

## DSaaS, an Innovative Cloud Cryptography Service

(Mar. 19, 2021)

The author believes that many readers are familiar with the term "SaaS", but considering that some non-IT readers may not know it, let me briefly introduce SaaS.

**SaaS is Software as-a-Service.** SaaS is an innovative software application model that has emerged in the 21st century with the development of Internet technology, cloud computing technology and the maturity of application software. In the traditional model, vendors deploy software products to multiple clients within the enterprise for delivery by selling software licenses. SaaS defines a new delivery method, and makes the software further return to the essence of service. The essence of enterprise deployment of software is for its own operation and management services. The appearance of software is the informatization of business processes, and the essence is still a service model. SaaS has changed the way of providing traditional software services, it greatly reduces a large amount of early-stage investment to further highlight the service attributes of software and has gradually become the main delivery model of the software market.

For document signature, in traditional model, software vendors develop PDF document readers or document e-signature tool software, support digital signature technology to implement PDF document digital signatures. The user deploys document readers or document e-signature software to multiple clients within the enterprise for delivery for free or for a fee. At the same time user also need to purchase and apply for PDF document signing certificate from the CA, and laboriously configure the PDF signing certificate for each client, and user also need to find and setup a free or charged timestamping service, then user can complete the digital signature of PDF document, thereby ensuring the security and trust of the document.

Traditional document digital signature solutions are very cumbersome and difficult to

implement. This leads everyone to know that the document does not have a digital signature that cannot be proven to be a trusted document and need to be signed. However, because the document digital signature technology is too troublesome, they have to give up document signature and letting unsecure unsigned documents continue to exist, there are many important documents such as notification or certification issued by the e-government system. The author believes that this is "ostrich thinking".

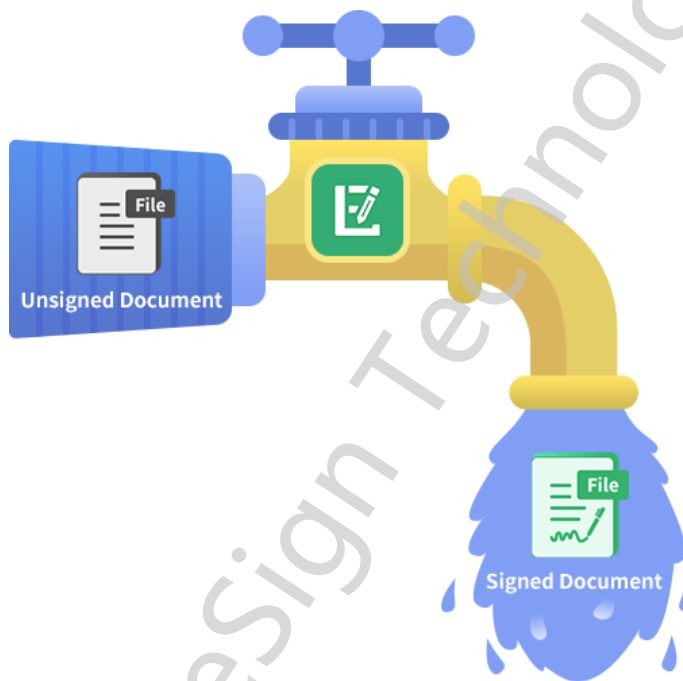
Of course, there are also vendors trying to solve this document signature problem, such as some e-signature platforms, users must upload the document to be signed to the e-signature platform, and the platform use its own PDF signing certificate to digitally sign these documents or use the untrusted signing certificate to digitally sign these documents.

The biggest problem with this solution is that users must first leak the document to the e-signature platform in order to sign the document, which cannot effectively protect the confidential information of the document. The second is the problems of document signing certificates that the former often uses electronic signature, not a digital signature, and the signatory does not have signing certificate, and it is impossible to ensure the trusted identity of the signatory. It is only guaranteed that the document will not be illegally tamper with using the platform signing certificate. The latter also does not guarantee the identity of the signatory. The Adobe reader will display "The signature has problems", so that the end user cannot confirm whether the identity of the document signatory is trusted, so we can't see the value of such digital signature.

MeSign Technology has found an innovative solution through years of hard work and exploration, allowing the e-signature tool software to return to the essence of service. What the users need is document signature service, not a document signing certificate, and not a document reader that does not support digital signature. MeSign Technology has developed the e-signature tool and e-signature system and built a cloud cryptography infrastructure. The combination of "cloud" and "client" allows users to digitally sign the document automatically using MeSign App without applying for a document signing certificate from the CA and without purchasing the timestamping service from other providers. This idea of solving the

problem of document signature is the same as that of **SaaS**, so we call "**DSaaS**".

**DSaaS** is Document Signature as-a-Service, which is the document digital signature service provided by MeSign Technology for users around the world now – MeSignDoc service. This is an innovative cloud cryptography service that makes the very complex and difficult-to-use document digital signature technology very easy, allowing users to sign PDF document with one click. Only in this way, the document digital signature can be popularized, and to truly guarantee the document security and trust. MeSign Technology make the document digital signature service as a cloud service (**DSaaS**) available as tap water at any time.



Finally, let me talk about the entire implementation process of DSaaS in detail. users only need to use the document signing service provided by MeSign App, select the document to be signed, and MeSign App will automatically connect to the cloud identity validation system to verify the user's identity, and automatically apply for document signing certificate to the cloud CA system and cloud key management system. At the same time, MeSign App will generate the HASH data of the document to be signed on the local computer and post it to the cloud e-Signing service system. The cloud e-Signing service system automatically uses the user's signing certificate to digitally sign the document HASH data, and automatically call cloud timestamping service to attach timestamp data to the signed HASH data to prove document signing time trusted, and at the same time call certificate revocation system to generate the

LTV data to ensure that the signature is still long time valid after the document signing certificate has expired, and finish the HASH data signature according to international standards, then return the finished signed data to MeSign App, and MeSign App completes the digital signature of the document locally, the signed document is global trusted and global legal effect.

The whole process may seem a little complicated for you, but just like tap water, you don't need to care about how the water comes, you just need to turn on the tap and the water will come. You only need to use MeSign App document signing service and click “Sign” to finish the document digital signature!

**DSaaS**, an innovative cloud cryptography service, is exclusively provided by MeSign Technology in the world! Welcome to [download](#) MeSign App, purchase the Starter Edition service (US\$9.80), enjoy the **DSaaS**!

----- END -----



Want to contact me to discuss this topic? Please use [MeSign App](#) (  ) to scan the QR code and send me an encrypted email, I will reply to your encrypted email ASAP.