Bagaimana Cara Menilai Bahwa Tanda Tangan Elektronik Itu Palsu

06-05-2020
Bagaimana cara menilai bahwa tanda tangan elektronik itu palsu? Adakah teknologi yang bisa menilai keabsahan tanda tangan elektronik? Apa badan yang berwenang untuk memeriksa itu? Sebenarnya bagaimana sih bentuk tanda tangan elektronik itu? Apakah bentuknya seperti tanda tangan basah yang kemudian di-*scan* bisa disebut tanda tangan elektronik? Apakah bentuk persetujuan pada pinjaman online dengan mengklik "Ya Setuju" bisa disebut tanda tangan elektronik sehingga pengguna harus tunduk pada ketentuan yang sudah disetujui pada aplikasi karena "Ya Setuju" adalah bentuk tanda tangan elektronik?

Fungsi Tanda Tangan secara Umum

Pada dasarnya, tanda tangan memiliki fungsi sebagai bukti tertulis yang menunjukkan pemenuhan syarat "kesepakatan" sebagaimana ditentukan sebagai salah satu syarat subjektif perjanjian yang sah berdasarkan Pasal 1320 angka 1 KUH Perdata.

Terhadap suatu tulisan (tulisan di bawah tangan) yang ditandatangani, para pihak yang dihadapkan terhadap tulisan tersebut dapat melakukan 2 hal : antara mengakui atau memungkiri kebenaran tulisan atau tanda tangannya.

Berdasarkan penjelasan di atas, maka suatu tanda tangan memiliki fungsi sebagai alat autentikasi dan verifikasi yang pada umumnya memastikan kebenaran terhadap identitas penanda tangan; dan integritas tulisan yang ditandatangani (keutuhan dan keautentikan informasi elektronik).

Surat atau tulisan yang ditandatangani dapat dikatakan sebagai tanda tangan yang palsu atau tidak sah digunakan sebagai alat bukti apabila tidak dapat dipastikan kebenaran terhadap keautentikan yang telah dijelaskan di atas.
Hal ini berlaku baik untuk tanda tangan basah/manual maupun tanda tangan elektronik.

Syarat Sah Tanda Tangan Elektronik
Untuk dapat memenuhi fungsi autentikasi, Pasal 11 ayat (1) UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menegaskan bahwa tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi 6 persyaratan, yaitu : data pembuatan tanda tangan

elektronik terkait hanya kepada penanda tangan; data pembuatan tanda tangan elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa penanda tangan; segala perubahan terhadap tanda tangan elektronik yang terjadi setelah waktu penandatanganan dapat diketahui; terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penandatangannya; dan terdapat cara tertentu untuk menunjukkan bahwa penanda tangan telah memberikan persetujuan terhadap informasi elektronik yang terkait.
Ketentuan lebih lanjut mengenai mekanisme pembuktian syarat-syarat tersebut diatur dalam Pasal 59 – Pasal 64 PP PSTE.

Jenis Tanda Tangan Elektronik
Berdasarkan Pasal 60 ayat (2) huruf a dan ayat (3) PP PSTE, tanda tangan elektronik meliputi:

Tanda tangan elektronik tersertifikasi, yang harus: memenuhi keabsahan kekuatan hukum dan akibat hukum tanda tangan elektronik;menggunakan sertifikat elektronik yang dibuat oleh jasa penyelenggara sertifikasi elektronik Indonesia; dan Dibuat dengan menggunakan perangkat pembuat tanda tangan elektronik tersertifikasi.
Tanda tangan elektronik tidak tersertifikasi, yang dibuat tanpa menggunakan jasa penyelenggara sertifikasi elektronik Indonesia.

Penjelasan Pasal 60 ayat (2) PP PSTE lebih lanjut menerangkan bahwa perbedaan antara tanda tangan elektronik tersertifikasi dan tidak tersertifikasi terletak pada pengaruh terhadap kekuatan nilai pembuktiannya.

Tanda Tangan Elektronik Tersertifikasi
Pada artikel cara kerja tanda tangan elektronik , diketahui bahwa implementasi tanda tangan elektronik tersertifikasi mengacu kepada penandatanganan terhadap dokumen elektronik dengan menggunakan metode kriptografi asimetris dengan menggunakan infrastruktur kunci publik.

Penyelenggara sertifikasi elektronik menerbitkan suatu pasangan kunci yang secara unik terkait pada suatu subjek hukum. Pasangan kunci yang kemudian disebut dengan kunci privat dan kunci publik memiliki karakteristik unik di mana suatu informasi atau dokumen elektronik yang diacak (*encrypt*) oleh salah satu kunci hanya dapat disusun kembali (*decrypt*) oleh kunci pasangannya.

Sesuai dengan namanya, kunci publik dapat diketahui oleh siapa pun, akan tetapi kunci privat hanya boleh diketahui oleh pemilik tanda tangan.

Pada praktiknya, penyelenggara sertifikasi elektronik akan mencantumkan kunci publik tersebut di dalam suatu sertifikat yang disebut dengan sertifikat elektronik. Sertifikat ini merupakan dokumen yang bersifat umum, karena memang fungsinya sebagai bukti identitas penanda tangan.
kunci publik yang telah dicantumkan di dalam sertifikat elektronik dilekatkan bersama dengan dokumen elektronik yang telah dienkripsi dengan kunci privat penanda tangan.

Terdapat suatu fitur keamanan khusus terhadap dokumen yang ditandatangani dengan tanda tangan elektronik tersertifikasi, yaitu apabila terjadi perubahan pada dokumen elektronik, maka secara otomatis sistem pembaca dokumen elektronik akan dapat mendeteksi perubahan dan menunjukkan perubahan tersebut.

Dengan memperhatikan karakteristik tanda tangan elektronik tersertifikasi tersebut, maka dapat disimpulkan secara pasti bahwa tanda tangan elektronik tersertifikasi memenuhi fungsi autentikasi, sehingga identitas penanda tangan dan integritas dokumen yang ditandatangani dapat dipastikan kebenarannya.

Tanda Tangan Elektronik Tidak Tersertifikasi

Untuk dapat mengenali tanda tangan elektronik tersertifikasi dan tidak tersertifikasi, maka cukup diperhatikan apakah tanda tangan elektronik dibuat dengan menggunakan jasa penyelenggara sertifikasi elektronik Indonesia atau tidak.

Oleh karena itu, segala yang dapat dikategorikan sebagai tanda tangan baik itu berbentuk QR *code*, gambar/pindaian dari gambar tanda tangan, klik “Setuju”, dan berbagai bentuk tanda tangan lainnya tidak dapat dianggap sebagai tanda tangan elektronik tersertifikasi apabila tidak dibuat dengan menggunakan sertifikat elektronik yang dibuat oleh jasa penyelenggara sertifikasi elektronik Indonesia.

Tanda Tangan Elektronik, Tanda Tangan Digital, dan Kaitannya dengan Jenis Tanda Tangan Elektronik

Istilah tanda tangan elektronik dan tanda tangan digital sering dimaknai sama, namun pada kenyataannya keduanya memiliki makna yang berbeda.

Tanda tangan elektronik merupakan istilah hukum sebagaimana diatur dalam peraturan perundang-undangan, sedangkan tanda tangan digital merupakan istilah yang secara spesifik digunakan untuk metode penandatanganan secara elektronik dengan menggunakan metode kriptografi asimetris dengan infrastruktur kunci publik.

Berdasarkan penjelasan di atas, maka dapat dikatakan bahwa tanda tangan digital merujuk kepada tanda tangan elektronik tersertifikasi berdasarkan pasal 60 ayat (2) huruf a PP PSTE.

Metode penandatanganan secara elektronik lainnya, seperti yang tidak tersertifikasi, masuk dalam ruang lingkup tanda tangan elektronik, termasuk di dalamnya adalah tanda tangan digital.

Segala bentuk tanda tangan elektronik akan memiliki kekuatan hukum dan akibat hukum yang sah sepanjang dapat dibuktikan pemenuhan persyaratan Pasal 11 ayat (1) UU ITE.

Perbedaan Kekuatan Hukum Tanda Tangan Elektronik

Beragam bentuk dan mekanisme pembubuhan tanda tangan elektronik tidak tersertifikasi digunakan dengan memperhatikan rentang kekuatan nilai pembuktian dari tanda tangan elektronik.

Pasal 58 ayat (1) PP PSTE kemudian menjelaskan bahwa penyelenggara sertifikasi elektronik Indonesia menanggung kerugian yang diakibatkan oleh kesengajaan atau kelalaian kepada orang, badan usaha atau instansi karena kegagalannya dalam memenuhi kewajibannya berdasarkan PP PSTE.
Hal tersebut dikecualikan ketika penyelenggara sertifikasi elektronik Indonesia dapat membuktikan bahwa kerugian tersebut terjadi bukan karena kesengajaan atau kelalaiannya.

Konsekuensi terhadap Pasal 58 ayat (1) dan (2) PP PSTE tersebut mengakibatkan penyelenggara sertifikasi elektronik juga memiliki peranan untuk memastikan bahwa persyaratan tanda tangan elektronik pada Pasal 11 ayat (1) UU ITE terpenuhi.

Pasal 59 ayat (1) PP PSTE lebih lanjut menjelaskan bahwa tanda tangan elektronik dapat dihasilkan melalui berbagai prosedur penandatanganan.
Akan tetapi perlu diingat untuk dapat dianggap sebagai tanda tangan yang memiliki kekuatan hukum dan akibat hukum yang sah, maka tanda tangan elektronik tersebut harus memenuhi persyaratan sebagaimana diatur dalam Pasal 11 ayat (1) UU ITE.

Sebagai contoh, akan sangat sulit untuk bisa memastikan keautentikan dari suatu tanda tangan hasil *scan*/pemindaian. Tidak adanya sertifikat elektronik pada tanda tangan hasil *scan* juga meniadakan metode untuk mendeteksi perubahan yang terjadi pada dokumen setelah dokumen tersebut ditandatangani.

Akibatnya, tanda tangan manual yang di-*scan* memiliki kemungkinan yang sangat besar untuk diidentifikasi sebagai tanda tangan palsu karena dapat dengan mudah ditampik oleh pihak yang bersangkutan.

Oleh karena itu, kekuatan hukum hasil *scan* tanda tangan basah sangat rendah, karena fungsi autentikasinya sangat sulit untuk dipenuhi serta kekuatan nilai pembuktiannya relatif lemah.

Tanda tangan hasil *scan* dianggap sebagai tanda tangan elektronik yang memiliki kekuatan hukum dan akibat hukum yang sah apabila dapat memenuhi Pasal 11 ayat (1) UU ITE.

Membuktikan Tanda Tangan Elektronik adalah Sah atau Palsu
Berdasarkan ketentuan pada Pasal 1877 KUH Perdata, hakim dapat memerintahkan untuk memeriksa kebenaran tulisan atau tanda tangan di muka pengadilan apabila terjadi penampikan.

Untuk memeriksa tulisan atau tanda tangan basah, maka pihak yang dapat memberikan keterangan asli atau tidaknya suatu tulisan atau tanda tangan, adalah grafolog, dengan ilmunya yaitu grafologi forensik. Grafologi forensik merupakan cabang ilmu grafologi yang berhubungan dengan analisa autentifikasi (uji keaslian) tanda tangan dan tulisan seseorang.
Pengujian berbeda dilakukan apabila penampikan terjadi terhadap dokumen yang ditandatangani secara elektronik.

Apabila terjadi penampikan terhadap tanda tangan elektronik, maka untuk pembuktiannya adalah melalui pembuktian pemenuhan syarat formil pada Pasal 11 ayat (1) UU ITE.

Ketentuan tersebut dimaksudkan untuk menjaga fungsi autentikasi sebagaimana yang telah dijelaskan sebelumnya. Penampikan dapat dilakukan dengan menguji pemenuhan terhadap 6 syarat formil tersebut. Rentang nilai pembuktiannya akan semakin tinggi apabila berdasarkan pemeriksaan, penampikan semakin sulit dilakukan.

Jika para pihak berhasil menampik suatu tanda tangan elektronik, maka tanda tangan elektronik tersebut dianggap sebagai palsu atau tidak sah.

Pemenuhan terhadap 6 syarat tersebut dapat dibantu dengan meminta keterangan tambahan dari ahli dari bidang kriptografi atau forensik digital.

Hingga saat ini, tidak ada suatu badan tertentu yang berwenang untuk memeriksa tanda tangan elektronik. Namun khusus untuk memeriksaan keaslian tanda tangan elektronik tersertifikasi, maka dokumen yang telah ditandatangani dapat dibuka dengan menggunakan perangkat lunak pembaca dokumen elektronik berformat *Portable Document Format* (PDF) yang akan menyajikan informasi terkait fungsi autentikasi tanda tangan elektronik, yaitu kebenaran identitas penanda tangan dan integritas dari dokumen yang telah ditandatangani.

Hal ini merupakan metode pemeriksaan untuk metode penandatanganan kriptografi asimetris dengan memanfaatkan infrastruktur kunci publik, karena merupakan standar internasional yang diakui secara universal.

Sedangkan mengenai pemeriksaan tanda tangan elektronik tidak tersertifikasi bergantung kepada metode penandatanganan yang digunakan dan/atau cara yang dianjurkan penyelenggara tanda tangan elektronik tidak tersertifikasi tersebut.

sumber : hukumonline.com