Aman Transaksi Elektronik (SET) Protocol

Karena semakin banyak perusahaan yang memilih internet sebagai media untuk perdagangan elektronik, kepercayaan dan keamanan persyaratan meningkat. Persyaratan keamanan penting untuk transaksi e-commerce yang sukses disajikan pada tabel 1.

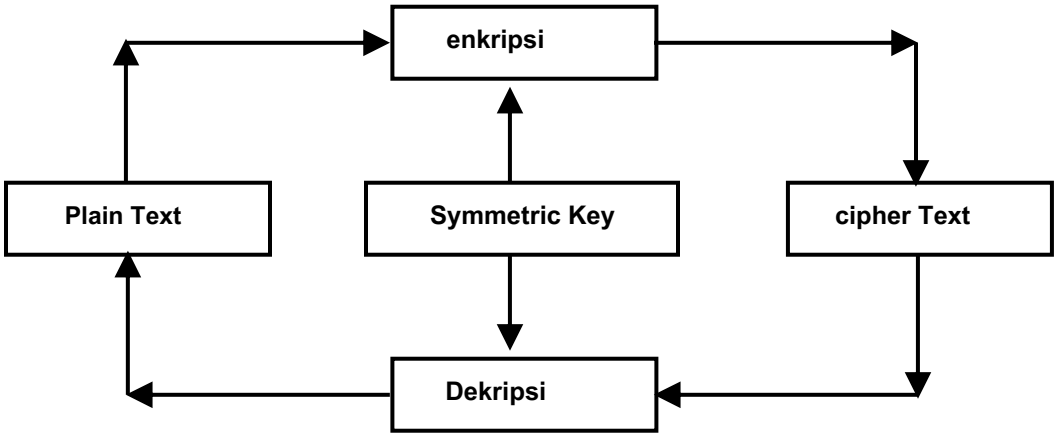
TABEL 1: PENTING KEAMANAN PERSYARATAN

KEBUTUHAN	DESKRIPSI
Pribadi	**Informasi dibagi di antara pihak-pihak yang berkomunikasi harus diketahui hanya kepada mereka. Semua orang lain harus terus keluar dari loop.**
pembuktian keaslian	**Kedua pihak berkomunikasi harus berada dalam posisi untuk membangun dan membuktikan identitas mereka.**
Integritas	**Pesan yang dikirimkan oleh pengirim tidak harus dirusak. Jika dirusak, penerima harus berada dalam posisi untuk mengidentifikasi yang sama dan membuang pesan.**
Non-Talak	**Kedua pihak berkomunikasi harus memiliki fasilitas untuk secara hukum membuktikan bahwa pesan telah dikirim dan diterima.**

H OW ADALAH INI PERSYARATAN KEAMANAN DICAPAI?

Keempat persyaratan keamanan utama yang dicapai dengan menggunakan teknik kriptografi. teknik kriptografi secara luas diklasifikasikan ke dalam teknik kriptografi kunci simetris dan teknik kriptografi asimetris kunci.

Dalam teknik kriptografi simetris kunci, kunci yang sama digunakan untuk enkripsi dan dekripsi. pengirim harus memiliki salinan kunci untuk enkripsi dan penerima harus memiliki salinan kunci untuk dekripsi. Gambar 1 menunjukkan bagaimana sebuah simetris karya enkripsi kunci.



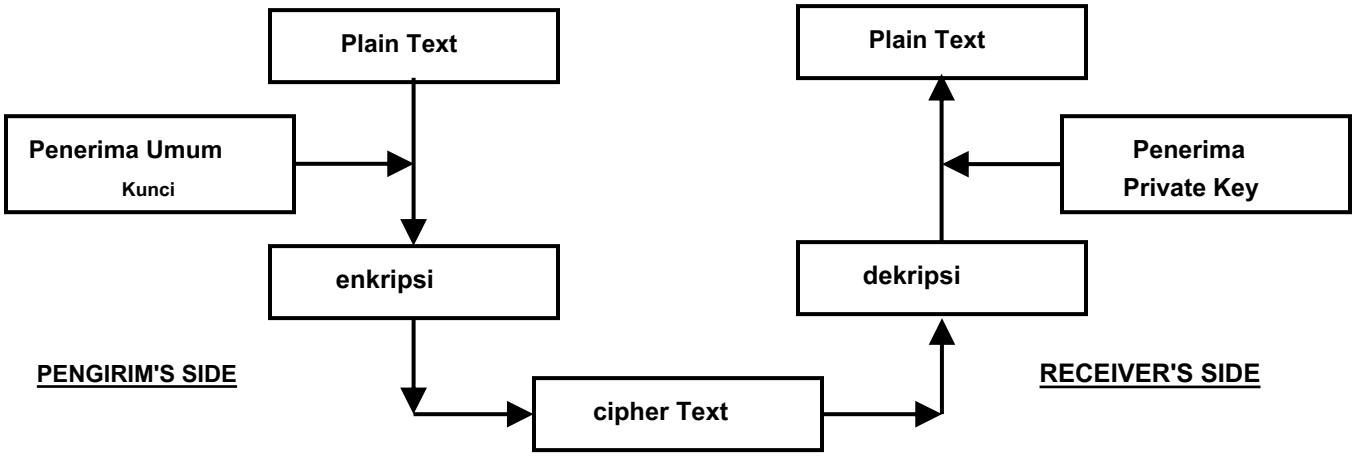
Gambar 1: Bekerja dari enkripsi simetris

teknik enkripsi kunci simetris yang efisien, cepat dan mengkonsumsi sumber daya komputer kurang dari prosesor dan memori. Namun, kelemahan utama mereka adalah:

1. **pengirim harus mengirimkan salinan kunci untuk penerima untuk dekripsi**
2. **Pengirim harus menggunakan kunci yang berbeda untuk pengguna yang berbeda dan**
3. **Hal ini tidak mungkin untuk menandatangani secara digital pesan.**
4. **Sulit untuk menegakkan non-penolakan untuk kedua berkomunikasi dengan pihak berbagi kunci yang sama.**

Data Encryption Standard (DES), Triple Data Encryption Standard (3DES) dan Advanced Encryption Standard (AES) adalah contoh yang baik dari algoritma enkripsi simetris.

Kekurangan dari metode enkripsi simetris diatasi dengan menggunakan teknik enkripsi kunci asimetris. Di sini, setiap pengguna memiliki sepasang kunci, kunci publik dan sebuah kunci pribadi. Kunci publik dari pengguna diketahui semua sementara kunci privat dirahasiakan. Setiap pesan yang dikirimkan dienkripsi menggunakan kunci publik dari penerima dan didekripsi menggunakan kunci pribadi penerima. Gambar 2 menunjukkan bagaimana sebuah asymmetric key karya sistem enkripsi.



Gambar 2: Bekerja dari Asymmetric Key Encryption System

Sedangkan kerugian dari simetris sistem enkripsi kunci diurus off, asimetris sistem enkripsi kunci lambat, tidak efisien dan mengkonsumsi sumber daya yang cukup komputer. RSA algoritma adalah contoh khas dari teknik enkripsi kunci asimetris.

TRANSACTION SECURITY PROTOCOLS

Untuk berhasil melaksanakan transaksi e-commerce, dua protokol diterima yang dikerahkan adalah:

a) Aman-Socket Layer (SSL) protokol
b) Aman Transaksi Elektronik (SET) protokol

SSL PROTOKOL

Netscape Inc awalnya dibuat Secure Sockets Layer (SSL) protokol. Pada rekening popularitas dan penerimaan, sekarang diterapkan di semua browser web.

SSL memiliki dua tujuan utama:

1. **Untuk menjamin kerahasiaan, dengan mengenkripsi data yang bergerak antara berkomunikasi pihak (klien dan server).**
2. **Untuk menyediakan otentikasi dari mitra sesi, menggunakan algoritma RSA.**

Protokol SSL terdiri dari dua protokol:

1. **SSL Handshake Protokol , Di mana berkomunikasi pihak (klien dan server) mengotentikasi diri dan menegosiasikan kunci enkripsi. Satu titik untuk dicatat di sini adalah bahwa SSL ada tambahan overhead yang signifikan dalam memulai sesi SSL.**

2. **SSL Rekam protokol , Di mana data sesi dipertukarkan antara pihak-pihak berkomunikasi (client dan server) dalam mode terenkripsi.**

Langkah-langkah sepuluh dalam transaksi SSL adalah:

1. **Klien pertama mengirimkan permintaan dengan memperkenalkan sendiri.**
2. **server mengakui.**
3. **server akan mengirimkan sertifikat kepada klien.**
4. **Pemeriksaan klien jika sertifikat dikeluarkan oleh Otoritas Sertifikat (CA) itu percaya.**
5. **Klien kemudian membandingkan informasi dalam sertifikat dengan Informasi itu hanya diterima mengenai situs.**
6. **Klien kemudian memberitahu server apa enkripsi algoritma yang akan digunakan.**
7. **Klien kemudian menghasilkan kunci sesi dengan menggunakan cipher setuju.**
8. **Klien kemudian mengenkripsi kunci sesi dengan menggunakan kunci publik server dan mengirimkannya ke server.**
9. **server menerima kunci sesi yang dienkripsi dan dekripsi dengan nya kunci pribadi.**
10. **Klien dan server kemudian menggunakan kunci sesi untuk sisa transaksi.**

Meskipun protokol SSL telah diterapkan di semua browser, ada dua risiko utama yang terkait dengan SSL.

Sebuah) pemegang kartu TIDAK dilindungi dari pedagang. Jika pedagang tidak jujur dan biaya lebih, pengguna akan kehilangan.

b) Demikian pula, pedagang juga tidak dilindungi dari pelanggan yang tidak jujur yang memasok nomor kartu kredit yang tidak valid.

Pendeknya,

- **SSL adalah protokol pesan aman, tidak protokol pembayaran**
- **SSL membutuhkan vendor untuk memiliki sertifikat**
- **protokol SSL tidak menyediakan fasilitas untuk non-penolakan.**

SSL diikuti oleh Transport Layer Security (TLS), yang merupakan Internet Engineering Task Force (IETF) versi SSL. TLS fungsi yang sangat mirip dengan SSL tetapi mereka tidak beroperasi.

IBM kemudian mengembangkan sebuah standar yang disebut Internet mengetik Pembayaran Protocol (IKP), yang menyebabkan perkembangan Aman Transaksi Elektronik Protocol (SET).

SECURE Electronic TRANSACTION (SET) PROTOKOL

Untuk melakukan transaksi berhasil dan tanpa mengorbankan keamanan dan kepercayaan, komunitas bisnis, lembaga keuangan dan perusahaan yang menawarkan solusi teknologi ingin sebuah protokol yang bekerja sangat mirip dengan cara bagaimana sebuah karya transaksi kartu kredit.

Visa dan MasterCard, memimpin perusahaan kartu kredit di dunia membentuk konsorsium dengan komputer vendor seperti IBM dan dikembangkan protokol terbuka yang muncul sebagai standar dalam menjamin keamanan, keaslian, privasi dan kepercayaan dalam transaksi elektronik.

SET Bisnis Requirements

Kebutuhan bisnis utama untuk SET adalah:

1. **Memberikan keamanan, keaslian, privasi, integritas dan kepercayaan sehubungan dengan pembayaran dan pemesanan informasi**
2. **Menyediakan otentikasi yang pemegang kartu adalah pengguna yang sah dari kartu kredit rekening**
3. **Menyediakan otentikasi yang pedagang dapat menerima transaksi kartu kredit.**
4. **Untuk merumuskan sebuah protokol yang memfasilitasi dan mendorong interoperabilitas antara perangkat lunak dan penyedia jaringan dan yang tidak tergantung pada mekanisme keamanan transportasi.**

PARTICIPANTS DARI SET SISTEM

The main participants of the SET system and their details are presented in table 2.

TABLE 2: MAIN PARTICIPANTS OF THE SET SYSTEM

PARTICIPANT	DETAILS
Cardholder	Refers to the person who holds the card and who makes the purchases on the Internet.
Merchant	A person or organization that has goods or services to sell to the cardholder.
Issuer	Refers to the financial institutions that provide the cardholder with the credit card and are responsible for the payment.
Acquirer	Refers to organizations that provide verbal or telephonic card authorization for merchants. Merchants pay a small fee to the acquirer for their services.
Acquirer Payment Gateway Acts as	an interface between SET and the computer networks of banks. To put it simpler terms, the acquirer payment gateway acts as a proxy for the bank's network functions.
Certifying Authority (CA)	Refers to the organization that provides public key certification. One of the best-known Certifying Authority (CA) is Verisign which offers several classes of certificates. Class 1 certificate is of the lowest level which binds e-mail address and associated public keys. Class 4 certificates are the highest level certificates that apply to servers and their organizations.

HOW SET WORKS?

The following is a simplified version of how SET works.

Before SET can work, there is a preliminary step which has to completed.

Preliminary Step : Both cardholders and merchants must register with the CA (certifying authority).

Actual Steps in SET

Step 1: Pelanggan menelusuri situs merchant, memutuskan apa yang harus membeli dan menambahkannya ke keranjang belanja.

Langkah 2: Pelanggan kemudian berkomunikasi dengan merchant dan gateway pembayaran dalam satu pesan. Pesan ini memiliki dua bagian:

Bagian: Purchase Order untuk digunakan oleh pedagang Bagian b: Informasi kartu untuk digunakan oleh bank merchant

Langkah 3: Merchant meneruskan informasi kartu (bagian b) ke bank mereka

Langkah 4: kontak Bank pedagang emiten dan cek dengan penerbit untuk otorisasi pembayaran

Langkah 5: Emiten kewenangan pembelian dan mengirimkan otorisasi ke bank Merchant

Langkah 6: Bank pedagang mengirimkan salinan otorisasi kepada pedagang

Langkah 7: Merchant melengkapi pesanan dan mengirimkan konfirmasi kepada pelanggan

Langkah 8: Pedagang menangkap transaksi dari bank mereka

Langkah 9: Emiten mencetak faktur kartu kredit untuk pelanggan

Proses enkripsi di SET

Algoritma yang digunakan: 1024 bit algoritma RSA untuk proses enkripsi asimetris

56 bit algoritma DES untuk proses enkripsi simetris

SHA-1 untuk menghitung message digest.

Urutan langkah-langkah pengirim S mengadopsi dalam proses enkripsi adalah sebagai berikut:

Langkah 1: Pengirim S subyek pesan melalui algoritma hash. SET menggunakan Secure Hash Algorithm (SHA-1) untuk ini. Output dari algoritma hash adalah message digest.

Langkah 2: Pengirim S kemudian mengenkripsi pesan mencerna menggunakan RSA swasta kuncinya. Output dari langkah ini adalah Digital Signature.

Langkah 3: Pengirim S kemudian menciptakan kunci untuk enkripsi simetris.

Langkah 4: **Sender S mengambil pesan, tanda tangan digital yang diperoleh pada langkah 2 dan sertifikat digital dan mengenkripsi semua dari mereka menggunakan metode enkripsi kunci simetris dari Data Encryption Standard (DES). Hasil Langkah 4 adalah pesan terenkripsi.**

Langkah 4: **Pengirim S kemudian mengambil kunci publik dari penerima R. mengenkripsi kunci simetris dari langkah 3. Output disebut sebagai amplop digital.**

Pesan terenkripsi yang diperoleh dari langkah 4 dan amplop digital yang diperoleh dari langkah 5 dikirim ke R. penerima

Proses dekripsi di SET

Algoritma yang digunakan:

1024 bit algoritma RSA untuk proses enkripsi asimetris

56 bit algoritma DES untuk proses enkripsi simetris

SHA-1 untuk menghitung message digest.

Urutan langkah-langkah penerima R mengadopsi dalam proses dekripsi adalah sebagai berikut:

Langkah 1: **Receiver R mendekripsi amplop digital menggunakan RSA kunci pribadi untuk mendapatkan DES simetris kunci.**

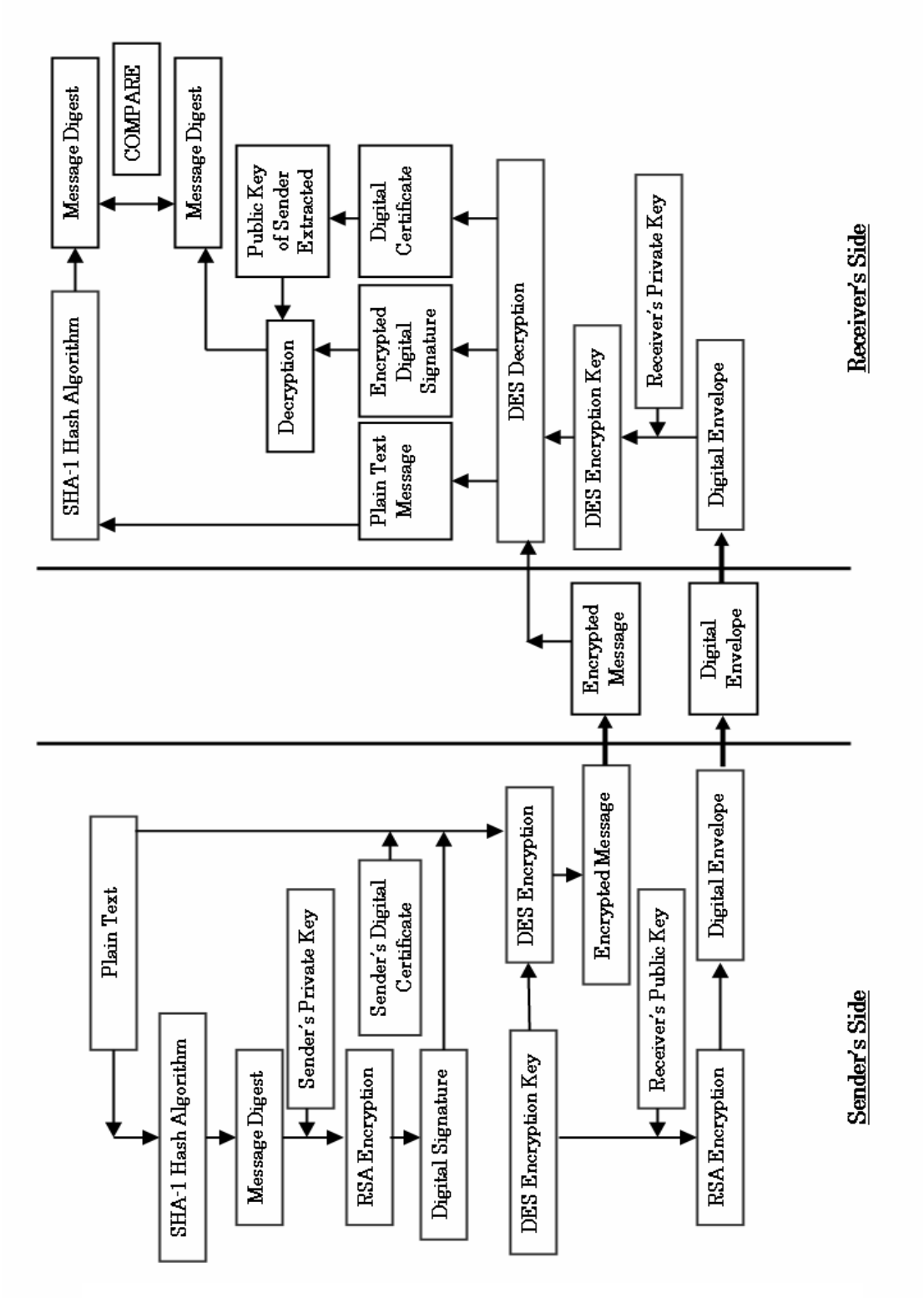
Langkah 2: **Menggunakan DES simetris kunci yang diperoleh dari langkah 1, penerima mendekripsi pesan terenkripsi untuk mendapatkan pesan teks biasa, tanda tangan digital dan sertifikat digital dari pengirim S.**

Langkah 3: **Receiver R kemudian ekstrak RSA kunci publik dari pengirim S dari sertifikat digital.**

Langkah 4: **Menggunakan RSA kunci publik pengirim S, pesan terenkripsi digest yang diperoleh dari langkah 3 didekripsi untuk mendapatkan pesan mencerna.**

Langkah 5: **Receiver R kemudian subyek pesan lagi melalui fungsi hash SHA-1. Sebuah message digest dengan demikian diperoleh. Pesan dihitung ini digest kemudian dibandingkan dengan pesan digest yang diperoleh dari langkah 4. Jika keduanya adalah sama, keaslian pengirim S dijamin.**

Gambar 3 menunjukkan enkripsi dan dekripsi proses.



Gambar 3: Enkripsi dan Dekripsi Proses

DUAL SIGNATURES

Seperti disebutkan sebelumnya, di SET, yang berkomunikasi pelanggan dengan merchant dan gateway pembayaran melalui pesan tunggal. Pesan ini memiliki dua bagian, bagian pesanan pembelian untuk digunakan oleh pedagang dan bagian informasi kartu untuk digunakan oleh bank merchant

pelanggan harus memastikan bahwa

1. pedagang tidak akan melihat melihat instruksi pembayaran
2. pengakuisisi tidak akan melihat instruksi agar

Hal ini juga diperlukan untuk menghubungkan pesanan dan pembayaran sehingga pelanggan dapat membuktikan bahwa pembayaran untuk urutan tertentu dan tidak untuk pesanan lainnya.

Hal ini dicapai dengan konsep baru yang diperkenalkan di SET dinamakan sebagai tanda tangan ganda.

HOW ADALAH DUAL TANDA TANGAN DICIPTAKAN?

Langkah-langkah berikut menjelaskan bagaimana tanda tangan ganda diciptakan.

Langkah 1: **Pelanggan mengambil Informasi Pembayaran (PI) data dan mata pelajaran yang sama melalui fungsi hash SHA-1. Dia mendapat Informasi Pembayaran Message Digest (PIMD).**

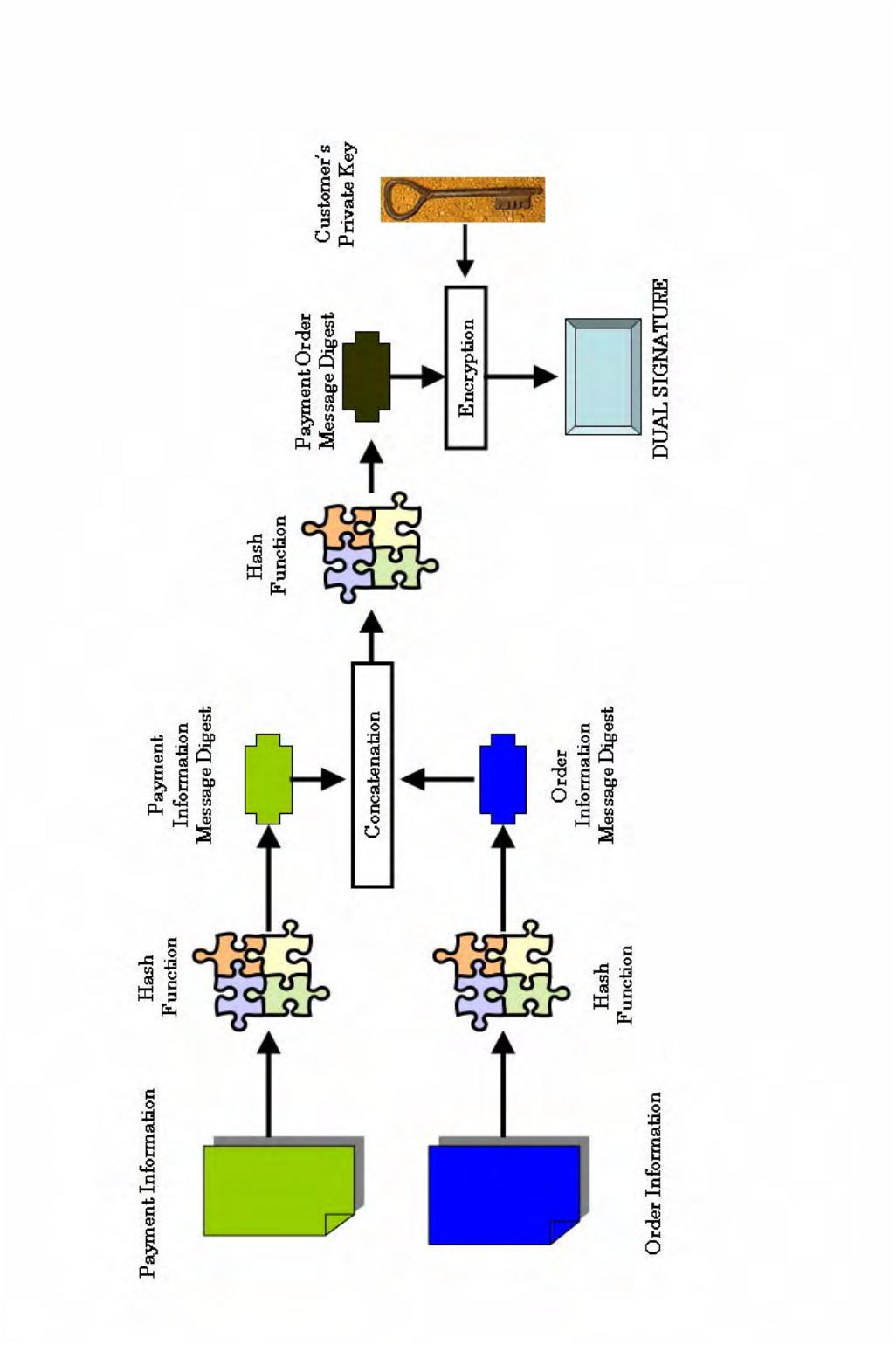
Langkah 2: **Pelanggan mengambil Informasi Order (OI) data dan mata pelajaran yang sama melalui fungsi hash SHA-1. Dia mendapat Informasi Pesanan Message Digest (OIMD).**

Langkah 3: **Kedua PIMD dan OIMD yang bersambung.**

Langkah 4: **Output bersambung ini lagi dikenakan melalui fungsi hash SHA-1. output disebut Pembayaran Orde Message Digest (POMD).**

Langkah 5: **POMD dienkripsi menggunakan RSA kunci pribadi dari pelanggan. Hasilnya adalah tanda tangan ganda.**

Gambar 4 menunjukkan bagaimana tanda tangan ganda diciptakan.



Gambar 4: Bagaimana Ganda Signatures diciptakan

H OW DUAL TANDA TANGAN MEMBANTU BANK?

Di sini juga, ada dua langkah, proses enkripsi dan proses dekripsi.

proses enkripsi

Algoritma yang digunakan: **1024 bit algoritma RSA untuk proses enkripsi asimetris**

56 bit algoritma DES untuk proses enkripsi simetris

SHA-1 untuk menghitung message digest.

Urutan langkah-langkah pelanggan C mengadopsi setelah tanda tangan ganda telah dibuat:

Langkah 1: **Pelanggan C menciptakan kunci untuk DES enkripsi simetris.**

Langkah 2: **Pelanggan C kemudian menggunakan metode enkripsi DES untuk mengenkripsi Payment Instruction (PI) pesan, tanda tangan ganda, sertifikat dan Informasi Orde Message Digest (OIMD). Hasilnya adalah pesan terenkripsi.**

Langkah 3: **Pelanggan C kemudian mengambil RSA kunci publik dari bank B. mengenkripsi DES simetris kunci dari langkah 1. Output disebut sebagai amplop digital.**

Pesan terenkripsi yang diperoleh dari langkah 2 dan amplop digital yang diperoleh dari langkah 3 dikirim ke bank B.

proses dekripsi

Algoritma yang digunakan: **1024 bit algoritma RSA untuk proses enkripsi asimetris**

56 bit algoritma DES untuk proses enkripsi simetris

SHA-1 untuk menghitung message digest.

Urutan langkah-langkah bank B mengadopsi setelah menerima pesan terenkripsi dan amplop digital adalah:

Langkah 1: **Bank B menggunakan RSA kunci pribadi untuk mendekripsi amplop digital untuk mendapatkan DES simetris kunci.**

Langkah 2: **Bank B kemudian menggunakan DES simetris kunci untuk mendekripsi bagian pertama dari pesan terenkripsi untuk mendapatkan Pembayaran Instruksi (PI) pesan, tanda tangan ganda, sertifikat pelanggan dan Informasi Pesanan Message Digest (OIMD).**

Langkah 3: **The bank B then subjects the Payment Instruction (PI) to the hash function SHA-1 to get the Payment Information Message Digest (PIMD).**

Step 4: **The bank concatenates the PIMD value and the OIMD and subjects the result again through the hash function SHA-1. The result is the Payment Order Message Digest (POMD).**

Step 5: **The bank then decrypts the second portion of the encrypted message which is the dual signature using the customer's public key (obtained from the digital certificate of the customer) and obtains a copy of the Payment Order Message Digest (POMD).**

Step 6: **The value of POMD obtained from steps 4 and 5 are compared. If they are same, then it is confirmed that the message has come from the customer.**

CERTIFICATES OF VARIOUS PARTICIPANTS

Sertifikat memainkan peran penting dalam SET untuk kepercayaan selalu dibangun di atas sertifikat.

Karena ada berbagai peserta dalam SET, masing-masing dari mereka memiliki sertifikat mereka sendiri. Tabel 3 memberikan rincian tentang sertifikat ini.

TABEL 3: PESERTA DAN RINCIAN SERTIFIKAT MEREKA

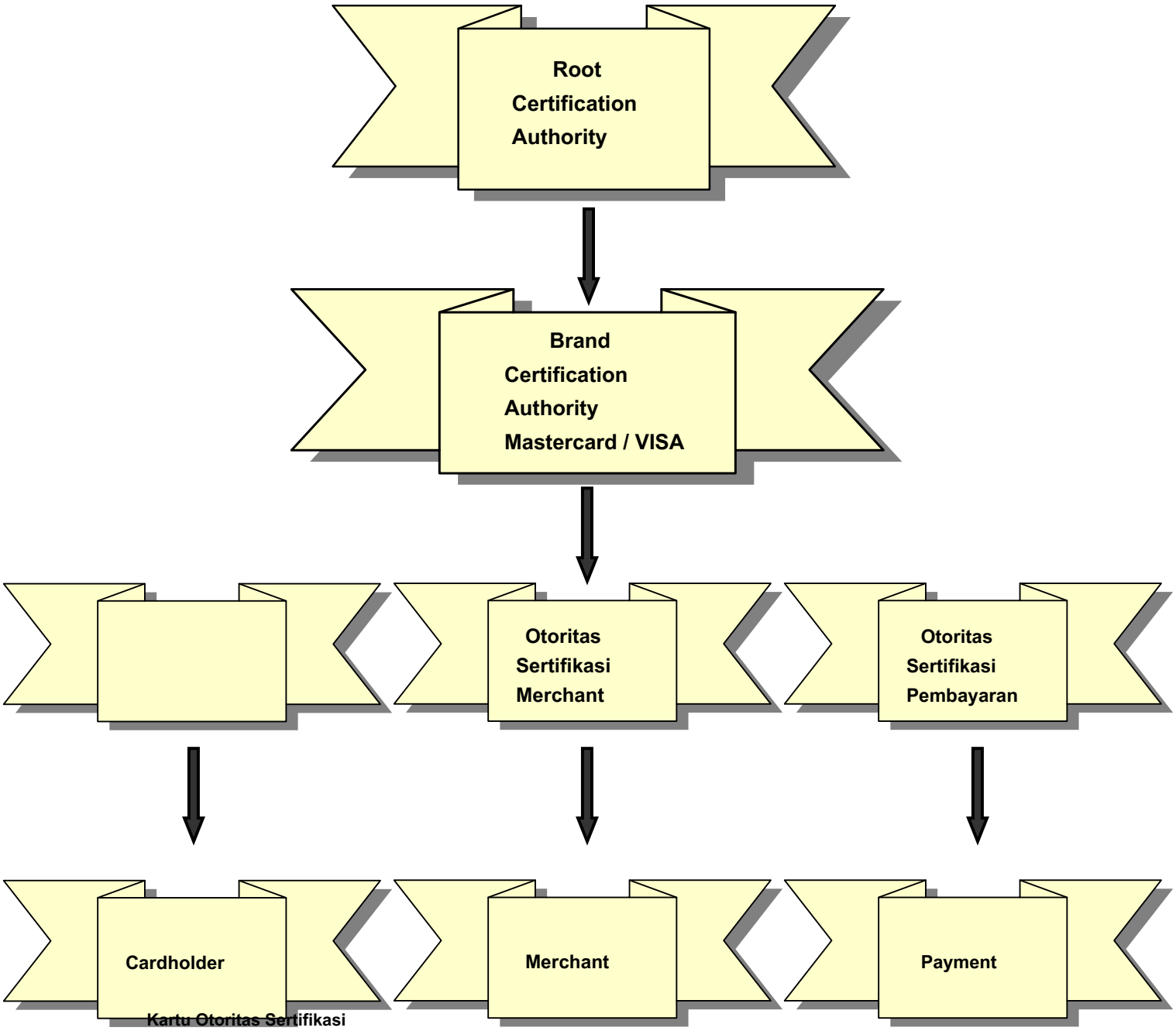
PESERTA	SERTIFIKAT RINCIAN
sertifikat pemegang kartu	Digunakan untuk memverifikasi bahwa pemegang kartu adalah orang asli. Ini digital ditandatangani oleh lembaga keuangan dan sertifikat tidak berisi nomor rekening dan tanggal kadaluarsa kartu
sertifikat pedagang	Ini secara digital ditandatangani oleh lembaga keuangan merchant dan memberikan jaminan bahwa pedagang memiliki perjanjian yang sah dengan pengakuisisi. Dalam SET, pedagang membutuhkan dua pasang kunci publik, satu untuk tanda tangan digital dan satu untuk mengenkripsi pertukaran kunci. Oleh karena itu akan membutuhkan dua sertifikat untuk setiap merek kartu pembayaran yang menerima.
Pembayaran Gateway Sertifikat	Gateway pembayaran memperoleh sertifikat nya dari acquirer mereka untuk sistem yang otorisasi proses.

HIERARCHY OF TRUST IN SET CERTIFICATES

Seperti Anda mungkin telah memperhatikan, semua peserta kebutuhan SET untuk memiliki sertifikat untuk operasi.

Sertifikat diciptakan oleh Sertifikasi Otoritas (CA) dan ada hirarki kepercayaan antara otoritas sertifikat SET.

Gambar 5 menunjukkan hirarki kepercayaan di antara SET CA.



Gambar 5: Hirarki kepercayaan di antara Sertifikasi SET Pihak berwenang. Pemegang

LIMITATIONS OF SET

1. **Despite being very secure, SET has not been a success in e-commerce environments. The reasons attributed are:**

2. **The overheads associated with SET are heavy. For a simple purchase transaction:**
   a. **Four messages are exchanged between the merchant and customer,**
   b. **Two messages are exchanged between the merchant and payment gateway,**
   c. **6 digital signatures are computed,**
   d. **There are 9 RSA encryption/decryption cycles,**
   e. **There are 4 DES encryption/decryption cycles and**
   f. **Four certificate verifications**

3. **It has been argued by merchants that they have to expend lot of money in order to process SET transactions. From consumer's point of view, they have to install appropriate software.**

4. **Inter-operability problem has not been solved.**

5. **With SET, while the payment information is secure, order information is not secure.**