DIGITAL SIGNATURE DALAM ASPEK LEGAL DAN PRAKTIK

Simon Batara – NIM : 13503109

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if13109@students.if.itb.ac.id

Abstrak

Dewasa ini aspek keamanan dalam segala hal mulai dipertimbangkan sebagai satu factor yang penting. Aspek keamanan mulai juga dihidupkan dalam dunia elektronik dan dunia maya. *Kriptografi* adalah salah satu langkah kemajuan pemikiran tentang keamanan yang dilakukan dalam bidang elektronik dan telekomunikasi. *Digital signature* menjadi salah satu implementasi krptografi dalam kehidupan sehari-hari.

Digital signature mulai berkembang penggunaannya dalam aspek keamanan sehingga mulai dipertimbangkan aspek legalitasnya. Beberapa *legislasi* di berbagai negara yang mengatur tentang efek dan validitas dari digital signature mulai tumbuh dan berkembang dengan cepat. Beberapa legislasi yang mengatur tentang *digital signature* akan dijelaskan dalam pembahasan yang agak mendalam.

Dalam implementasinya, digital signature bisa dibuat dengan menggunakan beberapa algoritma. Algoritma-algoritma tersebut diantaranya adalah *RSA, DSA, ElGamal signature scheme, Rabin signature*, dan lain sebagainya. Setiap algoritma-algoritma tersebut memiliki teknik khusus yang berbeda. Setiap *algoritma* memiliki kelebihan dan kekurangannya sendiri. Dalam kesempatan kali ini, pembahasan dan analisis tentang perbandingan antara *algoritma* akan dibahas lewat beberapa aspek yang akan ditentukan kemudian seperti efektifitas *algoritma*, aspek keamanannya, lingkup implementasi, dan lain sebagainya.

Jadi makalah ini secara umum akan membahas tentang perkembangan digital signature dilihat dalam aspek legislasinya serta perkembangan implementasinya ditinjau dari beberapa algoritma pembuatan dan penggunaannya.

Kata Kunci : *Digital Signature, Kriptografi, Legislasi, RSA, DSA, ElGamal signature scheme, algoritma*

LATAR BELAKANG

Dalam kehidupan manusia sekarang ini, informasi sudah menjadi suatu hal yang sangat penting. Informasi seringkali menjadi tumpuan utama seseorang melakukan suatu hal. Pada hakikatnya manusia sebagai mahkluk sosial haruslah melakukan interaksi dengan manusia lain. Dalam melakukan interaksinya, manusia haruslah memikirkan banyak hal seperti bagaimana cara melakukannya dan apa yang akan didapatkannya ketika melakukannya, dan tentunya lengkap dengan semua resiko yang akan diterima jika dia melakukannya. Dalam aktivitas-aktivitas yang dilakukannya inilah manusia membutuhkan informasi yang akurat sebagai bahan pertimbangan atau patokan pemikiran.

Di China dulu, sebuah pesan dari keluarga ataupun pejabat seringkali dijaga oleh biro pengawal. Stempel kerajaan yang seringkali menjadi tanda bahwa perintah tersebut adalah perintah valid dari sang kaisar. Seiring berjalannya waktu ternyata stempel kaisar ini mulai dipalsukan dan direbut oleh para pemberontak. Hal ini yang bisa menyebabkan akan timbulnya kesalahan perintah dan pemberontakkan karena kebijakan yang palsu dan lain sebagainya.

Pada waktu Perang Dunia II, seorang kurir nyawanya akan dihargai sama dengan satu tim pasukan. Seorang kurir biasanya membawa suatu informasi yang dianggap bisa menentukkan jalannya perang seperti lokasi musuh, kebijakan musuh, dan kondisi pasukkan musuh. Jika informasi ini bisa didapatkan maka kemenangan

akan semakin mudah diraih. Tetapi lain halnya jika ternyata informasi yang didapatkan ternyata adalah informasi yang tidak valid atau salah. Hal ini akan menyebabkan kerugian yang besar apabila informasi salah ini dijadikan suatu patokan kebijakan atau strategi. Bukan tidak mungkin kesalahan strategi tersebut menyebabkan kekalahan.

Dalam peradaban dunia barat, ternyata tanda tangan digital juga sudah dirasakan keperluannya ketika seorang tuan tanah atau pejabat atau pemimpin keluarga besar meninggal. Seperti pada kenyataannya, ketika tuan tanah atau raja meninggal maka harta yang dimilikinya akan diturunkan kepada orang lain. Kertas surat warisan ini seringkali dipalsukan untuk mendapatkan keinginan dari beberapa orang. Maka tuan tanah atau raja tersebut akan menyuruh orang untuk menjaga surat tersebut sampai disampaikan kepada sang ahli waris.

Dunia informasi sudah berkembang dengan sangat pesat. Dalam perkembangannya dewasa ini aspek keamanan dalam informasi sudah mulai diperhatikan. Hal ini bisa terjadi dan menjadi aspek penting karena informasi yang berputar ataupun beredar ternyata bisa saja menjadi salah atau *error*. Ketika informasi ini menjadi rusak atau salah maka akan terdapat resiko-resiko yang harus ditanggung oleh orang-orang baik yang mengirim, membutuhkan, ataupun sekedar melihatnya. Untuk itulah keamanan dalam dunia teknologi informasi mulai berkembang.

Dalam perjalanan perkembangan teknologi informasi khususnya di bidang keamanan informasi, banyak hal sudah diriset dan dilaksanakan oleh orang-orang. Sudah banyak periset yang menemukan dan mengimplementasikan cara mengamankan informasi atau memvalidasi informasi. Hal ini sudah dibuktikan dengan berkembangnya ilmu kriptografi yang diturunkan lagi menjadi beberapa bidang implementasi yang sesuai dengan maksud dan tujuannya.

Tanda tangan digital adalah salah satu implementasi kriptografi dalam bidang keamanan. Tanda tangan digital berguan untuk memastika kevalidan dari suatu pesan yang tertandatangan. Jika pesan tersebut tidak valid maka pengguna atau penerima pesan yang seharusnya akan mengetahui bahwa pesan yang diberikan sudah tidak valid lagi.

Tanda tangan digital bisa hadir dari tiga komponen yang ada yaitu : pesan yang ingin ditanda-tangan, kunci privat, dan kunci publik. Untuk membubuhkan tanda tangan, kunci privat digunakan untuk membentuk tanda tangan. Setelah itu pesan dibubuhkan dengan tanda tangan tersebut. Pesan yang sudah ditandatangan tersebut akan bisa dilihat kevalidan oleh pnerima pesan yang seharusnya dengan cara mengeceknya dengan kunci publik. Jika valid maka informasi yang ada memang tidak berubah dan pantas untuk diterima, jika tidak berarti pesan tersebut sudah rusak atau dirusak oleh orang lain.

Perkembangan tanda tangan digital sendiri bisa dilihat dalam beberapa waktu silam sudah berkembang dengan sangat cepat. Kenyataan bahwa aspek keamanan memang sangat penting dan dihargai oleh masyarakat banyak bisa dibuktikan dengan perkembangan ilmu kriptografi yang berjalan sudah cukup lama.

Tanda tangan digital sekarang sudah banyak digunakan orang sebagai sarana pemvalidasi informasi. Tanda tangan digital tersebut sudah menjadi tumpuan harapan aspek keamanan dari suatu informasi. Dengan makin maraknya penggunaan tanda tangan digital sebagai salah satu cara pengamanan, maka aspek keamananpun makin banyak ditingkatkan cara pengamanannya. Hal ini juga bisa dibuktikan dengan makin banyaknya algoritma untuk mendapatkan dan membubuhkan tanda tangan digital dalam pesan-pesan yang ingin ditanda tangan.

DIGITAL SIGNATURE

Seperti yang sudah disampaikan pada bagian sebelumnya sebenarnya penggunaan digital signature berawal dari penggunaan teknik kriptografi yang digunakan untuk mengamankan informasi yang hendak ditransmisikan/disampaikan kepada orang yang lain yang sudah digunakan sejak ratusan tahun yang lalu. Dengan demikian sebenarnya tanda tangan digital merupakan sesuatu yang telah dikenal, sedangkan sekarang ini tanda tangan digital lebih mengacu pada teknik penyandiaanya atau pengubahan dari yang sebenarnya yang cenderung lebih variatif dan sulit untuk dipecahkan. Beberapa sifat umum dari tanda tangan digital adalah :

1. Otentik (*authenticity)*, tak bisa/sulit ditulis/ditiru oleh orang lain. Pesan dan

tanda tangan pesan tersebut juga dapat menjadi barang bukti, sehingga penandatangan tak bisa menyangkal bahwa dulu ia tidak pernah menandatanganinya.

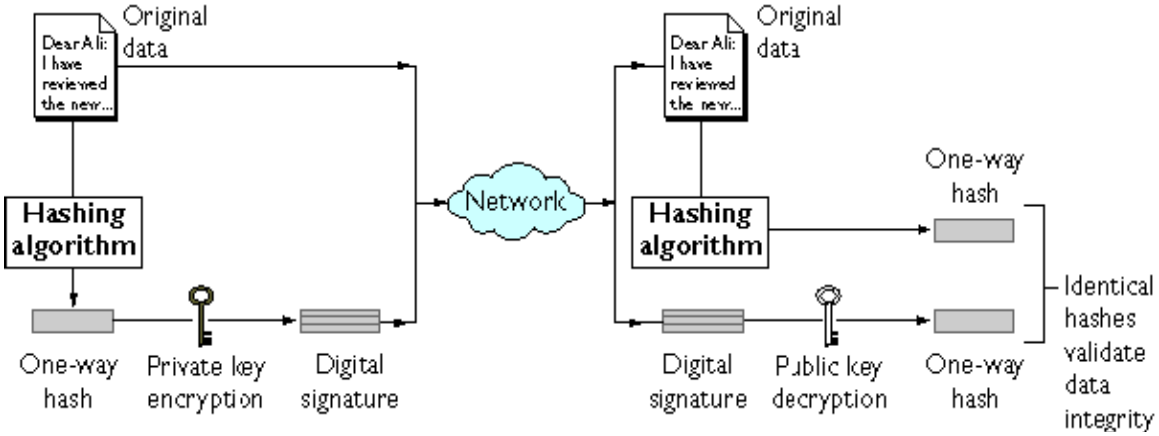
2. Sah *(integrity)* untuk dokumen (pesan) itu saja atau salinannya yang sama persis. Tanda tangan itu tidak bisa dipindahkan ke dokumen lainnya, meskipun dokumen lain itu hanya berbeda sedikit. Ini juga berarti bahwa jika dokumen itu diubah, tanda tangan digital dari pesan tersebut tidak lagi sah.
3. Tidak dapat disangkal keberadaannya *(Non Repudiation) non repudiation* ini timbul dari keberadaan digital signature yang menggunakan enkripsi asimetris (asymmetric encryption). Enkripsi asimetris ini melibatkan keberadaan dari kunci prifat dan kunci publik. Suatu pesan yang telah dienkripsi dengan menggunakan kunci prifat maka ia hanya dapat dibuka/dekripsi dengan menggunakan kunci publik dari pengirim. Jadi apabila terdapat suatu pesan yang telah dienkripsi oleh pengirim dengan menggunakan kunci prifatnya maka ia tidak dapat menyangkal keberadaan pesan tersebut karena terbukti bahwa pesan tersebut dapat didekripsi dengan kunci publik pengirim. Keutuhan dari pesan tersebut dapat dilihat dari keberadaan hash function dari pesan tersebut, dengan catatan bahwa data yang telah di-sign akan dimasukkan kedalam digital envelope
4. Dapat diperiksa dengan mudah, termasuk oleh pihak-pihak yang belum pernah bertatap muka langsung dengan penandatangan.

Teknologi tanda tangan digital memanfaatkan teknologi kunci publik. Sepasang kunci publik-privat dibuat untuk keperluan seseorang. Kunci privat disimpan oleh pemiliknya dan digunakan untuk membuat tanda tangan digital. Sedangkan kunci publik dapat diserahkan kepada siapa saja yang ingin memeriksa tanda tangan digital yang bersangkutan pada suatu dokumen. Proses pembuatan dan pemeriksaan tanda tangan ini melibatkan sejumlah teknik kriptografi seperti *hashing* (membuat 'sidik jari' dokumen) dan enkripsi asimetris.

Dalam suatu kriptografi suatu pesan dienkripsi *(encrypt)* dengan menggunakan suatu kunci *(key)*. Hasil dari enkripsi ini adalah berupa *chipertext* tersebut kemudian ditransmisikan/diserahkan kepada tujuan yang dikehendakinya. *Chipertext* tersebut kemudian dibuka/didekripsi *(decrypt)* dengan suatu kunci untuk mendapatkan informasi yang telah enkripsi tersebut. Terdapat dua macam cara dalam melakukan enkripsi yaitu dengan menggunakan kriptografi simetris *(symetric crypthography/secret key crypthography)* dan kriptografi simetris *(asymetric crypthography)* yang kemudian lebih dikenal sebagai public key crypthography.

Secret key crypthografi atau yang dikenal sebagai kriptografi simetris, menggunakan kunci yang sama dalam melakukan enkripsi dan dekripsi terhadap suatu pesan *(message)*, disini pengirim dan penerima menggunakan kunci yang sama sehingga mereka harus menjaga kerahasian (secret) terhadap kuci tersebut. Salah satu algoritma yang terkenal dalam kriptografi simetris ini adalah *Data Encryption standard (DES).*

Berikut ini adalah bagan cara penggunaan tanda tangan digital pada suatu jaringan dan pesan dalam dokumen yang divalidasi :



KUNCI SIMETRIS DAN PENGGUNAANNYA

Public key crypthography, atau dikenal juga sebagai kriptografi simetris, menggunakan dua kunci (key). Kunci yang pertama digunakan untuk melakukan enkripsi terhadap suatu pesan (messages) dan kunci yang lain digunakan untuk melakukan dekripsi terhadap pesan tersebut. Kedua kunci tersebut mempunyai hubungan secara matematis sehingga suatu pesan yang dienkripsi dengan suatu kunci hanya dapat didekripsi dengan kunci pasangannya. Seorang pengguna mempunyai dua buah kunci, yaitu sebuah kunci privat *(privat key)* dan juga sebuah kunci publik *(public key)*. Pengguna (user) tersebut kemudian mendistribusikan /menyebarluaskan kunci publik miliknya. Karena terdapat hubungan antara kedua kunsi tersebut, pengguna dan seseorang yang menerima kunci publik akan merasa yakin bahwa suatu data yang diterimanya dan telah berhasil didekripsi hanya dapat berasal dari pengguna yang mempunyai kunci privat. Kepastian /keyakinan ini hanya ada selama kunci privat ini tidak diketahui oleh orang lain. Kedua kunci ini berasal atau diciptakan sendiri oleh penggunanya. Salah satu algoritma yang terbaik yang dikenal selama ini adalah RSA (dinamakan sesuai dengan nama penciptanya Rivest, Shamir, Adleman).

Pada saat dua orang hendak saling berkomunikasi atau saling bertukar data/pesan secara aman, mereka kemudian saling mengirimkan salah satu kunci yang dipunyainya, yaitu kunci publiknya. Sedangkan mereka menyimpan kunci prifat sebagai pasangan dari kunci publik yang didistribusikannya. Karena data/pesan ini hanya dapat dienkripsi dan dekripsi dengan menggunakan kunci pasangannya maka data ini dapat dapat ditransmisikan dengan aman melalui jaringan yang relatif tidak aman (melalui internet). Contoh dari penggunaan kriptografi ini adalah jika Alice hendak mentransmisikan suatu data/pesan rahasian kepada Bob maka ia akan melakukan enkripsi data tersebut dengan menggunakan kunci publik Bob. Selama Bob yakin bahwa tidak ada seorang pun yang mengetahui kunci prifatnya, maka mereka dapat merasa yakin bahwa yang dapat membaca pesan tersebut hanyalah Bob.

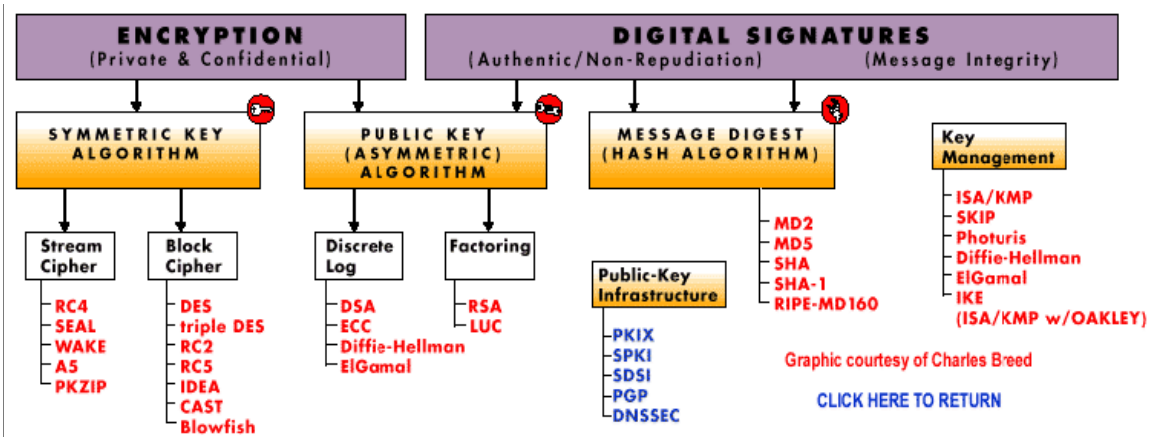
Dalam Digital signature suatu data/pesan akan dienkripsi dengan menggunakan kunci simetris yang diciptakan secara acak *(randomly generated symmetric key)*. Kunci ini kemudian akan dienkripsi dengan menggunakan kunci publik dari calon penerima pesan. Hasil dari enkripsi ini kemudian dikenal/disebut sebagai *"digital envelope"* yang kemudian akan dikirimkan bersama pesan/data yang telah dienkripsi. Setelah menerima *digital envelope* penerima kemudian akan membuka/mendekripsi dengan menggunakkan kunci kunci prifatnya. Hasil yang ia dapatkan dari dekripsi tersebut adalah sebuah kunci simetris yang dapat digunakannya untuk membuka data/pesan tersebut.

Kombinasi antara *digital signature* dengan *message digest* menyebabkan seorang pengguna dapat "menandatangani secara digital" *(digitally sign)* suatu data/pesan. Maksud dari menandatangani secara digital adalah memberikan suatu ciri khas terhadap suatu pesan. Pada saat message digests dienkripsi dengan menggunakan kunci privat dari pengirim dan "ditambahkan" kepada data/pesan yang asli maka hasil yang didapat adalah digital signature dari pesan tersebut.

Penerima dari digital signature akan dapat mempercayai bahwa data/pesan benar berasal pengirim. Dan karena apabila terdapat perubahan suatu data/pesan akan menyebabkan akan merubah *message digests* dengan suatu cara yang tidak dapat diprediksi *(in unpredictible way)* maka penerima akan merasa yakin bahwa data/pesan tersebut tidak pernah diubah setelah message digest diciptakan.

Sebelum kedua belah pihak (pengirim/penerima) hendak melakukan komunikasi diantaranya dengan menggunakan kriptografi kunci publik, masing-masing pihak harus merasa yakin akan keberaan mereka. Mereka kemudian akan melakukan otentifikasi terhadap keberadaan masing-masing pihak. maka mereka menunjuk pihak ketiga yang akan memberikan otentifikasi terhadap kunci publik mereka. Pihak ketiga ini kita kenal sebagai *Certification Authorithy*. *Certification authorithy* ini kemudian akan memberikan suatu sertifikat (certificate) yang berisi identitas dari pengguna (misalnya Bob), sertifikat ini ditandatangani secara digital oleh *Certification authority* tersebut. Isi dari sertifikat tersebut selain identitas ia juga berisi kunci publik dari pemiliknya.

Berikut ini akan ditunjukkan klasifikasi metode enkripsi dan digital signature



ASPEK LEGAL

Setelah ini akan dibahas beberapa bahasan yang berkaitan dengan tanda tangan digital dilihat dalam aspek legalitasnya.

LATAR BELAKANG CYBER LAW

Dalam perkembangan dunia teknologi informasi yang mengarah pada budaya penggunaan internet, banyak yang mengatakan bahwa dunia cyber (*cyberspace*) tidak dapat diatur. Cyberspace adalah dunia maya dimana tidak ada lagi batas ruang dan waktu. Padahal ruang dan waktu seringkali dijadikan acuan hukum. Jika seorang warga Indonesia melakukan transaksi dengan sebuah perusahaan Inggris yang menggunakan server di Amerika, dimanakah (dan kapan) sebenarnya transaksi terjadi? Hukum mana yang digunakan? Dalam hal ini, terjadi suatu perbedaan pandangan baik antara pandangan hukum sebagai suatu aturan dan penembusan ruang dan waktu sebagai kelebihan dunia teknologi informasi.

Teknologi digital yang digunakan untuk mengimplementasikan dunia cyber memiliki kelebihan dalam hal duplikasi atau regenerasi. Data digital dapat direproduksi dengan sempurna seperti aslinya tanpa mengurangi kualitas data asilnya. Hal ini sulit dilakukan dalam teknologi analog, dimana kualitas data asli lebih baik dari duplikatnya. Sebuah salian (fotocopy) dari dokumen yang ditulis dengan tangan memiliki kualitas lebih buruk dari aslinya. Seseorang dengan mudah dapat memverifikasi keaslian sebuah dokumen. Sementara itu dokumen yang dibuat oleh sebuah wordprocessor dapat digandakan dengan mudah, dimana dokumen "asli" dan "salinan" memiliki fitur yang sama. Jadi mana dokumen yang "asli". Apakah dokumen yang ada di dalam disk saya atau yang ada di memori komputer saat ini atau dokumen yang ada di CD-ROM atau flash disk. Dunia digital dan teknologi informasi memungkinkan kita memiliki lebih dari satu dokumen asli.

Seringkali transaksi yang resmi membutuhkan tanda tangan untuk meyakinkan keabsahannya. Bagaimana menerjemahkan tanda tangan konvensional ke dunia digital? Apakah bisa kita gunakan tanda tangan yang di-scan, atau dengan kata lain menggunakan *digitized signature*? Apa bedanya *digitized signature* dengan *digital signature* dan apakah tanda tangan digital ini dapat diakui secara hukum?

Tanda tangan ini sebenarnya digunakan untuk memastikan identitas. Apakah memang *digital identity* seorang manusia hanya dapat diberikan dengan menggunakan tanda tangan? Dapatkah kita menggunakan sistem biometrik yang dapat mengambil ciri kita dengan lebih akurat? Apakah e-mail, *avatar*, *digital dignature*, *digital certificate* dapat digunakan sebagai identitas (dengan tingkat keamanan yang berbeda-beda tentunya)?

Semua contoh-contoh (atau lebih tepatnya pertanyaan-pertanyaan) di atas menantang landasan hukum konvensional. Jadi, apakah dibutuhkan sebuah hukum baru yang bergerak di ruang cyber, sebuah cyberlaw? Jika dibuat sebuah hukum baru, manakah batas teritorinya? Riil atau virtual? Apakah hukum ini hanya

berlaku untuk *cybercommunity* – komunitas orang di dunia cyber yang memiliki kultur, etika, dan aturan sendiri – saja? Bagaimana jika efek atau dampak dari (aktivitas di) dunia cyber ini dirasakan oleh komunitas di luar dunia cyber itu sendiri?

Atau apakah kita dapat menggunakan dan menyesuaikan hukum yang sudah ada saat ini?
Kata "*cyber*" berasal dari "*cybernetics*," yaitu sebuah bidang studi yang terkait dengan komunikasi dan **pengendalian** jarak jauh. Norbert Wiener merupakan orang pertama yang mencetuskan kata tersebut. Kata pengendalian perlu mendapat tekanan karena tujuannya adalah "total control." Jadi agak aneh jika asal kata cyber memiliki makna dapat dikendalikan akan tetapi dunia cyber tidak dapat dikendalikan.

PERKEMBANGAN CYBER LAW DI DUNIA

Di dunia sendiri, tanda tangan digital memang sudah menyita perhatian banyak komunitas sehingga bermunculan legislasi di negara-negara tertentu untuk mengatur tentang tanda tangan digital. Selanjutnya akan diberikan beberapa legislasi yang mengatur tentang tanda tangan digital di beberapa negara ataupun komunitas.

Di Brazil, terdapat legislasi khusus yang mengatur tentang tanda tangan digital. Legislasi yang ada tersebut ditetapkan dan disahkan dengan nama **MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001.**

Di China, legislasi mengenai tanda tangan digital ditetapkan dengan sebutan Electronic Signature Law of the People's Republic of China

Masyarakat Eropa juga sangat memperhatikan aspek keamanan dalam kehidupan teknologi informasi. Masyarakat Eropa sudah menetapkan atau mendirikan framework dari tanda tangan digital yaitu :

1. Directive 1999/93/EC of the European Parliament and of the Council
2. Commission Decision 2003/511/EC

Setelah menyepakati suatu arahan bersama, maka negara-negara Eropa mulai mengimplementasikan hal-hal mengenai tanda tangan digital dalam ruang lingkup mereka. Negara-negara yang mengimplementasikannya antara lain :

1. Austria
   Signature Law, 2000
2. Belgium
   Signature Law, 2001
3. Republik Ceko
   Act on Electronic Signatures, 227/2000
4. Inggris, Skotlandia, dan Wales
   Electronic Communications Act, 2000
5. Estonia
   Digital Signature Law, 2000
6. Jerman
   Signature Law, 2001
7. Lituania
   Law on electronic signature, 2002
8. Norwegia
   Electronic Signature Act, 2001
9. Slovenia
   Electronic Business and Electronic Signature Act (in Slovene) .
10. Spanyol
    Ley 59/2003 , de 19 de diciembre, de firma electrónica (in Spanish).
11. Swedia
    - Qualified Electronic Signatures Act (SFS 2000:832) (in Swedish).
    - SFS 2000:832 in English translation

Selain dari wilayah Eropa yang sudah membentuk kesepakatan masih ada kesepakan lain khusus untuk membicarakan topik tentang tanda tangan digital seperti negara-negara yang juga sangat berbudaya dengan adanya digital signature, seperti :

- India dengan Information Technology Act, 2000
- New Zealand dengan Electronic Transactions Act 2002, sections 22-24
- Pakistan dengan Pakistan's Electronic Data Protection Act 2005
- Rusia dengan Federal Law of Russian Federation about Electronic Digital Signature (10.01.2002)
- Amerika Serikat dengan Uniform Electronic Transactions Act dan Electronic Signatures in Global and National Commerce Act
- Switzerland denrgan Federal Law on Certification Services Concerning the Electronic Signature, 2003
- Uruguay dengan n Concerning passwords or adequate information technology gestures dan Concerning electronic and digital signature and PKI
- Turki dengan Electronic Signature Law

Dalam perkembangan digital signature di dunia, efek dan validitas dari sebuah digital signature juga semakin dipertimbangkan. Peraturan-peraturan yang ada di atas menyebutkan beberapa ketentuan atau ketetapan yang ada di dunia. Setelah kita melihat lebih jauh lagi tentang penerapan digital signature yang akhirnya menyebabkan terciptanya satu peraturan atau ketetapan, kita bisa menyimpulkan bahwa pada akhirnya digital signature adalah sesuatu yang bisa menarik perhatian dunia.

PERKEMBANGAN CYBER LAW DI INDONESIA

Inisiatif untuk membuat "cyberlaw" di Indonesia sudah dimulai sebelum tahun 1999. Fokus utama waktu itu adalah pada "payung hukum" yang generik dan sedikit mengenai transaksi elektronik. Pendekatan "payung" ini dilakukan agar ada sebuah basis yang dapat digunakan oleh undang-undang dan peraturan lainnya. Karena sifatnya yang generik, diharapkan rancangan undang-undang tersebut cepat diresmikan dan kita bisa maju ke yang lebih spesifik. Namun pada kenyataannya hal ini tidak terlaksana.

Untuk hal yang terkait dengan transaksi elektronik, pengakuan digital signature sama seperti tanda tangan konvensional merupakan target. Jika digital signature dapat diakui, maka hal ini akan mempermudah banyak hal seperti *electronic commerce* (*e-commerce*), *electronic procurement* (*e-procurement*), dan berbagai transaksi elektronik lainnya.

Namun ternyata dalam perjalanannya ada beberapa masukan sehingga hal-hal lain pun masuk ke dalam rancangan "cyberlaw" Indonesia. Beberapa hal yang mungkin masuk antara lain adalah hal-hal yang terkait dengan kejahatan di dunia maya (*cybercrime*), penyalahgunaan penggunaan komputer, *hacking*, membocorkan password, *electronic banking*, pemanfaatan internet untuk pemerintahan (e-government) dan kesehatan, masalah HaKI, penyalahgunaan nama domain, dan masalah privasi. Penambahan isi disebabkan karena belum ada undang-undang lain yang mengatur hal ini di Indonesia sehingga ada ide untuk memasukkan semuanya ke dalam satu rancangan. Nama dari RUU ini pun berubah dari Pemanfaatan Teknologi Informasi, ke Transaksi Elektronik, dan akhirnya menjadi RUU Informasi dan Transaksi Elektronik. Di luar negeri umumnya materi ini dipecah-pecah menjadi beberapa undang-undang.

Ada satu hal yang menarik mengenai rancangan cyberlaw ini yang terkait dengan teritori. Misalkan seorang *cracker* dari sebuah negara Eropa melakukan pengrusakan terhadap sebuah situs di Indonesia. Dapatkah hukum kita menjangkau sang penyusup ini? Salah satu pendekatan yang diambil adalah jika akibat dari aktivitas *cracking*nya terasa di Indonesia, maka Indonesia berhak mengadili yang bersangkutan. Apakah kita akan mengejar cracker ini ke luar negeri? Nampaknya hal ini akan sulit dilakukan mengingat keterbatasan sumber daya yang dimiliki oleh kita. Yang dapat kita lakukan adalah menangkap *cracker* ini jika dia mengunjungi Indonesia. Dengan kata lain, dia kehilangan kesempatan / hak untuk mengunjungi sebuah tempat di dunia. Pendekatan ini dilakukan oleh Amerika Serikat.

RUU PEMANFAATAN TEKNOLOGI INFORMASI

Munculnya RUU Pemanfaatan Teknologi Informasi ini bermula dari mulai merasuknya pemanfaatan Teknologi Informasi dalam kehidupan sehari-hari kita saat ini. Jika kita lihat, kita mulai terbiasa menggunakan mesin ATM untuk mengambil uang; menggunakan *handphone* untuk berkomunikasi dan bertransaksi (mobile banking); menggunakan Internet untuk melakukan transaksi (Internet banking, membeli barang), berikirim e-mail atau untuk sekedar menjelajah Internet; perusahaan melakukan transaksi melalui Internet (e-procurement); dan masih banyak lainnya. Semua kegiatan ini merupakan pemanfaatan dari Teknologi Informasi.

Teknologi Informasi memiliki peluang untuk meningkatkan perdagangan dan perekonomian nasional yang terkait dengan perdagangan dan perekonomian global. Salah satu kendala yang muncul adalah ketidak-jelasan status dari transaksi yang dilakukan melalui media cyber ini. Untuk itu Cyberlaw Indonesia harus dipersiapkan.

Kata "Teknologi Informasi" di sini merupakan terjemahan dari kata "Information Technology" (IT). Singkatan yang akan digunakan dalam tulisan ini adalah "IT" bukan "TI", meskipun kalau kita lihat semestinya singkatan yang digunakan adalah TI. Hal ini dilakukan agar

tidak membingungkan pembaca. Singkatan "TI" sudah lazim digunakan untuk "Teknik Industri". Istilah lain yang sering juga digunakan di Indonesia adalah "Telematika". Namun untuk tulisan ini, penulis akan menggunakan istilah "IT" saja.

Ternyata efek dari pemanfaatan IT ini berdampak luar biasa. Selain memberikan kemudahan, dia juga menghasilkan efek negatif, seperti antara lain:

1. Penyadapan email, PIN (untuk Internet Banking).
2. Pelanggaran terhadap hak-hak privacy.
3. Masalah nama domain seperti kasus mustika-ratu.com yang didaftarkan oleh bukan pemilik Mustika Ratu, atau kasus typosquatter "kilkbca.com" (perhatikan huruf "i" dan "l" bertukar tempat) yang menyaru sebagai "klikbca.com".
4. Penggunaan kartu kredit milik orang lain.
5. Munculnya "pembajakan" lagu dalam format MP3, yang kemudian disertai dengan tempat tukar menukar lagu seperti Napster[2]. Napster sendiri kemudian dituntut untuk ditutup (dan membayar ganti rugi) oleh asosiasi musik.
6. Adanya spamming email.
7. Pornografi.

Hal-hal lain yang sifatnya tidak jelas sebelum adanya RUU Pemanfaatan Teknologi Informasi ini antara lain:

1. status dari transaksi yang menggunakan media Internet, misalnya e-procurement;
2. status legal dari tanda tangan digital;
3. status dari e-government.

Hal-hal di atas memaksa adanya sebuah undang-undang yang dapat memberikan kejelasan bagi pihak-pihak yang terkait. Karena banyaknya hal yang harus diberikan landasan, maka RUU yang dikembangan ini berupa sebuah "umbrela provision". Diharapkan nantinya ada UU atau PP yang lebih spesifik untuk bidang-bidang yang sudah diberikan slotnya oleh RUU Pemanfaatan Teknologi Informasi ini.

Pengaturan Dunia Cyber

Banyak orang yang mengatakan bahwa dunia cyber tidak dapat diatur. Hal ini cukup menganehkan karena kata "cyber" ini berasal dari kata "cybernetics" dimana tujuannya adalah mengendalikan sesuatu (misalnya robot) dari jarak jauh. Jadi tujuan utamanya adalah kendali total. Perfect control. Maka akan aneh jika dikatakan cyber tidak dapat diatur.

Ada beberapa sumber bacaan filosofis dan hukum yang dapat menjelaskan hal ini dengan lebih detail, seperti misalnya buku dari Lawrence Lessig (yang berjudul "Code and Other Laws of Cyberspace"). Buku Lessig ini pada intinya menunjukkan beberapa cara untuk mengatur atau mengendalikan dunia cyber melalui commerce. Jika kita tidak dapat mengendalikan indiviual, maka salah satu cara yang dapat ditempuh adalah dengan memberikan insentif kepada bisnis sehingga akhirnya orang-orang menerima peraturan dengan lebih mudah. Sebagai contoh, jika pemerintah memaksakan semua orang harus memiliki *digital identity* (digital ID), maka akan banyak yang protes karena merasa tidak perlu dan curiga kepada pemerintah[3]. Akan tetapi jika pemerintah memberikan insentif kepada bank yang menerapkan penggunaan digital ID pada nasabahnya (misalnya nasabah yang memiliki digital ID tidak dikenakan biaya untuk transaksi yang dilakukannya) maka lama kelamaan sebagian besar orang akan memiliki digital ID tanpa harus dipaksakan. Sama halnya dengan kepemilikan Surat Ijin Mengemudi (SIM). Tidak semua orang memiliki SIM, namun orang yang memiliki SIM memiliki banyak keuntungan. Selain merupakan syarat untuk mengemudi, SIM juga dapat digunakan sebagai identitas (untuk mengambil uang, wesel, dan sebagainya). Jadi banyak orang yang mengambil SIM.

Undang-Undang Global atau Spesifik ?

Banyak orang yang mempertanyakan soal pendekatan umbrela provision yang digunakan dalam mengembangkan RUU ini. Sebetulnya hal ini terkait dengan beberapa hal. Hal yang utama adalah belum adanya "pegangan" atau "cantolan" dalam bentuk UU lain di Indonesia, sementara jumlah topik yang harus dibahas sangat banyak. Kita dapat saja membuat UU untuk setiap bagian khusus (misal khusus untuk Digital Signature, khusus tentang e-Banking, khusus tentang e-Government, dan UU/PP yang khusus lainnya). Namun pendekatan seperti ini bisa berakibat lebih lama jadinya Cyberlaw kita (sementara tuntutan dari masyarakat mengharapkan cepatnya selesai) dan dapat terjadi ketidak-konsistenan UU-UU yang dibuat secara terpisah-pisah ini. Hal ini akan menyulitan dalam penggabungannya nanti (jika dibutuhkan).

Dengan pendekatan top down dan global seperti ini diharapkan ada landasan yang kuat untuk membuat UU atau PP yang lebih spesifik lainnya.

Filosofi dalam RUU

RUU ini dirancang dengan menganut beberapa filosofi sebagai berikut. Yang pertama, bahwa pengaturan dari pemerintah diaharapkan sesedikit mungkin. Atau dalam bahasa Inggrisnya adalah "*less government involvement, if possible*". Jika ada hal-hal yang tidak atau belum perlu diatur, sebaiknya tidak usah diatur. Peraturan dibuat jika memang benar-benar dibutuhkan. Pendekatan ini sama seperti yang dilakukan di Amerika Serikat. Hal ini sejalan dengan situasi di Indonesia dimana rakyat tidak terlalu suka diatur-atur oleh peraturan yang tidak perlu. Jika RUU ini terlalu mengatur dan represif, maka dia akan ditolak oleh masyarakat.

Beberapa Pengertian

Salah satu kesulitan yang dialami dalam pembuatan RUU ini adalah banyaknya istilah asing dan definisi-definisi yang sulit dicarikan padan katanya dalam Bahasa Indonesia. Sementara itu untuk menggunakan istilah dalam bahasa aslinya, yang umumnya adalah Bahasa Inggris, di dalam RUU sedikit kurang lazim. Belum lagi definisi dari beberapa hal harus dapat dijabarkan dalam kalimat yang singkat.

Beberapa istilah tersebut adalah :
1. Teknologi Informasi
2. Tanda tangan digital
3. Dokumen Elektronik
4. Komputer

Teknologi Informasi didefinisikan sebagai "*suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisa, dan menyebarkan informasi*". Dalam hal ini sebetulnya yang menjadi fokus adalah teknologi informasi yang berbasi elektronik. Teknologi informasi yang berbasis "asap", misalnya tidak menjadi pokok bahasan.

Tanda tangan digital atau tanda tangan elektronik adalah tanda jati diri yang berfungsi sebagai pengesahan oleh pengguna melalui metode elektronik atau prosedur yang telah ditentukan. Yang dimaksud dengan tanda tangan digital di sini adalah terjemahan dari "digital signature". Dalam implementasinya, digital signature berupa rentetan angka yang panjang yang dihasilkan oleh sebuah algoritma tertentu, misal dengan algoritma *RSA* atau *DSA*. (Untuk diskusi mengenai algoritma-algoritma ini, silahkan baca buku "Applied Cryptography" karangan Bruce Schneier.). Seringkali tanda tangan digital ini dianggap sebagai hasil proses *image scanning* dari tanda tangan biasa, yang hasilnya adalah sebuah *graphical image* (dalam format GIF, JPEG, atau PNG). Bukan ini yang dimaksud dengan digital signature! Kalau hasil scanning tanda tangan, ini mungkin lebih tepat disebut "digitalized signature".

Istilah "dokumen elektronik" di sini merupakan terjemahan dari "*electronic record*". Pada mulanya digunakan istilah "rekaman elektronik". Tapi istilah ini malah membingungkan dan rancu dengan rekaman musik. Pada akhirnya digunakan istilah "dokumen elektronik" saja.
Komputer adalah setiap alat pemroses data elektronik, magnetik, optikal, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan. Definisi dari "komputer" di sini memang cukup luas, meskipun dia termasuk perangkat komunikasi seperti modem, router, fiber optic, dan seterusnya. Termasuk di dalam kategori komputer adalah *personal computer* (PC), workstation, server, Personal Digital Assistant (PDA seperti yang dikembangkan oleh perusahaan Palm[4]). Definisi yang luas ini dilakukan mengingat perkembangan teknologi yang membuat semakin kaburnya batasan antara komputer dan bukan. Perangkat handphone yang canggih seperti Nokia Communicator dapat dikategorikan sebagai komputer juga sebab dia dapat digunakan untuk mengakses email, Internet, menerima fax, dan banyak fungsi pemroses data elektronik lainnya. Memang dalam kenyataanya Nokia Communicator ini memang seperti komputer dalam ukuran kecil (genggaman).

Beberapa definisi yang belum dimasukkan ke dalam RUU ini antara lain adalah definisi dari perangkat komunikasi (modem, router, hub, kabel-kabel UTP, fiber optic, dsb.). Ada kebutuhan untuk membasukkan perangkat komunikasi sebab dalam proses di lapangan ada kalanya dibutuhkan penyitaan perangkat tersebut. Beberapa pengertian lain yang lebih mendasar, seperti misalnya perbedaan antara analog dan digital, sempat dipertanyakan oleh

banyak orang yang tidak memiliki latar belakang elektro. Agak sukar dan terlalu melebar apabila hal ini dimasukkan di sini. Sebaiknya pembaca mengacu kepada bahan bacaan lain (yang mana? Akan saya tambahkan info ini pada versi berikutnya.).

Pembahasan Pasal Digital Signature

Berikut ini dikutip satu pokok bahasan dari perundangan yang ada di Indonesia dan berkenaan dengan digital signature. Kita bisa melihat untuk selanjutnya digital signature didefinisikan dan digunakan

---

BAB III
INFORMASI ELEKTRONIK

Pasal 5

1. Informasi elektronik dan atau hasil cetak dari informasi elektronik merupakan alat bukti yang sah dan memiliki akibat hukum yang sah.
2. Informasi elektronik dan atau hasil cetak dari informasi elektronik sebagaimana dimaksud dalam ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.
3. Informasi elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai peraturan perundangan yang berlaku.
4. Ketentuan mengenai informasi elektronik sebagaimana dimaksud dalam ayat (1) tidak berlaku untuk :
    a. pembuatan dan pelaksanaan surat wasiat;
    b. pembuatan dan pelaksanaan surat-surat terjadinya perkawinan dan putusnya perkawinan;
    c. csurat-surat berharga yang menurut undang-undang harus dibuat dalam bentuk tertulis;
    d. perjanjian yang berkaitan dengan transaksi barang tidak bergerak;
    e. dokumen-dokumen yang berkaitan dengan hak kepemilikan; dan
    f. dokumen-dokumen lain yang menurut peraturan perundang-undangan yang berlaku mengharuskan adanya pengesahan notaris atau pejabat yang berwenang.

Pasal 6

Dalam hal terdapat ketentuan hukum lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, maka informasi elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat dijamin keutuhannya, dipertanggungjawabkan, diakses, dan ditampilkan, sehingga menerangkan suatu keadaan.

Pasal 7

Setiap orang yang menyatakan suatu hak, memperkuat hak yang telah ada, atau menolak hak orang lain berdasarkan atas keberadaan suatu informasi elektronik harus memastikan bahwa informasi elektronik yang ada padanya berasal dari sistem elektronik terpercaya.

Pasal 8

1. Kecuali diperjanjikan lain, waktu pengiriman suatu informasi elektronik ditentukan pada saat informasi elektronik telah dikirim dengan alamat yang benar oleh pengirim ke suatu sistem elektronik yang ditunjuk atau dipergunakan penerima dan telah memasuki sistem elektronik yang berada di luar kendali pengirim.
2. Kecuali diperjanjikan lain, waktu penerimaan suatu informasi elektronik ditentukan pada saat informasi elektronik memasuki sistem elektronik di bawah kendali penerima yang berhak.
3. Dalam hal penerima telah menunjuk suatu sistem elektronik tertentu untuk menerima informasi elektronik, penerimaan terjadi pada saat informasi elektronik memasuki sistem elektronik yang ditunjuk.
4. Dalam hal terdapat dua atau lebih sistem informasi yang digunakan dalam pengiriman ataupun penerimaan informasi elektronik, maka:

waktu pengiriman adalah ketika informasi elektronik memasuki sistem informasi pertama yang berada diluar kendali pengirim.
waktu penerimaan adalah ketika informasi elektronik memasuki sistem informasi terakhir yang berada dibawah kendali penerima.

Pasal 9

Pelaku usaha yang menawarkan produk melalui media elektronik wajib menyediakan informasi yang lengkap dan benar berkaitan dengan syarat-syarat kontrak, produsen dan produk yang ditawarkan.

Pasal 10

1. Pemerintah atau masyarakat dapat membentuk lembaga sertifikasi keandalan yang fungsinya memberikan sertifikasi terhadap pelaku usaha dan produk yang ditawarkannya secara elektronik.
2. Ketentuan mengenai pembentukan lembaga sertifikasi keandalan sebagaimana dimaksud dalam ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 11

1. Tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:
   a. Data pembuatan tanda tangan terkait hanya kepada penanda tangan saja;
   b. Data pembuatan tanda tangan elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa penandatangan;
   c. Segala perubahan terhadap tanda tangan elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
   d. Segala perubahan terhadap informasi elektronik yang terkait dengan tanda tangan elektronik tersebut setelah waktu penandatanganan dapat diketahui;
   e. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penandatangannya;
   f. fTerdapat cara tertentu untuk menunjukkan bahwa penandatangan telah memberikan persetujuan terhadap informasi elektronik yang terkait.
2. Ketentuan lebih lanjut mengenai tanda tangan elektronik sebagaimana dimaksud dalam ayat (1) diatur dengan Peraturan Pemerintah

Pasal 12

1. Setiap orang yang terlibat dalam tanda tangan elektronik berkewajiban memberikan pengamanan atas tanda tangan elektronik yang digunakannya;
2. Pengamanan tanda tangan elektronik sebagaimana dimaksud dalam ayat (1) sekurang-kurangnya meliputi :
   a. sistem tidak dapat diakses oleh orang lain yang tidak berhak;
   b. penandatangan harus waspada terhadap penggunaan tidak sah dari data pembuatan tanda tangan oleh orang lain;
   c. penandatangan harus tanpa menunda-nunda, menggunakan cara yang dianjurkan oleh penyelenggara tanda tangan elektronik ataupun cara-cara lain yang layak dan sepatutnya harus segera memberitahukan kepada seseorang yang oleh penandatangan dianggap mempercayai tanda tangan elektronik atau kepada pihak pendukung layanan tanda tangan elektronik jika:
      1) Penandatangan mengetahui bahwa data pembuatan tanda tangan telah dibobol; atau
      2) Keadaan yang diketahui oleh penandatangan dapat menimbulkan resiko yang berarti, kemungkinan akibat bobolnya data pembuatan tanda tangan;
   d. dalam hal sebuah sertifikat digunakan untuk mendukung tanda tangan elektronik, memastikan kebenaran dan keutuhan dari semua informasi yang disediakan penandatangan yang terkait dengan sertifikat.
3. Setiap orang yang melakukan pelanggaran ketentuan sebagaimana dimaksud dalam ayat (1), bertanggung jawab atas segala kerugian dan konsekuensi hukum yang timbul.

Pasal 13

1. Setiap orang berhak menggunakan jasa penyelenggara sertifikasi elektronik untuk tanda tangan elektronik yang dibuat dalam bentuk tanda tangan digital.
2. Penyelenggara sertifikasi elektronik harus memastikan keterkaitan suatu tanda tangan digital dengan pemilik tanda tangan digital yang bersangkutan.
3. Penyelenggara sertifikasi elektronik Indonesia harus berbadan hukum Indonesia dan beroperasi di Indonesia.

Pasal 14

1. Penyelenggara sertifikasi elektronik sebagaimana dimaksud pada Pasal 13 wajib menyediakan informasi yang sepatutnya kepada para pengguna jasanya yang meliputi:
   a. Metode yang digunakan untuk mengidentifikasi penandatangan;

b. Hal-hal yang dapat digunakan untuk mengetahui data pembuatan tanda tangan elektronik;
c. Hal-hal yang dapat menunjukkan keberlakuan dan keamanan tanda tangan elektronik;

2. Ketentuan lebih lanjut mengenai penyelenggara sertifikasi elektronik diatur dengan Peraturan Pemerintah.

Dalam undang-undang ini jelas dikemukakan bahwa dokumen atau karya dalam bentuk informasi elektronik merupakan sesuatu yang dihargai dan harus dijaga. Suatu informasi elektronik yang seharusnya tidak bisa dengan bebas diakuisisi dan digunakan orang sebenarnya memiliki seseorang yang membuat, memikirkan, dan mengimplementasikannya maka dibutuhkanlah suatu alat untuk memvalidasi suatu informasi elektronik yang ada. Untuk hal tersebutlah digital signature kemudian makin harus dipahami dalam dunia informasi Indonesia.

Dalam penjelasan per pasal ditunjukkan bahwa tanda tangan digital pun ternyata harus dijaga dengan baik sehingga orang-orang yang masuk dalam alur informasi elektronik itu harus ikut menjaga informasi tersebut sehingga tetep valid. Selain itu mengenai hal-hal yang lain, sudah cukup dijelaskan dengan sangat jelas dalam kutipan pasal-pasal diatas.

Jadi pada undang-undang ini, dijelaskan digital signature memiliki peranan yang penting dalam efek dan validitas sebuah dokumen. Dimasukkan dalam aturan atau ketetapan untuk memberikan suatu cara memvalidkan suatu informasi digital. Hal ini merupakan suatu keberhasilan dalam dunia teknologi informasi karena hal ini akan menyelesaikan banyak permasalahan termasuk permasalahan penggunaan karya orang lain, pembajakan, dan lain-lain.

Pasal 32,33: Yuridiksi

Pasal 32

Setiap orang dilarang menggunakan dan atau mengakses komputer dan atau sistem elektronik Bank Sentral, lembaga perbankan dan atau lembaga keuangan yang dilindungi secara tanpa hak atau melampaui wewenangnya, untuk disalah gunakan, dan atau untuk mendapatkan keuntungan daripadanya.

Pasal 33

Setiap orang dilarang:

1. menyebarkan, memperdagangkan, dan atau memanfaatkan kode akses *(password)* atau informasi yang serupa dengan hal tersebut, yang dapat digunakan menerobos komputer dan atau sistem elektronik dengan tujuan menyalahgunakan yang akibatnya dapat mempengaruhi sistem elektronik Bank Sentral, lembaga perbankan dan atau lembaga keuangan, serta perniagaan di dalam dan luar negeri.
2. Menyebarkan, memperdagangkan, dan atau memanfaatkan kode akses *(password)* atau informasi yang serupa dengan hal tersebut, yang dapat digunakan menerobos komputer dan atau sistem elektronik dengan tujuan menyalahgunakan komputer dan atau sistem elektronik yang digunakan atau dilindungi oleh pemerintah.

Hal yang menarik dari pasal 32 ini adalah adanya pelebaran yuridiksi, dimana Pengadilan Indonesia berhak mengadili siapapun yang melakukan tindak pidana di bidang teknologi informasi yang akibatnya dirasakan di Indonesia. Sebagai contoh, jika seorang cracker Amerika melakukan kejahatan terhadap sebuah bank di Indonesia, maka pengadilan Indonesia berhak mengadili. Hal ini menimbulkan banyak pertanyaan, mulai dari justifikasinya sampai ke efektivas pelaksanaannya.

Pelebaran yuridiksi ini dengan sadar dan sengaja ditambahkan mengingat sifat teknologi informasi yang sudah global. Hal ini juga dilakukan oleh negara lain, seperti Amerika Serikat. Ada contoh kasus dimana seorang warga negara Rusia yang bernama Dmitri Sklyrov yang membuat sebuah program untuk menghilangkan proteksi yang diterapkan dalam *Adobe e-books*. Dia menulis programnya di Rusia, dimana hal ini bukanlah sesuatu yang ilegal. Ketika dia datang ke Amerika (untuk sebuah konferensi), dia ditangkap dan dipenjarakan. (Ada banyak sumber informasi di Internet yang membahas tentang kasus Dmitri Sklyrov ini secara lebih rinci.)

Kembali ke contoh seorang cracker Amerika yang melakukan kejahatan terhadap sebuah bank

Indonesia. Pasal 32 dan 33 ini memberikan kewenangan untuk menangkap dia ketika dia masuk ke wilayah Indonesia. Kita tidak harus secara proaktif mencoba menangkap dia di Amerika. Adanya sangsi ini membuat dia kehilangan kesempatan untuk mengunjungi Indonesia. Jika hal ini diterapkan oleh negara-negara lain maka cracker akan berpikir banyak untuk melakukan kejahatan jarak jauh karena semakin kecil dunia yang dapat dikunjunginya (secara fisik). Tanpa ada pasal ini, maka Indonesia akan menjadi tidak kuasa untuk mempertahankan diri dari serangan orang luar meskipun dampaknya dirasakan di Indonesia.

Permasalahan Lain dalam Hukum

Untuk lebih memahami dengan lebih dekat lagi hubungan legalitas dan dunia teknologi informasi serta bisnis, berikut ini akan dikemukakan sebuah pertanyaan sebagai pemicu atau *trigger*.

Bagaimana keabsahan suatu kontrak dan bentuk kontrak e-commerce, khususnya mengenai pembuktian dan masalah tanda tangan digital (digital signatur)?

Pada prinsipnya, menurut KUHPer, bentuk suatu perjanjian adalah bebas, tidak terikat pada bentuk tertentu. Namun, bila undang-undang menentukan syarat sahnya perjanjian seperti bila telah dibuat secara tertulis, atau bila perjanjian dibuat dengan akta notaris, perjanjian semacam ini di samping tercapainya kata sepakat terdapat kekecualian yang ditetapkan undang-undang berupa formalitas-formalitas tertentu. Perjanjian semacam ini dikenal dengan perjanjian formil, apabila formalitas-formalitas tersebut tidak dipenuhi, maka perjanjian tersebut akan terancam batal (seperti pendirian PT atau pengalihan hak atas tanah).

Untuk pengaturan e-commerce kita menerapkan KUHPer secara analogi, dimana terhadap ketentuan-ketentuan dari e-commerce diterapkan ketentuan dari Buku II tentang Hukum Perikatan dan KUHDagang). Dalam KUHPerdata ditentukan bahwa suatu persetujuan adalah suatu perbuatan dengan mana suatu orang atau lebih mengikatkan dirinya terhadap satu orang lain atau lebih (ps.1313 KUHPer). Untuk sahnya suatu kontrak maka kita harus melihat kepada syarat-syarat yang diatur di dalam ps.1320 KUHPer yang menentukan bahwa syarat sahnya suatu perjanjian adalah sebagai berikut:

1. kesepakatan para pihak;
2. kecakapan untuk membuat perjanjian;
3. suatu hal tertentu; dan
4. suatu sebab yang halal.

Dalam hal tidak terpenuhinya unsur pertama (kesepakatan) dan unsur kedua (kecakapan) maka kontrak tersebut dapat dibatalkan. Sedangkan apabila tidak terpenuhinya unsur ketiga (suatu hal tertentu) dan unsur keempat (suatu sebab yang halal) maka kontrak tersebut adalah batal demi hukum.

Suatu persetujuan tidak hanya mengikat apa yang dengan tegas ditentukan di dalamnya melainkan juga segala sesuatu yang menurut sifatnya persetujuan dituntut berdasarkan keadilan, kebiasaan atau undang-undang (ps.1339 KUHPer). Syarat-syarat yang selalu diperjanjikan menurut kebiasaan, harus dianggap telah termasuk dalam suatu persetujuan, walaupun tidak dengan tegas dimasukkan di dalamnya (ps.1347 KUHPer).

Saat ini, dengan makin pesatnya kemajuan teknologi informasi, dimana dengan adanya kemajuan tersebut orang dapat melakukan transaksi-transaksi perdagangan dengan tanpa kehadiran para pihak, seperti transaksi perdagangan dilakukan dengan *online trading*.

Menurut ajaran yang lazim dianut sekarang, perjanjian harus dianggap lahir pada saat pihak yang melakukan penawaran (*offerte*) menerima jawaban yang termaktub dalam surat tersebut, sebab detik itulah yang dapat dianggap sebagai detik lahirnya kesepakatan. Walaupun kemudian mungkin yang bersangkutan tidak membuka surat itu, adalah menjadi tanggungannya sendiri. Sepantasnyalah yang bersangkutan membaca surat-surat yang diterimanya dalam waktu yang sesingkat-singkatnya, karena perjanjian sudah lahir. Perjanjian yang sudah lahir tidak dapat ditarik kembali tanpa izin pihak lawan. Saat atau detik lahirnya perjanjian adalah penting untuk diketahui dan ditetapkan, berhubung adakalanya terjadi suatu perubahan undang-undang atau peraturan yang mempengaruhi nasib perjanjian tersebut, misalnya dalam pelaksanaannya atau masalah beralihnya suatu risiko dalam suatu peijanjian jual beli.

Tempat tinggal (domisili) pihak yang mengadakan penawaran *(offerte)* itu berlaku sebagai tempat lahirnya atau ditutupnya perjanjian. Tempat inipun menjadi hal yang

penting untuk menetapkan hukum manakah yang akan berlaku.

Sampai saat ini sistem pembuktian hukum privat masih mengunakan ketentuan yang diatur di dalam KUHPer, HIR (untuk Jawa Madura) dan RBg (untuk luar Jawa Madura). Dalam hukum pembuktian ini, alat-alat bukti dalam perkara perdata terdiri dari: bukti tulisan, bukti saksi-saksi, persangkaan-persangkaan, pengakuan dan bukti sumpah (ps.1866 KUHPer atau 164 HIR).

Sementara itu, dengan pesatnya Tekonologi Informasi melalui internet sebagaimana telah dikemukakan, yaitu telah mengubah berbagai aspek kehidupan, diantaranya mengubah kegiatan perdagangan yang semula dilakukan dengan cara kontak fisik, kini dengan internet kegiatan perdagangan dilakukan secara elektronik *(Electronic Commerce* atau *E-Commerce)* atau di Bursa Efek dikenal dengan *online trading.*

Keadaan tersebut di atas belum mendapat pengaturan dalam sistem hukum pembuktian, karena sampai saat ini hukum pembuktiannya masih menggunakan ketentuan hukum yang lama (KUHPer,HIR, dan RBg). Namun demikian, keberadaan Undang-undang No.8 Tahun 1997 tentang Dokumen Perusahaan (UU Dokumen Perusahaan) telah mulai menjangkau ke arah pembuktian data elektronik.

Memang, UU Dokumen Perusahaan tidak mengatur masalah pembuktian, namun UU ini telah memberi kemungkinan kepada dokumen perusahaan yang telah diberi kedudukan sebagai alat bukti tertulis otentik untuk diamankan melalui penyimpanan dalam mikro film. Selanjutnya, terhadap dokumen yang disimpan dalam bentuk elektronis *(paperless)* ini dapat dijadikan sebagai alai bukti yang sah. Di samping itu dalam ps.3 UU Dokumen Perusahaan telah memberi peluang luas terhadap pemahaman atas alat bukti, yaitu: "dokumen keuangan terdiri dari catatan, bukti pembukuaan, dan data pendukung administrasi keuangan, yang merupakan bukti adanya hak dan kewajiban serta kegiatan usaha perusahaan". Selanjutnya, ps.4 UU tersebut menyatakan: "dokumen lainnya terdiri dari data atau setiap tulisan yang berisi keterangan yang mempunyai nilai guna bagi perusahaan meskipun tidak terkait langsung dengan dokumen perusahaan". Berdasarkan uraian tersebut, maka tampaknya UU ini telah memberi kemungkinan dokumen perusahaan untuk dijadikan sebagai alat bukti.

Dari perspektif hukum, *digital signature* adalah sebuah pengaman pada data digital yang dibuat dengan kunci tanda tangan pribadi (*private siganture key*), yang penggunaannya tergantung pada kunci publik (*public key*) yang menjadi pasangannya. Eksistensi *digital signature* ini ditandai oleh keluarnya sebuah sertifikat kunci tanda tangan (*signature key certificate*) dari suatu badan pembuat sertifikat (*certifier*). Dalam sertifikat ini ditentukan nama pemilik kunci tanda tangan dan karakter dari data yang sudah ditandatangani, untuk kekuatan pembuktian (German Draft Digital signature Law, 1996).

Beberapa masalah yang mungkin timbul dari sistem *digital signature* ini terkait dengan sistem hukum yang sudah ada. Pada banyak negara, disyaratkan bahwa suatu transaksi haruslah disertai dengan bukti tertulis, dengan pertimbangan kepastian hukum.

Permasalahannya, bagaimana sebuah dokumen elektronik yang ditandatangani dengan sebuah *digital signature* dapat dikategorikan sebagai bukti tertulis? Di lnggris, bukti tertulis haruslah berupa tulisan *(typing),* ketikan *(printing),* litografi *(lithography),* fotografri, atau bukti-bukti yang mempergunakan cara-cara lain, yang dapat memperlihatkan atau mengolah kata kata dalam bentuk yang terlihat secara kasat mata. Definisi dari bukti tertulis itu sendiri sudah diperluas hingga mencakup juga “telex, telegram, atau cara-cara lain dalam telekomunikasi yang menyediakan rekaman dan perjanjian" (UNCITRAL Model Law on Internatinal Commercial Arbitration, art.7 (2)).

Sebenarnya, dari fakta-fakta tersebut dapatlah ditarik kesimpulan bahwa dokumen elektronik yang ditandatangani dengan sebuah *digital signature* dapat dikategorikan sebagai bukti tertulis. Tetapi, terdapat suatu prinsip hukum yang menyebabkan sulitnya pengembangan penggunaan dan dokumen elektronik atau *digital signature*, yakni adanya syarat bahwa dokumen tersebut harus dapat di lihat, dikirim dan disimpan dalam bentuk kertas.

Masalah lain yang dapat timbul berkaitan dengan dokumen elektronik dan *digital signature* ini adalah masalah cara untuk menentukan dokumen yang asli dan dokumen salinan. Berkaitan

dengan hal ini sudah menjadi prinsip hukum umum bahwa:

1. dokumen asli mestilah dalam bentuk perjanjian tertulis yang ditandatangani oleh para pihak yang melaksanakan perjanjian;
2. dokumen asli hanya ada satu dalam setiap perjanjian; dan
3. semua reproduksi dari perjanjian tersebut merupakan salinan.

ASPEK PRAKTIK

Setelah ini akan dibahas tentang tanda tangan digital jika ditelaah dari aspek praktiknya yaitu melihat cara implementasi algoritma yang ada.

Algoritma Digital Signature

Enkripsi Kunci Publik

Whitfield Diffie dan Martin Hellman memperkenalkan konsep public-key cryptography pada 1976. Public-key cryptosystems memiliki dua kegunaan primer, enkripsi dan tanda tangan digital. Pada sistemnya, setiap orang mendapatkan sepasang kunci, satu disebut kunci public dan yang lain disebut kunci privat. Kunci publik dipublikasikan, sedangkan kunci privat disimpan rahasia. Kebutuhan pengirim dan penerima untuk berbagi informasi rahasia dieliminasi; semua komunikasi hanya mencakup kunci publik, kunci privat tidak pernah ditransmisikan atau dipakai bersama. Pada sistem ini, tidak perlu lagi untuk mempercayai keamanan beberapa peralatan komunikasi. Kebutuhannya hanya kunci publik diasosiasikan dengan penggunanya dengan cara yang dapat dipercaya (diotentikasi) (sebagai contoh, dalam direktori yang dipercaya). Setiap orang dapat mengirimkan pesan rahasia hanya dengan menggunakan informasi publik, tetapi pesan hanya dapat didekripsi dengan kunci privat, yang merupakan milik penerima yang dituju. Lebih jauh lagi, public-key cryptography dapat digunakan tidak hanya untuk kerahasiaan (enkripsi), tetapi juga untuk otentikasi (tanda tangan digital) dan teknik-teknik lainnya.

Pada public-key cryptosystem, kunci privat selalu dihubungkan secara matematis dengan kunci publik. Karena itu, dimungkinkan untuk menyerang sistem public-key dengan menurunkan kunci privat dari kunci publik. Pada umumnya, antisipasi atas masalah ini adalah dengan membuat masalah penurunan kunci privat sesulit mungkin. Sebagai contoh, beberapa public-key cryptosystems dirancang sedemikian rupa sehingga penurunan kunci privat dari kunci publik membutuhkan penyerang untuk memfaktorkan angka yang besar, dalam kasus ini tidak mungkin secara komputasi untuk melakukan penurunan ini. Ini adalah ide dibalik RSA public-key cryptosystem.

RSA

RSA cryptosystem adalah public-key cryptosystem yang menawarkan baik enkripsi dan tanda tangan digital (otentikasi). Ronald Rivest, Adi Shamir, dan Leonard Adleman mengembangkan sistem RSA system pada tahun 1977.

Algoritma RSA bekerja seperti berikut: ambil dua bilangan prima besar, p dan q, dan hitung hasil kalinya $n = pq$; n disebut dengan modulus. Pilih sebuah bilangan, e, yang lebih kecil dari n dan merupakan bilangan prima secara relatif dari $(p-1)(q-1)$, yang artinya e dan $(p-1)(q-1)$ tidak memiliki faktor bersama kecuali 1. temukan bilangan lain d sehingga $(ed - 1)$ dapat dibagi dengan $(p-1)(q-1)$. Nilai-nilai e dan d masing-masing disebut eksponen publik dan privat. Kunci publik adalah pasangan (n, e); kunci privat adalah (n, d). Faktor p dan q dapat dihancurkan atau disimpan dengan kunci privat. Sulit untuk mendapatkan kunci privat d dari kunci publik (n, e). Jika seseorang dapat memfaktorkan n menjadi p dan q, maka ia bisa mendapatkan kunci privat d. Sehingga keamanan sistem RSA berdasar pada asumsi bahwa pemfaktoran sulit dilakukan. Dibawah ini adalah bagaimana sistem RSA dapat digunakan untuk enkripsi dan tanda tangan digital (dalam prakteknya, penggunaan aktualnya sedikit berbeda):

Enkripsi:
Anggap Alice ingin mengirim pesan m kepada Bob. Alice membuat ciphertext c dengan mengeksponenkan: $c = m^e \bmod n$, dimana e dan n adalah kunci publik Bob. Alice mengirim c kepada Bob. Untuk mendekripnya, Bob juga mengeksponenkan: $m = c^d \bmod n$; hubungan antara e dan d meyakinkan bahwa Bob mendapatkan m dengan benar. Karena hanya Bob yang mengetahui d, hanya Bob yang dapat mendekrip pesan ini.

Tanda tangan digital:
Anggap Alice ingin mengirim pesan m kepada Bob sehingga Bob yakin bahwa pesannya otentik, tidak dimodifikasi, dan dari Alice. Alice

membuat tanda tangan digital s dengan mengeksponenkan: $s = m^d \bmod n$, dimana d dan n adalah kunci privat Alice. Alice mengirim m dan s kepada Bob. Untuk memverifikasi tandatangan, Bob mengeksponenkan dan mengecek bahwa pesan m didapatkan: $m = s^e \bmod n$, dimana e dan n adalah kunci publik Alice.

Diffie Hellman Key Exchange

Diffie-Hellman key exchange adalah metode dimana subyek menukar kunci rahasia melalui media yang tidak aman tanpa mengekspos kunci. Metode ini diperlihatkan oleh Dr. W. Diffie dan Dr. M. E. Hellman pada tahun 1976 pada papernya "New Directions in Cryptography". Metode ini memungkinkan dua pengguna untuk bertukar kunci rahasia melalui media yang tidak aman tanpa kunci tambahan. Metode ini memiliki dua parameter sistem, *p* dan *g*. Kedua parameter tersebut publik dan dapat digunakan oleh semua pengguna sistem. Parameter *p* adalah bilangan prima, dan paramater *g* (sering disebut generator) adalah integer yang lebih kecil dari *p* yang memiliki properti berikut ini: Untuk setiap bilangan *n* antara 1 dan *p-1* inklusif, ada pemangkatan *k* pada *g* sehingga $g^k = n \bmod p$.

El Gamal

Dr. El Gamal memperluas konsep Diffie-Hellman untuk diterapkan pada enkripsi dan tanda tangan digitals. Sistem El Gamal adalah public-key cryptosystem yang tidak dipatenkan yang berdasar pada masalah logaritma diskret. Enkripsi dengan El Gamal diilustrasikan dengan contoh di bawah ini:

Diberikan bilangan prima, *p* dan integer, *g*, Alice menggunakan kunci privatnya, *a*, untuk menghitung kunci publiknya sebagai $y_a = g_a \bmod p$.
Untuk Bob untuk mengirim pesan ke Alice:

1. Bob menggenerate random #b < p.
2. Bob menghitung $y_b = g_b \bmod p$ dan $y_m = M$ XOR $y_{ab} = M$ XOR $g_{ab} \bmod p$.
3. Bob mengirim y_b, y_m kepada Alice, dan Alice menghitung $y_{ba}=g_{ab} \bmod p$.
4. Karena itu $M = y_{ba}$ XOR $y_m = g_{ab} \bmod p$ XOR M XOR $g_{ab} \bmod p$.

Elliptic Curve

Elliptic curve cryptosystems pertama kali diusulkan secara independen oleh Victor Miller dan Neal Koblitz pada pertengahan tahun 80an. Pada level tinggi, metode in merupakan analog dari public-key cryptosystems yang telah ada dimana aritmatika modular digantikan dengan operasi diseputar kurva eliptik.

Seperti pada semua public-key cryptosystems, keamanan elliptic curve cryptosystems tergantung pada masalah matematika berat yang digunakannya: Diberikan dua titik *G* dan *Y* pada kurva eliptik sehingga $Y = kG$ (sehingga, *Y* adalah *G* ditambah dengan dirinya sendiri sebanyak *k* kali), temukan integer *k*. Masalah ini biasanya disebut dengan *elliptic curve discrete logarithm problem*.

Sekarang ini, metode untuk menghitung logaritma diskret kurva eliptik yang umum tidak begitu efisien daripada metode untuk memfaktorkan atau menghitung logaritma diskret konvensional. Sebagai hasilnya, ukuran kunci yang lebih pendek dapat digunakan untuk mencapai keamanan yang sama dengan public-key cryptosystems konvensional, yang dapat membawa ke kebutuhan memori yang lebih baik dan perbaikan unjuk kerja. Seseorang dapat dengan mudah mengkonstruksi enkripsi kurva eliptik, signature, dan key agreement schemes dengan membuat analog dari ElGamal, DSA, dan Diffie-Hellman. Varian-varian ini tampaknya menawarkan keuntungan implementasi tertentu dengan skema aslinya, dan mendapatkan perhatian yang lebih dari komunitas akademik maupun industri.

KESIMPULAN

Setelah membahas tanda tangan digital dari beberapa pandangan dan literature dengan menggunakan dua garis besar yaitu legal dan praktik, telah dijelaskan secara umum perkembangan yang terjadi dalam dunia ilmu pengetahuan yaitu Kriptografi.

Bidang ini melahirkan suatu teknik pemvalidasian suatu informasi elektronik yang disebut tanda tangan digital. Tanda tangan digital mulai diperkenalkan dan mulai berkembang. Dari penggunaannya dari mulai keperluan-keperluan yang belum memasyarakat sampai ke keperluan masyarakat yang selalu dilakukan untuk memenuhi aktivitas sehari-sehari akhirnya muncul keinginan dari para periset untuk semakin mengembangkan teknik-teknik yang digunakan dalam tanda tangan digital.

Perkembangan ini memicu penggunaan yang semakin baik dan efektif untuk berbagai tujuan. Untuk mengatur sesuatu yang menyangkut berbagai kepentingan yang ada maka aspek legal pun menjadi sasaran untuk membatasi dan mendefinisikan segala sesuatu. Dalam aspek legalitas yang ada, tanda tangan digital menjadi salah satu alat juga untuk memberikan suatu penanda atau pemvalid kebenaran atau keabsahan informasi.

Akhirnya penulis menyimpulkan bahwa perkembangan tanda tangan digital baik dilihat dalam aspek legal ataupun praktik adalah perkembangan yang cepat. Perkembangan yang cepat ini didorong dengan keinginan orang untuk menggunakan tanda tangan digital dengan semakin baik dan efisien dan mungkin juga untuk tujuan yang lain lagi.

DAFTAR PUSTAKA

"Rancangan Undang-Undang Republik Indonesia tentang Informasi dan Transaksi Elektronik" URL : www.depkominfo.go.id/download/Penjelasan_RUU_ITE_Final140605.doc

Hukum Online URL : http://Hukumonline.com

Wikipedia . "Digital Signature" URL: http://en.wikipedia.org/wiki/Digital_signature

Wikipedia ."Digital Signature Algorithm" URL : http://en.wikipedia.org/wiki/Digital_Signature_Algorithm

Wikipedia ."Elliptic Curve DSA" URL: http://en.wikipedia.org/wiki/Elliptic_Curve_DSA

Wikipedia ."RSA" URL: http://en.wikipedia.org/wiki/RSA

Wikipedia ."ElGamal Signature" URL: http://en.wikipedia.org/wiki/ElGamal_signature_scheme

Ardana, Made."Digital Signature dengan WAP Identity Module" URL : http://budi.insan.co.id/courses/el7010/dikmenjur/made-report.pdf

Raharjo, Budi."Panduan Cyberlaw Untuk Orang Biasa" URL : www.cert.or.id/~budi/articles/**panduan-cyberlaw**.pdf

Latifulhayat, Atip. "Cyberlaw dan Urgensinya Bagi Indonesia". URL : http://polri.go.id

Mukti, Arrianto. "Tanda tangan digital dan sertifikat digital : Apa itu ?".1998. URL : http://www.geocities.com/amwibowo/resource/sertifik/

Sapty, Flourensia. "Suplemen Bahan ajar Mata Kuliah Proteksi dan Teknik Keamanan Sistem Informasi – IKI 83408T".2005.Magister Teknologi Informasi Fakultas Ilmu Komputer Universitas Indonesia.Jakarta URL : bebas.vlsm.org/v06/**Kuliah**/MTI-Keamanan-Sistem-Informasi/2005/124/124P-04-final2.0-**Cryptography**.pdf

Ardian, L." Jaringan Privat Virtual Dinamis: Sebuah Jawaban Keamanan untuk Intranet Bisnis" URL : http://www.elektroindonesia.com/elektro/

Raharjo, Budi." Cyberlaw: Teritori dalam cyberspace, realitas dan virtualitas" URL : www.cert.or.id/~budi/articles/it-within-**cyberlaw**.doc

Perkuliahan tentang tanda tangan digital dan algoritmanya (kunci simentris dan fungsi hash), URL : http://webmail.informatika.org/~rinaldi/Kriptografi/2006-2007/bahankuliah2006.htm