UNIVERSITI TEKNOLOGI MARA

GARIS PANDUAN PENGURUSAN ICT

BIL. 01/2022

GARIS PANDUAN PELAKSANAAN *SINGLE SIGN ON* (SSO) DI UNIVERSITI TEKNOLOGI MARA

1.0 TUJUAN

Tujuan Garis Panduan Pelaksanaan *Single Sign On* (SSO) ini diwujudkan adalah sebagai panduan pemakaian SSO di UiTM.

2.0 OBJEKTIF

Objektif garis panduan ini adalah seperti berikut:

i. Menyelaras dan menguatkuasakan pemakaian *Single Sign On;*
ii. Menerapkan amalan terbaik pelaksanaan *Single Sign On* dalam pembangunan sistem dan aplikasi; dan
iii. Menjelaskan peranan dan tanggungjawab dalam pelaksanaan *Single Sign On*.

3.0 SKOP

Skop garis panduan Pelaksanaan SSO di Universiti Teknologi MARA adalah meliputi:

i. Penggunaan dan maklumat tersedia dalam SSO;
ii. Pembangunan SSO untuk sistem dan aplikasi; dan
iii. Peranan dan tanggungjawab dalam pelaksanaan SSO.

4.0 DEFINISI DAN AKRONIM

4.1 Definisi

Takrifan yang digunakan di dalam garis panduan ini adalah seperti berikut:

i. **Metadata** adalah data yang diperlukan untuk tujuan pertukaran maklumat di antara SSO dengan sistem dan aplikasi.

ii. **Modul SSO** adalah suatu pengaturcaraan yang digunakan untuk menghubungkan sistem dan aplikasi dengan SSO.

iii. **Portal SSO** merujuk kepada portal laman sesawang SSO yang memaparkan sistem dan aplikasi yang menggunakan *Single Sign On*.

iv. **Sistem SSO** adalah perkhidmatan SSO yang membolehkan pengguna mengakses sistem dan aplikasi menggunakan akaun yang sama.

v. **Token** merujuk kepada suatu kunci yang digunakan sebagai sandaran sistem dipercayai (*trusted system*) sebagai pertukaran antara SSO dengan sistem dan aplikasi.

4.2 Akronim

API	*Application Programming Interface*
ICT	*Information and Communication Technology*
LDAP	*Lightweight Access Protocol*
OAuth	*Open-standard Authorization Protocol / Framework*
PTJ	Pusat Tanggungjawab
SAML	*Security Assertion Markup Language*
SOP	*Standard Operating Procedure*
SSO	*Single Sign On*
UiTM	Universiti Teknologi MARA

5.0 PENYATAAN

Single Sign On adalah perkhidmatan memudahkan pengguna untuk mengakses sistem dan aplikasi dengan menggunakan akaun yang sama. Konsep sistem yang dipercayai (*trusted system*) digunakan antara sistem dan aplikasi tersebut dengan SSO. SSO berfungsi sebagai penyedia identiti (*identity provider*). Manakala, sistem dan aplikasi berfungsi sebagai penyedia perkhidmatan (*service provider*).

SSO merupakan salah satu aplikasi pengurusan identiti pengguna sistem dan aplikasi. Ia disediakan kepada warga UiTM dengan tujuan berikut:

i. Memudahkan pengguna menggunakan satu (1) akaun dan satu (1) kata laluan untuk akses ke sistem dan aplikasi universiti.

ii. Mengurangkan risiko penggunaan kata laluan yang mudah untuk diceroboh.

iii. Meningkatkan tahap keselamatan sistem dan aplikasi kerana kata laluan pengguna tidak disimpan di sistem dan aplikasi tersebut.

5.1 Penggunaan SSO

SSO adalah platform untuk digunapakai dan tidak terhad kepada sistem dan aplikasi.

5.1.1 Kategori Pengguna

Kategori	Definisi
Pengguna	Pengguna yang menggunakan sistem dan aplikasi yang telah siap dibangunkan untuk input, proses dan output data dan maklumat. Pengguna SSO adalah terdiri daripada warga UiTM: • Staf UiTM. • Pelajar UiTM.
Pembangun Sistem	Individu atau kumpulan teknikal yang bertanggungjawab dalam membangunkan sistem/ aplikasi berdasarkan spesifikasi keperluan pengguna yang ditetapkan oleh pemohon/ pemilik proses. Ia boleh terdiri daripada skim F, penyelidik ataupun pembekal yang dilantik untuk membangunkan sistem/ aplikasi.
Pentadbir Sistem	Individu atau kumpulan pegawai yang bertanggungjawab untuk mengurus dan mentadbir sistem dan aplikasi yang dibangunkan untuk PTJ.

5.1.2 Tempoh Capaian SSO

i. Tempoh capaian kepada sistem dan aplikasi adalah tertakluk kepada status aktif pengguna di dalam sistem maklumat staf dan sistem maklumat pelajar.

ii. Tempoh capaian staf adalah **6 bulan** selepas **bersara/ berhenti/ meninggal dunia.**

iii. Tempoh capaian pelajar adalah **2 semester** selepas **tamat pengajian**.

5.1.3 Kemudahan SSO

i. **Pengaktifan Akaun SSO** - Staf UiTM boleh mengaktifkan akaun SSO kali pertama pada pautan *1st Time Login* di portal SSO. Manakala akaun pelajar UiTM diaktifkan secara automatis di portal pelajar.

ii. ***Reset* Kata Laluan SSO** - Tetapan kata laluan boleh dilakukan secara kendiri pada pautan *Forgot Password* di portal SSO.

iii. **Semak alamat emel alternatif** - Pengguna boleh menyemak alamat emel alternatif yang didaftarkan di dalam SSO pada pautan *Check email alternative*.

iv. **https://faqsso.uitm.edu.my** – Pengguna boleh menyemak soalan lazim mengenai penggunaan sistem SSO.

5.1.4 Maklumat Tersedia dalam SSO

Sistem SSO mempunyai pangkalan data tersendiri yang berfungsi untuk menyimpan dan menguruskan identiti pengguna secara setempat menurut SOP SSO. Sebarang perubahan kemaskini perlu dilakukan di sumber data iaitu sistem maklumat staf dan sistem maklumat pelajar.

5.2 Pembangunan

5.2.1 Pendekatan Pelaksanaan SSO

Pendekatan SSO dapat dilaksanakan melalui kaedah berikut:

i. **Kaedah konvensional -** LDAP merupakan kaedah konvensional untuk berkongsi maklumat identiti pengguna setempat. Rekod penyimpan maklumat identiti pengguna tidak perlu diwujudkan di dalam sistem dan aplikasi.

ii. **Kaedah moden -** OAuth dan SAML adalah kaedah moden untuk pengurusan identiti pengguna yang menggunakan konsep sistem dipercayai (*trusted system*). Konsep ini melibatkan dua (2) entiti yang saling mempercayai di antara penyedia identiti (*identity provider*) dan penyedia perkhidmatan (*service provider*). Token atau metadata digunakan untuk membenarkan pengesahan identiti tersebut dilakukan.

5.2.2 Pelaksanaan SSO dalam Sistem dan Aplikasi

Pembangun sistem perlu membuat konfigurasi akses SSO berdasarkan jadual di bawah:

<table>
<tr><th colspan="5">Status Sesi Selepas Logout</th><th>Paparan selepas Logout*</th></tr>
<tr><td colspan="2">Senario</td><td colspan="3">Jenis/ medium pengesahan</td><td rowspan="5">Setiap aplikasi perlu ada logout page. Penyataan berikut perlu dinyatakan dalam logout page: “Sesi SSO hanya boleh tamat dengan Logout dari portal SSO/ tutup pelayar.”</td></tr>
<tr><td>URL</td><td>Jenis Sesi</td><td>LDAP</td><td>OAuth</td><td>SAML</td></tr>
<tr><td rowspan="2">Capaian terus ke domain.</td><td>Sesi Aplikasi</td><td>Tamat</td><td>Tamat</td><td>Tamat</td></tr>
<tr><td>Sesi SSO</td><td>Tidak berkaitan</td><td>Kekal</td><td>Kekal</td></tr>
<tr><td rowspan="2">Capaian dari Portal SSO.</td><td>Sesi Aplikasi</td><td colspan="3">Tamat</td></tr>
<tr><td>Sesi SSO</td><td colspan="3">Kekal</td></tr>
</table>

* Pembangun sistem – apabila *logout button* atau menu di klik, sesi aplikasi tersebut ditamatkan.

5.2.3 *Platform* SSO

Kriteria	Penerangan
Perisian	1. SSO menyokong pembangunan *multi-platform*. 2. SSO menggunakan *port* yang dienkripsi untuk saluran pertukaran maklumat yang selamat.
Infrastruktur	1. Perkhidmatan SSO ini menyokong kaedah *High Availability*. 2. Penyimpanan rekod identiti SSO dienkripsi di dalam pangkalan data.

5.2.4 Pematuhan Pelaksanaan SSO

i. Penamatan penggunaan SSO

a) Penamatan sistem dan aplikasi hendaklah dimaklumkan kepada pihak Keselamatan ICT, melalui sistem perkhidmatan ICT untuk dikeluarkan daripada pelaksanaan SSO.

b) Pemindahan hak milik sistem dan aplikasi hendaklah dimaklumkan kepada pihak Keselamatan ICT melalui sistem perkhidmatan ICT untuk dikemaskini di dalam rekod.

ii. Pelanggaran penggunaan SSO

a) Penggunaan sebarang bentuk token *credential* SSO untuk sistem dan aplikasi lain adalah dilarang.

iii. Pengecualian penggunaan SSO

a) Sistem dan aplikasi yang diletakkan di luar rangkaian UiTM.

b) Sistem dan aplikasi yang diuruskan oleh pihak konsesi.

5.3 Peranan dan Tanggungjawab

Peranan	Tanggungjawab
i. Pengguna	a) Menjaga kerahsiaan kata laluan. b) Menjaga akaun pengguna SSO. c) Tidak berkongsi akaun.
ii. Keselamatan ICT	a) Memudahcara penggunaan SSO. b) Memberi latihan SSO. c) Mengawal selia sistem SSO. d) Memastikan ketersediaan sistem SSO. e) Menyelenggara sistem SSO.
iii. Infrastruktur ICT	a) Memastikan ketersediaan platform sistem SSO.
iv. Pemilik Proses/ Sistem	a) Mengenal pasti keperluan SSO. b) Membuat permohonan SSO. c) Mengesahkan ujilari sebelum SSO dilaksanakan.
v. Pemilik Data	a) Memastikan integriti rekod identiti pengguna sistem dan aplikasi sentiasa dikemaskini dan terkini.
vi. Pentadbir Sistem	a) Memastikan pelaksanaan SSO dalam sistem dan aplikasi. b) Menyediakan maklumat permohonan SSO. c) Menentukan kaedah pelaksanaan SSO yang sesuai untuk sistem dan aplikasi.
vii. Pembangun Sistem	a) Membangunkan modul SSO. b) Menggunakan token SSO dengan baik dan beretika. c) Melaksanakan penyelenggaraan SSO sistem dan aplikasi.

6.0 SENARAI RUJUKAN

i. Dasar ICT UiTM

ii. Dasar Keselamatan ICT UiTM