BAB II
TINJAUAN PUSTAKA

II.1. Saluran Telekomunikasi

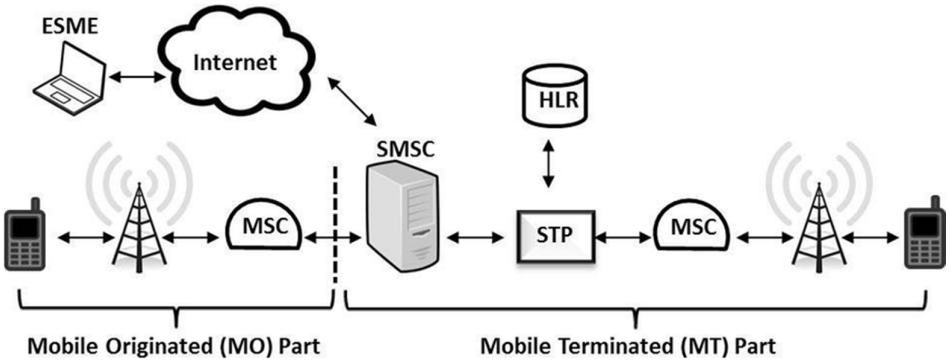
Komunikasi adalah proses transmisi informasi dan pemahaman bersama dari satu orang ke orang lain [8]. Saluran telekomunikasi merupakan data dan bentuk telekomunikasi yang ditransmisikan diantara pengirim dan penerima dalam suatu jaringan telekomunikasi. Transmisi telekomunikasi adalah adalah hubungan antar terminal telekomunikasi baik saat mentransimiskan maupun menerima paket melalui saluran telekomunikasi.

Di dalam Arsitektur *Multi-Channel and Public Participation (MPP)–Based Population Administration System* [7], terdapat dua saluran telekomunikasi yang dimanfaatkan dalam penunjang keberhasilan implementasi sistem yaitu:

1. *Short Message Service* (SMS)
2. *Internet Protokol* (Web atau *Data Service*)

II.1.1. *Short Message Service* (SMS)

SMS (*Short Message Service*), yang biasa disebut "pesan teks", adalah layanan untuk mengirim pesan singkat hingga 160 karakter (224 karakter jika menggunakan mode 7-bit) ke perangkat seluler, termasuk telepon seluler, ponsel pintar, dan PDA [9]. Layanan pesan singkat (SMS) adalah sebuah layanan nilai tambah penting dari komunikasi seluler. [10]



Gambar 2.1 Arsitektur jaringan untuk SMS.

Gambar 2.1 di atas mewakili arsitektur jaringan untuk SMS. SMS dari perangkat seluler atau perangkat eksternal lainnya entitas pesan (ESME) melewati ponsel asal pusat switching seluler operator jaringan (MSC). Saat itulah diterima oleh Pusat Layanan Pesan Singkat (SMSC), yang memastikan pengiriman ke perangkat seluler yang sesuai. Itu titik transfer sinyal (STP) membantu SMSC untuk berkomunikasi dengan register lokasi rumah (HLR) dan MSC dari penghentian operator jaringan seluler [11].

Dengan peningkatan pesat pengguna ponsel, SMS telah menjadi bisnis yang diterima secara luas sejak itu kenyamanan, kesederhanaan dan biaya rendah. Sementara itu, perluasan permintaan informasi pengguna mengarah ke *peer* tradisional ke rekan bisnis pesan singkat tidak demikian efektif dan SMS menjadi perkembangan yang cepat layanan, yang keduanya menyediakan dengan cepat dan nyaman informasi untuk pengguna dan juga menawarkan biaya-manfaat untuk penyedia layanan.

Berikut ini adalah keunggulan dari *Short Message Service* (SMS):

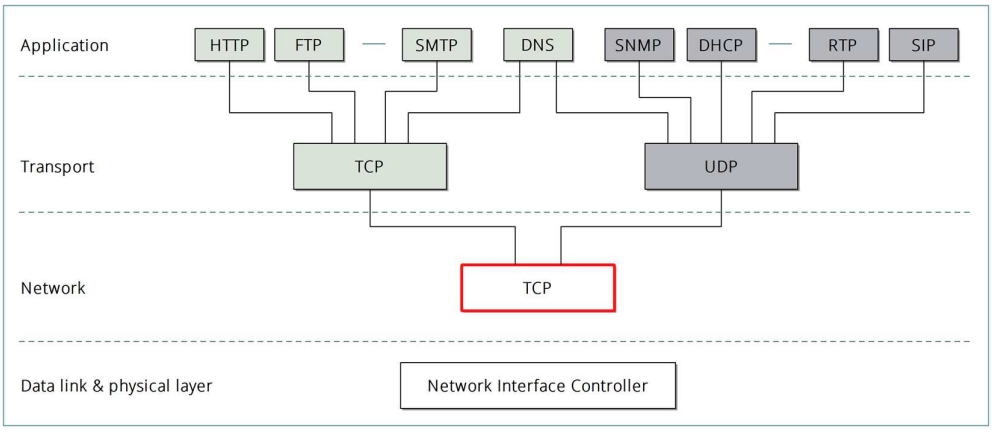
1. Pesan lebih cepat di terima dan di baca.
2. Jaringan telekomunikasi untuk SMS lebih banyak atau merata.

Sedangkan kelemahan dari *Short Message Service* (SMS) adalah sebagai berikut:

1. Batasan karakter yaitu 160 (dalam *Unicode*) untuk 1 kali pesan.
2. Bila ada masalah pada jaringan telekomunikasi, sistem tidak dalam melakukan pengiriman ulang.

II.1.2. *Internet Protocol*

IP (*Internet Protocol*) adalah protokol yang menggunakan datagram untuk berkomunikasi melalui jaringan *packet-switched*, seperti *Internet* [12]. Protokol IP beroperasi pada protokol lapisan jaringan dari model referensi OSI dan merupakan bagian dari rangkaian protokol yang dikenal sebagai TCP/IP.



Gambar 2.2 IP dalam Hirarki Protokol.

Gambar 2.2 menunjukkan bahwa IP mendefinisikan jaringan packet switched, di mana informasi dibawa dalam paket (juga dikenal sebagai datagrams) dari bit antar computer [13].

Protokol Internet adalah rangkaian protokol sistem terbuka (*nonproprietary*) paling populer di dunia karena mereka dapat digunakan untuk berkomunikasi di setiap set jaringan yang saling berhubungan dan sama cocok untuk komunikasi LAN dan WAN. Protokol Internet terdiri dari serangkaian protokol komunikasi, yang paling dikenal adalah *Transmission Control Protocol* (TCP) dan Protokol Internet (IP). Protokol Internet suite tidak hanya mencakup lapisan bawah protokol (seperti TCP dan IP), tetapi juga menentukan aplikasi umum seperti surat elektronik, emulasi terminal, dan *transfer file*.

Mobile Internet Protocol adalah sebuah Perluasan ke Protokol Internet yang diusulkan oleh *Internet Engineering Task Force* (IETF) yang memungkinkan mobile perangkat pengguna untuk berpindah dari satu jaringan ke jaringan lain terlepas dari lokasinya dan tanpa mengubah IP-nya alamat [14]. *Mobile Ad-hoc Network* (MANET) adalah sistem otonom dari host seluler yang terhubung dengan nirkabel tautan.

Berikut ini adalah keunggulan dari Protokol Internet:

1. Sarana komunikasi data yang efektif dan murah.
2. Kecepatan, konektivitas dan jangkauan yang global.

3. Interaktifitas dan fleksibilitas.

Sedangkan kelemahan dari Protokol Internet adalah sebagai berikut:

1. Jaringan telekomunikasi untuk *Internet Data Service* masih belum merata.

II.2. Arsitektur *Multi-Channel and Public Participation Based Population Administration System*

Arsitektur *Multi-Channel and Public Participation (MPP) – Based Population Administration System* adalah sebuah usulan arsitektur sistem yang melibatkan partisipasi publik baik masyarakat dan instansi pelaksana pemerintahan dalam pelaporan kejadian di masyarakat (kelahiran, kematian dan perpindahan) guna mendukung pemutakhiran data SIAK memanfaatkan ketersediaan infrastruktur telekomunikasi di Indonesia [7]. Jaringan *multi-channel* yang menggunakan saluran terpisah untuk pertukaran paket kontrol untuk mengkoordinasikan komunikasi data [15]. Banyak teknologi jaringan yang berbeda berhasil membagi media bersama umum menjadi beberapa saluran logis paralel, menyediakan eksploitasi sumber daya jaringan yang tersedia.

Arsitektur jaringan di dalam *MPP – Based Population Administration System* di dalam administrasi data kependudukan disebut sebagai jaringan multi-channel, karena terdiri dari beberapa saluran logis paralel dengan kapasitas yang sama. Di dalam jaringan *Multi-Channel*, beban transmisi data didistribusikan ke lebih banyak saluran untuk transmisi sehingga terjadi efesiensi di dalam komunikasi data sebanding dengan pemerataan jaringan telekomunikasi di Indonesia.

Penggunaan arsitektur *Multi-Channel* telah digunakan di bidang lain, seperti manajemen [16] dan bahkan pemerintahan [17][18]. Penelitian sebelumnya, kondisi semacam itu tidak dapat selalu diterapkan di Indonesia, karena kondisi yang berbeda dari infrastruktur telekomunikasi dan karakteristik Masyarakat Indonesia. Secara prinsip, *Multi-Channel* arsitektur mencoba memanfaatkan berbagai saluran telekomunikasi yang dapat digunakan di tempat-tempat dengan ketersediaan atau kendala infrastruktur yang berbeda.

Di dalam merencanakan arsitektur *MPP–Based Population Administration System*, mempertimbangkan:

1. Peraturan yang berlaku
    a. Kelahiran

        Aturan mengenai pencatatan kelahiran bayi, sehingga terjadi pemutakhiran data di dalam sistem dan menghasilkan akte kelahiran diatur oleh UU no.24 tahun 2013 pasal 27 dan pasal 49, yang hanya mengatur tentang batas waktu pelaporan pencatatan kelahiran oleh orang tua bayi. Menurut Peraturan Presiden RI no 025 tahun 2005 Pasal 105 tentang keterlambatan pelaporan dikenai denda administratif, namun secara praktis, aturan soal denda keterlambatan pelaporan ini secara khusus tertuang dalam peraturan setiap daerah.

    b. Kematian

        Pelaporan peristiwa kematian yang terjadi di masyarakat selama ini juga tergantung kepada iktikad keluarga dari penduduk yang meninggal. Jika tidak ada kebutuhan untuk memiliki akta kematian, maka keluarga umumnya enggan melaporkan hal ini. Padahal UU No. 24 Tahun 2013 Pasal 44 mewajibkan ketua rukun tetangga atau anggota masyarakat lainnya di sekitarnya untuk melaporkan selambat-lambatnya 30 hari sejak kejadian.

    c. Perpindahan Tempat Tinggal

        Perpindahan penduduk dari satu tempat ke tempat lain, kewajiban untuk melakukan pemutakhiran data diatur oleh UU no.23 tahun 2006 pasal 15 dan UU no.24 tahun 2013 pasal 63, yang juga menekankan kepada kewajiban pribadi penduduk yang melakukan pelaporan perpindahan tempat tinggal.

2. Karakteristik masyarakat Indonesia

    Bangsa Indonesia pada umumnya saling mengenal antar tetangga. Banyak dijumpai masyarakat di satu daerah masih memiliki hubungan kekerabatan

yang erat, sehingga tercipta budaya gotong-royong saling menolong saat ada peristiwa kelahiran, kematian atau pindah.

Karakterisitik masyarakat ini sesungguhnya dapat digunakan untuk mempercepat proses pemutakhiran sekaligus memvalidasi data kependudukan, apabila tersedia sarana pelaporan, pemutakhiran data dan validasinya dengan mudah dan murah. Penelitian ini mengusulkan suatu arsitektur sistem pelaporan, pemutakhiran dan validasi data yang bekerja sejalan dengan sistem yang sudah ada (SIAK) dan sesuai dengan kondisi infrastruktur telekomunikasi di Indonesia.

3. Kondisi infrastruktur telekomunikasi

   Pada tahun 2017, kondisi infrastruktur telekomunikasi di Indonesia adalah 9.000 desa atau 22% dari daerah yang terjangkau 2G yang belum tersentuh sinyal, jaringan 2G cakupannya 88,28% desa, dan jaringan 3G saat ini cakupannya menyentuh 75,06% desa. Sedangkan untuk penetrasi internet di Indonesia pada tahun 2017 adalah sekitar 54.68%. Dengan demikian skema pelaporan, pemutakhiran dan validasi data kependudukan yang digunakan harus sesuai dengan kondisi infrastruktur telekomunikasi di setiap daerah yang berbeda-beda, yaitu:

   - Daerah tanpa akses telekomunikasi,
   - Daerah dengan akses sms
   - Daerah dengan akses sms dan Internet.

Dalam penentuan tokoh publik (formal dan informal) yang akan melakukan tahapan verifikasi dan validasi, perancangan *MPP – Based Population Administration System* mempertimbangkan kesesuaian antara tokoh publik dengan peristiwa. Berikut ini adalah kesesuaian tokoh publik dengan peristiwa:

1. Kelahiran
   a. Utama: Paramedis dan Tokoh Formal
   b. Perlu lebih dari 1 verifikasi: Tokoh Masyarakat Lainnya
2. Kematian

a. Utama: Paramedis dan Tokoh Formal

b. Perlu lebih dari 1 verifikasi: Tokoh Masyarakat Lainnya

3. Perpindahan Tempat Tinggal

a. Utama: Tokoh Keamanan dan Tokoh Formal

b. Perlu lebih dari 1 verifikasi: Tokoh Masyarakat Lainnya

II.3. Multi-Factor Authentication

Multi-Factor Authentication (MFA) [19], adalah sistem keamanan yang membutuhkan lebih dari satu metode otentikasi untuk memverifikasi identitas pengguna [20]. MFA digunakan untuk interaksi antar manusia secara cepat, mudah digunakan, dan dapat diandalkan saat mengakses layanan.

Otentikasi multifaktor menggabungkan dua atau lebih kredensial independen: apa yang diketahui pengguna (kata sandi), apa yang dimiliki pengguna (token keamanan) dan apa pengguna itu (verifikasi biometrik). Tujuan dari MFA adalah untuk menciptakan pertahanan berlapis dan membuatnya lebih sulit bagi orang yang tidak sah untuk mengakses target seperti lokasi fisik, perangkat komputasi, jaringan atau basis data. Jika salah satu faktor dikompromikan atau rusak, penyerang masih memiliki setidaknya satu lagi penghalang untuk dilanggar sebelum berhasil membobol target.

Gambar 2.3 Contoh implementasi MFA.

Gambar 2.3 merupakan contoh implementasi MFA dimana untuk masuk kedalam sistem di perlukan identitas dari pengguna untuk mendapatkan informasi awal dan ditambahkan dengan verifikasi menggunakan saluran komunikasi yang lain dari yang bersangkutan.

II.3.1. Faktor Otentikasi MFA

Faktor otentikasi adalah kategori kredensial yang digunakan untuk verifikasi identitas. Untuk MFA, setiap faktor tambahan dimaksudkan untuk meningkatkan jaminan bahwa suatu entitas yang terlibat dalam suatu jenis komunikasi atau meminta akses ke suatu sistem adalah siapa, atau apa, mereka dinyatakan. Tiga kategori yang paling umum sering digambarkan sebagai sesuatu yang Anda ketahui (faktor pengetahuan), sesuatu yang Anda miliki (faktor kepemilikan) dan sesuatu yang Anda (faktor pewarisan).

1. Faktor pengetahuan - informasi yang harus dapat diberikan oleh pengguna untuk masuk. Nama pengguna atau ID, kata sandi, PIN, dan jawaban untuk pertanyaan rahasia semuanya termasuk dalam kategori ini.
2. Faktor kepemilikan - apa pun yang harus dimiliki pengguna untuk masuk, seperti token keamanan, token *One-Time Password* (OTP), kunci utama, kartu ID karyawan, atau kartu SIM telepon. Untuk autentikasi seluler, ponsel cerdas sering kali memberikan faktor kepemilikan, bersama dengan aplikasi OTP.
3. *Inherence factors* - setiap sifat biologis yang dimiliki pengguna yang dikonfirmasi untuk masuk. Kategori ini termasuk ruang lingkup metode otentikasi biometrik seperti scan retina, scan scan sidik jari iris, scan vena jari, pengenalan wajah, pengenalan suara, geometri tangan, bahkan geometri daun telinga.
4. Faktor lokasi - lokasi pengguna saat ini sering disarankan sebagai faktor keempat untuk autentikasi. Sekali lagi, di mana-mana smartphone dapat membantu meringankan beban otentikasi di sini: Pengguna biasanya membawa telepon mereka dan sebagian besar smartphone memiliki perangkat *Global Positioning System* (GPS), memungkinkan konfirmasi yang wajar dari lokasi login.
5. Faktor waktu - Waktu saat ini juga terkadang dianggap sebagai faktor keempat untuk otentikasi atau alternatif faktor kelima. Verifikasi ID

karyawan terhadap jadwal kerja dapat mencegah beberapa jenis serangan pembajakan akun pengguna.

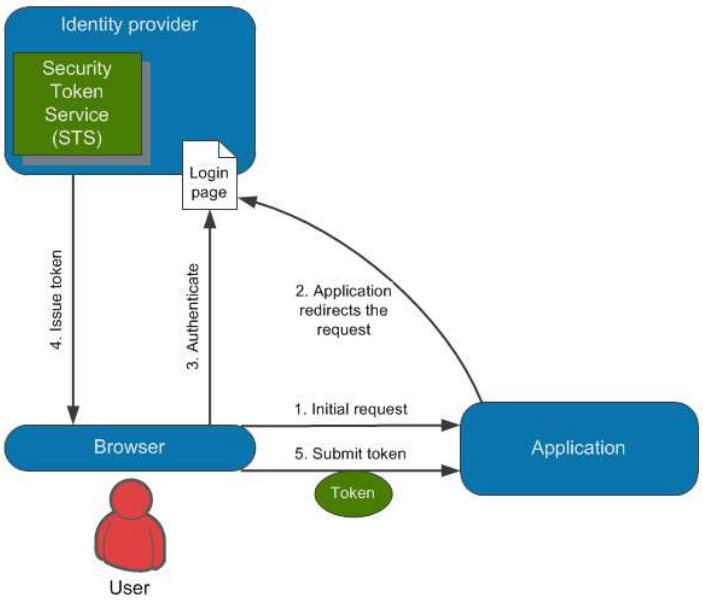
II.3.2. *Multi-Factor Authentication Technologies*

Teknologi otentikasi dalam *Multi-Factor* adalah suatu perkembangan ilmu pengetahuan yang dapat dimanfaatkan dalam implementasi *Multi-Factor* Otentikasi. Berikut ini adalah teknologi dalam *Multi-Factor* Otentikasi:

1. *Security tokens*: Perangkat perangkat keras kecil yang diberikan pemilik untuk mengotorisasi akses ke layanan jaringan. Perangkat mungkin dalam bentuk kartu pintar atau dapat disematkan dalam objek yang mudah dibawa seperti fob kunci atau drive USB. Token perangkat keras menyediakan faktor kepemilikan untuk otentikasi multifaktor. Token berbasis perangkat lunak menjadi lebih umum daripada perangkat perangkat keras.
2. *Soft tokens*: Aplikasi token keamanan berbasis perangkat lunak yang menghasilkan PIN login sekali pakai. Token lunak sering digunakan untuk autentikasi seluler multifaktor, di mana perangkat itu sendiri - seperti smartphone - menyediakan faktor kepemilikan.
3. *Mobile authentication*: Variasi termasuk: pesan SMS dan panggilan telepon yang dikirim ke pengguna sebagai metode *out-of-band*, aplikasi OTP smartphone, kartu SIM, dan kartu cerdas dengan data otentikasi yang tersimpan.
4. Metode otentikasi biometrik seperti retina scan, iris scan scan sidik jari, scan vena jari, pengenalan wajah, pengenalan suara, geometri tangan dan bahkan geometri daun telinga.
5. *Smartphone* GPS juga dapat menyediakan lokasi sebagai faktor otentikasi dengan perangkat keras papan ini.
6. ID karyawan dan kartu pelanggan, termasuk strip magnetik dan kartu pintar.

II.4. Claim-Based Authentication

Claims-Based Authentication (CBA) adalah proses menggunakan kredensial (klaim) yang berisi informasi otentikasi dalam salah satu dari banyak kemungkinan protokol otentikasi untuk menetapkan identitas para pihak yang ingin berkolaborasi [21]. Identitas berbasis klaim adalah cara mengautentikasi pengguna akhir, aplikasi, atau perangkat ke sistem lain dengan cara yang abstrak dari informasi spesifik entitas sambil menyediakan data yang menguasainya untuk interaksi yang sesuai dan relevan [22].



Gambar 2.4 Contoh implementasi CBA.

Gambar 2.4 merupakan contoh implementasi CBA dimana ketika pengguna mencoba mengakses bagian yang dibatasi, aplikasi mengalihkan mereka ke halaman logon dari penyedia identitas. Pengguna mengautentikasi ke penyedia identitas, yang memberi mereka token, yang kemudian diteruskan ke aplikasi untuk mengonfirmasi identitas pengguna.

Dapat juga diartikan bahwa CBA adalah suatu cara untuk memperoleh informasi yang dibutuhkan tentang identitas pengguna dan relevansinya terkait akses sistem. Metode otentikasi ini memberikan informasi pengguna secara otomatis sehingga aplikasi tidak perlu memintanya dari pengguna dan pengguna tidak harus memberikan informasi itu secara terpisah untuk aplikasi yang berbeda.

II.4.1. *Manfaat dari Claims-Based Identity*

Identitas berbasis klaim menawarkan sejumlah keunggulan ketika menerapkan otentikasi, termasuk:

1. *Outsourcing Authentication*. Identitas berbasis klaim menghilangkan kebutuhan aplikasi untuk melakukan tugas otentikasi, membuat manajemen akun lebih mudah dengan memusatkan otentikasi. Aplikasi tidak perlu bertanggung jawab untuk otentikasi pengguna, mencari detail identitas pengguna, menyimpan akun pengguna dan kata sandi, atau mengintegrasikan dengan sistem identitas lain. Selain itu, otentikasi memusatkan membuatnya lebih mudah untuk meng-upgrade aplikasi ke metode otentikasi yang lebih kuat.
2. Mendukung beberapa penyedia otentikasi. Identitas berbasis klaim memungkinkan perusahaan untuk dengan mudah menerapkan metode otentikasi yang berbeda menggunakan penyedia yang berbeda, misalnya, *Windows Live ID*, otentikasi *Windows Active Directory* atau otentikasi berbasis form untuk situs web. Ini dilakukan menggunakan single sign-on untuk mendukung pengguna yang mengakses layanan web atau aplikasi web dengan berbagai cara, termasuk melalui internet, dari dalam organisasi dan melalui organisasi yang berafiliasi.
3. Mendukung federasi identitas. Identitas berbasis klaim memungkinkan pengguna eksternal dalam satu organisasi untuk mengakses aplikasi jaringan dari perusahaan lain menggunakan identitas mereka sendiri.
4. Identitas berbasis klaim menawarkan lebih banyak keserbagunaan karena organisasi dapat membuat atribut tambahan sebagai klaim yang menjadi dasar kontrol akses.

II.4.2. Cara kerja dari *Claims-Based Identity*

Identitas berbasis klaim adalah salah satu jenis sistem manajemen akses identitas, yang merupakan kerangka kerja untuk proses bisnis yang memfasilitasi

pengelolaan identitas elektronik. Kerangka kerja ini mencakup teknologi yang dibutuhkan untuk mendukung manajemen identitas.

Klaim adalah potongan informasi tentang pengguna yang telah dikemas, ditandatangani ke token keamanan dan dikirim oleh penerbit atau penyedia identitas untuk mengandalkan aplikasi pihak melalui *Security token service* (STS). Data tersebut kemudian dikirimkan menggunakan metode standar, seperti *Security Assertion Markup Language* (SAML), sehingga klaim akan memiliki format yang sama di berbagai sumber dan aplikasi otentikasi yang berbeda.

Layanan token keamanan bertindak sebagai otoritas yang menerbitkan, menerima kredensial masuk, memvalidasi mereka, dan membuat token aman dengan daftar klaim. Token dienkripsi dan dikirim ke suatu aplikasi. Penting bahwa penerbit token adalah entitas tepercaya.

II.4.3. *Proses dari Claims-Based Identity*

Claim-Based Identify bergantung pada hubungan kepercayaan yang dibuat antara mereka yang membuat klaim dan pihak yang bersandar. Pihak yang mengandalkan adalah aplikasi atau perangkat yang bergantung pada klaim untuk identitas pengguna dan kontrol akses. Pihak yang mengandalkan hanya akan menerima klaim tentang identitas pengguna dari penerbit tepercaya.

Klaim dikirim ke pihak yang bergantung dalam bentuk token keamanan dalam sejumlah format, termasuk SAML berbasis *eXtensible Markup Language* (XML) atau *Simple Web Token* (SWT). STS memproses permintaan token dari pihak-pihak yang bersandar.

Paket STS satu atau lebih klaim menjadi token keamanan, menandatanginya secara kriptografi dan mengirimkannya ke pihak yang bergantung dienkripsi pada kawat. Kemudian, ketika pihak yang mengandalkan menerima token, itu memverifikasi tanda tangan tanda dan, jika itu valid, itu menggunakan klaim untuk pengambilan keputusan lain yang diperlukan, seperti pemeriksaan otorisasi atau personalisasi.

Proses identitas berdasarkan klaim adalah sebagai berikut:

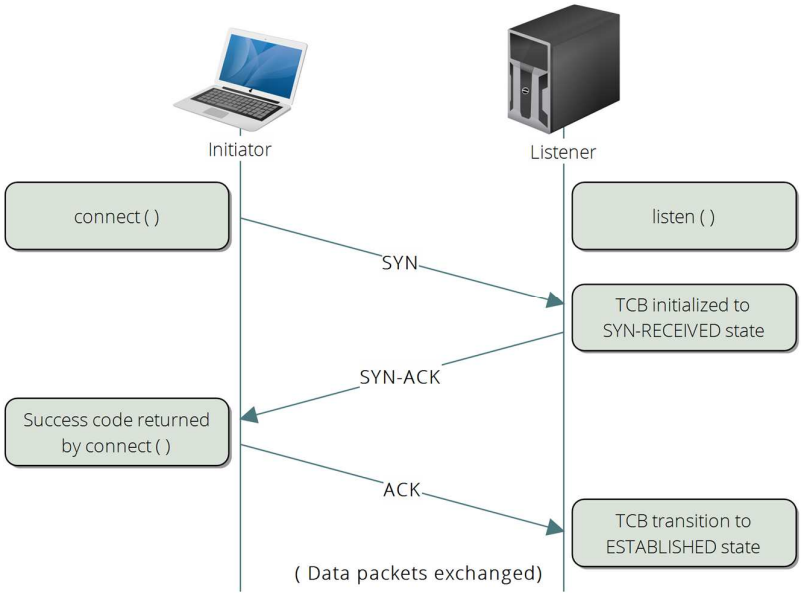
- Seorang pengguna meminta akses ke aplikasi.
- Aplikasi mengirim permintaan ke STS untuk token bagi pengguna itu.
- STS mengautentikasi pengguna, misalnya, dengan kata sandi, pemindaian biometrik atau kartu cerdas.
- STS membuat token.
- STS menandatangani token secara digital dan tanda tangan digital kemudian menjadi bagian dari token.
- STS mengirim token kembali ke aplikasi yang memintanya.
- Aplikasi memverifikasi validitas tanda tangan digital dan mengonfirmasi bahwa itu berasal dari STS yang dipercaya oleh layanan atau aplikasi.
- Aplikasi memproses data klaim untuk menentukan apakah mengizinkan pengguna untuk mengakses aplikasi, serta tingkat akses yang dimiliki pengguna.

Prosesnya bisa lebih rumit, karena ada dua jenis STS: *Identity Provider* STS *Authentication* bergantung pada layanan otentikasi, seperti yang disediakan oleh *Active Directory*; Pihak Pengganti STS mengautentikasi menggunakan token yang telah disediakan oleh Penyedia Identitas STS yang tepercaya.

II.5. 3-Way Handshaking

Way Handshaking atau SYN-SYN-ACK adalah metode yang awalnya digunakan oleh TCP mengatur TCP / IP koneksi melalui jaringan berbasis Protokol Internet. Gagasan protokol ini akan digunakan dalam prosedur otentikasi, melibatkan berbeda saluran komunikasi untuk mengirim kode tantangan dan untuk menerima kode konfirmasi [23][24][25].

Proses handshake 3 arah ini juga dirancang sehingga kedua ujungnya dapat memulai dan menegosiasikan koneksi soket TCP terpisah pada saat yang bersamaan. Mampu bernegosiasi koneksi soket TCP ganda di kedua arah pada saat yang sama memungkinkan antarmuka jaringan fisik tunggal, seperti *ethernet*, untuk *multiplexing* untuk mentransfer beberapa aliran data TCP secara bersamaan.



Gambar 2.5 Contoh implementasi *3-Way Handshaking*.

Gambar 2.5 merupakan contoh diagram sederhana dari proses *3-Way Handshaking*. Host AW mengirim paket TCP *SYNchronize* ke Host B. Tuan rumah B menerima A SYN. Host B mengirim SYNchronize-acknowledgment. Host A menerima B's SYN-ACK. Host A mengirimkan *ACKnowledge*. Host B menerima ACK. Koneksi soket TCP didirikan.

II.6. Majority Voting

Teorema May menyatakan bahwa pemilihan suara mayoritas sederhana adalah satu-satunya fungsi keputusan kelompok yang memenuhi ketegasan, anonimitas, netralitas, dan responsif positif antara dua alternatif [26]. Lebih lanjut, prosedur ini secara tegas diperlukan ketika ada jumlah ganjil pemilih dengan minimal 3 pemilih dan ikatan keragu-raguan tidak diperbolehkan. Jika salah satu alternative menerima mayoritas suara tempat pertama, maka alternative tersebut harus dinyatakan sebagai pemenang.

Fungsi keputusan kelompok: $D = f(D_1, D_2,, D_n)$, n adalah jumlah pemilih di dalam suatu kelompok. Setiap D_i mengambil nilai 1, 0 atau −1 dan sesuai dengan preferensi pemilih. Oleh karena itu, 1 berarti bahwa pemilih i lebih memilih x ke y, −1 berarti bahwa pemilih i lebih memilih y ke x dan 0 berarti bahwa tidak atau

belum menentukan pilihan antara *x* dan *y*. Dengan demikian, masing-masing D_i sesuai dengan proses pemungutan pilihan yang di pilih di antara dua alternatif. *F(.)* mewakili aturan agregasi yang menentukan dalam masalah kemenangan.

Dengan demikian, aturan pemilihan berdasarkan mayoritas secara sederhana dapat didefinisikan dengan cara berikut:

$$\left(\sum_{i=1}^{n} Di > 0\right) \rightarrow D = 1$$

$$\left(\sum_{i=1}^{n} Di = 0\right) \rightarrow D = 0$$

$$\left(\sum_{i=1}^{n} Di < 0\right) \rightarrow D = -1$$

Definisi ini berarti bahwa *x* lebih dipilih daripada *y* oleh suatu kelompok, jika jumlah pemilih yang memilih *x* lebih tinggi daripada jumlah pemilih yang memilih *y* dan begitupun sebaliknya. *D* hanya ditentukan oleh nilai-nilai D_i, dan tidak tergantung pada bagaimana tugas pemilih. Jika *D* sama dengan 0 atau 1, dan satu pemilih mengubah preferensi dari −1 ke 0 atau 1, atau dari 0 ke 1, dan semua hubungan preferensi pemilih lainnya tetap tidak berubah, maka *D* = 1.

II.7. *Control Access ISO/IEC* 27001:2005

Ancaman ataupun kelemahan dalam teknologi informasi dapat menggangu jalannya kegiatan pelayanan yang menggunakan teknologi informasi. Oleh karena itu diperlukan pengelolaan teknologi informasi berbasis risiko yang dituangkan dalam tata kelola untuk mengelola ancaman ataupun kelemahan yang muncul. ISO/IEC 27001:2005 merupakan *framework* sistem manajemen keamanan informasi yang dapat dijadikan dasar dalam pengelolaan keamanan informasi. Tata kelola keamanan informasi yang dibuat ini menitikberatkan pada kontrol akses yang merupakan salah satu kotrol keamanan dari ISO/IEC 27001:2005[27].

ISO/IEC 27001:2005 merupakan standard keamanan informasi yang diterbitkan *International Organization for Standarization dan International*

Electrotecnical Comission pada bulan Oktober 2005 untuk menggantikan standard BS7799-2. Standard ini berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan.

Identifikasi risiko dilakukan untuk mengidentifikasi seberapa besar dan risiko apa yang akan diterima oleh organisasi jika informasi organisasi mendapat ancaman atau gangguan keamanan yang menyebabkan gagalnya penjagaan aspek keamanan informasi. Untuk mengidentifikasi risiko dilakukan langkah-langkah sebagai berikut :

1. Mengidentifikasi aset yang dimiliki oleh organisasi sesuai dengan ruang lingkup SMKI serta menentukan juga pemilik asetnya
2. Menghitung nilai aset berdasarkan aspek keamanan informasi
3. Mengidentifikasi ancaman dan kelemahan terhadap asset
4. Melakukan analisis dampak bisnis jika terjadi kegagalan penjagaan aspek keamanan informasi

Tahap selanjutnya setelah organisasi melakukan identifikasi risiko, sehingga memahami risiko yang akan dihadapi dan dampaknya terhadap organisasi adalah melakukan analisis dan evaluasi risiko. Tahap ini bertujuan untuk menganalisis dan mengevaluasi risiko yang sudah diidentifikasi pada tahap sebelumnya, untuk memahami bagaimana dampak- dampak risiko terhadap bisnis organisasi, bagaimana level risiko yang mungkin timbul dan menentukan apakah risiko yang terjadi langsung diterima atau masih perlu dilakukan pengelolaan agar risiko dapat diterima dengan dampak yang bisa ditoleransi. Tahap-tahap nya adalah sebagai berikut :

1. Melakukan analisis dampak bisnis
2. Mengestimasi level risiko

3. Menentukan apakah risiko yang timbul diterima atau masih perlu pengelolaan risiko dengan menggunakan kriteria penerimaan risiko terlebih dahulu.

II.8. Database

Basis data (*Database*) adalah kumpulan data yang disimpan secara sistematis di dalam komputer yang dapat diakses, diolah atau dimanipulasi menggunakan perangkat lunak (program aplikasi) untuk menghasilkan informasi [28]. Pendefinisian basis data meliputi spesifikasi berupa tipe data, struktur data dan juga batasan-batasan pada data yang akan disimpan. Basis data merupakan aspek yang sangat penting dalam sistem informasi karena berfungsi sebagai gudang penyimpanan data yang akan diolah lebih lanjut. Basis data menjadi penting karena dapat mengorganisasi data, menghidari duplikasi data, menghindari hubungan antar data yang tidak jelas dan juga update yang rumit.

Data Base Management System (DBMS) merupakan sistem perangkat lunak yang memungkinkan pengguna basis data (database user) untuk memelihara, mengontrol dan mengakses data secara praktis dan efisien [29]. Dengan kata lain, semua akses ke basis data akan ditangani oleh DBMS. DBMS ini menjadi lapisan yang menghubungkan basis data dengan program aplikasi untuk memastikan bahwa basis data tetap terorganisasi secara konsisten dan dapat diakses dengan mudah.

Ada beberapa fungsi yang harus ditangani DBMS seperti pendefinisian data, menangani permintaan pengguna untuk mengakses data, memeriksa sekuriti dan integriti data yang didefinisikan oleh DBA (*Database Administrator*), menangani kegagalan dalam pengaksesan data yang disebabkan oleh kerusakan sistem maupun media penyimpanan (disk) dan juga menangani unjuk kerja semua fungsi secara efisien.

Tujuan utama DBMS adalah untuk memberikan tinjauan abstrak data kepada pengguna. Jadi sistem menyembunyikan informasi tentang bagaimana data disimpan, dipelihara dan juga bisa diakses secara efisien. Pertimbangan efisien di sini adalah rancangan struktur data yang kompleks tetapi masih bisa digunakan oleh pengguna awam tanpa mengetahui kompleksitas strukturnya.

Menurut jenisnya, basis data dapat dibagi menjadi:

1. Basis data flat-file.

   Basis data ini ideal untuk data berukuran kecil dan dapat dirubah dengan mudah. Pada dasarnya, basis data flat-file tersusun dari sekumpulan string dalam satu atau lebih file yang dapat diurai untuk mendapatkan informasi yang disimpan. Basis data flat-file cocok untuk menyimpan daftar atau data yang sederhana dan dalam jumlah kecil. Basis data flat-file akan menjadi sangat rumit apabila digunakan untuk menyimpan data dengan struktur kompleks walaupun dimungkinkan pula untuk itu.

   Beberapa kendala dalam menggunakan basis data jenis ini adalah rentan pada korupsi data karena tidak adanya penguncian yang melekat ketika data digunakan atau dimodifikasi dan juga adanya duplikasi data yang mungkin sulit dihindari. Salah satu tipe basis data flat-file adalah file CSV yang menggunakan pemisah koma untuk setiap nilainya.

2. Basis data relasional.

   Basis data ini mempunyai struktur yang lebih logis terkait cara penyimpanan. Kata "relasional" berasal dari kenyataan bahwa tabel-tabel yang ada di basis data relasional dihubungkan satu dengan lainnya. Basis data relasional menggunakan sekumpulan tabel dua dimensi yang masing-masing tabel tersusun atas baris (tupel) dan kolom (atribut).

   Untuk membuat hubungan antara dua atau lebih tabel, digunakan *key* (atribut kunci) yaitu primary key di salah satu tabel dan foreign key di tabel yang lain. Saat ini, basis data relasional menjadi pilihan utama karena keunggulannya. Program aplikasi untuk mengakses basis data relasional menjadi lebih mudah dibuat dan dikembangkan dibandingkan dengan penggunaan basis data flat-file.