



GARIS PANDUAN PENGGUNAAN

SIEMENS









BAGI AGENSI-AGENSI SEKTOR AWAM

GARIS PANDUAN PENGGUNAAN

SIEMENS

BAGI AGENSI-AGENSI SEKTOR AWAM

KANDUNGAN

 Pengenalan	3	 Pertimbangan Pemilihan Sistem Biometrik	19
Latar Belakang	4	Ciri-ciri Keselamatan	20
 Jenis-jenis Biometrik	5	Kesesuaian Dengan Pengguna	21
Cap Jari	6	Mesra Pengguna	21
Anak Mata (<i>Iris</i>)	6	Kebolehpercayaan (<i>reliability</i>)	21
Muka	6	Keupayaan Sistem	21
Suara	7	Prestasi Ukuran Penilaian	22
Pengecaman Asid Deoxyribonucleic (DNA)	7	Pengujian	22
Geometri Tangan	7	Penyelenggaraan	22
Urut Saraf (<i>Vein</i>)	7	 Standard-standard Biometrik	23
Tandatangan (<i>Signature</i>)	8	ISO/IEC JTC 1/SC 37 Biometrics	24
<i>Keystroke</i>	8	Standard-standard yang telah dikeluarkan (<i>Published Standards</i>)	26
Lain-lain	8	Standard-standard Dalam Peringkat Pembangunan (<i>Standards under development</i>)	26
 Sistem Biometrik	9	Standard Malaysia	26
Fungsi-fungsi Sistem Biometrik	10	 Penutup	27
Komponen-komponen Sistem Biometrik	11		
Penggunaan Sistem Biometrik	14		
Kebaikan Sistem Biometrik	14		
Kelemahan Sistem Biometrik	14		
 Ukuran Penilaian	15		
<i>False Match Rate</i> (FMR)	16		
<i>False Non Match Rate</i> (FNMR)	16		
<i>Failure To Enroll Rate</i> (FTE)	16		
<i>Equal Error Rate</i> (EER)	16		
 Pertimbangan Penggunaan Teknologi Biometrik di Agensi	17		
Peningkatan dan Keberkesanan Perkhidmatan	18		
Keselamatan	18		
Kesediaan Pelanggan	18		
Polisi/Perundangan	18		
Kos	18		



PENGENALAN

Dokumen ini bertujuan memberi panduan kepada agensi-agensi Sektor Awam berkaitan penggunaan teknologi biometrik di agensi-agensi. Kumpulan sasaran bagi garis panduan ini adalah agensi-agensi Sektor Awam di Malaysia.

LATAR BELAKANG

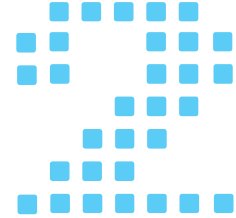
Biometrik merupakan kaedah untuk mengecam (*recognize*) individu berdasarkan ciri-ciri biologi (*biological*) dan tingkah laku (*behavioral*) individu tersebut. Ciri-ciri biologi dan tingkah laku individu seperti cap jari, tapak tangan, anak mata, suara, muka, pengecaman asid deoxyribonucleic (DNA), keystroke, tandatangan dan sebagainya telah digunakan untuk mengenal pasti individu sejak dahulu lagi.

Di peringkat global, penggunaan teknologi biometrik telah meningkat terutamanya dalam bidang keselamatan dan forensik bagi tujuan pengenalpastian dan pengesahan identiti seseorang individu. Contohnya, semua lapangan terbang di Amerika Syarikat menggunakan sistem pengenal biometrik yang mengandungi gambar serta cap jari pelawat-pelawat asing. Negara Jepun pula banyak menggunakan kaedah urat saraf (*vein*) bagi sistem kedatangan di pejabat/syarikat dan sistem maklumat peribadi di institusi-institusi pendidikan serta kesihatan.

Di Malaysia, teknologi biometrik juga telah dimanfaatkan oleh banyak agensi Sektor Awam dalam meningkatkan tahap keselamatan dan kualiti sistem penyampaian perkhidmatan mereka. Antara aplikasi yang menggunakan teknologi biometrik adalah MyKad sebagai dokumen pengenal warga Malaysia dan *Automated Fingerprint Identification System* (AFIS) bagi mengenal pasti identiti warga Malaysia melalui pengesanan cap ibu jari.

Teknologi biometrik yang menggunakan cap jari juga digunakan bagi Sistem Pasport, Sistem Biometrik Pengesanan Pemandang Tanpa Izin (PATI) dan *Biometric Fingerprint Identification System* (BIOFIS) untuk mengesan penjenayah. Terdapat juga agensi-agensi yang menggunakan biometrik untuk akses masuk bangunan pejabat.





JENIS-JENIS BIOMETRIK

Jenis-jenis biometrik yang biasa digunakan adalah cap jari, anak mata, muka, suara, DNA, geometri tangan, urat saraf, tandatangan, *keystroke* dan lain-lain.

JENIS JENIS BIOMETRIK

Terdapat beberapa jenis biometrik yang biasa digunakan seperti berikut:

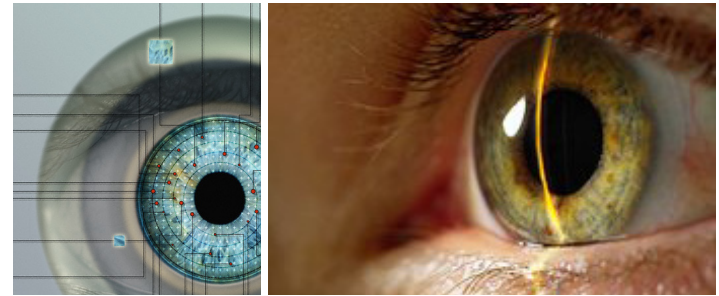
Cap Jari

Teknologi cap jari menggunakan imej optik atau *electronic field imaging* untuk mengenal pasti identiti melalui *pattern-matching* dan *minutiaes*. Imbasan cap jari individu akan dibandingkan dengan templat cap jari yang disimpan di dalam sistem. Kaedah biometrik ini mempunyai tahap ketepatan yang tinggi di mana telah terbukti tidak terdapat lebih dari satu individu yang mempunyai cap jari yang serupa. Kaedah ini telah lama digunakan di peringkat global bagi pengesahan identiti individu dan pengenalpastian penjenayah.



Anak Mata (*Iris*)

Teknik ini menggunakan ciri-ciri imej anak mata yang unik. Alat pengimbas mata akan mengambil foto mata yang beresolusi tinggi dan merekodkan data tersebut. Data ini seterusnya akan ditukarkan kepada algoritma dan dibandingkan dengan karakter dan bentuk anak mata yang telah direkodkan. Kaedah ini sesuai digunakan untuk akses lokasi-lokasi yang bertahap keselamatan yang tinggi, contohnya memasuki bilik kebal yang mengandungi bahan-bahan rahsia.



Muka

Teknologi biometrik ini menggunakan imbasan imej muka iaitu reka bentuk muka sebagai pengesahan identiti seperti kedudukan hidung, mata, dagu dan mulut. Sistem pengenalpastian muka akan membuat analisis ke atas data dan membandingkannya dengan templat muka yang terdapat di dalam kad pintar (*smart card*) atau templat muka di dalam pangkalan data. Dari segi ketepatan, kaedah ini adalah kurang tepat jika imej muka yang diimbas dibandingkan dari sudut yang berbeza. Kaedah ini sesuai digunakan bagi mengesan penjenayah terutamanya di kawasan-kawasan tumpuan orang awam seperti di lapangan terbang dan sebagainya.



Suara

Kaedah imbasan suara membolehkan rakaman suara yang direkodkan, disimpan dalam komputer dalam jangka masa tertentu. Perisian bagi pengenalpastian suara individu akan merekodkan cara percakapan serta frekuensi setiap perkataan. Sistem yang baik akan dapat mengenal pasti suara percakapan walaupun berubah, contohnya serak. Kaedah ini sesuai digunakan bagi aplikasi yang banyak berinteraksi dengan suara. Antaranya, capaian kepada akaun bagi perkhidmatan perbankan dan pengenalpastian pelanggan bagi perkhidmatan panggilan oleh operator.

Pengecaman Asid Deoxyribonucleic (DNA)

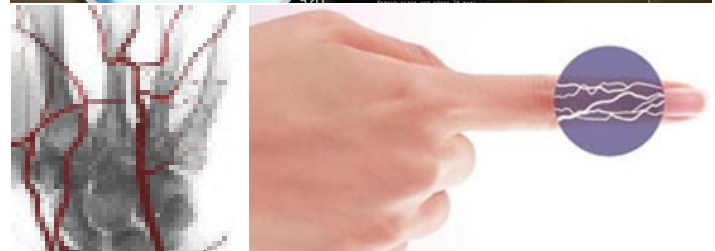
Kaedah identifikasi asid deoxyribonucleic (DNA) adalah kaedah pengecaman yang agak tepat berdasarkan hasil kajian yang menunjukkan kebarangkalian 2 individu berkongsi DNA yang sama adalah kurang dari satu bagi setiap seratus bilion. Walau bagaimanapun, kaedah ini sukar digunakan kerana agak kompleks serta memerlukan kemahiran yang tinggi. Kaedah ini biasa digunakan bagi mengenal pasti identiti seseorang individu yang tidak dapat dikenali melalui proses pengecaman secara fizikal.

Geometri Tangan

Pengenalpastian individu menggunakan kaedah imbasan tapak tangan adalah mudah dan ringkas. Kaedah ini menumpukan kepada tiga (3) dimensi bentuk tapak tangan iaitu merangkumi imej tapak tangan yang terdiri daripada panjang (*length*), tebal (*thickness*), struktur tulang, lengkungan (*curve*) dan jarak antara sendi tangan (*joints of the hand*). Sistem/alat imbasan tangan akan membuat pepadanan antara imej yang dibaca dengan imej yang telah didaftarkan.

Urut Saraf (Vein)

Kaedah pengesanan menggunakan urat saraf yang biasa dilakukan adalah melalui imbasan urat saraf pada tangan individu. Teknologi ini mengenal pasti corak urat saraf pada tangan individu. Antara urat saraf yang digunakan bagi pengesanan adalah urat saraf pada jari, pergelangan tangan, tapak tangan dan belakang tangan. Penggunaan urat saraf mempunyai kelebihan kerana urat saraf pada individu adalah unik coraknya dan tidak mudah bertukar. Selain itu, kedudukan urat saraf yang berada di bawah lapisan kulit menyebabkan kerosakan tidak mudah berlaku dan sukar untuk dipalsukan. Walau bagaimanapun kaedah ini agak mahal dan penggunaannya masih belum menyeluruh.



Tandatangan (*Signature*)

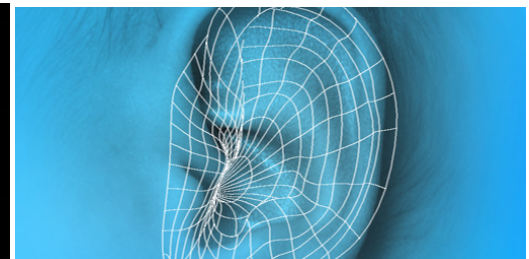
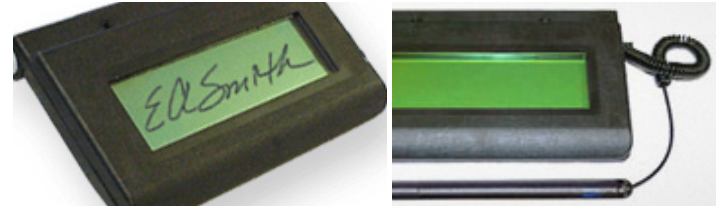
Kaedah pengesahan ini menggunakan imej tandatangan. Teknologi imbasan tandatangan akan meneliti dan menganalisis aspek-aspek seperti bentuk, *stroke order*, kecepatan dan tekanan sesuatu tandatangan dibuat dan membandingkan dengan tandatangan yang telah direkodkan bagi mengesahkan individu.

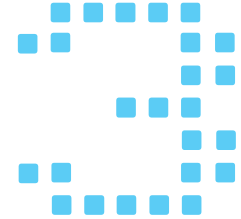
Keystroke

Imbasan *keystroke* adalah melalui kaedah/cara taipan di papan kekunci. Imbasan ini akan diukur melalui kawasan jari pengguna menekan kekunci, jangka masa pengguna menekan sesuatu kekunci dan perbezaan masa antara satu kekunci ke kekunci yang lain. Proses pengenalpastian akan membandingkan ciri-ciri tekanan kekunci dengan data sedia ada di dalam sistem untuk pengesahan. Kaedah ini sesuai digunakan oleh agensi yang menjalankan risikan dan aktiviti-aktiviti yang mendatangkan impak yang tinggi terhadap keselamatan negara.

Lain-lain

Selain kaedah pengesahan biometrik yang telah dinyatakan, terdapat beberapa kaedah lain yang tidak dikomersialkan antaranya adalah **pengecaman cara berjalan (*gait*)** dengan merekodkan cara individu melangkah, jarak luas setiap langkah, kelajuan berjalan dan masa kitaran (*cycle time*). Kaedah-kaedah pengecaman lain termasuk **imbasan suhu tangan** yang menggunakan struktur tisu di bawah lapisan kulit di telapak tangan, **imbasan suhu wajah** yang menggunakan bentuk infrared di bawah kulit muka, **pengecaman pergigian** dan **pengecaman struktur telinga**.





SISTEM BIOMETRIK

Sistem Biometrik pada dasarnya merupakan sistem pencetakan untuk mengesahkan (*verify*) atau mengenal pasti (*identify*) seseorang individu berdasarkan ciri-ciri biologi atau tingkah laku.

SISTEM BIOMETRIK

Fungsi-fungsi Sistem Biometrik

Secara umumnya fungsi-fungsi asas di dalam sistem biometrik adalah:

- (i) Pendaftaran (*Enrollment*);
- (ii) Pengesahan (*Verification*); dan
- (iii) Identifikasi (*Identification*).

Pendaftaran (*Enrollment*)

Dalam fungsi pendaftaran, sistem akan menjana dan menyimpan templat pendaftaran biometrik individu.

Pengesahan (*Verification*)

Pengesahan adalah fungsi di mana sistem mengesahkan identiti seseorang (*Am I who I claim I am?*). Pengesahan menggunakan kaedah pepadanan satu ke satu. Proses pengesahan dan pepadanan boleh dibuat dengan membandingkan sampel biometrik semasa yang diperolehi daripada individu dengan templat biometrik individu tersebut yang disimpan dalam sistem sama ada menggunakan media mudah alih ataupun pangkalan data.

Media mudah alih seperti kad pintar mengandungi hanya satu templat biometrik bagi individu untuk tujuan pengesahan. Sampel biometrik individu akan dibandingkan terus dengan templat biometrik yang terkandung dalam media mudah alih. Contoh kaedah pengesahan menggunakan media mudah alih ialah penggunaan biometrik cap jari untuk tujuan akses di lapangan terbang. Templat cap jari yang disimpan di dalam pasport akan dibandingkan dengan sampel cap jari pengguna yang diimbas di *auto gate*.

Bagi pengesahan dan pepadanan dengan templat biometrik dalam pangkalan data, data pengenalan awal seperti nombor atau id pengguna dimasukkan terlebih dahulu sebelum pepadanan dibuat memandangkan pangkalan data mempunyai banyak templat biometrik.

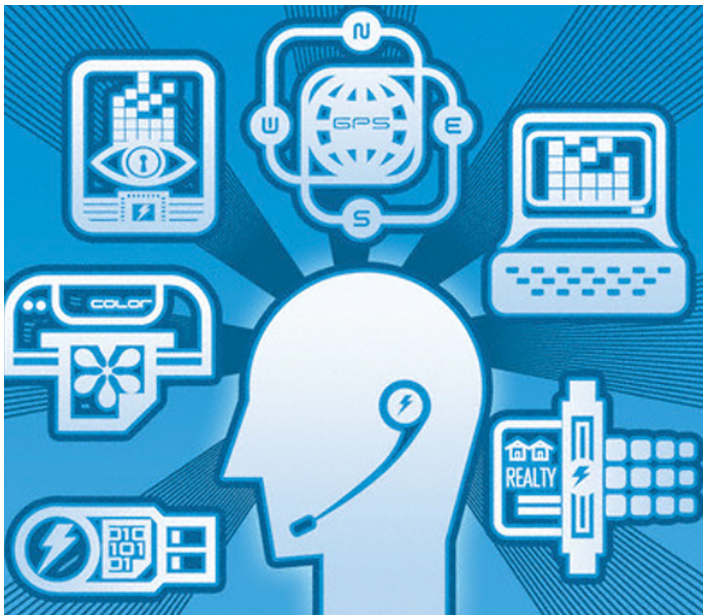
Contohnya adalah kaedah pengesahan menggunakan cap jari bagi mengakses sistem di mana pengguna akan memasukkan nombor atau id pengguna sebelum mengimbas cap jari untuk dibandingkan dengan templat cap jari pengguna di dalam pangkalan data.

Identifikasi

Identifikasi adalah fungsi di mana sistem perlu mengenal pasti identiti seseorang (*Who I am?*) daripada senarai pengguna yang sedia ada. Identifikasi memerlukan pepadanan satu ke banyak. Proses pengesahan dan pepadanan dilaksanakan dengan membandingkan ciri-ciri sampel biometrik semasa individu dengan kesemua templat yang ada di dalam sistem untuk mengenal pasti identiti individu.

Sebagai contoh, kaedah identifikasi digunakan bagi mengesan penjenayah, di mana ciri-ciri sampel biometrik yang diperolehi di tempat kejadian akan dibandingkan dengan data biometrik dari senarai suspek di pangkalan data.





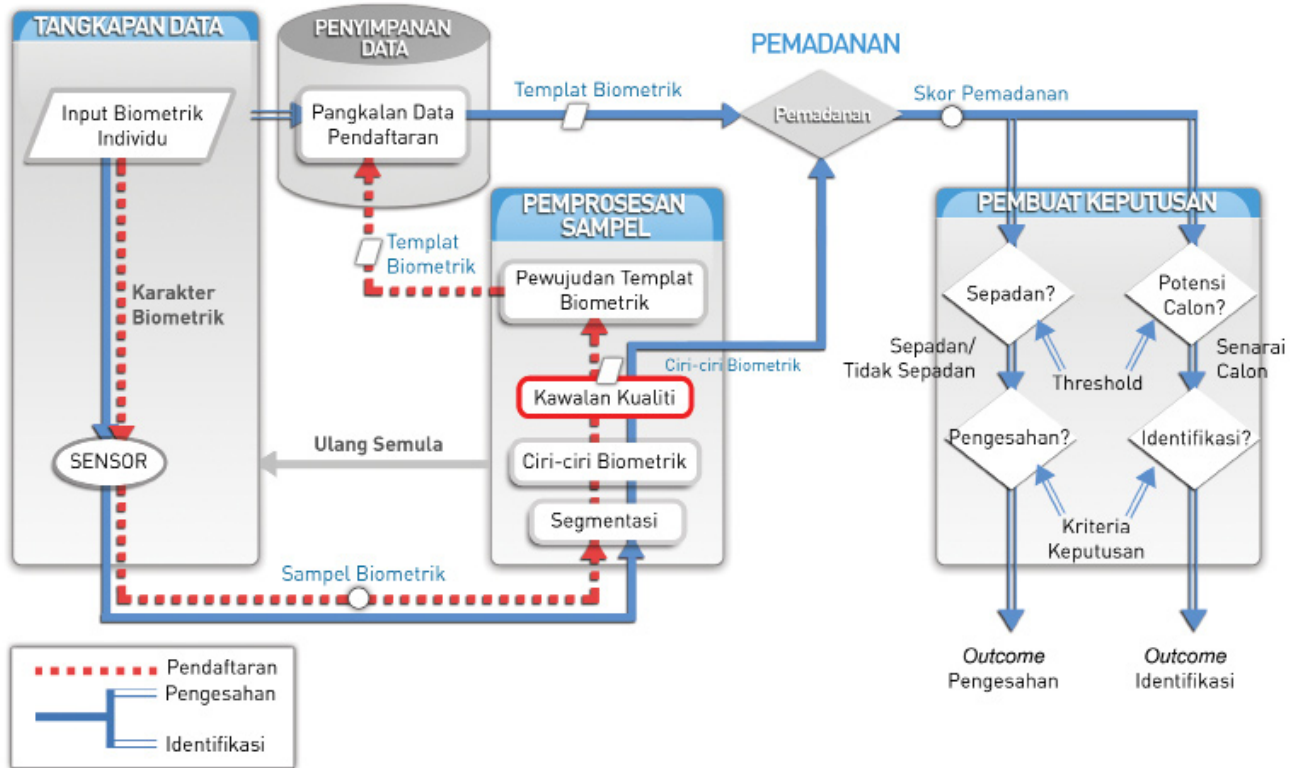
Komponen-komponen Sistem Biometrik

Secara umumnya komponen-komponen yang terkandung di dalam sistem biometrik adalah:

- (i) Subsistem Tangkapan Data (*Data Capture*)
- (ii) Subsistem Pemrosesan Sampel (*Sample Processing*)
- (iii) Subsistem Penyimpanan Data (*Data Storage*)
- (iv) Subsistem Pepadanan (*Matching*)
- (v) Subsistem Pembuat Keputusan (*Decision*)

Rajah 1 menunjukkan aliran maklumat di dalam sistem biometrik secara umumnya merangkumi tangkapan data, pemrosesan sampel, penyimpanan data, pepadanan dan penetapan keputusan. Rajah ini juga menunjukkan proses pendaftaran (*enrollment*) dan operasi pengesahan dan identifikasi. Kewujudan komponen-komponen tersebut di dalam sistem biometrik yang sebenar bergantung kepada komponen fizikal sistem berkenaan.

Rajah 1 : Komponen-komponen Asas Sistem Biometrik Secara Umum



Subsistem Tangkapan Data

Subsistem tangkapan data mengumpulkan imej karakter biometrik individu yang diterima daripada sensor sebagai input dan memprosesnya sebagai **sampel** biometrik.

Subsistem Pemprosesan Sampel

Subsistem pemprosesan sampel mengenal pasti ciri-ciri tertentu dari sampel biometrik dan melaksanakan kawalan kualiti bagi ciri-ciri tersebut. Sekiranya ciri-ciri tersebut tidak memenuhi kawalan kualiti, isyarat akan dihantar kepada subsistem tangkapan data supaya tangkapan data dilaksanakan semula.

Untuk tujuan pendaftaran, subsistem pemprosesan sampel akan mewujudkan **templat** dari ciri-ciri biometrik tersebut. Biasanya proses pendaftaran memerlukan ciri-ciri biometrik dari pelbagai posisi.

Subsistem Penyimpanan Data

Templat biometrik disimpan di dalam pangkalan data pendaftaran di bawah subsistem penyimpanan data. Setiap templat perlu mengandungi perincian individu yang didaftarkan. Templat perlu disimpan dalam format *biometric data interchange* untuk memudahkan perkongsian data dilaksanakan. Selain dari pangkalan data pendaftaran, templat juga boleh disimpan di dalam alat tangkapan data (*data capture device*), media mudah alih seperti *smart card* atau pangkalan data.

Subsistem Pemadanan

Dalam subsistem pemadanan, ciri-ciri sampel biometrik semasa yang diperoleh dipadankan dengan templat yang ada di dalam pangkalan data pendaftaran. Skor pemadanan yang menunjukkan tahap persamaan antara ciri-ciri sampel dan templat dikeluarkan dalam subsistem ini. Bagi tujuan pengesahan, pemadanan dibuat antara ciri-ciri sampel biometrik semasa dengan satu templat sahaja. Bagi tujuan identifikasi pula, ciri-ciri sampel biometrik tersebut dibandingkan dengan kesemua templat yang ada dalam pangkalan data dan skor pemadanan dikeluarkan bagi setiap perbandingan yang dibuat. Seterusnya, skor pemadanan tersebut dihantar kepada subsistem pembuat keputusan.

Subsistem Pembuat Keputusan

Subsistem pembuat keputusan menggunakan skor pemadanan bagi memutuskan *outcome* transaksi pengesahan atau identifikasi. Untuk tujuan pengesahan, ciri-ciri sampel biometrik semasa dianggap sama dengan templat yang dibandingkan jika skor perbandingan melebihi *threshold* yang ditetapkan. Templat yang mempunyai skor pemadanan yang melebihi *threshold* yang ditetapkan disenaraikan sebagai calon yang menyamai ciri-ciri sampel biometrik semasa yang dibandingkan untuk tujuan identifikasi.



Penggunaan Sistem Biometrik

Kebanyakan aplikasi biometrik digunakan untuk memenuhi tujuan berikut:

Kawalan Akses Fizikal

Kaedah biometrik digunakan untuk tujuan akses fizikal seperti perbandingan templat biometrik di dalam maklumat pasport/visa penumpang untuk memasuki negara lain dan kad akses pejabat untuk masuk ke bangunan/pejabat.

Kawalan Akses Logikal

Aplikasi biometrik juga boleh digunakan untuk kawalan akses logikal bagi mengenal pasti identiti pengguna yang melaksanakan transaksi secara atas talian (*online*) seperti *E-Banking*, *E-Commerce* dan *E-Government* menggantikan kawalan secara fizikal (*face-to-face*).

Pengenalan diri

Biometrik juga digunakan untuk tujuan pengesahan pengenalan diri. Sebagai contoh, templat biometrik cap jari individu dimasukkan dalam MyKad sebagai sebahagian dari dokumen pengenalan diri.

Forensik

Biometrik juga digunakan untuk tujuan forensik bagi pengecaman identiti. Sebagai contoh, pengesanan penjenayah oleh polis melalui cap jari dan juga pengecaman Asid Deoxyribonucleic (DNA).

Kebaikan Sistem Biometrik

Sistem biometrik mempunyai kelebihan berbanding dengan kaedah pengesahan lain kerana ciri-ciri biologi individu adalah unik dan tidak sama antara satu sama lain. Berbanding dengan kaedah lain seperti *Personel Identification Number* (PIN) ataupun kata laluan, kaedah biometrik sukar ditiru dan ini dapat menyukarkan pemalsuan identiti. Kaedah biometrik juga tidak memerlukan pengguna mengingati nombor pin atau kata laluan.

Kelemahan Sistem Biometrik

Antara perkara-perkara yang dikenal pasti menjadi kekangan dan boleh mempengaruhi penggunaan sistem biometrik ialah:

Faktor Fizikal dan Kesihatan Individu

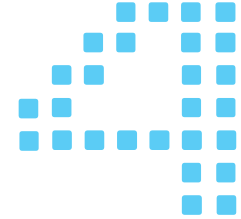
Faktor fizikal dan perubatan boleh mempengaruhi penggunaan dan ketepatan sistem biometrik. Contohnya, individu yang cacat penglihatan mengalami kesulitan untuk menyelaraskan kedudukan mata dengan kamera bagi sistem biometrik iris, manakala pesakit sendi sukar untuk meletakkan ibu jari/tangan di posisi sebenar alat pembaca. Ini juga termasuk semua jenis pembedahan yang akan merubah struktur asal ciri pengesanan seperti muka, mata, tangan dan lain-lain.

Risiko Kesihatan

Penggunaan sistem biometrik boleh mendatangkan risiko kepada individu di mana ada kemungkinan berlakunya kecederaan kepada sistem tubuh individu. Kesan secara langsung ialah risiko kecederaan disebabkan penggunaan alat-alat biometrik seperti *contact sensor*, penggunaan *UV light* serta lain-lain yang seumpamanya. Risiko lain ialah data biometrik individu boleh disalah guna untuk mendedahkan maklumat kesihatan seseorang.

Privasi

Sesetengah individu merasakan penggunaan data biometrik adalah bertentangan dengan hak privasi. Data-data biometrik yang diperoleh/simpan boleh digunakan untuk tujuan lain yang tidak dipersetujui oleh pengguna.



UKURAN PENILAIAN

Terdapat pelbagai ukuran penilaian yang digunakan untuk menilai keberkesanan sistem biometrik. Analisis terhadap pelbagai ukuran adalah penting bagi menentukan kekuatan dan kelemahan setiap produk. Pengujian bagi menilai ukuran penilaian perlu dilaksanakan untuk mendapat gambaran tahap keberkesanan sistem tersebut apabila digunakan.

UKURAN PENILAIAN

Berikut adalah ukuran yang biasa digunakan di peringkat global untuk menilai sistem biometrik:

False Match Rate (FMR)

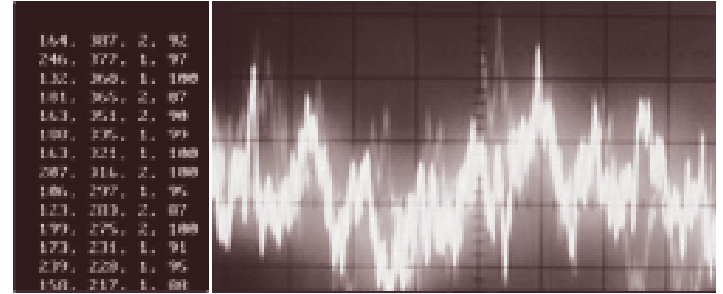
False Match Rate (FMR) digunakan bagi melihat kadar kebarangkalian sistem membuat kesilapan di mana, ciri-ciri sampel biometrik seseorang individu diterima sebagai berpadanan dengan templat individu yang berlainan di dalam sistem yang boleh menyebabkan seseorang pengguna yang tidak sah ataupun penceroboh mendapat akses kepada sistem. FMR juga dikenali sebagai *False Acceptance Rate* (FAR).

Nilai FMR 1% bermaksud bahawa, daripada 100 cubaan untuk mengakses sistem oleh pengguna yang tidak sah, kemungkinan 1 cubaan akan berjaya. Bagi aplikasi-aplikasi kritikal terutama yang berkait dengan keselamatan, nilai FMR mestilah rendah.

False Non Match Rate (FNMR)

False Non Match Rate (FNMR) pula digunakan bagi melihat kadar kebarangkalian sistem membuat kesilapan di mana ciri-ciri sampel biometrik seseorang individu tidak diterima sebagai berpadanan dengan templat individu tersebut di dalam sistem yang boleh menyebabkan seseorang pengguna yang sah tidak mendapat akses kepada sistem.

FNMR juga dikenali sebagai *False Rejection Rate* (FRR). Nilai FNMR 1% bermaksud bahawa, daripada 100 cubaan untuk akses kepada sistem oleh pengguna yang sah, kemungkinan 1 cubaan tidak berjaya. Bagi aplikasi biometrik yang kurang kritikal dari segi keselamatan tetapi melibatkan produktiviti seperti akses kakitangan kepada bangunan pejabat, nilai FNMR mestilah rendah.



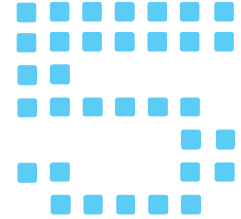
Failure To Enroll Rate (FTE)

Failure To Enroll (FTE) Rate pula merupakan kadar kebarangkalian seseorang pengguna tidak dapat didaftarkan ke dalam sesuatu sistem biometrik. Ini biasanya berlaku apabila reka bentuk sistem tersebut tidak dapat menerima data biometrik pengguna yang tidak bersesuaian. Sebagai contoh kes cap jari yang mempunyai parut tidak boleh diimbas ke dalam sistem. Nilai FTE 1% bermaksud bahawa, daripada 100 cubaan untuk mendaftar kepada sistem, kemungkinan 1 cubaan tidak akan berjaya.

Equal Error Rate (EER)

Equal Error Rate (EER) adalah keadaan apabila FMR dan FNMR adalah sama. Sebagai contoh, jika nilai FMR dan FNMR adalah 1%, nilai EER juga adalah 1%. EER biasanya digunakan untuk menguji ketepatan sistem biometrik di mana sistem dengan nilai EER yang lebih rendah mempunyai ketepatan yang lebih tinggi. Pemilihan sistem biometrik perlu mengambil kira ketiga-tiga ukuran FMR, FNMR dan FTE secara menyeluruh. Oleh kerana nilai FMR dan FNMR bagi sesuatu sistem biometrik ditentukan oleh threshold yang sama, apabila nilai FMR direndahkan, nilai FNMR akan menjadi tinggi dan sebaliknya.

FTE juga memberi kesan kepada FMR dan FNMR. Contohnya, jika sistem biometrik itu direka bentuk mempunyai FTE yang rendah agar lebih toleran kepada pelbagai variasi input, FMR akan menjadi tinggi, manakala jika sistem tersebut direka bentuk dengan FTE yang tinggi di mana variasi input dikurangkan, FNMR pula akan menjadi tinggi.



PERTIMBANGAN PENGGUNAAN TEKNOLOGI BIOMETRIK DI AGENSI

Agensi perlu menjalankan analisis keperluan sama ada teknologi biometrik diperlukan sebelum membuat keputusan menggunakannya.

PERTIMBANGAN PENGGUNAAN TEKNOLOGI BIOMETRIK DI AGENSI

Berikut adalah di antara perkara-perkara yang perlu dipertimbangkan:

Peningkatan dan Keberkesanan Perkhidmatan

Penggunaan biometrik boleh meningkatkan kecekapan dan keberkesanan penyampaian perkhidmatan agensi. Contohnya penggunaan biometrik boleh mengurangkan kes penipuan dan menjimatkan masa pemrosesan.

Keselamatan

Penggunaan biometrik boleh meningkatkan tahap keselamatan fizikal bagi lokasi tertentu atau tahap keselamatan logikal bagi sistem aplikasi terutamanya yang melibatkan capaian kepada maklumat sulit atau rahsia.

Kesediaan Pelanggan

Kesediaan pelanggan terutamanya dari kalangan orang awam untuk menggunakan kaedah biometrik perlu diambil kira sebelum menggunakan teknologi ini. Sikap pelanggan terhadap penggunaan teknologi ini boleh memberi kesan terhadap prestasi penggunaan sistem.

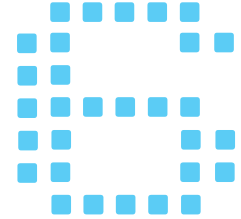
Polisi/Perundangan

Agensi perlu mengkaji sama ada penggunaan biometrik dilindungi dan diiktiraf dari segi perundangan/polisi sedia ada. Jika tidak, agensi perlu melihat kemungkinan untuk membuat pindaan sekiranya terdapat keperluan. Sebagai contoh, jika akta yang berkaitan dengan perkhidmatan di agensi menyatakan pengesahan identiti seseorang adalah cukup dengan dokumen pengenalan, akta tersebut perlu dipinda dengan memasukkan elemen penggunaan biometrik jika agensi ingin menguatkuasakan penggunaan biometrik bagi meningkatkan faktor keselamatan. Agensi perlu melihat kemungkinan untuk membuat pindaan terhadap akta sedia ada sekiranya terdapat keperluan.

Kos

Penggunaan teknologi biometrik perlulah kos efektif. Analisis kos dan faedah (*cost-benefit*) perlu dibuat sebelum teknologi biometrik digunakan. Jika penggunaan biometrik memberi impak yang tinggi, elemen kos mungkin menjadi kurang penting berbanding faedah yang diperoleh.





PERTIMBANGAN PEMILIHAN SISTEM BIOMETRIK

Apabila merancang untuk menggunakan teknologi biometrik, terdapat beberapa faktor yang perlu dipertimbangkan oleh agensi dalam memilih sistem biometrik yang bersesuaian.

PERTIMBANGAN PEMILIHAN SISTEM BIOMETRIK

Berikut adalah antara perkara-perkara yang perlu diberi perhatian:

Ciri-ciri Keselamatan

Ciri-ciri keselamatan sistem biometrik perlu diambil kira untuk mengelakkan ancaman keselamatan apabila menggunakan teknologi biometrik. Ciri-ciri keselamatan sistem biometrik yang dipilih perlu bersesuaian dengan tahap kerahsiaan maklumat.

Ancaman-ancaman keselamatan yang mungkin berlaku dan perlu ditangani adalah:

- Penggunaan salinan sampel biometrik (contohnya: suara yang direkodkan ataupun foto muka);
- Penggunaan sampel biometrik pengguna secara paksa (contoh: jari yang dipotong);
- Pencerobohan dengan meniru sampel biometrik pengguna (contoh: suara, tandatangan);
- Pendaftaran dalam sistem secara tidak sah;
- Pencerobohan data dalam pangkalan data sistem; dan
- Pencurian data melalui rangkaian.



Langkah-langkah keselamatan yang perlu dipertimbangkan adalah seperti berikut:

- Mengenal pasti kemungkinan terdapat ancaman keselamatan bagi setiap langkah dalam proses kerja dan menyediakan langkah-langkah untuk mengatasinya;
- Memastikan sistem mempunyai jejak audit bagi merekodkan sebarang akses kepada sistem;
- Memastikan sistem mempunyai fungsi '*lockout*' atau alarm apabila akses yang tidak sah dilakukan berkali-kali melebihi had yang ditetapkan;
- Memastikan data disimpan di dalam server yang khusus (*dedicated*) dan selamat untuk mengelak dari pencerobohan;
- Memastikan transmisi data biometrik adalah selamat. Jika perlu, data hendaklah *diencrypt*; dan
- Memastikan sistem biometrik dapat mengenal pasti data biometrik yang sebenar dan palsu.

Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia (MyMIS) perlu dirujuk dalam memastikan aspek keselamatan sistem biometrik di agensi dipenuhi.



Kesesuaian dengan Pengguna

Sistem perlu boleh digunakan oleh majoriti pengguna. Jika terdapat masalah di mana sampel biometrik pengguna tidak dapat didaftarkan, kaedah alternatif perlu disediakan. Contohnya, bagi pengguna cacat penglihatan yang tidak dapat didaftarkan melalui sistem yang menggunakan teknologi iris, kaedah alternatif perlu disediakan. Terdapat sistem biometrik multi-model di mana kombinasi lebih dari satu teknologi biometrik digunakan. Ini bergantung pada keperluan kerana sistem biometrik multi-model melibatkan kos dan proses tambahan.

Mesra Pengguna

Sistem biometrik perlu mudah untuk digunakan oleh pengguna dan operator sistem. Antara amalan terbaik bagi memudahkan penggunaan aplikasi biometrik meliputi perkara-perkara berikut:

- Penggunaannya mestilah ringkas dan secara automatik;
- Alat pembaca perlulah fleksibel, di mana karakter biometrik individu boleh diimbas dari pelbagai posisi;
- Mengambil kira keperluan Orang Kurang Upaya (OKU);
- Menyediakan arahan penggunaan yang mudah difahami antaranya seperti berikut:
 - Arahan disediakan secara berturutan (audio atau paparan sistem);
 - Memaklumkan pengguna jika sesuatu langkah itu berjaya atau perlu diulangi;
 - Memaklumkan pengguna jika pembaca/pengimbas memerlukan tindakan pengguna
 - Pengguna yang biasa menggunakan sistem diberi pilihan untuk tidak menggunakan arahan audio (*skip audio instruction*).

Kebolehpercayaan (*reliability*)

Sistem biometrik perlu *reliable* bagi memastikan penggunaannya tidak terganggu dalam jangka masa yang ditetapkan seperti 24 jam sehari dan sebagainya. Dalam hal ini, *down time* bagi sistem perlu minimum. Agensi juga perlu mengkaji alternatif seperti proses penduaan (*backup*) dan sebagainya. Sebagai contoh, perkhidmatan sistem biometrik di kiosk perlu mempunyai tahap *reliability* yang tinggi berbanding penggunaan di kaunter yang hanya beroperasi semasa waktu pejabat.

Keupayaan sistem

Keupayaan sistem pemrosesan komputer dan saiz storan perlu diambil kira mengikut keperluan. Keupayaan sistem pemrosesan komputer akan mempengaruhi tahap kelajuan sistem semasa melaksanakan sesuatu proses, contohnya semasa pendaftaran (*enrollment*) dan pengenalpastian (*authentication*). Bagi proses identifikasi yang melibatkan kaedah pemedanan 1 ke banyak, bilangan data di dalam sistem juga mempengaruhi kelajuan sistem. Saiz storan yang diperlukan mesti mengambil kira saiz templat biometrik yang disimpan dan bilangan pengguna.



Prestasi Ukuran Penilaian

Adalah mustahil untuk mendapatkan sistem yang boleh mencapai prestasi ketepatan 100% setiap masa. Oleh itu, agensi perlu menetapkan nisbah penerimaan ralat (*error tolerance rate*) bagi sistem biometrik yang ingin diperolehi.

Prestasi sistem boleh dinilai menggunakan ukuran penilaian biometrik FMR dan FNMR. Nilai kedua-dua ukuran perlulah dikenal pasti untuk mengambil kira nisbah kesilapan yang mungkin berlaku.

False Match berlaku apabila sistem biometrik individu yang menyamar sebagai pengguna yang sah dibenarkan akses kepada sistem. Agensi perlu menetapkan kadar FMR yang boleh diterima untuk mengelakkan pencerobohan ke dalam sistem oleh pengguna yang tidak sah.

False Non Match berlaku apabila sistem biometrik gagal mengenal pasti pengguna yang sah menyebabkan pengguna tersebut tidak dibenarkan akses kepada sistem. Perkara ini kadang kala disebabkan perubahan kepada data biometrik pengguna. Ini juga boleh berlaku jika data biometrik pengguna tidak *dicapture* oleh peralatan dengan betul. Agensi perlu menetapkan kadar FNMR yang boleh diterima untuk mengurangkan insiden halangan akses kepada pengguna yang sah.



Pengujian

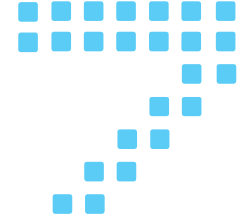
Pengujian dan penandaarasan terhadap sistem biometrik yang dinilai perlu dijalankan untuk memastikan kesesuaian dan kualiti sistem tersebut sebelum perolehan dibuat. Pengujian yang dibuat perlu mengambil kira aspek keselamatan, kebolehpercayaan (*reliability*), ketepatan dan keberkesanan sistem.

Berikut adalah faktor-faktor yang boleh mempengaruhi prestasi sistem biometrik dan perlu di ambil kira semasa pengujian:

- Cubaan pemalsuan/pencerobohan;
- Ciri-ciri biologi atau tingkah laku (*behaviora*) individu seperti warna kulit, jantina, umur, ketinggian, pekerjaan, kesihatan dan lain-lain. Individu-individu yang terlibat dengan pengujian perlulah mewakili pelbagai sifat biologi dan tingkahlaku yang berlainan.
- Perubahan pada sifat biometrik contohnya disebabkan faktor umur dan kecederaan;
- Prestasi sensor; dan
- Persekitaran yang mempengaruhi peralatan biometrik seperti suhu, kelembapan, cahaya dan lain-lain.

Penyelenggaraan

Bagi tujuan penyelenggaraan sistem biometrik, faktor-faktor seperti kekerapan dan kompleksiti perlu diambil kira untuk menentukan sama penyelenggaraan perlu dilaksanakan secara dalaman atau memerlukan sokongan pembekal. Sekiranya sokongan pembekal diperlukan, keupayaan sokongan pembekal perlu diambil kira.



STANDARD-STANDARD BIOMETRIK

Pematuhan kepada standard biometrik adalah penting untuk memastikan interoperability dan membolehkan perkongsian data di kalangan agensi pengguna biometrik. Antara standard yang perlu dipatuhi ialah *Biometric Application Programming Interface (API)* dan *Common Biometric Exchange File Format (CBEFF)*.

STANDARD-STANDARD BIOMETRIK

Penggunaan standard juga dapat mengelakkan masalah apabila peningkatan atau penggantian sistem biometrik sedia ada perlu dilaksanakan.

ISO/IEC JTC 1/SC 37 *Biometrics*

ISO (*International Organization for Standardization*) dan IEC (*International Electrotechnical Commission*) merupakan badan standard di peringkat antarabangsa. Dalam bidang ICT, ISO dan IEC telah menubuhkan *Joint Technical Committee* JTC1. Dalam tahun 2002, JTC1 telah menubuhkan *sub-committee* 37 (SC 37) bagi bidang biometrik. Matlamat JTC1 SC 37 adalah untuk membangunkan standard-standard bagi biometrik. Ahli-ahli SC 37 terdiri daripada badan-badan standard pelbagai negara termasuk Malaysia. SC 37 mempunyai kumpulan-kumpulan kerja (*working group*) seperti berikut:

WG 1 - *Harmonized Biometric Vocabulary*

WG 1 berperanan untuk membangunkan konsep, terminologi dan definisi standard bagi biometrik di peringkat antarabangsa. Penggunaan standard ini dapat menyelaraskan perbendaharaan kata (*vocabulary*) bagi biometrik dan mengurangkan kekeliruan terutamanya dari segi bahasa. Contoh standard yang dibangunkan di bawah WG 1 adalah ISO 2382-37 *Information Processing Systems – Vocabulary – Part 37: Biometrics*.

WG 2 - *Biometric Technical Interfaces*

WG 2 berperanan untuk membangunkan standard bagi antara muka dan interaksi antara komponen-komponen dan subsistem biometrik. Standard-standard yang dibangunkan mengambil kira model bagi reka bentuk dan operasi sistem biometrik untuk menyokong sistem biometrik dari pelbagai pembekal yang berbeza. Dengan adanya standard ini, produk-produk biometrik boleh berinteraksi antara satu dengan yang lain. Contoh standard yang dibangunkan di bawah WG 2 adalah seperti berikut:

- ISO/IEC 19784-1:2006 *Information Technology – Biometric Application Programming Interface - Part 1: BioAPI Specification*; dan
- ISO/IEC 19784-2:2007 *Information Technology – Biometric Application Programming Interface - Part 2: Biometric Archive Function Provider Interface*.

WG 3 - *Biometric Data Interchange Formats*

WG 3 merupakan kumpulan kerja yang berperanan membentuk standard format data biometrik dari segi kandungan dan makna, bagi membolehkan pertukaran data biometrik antara satu sistem biometrik ke sistem yang lain tanpa mengira jenis platform yang digunakan.

Contoh standard yang dibangunkan di bawah WG 3 adalah seperti berikut:

- ISO/IEC 19794-1:2006 *Information Technology –Biometric Data Interchange Formats – Part 1: Framework*;
- ISO/IEC 19794-3:2006 *Information Technology –Biometric Data Interchange Formats – Part 3: Finger Pattern Spectral Data*; dan
- ISO/IEC 19794-8:2006 *Information Technology –Biometric Data Interchange Formats – Part 8: Finger Pattern Skeletal Data*.

WG 4 - *Biometric Functional Architecture and Related Profiles*

WG 4 berperanan untuk membangunkan standard berkaitan arkitektur fungsi biometrik dan profil standard-standard biometrik yang berkaitan dengan fungsi tersebut bagi membolehkan *interoperability*.

Contoh standard yang dibangunkan di bawah WG 4 adalah seperti berikut:

- ISO/IEC 24713-2 *Information Technology - Biometric Profiles for Interoperability and Data Interchange - Part 2: Physical Access Control for Employees at Airports*; dan
- ISO/IEC 24713-2 *Information Technology - Biometric Profiles for Interoperability and Data Interchange – Part 3: Biometric-Based Verification and Identification of Seafarer*.

WG 5 - Biometric Testing and Reporting

WG 5 berperanan untuk membangunkan standard yang berkaitan dengan kaedah pengujian dan pelaporan sistem biometrik merangkumi teknologi, sistem dan komponen biometrik.

Contoh standard yang dibangunkan di bawah WG 5 adalah seperti berikut:

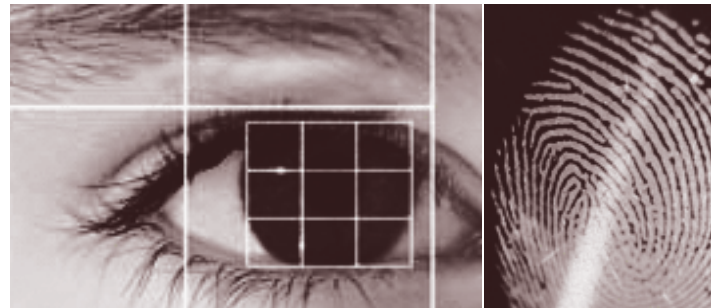
- ISO/IEC 19795-1:2006 *Information Technology - Biometric Performance Testing and Reporting - Part 1: Principles and Framework*; dan
- ISO/IEC 19795-2:2007 *Information Technology - Biometric Performance Testing and Reporting - Part 2: Testing Methodologies for Technology and Scenario Evaluation*.

WG 6 - Cross-Jurisdictional and Societal Aspects of Biometrics

WG 6 berperanan untuk membangunkan standard yang berkaitan penggunaan biometrik dari aspek sosial dan perundangan. Dari aspek sosial, standard yang dibangunkan merangkumi perancangan dan pelaksanaan teknologi biometrik dari segi *accessibility*, kesihatan dan keselamatan serta pertimbangan masyarakat berhubung dengan maklumat peribadi. Standard ini juga merangkumi sokongan perundangan bagi penggunaan biometrik.

Contoh standard yang dibangunkan di bawah WG 6 adalah seperti berikut:

- ISO/IEC TR 24714-1 *Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies - Part 1: Guide to the Accessibility, Privacy and Health and Safety Issues in Deployment of Biometric Systems for Commercial Application*; dan
- ISO/IEC TR 24714-2 *Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies - Part 2: Practical Application to Specific Contexts*.



Standard-standard yang telah dikeluarkan (Published Standards)

Standard-standard biometrik yang telah diguna pakai di peringkat antarabangsa boleh dirujuk dari laman web http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=313770 dengan memilih pada pautan "Number of published ISO standards under the direct responsibility of JTC 1/SC 37".

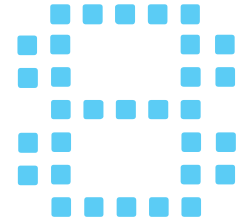
Standard-standard dalam peringkat pembangunan (Standards under development)

Standard-standard biometrik yang masih dalam peringkat pembangunan boleh dirujuk dari laman web http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=313770 dengan memilih pada pautan "Work programme (drafts and new work items of JTC 1/SC 37)".

Standard Malaysia

Malaysia juga terlibat dalam usaha-usaha pembangunan standard biometrik di dalam negara dan di peringkat antarabangsa. Jabatan Standard Malaysia dan SIRIM merupakan badan standard yang bertanggungjawab untuk mengenal pasti standard-standard biometrik yang sesuai digunakan dalam persekitaran Malaysia. Jawatankuasa Teknikal Biometrik atau *Technical Committee for Biometrics* (TC 10) telah ditubuhkan pada Oktober 2003 di mana skop kerja TC 10 merangkumi pembangunan standard bagi teknologi biometrik yang menyokong *interoperability* dan pertukaran data merentasi aplikasi. Jawatankuasa ini berperanan mengikuti secara menyeluruh aktiviti-aktiviti standard di peringkat kebangsaan dan antarabangsa di mana Malaysia merupakan *participating member* bagi ISO/IEC JTC1/SC 37-Biometrics. Bagi memastikan standard-standard yang diterima pakai sebagai standard Malaysia adalah berkualiti, praktikal dan memelihara kepentingan bersama, maklum balas diperoleh daripada pelbagai organisasi seperti Kerajaan, swasta, persatuan, penyelidik dan universiti. Maklum balas tersebut dijadikan input dalam aktiviti pembangunan standard. Standard-standard Malaysia berkaitan biometrik boleh dirujuk dari laman web <http://msonline.sirim.my> dengan memilih pada pautan "Advanced Search" dan seterusnya melaksanakan carian standard-standard biometrik berkaitan.





PENUTUP

PENUTUP

Penggunaan teknologi biometrik mempunyai potensi yang besar dalam meningkatkan penyampaian perkhidmatan Sektor Awam terutamanya dari aspek keselamatan dan integriti. Agensi-agensi hendaklah merujuk kepada garis panduan ini apabila merancang untuk melaksanakan teknologi biometrik di agensi masing-masing.

SUMBER RUJUKAN

- *Biometric for Identification and Authentication Advice on Product Selection – Issue 2.0 by UK Biometrics Working Group*
- *Introduction to Biometrics Technology* oleh Universiti Teknologi Malaysia
- *Overview of Biometrics Technology* oleh Universiti Teknologi Malaysia
- *Biometrics Standards Today by Business Information*
- <http://www.iso.org>
- <http://www.sirim.my>
- <http://www.bromba.com>
- <http://biometrics.cse.msu.edu>
- <http://www.tiresias.org/guidelines>
- <http://www.globalsecurity.org/security/systems/biometrics.htm>
- <http://www.biometrics.org>
- <http://ieeexplore.ieee.org>
- <http://biometrics.cse.msu.edu>



Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)

Jabatan Perdana Menteri

Aras 6, Blok B2

Kompleks Jabatan Perdana Menteri

Pusat Pentadbiran Kerajaan Persekutuan

62502 Putrajaya

www.mampu.gov.my