TIS13534P KOMUNIKASI DAN KEAMANAN DATA

Minggu 6 - Autentifikasi

Daftar Menu:

- Definisi Autentifikasi
- Kegunaan Autentifikasi
- Jenis Autentifikasi
- Faktor Autentifikasi

Definisi Autentifikasi

-> Autentifikasi, berasal dari kata Yunani: *authenthikos* yang berarti “asli”. Dan *authentes* yang berarti “author”/pembuat/pengarang.

-> Autentifikasi adalah sebuah proses mengonfirmasi kebenaran atribut dari sebuah data yang diklaim benar oleh sebuah entitas

Analogi Sederhana

- Ketika kita ingin jalan-jalan ke luar negeri, kita akan mengalami 2 proses autentifikasi:
  - Imigrasi dalam negeri
  - Imigrasi luar negeri
- Petugas imigrasi ini akan memastikan bahwa baik dokumen maupun orang yang akan pergi adalah benar-benar orang tersebut.

Analogi Sederhana

Atribut yang diperika oleh petugas imigrasi:
-> Foto
-> Nama
-> Nomor Paspor
-> Negara Asal
-> Tanggal Kadaluarsa Paspor

Jika atribut sudah benar, maka orang tersebut diizinkan pergi. Jika tidak petugas berhak menolak orang tersebut.

Autentifikasi Analog

- Autentifikasi yang ada di benda-benda fisik, untuk mengecek kebenaran atau keasliannya diperlukan orang yang ahli atau dokumen yang mendukung.
- Contoh: Paspor, Stiker, dan lain-lain

Autentifikasi Digital

- Sesuai dengan namanya, autentifikasi ini bekerja di dunia digital. Proses autentifikasinya bisa berupa pengecekan Password, kode One Time Pad, kode checksum hash, dan lain-lain.
- Contoh yang disebutkan merupakan benda yang unik, dan tidak sama satu dengan yang lain.

Otentifikasi Password

- Sebuah proses autentifikasi yang sudah sangat umum digunakan di manapun. Di dunia digital, password digunakan sebagai kunci pembuka data/akun media sosial.
- Kekuatan password tergantung oleh:
  - Panjang Password
  - Variasi Password
- Namun ini lemah dengan Sniffer, Tamper

Contoh Password

- Password Lemah:
  - topisaya
- Password Sedang:
  - TopiSaya8854
- Password Kuat:
  - TDP8%TDPzfwi*4FEj2zG

Otentifikasi Checksum

- Proses ini melakukan pengecekan bahwa file yang didapat adalah 100% mirip tanpa ada perubahan. Jika ada perubahan, maka checksum akan berubah 100%.
- Contoh:
  - MD5Sum: TOPI: bdc17201a70f92e5aa97df6990f3c937
  - MD5Sum: TOPi: a68abe80627a27ff3da1caa56a071cef

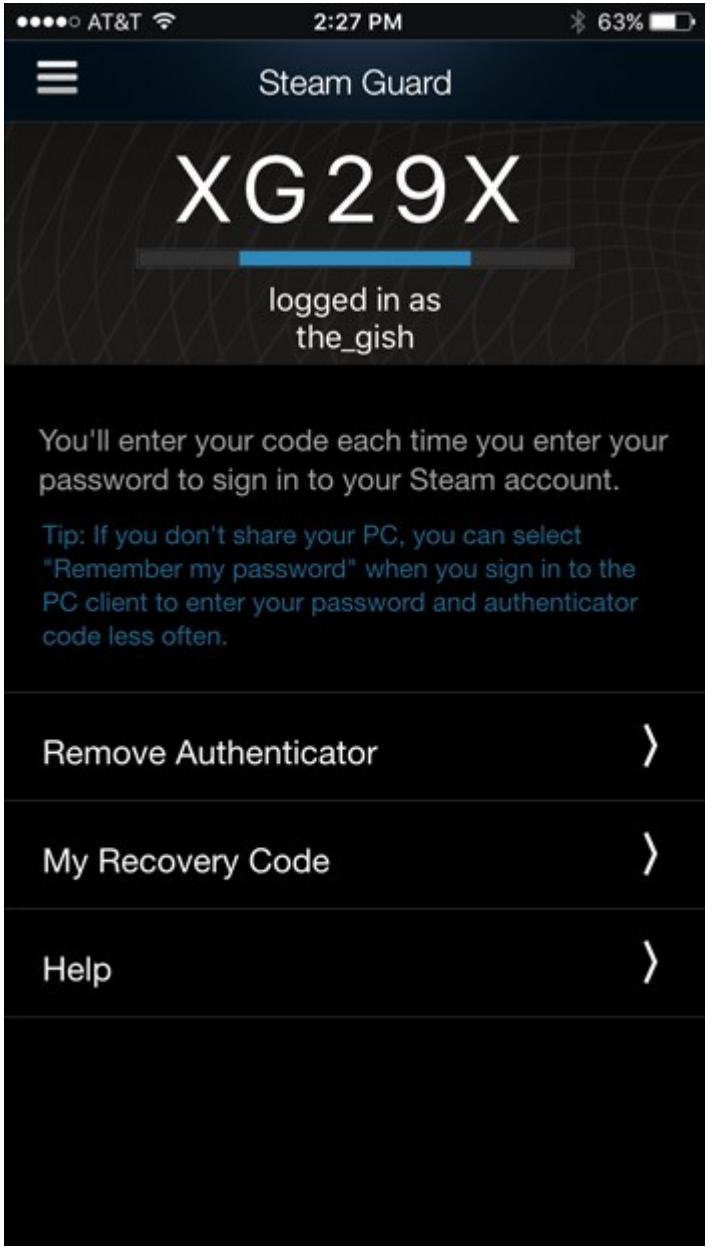
Algoritma Checksum

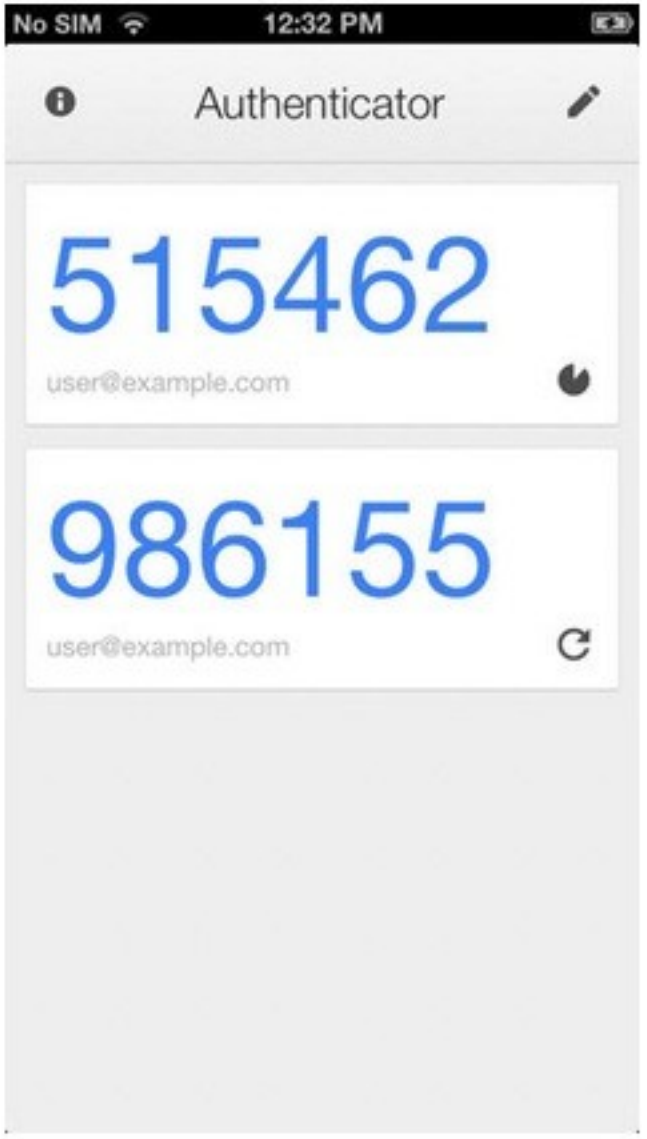
- MD5Sum
- SHA1
- SHA256
- SHA3
- SysV Checksum
- BSD Checksum

Otentifikasi One-Time Pad

- Sebuah kode yang digunakan untuk membantu proses autentifikasi. Kodenya dibuat acak per menit, sehingga kuat dan tidak mudah dipecahkan
- Biasanya digunakan di sistem Two-Factor Mechanism. Dan kode hanya bisa digunakan sekali
- Contoh: Steam Guard, Microsoft Authentificator

Contoh App


AT&T
2:27 PM
63%
Steam Guard
XG29X
logged in as
the_gish
You'll enter your code each time you enter your password to sign in to your Steam account.
Tip: If you don't share your PC, you can select "Remember my password" when you sign in to the PC client to enter your password and authenticator code less often.
Remove Authenticator
My Recovery Code
Help


No SIM
12:32 PM
Authenticator
515462
user@example.com
986155
user@example.com

Jenis-jenis Autentifikasi

- Jenis 1
  - Autentifikasi ini memerlukan orang pertama yang credible yang memiliki/merasakan/melihat bukti bahwa objek tersebut asli.
  - Jika objeknya adalah benda/seni, yang bisa membuktikannya adalah teman, keluarga, atau kolega.

Jenis-jenis Autentifikasi

- Jenis 2
  - Proses autentifikasi ini membandingkan sebuah objek dengan bukti/tanda khusus mengenai benda asalnya.
  - Contoh: Lukisan yang dicek kesamaannya dalam lokasi, bentuk tanda khas (signature), gaya melukis.

Jenis-jenis Autentifikasi

- Jenis 3
  - Jenis ini memerlukan bantuan luar seperti dokumen atau konfirmator eksternal lainnya.

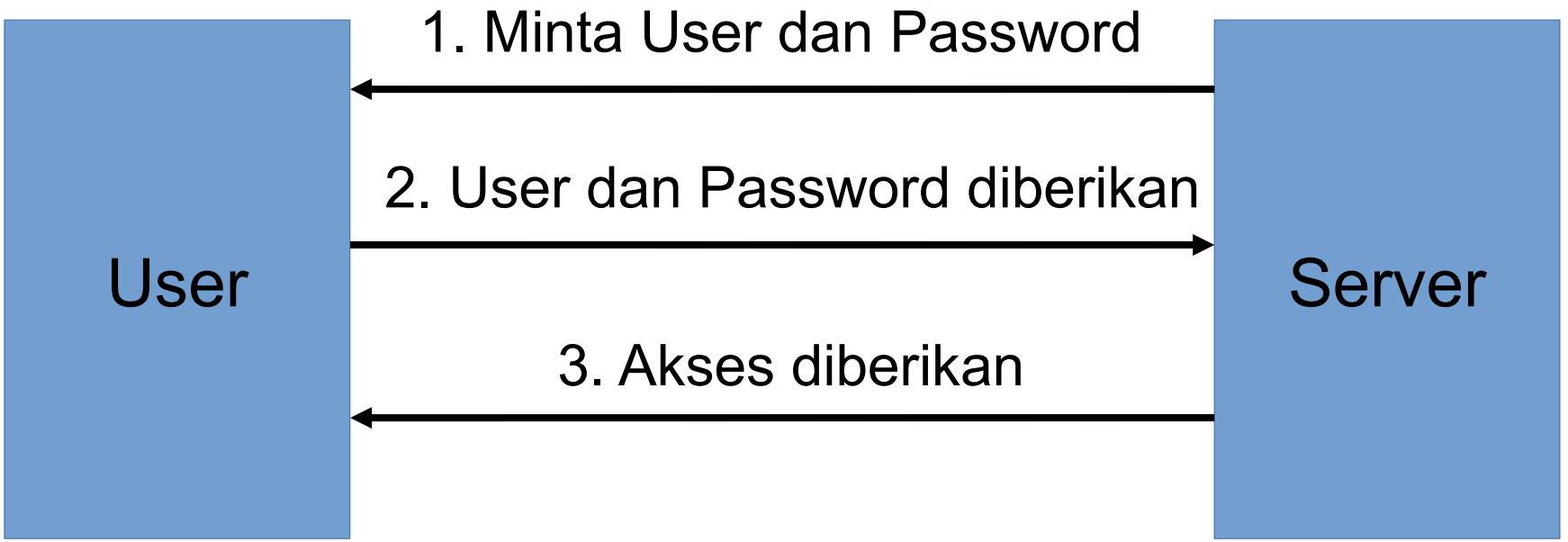
Faktor Autentifikasi

- Faktor di sini merujuk ke berapa banyak lapisan autentifikasi yang harus dilewati entitas/orang untuk mendapatkan aksesnya.
- Ada:
  - Single-Factor Authentication
  - Two-Factor Authentication
  - Multi-Factor Authentication
  - Strong Authentication
  - Continuous Authentication

Single-Factor Authentication

- Proses autentifikasi di sini hanya memerlukan satu faktor saja untuk masuk ke dalam sistem. Dan sistem ini paling banyak digunakan dibanding sistem lainnya.
- Login e-mail, login media sosial, PIN ATM

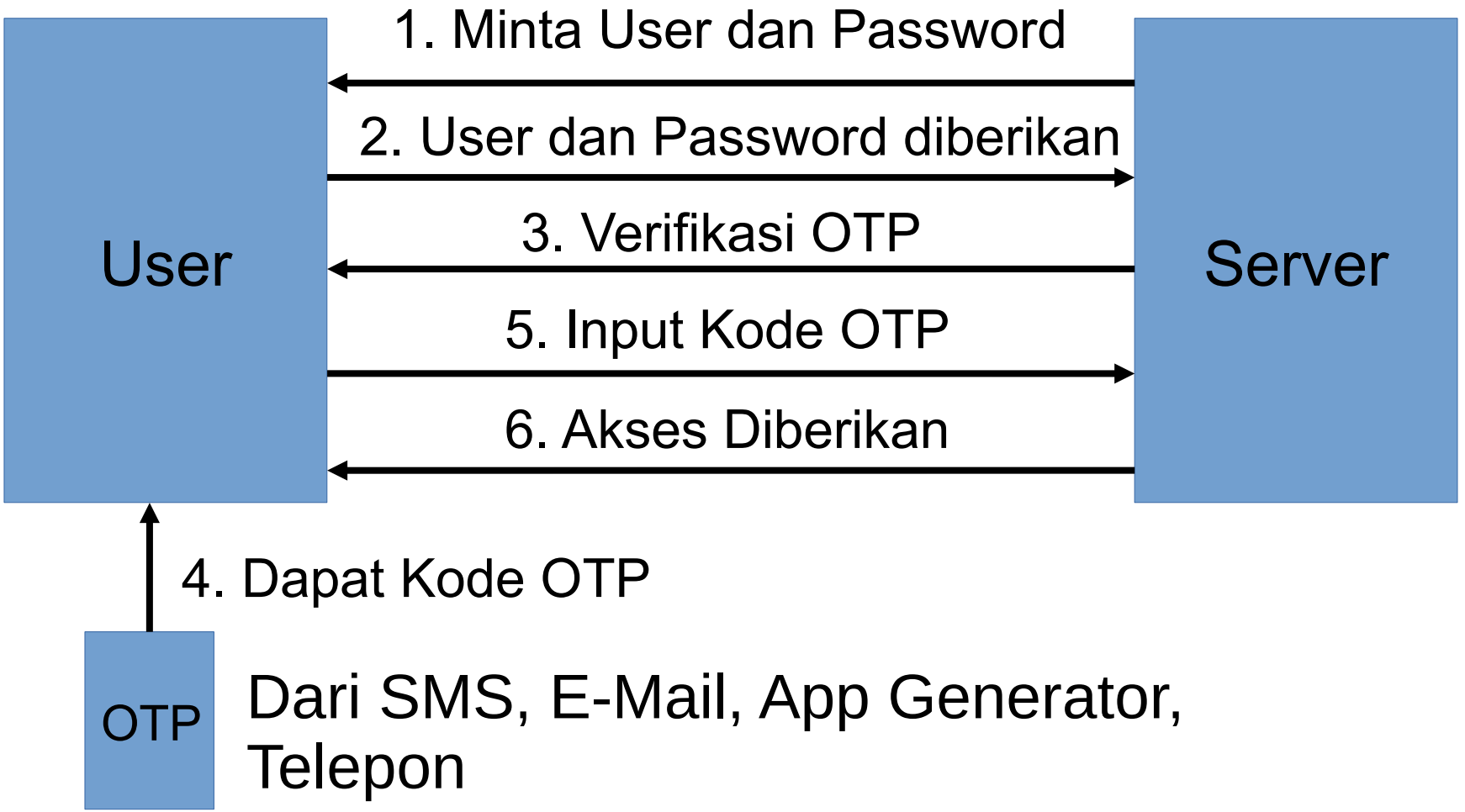
Ilustrasi


1. Minta User dan Password
2. User dan Password diberikan
3. Akses diberikan
User
Server

Two-Factor Authentication

- Proses autentifikasi di sistem ini memerlukan 2 faktor yang harus diberikan untuk masuk ke dalam sistem. Faktor kedua akan diminta jika faktor pertama diberikan.
- Kode bisa diberikan melalui:
  - SMS, Kode App, E-Mail, Telepon.
- Steam Guard, Google Authenticator

Ilustrasi


1. Minta User dan Password
2. User dan Password diberikan
3. Verifikasi OTP
5. Input Kode OTP
6. Akses Diberikan
User
Server
4. Dapat Kode OTP
OTP
Dari SMS, E-Mail, App Generator, Telepon

RADIUS

-> Singkatan dari Remote Authentication Dial In User Service

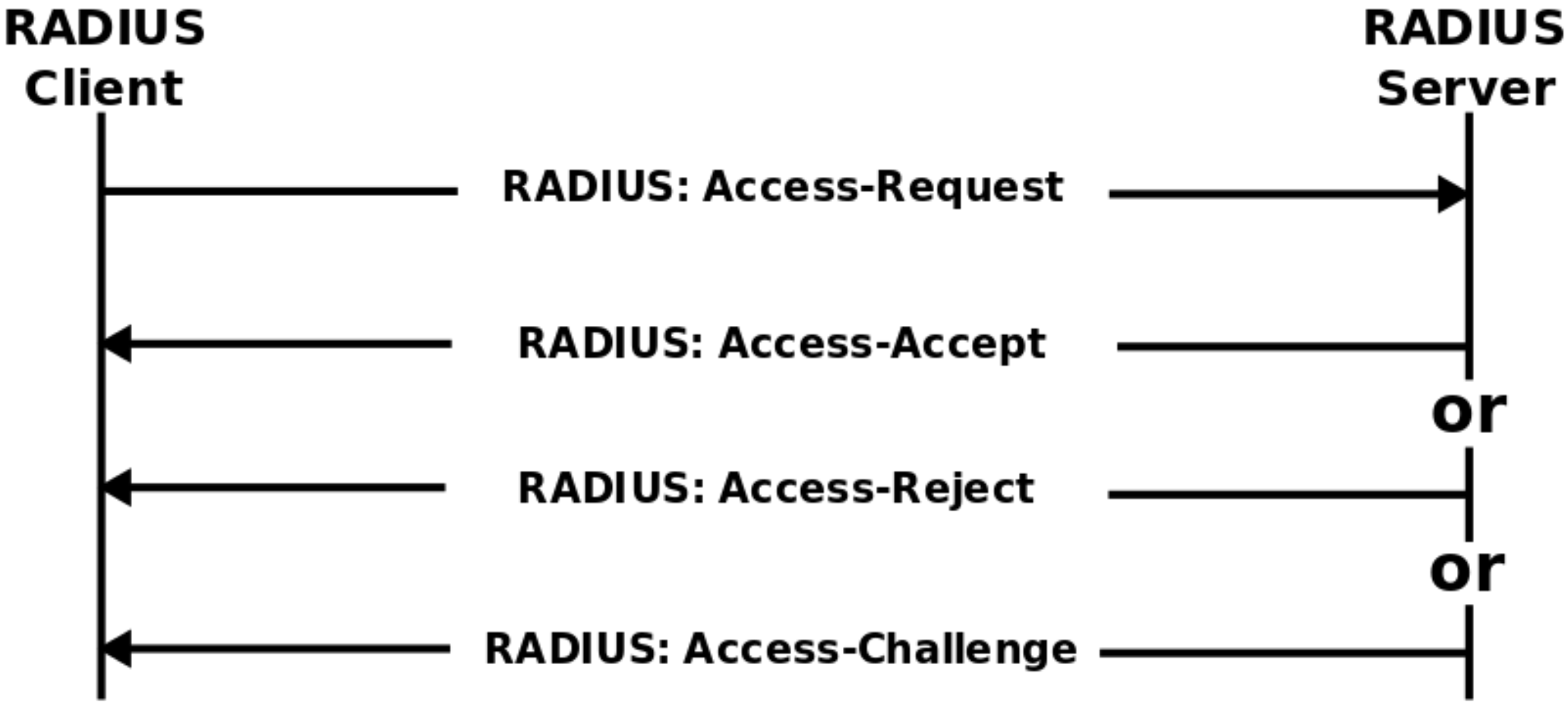
-> Sebuah protokol jaringan yang berguna sebagai Authentication, Authorizing, dan Accounting (Triple A/AAA)

-> Sering digunakan di Internet Service Provider dan Enterprise untuk mengatur jaringan

RADIUS

- RADIUS sendiri adalah protokol klien/server yang berjalan di lapisan aplikasi (OSI Model), dan bisa menggunakan TCP atau UDP sebagai media.
- Server Pengakses Jaringan (gateway) yang mengontrol akses ke jaringan, biasanya memiliki komponen klien RADIUS, yang dapat berkomunikasi dengan server RADIUS

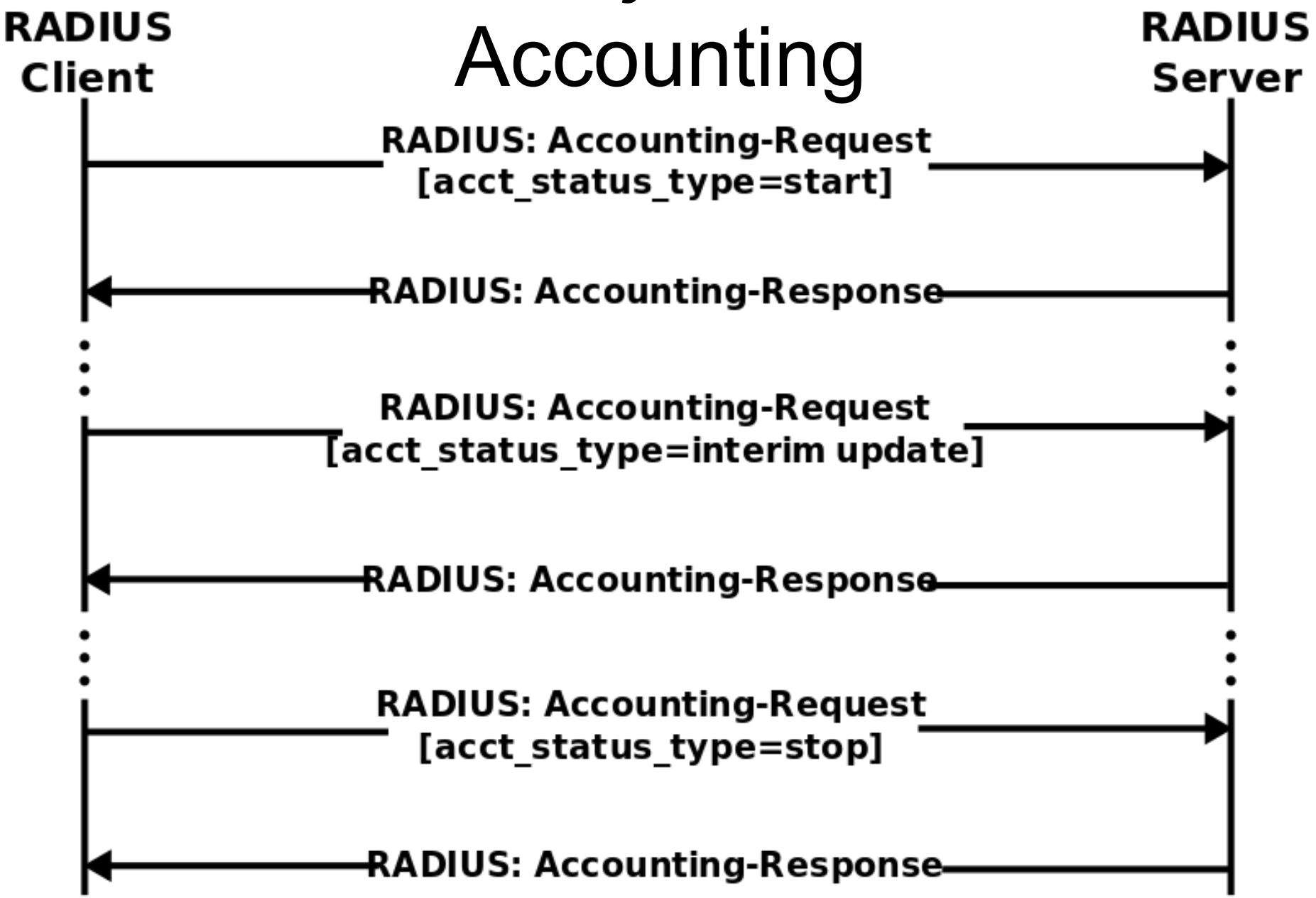
Cara Kerja RADIUS Authentication dan Authorizing



Penjelasan

- Setiap jawaban dari Server RADIUS, server akan memberikan tiga jenis respons
  - Alasan ketika autentikasi gagal
  - Permintaan Input jika ada keamanan 2 lapis
  - Pesan Selamat Datang jika berhasil

Cara Kerja RADIUS Accounting



Penjelasan

Dalam accounting RADIUS, ada tiga tahap yang harus dikerjakan oleh klien dan server:

1. Accounting-Request(acct_status_type=start)
2. Accounting-Request(acct_status_type=interim_update)
3. Accounting-Request(acct_status_type=stop)

Yang berarti: **Mulai Sesi, Update Sesi, Akhiri Sesi**.

Keamanan RADIUS

- RADIUS mentransmisikan password yang rumit menggunakan *shared secret* dan Algoritma Hashing MD5.
- Karena dinilai lemah, kemanan tambahan seperti Terowongan IPSec atau Jaringan Data Center Fisik harus digunakan untuk melindungi lalu lintas RADIUS dengan Server Pengakses Jaringan, dan RADIUS Server.

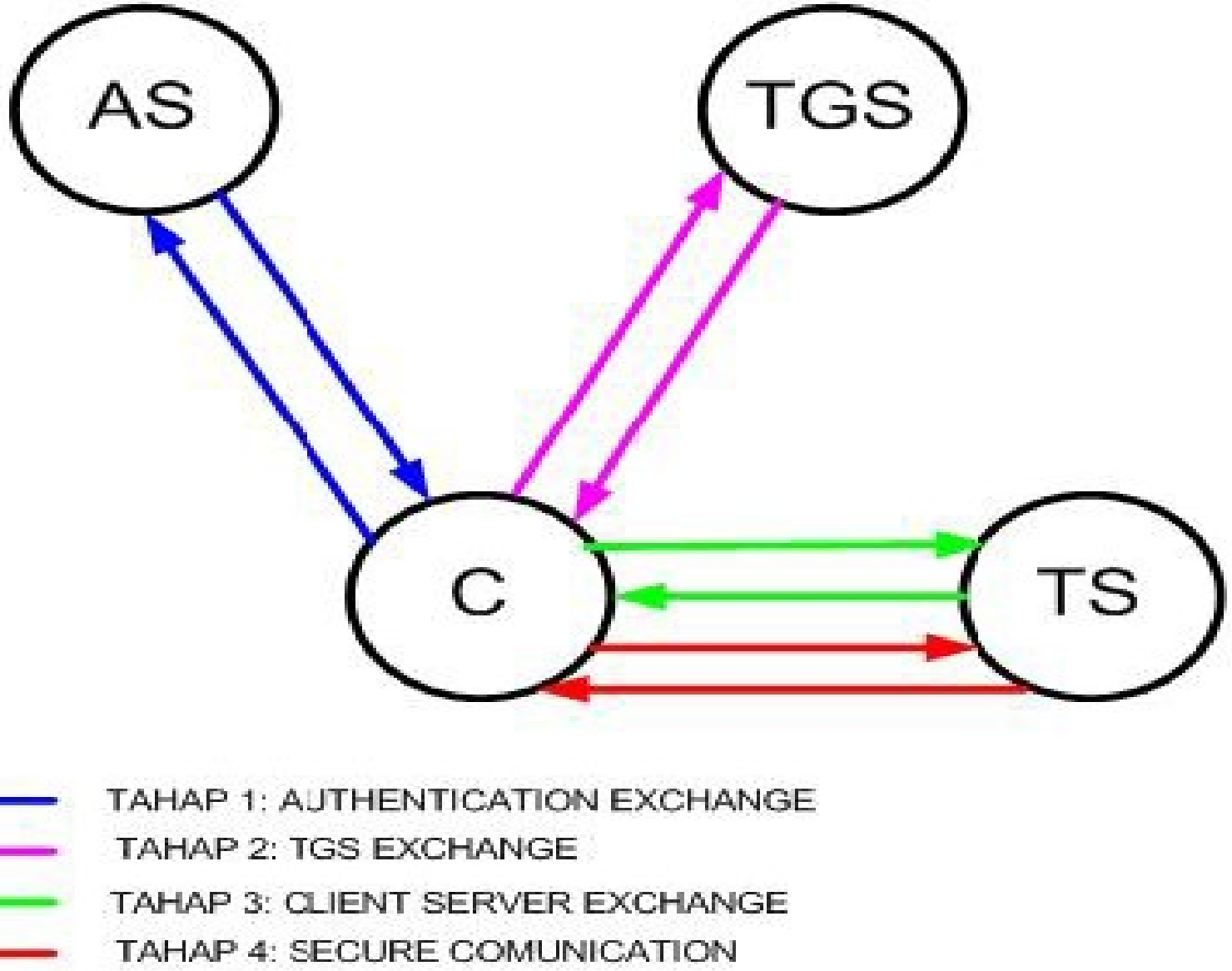
Kerberos

- Kerberos mirip dengan RADIUS namun bekerja dengan cara yang berbeda.
- Kerberos menggunakan sistem tiket untuk memberikan izin kepada *nodes* untuk berkomunikasi melalui media yang tidak aman. Ini dilakukan untuk melakukan identifikasi satu sama lain dengan cara yang aman.

Kerberos

- Protokol mengharuskan Klien dan Server untuk mengidentifikasikan diri satu sama lain (mutual authentication)
- Transmisi kerberos terlindungi dari serangan Sniffer dan Replay Attack
- Kerberos dibangun dengan Kriptografi Simetris, dan *Orang Ketiga Terpercaya*. Namun terkadang, Kerberos menggunakan Kunci Publik

Kerberos Negosiasi



Tahap 1 – User Logon

- Seorang user mengirimkan username dan password dari mesin klien, atau menggunakan kunci publik sebagai password
- Klien merubah password menjadi cipher simetris, untuk proses selanjutnya.

Tahap 2 – Otentifikasi Klien

- Klien mengirimkan pesan jelas ke Authentication Server
- AS kemudian mengecek kebenarannya, dan membalas dua pesan jika benar.
  - Client Session Key, dan Ticket-Granting Ticket
- Klien akan mendekrip pesan Client Session Key dengan password yang dirubahnya tadi

Tahap 3 – Otorisasi Layanan Klien

- Ketika akan meminta Pelayanan (Service), klien akan mengirimkan:
  - Pesan Tertulis TGT berdasarkan TGT AS, dan ID Pelayanannya
  - Otentikator terenkripsi dengan TGS Session Key
- Pesan-pesan itu kemudian akan didekripsi oleh server, dan dibalas dengan dua pesan:
  - Client-to-server Ticket
  - Client/Server Session Key

Tahap 4 – Permintaan Pelayanan Klien

- Setelah menerima pesan dari TGS, klien bisa melakukan otentifikasi diri ke Service Server. Dan mengirimkan dua pesan ke sana:
  - Client-to-Server Ticket
  - Otentikator Baru
- SS akan mendekripsi pesan, dan jika benar SS mengirimkan pesan:
  - Timestamp Otentikator
- Klien mendekripsikan, dan mengecek kebenarannya
- Dan Server bisa mulai melayani Klien.

Kelemahan Kerberos

- Server Kerberos adalah terpusat, sehingga diperlukan availability hingga 100%. Bisa diatas dengan banyak server Kerberos
- Jam Kerberos harus disinkronisasi, dikarenakan Kerberos sangat ketat persyaratan waktunya
- Setiap Pelayanan Jaringan memerlukan hostname yang berbeda-beda

Bersambung ....