e 签宝快捷签产品服务手册 v2.1

杭州天谷信息科技有限公司

2017 年 8 月

目 录

1 产品优势

e 签宝是全国领先的第三方电子签名平台，定位是全生态的电子签名解决方案专家。

- 多样化签署服务

快捷签以“合法合规、简便易用、用户体验第一“作为核心设计理念，满足电子签名法要求的可靠电子签名“真实身份，真实意愿，签名未改，原文未改”四要素。为客户提供从用户数字证书申请、模板/手绘印章创建、多样化签署服务，到签署后出具签署证据报告，提供司法诉讼支撑，以实现全流程的电子签署服务及司法证据链闭环。

- 合规合法

快捷签完全符合《中华人民共和国电子签名法》、《商用密码管理条例》、《电子认证服务管理办法》、《电子认证服务密码管理办法》等法律法规要求，为您创建安全可靠的电子签名。

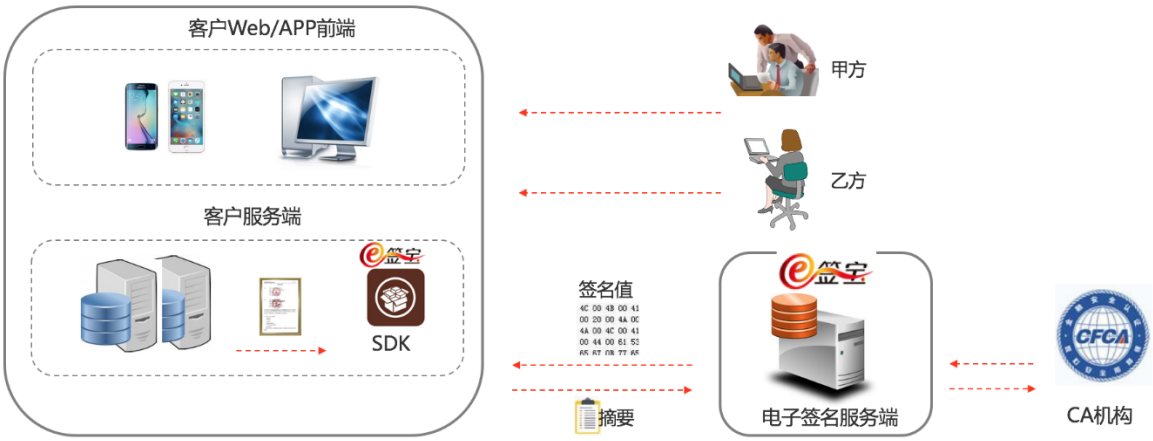
快捷签通过权威认证，成功通过国密局、公安部技术鉴定，获得《商用密码产品型号证书》、《计算机信息系统安全专用产品销售许可证》；成功通过北京网络行业协会电子数据司法鉴定中心评估，为 e 签宝开通专用绿色通道；采用第三方电子认证机构数字证书。

- 技术领先

快捷签具备领先的技术优势。采用 2048 位公钥密码算法、128 位传输和存储加密、256 位摘要算法 ,让您的数据时刻处于加密状态 ;唯一支持国密 SM1、SM2、

SM3、SM4 算法的互联网签名平台；原文沙箱保护技术不仅保障您数据的法律效力，并且完全无需担忧隐私泄漏。

- 灵活部署



e 签宝快捷签是 SDK 的产品形态，嵌入客户应用系统提供服务支撑。

客户在使用快捷签服务发放用户数字证书前，需要对所有用户进行严格的实名认证。

2 产品功能与服务

2.1 数字证书生成服务

证书生成服务指根据业务系统的用户实名身份信息生成可信用户数字证书，以此证书签署的文档代表签署人意愿，签署文档具有法律效力。

e 签宝支持的证书类型包含用户数字证书、时间戳证书、事件型签名证书和指纹隐私证书。证书介绍如下：

证书类型	描述
用户数字证书	e 签宝为使用快捷签的平台以及平台用户，根据相关实名认证信息向国家权威 CA 机构申请用户专属的长期数字证书。证书内包含用户名称和证件号等信息，代表用户的签署主体意愿。可以看做是电子签名的“身份证”。
事件证书	与用户证书的不同的是，事件证书是一种短期证书，用于对某一个事件本身进行认证。在事件证书内包含事件描述信息和所有签署人信息。该证书一次性有效，使用后即失效，保证了使用安全。
时间戳证书	e 签宝快捷签服务在每一次签署时都加盖时间戳，固化文档签署时间。时间戳证书也由 CA 机构提供。
指纹隐私证书	指纹隐私证书是 e 签宝独创的隐私保护签名技术。 基于隐私保护考虑，接入平台不愿意将用户信息在合同中展示；但是合法电子签名必须基于用户身份的真实性来实现。

	解决方案师平台方将用户身份信息传递给 e 签宝后，e 签宝直接通过用户身份信息哈希值制作数字证书；虽然是哈希值，但是由于哈希值的“指纹特性”，仍然能够达到实名身份认证的目的。方案价值：既保护了用户隐私，又确保了电子签名的法律效力。

此服务以 SDK 接口方式提供，业务系统调用接口，传递用户实名信息，e 签宝平台根据信息生成云证书后立即返回该用户在 e 签宝平台的唯一标识，业务系统妥善保管该标识作为后续证书使用的依据。

- 合作 CA 机构

e 签宝与权威数字证书认证中心（CA）和时间戳数据源中心合作，保证了电子签名服务的稳定性。所有申请证书的用户资料在 CA 机构备份，保证电子签名的合法合规。只要是国家认证的 CA 机构颁发的证书法律效力是等同的。

e 签宝具备多 CA 渠道切换机制，保证证书申请服务的连续性。

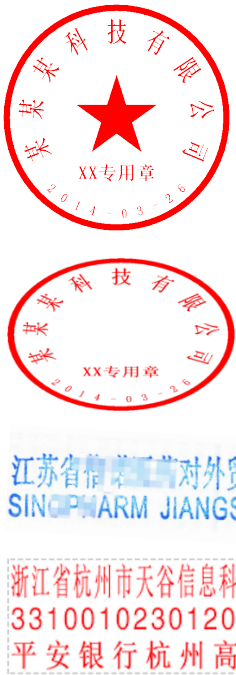
2.2 模板印章/手绘签名服务

模板印章生成服务是根据用户实名身份信息为用户制作指定的模板印章。支持移动端手绘签名；支持上传印章图片；支持自定义印章大小。

印章私密性保护。客户可选择不将印模图片传给 e 签宝。

此服务以 SDK 接口方式提供，业务系统调用接口，传递用户的 e 签宝唯一标识，e 签宝平台根据用户信息完成模板印章制作后立即返回制作完成的电子印章数据，需业务系统妥善保管，作为用户签署印章使用。

签名模板样式请看下表：

印章类型	样例
个人印章模板	
企业印章模板	
二维码印章	*扫描二维码即可查看签署记录信息。使用签名下方的存证 ID 可访问 e 签宝官网查询存证信息。

	
手绘签名	
含时间戳的印章	 2017-08-24 14:51:55

2.3 签署服务

e 签宝提供多样化的签署服务，签署类型支持关键字签署、骑缝章、单页签署和多页签署，签署服务包括 PDF 文档签署、批量文档签署、多人联合签署等。

PDF 文档签署服务：指提取指定 PDF 文档的摘要，并使用指定用户的第三方可信云证书和印章对摘要完成签署，最终组装形成有效的签署后文档。支持平台自身以及平台用户的摘要签署。

多人联合签名：e 签宝提供基于事件证书的多人联合签署，支持上百人签署的场景。该证书只用于证明一个事件本身，包含事件描述和所有签署人信息。

文档批量签名：支持一次意愿认证（例如发送一次手机验证码）实现多份文档签署的场景。

签署位置的定位支持坐标和关键字定位。

2.4 时间戳服务

e 签宝提供同步国家授时中心时间源的可信时间戳签名服务，可用于对用户签署文档进行时间戳固化，证明电子数据在某一个时间点是已经存在的、完整的。可起到防篡改、防抵赖的作用，确保电子文件产生的准确时间点。时间戳固化后的电子数据是具备法律效力的电子凭证。

e 签宝标准签名流程中里都包含时间戳固化。用户可在签名信息中查看时间戳值。

2.5 签署身份认证服务（意愿认证）

意愿认证是指在每一次签署前对用户的身份进行确认，保证是用户本人操作

的认证方式。例如在使用支付宝付款时用户需要输入密码或按指纹。快捷签提供的意愿认证方式有短信验证码、语音验证码、UKEY 和刷脸登录。

2.6 查看签署证明 & 验签

二维码样式印章扫码后可跳转签署证明页面，包含签署记录信息和用户数字证书信息，支持点击一键出证。

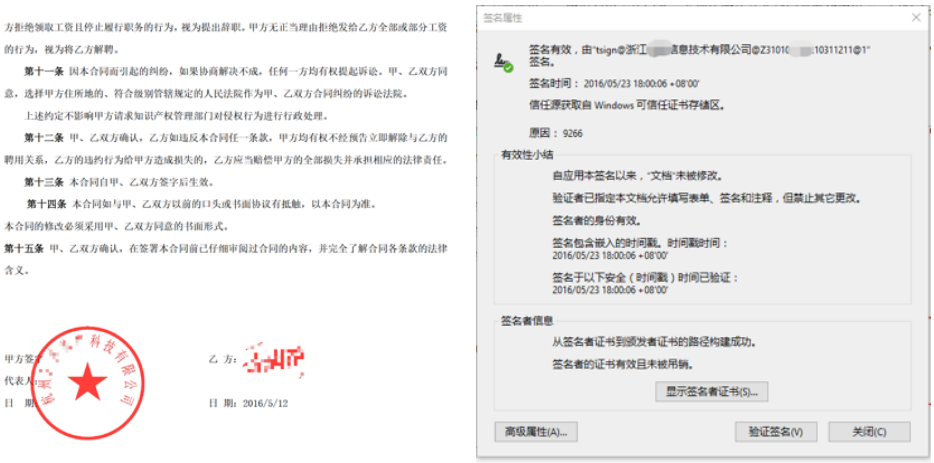
所有签署电子合同或数据可验证有效性和真实性 ,保证原文未改、签名未改。验签服务包括：

- e 签宝官网验签服务

- 快捷签验签接口服务

  在快捷签 SDK 中提供验签 API 接口，验证签署文档的真实性。

- Adobe reader 离线验签服务

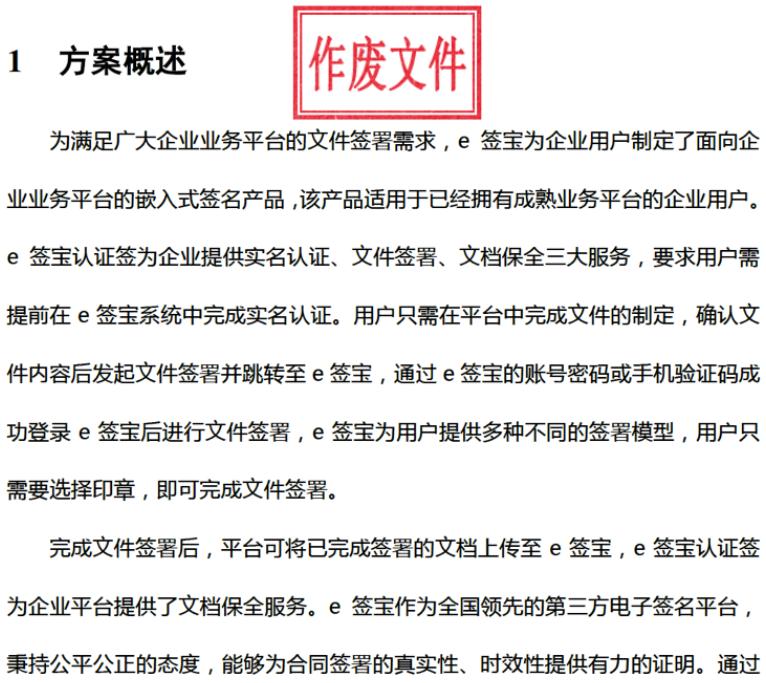


2.7 合同解除/作废

根据《合同法》对于合同解除权的相关规定：当事人协商一致，可以解除合同。合同解除后，尚未履行的，终止履行；已经履行的，根据履行情况和合同性质，当事人可以要求恢复原状、采取其他补救措施，并有权要求赔偿损失。

因此，平台商户需把控业务流程，确保合同解除的发起经过所有签署人的同意。

e 签宝提供合同解除接口，并且在合同上加盖“文件作废章”。



2.8 文本签名

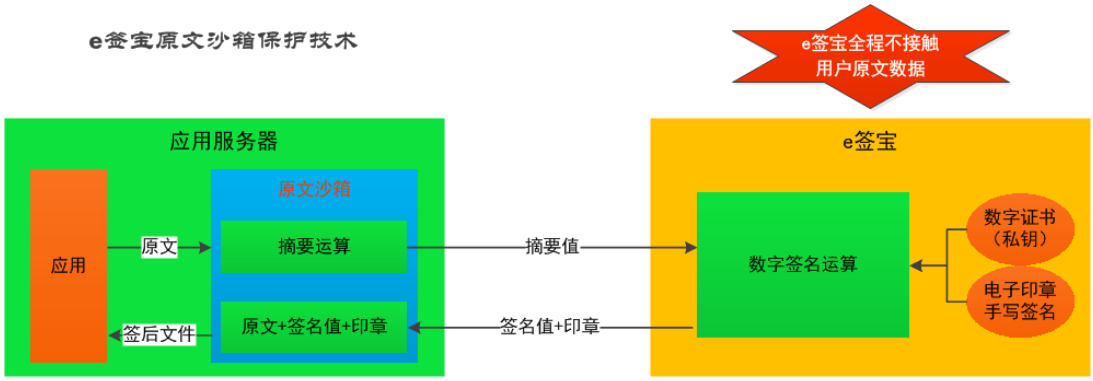
就是提取指定文本数据的摘要，并使用指定用户的第三方可信云证书对摘要完成签名，最终组装成可验证的签名结果数据包，可以直接解析签名结果数据包验证签名内容的有效性。签名结果数据包需业务系统妥善保管，作为后续验签服务的依据。支持平台自身以及平台用户的签名验签。

2.9 签署记录统计服务

统计审计服务指 e 签宝平台提供专用的管理平台供业务系统管理员查看所有签署记录，了解使用情况。

3 系统安全与性能

3.1 原文沙箱技术



原文保密性：应用平台在调用 e 签宝签署服务时，只需要将摘要发送给 e 签宝。e 签宝全流程不接触用户原文，从而保障用户信息安全。

印章保密性：应用平台可选择不使用 e 签宝模板印章生成服务。在签署过程中直接传入印章图片 base64 完成签名，e 签宝全程不触碰印章图片。

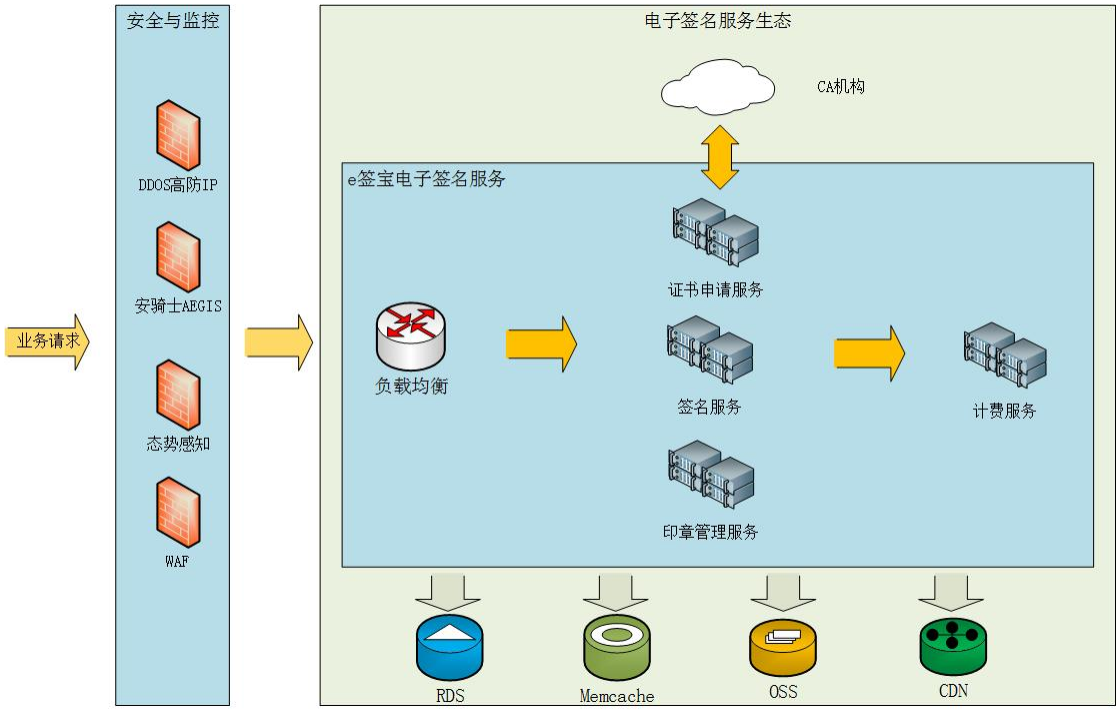
3.2 数据加密/HTTPS 传输加密技术

为确保用户信息和文档在 e 签宝平台中的机密性，e 签宝对所有用户数据和文档均进行了加密处理。同时，对 e 签宝所有的 web 页面访问、接口服务访问，全部采用 HTTPS 确保传输机密性。全程采用 2048 位非对称加密交换加密密钥；采用 128 位对称加密，确保传输通道时刻处于加密状态。

3.3 区块链分布式存证

e 签宝成立了专门的区块链研发团队，与众安等合作，共同推进基于区块链的存证应用。用户通过 e 签宝可以将电子合同、签署主体、文件哈希值等信息在区块链存储，一经存储任何一方无法篡改，确保用户的电子证据有效性和安全性。

3.4 连续性保障



- 热备容灾

e 签宝具备“两城三中心”容灾体系。每份数据多份副本存储，接近实时备份机制。在各个地域采用多物理机房部署，实现同城容灾。

- 负载均衡

实现 7 层的负载均衡。所有负载均衡均采用集群部署，集群之间实时会话同步，以消除服务器单点，提升冗余，保证服务稳定。SLB 在整体设计上让其可用性高达 99.99%。且能够根据应用负载进行弹性扩容，在任意一台 SLB 故障或流量波动等情况下都能做到不中断对外服务。

- RDS 关系型数据库

RDS 是一种稳定可靠、可弹性伸缩的在线数据库服务。RDS 默认采用主备架构（备用实例正常情况下对用户不可见），两个实例位于不同服务器，自动同步数

据。主实例不可用时，系统会自动将数据库连接切换至备用实例。切换是分钟级别，而且不需要人工介入，全部由系统自动完成，应用系统也无需任何变更。这种架构足以满足大部分 d 用户的高可用需求。

- 多 CA 通道切换

e 签宝与国内权威 CA 中心合作，包括 CFCA、浙江 CA、中认环宇、四川 CA 和河南 CA 等长期合作。在证书申请过程中具备多 CA 证书申请机制，保证整个证书申请流程的流畅、可靠。

- 多云部署

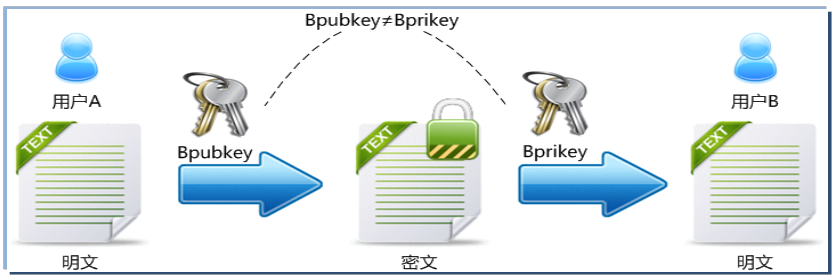
e 签宝在阿里云、百度云和腾讯云都有相应服务部署，确保服务性能和质量，用户对电子签署服务连续性可 100%放心。

- 24h 服务应急中心

e 签宝安全技术支持团队建立了 7*24 应急响应中心，为客户提供高质量、贴心的售后服务。

4 电子签名技术原理

4.1 非对称算法



传统的算法加密密钥与解密密钥相同，称之为对称算法；1976 年出现的非对称算法，加密密钥与解密密钥不同，这对密钥一个称为公钥，一个称为私钥。公钥是公开的，互联网中任何人都可以取得所有他人的公钥；私钥是私密的，只有持有人自己才能使用。

用户 A 向用户 B 发送秘密信息时，使用 B 的公钥加密信息；B 收到文件后，使用私密的私钥解密信息。

除了实现数据的机密性传输之外，非对称算法还可以达到防抵赖的目的。原理是 A 使用自己的私钥加密文件；B 收到文件后，使用 A 的公钥解密；如果能够解密的，证明文件一定来源于 A。

4.2 摘要算法

摘要算法，也叫做哈希算法、指纹算法、杂凑算法。就像每个人的指纹一样，任何不同的数据经过摘要算法后得到的结果都是不同的，而任何相同的数据经过

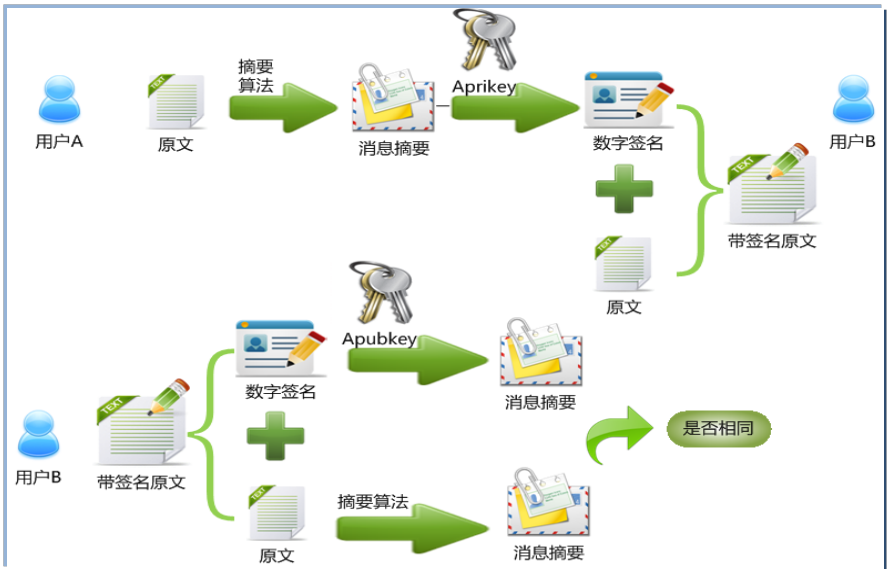
摘要算法后得到的结果都是相同的。因此，摘要结果又称之为数据的数字指纹。

摘要算法常常用于密码的校验。为了防止密码以明文方式保存数据库造成的安全隐患，常常对密码进行摘要算法后保存在数据库；在身份认证时，对用户输入的密码再做一次摘要，并与数据库中的摘要进行比较；如果相同，则认证通过。

摘要算法也常常用于实现数据的完整性校验。我们将数据进行一次摘要运算，将结果与数据原文同时保存或发送给另一方；在校验时，将数据原文再做一次摘要，并将结果与原摘要结果进行比对，如果相同说明未被篡改，如果不同则说明原文被篡改。

4.3 数字签名

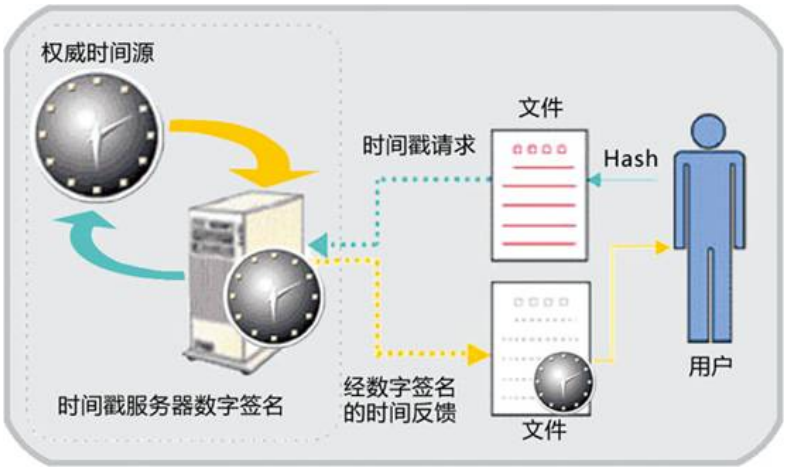
数字签名的目的有两个，分别是防抵赖和防篡改。因此，数字签名是非对称算法和摘要算法的联合使用。其原理如下：



4.4 时间戳

时间戳是“数字证明”中的另一个关键环节，即证明某数据在某个时间存在，

并且未被篡改。时间戳的原理是将原始数据经过一次摘要运算，将摘要结果发送给时间戳签发中心，时间戳签发中心使用数字签名技术对摘要结果和当前时间进行一次数字签名，由于摘要结果是原文的数字指纹从而得以证明该原文在这个时间存在，同时解决了防篡改问题。其原理如下：



4.5 PADES 数字签名标准

PAdES 是由 ISO32000 定义、由 ETSI 维护的 PDF 数字签名规范。几乎所有的 PDF 阅读器均遵循这一规范 ,从而确保生成的数字签名可以在不同的 PDF 阅读器中被正确验证。

4.6 e 签宝核心技术总结

e 签宝通过数字签名+时间戳技术，生成符合 PADES 标准的数字签名，并且最终以 PDF 形式来保存和展现。

1) e 签宝通过数字签名技术解决了防抵赖、防篡改目的；

2) e 签宝通过时间戳技术解决了证明某文件在某时间存在目的；

3) e 签宝通过符合最终生成符合 PADES 标准的 PDF 文件 ,达到数字签名和

时间戳能够被所有标准 PDF 阅读器识别和直观验证的目的。