Aug 27, 2020

NEWSLETTER

By : Thomas Ariyanto

THE FUNCTION AND LEGAL POWER OF ELECTRONIC SIGNATURES IN INDONESIA

During the COVID-19 pandemic in Indonesia since March 2020, various services such as overseas flights and other economic activities in Indonesia have stopped. Lots of Indonesian investors are unable to fly back to Indonesia to continue their business activities. Numerous obstacles caused this to happen, and one of them is the signing of documents for their company in Indonesia. In such circumstances, documents that were signed from overseas by the investor and will be used in Indonesia shall be consularized to the Indonesian Embassy. However, during this pandemic, some of the Indonesian Embassies have closed their services. In that case, this can be solved by using a certified electronic signature ("**E-signature**") created by an Indonesian electronic certification organizer.

E-signature is regulated by Law No. 11 of 2008 on Electronic Information and Transactions which has been amended by Law No. 19 of 2016 on Amendment of Law No. 11 of 2008 on Electronic Information and Transaction ("**UU ITE**") and Government Regulation No. 71 of 2019 on Electronic Systems and Transactions ("**PP PSTE**").

Based on UU ITE and PP PSTE, E-signature is a signature consisting of electronic information that is attached, associated, or related to other electronic Information, used as a verification and authentication tool.

E-signatures serve as a means of authenticating and verifying the identity of the signing and the integrity and authenticity of electronic information.

In Indonesia there are two types of E-signature as follows:

1) Certified E-signature

   A certified E-signature shall meet the following requirements:

   a) fulfill the validity of the legal force and the legal consequences of the Electronic Signature;
   b) use Electronic Certification made by electronic certification organizer services; and
   c) created using a certified Electronic Signature Maker Tool.

2) Uncertified E-signature

   An uncertified E-signature is made without using the services of the Indonesian electronic certification service.

Based on the legal perspective, a certified E-signature has a strong evidentiary power before a court.

E-signatures have legal force and legal consequences if:

1) E-signatures source data related only to signatories;
2) E-signatures source data during the signing process is only in the power of the signatory;
3) any changes to the E-signature that occur after the time of signing can be known;
4) all changes to electronic information related to the E-signature after the signing time can be known;
5) there are certain methods used to identify who is the signatory;
6) there are certain ways to show that the signatory has approved the related electronic information.

The above terms are the minimum requirements that must be fulfilled in every electronic signature. This provision opens the broadest opportunity for anyone to develop methods, techniques, or the process of making electronic signatures.

In Indonesia, there are currently six electronic certification organizers consisting of two government and 4 private institutions namely;

1) The National Cyber and Code Agency (*Badan Siber dan Sandi* "BSSN");
2) The Technology Assessment and Implementation Agency (*Badan Pengkajian dan Penerapan Teknologi* "iOTENTIK");
3) Money Printing Agency of the Republic of Indonesia (*Badan Percetakan Uang Republik Indonesia* "Peruri");
4) PT Privy Identitas Digital ("PrivyID");
5) PT Indonesia Digital Identity ("VIDA");
6) PT Solusi Net Internusa ("Digisign").

The UU ITE & PP PSTE acknowledges that even though it is only a code, E-signatures have the same status as wet signatures in general which have legal force and legal consequences.

Problems in implementing E-signatures in Indonesia is that only a few sectors have explicit rules that require the use of E-signatures. Some sectors that have already governed E-signatures includes OJK Regulation No. 77/POJK.01/2016, concerning Information Technology-Based Money Lending and Borrowing Services, and OJK Circular No. 18/SEOJK.02/2017 concerning Information Technology Risk Management and Management in Information Technology-Based Lending and Borrowing Services. However, without explicit rules, E-signatures replace the function of wet signatures on electronic documents because wet signatures cannot be done on electronic documents.

Digital signatures are created using an asymmetric cryptography system using a public key infrastructure. In the public key infrastructure, there is something called a public key and a private key. The private key, which is uniquely created for each individual, have systematically associated pairs of keys called a public key. This public key is then attached to the electronic certificate along with the electronic document that has been encrypted using the private key. The recipient can validate the digital signature of the signature by using the public key attached to the electronic certificate. In this regard, it is not possible for the signatures between A and B to be the same, because the public and private key pairs are uniquely created.

The recipient of the document can validate the digital signature of the certified E-signature using a PDF reader. PDF readers can check whether the public key to an individual listed on the electronic certificate can open the encryption which is done using a private key. If a public key can be opened, then the system will check whether the encrypted electronic information has the same hash value with the hash value of the original electronic information. If the values are the same, then the integrity of said electronic document can be guaranteed. On the contrary, if the hash value is different, then there is a change after the electronic document was signed.

In terms of proofing the validity of certified E-signature, the relevant parties will obtain information from the electronic certification organizer services which states that the validity of the signature. Whereas for uncertified E-signatures, the proof is obtained through a digital forensic test whose test results will be contained in the form of a digital forensic test report on the system or file or document that was tested. In any case, certified E-signature has stronger evidentiary power compared to uncertified E-signature, although both are legally recognized.

Note: The content of this article does not constitute legal advice and should not be relied as such. Judge's opinion may also be different, due to the facts relevant to the case. If you need specific advice related to this topic, please contact us by email through info@yangandco.com.