LAMPIRAN B2

INTERFACE DESCRIPTION DOCUMENT (IDD)

MIGRASI DAN PEMBANGUNAN API

<NAMA SERVIS>

PROJEK PENINGKATAN NATIONAL REGISTRIES (MyGDX 2.0)

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

Disediakan oleh:

< Nama Agensi Pembekal >

Tarikh Disediakan:

xx/xx/202x

NAMA AGENSI	**:**	**xxxx**
NAMA AGENSI INDUK	**:**	**xxxxx**
TARIKH DOKUMEN	**:**	**xxxx**
VERSI DOKUMEN	**:**	**xxx**

KETERANGAN DOKUMEN

Dokumen ini menentukan keperluan pelaksaan proses migrasi dan pembangunan API.

Melalui dokumen ini, migrasi dan pembangunan API boleh mendapatkan maklumat terperinci berkenaan matlamat dan memahami keperluan pelaksaan proses migrasi yang akan dibangunkan.

SEMAKAN DOKUMEN

Aktiviti	Nama/Jawatan	Tandatangan	Tarikh
Disediakan Oleh			
Disemak Oleh			
Disahkan Oleh			

PENGESAHAN DOKUMEN OLEH <AGENSI>

Aktiviti	Nama/Jawatan	Tandatangan	Tarikh
Disemak Oleh			
Disahkan Oleh			

PENGESAHAN DOKUMEN OLEH MYGDX

Aktiviti	Nama/Jawatan	Tandatangan	Tarikh
Diluluskan Oleh			

KAWALAN DOKUMEN

Versi	Tarikh	Ringkasan Pindaan	Penyedia

KANDUNGAN

TAJUK **MUKA SURAT**

SENARAI AKRONIM

Terma	Keterangan
API	*Application Programming Interface*
DDSA	Data *Dictionary* Sektor Awam
IDD	*Interface Description Document*
MAMPU	Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia
MyGDX	*Malaysian Government Data Exchange*
URL	*Uniform Resource Locator*
UXP	*Unified eXchange Platform*

SENARAI TERMA/ISTILAH

Terma/Istilah	Definisi
Agensi	Sesebuah organisasi yang meliputi pelbagai sektor seperti awam, swasta, badan berkanun dan institusi bukan kerajaan yang lain, yang mana ianya mempunyai kepentingan yang kukuh untuk melanggan dan menggunakan perkhidmatan yang disediakan oleh MyGDX.
Agensi Pembekal	Agensi yang membekalkan data dan memberi kebenaran kepada agensi lain untuk menggunakan data tersebut.

SUMBER RUJUKAN

Bil.	Keterangan
1.	Dokumen Pelan Migrasi dan Spesifikasi API

1 PENGENALAN MENGENAI DOKUMEN

Dokumen ini merupakan salah satu keperluan utama dalam mendapatkan maklumat terperinci berkaitan perlaksanaan aktiviti pembangunan dan migrasi API bagi projek Peningkatan National Registries – *Malaysian Government Central Data Exchange* (MyGDX).

1.1 Objektif

Objektif dokumen *Interface Description Document* (IDD) ini adalah untuk menerangkan struktur dan format data yang terlibat dalam migrasi dan pembangunan API bagi agensi pembekal dalam projek *Malaysian Government Central Data Exchange* (MyGDX).

Dokumen IDD perlu dipersetujui oleh agensi pembekal bagi memastikan semua struktur dan format data yang diperlukan adalah menepati keperluan migrasi dan pembangunan API.

1.2 Skop

Keperluan pembangunan dan migrasi API yang dihuraikan dalam dokumen ini adalah mengenai keterangan *interface* API dan juga data format *request* dan *response* bagi setiap API yang akan terlibat dalam pembangunan dan migrasi API ini.

1.3 Organisasi Dokumen

Dokumen ini telah disediakan mengikut susunan seperti yang diterangkan dalam Jadual 1 di bawah.

Jadual 1 Organisasi Dokumen

BIL.	SEKSYEN	PENERANGAN
1.	Pengenalan Mengenai Dokumen	Bahagian ini menerangkan secara ringkas berkenaan dokumen ini.
2.	Keterangan *Interface*	Bahagian ini akan menerangkan mengenai maklumat *interface*.

2 KETERANGAN *INTERFACE*

2.1 <NAMA SERVIS>

2.1.1 Keterangan *Interface*

Nama Servis	<Nama Servis>
Keterangan Servis	Servis ini untuk ….
Jenis Data	Contoh: Sulit, Terbuka
Agensi Pembekal	Contoh: MAMPU
Kaedah Integrasi	SOAP Atau REST
Servis ID	<KodAgensi>-<NamaSistemPembekal>-<PilihanCRUD>-<JenisMaklumat> Contoh: MAMPU-DDSA-R-KodTarafKahwin
Method	POST/GET
URL API	
Authentication	Certificate

2.1.2 Senarai Agensi Pengguna

Bil.	Nama Agensi Pengguna	memberCode	subsystemCode
1.	Contoh: Jabatan Kebajikan Masyarakat	Contoh: JKM	Contoh: SMOKU

2.1.3 Format dan *Standard* API MyGDX

Berikut merupakan Standard *Header* untuk UXP bagi jenis kaedah integrasi SOAP yang baharu:

Standard Header *Format untuk SOAP*			
Parameter Input	**Keterangan**	**Header/Body**	**Value**
Maklumat Agensi Pengguna			
xRoadInstance	RoadInstance Agensi Pengguna	Header	MYGDX
memberClass	memberClass Agensi Pengguna	Header	GOV
memberCode	memberCode Agensi Pengguna	Header	<KodAgensiPengguna>
subsystemCode	subsystemCode Agensi Pengguna	Header	<KodSistemAgensiPengguna>
Maklumat Agensi Pembekal			
xRoadInstance	RoadInstance Agensi Pembekal	Header	MYGDX
memberClass	memberClass Agensi Pembekal	Header	GOV
memberCode	memberCode Agensi Pembekal	Header	<KodAgensiPembekal>
subsystemCode	subsystemCode Agensi Pembekal	Header	<KodSistemAgensiPembekal>
serviceCode	serviceCode Agensi Pembekal	Header	<ServisID>
serviceVersion	Service Version	Header	v1

2.1.3.1 Contoh *Header* Mesej (SOAP)

```
<soapenv:Header>
    <xro:client iden:objectType="SUBSYSTEM">
      <iden:xRoadInstance>MYGDX</iden:xRoadInstance>
      <iden:memberClass>GOV</iden:memberClass>
      <iden:memberCode>MAMPU</iden:memberCode>
      <!--Optional:-->
      <iden:subsystemCode>GOSG</iden:subsystemCode>
    </xro:client>
    <xro:service iden:objectType="SERVICE">
      <iden:xRoadInstance>MYGDX</iden:xRoadInstance>
      <iden:memberClass>GOV</iden:memberClass>
      <iden:memberCode>MAMPU</iden:memberCode>
      <!--Optional:-->
      <iden:subsystemCode>DDSA</iden:subsystemCode>
<iden:serviceCode>MAMPU-DDSA-R-
KodTarafKahwin</iden:serviceCode>
      <!--Optional:-->
      <iden:serviceVersion>v1</iden:serviceVersion>
    </xro:service>
    <xro:protocolVersion>4.0</xro:protocolVersion>
  </soapenv:Header>
```

Standard Header Format *untuk UXP REST-API*		
Paramater Name	**Data Structure**	**Value**
Maklumat Agensi Pengguna		
UXP-client	InstanceName/MemberClass/MemberName/ Subsystem/	MYGDX/GOV/<KodAgensi Pengguna>/<KodSistemA gensiPengguna>
Maklumat Agensi Pembekal		
UXP-Service	InstanceName/MemberClass/MemberName/ Subsystem/ServiceName/Version	MYGDX/GOV/<KodAgensi Pembekal>/<KodSistemA gensiPembekal>/<ServisI D>/v1

2.1.3.2 Contoh Header Mesej (REST)

```
“header":{
        "UXP-client":"MYGDX/GOV/MAMPU/GOSG",
        "UXP-Service":"
MYGDX/GOV/MAMPU/DDSA/MAMPU-DDSA-R-
KodTarafKahwin"
    }
```

2.1.4 Data Format (Request)

Bil	Nama Medan	Keterangan	Jenis Data	Header/ Body
1.				

2.1.5 Data Format (Response)

Bil	Nama Medan	Keterangan	Jenis Data	Header/ Body
1.				
2.				

2.1.5.1 Contoh Response Mesej (SOAP)

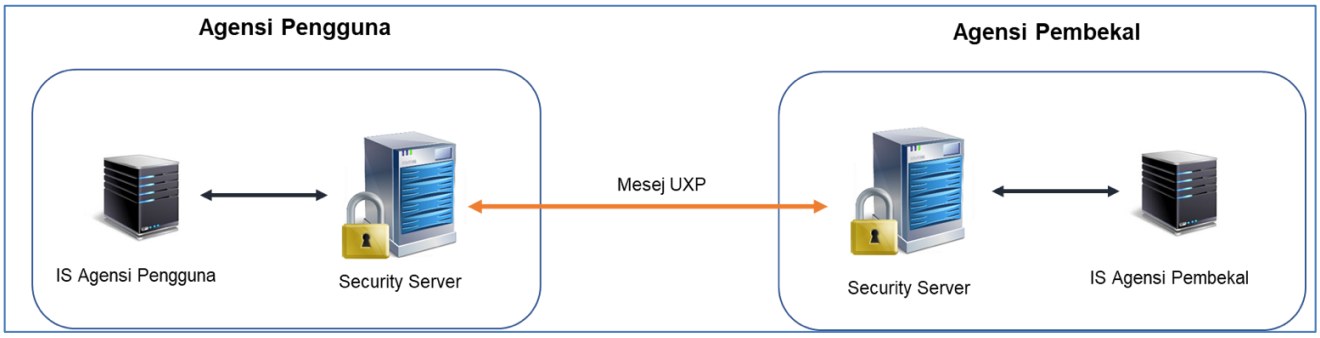
2.1.6 *Error Handling*

Bagi maklumat *error handling* boleh rujuk pada **Lampiran 1**.

3 LAMPIRAN

3.1 LAMPIRAN 1: *Error Handling*

3.1.1 Format atau Struktur Kod Ralat dan Mesej Ralat



Rajah 1: Pertukaran Mesej UXP

Semasa pertukaran mesej di antara *Security Server* Agensi Pengguna dan *Security Server* Agensi Pembekal, ralat boleh berlaku dan mesej ralat ini akan disimpan di dalam log di *Security Server*.

Ralat yang dijana oleh *Security Server* mempunyai struktur dan informasi yang konsisten. Struktur mesej ralat adalah berbeza mengikut kepada kaedah servis yang digunakan samada REST atau SOAP.

3.1.1.1 Format atau Struktur Kod Ralat dan Mesej Ralat (SOAP)

Bagi kaedah SOAP berikut merupakan sturktur dan format ralat yang akan dijana oleh *Security Server*. Ralat yang dijana adalah dalam format XML:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
     <faultcode>Server.ClientProxy.ServiceFailed.MissingBody</faultcode>
      <faultstring>Malformed SOAP message: body missing</faultstring>
      <faultactor />
      <detail>
        <faultDetail>f31e7451-f0ac-48f6-9f05-1f0459e48eea</faultDetail>
      </detail>
    </SOAP-ENV:Fault>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

(1) <faultcode> akan menunjukkan dimana punca ralat berlaku.

i. “Server.ClientProxy” dan “Client”membawa maksud ralat yang berlaku adalah di *Security Server* Agensi Pengguna.

ii. “Server.ServerProxy” membawa maksud ralat yang berlaku adalah di *Security Sever* Agensi Pembekal.

(2) <faultString> akan menunjukkan punca ralat dengan lebih terperinci.

(3) <faultDetail> merupakan pengenal unik bagi mesej ralat yang diterima.Pengenal unik ini boleh digunakan bagi tujuan carian mesej ralat di log *proxy* (var/log/uxp/proxy.log atau dari Logs di Security Server)

3.1.1.2 Format atau Struktur Kod Ralat dan Mesej Ralat (REST)

Bagi kaedah REST berikut merupakan sturktur dan format ralat yang akan dijana oleh *Security Server*. Ralat yang dijana adalah di dalam format text:

Security server has no valid authentication certificate

Di HTTP *Headers* akan mempunyai kod ralat (UXP-FaultCode), mesej ralat (UXP-FaultString) dan keterangan ralat (UXP-FaultDetail).

Uxp-*FaultCode*: Server.ClientProxy.SslAuthenticationFailed

Uxp-*FaultString*: *Security server has no valid authentication certificate*

Uxp-*FaultDetail*: f31e7451-f0ac-48f6-9f05-1f0459e48eea

(1) Uxp-*FaultCode* akan menunjukkan dimana punca ralat berlaku.

   i. “Server.ClientProxy” dan “Client”membawa maksud ralat yang berlaku adalah di *Security Server* Agensi Pengguna.

   ii. “Server.ServerProxy” membawa maksud ralat yang berlaku adalah di *Security Sever* Agensi Pembekal.

(2) Uxp-*FaultString* akan menunjukkan punca ralat dengan lebih terperinci.

(3) Uxp-FaultDetail merupakan pengenal unik bagi mesej ralat yang diterima.Pengenal unik ini boleh digunakan bagi tujuan carian mesej ralat di log *proxy* (var/log/uxp/proxy.log atau dari Logs di Security Server)

3.1.2 Ralat Daripada Sistem Agensi Pengguna

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
405 Not Found	1. Ia menunjukkan bahawa URL yang anda gunakan dalam permintaan anda tidak wujud pada pelayan. 2. Walaupun ini adalah ralat 404, yang biasanya bermaksud sesuatu pada bahagian *klien* adalah salah, ini juga boleh menunjukkan masalah pelayan. Kadangkala URL API berubah selepas kemas kini versi, tetapi kadangkala ia berubah kerana ada masalah pada pelayan. 3. Tindakan terbaik ialah menyemak sama ada anda tidak mempunyai kesilapan menaip dalam kod pelanggan anda sebelum menyemak sama ada API mempunyai masalah.	
401 *Unauthorized*	1. Kod status ini bermakna anda belum lagi mengesahkan terhadap API. API tidak tahu siapa anda dan oleh itu ia tidak akan melayani anda. 2. Untuk kebanyakan API, anda perlu mendaftar dan mendapatkan kunci API. Kunci ini kemudiannya digunakan dalam medan *header* HTTP apabila anda menghantar permintaan, memberitahu API siapa anda.	
403 *Forbidden*	1. Status terlarang menunjukkan bahawa anda tidak mempunyai kebenaran untuk meminta URL tersebut. Perbezaan kepada status Tanpa Kebenaran ialah anda telah disahkan, tetapi pengguna atau peranan yang anda sahkan tidak dibenarkan membuat permintaan. 2. Ini juga berlaku apabila anda mempunyai isu pengesahan, seperti apabila menggunakan kunci API yang salah atau cuba mengakses ciri yang tidak dibenarkan oleh pelan langganan anda.	
400 *Bad Request*	1. Status permintaan buruk ialah salah satu mesej *error* yang paling generik. Ini	

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
	menunjukkan bahawa anda melakukan sesuatu yang salah dalam permintaan anda. 2. Anda perlu menyemak dokumen. Anda mungkin kehilangan pertanyaan atau *body field* dalam permintaan, atau *header* mungkin salah. Mungkin juga sesetengah data permintaan anda mungkin mempunyai format yang salah.	
429 *Too Many Requests*	1. Kebanyakan pelan langganan API mempunyai had: lebih murah pelan, lebih sedikit permintaan sesaat dibenarkan untuk kunci API anda. Jika anda menghantar terlalu banyak permintaan dalam masa yang singkat, pertimbangkan untuk mengecilkannya dalam pelanggan anda. Status ini juga boleh menunjukkan bahawa anda mencapai had harian, mingguan atau bulanan pada akaun anda. 2. Kadangkala API kelihatan seperti sesuai sehingga anda melihat hadnya, dan tiba-tiba ia tidak berfungsi untuk kes penggunaan anda lagi. Semak bahagian langganan API anda sebelum menyepadukan jika tidak, anda mungkin menghadapi masalah beberapa minggu atau bulan selepas menyepadukan API.	
500 *Internal Server Error*	1. Status ini boleh bermakna apa sahaja, tetapi ia biasanya menunjukkan *server* API *error*. Ia mungkin disebabkan oleh sesuatu yang berkaitan dengan permintaan. Semak semula dokumen untuk memastikan anda melakukan semuanya dengan betul seperti *query fields, body fields, headers, format*, etc. 2. Jika itu tidak menyelesaikan masalah, ia mungkin juga berkaitan dengan kemas kini API yang memperkenalkan kod buggy, atau data yang dimuatkan oleh API daripada perkhidmatan *upstream*. Dalam kes itu, satu-	

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
	satunya punca tindakan anda ialah menghubungi sokongan API.	
502 *Bad Gateway*	1. Status ini memberitahu anda bahawa pelayan yang anda panggil bukanlah pelayan API sebenar, tetapi gerbang atau proksi. Pelayan proksi cuba memanggil pelayan API atas nama anda. Status juga menunjukkan bahawa pelayan API tidak menjawab. Ini mungkin berkaitan dengan masalah rangkaian, atau hanya kerana *server* API tidak berfungsi. 2. Masalah ini biasanya hanya sementara dan harus diselesaikan oleh penyedia API, tetapi anda perlu menghubungi sokongan jika ia berterusan.	
503 *Service Unavailable*	1. Status perkhidmatan tidak tersedia bermakna pelayan terlebih muatan. Terlalu banyak permintaan API telah dihantar dan kini API tidak dapat mengendalikannya lagi. Masalah ini selesai dengan sendirinya apabila pelanggan menghantar lebih sedikit permintaan, tetapi ini juga boleh bermakna penyedia API tidak merancang sumber yang mencukupi untuk semua pelanggannya. 2. Jika ia sesuai dengan kes penggunaan anda, anda boleh menjadikan pelanggan anda lebih berdaya tahan terhadap *error* ini dengan menunggu untuk menghantar lebih banyak permintaan. Tetapi jika *error* muncul, anda perlu menghubungi pembekal API.	
501 *Not Implemented*	1. Status tidak dilaksanakan adalah berkaitan dengan kaedah HTTP yang anda gunakan untuk meminta URL. Anda boleh mencuba kaedah lain untuk membuat permintaan. 2. Biasanya, permintaan dengan kaedah yang salah hanya menghasilkan status 404 tidak ditemui. Status yang tidak dilaksanakan menunjukkan bahawa kaedah itu belum dilaksanakan "belum." Pencipta API boleh	

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
	menggunakan status ini untuk memberitahu pelanggan bahawa kaedah ini akan tersedia untuk mereka pada masa hadapan.	
Different possible error messages. *For example*: *Unexpected SOAP message*	1. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PR-MESS]). 2. Untuk butiran lanjut tentang *error*, semak log proksi *Security Server* klien perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server).	
Invalid content type: *<content type>*	1. Jenis kandungan mesej SOAP mestilah teks/xml, xop/xml, soap/xml atau *multipart/related*. 2. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PR-MESS]).	
Must use POST request method instead of	1. Sistem maklumat pelanggan perkhidmatan mesti menghantar mesej permintaan SOAP menggunakan kaedah HTTP POST.	
Unsupported HTTP *method*	1. Sistem maklumat pelanggan perkhidmatan mesti menghantar mesej permintaan REST menggunakan kaedah HTTP HEAD, GET, DELETE, POST, PUT atau PATCH.	
A number of different error messages depending on cause of the error. Contohnya, org.xml.sax.SAXParseException; *Premature end of file*.	1. Sistem maklumat pelanggan perkhidmatan menghantar mesej SOAP yang tidak betul. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PR-MESS]). 2. Untuk butiran lanjut tentang *error*, semak log proksi *Security Server* klien perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server).	
Malformed SOAP message: *body missing*	1. Sistem maklumat pelanggan perkhidmatan menghantar mesej SOAP tanpa *body*. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PRMESS]). 2. Untuk butiran lanjut tentang ralat, semak log proksi *Security Server* klien perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server).	

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
Malformed SOAP message: *header missing*	1. Sistem klien perkhidmatan menghantar mesej SOAP tanpa *header*. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PRMESS]). 2. Untuk butiran lanjut tentang *error*, semak log proksi *Security Server* klien perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server).	
Request does not have SOAP message	1. Sistem klien perkhidmatan menghantar *multipart* MIME *envelope* yang tidak mempunyai mesej SOAP sebagai komponen pertamanya. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PR-MESS]). 2. Untuk butiran lanjut tentang ralat, semak log proksi *Security Server* klien perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server).	

3.1.3 Ralat Daripada Security Server Agensi Pengguna

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
Could not find addresses for service provider 'SERVICE:EE_DEV/GOV/ E XAMPLE_ORGANIZATIO N/E XAMPLE_DEPARTMENT/ EXA MPLE_SERVICE'	1. Perkhidmatan ini tidak didaftarkan dalam *Security Server* pembekal perkhidmatan. Semak sama ada kod perkhidmatan dalam mesej permintaan adalah sama dengan kod yang didaftarkan dalam *Security Server* pembekal perkhidmatan.	
Client 'SUBSYSTEM:EE_DEV/G OV /EXAMPLE_ORGANIZATI ON	1. Hubungi pentadbir *Security Server* pelanggan perkhidmatan	1. Subsistem tidak didaftarkan dalam *Security Server* pelanggan perkhidmatan.

/EXAMPLE_DEPARTMENT' not found		Daftarkan subsistem (lihat Bahagian User Guide-Security Server Menambah Klien Pelayan Keselamatan)
A number of different error messages depending on cause of the error.	1. Terdapat pelbagai sebab yang berbeza. Semak log proksi untuk mendapatkan butiran lanjut (var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server)	
Token 'softToken' not active.	1. Hubungi pentadbir *Security Server* pelanggan perkhidmatan	1. Token perisian *Security Server* pelanggan perkhidmatan tidak dilog masuk. Masukkan PIN token perisian daripada *User Interface Security Server* pelanggan perkhidmatan.
Security server has no valid authentication certificate	1. Hubungi pentadbir *Security Server* pelanggan perkhidmatan	1. *Security Server* pelanggan perkhidmatan tidak mempunyai sijil pengesahan yang sah. Pastikan semua syarat berikut dipenuhi: (i) *Security Server* mempunyai sekurang-kurangnya satu sijil pengesahan (lihat Bahagian User Guide-Security Server Mengkonfigurasi Kunci Pengesahan dan Sijil untuk

		Pelayan Keselamatan) (ii) Sijil adalah pada token yang dilog masuk dan tersedia (lihat Bahagian User Guide-Security Server Ketersediaan Keadaan Token Keselamatan, Kunci dan Sijil). (iii) Sijil didaftarkan (lihat Bahagian User Guide-Security Server Pendaftaran Negeri Pengesahan dan Sijil Penyulitan). (iv) Sijil aktif (lihat Bahagian User Guide-Security Server Mengaktifkan dan Melumpuhkan Sijil). (v) Sambutan OCSP bagi sijil adalah baik (lihat Bahagian User Guide-Security Server Status Kesahan Sijil)
Service provider did not send correct authentication certificate	1. Hubungi pentadbir *Security Server*	1. *Security Server* pembekal perkhidmatan tidak mempunyai sijil pengesahan yang

	pembekal perkhidmatan	sah. Pastikan semua syarat berikut dipenuhi: (i) *Security Server* mempunyai sekurang-kurangnya satu sijil pengesahan (lihat Bahagian User Guide-Security Server Mengkonfigurasi Kunci Pengesahan dan Sijil untuk Pelayan Keselamatan). (ii) Sijil adalah pada token yang dilog masuk dan tersedia (lihat Bahagian User Guide-Security Server Ketersediaan Keadaan Token Keselamatan, Kunci dan Sijil). (iii) Sijil didaftarkan (lihat Bahagian User Guide-Security Server Pendaftaran Negeri Pengesahan dan Sijil Penyulitan). (iv) Sijil aktif (lihat Bahagian User Guide-Security Server Mengaktifkan dan

		Melumpuhkan Sijil). (v) Sambutan OCSP bagi sijil adalah baik (lihat Bahagian User Guide-Security Server Status Kesahan Sijil).
Client specifies HTTPS but did not supply TLS certificate	1. Sijil TLS sistem maklumat pelanggan perkhidmatan mesti dimuat naik ke *Security Server* pelanggan perkhidmatan (lihat Bahagian Komunikasi dengan Sistem Maklumat Pelanggan).	
Could not find any certificates for member	1. Hubungi pentadbir *Security Server* pelanggan perkhidmatan	1. Subsistem pelanggan perkhidmatan tidak mempunyai sijil tandatangan yang sah. Pastikan syarat berikut adalah benar: (i) Terdapat sekurang-kurangnya satu sijil tandatangan untuk ahli yang dimiliki oleh subsistem tersebut (lihat Bahagian User Guide-Security Server Mengkonfigurasi Kunci Tandatangan dan Sijil untuk Pelanggan Pelayan Keselamatan). (ii) Sijil adalah pada token yang dilog

		masuk dan tersedia (lihat Bahagian User Guide Security Server Ketersediaan Keadaan Token Keselamatan, Kunci dan Sijil). (iii) Sijil didaftarkan (lihat Negeri Pendaftaran Bahagian User Guide-Security *Server* bagi Sijil Menandatangani) . (iv) Sijil aktif (lihat Bahagian User Guide-Security Server Mengaktifkan dan Melumpuhkan Sijil). (v) Sambutan OCSP sijil adalah baik (lihat Bahagian User Guide-Security Server Kesahan Negeri Sijil)
No space left on device	1. Hubungi pentadbir *Security Server* pelanggan perkhidmatan	1. Pastikan *Security Server* pelanggan perkhidmatan mempunyai ruang cakera kosong. Jika cakera dipisahkan, pastikan *partition* yang berkaitan mempunyai ruang kosong

Cannot timestamp messages: no timestamping services configure	1. Hubungi pentadbir Security Server pelanggan perkhidmatan	1. Pastikan syarat berikut adalah benar: (i) *Security Server* pelanggan perkhidmatan boleh menyambung ke perkhidmatan *timestamp*. Semak bahawa semua *firewall* api dikonfigurasikan dengan betul. (ii) Perkhidmatan *timestamp* tersedia. Semak log proksi (/var/log/uxp/proxy.log) untuk butiran lanjut
Global configuration is expired	1. Hubungi pentadbir *Security Server* pelanggan perkhidmatan	1. *Security Server* klien perkhidmatan tidak boleh memuat turun konfigurasi global daripada pelayan pendaftaran. Semak log klien konfigurasi (/var/log/uxp/configuration_client.log) untuk butiran
Could not connect to target host (https://:5500)	1. Hubungi pentadbir *Security Server* pelanggan perkhidmatan	1. *Security Server* pelanggan perkhidmatan tidak boleh menyambung ke *Security Server* pembekal perkhidmatan. Pastikan firewall dikonfigurasikan dengan betul pada kedua-dua belah pihak: *Security*

		Server pelanggan perkhidmatan mesti membenarkan trafik keluar ke port *Security Server* penyedia perkhidmatan 5500 dan 5577, *Security Server* penyedia perkhidmatan mesti membenarkan trafik masuk ke port 5500 dan 5577.
Name or service not known. No address associated with hostname.	1. Hubungi pentadbir *Security Server* pembekal perkhidmatan	1. *Security Server* pembekal perkhidmatan tidak dapat ditemui kerana *Security Server* didaftarkan dengan FQDN yang salah.

3.1.4 Ralat Daripada Security Server Agensi Pembekal

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
Request is not allowed: SERVICE:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT/EXAM PLE_SERVICE	*Security Server* pembekal perkhidmatan mesti memberikan hak akses kepada perkhidmatan dan kepada subsistem pelanggan perkhidmatan. Lihat Hak Akses Bahagian	
Malformed SOAP message: header missing	Sistem maklumat pembekal perkhidmatan mesti mengembalikan semua pengepala UXP yang wajib. Lihat [UXP-PR-MESS] untuk butiran lanjut.	
A number of different error messages depending on cause of the error. For example,	Sistem maklumat pembekal perkhidmatan mengembalikan mesej SOAP yang tidak betul. Untuk butiran lanjut tentang error, semak log proksi *Security Server* penyedia perkhidmatan (/var/log/uxp/proxy.log atau	

org.xml.sax.SAXParseException; Premature end of file.	daripada Log dalam User Interface Security Server)	
Unknown service: SERVICE:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT/EXAM PLE_SERVICE	Pastikan kod perkhidmatan dalam mesej permintaan sepadan dengan perkhidmatan di bahagian pembekal perkhidmatan.	
The reason the connection failed. For example, Server responded with error 403: Forbidden	1. Pastikan *Security Server* pembekal perkhidmatan dibenarkan untuk menyambung ke sistem maklumat pembekal perkhidmatan dan sambungan dikonfigurasikan dengan betul. 2. Untuk maklumat lanjut tentang mengkonfigurasi sambungan, lihat Bahagian Komunikasi dengan Sistem Maklumat Pelanggan. Untuk butiran lanjut tentang ralat, lihat log proksi *Security Server* pembekal perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam *User Interface Security Server*.	
Server certificate is not trusted	Pilihan "Sahkan sijil TLS" dipilih dalam konfigurasi perkhidmatan, tetapi sijil sistem maklumat pembekal perkhidmatan belum dimuat naik ke *Security Server* penyedia perkhidmatan. Muat naik sijil sistem maklumat pembekal perkhidmatan ke *Security Server* (lihat Bahagian Komunikasi dengan Sistem Maklumat Pelanggan).	
Could not find any certificates for member 'SUBSYSTEM:SERVICE:EE_DEV/GOV/EXAMPLE_ORGA NIZATION/EXAMPLE_DEPARTMENT'	1. Hubungi pentadbir *Security Server* pembekal perkhidmatan	1. Subsistem pembekal perkhidmatan tidak mempunyai sijil tandatangan yang sah. Pastikan syarat berikut adalah benar: (i) Terdapat sekurang-kurangnya satu sijil tandatangan untuk ahli yang dimiliki oleh subsistem tersebut (lihat Bahagian User Guide *Security Server* - Mengkonfigurasi Kunci Tandatangan dan Sijil untuk

		Pelanggan Pelayan Keselamatan). (ii) Sijil adalah pada token yang dilog masuk dan tersedia (lihat Bahagian *User Guide Security Server* Ketersediaan Keadaan Token Keselamatan, Kunci dan Sijil). (iii) Sijil didaftarkan (lihat Negeri Pendaftaran Bahagian *User Guide-Security Server* bagi Sijil Menandatangani) (iv) Sijil aktif (lihat Bahagian *User Guide-Security Server* Mengaktifkan dan Melumpuhkan Sijil). (v) Sambutan OCSP bagi sijil adalah baik (lihat Bahagian *User Guide-Security Server* Status Kesahan Sijil).
Connection pool shut down	Hubungi pentadbir *Security Server* pembekal perkhidmatan	*Security Server* pembekal perkhidmatan tidak boleh mengakses pangkalan datanya. Semak log proksi (/var/log/uxp/proxy.l og) dan log Postgres (/var/log/postgresql/) untuk butiran lanjut
Failed to get signing info for member HttpError: Connection to Signer (port 5558) timed out	Hubungi pentadbir *Security Server* pembekal perkhidmatan	Cuba mulakan semula proses penandatangan $ systemctl mulakan semula uxp-signer. Semak log penandatangan var/log/uxp/signer.log untuk mendapatkan maklumat lanjut.

Token 'softToken' not active	Hubungi pentadbir *Security Server* pembekal perkhidmatan	Pastikan bahawa token perisian *Security Server* pembekal perkhidmatan telah dilog masuk. Jika ia tidak dilog masuk, log masuk daripada *Security Server User Interface* pembekal perkhidmatan.
Cannot timestamp messages: no timestamping services configured	Hubungi pentadbir *Security Server* pembekal perkhidmatan	Anda mesti mengkonfigurasi perkhidmatan timestamp untuk *Security Server* pembekal perkhidmatan (lihat Bahagian *User Guide-Security Server* Mengurus Perkhidmatan Timestamp).
Cannot timestamp messages	Hubungi pentadbir *Security Server* pembekal perkhidmatan	1. Walaupun terdapat perkhidmatan *timestamp* yang dikonfigurasikan (lihat mesej ralat sebelumnya),*timestamp* masih boleh gagal. Masalah berikut mungkin berlaku: (i) Terdapat masalah pada bahagian perkhidmatan timetamp dan perkhidmatan tidak tersedia. Semak log proksi (var/log/uxp/proxy .log) untuk butiran lanjut. (ii) *Security Server* pembekal perkhidmatan tidak boleh menyambung ke perkhidmatan timestamp. Pastikan bahawa firewall dan port dikonfigurasikan dengan betul untuk kedua-dua perkhidmatan

		Security Server dan *timestamp*.
Global configuration is expired	Hubungi pentadbir *Security Server* pembekal perkhidmatan	Cuba mulakan semula proses klien konfigurasi $ systemctl mulakan semula uxp-confclient. Ada kemungkinan *Security Server* penyedia perkhidmatan tidak dapat menyambung ke pelayan pendaftaran untuk memuat turun konfigurasi global. Pastikan konfigurasi *firewall* api di kedua-dua belah adalah betul. Lihat log klien konfigurasi untuk butiran lanjut (/var/log/uxp/configuration_client.log)