eID Integration Document

Implementation of the Malta Electronic Identity

Date: 20/05/2010
Version: 2.1

Sensitive but Unclassified

Document Control Information

01.   Document reference

eID Integration Document_MITA_v2.1.doc

02.   Document type

Procedure

03.   Security classification

Sensitive but Unclassified

04.   Synopsis

This document provides the required instructions for the integration of systems with the eID

05.   Document control

Author	Change controller	Distribution controller

06.   Authorisation

Issuing authority	Approval authority
NIDMS Project Manager	NIDMS Project Manager
Signature / Date	Signature / Date

07.   Modification history

Version	Date	Comments
Version 1.5.1	11/08/2009	Updated Exigy document for release
Version 2.0	20/01/2010	Updated to a MITA document and additions made relating to integration principles
Version 2.1	20/05/2010	Update organisation schema to include Organisation Legal Types

08.   Acknowledgements

Exigy Ltd.

09.   References

All relevant MITA standards and policies

10.   Distribution list (for reports only)

Table of Contents

01.   Introduction

01.1   Purpose

The primary audiences are all the development team and project managers engaged by the Service Providers and organisations that are using the eID as their authentication mechanism ('Integrating Party'). This document is to be used as an integration guide that provides technical information on the integration interfaces provided by the eID and does not explain the detailed business processes provided by the eID.

01.2   Scope

The purpose of this document is to illustrate the procedure and methods that will need to be used by 3rd parties carrying out the integration with the eID.

The document is subdivided into a number of areas that should be used as follows:

- eID Integration Principles – provides the main business and integration principles to be followed by Service Providers and Integrating Parties.

- Integration – provides a detailed explanation of the single sign-on mechanism and integration with the myGov portal.

- Business Flows – provides information on various scenarios that must be followed by Integrating Parties depending on their integration requirements.

- Web Services – provides a detailed description of the input parameters expected by each web service that will be consumed. The WSDL of the soap request and response messages is also given.

02.   eID Integration Principles

02.1   eID Business Principles

1. eID accounts are issued exclusively to holders of a valid Maltese identity card. The accounts are personal and non-transferable.

2. eID organisations are organisations that are registered with the Malta Financial Services Authority, exclusively.

3. Sole Traders are treated within eID as normal citizens, i.e. they are *not* organisations.

4. eID organisations are created as a separate entity to that of an eID individual user within myGov and eID organisations can subscribe to the available eServices and make use of the available functionality.

5. eID accounts or organisations which have subscribed to an eService can choose to delegate this service to another eID registered organisation or to an eID registered individual user.

6. eID accounts or organisations which have subscribed to an eService have the functionality to assign the responsibility of the use of this service to an employee within that organisation.

7. Agent enabled eServices allow that for agent type organisation an agent can only subscribe and make use of that eService on behalf of a valid Identity Card holder who is not eID registered and who requests use of that service.

02.2   eID Integration Principles

1. This document is the only approved integration method to the eID.

2. It is the sole responsibility of the integrating party to maintain the logs and audit records of the electronic service, including logs of access to all the eID web services. The integrating party shall not make reliance implicit or otherwise on any other logs.

3. It is the sole responsibility of the Integrating Party to implement the certificate revocation check.

4. The eID accounts and eID organisations shall only be used for the purposes of authentication to electronic services offered through the portal of the Government of Malta according to the Subscriber Agreement and Organisation Services Agreement

5. There is a distinction between an eID holder subscribing to a service on his personal capacity or on that of the organisation s/he is managing. The eID provides the mechanism for the Integrating Party to distinguish between the two scenarios but it is the sole responsibility of the Integrating Party to use this mechanism appropriately.

03.   Integration

This section will describe in detail the integration process and components that will need to be used by 3rd parties wishing to integrate and make use the eID.

03.1   Single Sign-On

This section describes how the single sign-on concept can be achieved through the eID.
Note: The single sign-on concept is only available when users authenticate via the mygov.mt portal and then navigate to the service provider web site.

03.1.1 Single Sign-On cookie

The single sign-on implementation will be achieved through a cookie created at the domain level. All web sites hosted under the gov.mt domain will be able to make use of the domain cookie to achieve seamless user authentication across sites.

03.1.1.1 Technical Implementation

Detailed description of the cookie contents and encryption algorithms used for the contents.

Name	Value	Description
Cookie Name	randa2	
Domain	gov.mt	Top level domain to allow access by all sites hosted underneath.
Duration	Session	Cookie is a session cookie and will be valid throught the browser session.
Value	Encrypted value will contain the userid and sessionid. The locale will be stored in plain text.	userid – string representing a GUID (encrypted) sessionid – string representing a GUID (encrypted) locale – localization in the form of "en-US" (plain text)

The value of the cookie is being encrypted and will be decrypted by the eID to determine authentication credentials when passed as a paremeter during calls to web servicess. Below is a detailed explanation on how the cookie can be consumed by sites hosted both on the e-Government Platform and outside.

The cookie value will contain an encrypted segment and a plain text segment containing the following information:

Encrypted segment of cookie
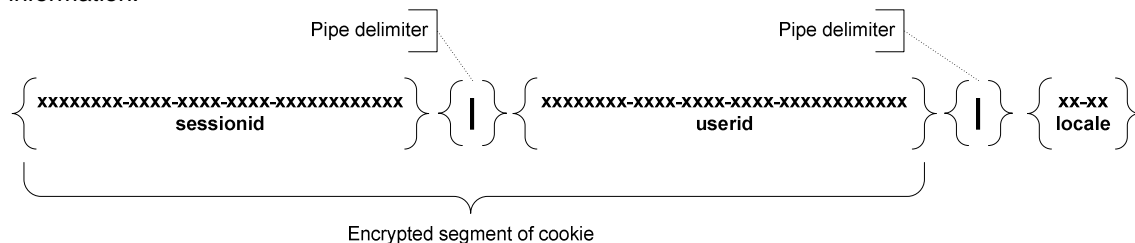
Only the encrypted segment of the cookie must be used as the CypherText value. The locale should be used to determine the language selected by the user from the mygov.mt portal before moving to the Service Provider web site. The same language should be offered to the user once he/she lands on the Service Provider site. The locales are described in Section 08 Appendix C – Locales

03.1.1.2 Cookie consumption

This section will describe how 3rd parties should make use of the cookie to achieve single sign-on functionality while adhering to the required security requirements.

03.1.1.2.1 Sites hosted under the mygov.mt and gov.mt domain

All sites hosted under the gov.mt domain can retrieve the cookie and read the cookie value. The cookie value will be used later to access the eID web services without the need to authenticate again. Sites that are not hosted under the mygov.mt or gov.mt domain will not have access to the cookie.

03.1.2   Redirection from myGov

The redirection from myGov will be used when users authenticate initially through the myGov Portal. In these cases the user is authenticated through the myGov Portal and then redirected to the appropriate service provider web site based on the eService selected by the user.
When the user selects an eService from the myGov Portal, the portal will redirect the user to the url configured for the selected eService and pass additional parameters required to retrieve the eService attributes.

03.1.2.1 Redirection URL

A URL is configured for each eService and used to redirect the user when an eService is selected from the myGov portal.

03.1.2.2 Parameters

The parameters are passed along the URL used to redirect the user. The parameters will be used at a later stage to retrieve eService attributes that are defined by the eCitizen when subscribing for the eService.

The following parameters will be passed:

Parameter	Value
UserID	The UUID of the eCitizen that is currently logged in and trying to access the eService.
OwnerID	The UUID of the Citizen or Organisation that subscribed to the eService.
EntityType	Determines if the eService owner is an eCitizen or an Organisation.
eServiceID	UUID of the eService.
eServiceKey	Unique key assigned by the Service Provider to the eService.
SubscriptionType	Determines the relationship that exists between the eCitizen or Organisation and the eService.

The eCitizen will be redirected to the service provider web site with the following URL.

http://<configured eService *URL*>?userid=<*eCitizen UUID*>&ownerid=<*Service Owner Guid*>&entitytype=<eCitizen | Organisation>&eserviceid=<*eService UUID*>&eservicekey=<*eService Key*>&subscribtiontype=<*Subscribed | Delegated | Assigned*>

Upon receiving the request the service provider web site will extract the parameters from the query string and use as required by the various eID web services.

03.1.3 Redirection from myGov for Trusted Agents

The redirection from myGov will be used when trusted agents authenticate through the myGov Portal. In these cases the trusted agent is authenticated through the myGov Portal and then redirected to the appropriate service provider web site based on the eService selected by the Citizen.
When the trusted agent selects an eService from the myGov Portal, the portal will redirect the trusted agent to the url configured for the selected eService and pass additional parameters required to retrieve the information configured for the eService.

03.1.3.1 Redirection URL

A URL is configured for each eService and used to redirect the trusted agent when an eService is selected from the myGov portal.

03.1.3.2 Parameters

The parameters are passed along the URL used to redirect the trusted agent. The parameters will be used at a later stage to retrieve the information that has been configured for the selected eService.
The following parameters will be passed:

Parameter	Value
UserID	The UUID of the Trusted Agent that is currently logged in and trying to access the eService.
OwnerID	The UUID of the Citizen that is delegating the eService to the Trusted Agent.
EntityType	Determines the eService owner that will always be an eCitizen.
eServiceID	UUID of the eService.
eServiceKey	Unique key assigned by the Service Provider to the eService.
SubscriptionType	Determines the relationship that exists between the eCitizen and the eService.
AgreementNo	The unique number attached to the delegation agreement that was signed by the Citizen to delegate a particular eService to a Trusted Agent.

Note: The Trusted Agent will collect the necessary information about the Citizen during the delegation process. The information collected about the Citizen can be retrieved using the OwnerID parameter.

The Trusted Agent will be redirected to the service provider web site with the following URL.

http://<configured eService *URL*>?userid=<*Trusted Agent UUID*>&ownerid=<*Delegating Citizen UUID*>&entitytype=<eCitizen>&eserviceid=<*eService UUID*>&eservicekey=<*eService Key*>&subscribtiontype=<*AgentDelegated*>&agreementno=<*unique no linked to current delegation*>

Upon receiving the request the service provider web site will extract the parameters from the query string and use as required by the various eID web services.

04.   Business Flows

This section will highlight the processes that need to be followed by 3rd parties when integrating with the eID. Three different scenarios are discussed in detail.

1. Authentication for gov.mt domain sites describes the process that must be adopted by all web sites that are hosted under the gov.mt domain. This applies to sites hosted both on the e-Government Platform and outside the e-Government Platform.

2. Certificate Verification and Validation describes the process that is carried out by the eID Framework to verify the digital certificate.

3. eService Access from myGov describes the process were a user has authenticated through the myGov portal and selects and eService that he/she would like to access.

4. eService Access from myGov by Trusted Agent describes the process were a Trusted Agent has authenticated through the myGov portal and selects and eService that a Citizen has indicated for delegation.

5. eService Access from Service Provider describes the process were a user authenticates directly through the service provider web site and does not make use of the myGov portal.

04.1   Authentication for gov.mt domain sites

This is the authentication process that will be followed by sites hosted under the gov.mt domain. The sites can be hosted either on the e-Government Platform or outside the e-Government Platform.

Authentication for sites hosted under the gov.mt domain
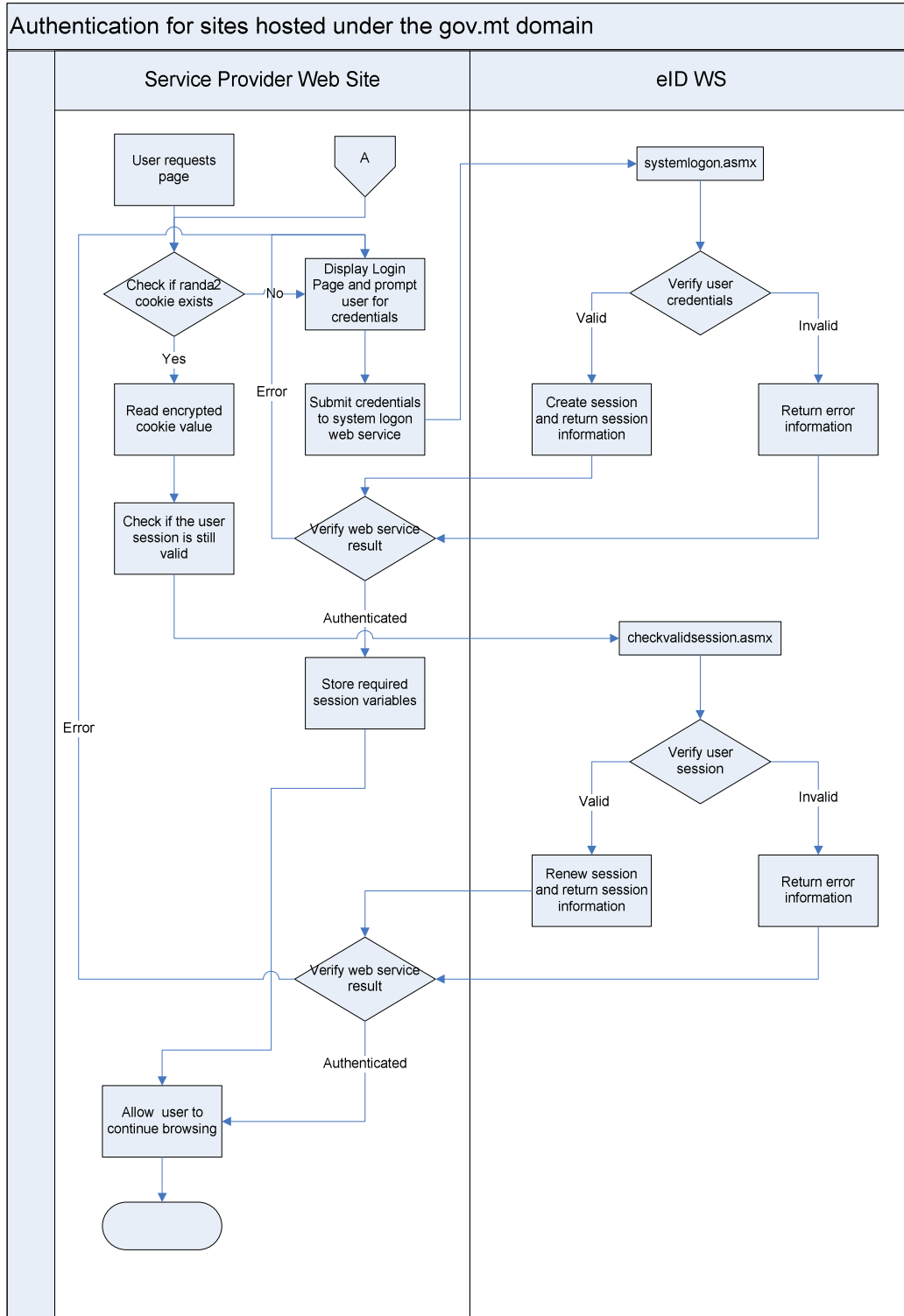
1. User requests a page from the service provider web site.

2. Service provider checks if the randa2 single sign-on cookie exists.

3. If the single sign-on cookie exists then the Service Provider will perform the following tasks:

a. The service provider will read the encrypted contents of the cookie.

b. Verify that the user has an active eID session by calling the web service checkvalidsession.asmx using the encrypted cookie value as a parameter (Refer to Check Valid Session).

c. If a valid eID session exists store the **<UserID>** element, **<SessionID>** element and **<Locale>** element in the session (or any method determined by the service provider) for use in following steps.

d. If a valid eID session is not found the single sign-on cookie must be ignored and the user is taken to the login page and asked to authenticate.

4. If the single sign-on cookie does not exist then the Service Provider will perform the following tasks:

   a. The user is taken to the login paged and asked to authenticate.

   b. Authenticate the user by calling the web service systemlogon.asmx using the username and password entered by the user as parameters (Refer to System Logon).

   c. If a valid eID session is returned store the **<UserID>** element, **<SessionID>** element and **<Locale>** element in the session (or any method determined by the service provider) for use in following steps.

   d. If a valid eID session is not created the user is taken to the login paged and asked to authenticate.

5. Allow user access to the site following any other checks external to the eID that need to be done by the service provider.

04.2   Certificate Verification and Validation

This section will describe the certificate validation and verification process that is carried out by the eID framework. This description is for information purposes only and the Integrating Party is fully and solely responsible to implement the certificate revocation check.
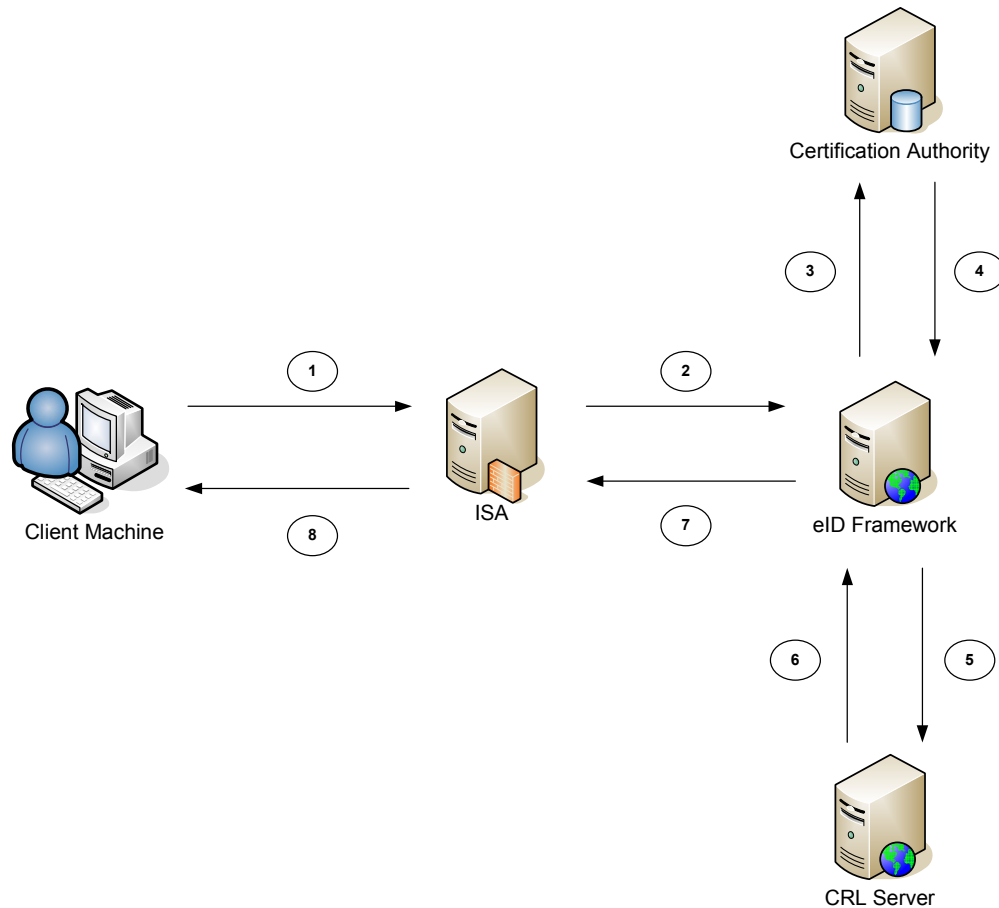
1. The client and ISA server perform an SSL handshake and an SSL connection is established. During this process various tokens are exchange and the client will have presented the certificate containing the public key to the server.

2. The ISA server forwards the serial number of the certificate to the eID framework which then determines the source that will be used to verify the certificate using the following logic.

    a. By default the verification is performed against the certification authority directly as in Step 3.

    b. If the certification authority is unreachable then the certificate is checked against the CRL as in Step 5.

3. The certificate is checked against the certification authority.   Verification against the Certification Authority covers the following checks:

    a. Checks certificate status against the live CA database.

    b. Checks that the certificate is part of a chain that contains a trusted root.

    c. Checks the time validity of all certificates in the chain.

    d. Checks that all certificates in the chain have a valid signature.

4. The Certification Authority returns the certificate status information to the eID Framework. User is authenticated and a response is returned to the client server. Proceed to Step 7.

5. The certificate is checked against the CRL. Verification against the CRL covers the following checks:

   a. Checks certificate against the latest CRL available online if the local CRL has expired.

   b. Checks that the certificate is part of a chain that contains a trusted root.

   c. Checks the time validity of all certificates in the chain.

   d. Checks that all certificates in the chain have a valid signature.

6. The Certification Authority returns the certificate status information to the eID Framework. User is authenticated and the http response is returned to the client server. Proceed to Step 7.

7. The http response is returned to the ISA server.

8. The http response is returned to the client machine.

04.3   eService Access from myGov

This process describes the procedure for users that have been authenticated through the myGov portal and are being redirected to a service provider web site.
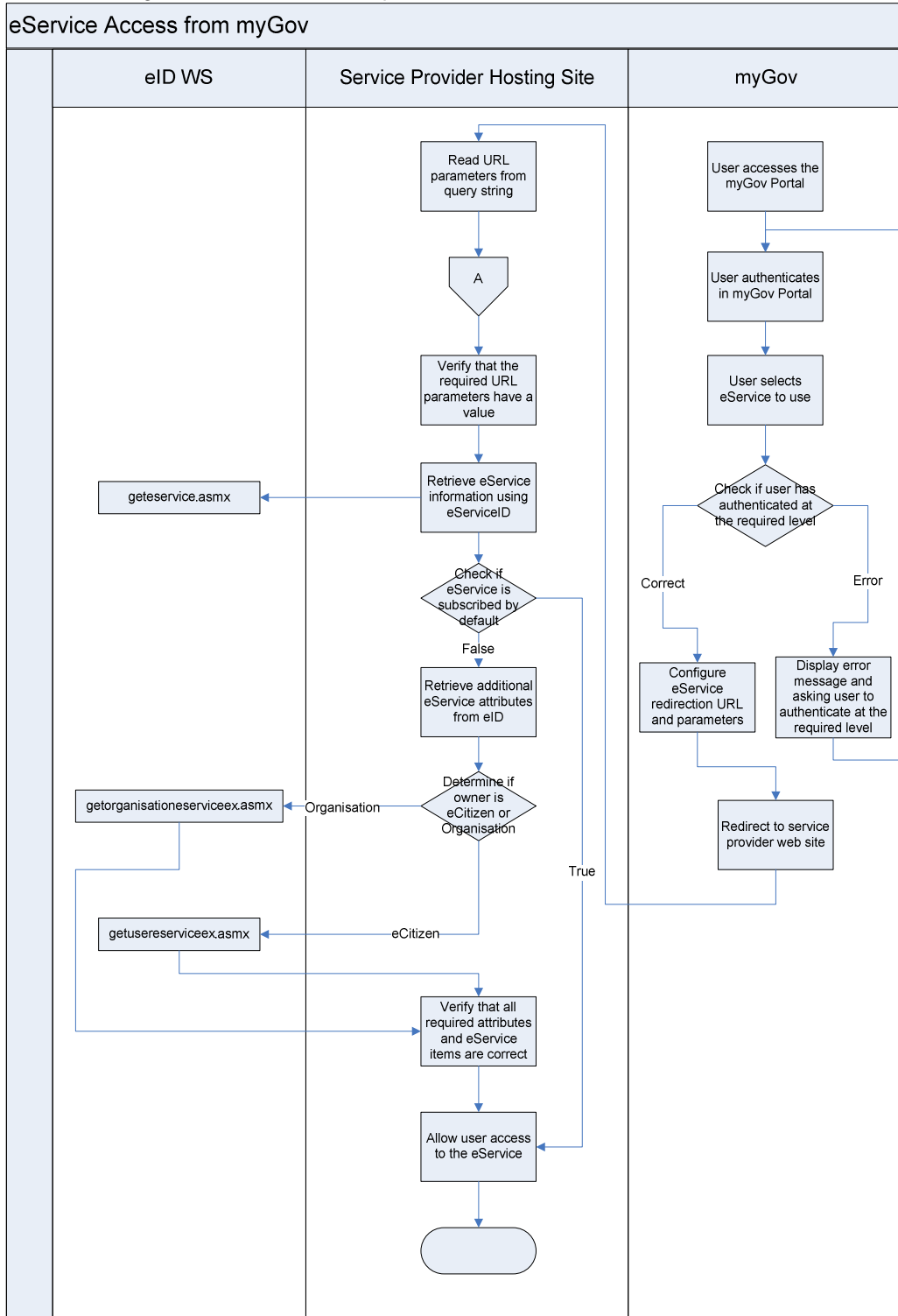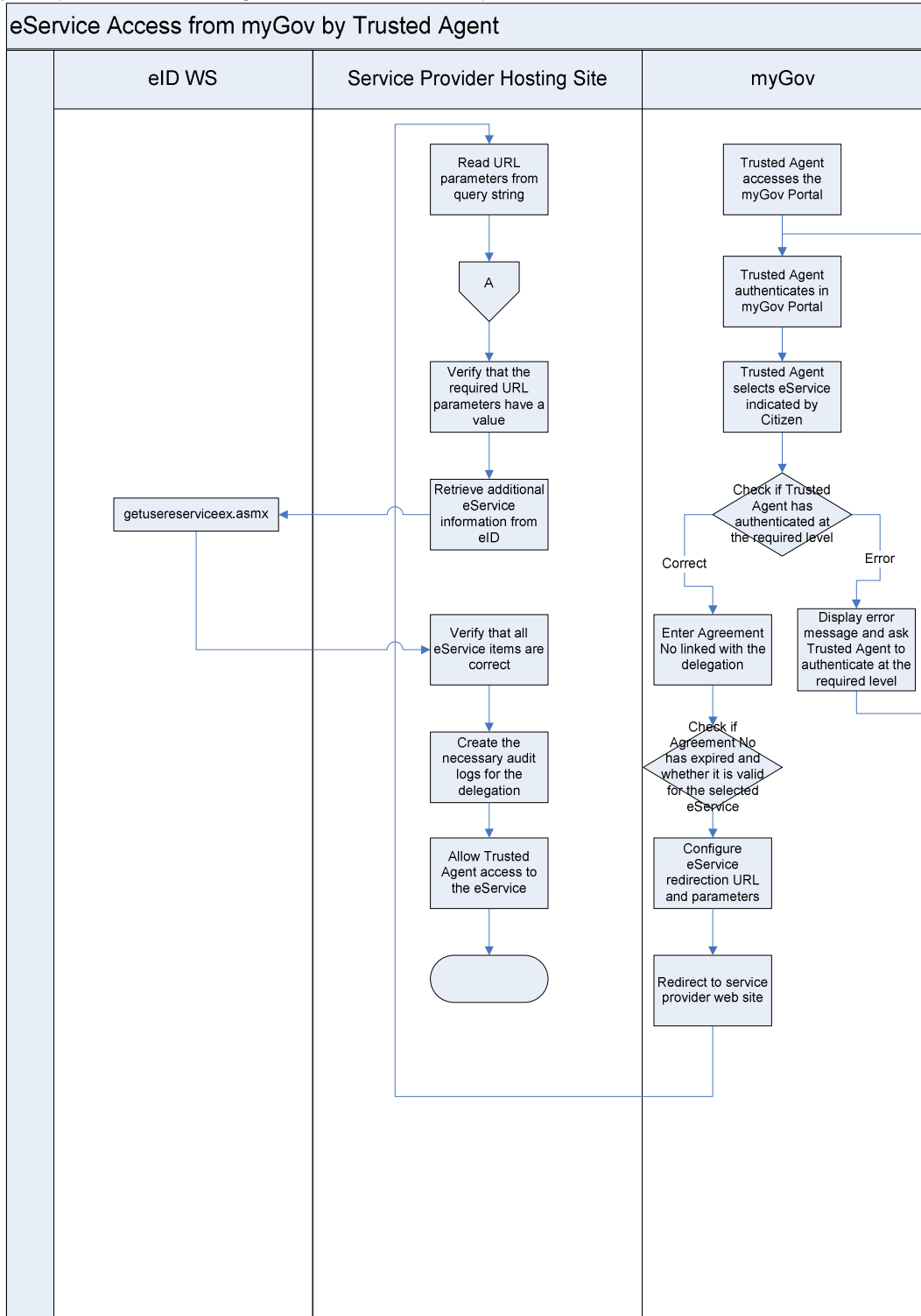
1. User navigates to the myGov Portal and will be asked to authenticate.

2. User authenticates through myGov at Level 1 (username, password) or Level 2 (username, password and certificate)

3. User selects the required eService from the myGov navigation bar.

4. myGov checks if the user has authenticated at the level required by the eService.

5. If user is not authenticated at the required level, the system will prompt the user to authenticate at the required level.

6. If the user has authenticated at the required level, the system will generate the required eService URL and parameters and redirect the user to the service provider web site.

7. Service provider will read the URL parameters passed in the query string by the eID.

8. Service provider will verify the user authentication according to the Authentication for gov.mt domain sites process.

9. Following the above process the service provider should have the **UserID** and **SessionID** values that should be kept in the session (or any method determined by the service provider)[1].

10. Service provider will verify all the URL parameters according to the following procedure

    e. Verify that all the required parameter keys are in the query string.

    f. Compare the *userid* from the URL parameters to the **UserID** value held by the service provider. This check will verify that the user has not changed and is the same person that selected the eService from myGov.

    g. The entity associated with the *ownerid* URL parameter can be determined from to the *entitytype* URL parameter.   The *entitytype* can contain either eCitizen or Organisation.

11. Retrieve the additional eService information from the eID by calling the webservice geteservice.asmx using the query parameters EserviceID =   *eserviceid* (Refer to Get eService).

12. Service provider checks if the eService is subscribed by default to all eCitizens by checking the `<SubscribedByDefault>` element. If the element is set to **true** then the eCitizen can be allowed access (Proceed to Step 16) after any other validation required by the Service Provider has been performed.

13. Service provider checks if the user has authenticated at the level required by the eService.

    h. Verify that the user is authenticated at the require level. Compare the `<AccessLevel>` element against the `<AuthenticationLevel>` element in the EgovResponseHeader soap header returned with each web service response.

    i. If user is not authenticated at the required level, the service provider should prompt the user to authenticate at the required level.

14. If the user has authenticated at the required level, the service provider will retrieve the additional eService information from the eID depending on the *entitytype* URL parameter:

    j. eCitizen – call the webservice getusereserviceex.asmx using the query parameters EserviceID = *eserviceid*, UserID = *ownerid* and EServiceRelation = **"Subscribed"**. (Refer to Get User eService Extended).

    k. Organisation - call the webservice getorganisationeserviceex.asmx using the URL parameters EserviceID =   *eserviceid*, OrganisationID = *ownerid* and EServiceRelation = **"Subscribed"**. (Refer to Get Organisation EService Extended)

---

[1] It is the sole responsibility of the integrating party to maintain the logs and audit records of the electronic service, including logs of access to all the eID web services. The integrating party shall not make reliance implicit or otherwise on any other logs.

15. Verify the information returned by the web service against the URL parameters and single-sign cookie by following this procedure:

     l.   Verify that the **\<Status\>** element is set to **Active**, indicating that the eService has been approved.

     m. Verify that all eService attributes in the **\<OwnerAttributes\>** element that have the **\<Mandatory\>** element set to true have a corresponding value in the **\<AttributeValue\>** element. All mandatory attributes should have a value assigned.

16. Allow user access to the eService following any other checks external to the eID that need to be done by the service provider.

04.4   eService Access from myGov by Trusted Agent

This process describes the procedure for Trusted Agents that have been authenticated through the myGov portal and are being redirected to a service provider web site.

> **Note:** The current release of the Trusted Agent does not cater for eServices that require additional attributes to be provided by the Citizen before the eService can be accessed.

1. Trusted Agent navigates to the myGov Portal and will be asked to authenticate.

2. Trusted Agent authenticates through myGov at Level 1 (username, password) or Level 2 (username, password and certificate)

3. Trusted Agent selects the eService indicated by the Citizen requesting the delegation from the myGov navigation bar.

4. myGov checks if the Trusted Agent has authenticated at the level required by the eService.

5. If Trusted Agent is not authenticated at the required level, the system will prompt the Trusted Agent to authenticate at the required level.

6. If the Trusted Agent has authenticated at the required level, the system will ask the Trusted Agent to enter the Agreement No that is linked to the current delegation request. If an Agreement No does not yet exist the system will allow the Trusted Agent to create a delegation agreement.

7. The system will check if the Agreement No entered belongs to a delegation agreement that is still valid and whether the delegation agreement was signed for the selected eService.

8. If the Agreement No is valid the system will generate the required eService URL and parameters and redirect the Trusted Agent to the service provider web site.

9. Service provider will read the URL parameters passed in the query string by the eID.

10. Service provider will verify the user authentication according to the Authentication for gov.mt domain sites process.

11. Following the above process the service provider should have the **UserID** and **SessionID** values that should be kept in the session (or any method determined by the service provider)[2].

12. Service provider will verify all the URL parameters according to the following procedure

    a. Verify that all the required parameter keys are in the query string.

    b. Compare the *userid* from the URL parameters to the **UserID** value held by the service provider. This check will verify that the user has not changed and is the same person that selected the eService from myGov.

    c. The entity associated with the *ownerid* URL parameter can be determined from to the *entitytype* URL parameter. The *entitytype* will always contain an eCitizen.

    d. Retrieve the additional eService information from the eID by calling the webservice getusereserviceex.asmx using the query parameters

        i. EServiceID = *eserviceid*, UserID = *ownerid* and EServiceRelation = *subscriptiontype*. (Refer to Get User eService Extended).

    e. Verify the information returned by the web service against the URL parameters and single-sign cookie by following this procedure:

        ii. the *subscriptiontype* URL parameter should be set to *AgentDelegated*

        iii. Verify that the user is authenticated at the require level. Compare the <AccessLevel> element against the <AuthenticationLevel> element in the EgovResponseHeader soap header returned with each web service response.

    f. The SP should create the necessary delegation audit using as minimum the User ID, Owner ID, eService ID and Agreement No. The Agreement No should always be

---

[2] It is the sole responsibility of the integrating party to maintain the logs and audit records of the electronic service, including logs of access to all the eID web services. The integrating party shall not make reliance implicit or otherwise on any other logs.

stored with the transaction to allow cross-referencing with the delegation agreement when necessary.[3]

 g. Allow Trusted Agent access to the eService following any other checks external to the eID that need to be done by the service provider.

---

[3] It is the sole responsibility of the integrating party to maintain the logs and audit records of the electronic service, including logs of access to all the eID web services. The integrating party shall not make reliance implicit or otherwise on any other logs.

04.5   eService Access from Service Provider

This process describes the procedure for users that have been authenticated through the Service Provider web site.
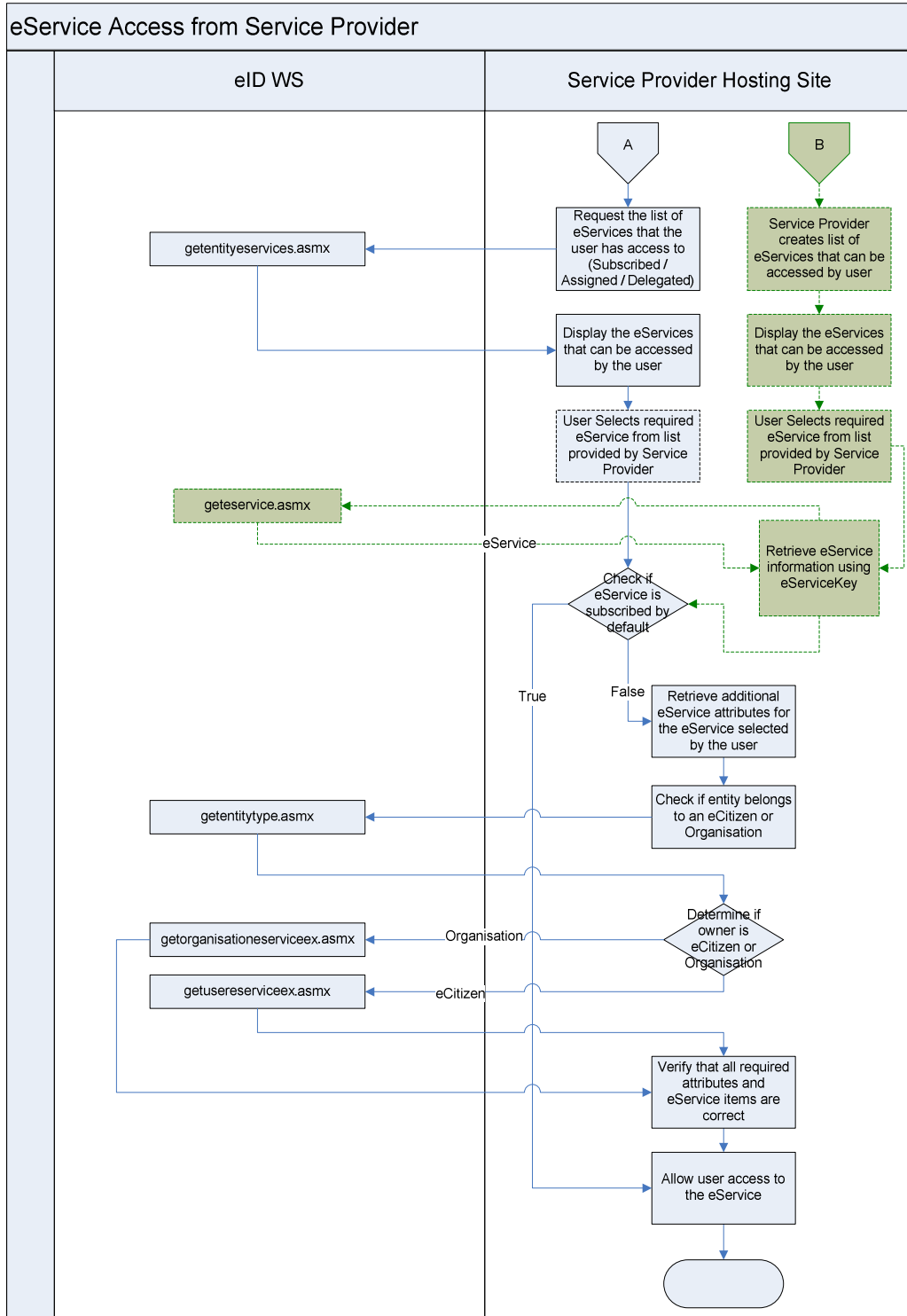
The diagram illustrates the 2 options that are available to Service Providers:

Option A: is the preferred integration option that must be followed by Service Providers

Option B: has been included only to offer backward compatibility.

1. Service provider will authenticate user according to the Authentication for gov.mt domain sites process.

2. Following the above process the service provider should have the **UserID** and **SessionID** values[4].

3. The service provider will display the eServices that can be accessed by the logged on user (Refer to section Additional Information to display eServices). The eServices that can be retrieved are subdivided into 3 **EServiceRelation** values being **Subscribed**, **Assigned** and **Delegated**.

    a. Retrieve the eServices by calling the webservice getentityeservices.asmx using the **UserID** value and **EServiceRelation** value (Refer to Get Entity eServices).

    b. Alternatively the service provider will display the eServices that can be accessed by the logged on user through its own preferred method by building a list of eServices using its own logic and database. (**It is important that for each eService the eService key is known as it will be used further on in the process**)

4. User selects the required eService from the service provider navigation bar. The service provider will need to retain the **<UUID>** and **<SubscriberID>** elements of the selected eService.

    a. If the service provider chooses the option of building its own list of eServices than the information for the selected eService can be retrieved by calling the web service geteservice.asmx using the *eServiceKey* as parameter (Refer to Get eService).

5. The service provider checks if the eService owner is an eCitizen or an Organisation depending on the **<EntityType>** element. If the entity type is an eCitizen then the service provider will check if the eService has been subscribed by default to all eCitizens by checking the **<SubscribedByDefault>** element. If the element is set to **true** then the eCitizen can be allowed access (Proceed to Step 9) after any other validation required by the Service Provider has been performed.

6. Service provider checks if the user has authenticated at the level required by the eService.

    a. Verify that the user is authenticated at the require level. Compare the **<AccessLevel>** element against the **<AuthenticationLevel>** element in the EgovResponseHeader soap header returned with each web service response.

    b. If user is not authenticated at the required level, the service provider should prompt the user to authenticate at the required level.

7. If the user has authenticated at the required level, the service provider will retrieve the additional eService information from the eID depending on the **<EntityType>** element:

    a. Determine the entity associated with the **<SubscriberID>** element by calling the web service getentitytype.asmx. The entity can be either an eCitizen or Organisation. The service provider will need to retain the **<EntityType>** element returned by the web service.

        i. eCitizen – Retrieve the additional eService information from the eID by calling the webservice getusereserviceex.asmx using the **<UUID>** element, **<SubscriberID>** element and *eservicerelation* (Refer to Get User eService Extended).

        ii. Organisation - Retrieve the additional eService information from the eID by calling the webservice getorganisationeserviceex.asmx using the **<UUID>**

---

[4] It is the sole responsibility of the integrating party to maintain the logs and audit records of the electronic service, including logs of access to all the eID web services. The integrating party shall not make reliance implicit or otherwise on any other logs.

element, **<SubscriberID>** element and *eservicerelation* (Refer to Get Organisation EService Extended).

8. Verify the information returned by the web service against the values held by the service provider by following this procedure:

    a. Verify that the **<Status>** element is set to **Active**, indicating that the eService has been approved.

    b. Verify that all eService attributes in the **<OwnerAttributes>** element that have the **<Mandatory>** element set to true have a corresponding value in the **<AttributeValue>** element. All mandatory attributes should have a value assigned.

9. Allow user access to the eService following any other checks external to the eID that need to be done by the service provider.

04.5.1   Additional Information to display eServices

This section describes the different relations that can exist between an eCitizen and an eService. Understanding these relations will help service providers in building an appropriate UI that will be presented to the end user.

Relation	Description
Subscribed	The subscribed eServices are those eServices that an eCitizen has subscribed for directly in his/her own capacity
Delegated	The delegated eServices are those eServices that have been delegated to the eCitizen by another eCitizen or by an Organisation.
Assigned	The assigned eServices are those eServices that have been subscribed to by an Organisation and then delegated to an eCitizen or Group. The eCitizen would have to be an employee of the Organisation assigning the eService.

The diagram below illustrates a sample UI that can be adopted by Service Providers to present eServices to an eCitizen.
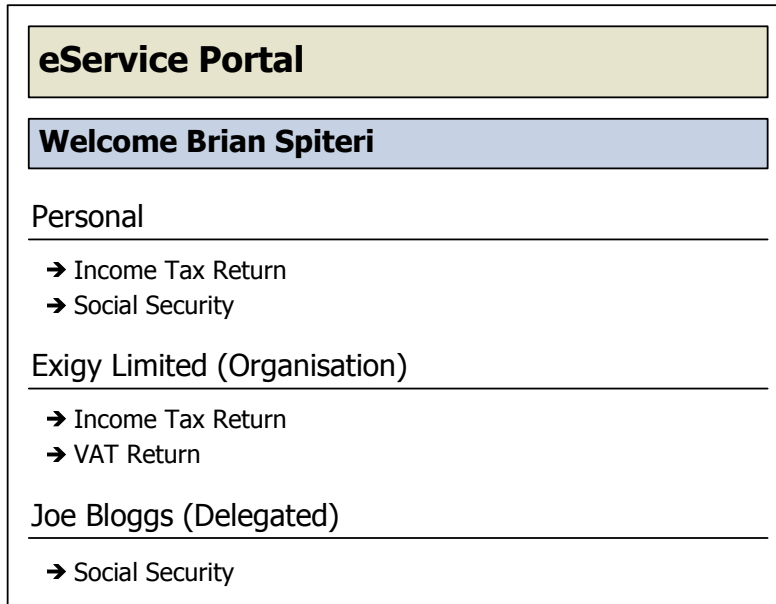
Personal – this section would be equivalent to the Subscribed relation, showing eServices that an eCitizen has subscribed for.

Exigy Limited (Organisation) – this section would be equivalent to the Assigned relation, showing eService that have been assigned to the eCitizen.

Joe Bloggs (Delegated) – this section would be equivalent to the Delegated relation, showing eServices that have been delegated to the eCitizen.

04.6   Web Service Summary

This section provides a brief description of each web service that can be consumed by 3rd parties integrating with the eID.

04.6.1   System Logon

Before any interactions can be done the eCitizen will need to authenticate with the eID.

The authentication can be achieved by calling the web service systemlogon.asmx (Refer to System Logon).

04.6.2   System Logoff

When an eCitizen has finished using the required eservices the eID session needs to be terminated.

To terminate the session call the web service systemlogoff.asmx (Refer to System Logoff).

04.6.3   Check Valid Session

The web service will be used to check that the existing session information held by a service provider is still valid. Calling the web service will also renew the existing session, which will be extended by the configured session lifetime.

To check if the user has an existing valid session and renew session timeout, call the web service checkvalidsession.asmx (Refer to Check Valid Session).

04.6.4 Get Entity Type

The web service will return the entity associated with a given entity id. Each entity id can only be associated with one entity type. The entity type can be either an eCitizen or Organisation.

To determine the entity type call the web service getentitytype.asmx (Refer to Get Entity Type).

04.6.5   Get Eservice

The web service will return all the information held about an eService.

To retrieve the eService and related information call the web service geteservice.asmx (Refer to Get eService).

04.6.6   Get Entity eServices

The web service will return all the eServices that an eCitizen has subscribed for. The web service will also return eServices that have been assigned or delegated by another eCitizen.

To retrieve the list of eServices that can be accessed call the web service getentityeservices.asmx (Refer to Get Entity eServices).

04.6.7   Get User eService Extended

The web service will return the eService information and also the information submitted by the user when subscribing for the eService including any eService attributes.

To retrieve all the subscription information for an eService subscribed for by an eCitizen call the web service getusereserviceex.asmx (Refer to Get User eService Extended).

04.6.8   Get Organisation EService Extended

The web service will return the eService information and also the information submitted by the user on behalf of the organisation when subscribing for the eService including any eService attributes.

To retrieve all the subscription information for an eService subscribed for by an organisation manager on behalf of an organisation call the web service getorganisationserviceex.asmx (Refer to Get Organisation eService Extended).

04.6.9   Get Citizen

The Get Citizen web service will return the eCitizen information held by the eID.

To retrieve the information for an eCitizen call the web service getcitizen.asmx (Refer to Get Citizen)

04.6.10   Get Organisation

The Get Organisation web service will return the Organisation information held by the eID.

To retrieve the information for an Organisation call the web service getorganisation.asmx (Refer to Get Organisation).

05.   Web Services

This section will give a description of the soap message structure adopted by the eID web services. A detailed description of each web service to be consumed is also presented.

The schemas provided reflect the complete set of elements that make up the eID schema. The document however will only describe the elements that are required and will be consumed by 3rd parties. All elements that are not documented should be ignored and their values should not be relied upon.

All web services are protected by means of BASIC authentication and are accessible over SSL. The consumption of these web services requires authentication.

05.1   Soap Message Structure

Description of the soap envelop that will be used by the eID web services. Each soap message will be made up of 2 section being the Header and Body.

<?xml version="1.0" encoding="utf-8"?>

<soap:Envelope>

   <soap:Header>

   </soap:Header>

   <soap:Body>

   </soap:Body>

</soap:Envelope>

05.2   Soap Headers

Soap Headers have been adopted by the eGovernment Framework to provide authentication, session management and error handling functionality that are common across all the web services.

05.2.1   EgovRequestHeader

The request header must be attached to all web service requests and is used for authentication and authorization purposes.

The UserID/SessionID or CypherText must be used to access web services without the need to re-authenticate. The CypherText parameter is used to replace the UserID and SessionID parameters and when used should contain the encrypted portion of the single sign-on cookie.

The CertificateSerial must be passed when the user has authenticated using a digital certificate. The serial number will be checked against the serial number used during initial authentication to verify that the same certificate is used throughout the session.

The serial number is expected to be a contiguous string of hexadecimal numbers without any spaces or special characters e.g. "1ebd195c0000000000bd". Other formats like "1e bd 19 5c 00 00 00 00 00 bd" or "1e-bd-19-5c-00-00-00-00-00-bd" are not accepted.

The AppKey must always be present and must be the key assigned to the Service Provider when registering with the eID.

The Locale if present will be used to determine which language will be used to return error messages and data. If the Locale is not used the default en-US locale will be used. For a list of applicable locales refer to Appendix C – Locales.

Element	Description	Type
UserID	UUID of citizen returned after login	Session
SessionID	UUID of session returned after login	Session
CertificateSerial	The serial number of the digital certificate	Session
AppKey	Key assigned to the Service Provider	
Locale	Localization in the form of "en-US"	
CypherText	Encrypted string representing the authentication information. The cyphertext value can be used to replace the UserID and SessionID parameters.	Session

<EgovRequest xmlns="http://malta.government.com/eid/">
  <SessionID>string</SessionID>
  <UserID>string</UserID>
  <CertificateSerial>string</CertificateSerial>
  <AppKey>string</AppKey>
  <Locale>string</Locale>
  <CypherText>string</CypherText>
</EgovRequest>

05.2.2   EgovResponseHeader

The response header is returned in all the web service responses to maintain session state and to report any errors encountered during web service execution.

The UserID, SessionID are always returned if the request header is successfully validated.   The AuthenicationLevel will indicate what method was used by the user to authenticate against the eID.

The CypherText value will only be returned if it was originally passed as a parameter in the request header.

The ErrorCode and ErrorString nodes will always be present but will be empty if no errors are encountered. After each call to a web service the user should check the contents of the ErrorCode to check if the web service call was successful.

Element	Description	Type
SessionID	UUID of citizen returned after login	Session
UserID	UUID of session returned after login	Session
ErrorCode	Error code returned by the system	Error
ErrorString	Error message returned by the system	Error
Locale	Localization in the form of "en-US"	
CypherText	Encrypted string representing the authentication information	Session
AuthenticationLevel	The authentication method used by the user to authenticate with the eID. Level 0 – no authentication Level 1 – username and password Level 2 – username, password and digital certificate	Session

```
<EgovResponse xmlns="http://malta.government.com/eid/">
  <SessionID>string</SessionID>
  <UserID>string</UserID>
  <ErrorCode>string</ErrorCode>
  <ErrorString>string</ErrorString>
  <Locale>string</Locale>
  <CypherText>string</CypherText>
  <AuthenticationLevel>integer</AuthenticationLevel>
</EgovResponse>
```

05.2.3   EgovHeaderExtension

The extension is used to determine what authentication check will be performed before each web service is executed. Parties calling a web service must check what type of header is expected before consuming such service. The type of header will indicate what information should be included in the soap header before calling the web service. Below is a table showing the various options that can be used.

HeaderType	Description
HEADERREQUIRED	This is the basic header type and is used to check that a soap header of type EgovRequestHeader is submitted with the request. The header can be submitted as empty.
CHECKSESSION	This header type will check that a user has already logged in and will check that the soap header of type EgovRequestHeader contains a valid UserID and SessionID or CypherText.

05.2.3.1 Soap Header Error Codes

This table shows the error code that can be returned by soap extension for all web services. The description is not the error description returned but an explanation of why the error occurred.

Error Code	Description
5201	The user session is invalid.
5202	The userid does not have the correct format.
5203	The userid is required.
5212	The sessionid is required.
5213	A soap header of type EgovRequestHeader is required.
5214	An invalid soap header was passed.
5215	The sessionid does not have the correct format.
5228	The EgovRequestHeader does not contain the required audit information.
5233	The application key is invalid or does not represent a valid service provider.

05.3   Authentication

05.3.1   System Logon

Web Service Name : systemlogon.asmx

The web service will create a session for the user and return a valid UserID/SessionID that must be used in subsequent calls to other web services that require the user to be authenticated. The *Username* and *Password* are required for Level 1 authentication. The *CertificateSerial* is required if the user is authenticating using a digital certificate being Level 2.

05.3.1.1 Soap Request

Headers required for the message.

HeaderType	Description	Header Type
EgovRequestHeader		HEADERREQUIRED

Elements used in the request message body.

Element	Description	Required
Username	The user login name	☑
Password	The password of the citizen	☑
CertificateSerial	The serial number of the citizen digital certificate	☐
Profiles	This field must be set to "Citizen"	☑

WSDL document for soap request.

```xml
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>
<EgovRequest xmlns="http://malta.government.com/eid/">
  <SessionID>string</SessionID>
  <UserID>string</UserID>
  <CertificateSerial>string</CertificateSerial>
  <AppKey>string</AppKey>
  <Locale>string</Locale>
  <CypherText>string</CypherText>
</EgovRequest>
</soap:Header>
<soap:Body>
<SystemLogon xmlns="http://egov.malta.com/eid">
  <userName>string</userName>
  <password>string</password>
  <certificateserial>string</certificateserial>
  <profiles>string[]</profiles>
</SystemLogon>
</soap:Body>
</soap:Envelope>
```

05.3.1.2 Soap Response

Headers returned by the message.

HeaderType	Description	Header Info
EGovResponseHeader		Session
		Error

Elements returned by the request message body.

Element	Description
SystemLogonResult	Boolean value indicating the result of the request.

WSDL document for soap response.

<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>

<EgovResponse xmlns="http://malta.government.com/eid/">
 <SessionID>string</SessionID>
 <UserID>string</UserID>
 <ErrorCode>string</ErrorCode>
 <ErrorString>string</ErrorString>
 <Locale>string</Locale>
 <CypherText>string</CypherText>
 <AuthenticationLevel>integer</AuthenticationLevel>
</EgovResponse>
</soap:Header>
<soap:Body>
<SystemLogonResponse xmlns="http://egov.malta.com/eid">
 <SystemLogonResult>boolean</SystemLogonResult>
</SystemLogonResponse>
</soap:Body>
</soap:Envelope>

05.3.1.3 Error Codes

This table shows the error code that can be returned by the web service. The description is not the error description returned but an explanation of why the error occurred.

Error Code	Description
1311	No logon servers were available to authenticate the user.
1326	An error occurred during authentication.
1327	The user account has some restrictions restriction. Possible reasons are blank passwords not allowed, login hour restrictions, or a policy restriction has been enforced.
1328	Authentication is being performed outside the allowed time restriction.
1329	Authentication is not allowed from the computer.
1330	The password for the account has expired.

1331	The account has not yet been enabled.
1380	The requested login has not been granted at this computer.
1385	The requested login type has not been granted at this computer.
1793	The account has expired.
1907	The password must be changed before the user is allowed to authenticate.
5101	The user name was not submitted and is required.
5102	The password was not submitted and is required.
5104	The Personal Identification Number is required.
5108	The account has been approved, but has not yet been activated.
5405	The user does not hold the "Citizen" profile passed in the profiles array.
7012	The certificate serial submitted belongs to an invalid certificate or the revocation status of the certificate could not be verified.
7013	The certificate serial submitted does not belong to the user being authenticated.
7019	The certificate serial submitted could not be found in the eID system. The certificate might have been issued by a different CA.
7022	The certificate serial submitted does not have the required key usage to be used by a "Citizen".
9000	A runtime exception has occurred.
20101	The request for the certificate has not been completed.
20102	The request for the certificate has failed.
20103	The certificate has been revoked.
20105	The certificate was never been issued by the Certification Authority.
20106	The certificate is still pending approval and has not yet been issued.
20107	The certificate has an invalid disposition code.
20108	The certificate is not yet valid.
20109	The certificate has expired.
20112	The certificate could not be verified by the Certification Authority.

05.3.2   System Logoff

Web Service Name : systemlogoff.asmx

The web service will remove the session for the citizen. The session will be removed and the citizen will need to authenticate again to make use of the eGovernment Framework.

05.3.2.1 Soap Request

Headers required for the message.

HeaderType	Description	Header Type
EGovRequestHeader		CHECKSESSION

Elements used in the request message body.

Element	Description	Required

WSDL document for soap request.

<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>
<EgovRequest xmlns="http://malta.government.com/eid/">
  <SessionID>string</SessionID>
  <UserID>string</UserID>
  <CertificateSerial>string</CertificateSerial>
  <AppKey>string</AppKey>
  <Locale>string</Locale>
  <CypherText>string</CypherText>
</EgovRequest>
</soap:Header>
<soap:Body>
  <SystemLogoff xmlns="http://egov.malta.com/eid" />
</soap:Body>
</soap:Envelope>

05.3.2.2 Soap Response

Headers returned by the message.

HeaderType	Description	Header Info
EGovResponseHeader		Error

Elements returned by the request message body.

Element	Description
SystemLogoffResult	Boolean value indicating the result of the request.

WSDL document for soap response.

<?xml version="1.0" encoding="utf-8" ?>

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">

```
<soap:Header>

<EgovResponse xmlns="http://malta.government.com/eid/">
  <SessionID>string</SessionID>
  <UserID>string</UserID>
  <ErrorCode>string</ErrorCode>
  <ErrorString>string</ErrorString>
  <Locale>string</Locale>
  <CypherText>string</CypherText>
  <AuthenticationLevel>integer</AuthenticationLevel>
</EgovResponse>
</soap:Header>
<soap:Body>
<SystemLogoffResponse xmlns="http://egov.malta.com/eid">
  <SystemLogoffResult>boolean</SystemLogoffResult>
</SystemLogoffResponse>
</soap:Body>
</soap:Envelope>
```

05.3.2.3 Error Codes

This table shows the error code that can be returned by the web service. The description is not the error description returned but an explanation of why the error occurred.

Error Code	Description
5206	The session could not be removed.
5702	A user matching the given userid was not found.
9000	A runtime exception has occurred.

05.3.3   Check Valid Session

Web Service Name : checkvalidsession.asmx

The web service will verify that the session information passed to the web service is still valid and that the eCitizen still has an active session. If the session information is valid the existing eID session will be renewed and extended by the configured timeout period.

05.3.3.1 Soap Request

Headers required for the message.

HeaderType	Description	Header Type
EGovRequestHeader		CHECKSESSION

Elements used in the request message body.

Element	Description	Required

WSDL document for soap request.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>
<EgovRequest xmlns="http://malta.government.com/eid/">
  <SessionID>string</SessionID>
  <UserID>string</UserID>
  <CertificateSerial>string</CertificateSerial>
  <AppKey>string</AppKey>
  <Locale>string</Locale>
  <CypherText>string</CypherText>
</EgovRequest>
</soap:Header>
<soap:Body>
  <CheckValidSession xmlns="http://egov.malta.com/eid" />
</soap:Body>
</soap:Envelope>
```

05.3.3.2 Soap Response

Headers returned by the message.

HeaderType	Description	Header Info
EGovResponseHeader		Session Error

Elements returned by the request message body.

Element	Description
CheckValidSessionResult	Boolean value indicating whether the session is still valid or not.

WSDL document for soap response.

```
<?xml version="1.0" encoding="utf-8" ?>
```

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>

<EgovResponse xmlns="http://malta.government.com/eid/">
  <SessionID>string</SessionID>
  <UserID>string</UserID>
  <ErrorCode>string</ErrorCode>
  <ErrorString>string</ErrorString>
  <Locale>string</Locale>
  <CypherText>string</CypherText>
  <AuthenticationLevel>integer</AuthenticationLevel>
</EgovResponse>
</soap:Header>
<soap:Body>
<CheckValidSessionResponse xmlns="http://egov.malta.com/eid">
  <CheckValidSessionResult>boolean</CheckValidSessionResult>
</CheckValidSessionResponse>
</soap:Body>
</soap:Envelope>
```

05.3.3.3 Error Codes

This table shows the error code that can be returned by the web service. The description is not the error description returned but an explanation of why the error occurred.

Error Code	Description
9000	A runtime exception has occurred.

The check valid session does not return any errors in addition to those returned by the Soap Headers section.

05.4   eServices Web Services

05.4.1   Get Entity Type

Web Service Name : getentitytype.asmx

The web service will return the entity associated with a particular ID. The entity type can be either an eCitizen or Organisation.

05.4.1.1 Soap Request

Headers required for the message.

HeaderType	Description	Header Type
EGovRequestHeader		CHECKSESSION

Elements used in the request message body.

Element	Description	Required
EntityID	The UUID of the entity whose type is required.	☑

WSDL document for soap request.

```xml
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>
<EgovRequest xmlns="http://malta.government.com/eid/">
 <SessionID>string</SessionID>
 <UserID>string</UserID>
 <CertificateSerial>string</CertificateSerial>
 <AppKey>string</AppKey>
 <Locale>string</Locale>
 <CypherText>string</CypherText>
</EgovRequest>
</soap:Header>
<soap:Body>
<GetEntityType xmlns="http://egov.malta.com/eid">
 <egovContainer>
   <EntityID>string</EntityID>
 </egovContainer>
</GetEntityType>
</soap:Body>
</soap:Envelope>
```

05.4.1.2 Soap Response

Headers returned by the message.

HeaderType	Description	Header Info
EGovResponseHeader		Session
		Error

Elements returned by the request message body.

> **Note**: Only the elements declared in the table below must be used from the web service response. Other elements returned by the web service form part of the complete schema but must not be used by 3rd party integrators

Element	Description
EntityType	The entity associated with the given UUID. The entity can be either an eCitizen or Organisation.

WSDL document for soap response.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>

<EgovResponse xmlns="http://malta.government.com/eid/">
 <SessionID>string</SessionID>
 <UserID>string</UserID>
 <ErrorCode>string</ErrorCode>
 <ErrorString>string</ErrorString>
 <Locale>string</Locale>
 <CypherText>string</CypherText>
 <AuthenticationLevel>integer</AuthenticationLevel>
</EgovResponse>
</soap:Header>
<soap:Body>
<GetEntityTypeResponse xmlns="http://egov.malta.com/eid">
 <GetEntityTypeResult>
  <EntityType>string</EntityType>
 </GetEntityTypeResult>
</GetEntityTypeResponse>
</soap:Body>
</soap:Envelope>
```

05.4.1.3 Error Codes

This table shows the error code that can be returned by the web service. The description is not the error description returned but an explanation of why the error occurred.

Error Code	Description
5704	An entity matching the given entityid could not be found.
9000	A runtime exception has occurred.

05.4.2   Get eService

Web Service Name : geteservice.asmx

The web service will return the eservice information held by the eID.

05.4.2.1 Soap Request

Headers required for the message.

HeaderType	Description	Header Type
EGovRequestHeader		CHECKSESSION

Elements used in the request message body. The web service will required either of the parameters defined below to return the information related to the eService.

Element	Description	Required
EServiceID	The UUID of the eService.	
EServiceKey	The key assigned to the eService	

WSDL document for soap request.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>
<EgovRequest xmlns="http://malta.government.com/eid/">
  <SessionID>string</SessionID>
  <UserID>string</UserID>
  <CertificateSerial>string</CertificateSerial>
  <AppKey>string</AppKey>
  <Locale>string</Locale>
  <CypherText>string</CypherText>
</EgovRequest>
</soap:Header>
<soap:Body>
  <GetEService xmlns="http://egov.malta.com/eid">
   <egovContainer>
    <EServiceID>string</EServiceID>
    <EServiceKey>string</EServiceKey>
   </egovContainer>
  </GetEService>
</soap:Body>
</soap:Envelope>
```

05.4.2.2 Soap Response

Headers returned by the message.

HeaderType	Description	Header Info
EGovResponseHeader		Session
		Error

Elements returned by the request message body.

Note: Only the elements declared in the table below must be used from the web service response. Other elements returned by the web service form part of the complete schema but must not be used by 3rd party integrators

Element	Description
EServiceProviderID	The UUID of the organisation providing the eService
EServiceProvider	The name of the organisation providing the eService
ServiceName	The name of the eService
ServiceDescription	The description of the eService
EServiceKey	The unique key assigned to the eService
AccessLevel	The authentication level required to access the eService (See Appendix A – Configuration and Parameters - Access Level)
ServiceURL	The URL that will be used when moving from the myGov portal to the service provider web site

WSDL document for soap response.

```xml
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>

<EgovResponse xmlns="http://malta.government.com/eid/">
  <SessionID>string</SessionID>
  <UserID>string</UserID>
  <ErrorCode>string</ErrorCode>
  <ErrorString>string</ErrorString>
  <Locale>string</Locale>
  <CypherText>string</CypherText>
  <AuthenticationLevel>integer</AuthenticationLevel>
</EgovResponse>
</soap:Header>
<soap:Body>
<GetEServiceResponse xmlns="http://egov.malta.com/eid">
  <GetEServiceResult ID="6c6e8ac5-b160-42ca-814b-f943a9903529">
  <EServiceProviderID>string</EServiceProviderID>
  <EServiceProvider>string</EServiceProvider>
  <ServiceName>string</ServiceName>
  <ServiceDescription>string</ServiceDescription>
  <EServiceKey>string</EServiceKey>
```

```
<AccessLevel>int</AccessLevel>
<AccessMode>int</AccessMode>
<SubscribedByDefault>boolean</SubscribedByDefault>
<RequiresApproval>boolean</RequiresApproval>
<CanDelegate>boolean</CanDelegate>
<RequiresDelegationApproval>boolean</RequiresDelegationApproval>
</Status>
<Comments />
</SubscriberID>
</DelegatedBy>
</AssignedBy>
</DelegatedTo>
</AssignedTo>
</DelegationStatus>
</PermanentDelegation>
</DelegationDuration>
</TrustedAgentEnabled>
</DelegationDateFrom>
</DelegationDateTo>
<ServiceURL>string</ServiceURL>
</InUse>
</GetEServiceResult>
</GetEServiceResponse>
</soap:Body>
</soap:Envelope>
```

05.4.2.3 Error Codes

This table shows the error code that can be returned by the web service. The description is not the error description returned but an explanation of why the error occurred.

Error Code	Description
5209	The Service ID has an invalid format.
5231	The eService Key is invalid.
5701	An eService matching the eService ID or eService Key was not found
9000	A runtime exception has occurred.

05.4.3   Get Entity eServices

Web Service Name : getentityeservices.asmx

The web service will retrieve a list of eServices (Subscribed / Assigned / Delegated) to a particular eCitizen.

05.4.3.1 Soap Request

Headers required for the message.

HeaderType	Description	Header Type
EGovRequestHeader		CHECKSESSION

Elements used in the request message body.

Element	Description	Required
OwnerID	The UUID of the entity whose eServices are required. The entity will always be an eCitizen UUID. For additional information refer to section Additional Information to display eServices on Page 24	☑
EServiceRelation	The relationship established between the eCitizen and the eService. (See Appendix A – Configuration and Parameters - Eservice Relation)	☑

WSDL document for soap request.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>
<EgovRequest xmlns="http://malta.government.com/eid/">
 <SessionID>string</SessionID>
 <UserID>string</UserID>
 <CertificateSerial>string</CertificateSerial>
 <AppKey>string</AppKey>
 <Locale>string</Locale>
 <CypherText>string</CypherText>
</EgovRequest>
</soap:Header>
<soap:Body>
<GetEntityEServices xmlns="http://egov.malta.com/eid">
 <egovContainer>
  <OwnerID></OwnerID>
  <EServiceRelation></EServiceRelation>
 </egovContainer>
</GetEntityEServices>
</soap:Body>
</soap:Envelope>
```

05.4.3.2 Soap Response

Headers returned by the message.

HeaderType	Description	Header Info
EGovResponseHeader		Session
		Error

Elements returned by the request message body.

Note: Only the elements declared in the table below must be used from the web service response. Other elements returned by the web service form part of the complete schema but must not be used by 3rd party integrators

Element	Description
EntityEService	Element will contain the information for each eService that has been subscribed for by the eCitizen or assigned, delegated to the Citizen.
UUID	The UUID assigned to the eService.
OrganisationID	The UUID assigned to the Service Provider organisation.
Organisation	The name of the Service Provider.
Name	The name of the eService.
URL	Configured URL for the eService.
Description	Description of the eService.
EServiceKey	The unique key assigned to the eService by the Service Provider
AccessLevel	The authentication level required to access the eService (See Appendix A – Configuration and Parameters - Access Level)
Status	The current subscription status of the eService (See Appendix A – Configuration and Parameters - eService Status)
SubscriberID	The UUID of the entity that subscribed for the eService

WSDL document for soap response.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>

<EgovResponse xmlns="http://malta.government.com/eid/">
 <SessionID>string</SessionID>
 <UserID>string</UserID>
 <ErrorCode>string</ErrorCode>
 <ErrorString>string</ErrorString>
 <Locale>string</Locale>
 <CypherText>string</CypherText>
 <AuthenticationLevel>integer</AuthenticationLevel>
</EgovResponse>
</soap:Header>
```

```
<soap:Body>
<GetEntityEServicesResponse xmlns="http://egov.malta.com/eid">
 <GetEntityEServicesResult>
  <EntityEServices xmlns="">
  <EntityEService>
  <UUID>string</UUID>
  <ORGANISATIONID>string</ORGANISATIONID>
  <ORGANISATION>string</ORGANISATION>
  <Name>string</Name>
  <URL>string</URL>
  <Description>string</Description>
  <AccessLevel>integer</AccessLevel>
  <SubscribedByDefault>boolean</SubscribedByDefault>
  <RequiresApproval>boolean</RequiresApproval>
  <CanDelegate>boolean</CanDelegate>
  <RequiresDelegationApproval>boolean</RequiresDelegationApproval>
  <Locale>integer</Locale>
  <CreatorID />
  <OwnerID />
  <StatusID>string</StatusID>
  <Comments />
  <SubscriberID>string</SubscriberID>
  <AssignedToID />
  <DelegatedToID />
  <AssignedByID />
  <DelegatedByID />
  <DelegationStatusID />
  <AccessMode>integer</AccessMode>
  <LastModified />
  <Status>string</Status>
  <DelegationStatus />
  </EntityEService>
  </EntityEServices>
 </GetEntityEServicesResult>
 </GetEntityEServicesResponse>
</soap:Body>
</soap:Envelope>
```

05.4.3.3 Error Codes

This table shows the error code that can be returned by the web service. The description is not the error description returned but an explanation of why the error occurred.

Error Code	Description
5219	The eservice relation is invalid.
5223	The entityid does not have the correct format.
5704	An entity matching the given entityid could not be found.
9000	A runtime exception has occurred.

05.4.4   Get User eService Extended

Web Service Name: getusereserviceex.asmx

The web service will retrieve all the information and attributes for an eService that has been subscribed for by an eCitizen, or that has been delegated or assigned to an eCitizen.

05.4.4.1 Soap Request

Headers required for the message.

HeaderType	Description	Header Type
EGovRequestHeader		CHECKSESSION

Elements used in the request message body.

Element	Description	Required
EServiceID	The UUID of the eService subscribed for by the eCitizen.	☑
UserID	The UUID of the eCitizen who is related to the eService.	☑
EServiceRelation	The relationship established between the eCitizen and the eService. (See Appendix A – Configuration and Parameters - Eservice Relation)	☑

WSDL document for soap request.

<?xml version="1.0" encoding="utf-8" ?>

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">

<soap:Header>

<EgovRequest xmlns="http://malta.government.com/eid/">

  <SessionID>string</SessionID>

  <UserID>string</UserID>

  <CertificateSerial>string</CertificateSerial>

  <AppKey>string</AppKey>

  <Locale>string</Locale>

  <CypherText>string</CypherText>

</EgovRequest>

</soap:Header>

<soap:Body>

<GetUserEServiceEx xmlns="http://egov.malta.com/eid">

  <egovContainer>

   <EServiceID>string</EServiceID>

   <UserID>string</UserID>

   <EServiceRelation>string</EServiceRelation>

  </egovContainer>

</GetUserEServiceEx>

</soap:Body>

</soap:Envelope>

05.4.4.2 Soap Response

Headers returned by the message.

HeaderType	Description	Header Info
EGovResponseHeader		Session
		Error

Elements returned by the request message body.

Note: Only the elements declared in the table below must be used from the web service response. Other elements returned by the web service form part of the complete schema but must not be used by 3rd party integrators

Element	Description
EServiceProviderID	The UUID assigned to the Service Provider organisation.
EServiceProvider	The name of the Service Provider organisation.
ServiceName	The name of the eService.
ServiceDescription	The description of the eService.
AccessLevel	The authentication level required to access the eService (See Appendix A – Configuration and Parameters - Access Level)
SubscriberID	The UUID of the eCitizen that subscribed for the eService
DelegatedBy	The UUID of the eCitizen that delegated the eService.
AssignedBy	The UUID of the Organisation that assigned the eService.
DelegatedTo	The UUID of the eCitizen that has been delegated the eService.
AssignedTo	The UUID of the eCitizen or Group that has been assigned the eService.
DelegationStatus	The current status of the delegation. Applicable only if the **EServiceRelation** has been set to **Delegated**. (See Appendix A – Configuration and Parameters - Delegation Status)
OwnerAttributes	List of the attributes belonging to the owner for the eService. The element will contain an iteration of the <OwnerAttribute> element representing each attribute held by the owner for the eService. The following list shows who owns the attributes depending on the EServiceRelation Subscribed – the attributes belong to the eCitizen that subscribed for the eService. Delegated - the attributes belong to the eCitizen that subscribed for and then delegated the eService. Assigned – the attributes belong to the Organisation that subscribed for and then assigned the eService. AgentDelegated – attributes not implemented
AttributeOwnerID	The UUID of the eCitizen who owns the attributes.
AttributeName	The name of the attribute.

AttributeValue	The value defined by the owner when subscribed for the eService.
Mandatory	Flag to determine if the attribute is mandatory when subscribing for the eService.

WSDL document for soap response.

<?xml version="1.0" encoding="utf-8" ?>

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">

<soap:Header>

<EgovResponse xmlns="http://malta.government.com/eid/">
 <SessionID>string</SessionID>
 <UserID>string</UserID>
 <ErrorCode>string</ErrorCode>
 <ErrorString>string</ErrorString>
 <Locale>string</Locale>
 <CypherText>string</CypherText>
 <AuthenticationLevel>integer</AuthenticationLevel>
</EgovResponse>
</soap:Header>
<soap:Body>
<GetUserEServiceExResponse xmlns="http://egov.malta.com/eid">
 <GetUserEServiceExResult>
  <EService xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="string" xmlns="">
  <EServiceProviderID>string</EServiceProviderID>
  <EServiceProvider>string</EServiceProvider>
  <ServiceName>string</ServiceName>
  <ServiceDescription>string</ServiceDescription>
  <AccessLevel>integer</AccessLevel>
  <AccessMode>integer</AccessMode>
  <SubscribedByDefault>boolean</SubscribedByDefault>
  <RequiresApproval>boolean</RequiresApproval>
  <CanDelegate>boolean</CanDelegate>
  <RequiresDelegationApproval>boolean</RequiresDelegationApproval>
  <Status>Active</Status>
  <Comments />
  <SubscriberID>string</SubscriberID>
  <DelegatedBy>string</DelegatedBy>
  <AssignedBy>string</AssignedBy>
  <DelegatedTo>string</DelegatedTo>
  <AssignedTo>string</AssignedTo>
  <DelegationStatus>string</DelegationStatus>
  <ServiceURL>string</ServiceURL>
  <InUse>boolean</InUse>
  <Attributes>
   <Attribute>
    <AttributeOwnerID />

```
    <DefinitionID />
    <AttributeName />
    <AttributeValue />
    <CreatorID />
    <OwnerID />
  </Attribute>
 </Attributes>
 <EServiceAttributeDefinitions>
  <EServiceAttributeDefinition>
   <UUID>string</UUID>
   <AttributeName>string</AttributeName>
   <Mandatory>boolean</Mandatory>
   <Locale />
   <CreatorID />
   <OwnerID />
  </EServiceAttributeDefinition>
 </EServiceAttributeDefinitions>
 <OwnerAttributes>
  <OwnerAttribute>
   <AttributeOwnerID>string</AttributeOwnerID>
      <DefinitionID>string</DefinitionID>
      <AttributeName>string</AttributeName>
      <AttributeValue>string</AttributeValue>
      <Mandatory>boolean</Mandatory>
      <CreatorID />
      <OwnerID />
  </OwnerAttribute>
 </OwnerAttributes>
 </EService>
 </GetUserEServiceExResult>
</GetUserEServiceExResponse>
</soap:Body>
</soap:Envelope>
```

05.4.4.3 Error Codes

This table shows the error code that can be returned by the web service. The description is not the error description returned but an explanation of why the error occurred.

Error Code	Description
5202	The userid does not have the correct format.
5209	The eserviceid does not have the correct format.
5219	The eservice relation is invalid.
5224	The subscriberid does not have the correct format.
5701	An eservice matching the given eserviceid could not be found.
5702	A user matching the given userid could not be found.
9000	A runtime exception has occurred.

05.4.5   Get Organisation eService Extended

Web Service Name: getorganisationeserviceex.asmx
The web service will retrieve all the information and attributes for an eService that has been subscribed for by an Organisation or that has been delegated to an Organisation.

05.4.5.1 Soap Request

Headers required for the message.

HeaderType	Description	Header Type
EGovRequestHeader		CHECKSESSION

Elements used in the request message body.

Element	Description	Required
EServiceID	The UUID of the eService subscribed for by the Organisation.	☑
OrganisationID	The UUID of the Organisation that is related to the eService.	☑
EServiceRelation	The relationship established between the eCitizen and the eService. (See Appendix A – Configuration and Parameters - Eservice Relation)	☑

WSDL document for soap request.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>
<EgovRequest xmlns="http://malta.government.com/eid/">
  <SessionID>string</SessionID>
  <UserID>string</UserID>
  <CertificateSerial>string</CertificateSerial>
  <AppKey>string</AppKey>
  <Locale>string</Locale>
  <CypherText>string</CypherText>
</EgovRequest>
</soap:Header>
<soap:Body>
<GetOrganisationEServiceEx xmlns="http://egov.malta.com/eid">
  <egovContainer>
   <EServiceID>string</EServiceID>
   <OrganisationID>string</OrganisationID >
   <EServiceRelation>string</EServiceRelation>
  </egovContainer>
</GetOrganisationEServiceEx>
</soap:Body>
</soap:Envelope>
```

05.4.5.2 Soap Response

Headers returned by the message.

HeaderType	Description	Header Info
EGovResponseHeader		Session
		Error

Elements returned by the request message body.

Element	Description
EServiceProviderID	The UUID assigned to the Service Provider organisation.
EServiceProvider	The name of the Service Provider organisation.
ServiceName	The name of the eService.
ServiceDescription	The description of the eService.
AccessLevel	The authentication level required to access the eService (See Appendix A – Configuration and Parameters - Access Level)
SubscriberID	The UUID of the eCitizen or Organisation that subscribed for the eService
DelegatedBy	The UUID of the eCitizen or Organisation that delegated the eService.
AssignedBy	The UUID of the Organisation that assigned the eService
DelegatedTo	The UUID of the eCitizen or Organisation that has been delegated the eService.
AssignedTo	The UUID of the eCitizen that has been assigned the eService.
DelegationStatus	The current status of the delegation. Applicable only if the **EServiceRelation** has been set to **Delegated**. (See Appendix A – Configuration and Parameters -
	Delegation Status)
InUse	Flag showing whether the eService is currently active.
OwnerAttributes	List of the attributes belonging to the owner for the eService. The element will contain an iteration of the <OwnerAttribute> element representing each attribute held by the owner for the eService. The following list shows who owns the attributes depending on the EServiceRelation Subscribed – the attributes belong to the eCitizen or Organisation that subscribed for the eService. Delegated - the attributes belong to the eCitizen or Organisation that subscribed for and then delegated the eService. Assigned - the attributes belong to the Organisation that subscribed for and then assigned the eService.
AttributeOwnerID	The UUID of the eCitizen or Organisation who owns the attributes.
AttributeName	The name of the attribute.
AttributeValue	The value defined by the owner when subscribing for the eService.

Mandatory	Flag to determine if the attribute is mandatory when subscribing for the eService.

WSDL document for soap response.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>

<EgovResponse xmlns="http://malta.government.com/eid/">
  <SessionID>string</SessionID>
  <UserID>string</UserID>
  <ErrorCode>string</ErrorCode>
  <ErrorString>string</ErrorString>
  <Locale>string</Locale>
  <CypherText>string</CypherText>
  <AuthenticationLevel>integer</AuthenticationLevel>
</EgovResponse>
</soap:Header>
<soap:Body>
<GetOrganisationEServiceExResponse xmlns="http://egov.malta.com/eid">
  <GetOrganisationEServiceExResult>
   <EService xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="string" xmlns="">
   <EServiceProviderID>string</EServiceProviderID>
   <EServiceProvider>string</EServiceProvider>
   <ServiceName>string</ServiceName>
   <ServiceDescription>string</ServiceDescription>
   <AccessLevel>integer</AccessLevel>
   <AccessMode>integer</AccessMode>
   <SubscribedByDefault>boolean</SubscribedByDefault>
   <RequiresApproval>boolean</RequiresApproval>
   <CanDelegate>boolean</CanDelegate>
   <RequiresDelegationApproval>boolean</RequiresDelegationApproval>
   <Status>Active</Status>
   <Comments />
   <SubscriberID>string</SubscriberID>
   <DelegatedBy>string</DelegatedBy>
   <AssignedBy>string</AssignedBy>
   <DelegatedTo>string</DelegatedTo>
   <AssignedTo>string</AssignedTo>
   <DelegationStatus>string</DelegationStatus>
   <ServiceURL> string </ServiceURL>
   <InUse>boolean</InUse>
   <Attributes>
    <Attribute>
    <AttributeOwnerID />
    <DefinitionID />
```

```
      <AttributeName />
      <AttributeValue />
      <CreatorID />
      <OwnerID />
    </Attribute>
  </Attributes>
  <EServiceAttributeDefinitions>
   <EServiceAttributeDefinition>
    <UUID>string</UUID>
    <AttributeName>string</AttributeName>
    <Mandatory>boolean</Mandatory>
    <Locale />
    <CreatorID />
    <OwnerID />
   </EServiceAttributeDefinition>
  </EServiceAttributeDefinitions>
  <OwnerAttributes>
   <OwnerAttribute>
    <AttributeOwnerID>string</AttributeOwnerID>
        <DefinitionID>string</DefinitionID>
        <AttributeName>string</AttributeName>
        <AttributeValue>string</AttributeValue>
        <Mandatory>boolean</Mandatory>
        <CreatorID />
        <OwnerID />
   </OwnerAttribute>
  </OwnerAttributes>
  </EService>
 </GetOrganisationEServiceExResult>
</GetOrganisationEServiceExResponse>
</soap:Body>
</soap:Envelope>
```

05.4.5.3 Error Codes

This table shows the error code that can be returned by the web service. The description is not the error description returned but an explanation of why the error occurred.

Error Code	Description
5209	The eserviceid does not have the correct format.
5211	The organisationid does not have the correct format.
5219	The eservice relation is invalid.
5224	The subscriberid does not have the correct format.
5701	An eservice matching the given eserviceid could not be found.
5703	An organisation matching the given organisationid could not be found.
9000	A runtime exception has occurred.

05.5   Profile Web Services

05.5.1   Get Citizen

Web Service Name: getcitizen.asmx
The web service will retrieve all the profile information for a citizen.

05.5.1.1 Soap Request

Headers required for the message.

HeaderType	Description	Header Type
EGovRequestHeader		CHECKSESSION

Elements used in the request message body.

Element	Description	Required
CitizenID	The UUID of the required eCitizen	☐
IDNo	The identity card number of the required eCitizen	☐
DateOfBirth	The date of birth of the required eCitizen	☐

Note: The DateofBirth must always be used in conjunction with the IDNo.

WSDL document for soap request.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>
<EgovRequest xmlns="http://malta.government.com/eid/">
 <SessionID>string</SessionID>
 <UserID>string</UserID>
 <CertificateSerial>string</CertificateSerial>
 <AppKey>string</AppKey>
 <Locale>string</Locale>
 <CypherText>string</CypherText>
</EgovRequest>
</soap:Header>
<soap:Body>
<GetCitizen xmlns="http://egov.malta.com/eid">
 <egovContainer>
  <CitizenID>string</CitizenID>
  <IDNo>string</IDNo>
  <DateOfBirth>date</DateOfBirth>
 </egovContainer>
</GetCitizen>
</soap:Body>
</soap:Envelope>
```

05.5.1.2 Soap Response

Headers returned by the message.

HeaderType	Description	Header Info
EGovResponseHeader		Session
		Error

Elements returned by the request message body.

> **Note**: Only the elements declared in the table below must be used from the web service response. Other elements returned by the web service form part of the complete schema but must not be used by 3rd party integrators

Element	Description
ID	The UUID of the eID eCitizen record.
IDCardNo	The identity card number of the eCitizen.
TitleID	The CDR primary key corresponding to the *Title* value.
Title	The title of the eCitizen.
Name	The first name of the eCitizen.
MiddleName	The middle name of the eCitizen.
MaidenName	The maiden name of the eCitizen.
Surname	The surname of the eCitizen.
FullName	Concatenation of *Title*, *Name*, *MiddleName* and *Surname* of the eCitizen.
DoorNumber	The door number of the eCitizen address.
HouseName	The house name of the eCitizen address.
Street	The street name of the eCitizen address.
PostalCodeID	The CDR primary key corresponding to the *PostalCode* value.
PostalCode	The post code of the eCitizen address.
LocalityID	The CDR primary key corresponding to the *Locality* value.
Locality	The locality name of the eCitizen address.
County	The county of the eCitizen address.
Country	The country of the eCitizen address.
TelNo	The telephone number of the eCitizen.
FaxNo	The fax number of the eCitizen.
MobileNo	The mobile number of the eCitizen.
Email	The email address of the eCitizen.
Gender	The gender of the eCitizen.
GenderID	The CDR primary key corresponding to the *Gender* value.
DateOfBirth	The date of birth of the eCitizen
Photo	Image of the eCitizen encoded as a base64 string

WSDL document for soap response.

```xml
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>

<EgovResponse xmlns="http://malta.government.com/eid/">
  <SessionID>string</SessionID>
  <UserID>string</UserID>
  <ErrorCode>string</ErrorCode>
  <ErrorString>string</ErrorString>
  <Locale>string</Locale>
  <CypherText>string</CypherText>
  <AuthenticationLevel>integer</AuthenticationLevel>
</EgovResponse>
</soap:Header>
<soap:Body>
<GetCitizenResponse xmlns="http://egov.malta.com/eid">
  <GetCitizenResult>
  <ID>string</ID>
  <IDCardNo>string</IDCardNo>
  <TitleID>integer</TitleID>
  <Title>string</Title>
  <Name>string</Name>
  <MiddleName />
  <MaidenName />
  <Surname>string</Surname>
  <FullName>string</FullName>
  <Login />
  <DoorNumber>string</DoorNumber>
  <HouseName>Aslan</HouseName>
  <Street>string</Street>
  <PostalCodeID>integer</PostalCodeID>
  <PostalCode>string</PostalCode>
  <LocalityID>integer</LocalityID>
  <Locality>string</Locality>
  <County />
  <Country>string</Country>
  <TelNo>string</TelNo>
  <FaxNo />
  <MobileNo>string</MobileNo>
  <Email>string</Email>
  <SocialSecurityNo />
  <KnownAs />
  <DateOfBirth />
  <CreatedDate />
  <PassportNo />
```

<GenderID>integer</GenderID>
<Gender>string</Gender>
<MaritalStatusID />
<MaritalStatus />
<UseMainAddress>boolean</UseMainAddress>
<AlternativeDoorNumber />
<AlternativeHouseName />
<AlternativeStreet />
<AlternativePostalCodeID />
<AlternativePostalCode />
<AlternativeLocalityID />
<AlternativeLocality />
<AlternativeCounty />
<AlternativeCountry />
<IsAccountLockedOut>boolean</IsAccountLockedOut>
<UserComments />
<RegistrationComments />
<AdministrationComments />
<AccountStatus>string</AccountStatus>
<ReviewDate>datetime</ReviewDate>
<IsDueForReview>boolean</IsDueForReview>
<Photo>base64string</Photo>
<SecretQuestion />
<SecretQuestionCode>integer</SecretQuestionCode>
<SecretPassPhrase />
<Certificates />
<Roles>string</Roles>
</GetCitizenResult>
</GetCitizenResponse>
</soap:Body>
</soap:Envelope>

05.5.1.3 Error Codes

This table shows the error code that can be returned by the web service. The description is not the error description returned but an explanation of why the error occurred.

Error Code	Description
5209	The eserviceid does not have the correct format.
5219	The eservice relation is invalid.
5224	The subscriberid does not have the correct format.
5701	An eservice matching the given eserviceid could not be found.
9000	A runtime exception has occurred.

05.5.2   Get Organisation

Web Service Name: getorganisation.asmx
The web service will retrieve all the profile information for an organisation.

05.5.2.1 Soap Request

Headers required for the message.

HeaderType	Description	Header Type
EGovRequestHeader		CHECKSESSION

Elements used in the request message body.

Element	Description	Required
OrganisationID	The UUID of the required organisation.	☐
OrganisationKey	The organisation key of the required organisation.	☐
OrganisationRegNo	The company registration number of the required organisation.	☐

WSDL document for soap request.

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>
<EgovRequest xmlns="http://malta.government.com/eid/">
 <SessionID>string</SessionID>
 <UserID>string</UserID>
 <CertificateSerial>string</CertificateSerial>
 <AppKey>string</AppKey>
 <Locale>string</Locale>
 <CypherText>string</CypherText>
</EgovRequest>
</soap:Header>
<soap:Body>
<GetOrganisation xmlns="http://egov.malta.com/eid">
 <egovContainer>
 <OrganisationID />
 <OrganisationKey>string</OrganisationKey>
 <OrganisationRegNo>string</OrganisationRegNo>
 </egovContainer>
</GetOrganisation>
</soap:Body>
</soap:Envelope>
```

05.5.2.2 Soap Response

Headers returned by the message.

HeaderType	Description	Header Info
EGovResponseHeader		Session
		Error

Elements returned by the request message body.

Element	Description
Organisation->ID	The UUID of the Organisation record.
Organisation-> IsEServiceProvider	Flag that determines whether the organisation is also a service provider.
Name	The name assigned to the Organisation.
Description	A description assigned to the Organisation.
OrganisationKey	The unique system key used by the eID.
TradeMark	The trademark name of the Organisation.
RegNo	The company registration number of the Organisation.
TelNo	The telephone number of the Organisation.
FaxNo	The fax number of the Organisation.
MobileNo	The mobile number of the Organisation.
Email	The email address of the Organisation.
DoorNo	The door number of the Organisation address.
BuildingName	The building name of the Organisation address.
Street	The street name of the Organisation address.
PostalCodeID	The CDR primary key corresponding to the *PostalCode* value.
PostalCode	The post code of the Organisation address.
LocalityID	The CDR primary key corresponding to the *Locality* value.
Locality	The locality name of the Organisation address.
Status	The current account status of the Organisation.
OrganisationLegalType	The legal type for the Organisation: Notified_RFLP - Organisations Notified with the Registrar for Legal Persons Registered_RFLP - Organisations Registered with the Registrar for Legal Persons Registered_Organisation.- MFSA Registered Organisation
Logo	Image of the Organisation logo encoded as a base64 string.
MainEmployee	Information on the eCitizen representing the organisation manager
ID	The UUID of the eCitizen.
FullName	Concatenation of *Name*, *Surname* and *IDNO* of the eCitizen
Name	The first name of the eCitizen.
Surname	The surname of the eCitizen.
IDNO	The identity card number of the eCitizen.

Login	The login name of the eCitizen.
Email	The email address of the eCitizen.
DOB	The date of birth of the eCitizen.

WSDL document for soap response.

```xml
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Header>

<EgovResponse xmlns="http://malta.government.com/eid/">
  <SessionID>string</SessionID>
  <UserID>string</UserID>
  <ErrorCode>string</ErrorCode>
  <ErrorString>string</ErrorString>
  <Locale>string</Locale>
  <CypherText>string</CypherText>
  <AuthenticationLevel>integer</AuthenticationLevel>
</EgovResponse>
</soap:Header>
<soap:Body>
<GetOrganisationResponse xmlns="http://egov.malta.com/eid">
  <GetOrganisationResult IsEServiceProvider="boolean" ID="string">
  <Name>string</Name>
  <Description />
  <OrganisationKey>string</OrganisationKey>
  <TradeMark />
  <RegNo>string</RegNo>
  <TelNo>string</TelNo>
  <FaxNo />
  <MobileNo />
  <Email>string</Email>
  <DoorNumber />
  <BuildingName>string</BuildingName>
  <Street>string</Street>
  <LocalityID>integer</LocalityID>
  <Locality>string</Locality>
  <PostalCodeID>integer</PostalCodeID>
  <PostalCode>string</PostalCode>
  <County />
  <Country>string</Country>
  <Comments />
  <Status>Active</Status>
  <OrganisationLegalType>None or Notified_RFLP or Registered_RFLP or
Registered_Organisation</OrganisationLegalType>
  <Logo />
  <MainEmployee ID="string">
```

```
   <FullName>string</FullName>
   <Name>string</Name>
   <Surname>string</Surname>
   <IDNO>string</IDNO>
   <Login>string</Login>
   <EMail>string</EMail>
   <DOB>string</DOB>
  </MainEmployee>
  </GetOrganisationResult>
  </GetOrganisationResponse>
</soap:Body>
</soap:Envelope>
```

05.5.2.3 Error Codes

This table shows the error code that can be returned by the web service. The description is not the error description returned but an explanation of why the error occurred.

Error Code	Description
5211	The organisationid does not have the correct format.
5703	An organisation matching the given organisationid could not be found.
9000	A runtime exception has occurred.

06.   Appendix A – Configuration and Parameters

06.1   Web Service Definitions

This section describes the meaning of the definition used throughout the various web service used in this document.

06.1.1   Access Level

The AccessLevel describes the authentication level required to access an eService.   The AccessLevel is determined by the Service Provider when the eService is registered with the eID.

Option	Description
0	Level 0 authentication – no authentication required. If the SubscribedByDefault flag is set to **true** then the eService will be assigned to allow eCitizens
1	Level 1 authentication – username and password
2	Level 2 authentication – digital certificate
3	Not used

06.1.2   Subscribed By Default

The SubscribedbyDefault flag determines whether the eService is assigned to all eCitizens by default. The flag is only available if the **AccessLevel** is set to **0**.   The flag is determined by the Service Provider when the eService is registered with the eID.

Option	Description
False	The eService must be subscribed to. When subscribed for the eService will be approved automatically.
True	The eService is subscribed automatically to all eCitizens that access the eID.

06.1.3   eService Status

The status enumeration describes the current subscription status for an eService.   Access to the eService should only be allowed when the status is set to Active, otherwise the user should be denied access.

Option	Description
Active	The eService has been approved and can be accessed.
Pending Approval	The eService has been requested, but has not yet been approved by the service provider. Access must not be allowed.
Suspended	The eService has been suspended by the service provider. Access must not be allowed.

06.1.4 Delegation Status

The DelegationStatus describes the current status for an eService that has been delegated. Access to the eService should only be allowed when the status is set to Active, otherwise the user should be denied access.

Option	Description
Unavailable	No delegation has been made.
Active	The delegation has been approved by all required parties and can be used.
Pending Service Provider Approval	The delegation request has been submitted by an eCitizen and is awaiting approval by the Service Provider.

06.1.5 Account Status

The status enumeration describes the current account status for an eCitizen. Access to the eCitizen should only be allowed when the status is set to Active, otherwise the user should be denied access.

Option	Description
Pending Approval	The account has been requested, but has not yet been approved by the competent authority. Access must not be allowed.
Pending Account Activation	The account has been requested, but has not yet been activated by the eCitizen. Access must not be allowed.
Pin Required	
Active	The account has been approved and activated by the eCitizen
Suspended	The account has been suspended by the competent authority. Access must not be allowed.
Terminated	The account has been terminated by competent authority. Access must not be allowed.

06.1.6 Eservice Relation

The eServiceRelation enumeration describes how an eCitizen is linked to an eService.

Option	Description
Subscribed	The eCitizen or Organisation has subscribed for the eService.
Delegated	The eService has been delegated to the eCitizen or Organisation.
Assigned	The eService has been assigned to the eCitizen. The **Assigned** option is only available to eCitizens, because eServices can only be assigned by an Organisation to an eCitizen (as employee).
AgentDelegated	The eService has been delegated by a Citizen to a Trusted Agent.

07.   Appendix B – Error Messages

07.1   Error Messages English

Error Code	Description in English
1311	Login failure: There are currently no logon servers available to service the logon request.
1326	Login failure: unknown UserName number or bad password.
1327	Login failure: user account restriction. Possible reasons are blank passwords not allowed, login hour restrictions, or a policy restriction has been enforced.
1328	Login failure: account login time restriction violation.
1329	Login failure: You are not allowed to log in this computer.
1330	Login failure: the specified account password has expired.
1331	Login failure: account not yet enabled. EL: Login failure: account not yet enabled
1380	Login failure: You have not been granted the requested login at this computer.
1385	Login failure: You have not been granted the requested login type at this computer.
1793	This account has expired - please contact Administrator.
1907	You must change your password after your first login to continue using this service.
5101	The user name is required.
5102	The password is required.
5104	The Personal Identification Number (PIN) has to be entered.
5108	The account must be activated. The Personal Identification Number (PIN) has to be entered.
5202	The user name is invalid.
5206	The current session could not be removed.
5209	The Service ID has an invalid format.
5211	The Organisation ID is invalid.
5219	An invalid EServiceRelationship was specified.
5223	The EntityID is invalid.
5224	Suscribtion ID is invalid.
5405	The user does not hold the required profile to access the site.
5701	A service with ID {0} was not found.
5702	A user with ID {0} was not found.
5703	An organisation with ID {0} was not found.
5704	An entity with ID {0} was not found.
7012	The certificate with serial no '{0}' is invalid.
7013	The certificate with serial no '{0}' does not match your login credentials. Select another certificate to login.
7019	The certificate with serial no '{0}' could not be retrieved.

7022	The certificate provided is not valid for the select user profile.
9000	A problem has occurred - please contact Administrator.
20101	The certificate request call was not completed.
20102	The certificate request call failed.
20103	The certificate has been revoked.
20105	The certificate was never issued.
20106	The certificate request is still pending.
20107	An invalid disposition code was returned.
20108	The certificate is not yet valid.
20109	The certificate has expired.
20112	The certificate could not be verified.

07.2   Error Messages Maltese

Error Code	Description in Maltese
1311	Il-login falla: Bħalissa m'hemmx servers disponibbli biex jilqgħu t-talba għal-logon.
1326	In-numru ta' isem l-utent mhux magħruf jew password ħażina.
1327	Il-login falla: restrizzjoni fuq il-kont. Ir-raġunijiet jistgħu jkunu: Ma tistax tħalli passwords vojta, restrizzjonijet fuq is-sigħat tal-login, jew restrizzjoni ta' policy li ġiet infurzata.
1328	Il-login falla: Vjolazzjoni tar-restrizzjoni tal-ħin tal-kont tal-login.
1329	Il-login falla: Ma tistax tilloggja minn fuq dan il-kompjuter.
1330	Il-login falla: skadiet il-password speċifikata tal-kont.
1331	Login failure: account not yet enabled
1380	Il-login falla: Għadek ma ngħatajtx il-login li tlabt għal fuq dan il-kompjuter.
1385	Il-login falla: Għadek ma ngħatajtx it-tip ta' login li tlabt għal fuq dan il-kompjuter.
1793	Dan il-kont skada – jekk jogħġbok ikkuntattja lill-Amministratur.
1907	Għandek tibdel il-password wara li tillogja għall-ewwel darba sabiex tibqa' tuża dan is-servizz.
5101	Isem l-utent hu meħtieġ.
5102	Il-password hija meħtieġa.
5104	Trid iddaħħal il-PIN (Numru ta' l-Identifikazzjoni Personali).
5108	Dan il-kont irid jiġi attivat. Trid iddaħħal il-PIN (In-Numru ta' l-Identifikazzjoni Personali).
5202	Isem l-utent huwa invalidu.
5206	Din is-sessjoni ma setgħetx titneħħa.
5209	
5211	
5219	

5223	
5224	
5405	L-utent m'għandux il-profil meħtieġ biex jidħol f'dan is-sit.
5701	Servizz b'ID {0} ma nstabx.
5702	Utent b'ID {0} ma nstabx.
5703	Organizzazzjoni b'ID {0} ma nstabetx.
5704	Entità b'ID {0} ma nstabetx.
7012	Iċ-ċertifikat bis-serial number '{0}' huwa invalidu.
7013	Iċ-ċertifikat bis-serial number '{0}' ma jaqbilx mal-kredenzjali tal-login tiegħek. Agħżel ċertifikat ieħor biex tilloggja.
7019	Ma setax jinstab iċ-ċertifikat bis-serial number '{0}'.
7022	Iċ-ċertifikat ipprovdut m'huwiex validu għall-profil ta' l-utent partikolari.
9000	Inqalgħet problema – jekk jogħġbok ikkuntattja lill-Amministratur.
20101	
20102	
20103	
20105	
20106	
20107	
20108	
20109	
20112	

08.   Appendix C – Locales

This section contains the list of locales that can be used with the eID.

08.1   eID Locales

Locale	Description
mt	Locale to be used for Maltese language.
en-US	Locale to be used for English language.