SESI PERKONGSIAN ILMU KESELAMATAN SIBER:

PANDUAN TEKNIKAL KESELAMATAN SIBER GERBANG PERKHIDMATAN DALAM TALIAN KERAJAAN

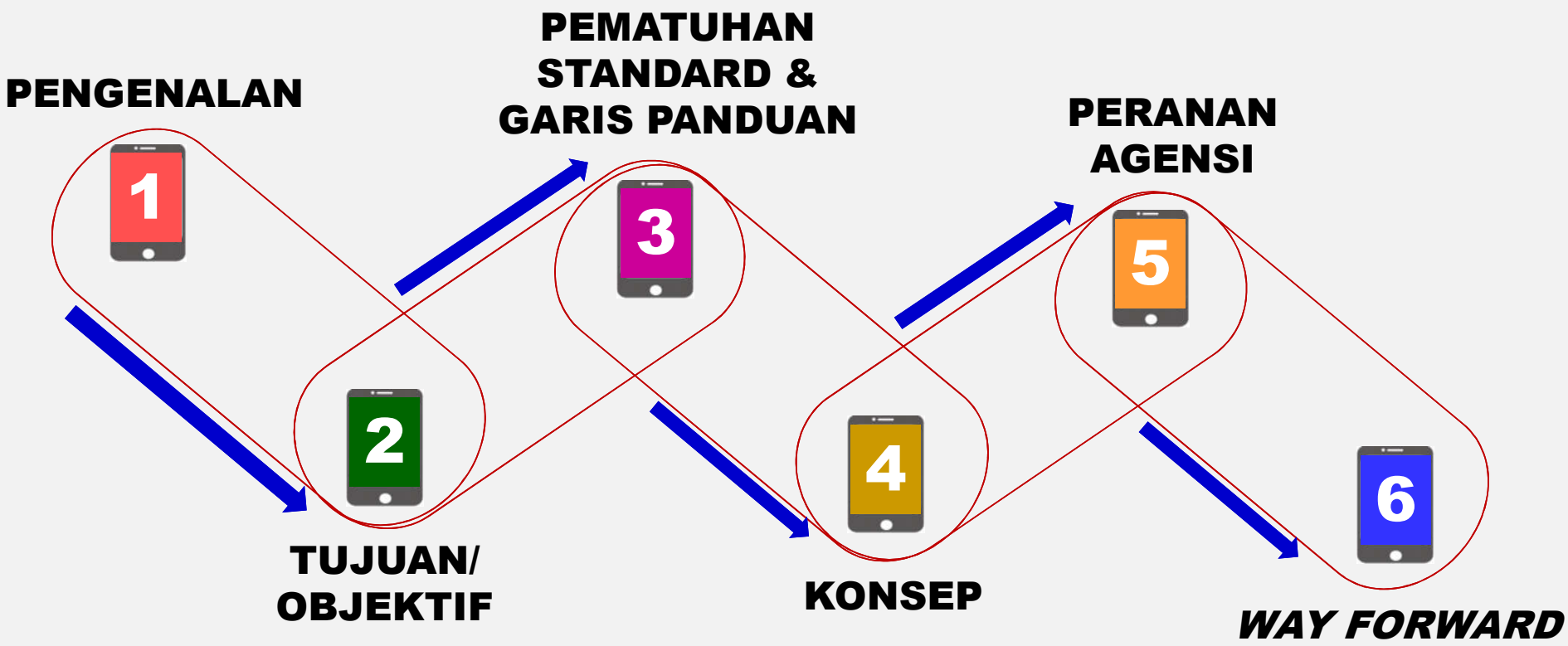
Gerbang Rasmi Kerajaan Malaysia
MyGovernment

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

MAMPU
BERSAMA-SAMA MELAKSANAKAN TRANSFORMASI

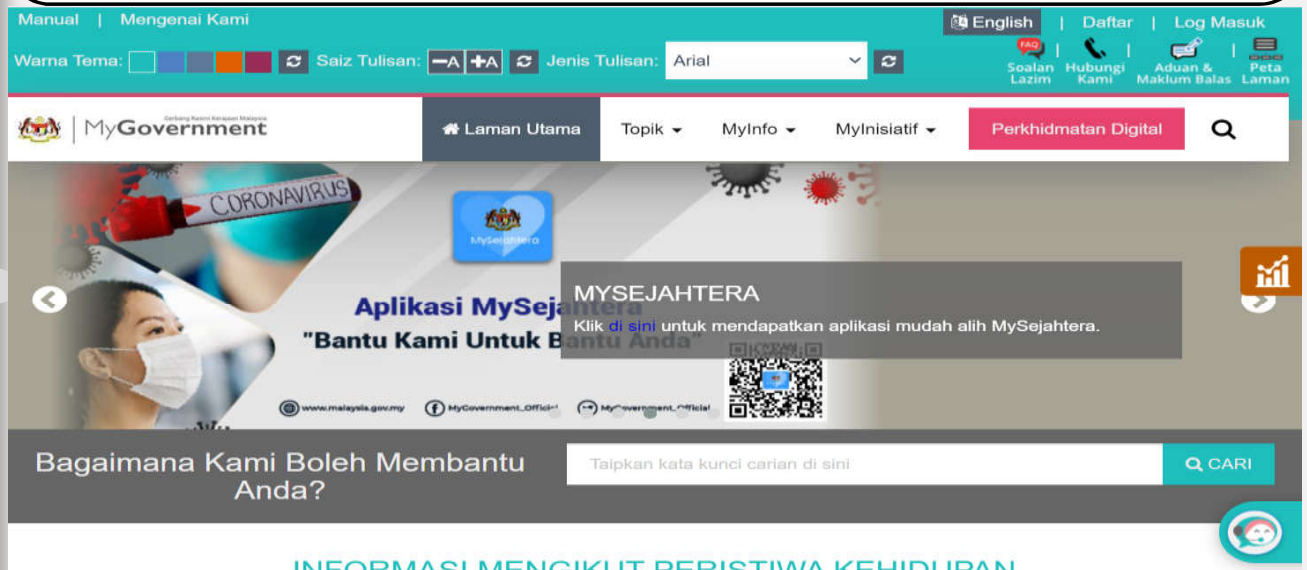
Hotel Avenue Garden, Bangi

KANDUNGAN


PENGENALAN
1
TUJUAN/
OBJEKTIF
2
PEMATUHAN
STANDARD &
GARIS PANDUAN
3
KONSEP
4
PERANAN
AGENSI
5
WAY FORWARD
6

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

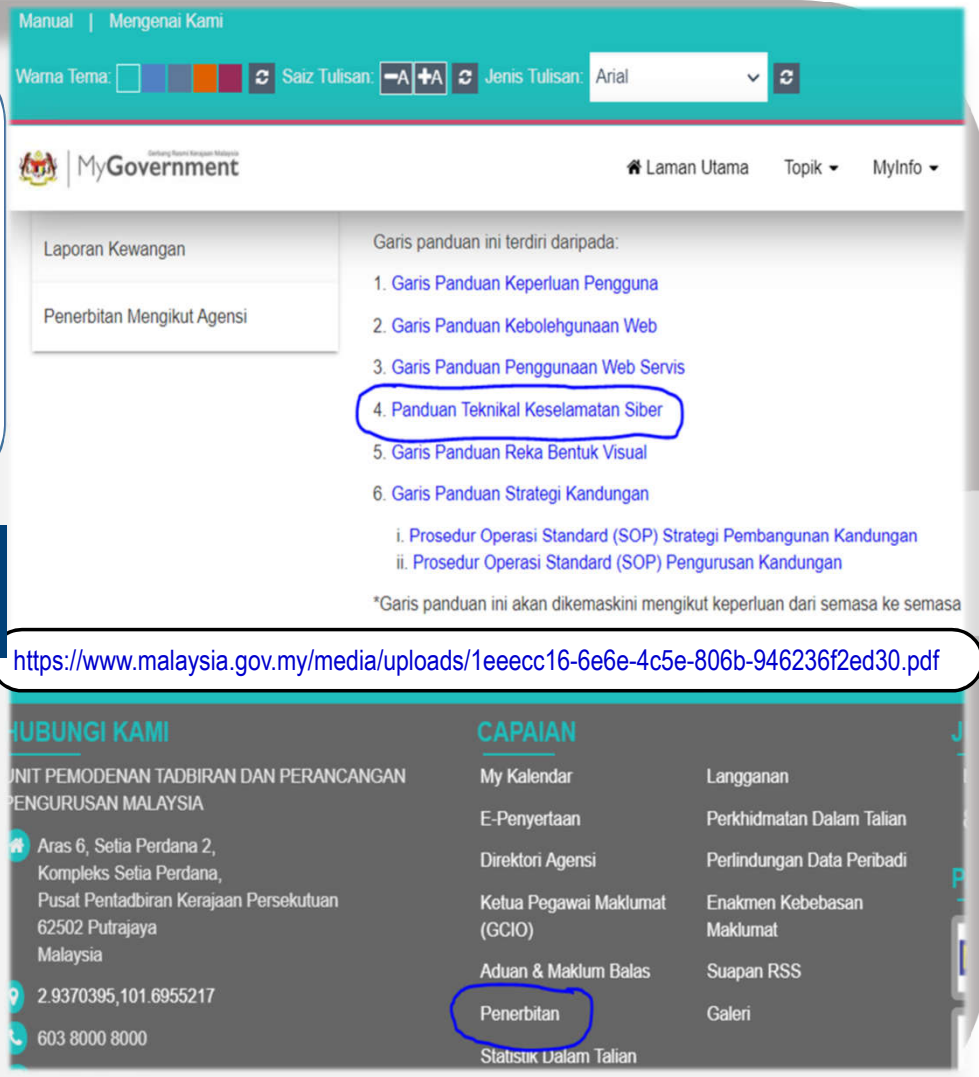
merupakan salah satu inisiatif MAMPU bagi mewujudkan **Gerbang Tunggal Kerajaan** yang berkonsepkan **peristiwa kehidupan** dan **berpaksikan rakyat**

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)

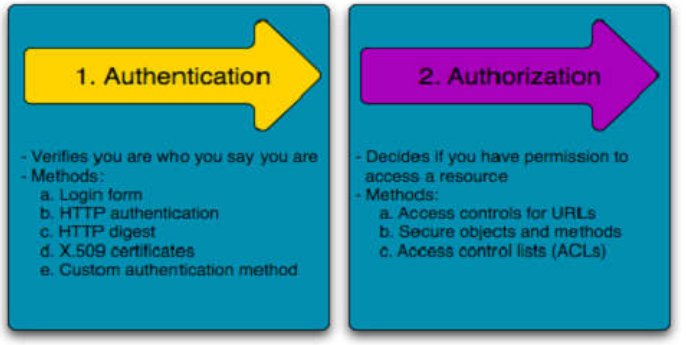
1. **Menyediakan panduan pembangunan laman web berdasarkan *life-event* dan berpaksikan rakyat**

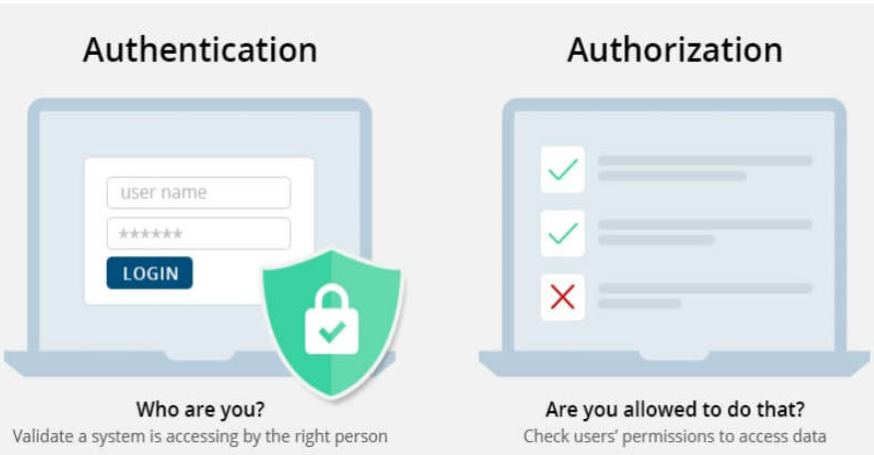
2. **Menyediakan panduan kepada pembangunan dan penyenggaraan perkhidmatan dalam talian kerajaan bagi mewujudkan keseragaman interaksi portal MyGovernment dan perkhidmatan dalam talian agensi**

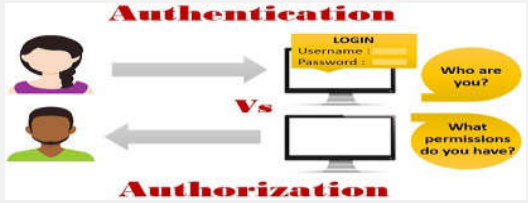
3 PEMATUHAN STANDARD & GARIS PANDUAN

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

KONSEP







Authentication	Authorization
Authentication confirms your identity to grant access to the system.	Authorization determines whether you are authorized to access the resources.
It is the process of validating user credentials to gain user access.	It is the process of verifying whether access is allowed or not.
It determines whether user is what he claims to be.	It determines what user can and cannot access.
Authentication usually requires a username and a password.	Authentication factors required for authorization may vary, depending on the security level.
Authentication is the first step of authorization so always comes first.	Authorization is done after successful authentication.
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.	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

5 PERANAN AGENSI

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

6 WAY FORWARD

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

MyGovISSO

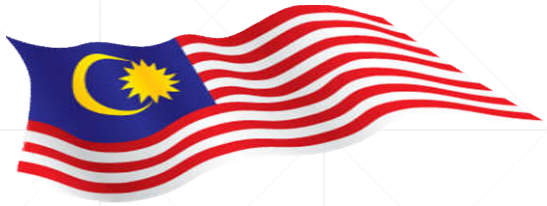
Panduan **komprehensif** dalam mengurus projek **integrasi SSO** aplikasi-aplikasi agensi sektor awam dengan Portal MyGovernment

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

Co-sourcing (Gabungan Dalaman dan *Outsoursing*)

Luaran/ *Outsourcing*

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



Terima kasih

Unit Pengurusan Keselamatan Maklumat, BPI

MAMPU
BERSAMA-SAMA MELAKSANAKAN TRANSFORMASI

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