Public Key Infrastructure dan Certificate Authority

Arrianto Mukti Wibowo
National University of Singapore, 2 Mei 2000
amwibowo@excite.com

Sedikit mengenai pembicara

- Peneliti e-commerce, terutama pada bidang "digital payment systems" dan "financial cryptography", kontinu sejak tahun 1995.
- Pengalaman kerja sejak 1986, menjadi pengajar/peneliti di Fakultas Ilmu Komputer UI 1997-2000
- Manager pelaksana riset "Digital Security & E-Commerce", Fasilkom UI 1998-1999: SET+Java+Smarcard, Digital signature law
- Menerima beasiswa S2 (research scholar) dari NUS, Dept.of Computer Science.

E-Commerce

- Booming sejak 1994-an, sebenarnya lebih tepat disebut: "Internet Commerce"
- *Commerce* → "Perniagaan" → secara intuisi dapat terpikirkan bahwa *commerce* lebih merupakan masalah hubungan ***antar-perusahaan***.
- Sifatnya secara umum ***external***, meskipun terkait dengan hal-hal intern perusahaan.

Masalah keamanan komunikasi

- Internet bukan jaringan yang aman. E-mail bisa disadap, dan diganti ditengah jalan.
- Informasi transaksi bisa dibaca orang lain dengan sangat mudah: tugas mahasiswa tk.3!
- Demikian pula untuk wireless network, harus ada pengamanan saluran komunikasi
- Lagipula… bukankah lebih baik tetap mengamankan komunikasi di private network (contoh: G - H)

Apa yang diamankan?

- Transaksi keuangan
- E-mail
- File transfer
- Tanda-tangan suatu kontrak dalam bentuk digital
- Informasi penting yang amat rahasia (baik bagi perusahaan maupun untuk negara)
- Transaksi bisnis lainnya

Pengorganisasian Presentasi

- Bab 2: Kriptografi sebagai dasar teknik pengamanan penting di Internet & wireless network
- Bab 3: Konsep Public Key Infrastructure (PKI) dan manajemennya
- Bab 4: Berbagai jenis "kepercayaan" dalam PKI
- Bab 5: Certificate Policy & Certificate Practice Statement
- Bab 6: Masalah-masalah seputar PKI
- Bab 7: Penutup

Bab II

Konsep Public Key Cryptography

Isu-isu sekurity

- privacy
- authenticity
- integrity
- non-repudiation

Kerahasiaan & Keutuhan

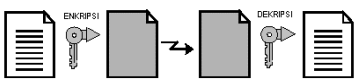
- ✓ Kerahasiaan (*confidentiality*)
  Apakah data-data transaksi tetap rahasia dari orang yang tidak berkepentingan?
- ✓ Keutuhan (*integrity*)
  Apakah transaksi bernilai Rp.10.000,- berubah menjadi Rp.10.000.000,-?

Keabsahan & Pembuktian

- ✓ Keabsahan (*authenticity*)
  Apa benar *ibu-dibyo@cybertickets.com* = Ibu Dibyo penjual karcis di Cikini?
  Apa pembeli tidak menggunakan identitas / kartu kredit orang lain?
- ✓ Pembuktian tak tersangkal (*non-repudiation*)
  Bagaimana pencatatan transaksi sebagai barang bukti tak tersangkal?

Symetric Cryptography

- Sebuah kunci yang dipakai bersama-sama oleh pengirim pesan dan penerima pesan



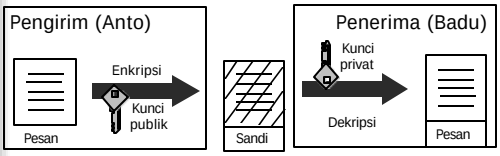
- Ada problem "pendistribusian kunci rahasia"

Public Key Cryptography

- Ada 2 kegunaan yang mendasar:
  - Menandatangani pesan
  - Mengirim surat rahasia dalam amplop yang tidak bisa dibuka orang lain
- Ada sepasang kunci untuk setiap orang (entitas):
  - kunci publik (didistribusikan kepada khalayak ramai / umum)
  - kunci privat (disimpan secara rahasia, hanya diketahui diri sendiri)

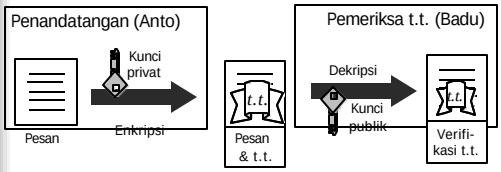
Membungkus pesan

- Semua orang bisa (Anto, Chandra, Deni) mengirim surat ke “Penerima” (Badu)
- Hanya “penerima” yang bisa membuka surat
- *(pada prakteknya tidak persis spt ini)*



Menandatangani pesan dgn public-key cryptography

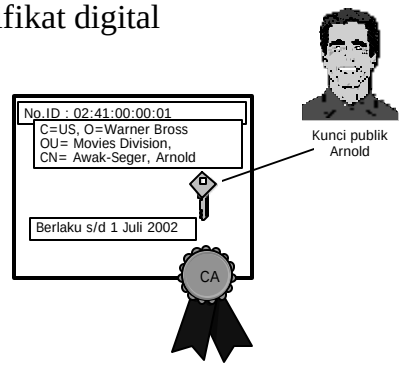
- Hanya pemilik kunci privat (penandatangan, Anto) saja yang bisa membuat tanda tangan digital
- Semua orang (Badu, Chandra, Deni) bisa memeriksa tanda tangan itu jika memiliki kunci publik Anto
- *(disederhanakan)*



Sifat tanda tangan digital:

- Otentik, dapat dijadikan barang bukti di peradilan
- hanya sah untuk dokumen (pesan) itu saja, atau kopinya. Dokumen berubah satu titik, tanda tangan jadi invalid!
- dapat diperiksa dengan mudah oleh siapapun, bahkan oleh orang yang belum pernah bertemu (dgn sertifikat digital tentunya)

Sertifikat digital

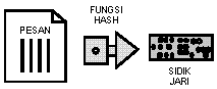


Keuntungan sertifikat digital

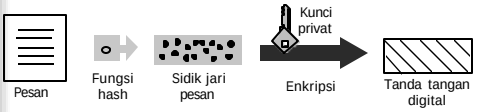
- bisa membuat “pipa komunikasi” tertutup antara 2 pihak
- bisa dipergunakan untuk mengotentikasi pihak lain di jaringan (mengenali jati dirinya)
- bisa dipakai untuk membuat dan memeriksa tanda tangan
- bisa dipakai untuk membuat surat izin “digital” untuk melakukan aktifitas tertentu, atau identitas digital
- bisa untuk off-line verification

Fungsi Hash

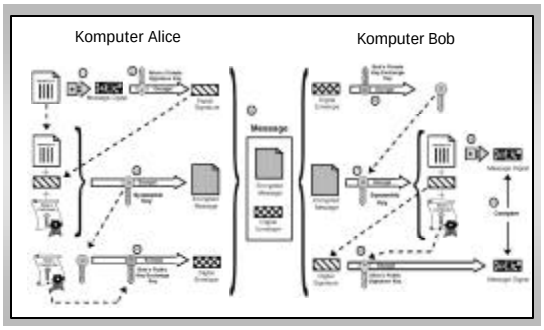
- Disebut juga sidik jari (*fingerprint*), *message integrity check,* atau *manipulation detection code*
- Untuk integrity-check
- Dokumen/pesan yang diubah 1 titik saja, sidik jarinya akan sangat berbada



Tanda tangan digital sebenarnya



Transaksi aman yang umum



Dipakai di mana?

- Browser, terutama dengan SSL
- SET (meskipun beberapa pilot project gagal. UI thn 1998-1999 pernah meneliti SET)
- Secure E-mail
- Document signing
- Secure communication di public network
- Secure wireless network
- Smartcard applications

Bab III

Konsep PKI & Manajemennya

Entitas PKI

- Certificate Authority
- Subscriber
- Registration Authority

Certificate Authority

- Yakni entitas yang namanya tertera sebagai “issuer” pada sebuah sertifikat digital
- Tidak harus pihak ketiga diluar organisasi sang subscriber. Misal: CA di sebuah perusahaan yang mengeluarkan digital ID buat pegawainya

Subscriber

- Entitas yang menggunakan sertifikat digital (diluar RA dan CA) sebagai “jati dirinya”
- Bisa juga berupa software, downloadable application atau mobile agent
- Memegang private key: harus dijaga baik-baik!
- PSE: personal security environment.
  - Smartcard
  - hard disk / disket (PKCS #5)

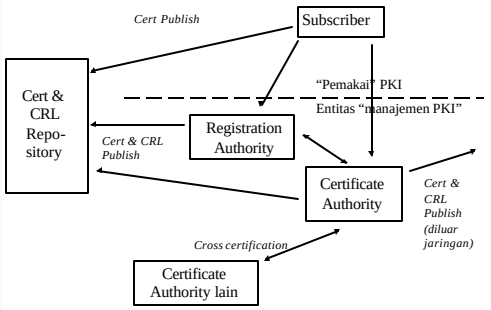
Registration Authority

- Menjalankan beberapa tugas RA, misalnya:
  - registrasi / physical authentication
  - key generation
  - key recovery
  - revocation reporting
- Sifatnya optional, dan skenario CA-RA bisa berbeda-beda tergantung situasi kondisi

Tingkat kepercayaan & keabsahan sertifikat

- Ada sertifikat yang gratisan. Hanya bisa dipakai untuk menunjukkan bahwa X adalah X. (Class 1)
- Ada sertifikat yang mahal sekali (ribuan dollar). Harus menunjukkan akta perusahaan dan harus diaudit. Secara fisik, harus hadir di CA utk mendaftar. (Class 4)
- Kesimpulan: level sertifikat menunjukkan “trustworthiness” dari suatu entitas

Diagram Entitas PKI



PKI Management Requirement

- Mengikuti standar ISO 9594-8 (kemudian menjadi ITU X.509, lalu RFC 2459 dkk)
- Ada teknik untuk mengupdate key-pair
- PKI bukan tirai besi: faktor kerahasiaan dalam PKI diminimalisir
- Bisa pakai banyak jenis algoritma: RSA, DSA, El-Gamal, Schnoor, MD5, SHA1, DES, RC4…
- Key generation oleh subscriber diperkenankan
- Ketiga entitas PKI, bisa mempublish sertifikat mereka
- CRL harus ada

lanjutan...

- Bisa menggunakan berbagai macam protokol: mail, HTTP, TCP/IP
- CA adalah “Maha Dewa” yang menentukan diisukannya sebuah sertifikat. Jadi bisa seorang subscriber minta sertifikat dengan “hak” tinggi, tapi hanya diberi “hak” rendah, karena sebenarnya sang subscriber memang tidak berhak setinggi itu.
- Harus ada mekanisme untuk pergantian kunci, kalau CA dibobol.
- Fungsi RA boleh dikerjakan oleh CA, tetapi dari sudut pandang subscriber, tetap saja harus nampak sama.

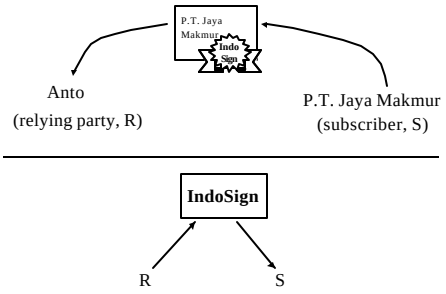
Certificate Revocation List

- Misalnya kalau seorang credit cardholder (dgn sertifikat digital), ternyata tidak pernah membayar tagihan bulanan, maka issuer bisa memasukkan sertifikat cardholder itu ke dalam CRL
- Kalau verifikasi off-line, bisa saja, tapi data tidak yang terbaru. Jadi pakai kalkulasi risk-management.

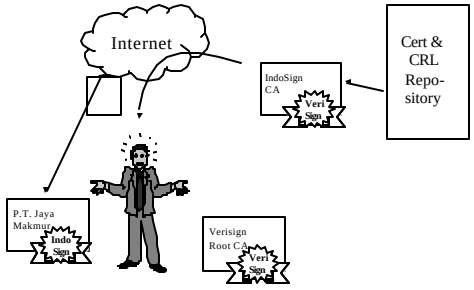
Bab IV

Trust Model

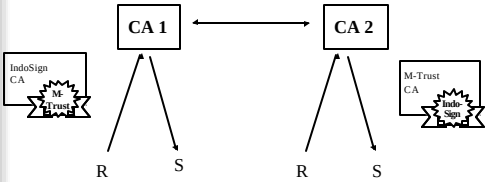
Relying Party



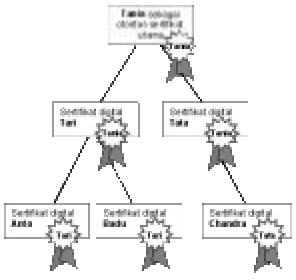
Certification Path



Direct Cross-Certification

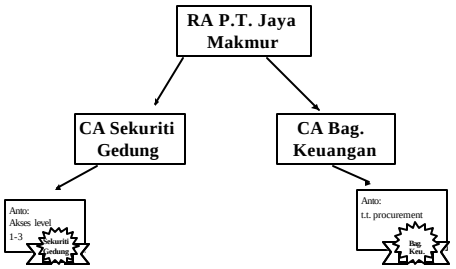


Hirarkis

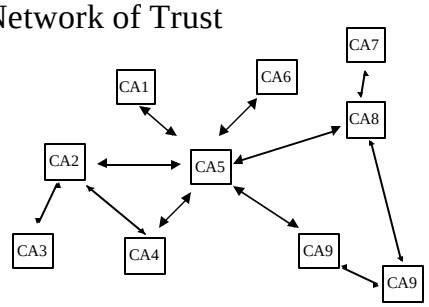


- Root CA: CA yang menandatangni sertifikat CA yang lain
- Sertifikat root CA: self-sign
- Distribusi sertifikat Root CA biasanya di luar network

Hub Authenticity



Network of Trust



Pada prakteknya, hanya bisa untuk limited certification path

Bab V

Certificate Policy & Certificate Practice Statement

Certificate Policy

- Tiap sertifikat bisa memiliki beberapa kegunaan
- Bisa juga, ada jenis sertifikat yang hanya bisa dipergunakan untuk maksud tertentu
- Bisa juga ada CA khusus untuk setiap jenis kepentingan.
- Misalnya (lihat hub authority)

Contoh policy (1)

- Kalau kita lihat pada browser MS-IE, kita dapat melihat bahwa setiap sertifikat memiliki izin kegunaan tertentu (policy tertentu):
  - server authentication
  - client authentication
  - signing e-mail (untuk tanda tangan saja)
  - membuat secure channel (pipa komunikasi aman)
  - menandatangani software, agar tidak bisa dikutak-katik
  - timestamping
- Berhubungan erat dengan level “kekuatan”, “kepercayaan” terhadap sertifikat digital (spt telah disebut di atas)

Contoh policy (2)

- CA-IATA hendak membuat policy CA untuk *airliners.* IATA bisa membuat 2 macam policy
- Policy ke-1: General Purpose
  Sertifikat yang policy-nya “berlabel” “General Purpose” hanya bisa dipergunakan untuk e-mail reguler, stempel tiket pesawat digital, keperluan delivery forms internal, dll.
- Policy ke-2: Commercial-Grade
  Sedangkan yang label policy-nya “Commercial-Grade” dipergunakan untuk transaksi finansial dgn bank, atau untuk membuat perjanjian kerjasama antar-airliners.

Certification Practice Statement

- Merupakan statement tertulis yang menjelaskan secara detial bagaimana CA ybs menjalankan prakteknya (registrasi, penerbitan, pencabutan, dll)
- CPS bisa juga berupa kontrak antara CA-subscriber
- Bisa juga merupakan dokumen komposit yang terdiri dari hukum publik, kontrak CA-subscriber, atau deklarasi dari CA
- Sebaiknya mengikuti standar praktek / konvensi

Hal-hal penting dlm CPS

- Hak dan kewajiban: CA, RA, subscriber, relying party, repository
- Tanggung jawab kemungkinan kerugian (mis: akibat hacking)
- Masalah keamanan CA
- Biaya
- Masalah audit: siapa yang mengaudit? Frekuensinya? Yang diperiksa apa?
- Masalah kerahasiaan data subscriber (kalau ada: misalnya hasil audit keuangan subscriber)
- Masalah hak atas nama domain atau nama perusahaan
- Interpretasi statement

Bab VI

Masalah-masalah lain seputar PKI

Browser: MS & NS

- Meskipun sertifikat digital bisa dipakai untuk berbagai macam kepentingan…
- Realitanya: pemanfaat sertifikat digital jadi penting setelah adanya protokol SSL
- Yang paling banyak menggunakan protokol SSL adalah on-line transaction dengan browser dari Netscape (NS) dan Microsoft (MS)
- Jadi realitanya: yang paling untung adalah CA-CA yang berhasil memasukkan root certificatenya ke dalam browser NS dan MS

Yang beruntung…

- American Bankers Association Inc.
- ANX Network (by DST)
- Certisign Certificadora Digital Ltda. (Brazil)
- Deutch Telekom AG (Jerman)
- Digital Signature Trust / DST / Zions First National Bank (Amerika)
- Entrust (Amerika)
- Equifax (Amerika)
- GTE Cybertrust (Amerika), sekarang dimiliki Baltimore
- Keywitness (Kanada)
- National Retail Federation (by DST)
- TC TrustCenter (Jerman)
- Thawte (Afrika Selatan), sekarang dimiliki Verisign
- Verisign (Amerika)

Apa hubungannya dengan kita?

- Masalah PKI dan CA lebih condong ke masalah “kepercayaan” ketimbang masalah teknis.
- Kalau CA-CA di Indonesia rentan KKN, maka pihak MS maupun NS (meskipun sekarang sudah open source), mereka akan pikir-pikir banyak sebelum memasukkan serfikat root CA dari Indonesia ke browser mereka.
- Bisa pula, kita memasukkan sertifikat root CA Indonesia secara manual, cuma tak berguna

Masih sekitar browser

- Jenis certification path apa yang disupport oleh MS dan NS? Apakah mereka telah mengikuti sepenuhnya pada standar X.509v3?
- Mengapa WISekey root CA-nya tidak ada di situ?
- Bagaimana "teknik" agar Indonesia bisa "masuk" ke dalam 2 broser terkenal itu?
- Tapi ingat: PKI & CA bukan cuma untuk browser!

Who holds the key?

- Jadi siapa yang berhak mendirikan PKI dan jadi CA?
- Lihat ke dompet Anda. Ada berapa kartu identitas?
- Jadi sebenarnya siapa saja yang memiliki kewenangan mengeluarkan identitas, (seharusnya) boleh mengeluarkan sertifikat digital

Masalah Legislasi

- Menurut hemat saya pribadi, sebaiknya dibuat hukum yang berlapis-lapis.
- Misalnya: hukum yang paling atas adalah hukum tanda tangan digital (digital signature law): "menyatakan bahwa tanda tangan digital dapat menjadi alat bukti yang sah, dll."
- Kerangkanya sudah ada (dulu dari riset Pusilkom UI & FH-UI)
- Tapi mekanisme detialnya (yang kadang-kadang suka berubah), sebaiknya dalam tingkat perundangan yang lebih rendah.

Masalah Key Recovery

- Bagaimana kalau kunci privat subscriber hilang? (misalnya smartcardnya hilang atau hard disknya kena virus)
- Harus ada mekanisme agar kunci privat bisa didapatkan kembal dari CA
- Tapi jaminan apa dari CA bahwa CA tidak akan menyalahgunakan kunci privat sang subscriber yang "disimpan" di CA?

Masalah Key Escrow

- Strong encryption bisa dimanfaatkan untuk membuat jaringan komunikasi bawah tanah untuk kejahatan!
- Bagaimana cara pemerintah memantau (menyadap) saluran komunikasi?
- Karena sekarang sudah sulit, maka ada beberapa cara:
  - kunci privat dipecah jadi 3, diserahkan ke polisi, hakim, dan CA
  - kunci privat diserahkan seluruhnya ke CA
  - hanya boleh pakai weak encryption
  - kalau tidak mau menyerahkan kunci privat (apapun alasannya) akan dipenjara

Contoh subscriber licik

- Anto menendatangani kontrak bisnis dengan Badu.
- Anto kemudian dengan sengaja menghilangkan kunci privatnya
- Kemudian Anto mengklaim kepada CA bahwa ada orang lain yang mencuri kunci privatnya. Akibatnya, membatalkan secara sepihak kontrak dengan Badu (padahal Antolah yang licik)
- Bagiamana hukumnya? Bagaimana pembuktiannya?

Penutup

Resource on-line

- Situs Informasi Electronic Commerce Indonesia:
  http://www.geocities.com/amwibowo/resource.html
- Mencakup seluruh hasil penelitian/tulisan kami, termasuk kerangka hukum untuk digital signature.

Saran tambahan

- Sebaiknya kalau hendak membuat hukum tentang digital signature, PKI dan CA, melibatkan orang dari berbagai aspek: teknis, bisnis dan hukum.
- Banyak bolong-bolong pada digital signature law, adalah karena “oversimplification” policy makers.
- Di sisi lain, amat mustahil orang teknis saja yang membuat policy PKI.
- Jika salah satu tidak ada, akan banyak bolongnya. Jadi sangat perlu teamwork yang solid.

Sumber Penulisan

- Trust Management in PKI, Tim Moses
- RFC 2510, 2527, 2459
- www.digsigtrust.com
- www.opengroup.org
- www.cybertrust.com
- www.iseto.ch
- www.baltimore.com
- www.wisekey.com
  www.eto.ch
- www.setco.org
- www.geocities.com/amwibowo/resource.html
- “Applied Cryptography , 2nd ed, Bruce Schneier, 1996