文档安全需要“看得见”

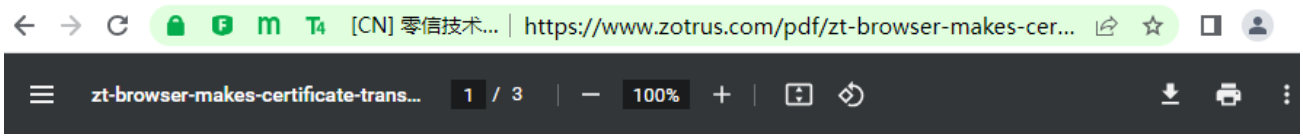
笔者写过文章《网站安全需要“看得见”》讲的是零信浏览器全球独家在浏览器地址展示 4 个不同的图标来让用户一眼就能了解正在访问的这个网站是否安全可信，没有读过这篇文章的读者可以去看看，有利于全面了解零信浏览器的用户界面(UI)创新。今天的文章是文档安全需要“看得见”，属于《网站安全需要“看得见”》的兄弟姐妹篇，都是讲零信浏览器的 UI 创新，而本文讲的是零信浏览器最新推出的 PDF 阅读器功能的 UI 创新，这些创新当然也是密码的应用创新，因为密码看不见摸不着，必须有醒目的 UI 来体验密码应用，体验密码在保护文档安全所做的贡献。

一个文档是否安全，一般来讲是看不见的，大家打开一个 PDF 文件只能看到文档内容，但是这个文档是谁发布了？文档版头所显示的单位名称可信吗？文档末尾的红章可信吗？在纸质文件的时代通过可信渠道收到的公文当然可以依据版头和后面的公章来识别发文单位，这是可信的方式。但是，在互联网数字时代，制作一个精美的假冒身份 PDF 公文非常容易，造假成本为零，这就使得假冒身份文档泛滥，不仅假冒政府公文，而且假冒银行账单通知，假冒学历证书等等，怎么才能有效地帮助用户识别 PDF 文档的真实可信，这是摆在所有电子文档阅读器面前的责任和义务。

所幸的是，Adobe 在发明 PDF 版式文档的同时也采用了密码技术来保证 PDF 文档发布者的可信身份，我国的 ODF 版式文件也有类似的解决解决方案，也是用密码技术实现文档数字签名来保证文档发布者的可信身份。而目前的现状是各种能打开 PDF 文档的阅读器(包括浏览器和各种 APP 内嵌的阅读器和内嵌的浏览器)都不支持实时识别电子文档的数字签名，并没有把密码技术来保障文档安全的应用展示给最终用户，让用户看到文档已有数字签名来保障文档的可信身份。

这就是零信浏览器本次发布升级版本所要解决的问题-让文档安全看得见，让用户在打开文档时就能知道这个文档是否可信，一目了然。用户在使用零信浏览器阅读一个 PDF 文档时，浏览器地址栏上展示的各种图标笔者在《网站安全需要“看得见”》都讲清楚的，本文详细讲一讲浏览器文档阅读栏(PDF 栏)的创新 UI 展示，也就是地址栏下面的一栏。

如下图所示，目前几乎所有浏览器在阅读 PDF 文档时会在地址栏下面增加一个文档阅读栏来展示文档相关的功能，如展示文档所有页面、文档文件名、页码、放大缩小、窗口宽度、页面旋转、文档下载、文档打印、全屏演示等等各种文档操作相关的功能。



零信浏览器认为在文档阅读栏的第二个黄金位置重复显示文档文件名完全没有必要，因为地址栏上已经显示了完整的文件名。零信浏览器创新地把黄金位置变成了文档安全展示栏，零信浏览器会在打开阅读文档时实时验证此文档是否有数字签名，如果有，则验证是否可信，如果可信则展示文档签名者可信身份，如下图 1 所示。如果没有，则显示“此文档无数字签名，发布者身份未知。请谨慎！”这是最重要的文档不安全“看得见”，非常醒目的提醒用户注意，以便上当受骗！如下图 2 所示。

图 1

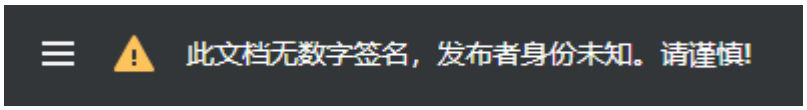


图 2

这就是文档安全看得见！那么，文档安全看得见有哪些图标呢？如下图 3 所示，零信浏览器除了提醒用户注意没有数字签名的文档的安全外，还创新地增加了 5 个非常有特色的“看得见”的文档安全，能真正帮助用户看得见正在阅读的文档是否安全可信。

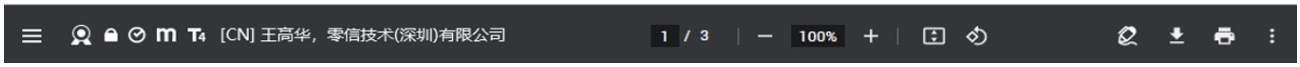


图 3

第一个“看得见”的安全是文档已数字签名标识

这个标识明确告诉用户正在阅读的文档有可信数字签名，用户还可以点击文档阅读栏最右边的“签名面板”图标 来查看文档数字签名的详细信息，如下图 4 和图 5 所示，这些信息包括信任源来自哪里、文档是否被修改、文档是否有时间戳、是否支持 LTV(签名长期有效)、签名证书的详细信息等等。

图 4

图 5

第二个“看得见”的安全是文档已加密标识

这个标识明确告诉用户正在阅读的文档是已经加密的文档，如果用户有权阅读此文档，则自动解密文档无缝阅读，如下图 6 所示。如果零信浏览器找不到用于解密的数字证书，则提醒用户无法解密，如下图 7 所示。这是保障机密文档安全的唯一可靠技术手段，因为只要文档不加密，就无法保障文档不会被非法泄露出去。但是，如果文档用有权阅读者的加密证书加密的话，则即使机密文档被泄露出去，但是由于无法获得有权阅读者的证书私钥而无法解密，从而有力保障机密文档的安全。

图 6

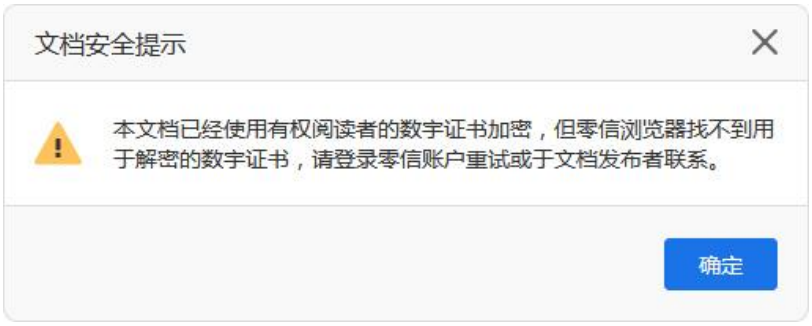


图 7

第三个“看得见”的安全是文档已有时间戳标识

这个标识明确告诉用户正在阅读的文档是有时间戳签名的，文档签名时间是可信的，如下图 8 所示，此文档不仅有数字签名而且还是零信浏览器信任的时间戳签名-“签名包含嵌入的时间戳”。如果文档签名时没有使用时间戳签名服务，则显示“签名时间来自签名者计算机上的时钟”，如下图 9 所示。大家都知道计算机时间是可以随意修改的，这是一个不可信的时间。所以，对于需要证明签名者是何时签署文档的，时间戳就是唯一解决方案，能保证签名时间是可信的、不可否认的和不可篡改的。有很多应用都是需要有时间戳的，如电子合同签署、公文发布、投稿文件、投标文件等都是有可信签名时间要求的。零信浏览器已经预置信任了部分时间戳服务提供商的时间戳签名证书，仅显示零信浏览器信任的时间戳签名。

请同时注意另一个相关的“看得见”-LTV(签名长期有效)，这是同时间戳有关的技术参数。如果签名时间来自签名者计算机时钟，这是一个 Adobe 阅读器设置的默认 LTV 状态，前提是信任签名者的计算机时间。而对于“严格 LTV”状态仅在文档签名内嵌时间戳时才会显示，表示不信任签名者的计算机时间，因为这是可以随意修改的。

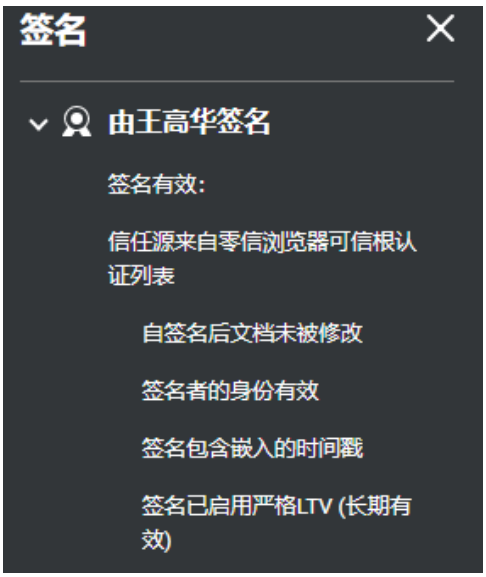


图 8

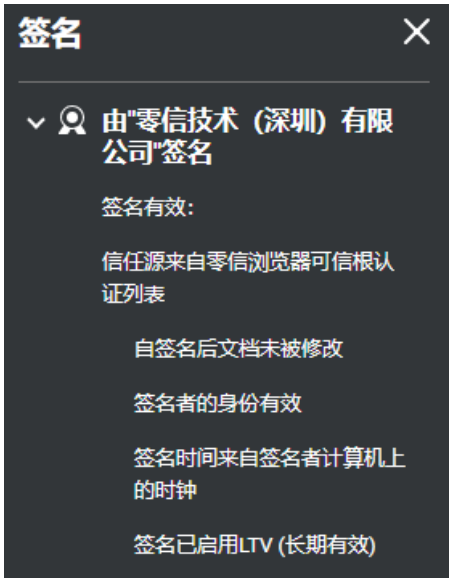


图 9

第四个“看得见”的安全是文档已国密合规标识 m

这个标识明确告诉用户正在阅读的文档是采用国密算法数字签名证书签名的，或者采用国密算法加密证书加密的。根据我国《电子签名法》和《密码法》，可靠的数字签名应该采用国密算法来实现，但鉴于常用的 Adobe 阅读器不支持国密算法，这就限制了采用国密算法实现文档签名的应用场景。零信浏览器 PDF 阅读器支持验证国密算法数字签名 PDF 文档和 OFD 文档，并展示国密合规标识，为普及国密算法数字签名电子文档打下了应用基础。

零信浏览器 PDF 阅读器支持双算法双数字签名实时验证，并优先展示文档中的国密算法数字签名。计划提供的零信文档数字签名服务也都是默认采用双算法文档签名证书实现双签名和双时间戳，RSA 签名仅用于兼容 Adobe 阅读器，而国密签名则是为了国密合规。而对于文档加密，采用国密算法实现加密更加安全可靠，所以，零信浏览器 PDF 阅读器采用了国密 HTTPS 加密一样的国密合规标识(**m**)来展示国密算法数字签名和文档加密，如下图 10 所示。

图 10

第五个“看得见”的安全是文档签名者身份认证级别标识和签名者的可信身份信息 T4

这个标识明确告诉用户正在阅读的文档的签名者的可信身份认证级别，分 T1/T2/T3/T4 四个级别，并认证标识后面展示签名证书中的 CN 字段和 O 字段(如果有)信息，按照[国家缩写]+CN 字段格式展示。其中 T1 级别只显示签名者的电子邮件地址，因为签名者仅验证了电子邮箱，如下图 11 所示；T2 级别展示签字者的个人姓名，因为签名者已验证了个人身份，如下图 12 所示；T3 级别展示签名者的单位名称，因为签名者验证了单位身份，如下图 13 所示；T4 级别展示签名者的个人姓名和单位名称，因为签名者不仅验签了个人身份而且验证了单位身份，签名者属于这个单位的员工，如下图 14 所示。

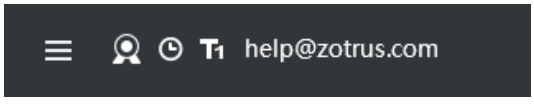


图 11

图 12

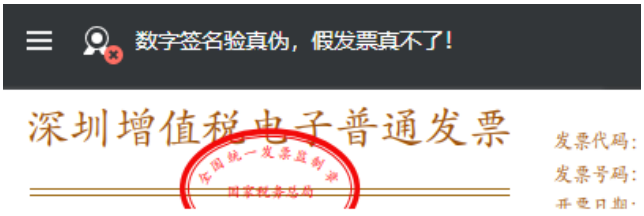
图 13

图 14

可能有读者有疑问，为何单位员工签名的认证级别为 T4 比单位签名的认证级别 T3 还要高呢？这是沿用了 SSL 证书的身份认证级别的前 3 类，T3 认证类似于 OV SSL 证书的认证级别，验证了单位身份。在 SSL 证书的 T4 认证标识用于扩展验证身份的 EV SSL 证书，而零信浏览器沿用 T4 标识用于单位员工的数字签名，意思是 T3+1 认证，不仅认证了单位身份，而且还认证了单位员工身份，所以使用 T4 认证标识也是合理的。

零信浏览器认为区分文档数字签名的可信认证级别非常重要，因为仅仅展示文档有数字签名还是不够的，在欧洲许多公司名称同个人姓名是一样的，不像我国的公司名称同个人姓名有明显的不同，所以，直接明确地告诉用户签名者是个人还是单位或是单位员工就非常重要，让用户能准确地根据签名者的身份来做出正确的处理决策。

值得一提的是，零信浏览器不仅展示文档数字签名者的可信身份，而且特别为我国的电子发票的验证和展示做了优化，虽然电子发票也是 PDF 文档，但是电子发票是有特殊用途的 PDF 文档，所以，零信浏览器在验证了电子发票数字签名后直接提示发票真假，这就大大方便了用户识别电子发票的真假。而 Adobe 阅读器只会显示“至少一个签名有问题”，这是因为电子发票所用的数字签名证书不是 Adobe 信任的证书。



相信广大读者通过上面的 5 个“**看得见**”的文档安全一定能全面了解一个文档是否安全可信，5 个安全“**看得见**”加上 1 个“不安全”的“**看得见**”，共计 6 个“**看得见**”能有效和高效帮助用户对正在阅读的文档是否安全可信一目了然，这些创新由零信浏览器全球独家提供，能真正切实保障用户的上网安全。

笔者坚信：文档安全是继网站安全(HTTPS 加密)之后的最重要的最主要的安全业界的第二个发力点，因为文档已经无处不在，也正是因为其无处不在而导致了文档安全问题成为了一个急需解决的问题，而要解决文档安全问题的唯一解决方案是用密码技术来保护文档安

全，用数字签名、加密和时间戳来保障文档的身份可信、不可篡改、加密保护和文档发布时间可信。

保障文档安全要做的第一件大事就是让文档安全看得见，让用户非常容易地知晓正在阅读的文档是否安全，零信浏览器全球独家率先实现了，欢迎广大用户免费 下载 使用零信浏览器，体验文档安全看得见，保护自身上网安全。

有诗为证：

文档安全很重要，

数字签名是关键。

展示签名为必须，

签名可视真安全。

王高华

2023 年 10 月 11 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。