务机构和为电子签名提供电子认证服务，适

用本办法。中华人民共和国工业和信息化部（简称“工业和信息化部”）依法对电子认证服务机构和电子认证服务实施监督管理。

16) 《信息安全等级保护管理办法》（公通字[2007]43 号）

该办法是由四部委颁发的，为规范信息安全等级保护管理，提供信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设而制定。该办法对信息系统安全等级保护工作的范围、等级划分与保护、等级保护的实施与管理进行了明确的规定。

17) GM/T 0054-2018《信息系统密码应用基本要求》

该标准规定了信息系统商用密码应用的基础要求。适应于指导、规范和评估信息系统中的商用密码应用。

18) GM/T 0070-2019 《电子保单密码应用技术要求》

本标准描述了保险行业电子保单业务的密码应用需求，规定了电子保单的投保、签发、存储、验证、递送等电子保单管理主要环节的密码应用技术要求，本标准可为电子保单的密码应用提供指导 。

19) 《互联网金融个体网络借贷电子合同安全规范》

该标准提供了互联网络金融网络借贷信息中介从业机构（以下称“从业机构”）在开展网络借贷信息中介业务活动中，当事人在中华人民共和国境内通过互联网在线订立电子合同时采用可靠的电子签名，保证订立后的电子合同满足防篡改、抗抵赖性等各项安全要求，以提高通过此种方式订立的电子合同的安全性和证据效力。该标准适用于指导从业机构开展网络借贷信息中介业务活动时使用电子签名技术对电子合同进行在线订立，并将订立后的电子合同进行第三方存储，进一步满足互联网金融个体网络借贷行业安全性及合法合规性要求。

4.2.2 服务平台使用的密码技术层面

自 2012 年以来，国家密码管理局陆续发布了由我国制定的密码技术标准，已发布密码行业标准近 142 项，范围涵盖了基础密码算法、密码应用协议、密码设备接口等多个方面，已经初步形成体系化的密码技术标准，基本能够满足我国社会各行业在构建信息安全保障体系时的应用需求。

密码标准体系框架由三个维度组成如图 4-3，包括技术维、管理维、应用维，从技术维分：密码基础类标准、基础设施类标准、密码产品类标准、应用支撑类标准、密码应用类标准、密码检测类标准和密码管理类标准七大类密码标准，每一大类又细分若干子类。

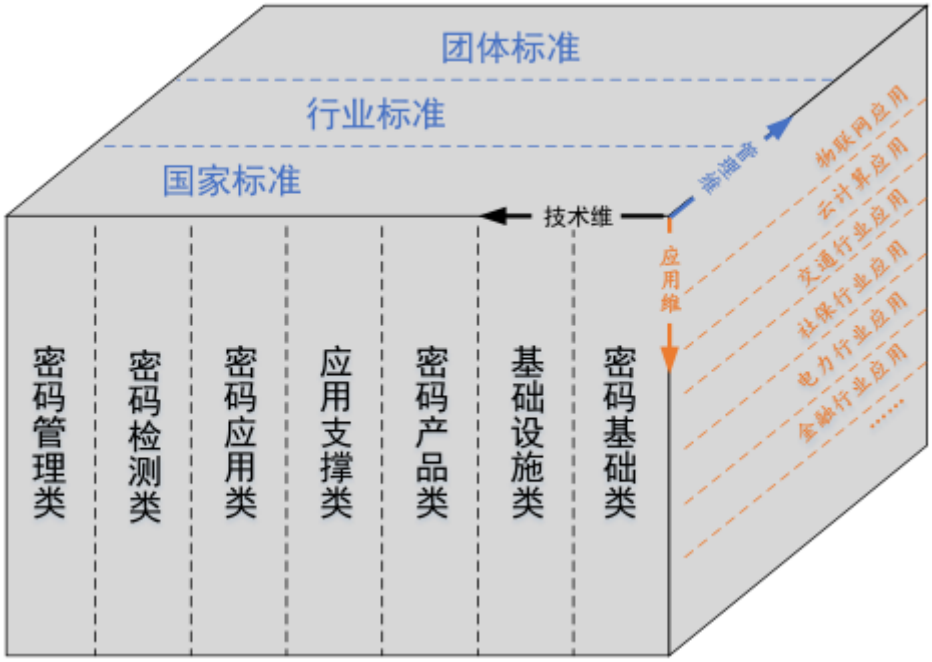

图 4-3　密码标准体系框架图

密码基础类标准主要对通用密码技术进行规范，它是体系框架内的基础性规范，主要包括密码术语与标识标准、密码算法标准、密码设计与使用标准、密码协议标准等。

基础设施类标准主要针对密码基础设施进行规范，包括：证书认证系统密码协议、数字证书格式、证书认证系统密码及相关安全技术等。目前已颁布的密码标准只涉及公钥基础设施，未来可能还会出现标识基础设施等其他密码基础设施类标准。

密码产品类标准主要规范各类密码产品的接口、规格以及安全要求。对于智能密码钥匙、VPN、安全认证网关、密码机等密码产品给出设备接口、技术规范和产品规范；对于密码产品的安全性，则不区分产品功能的差异，而以统一的准则给出要求；对于密码产品的配置和技术管理架构，则以 GM/T 0050《密码设备管理 设备管理技术规范》为基础统一制定。

应用支撑类标准针对密码报文、交互流程、调用接口等方面进行规范，包括通用支撑和典型支撑两个层次。通用支撑规范（GM/T 0019）通过统一的接口向典型支撑标准和密码应用标准提供加解密、签名验签等通用密码功能，典型支撑类标准是基于密码技术实现的与应用无关的安全机制、安全协议和服务接口，如可信计算可信密码支撑平台接口、证书应用综合服务接口等。

密码应用类标准是对使用密码技术实现某种安全功能的应用系统提出的要求以及规范，包括应用要求、应用指南、典型应用和密码服务三类。应用要求旨在规范社会各行业信息系统对密码技术的合规使用。应用指南用于指导社会各行业建设符合密码应用要求标准的信息系统。典型应用定义了具体的密码应用，如动态口令、安全电子签章等，典型应用类标准也包括其它行业标准机构制定的跟行业密切相关的密码应用类标准，如 JR/T 0025《中国金融集成电路（IC）卡规范》中，对金融 IC 卡业务过程中的密码技术应用做了详细规范。密码服务类则用以规范面向公众或特定领域提供的各类密码服务，截止 2020 年 5 月该类标准

暂时空缺，具体如下图：

大类	一级子类	二级子类	密码行业标准	密码国家标准
密码应用类	应用要求		GM/T 0054-2018 信息系统密码应用基本要求	
			GM/T 0070-2019 电子保单密码应用技术要求	
			GM/T 0072-2019 远程移动支付密码应用技术要求	
			GM/T 0073-2019 手机银行信息系统密码应用技术要求	
			GM/T 0074-2019 网上银行密码应用技术要求	
			GM/T 0075-2019 银行信贷信息系统密码应用技术要求	
			GM/T 0076-2019 银行卡信息系统密码应用技术要求	
			GM/T 0077-2019 银行核心信息系统密码应用技术要求	
	典型应用		GM/T 0021-2012 动态口令密码应用技术规范	
			GM/T 0031-2014 安全电子签章密码技术规范	
			GM/T 0035-2014（所有部分） 射频识别系统密码应用技术要求	GB/T 37033-2018（所有部分） 信息安全技术 射频识别系统密码应用技术要求
			GM/T 0036-2014 采用非接触卡的门禁系统密码应用技术指南	
			GM/T 0055-2018 电子文件密码应用技术规范	
			GM/T 0071-2019 电子文件密码应用指南	

图 4-4　密码应用类标准体系框架

密码检测类标准针对标准体系所确定的基础、产品和应用等类型的标准出台对应检测标准，如针对随机数、安全协议、密码产品功能和安全性等方面的检测规范。其中对于密码产品的功能检测，分别针对不同的密码产品定义检测规范；对于密码产品的安全性检测则基于统一的准则执行。

密码管理类标准主要包括国家密码管理部门在密码标准、密码算法、密码产业、密码服务、密码应用、密码监查、密码测评等方面的管理规程和实施指南。

4.2.3 小结

如上所述，目前对电子合同的标准规范体系主要集中在法律标准、基础信息标准、平台功能规范。电子合同安全规范，在密码标准体系中，也无明确的描述第三方电子合同服务平台中的密码应用技术要求或标准规范。因此通过对本项目的研究，提出第三方电子合同服务平台密码应用技术的规范，为电子合同的平台建设提供参考和指引具有重要的意义。

4.3 发展趋势

随着电子商务的蓬勃发展，特别大湾区的政策扶持，网络交易日益增多，人们对网络商业交易的标准化和规范性提出了更高的要求，此外，移动互联网和云计算时代的到来，使得电子合同的发展也越来越趋于移动化、远程化、在线化，随之而来的安全性问题也越来越受到社会各界的关注。因此，电子合同的未来趋势是需要建立一套健全的规范体系，需要加强电子合同的相关技术方面的创新，为电子合同从生产到消亡的整个生命周期提供强有力的技术保障。

5. 密码应用技术研究

5.1 需求分析

5.1.1 电子合同面临的问题

电子合同的本质还是合同，是用于保障签约主体的合法权益，维护契约精神。但是由于电子合同签署环境和签署方式发生了较大的变化，用户对电子合同的需求和认识度也在逐步提升，因此在网络环境实现电子合同签署服务还面临以下问题需要解决。

1) 面临真实性、完整性、不可否认性的挑战

案例一：四川省成都市青白江区人民法院在 2018 年审理的一起民间借贷纠纷，就是一起个人运用电子合同的真实案例：被告颜某，因房屋装修急需资金，通过中介向北京市一家投资管理公司借取了一笔房屋装修资金，并通过电子合同缔约，这份电子合同成为了后来法院作出判决的事实依据。（电子合同的合法性）

案例二：一位刚上小学二年级的男童，在某购物网站以他父亲李某的身份证号码注册了客户信息，并且订购了一台价值 1000 元的小型打印机。但是当该网站将货物送到李某家中时，曾经学过一些法律知识的李某却以“其子未满 10 周岁，是无民事行为能力人”为由，拒绝接收打印机并拒付货款。由此交易双方产生了纠纷。

李某主张，电子商务合同订立在虚拟的世界，但却是在现实社会中得以履行，应该也能够受现行法律的调控。而依我国现行《民法通则》第 12 条第 2 款和第 55 条的规定，一个不满 10 周岁的未成年人是无民事行为能力人，不能独立进行民事活动，应该由他的法定代理人代理民事活动。其子刚刚上小学二年级，未满 10 周岁，不能独立订立货物买卖合同，所以该打印机的网上购销合同无效；其父母作为其法定代理人有权拒付货款。

对此，网站主张：由于该男童是使用其父亲李某的身份证登录注册客户信息的，从网站所掌握的信息来看，与其达成打印机网络购销合同的当事人是一个有完全民事行为能力的正常人，而并不是此男童。由于网站是不可能审查身份证来源的，也就是说网站已经尽到了自己的注意义务，不应当就合同的无效承担民事责任。（电子合同签署过程的真实性、完整性、不可否认性受到挑战）。

案例三：中国北京 A 公司与美国纽约一家公司一直有业务来往，近年来随着计算机网络的发展，双方越来越多地通过电子邮件进行商务活动。2000 年 6 月 1 日上午，北京时间 9 点，北京公司通过电子邮件向纽约公司发盘，出售 400 吨咖啡豆，每吨价格 1800 美元。该邮件还称，本发盘的有效期为一个星期。纽约时间 6 月 1 日上午，纽约公司职员在打开公司电脑后发现了北京公司的发盘，遂派业务员汤姆负责了解同类咖啡豆的市场情况。6 月 7 日，纽约公司经过研究认为北京公司的发盘条件可以接受，电话指示汤姆发出接受通知。当时汤姆正在前往加拿大出差途中，因而汤姆至纽约时间当天晚上 8 时许在加拿大蒙特利尔市，用自己携带的手提电脑给北京公司的另一个电子邮件信箱发出了接受发盘的电子邮件通知，并表示其已作好履行合同的准备。北京公司发现纽约公司发来的邮件时是北京时间 6 月 9 日上午 11 时许，电脑显示的接收时间是北京时间 6 月 8 日上午 8 时 22 分。这时，北京公司知悉国际市场上咖啡豆的价格已经开始上涨，

于是向纽约公司发出通知，将该批咖啡豆的价格提高至 2000 美元/吨。纽约公司回邮拒绝接受，要求北京公司按合同履行其交货义务。后北京公司将该批咖啡豆以 2300 美元/吨的价格卖给了美国的另外一家公司。纽约公司遂向北京法院起诉，要求北京公司赔偿其损失；北京公司则辩称，其与纽约公司之间的合同并未成立，在没有合同关系的情况下，纽约公司的索赔缺乏依据。（电子合同签署过程和数据的真实性、完整性、不可否认性受到挑战）。

上述三个案例显示，当前国内电子合同的合法性已经获得法律层的保护，但是在合同签署过程和数据的安全性、完整性、真实性、不可否认性等方面，还有很大的提升空间，这也是国内企业用户选择电子合同服务平台时首要考虑的因素。

2018年国内企业用户选择电子签名平台首要考虑因素

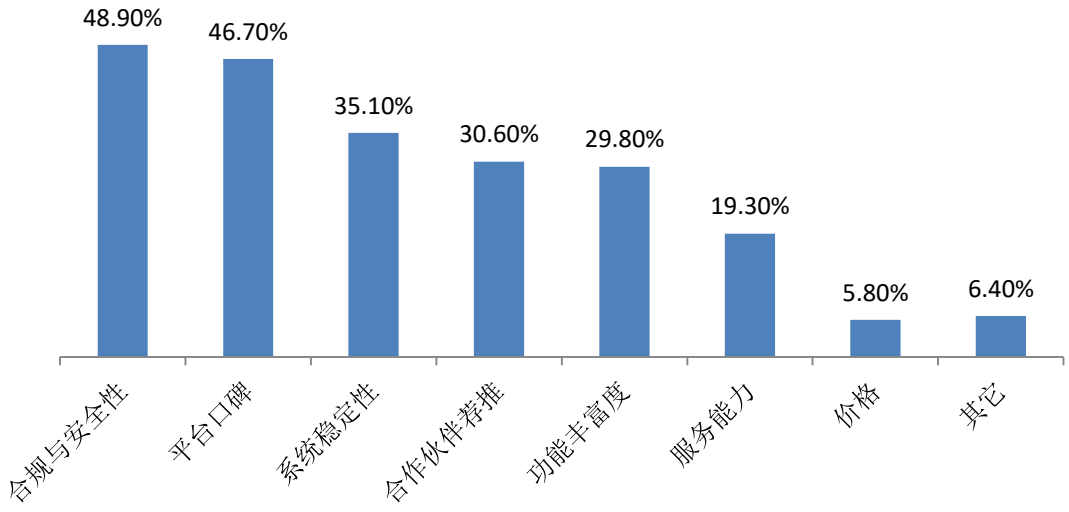

图 5-1　2018 年国内企业用户选择电子签名平台首要考虑因素

调查数据显示，48.9%的国内企业在选择电子合同服务平台时考虑的首要因素是合规与安全性。根据《电子签名法》的规定，“电子签名平台必须要具备相关资质，具有符合国家安全标准的技术和设备”，电子签名的法律效力和安全性是用户的痛点，同时也是企业的壁垒，取得相关的资质认证和拥有维护数据安全的核心技术成为用户选择第三方电子签名服务商的关键所在。

此外，电子合同服务是支持企业级实现实时合同签署功能交付于终端用户的技术。通过后端服务平台统一存储每个终端用户的电子合同及其相关操作数据，由终端计算机或者移动设备连入服务平台来进行在线签署操作。一个形象的类比，我们可以通过任何设备、在任何地点，任何时间在网络上进行电子合同的签署。电子合同服务带来低成本，高效率的同时，依旧存在传统的信息存储、传输和使用过程中的安全风险问题。

2)　数据被破坏的风险

在电子合同服务环境下，合同签署过程必须通过互联网络来进行，而互联网体系使用的是开放式的 TCP/IP 协议它以广播的形式进行传播。容易受到计算机病毒、黑客的攻击，签署信息和数据易于搭截侦听、口令试探和窃取，给企业的数据信息安全带来极大威胁，如遭破坏或泄密，将会给电子企业、商户造成巨大的损失 。

3) 面临数据安全性挑战

由于现阶段广泛应用的主流操作系统和数据库管理系统是从国外引进直接使用的产品。核心技术还是使用引进的版本。这些系统安全性存在系统漏洞等不少危及信息安全的问题，例如：Windows 操作系统中存在着的漏洞和陷门，就不断引起世界性的“冲击波”和“震荡波”，存在极大风险，数据泄露已经成为全球最常见的威协网络安全事件之一，而且已经有愈演愈烈的趋势，云端数据面临严重威胁。系统软件安全漏洞带来的风险主要来自操作系统软件和数据库管理系统软件的安全漏洞。数据管理体系出现了缺陷，没有采用通过商用密码检测认证机构认证的加密设备，不支持符合密码相关国家标准、行业标准的算法，不具备独立于数据库的密钥管理体系，入侵者可以直接利用操作系统的漏洞窃取数据库文件，或者直接利用操作系统工具来进行非法伪造、篡改数据库文件内容，从而危及到电子合同签署的数据安全。

4) 来自社会的外来入侵风险

电子合同服务平台容易被来自社会上的不法分子通过互联网络非法入侵，主要表现形式是黑客和病毒等对电子合同服务平台和系统的文件和数据的篡改和破坏，是一种社会道德风险。黑客通过闯入他人计算机系统进行破坏，这些人利用电子合同服务平台和管理上的一些漏洞，进入计算机系统后，破坏或篡改重要数据，盗取机密与资源，控制他人的机器，清除记录。设置后门，给电子合同服务平台和系统带来灾难性的后果。计算机病毒是人为编写的一组程序，可以攻击电子合同服务平台和系统的数据区、文件和内存，以致使计算机的硬件失灵，软件瘫痪。数据破坏，系统崩溃，给企业和商户造成无法挽回的巨大损失。

5.1.2 电子合同服务平台的基本框架

根据 GB/T 36320-2018《第三方电子合同服务平台功能建设规范》的要求，企业在建设第三方电子合同服务平台时，必须满足以下条件：

1) 第三方电子合同服务平台必须独立于合同缔约人，具备身份认证、谈判磋商、电子签名、合同存储与调用等功能，能实现电子合同在线订立及处理的信息系统；

2) 第三方电子合同服务平台的功能模块必须包括：用户身份管理、电子合同业务管理、电子合同归档与存储、电子合同利用和系统维护。其中：

- 用户身份管理的功能设计应包括身份登记、身份认证、身份变更与注销等；
- 电子合同业务管理的功能设计应包括创建合同、起草合同、签署合同、变更合同、合同验证、合同谈判等等；
- 电子合同归档与存储管理的功能设计应包括电子合同归档管理、存储与备份管理；
- 电子合同利用的功能设计应包括对于电子合同的阅读打印、查询、统计等；系统维护功能设计应包括用户管理、权限管理、日志管理、分类方案管理、模板管理、接口管理以及安全管理等。

根据 GB/T 36298-2018《电子合同订立流程规范》的要求，电子合同的签订主要业务有 4 个主要业务和 4 个辅助业务。

4 个主要业务是：缔约人身份登记、缔约人身份认证、电子合同签署、电子合同查询/下载/验证；

4 个辅助业务是：缔约人身份信息变更、缔约人身份注销、电子合同变更以

及电子合同撤销。

可信电子合同必须满足以下两个条件：合同签署各方都经过实名认证，且是根据《电子签名法》认可的可靠电子签名，这份电子合同则具备和纸质合同手写签章同等的法律效力。同时根据《电子签名法》规定完成可靠的电子合同还需相关的密码功能包括：身份认证、电子签章、时间戳、加密/解密、签名/验证、密钥管理、第三方数字证书认证机构。整个基本框架如下图：

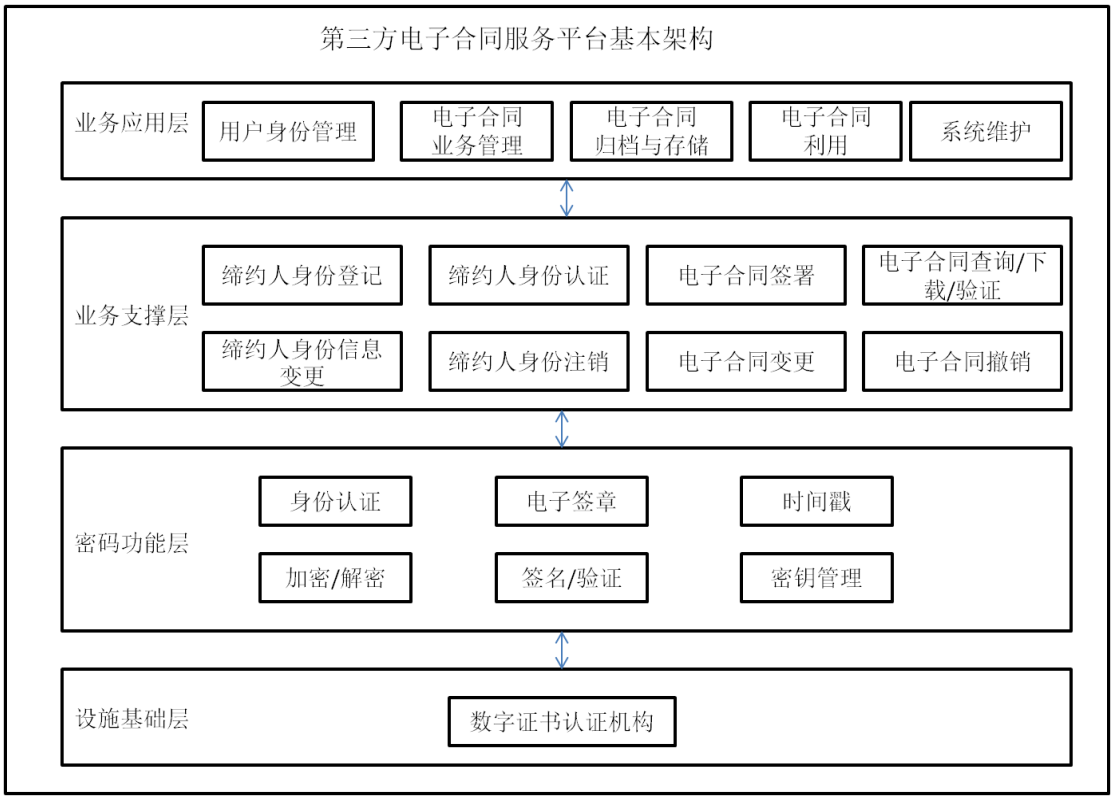

图5-2　第三方电子合同服务平台基本架构

5.1.3 密码技术需求

5.1.3.1 总体需求分析

基于上述电子合同服务平台的基本架构以及当前电子合同面临的问题，无论是电子合同服务平台还是签署流程都需要利用密码相关技术，来确保签署的电子合同合法合规，保证电子合同服务平台的数据机密性、真实性、完整性、不可否认性。

1)　机密性

机密性，保证信息不被泄露给非授权的个人、进程等实体的性质。使用密码加密功能实现机密性，确保电子合同服务平台中以下内容得到保护：传输的重要数据、敏感信息数据或整个报文、存储的重要数据和敏感信息数据、身份鉴别信息、密钥数据。

2)　真实性

真实性，确保主体或资源的身份正是所声称的特性。为保证电子合同服务平台的合同签署数据真实性，需要在以下场景中使用对称加密、动态口令、数字签名等技术实现数据的真实性：通信双方的身份鉴别、采用可信计算技术的平台身份鉴别、登录操作系统和数据库系统的用户身份鉴别、应用系统的用户身份鉴别。

3) 完整性

完整性，数据没有遭受以非授权方式所作的篡改或破坏的性质。为保证电子合同服务平台数据完整性，需要使用数字签名技术实现完整性，确保电子合同服务平台中以下内容得到保护：传输的重要数据、敏感信息数据或整个报文、存储的重要数据和敏感信息数据、身份鉴别信息、密钥数据、日志记录、访问控制信息；重要信息资源敏感标记、重要程序、采用可信计算技术建立从系统到应用的信任链。

4) 不可否认性

不可否认性，证明一个已经发生的操作行为无法否认的性质。为保证电子合同服务平台数据和用户身份的不可否认性，需要使用数字签名等密码技术让电子合同服务平台中的发送、接收、审批、创建、修改、删除、添加、配置等操作的实体行为具有不可否认性。

5.1.3.2 基础需求分析

电子合同服务平台属于信息系统，根据 GM/T0054-2018《信息系统密码应用基本要求》、GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》和 GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》的相关规定，确保平台的安全性。

1) 物理和环境安全需求

- 确保对机房等重要场所、监控设备等物理访问控制安全；
- 确保对物理访问控制记录、监控信息等物理和环境敏感信息数据实施完整性保护。

2) 网络和通信安全需求

- 确保对连接到内部网络的设备进行安全认证；
- 确保对通信双方身份进行认证；
- 确保通信过程中数据的完整性；
- 确保通信过程中敏感数据字段或整个报文的机密性；
- 确保网络边界控制信息、系统资源访问控制信息的完整性；
- 建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理。

3) 设备和计算安全需求

- 确保对登陆的用户进行身份鉴别；
- 保证系统资源访问控制信息的完整性；
- 保证重要信息资源敏感标记的完整性；
- 保证程序或文件的完整性；
- 保证日志记录的完整性。

4) 应用和数据安全需求

- 保证重要数据在传输过程中的机密性和完整性；
- 保证重要数据在存储过程中的机密性和完整性；
- 对重要程序的加载和卸载进行安全控制；
- 实现对实体行为的不可否认性。

5) 密钥管理系统需求

密钥管理系统是提供密钥安全的基础性硬件和软件保障。在电子合同服务环境中，密钥安全仍是整个安全体系的关键，数据加密、合同签署、身份认证与访

问控制等技术，都需要密钥管理系统的技术支持。

构建安全的密钥管理、密钥监管、密钥维护等机制，对电子合同服务环境下密钥管理系统的正常运行至关重要，系统中的密钥分发、密钥协商、密钥保存、安全加密等需要和电子合同服务紧密相关，在综合考虑 USB-KEY、防篡改模块、智能卡、密钥分割、密钥恢复等技术的应用同时，还需要结合电子合同服务环境的灵活性、实时性的特点和具体业务展开研究和部署。

国内外关于电子合同服务环境下密钥管理研究还存在很多问题，具体表现在两个方面：①各电子合同服务提供商对已有国际/国家标准执行力较弱，所使用的密码技术规范、标准、应用模式和部署方式都有所不同，电子合同服务安全相关标准还处于研讨过程中，因此电子合同服务环境下密钥管理规范亟待确定；②传统的密码体制、密钥技术在电子合同服务环境下的应用遇到阻碍，新兴的密码技术（如同态加密、属性加密、量子密码）尚停留在理论探索阶段，在电子合同服务领域中成功应用部署还需要一定的时间和工作，针对电子合同服务具体应用场景仍需探索。

5.1.3.3 业务需求分析

1) 用户身份登记

电子合同要约人、电子合同受要约人都属于电子合同服务平台的用户。在用户身份登记过程中，若用户已持有可信第三方 CA 颁发的数字证书，则需要在电子合同服务平台中将该数字证书与用户进行绑定，绑定时需要验证数字证书的有效性、数字证书的格式及密码算法应符合国家密码主管部门的相关规定；若用户尚无可信第三方 CA 颁发的数字证书，则用户需要向电子合同服务平台提交可信身份信息，提交过程中涉及的重要敏感信息需要在传输过程中进行加密保护，加密方法应符合国家密码主管部门规定的密码算法要求。

2) 用户身份认证

用户身份认证的过程需要满足国家的相关实体鉴别规范，规范中所使用的密码算法应符合国家密码主管部门规定的密码算法要求。

3) 合同签署申请

只有用户身份认证成功后才能在电子合同服务平台上发起合同签署申请。发起合同签署申请后，用户与电子合同服务平台之间需要建立起加密通道，加密方法应符合国家密码主管部门规定的密码算法要求。

4) 合同创建

只有用户发起合同签署申请成功后才能创建合同，合同数据需要通过加密通道传输到电子合同服务平台。

5) 合同签署

电子合同服务平台需要首先与用户建立起加密通道后，才能通过加密通道将待签署的合同发送或者展现给用户。需要建立必要的密钥管理机制，保证只有用户本人或者获得用户授权的人才能调用相应的签名私钥。在签署合同时，应当验证签名私钥对应的数字证书的有效性，数字证书无效应拒绝合同签署。除此之外，签署合同时需要加入时间戳，以保证签署的时效性。

6) 合同验证

需要验证合同的电子签名的有效性、时间戳的有效性、签署时数字证书的有效性。

7) 合同归档

需要支持明文归档和密文归档两种方式。密文归档的合同只有给定权限的用户才能解密查看。密文归档方法应符合国家密码主管部门规定的密码算法要求。

5.2 电子合同服务平台密码技术框架

5.2.1 技术框架-业务角度

根据前面电子合同服务平台各项业务对密码技术的需求，从业务角度可对电子合同服务平台的密码技术提出以下技术框架。

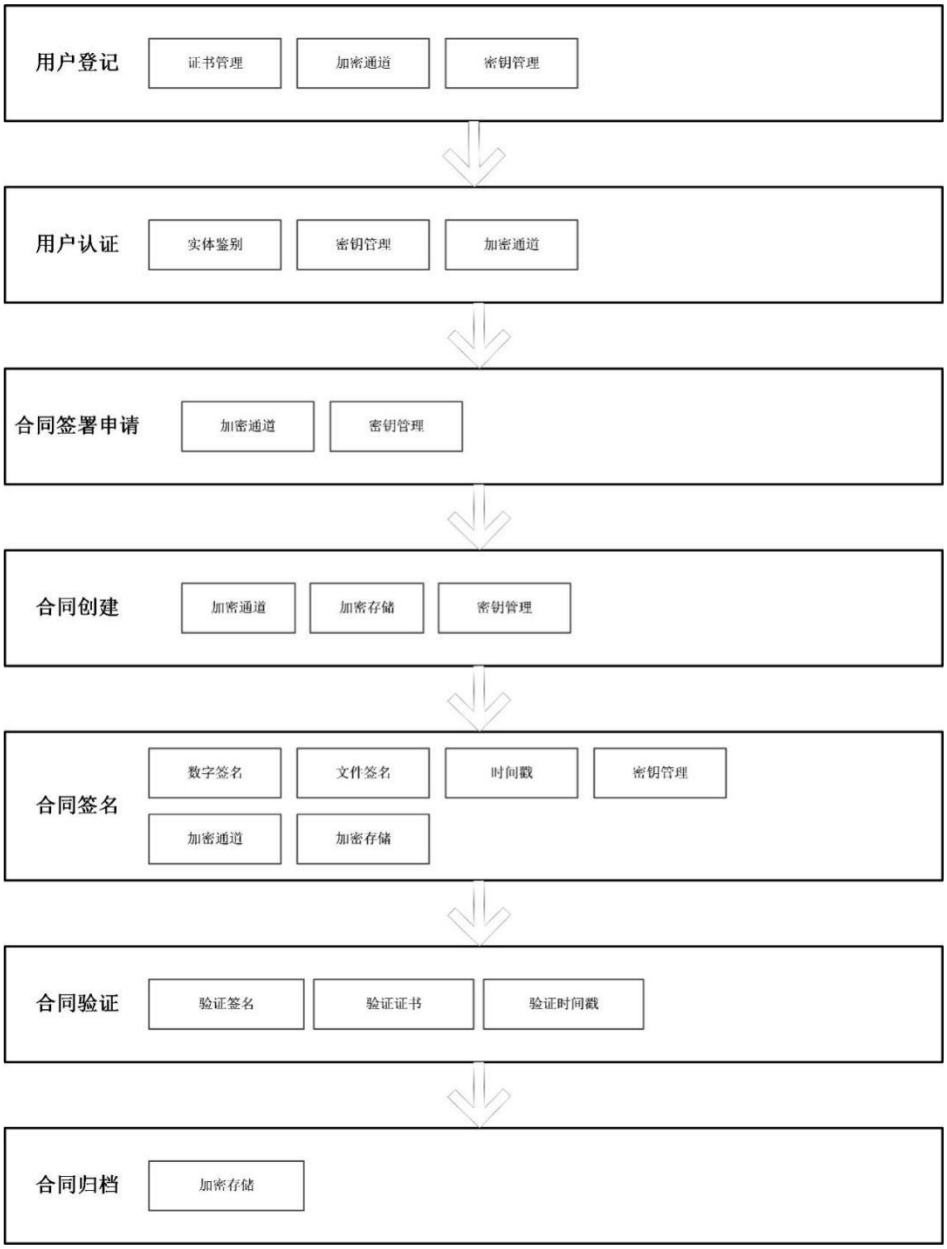

图 5-3　电子合同密码技术框架图-业务角度

1)　证书管理

根据不同的业务场景，可向 CA 机构申请长期证书或短期事件证书。申请长期证书时，需要用户向 CA 机构提交可信的身份资料，CA 机构对身份资料进行审核，只有审核成功后才能向用户颁发较长期限的数字证书（通常为一年）。申请

短期事件证书时，用户只需向 CA 机构提交当前的事件信息，如：身份证照片、指纹照片、手写签名图片等，CA 对当前的事件信息审核通过后向用户颁发期限极短的数字证书（通常为 24 小时）。

2) 密钥管理

根据不同的业务场景，需要产生、存储、调用、更新、销毁各种密钥。密钥管理的基础是基于密码模块，密码模块可分为：移动端密码模块、PC 端密码模块、服务端密码模块。密码模块的安全性应满足国家的相关规范。

3) 加密通道

根据不同的业务场景，加密通道可以通过 SSL 技术或数字信封技术来实现。SSL 是基于网络传输的加密通道，优点是能对网络传输的所有业务数据都进行加密保护，缺点是支持 SM 系列密码算法的 SSL 还不普及。数字信封技术是对特定数据的加密保护，优点是能成熟的支持 SM 系列密码算法，缺点是在实现过程中可能会遗漏对某些业务数据的加密保护。

4) 加密存储

根据不同的业务场景，加密存储可分为字段加密、文件加密、目录加密、文件系统加密。字段加密通常是对极少量的关键数据进行加密，加密结果存储在密码设备或者数据库中。文件加密是对整个文件的数据进行加密，加密结果存储在数据库或者文件系统中。目录加密是对文件系统中某个目录下的所有文件进行加密，加密后存放在文件系统中。文件系统加密是对整个文件系统中的所有文件进行加密

5) 用户认证

根据不同的业务场景，对已持有证书用户的实体鉴别可使用数字签名技术的机制或者使用零知识技术的机制；对未持有证书用户的实体鉴别可使用数字签名技术的机制或者使用对称加密算法的机制。

6) 数字签名

根据不同的业务场景，可使用不同的签名算法进行数字签名，常用的签名算法主要是 RSA 算法和 SM2 算法。签名时需要通过 OCSP 或者 CRL 验证签名证书是否有效，只有有效的签名证书才能签名。

7) 时间戳

必须使用可信的时间戳服务器为文件签发时间戳，其中的时间信息来自国家可信时间源。

8) 文件签名

根据不同的业务场景，合同文件可能存在不同的文件格式，对常用文件格式的签名包括：PDF 签名、OFD 签名、XML 签名、微软 Office 文件签名。签名过程中根据不同的文件格式，将签名结果、签名外观、时间戳等合成到文件中。

9) 验证签名

验证文件内容是否被篡改。

10) 验证时间戳

验证时间戳签名是否有效，验证时间戳的签名证书是否为可信的第三方 CA 签发。

11) 验证证书

验证签名证书是否为可信的第三方 CA 签发。验证时间戳中的时间是否处于签名证书的有效期内。

5.2.2 技术框架-安全角度

基于主流的第三方电子合同服务平台的四个基本环节：实名认证、合同签署、合同存证、司法落地等环节，为了保障合同签署过程的合规性与安全性，从安全角度可对电子合同服务平台的密码技术提出以下技术框架。

图 5-4　电子合同密码技术框架图-安全角度

1)　密码设备

服务端密码模块：包括软件密码模块和硬件密码模块，提供服务端的密钥生成、公钥导出、私钥计算、会话密钥计算等功能；

客户端密码模块：包括软件密码模块和硬件密码模块，提供客户端的密钥生成、公钥导出、私钥计算、会话密钥计算等功能。

2)　密码基础设施

RA 系统：对用户资料进行审核；

CA 系统：为用户签发数字证书。

3)　用户安全

用户身份认证：通过用户名密码、PIN 码、指纹识别、人脸识别等方式认证用户身份；

用户特征数据采集：采集用户的身份证正反面照片、营业执照照片等可用于标识用户真实身份的特征数据；

用户与密钥绑定：通过为用户所持有的密钥对签发数字证书实现用户身份与密钥的绑定。

4)　网络安全

网络传输加密：对网络上传输的数据进行加密，包括密钥协商、数据加密、

数据解密等；

网络传输完整性保护：对网络上传输的数据通过数字签名、消息鉴别码等技术进行完整性保护；

网络传输身份验证：验证数字签名中的数字证书是否为可信的第三方 CA 机构签发，验证通过后提取数字证书中的信息作为身份验证中的依据。

5) 数据安全

文档存储加密：多种数据层面的加密，包括基于磁盘的加密、基于文件系统的加密、基于文件目录的加密、基于单个文档的加密、基于文档部分关键数据的加密等；

文档访问控制：控制哪些用户可以执行文档的读、写、创建、删除操作；

密钥存储加密：托管密钥的加密，包括使用密码模块中的密钥对托管密钥进行加密、使用基于用户口令生成的密钥对托管密钥进行加密等；

密钥访问控制：控制哪些用户可以执行托管密钥的私钥计算、密钥更新、创建、删除操作；

用户身份验证：验证用户是否为电子合同服务平台的合法用户；

用户授权管理：管理用户在电子合同服务平台上的各种权限，包括文档访问控制权限、密钥访问控制权限等；

可信证据生成：将签名后的电子合同上传到第三方证据平台。

5.2.3 技术框架-部署角度

电子合同服务平台既可以通过公有云，也可以通过私有云进行部署；同时可根据业务的需求采用高可用（集群）模式，也可以单机模式；可以物理机也可以虚拟机，但从整个平台的密码技术的应用角度上看，其简要技术框架如下：

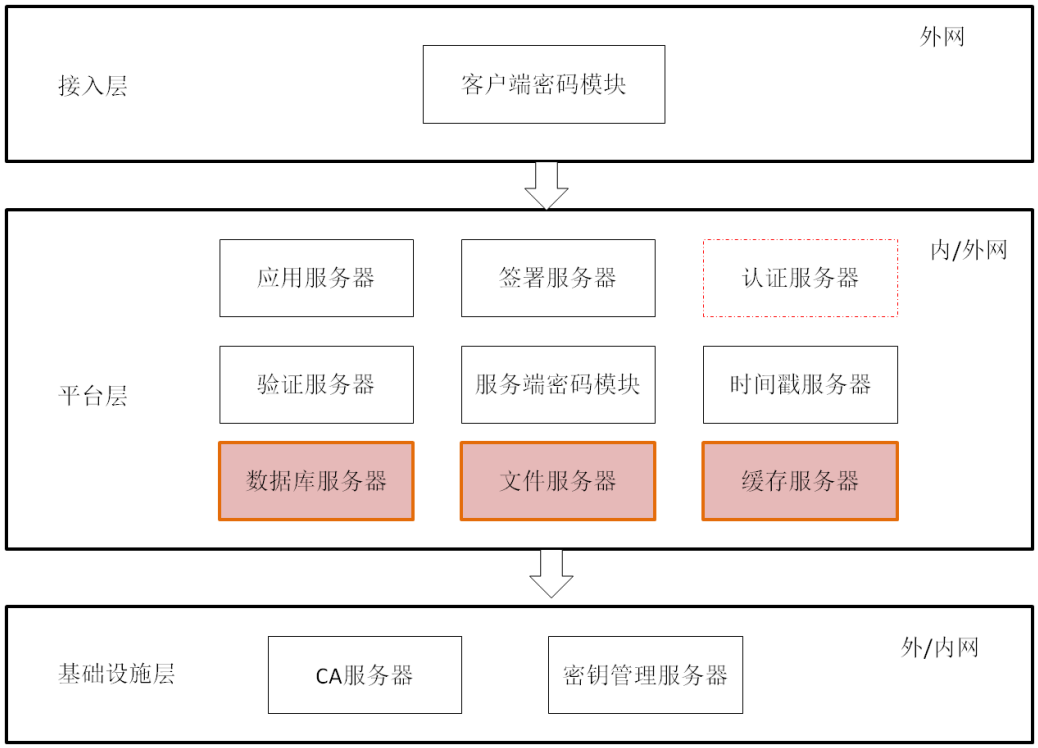

图 5-5 电子合同密码技术框架图-部署角度

1) **接入层：**指用户通过 PC 端或是移动端接入到平台，由客户端密码模块

（包括软件密码模块和硬件密码模块）提供客户端的密钥生成、公钥导出、私钥计算、会话密钥计算等功能，属于外网。

2) **平台层**：包括应用服务器、签署服务器、认证服务器、验证服务器、服务密码模块、时间戳服务器，以及存储服务器（数据库服务器、文件服务器、缓存服务器），整个平台层构建于局域网内，并对外提供相关的应用服务，且基于 https 协议与接入层进行信息交互。如果平台不能提供权威的认证服务、电子印章等服务，则可通过 https 等接入第三方权威机构，由第三方提供相应的服务。

3) **基础设施层**：包括 CA 服务器和密钥管理服务器，一般由第三方权威机构提供。如果平台层与基础设施层是同一个机构，则平台层与基础设施层可以通过内网访问，否则需通过 https、专线、VPN 等来保证数据链路的安全。

5.2.4 小结

综合上述的分析对于电子合同服务平台的密码应用主要包括 2 个层面：基础密码应用技术和业务密码应用技术，总体框架如下：

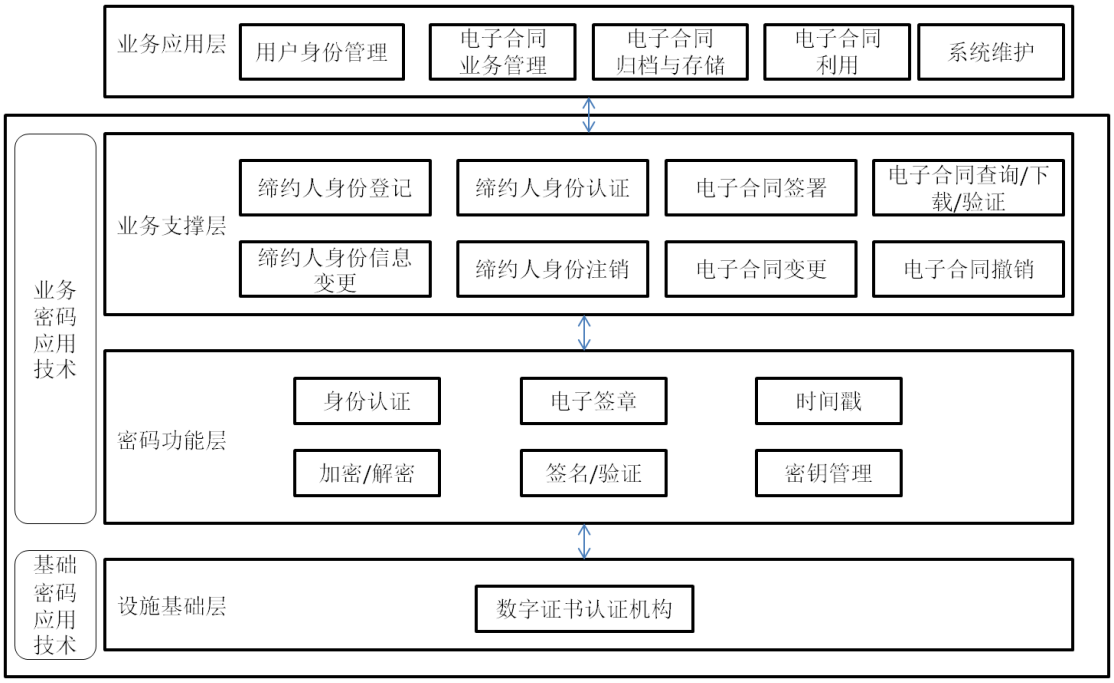

图 5-6　电子合同服务平台密码应用技术框架

基础密码应用技术：GM/T0054-2018《信息系统密码应用基本要求》、GB/T22239-2019《信息安全技术 网络安全等级保护基本要求》和 GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》已经做了明确的要求和规范，根据上述的要求，通过对基础层的密码应用，可确保基础层安全可靠，这里不再阐述。

业务密码应用技术：由于无相关的要求、规范和标准，因此通过上述的分析，采用下面的技术手段来进行实现，最终形成技术要求和规范，形成指导性文件，也是本课题研究的核心目标。

5.3 电子合同服务平台密码应用技术实现

5.3.1 业务流程的技术路线

5.3.1.1 电子合同服务平台密码技术路线

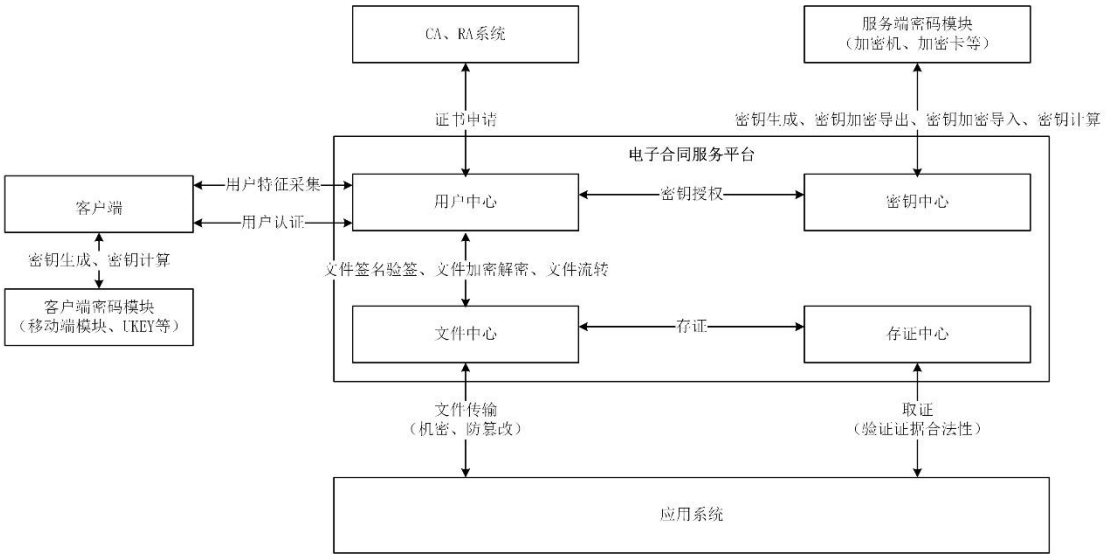

图 5-7　电子合同服务平台密码技术路线

下面以电子合同服务平台的典型的业务流程来对上图中的技术路线进行说明。根据 GB/T 36298-2018 电子合同订立流程规范，电子合同服务平台典型的业务包括：身份登记、身份认证、合同签署申请、创建合同文本、电子签名、形成电子合同数据、发送/接收电子合同数据、电子合同存储、电子合同查询、电子合同下载、电子合同验证。

5.3.1.2 身份登记中的密码技术

身份登记可分为个人身份登记和机构身份登记。为了能实现电子合同的数字签名，通常都在身份登记过程中为个人和机构生成密钥和数字证书。身份登记过程中提交个人和机构的信息到平台时需要使用加密通道技术保证信息交互的安全。

1)　个人身份登记

个人第一次使用电子合同服务平台时，需要在平台上登记。个人通过用户特征采集向用户中心提交个人的真实身份信息，如：身份证照片、人脸活体视频等。用户中心验证通过后，通知个人使用客户端上的客户端密码模块产生密钥对并获取用户公钥，用户中心向 CA、RA 系统发起证书申请。用户中心收到 CA、RA 系统返回的数字证书后，将该数字证书与用户账号进行关联。数字证书的生成、分发、使用和管理将用到 PKI 技术。

2)　机构身份登记

机构第一次使用电子合同服务平台时，需要在平台上登记。机构通过用户特征采集向用户中心提交机构的真实身份信息，如：营业执照原件复印件、授权人身份证信息等。用户中心验证通过后，可根据机构密钥的不同持有方式来分别进行后续的流程。

- **机构直接持有密钥的方式**：用户中心验证通过后，通知机构的代表人使用客户端上的客户端密码模块产生密钥对，并获取用户公钥，用户中心向 CA、RA 系统发起证书申请。用户中心收到 CA、RA 系统返回的数字证书后，将该数字证书与用户账号进行关联。数字证书的生成、分发、使用和管理将用到 PKI 技术。
- **机构将私钥托管在密钥中心的方式**：用户中心通知密钥中心调用服务端密码模块产生密钥对，并获取公钥，用户中心向 CA、RA 系统发起证书申请。用户中心收到 CA、RA 系统返回的数字证书后，将该数字证书与用户账号进行关联。服务端密码模块将私钥加密导出后返回给密钥中心，密钥中心将私钥索引号返回给用户中心。用户中心将该索引号与用户账号进行关联。私钥托管方式需要用到私钥托管技术。

5.3.1.3 身份认证中的密码技术

身份认证技术主要应用于用户注册时身份认证及签署时的身份意愿认证，所以电子合同服务平台需提供多种身份认证手段，如下所示：

1) 通过姓名、身份证号方式实现个人用户身份认证；
2) 通过姓名、身份证号、手机号方式实现个人用户身份认证；
3) 通过姓名、身份证号、手机号、银行卡号方式实现个人用户身份认证；
4) 通过人脸识别方式实现个人用户身份认证；
5) 通过企业信息查询方式实现企业用户身份认证；
6) 通过对公打款认证方式实现企业用户身份认证；
7) 通过口令密码、短信验证码、人脸识别、Ukey 认证等方式实现签署意愿身份认证。

根据 GB/T 36298-2018 电子合同订立流程规范，电子合同服务平台必须要支持基于数字证书的身份认证。基于数字证书的身份认证将用到随机数技术、数字证书技术、非对称密码签名验签技术、OCSP 技术、CRL 技术。

5.3.1.4 合同签署申请、创建合同文本中的密码技术

电子合同要约人向电子合同服务平台提交电子合同签署申请，电子合同服务平台受理申请后，建立加密通道后，由电子合同要约人创建合同文本，并将创建后的电子合同文本提交到电子合同平台。合同签署申请中需要使用加密通道技术保证信息交互的安全。

5.3.1.5 电子签名中的密码技术

电子合同通常会使用某种特定的文件格式来组织电子合同数据，常用的文件格式为 PDF 格式、OFD 格式、XML 格式等，对这些文件格式的电子签名需要用到文件签名技术。如果在电子签名后的文件中需要嵌入权威机构签发的电子签名外观，则需要使用电子印章技术。如果在电子签名后的文件中需要嵌入权威机构签发的签名时间信息，则需要使用时间戳技术。

合同的电子签名可分为个人代表自己对合同签名和个人代表机构对合同签名。

1) 个人代表自己对合同签名

应用系统将待签合同的原文（或消息摘要）、待签人信息上传到电子合同服务平台的文件中心。文件中心通过用户中心通知对应的个人代表机构对合同进行

签名。个人使用客户端上的客户端密码模块中的私钥对合同进行签名，将签名结果提交给用户中心。用户中心将签名结果返回给文件中心，文件中心生成签名后的电子合同。

2) 个人代表机构对合同签名

个人代表机构对合同签名首先要获取机构的授权。个人用户登录到电子合同服务平台，在平台的用户中心申请获取某个机构的授权。用户中心查询该机构的授权人身份证信息以及该个人的身份证信息，如果身份证号相同，则通知个人通过用户特征采集向用户中心提交个人的真实身份验证信息，如：人脸活体视频。身份验证通过后，用户中心将个人的数字证书以及机构的密钥对索引号作为密钥授权信息发送到密钥中心进行密钥授权。

应用系统将待签合同的原文（或消息摘要）、待签人信息上传到电子合同服务平台的文件中心。文件中心通过用户中心通知对应的个人代表机构对合同进行签名。个人使用客户端上的客户端密码模块中的私钥对合同进行签名，将签名结果提交给用户中心。用户中心将签名结果发送给密钥中心并通知密钥中心进行使用机构的密钥进行签名。密钥中心使用该机构授权人的数字证书验证电子合同签名结果，若验证通过，则将机构密钥对密文导入到服务端密码模块，服务端密码模块内部解密得到机构密钥对，服务端密码模块使用机构密钥对进行签名，将签名结果返回给密钥中心，密钥中心将签名结果返回给用户中心。用户中心将签名结果返回给文件中心，文件中心生成签名后的电子合同。

5.3.1.6 形成电子合同数据的密码技术

电子合同服务平台将待签数据、签名结果、签名外观、时间戳等按一定的文件格式合成为电子合同数据，这需要用到文件签名技术。

5.3.1.7 发送/接收电子合同数据

发送/接收电子合同数据需要使用加密通道技术来保证信息交互的安全。

5.3.1.8 电子合同存储的密码技术

根据电子合同内容敏感程度的不同，需要对电子合同服务平台需要对电子合同的存储进行分级管理。对于内容敏感程度高的电子合同，需要使用文件加密技术对电子合同进行加密存储。

5.3.1.9 电子合同查询的密码技术

对于未加密存储的电子合同，电子合同服务平台直接使用用户输入的关键词来查询电子合同。对于加密存储的电子合同，电子合同服务平台需要使用文件加密技术对文件密文进行查询。

5.3.1.10 电子合同下载的密码技术

电子合同下载需要使用加密通道技术来保证信息交互的安全。

5.3.1.11 电子合同验证的密码技术

电子合同验证需要使用文件签名技术对电子合同数据进行解析，解析出其中的原文数据、原文签名值、签名证书数据、电子印章数据、时间戳数据，然后使用非对称密码签名验签技术对原文签名值、签名证书中的签名值、电子印章数据

中的签名值、时间戳数据中的签名值进行验证签名。

5.3.2 电子合同常用的密码技术

5.3.2.1PKI 技术

电子合同服务平台系统设计需要遵循PKI技术体系，PKI(Public Key Infrastructure)公钥基础设施提供公钥加密和数字签名服务，是一种遵循标准的密钥管理平台,它能够为所有网络应用透明地提供采用加密和数字签名等密码服务所必需的密钥和证书管理。PKI体系实际上就是计算机软硬件、权威机构及应用系统的结合。它采用电子证书的形式管理公钥，通过CA把用户的公钥和用户的其他标识信息（如名称、身份证号码、e-mail地址等）捆绑在一起，实现对用户身份的验证；它将公钥密码和对称密码结合起来，通过网络和计算机技术实现密钥的自动管理，保证机密数据的保密性和完整性。

在PKI技术中，证书申请者通过发起“证书签名请求（CSR）”来得到一份被签名的证书。为此，证书申请者需要生成一个密钥对，然后用其中的私钥对CSR签名（私钥本身要妥善保存，对外保密），CSR包含申请人的身份信息、用于验真CSR的申请人的公钥和专有名称（DN），CSR还可能带有CA要求的其它有关身份证明的信息,然后CA对这个专有名称及其相关信息以及密钥对的公钥签发一份符合X.509格式的数字证书。

5.3.2.2 数字证书技术

数字证书就是标识用户身份信息的一系列数据,其作用类似于现实生活中的身份证。数字证书是由一个权威机构签发的，人们可以在互联网上用它来识别对方的身份。数字证书的格式遵循 ITUT X.509 国际标准，一个标准的 X.509 数字证书包含以下一些内容：

- 证书的版本信息；
- 证书的序列号，每个证书都有一个唯一的证书序列号；
- 证书所使用的签名算法；
- 证书的发行机构名称，命名规则一般采用 X.500 格式；
- 证书的有效期，现在通用的证书一般采用 UTC 时间格式；
- 证书所有人的名称，命名规则一般采用 X.500 格式；
- 证书所有人的公钥；
- 证书签发者对证书内容的签名。

5.3.2.3 CRL 技术

证书吊销列表(Certificate Revocation List，简称CRL)是PKI系统中的一个结构化数据文件,该文件包含了证书颁发机构(CA)已经吊销的证书的序列号及其吊销日期。CRL文件中还包含证书颁发机构信息、吊销列表失效时间和下一次更新时间，以及采用的签名算法等。证书吊销列表最短的有效期为一个小时，一般为1天,甚至一个月不等,由各个证书颁发机构在设置其证书颁发系统时设置。

证书吊销列表分发点(CRL Distribution Point，简称CDP)是含在数字证书中的一个可以供各种应用软件自动下载的最新的CRL的位置信息。一个CDP通常出现在数字证书中的CRL分发点域，CDP一般是一个可以访问URL地址。

5.3.2.4 OCSP 技术

在线证书状态协议（OCSP）是一个互联网协议，用于获取符合X.509标准的数字证书的状态。该协议符合互联网标准规范，文档RFC6960对其进行了详细地描述。OCSP协议的产生是用于在公钥基础设施（PKI）体系中替代证书吊销列表（CRL）来查询数字证书的状态，OCSP克服了CRL的主要缺陷：必须经常在客户端下载以确保列表的更新。通过OCSP协议传输的消息使用ASN.1的语义进行编码。消息类型分为“请求消息”和“响应消息”，因此OCSP服务器被称为OCSP响应端。OCSP的一个典型交互场景为：

Alice和Bob使用Ivan颁发的数字证书。该场景中Ivan是数字证书认证中心（CA）；

Alice向Bob发送其由Ivan颁发的数字证书，并发出请求建立连接的申请；

Bob担心Alice的私钥已经泄露，因此向Ivan发送‘OCSP request’消息并包含Alice的数字证书序列号；

Ivan的OCPS响应端从Bob发送的消息中获取数字证书的序列号，并在CA数据库中查找该数字证书的状态；

Ivan向Bob发送由其私钥加密的消息‘OCSP response’，并包含证书状态正常的信息；

由于Bob事先已经安装了Ivan的数字证书，因此Bob使用Ivan的公钥解密消息并获取到Alice的数字证书状态信息；

Bob决定与Alice进行通信。

5.3.2.5 随机数技术

随机数技术在密钥生成、身份认证、加密通道等技术中都至关重要。随机数技术主要分为随机数生成和随机数检测。

真正的随机数是使用物理现象产生的：比如掷钱币、骰子、转轮、使用电子元件的噪音、核裂变等等，这样的随机数发生器叫做物理性随机数发生器，它们的缺点是技术要求比较高。使用计算机产生真随机数的方法是获取CPU频率与温度的不确定性以及统计一段时间的运算次数每次都会产生不同的值，系统时间的误差以及声卡的底噪等。

在安全性较低的场景中可以使用伪随机数。伪随机数是“似乎”随机的数，实际上它们是通过一个固定的、可以重复的计算方法产生的。计算机或计算器产生的随机数有很长的周期性。它们不真正地随机，因为它们实际上是可以计算出来的，但是它们具有类似于随机数的统计特征。

随机性检测亦称观测结果随机性检测、样本随机性检测，是随机性假设“n次观测结果构成简单随机样本”的一类统计检测。常用随机性检测有:游程检测，反演总数检测，递差检测，递差符号游程检测，临界点频数检测，相频数检测，相长度检测等。

5.3.2.6 非对称密码签名验签技术

非对称密码签名验签技术是非对称密码算法和消息摘要算法的结合体，一个最基本的签名验签过程如下：

1)A把原文数据用消息摘要算法处理生成消息摘要，并将摘要用签名私钥进行加密生成签名值，把原文数据和签名值一起发送给B；

2)B接收原文数据和签名值后，采用相同的消息摘要算法对原文数据进行处理生成消息摘要，将其与接收的签名用配对的公钥解密的结果对比，如果相同，说明签名验证成功，不相同则签名验证失败。

目前常用的非对称密码算法有:RSA、SM2等,常用的消息摘要算法有:SHA256、SM3等。

5.3.2.7 电子印章技术

电子印章技术包括：印章制作、印章加密、印章审核、印章权限管理、印章使用记录。

1) **印章制作**

通过上传印章图片生成电子印章；

通过用户名称自动生成电子印章。

2) **印章加密**

支持对电子印章进行防伪水印加密、密度水印加密、光学防伪加密。

3) **印章审核**

应符合企业原有印章管理要求,通过企业内部的流程审批系统实现印章审核通过，并与电子合同服务平台对接实现。

4) **印章权限管理**

对不同的用户可分配不同的电子印章；

对不同的电子印章可设置不同的使用业务。

5) **印章使用记录**

记录电子印章每次使用的详细记录。

5.3.2.8 文件签名技术

文件签名技术基于非对称密码签名验签技术。文件签名技术的主要特性是将签名原文、签名值、时间戳等数据以标准文件格式组织成一个数据文件。目前电子合同常用的标准文件格式为PDF、OFD、XML。OFD是基于XML的文件格式，下面以XML格式为例对文件签名进行说明：

所有与XML 数字签名相关的信息都存放在 〈Signature〉 元素中。〈Signature〉 元素包含有几个主要的子元素：

1) **<Signature> 元素**:至少包含一个 <Reference> 元素,每个 <Reference> 元素用于对待签名数据进行引用，包含有引用方式、转换方法、摘要算法和摘要值等信息。<Reference> 还包含有 XML 数据的规则化方法，并指定了数字签名所使用的算法。
2) **<SignatureValue> 元素**：包含对 <Reference> 元素规范化后的内容进行签名生成的数字签名的值。
3) **<KeyInfo> 元素**：用于指定验证签名所需的公共密钥相关信息。

生成XML签名时，首先根据每个〈Reference〉元素中指定的资源引用方式，摘要算法，数据转换方法等信息，对引用资源进行转换，然后对转换后的结果计算出摘要值。然后根据〈SignedInfo〉元素中指定的 XML 数据的规范化方法对〈SignedInfo〉规则化，对规范化之后的数据生成摘要值，并使用私钥对摘要值进行加密，将生成的加密摘要值存放在〈SignatureValue〉元素中。

验证XML签名时，首先需要对〈SignedInfo〉元素中包含的数据引用部分进行验证，然后对整个〈SignedInfo〉元素的签名值进行验证。其间任何一步验证失败则代表整个 XML 数字签名验证失败。

5.3.2.9 文件加密技术

文件加密技术从加密的粒度可分为：透明加密、文件加密。从加密算法可分为：对称加密、非对称加密、对称与非对称结合的加密。

透明加密对应用层是透明的，通常是在操作系统层面实现加密解密，当使用者创建或保存文件时，操作系统自动对文件进行加密，当使用者在打开或编辑指定文件时，操作系统将自动对加密的文件进行解密。文件在硬盘上是密文，在内存中是明文。

文件加密则是对单个文件进行加密，这通常是在应用系统中通过选择文件来进行加密或解密。

对称加密是指加密文件和解密文件使用同一个密钥，例如使用DES、AES、SM1、SM4等算法。对称加密的优势是运算速度快，劣势是加密方需要通过安全的方式将对称密钥分发给解密方。

非对称加密是指加密文件和解密文件使用不同的密钥，通常是用公钥进行加密用私钥进行解密，例如使用RSA、SM2等算法。非对称加密的优势是加密方可以用完全公开的公钥进行加密，只有持有对应的私钥才能解密，劣势是非对称加密的运算速度慢。对称与非对称结合的加密是为了解决非对称加密速度慢的问题。文件本身用对称密钥来进行加密解密，这个对称密钥随后又被公钥进行加密。加密方将文件密文和对称密钥密文发送给解密方，解密方用私钥先解密得到对称密钥，然后用对称密钥解密得到文件原文。数字信封技术就是使用的对称与非对称结合的加密。

5.3.2.10 时间戳技术

电子合同服务平台需要具备或通过第三方提供时间戳服务，获取精确可靠的时间源并采用高强度高标准的安全机制，将用户在线签署合同的关键操作时间进行固化，有效预防电子合同签署的日期及时间信息被任意篡改，确保签署时间信息的真实性、准确性。

时间戳是使用数字签名技术产生的数据，签名的对象包括了原始文件信息、签名参数、签名时间等信息。时间戳系统用来产生和管理时间戳，对签名对象进行数字签名产生时间戳，以证明原始文件在签名时间之前已经存在。

可信时间戳是由可信时间戳服务中心签发的一个电子凭证，用于证明电子数据文件自申请可信时间戳后内容保持完整、未被更改。根据《电子签名法》有关数据电文原件形式的要求，申请了可信时间戳认证的电子文件、电子档案或纸质档案的数字化副本等可视为法规规定的原件形式。

5.3.2.11 加密通道技术

加密通道技术通常又称为虚拟专用网(VPN)，是通过互联网建立一个临时的、安全的连接，是一条穿过公用网络的安全、稳定的通信隧道。目前的VPN技术中主要分为IPSec VPN和SSL VPN两大类。IPSec VPN是指采用IPSec安全技术标准的VPN技术，而SSL VPN指采用SSL协议来加密IP数据链路的VPN技术。SSL VPN与IPSec VPN相比有如下4大明显的技术优势：

1) SSL VPN 比 IPSec VPN 部署和管理成本更低。IPSec VPN 最大的难点在于客户端需要安装复杂的软件，而且当用户的 VPN 策略稍微有所改变时，VPN 的管理难度将呈几何级数增长。SSL VPN 则正好相反，客户端不需要安装任何软件或硬件，使用标准的浏览器，就可通过简单的 SSL 安全加密协议，安全地访问网络中的信息；
2) SSL VPN 比 IPSec VPN 更安全。SSL VPN 只需要开放一个端口（如：443 端口），而 IP Sec VPN 需要根据不同的应用开放不同的端口，而且是等于直接物理访问内部网络，会因为外部接入点的不安全而影响到内网的安全；
3) SSL VPN 比 IPSec VPN 有更好可扩展性。 IPSec VPN 在部署时一般放置在网络网关处，SSL VPN 一般部署在内网中任一节点处，IPSec VPN 的可扩展性比较差；
4) SSL VPN 在访问控制方面比 IPSec VPN 有更细粒度。IPSec VPN 部署在网络层，可以访问整个内部网；而 SSL VPN 则在应用层，可以控制用户访问不同的应用系统和不同的数据，具有更细的控制度。

5.3.3 主要研究的密码技术

5.3.3.1 目前面临的风险

目前，电子合同常用的密码技术从理论上已能解决电子合同服务平台所需解决的各种数据安全问题。然而，人们对电子合同服务平台使用便捷性的强烈需求给平台带来了极大风险。这些便捷性的需求及风险归类为以下三点：

1) 需要能使用没有任何专用硬件密码模块的普通移动端设备（如：普通手机）随时随地的进行签名；其风险点是：普通移动端设备无法保证密钥生成随机数熵源的随机性能达到密钥强度的要求。普通移动端设备的运行环境容易受到恶意攻击，密钥可能在存储时或者使用时被窃取。针对这些风险，下面进行了软件密码模块技术的研究。
2) 需要能由多个人来代表同一个机构进行签名，并且这些人还可以灵活变更；其风险点是：当多个人可以代表同一个机构进行签名时，如何保证机构的签名私钥不会被冒用或者被窃取。如何保证当一个人终止代表一个机构时，这个人无法再次调用机构的签名私钥。针对这些风险，下面进行了私钥托管技术的研究。
3) 需要能在电子合同服务平台上对电子合同内容进行快速搜索；其风险点是：对于内容高度敏感的电子合同，如何保证电子合同服务平台不会因为已知搜索关键字而对电子合同的进行统计分析或者已知明文分析。针对这些风险，下面进行了可搜索加密技术的研究。

另外为推进电子合同的国产化，提高系统的安全、高效，下面进行SM系列密码算法的应用研究。

5.3.3.2 软件密码模块技术研究

软件密码模块的安全性通常需要达到 GM/T0028-2014《密码模块安全技术要求》中的安全等级二级要求。通过纯软件的技术方案达到安全等级二级主要需要解决两大难点：如何获取随机比特生成器所需要的熵；如何保证私钥在纯软件环境中的安全。

5.3.3.2.1 如何获取随机比特生成器所需要的熵

如果熵完全在软件密码模块内生成，随机性很难达到最小熵值不小于 256 比特。如果熵完全在软件密码模块外部的硬件密码模块内产生，则需要解决硬件密码模块恶意缓存熵的问题。目前比较理想的解决方案是，软件密码模块与外部硬件密码模块共同产生熵，基于这种方案产生随机数的流程如下：

1) **生成客户端熵（ClientEntropy）**

每次产生随机数时，采集当前时刻下随机的硬件信息，由此生成 256 比特客户端熵(ClientEntropy)：

a) 获取陀螺仪的坐标值（X、Y、Z）；
b) 获取加速度传感器的输出（AX、AY、AZ）；
c) 获取地理位置信息，包括：经度Lon，纬度Lat，高度H；
d) 获取磁力计的输出信息MagNet（磁北、真北、磁偏角）；
e) 获取当前 CPU 使用率UR；
f) 获取当前时间 Time（精确到毫秒）；
g) 将上述数据串接作为随机硬件信息串：

Hinfo = X ‖ Y ‖ Z ‖ AX ‖ AY ‖ AZ ‖ Lon ‖ Lat ‖ H ‖ MagNet ‖ UR ‖ Time；

h) 使用随机硬件信息串Hinfo作为输入，计算 SM3 摘要值获得 256 比特客户端熵：

ClientEntropy = SM3_Hash(Hinfo)

2) **获取服务端随机数（ServerRandom）**

服务端提供公共的随机数生成接口，该接口为 RESTful API 形式，通过 HTTPS 协议对外提供服务。服务端随机数（ServerRandom）的长度为 2048 比特，具体的获取流程如下：

a) 软件密码模块向服务端发起 HTTPS 连接，连接成功后对服务端的服务器证书进行有效性验证，只有当服务器证书有效并且与软件密码模块中预设的服务器证书相同时才进行后续的操作，否则返回错误信息；
b) 软件密码模块每次调用服务端接口前，都在移动端本地内存中生成一个新的临时 SM2 密钥对，其中私钥为 TempSM2PrivateKey、公钥为 TempSM2PublicKey；
c) 软件密码模块构建随机数请求 Request：Request=256 比特随机请求序号（SN）+TempSM2PublicKey+请求类型（获取服务端随机数）；
d) 软件密码模块使用预设的服务端 SM2 公钥 ServerSM2PublicKey 对 Request 进行 SM2-SM4 数字信封加密得到随机数请求密文 RequestCipher；
e) 软件密码模块将 RequestCipher 发送到服务端接口；
f) 服务端接口收到 RequestCipher 后，调用服务端密码机中的 SM2 私钥 ServerSM2PrivateKey 对 RequestCipher 进行 SM2-SM4 数字信封解密得到 SN、TempSM2PublicKey、请求类型（获取服务端随机数）；
g) 服务端调用服务端密码机的随机数生成功能来生成两个 2048 比特的随机数，第一个 2048 比特随机数经 SM4 加密后得到服务端随机数密文（ServerRandomCipher），第二个 2048 比特随机数经 SM4 加密后得到缓存服务端随机数密文（CacheServerRandomCipher），生成 ServerRandomCipher 和 CacheServerRandomCipher 的 SM4 密钥预设在服务端密码机内部，SM4 计算在密码机内部完成；
h) 服务端构建随机数响应 Response：Response= SN+ ServerRandomCipher+

CacheServerRandomCipher；

i) 服务端使用 TempSM2PublicKey 对 Response 进行 SM2-SM4 数字信封加密得到随机数响应密文 ResponseCipher；

j) 服务端调用服务端密码机中的 SM2 私钥 ServerSM2PrivateKey 对 ResponseCipher 进行 SM2 签名得到 ResponseCipherSignature；

k) 服务端将 ResponseCipher 和 ResponseCipherSignature 通过 HTTPS 协议安全通道返回给软件密码模块；

l) 软件密码模块使用预设的服务端 SM2 公钥 ServerSM2PublicKey 对 ResponseCipher 和 ResponseCipherSignature 进行 SM2 验签，若验签失败则获取服务端随机数失败；

m) 软件密码模块使用临时 SM2 密钥对的私钥 TempSM2PrivateKey 对 ResponseCipher 进行 SM2-SM4 数字信封解密，得到 SN、ServerRandomCipher 和 CacheServerRandomCipher；

n) 软件密码模块对比解密得到的 SN 是否与该次请求时的 SN 相同，若相同则成功获取 ServerRandomCipher 和 CacheServerRandomCipher;若不同，则获取服务端随机数失败；

o) 软件密码模块使用 SM4 白盒算法解密 ServerRandomCipher 得到服务端随机数 ServerRandom；

p) 软件密码模块使用新获取到的 CacheServerRandomCipher 替换 Keychain 中的当前 CacheServerRandomCipher；

q) 软件密码模块从内存中完全清除掉 SN、临时 SM2 密钥对 TempSM2PrivateKey 和 TempSM2PublicKey、SM2-SM4 数字信封中的临时 SM4 密钥。

3) 生成服务端熵（ServerEntropy）

按步骤 2 的方法从服务端获取 2048 比特服务端随机数(ServerRandom)后，对服务端随机数(ServerRandom)进行 SM3 摘要得到 256 比特的服务端熵 ServerEntropy，即：

ServerEntropy = SM3_Hash(ServerRandom)

4) 生成熵（Entropy）

将 256 比特客户端熵(ClientEntropy)与 256 比特服务端熵(ServerEntropy)进行按位异或得到 256 比特熵(Entropy),即：

Entropy = ClientEntropy XOR ServerEntropy

5) 生成随机数（Random）

随机数的生成采用 NIST 的确定性随机数产生器推荐标准（SP800-90）中的 Hash_DRBG 算法，其中的 Hash 算法改用 SM3 算法，输入前面步骤产生的 256 比特熵(Entropy)以及随机数长度(RandomLen)即可产生随机数，即：

Random = Hash_DRBG_SM3(Entropy,RandomLen)

每次产生随机数前都生成一个新的熵，产生随机数后立刻在内存中对熵(Entropy)、客户端熵(ClientEntropy)、服务端熵(ServerEntropy)、服务端随机数(ServerRandom)进行置零和销毁，不对这些数据进行保存。

5.3.3.2.2 如何保证私钥在纯软件环境中的安全

如果私钥的生成、存储、调用都在软件密码模块中进行，则必然会在软件运行时的内存中出现完整的私钥，这很容易被恶意软件窃取。解决这个难点的有效

方案是软件密码模块中仅独立生成、存储、调用部分私钥（又称：私钥分量），私钥的其它部分则在软件模块外（如：服务器端）独立生成、存储、调用。利用椭圆曲线算法的数学特性，目前已有协同密码算法和门限密码算法可用于实现私钥的分量计算。下面以协同密码算法在移动端 APP 上的实现来进行说明。

SM2 密钥对由客户端和后台管理系统协同生成，双方随机生成私钥分量和对应的公钥分量，交换各自的公钥分量，通过约定的算法生成最终的公钥。客户端和后台管理系统分别安全存储私钥分量。

1) 客户端私钥分量的生成存储及恢复

- 客户端私钥分量d_1的生成及存储。

a）生成非敏感参数：（i）客户端用随机数发生器生成 32 比特盐值 Salt；（ii）客户端用随机数发生器生成一个 4096～8192 之间的随机整数 Rounds，用作密钥派生函数 KDF 的迭代次数；（iii）客户端用随机数发生器生成 128 比特用于标识设备身份的 UUID；（iv）将 Salt、Rounds 和 UUID 保存在移动端 App 的隔离容器内部的非挥发性存储空间。

b）生成设备指纹（MobileID）：客户端从移动设备中读取 CPU 类型、CPU 个数等硬件参数，读取操作系统类型等软件参数；读取唯一标识 UUID；将硬件、软件参数和 UUID 串接作为输入，执行 SM3 摘要算法计算出 256 比特设备指纹（MobileID）。

c）生成客户端私钥分量：客户端用随机数发生器生成 256 比特随机数作为客户端私钥分量d_1。

d）生成临时密钥 TK：参考 PKCS#5 标准，基于证书私钥对应的保护 PIN 码来派生临时密钥 TK，具体流程如下：（i）提示用户输入证书私钥对应的保护 PIN 码；（ii）读取盐值 Salt、迭代次数 Rounds；（iii）将 PIN 码、盐值 Salt、设备指纹 MobileID 串接作为输入参数，执行 Rounds 次密钥派生算法 KDF，得到 128 比特临时密钥 TK。

e）加密存储私钥分量：将客户端私钥分量d_1作为输入，使用临时密钥 TK 作为对称密钥执行 ECB 模式的 SM4 加密算法获得客户端私钥分量密文 SD1，然后将 SD1 保存在移动端 App 的隔离容器内部的非挥发性存储空间。

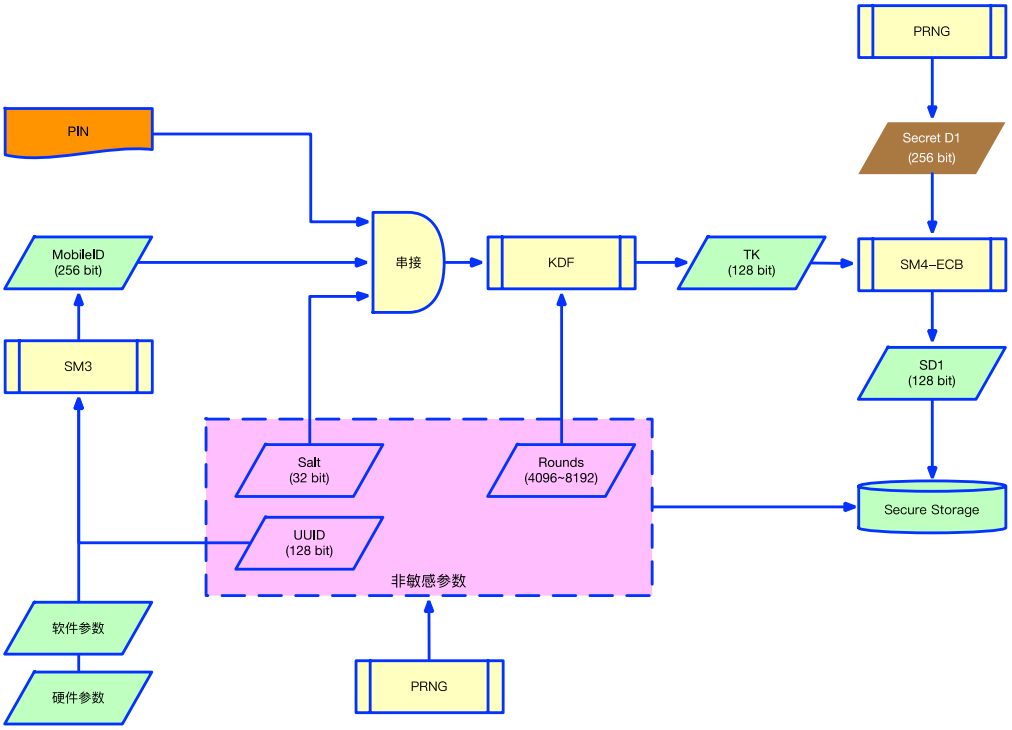

图 5-8　客户端私钥分量生成及存储

- 在执行签名阶段，客户端私钥分量d_1的恢复。

  a）提取参数：从非挥发性存储空间读取以下数据：盐值 Salt、迭代次数 Rounds、唯一标识 UUID、客户端私钥分量密文 SD1。

  b）恢复设备指纹（MobileID）：客户端从移动设备中读取 CPU 类型、CPU 个数等硬件参数，读取操作系统类型等软件参数；将硬件、软件参数和 UUID 串接作为输入，执行 SM3 摘要算法计算出 256 比特设备指纹（MobileID）。

  c）生成临时密钥 TK：提示用户输入证书私钥对应的保护 PIN 码；将 PIN 码、盐值 Salt、设备指纹 MobileID 串接作为输入参数，执行 Rounds 次密钥派生算法 KDF，得到 128 比特临时密钥 TK。

  d）计算私钥分量：将客户端私钥分量密文 SD1 作为输入，使用临时密钥 TK 作为对称密钥执行 ECB 模式的 SM4 解密算法获得 256 比特的客户端私钥分量d_1。

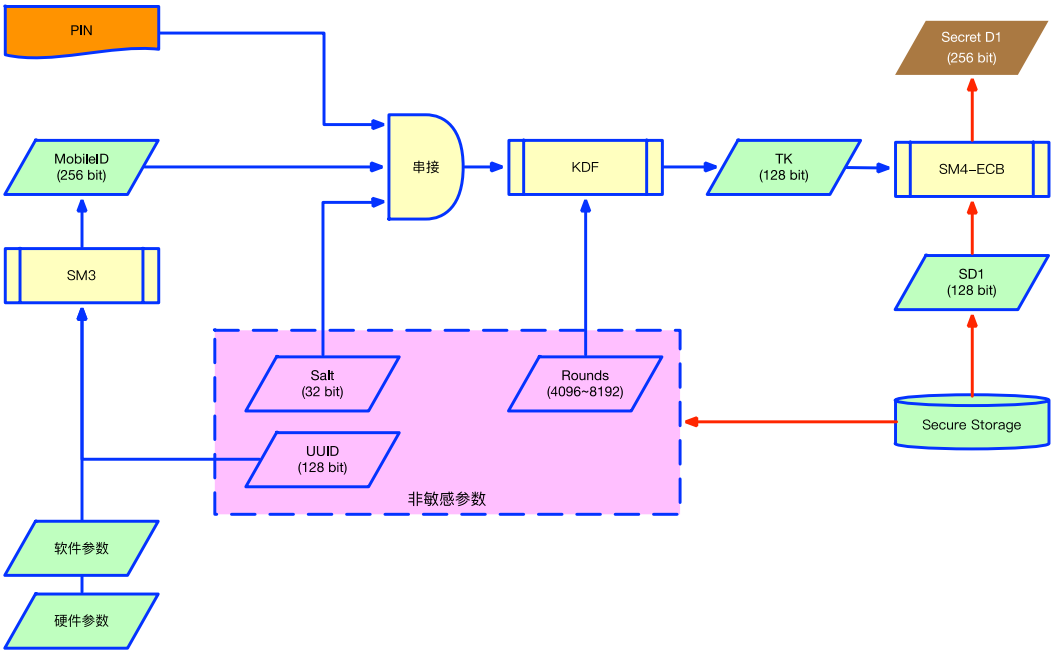

图 5-9　客户端私钥分量恢复

2)　服务端私钥分量生成及存储

服务端在密码机内部存储一个全局的 128 比特 SM4 对称密钥 X，然后采用密钥派生算法为特定用户产生服务端私钥分量d_2；产生私钥分量d_2，并计算d_2对应的部分公钥的过程在密码机内部完成，并确保计算出的私钥分量d_2不能以明文形式导出密码机外部；在客户端与服务端协同执行数字签名的阶段，服务端通过发送指令给密码机，在密码机内部根据 X 计算出私钥分量d_2，完成协同签名的步骤；密码机产生的私钥分量d_2，不允许存储在非挥发性存储部件；无论是计算公钥，还是协同签名，在密码机使用私钥分量d_2之后，服务端通过向密码机发送指令来销毁内存中的私钥分量副本。

服务端私钥分量的生成流程如下：

- 客户端将AppID和KeyID发送给服务端；
- 服务端调用加密机接口，加密机内部计算：

  seed=SDF_Encrypt(algID=SM4，AppID||PlatformID||KeyID,X)；

  $d_2 = \mathrm{KDF}(\mathrm{seed}, \mathrm{klen})$

其中，KDF 采用《GM/T 0003.4-2012 SM2 椭圆曲线公钥密码算法第 4 部分：公钥加密算法》中定义的密钥派生算法。

3)　生成共同公钥

- 客户端生成私钥参数d_1，$d_1 \in \{1, \ldots, n-1\}$，计算公钥参数$P_1 = [d_1]G$，并发送公钥参数$P_1$给服务端。
- 服务端生成私钥参数d_2，$d_2 \in \{1, \ldots, n-1\}$，根据接收的公钥参数$P_1$和计算的公钥参数$P_2 = [d_2]G$，生成双方的共同公钥$P_{pub} = [d_2]P_1 - G$，并公开共同公钥$P_{pub}$。

4)　SM2 协同签名原理

由于客户端和后台管理系统各自保管部分私钥分量，因此 SM2 签名需要由客户端和后台管理系统协同完成。由客户端计算消息摘要，发送给后台管理系统请求协助签名，最终也是由客户端输出签名结果，避免泄露用户隐私。SM2 签名由

客户端和服务端使用各自的私钥分量，进行协同计算，最终生成标准的签名值。设待签名的消息为M，为了获取消息M的数字签名(r,s)，作为签名者的用户A实现以下运算步骤：

- 预先处理阶段

作为签名者的用户 A 具有长度为$entlen_A$比特的可辨别标识ID_A，记$ENTL_A$是由整数$entlen_A$转换而成的两个字节，使用密码杂凑函数H_v求得用户A的杂凑值

$Z_A = H_{256}(ENTL_A \| ID_A \| a \| b \| x_G \| y_G \| x_A \| y_A)$。客户端置$\overline{M} = Z_A \| M$，计算$e = H_v(\overline{M})$，按 GM/T 0003.1-2012 4.2.4 和 4.2.3 给出的方法将e的数据类型转换为整数。

- 签名阶段

a）服务端选择随机数$k_1 \in \{1, \ldots, n-1\}$，随机数$k_2 \in \{1, \ldots, n-1\}$，计算椭圆曲线群元素$R_1 = [k_1]P_1$，椭圆曲线群元素$R_2 = [k_2]G$，并发送椭圆曲线群元素$R_1$和椭圆曲线群元素$R_2$给客户端。

b）客户端选择随机数$k_3 \in \{1, \ldots, n-1\}$，随机数$k_4 \in \{1, \ldots, n-1\}$，结合接收的椭圆曲线群元素$R_1$，椭圆曲线群元素$R_2$，计算$(x_1, y_1) = [k_3]R_1 + R_2 + [k_4]G$，计算中间量$r = (e + x_1) \bmod n$，如果$r = 0$或者$[r]G + [k_3]R_1 + R_2 + [k_4]G = O$则返回步骤 c）由服务端重新选择随机数，否则客户端使用随机数k_4和中间量r计算数$r' = (r + k_4) \bmod n$，并把数r'发送给服务端。

c）服务端使用私钥参数d_2，随机数k_1，随机数k_2和接收的数r'，计算数$s_1 = (k_1 \cdot d_2^{-1}) \bmod n$，数$s_2 = ((r' + k_2) \cdot d_2^{-1}) \bmod n$，并发送数$s_1$和数$s_2$给客户端。

d）客户端检查接收的数s_1和数s_2，若$s_1 = 0$或$s_2 = 0$则返回步骤 c）由服务端重新选择随机数，否则使用私钥参数d_1，随机数k_3，中间量r，接收的数s_1，数s_2，计算使用共同公钥P_{pub}可以验证的、符合 SM2 签名格式要求的数字签名(r,s)，其中$s = k_3 \cdot s_1 + s_2 \cdot d_1^{-1} - r$，若$s = 0$则返回步骤 c）由服务端重新选择随机数。

e）客户端按 GM/T 0003.1-2012 标准 4.2.2 给出的细节将r、s的数据类型转换为字节串，然后输出消息M的数字签名结果(r,s)。

5.3.3.3 私钥托管技术研究

私钥托管在电子签名领域一直是一个存在争议的技术，《电子签名法》要求签名者能唯一控制签名材料（通常也就是签名私钥），而将签名私钥保存在第三方，签名者在使用私钥时也通过第三方来调用私钥，这从直观上看似乎是无法满足《电子签名法》对唯一控制性的要求的。但私钥托管在当前推广的移动互联网环境、云计算环境中却能给用户带来极大的便利，应用的需求十分强烈。对于这个矛盾，目前国内业界还未形成一致处理意见，因此针对在平台中涉及到私钥托管的需求，建议在国家未出台相关标准规范前，仍然采用符合 GM/T0028 相关安全等级的硬件密码模块或软件密码模块，而最为全面的研究来自欧盟的 eIDAS 的相关标准和规范。

欧盟在推出 Regulation EU 910/2014 (eIDAS)之前，合格的电子签名要求为每个签名者配备一个智能卡，签名必须使用智能卡中的私钥。Regulation EU 910/2014 (eIDAS)的推出，提出了一种重要的智能卡替代方案，这种替代方案基于合格可信服务提供者 Qualified Trust Service Providers（QTSP）来保存和

调用签名私钥，并为之定义了一套严格的技术、机制、流程规范来保证签名者对签名私钥的唯一控制。该替代方案的提出，从标准法规层面承认了远程签名（或者也叫服务器签名、云签名）的合法性。

QTSP 由合格电子签名生成设备 Qualified Electronic Signature Creation Device（QSCD）和必要的软件构成，主要提供以下服务：

1) 安全的加密保护用户的认证数据；
2) 生成和存储每个用户的签名私钥；
3) 保证用户对其签名私钥的唯一控制，也就是只有通过认证的用户才能调用其签名私钥；
4) 调用签名私钥产生签名值。

为了保证远程签名的合法性和可靠性，eIDAS 进行了如下规定：

1) 用户的签名私钥必须由经认证的合格的硬件安全模块来生成和存储；
2) 签名激活过程(也就是对用户进行认证然后对签名私钥进行调用的过程，这个过程保证了用户对签名私钥的唯一控制）安全性分为两个级别。安全级别 1 的签名激活过程由外部软件代码控制。安全级别 2 的签名激活过程由 QSCD 的内部代码控制；
3) 用户必须自行保证个人智能设备（如：手机）的安全：保证个人智能设备没有安装恶意软件，为个人智能设备设置访问控制（如：手机登录密码），若手机里保存了认证密钥则还需为其设置保护 PIN 码；
4) 必须对 QTSP 进行合格性审计,审计对 QTSP 的整个体系(包括物理环境、管理制度）进行检查，以评价是否能达到提供远程签名服务的要求。

在 EN 419 241-1/2/3、EN 419 221-5、TS 119 431-1/2 及 TS 119 432 对 QSCD 的要求进行了规定。QSCD 的核心是硬件安全模块 Hardware Security Modules（HSM）和签名激活模块 Signature Activation Module(SAM)，HSM 实现了签名私钥的生成、存储和调用，SAM 实现了用户对签名私钥的唯一控制。HSM 和 SAM 都处于防篡改的环境中，整个签名体系架构如下：

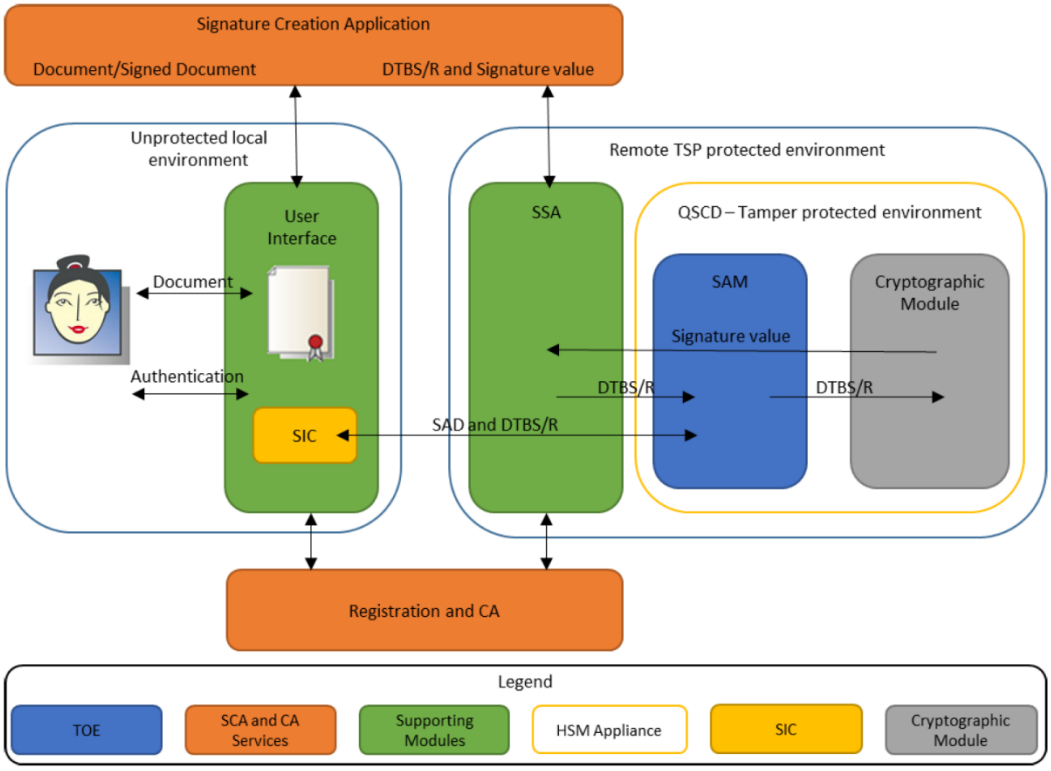

图 5-10　远程签名体系

5.3.3.4 可搜索加密技术研究

为了解决如何在密文上进行关键词搜索的问题，可搜索加密的概念被提了出来，可搜索加密的工作流程如下：首先数据拥有者把加密的文件数据以及相关的关键词密文上传到云服务器，然后用户利用私钥生成搜索陷门，并把该陷门信息发送给云服务器，云服务器通过使用该陷门信息搜索到用户感兴趣的数据，并把数据发回给用户。该技术实现了用户在不可信赖云服务器环境下进行快速有效的密文关键词检索，同时不泄漏任何关于数据的信息。可搜索加密体制分为对称可搜索加密体制和公钥可搜索加密体制。

根据对称加密体制的性质，对称可搜索加密体制中的数据文件和要检索的关键词陷门都必须使用同一个的密钥进行加密，因此对称可搜索加密体制更适合应用于个人的数据存储等应用场景中。

公钥可搜索加密方案发送方使用接收方的公钥来加密文件和关键词信息，接收方使用自身的私钥生成搜索陷门，最后由存储文件密文的服务器来进行数据检索，将包含某个关键词的文件密文发送给接收方。

与对称可搜索加密方案不同，大部分的公钥可搜索加密方案都是基于双线性对构造的，因此其运算效率比对称可搜索加密方案要低不少。但是由于公钥可搜索加密方案使用了数据共享者的公钥对数据进行加密，因此在整个加密过程中，数据加密者不需要与数据共享者进行密钥协商，这使得该方案更适合于多用户的数据共享等领域，其应用场景比对称可搜索加密的应用场景更为广阔。

云存储服务是公钥可搜索加密的一个重要应用场景，在该应用场景中公钥可搜索加密提供了安全的数据存储以及数据检索功能，其中涉及到三个参与方：云服务器、数据拥有者和用户。云服务器提供第三方的数据存储以及检索服务。由

于云服务器往往是不可信的，并且存放在其上的数据可能包含用户的个人敏感信息。因此，出于安全性的考虑，云服务器上的数据文件必须先进行加密，以保证数据存储的机密性。当用户想要搜索包含特定关键词的数据时，用户会经过数据拥有者的授权得到相应的搜索凭证，然后在云服务器上进行关键词检索。云服务器对存储在本地的密文文件进行匹配检索，如果匹配成功，则说明该密文中包含用户要检索的关键词。采用公钥可搜索加密方案的云存储系统节约了用户大量的通信开销和存储开销。用户可以直接检索到自己感兴趣的密文，下载到本地并进行解密操作，而无需把密文文件全部下到本地，然后再一一解密。

公钥可搜索加密体制一般由以下 4 个算法构成：

1) KeyGen(λ):输入安全参数 λ，输出公钥 pk 和私钥 sk；
2) PEKS（pk，w）：输入公钥 pk 和关键词 w，输出关键词密文C_w；
3) Trapdoor（sk，w'）：输入私钥 sk 和关键词w'，输出陷门$T_{w'}$；
4) Test(pk, C_w, $T_{w'}$):输入公钥 pk，关键词密文C_w和陷门$T_{w'}$，如果 w=w'则输出 1，否则输出 0。

5.3.4 其他关键技术研究

5.3.4.1 文档安全存储的密码技术研究

云存储属于一种基于服务的系统，其本质是将云计算技术应用于数据存储领域。云存储技术是将分布式文件系统、网络通信技术以及计算机集群管理技术等技术结合起来，将大量的数据存储设备通过集群管理软件进行管理，使得这些设备能够协同工作，共同完成数据存储的任务。

随着云计算技术快速发展，云存储必然是未来的数据存储趋势，而加密存储在云存储安全中占有很重要的地位。加密存储是指对数据文件进行加密后再进行存储，它实现了敏感数据在存储以及传送过程中的机密性保护，是保证用户私有数据在云存储平台安全性的核心技术。云存储系统中的数据加密可分为两大模式:客户端加密模式和服务端加密模式。

客户端加密模式，首先对数据进行加密操作，然后将加密后的密文发送到云存储服务器上进行存储。大多数客户端加密模式的解决方案都是采用基于客户端数字证书的。用户持有解密密钥，只有用户可以对云存储服务端的数据进行解密。这种模式能最大限度的保护用户数据的安全，但是在实现文档流转时会需要用户对文件解密后才能流转，给使用带来不便。

服务端加密模式，由云存储服务端对需要保护的用户数据进行加密，云存储服务端对数据的加密密钥进行统一管理，便于用户使用。这种模式优点是用户使用方便，缺点是一旦服务端的加密密钥泄露，就会对用户数据的安全带来极大的威胁。

5.3.4.2 即时签名的密码技术研究

在电子合同的实际应用场景中，待签名的用户并不一定提前准备好了私钥存储介质以及CA机构为其颁发的数字证书，却要在很短的时间（如：几十秒）内完成电子签名。

通过移动端设备现场采集用户所特有的特征数据（如：手写签名笔迹、活体影像、身份证影像、指纹、声纹、虹膜、意愿视频等），并且现场为用户产生一个临时密钥对，CA即时为这些特征数据的Hash值以及临时密钥对签发一张短期用户证书，用户可即时使用这个临时密钥对完成签名，签名完成后随即销毁这个临

时密钥对。现场采集的特征数据及其Hash值，都上传到服务器进行存证，用于后期发生纠纷时的取证。

5.3.4.3 密钥管理技术研究

在现代密码学中，密钥是加密运算和解密运算的关键，也是密码系统的关键。密码系统的安全取决于密钥的安全，而不是密钥算法或保密装置本身的安全，因此电子合同服务平台中密钥的管理至关重要。密钥管理涉及到的技术则包括密钥生成技术、密钥分配技术、存储保护技术、备份恢复技术、密钥更新技术等一列技术问题。

1) 密钥生成技术

支持 RSA、DES、SM2 等密钥的生成。

2) 密钥分配技术

提供公开密钥的分配和对称密钥的分配，其中公开密钥（RSA 算法、椭圆曲线密码算法等）分配需从 KDC（Key Distribution Center）中申请；对称密钥分配必须通过密钥交换技术，如 Diffie-Hellman 算法或者以诸如 RSA 算法、椭圆曲线密码算法等改进的 Diffie-Hellman 算法等。

3) 存储保护技术

平台需支持整体保存技术和分散保存技术，整体保存包括人工记忆、外部记忆装置、密钥恢复、系统内部保存等；分散保存包括秘密共享技术等。

4) 备份恢复技术

密钥的存储机制的重点在于安全问题，但也有可靠性问题，因此密钥的备份机制也是必要的。密钥的备份和恢复通常使用秘密共享技术和密钥托管技术。

5) 密钥更新技术

为安全起见，密钥需要定期更换。更换内容包括用户登记更新、密钥更新。对于会话密钥的更新可使用一次一密的方法，也可从旧的密钥自动生成新密钥，如单向函数方法。

6.标准化研究

6.1 标准体系

目前，国内在第三方电子合同服务平台领域尚无针对密码应用的技术标准。现有的第三方电子合同平台相关标准可为新标准的制定提供参考依据，且与本研究的技术框架相互兼容。此举将有助于补充和完善现有的密码标准体系。为进一步规范并推动我国第三方电子合同服务平台行业的发展，建议开展第三方电子合同服务平台密码应用技术标准的研究，填补该领域的标准化空白，促进密码应用类标准化工作的进程。

6.2 标准化建议

6.2.1 标准化的目的

在目前第三方电子合同服务平台的建设中，密码技术方案的设计存在较大的随意性，特别在是否要选用SM系列密码算法方面没有十分一致的意见。这会导致个别设计可能存在较大的安全风险和隐患。

标准化的目的是为了对第三方电子合同服务平台中基础性、公共性的功能所需用到的密码技术提出规范化、标准化的设计方案，供业内参考，以全面提高第三方电子合同服务平台的安全性。

6.2.2 标准化思路

标准化的思路大致可分为以下四个步骤：

步骤一：**通过本研究报告前面各部分的分析和研究，可得出第三方电子合同服务平台中具有基础性、公共性的功能。**

- 个人用户注册；
- 机构用户注册；
- 个人身份认证；
- 机构身份认证；
- 个人签名；
- 机构授权个人签名；
- 机构签名；
- 文件数据签名；
- 文件数据加密；
- 个人密钥管理；
- 机构密钥管理；
- 信息系统基础功能（物理环境、设备、网络、通信、计算等）。

步骤二：分析上述功能所需要密码应用技术要求以及引用相关标准的分析。

- 国标

GB/T 25062-2010 信息安全技术 鉴别与授权 基于角色的访问控制模型与管理规范

GB/T 25056-2010 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 25064-2010 信息安全技术 公钥基础设施 电子签名格式规范
GB/T 29242-2012 信息安全技术 鉴别与授权 安全断言置标语言
GB/T 29243-2012 信息安全技术 数字证书代理认证路径构造和代理验证规范
GB/T 30281-2013 信息安全技术 可扩展访问控制标记语言
GB/T 31508-2015 信息安全技术 公钥基础设施 数字证书策略分类分级规范
GB/T 32399-2015 信息技术 云计算 参考架构
GB/T 32400-2015 信息技术 云计算 概览与词汇
GB/T 31916.1-2015 信息技术 云数据存储和管理 第一部分 总则
GB/T 31916.2-2015 信息技术 云数据存储和管理 第二部分 基于对象的云储存应用
GB/T 32010.1-2015 文献管理 可移植文档格式 第1部分：PDF1.7
GB/T 32905-2016 信息安全技术 SM3密码杂凑算法
GB/T 32907-2016 信息安全技术 SM4分组密码算法
GB/T 15843.3-2016 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
GB/T 32918.1-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第1部分：总则
GB/T 32918.2-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法
GB/T 32918.3-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议
GB/T 32918.4-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法
GB/T 32918.5-2017 信息安全技术 SM2椭圆曲线公钥密码算法 第5部分：参数定义
GB/T 35275-2017 信息安全技术 SM2密码算法 加密签名消息语法规范
GB/T 35276-2017 信息安全技术 SM2密码算法使用规范
GB/T 33560-2017 信息安全技术 密码应用标识规范
GB/T 35291-2017 信息安全技术智能密码钥匙应用接口规范
GB/T 36298-2018 电子合同订立流程规范
GB/T 36319-2018 电子合同基础信息描述规范
GB/T 36320-2018 第三方电子合同服务平台功能建设规范
GB/T 25056-2018 信息安全技术 证书认证系统密码及其相关安全技术规范
GB/T 36322-2018 信息安全技术密码设备应用接口规范
GB/T 37092-2018 信息安全技术 密码模块安全要求
GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式
GB/T 37076-2018 信息安全技术 指纹识别系统技术要求
GB/T 36624-2018 信息技术 安全技术 可鉴别的加密机制
GB/T 39321-2020 电子合同取证流程规范
GB/T 38540-2020 信息安全技术 安全电子签章密码技术规范

- 行标

GM/T 0020-2012 证书应用综合服务接口规范

GM/T 0022-2014 IPSec VPN技术规范
GM/T 0023-2014 IPSec VPN 网关产品规范
GM/T 0024-2014 SSL VPN技术规范
GM/T 0025-2014 SSL VPN网关产品规范
GM/T 0026-2014 安全认证网关产品规范
GM/T 0029-2014 签名验签名服务器技术规范
GM/T 0032-2014 基于角色的授权管理与访问控制技术规范
GM/T 0033-2014 时间戳接口规范
GM/T 0034-2014 基于SM2密码算法的证书认证系统密码及其相关安全技术规范
GM/T 0043-2015 数字证书互操作检测规范
GM/T 0054-2018 信息系统密码应用基本要求
GM/T 0070-2019 电子保单密码应用技术要求

步骤三：由于 GM/T0054-2018《信息系统密码应用基本要求》、GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》和 GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》中已对电子合同服务平台的基础密码应用做了要求规范，但对业务应用流程未作规范，故第三方电子合同服务平台密码技术标准中主要分析应用业务的密码应用技术，通过分析上述功能涉及的密码技术方案如下：

- 个人用户注册

用户特征数据的收集方案、用户特征数据的验证方案、用户数字证书的生成方案、用户身份认证方式的初始化方案、用户签名外观的初始化方案。

- 机构用户注册

用户特征数据的收集方案、用户特征数据的验证方案、用户数字证书的生成方案、用户身份认证方式的初始化方案、用户签名外观的初始化方案。

- 个人身份认证

个人身份认证可使用的流程、协议。

- 机构身份认证

机构身份认证可使用的流程、协议。

- 个人签名

个人签名的流程、格式、应用接口。

- 机构授权个人签名

机构授权个人签名的流程、格式、应用接口。

- 机构签名

机构签名的流程、格式、应用接口。

- 文件数据签名

文件数据的格式、签名的格式、签名外观的格式、签名及签名外观合成到文件的格式。

- 文件数据加密

文件数据的格式、加密的格式、部分加密/全部加密的协议。

- 个人密钥管理

个人密钥介质的选择、密码算法的选择、密钥长度的选择、密钥生成/更新/销毁的协议。

- 机构密钥管理

机构密钥介质的选择、密码算法的选择、密钥长度的选择、密钥生成/更新/销毁的协议。

步骤四：对这些密码技术方案进行标准化、规范化的描述，形成相应的标准内容。

6.3 其他标准建议

通过本报告的研究，对于私钥托管技术，目前国内业界尚未形成一致意见，仅有欧盟的Regulation EU 910/2014 (eIDAS)对远程签名体系做了规范，而私钥托管在当前广泛推广的移动互联网环境、云计算环境中却能给用户带来极大的便利，应用的需求十分强烈。因此建议对Regulation EU 910/2014 (eIDAS)中基于合格可信服务提供者Qualified Trust Service Providers（QTSP）来保存和调用签名私钥方案进行采标并结合国内的法律法规、SM算法以及第三方电子合同服务平台的业务特点，形成《远程签名体系规范》，对第三方电子合同服务平台中所使用的私钥托管形成技术规范和约束。

7.总结

综上所述，构建一款安全可靠的电子合同服务平台，既要考虑电子合同服务平台功能框架的规范性、完整性，也要重点规范电子合同服务平台技术规范性，即电子合同服务平台密码技术应用的规范性，保障第三方电子合同服务平台的安全可靠性。

目前，在电子合同服务领域中，国内标准已发布的《电子合同订立流程规范》、《电子合同基础信息描述规范》、《第三方电子合同服务平台功能建设规范》均是从电子合同业务与功能层面提出规范要求，但是技术层面的规范要求却处于缺失状态。建立第三方电子合同服务平台密码技术标准显得尤为迫切。

电子合同服务平台可以充分利用已有国际密码标准、国家密码标准、密码行业标准等实现密码应用。基于等级保护2.0实施的情况下，可以尽快申请制定第三方电子合同服务平台密码应用技术规范、密码应用技术要求以及远程签名体系等相关标准规范。

参考文献

[1]GB/T36298-2018 电子合同订立流程规范
[2]GB/T36319-2018 电子合同基础信息描述规范
[3]GB/T36320-2018 第三方电子合同服务平台功能建设规范
[4]2018 年度中国第三方电子合同市场及应用行业研究报告
[5]2019 中国电子签名安全专题研究报告
[6]ISO/IEC 27018:2014 nformation technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
[7]ETSI SR 001 604-2012 Rationalised Framework for Electronic Signature Standardisation
[8]https://baijiahao.baidu.com/s?id=1664179843558683325&wfr=spider&for=pc
[9]http://www.taiwan.cn/flfg/flshy/200804/t20080416_625724.htm