基于文档的电子签名白皮书

目录

概念

电子签名是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。通俗点说，电子签名就是通过密码技术对电子文档的电子形式的签名，并非仅仅是书面签名的数字图像化。它是电子文档数据安全的重要保障手段。例如在涉密文件或重要合同文件上的电子签名等。电子签名系统一般采用 PDF 版式文档格式来实现电子签名功能。

在国家政策鼓励、厂商产品迭代升级、企业数字化转型需求等因素的推动下，电子签章的应用场景变得越来越广泛。国内外也涌现出很多耳熟能详的电子签名服务提供商，包括互联网电子签名提供商、版式文档提供商引入电子签名服务、CA 公司对业务的扩展等。

抛去不同电子签名厂商不同的身份认证方式、以及电子签名过程多种多样的增值服务，目前互联网电子签名的核心过程都是需要先将待签署文档转换成 PDF 格式，上传至某个服务器，额外再定义一些独立于 PDF 文档本身的签名流程，比如签名顺序、签名位置、需要填写的字段等，文档从发起那一时刻起，就决定了只能在某个指定的系统上完成。利用 PDF 的数字签名和验证原理，可以对单个数字签名有效性和文档完整性进行验证。对于签署过程信息、签署方身份认证信息以及意愿认证信息等内容，都需要由电子签名服务提供商的增值服务来提供，比如针对签署过程出示的签署证明等材料。

我们将这种签署前需要将待签署文档上传至某服务器，签名在发起以后，都需要在同一个第三方平台上完成签署的过程称为 – 基于交易的签名（transaction-based signature）。

跟此种签名方式对应的有 – 基于文档的签名 （document based signature），基于文档的签名是以文档为中心的签名，可以不对身份认证方式和途径做限制，不对签名时所用证书来源做限制，签署方不限定必须使用某个平台，却可以将签署过程信息都直接保存在文档里。用户只需要使用 PDF 文档处理工具打开文档，选择各签署相关方认可的身份认证方式和途径在 PDF 文件上做签名即可，签名验证时签署过程信息以及身份认证信息都可以直接从文档中读取并展示出来。基于文档的签署，是一种更贴近和还原物理签章体验的签名方式。

基于文档的电子签名应用

基于文档的签名以文档本身为核心，用户在使用 PDF 文档处理工具打开待签字盖章的文档，进行必要的填写并定稿以后，继续在 PDF 文档处理工具里就可以继续完成签名，就像是物理签字盖章过程中，拿着笔签字书写或者拿着章加盖一样流畅自然。

基于文档的签名，当需要多人填写并签署时，并不需要像基于交易的签名一样，填写和签署需要分成两个过程来进行，所有的签署相关方都需要先填写完毕，再重新进行一轮签署。基于文档的签名，当进行到某个签署相关方时，填写和签署可以同时进行，一步完成。

基于文档的签名，在签名结束后就将签名者的身份信息、签署过程信息、意愿认证信息、签署过程的操作日志信息全部保存在 PDF 文档里。签署好的 PDF 文件本身就像是一个容器一样，不仅可以包含签署时的文档内容，还可以包含这些额外信息。在签名验证时，从文档里读取出这些信息，并进行客观呈现。

基于文档的签名，由于签署信息都可以包含在文档里，可以为被签署文档的后续自动化处理提供方便。文档中包含标准的、可以被机器读取的结构信息，为签署文档的后续存

档、验证以及搜索提供方便，比如可以方便的直接从文档中提取出谁在什么时候签署了文档等信息。

当用户使用基于文档的签名时，可以复用已有的身份认证体系，比如存储在 USB Key 中的证书、第三方平台的账号等。

当用户使用基于文档的签名时，需要进行电子签名的 PDF 文档可以直接在用户之间流转，用户在 PDF 文档处理工具中就可以完成所有的签名相关动作，省去了将文档上传到第三方电子签名系统并且要在文档以外额外创建流程的麻烦。

PDF 标准扩展

为实现基于文档的电子签名，福昕软件对标准的 PDF 表单域做了扩展，在 PDF 表单域的数据字典里可以写入指定的签名者的信息、签名顺序、签名者身份认证方式信息等。

当文档被 PDF 文档处理工具打开时，文档处理工具可以读取 PDF 表单域中的信息，从而判断是否文档是否需要被填写和签署。

根据签章发起者在发起时写入的签名者身份认证数据字典，判断签署者身份是否符合发起者要求。

当身份认证通过的签名者进行签名时，应用可以根据扩展后的标准遍历需要当前签名者填写或签署的 PDF 表单域。

展望

基于文档的电子签名标准已经由福昕软件开放有限公司向 PDF 国际标准委员会提案，获取协会内其他成员的意见反馈后进一步完善。

当市面上的电子签章提供商都使用基于文档的电子签名标准来开发电子签名应用，那么每个签署方只要使用发起方认可的身份认证方式来签名即可，不必须使用发起方所在的签署平台来签署。

文档签署完毕以后，身份认证信息、意愿认证信息都会包含在文档本身，使用任何电子签名验证工具做验证时，签名验证结果、签名流程、签署过程日志信息都可以从 PDF 直接读取出来，帮助签名验证者简洁高效的获取签名验证结果。

当需要从已经存档的海量已签署文档中检索指定人员在指定时间签署的文档时，不需要打开文档，可以直接抽取文档结构中的标准数据，完成目标文档的检索工作。