

BAB 2

HUKUM PERLINDUNGAN PENGGUNA KARTU PEMBAYARAN DAN PENYELENGGARAAN SISTEM TRANSAKSI ELEKTRONIK

2.1 Tinjauan Umum Alat Pembayaran Elektronik

Alat pembayaran adalah alat tukar menukar yang sah, secara umum dikenal sebagai uang. Uang diakui dalam ilmu ekonomi tradisional dan modern sebagai suatu alat pembayaran yang berlaku secara universal. Bentuk dan fungsi dari uang itu sendiri terus berkembang seiring dengan perkembangan jaman. Dengan pertumbuhan ekonomi yang semakin pesat, maka fungsi dari uang juga diharapkan dapat menjembatani proses pembayaran yang serba cepat, tepat dan aman. Konsep ini berkembang terus sesuai dengan perkembangan jaman dan teknologi.

Bentuk uang yang semula berupa logam dan kertas tidak lagi cukup untuk memenuhi kebutuhan masyarakat masa kini. Kini sebuah bentuk baru dari uang tercipta, yaitu dalam bentuk informasi dan data atau aplikasi yang tersimpan dalam sebuah objek yang umumnya berbentuk kartu. Melalui bab ini penulis akan menuturkan apa yang dimaksud dengan alat pembayaran elektronik khususnya yang menggunakan kartu serta sistem pembayaran elektronik tersebut dan bagaimana fungsi serta sistem bekerjanya.

2.1.1 Sejarah Alat Pembayaran

Pada awalnya manusia tidak mengenal apa yang dimaksud dengan alat pembayaran. Jaman dahulu jika seseorang menginginkan sesuatu dia akan menukar barang miliknya dengan barang yang dia inginkan atau dinamakan dengan sistem barter. Contohnya adalah ketika seseorang menginginkan beras dia akan menukar hewan ternaknya dengan orang lain yang mempunyai beras tersebut. Dengan sistem barter ini orang belum mengenal apa yang dimaksud

dengan kepastian, sehingga nilai dari suatu barang menjadi rancu atau tidak jelas.

Seiring dengan waktu dan kegiatan perdagangan yang terus berkembang, manusia memerlukan akan adanya kepastian. Lalu manusia mulai mengembangkan suatu alat pembayaran yang dikenal dengan uang, yaitu suatu alat yang berfungsi untuk menentukan nilai suatu barang serta sebagai alat tukar yang pasti. Uang yang pertama kali diciptakan adalah uang dalam bentuk logam lalu berevolusi menjadi bentuk kertas dan terus berkembang. Evolusi alat pembayaran terus terjadi sesuai dengan tuntutan masyarakat terhadap suatu alat pembayaran yang lebih praktis dan efisien untuk di gunakan. Sampai dengan akhir tahun 1800-an konsumen dan pedagang telah melakukan tukar menukar barang melalui konsep kredit atau hutang.

Pada awal 1900-an, perusahaan-perusahaan minyak dan pusat perbelanjaan (*department store*) di Amerika Serikat mulai mengeluarkan kartu milik mereka sendiri. Namun kartu ini digunakan masih terbatas hanya pada perusahaan-perusahaan yang mengeluarkan kartu saja dan di lokasi yang terbatas.

Kartu pembayaran bank yang pertama kali bernama *charge-it* diperkenalkan pada tahun 1946 oleh John Biggins, seorang bankir di Brooklyn, New York. Ketika seorang pelanggan menggunakannya untuk melakukan pembelian, tagihan itu diteruskan ke bank miliknya. Untuk selanjutnya pihak bank melakukan penggantian kepada pedagang dan memperoleh pembayaran dari pelanggan. Meskipun demikian kartu ini hanya berlaku terbatas, pembelian hanya bisa dibuat secara lokal dan pemegang kartu *charge-it* harus memiliki akun di Bank Biggins.²⁶

²⁶ Emiliy Starbuck Gerson and Ben Woolsey. *The History of Credit Cards*. <http://www.creditcards.com/credit-card-news/credit-cards-history-1264.php>, diakses pada tanggal 21 Juli 2010.

Setelah mengalami perkembangan pada tahun 1951, kartu kredit bank pertama muncul pada *Franklin National Bank* di New York, Amerika Serikat yang berlaku untuk pinjaman pelanggan. Namun kartu ini juga tetap terbatas hanya dapat digunakan oleh apra pemilik rekening bank saja.²⁷

Pada pertengahan abad 20 yaitu tepatnya sekitar tahun 1950-an, suatu bentuk alat pembayaran yang lebih praktis mulai dikenal. Sebuah konsep baru dengan menggunakan sebuah alat yang lebih mudah digunakan sebagai bentuk jaminan kepada pihak yang menawarkan barang dan jasa. Sejarah mencatat, alat pembayaran seperti ini dikenal pertama kali pada tahun 1950-an di New York tepatnya, pada saat itu alat pembayaran kartu yang pertama kali dikeluarkan merupakan produk dari *Diners Club* dan *American Express*. Sebuah kartu plastik yang diberikan kepada kurang lebih 200 pelanggan dan dapat di gunakan pada 27 restoran di New York. Alat pembayaran ini pertama kali dikenal sebagai kartu kredit (*credit card*) yang namanya berasal dari bahasa latin *credit* yang berarti *trust* (kepercayaan) dan *card* yang berarti kartu.²⁸

Pada tahun 1959, mekanisme pembayaran yang menjaga keseimbangan terhadap perputaran pembayaran mulai diperkenalkan. Mekanisme tersebut bekerja dengan cara pemegang kartu tidak lagi harus membayar tagihan mereka langsung penuh pada tagihan pertama, melainkan pengguna dapat melakukan cicilan pembayaran terhadap hutang mereka kepada penerbit kartu. Meskipun sistem ini dapat mengakibatkan masalah baru kepada pemegang kartu, yaitu dengan akumulasi jumlah bunga pada tagihan apabila pembayaran tidak dilakukan dengan baik dan terencana, namun sesungguhnya sistem ini juga dapat membawa kegunaan yang lebih efektif dan efisien jika dilakukan dengan benar.²⁹

²⁷ *Ibid.*

²⁸ David Evans dan Richard Schmless. *Paying With Plastic : The Digital Revolution In Buying and Borrowing*. MIT press. 2001. Hlm 61.

²⁹ Emiliy Starbuck Gerson and Ben Woolsey. Loc Cit.

Pada tahun 1966 lahir dua pesaing besar di dunia alat pembayaran menggunakan kartu, yaitu Visa dan Mastercard, yang pada awalnya di kenal dengan nama *Bank Americard* (Visa) dan *Inter Bank Card Association* (Mastercard). Kedua perusahaan besar ini memperkenalkan sistem baru yang disebut dengan *Open Loop* , yaitu suatu sistem yang menggunakan kerjasama dan transfer dana antar bank.

Di Indonesia sendiri usaha kartu kredit mulai dikembangkan pada tahun 1973 dengan masuknya kartu produk *Diners Club*. Pada tahun 1983 Bank Central Asia mulai memasuki usaha kartu kredit yang ditandai dengan diterbitkannya “*MasterCard*” lalu diikuti oleh Bank Duta setahun kemudian yang menerbitkan kartu berlogo “*Visa*” dan mempelopori penyediaan fasilitas kartu kredit dengan penagihan dalam mata uang rupiah.³⁰

Setelah perkembangan yang dialami oleh kartu kredit lalu munculah jenis-jenis pembayaran baru seperti *debit card* (kartu debit) dan *stored value card* (kartu penyimpan dana). Kemunculan kartu-kartu ini dengan berbagai jenis telah memberikan pilihan kepada pengguna untuk memilih cara pembayaran yang sesuai dengan keperluan masing-masing.

2.1.2 Definisi Alat Pembayaran Menggunakan Kartu

Dilihat dari namanya secara nalar definisi yang kita bayangkan atas apa itu alat pembayaran menggunakan kartu adalah suatu alat yang berfungsi sebagai alat pembayaran dan mempunyai fisik berbentuk sebuah Kartu. Namun tidak semua alat pembayaran yang mempunyai ciri-ciri seperti itu termasuk dalam pengaturan APMK.

Peraturan mengenai APMK sendiri diatur dalam Peraturan Bank Indonesia No. 11/11/PBI/2009 tentang Penyelenggaraan Kegiatan APMK. Jenis APMK yang diatur dalam PBI tersebut meliputi kartu ATM, kartu debit

³⁰ Zufidah Erlimah Pasaribu. Tinjauan Yuridis Tentang Pengawasan Bank Indonesia Terhadap Bank Penerbit Kartu Kredit Sehubungan dengan Perkembangan Produk dalam Layanan Jasa Kartu Kredit. Thesis. Universitas Indonesia. 2004. Hlm 33.

dan kartu kredit. Dalam PBI itu dijelaskan, pada prinsipnya penyelenggaraan kegiatan penerbitan kartu ATM, kartu debit dan kartu kredit masing-masing memiliki karakteristik tersendiri, sehingga izin yang diberikan oleh BI bersifat per jenis kartu.

Peraturan Bank Indonesia (PBI) No 11/12/PBI/2009 yang mulai berlaku 13 April 2009 tentang uang elektronik BI memisahkan *prepaid card cash (e-money)* dengan APMK, dimana *e-money* juga berfungsi sebagai alat pembayaran dan biasanya menggunakan kartu. Namun *e-money* sebenarnya mempunyai beberapa bentuk lain yaitu dalam bentuk digital sehingga *e-money* juga mempunyai karakteristik yang berbeda dari APMK. Karakteristik tersebut yaitu (1) diterbitkan atas dasar nilai uang yang disetor terlebih dahulu oleh pemegang kepada penerbit; (2) nilai uang disimpan secara elektronik dalam suatu media seperti *server* atau *chip*; (3) digunakan sebagai alat pembayaran kepada pedagang yang bukan merupakan penerbit uang elektronik tersebut; dan (4) nilai uang elektronik yang disetor oleh pemegang dan dikelola oleh penerbit bukan merupakan simpanan sebagaimana dimaksud dalam undang-undang yang mengatur mengenai perbankan.³¹

2.1.3 Model Alat Kartu Pembayaran Elektronik

A. *Credit Card* (Kartu Kredit)

Walaupun belum ada pengertian kartu kredit yang diakui secara universal, namun beberapa literatur mencoba memberikan definisi yang tepat tentang apa itu kartu kredit antara lain dari, *Black law dictionary* yang menuliskan kartu kredit sebagai :

“any card, plate or any other like credit device existing for the purpose of obtaining money, property, labour or services on credit.

³¹BankIndonesia.
http://www.bi.go.id/web/id/Peraturan/Sistem+Pembayaran/pbi_111209.htm.
Ringkasan nomor 2.

The term does not include a note, cheque, draft, money order or other like negotiable instrument”³²

Tony Drury dan Charles W. Ferrier dalam bukunya yang berjudul *Credit Card*, mengatakan :

“credit card is an instrument of payment wich enables the cardholder to obtain either goods or services from merchants where arrangements have been made (directly or indirectly) by the card issuer, who also makes arrangements to reimburse the merchant. The cardholder settles with the card issuer in accordance with the terms of the particular scheme. In certain instances credit cards may be used to obtain cash.”³³

Sedangkan pendapat Abdul Kadir Muhammad dan Rilda Murniati berpendapat bahwa kartu kredit adalah :

*“Alat pembayaran melalui jasa bank/perusahaan pembiayaan dalam transaksi jual beli barang/jasa, atau alat untuk menarik uang tunai dari bank/perusahaan pembiayaan. Kartu kredit tersebut diterbitkan. Berdasarkan perjanjian tersebut, peminjam memperoleh pinjaman dana dari bank.perusahaan pembiayaan. Peminjam dana adalah pihak yang menerima kartu kredit, yang disebut Pemegang Kartu (*card holder*) , dan bank/perusahaan pembiayaan adalah pihak yang menyerahkan kartu kredit, yang disebut Penerbit (*issuer*).”³⁴*

Kartu kredit sebagai alat pembayaran elektronik merupakan wujud bentuk atas pemenuhan kebutuhan masyarakat akan adanya alat pembayaran yang efisien dan efektif. Sekarang ini dengan perubahan gaya hidup masyarakat, kartu kredit tidak lagi dianggap sebagai sebuah barang mewah.

Di Indonesia penggunaan kartu kredit sudah sangat lazim dan banyak sekali penggunaanya. Tercatat pada Tahun 2007, tingkat pembelanjaan kartu kredit secara nasional mencapai Rp72,77 triliun. Jumlah itu naik 27 persen dari realisasi tahun 2006 yang masih Rp57,42

³² Henry Campbell Black’s Dictionary. *Sixth Edition*. St. Paul Minn: West Publishing Co. 1990. Hlm. 369.

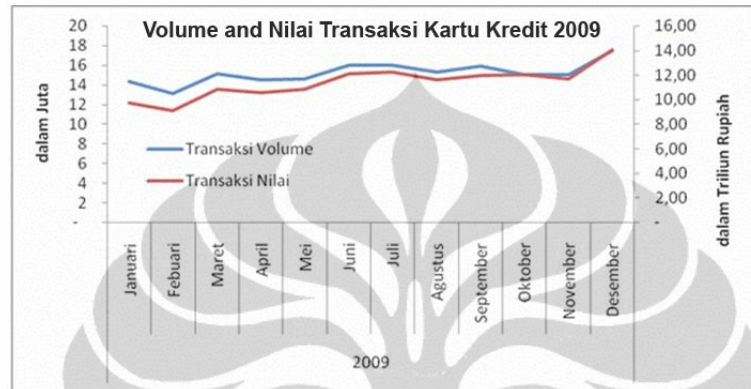
³³ Tony Drury and Charles W. Ferrier. *Credit Card*. London Butterworths. 1984. Hlm Xii.

³⁴ Muhammad Abdulkadir dan Rilda Muniarti. Segi Hukum Lembaga Keuangan dan Pembiayaan. Bandung: PT Citra Aditya Bakti. 2000. Hlm. 510.

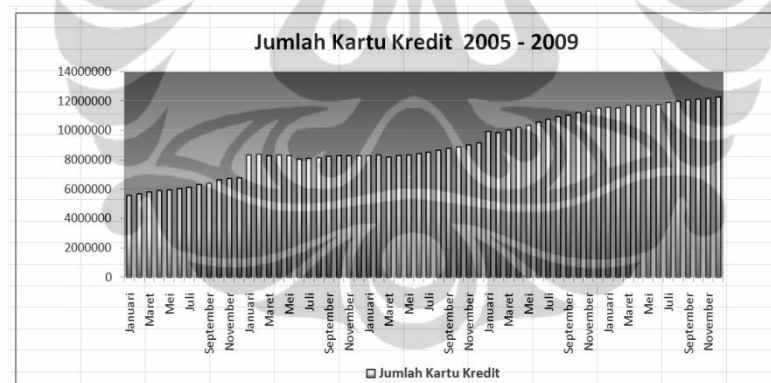
triliun. Sementara, jumlah kartu yang beredar pada tahun 2007 mencapai 9,1 juta atau naik 12 persen dari realisasi 2006 yang masih 8,2 juta kartu.³⁵

Berikut Tabel dari situs resmi AKKI terhadap penggunaan kartu kredit di Indonesia :³⁶

Tabel 2.1



Tabel 2.2



Sebagai alat pembayaran tentunya kartu kredit mempunyai sifat-sifat tertentu yang menjadi pembeda dengan alat pembayaran yang lain dalam hal fungsi. Beberapa karakter dasar yang melekat pada kartu kredit

³⁵ Diki Sumadi. Empat Kasus Kejahatan Kartu Kredit Ditemukan. <http://www.antaraneews.com/view/?i=1202827007&c=EKB&s=> . Di akses tanggal 26 Agustus 2010. Pukul 0:51 WIB.

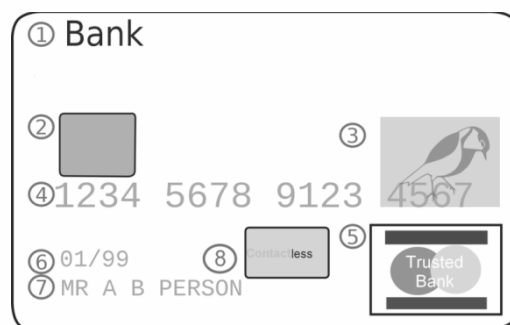
³⁶ Situs resmi Asosiasi Kartu Kredit Indonesia. <http://akki.or.id/>. Di akses tanggal 2september 2010. Pukul 15:57 WIB.

menurut Flory Santosa dalam bukunya “Pedoman Praktis Menghindari Perangkap Utang Kartu Kredit” adalah :³⁷

- a. Kartu kredit merupakan produk massal (*mass product*);
- b. Tanpa sekat antar negara (*borderless*) dapat digunakan di semua negara sepanjang terdapat penyelenggaraan sistem kartu kredit (yang paling luas saat ini adalah Visa dan Mastercard);
- c. Dalam produk kartu kredit terdapat perjanjian tanpa batas akhir dan bersifat revolving (*open end and revolve*) yaitu tidak seperti perjanjian kredit pada umumnya klausul mengenai berakhirnya perjanjian kredit yaitu sesuai dengan tenor kredit yang diajukan, dalam produk kartu kredit tidak dicantumkan masa berakhirnya kartu kredit. Dengan kata lain bahwa pada prinsipnya utang kartu kredit tanpa batas akhir yang definitif;
- d. Didukung dengan teknologi;
- e. Dari sudut pandang Bank Penerbit bisnis kartu kredit sering sebagai salah satu lini bisnis berisiko tinggi dengan keuntungan tinggi (*high gain high risk*).

Selain dari fungsinya, bentuk kartu kredit secara fisik juga relatif berbeda dengan alat pembayaran kartu yang lain. Sebuah kartu kredit mempunyai bentuk tertentu seperti contoh *Gambar* di bawah :

Tampak depan kartu kredit

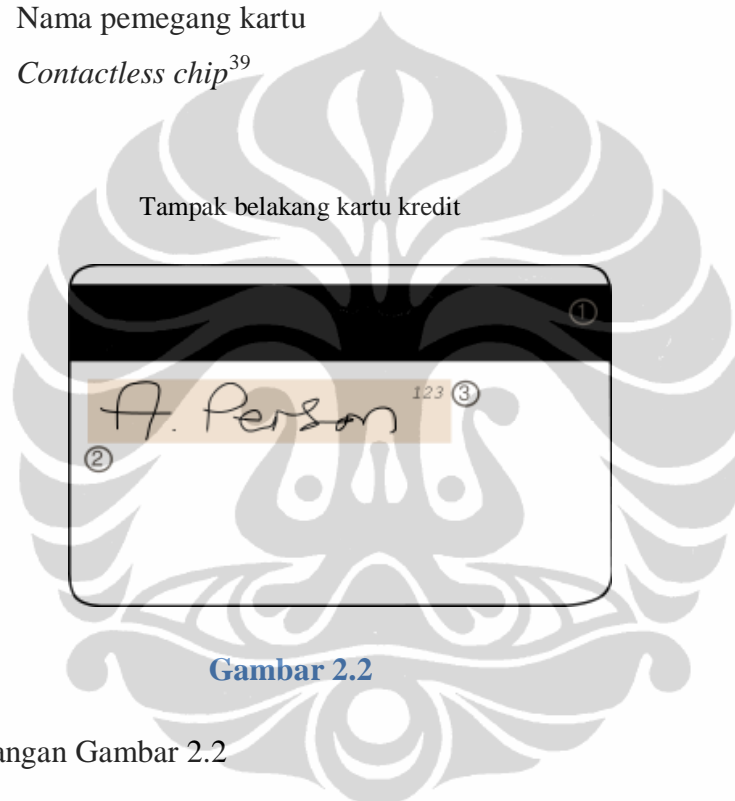


Gambar 2.1

³⁷ Flory Santosa, Pedoman Praktis Menghindari Perangkap Utang Kartu Kredit, (Jakarta : Forum Sahabat, 2009), hlm. 1.

Keterangan Gambar 2.1 :

1. Logo Bank Penerbit
2. EMV *chip*³⁸
3. *Hologram*
4. Nomor Kartu Kredit
5. Logo Merk Kartu Kredit
6. Tanggal daluwarsa
7. Nama pemegang kartu
8. *Contactless chip*³⁹



Gambar 2.2

Keterangan Gambar 2.2

1. Garis magnetik kartu
2. Kolom tanda tangan pemilik
3. Kode keamanan kartu⁴⁰

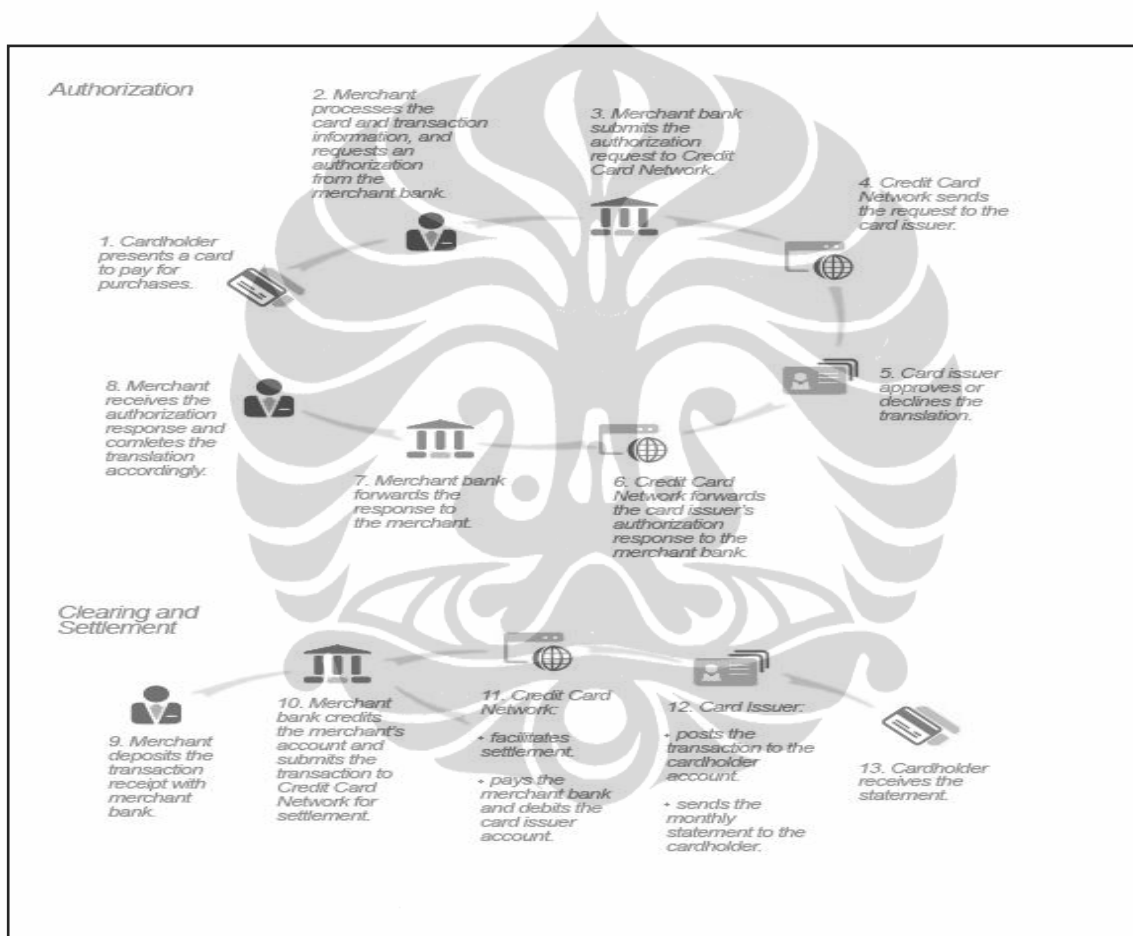
³⁸ EMV yang merupakan kepanjangan dari Europay, Mastercard dan Visa, ketiga perusahaan yang melakukan pengembangan terhadap *chip* ini yang berfungsi sebagai alat otentifikasi terhadap transaksi penjualan atau penggunaan pada mesin ATM.

³⁹ *Chip* yang ada di dalam kartu kredit diterapkan dengan teknologi daya elektromagnet sehingga dalam penggunaannya *chip* ini cukup disentuh pada mesin *Electronic Draft Capture* (EDC). Biasa disebut sebagai transaksi *touch and go* atau *wave and pay* karena biasanya transaksi dengan menggunakan metode ini tidak memerlukan otentifikasi di bawah jumlah transaksi tertentu yang telah ditetapkan penerbit sebelumnya (*micropayment*).

⁴⁰ Kode keamanan kartu atau yang biasa disebut sebagai *Card Security Code* (CSC) adalah pengamanan tambahan terhadap penggunaan kartu terutama ketika melakukan transaksi tidak langsung, seperti transaksi melalui *internet* di mana penjual dan pembeli berada di tempat

Dalam penggunaan kartu kredit ini dalam sebuah sistem pembayaran elektronik ada suatu standar yang diberlakukan atau diperjanjikan sebelumnya pada pihak-pihak yang melakukan pembayaran elektronik tersebut. Salah satu prosedur yang dapat kita lihat adalah seperti yang dijelaskan pada *Gambar* skema di bawah berikut keterangannya.

Skema transaksi kartu kredit



Gambar 2.3

Keterangan Gambar 2.3:

1. Pemegang Kartu kredit memperlihatkan atau menyerahkan kepada kartu kepada penjual untuk digunakan;

yang berbeda, sebagai bentuk otorisasi biasanya penjual dalam melakukan transaksi tersebut harus memasukkan terlebih dahulu nomor kartu, nomor CSC dan tanggal kadaluarsa kartu.

2. Penjual memproses kartu dan melakukan transaksi informasi kepada pengelola (*acquire*);
3. *Acquirer* memberikan otorisasi kepada jaringan sistem kartu kredit (prinsipal);
4. Prinsipal mengirimkan permintaan transaksi kepada bank penerbit (*issuer*) karena berfungsi sebagai pembiaya transaksi;
5. Bank penerbit menerima atau menolak permohonan;
6. Jaringan sistem pembayaran memberikan informasi dari bank penerbit kepada bank penjual;
7. Bank penjual menginformasikan kepada penjual;
8. Penjual menerima secara lengkap otorisasi tersebut dan menyelesaikan transaksi;
9. Penjual memberikan tanda transaksi kepada bank penjual ;
10. Bank penjual mengkredit akun dari pemegang kartu kredit dan melakukan penyelesaian terhadap transaksi;
11. Jaringan sistem kartu kredit memfasilitasi penyelesaian tersebut dan mendebet akun dari si pemegang kartu kredit;
12. Bank penerbit membuat catatan atas transaksi tersebut dan mengirimkan tagihan bulanan kepada pemegang kartu kredit;
13. Pemegang kartu kredit memperoleh tagihan tersebut.

B. Debit Card/ATM (Kartu Debet/ATM)

Sama halnya dengan kartu kredit, kartu debit adalah suatu bentuk alat pembayaran yang dapat digunakan pada suatu sistem pembayaran elektronik. Media yang digunakan juga sama, yaitu suatu wadah penyimpan data informasi berupa magnetik atau *microprocessor* dan diaplikasikan penempatannya pada sebuah kartu.

Yang menjadi perbedaan dari kedua APMK tersebut secara garis besar dapat dilihat dari sumber pendanaan. Kartu kredit merupakan produk usaha pembiayaan yaitu segala kegiatan ekonomi yang digunakan si pemilik menggunakan kartu tersebut adalah tanggungan dari si pengelola

sistem yang ada. Sistem seperti ini biasa dikenal sebagai “*buy now pay later*” jadi jelas terlihat bahwa bank meminjamkan dulu dana yang diperlukan kepada nasabah, untuk dibayarkan nanti dengan cara kredit/cicilan atau secara keseluruhan di akhir bulan (*charge card*). Sedangkan pada penggunaan kartu debit, dana yang digunakan langsung diambil/didebet dari rekening pemilik APMK tersebut.

Dalam PBI 11/11/PBI/2009 diatur pengertian tentang kartu ATM dan kartu debit, yaitu kartu ATM adalah APMK yang dapat digunakan untuk melakukan penarikan tunai dan/atau pemindahan dana dimana kewajiban pemegang kartu dipenuhi seketika dengan mengurangi secara langsung simpanan pemegang kartu pada bank atau Lembaga Selain Bank (LSB) yang berwenang untuk menghimpun dana sesuai ketentuan perundang-undangan yang berlaku.⁴¹

Sedangkan Kartu Debet dalam PBI 11/11/2009 diartikan sebagai sebuah APMK yang dapat digunakan untuk melakukan pembayaran atas kewajiban yang timbul dari suatu kegiatan ekonomi, termasuk transaksi pembelanjaan, dimana kewajiban pemegang kartu dipenuhi seketika dengan mengurangi secara langsung simpanan pemegang kartu pada Bank atau Lembaga Selain Bank yang berwenang untuk menghimpun dana sesuai ketentuan perundang-undangan yang berlaku.⁴²

Kartu debit/ATM merupakan produk dari sebuah bank dimana nasabah menabung/menyimpan sejumlah dana, yang dapat digunakan untuk bertransaksi secara elektronik atas rekening tersebut. Pada saat kartu digunakan bertransaksi, akan langsung mengurangi dana yang tersedia pada rekening sejumlah dana yang digunakan tersebut. Berikut skema penggunaan kartu debit dalam transaksi non-tunai sebagai berikut :

⁴¹ Indonesia. Peraturan Bank Indonesia nomor 11/11/PBI/2009 tentang Penyelenggaraan Alat Pembayaran dengan Menggunakan Kartu. Pasal 1 angka 5.

⁴² *Ibid.*, Pasal 1 angka 6.

Skema transaksi kartu debit



Gambar 2.4

Keterangan Gambar 2.4 :

1. Pemilik kartu melakukan transaksi pada toko penjual (*merchant*)
2. Transaksi disahkan dengan permintaan otorisasi kepada bank
3. Dana dengan jumlah transaksi akan ditahan oleh bank
4. Jumlah dana tersebut akan di debet dari akun pemilik kartu

Kartu debit dan kartu ATM adalah sebuah kesatuan, perbedaan penyebutan dikarenakan dari penggunaannya yang multifungsi. Sebuah kartu dapat dikatakan sebagai sebuah kartu ATM jika kartu tersebut digunakan untuk melakukan transaksi pada mesin ATM, khususnya ditujukan untuk mengambil dana. Jika kartu tersebut digunakan untuk melakukan transaksi pembayaran dan pembelanjaan non-tunai dengan menggunakan mesin *Electronic Data Capture* (EDC), maka kartu tersebut dikenal sebagai kartu debit.⁴³

Fungsi dan kegunaan dari kartu debit dan kartu ATM adalah sebagai alat bantu untuk melakukan transaksi dan memperoleh informasi perbankan secara elektronik. Kegunaan tersebut antara lain adalah untuk melakukan penarikan tunai, setoran tunai, transfer dana, pembiayaan, pembayaran, pembelanjaan dan informasi yang tersedia adalah informasi saldo dan kurs. Namun seiring dengan kemajuan teknologi informasi, fitur-fitur yang disediakan pun terus berkembang.

⁴³ Mengetahui Kartu Debet dan ATM. <http://www.docstoc.com/docs/10883840/kartu-debet-atau-atm>. diakses tanggal 30 Desember 2010.

Keuntungan dari penggunaan kartu debit dan ATM ini antara lain adalah kemudahan karena dapat dilakukan langsung tanpa mendatangi bank; keamanan karena tidak perlu membawa uang tunai; fleksibel karena penggunaan kartu ini dapat dilakukan di berbagai jaringan baik itu dimiliki bank sendiri, lokal atau bahkan internasional; dan dapat digunakan ketika waktu libur bank.⁴⁴

Dalam penggunaannya, kartu debit/ATM biasanya akan dikenakan biaya bulanan berupa administrasi yang dibebankan langsung pada saldo rekening si pemilik. Selain itu juga adanya biaya transaksi yang biasanya diberlakukan pada transaksi antar jaringan atau pembayaran seperti kartu kredit, listrik atau telepon dan layanan lainnya yang melakukan kerjasama dengan bank tersebut.

Berbeda dengan penggunaannya di beberapa negara maju, kartu debit di Indonesia belum digunakan secara maksimal. Melihat dari faktor keamanan yang kurang, kartu debit/ATM pada umumnya masih digunakan dengan bentuk penyimpanan data yang berupa magnet. Penggunaan penyimpan data magnet ini sudah berulang kali mengakibatkan kerugian besar baik pada nasabah maupun bank itu sendiri karena kemudahannya dipenetrasi oleh para pelaku kejahatan. Salah satu contoh yang paling marak dilakukan pelaku kejahatan terhadap kartu debit/ATM ini adalah dengan menggunakan alat *skimmer* pada mesin-mesin ATM atau pada toko penjual yang “nakal”.

C. *Stored Value Card* (kartu penyimpan dana)

Stored value card adalah sebuah kartu yang berfungsi untuk menyimpan sebuah dana dengan jumlah yang telah didepositkan. Fungsinya hampir sama dengan kartu debit, namun pada *stored value card* ini tidak menyimpan identitas dari si pengguna (*anonymous*). Dengan

⁴⁴ *Ibid.*

istilah *stored value card* ini berarti dana atau data dari dana tersebut disimpan langsung pada kartu berupa data. Sedangkan pada penggunaan kartu debit atau kredit dana tetap disimpan pada komputer pengelola dan kartu berfungsi hanya sebagai alat otorisasi saja. Penggunaan kartu ini bisa diterapkan dengan berbagai macam bentuk teknologi seperti menggunakan daya magnet atau *microprocessor chip*.

Suatu nilai dana yang tersimpan dalam *stored value card* ini dinamai dengan *e-money* atau uang elektronik. Dalam PBI 11/12/PBI/2009 tentang uang elektronik mengatur mengenai definisi dari uang elektronik yang berbunyi, Uang Elektronik (*Electronic Money*) adalah alat pembayaran yang memenuhi unsur-unsur sebagai berikut:

- a. Diterbitkan atas dasar nilai uang yang disetor terlebih dahulu oleh pemegang kepada penerbit;
- b. Nilai uang disimpan secara elektronik dalam suatu media seperti *server* atau *chip*;
- c. Digunakan sebagai alat pembayaran kepada pedagang yang bukan merupakan penerbit uang elektronik tersebut; dan
- d. Nilai uang elektronik yang disetor oleh pemegang dan dikelola oleh penerbit bukan merupakan simpanan sebagaimana dimaksud dalam undang-undang yang mengatur mengenai perbankan.

TABEL 2.3 PERBANDINGAN ALAT PEMBAYARAN ELEKTRONIK

	Kartu Kredit	Kartu Debet/ATM	Uang Elektronik
Letak Dana	Pembiayaan oleh Bank penerbit	Deposit/tabungan pada Bank penerbit	Prabayar & Tersimpan pada media pembayaran
Keterlibatan Bank	Pembayaran dengan menggunakan rekening Kartu Kredit	Pembayaran dilakukan dengan rekening yang terdapat pada bank	Pembayaran dengan menggunakan rekening yang ada pada kartu
Informasi Pemilik	Otorisasi Penjual dan Bank	Menggunakan identitas pemilik rekening	Tanpa identitas (<i>anonymous</i>)
Waktu Pembayaran	Dilakukan setelah melakukan transaksi	Pada saat melakukan transaksi	Sebelum melakukan transaksi
Risiko Penyalahgunaan	Sebagian besar ditanggung oleh Bank	Konsumen menanggung sebagian risiko	Konsumen menanggung semua risiko
Limit Pembayaran	Tergantung perjanjian antara nasabah dan bank	Tergantung dari jumlah saldo pada rekening pengguna	Tergantung dari deposit yang ada pada kartu tersebut.
<i>Micropayment</i>	Tidak cocok karena biaya yang besar	Biaya kecil, cocok untuk <i>micropayment</i>	Hanya biaya pembuatan kartu, paling cocok
Tingkat Popularitas	Paling populer karena dapat digunakan secara internasional	Hanya lokal dan nasional	Cara pembayaran elektronik paling baru

2.1.4 Teknologi Alat Pembayaran Elektronik

Secara tidak langsung transaksi elektronik adalah konversi pembayaran konvensional menjadi bentuk data digital dengan penerapan teknik enkripsi. Data-data atau aplikasi tersebut tersimpan dalam beberapa jenis media elektronik yang dapat di lekatkan file-file tersebut. Jika kita melihat pada jenis media yang biasa dipergunakan dalam transaksi elektronik berdasarkan teknologi yang digunakan, maka media tersebut terbagi menjadi beberapa jenis, yaitu :⁴⁵

A. Kartu Magnetik (*Magnetic Card*)

Kartu magnetik adalah kartu plastik kecil yang memiliki pita termagnetasi di permukaannya. Kartu magnetik biasanya memiliki pita magnetik yang mengandung 2 atau 3 jalur informasi. Jenis informasi yang terdapat dalam kartu magnetik biasanya ada tiga macam, yaitu *offline stripe*, *online stripe*. (1) *Online stripe* adalah jenis penyimpanan informasi yang berisi informasi dari si pengguna, biasa digunakan dalam transaksi untuk mengakses informasi-informasi terhadap si pengguna kepada komputer pusat; (2) *offline stripe* biasa digunakan untuk menyimpan suatu informasi yang dapat langsung di tafsirkan oleh alat pembaca kartu tersebut. Contohnya : kartu telpon yang menyimpan informasi tentang saldo pulsa, dan begitu digunakan alat pembaca kartu mengirimkan informasi untuk mengurasi saldo yang terdapat pada kartu tersebut.

Penggunaan kartu magnetik ini adalah bentuk yang paling umum ditemukan pada alat pembayaran menggunakan kartu seperti kartu kredit dan kartu debit. Namun karena faktor keamanan dimana teknologi ini mengalami beberapa kali serangan secara fisik, maka penggunaan teknologi *magnetic stripe* sebagai media penyimpan data di kartu pembayaran mulai ditinggalkan untuk beralih pada teknologi *smartcard* (*microprocessor chip*).

⁴⁵ Adi Nugroho. E-commerce : Memahami Perdagangan Modern Di Dunia Maya. Informatika, Bandung. Hlm 79-94.

B. Cek Elektronik (*e-check*)

Cek dalam bentuk konvensional pada dasarnya merupakan pesan pada bank milik konsumen untuk mentransfer dana dari rekening milik konsumen ke rekening seseorang yang lain. Sama halnya dengan cek konvensional tersebut, cek elektronik pun mempunyai fitur yang sama. Cek elektronik sebenarnya juga berupa pesan yang telah tersandi untuk mengirimkan pesan kepada bank untuk mengirimkan dana.

Cek elektronik dapat dibuktikan lebih unggul dari cek kertas dalam satu aspek yang signifikan. Sebagai pengirim, kita dapat melindungi diri kita sendiri dari kecurangan-kecurangan yang mungkin muncul dari penyingkapan nomor rekening oleh orang yang tidak berhak. Dengan protokol SET (*Secure Electronic Transaction*), sertifikat-sertifikat elektronik dapat digunakan untuk melakukan pengujian otentifikasi terhadap pembayar, bank pembayar, dan rekening bank.⁴⁶

Dalam pembayaran dengan cek elektronik, pertama-tama konsumen harus membuka sebuah akun bank di *internet*. Untuk melakukan transaksi si pemilik cek elektronik akan mengirimkan cek tersebut sebagai pembayaran. Melalui prosesnya cek ini akan di validasi oleh bank, setelah itu bank akan mengirimkan pembayaran yang tertera pada cek tersebut dari si pembayar kepada penerima pembayaran. Tentu saja semua ini dilakukan secara elektronik.

C. Uang Elektronik (*e-money*)

Digital cash merupakan versi elektronik dari uang tunai, biasa disebut dengan nama *e-cash*, *digital currency* atau *electric money*. Penggunaan uang elektronik ini adalah metode yang paling cocok digunakan untuk pembayaran recehan (*micropayment*). Uang

Penggunaan dari uang elektronik adalah dengan cara pendebitan secara langsung saldo yang kita miliki dengan cara pemberian kode

⁴⁶ Adi Nugroho. *Op. Cit.*, Hlm 85.

otorisasi (sering disebut dengan nama *token*). Bank dapat melakukan validasi masing-masing *token* dengan penanda digital (*digital signature*) sebelum mentransmisikannya kembali ke komputer kita. Saat kita mau membelanjakan sejumlah *token* ke penjual, yang kemudian akan melakukan verifikasi ke bank dan menarik dananya. *Token* ini hanya dapat dibelanjakan sekali dengan sistem pengamanan dari bank untuk mencatat nomor seri setiap *token*, maka *token* tidak akan dapat digunakan secara berulang.

Variasi terhadap implementasi sistem uang elektronik ini telah dikembangkan oleh beberapa institusi keuangan, misalnya pembelian *token* melalui transfer antar pulsa telepon secara prabayar, sehingga calon konsumen tidak harus memiliki suatu deposit/simpanan pada bank atau lembaga penerbit uang elektronik tersebut. Uang elektronik ini juga dapat dibelanjakan di toko-toko virtual mana saja yang ada di *internet* yang menerima cara pembayaran tersebut. Variasi lain dari pembelian uang elektronik tersebut adalah dengan cara dengan membelinya menggunakan jasa pada kartu kredit atau kartu debit di sebuah lembaga keuangan tertentu.

D. Kartu Pintar (*Smart/Chip/Integrated Circuit Card*)

Kartu pintar memiliki bentuk yang sama dengan kartu magnetik, namun perbedaan ada pada *microprocessor* (mikroprosesor) dan tempat penyimpanan (memori) yang di tempatkan pada kartu ini. Secara fisik daya tahan kartu pintar ini relatif lebih kuat dibandingkan dengan kartu magnetik yang cenderung mudah tergores atau rusak akibat terkena daya magnet yang lebih kuat dari benda lain.

Melihat teknologi yang ada pada sebuah *smart card*, maka bentuk asli dari *smart card* ini bukanlah kartu yang digunakan melainkan *chip* atau *Integrated Circuits Card* (ICC) yang terdapat di dalam kartu tersebut. Kartu hanyalah sebagai wadah untuk menaruh *chip* tersebut. *Chip* biasa di digunakan dalam dua bentuk, yaitu sebagai media penyimpan saja, atau

sebagai sebuah mikroprosesor yang berfungsi untuk menjalankan suatu sistem dalam penggunaan kartu tersebut.

Sesuai dengan ketentuan Surat Edaran BI nomor 11/10/DASP tentang Pelaksanaan Penyelenggaraan Kegiatan Alat Pembayaran dengan Menggunakan Kartu dikatakan pada bagian VII C nomor 2 huruf a bahwa Peningkatan Keamanan perlu dilakukan dengan menggunakan teknologi *Chip (integrated circuit)* yang mempunyai kemampuan untuk menyimpan dan/atau memproses data, sehingga pada kartu dapat ditambahkan aplikasi untuk kepentingan pengamanan pemrosesan data transaksi.

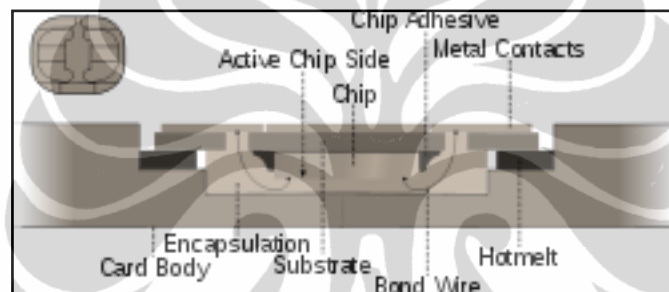
Dalam penerapannya pada alat pembayaran menggunakan kartu, penggunaan *chip* ini seharusnya wajib diimplementasikan pada setiap alat pembayaran elektronik terutama pada kartu debit/ATM, kartu kredit dan kartu prabayar. Dengan penerapan ini maka secara otomatis seluruh sistem pembayaran kartu kredit yang berlaku di Indonesia wajib mengadaptasi penggunaan *chip* tersebut dalam pemrosesan pembayaran.

Penggunaan *chip* tergolong lebih aman karena dengan menggunakan *chip* ini dimungkinkan untuk melakukan identifikasi, otentifikasi, penyimpanan data dan untuk memproses aplikasi. Dibandingkan dengan kartu magnetis yang lebih menggunakan visual kita untuk mengidentifikasi keaslian dari kartu tersebut, biasanya dilihat dari tanda tangan pengguna yang tertera pada kartu dan *hologram* yang diberikan penerbit pada kartu. Sedangkan dengan penggunaan teknologi *chip* sebagai mikroprosesor, peningkatan keamanan sangat memungkinkan. Dengan *chip*, sistem pembayaran dapat diaplikasikan menggunakan *Personal Identification Number (PIN)* dan sistem kriptografis, baik secara simetris maupun asimetris.

Dalam penggunaannya *chip* pada kartu (*smart card*) diterapkan melalui dua metode, yaitu *contactless card* dan *contact card*. *Contactless card* adalah penggunaan *smart card* yang dikombinasikan dengan penerapan teknologi elektromagnetik, yaitu suatu cara pengiriman data

melalui daya magnet. Sehingga dalam penggunaannya *contactless card* ini tidak perlu menyentuh mesin pembacanya. *Contactless card* biasa digunakan pada mesin layanan publik yang memerlukan transaksi dalam waktu cepat seperti pembayaran pada stasiun kereta di Jepang. Jenis kedua adalah *Contact Card*, penggunaan *smart card* ini adalah dengan menggunakan tenaga listrik yang terdapat pada mesin pembaca melalui sebuah lapisan emas yang berfungsi sebagai konduktor untuk mengaktifkan *chip* yang terdapat di bagiannya seperti terlihat pada Gambar di bawah.

Contoh gambar mikroprosesor



Gambar 2.5

Fisik dari kartu *chip* (*smart card*) itu sendiri mengikuti *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (ICE) nomor 7810 mengenai dimensi dan bahan yang digunakan, ISO/ICE 7816 mengenai standar metode dan prosedur yang digunakan dalam *contact card*. ISO/ICE 14443 atau ISO/ICE 15693 untuk standar metode dan prosedur sistem yang digunakan pada *contactless card*.

Dalam penggunaan *chip* ini beberapa hal menjadi pertimbangan terutama karena masalah keamanan. Teknologi yang dimiliki oleh mikroprosesor yang terdapat dalam sistem *smart card* ini adalah :⁴⁷

⁴⁷ http://www.bi.go.id/web/id/FAQ_web/Sistem+Pembayaran/?kat=APMK. Diakses pada tanggal 23 November 2010. Pukul 14.18WIB.

- a. Aplikasi yang dapat mengenkripsi data. Enkripsi tersebut dapat melindungi data nasabah pada saat kartu dimasukkan (di *dip*) ke dalam mesin EDC sehingga data tersebut sulit diduplikasikan.
- b. Adanya tanda tangan digital yang unik yang ditanam dalam *chip* juga merupakan salah satu bentuk pengamanan.
- c. *Chip* merupakan *microprocessor* yang juga berfungsi sebagai mini computer dapat memproses berbagai aplikasi dan dapat menyimpan lebih banyak informasi.

Dengan pengamanan yang berlapis-lapis, penggunaan teknologi *chip* diharapkan dapat mengurangi risiko terjadinya pemalsuan kartu kredit dan pencurian identitas pada kartu yang kian marak terjadi saat ini sehingga pemegang kartu dapat bertransaksi dengan lebih aman dan nyaman.

2.2 Tinjauan Umum Sistem Transaksi Elektronik

2.2.1 Perdagangan Secara Elektronik (*E-commerce*)

Sebelum kita melihat apa yang dimaksud dengan transaksi elektronik ada lebih baiknya jika meninjau terlebih dahulu apa yang dimaksud dengan *E-commerce* (*electronic commerce*) dan hubungannya dengan transaksi elektronik. Saat awal ditemukannya jaringan komputer, kebanyakan perusahaan bisnis skala besar di seluruh dunia, terutama di Amerika Serikat, menggunakan suatu bagian tertentu dari perdagangan elektronik (*electronic commerce*) untuk mengendalikan transaksi antarbisnis. EDI (*Electronic Data Interchange*), yang memungkinkan pertukaran dokumen antar bagian dalam suatu perusahaan dengan bentuk yang terstandarisasi di jaringan pribadi, telah dimulai pada sekitar tahun 1960-an di Amerika Serikat. Kemudian, aplikasi-aplikasi perbankan berskala besar telah lama menggunakan jaringan mandiri (*dedicated network*) untuk metode-metode pentransferan dana dengan menggunakan sistem EFT (*Electronic Fund Transfer*), yang merupakan

metode pentransferan dana secara elektronik, yang dirancang untuk mengoptimalkan pembayaran secara elektronik.⁴⁸

E-commerce mengalami perkembangan pesat sejak tahun 1990, yang pada akhirnya telah membawa perkembangan pada dunia bisnis. Untuk menyeimbangi perkembangan tersebut para pelaku bisnis mempunyai fokus baru dalam keamanan informasi dan keabsahan *e-commerce* itu sendiri dari sudut pandang implikasi hukum. Berikut beberapa faktor yang mendukung perkembangan tersebut.⁴⁹

- a. Perkembangan infrastruktur komunikasi : perkembangan terus terjadi dalam infrastruktur komunikasi mulai dari yang bersifat tertutup seperti LAN (*Local Area Network*) lalu *point to point* terhadap beberapa pelaku bisnis besar di lain tempat, hingga sekarang berkembang menjadi komunikasi terbuka, tidak terawasi, tidak terbatas, tanpa kebijakan dan peraturan yang mengatur secara universal seperti Internet (*interconnected Network*.)
- b. Ledakan terhadap kegiatan perdagangan global : Bisnis saat ini sangat memerlukan pasar yang luas secara global dan tidak terbatas. seiring dengan itu perdagangan secara global ini dimana para pelaku bisa berada di belahan dunia yang berbeda memerlukan sebuah keamanan atau jaminan. Dengan memberlakukan dan menyediakan metode transaksi yang baik dan benar dari semua pihak, maka pembuktian dari transaksi tersebut pun dapat diterapkan dengan baik. Pemberlakuan kebijakan seperti ini sangat baik dalam menciptakan suasana kondusif pada kegiatan *e-commerce*.
- c. Perdagangan Waktu Nyata (*Real Time Trading*) : fitur ini sekarang menjadi sebuah keharusan dalam melakukan transaksi elektronik dimana pentingnya waktu dalam melakukan pembayaran menjadi hal yang vital dalam melakukan bisnis.

⁴⁸ Adi Nugroho. *Op. Cit.*, Hlm. 1

⁴⁹ Warwick Ford dan Michael S. Baum. *Op. Cit.*, Hlm 7-9

- d. Meningkatnya Perhatian terhadap Risiko-risiko: Risiko-risiko yang dapat terjadi dalam perdagangan elektronik menjadi perhatian khusus dari berbagai pihak.
- e. Tersedianya Teknologi Keamanan : Teknologi Keamanan menjadi bagian yang sangat melekat dalam transaksi itu sendiri, dimana hampir setiap *operating sistem* komersil menyertakan teknologi keamanan mereka sendiri. Terutama dalam hal pembayaran digital, teknologi keamanan adalah syarat utamanya.
- f. Bidang keamanan menjadi sebuah aset : pentingnya segi keamanan dalam melaksanakan kegiatan *e-commerce* ini maka menjadikan segi keamanan itu sebuah hal yang penting dalam melaksanakan usaha. Keamanan dapat mengokohkan alur informasi, desain produk, struktur biaya, jaminan hukum dan organisasi bisnis. Sehingga dapat dianggap keamanan informasi adalah kekuatan (*power*).
- g. Politik : keamanan informasi dalam bidang politik terutama dalam hal keamanan negara atau isu-isu politik.
- h. Pendekatan dari sektor hukum : keamanan terhadap informasi kian menjadi sebuah isu yang harus dilindungi secara hukum dan diakui sebagai bagian dari hukum perdagangan elektronik.

Tabel 2.4 penjualan e-commerce 2006-2011 di Asia Pasific

Countries	2006	2007	2008	2009	2010	2011
Australia	9.5	13.6	20.4	26.4	28.7	31.1
China**	2.4	3.8	6.4	11.1	16.9	24.1
India	0.8	1.2	1.9	2.8	4.1	5.6
Japan	36.8	43.7	56.6	69.9	80.0	90.0
South Korea	9.6	10.9	12.4	14.0	15.9	17.9
Asia-Pacific	59.1	73.3	97.7	124.1	145.5	168.7

Note: Converted at average annual exchange rates (projected for future year): Total B2C sales include all purchase made on a retail website, regardless of device used to complete the transaction;
*Includes online travel, event tickets and digital download sales; **excludes Hong Kong
Source: eMarketer, January 2008

50

Perdagangan elektronik atau apa yang lebih dikenal dengan istilah *e-commerce* adalah suatu kegiatan perdagangan dengan menggunakan sarana dan sistem elektronik. Beberapa pendapat ahli seperti Michael Chissick menerangkan pengertian umum tentang *e-commerce* dalam bukunya yang berjudul *Electronic Commerce : Law and Practice* yang dimaksud dengan *e-commerce*⁵¹ adalah “a broad term describing business activities with associated technical data that are conducted electronically.”

Sedangkan menurut Ford Warwick dan Michael S. Baum dalam bukunya *Secure Electronic Commerce : Building the Infrastructure for Digital Signatures and Encryption*, *e-commerce* adalah :

*“Electronic commerce is an umbrella term that describes automated business-related transactions, spanning the purchase of pencils via an electronic mail message to an office supplies store, a shopping trip to an electronic mall on the world wide web, the electronic filling of tax returns or other government-oriented information, and high-dollar industrial inventory control transactions.”*⁵²

⁵⁰ Singh Sumanjeet. *Emergence of Payment Systems In The Age Of Electronic Commerce : The State Of Art*. *Global Journal of International Business Research*. Vol 2. 2009. Hlm 2.

⁵¹ Michael Chissick. *Electronic Commerce Law and Practice*. third edition. Sweet & Maxwell. London. 2002. Hlm xiv.

⁵² Warwick Ford dan Michael S. Baum. *Op. Cit.*, Hlm. 1.

Dan pemahaman umum tentang *e-commerce* dari beberapa rujukan seperti :⁵³

The Challenge of the information Highway: Final report of the information Highway Advisory Council. (September 1995).

“Consumer and Business transactions conducted over a network, using computers and telecommunications.”

The protection of personal information: Building Canada’s information Economy and Society, Industry Canada, task force on Electronic Commerce, January 1998.

“Electronic Commerce, which is at the heart of the information economy, is the conduct of commercial activities and transactions by means of computer-based information and communications technologies. It generally involves the processing and transmission of digitized information. Examples of electronic commerce range from the exchange of vast amount of financial assets between financial institutions, to electronic data interchange between wholeseller and retailers, to telephone banking, and to the purchase of products and services on the internet.”

Masalah *e-commerce* ini juga diatur dalam beberapa konvensi internasional karena sangat erat sekali hubungannya dengan perdagangan internasional atau antar negara. Salah satunya pada departemen Perserikatan Bangsa-Bangsa yang khusus membahas tentang perdagangan bernama *United Nation Comission on International Trade Law (UNCITRAL)*. UNCITRAL telah melahirkan contoh peraturan (*Model Laws on Electronic Commerce*) yang ditujukan sebagai acuan Negara-Negara di seluruh dunia terhadap bidang perdagangan antar batas Negara. Menurut UNCITRAL *model Laws on electronic commerce article 5* apa yang dimaksud dengan *e-commerce* adalah:

“electronic commerce can be defined as commercial activities conducted through an exchange of information generated, stored, or communicated

⁵³ Barry B. Sookman. *Computer, Internet and Electronic Commerce Terms : Judicial, Legislative and Technical Definitions*. Thomson Canada Limited. 2001.

by electronical, optical or analogies means, including EDI, E-mail, and so forth."⁵⁴

Dengan banyaknya pendapat beberapa ahli yang mengemukakan apa itu *e-commerce* membuat arti sebenarnya dari *e-commerce* semakin luas. Untuk dapat melihat apa sebenarnya kegiatan yang dilakukan dalam *e-commerce* kita perlu melihat media yang digunakan dalam perdagangan elektronik (*e-commerce*) ini :⁵⁵

1. Perdagangan melalui *internet (internet commerce)*
2. Perdagangan menggunakan fasilitas web (*web commerce*)
3. Perdagangan dengan sistem pertukaran data terstruktur secara elektronik (*Electronic Data Interchange*)

Selain itu kita juga dapat melihat komponen hubungan hukum antara para pihak dalam *e-commerce* ini. Dalam kegiatan *e-commerce* pasti terjadi kegiatan hukum perjanjian sebagaimana mestinya kegiatan jual beli konvensional. Dengan adanya kegiatan dalam *e-commerce* tersebut, maka terjadi pula beberapa hubungan hukum yaitu :⁵⁶

1. *Business to business*

Transaksi *business to business* atau yang sering disebut sebagai *b to b* adalah transaksi antar perusahaan (baik pembeli maupun penjual adalah perusahaan). Biasanya di antara mereka telah saling mengetahui satu sama lain dan sudah terjalin hubungan yang cukup lama. Pertukaran informasi hanya berlangsung di antara mereka dan pertukaran informasi itu didasarkan pada kebutuhan dan kepercayaan.

2. *Business to customer*

Business to customer atau yang lebih dikenal dengan nama *b to c* adalah transaksi antara perusahaan dengan konsumen/individu. Contohnya adalah *amazon.com* sebuah situs *e-commerce* yang besar dan terkenal. Pada jenis ini, transaksi disebarluaskan secara

73. ⁵⁴ Lorna Brazell. *Electronic Signatures Law and Regulation*. Bird and Bird. 2004. Hlm

⁵⁵ Edmon Makarim. Op. Cit., Hlm 257-258.

⁵⁶ *Ibid.*, Hlm. 259-260.

umum, dan konsumen yang berinisiatif melakukan transaksi. Produsen harus siap menerima respons dari konsumen tersebut. Biasanya menggunakan sistem *web*.

3. *Customer to customer*

Customer to customer ini adalah transaksi dimana individu saling menjual barang pada satu sama lain.

4. *Customer to business*

Customer to business yaitu transaksi yang memungkinkan individu menjual barang pada perusahaan.

5. *Customer to government*

Customer to government adalah transaksi di mana individu dapat melakukan transaksi dengan pihak pemerintah, seperti membayar pajak.

2.2.2 Definisi Transaksi Elektronik (*Electronic Transaction*)

Menurut ketentuan hukum yang berlaku, pada Pasal 1 angka (2) Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, yang dimaksud dengan transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya. Perbuatan hukum ini dapat terjadi dalam lingkup publik dan privat. Dalam kajian ini penulis akan membahas transaksi elektronik yang terjadi dalam penggunaannya yang diterapkan dengan alat pembayaran kartu. Dengan alat pembayaran kartu sebagai objek hukum pembahasan maka lingkup kajian ini adalah transaksi elektronik dalam ruang privat.

Selanjutnya yang perlu kita lihat adalah masalah transaksi elektronik pada sistem pembayaran dalam *e-commerce*. Transaksi elektronik pada konsepnya adalah sama dengan transaksi secara tradisional/konvensional dimana penjual menampilkan produk, harga dan persyaratan serta peraturan kepada calon pembeli lalu pembeli mempertimbangkan pilihan mereka, bernegosiasi harga dan juga persyaratan serta peraturannya (jika memungkinkan), tempat, pesanan dan juga cara pembayaran. Setelah

kesepakatan terjadi lalu penjual akan mengantar produk yang telah dibeli tersebut kepada pembeli. Urutan kejadian dan mekanisme seperti adalah apa yang biasa terjadi dan merupakan dasar serta fundamental cara bertransaksi baik menggunakan sistem elektronik maupun tradisional.⁵⁷

Transaksi elektronik perbankan merupakan produk jasa yang diberikan oleh pihak bank kepada nasabahnya untuk melakukan pembayaran pada *merchant* (penjual) yang telah ditunjuk sebelumnya oleh pihak bank. Baik pihak bank maupun penjual yang bersedia menawarkan sistem pembayaran elektronik pasti telah memikirkan pentingnya efisiensi dan kecepatan pengguna dalam melakukan pembayaran. Dengan menggunakan metode ini untuk melakukan pembayaran, tentu saja waktu yang digunakan relatif jauh lebih cepat dan efisien.

Metode-metode yang dapat digunakan pada untuk melakukan pembayaran menggunakan kartu antara lain :⁵⁸

a. Transaksi model ATM

Transaksi ini hanya melibatkan institusi finansial dan pemegang *account* yang akan melakukan pengambilan atau menyetorkan uangnya. Untuk melakukan transaksi model ini diperlukan sebuah mesin *Automated Teller Machine* atau di Indonesia lebih dikenal dengan Anjungan Tunai Mandiri. Penggunaan metode ini mempunyai kelebihan atas waktu yang digunakan, dimana transaksi dapat dilakukan secara instan dan juga tidak mengikuti waktu kerja bank, sehingga dapat dilakukan setiap saat.

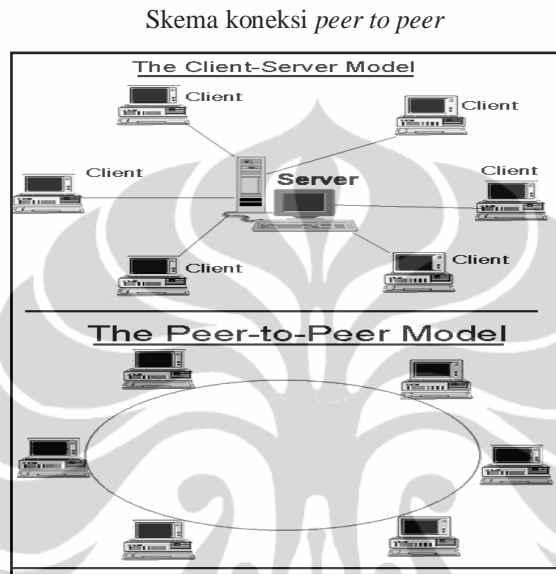
b. Pembayaran dua pihak tanpa perantara

Transaksi dilakukan langsung antara dua pihak tanpa perantara menggunakan sistem elektronik yang disetujui. Cara melakukan transaksi model ini adalah salah satu yang telah disetujui oleh pemerintah. Tertulis pada pasal 21 UU ITE yang mengatakan bahwa transaksi elektronik dapat dilakukan pengirim atau

⁵⁷ Warwick Ford dan Michael S. Baum. *Op. Cit.*, hlm 36.

⁵⁸ Edmon Makarim. *Op. Cit.*, Hlm. 262-263.

penerima sendiri, dengan dikuasakan atau melalui agen elektronik.⁵⁹ Teknologi tersebut dinamakan sebagai metode *peer to peer*, yaitu sebuah metode pembayaran yang memungkinkan setiap individual untuk melakukan hubungan secara langsung seperti dijelaskan pada contoh *Gambar* di bawah.



Gambar 2.6

- c. **Pembayaran dengan perantara pihak ketiga (Agen Elektronik)**
- Pembayaran jenis ini adalah model transaksi yang paling sering digunakan, terutama pada dunia *internet* dengan model penjualan *web based*. Pada prakteknya penggunaan agen elektronik ini dalam transaksi pembayaran elektronik adalah sebagai pihak penengah atau perantara. Ketika seorang pembeli yang menginginkan suatu barang yang dijual pada suatu *web address* dia akan melakukan pembayaran terlebih dahulu kepada agen elektronik, bukan langsung kepada penjual tersebut. Setelah mendapatkan pembayaran agen elektronik akan mengotorisasi kepada penjual bahwa transaksi pembayaran telah dilakukan. Jasa agen elektronik ini dikenal juga dengan nama *payment gateway*.

⁵⁹ Indonesia. UU ITE. Pasal 21

2.3 Teknologi Keamanan Sistem Elektronik

Sistem elektronik dan kegiatan transaksi elektronik sebagai pengaplikasian teknologi informasi haruslah diimbangi dengan keamanan yang didapatkan dari teknologi itu sendiri. Penggunaan teknologi keamanan ini antara lain meliputi teknik kode sandi pengekripsian, otoritas kunci publik, tanda tangan digital dan sistem otentifikasi.

Dalam fundamental pengaplikasian teknologi keamanan, ada 4 dasar pemikiran yang harus dipenuhi, yaitu :⁶⁰

- a. *Confidentiality* (kerahasiaan) : sebuah informasi elektronik harus bersifat tertutup terhadap pihak yang tidak berwenang.
- b. *Integrity* (integritas) : sebuah informasi harus dapat dijamin konsistensinya, pada umumnya sebuah informasi harus terjamin tidak dapat dirubah, ditambahkan, atau dihancurkan.
- c. *Availability* (ketersediaan) : sebuah informasi harus dapat dijamin ketersediaannya kepada pihak yang berhak untuk dapat mengaksesnya.
- d. *Legitimate use* (penggunaan yang sah) : sebuah informasi harus dapat dijamin untuk tidak dapat dipergunakan oleh pihak yang tidak sah atau dengan cara yang tidak sah.

Agar ke empat disiplin seperti apa yang sudah di terangkan di atas dapat berjalan dengan baik, maka di perlukan teknologi-teknologi keamanan atas teknologi informasi yang ada. Teknologi keamanan ini adalah pengamanan yang mencakup keamanan sistem komputer (komunikasi) secara luas, serta keamanan dari dalam komputer itu sendiri. Hal pertama yang harus kita bahas jika menyangkut masalah keamanan dalam teknologi informasi adalah mengenai masalah pengkodean atau pemberian sandi pada suatu data/ionformasi elektronik. Penerapan metode teknologi keamanan ini dinamakan sebagai metode

⁶⁰ Warwick Ford dan Michael S. Baum. *Op. Cit.*, Hlm 94.

Cryptography, electronic Signatures (tanda tangan elektronik) dan *digital certificates* (sertifikat digital).

A. Kriptografis (*Cryptography*)

Cryptography atau *Cryptosystem* merupakan sebuah ilmu atau teknik yang sangat mendasar dalam teknologi keamanan. Proses kriptografis ini merupakan proses dua hal yang dikatakan sebagai transformasi enkripsi dan deskripsi. *Encryption* (Enkripsi) adalah sebuah proses dimana penerapan sebuah data kepada file sehingga mempunyai sebuah arti sebagai suatu pesan, seperti rangkaian kata - kata atau angka. Data ini dikenal dengan nama *plaintext*. Sedangkan untuk *decryption* (dekripsi) adalah proses kebalikan dari enkripsi dimana dalam proses ini terjadi transformasi *plaintext* sebuah data yang tidak dapat di mengerti secara langsung atau biasa disebut sebagai *ciphertext*.

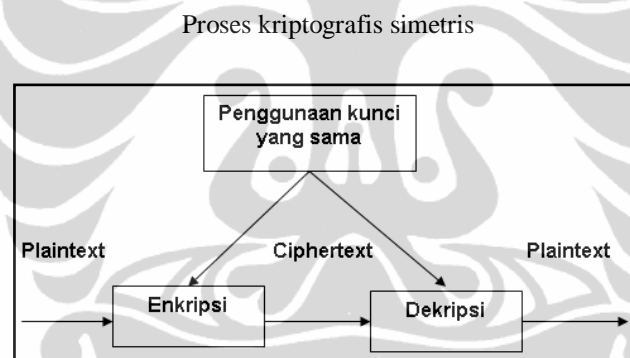
Penggunaan kriptografis ini adalah sebagai cara untuk mengirimkan data secara rahasia. *Plaintext* tidak lain merupakan sebuah data yang tidak terlindungi dan sensitif. Sedangkan *ciphertext* merupakan bentuk aman dari data tersebut yang dapat dikirimkan melalui lingkungan dan media mana saja. Penggunaan yang paling sederhana pada teknik ini adalah pergeseran 3 angka. Metode yang di gunakan adalah menggeser 3 angka dari urutan abjad pada pesan yang dikirim untuk menguak arti yang sebenarnya. Contohnya untuk mengirim sebuah pesan dengan teks INDONESIA maka pengirim harus mengirimkan pesan LQGRQHVL D.

Di dalam penggunaannya pada dunia teknologi teknik kriptografis sejauh ini mempunyai dua jenis sistem, yaitu kriptografis simetris dan kriptografis asimetris. Perbedaan utama dari kedua teknik ini ada pada kunci yang digunakan. Pada kriptografis simetris, teknik ini hanya menggunakan satu kunci rahasia untuk mendriskripsi dan mengenkripsi pesan. Sedangkan teknik kriptografis asimetris menggunakan dua buah kunci rahasia yang yang disebut sebagai kunci publik dan kunci privat. Cara kerja dari kriptografis asimetris ini adalah penggunaan kedua kunci tersebut untuk proses dekripsi

dan enkripsi. Teknik kriptografis asimetris inilah yang menjadi dasar lahirnya tanda tangan elektronik.

a. Kriptografis Simetris

Teknik pertama penggunaan kriptografi dalam dunia teknologi adalah dengan menggunakan teknik simetris. Teknik simetris ini biasa juga disebut dengan teknik *single key* atau *private key* karena dalam pemakaiannya teknik ini hanya memakai satu *key*/kunci. Jadi dalam suatu hubungan antara A ingin mengirimkan pesan kepada B, maka kunci yang digunakan A untuk mengenkripsi pesan akan digunakan kembali oleh B untuk mendekripsi pesan tersebut. Proses mengenkripsi dan mendekripsi ini dapat dilihat pada *Gambar 2.7*. Teknik simetris ini terbagi lagi menjadi dua metode yaitu *block cypher*⁶¹ dan *stream cypher*.⁶²



Gambar 2.7

Teknik simetris ini sudah sangat jarang digunakan, dikarenakan mempunyai beberapa kelemahan, yaitu :

1. Jika secara kebetulan dua atau lebih orang memilih kunci yang sama, yang bersangkutan dapat mencuri dan mendekripsikan pesan orang lain; dan

⁶¹ *Block-cipher* adalah skema algoritma sandi yang akan membagi-bagi teks terang yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang t , dan setiap blok dienkripsi dengan menggunakan kunci yang sama.

⁶² *Stream-cipher* adalah algoritma sandi yang mengenkripsi data persatuan data, seperti *bit*, *byte*, *nibble* atau per lima *bit*

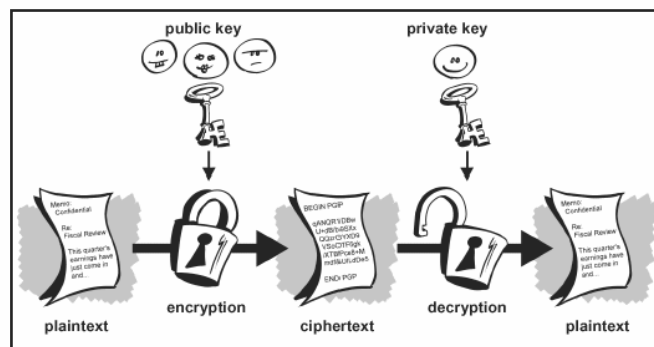
- Masalah otentifikasi juga akan menjadi isu utama karena si penerima belum tentu yakin bahwa pengirim adalah orang yang sesungguhnya. Orang lain yang secara sengaja mengetahui kunci enkripsi pengirim mungkin saja akan mencoba mengirimkan dokumen atas nama orang lain.

b. Kriptografi Asimetris

Kriptografi asimetris ini merupakan perkembangan dari teknik kriptografis simetris. Dalam teknik asimetris proses enkripsi dan dekripsi mempunyai kunci yang berbeda. Sistem kriptografi asimetris ini biasa juga disebut sebagai sistem kriptografi kunci publik karena kunci untuk enkripsi dibuat untuk diketahui oleh umum atau dapat diketahui siapa saja, tapi untuk proses dekripsinya hanya dapat dilakukan oleh yang berwenang yang memiliki kunci rahasia untuk mendekripsinya, kunci ini disebut sebagai *private-key*.

Dapat dianalogikan seperti kotak pos yang hanya dapat dibuka oleh tukang pos yang memiliki kunci tapi setiap orang dapat memasukkan surat ke dalam kotak tersebut. Keuntungan algoritma model ini adalah untuk melakukan korespondensi secara rahasia dengan banyak pihak tidak diperlukan kunci rahasia sebanyak jumlah tersebut seperti pada sistem kriptografi simetris. Penggunaan kunci publik dan kunci privat dalam satu proses dapat terlihat pada Gambar 2.8.

Skema proses kriptografis asimetris (kunci publik)



Gambar 2.8

Dengan adanya sistem ini, kekurangan-kekurangan pada enkripsi simetris dapat teratasi, yaitu :

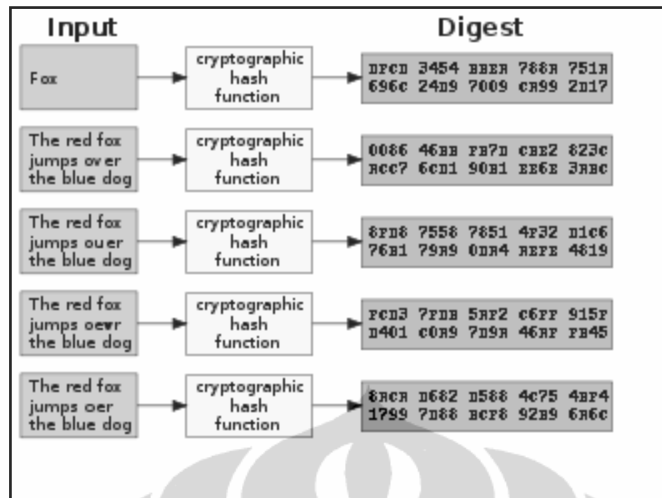
1. Algoritma pemetaan bekerja berdasarkan pasangan kunci sehingga walaupun seseorang memiliki salah satu kunci yang sama, namun jika pasangan kuncinya berbeda, kunci tersebut tidak akan dapat dipergunakan untuk mendekripsikan pesan orang lain; dan
2. Dengan sendirinya problem otentifikasi akan terselesaikan karena yang bersangkutan pasti akan menggunakan kunci yang benar (bukan kunci orang lain) agar dapat dibaca oleh mereka yang memiliki pasangan kuncinya.

B. Fungsi Hash

Fungsi *hash* adalah suatu sistem yang digunakan untuk mengotentifikasi dan menjamin integritas data dari gangguan transmisi (*noise*), dalam hal ini biasa digunakan fungsi *hash* satu arah (*one way hash function*) yang terkadang disebut sidik jari (*finger print*), *hash message integrity* atau *manipulation detection code*.

Contoh masalah, misalkan A yang ingin mengirimkan pesan kepada B. pertama-tama A mendapatkan nilai *hash* dari pesan yang akan dikirimkannya tersebut. Kemudian pesan bersama nilai *hash* tersebut dikirimkan kepada B. ketika B menerima pesan tersebut, dia membuat suatu nilai *hash* yang baru dari pesan yang dikirimkan oleh A. Jika nilai *hash* tersebut sama, maka B dapat yakin bahwa pesan A tersebut tidak mengalami perubahan selama perjalanan.

Skema proses penerapan fungsi hash



Gambar 2.9

Fungsi hash satu arah ini berangkat dari asumsi bahwa hampir tidak ada dua *message digest* yang mempunyai nilai *hash* yang sama, atau bisa dibalang sangat kecil kemungkinannya. Dan asumsi berikutnya adalah sangat sulit atau hampir tidak mungkin untuk mendapatkan *message digest* dari suatu nilai hash.

C. Tanda Tangan Elektronik (*Electronic Signatures*)

Electronic signatures adalah apa yang dikenal sebagai tanda tangan elektronik. Tanda tangan elektronik merupakan sebuah data yang terkait dengan sebuah pesan yang telah tersandikan dan data ini berfungsi untuk memverifikasi identitas pengirimnya, sekaligus menjamin keaslian dari pesan tersebut karena identitas pengirim yang tertera pada pesan tadi.

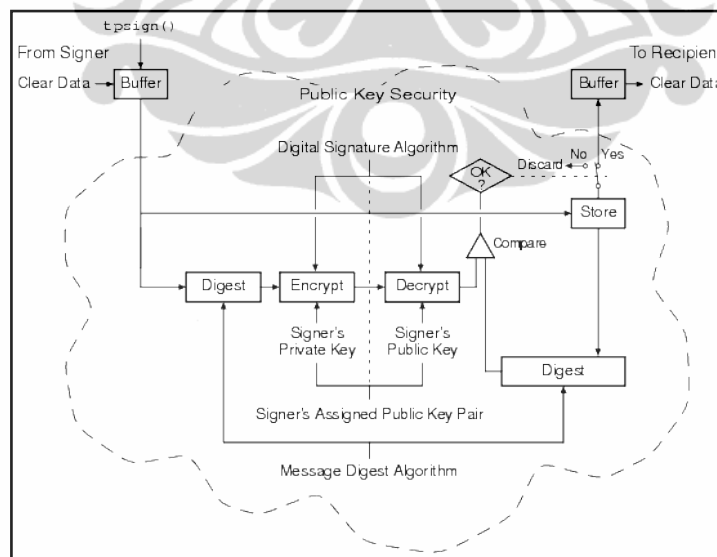
Untuk menandatangani secara digital sebuah pesan, dengan bantuan piranti lunak, pengirim akan membuat pertama-tama sebuah *message digest*⁶³

⁶³ Merupakan “DNA” dari pesan asli. bila terjadi perubahan satu karakter saja maka “DNA” nya akan berubah, dengan kata lain, satu pesan akan mempunyai satu “DNA” unik.

(MD) dari pesan asli dengan menggunakan *hash function*⁶⁴. MD dari setiap pesan aslinya adalah unik, layaknya sebuah sidik jari. Sehingga perubahan sedikit pun pada sebuah *message digest* akan mengakibatkan perubahan “sidik jarinya” pula. Keuntungannya, baik sang pengirim maupun penerima dapat mengetahui keintegritasan pesan tersebut.

Selanjutnya *message digest* tersebut akan ditanda tangani dengan menggunakan kunci privat pengirim, dengan kata lain tanda tangan elektronik adalah *message digest* yang dienkripsi oleh kunci privat Pengirim. Kemudian pesan asli dan tanda tangan elektronik dikirim bersama-sama ke tujuan yang diinginkan. Berkat kunci publik dari Pengirim yang dikomunikasikan terlebih dahulu ke penerima pesan, Penerima dapat mendekripsi tanda tangan elektronik tersebut, katakanlah hasilnya D1, selanjutnya penerima akan membuat *message digest* pada pesan asli yang diterima, katakanlah hasilnya D2. Maka langkah terakhir adalah membandingkan keduanya, yaitu D1 dan D2. Bila keduanya memiliki “sidik jari” yang sama, maka dapat dipastikan bahwa itu pesan asli dan belum pernah dirubah.

Skema penerapan tanda tangan elektronik pada pesan elektronik



Gambar 2.10

⁶⁴ Algoritma yang digunakan antara lain, *Secure Hash Algorithm*-1 (selanjutnya disebut SHA-1) atau *Message Digest* 5 (selanjutnya disebut MD-5).

Di dalam Pasal 1 nomor 12 Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik disebutkan bahwa yang dimaksud dengan Tanda Tangan Elektronik adalah “Tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat **verifikasi atau autentikasi**.”

D. Sertifikat Elektronik (*Electronic Certification*)

Suatu masalah yang sering kali yang terjadi pada transaksi melalui jalur *internet* adalah posisi dimana si pembeli dan si penjual tidak dapat bertemu muka langsung (*distance selling*). Hal tersebut dikarenakan lokasi si penjual dan pembeli yang berada sangat jauh dan mungkin ada di negara yang berbeda. Tentu saja hal ini membawa suatu masalah baru yaitu keraguan calon penjual dan pembeli untuk bertransaksi. Penipuan sangat riskan terjadi apalagi jika kita bertransaksi dengan pihak yang kita tidak kenal sebelumnya.

Sertifikat elektronik membawa solusi untuk masalah ini, fungsinya adalah memberikan informasi mengenai identitas pemilik sertifikat tersebut. Setiap pemilik sertifikat elektronik ini telah di evaluasi dan dijamin keabsahannya oleh sebuah lembaga sertifikasi. Beberapa lembaga sertifikasi yang sudah terpercaya hampir di seluruh belahan dunia adalah Verisign, Mountain View, Thawte. Lembaga sertifikasi ini selanjutnya disebut sebagai *Certification Authority (CA)*.

Salah satu informasi yang didaftarkan dan terdapat dalam sertifikat elektronik adalah kunci publik, sehingga sertifikat elektronik ini juga bisa dibidang sebagai mekanisme pertukaran kunci publik.⁶⁵ Untuk mengatasi masalah keamanan pendistribusian kunci publik, maka kunci publik itu ‘direkatkan’ pada sertifikat elektronik. Sertifikat elektronik selain berisi kunci publik juga berisi informasi lengkap mengenai jati diri pemilik kunci tersebut, sebagaimana layaknya KTP, seperti nomor seri, nama pemilik, kode

⁶⁵ David Kosiur. *Understanding Electronic Commerce*. Washington. Microsoft Press. 1997. Hlm. 75-76.

negara/perusahaan, masa berlaku dan sebagainya. Dengan menggunakan kunci publik dari sertifikat digital, pemeriksa tanda tangan dapat merasa yakin bahwa kunci publik itu memang berkorelasi dengan seseorang yang namanya tercantum dalam sertifikat elektronik itu.

CA tidak hanya menerbitkan sertifikat saja, namun juga memeriksa apakah suatu sertifikat elektronik masih berlaku atau tidak. CA selain memiliki daftar sertifikat elektronik yang telah diterbitkannya, juga memiliki apa yang disebut dengan daftar sertifikat yang dibatalkan (*certification revocation list*). Daftar sertifikat terbatalan (DSB) itu berisi sertifikat-sertifikat apa saja yang sudah tidak lagi berlaku karena tercuri, hilang, atau ada perubahan identitas (misalnya perubahan alamat surat elektronik dan alamat rumah). Setiap kali ada pihak yang ingin memeriksa sertifikat digital, ia dapat menghubungi otoritas sertifikat secara *online* untuk memastikan bahwa sertifikat elektronik yang diterimanya masih berlaku. Jika semakin banyak sertifikat yang dibatalkan, tentu otoritas sertifikat akan terbebani dan akan memperlambat proses pemeriksaan sertifikat elektronik yang ingin diuji keabsahannya. Oleh karena itu, dalam sertifikat elektronik terdapat tanggal kadaluarsa. Sertifikat elektronik yang sudah melampaui tanggal kadaluarsa akan dihapus dari dalam DSB, karena tidak ada pihak manapun yang akan mau memeriksa sertifikat elektronik yang sudah kadaluarsa.⁶⁶

Untuk melihat apakah sebuah website yang menyediakan transaksi elektronik sudah memiliki sertifikat digital yang sah atau belum bisa dilihat dari menu browser yang kita gunakan. Sebagai contohnya ketika kita menggunakan *internet explorer*⁶⁷ maka kita dapat melihatnya dengan masuk ke menu file (alt+f) lalu klik *properties*. Kemudian klik pada dialog *box certificates*. Nanti akan muncul sertifikat digital apakah yang digunakan pada situs tersebut.

⁶⁶ *Ibid.*, Hlm. 77.

⁶⁷ Sebuah penjelajah web/*internet* yang merupakan buatan Microsoft dan diberikan gratis kepada publik untuk kepentingan non komersial.

E. Amplop Digital (*Digital Envelope*)

Amplop digital mempunyai konsep yang sama seperti amplop dalam bentuk konvensional, yaitu sebagai penyimpan pesan agar dapat dibaca hanya oleh penerima yang sah. Secara digital, proses pengamplopan ini adalah data yang mau dikirimkan dienkripsi menggunakan kunci kriptografis yang dibuat secara acak. Kemudian kunci ini juga dienkripsi menggunakan kunci publik si penerima. Data yang mau dikirimkan tersebut bisa dikatakan teramplop karena hanya bisa di baca oleh si penerima, yang bisa membuka amploponya hanya kunci privat si penerima dan ini hanya dimiliki oleh si penerima.

Data yang mau dikirimkan perlu dienkripsi dengan kunci simetris terlebih dahulu, tidak langsung dienkripsi dengan kunci publik si penerima, hal ini untuk menghemat waktu komputasi, waktu komputasi untuk enkripsi dengan kunci publik/privat jauh lebih lama daripada enkripsi dengan kunci simetris, apalagi jika ukuran datanya besar. Pada protokol SET, amplop digital berfungsi untuk menjamin kerahasiaan pesan.⁶⁸

2.4 Prosedur Keamanan dalam Transaksi Elektronik

Transaksi melalui *internet* merupakan transaksi dengan media yang sifatnya terbuka atau publik. Oleh sebab itu transaksi seperti ini dapat terbilang rawan dari intervensi pihak yang tidak diinginkan. Untuk itulah para ahli menciptakan penangkal-penangkal seperti teknik *cryptosystem* dan *digital signatures*, namun hal tersebut tidak akan berfungsi jika tidak diaplikasikan pada sebuah metode atau prosedur keamanan.

Ada banyak metode pengamanan dalam melakukan transaksi elektronik namun penulis hanya akan membahas beberapa yang dianggap paling mutakhir dan sering digunakan sehari-hari. Berikut adalah beberapa metode pengamanan yang populer digunakan dalam transaksi *online*, antara lain:

⁶⁸ I. Arif Priharsanta. Implementasi *Prototipe* Proses Otorisasi Kartu Pembayaran Anatar *Merchant* dan *Payment Gateway* pada *Protocol Secure Electronic Transaction*. Skripsi. Depok. Universitas Indonesia. 1999. Hlm. 10-11.

2.4.1 Prosedur *Secure Sockets Layer* (SSL)

Secure Socket Layer atau yang lebih dikenal dengan nama SSL adalah instrumen yang sering dipakai dalam *website*. Dalam penggunaan *internet* ada yang dinamakan sebagai standar komunikasi, jenisnya ada seperti *Transmission Control Protocol/Internet Protocol* (TCP/IP) dan *Hypertext Transfer Protocol* (HTTP). Keduanya merupakan jalur komunikasi terbuka yang tidak aman, dengan perkembangannya pemanfaatan teknologi kriptografi dan *Netsscape Communication Corporation* mengusulkan sistem pengamanan dengan menggunakan SSL.

Kegunaan prosedur SSL ini adalah untuk mengamankan komunikasi *web* yang menggunakan protokol HTTP antara *browser* dengan *web server*. HTTP yang telah aman ini disebut juga HTTPS (*HTTP over SSL*). Pada *website* yang telah menjalankan SSL, alamat pada *browser* tidak menampilkan `http://.....`, melainkan `https://.....` dan terlihat tanda “gembok” pada pojok kanan bawah.

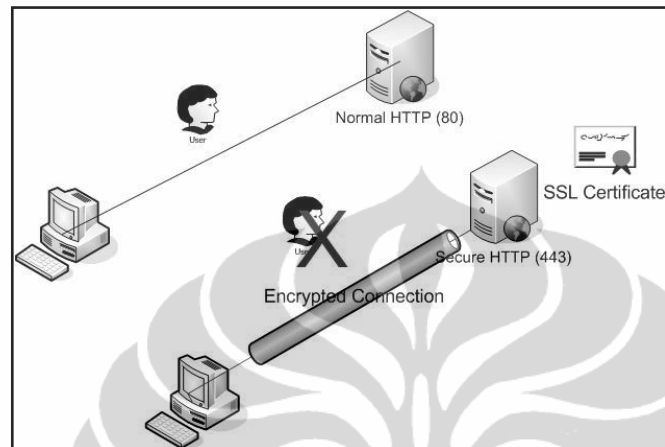
SSL melindungi informasi pribadi dalam kontak antara konsumen dengan pedagang. Keamanan data yang dikirim melalui jaringan juga terjamin. Konsumen dalam melakukan transaksi harus memastikan bahwa data-data tersebut sudah dalam bentuk terenkripsi dengan baik. Dengan pemanfaatan SSL, aplikasi *internet* dapat melakukan komunikasi yang aman melalui fasilitas yang disediakan oleh SSL seperti :

1. Kerahasiaan pesan (*avoid eavesdropping*), sehingga tidak bisa dibaca oleh pihak yang tidak diinginkan;
2. Keutuhan pesan (*avoid message forgery*), sehingga tidak bisa diubah-ubah dalam proses transaksi berjalan;
3. Keabsahan (*avoid tampering*), sehingga meyakinkan pihak-pihak yang berkomunikasi mengenai keabsahan pesan dan keabsahan jati diri lawan bicaranya.

Pada dasarnya apa yang dilakukan oleh protokol SSL ini adalah membuat sebuah pipa antara *browser* pengguna dengan *website* penjual,

sehingga penyerang tidak dapat menyadap atau melakukan intervensi terhadap proses transaksi. Contoh penerapan SSL pada komunikasi HTTP terlihat pada Gambar 2.11.

Penerapan SSL pada proses komunikasi di internet



Gambar 2.11

Protokol SSL ini bukan tanpa kelemahan, tanpa dilengkapi dengan sertifikat elektronik, maka serangan terhadap informasi dalam transaksi masih ada. Dalam hal tersebut seorang penyerang dapat mempertukarkan kunci publik pengirim dengan kunci publik penyerang, serta menukarkan kunci publik penerima dan kunci publik penyerang. Dengan melakukan hal tersebut maka penyerang dapat mengakses informasi tersebut seluruhnya.

Untuk mencegah penyerangan dari pihak ketiga maka biasanya *website* dari penjual telah dilengkapi dengan sertifikat elektronik yang fungsinya untuk membungkus kunci publik *website* mereka dalam sebuah amplop digital. Cara ini dianggap lebih aman karena dapat mencegah penyerangan tersebut dikarenakan setelah pada *browser* pengguna yang dapat memeriksa secara otomatis sertifikat elektronik tersebut dari *website* si penjual.

2.4.2 Prosedur *Secure Electronic Transaction* (SET)

Metode SET ini adalah metode yang pertama kali dikembangkan oleh Visa dan Mastercard dalam melakukan transaksi pembayaran menggunakan kartu. SET menggunakan dua sertifikat elektronik untuk membuktikan bahwa

konsumen dan pedagang memiliki hak untuk menggunakan dan menerima kartu. SET sendiri bukanlah merupakan suatu program, melainkan sebuah prosedur.

Penggunaan SET ini oleh pengembangnya dirasakan perlu dikarenakan ada beberapa faktor dalam transaksi yang harus di tangani dalam pembayaran menggunakan transaksi elektronik, antara lain : ⁶⁹

1. Keamanan pengiriman informasi pemesanan dan pembayaran;
2. Integritas data dalam setiap transaksi;
3. Otentifikasi bahwa seorang konsumen adalah seorang pemegang kartu (*cardholder*) yang sah pada suatu perusahaan penyelenggara pembayaran (*prinsipal*) tertentu (cth: Visa dan Mastercard);
4. Otentikasi bahwa seorang pedagang memang benar-benar bisa menerima jenis pembayaran yang diajukan;
5. Menyediakan suatu sistem pembayaran yang tidak terikat kepada suatu protokol perangkat keras atau perangkat lunak tertentu, dengan kata lain dapat bekerja dengan berbagai macam perangkat lunak dan berbagai penyedia jasa;

Transaksi pada protokol SET ini juga melibatkan CA (*Certification Authority*) sebagai pihak ke tiga. CA sebagai pengelola sertifikat elektronik akan memberikan informasi yang dibutuhkan oleh kedua belah pihak atas keaslian identitas. Sebagai contoh, CA akan mengecek ke *issuer*, apakah nama, nomor kartu kredit, *expiry date*, dan alamat pemegang kartu yang memohon dibuatkan sertifikat digital itu sah (*authentic*). CA kemudian membuat sertifikat elektronik berisi informasi jati diri dan kunci publik pemegang kartu, berikut informasi kartu kredit yang "disembunyikan". Dengan memiliki sertifikat elektronik, seolah-olah mereka memiliki KTP digital yang tidak bisa disalahgunakan.

Didalam menjalankan prosedur SET ini, ada 6 pihak yang terlibat di dalamnya, yaitu : ⁷⁰

⁶⁹ <http://setco.org> . diakses pada tanggal 17 November 2010. Pukul 11:46WIB.

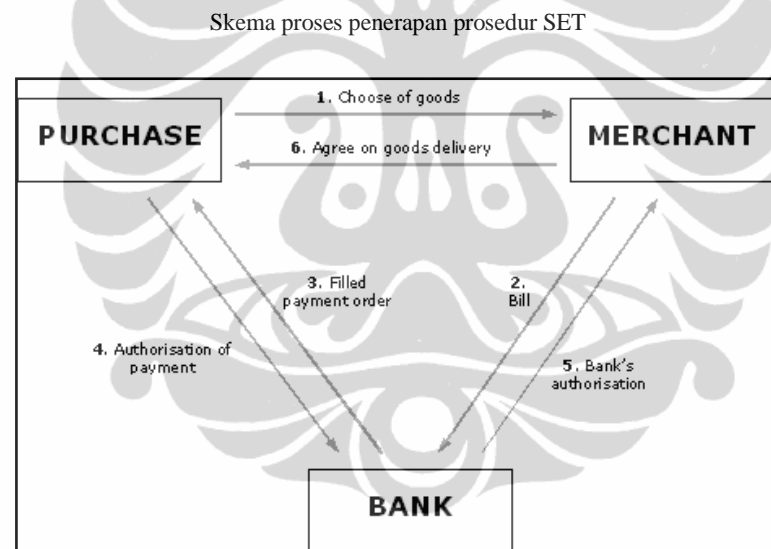
Pihak Utama

1. *Issuer* (bank atau lembaga selain bank yang menerbitkan kartu pembayaran);
2. *Cardholder* (pemilik kartu pembayaran);
3. *Merchant* (penjual barang, jasa atau informasi yang menerima pembayaran secara elektronik);
4. *Acquirer* (pengelola jaringan).

Pihak Pendukung

5. *Payment gateway* (agen elektronik);
6. *Certification authorities* (lembaga sertifikasi).

Skema prosedur dalam SET dijelaskan pada Gambar 2.12 di bawah.



Gambar 2.12

⁷⁰ Ford, Warwick dan Michael S. Baum. *Op. Cit.*, Hlm 174.

Urutan prosedur yang dilakukan dalam transaksi SET seperti gambar di atas adalah : ⁷¹

1. Pembeli harus memiliki alat pembayaran kartu dari lembaga penerbit yang sudah mengadakan kerjasama dengan pengelola jaringan;
2. Pembeli menerima sertifikat elektronik penjual (*merchant*) yang telah di tanda tangani oleh *issuer* dan/atau *acquirer*;
3. Pembeli melakukan instruksi pemesanan;
4. Penjual mengirimkan duplikat sertifikat elektronik miliknya kepada *acquirer* agar *acquirer* dapat memvalidasi sah atau tidaknya toko si Penjual kepada *issuer*;
5. Setelah otorisasi disetujui, maka *acquirer* menginstruksikan pemesanan dan pembayaran di kirim kepada *merchant*;
6. Penjual mengkonfirmasi pemesanan Pembeli;
7. Penjual memberikan barang, jasa atau informasi kepada Pembeli;
8. Penjual meminta pembayaran dari Penerbit/Pengelola.

Seluruh pihak yang melakukan pertukaran informasi melalui *internet* melakukan pengamanan transaksi dengan menggunakan teknologi kriptografi kunci publik, kunci simetris, dan fungsi *hash*. Hampir semua pesan yang dipertukarkan juga menggunakan tanda tangan digital. Penggunaan teknologi kriptografi yang sangat ekstensif ini menyebabkan protokol SET dengan aman dijalankan.

Sekarang ini sudah banyak pengembang sistem dalam pengamanan transaksi bank terhadap protokol SET ini sebagai penunjang sistem perdagangan *internet* mereka, seperti Microsoft, IBM, Netscape, SAIC, GTE, Open Market, Cybercash, Terisa Systems dan Verisign. Bahkan kini

⁷¹ *Secure Electronic Transaction*.
http://en.wikipedia.org/wiki/Secure_Electronic_Transaction#Transaction. Diakses pada tanggal 24-oktober-2010. Pukul 13:49WIB.

perusahaan penyelenggara *charge card* pesaing seperti American Express, juga menyatakan dukungannya kepada protokol SET.⁷²

2.5 Aspek Hukum Internasional Sistem Pembayaran Elektronik dan *Cybercrime*

Pada awal sistem pembayaran elektronik, banyak dari para pembuat kebijakan umumnya kurang memberi perhatian terhadap masalah-masalah yang terjadi. Seiring perkembangan perdagangan elektronik dan implikasinya yang terjadi secara global, perhatian yang lebih fokus tampak diperlihatkan oleh para ahli dari seluruh dunia. Kebijakan-kebijakan internasional akhirnya dicanangkan untuk dapat mengatur perdagangan elektronik ini dan segala macam kegiatannya secara universal/umum. Produk dari kebijakan ini adalah peraturan-peraturan yang berupa draft atau proposal yang dapat berlaku umum sehingga dapat diaplikasikan pada hukum negara para pesertanya. Awal pengembangan kebijakan hukum perdagangan elektronik ini melahirkan suatu kesepakatan internasional dari departemen perdagangan PBB, kebijakan tersebut adalah *UN Model Law On Electronic Commerce* selanjutnya disebut sebagai *Model Law* saja.

Di Amerika, pembahasan dan pemberlakuan atas peraturan-peraturan tentang sistem pembayaran elektronik telah menghasilkan banyaknya pelaku baru dalam dunia perdagangan elektronik. Peraturan yang digunakan di Amerika sebagai panduan membuat peraturan-peraturan baru tentang perdagangan di Amerika adalah *Uniform Commercial Codes (UCC)*.⁷³

Mengikuti perkembangan teknologi yang terjadi pada tahun 1960an dan 1970an, beberapa peraturan yang terdapat pada UCC dianggap kurang memadai untuk diterapkan pada dunia perdagangan elektronik saat. Beberapa revisi dilakukan UCC untuk melakukan adaptasi terhadap pengaplikasian teknologi baru dalam dunia perdagangan. Akhirnya pada tahun 1999 *Uniform Law Commission*

⁷² Iman Budi Setiawan. *Smartwallet-Java Wallet* Berbasis *Smartcard* dan Protokol SET. Skripsi. Depok Universitas Indonesia. 1999. Hlm. 14.

⁷³ <http://www.law.cornell.edu/ucc/ucc.table.html>. diakses tanggal 18 November 2010. Pukul 7.06WIB.

(ULC) membuat suatu komite untuk membentuk peraturan yang mampu menghilangkan hambatan atas adaptasi tersebut, peraturan tersebut berhasil dibentuk dengan nama *Electronic Funds Transfer Act* (EFTA). Di dalam peraturan ini ada bagian yang sangat penting dalam melakukan transaksi elektronik, yaitu mengenai catatan elektronik.

Berikut adalah beberapa hasil konvensi atau beberapa peraturan di negara lain yang menjadi model adaptasi beberapa peraturan tentang perdagangan elektronik di banyak negara :

2.5.1 UNCITRAL Model Law on Electronic Commerce

Model law ini merupakan sebuah produk dari komisi Perserikatan Bangsa Bangsa (PBB) yang bertugas dalam pengembangan hukum perdagangan internasional yaitu *United Nations Commission on International Trade Law* (UNCITRAL). Tujuan dari *model law* ini adalah sebagai dasar hukum yang mampu menghapus permasalahan perdagangan elektronik tanpa dibatasi dengan perbedaan-perbedaan yang ada pada perdagangan menggunakan komputer. *Model law* ini tentu tidak berlaku terhadap sebuah transaksi elektronik dimana para pihak tidak ingin mengadopsinya. *Model law* hanyalah sebagai acuan hukum yang dapat menjembatani para pihak yang ingin bertransaksi secara elektronik.⁷⁴

Model law ini akhirnya diselesaikan oleh UNCITRAL pada bulan juni tahun 1996⁷⁵, berdasarkan sesuatu yang dikerjakan semenjak 1978. Setengah tahun kemudian *model law* ini disetujui oleh Majelis Umum PBB dengan dikeluarkannya resolusi 51/162 pada tanggal 16 Desember 1996. UNCITRAL *model law* merupakan landasan untuk mengatur otentikasi, perlengkapan, dan dampak pesan elektronik berbasis komputer dalam perdagangan. Pasal 5 bis

⁷⁴ Ford Warwick dan Michael S. Baum. *Op. Cit.*, hlm 58.

⁷⁵ Benjamin Wright dan Jane K. Winn. *The Law of Electronic Commerce*. Aspen Law & Business. 3rd Edition. Hlm 14(30).

pada *model law* kemudian diadopsikan oleh UNCITRAL sebagai sebuah amandemen pada Juni 1998.⁷⁶

Beberapa prinsip utama dalam UNCITRAL *Model Law on Electronic Commerce* adalah sebagai berikut.⁷⁷

1. Segala bentuk informasi elektronik dalam bentuk data elektronik dapat dikatakan memiliki akibat hukum, keabsahan ataupun kekuatan hukum.
2. Dalam hukum mengharuskan adanya suatu informasi dalam bentuk tertulis, suatu data elektronik dapat memenuhi syarat untuk itu. Hal ini disebutkan dalam pasal 6 UNCITRAL *Model Law*.
3. Dalam hal tanda tangan, suatu tanda tangan elektronik merupakan tanda tangan yang sah. Transaksi elektronik dapat dilakukan dengan tanda tangan digital atau tanda tangan elektronik. Tanda tangan digital adalah pendekatan yang dilakukan oleh teknologi *encryption* terhadap kebutuhan akan adanya suatu tanda tangan dengan orang yang membuat atau menyetujui dokumen tersebut. Sementara tanda tangan elektronik adalah suatu teknik penandatanganan yang menggunakan biometric ataupun berbagai cara lainnya, artinya tidak selalu harus menggunakan *public key cryptography*.

Pada pasal 2 *model law* ini kurang lebih berisi tentang definisi - definisi dalam perdagangan elektronik seperti *data messages* yang diartikan sebagai suatu informasi yang dihasilkan (*generated*). Diterima, disimpan secara elektronik, optik atau cara-cara sejenis; termasuk tetapi tidak terbatas pada EDI (*Electronic Data Interchange*), e-mail, telegram, telex, telecopy. Lalu *model law* juga menerangkan tentang *originator* sebagai pengirim pesan data dan *addressee* sebagai penerima pesan data.

⁷⁶ <http://www.mnurjaya.co.cc/2010/01/tentang-uncitral-model-law-on-e.html>. diakses tanggal 18 November 2010. Pukul 15.40 WIB.

⁷⁷ Edmon Makarim. *Op. Cit.*, hlm 258-259

Pada bagian badannya *model law* yang terdiri dari 17 pasal dan terbagi dalam dua bagian ini kurang lebih mengatur mengenai definisi kontrak elektronik dan memberikan pengaturan penerimaan dan kekuatan pembuktian dari bukti elektronik; peraturan yang didasarkan pada prinsip non diskriminasi, mengatur *e-commerce* secara spesifik untuk perundang-undangan nasional atau undang-undang lain yang dibuat oleh negara/negara bagian; memberikan aturan yang pasti untuk transaksi elektronik.

Semenjak *model law* ini disahkan oleh PBB pada Desember 1996, UNCITRAL telah mengeluarkan peraturan-peraturan internasional baru dalam hal perdagangan elektronik, diantaranya adalah pengaturan mengenai tanda tangan elektronik dengan peraturan pelaksanaannya pada tahun 2001; peraturan mengenai transaksi elektronik; pengaturan mengenai privasi; dan pengaturan mengenai keamanan informasi yang termasuk keamanan *cyber, cyber crime and public key infrastructure*; yang terakhir adalah masalah kontrak elektronik secara *online (online electronic contracting)*.

2.5.2 Uniform Electronic Transaction Act (UETA)

Uniform Act di Amerika adalah sebuah model hukum yang dibentuk oleh suatu lembaga beranggotakan praktisi hukum mulai dari advokat, jaksa, hakim hingga para akademisi.⁷⁸ Lembaga yang dimaksud dikenal dengan nama *National Conference of Commissioners on Uniform State Laws (NCCUSL)*. Tujuan dari model hukum ini adalah sebagai panduan oleh negara-negara bagian agar dapat terjadinya kesamaan dan keseragaman peraturan. UETA ini sendiri telah di adopsi oleh 47 negara bagian di Amerika.

UETA terdiri dari 21 seksi yang antara lain membahas mengenai penggunaan *electronic records* dan *electronic signatures (section 5)* dan keabsahan dari *electronic records, electronic signatures* dan *electronic contracts (section 7)*. Pengaturan mengenai *electronic records* dan *electronic*

⁷⁸ *Uniform Act*. (http://en.wikipedia.org/wiki/Uniform_Act). Diakses tanggal 5 Januari 2011.

signatures pada UETA merupakan bagian yang terpenting dalam *uniform act* ini.

Berikut adalah pemaparan beberapa bagian yang ada dalam UETA yang dianggap penting terhadap perkembangan perlindungan hukum transaksi elektronik, antara lain :

- 1) Definisi mengenai *electronic records* dan *electronic signature* tertulis pada *section 2* nomor 7 dan 8. UETA mendefinisikan *electronic record* sebagai sebuah catatan yang tercipta, terbentuk, terkirim, terkomunikasi, diterima, atau disimpan dengan cara elektronik. Sedangkan *electronic signatures* di definisikan sebagai sebuah suara, simbol elektronik, atau sebuah proses yang dilakukan kepada atau yang secara logika dapat diasosiasikan dengan sebuah catatan yang lalu di laksanakan atau di adopsi oleh seseorang yang bermaksud untuk menandai/menandatangani catatan tersebut.
- 2) *Section 3* menjelaskan cakupan pada UETA, menurut keterangannya, UETA hanya berlaku terhadap transaksi yang berhubungan dengan bisnis, komersil, dan yang berhubungan dengan pemerintahan. Maka secara tidak langsung juga menjelaskan bahwa transaksi di luar yang bersangkutan dengan hubungan bisnis, komersil atau pemerintahan tidaklah dilindungi oleh UETA. Hal ini menegaskan bahwa *electronic records* dan *electronic signatures* yang dibuat secara sepihak tidaklah dilindungi oleh UETA.
- 3) *Section 7* diatur mengenai pengakuan *electronic signatures, records* dan *contracts* secara hukum yang berbunyi.
 - a. Efek hukum dan kekuatan hukum dari sebuah *record* (catatan) atau *signatures* (tanda tangan) tidak boleh di tolak karena semata-mata berbentuk elektronik.

- b. Sebuah kontrak tidak dapat di tolak akibat dan kekuatan hukumnya hanya semata-mata karena sebuah catatan elektronik dipakai dalam ketentuannya.
 - c. Jika hukum mengatakan bahwa sebuah catatan diperlukan, maka catatan elektronik berlaku sah.
 - d. Jika hukum mengatakan bahwa sebuah tanda tangan diperlukan, maka tanda tangan elektronik berlaku sah.
- 4) *Section 9* dibahas mengenai kegunaan dan efek dari catatan elektronik dan tanda tangan elektronik. Disitu dijelaskan bahwa sebuah catatan elektronik dan tanda tangan elektronik merupakan atribut dari seseorang yang melakukan transaksi tersebut. Tindakan dari para pihak dapat ditentukan dengan menunjukkan kabsahan dari prosedur keamanan yang di gunakan pada catatan elektronik dan tanda tangan elektronik tersebut. Selain itu pada *section* ini dijelaskan pula mengenai efek dari catatan elektronik dan tanda tangan elektronik yang dilekatkan pada para pihak seperti yang sudah dijelaskan di atas ditentukan oleh konteks dan kondisi pada saat waktu pembuatan, eksekusi atau adopsi, termasuk kontrak antar pihak jika ada atau sesuai yang ditentukan oleh undang-undang.
- 5) *Section 12* menjelaskan pentingnya penyimpanan catatan elektronik sebagai bukti. Dijelaskan bahwa jika hukum membutuhkan sebuah catatan untuk disimpan, maka catatan elektronik tersebut harus secara akurat memperlihatkan informasi yang sama pada saat pengiriman pertama; dan tetap dapat diakses sebagai referensi di kemudian waktu. Hal tersebut dapat dilakukan seseorang dengan bantuan pihak ketiga.
- 6) *Section 13* pada pembuktian, catatan elektronik dan tanda tangan elektronik tidak dapat diberikan secara terpisah karena keduanya merupakan bentuk transaksi elektronik.
- 7) *Section 14* membahas mengenai transaksi yang dilakukan secara otomatis. (1) membahas tentang situasi dimana transaksi dilakukan

oleh agen elektronik kedua belah pihak, maka kontrak tetap berlaku walaupun tidak ada pihak yang sadar atau menelaah terlebih dahulu tindakan dari si agen elektronik tersebut. (2) berlakunya kontrak dimana perjanjian dibentuk berdasarkan interaksi antara agen elektronik dan individu.

- 8) *Section 15* membahas tentang waktu dan tempat dari sebuah transmisi elektronik. Bagian ini membahas mengenai kapan dan darimana sebuah catatan elektronik dikirim dan diterima. Bagian ini tidak membahas mengenai efek hukum dari catatan elektronik tersebut, dikarenakan sebuah catatan elektronik belum tentu dapat digunakan atau bahkan dibaca oleh si penerima. Dalam masalah kekuatan catatan elektronik dalam mengikat para pihak adalah masalah yang harus diserahkan dalam penafsiran hukum.

Adaptasi yang dilakukan UU ITE terhadap hasil traktat ini terlihat dengan jelas pada pengaturan yang ada dalam pasal 6 UU ITE yang mengatakan kekuatan informasi dan dokumen elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.⁷⁹ Hal ini menegaskan bahwa adanya perbandingan hukum antara UETA dan UU ITE terutama pada pasal 6 UU ITE dengan *section 7* UETA. Namun yang disayangkan adalah pengaturan mengenai catatan elektronik yang terdapat pada UETA belum diatur dengan jelas pada UU ITE atau peraturan pembayaran lainnya di Indonesia.

2.5.3 *Convention on Cybercrime (COC)*

Konvensi ini merupakan traktat pertama yang membahas mengenai (*cybercrime*) kejahatan siber/maya dan *internet* dengan cara mengadaptasi pada hukum nasional negara-negara, mengembangkan teknik investigasi terhadap *cybercrime* dan meningkatkan kerjasama antara negara-negara di

⁷⁹ Indonesia. Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 6.

dunia dalam menangani masalah *cybercrime*. COC merupakan gagasan dari anggota *Council of Europe*⁸⁰ di Stratsbourg, Perancis yang dijalankan dengan observasi yang dilakukan oleh negara Kanada, Jepang dan China.

COC dan bagian penjelasannya akhirnya diadopsi oleh negara-negara peserta pada 8 November 2001. COC ini dinyatakan terbuka untuk ditandatangani di Budapest pada 23 November 2001 dan memasuki masa berlaku pada 1 Juli 2004. Pada 2 September 2006, 15 negara telah menandatangani traktat ini, meratifikasi dan menyetujui konvensi tersebut. Sedangkan 28 negara juga telah menandatangani perjanjian ini namun tidak meratifikasinya.⁸¹

Pembentukan COC adalah untuk menanggulangi masalah kejahatan yang dilakukan melalui *internet* dan melalui koneksi komputer lainnya, menangani terutama masalah pelanggaran hak karya intelektual, penipuan dengan menggunakan komputer, pornografi pelanggaran pada keamanan jaringan. Didalamnya juga mengatur mengenai kekuasaan dan prosedur seperti penyelidikan pada jaringan komputer atau intersepsi yang berdasarkan hukum/sah.

Tujuan utama dari konvensi ini dijelaskan pada bagian pembukaannya, yaitu untuk menghasilkan sebuah kebijakan universal namun fokus pada perlindungan masyarakat terhadap kejahatan telematika (konvergensi antara informasi, media dan telekomunikasi), terutama dengan cara mengadopsi peraturan yang sesuai serta mengasuh juga hubungan kerjasama internasional. Secara prinsipnya, COC ingin mencapai :⁸²

⁸⁰ *Council of Europe* atau Dewan Negara-Negara Eropa merupakan salah satu organisasi internasional yang tertua di dunia. Berdiri sejak tahun 1949 dewan ini bertujuan untuk mengintegrasikan negara-negara Eropa menjadi satu kesatuan. Dewan ini beranggotakan 47 negara dari seluruh daratan Eropa. Produk-produk dari Dewan Eropa merupakan masalah hukum yang biasa berhubungan dengan masalah Hak Asasi Manusia, perkembangan Demokrasi dan kerjasama budaya.

⁸¹ Situs resmi *Council of Europe*. . Daftar Anggota.

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/10/2010&CL=ENG>. Diakses tanggal 21 November 2010. Pukul 14.28WIB.

⁸² Wikipedia. *Convention of Cybercrime*.

http://en.wikipedia.org/wiki/Convention_on_Cybercrime. Diakses tanggal 1 Januari 2011.

1. Harmonisasi atas hukum yang mengatur mengenai elemen-elemen dan ketentuan-ketentuan pada pelanggaran kriminal dalam konteks *Cyber-crime*.
2. Memberikan panduan pada prosedural penyelidikan dan penuntutan terhadap tindak kejahatan dengan penggunaan sisetm komputer atau pembuktian menggunakan alat bukti elektronik.
3. Membangun kerjasama internasional yang cepat dan efektif.

COC pada *chapter II section 1* yang membahas mengenai Hukum Kriminal Secara Substantif memberikan definisi terhadap beberapa bentuk pelanggaran dalam dunia maya yang penting, antara lain :

- a. *Illegal access* : adalah perbuatan hukum yang dilakukan oleh pihak ketiga untuk mengakses data seseorang dengan sengaja secara sebagian atau keseluruhan dari sebuah sistem komputer tanpa hak dari pemiliknya. Hal ini dilakukan dengan melanggar sistem keamanan untuk memiliki data dari komputer tersebut dengan itikad buruk, atau dengan menggunakan komputer lain untuk mengakses komputer tersebut.
- b. *Illegal Interception* : adalah perbuatan yang dilakukan untuk mengintersepsi tanpa hak, dilakukan dengan cara teknis pada transmisi data komputer yang tidak bersifat publik, dari atau melalui sebuah sistem komputer.
- c. *Data Interference* : adalah perbuatan merusak, menghapus, mengurangi, mengubah atau menutup-nutupi tanpa hak terhadap sebuah data komputer yang dilakukan dengan sengaja. Hal ini dapat mengakibatkan bahaya.
- d. *System Interference* : adalah perbuatan untuk menghalangi sebuah sistem komputer tanpa hak, dengan cara meng-input, mentransmisikan, merusak, menghapus, memperburuk, mengubah atau menutupi data komputer.
- e. *Misuse of Devices* : adalah produksi, penjualan, penyediaan, import, distribusi, atau tindakan lain yang menyebabkan sebuah

alat, termasuk program komputer yang didisain dan digunakan untuk melakukan pelanggaran-pelanggaran di atas. Atau sebuah password komputer, kode akses atau data yang menyerupai yang dapat menyebabkan sebagian atau seluruh sistem komputer dapat diakses untuk melakukan pelanggaran - pelanggaran seperti apa yang dijelaskan di atas.

- f. *Computer-related forgery* : adalah perbuatan yang dilakukan tanpa hak untuk meng-input, mengubah, menghapus atau menutupi sebuah data komputer yang dapat mengubah sebuah data yang tidak asli untuk membuatnya menjadi asli sehingga dapat terlihat sebagai data yang sah, walaupun data tersebut padat dibaca atau diterjemahkan.
- g. *Computer-related Fraud* : adalah perbuatan yang dilakukan untuk meng-input, mengubah, menghapus atau menutupi sebuah data komputer serta mengintervensi sebuah sistem komputer dengan tujuan untuk mengelabui seorang pengguna dengan tujuan ekonomi.

Penerapan pengertian-pengertian tentang kejahatan *cybercrime* seperti yang telah didefinisikan oleh COC dapat kita lihat pada UU ITE. Adaptasi yang dilakukan oleh UU ITE terhadap peraturan COC ini terlihat dengan jelas pada pengaturan UU ITE tentang perbuatan yang dilarang dalam pasal 27 hingga 37 UU ITE.

2.5.4 International Telecommunication Union (ITU) Toolkit for Cybercrime Legislation

International Telecommunication Union (ITU) merupakan sebuah agensi dalam badan PBB yang bertugas menyusun peraturan yang berhubungan dengan masalah informasi dan teknologi komunikasi. Pergerakan ITU aktif pada beberapa bidang seperti, *internet*, teknologi nirkabel, navigasi penerbangan dan maritim, penggunaan radio untuk kepentingan astrologi,

meteorologi menggunakan satelit, konvergensi pada telepon selular, akses *internet*, data suara, TV broadcasting, dan jaringan. ITU sendiri berlokasi di Jenewa, Swiss dan mempunyai anggota sebanyak 192 negara.⁸³

ITU mempunyai sebuah agenda tersendiri dalam melaksanakan amanatnya sebagai sebuah organisasi. Agenda tersebut yang dinamai dengan (*Global Cybersecurity Agenda*) CGA mempunyai 5 pilar dan 7 tujuan. Pilar dan tujuan tersebut adalah.⁸⁴

Lima Pilar (*The five Pilar*)

1. Penyusunan Hukum
2. Pengaturan teknis dan prosedural
3. Struktur Organisasi
4. Pembangunan kapasitas
5. Kerjasama Internasional

Tujuh Sasaran (*The seven goals*)

1. Perluasan strategi untuk perkembangan dari model peraturan masalah *cybercrime* yang dapat diaplikasikan dan dioperasikan dengan peraturan-peraturan negara dan regional yang sudah ada.
2. Perluasan strategi untuk menciptakan struktur organisasi dan kebijakan terhadap *cybercrime* yang layak.
3. Perkembangan strategi atas penerimaan kriteria keamanan dan akreditasi dari skema perangkat keras dan aplikasi serta sistem dari perangkat lunak .
4. Mengembangkan strategi untuk menciptakan jaringan atas pengawasan, peringatan dan respon terhadap insiden yang terjadi melewati antar batas negara baik yang baru maupun yang sudah ada.

⁸³ Situs resmi I.T.U. <http://www.itu.int/net/about/>. Diakses tanggal 1 Januari 2011.

⁸⁴ Ibid. <http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html>. diakses pada tanggal 22 November 2010. Pukul 19.33WIB.

5. Mengembangkan strategi secara global atas penciptaan dan penerapan atas sebuah sistem pengenalan identitas digital yang dapat berlaku secara umum dan universal dan mengempungkan struktur organisasi agar dapat menjamin pengenalan atas surat-surat kepercayaan melewati batas geografis negara.
6. Mengembangkan strategi global dalam memfasilitasi perkembangan kapasitas manusia serta institusinya dalam memperluas pengetahuan dan pembelajaran di semua sector dan dalam area yang disebutkan di atas.
7. Membuat suatu proposal terhadap kerangka suatu strategi penanaman modal terhadap kerjasama, dialog dan koordinasi internasional.

Toolkit ini merupakan produk dari ITU yang merupakan alat untuk mencapai *goal* (tujuan) pertama dari *seven strategic goals* (tujuh tujuan strategis). Penerapan *toolkit* ini terhadap seluruh negara peserta merupakan hal yang sangat penting sebagai langkah perlawanan terhadap kejahatan menggunakan teknologi informasi dan komunikasi. *Toolkit* ini dibentuk dengan bahan pertimbangan karena kejahatan seperti ini dapat terjadi dimana saja dibelahan bumi, maka dari itu diperlukan sebuah kerjasama internasional, kerjasama dalam penyelidikan, dan penyamaan dalam masalah prosedural. Dengan itu dirasakan kepentingan dari penyamaan atau harmonisasi atas sebuah kerangka hukum dalam memerangi *cybercrime* dan memfasilitasi kerjasama internasional tersebut.

Inti dari pengaturan ITU *toolkit* ini terdiri dari 6 *title* dan 34 *section* ini mengatur antara lain masalah definisi pada *cybercrime*, tindakan substantif dari *cybercrime*, peraturan prosedur penyidikan dan penyelesaian masalah, serta masalah yurisdiksi dan kerjasama internasional.

Perkembangan yang dilakukan dalam ITU ini sebenarnya ada pada masalah kerjasama internasional dalam penindakan *cybercrime* dalam lingkup yang terjadi antar batas negara. Terlihat pada *title 5* dalam ITU *toolkit* ini pengaturan mengenai ketersediaan negara yang mengadaptasi peraturan ini

untuk terbuka terhadap segala bentuk kerjasama yang dilakukan dalam rangka pemberantasan *cybercrime*.

2.5.5 *Electronic Fund Transfer Act (EFTA)*

Electronic Fund Transfer adalah salah bentuk hukum di Amerika Serikat yang dibentuk oleh anggota kongres Amerika pada 1978 untuk mengatur masalah hak dan kewajiban dari konsumen dan juga tanggung jawab dari semua pihak yang terlibat dalam kegiatan tersebut. EFT jika diterjemahkan dalam bahasa Indonesia merupakan Transfer Dana Elektronik, yang pada saat ini pengaturannya masih berupa RUU Transfer Dana. Dalam RUU Transfer Dana tersebut diatur pada ketentuan umum nomor 2 bahwa yang dimaksud dengan dana adalah :

- a. Uang tunai yang diserahkan oleh Pengirim kepada Bank Penerima;
- b. Uang yang tersimpan dalam Rekening Bank Pengirim pada Bank Penerima;
- c. Uang yang tersimpan dalam rekening Bank Penerima pada Bank Penerima lainnya;
- d. Uang yang tersimpan dalam Rekening Penerima pada Bank Penerima Akhir;
- e. Uang yang tersimpan dalam Rekening Bank Penerima yang dialokasikan untuk kepentingan Penerima yang tidak mempunyai Rekening pada Bank tersebut; dan/atau
- f. Fasilitas cerukan (*overdraft*) atau fasilitas kredit yang diberikan Bank kepada Pengirim.

Sedangkan pada ketentuan umum nomor 3 mengatakan yang dimaksud dengan transfer dana adalah rangkaian kegiatan yang dimulai dengan perintah dari Pengirim Asal yang bertujuan untuk memindahkan sejumlah Dana kepada Penerima yang disebutkan dalam Perintah Transfer Dana sampai dengan diterimanya Dana oleh Penerima Dana dan pada nomor 20 menjelaskan mengenai sistem transfer dana yaitu suatu sistem terpadu untuk memproses

perintah Transfer Dana dengan menggunakan sarana elektronik atau sarana lainnya.

Di dalam EFTA yang dimaksud dengan transfer dana adalah transfer elektronik selain melalui cek, draft atau instrumen sejenis. Transfer adalah yang dilakukan melalui terminal, instrumen telepon, komputer, atau *magnetic tape*, untuk memberikan arahan, instruksi/perintah, atau memberikan wewenang kepada institusi keuangan (bank, *credit union*) untuk melakukan pendebitan atau pengkreditan terhadap suatu rekening. Termasuk didalam pengertiannya adalah transaksi menggunakan sistem *point of sale*, ATM, penarikan atau penyetoran secara langsung, dan transfer melalui telepon.

Dalam EFTA ada yang dikenal sebagai *Unathorized Electronic Fund Transfer* yaitu, transfer elektronik yang dilakukan oleh orang lain selain nasabah tanpa kewenangan untuk melakukan hal tersebut dan nasabah tidak memperoleh manfaat dan keuntungan apapun dari transfer elektronik tersebut. Dalam hal terjadi *unauthorized EFT* ini, maka beban pembuktian ada pada lembaga keuangan yang menangani transaksi tersebut. Namun jika memang transaksi tersebut adalah sah atau, lembaga keuangan yang bersangkutan mempunyai kewajiban untuk membuktikan bahwa terdapat kondisi-kondisi tertentu sebagaimana tersebut di atas sehingga nasabahlah yang bertanggungjawab atas transaksi tersebut.

Perlunya pengadopsian EFTA ini pada sistem hukum kita sangatlah penting, terutama dalam hal penyelenggaraan kegiatan transaksi elektronik. Dengan disahkannya RUU Transfer Dana maka, pengaturan terhadap sistem pembayaran elektronik menjadi semakin terang dan jelas.

2.6 Aspek Hukum Sistem Pembayaran Elektronik Menggunakan Kartu di Indonesia

Dalam sistem pembayaran elektronik terdapat beberapa aspek yang harus diperhatikan. Selain aspek teknologi itu sendiri yang harus kita cermati sebagai

langkah menentukan tindakan prefentif, kita juga harus melihat dari aspek hukumnya. Pencermatan dari aspek hukum ini dapat dilakukan baik itu dalam rangka menentukan langkah represif atau dapat juga sebagai langkah prefentif.

Dalam mencermati aspek hukum itu sendiri, kita harus melihat apa saja yang terkait didalamnya. Baik itu dari subjek hukum seperti konsumen, pelaku usaha, pedagang, dan pemerintah. Selain itu juga ada objek hukum yaitu sistem pembayaran elektronik dan alat pembayaran menggunakan kartu. Pada subbab ini penulis akan mencoba memaparkan bagaimana peraturan hukum yang ada di Indonesia dalam kaitannya dengan penyelenggaraan sistem pembayaran elektronik menggunakan kartu.

2.6.1 Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

Peraturan perundang-undangan yang terdiri dari 13 bab dan 54 pasal ini merupakan *cyber law* di Indonesia. Di dalam UU ITE ini selain mengatur masalah informasi dan penggunaannya, ada juga peraturan yang mengatur masalah transaksi elektronik. Dengan adanya peraturan yang dapat mengatur tentang transaksi elektronik diharapkan perkembangan transaksi elektronik ini jauh lebih baik dan mampu mendapatkan kepercayaan dari dunia internasional.

Pasal 3 UU ITE mengatur mengenai asas dan tujuan dari pelaksanaan peraturan ini. Dalam pasal ini menyatakan bahwa UU ITE dibentuk dengan dasar agar dapat dipergunakan sebagai alat untuk menciptakan pemanfaatan teknologi informasi dan transaksi elektronik yang baik, untuk menciptakan hal ini UU ITE harus dijalani dengan :⁸⁵

- a. Asas Kepastian Hukum, yang berarti landasan hukum bagi pemanfaatan teknologi informasi dan transaksi elektronik serta segala sesuatu yang mendukung penyelenggaraannya yang mendapatkan pengakuan hukum di dalam dan luar pengadilan.

⁸⁵ Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Penjelasan Pasal 3.

- b. Asas Manfaat, berarti asas bagi pemanfaatan teknologi informasi dan transaksi elektronik diupayakan untuk mendukung proses berinformasi sehingga dapat meningkatkan kesejahteraan rakyat.
- c. Asas Kehati-hatian, berarti landasan bagi pihak yang bersangkutan harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian, baik bagi dirinya maupun bagi pihak lain dalam pemanfaatan teknologi informasi dan transaksi elektronik.
- d. Asas Itikad Baik, berarti asas yang digunakan para pihak dalam melakukan transaksi elektronik tidak bertujuan untuk secara sengaja dan tanpa hak atau melawan hukum mengakibatkan kerugian bagi pihak lain tanpa sepengetahuan pihak lain tersebut.
- e. Asas Kebebasan Memilih Teknologi atau Netral Teknologi, berarti asas pemanfaatan Teknologi Informasi dan Transaksi Elektronik tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan pada masa yang akan datang.

Salah satu pasal yang penting dalam UU ITE adalah pasal 5 ayat (1) dimana dinyatakan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Peraturan ini sangat penting karena dengan tegas penggunaan dokumen elektronik dapat menjadi alat bukti yang sah dalam hukum pembuktian. Selain itu dalam UU ITE juga mendefinisikan mengenai kontrak elektronik pada pasal 1 huruf 17 yang mengatakan bahwa kontrak elektronik adalah perjanjian para pihak yang dibuat melalui sistem elektronik.

Melihat UU ITE sebagai regulasi yang diberlakukan untuk penyelenggaraan sistem elektronik, terkait dengan itu maka perlu ditelaah beberapa pasal terkait. Pasal 9 UU ITE menyatakan bahwa para pelaku usaha yang menawarkan produk melalui sistem elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan.⁸⁶ Informasi yang tepat dan benar ini haruslah mencakup (i) identitas serta status subjek hukum dan kompetensinya, baik

⁸⁶*Ibid.*, Pasal 9.

sebagai produsen, pemasok, penyelenggara maupun perantara (ii) menjelaskan hal tertentu yang menjadi syarat sahnya perjanjian serta menjelaskan barang dan/atau jasa yang ditawarkan, seperti nama, alamat, dan deskripsi barang/jasa.⁸⁷

Selanjutnya kita melihat pasal 10 ayat (1) UU ITE yang menyatakan bahwa pelaku transaksi elektronik harus dapat disertifikasi oleh Lembaga Sertifikasi Keandalan. Sedangkan ayat (2) dalam pasal ini menyatakan bahwa pembentukan akan Lembaga Sertifikasi Keandalan ini diatur dengan Peraturan Pemerintah⁸⁸ (hingga saat ini belum ada Peraturan Pemerintah yang dimaksud). Walaupun sertifikasi ini belum menjadi sebuah syarat atas penyelenggaraan sistem transaksi elektronik, tapi ada indikasi akan hal dimana dengan melakukan sertifikasi ini akan “mendongkrak” sistem keamanan dari transaksi elektronik itu sendiri.

Bagian kedua UU ITE mengatur mengenai penyelenggaraan sistem elektronik, hal ini tercantum pada pasal 15 dan pasal 16 yang mengatur mengenai penyelenggaraan sistem elektronik yang harus andal : sistem elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunanya; aman : sistem elektronik terlindungi secara fisik (*hardware/sotware*) dan nonfisik (*communication*).; beroperasi sebagaimana mestinya : sistem elektronik memiliki kemampuan sesuai dengan spesifikasinya, serta bertanggung jawab : ada subjek hukum yang bertanggung jawab secara hukum terhadap penyelenggaraan sistem elektronik tersebut.⁸⁹ Sedangkan pada pasal 16 mengatur mengenai minimum persyaratan yang harus terpenuhi dalam penyelenggaraan sistem elektronik, antara lain :

- a. Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan;

⁸⁷ *Ibid.*, Penjelasan pasal 9.

⁸⁸ *Ibid.*, Pasal 10.

⁸⁹ *Ibid.*, Penjelasan pasal 15 ayat (1) dan (2).

- b. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut;
- c. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik;
- d. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan Sistem Elektronik tersebut; dan
- e. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Dalam penggunaan sistem elektronik sebagai media untuk melakukan pembayaran maka kita harus melihat kegiatan tersebut sebagai transaksi elektronik. Sebagaimana dijelaskan pada pasal 1 angka 2 tentang transaksi elektronik sebagai perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan komputer, dan/atau media elektronik lainnya.⁹⁰ Dalam UU ITE peraturan tentang transaksi elektronik ini diatur pada pasal 17 hingga 22, dimana didalamnya mengatur mengenai lingkup transaksi elektronik, kekuatan kontrak elektronik dalam transaksi elektronik, pemilihan hukum dalam melakukan transaksi elektronik, kesepakatan penggunaan sistem elektronik yang sama dalam melakukan transaksi elektronik, waktu penerimaan dan persetujuan transaksi elektronik, akibat hukum dalam melakukan transaksi elektronik baik dilakukan sendiri, melalui kuasa atau melalui agen elektronik.

2.6.2 Peraturan Bank Indonesia Nomor 11/11/PBI/2009 tentang Penyelenggaraan Kegiatan Penggunaan Alat Pembayaran Menggunakan Kartu

Peraturan ini merupakan pengganti dari Peraturan Bank Indonesia nomor 11/11/PBI/2009 Jo. 7/52/PBI/2005 yang pada tanggal 28 Desember

⁹⁰ *Ibid.*, Pasal 1 angka 2.

2005 menggantikan Peraturan Bank Indonesia nomor 6/30/PBI/2004 selanjutnya ditulis sebagai PBI APMK. Peraturan ini dikuatkan dengan peraturan pelaksana atas Surat Edaran Bank Indonesia nomor 11/10/DASP/2009. Secara keseluruhan PBI APMK ini merupakan peraturan perundang-undangan yang mengatur tentang :

- a. Persyaratan dan tata cara perolehan izin Prinsipal;
- b. Persyaratan dan tata cara perolehan izin sebagai Penerbit;
- c. Persyaratan dan tata cara perolehan izin sebagai *Acquirer*;
- d. Persyaratan dan tata cara memperoleh izin sebagai Penyelenggara Kliring dan/atau Penyelenggara Penyelesaian Akhir;
- e. Pemrosesan perizinan sebagai Prinsipal, Penerbit, *Acquirer*, Penyelenggara Kliring dan/atau Penyelenggara Penyelesaian Akhir;
- f. Pemberitahuan tanggal efektif dimulainya kegiatan sebagai Prinsipal, Penerbit, *Acquirer*, Penyelenggara Kliring dan/atau Penyelenggara Penyelesaian Akhir;
- g. Penyelenggaraan Alat Pembayaran Menggunakan Kartu;
- h. Persyaratan dan tata cara memperoleh izin dan menyampaikan laporan dalam rangka peralihan perizinan melalui penggabungan, peleburan, pemisahan, atau pengambilalihan;
- i. Pengawasan, laporan penyelenggaraan kegiatan APMK, dan tata cara pengenaan sanksi denda;
- j. Pengembangan dan penyediaan sistem APMK yang dapat saling dikoneksikan (*Interoperability*) dengan sistem APMK lainnya;
- k. Pemrosesan perizinan sebagai prinsipal, penerbit, *technical* dan *financial acquirer* serta lembaga keuangan non bank yang melakukan penyelenggaraan kartu kredit.

Di dalam peraturan ini mengatur mengenai perbedaan APMK yang didefinisikan sebagai Kartu Kredit, Kartu Debet/ATM dan dibedakan dengan pengertian *E-money* (uang elektronik). Definisi APMK menurut peraturan ini adalah :

1. Kartu Kredit adalah APMK yang dapat digunakan untuk melakukan pembayaran atas suatu kewajiban yang timbul dari suatu kegiatan ekonomi, termasuk transaksi pembelanjaan dan/atau untuk melakukan penarikan tunai, dimana kewajiban pembayaran pemegang kartu dipenuhi terlebih dahulu *acquirer* atau penerbit, dan pemegang kartu berkewajiban untuk melakukan pembayaran pada waktu yang di sepakati baik dengan pelunasan secara sekaligus (*charge card*) ataupun pembayaran secara angsuran.
2. Kartu ATM adalah APMK yang dapat digunakan untuk melakukan penarikan tunai dan/atau pemindahan dana dimana kewajiban pemegang kartu dipenuhi seketika dengan mengurangi secara langsung simpanan pemegang kartu pada Bank atau Lembaga Selain Bank yang berwenang untuk menghimpun dana sesuai dengan ketentuan yang berlaku.
3. Kartu debit jenis APMK terakhir yang dapat digunakan untuk melakukan pembayaran atas kewajiban yang timbul dari suatu kegiatan ekonomi, termasuk transaksi pembelanjaan, dimana kewajiban pemegang kartu dipenuhi seketika dengan mengurangi secara langsung simpanan pemegang kartu pada Bank atau Lembaga Selain Bank yang berwenang untuk menghimpun dana sesuai dengan peraturan yang berlaku.

Dalam rangka pemberian sistem elektronik yang aman, andal dan bertanggung jawab seperti yang telah diatur pada UU ITE. PBI APMK ini mengatur lebih lanjut tentang kewajiban para penyelenggara dalam kegiatan menggunakan kartu pembayaran. Hal ini terlihat pada pasal 14 hingga pasal 25 PBI APMK, yang antara lain mengatur :⁹¹

- a. Penerapan manajemen resiko oleh pihak penerbit dan *acquirer*;
- b. Kewajiban penerbit dalam memberikan informasi kepada pemegang kartu yang terdiri dari :
 - 1) prosedur dan tata cara penggunaan Kartu Kredit;

⁹¹ Lihat Bank Indonesia. Peraturan Bank Indonesia nomor 11/11/PBI/2009 tentang Penyelenggaraan Alat Pembayaran Menggunakan Kartu. Bab III. Pasal 14 – 25.

- 2) hal-hal penting yang harus diperhatikan oleh Pemegang Kartu dalam penggunaan kartunya dan konsekuensi atau risiko yang mungkin timbul dari penggunaan Kartu Kredit;
 - 3) hak dan kewajiban Pemegang Kartu;
 - 4) tata cara pengajuan pengaduan atas Kartu Kredit yang diberikan dan perkiraan lamanya waktu penanganan pengaduan tersebut;
 - 5) komponen dalam penghitungan bunga;
 - 6) komponen dalam penghitungan denda; dan
 - 7) jenis dan besarnya biaya administrasi yang dikenakan.
- c. Penerbit Kartu Kredit wajib mencantumkan informasi dalam lembar penagihan yang disampaikan kepada Pemegang Kartu, paling kurang meliputi:
- 1) besarnya minimum pembayaran oleh Pemegang Kartu;
 - 2) tanggal jatuh tempo pembayaran;
 - 3) besarnya persentase bunga per bulan dan persentase efektif bunga per tahun (*annualized percentage rate*) atas transaksi yang dilakukan, termasuk bunga atas transaksi pembelian barang atau jasa, penarikan tunai, dan manfaat lainnya dari Kartu Kredit apabila bunga atas masing-masing transaksi tersebut berbeda;
 - 4) besarnya denda atas keterlambatan pembayaran oleh Pemegang Kartu; dan
 - 5) *nominal bunga yang dikenakan.*
- d. Larangan terhadap penerbit kartu kredit untuk memberikan fasilitas yang mempunyai dampak tambahan biaya kepada pemegang kartu;
- e. Pengelolaan informasi pemegang APMK;
- f. Penetapan batas maksimum nilai transaksi (Rp 25jt pada hari yang sama antar bank tidak berlaku pada transfer intra bank) dan penarikan uang tunai oleh Bank Indonesia (Rp 10jt pada hari yang sama) ;

- g. Memberikan informasi kepada pemegang kartu ATM dan/atau debit tentang prosedur penggunaan, hak dan kewajiban pemegang kartu, tata cara pengajuan pengaduan permasalahan.
- h. Penggunaan uang rupiah dalam penggunaan kartu kredit dan kartu debit.
- i. Pelaksanaan audit teknologi informasi secara berkala yang dilakukan oleh prinsipal, penerbit, *acquirer*, penyelenggara kliring dan/atau penyelenggara penyelesaian akhir.

2.6.3 Peraturan Bank Indonesia nomor 11/12/PBI/2009 tentang Uang Elektronik (*E-Money*)

Uang elektronik dalam pengaplikasiannya pada sebuah alat pembayaran kartu biasa disebut sebagai *stored value/prepaid cash card* (kartu prabayar) dibedakan dari APMK karena metode penggunaannya yang berbeda dari kartu kredit dan debit/ATM. Uang elektronik merupakan suatu kegiatan prabayar antara pengguna dan penerbit, dimana pengguna mendepositkan terlebih dahulu sejumlah dana pada *server* penerbit sebelum menggunakan uang elektronik tersebut. Karena sifatnya yang demikian, maka pengaturan mengenai uang elektronik dipisahkan dari APMK.

Tidak jauh berbeda dengan PBI APMK, dalam ketentuan Peraturan Bank Indonesia nomor 11/12/PBI/2009 tentang Uang Elektronik (*E-Money*) selanjutnya pada penulisan ini disebut dengan PBI *E-Money* mendefinisikan tentang apa itu uang elektronik dan nilai uang elektronik serta pemegang. Uang elektronik dalam peraturan ini didefinisikan sebagai alat pembayaran yang memenuhi unsur-unsur sebagai berikut :⁹²

1. diterbitkan atas dasar nilai uang yang disetor terlebih dahulu oleh pemegang kepada penerbit;
2. nilai uang disimpan secara elektronik dalam suatu media seperti *server* atau *chip*;

⁹² Bank Indonesia. Peraturan Bank Indonesia nomor 11/12/PBI/2009 tentang Uang Elektronik (*E-Money*). Pasal 1 angka 3.

3. digunakan sebagai alat pembayaran kepada pedagang yang bukan merupakan penerbit uang elektronik tersebut; dan
4. nilai uang elektronik yang disetor oleh pemegang dan dikelola oleh penerbit bukan merupakan simpanan sebagaimana dimaksud dalam undang-undang yang mengatur mengenai perbankan.

Sedangkan tentang nilai uang elektronik diartikan sebagai nilai yang yang disimpan secara elektronik pada suatu media yang dapat dipindahkan untuk kepentingan transaksi pembayaran dan/atau transfer dana.⁹³ Serta pemegang adalah pihak yang menggunakan uang elektronik.⁹⁴

Dalam PBI ini juga mengatur mengenai penyelenggaraan kegiatan uang elektronik ini yang terdapat pada BAB III tentang Penyelenggaraan Kegiatan Pasal 13 hingga pasal 20 PBI *E-Money*. Isi dari peraturan-peraturan tersebut adalah :

- a. nilai uang elektronik tidak boleh lebih besar atau kecil dengan uang yang disetorkan oleh pemegang;
- b. penetapan batas maksimal yang dapat disimpan oleh suatu media elektronik (*registered Rp 5jt & unregistered Rp 1jt*);
- c. nilai pada uang elektronik tidak boleh dihapus, walaupun kartu sudah tidak berlaku untuk transaksi;
- d. penerapan manajemen resiko operasional dan keuangan oleh penerbit;
- e. kewajiban penggunaan uang rupiah dalam penerbitan uang elektronik dan penggunaannya dalam wilayah Indonesia.

2.6.4 Undang-undang nomor 7 tahun 1992 Jo. nomor 10 tahun 1998 tentang Perbankan

Pendefinisian yang terdapat dalam pasal 1 huruf 2 UU Perbankan menjelaskan pengertian bank yaitu sebagai badan usaha yang menjalankan dengan menghimpun dana dari masyarakat dalam bentuk simpanan dan

⁹³ Ibid., Pasal 1 angka 4.

⁹⁴ Ibid., Pasal 1 angka 8.

menyalurkannya kepada masyarakat dalam bentuk kredit. Dan usaha kredit tersebut di jelaskan kembali pada pasal 1 huruf 11 UU Perbankan yang menjelaskan bahwa kredit adalah penyediaan uang atau tagihan yang dapat dipersamakan dengan itu, berdasarkan persetujuan atau kesepakatan pinjam meminjam antara bank dengan pihak lain yang mewajibkan pihak peminjam untuk melunasi utangnya setelah jangka waktu tertentu dengan pemberian bunga.

Sejauh yang berhubungan dengan perbankan, maka kegiatan yang berkenaan dengan APMK mendapat legitimasinya. Dalam Undang-Undang nomor 7 tahun 1992 pasal 6 huruf I nya dengan tegas menyatakan bahwa salah satu kegiatan bank adalah melakukan usaha kredit.

2.6.5 Undang-undang nomor 23 tahun 1999 tentang Bank Indonesia Jo. Undang-undang nomor 6 tahun 2009 tentang Penetapan Peraturan Pemerintah Pengganti Undang-undang nomor 2 tahun 2008.

Segala yang berhubungan dengan pengawasan dan penyelenggaraan APMK tentu berhubungan dengan kekuasaan Bank Indonesia sebagai Bank Sentral. Peraturan pelaksana dari Undang-undang ini biasanya dikeluarkan dengan bentuk Peraturan Bank Indonesia, dikatakan pada pasal 15 ayat 1 bahwa dalam rangka mengatur dan menjaga kelancaran sistem pembayaran, Bank Indonesia berhak mengatur antara lain masalah (a) melaksanakan dan memberikan persetujuan dan izin atas penyelenggaraan jasa sistem pembayaran; (b) mewajibkan penyelenggara jasa sistem pembayaran untuk menyampaikan laporan tentang kegiatannya; (c) menetapkan penggunaan alat pembayaran. Sedangkan ayat 2 mengatakan bahwa pelaksanaan kewenangan sebagaimana dimaksud pada ayat 1 tersebut ditetapkan dengan Peraturan Bank Indonesia.

Dalam penjelasan pasal 15 ayat 2 dinyatakan dengan jelas territorial Bank Indonesia sebagai pengawas dan pengatur penyelenggaraan kegiatan

APMK, dikatakan bahwa pokok-pokok ketentuan yang akan di tetapkan dalam Peraturan Bank Indonesia memuat antara lain :

- a. Jenis penyelenggaraan jasa sistem pembayaran yang memerlukan persetujuan Bank Indonesia dan prosedur pemberian persetujuan oleh Bank Indonesia.
- b. Cakupan wewenang dan tanggung jawab penyelenggara jasa sistem pembayaran, termasuk tanggung jawab yang berkaitan dengan manajemen risiko;
- c. Persyaratan keamanan dan efisiensi dalam penyelenggaraan jasa sistem pembayaran;
- d. Penyelenggara jasa sistem pembayaran yang wajib menyampaikan laporan kegiatan;
- e. Jenis laporan kegiatan yang perlu disampaikan kepada Bank Indonesia dan tata cara pelaporannya;
- f. Jenis alat pembayaran yang dapat digunakan oleh masyarakat termasuk alat pembayaran yang bersifat elektronik seperti kartu ATM, kartu debit, kartu pra bayar dan uang elektronik;
- g. Persyaratan keamanan alat pembayaran;
- h. Sanksi administratif berupa denda bagi pelanggaran ketentuan pada huruf a, huruf d dan huruf f tersebut di atas.

2.6.6 Undang-undang nomor 8 tahun 1999 tentang Perlindungan Konsumen

Undang-Undang Perlindungan Konsumen (UU PK) ini sangat bersinggungan erat terhadap perlindungan pengguna APMK. Pengaturan yang ada pada Peraturan Bank Indonesia dan Perbankan lebih cenderung melihat sudut pengaturan kegiatan APMK dari sisi pelaku usaha. Dengan adanya UU PK ini diharapkan dapat mengisi kekosongan hukum positif yang dapat lebih mengakomodir kepentingan konsumen.

Pengertian konsumen menurut pasal 1 angka (2) UU PK adalah setiap orang pemakai barang dan/atau jasa yang tersedia dalam masyarakat, baik bagi kepentingan diri sendiri, keluarga, orang lain, maupun makhluk hidup lain dan tidak diperdagangkan. Menurut penjelasan pasal 1 angka (2) UUPK ini, ada dua macam konsumen yang dikenal dalam kepustakaan ekonomi yaitu konsumen akhir dan konsumen antara. Konsumen akhir adalah pengguna atau pemanfaat akhir dari suatu produk, sedangkan konsumen antara adalah konsumen yang menggunakan suatu produk sebagai bagian dari proses produksi suatu produk lainnya. Berdasarkan pengertian tersebut, maka pengguna APMK dapat dikatakan sebagai konsumen akhir.

Pengaturan hak-hak seorang konsumen di atur menurut pasal 4 UU PK yang antara lain menyebutkan :

- a. Hak atas kenyamanan, keamanan dan keselamatan dalam mengkonsumsi barang atau jasa.
- b. Hak untuk memilih barang atau jasa serta mendapatkan barang atau jasa tersebut sesuai dengan nilai tukar dan kondisi, serta jaminan yang dijanjikan.
- c. Hak atas informasi yang benar jelas dan jujur mengenai kondisi dan jaminan barang atau jasa.
- d. Hak untuk didengar pendapat dan keluhannya atas barang atau jasa.
- e. Hak untuk mendapatkan advokasi, perlindungan dan upaya penyelesaian sengketa perlindungan hukum secara patut.
- f. Hak untuk mendapatkan pembinaan dan pendidikan konsumen.
- g. Hak untuk diperlakukan atau dilayani secara benar, jujur serta tidak diskriminatif.
- h. Hak untuk diatur dalam ketentuan peraturan perundang-undangan.

Sesuai dengan peraturan yang mengatur hak konsumen tersebut, maka pemegang APMK berhak tidak kurang dari apa yang telah di tentukan tersebut dengan hak nya sebagai konsumen. Dalam hal penggunaan sistem pembayaran

elektronik menggunakan kartu, maka hal keamanan, kenyamanan dan kejelasan informasi menjadi hal yang sangat signifikan diperlukan.

Untuk memenuhi hak dari konsumen tersebut maka para pelaku usaha dalam hal ini penyelenggara sistem elektronik dibebankan juga dengan kewajiban sebagaimana diatur pada pasal 7 UU PK, yang menyatakan antara lain :

- a. beritikad baik dalam melakukan kegiatan usahanya;
- b. memberikan informasi yang benar, jelas dan jujur mengenai kondisi dan jaminan barang dan/atau jasa serta memberi penjelasan penggunaan, perbaikan dan pemeliharaan;
- c. memperlakukan atau melayani konsumen secara benar dan jujur serta tidak diskriminatif;
- d. menjamin mutu barang dan/atau jasa yang diproduksi dan/atau diperdagangkan berdasarkan ketentuan standar mutu barang dan/atau jasa yang berlaku;
- e. memberi kesempatan kepada konsumen untuk menguji, dan/atau mencoba barang dan/atau jasa tertentu serta memberi jaminan dan/atau garansi atas barang yang dibuat dan/atau yang diperdagangkan;
- f. memberi kompensasi, ganti rugi dan/atau penggantian atas kerugian akibat penggunaan, pemakaian dan pemanfaatan barang dan/atau jasa yang diperdagangkan;
- g. memberi kompensasi, ganti rugi dan/atau penggantian apabila barang dan/atau jasa yang diterima atau dimanfaatkan tidak sesuai dengan perjanjian.

Salah satu acuan yang penting pada UU PK yaitu dengan adanya peraturan mengenai pencatuman klausula baku pada perjanjian. Dimana dasar peraturan dalam penggunaan alat pembayaran kartu adalah dengan menggunakan sebuah perjanjian baku, maka pencantuman klausula baku yang seimbang haruslah diatur. Menurut penjelasan pasal 18 ini, adanya peraturan akan pencantuman klausula baku bertujuan untuk menempatkan kedudukan

konsumen setara dengan pelaku usaha berdasarkan prinsip kebebasan berkontrak. Berikut pengaturan tentang klausula baku yang terdapat pada pasal 18 UU PK mengatakan bahwa :⁹⁵

- a. Pelaku usaha dalam menawarkan barang dan/atau jasa yang ditujukan untuk diperdagangkan dilarang membuat atau mencantumkan klausula baku pada setiap dokumen dan/atau perjanjian apabila:
 - 1) menyatakan pengalihan tanggung jawab pelaku usaha;
 - 2) menyatakan bahwa pelaku usaha berhak menolak penyerahan kembali barang yang dibeli konsumen;
 - 3) menyatakan bahwa pelaku usaha berhak menolak penyerahan kembali uang yang dibayarkan atas barang dan/atau jasa yang dibeli oleh konsumen;
 - 4) menyatakan pemberian kuasa dari konsumen kepada pelaku usaha baik secara langsung maupun tidak langsung untuk melakukan segala tindakan sepihak yang berkaitan dengan barang yang dibeli oleh konsumen secara angsuran;
 - 5) mengatur perihal pembuktian atas hilangnya kegunaan barang atau pemanfaatan jasa yang dibeli oleh konsumen;
 - 6) memberi hak kepada pelaku usaha untuk mengurangi manfaat jasa atau mengurangi harta kekayaan konsumen yang menjadi obyek jual beli jasa;
 - 7) menyatakan tunduknya konsumen kepada peraturan yang berupa aturan baru, tambahan, lanjutan dan/atau perubahan lanjutan yang dibuat sepihak oleh pelaku usaha dalam masa konsumen memanfaatkan jasa yang belinya;
 - 8) menyatakan bahwa konsumen memberi kuasa kepada pelaku usaha untuk pembebanan hak tanggungan, hak gadai, atau hak jaminan terhadap barang yang dibeli oleh konsumen secara angsuran.

⁹⁵ Indonesia. Undang-Undang nomor 8 tahun 1999 tentang Perlindungan Konsumen. Pasal 18 ayat (1), (2), (3) dan (4).

- b. Pelaku usaha dilarang mencantumkan klausula baku yang letak atau bentuknya sulit terlihat atau tidak dapat dibaca secara jelas, atau yang mengungkapkannya sulit dimengerti.
- c. Setiap klausula baku yang telah ditetapkan oleh pelaku usaha pada dokumen atau perjanjian yang memenuhi ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) dinyatakan batal demi hukum.
- d. Pelaku usaha wajib menyesuaikan klausula baku yang bertentangan dengan undang-undang ini.

Terkait dengan perlindungan pengguna APMK sebagai konsumen, hal ini diatur dalam Undang-Undang nomor 8 tahun 1999 tentang Perlindungan Konsumen (UU PK) yang secara garis besar telah memberikan perlindungan terhadap konsumen untuk menikmati produk yang mereka beli secara fair dan tidak menyesatkan. UU PK mengatur pelaku usaha perbankan untuk memberikan tanggung jawabnya kepada konsumen berupa :⁹⁶

1. Beritikad baik dalam melakukan kegiatan usahanya;
2. Memberikan informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan jasa yang diberikannya;
3. Memperlakukan atau melayani konsumen secara benar jujur serta tidak diskriminatif;
4. Menjamin kegiatan usaha perbankan berdasarkan ketentuan standar perbankan yang berlaku.

Walaupun keberadaan UU PK telah memberikan posisi tawar menawar yang lebih kuat terhadap pelaku usaha. Namun berhubungan dengan pengguna APMK ini dalam sistem pembayaran elektronik (*e-payment*) UU PK tidak mengatur secara jelas mengenai bagaimana menyelenggarakan sebuah sistem elektronik andal dan aman dalam melindungi konsumen. Pengaturan terhadap penyelenggaraan sistem elektronik ini diatur lebih lanjut pada UU ITE. Namun peraturan yang terdapa pada UU PK seperti ketentuan pencatuman masalah klausula baku

⁹⁶ Muhammad Djumhana. Hukum Perbankan di Indonesia. Citra Aditya. Bandung. 2006. Hlm 338.

dapat diterapkan pada perjanjian antara pemegang APMK dengan bank penerbit.

2.6.7 Aspek Hukum Perjanjian Dalam Sistem Pembayaran Elektronik Menggunakan Kartu

A. Asas-asas Perjanjian

Kontrak atau perjanjian adalah salah satu dari dua dasar hukum yang ada selain dari undang-undang yang dapat menimbulkan perikatan. Perikatan adalah suatu hubungan hukum yang mengikat satu atau lebih subjek hukum dengan kewajiban-kewajiban yang berkaitan satu sama lain. asas-asas yang mendasar dari suatu perjanjian antara lain :

- a. Asas konsensualisme : suatu perjanjian lahir manakala telah terjadi kesepakatan antara para pihak. Asas ini sangat erat hubungannya dengan prinsip kebebasan dalam mengadakan perjanjian.
- b. Asas kekuatan mengikat : terikatnya para pihak pada apa yang disepakati dalam perjanjian dan juga terhadap beberapa unsur lain sepanjang dikehendaki oleh para pihak adalah sama halnya dengan kekuatan mengikat undang-undang.
- c. Asas kepercayaan : seseorang yang mengadakan perjanjian dengan pihak yang lain harus dapat menumbuhkan kepercayaan di antara kedua belah pihak bahwa satu sama lain akan memenuhi prestasinya di kemudian hari. Tanpa adanya kepercayaan, maka perjanjian itu tidak mungkin akan diadakan oleh para pihak. Dengan kepercayaan ini kedua belah pihak mengikatkan dirinya kepada perjanjian yang telah mempunyai kekuatan mengikat sebagai undang-undang.
- d. Asas persamaan hak : asas ini menempatkan para pihak dalam persamaan derajat, tidak ada perbedaan, masing-masing pihak

wajib melihat adanya persamaan ini dan mengharuskan kedua belah pihak untuk menghormati satu sama lain.

- e. Asas keseimbangan : asas ini menghendaki kedua belah pihak untuk memenuhi dan melaksanakan perjanjian. Asas ini merupakan kelanjutan dari asas persamaan. Kreditur mempunyai kekuatan untuk menuntut pelunasan prestasi melalui kekayaan debitur. namun kreditur memikul pula beban untuk melaksanakan perjanjian itu dengan itikad baik. Dengan demikian kedudukan kreditur yang kuat juga diimbangi dengan kewajiban untuk memperhatikan itikad baik melaksanakan segala kewajibannya, sehingga kedudukan debitur dan kreditur seimbang.
- f. Asas moral : Asas ini sangat nampak dalam perikatan wajar, dimana suatu perbuatan sukarela dari seorang tidak menimbulkan hak baginya untuk menuntut kontraprestasi dari pihak debitur. Adapun faktor-faktor yang memberi motivasi pada yang bersangkutan untuk melakukan perbuatan hukum adalah berdasarkan pada aspek kesusilaan (moral) sebagai panggilan dari hati nuraninya.
- g. Asas kepatutan : asas ini dituangkan dalam pasasl 1339 KUH Perdata yang berhubungan dengan isi perjanjian, di mana titik beratnya adalah mengenai aspek keadilan dalam masyarakat.
- h. Asas kebiasaan : suatu perjanjian tidak hanya mengikat untuk hal-hal yang diatur secara tegas akan tetapi juga hal-hal yang dalam keadaan dan kebiasaan yang lazim diikuti.
- i. Asas kepastian hukum : perjanjian sebagai suatu figur hukum harus mengandung kepastian hukum. Kepastian ini terungkap dari kekuatan mengikatnya perjanjian tersebut, yaitu undang-undang bagi para pihak.
- j. Asas kebebasan berkontrak : setiap orang bebas untuk mengadakan perjanjian apa saja asas tidak bertentangan dengan undang-undang, ketertiban umum dan kesusilaan.

Dalam kegiatan pembayaran melalui sistem elektronik ada dua pelaksanaan perjanjian yang dilakukan oleh pemegang kartu, yaitu antara penerbit dan penyelenggara sistem elektronik. Untuk melihat hal ini kita perlu melihat lebih dalam pengertian dari perjanjian itu sendiri. Pengertian dasar dari perjanjian dalam penerapan hukum di Indonesia dapat kita jumpai pada pasal 1313 KUH Perdata yang mengatakan bahwa perjanjian adalah suatu perbuatan yang dilakukan oleh satu orang atau lebih mengikatkan dirinya terhadap satu orang lain atau lebih.

Pasal 1320 KUH Perdata menyatakan untuk sahnya perjanjian diperlukan empat syarat, yaitu :

a. Kesepakatan mereka yang mengikatkan diri

Kata sepakat dalam suatu perjanjian merupakan suatu keadaan yang menunjukkan kehendak kedua belah pihak lawannya dengan tiada kesesatan atau kekeliruan, paksaan atau penipuan. Menurut pasal 1321 KUH Perdata “tiada sepakat yang sah apabila sepakat itu diberikan karena kekhilafan, atau diperolehnya dengan paksaan atau penipuan” dengan adanya kata sepakat maka perjanjian itu telah ada, mengikat kedua belah pihak dan dapat dilaksanakan. Dalam UU ITE kata sepakat dalam transaksi elektronik diatur pada pasal 20 ayat (1) dan (2).⁹⁷

b. Kecakapan untuk membuat suatu perikatan

Menurut Pasal 1329 KUH Perdata bahwa “Setiap orang adalah cakap untuk membuat perikatan-perikatan, jika ia oleh undang-undang tidak dinyatakan tidak cakap”. Menurut ketentuan hukum yang berlaku (Pasal 1330 KUH Perdata), bahwa semua orang cakap (berwenang) membuat perjanjian kecuali mereka

⁹⁷ Lihat pasal 20 ayat (1) dan (2) UU ITE. (1) kecuali ditentukan lain oleh para pihak, transaksi elektronik terjadi pada saat penawaran transaksi yang dikirim pengirim telah diterima dan disetujui penerima; (2) persetujuan atas penawaran transaksi elektronik sebagaimana dimaksud pada ayat (1) harus dilakukan dengan pernyataan penerimaan secara elektronik.

yang tergolong sebagai (1) Orang yang belum dewasa; dan (2) Orang yang ditempatkan dibawah pengampuan.

c. Suatu hal tertentu

Suatu hal tertentu dalam perjanjian adalah barang yang menjadi objek perjanjian. Jadi suatu perjanjian haruslah mempunyai objek tertentu. Beberapa persyaratan ditentukan dalam KUH Perdata terhadap obyek tertentu dari suatu perjanjian, khususnya jika obyek kontrak tersebut berupa barang sebagai berikut :

- 1) Benda yang merupakan obyek kontrak tersebut haruslah barang yang dapat diperdagangkan (Pasal 1332);
- 2) Pada saat kontrak dibuat, minimal barang tersebut sudah dapat ditentukan jenisnya (Pasal 1333 Ayat (1));
- 3) Jumlah barang tersebut boleh tidak tertentu, asal saja jumlah tersebut kemudian dapat ditentukan atau dihitung (Pasal 1333 Ayat (2));
- 4) Barang tersebut dapat juga barang yang baru akan ada dikemudian hari (Pasal 1334 Ayat (1));
- 5) Tetapi tidak dapat dibuat kontrak terhadap barang yang masih ada dalam warisan yang belum terbuka (Pasal 1334 Ayat (2)).

d. Suatu sebab yang halal

Suatu sebab yang halal merupakan syarat terakhir untuk sahnya suatu perjanjian. Menurut KUH Perdata Pasal 1335 disebutkan bahwa “suatu perjanjian tanpa sebab atau yang telah dibuat karena sesuatu sebab yang palsu atau terlarang, tidak mempunyai kekuatan”. Pengertian sebab yang halal menurut Pasal 1337 KUH Perdata, adalah :

- 1) Sebab yang tidak terlarang atau bertentangan dengan undang-undang

- 2) Sebab yang sesuai dengan kesusilaan
- 3) Sebab yang sesuai dengan ketertiban umum.

Mengenai syarat sahnya suatu perjanjian seperti yang tersebut dalam Pasal 1320 KUH Perdata dimana jika tidak dipenuhinya dua syarat pertama yaitu syarat sepakat antar kedua belah pihak dan kecakapan akan berakibat perjanjian dapat dibatalkan.

Pihak yang dapat meminta pembatalan itu adalah pihak yang tidak cakap atau pihak yang memberikan sepakatnya tidak secara bebas. Jadi perjanjian yang telah dibuat itu mengikat juga selama tidak dibatalkan atas permintaan pihak yang berhak meminta pembatalan tersebut. Dengan demikian nasib suatu perjanjian seperti itu tidaklah pasti dan tergantung pada kesediaan suatu pihak yang mentaatinya. Dua syarat pertama dalam Pasal 1320 KUH Perdata disebut syarat subyektif karena mengenai orang-orangnya atau subyeknya yang mengadakan perjanjian.

Sedangkan jika tidak dipenuhinya salah satu dari dua syarat terakhir dalam Pasal 1320 yaitu syarat suatu hal tertentu dan sebab yang halal maka perjanjian tersebut batal demi hukum. Artinya dari semula tidak pernah dilahirkan suatu perjanjian dan tidak pernah ada suatu perikatan. Tujuan para pihak yang mengadakan perjanjian tersebut untuk melahirkan suatu perikatan hukum adalah gagal. Dua syarat terakhir ini disebut syarat obyektif karena berkaitan langsung dengan obyek perjanjian.

B. Klausula Baku Pada Perjanjian Penerbitan Kartu Kredit

Dalam perjanjian penerbitan kartu kredit bentuk yang paling sering digunakan adalah bentuk perjanjian baku. Yaitu suatu perjanjian yang telah dibentuk sedemikian rupa atau distandarisasi oleh salah satu pihak saja. Dalam perjanjian baku ini proses negosiasi tidak dilakukan secara seimbang, perjanjian menjadi seperti sebuah form yang harus dilengkapi oleh pihak nasabah.

Dalam pasal 1 UU PK klausula baku disebutkan adalah setiap aturan atau ketentuan dan syarat-syarat yang telah dipersiapkan dan ditetapkan terlebih dahulu secara sepihak oleh pelaku usaha yang dituangkan dalam suatu dokumen dan/atau perjanjian yang mengikat dan wajib dipenuhi oleh konsumen.⁹⁸ Hal ini umumnya menyebabkan posisi tawar pihak konsumen di dalam kontrak-kontrak standar pada umumnya tidak lagi sama dengan pelaku usaha. Konsumen hanya dapat menerima atau menolak isi kontrak secara utuh atau secara keseluruhan (*take it or leave it*).

Walaupun isi dari klausula baku telah diatur dengan jelas pada pasal 18 UUPK, namun pada prakteknya di lapangan klausula baku ini tidak mencerminkan adanya keseimbangan antara pelaku usaha dan konsumen. Hal ini terlihat dari contoh Perjanjian Penerbitan Kartu Kredit Bank BCA (terlampir). Isi dari klausula baku perjanjian kartu kredit cenderung lebih memihak si pelaku usaha dalam hal ini bank penerbit yang telah menyusunnya, sehingga merugikan konsumen. Atas dasar ini maka diperlukan suatu penindakan yang tegas terhadap pelanggaran pencantuman klausula baku yang isinya bertentangan dengan pasal 18 UU PK.

⁹⁸ Indonesia. Undang-undang nomor 8 tahun 1999 tentang Perlindungan Konsumen. Pasal 1 angka 10.