



**INTERFACE DESCRIPTION DOCUMENT (IDD)**  
**MIGRASI DAN PEMBANGUNAN API**  
**<NAMA SERVIS>**

---

**PROJEK PENINGKATAN NATIONAL  
REGISTRIES (MyGDX 2.0)**

**JABATAN DIGITAL NEGARA**



Disediakan oleh:

< Nama Agensi Pembekal >

Tarikh Disediakan:

xx/xx/202x

<b>NAMA AGENSI</b>	:	<b>XXXX</b>
<b>NAMA AGENSI INDUK</b>	:	<b>XXXXXX</b>
<b>TARIKH DOKUMEN</b>	:	<b>XXXX</b>
<b>VERSI DOKUMEN</b>	:	<b>XXXX</b>

## KETERANGAN DOKUMEN

---

Dokumen ini menentukan keperluan pelaksanaan proses migrasi dan pembangunan API.

Melalui dokumen ini, migrasi dan pembangunan API boleh mendapatkan maklumat terperinci berkenaan matlamat dan memahami keperluan pelaksanaan 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
<b>1 PENGENALAN MENGENAI DOKUMEN .....</b>	<b>1</b>
1.1 Objektif .....	1
1.2 Skop .....	1
1.3 Organisasi Dokumen .....	1
<b>2 KETERANGAN INTERFACE .....</b>	<b>3</b>
2.1 <NAMA SERVIS> .....	3
2.1.1 Keterangan <i>Interface</i> .....	3
2.1.2 Senarai Agensi Pengguna .....	3
2.1.3 Format dan <i>Standard</i> API MyGDX.....	4
2.1.3.1 Contoh <i>Header</i> Mesej (SOAP) .....	5
2.1.3.2 Contoh <i>Header</i> Mesej (REST).....	6
2.1.4 Data Format (Request) .....	6
2.1.5 Data Format (Response).....	6
2.1.5.1 Contoh <i>Response</i> Mesej (SOAP).....	6
2.1.6 <i>Error Handling</i> .....	6
<b>3 LAMPIRAN .....</b>	<b>7</b>
3.1 LAMPIRAN 1: <i>Error Handling</i> .....	7
3.1.1 Format atau Struktur Kod Ralat dan Mesej Ralat.....	7
3.1.1.1 Format atau Struktur Kod Ralat dan Mesej Ralat (SOAP).....	7
3.1.1.2 Format atau Struktur Kod Ralat dan Mesej Ralat (REST) .....	9
3.1.2 Ralat Daripada Sistem Agensi Pengguna.....	9
3.1.3 Ralat Daripada Security Server Agensi Pengguna .....	14
3.1.4 Ralat Daripada Security Server Agensi Pembekal.....	20

## SENARAI AKRONIM

---

Terma	Keterangan
API	<i>Application Programming Interface</i>
DDSA	<i>Data Dictionary Sektor Awam</i>
IDD	<i>Interface Description Document</i>
JDN	Jabatan Digital Negara
MyGDX	<i>Malaysian Government Central Data Exchange</i>
URL	<i>Uniform Resource Locator</i>
UXP	<i>Unified eXchange Platform</i>

## 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 pelaksanaan 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 <i>Interface</i>	Bahagian ini akan menerangkan mengenai maklumat <i>interface</i> .

## 2 KETERANGAN *INTERFACE*

### 2.1 <NAMA SERVIS>

#### 2.1.1 Keterangan *Interface*

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

#### 2.1.2 Senarai Agensi Pengguna

<b>Bil.</b>	<b>Nama Agensi Pengguna</b>	<b>memberCode</b>	<b>subsystemCode</b>
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 <i>Format untuk SOAP</i>			
Parameter Input	Keterangan	Header/Body	Value
<b>Maklumat Agensi Pengguna</b>			
xRoadInstance	RoadInstance <b>Agensi Pengguna</b>	Header	MYGDX
memberClass	memberClass <b>Agensi Pengguna</b>	Header	GOV
memberCode	memberCode <b>Agensi Pengguna</b>	Header	<KodAgensiPengguna>
subsystemCode	subsystemCode <b>Agensi Pengguna</b>	Header	<KodSistemAgensiPengguna>
<b>Maklumat Agensi Pembekal</b>			
xRoadInstance	RoadInstance <b>Agensi Pembekal</b>	Header	MYGDX
memberClass	memberClass <b>Agensi Pembekal</b>	Header	GOV
memberCode	memberCode <b>Agensi Pembekal</b>	Header	<KodAgensiPembekal>
subsystemCode	subsystemCode <b>Agensi Pembekal</b>	Header	<KodSistemAgensiPembekal>
serviceCode	serviceCode <b>Agensi Pembekal</b>	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>JDN</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>JDN</iden:memberCode>
    <!--Optional:-->
    <iden:subsystemCode>DDSA</iden:subsystemCode>
  <iden:serviceCode>JDN-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
<b>Maklumat Agensi Pengguna</b>		
UXP-client	InstanceName/MemberClass/MemberName/ Subsystem/	MYGDX/GOV/<KodAgensi Pengguna>/<KodSistemA gensiPengguna>
<b>Maklumat Agensi Pembekal</b>		
UXP- Service	InstanceName/MemberClass/MemberName/ Subsystem/ServiceName/Version	MYGDX/GOV/<KodAgensi Pembekal>/<KodSistemA gensiPembekal>/<Servisl D>/v1

### 2.1.3.2 Contoh Header Mesej (REST)

```
"header":{  
    "UXP-client":"MYGDX/GOV/JDN/GOSG",  
    "UXP-Service":" MYGDX/GOV/JDN/DDSA/JDN-  
    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)

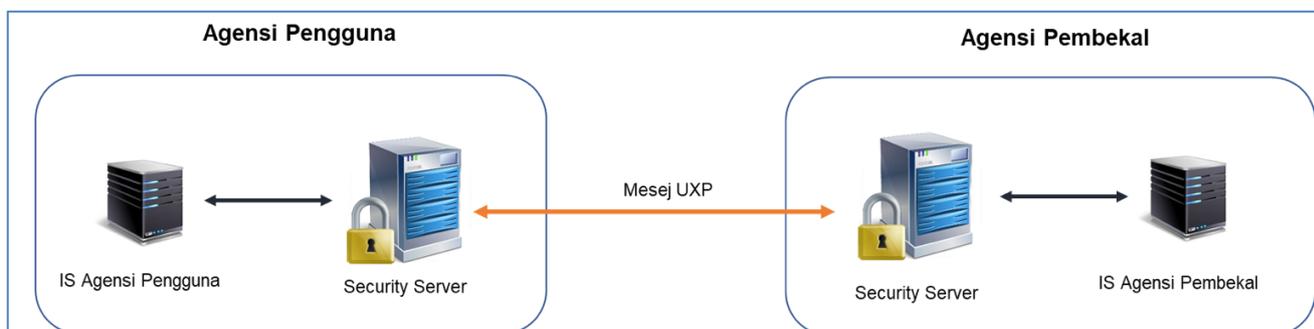
### 2.1.6 Error Handling

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 struktur 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.MissingBod
y</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 struktur 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 <i>Security Server</i>
405 Not Found	1. Ia menunjukkan bahawa URL yang anda gunakan dalam permintaan anda tidak wujud pada pelayan.	

Mesej Ralat	Penyelesaian Pentadbir Perkhidmatan	Penyelesaian Pentadbir Security Server
	<ol style="list-style-type: none"> <li>Walaupun ini adalah ralat 404, yang biasanya bermaksud sesuatu pada bahagian <i>klien</i> 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.</li> <li>Tindakan terbaik ialah menyemak sama ada anda tidak mempunyai kesilapan menaip dalam kod pelanggan anda sebelum menyemak sama ada API mempunyai masalah.</li> </ol>	
401 <i>Unauthorized</i>	<ol style="list-style-type: none"> <li>Kod status ini bermakna anda belum lagi mengesahkan terhadap API. API tidak tahu siapa anda dan oleh itu ia tidak akan melayani anda.</li> <li>Untuk kebanyakan API, anda perlu mendaftar dan mendapatkan kunci API. Kunci ini kemudiannya digunakan dalam medan <i>header</i> HTTP apabila anda menghantar permintaan, memberitahu API siapa anda.</li> </ol>	
403 <i>Forbidden</i>	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol>	
400 <i>Bad Request</i>	<ol style="list-style-type: none"> <li>Status permintaan buruk ialah salah satu mesej <i>error</i> yang paling generik. Ini menunjukkan bahawa anda melakukan sesuatu yang salah dalam permintaan anda.</li> <li>Anda perlu menyemak dokumen. Anda mungkin kehilangan pertanyaan atau <i>body field</i> dalam permintaan, atau <i>header</i> mungkin salah. Mungkin juga sesetengah data permintaan anda mungkin mempunyai format yang salah.</li> </ol>	
429 <i>Too Many Requests</i>	<ol style="list-style-type: none"> <li>Kebanyakan pelan langganan API mempunyai had: lebih murah pelan, lebih sedikit permintaan sesaat</li> </ol>	

Mesej Ralat	Penyelesaian Pentadbir Perkhidmatan	Penyelesaian Pentadbir Security Server
	<p>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.</p> <p>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.</p>	
500 <i>Internal Server Error</i>	<p>1. Status ini boleh bermakna apa sahaja, tetapi ia biasanya menunjukkan <i>server API error</i>. Ia mungkin disebabkan oleh sesuatu yang berkaitan dengan permintaan. Semak semula dokumen untuk memastikan anda melakukan semuanya dengan betul seperti <i>query fields, body fields, headers, format, etc.</i></p> <p>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 <i>upstream</i>. Dalam kes itu, satu-satunya punca tindakan anda ialah menghubungi sokongan API.</p>	
502 <i>Bad Gateway</i>	<p>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 <i>server API</i> tidak berfungsi.</p> <p>2. Masalah ini biasanya hanya sementara dan harus diselesaikan oleh penyedia API, tetapi anda perlu menghubungi sokongan jika ia berterusan.</p>	

Mesej Ralat	Penyelesaian Pentadbir Perkhidmatan	Penyelesaian Pentadbir Security Server
503 <i>Service Unavailable</i>	<ol style="list-style-type: none"> <li>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.</li> <li>2. Jika ia sesuai dengan kes penggunaan anda, anda boleh menjadikan pelanggan anda lebih berdaya tahan terhadap <i>error</i> ini dengan menunggu untuk menghantar lebih banyak permintaan. Tetapi jika <i>error</i> muncul, anda perlu menghubungi pembekal API.</li> </ol>	
501 <i>Not Implemented</i>	<ol style="list-style-type: none"> <li>1. Status tidak dilaksanakan adalah berkaitan dengan kaedah HTTP yang anda gunakan untuk meminta URL. Anda boleh mencuba kaedah lain untuk membuat permintaan.</li> <li>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 menggunakan status ini untuk memberitahu pelanggan bahawa kaedah ini akan tersedia untuk mereka pada masa hadapan.</li> </ol>	
<i>Different possible error messages. For example: Unexpected SOAP message</i>	<ol style="list-style-type: none"> <li>1. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PR-MESS]).</li> <li>2. Untuk butiran lanjut tentang <i>error</i>, semak log proksi Security Server klien perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server).</li> </ol>	
<i>Invalid content type: &lt;content type&gt;</i>	<ol style="list-style-type: none"> <li>1. Jenis kandungan mesej SOAP mestilah teks/xml, xop/xml, soap/xml atau <i>multipart/related</i>.</li> <li>2. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PR-MESS]).</li> </ol>	
<i>Must use POST request method instead of</i>	<ol style="list-style-type: none"> <li>1. Sistem maklumat pelanggan perkhidmatan mesti menghantar mesej permintaan SOAP menggunakan kaedah HTTP POST.</li> </ol>	

Mesej Ralat	Penyelesaian Pentadbir Perkhidmatan	Penyelesaian Pentadbir Security Server
<p><i>Unsupported method</i> HTTP</p>	<p>1. Sistem maklumat pelanggan perkhidmatan mesti menghantar mesej permintaan REST menggunakan kaedah HTTP HEAD, GET, DELETE, POST, PUT atau PATCH.</p>	
<p><i>A number of different error messages depending on cause of the error.</i></p> <p>Contohnya, <i>org.xml.sax.SAXParseException; Premature end of file.</i></p>	<p>1. Sistem maklumat pelanggan perkhidmatan menghantar mesej SOAP yang tidak betul. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PR-MESS]).</p> <p>2. Untuk butiran lanjut tentang <i>error</i>, semak log proksi Security Server klien perkhidmatan (<i>/var/log/uxp/proxy.log</i> atau daripada Log dalam User Interface Security Server).</p>	
<p><i>Malformed SOAP message: body missing</i></p>	<p>1. Sistem maklumat pelanggan perkhidmatan menghantar mesej SOAP tanpa <i>body</i>. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PRMESS]).</p> <p>2. Untuk butiran lanjut tentang ralat, semak log proksi Security Server klien perkhidmatan (<i>/var/log/uxp/proxy.log</i> atau daripada Log dalam User Interface Security Server).</p>	
<p><i>Malformed SOAP message: header missing</i></p>	<p>1. Sistem klien perkhidmatan menghantar mesej SOAP tanpa <i>header</i>. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PRMESS]).</p> <p>2. Untuk butiran lanjut tentang <i>error</i>, semak log proksi Security Server klien perkhidmatan (<i>/var/log/uxp/proxy.log</i> atau daripada Log dalam User Interface Security Server).</p>	
<p><i>Request does not have SOAP message</i></p>	<p>1. Sistem klien perkhidmatan menghantar <i>multipart MIME envelope</i> yang tidak mempunyai mesej SOAP sebagai komponen pertamanya. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PR-MESS]).</p> <p>2. Untuk butiran lanjut tentang ralat, semak log proksi Security Server klien perkhidmatan (<i>/var/log/uxp/proxy.log</i> atau daripada Log dalam User Interface Security Server).</p>	

### 3.1.3 Ralat Daripada Security Server Agensi Pengguna

Mesej Ralat	Penyelesaian Pentadbir Perkhidmatan	Penyelesaian Pentadbir Security Server
<p><i>Could not find addresses for service provider 'SERVICE:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT/EXAMPLE_SERVICE'</i></p>	<p>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.</p>	
<p><i>Client 'SUBSYSTEM:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT' not found</i></p>	<p>1. Hubungi pentadbir Security Server pelanggan perkhidmatan</p>	<p>1. Subsistem tidak didaftarkan dalam Security Server pelanggan perkhidmatan. Daftarkan subsistem (lihat Bahagian User Guide-Security Server Menambah Klien Pelayan Keselamatan)</p>
<p><i>A number of different error messages depending on cause of the error.</i></p>		<p>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)</p>
<p><i>Token 'softToken' not active.</i></p>	<p>1. Hubungi pentadbir Security Server pelanggan perkhidmatan</p>	<p>1. Token perisian Security Server pelanggan perkhidmatan tidak dilog masuk. Masukkan PIN token perisian daripada User Interface Security Server pelanggan perkhidmatan.</p>
<p><i>Security server has no valid authentication certificate</i></p>	<p>1. Hubungi pentadbir Security Server</p>	<p>1. Security Server pelanggan perkhidmatan tidak</p>

	pelanggan perkhidmatan	mempunyai sijil pengesahan yang sah. Pastikan semua syarat berikut dipenuhi: <ul style="list-style-type: none"> <li>(i) <i>Security Server</i> mempunyai sekurang-kurangnya satu sijil pengesahan (lihat Bahagian User Guide-Security Server Mengkonfigurasi Kunci Pengesahan dan Sijil untuk Pelayan Keselamatan)</li> <li>(ii) Sijil adalah pada token yang dilog masuk dan tersedia (lihat Bahagian User Guide-Security Server Ketersediaan Keadaan Token Keselamatan, Kunci dan Sijil).</li> <li>(iii) Sijil didaftarkan (lihat Bahagian User Guide-Security Server Pendaftaran Negeri Pengesahan dan Sijil Penyulitan).</li> <li>(iv) Sijil aktif (lihat Bahagian User Guide-Security Server</li> </ul>
--	------------------------	--

		<p>Mengaktifkan dan Melumpuhkan Sijil).</p> <p>(v) Sambutan OCSP bagi sijil adalah baik (lihat Bahagian User Guide-Security Server Status Kesahan Sijil)</p>
<p><i>Service provider did not send correct authentication certificate</i></p>	<p>1. Hubungi pentadbir Security Server pembekal perkhidmatan</p>	<p>1. <i>Security Server</i> pembekal perkhidmatan tidak mempunyai sijil pengesahan yang sah. Pastikan semua syarat berikut dipenuhi:</p> <p>(i) <i>Security Server</i> mempunyai sekurang-kurangnya satu sijil pengesahan (lihat Bahagian User Guide-Security Server Mengkonfigurasi Kunci Pengesahan dan Sijil untuk Pelayan Keselamatan).</p> <p>(ii) Sijil adalah pada token yang dilog masuk dan tersedia (lihat Bahagian User Guide-Security Server Ketersediaan Keadaan Token</p>

		<p>Keselamatan, Kunci dan Sijil).</p> <p>(iii) Sijil didaftarkan (lihat Bahagian User Guide-Security Server Pendaftaran Negeri Pengesahan dan Sijil Penyulitan).</p> <p>(iv) Sijil aktif (lihat Bahagian User Guide-Security Server Mengaktifkan dan Melumpuhkan Sijil).</p> <p>(v) Sambutan OCSP bagi sijil adalah baik (lihat Bahagian User Guide-Security Server Status Kesahan Sijil).</p>
<i>Client specifies HTTPS but did not supply TLS certificate</i>	1. Sijil TLS sistem maklumat pelanggan perkhidmatan mesti dimuat naik ke <i>Security Server</i> pelanggan perkhidmatan (lihat Bahagian Komunikasi dengan Sistem Maklumat Pelanggan).	
<i>Could not find any certificates for member</i>	1. Hubungi pentadbir <i>Security Server</i> pelanggan perkhidmatan	1. Subsistem pelanggan perkhidmatan tidak mempunyai sijil tandatangan yang sah. Pastikan syarat berikut adalah benar: <p>(i) Terdapat sekurang-kurangnya satu sijil tandatangan untuk ahli yang dimiliki oleh</p>

		<p>subsistem tersebut (lihat Bahagian User Guide-Security Server Mengkonfigurasi Kunci Tandatangan dan Sijil untuk Pelanggan Pelayan Keselamatan).</p> <p>(ii) Sijil adalah pada token yang dilog masuk dan tersedia (lihat Bahagian User Guide Security Server Ketersediaan Keadaan Token Keselamatan, Kunci dan Sijil).</p> <p>(iii) Sijil didaftarkan (lihat Negeri Pendaftaran Bahagian User Guide-Security Server bagi Sijil Menandatangani).</p> <p>(iv) Sijil aktif (lihat Bahagian User Guide-Security Server Mengaktifkan dan Melumpuhkan Sijil).</p> <p>(v) Sambutan OCSP sijil adalah baik (lihat Bahagian User Guide-Security Server</p>
--	--	--

		Kesahan Negeri (Sijil)
<i>No space left on device</i>	1. Hubungi pentadbir <i>Security Server</i> pelanggan perkhidmatan	1. Pastikan <i>Security Server</i> pelanggan perkhidmatan mempunyai ruang cakera kosong. Jika cakera dipisahkan, pastikan <i>partition</i> yang berkaitan mempunyai ruang kosong
<i>Cannot timestamp messages: no timestamping services configure</i>	1. Hubungi pentadbir <i>Security Server</i> pelanggan perkhidmatan	1. Pastikan syarat berikut adalah benar: (i) <i>Security Server</i> pelanggan perkhidmatan boleh menyambung ke perkhidmatan <i>timestamp</i> . Semak bahawa semua <i>firewall</i> api dikonfigurasi dengan betul. (ii) Perkhidmatan <i>timestamp</i> tersedia. Semak log proksi (/var/log/uxp/proxy.log) untuk butiran lanjut
<i>Global configuration is expired</i>	1. Hubungi pentadbir <i>Security Server</i> pelanggan perkhidmatan	1. <i>Security Server</i> klien perkhidmatan tidak boleh memuat turun konfigurasi global daripada pelayan pendaftaran. Semak log klien konfigurasi (/var/log/uxp/configuration_client.log) untuk butiran

<p><i>Could not connect to target host (https://:5500)</i></p>	<p>1. Hubungi pentadbir Security Server pelanggan perkhidmatan</p>	<p>1. Security Server pelanggan perkhidmatan tidak boleh menyambung ke Security Server pembekal perkhidmatan. Pastikan firewall dikonfigurasi 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.</p>
<p><i>Name or service not known. No address associated with hostname.</i></p>	<p>1. Hubungi pentadbir Security Server pembekal perkhidmatan</p>	<p>1. Security Server pembekal perkhidmatan tidak dapat ditemui kerana Security Server didaftarkan dengan FQDN yang salah.</p>

### 3.1.4 Ralat Daripada Security Server Agensi Pembekal

Mesej Ralat	Penyelesaian Pentadbir Perkhidmatan	Penyelesaian Pentadbir Security Server
<p><i>Request is not allowed: SERVICE:EE_DEV/GOV/EX AMPLE_ORGANIZATION/EX</i></p>	<p>Security Server pembekal perkhidmatan mesti memberikan hak akses kepada perkhidmatan dan kepada subsistem pelanggan perkhidmatan. Lihat Hak Akses Bahagian</p>	

<p><i>AMPLE_DEPARTMENT/EXAMPLE_SERVICE</i></p>		
<p><i>Malformed SOAP message: header missing</i></p>	<p>Sistem maklumat pembekal perkhidmatan mesti mengembalikan semua pengepala UXP yang wajib. Lihat [UXP-PR-MESS] untuk butiran lanjut.</p>	
<p><i>A number of different error messages depending on cause of the error. For example, org.xml.sax.SAXParseException; Premature end of file.</i></p>	<p>Sistem maklumat pembekal perkhidmatan mengembalikan mesej SOAP yang tidak betul. Untuk butiran lanjut tentang error, semak log proksi <i>Security Server</i> penyedia perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server)</p>	
<p><i>Unknown service: SERVICE:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT/EXAMPLE_SERVICE</i></p>	<p>Pastikan kod perkhidmatan dalam mesej permintaan sepadan dengan perkhidmatan di bahagian pembekal perkhidmatan.</p>	
<p><i>The reason the connection failed. For example, Server responded with error 403: Forbidden</i></p>	<ol style="list-style-type: none"> <li>1. Pastikan <i>Security Server</i> pembekal perkhidmatan dibenarkan untuk menyambung ke sistem maklumat pembekal perkhidmatan dan sambungan dikonfigurasi dengan betul.</li> <li>2. Untuk maklumat lanjut tentang mengkonfigurasi sambungan, lihat Bahagian Komunikasi dengan Sistem Maklumat Pelanggan. Untuk butiran lanjut tentang ralat, lihat log proksi <i>Security Server</i> pembekal perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam <i>User Interface Security Server</i>).</li> </ol>	
<p><i>Server certificate is not trusted</i></p>	<p>Pilihan "Sahkan sijil TLS" dipilih dalam konfigurasi perkhidmatan, tetapi sijil sistem maklumat pembekal perkhidmatan belum dimuat naik ke <i>Security Server</i> penyedia perkhidmatan. Muat naik sijil sistem maklumat pembekal perkhidmatan ke <i>Security Server</i> (lihat Bahagian Komunikasi dengan Sistem Maklumat Pelanggan).</p>	
<p><i>Could not find any certificates for member 'SUBSYSTEM:SERVICE:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT'</i></p>	<ol style="list-style-type: none"> <li>1. Hubungi pentadbir <i>Security Server</i> pembekal perkhidmatan</li> </ol>	<ol style="list-style-type: none"> <li>1. Subsistem pembekal perkhidmatan tidak mempunyai sijil tandatangan yang sah. Pastikan syarat berikut adalah benar:                     <ol style="list-style-type: none"> <li>(i) Terdapat sekurang-kurangnya satu sijil tandatangan untuk ahli yang dimiliki oleh</li> </ol> </li> </ol>

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

<i>Token 'softToken' not active</i>	Hubungi pentadbir <i>Security Server</i> pembekal perkhidmatan	Pastikan bahawa token perisian <i>Security Server</i> pembekal perkhidmatan telah dilog masuk. Jika ia tidak dilog masuk, log masuk daripada <i>Security Server User Interface</i> pembekal perkhidmatan.
<i>Cannot timestamp messages: no timestamping services configured</i>	Hubungi pentadbir <i>Security Server</i> pembekal perkhidmatan	Anda mesti mengkonfigurasi perkhidmatan timestamp untuk <i>Security Server</i> pembekal perkhidmatan (lihat Bahagian <i>User Guide-Security Server</i> Mengurus Perkhidmatan Timestamp).
<i>Cannot timestamp messages</i>	Hubungi pentadbir <i>Security Server</i> pembekal perkhidmatan	<p>1. Walaupun terdapat perkhidmatan <i>timestamp</i> yang dikonfigurasi (lihat mesej ralat sebelumnya), <i>timestamp</i> masih boleh gagal. Masalah berikut mungkin berlaku:</p> <ul style="list-style-type: none"> <li>(i) Terdapat masalah pada bahagian perkhidmatan <i>timestamp</i> dan perkhidmatan tidak tersedia. Semak log proksi (<i>var/log/uxp/proxy .log</i>) untuk butiran lanjut.</li> <li>(ii) <i>Security Server</i> pembekal perkhidmatan tidak boleh menyambung ke perkhidmatan <i>timestamp</i>. Pastikan bahawa firewall dan port dikonfigurasi dengan betul untuk kedua-dua perkhidmatan <i>Security Server</i> dan <i>timestamp</i>.</li> </ul>
<i>Global configuration is expired</i>	Hubungi pentadbir <i>Security Server</i> pembekal perkhidmatan	Cuba mulakan semula proses klien konfigurasi \$ <i>systemctl</i> mulakan semula <i>uxp-confclient</i> . Ada kemungkinan

		<p><i>Security Server</i> penyedia perkhidmatan tidak dapat menyambung ke pelayan pendaftaran untuk memuat turun konfigurasi global. Pastikan konfigurasi <i>firewall</i> api di kedua-dua belah adalah betul. Lihat log klien konfigurasi untuk butiran lanjut (/var/log/uxp/configuration_client.log)</p>
--	--	---