

SESI PERKONGSIAN ILMU KESELAMATAN SIBER: PANDUAN TEKNIKAL KESELAMATAN SIBER GERBANG PERKHIDMATAN DALAM TALIAN KERAJAAN



Gerbang Rasmi Kerajaan Malaysia
MyGovernment



3.00-4.00 petang

SEP, 2020

24

Khamis

Oleh: **Nur Hidayah binti Abdullah**
Perunding ICT (Pengurusan Keselamatan Maklumat)
Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia

MAMPU
BERSAMA-SAMA MELAKSANAKAN TRANSFORMASI

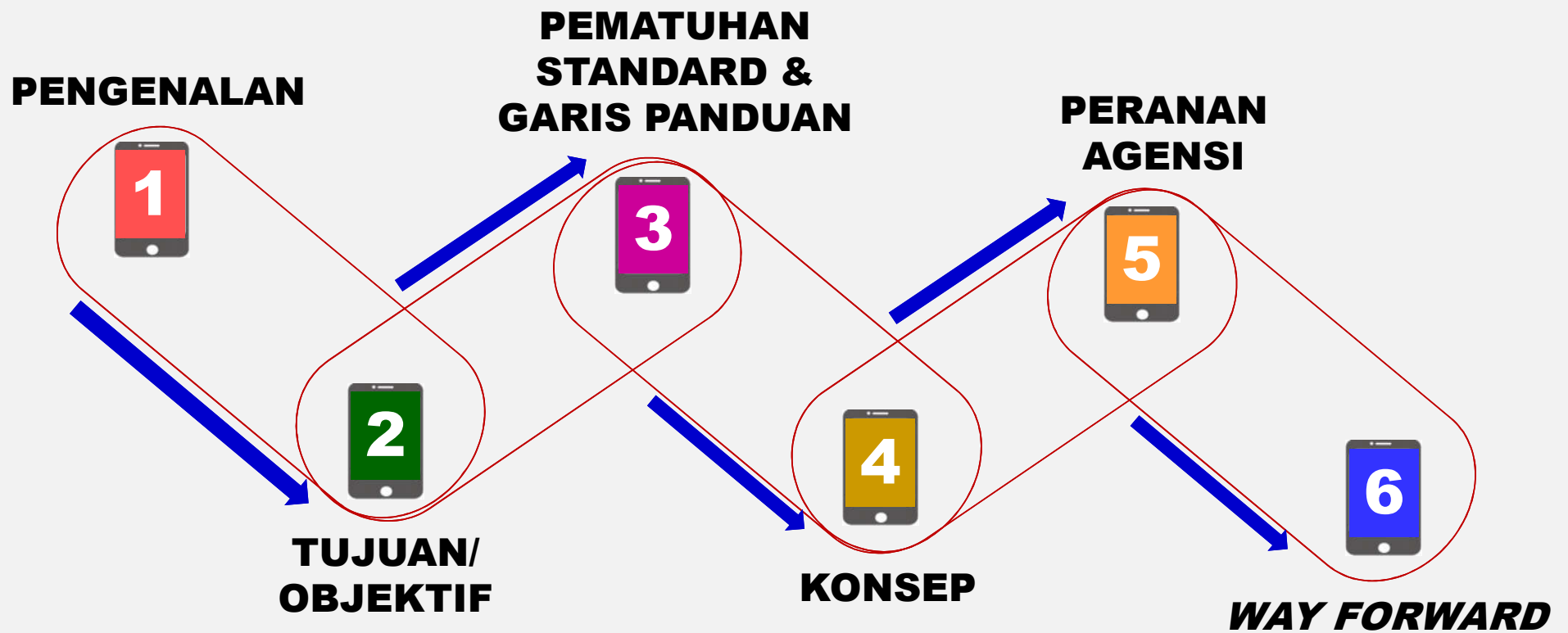


Hotel Avenue Garden,
Bangi





KANDUNGAN





PENGENALAN

Portal/Gerbang rasmi Kerajaan Malaysia www.malaysia.gov.my



INFORMASI MENGIKUT PERISTIWA KEHIDUPAN

- 1 Menyediakan penyampaian perkhidmatan digital Kerajaan yang lancar (*seamless*) melalui konsep *whole of government*
- 2 Menyediakan perkhidmatan digital *end-to-end* yang menyeluruh, berkualiti dan selamat
- 3 Menyediakan informasi dan perkhidmatan digital yang komprehensif dan mesra rakyat

Portal MyGovernment

merupakan salah satu inisiatif MAMPU bagi mewujudkan **Gerbang Tunggal Kerajaan** yang berkonsepkan **peristiwa kehidupan** dan **berpaksikan rakyat**





2

TUJUAN/OBJEKTIF



Menerangkan & berkongsi dengan para peserta *Bootcamp* mengenai

Panduan Teknikal Keselamatan Siber Gerbang Perkhidmatan Dalam Talian Kerajaan Versi 1.0

(ruangan CAPAIAN > Penerbitan di Portal MyGovernment)

Garis Panduan Gerbang Perkhidmatan Dalam Talian Kerajaan (MyGovernment)

- 1 Menyediakan panduan pembangunan laman web berdasarkan *life-event* dan berpaksikan rakyat
- 2 Menyediakan panduan kepada pembangunan dan penyenggaraan perkhidmatan dalam talian kerajaan bagi mewujudkan keseragaman interaksi portal MyGovernment dan perkhidmatan dalam talian agensi

Manual | Mengenai Kami

Warna Tema: [] Saiz Tulisan: [A+] Jenis Tulisan: Arial

MyGovernment

Laman Utama | Topik | MyInfo

Laporan Kewangan

Penerbitan Mengikut Agensi

Garis panduan ini terdiri daripada:

1. Garis Panduan Keperluan Pengguna
2. Garis Panduan Kebolehgunaan Web
3. Garis Panduan Penggunaan Web Servis
4. Panduan Teknikal Keselamatan Siber
5. Garis Panduan Reka Bentuk Visual
6. Garis Panduan Strategi Kandungan
 - i. Prosedur Operasi Standard (SOP) Strategi Pembangunan Kandungan
 - ii. Prosedur Operasi Standard (SOP) Pengurusan Kandungan

*Garis panduan ini akan dikemaskini mengikut keperluan dari semasa ke semasa

<https://www.malaysia.gov.my/media/uploads/1eeecc16-6e6e-4c5e-806b-946236f2ed30.pdf>

HUBUNGI KAMI

UNIT PEMODENAN TADBIRAN DAN PERANCANGAN
PENGURUSAN MALAYSIA

Aras 6, Setia Perdana 2,
Kompleks Setia Perdana,
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya
Malaysia

2.9370395,101.6955217
603 8000 8000

CAPAIAN

My Kalendar	Langganan
E-Penyertaan	Perkhidmatan Dalam Talian
Direktori Agensi	Perlindungan Data Peribadi
Ketua Pegawai Maklumat (GCIO)	Enakmen Kebebasan Maklumat
Aduan & Maklum Balas	Suapan RSS
Penerbitan	Galeri
Statistik Dalam Talian	



PEMATUHAN STANDARD & GARIS PANDUAN

1 **Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)**

2 **Pelan Pengurusan Keselamatan Maklumat (ISMP) berdasarkan RAKKSSA**

3 **Penilaian Pematuhan, Pemantauan & Penyelenggaraan ISMP**

1 Pematuhan Pengurusan Keselamatan Maklumat (ISMS)

2 Pelan Pemulihan Bencana (DRP)

3 Capaian menggunakan Saluran Selamat – TLS versi 1.2

4 Log Transaksi sekurang-kurangnya 6 Bulan – mengambil kira Sandaran (*Back-up*) di Luar Premis

5 Pemantauan ke atas Trafik Rangkaian

4 **Mematuhi semua Arahan Keselamatan Maklumat yang sedang Berkuat Kuasa**

5 **Mematuhi Peraturan yang sedang Berkuat Kuasa**

6 ***Personally Identifiable Information (PII)* – mengambil kira kawalan-kawalan sepadan dengan risiko yang dinyatakan dalam RAKKSSA**



4

KONSEP



THE GAINING ACCESS PROCESS



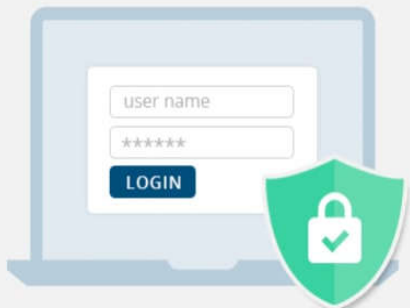
1. Authentication

- Verifies you are who you say you are
- Methods:
 - Login form
 - HTTP authentication
 - HTTP digest
 - X.509 certificates
 - Custom authentication method

2. Authorization

- Decides if you have permission to access a resource
- Methods:
 - Access controls for URLs
 - Secure objects and methods
 - Access control lists (ACLs)

Authentication



Who are you?

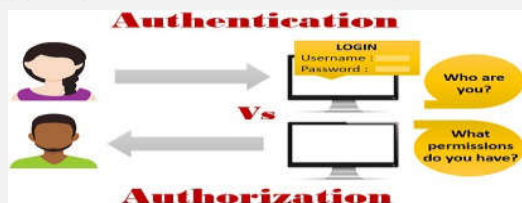
Validate a system is accessing by the right person

Authorization



Are you allowed to do that?

Check users' permissions to access data



Authentication

Authentication confirms your identity to grant access to the system.

It is the process of validating user credentials to gain user access.

It determines whether user is what he claims to be.

Authentication usually requires a username and a password.

Authentication is the first step of authorization so always comes first.

For example, students of a particular university are required to authenticate themselves before accessing the student link of the university's official website. This is called authentication.

Authorization

Authorization determines whether you are authorized to access the resources.

It is the process of verifying whether access is allowed or not.

It determines what user can and cannot access.

Authentication factors required for authorization may vary, depending on the security level.

Authorization is done after successful authentication.

For example, authorization determines exactly what information the students are authorized to access on the university website after successful authentication.

Sumber: <https://medium.com/@audira98/authorization-and-authentication-cd0a7c994278>

**Authentication**

1. Standard ISO/IEC 29115 – *Entity Authentication Assurance Framework*
2. Tahap Jaminan/Level of Assurance (LoA) – sekurang-kurangnya LoA 3
3. Penilaian Pematuhan Tahap Jaminan

Credential

1. Agensi yang Menguruskan Akuan – Sama atau Berbeza
2. Akuan Tunggal – *Credential Management System (CMS)*
3. CMS Disahkan Kerajaan berdasarkan Standard dan Garis Panduan
4. Mematuhi Standard
 - Pengesahan Identiti LoA 3 – *Single Factor Credential*
 - Pengesahan Identiti LoA 4 – *Two Factor Credential*

SSO

1. Akuan Tunggal – Pengguna Berdaftar sahaja
2. Akuan Tunggal melalui Satu Log Masuk sahaja – sekurang-kurangnya LoA 3
3. Mematuhi Standard – Pengesahan Identiti melalui Standard SAML 2.0

Authorisation

Kebenaran Capaian Perkhidmatan berdasarkan Capaian Minimum (*Least Privileged Access*)

Indeks Umum – IC

Menggunakan Indeks Umum untuk Kebenaran Capaian

- Nombor Kad Pengenalan – Warganegara
- Nombor Pasport – Bukan Warganegara



PANDUAN TEKNIKAL KESELAMATAN SIBER
GERBANG PERKHIDMATAN DALAM TALIAN KERAJAAN
(MyGOVERNMENT)

VERSI 1.0



VERSI
2.0

Garis Panduan Integrasi *Single Sign-On* Aplikasi Agensi Sektor Awam dengan Portal MyGovernment

MyGovSSO

Panduan **komprensif** dalam mengurus projek **integrasi SSO** aplikasi-aplikasi agensi sektor awam dengan Portal MyGovernment

Panduan **standard** supaya **integrasi SSO** aplikasi-aplikasi agensi sektor awam dilaksanakan dengan cara yang lebih **konsisten dan teratur**

Dalaman



Pelaksanaan
Integrasi SSO



Luaran/
Outsourcing

Co-sourcing
(Gabungan Dalam dan
Outsourcing)



JABATAN PERDANA MENTERI
UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA
(MAMPU)



Terima kasih

Unit Pengurusan Keselamatan Maklumat, BPI



hidayah@mampu.gov.my/pkeselamatan@mampu.gov.my

Maklumat yang dipaparkan dalam slaid ini adalah hak milik
Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri.
Sebarang salinan hendaklah mendapat persetujuan dan kelulusan MAMPU.