Nama : Ichsanul Aulia

NRP : 05111840007001

Keamanan Informasi Jaringan – A

Distribusi dari *Public Key*

Pendistribusian *Public Key* dapat dilakukan dengan 4 cara

Public Announcement

Pendistribusian *Public Key* ini diumumkan secara luas kepada masyarakat melalui saluran komunikasi yang dapat diakses oleh semua orang , tujuan utamanya adalah memastikan bahwa setiap orang memiliki akses ke *Public Key* yang relevan. Informasi *Public Key* dapat disebarkan melalui media massa, situs web, sosial media, atau platform komunikasi lainnya. Dengan pengumuman publik, semua orang dapat mengetahui *Public Key* dan menggunakannya untuk mengirim pesan terenkripsi kepada pemilik kunci privat yang sesuai

- Keuntungan
  Informasi dari *Public Key* dapat diakses secara mudah, pendistribusian metode ini relatif lebih murah
- Kekurangan
  Public Key dapat diakses oleh pihak yang tidak bertanggungjawab dengan mudah, bisa dimanipulasi oleh pihak yang tidak bertanggungjawab

Publicly Available Directory

Pendistribusian *Public Key* dengan cara menyimpan di sebuah direktori publik yang dapat diakses oleh semua orang agar berfungsi sebagai tempat sentral untuk menyimpan dan mencari *Public Key* dari berbagai pengguna. Dengan mencari di direktori ini, pengirim pesan dapat menemukan *Public Key* penerima dan menggunakan *Public Key* tersebut untuk mengenkripsi pesan. Direktori ini dapat berupa database online, server terpusat, atau sumber daya yang dapat diakses melalui protokol tertentu.

- Keuntungan
  Kemudahan akses pengguna, yang bisa mencari dan menggunakan Public Key yang diinginkan , Direktori dapat diperbaharui

- Kekurangan
  Data pemilik Public Key mungkin untuk dimanipulasi (tergantung keamanan dari direktoruy), Jika direktory tidak bisa diakses, maka penggunaan dan pencarian Public Key akan terganggu

Public-Key Authority

Pendistribusian *Public Key* dengan melibatkan lembaga ataupun organisasi yang mengelola dan mendistribusikan *Public Key*. Lembaga atau organisasi ini bertanggung jawab untuk memverifikasi data dari pemilik *Public Key* dengan tujuan

menyediakan *Public Key* yang dapat dipercaya kepada pihak-pihak yang membutuhkan

- Keuntungan
  Tingkat kepercayaan untuk penggunaan menjadi tinggi dikarenakan dikeluarkan oleh lembaga ataupun organisasi yang berwenang
- Kekurangan
  Ketergantungan kepercayaan, jika ada masalah maka satu atau beberapa *Public Key* akan juga terpengaruh, Proses verifikasi data yang diperlukan dapat memakan waktu

Public-Key Certificates

Pendistribusian *Public Key* dengan melibatkan penggunaan sertifikat *Public Key* yang dikeluarkan oleh *Certification Authority (CA)* atau lembaga sertifikasi yang terpercaya. Sertifikat ini berisi informasi tentang pemilik kunci publik dan ditandatangani oleh *CA* untuk memverifikasi keasliannya

- Keuntungan
  Menyediakan lapisan keamanan tambahan dikarenakan dikeluarkan oleh *Certification Authority ,* Dapat diverifikasi keasliannya dengan mengecek *Digital Signature* dari sertifikat yang dikeluarkan oleh *Certification Authority*

- Kekurangan
  Memerlukan upaya dan sumber daya yang lebih besar dibandingkan metode lainnya.

Digital Certificates

Juga dikenal sebagai sertifikat digital atau sertifikat *SSL/TLS*, adalah dokumen elektronik yang digunakan untuk mengautentikasi dan memverifikasi identitas pihak yang terlibat dalam komunikasi atau transaksi online. Digunakan untuk menjaga keamanan dan privasi informasi dalam lingkungan digital.

Digital certificates beroperasi berdasarkan teknologi kunci publik (*public key infrastructure*/*PKI*), yang melibatkan pasangan kunci kriptografi, yaitu kunci publik dan kunci pribadi. Kunci publik digunakan untuk mengenkripsi data, sedangkan kunci pribadi digunakan untuk mendekripsi data yang telah dienkripsi menggunakan kunci publik. Kunci publik ini dimasukkan ke dalam digital certificates untuk mengidentifikasi dan memverifikasi pemilik sertifikat.

Isi-isi dari sertifikat digital

- Nama Pemilik
  Sertifikat mencantumkan nama lengkap atau entitas pemilik sertifikat, yang dapat berupa individu, organisasi, atau entitas lainnya.

- Informasi Identitas

  Sertifikat mencakup informasi identitas yang membedakan pemilik sertifikat, seperti alamat email, nomor identitas, atau informasi lainnya yang relevan.
- *Public Key* (Kunci Publik)

  Sertifikat mengandung kunci publik pemilik sertifikat. Kunci publik ini digunakan oleh pihak lain untuk memverifikasi tanda tangan digital atau mengenkripsi pesan yang hanya dapat didekripsi oleh kunci privat yang sesuai.
- Tanda Tangan Digital

  Sertifikat digital memiliki tanda tangan digital yang ditambahkan oleh pihak yang menerbitkan sertifikat (*Certification Authority* atau *CA*). Tanda tangan ini memastikan integritas dan otentikasi sertifikat, sehingga penerima sertifikat dapat memverifikasi keasliannya.
- Periode Validitas

  Mencakup tanggal mulai dan berakhirnya validitas sertifikat. Setelah melewati tanggal berakhir, sertifikat tidak lagi dianggap valid.
- Informasi *CA*

  Sertifikat berisi informasi tentang *Certification Authority* yang menerbitkan sertifikat, termasuk nama *CA*, nomor seri sertifikat, dan tanda tangan *CA*.
- Sertifikat Induk (*Root Certificate*):

  Beberapa sertifikat digital juga mencantumkan sertifikat induk atau root certificate yang digunakan sebagai titik awal dalam rantai kepercayaan PKI. *Root certificate* ini merupakan sertifikat yang dipercaya secara global dan digunakan untuk memverifikasi tanda tangan digital pada sertifikat lainnya.

Proses penerbitan sertifikat digital melibatkan otoritas sertifikat (*certification authority/CA*), yang merupakan entitas tepercaya yang mengeluarkan dan mengelola sertifikat digital. *CA* secara independen memverifikasi identitas pihak yang meminta sertifikat dan menandatanganinya dengan kunci pribadi *CA* yang tepercaya. Tindakan ini memvalidasi bahwa sertifikat yang diterbitkan adalah otentik dan tidak dapat dimanipulasi. Sertifikat digital sering digunakan dalam beberapa konteks, termasuk:

- Keamanan Protokol Komunikasi

  Sertifikat digital digunakan dalam protokol keamanan seperti SSL/TLS untuk mengamankan komunikasi antara server web dan klien. Mereka memastikan bahwa koneksi aman dan melindungi informasi sensitif seperti data pribadi, kata sandi, dan transaksi keuangan dari akses yang tidak sah atau perubahan.
- Verifikasi Identitas

  Sertifikat digital memverifikasi identitas pihak yang terlibat dalam transaksi online. Ketika pengguna mengunjungi situs web yang menggunakan sertifikat digital, klien akan memverifikasi keabsahan sertifikat tersebut dengan menggunakan kunci publik *CA*. Ini membantu pengguna untuk memastikan bahwa mereka berkomunikasi dengan entitas yang sebenarnya dan bukan dengan pihak yang berusaha melakukan penipuan.
- Tanda Tangan Digital

  Sertifikat digital juga digunakan untuk membuat tanda tangan digital yang sah. Tanda tangan digital adalah mekanisme yang digunakan untuk memverifikasi

integritas dan otentikasi dokumen elektronik. Dengan menggunakan sertifikat digital, tanda tangan digital dapat diasosiasikan dengan identitas individu atau organisasi tertentu dan memastikan bahwa dokumen tidak berubah setelah ditandatangani.