CA 是数据安全的保护神-“靠神”

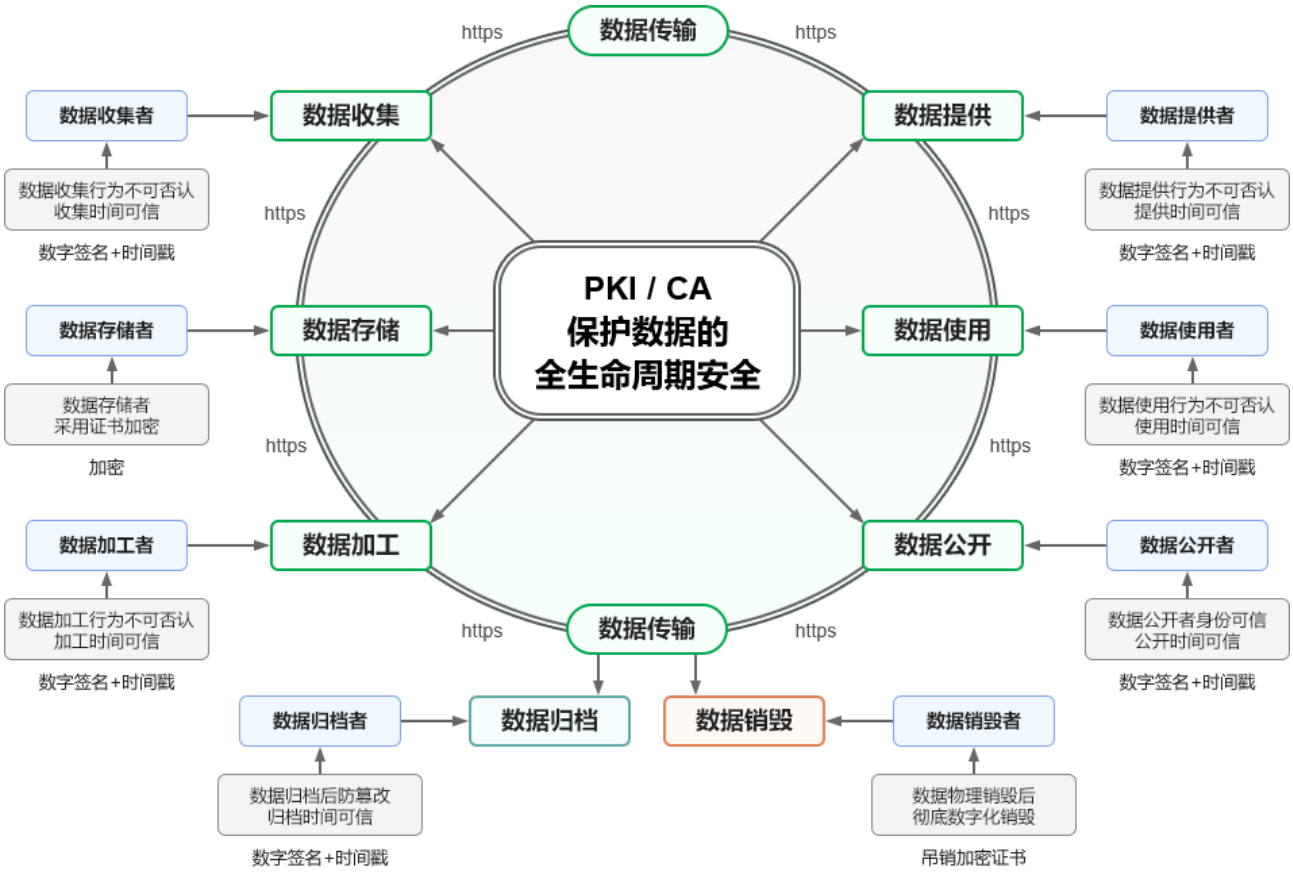
数据安全有多重要，从专门出台一部《数据安全法》就知道了。但是《数据安全法》只在第三条定义了何为“数据安全”–“指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。” 全文都没有“加密”和“密码”等文字，也就是说只是强调必须采用必要的措施来保障，至于什么措施，未做具体要求。

笔者认为：密码是这个“必要措施”的最可靠的措施，CA 是数据安全的保护神。根据 CA 英文谐音，笔者把这个保护神命名为“**靠神**”，一个**靠**谱的、可**靠**的、**靠**得住的保护**神**，一个数据安全的**靠山**！本文的“CA”泛指 CA 机构、CA/PKI 系统和 CA 证书。本文首先讲一讲 CA/PKI 密码技术是如何保护数据安全的，再讲一讲 CA 机构的哪些特质是保护数据安全的关键力量，最后讲一讲 CA 机构应该如何抓住机遇当好这个保护神，做一个可信赖的数据安全的“靠神”。

根据《密码法》第二条对密码的定义-“密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务”，密码就是用于加密保护数据安全的技术、产品和服务，同时用于数据访问者的安全认证，讲得非常清楚。而 PKI/CA 技术是密码的一个最重要的应用，用数字证书实现数字签名、加密和时间戳来有效保护数据安全，保护数据的全生命周期安全。

一、PKI/CA 是保护数据安全的最可靠的技术

依据《数据安全法》第三条对“数据处理”的定义，数据处理包括数据的收集、存储、使用、加工、传输、提供、公开等。PKI/CA 技术有效保障每一个数据处理过程中的数据处于有效保护和合法利用中，使得数据从生产到销毁的全生命周期都处于持续安全状态。其中，最重要、最核心和最基础的数据保护是：数据在全生命周期中的流通传输都必须是通过 https 加密通道传输，当然是采用商密算法的 https 加密。



在数据收集阶段，数据收集者必须有身份证书，并用其身份证书数字签名收集的数据，同时附署时间戳签名，以证明数据收集行为不可否认和数据收集时间可信。这一点非常重要，很多应用场景要求事后追责时如果有原始数据的数字签名加时间戳，那就能证明这份数据就是原始数据，能依据《电子签名法》确认原始数据是可信的数据，是没有被篡改的。

在数据存储阶段，数据存储者必须用数字证书或加密密钥来加密数据，只有这样才能保证数据在存储中的安全，特别是现在是云存储时代，用证书加密存放在云上才是唯一一个能保证数据安全的技术手段。欧洲 eIDAS (电子身份认证和信任服务法) 就有对加密数据泄露的免责和减轻责任的条款，这个也很好理解，因为加密数据即使是泄密了，只要加密的私钥没有泄露，数据还是安全的。

在数据加工阶段，数据加工者必须有身份证书，并用其身份证书数字签名加工的数据，同时附署时间戳签名，以证明数据加工行为不可否认和数据加工时间可信。这一点非常重要，很多应用场景要求事后追责时如果有已加工数据的数字签名加时间戳，那就能证明这份数据是谁加工的和何时加工的，这是不可否认的，具有法律效力。

在数据提供阶段，数据提供者必须有身份证书，并用其身份证书数字签名提供的数据，同时附署时间戳签名，以确保数据提供行为不可否认和数据提供时间可信。这一点非常重要，很多应用场景要求事后追责时如果有已提供数据的数字签名加时间戳，那就能证明这份数据是谁

提供的和何时提供的，这是不可否认的，具有法律效力。

在数据使用阶段，数据使用者必须有身份证书，并用其身份证书数字签名使用的数据，同时附署时间戳签名，以证明数据使用行为不可否认和数据使用时间可信。这一点非常重要，很多应用场景要求事后追责时如果有已使用数据的数字签名加时间戳，那就能证明这份数据是谁使用过和何时使用的，这是不可否认的，具有法律效力。

在数据公开阶段，数据公开者必须有身份证书，并用其身份证书数字签名公开的数据，同时附署时间戳签名，以证明数据公开的身份可信和和数据公开时间可信。这一点非常重要，可以有效防止各种假冒文件、虚假信息的传播，只信任有可信数字签名的数据(文件、信息)，提升数据公开发布者的可信度。由于公开的数据有数字签名加时间戳，那就能证明这份数据是谁公开的和何时公开的，这是不可否认的，具有法律效力。

当数据不再使用和不再有效时，会归档此数据或销毁此数据。数据归档者必须有身份证书，并用其身份证书数字签名归档的数据，同时附署时间戳签名，可以保证归档后的数据不会被非法篡改和归档时间可信，以备以后需要查档时验证数据的真实性。同时，由于归档的数据有数字签名加时间戳，就能证明这份数据是谁归档的和何时归档的，这是不可否认的，具有法律效力。而对于销毁数据，除了物理删除数据外，还必须吊销用于加密此数据的加密证书，以确保即使此数据有未知的泄露，但是由于加密证书已吊销，则即使拥有这份泄密数据的副本也将无法解密，实现彻底的数字化销毁。

二、CA 机构是保护数据安全的关键力量

从上一段落的数据安全解决方案可以看出，PKI/CA 系统签发的身份证书可用于保证数据处理者的可信身份和数据处理时间的可信及不可否认。SSL 证书则用于整个数据处理流通过程的全程 https 加密，保证了数据在传输过程中不会被非法窃取和非法篡改，这是数据处理的最低的、最基本的安全保障要求。

CA 机构不仅是依据《电子签名法》的唯一签发用于数字签名的身份证书的机构，而且一直在用户提供各种数据的数字签名和时间戳签名服务。不仅有《电子签发法》的法律保障，而且还有相关主管部门的行政管理，使得 CA 机构为用户提供可靠的数据的数字签名和时间戳服务不仅有法律保障，而且有服务质量的保证。

CA 机构同时作为 SSL 证书提供商也可以为用户签发 SSL 证书用于各种数据流通系统的 https 加密，签发双算法双 SSL 证书，实现自适应加密算法的 https 加密。

CA 机构的客户服务体系也是一个珍贵的资源，包括在覆盖全省全市的政务服务中心的服

务网点，还有优质的客服呼叫中心，这些都能有效地为保护数据安全服务提供有力的服务保障。

更重要是，CA 机构同时拥有国密局和工信部颁发的 CA 服务许可证，受两个部门的监督和管理，这为作为数据安全保障服务提供了坚强的信用保证和实力证明，大大增强了用户对 CA 机构提供的数据安全产品和服务的信心。所以，笔者认为：CA 机构是保护数据安全的关键力量，是可靠的数据安全产品和服务提供商。

三、CA 机构应当及时抓住机遇，做一个可信赖的数据安全的“靠神”

我国已经组建国家数据局，将在统筹数字中国全面建设、推动数字经济高质量发展、推进数字社会治理创新等方面提供坚实的支撑，增强国家在数据领域的核心竞争力，进一步推动数据的整合共享，进一步加强数据安全保障和管理。CA 机构应该当仁不让地抓住这个大好机遇，积极改革创新，从以下四个方面布局和努力，尽快从一个证书颁发机构转型为一个数据安全服务提供商，做一个**靠**谱的、可**靠**的、**靠**得住的数据安全保护**神**。

第一，在现有的 USB Key 证书签发和服务体系的基础上，研发和完善数据安全认证相关产品和解决方案，为数据安全认证提供更好用的产品和服务。

第二，改造和升级现有 CA 系统，能为用户签发合规的和合格的国密 SSL 证书和全球信任的国际 SSL 证书，以支持自适应加密算法的 https 加密。

第三，必须能为用户提供零改造实现国密 https 加密的相关产品和解决方案，让用户轻松实现整个数据流通过程的全自动化国密 https 加密，保障数据传输链路的安全。

第四，建设或升级云密码服务基础设施，为各种云服务提供保障数据安全所需的密码服务，如：网站安全云服务、云签名服务、云时间戳服务、云密钥管理服务、云加解密服务等等，让密码真正能融入到整个数据处理的各种环节中来保障数据的全生命周期安全。

王高华

2023 年 4 月 26 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。