Malayan Banking Berhad

Web Service Integration Technical Specification for Centralized Authentication System

26 January 2011

Prepared By:

Penril Datability (M) Sdn Bhd (816792-X)
Suite A-07-07 Plaza Mon't Kiara
No. 2, Jalan Kiara, Mon't Kiara
50480 Kuala Lumpur, Malaysia
Tel: (603) 6201 2622 Fax: (603) 6201 7622

Document Administration

Document Amendment Log

Version No	Date Updated	Description of Change	Updated By <Name, Dept>	Reviewed By <Name, Dept>	Approved By <Name, Dept>
1.0	26/01/11	Initial Release	Danniell Cheang, Professional Services	Tan Lee Yong, Professional Services	Tan Lee Yong, Professional Services
1.1	24/02/11	Amended data structure	Danniell Cheang, Professional Services	Tan Lee Yong, Professional Services	Tan Lee Yong, Professional Services
1.2	14/03/11	Added detailed description of each function	Danniell Cheang, Professional Services	Tan Lee Yong, Professional Services	Tan Lee Yong, Professional Services
1.3	02/03/11	Added enable user and amended typo	Danniell Cheang, Professional Services	Tan Lee Yong, Professional Services	Tan Lee Yong, Professional Services
1.4	01/04/11	Updated response codes	Danniell Cheang, Professional Services	Tan Lee Yong, Professional Services	Tan Lee Yong, Professional Services
1.5	01/06/11	Added sample response	Danniell Cheang, Professional Services	Tan Lee Yong, Professional Services	Tan Lee Yong, Professional Services
1.6	10/06/11	Added pin mailer enhancement	Danniell Cheang, Professional Services	Tan Lee Yong, Professional Services	Tan Lee Yong, Professional Services
1.7	17/06/11	Added samples	Danniell Cheang, Professional Services	Tan Lee Yong, Professional Services	Tan Lee Yong, Professional Services
1.8	18/11/11	Added map response for query company and user profile	Danniell Cheang, Professional Services	Tan Lee Yong, Professional Services	Tan Lee Yong, Professional Services
1.9	16/12/11	• Fixed response code 99 to generic error message • Consolidated Self registration from CMS to verify OTP after registration • Add SSO password character allowable during password verifications • Amend field length validation to cater for CMS requirement	Danniell Cheang, Professional Services	Tan Lee Yong, Professional Services	Tan Lee Yong, Professional Services

Table of Contents

1 Introduction

This document describes the technical documentation of Centralized Authentication System (CAS) web service being introduced to Maybank Cash Management System, Trade Finance System and Custody System. This document will be updated when new changes on requirements are applied and agreed across all parties. It includes the following details:

No.	Business Process	Functionality
1.	User Creation	• Create user • Query user profile • Add user access rights
2.	First Time Login	• First time login • Force reset password • Assign VASCO token • Self VASCO registration with OTP verification
3.	Login	• Normal login
4.	Company	• Query company name • Query company profile • Update company name • Update company profile
5.	User Maintenance	• Update user profile • Change authentication mode • Remove user access rights • Remove VASCO token ownership • Reset password • Change password • Verify Token OTP • Enable user status

2 Business Process Flow

2.1 User Creation

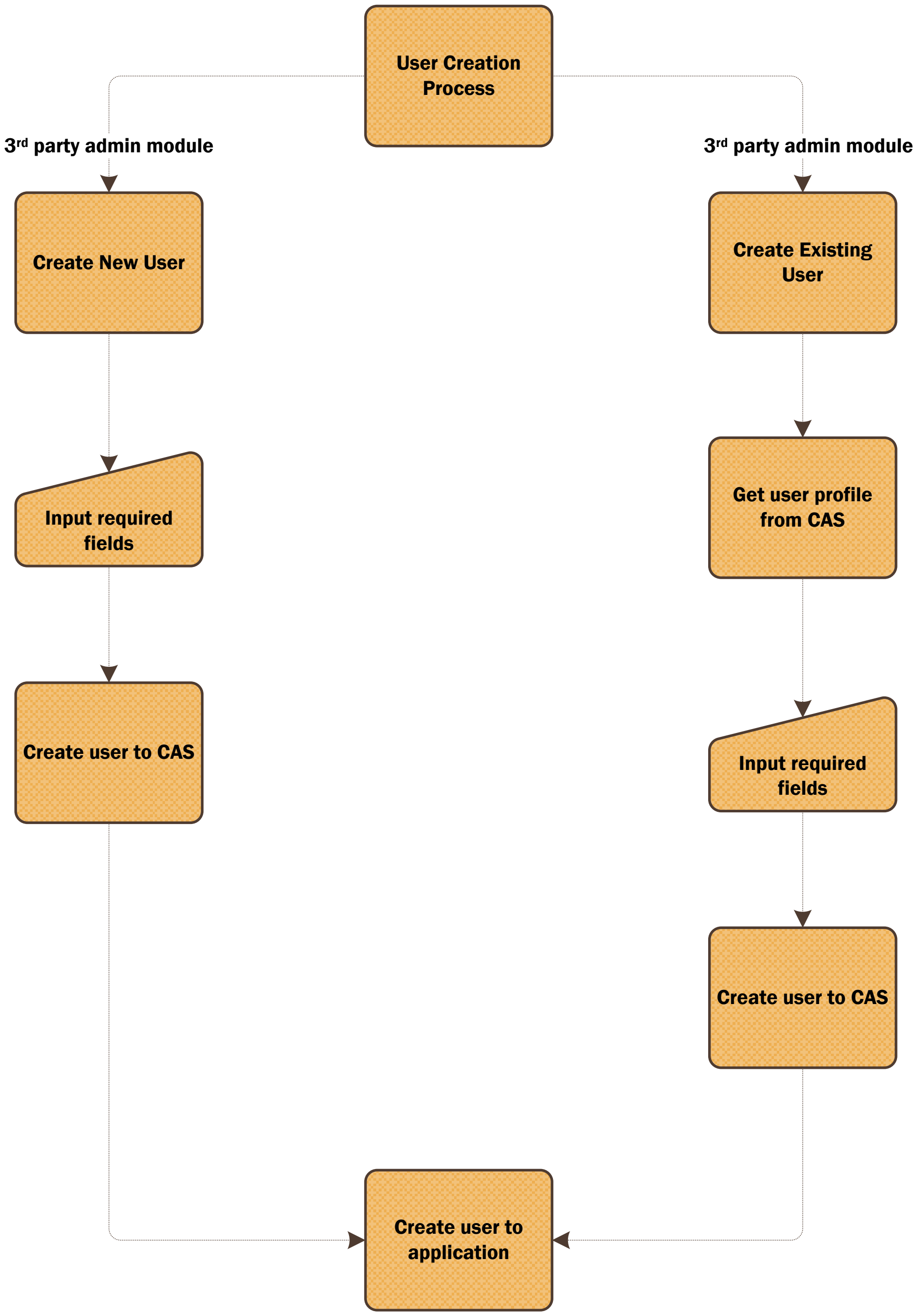

Fig 2.1: User creation process

2.2 First Time Login

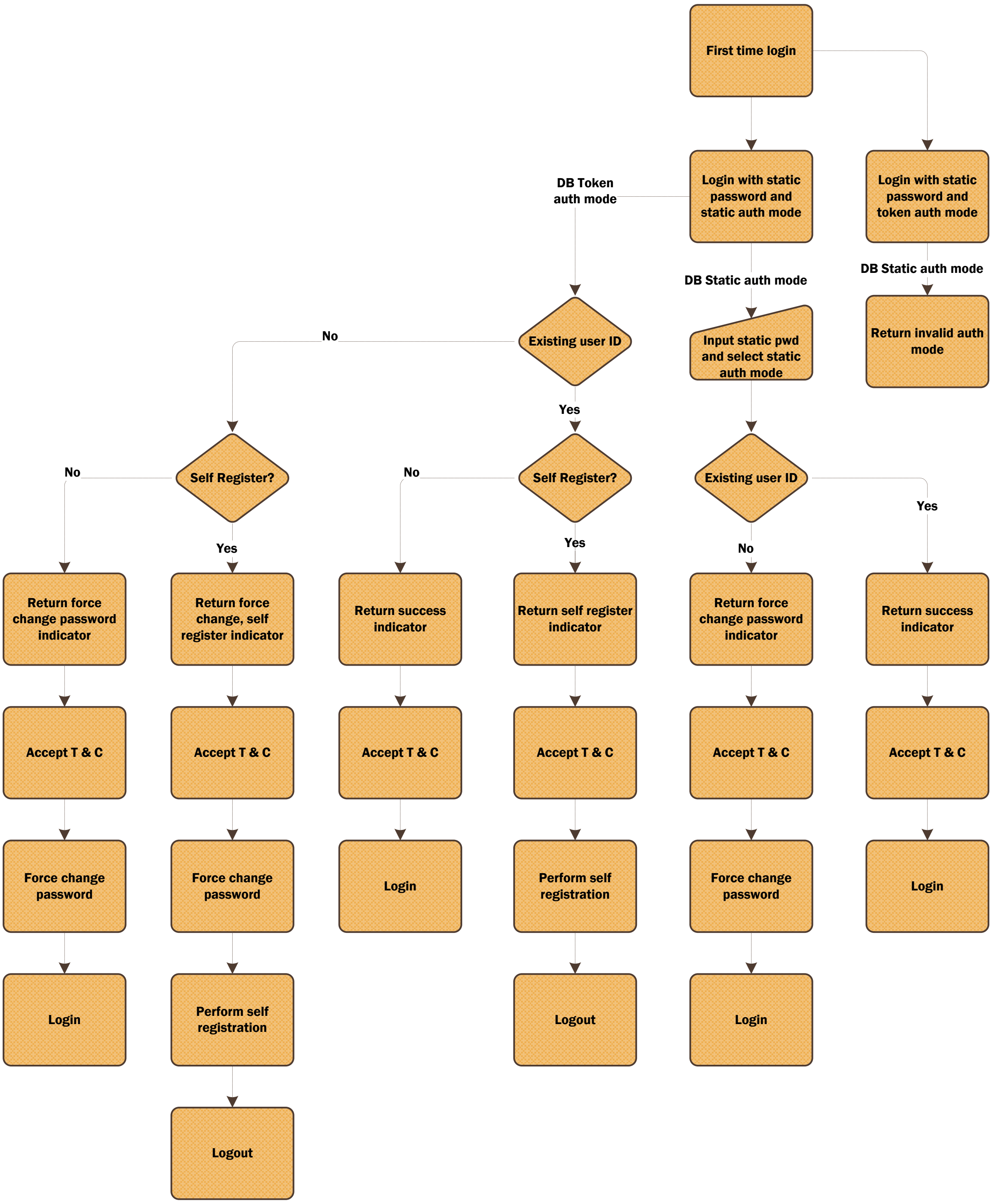

Fig 2.2: First time login process

2.3 Normal Login

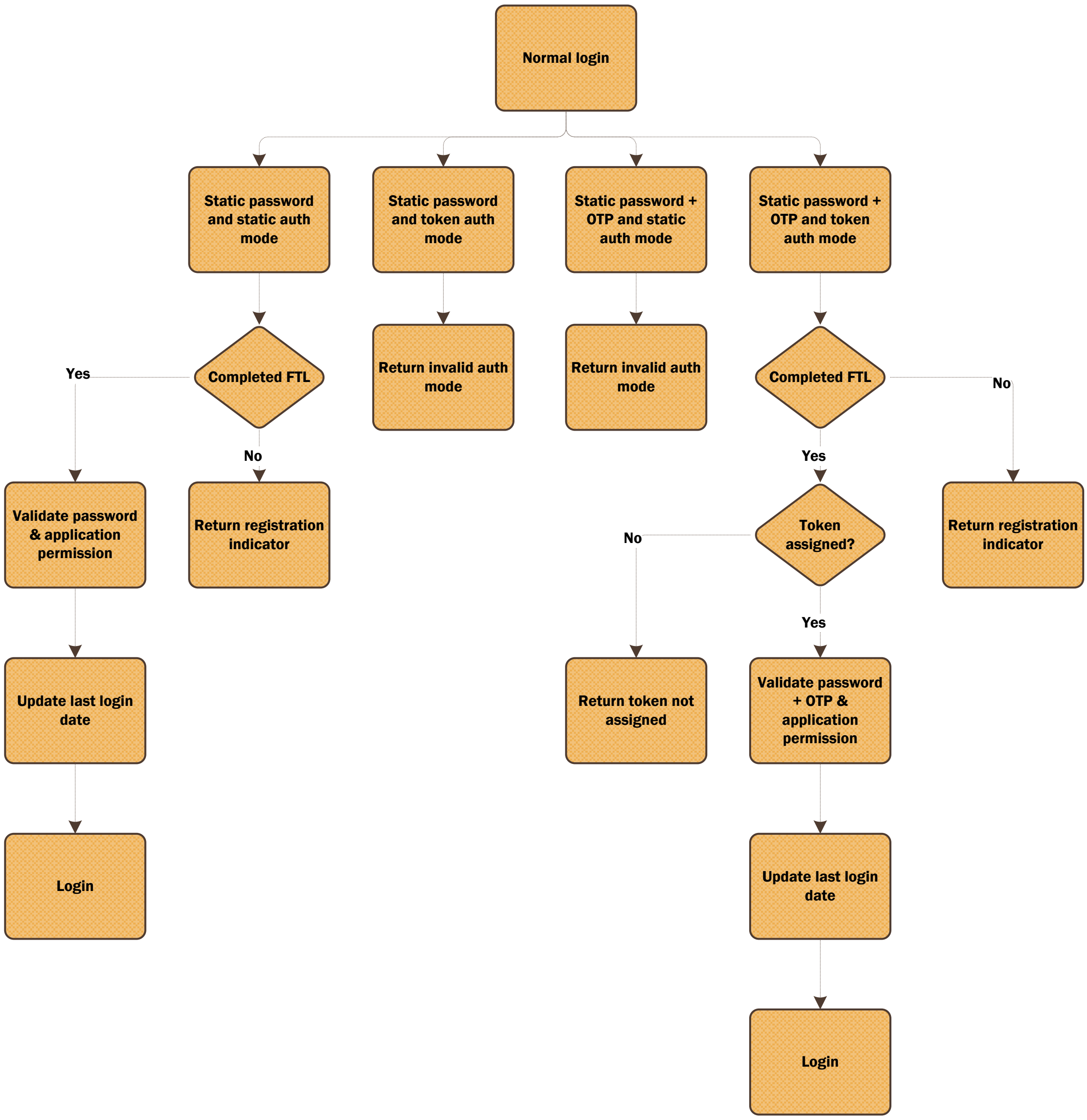
Normal login
Static password and static auth mode
Static password and token auth mode
Static password + OTP and static auth mode
Static password + OTP and token auth mode
Yes
Completed FTL
Return invalid auth mode
Return invalid auth mode
Completed FTL
No
No
Yes
Validate password & application permission
Return registration indicator
No
Token assigned?
Return registration indicator
Yes
Update last login date
Return token not assigned
Validate password + OTP & application permission
Login
Update last login date
Login

Fig 2.3: Normal login process

3 CAS Web Services

USER CREATION

3.1 Create User (wsCreateUser)

Create user is an administrative function. It is used by bank administrator to perform user creation via 3rd party administration application. It is invoked upon mandatory fields are met to create a new user in CAS. The event will create a new user in CAS that is pending for first time registration on the assigned application. Existing CAS user will need to add access rights in order to access a different application. It is detailed in section 3.3. Each field will be explained in greater detail during its sub chapter.

3.1.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	userID	AN	Y	10	-
4.	password	ANSC	Y	-	-
5.	companyID	AN	Y	10	-
6.	userName	ANSCP	Y	40	-
7.	userIdentification	AN	Y	40	-
8.	email	ANSC	Y	100	-
9.	mobileNo	N	Y	40	-
10.	countryCode	A	Y	2	-
11.	internalUserIndi	A	Y	1	I or E
12.	autoSendIndi	A	Y	1	B or R or P or N
13.	authMode	A	Y	1	T or S
14.	applicationID	N	Y	3	Provided

Fields Description

Field: adminID **Required**

This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**

This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: userID **Required**

This field describes the ID to be used during user creation. It may contain alphabets or numbers without white space. This field will be checked for uniqueness during the creation process and will be used as the login ID via login portal of each 3rd party application.

Field: password **Required**

This field describes the password to be used during user creation. It must have a minimum length of 5 characters and may contain alphabets or numbers or symbols without white space. A random password will be generated in CAS if blank is provided. This is to facilitate the notification services through SMS. This field will be checked for password complexity rule during the creation process and will be used as the login password via login portal of each 3rd party application.

Field: companyID **Required**

This field describes the corporate ID belongs to the new user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: userName **Required**
This field describes the full name belongs to the new user. It may contain alphabets, numbers or symbols with white space. This field will be stored as updatable information.

Field: userIdentification **Required**
This field describes the I.C number or passport number belongs to the new user. It may contain alphabets or numbers. This field will be stored as updatable information.

Field: email **Required**
This field describes the valid email address belongs to the new user. It may contain alphabets, numbers or symbol (specifically '@'). This field will be stored as updatable information and to be used for notification services.

Field: mobileNo **Required**
This field describes the valid mobile number belongs to the new user. It may contain numbers only. This field will be stored as updatable information and to be used for notification services.

Field: countryCode **Required**
This field describes the country of origin belongs to the new user. It may contain alphabets only. This field will be stored as updatable information.

Field: internalUserIndi **Required**
This field describes the user type belongs to the new user. Internal users are referring to Maybank bank administrators while external users are referring to 3rd party application users. Internal users are represented by 'I' while external users are represented by 'E'. It may contain alphabets only. This field will be stored as updatable information. This indicator is used to differentiate the dormant/password expiry period between bank users and customers.

Field: autoSendIndi **Required**
This field describes Auto sending mode of SMS or email belongs to the new user. This feature will trigger an SMS or email send service to notify the success of user creation. If 'R' is used, CAS will trigger an SMS and email send. If 'B' is used, CAS will keep this record to be placed as a pending activation item in CAS Administration. If 'N' is used, no services will be triggered. If 'P' is used, CAS will keep this record to be placed as a pending item to be printed out in Pin Mailer system. It may contain alphabets only. This field will be stored as updatable information.

Field: authMode **Required**
This field describes authentication mode belongs to the new user. This feature will identify the authentication mode of either Static or Token. Static mode is represented by 'S' while Token mode is represented by 'T'. It may contain alphabets only. This field will be stored as updatable information.

Field: applicationID **Required**
This field describes application ID assigned to the new user which is similar to the application that creates the user. It may contain numbers only. This field will be stored as updatable information. It is provided by CAS.

3.1.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (refer Response Code)

3.1.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
11	User ID has been used. Please choose a new one.
96	Password does not comply not contain a combination of upper case, lower case, number and special character.
97	Invalid required input
98	System is currently not available
206	Invalid user creation dependency (refer 3.1.4)

3.1.4 Allowable Conditions

CAS will perform user creation based on the following conditions. A response code of 206 will be returned if the conditions are not met.

Description	Auto Send	Process
Manual password input	N	CAS to create accordingly and no sending triggered.
	R	*Not allowed*
	B	*Not allowed*
	P	*Not allowed*
System generated	R	CAS to create accordingly and will trigger sending of both SMS and email
	B	CAS to create accordingly and place item in batch activation by CAS admin
	N	*Not allowed*
	P	CAS to create accordingly and place item in pin mailer queue

3.1.5 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soapenv:Body>
        <wsCreateUserResponse xmlns="http://upass.cas.ws.my">
            <wsCreateUserReturn>0</wsCreateUserReturn>
        </wsCreateUserResponse>
    </soapenv:Body>
</soapenv:Envelope>
```

3.2 Query User Profile (`wsQueryUserProfile`)

Query User Profile is an administrative function. This feature is used to perform user inquiry on a specified user ID using 3rd party application administration module. It is used by bank administrator. The event will return a user profile based on the requested userID. Each field will be explained in greater detail during its sub chapter.

3.2.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	userID	ANSC	Y	10	-
4.	companyID	AN	Y	10	-
5.	applicationID	N	Y	3	Provided

Fields Description

Field: adminID **Required**

This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**

This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: userID **Required**

This field describes the ID to be used for query. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: companyID **Required**

This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**

This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.2.2 Response

No.	Field	Description
<msg>		
<msgHeader>		
1.	<responseCode>	Numeric response from CAS (refer Response Code)
</ msgHeader >		
<msgBody>		
1.	<userID>	userID to be echoed back to application.
2.	<userStatus>	Status of user which is New, Active, Dormant and Disable
3.	<companyID>	Unique corporate identifier that the user belongs to
4.	<userName>	User full name
5.	<icPassport>	User I.C number or passport number
6.	<email>	User email address
7.	<mobileNo>	User mobile number
8.	<countryCode>	User country of origin
9.	<internalUserIndi>	Internal or external indicator of the user
10.	<authMode>	User authentication mode
11.	<autoSendIndi>	User auto send mode of SMS or email
12.	<application>	User access rights echoed back to the application
13.	<tokenSerial>	User VASCO token serial number if available
</msgBody>		
</msg>		

3.2.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below. If the response is other than successful, no message body will be returned.

Response Code	Description
0	Successful
6	User not found
20	User has been deleted
97	Invalid required input
98	System is currently not available

3.2.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soapenv:Body>
        <wsQueryUserProfileResponse xmlns="http://upass.cas.ws.my">
            <wsQueryUserProfileReturn>
                <msg>
                    <msgHeader>
                        <responseCode>0</responseCode>
                    </msgHeader>
                    <msgBody>
                        <userID>MAYBANKTESTSERVICEUSER</userID>
                        <userStatus>NEW</userStatus>
                        <companyID>MAYBANK</companyID>
                        <userName>test Service User</userName>
                        <icPassport>111111111</icPassport>
                        <email>mail@mail.com</email>
                        <mobileNo>0111111111</mobileNo>
                        <countryCode>MY</countryCode>
                        <internalUserIndi>I</internalUserIndi>
                        <authMode>S</authMode>
                        <autoSendIndi>N</autoSendIndi>
                        <application>101</application>
                        <tokenSerial />
                    </msgBody>
                </msg>
            </wsQueryUserProfileReturn>
        </wsQueryUserProfileResponse>
    </soapenv:Body>
</soapenv:Envelope>
```

3.3 Query User Profile Map (`wsQueryUserProfileMap`)

Query User Profile is an administrative function. This feature is used to perform user inquiry on a specified user ID using 3rd party application administration module. It is used by bank administrator. The event will return a user profile based on the requested userID. Each field will be explained in greater detail during its sub chapter.

3.3.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	userID	ANSC	Y	10	-
4.	companyID	AN	Y	10	-
5.	applicationID	N	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: userID **Required**
This field describes the ID to be used for query. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: companyID **Required**
This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.3.2 Response

No.	Field	Description
1.	responseCode	Numeric response from CAS (refer Response Code)
2.	userID	userID to be echoed back to application.
3.	userStatus	Status of user which is New, Active, Dormant and Disable
4.	companyID	Unique corporate identifier that the user belongs to
5.	userName	User full name
6.	icPassport	User I.C number or passport number
7.	email	User email address
8.	mobileNo	User mobile number
9.	countryCode	User country of origin
10.	internalUserIndi	Internal or external indicator of the user
11.	authMode	User authentication mode
12.	autoSendIndi	User auto send mode of SMS or email
13.	application	User access rights echoed back to the application
14.	tokenSerial	User VASCO token serial number if available

3.3.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below. If the response is other than successful, no message body will be returned.

Response Code	Description
0	Successful
6	User not found
20	User has been deleted
97	Invalid required input
98	System is currently not available

3.4 Add User Application Access (`wsGrantUserAccess`)

Add User Application Access is and administrative function. It is used to update user access matrix for existing user ID that wish to access different application. The event will add an access rights to the desired application in order to login through 3rd party application login portal. Each field will be explained in greater detail during its sub chapter.

3.4.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	userID	ANSC	Y	10	-
4.	companyID	AN	Y	10	-
5.	applicationID	N	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: userID **Required**
This field describes the ID to be used for adding of access rights. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: companyID **Required**
This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.4.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (refer Response Code)

3.4.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
6	User not found
97	Invalid required input
98	System is currently not available

3.4.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <soapenv:Body>
                <wsGrantUserAccessResponse xmlns="http://upass.cas.ws.my">
                        <wsGrantUserAccessReturn>6</wsGrantUserAccessReturn>
                </wsGrantUserAccessResponse>
        </soapenv:Body>
</soapenv:Envelope>
```

FIRST TIME REGISTRATION

3.5 Self Register VASCO Token (wsSelfRegisterVASCOToken)

Self Register VASCO Token is a user function. It is used to allow user to self register VASCO token based on the device's serial number and generated One Time Password (OTP). CAS will perform assignment of the VASCO token and verification of OTP. In case of OTP verification failure, CAS will perform reversal which is VASCO token revocation. The event will return a response to 3rd party application. Each field will be explained in greater detail during its sub chapter.

3.5.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	tokenSerial	N	Y	10	-
4.	userID	AN	Y	10	-
5.	companyID	AN	Y	10	-
6.	tokenOTP	N	Y	8	-
7.	applicationID	N	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: tokenSerial **Required**
This field describes the token serial number of the device. It may contain numbers only.

Field: userID **Required**
This field describes the ID belongs to the user. Token will be assigned from this ID. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: companyID **Required**
This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space.

Field: tokenOTP **Required**
This field describes the dynamic OTP generated by VASCO token held by the user. It must have a length of 8 digits and contain numbers only. This field will be checked for validity during authentication process and will be used as the 2nd factor authentication of each 3rd party application.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.5.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (Refer Response Code)

3.5.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
8	Token has been used by another ID
9	Token does not exist
30	Invalid OTP
31	Exceeded max attempts of OTP
32	OTP has been previously used
33	Invalid token status
97	Invalid required input
98	System is current not available
99	System is current not available

3.6 First Time Login (`wsVerifyFirstTimeLogin`)

First Time Login function is a user function. It is used to perform first time registration process in order to determine the necessity to force change password or assign token. The event will return indicators to alert for force change password, perform self-registration or both. Each field will be explained in greater detail during its sub chapter.

3.6.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	userID	AN	Y	10	-
2.	password	ANSCS	Y	-	-
3.	userTokenOTP	N	O	8	Device generated
4.	authMode	A	Y	1	-
5.	companyID	AN	Y	10	-
6.	applicationID	N	Y	3	Provided

Fields Description

Field: userID **Required**
This field describes the ID belongs to the user. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: password **Required**
This field describes the static password to be used to login. It must have a minimum length of 5 characters and may contain alphabets or numbers or symbols without white space. This field will be checked for password complexity rule during the authentication process and will be used as the login password via login portal of each 3rd party application.

Field: userTokenOTP **Required**
This field describes the dynamic OTP generated by VASCO token held by the user. It must have a length of 6 digits and contain numbers only. This field will be checked for validity during authentication process and will be used as the login OTP via login portal of each 3rd party application.

Field: authMode **Required**
This field describes authentication mode belongs to the user. This feature will identify the authentication mode of either Static or Token. Static mode is represented by ‘S’ while Token mode is represented by ‘T’. It may contain alphabets only. This field will be stored as updatable information.

Field: companyID **Required**
This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.6.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (Refer Response Code)

3.6.3 Response Code

CAS will return a response code for this service as per below. For response code of **202**, 3rd party application needs to confirm subsequent request has to be fulfilled prior granting user to access to application. E.g. for **202**, application needs to confirm that reset password and self registration has been completed with success prior proceed to home screen.

Response Code	Description
0	Successful
1	Wrong user ID or password
2	Exceeded maximum login attempts
5	Invalid user status
6	User not found
10	Invalid access to application
21	User is locked
22	User is inactive
30	Invalid OTP
31	Exceeded max attempts of OTP
32	OTP has been previously used
33	Invalid token status
96	Password does not contain a combination of upper case, lower case, number and special character
97	Invalid required input
98	System is current not available
99	System is current not available
200	Reset password is required
201	Self registration of VASCO token is required
202	Reset password and self registration of VASCO token is required
203	Invalid authentication mode

3.6.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soapenv:Body>
        <wsVerifyFirstTimeLoginResponse xmlns="http://upass.cas.ws.my">
            <wsVerifyFirstTimeLoginReturn>97</wsVerifyFirstTimeLoginReturn>
        </wsVerifyFirstTimeLoginResponse>
    </soapenv:Body>
</soapenv:Envelope>
```

3.7 Force Reset Password (`wsForceChangeStaticPassword`)

Force Reset Password function is a user function. It is used to reset password during first time login based on its indicators returned to 3rd party application. The event will perform password reset in CAS and a response will be return. This service shall be invoked if response code is **'200'** or **'202'** during `wsVerifyFirstTimeLogin` or `wsVerifyNormalLogin`. Each field will be explained in greater detail during its sub chapter.

3.7.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	userID	AN	Y	10	-
2.	newPassword	ANSC	Y	-	-
3.	oldPassword	ANSCS	Y	-	-
4.	companyID	AN	Y	10	-
5.	applicationID	N	Y	3	Provided

Fields Description

Field: userID **Required**
This field describes the ID belongs to the user. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: newPassword **Required**
This field describes the new static password to be used to login. It must have a minimum length of 5 characters and may contain alphabets or numbers or symbols without white space. This field will be checked for password complexity rule and history list during the change password process and will be used as the new login password via login portal of each 3rd party application.

Field: oldPassword **Required**
This field describes the existing valid static password to be used to login. It must have a minimum length of 5 characters and may contain alphabets or numbers or symbols without white space. This field will be checked for password complexity rule during the authentication process and will be used as the login password via login portal of each 3rd party application.

Field: companyID **Required**
This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.7.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (refer Response Code)

3.7.3 Response Code

CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
1	Wrong user ID or password
2	Exceeded maximum login attempts
3	Password has been previously used
6	User not found
96	Password does not contain a combination of upper case, lower case, number and special character
97	Invalid required input
98	System is current not available

3.7.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <soapenv:Body>
                <wsForceChangeStaticPasswordResponse
                        xmlns="http://upass.cas.ws.my">
        <wsForceChangeStaticPasswordReturn>97</wsForceChangeStaticPasswordReturn>
                </wsForceChangeStaticPasswordResponse>
        </soapenv:Body>
</soapenv:Envelope>
```

3.8 Assign VASCO Token (`wsAssignVASCOToken`)

Assign Token is a token management function. It is used to assign token for a specified user where self registration is needed. The event will allow CAS to assign token for the specified userID based on the provided serialNumber. Each field will be explained in greater detail during its sub chapter.

3.8.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	serialNumber	N	Y	10	-
4.	userID	ANSC	Y	10	-
5.	companyID	AN	Y	10	-
6.	applicationID	N	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: serialNumber **Required**
This field describes the 10 digit VASCO token serial number to be assigned to the user. It may contain numbers. This field will be check for integrity rules during the assignment process.

Field: userID **Required**
This field describes the ID belongs to the user. Token will be assigned to this ID. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: companyID **Required**
This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.8.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (Refer Response Code)

3.8.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
8	VASCO token has been assigned and in used
9	VASCO token not found
33	Invalid token status
97	Invalid required input
98	System is current not available
99	System is current not available

3.8.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soapenv:Body>
        <wsAssignVASCOTokenResponse xmlns="http://upass.cas.ws.my">
            <wsAssignVASCOTokenReturn>9</wsAssignVASCOTokenReturn>
        </wsAssignVASCOTokenResponse>
    </soapenv:Body>
</soapenv:Envelope>
```

LOGIN

3.9 Normal Login (`wsVerifyNormalLogin`)

Normal Login is a user function. It is used to verify user ID and password or user ID, password and OTP based on authentication mode. The event will authenticate user credentials and returns a response to 3rd party application. Each field will be explained in greater detail during its sub chapter.

3.9.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	userID	AN	Y	10	-
2.	password	ANSCS	Y	-	-
3.	userTokenOTP	N	O	8	Device generated
4.	authMode	A	Y	1	-
5.	companyID	AN	Y	10	-
6.	applicationID	N	Y	3	Provided

Fields Description

Field: userID **Required**
This field describes the ID belongs to the user. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: password **Required**
This field describes the static password to be used to login. It must have a minimum length of 5 characters and may contain alphabets or numbers or symbols without white space. This field will be checked for password complexity rule during the authentication process and will be used as the login password via login portal of each 3rd party application.

Field: userTokenOTP **Required**
This field describes the dynamic OTP generated by VASCO token held by the user. It must have a length of 6 digits and contain numbers only. This field will be checked for validity during authentication process and will be used as the login OTP via login portal of each 3rd party application.

Field: authMode **Required**
This field describes authentication mode belongs to the user. This feature will identify the authentication mode of either Static or Token. Static mode is represented by ‘S’ while Token mode is represented by ‘T’. It may contain alphabets only. This field will be stored as updatable information.

Field: companyID **Required**
This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.9.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (Refer Response Code)

3.9.3 Response Code

CAS will return a response code for this service as per below. For response code of **202**, 3rd party application needs to confirm subsequent request has to be fulfilled prior granting user to access to application. E.g. for **202**, application needs to confirm that reset password and self registration has been completed with success prior proceed to home screen.

Response Code	Description
0	Successful
1	Wrong user ID or password
2	Exceeded maximum login attempts
5	Invalid user status
6	User not found
10	Invalid access to application
21	User is locked
22	User is inactive
30	Invalid OTP
31	Exceeded max attempts of OTP
32	OTP has been previously used
33	Invalid token status
96	Password does not contain a combination of upper case, lower case, number and special character
97	Invalid required input
98	System is current not available
99	System is current not available
200	Reset password is required
201	Self registration of VASCO token is required
202	Reset password and self registration of VASCO token is required
203	Invalid authentication mode
204	Registration not completed. Proceed to first time login.

3.9.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
	xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
	<soapenv:Body>
		<wsVerifyNormalLoginResponse xmlns="http://upass.cas.ws.my">
			<wsVerifyNormalLoginReturn>0</wsVerifyNormalLoginReturn>
		</wsVerifyNormalLoginResponse>
	</soapenv:Body>
</soapenv:Envelope>
```

COMPANY

3.10 Query Company Name (wsQueryCompany)

Query Company Name is an administrative function. It is used to obtain the company name based on the requested companyID. It is used by bank administrator during company creation at 3rd party application administration. The event will return the company name of the request companyID or blank if company is not available. Each field will be explained in greater detail during its sub chapter.

3.10.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	companyID	AN	Y	10	-
4.	applicationID	ANSC	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: companyID **Required**
This field describes the corporate ID to be used in the query. It may contain alphabets or numbers without white space.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.10.2 Response

No.	Field	Description
<msg>		
<msgHeader>		
1.	<responseCode>	Numeric response from CAS (refer Response Code)
</ msgHeader >		
<msgBody>		
1.	<companyName>	Full name of requested company.
</msgBody>		
</msg>		

3.10.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
97	Invalid required input
98	System is current not available

3.10.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soapenv:Body>
        <wsQueryCompanyResponse xmlns="http://upass.cas.ws.my">
            <wsQueryCompanyReturn>
                <msg>
                    <msgHeader>
                        <responseCode>0</responseCode>
                    </msgHeader>
                    <msgBody>
                        <companyName>Maybank Berhad</companyName>
                    </msgBody>
                </msg>
            </wsQueryCompanyReturn>
        </wsQueryCompanyResponse>
    </soapenv:Body>
</soapenv:Envelope>
```

3.11 Query Company Name Map (`wsQueryCompanyMap`)

Query Company Name is an administrative function. It is used to obtain the company name based on the requested companyID. It is used by bank administrator during company creation at 3rd party application administration. The event will return the company name of the request companyID or blank if company is not available. Each field will be explained in greater detail during its sub chapter.

3.11.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	companyID	AN	Y	10	-
4.	applicationID	ANSC	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: companyID **Required**
This field describes the corporate ID to be used in the query. It may contain alphabets or numbers without white space.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.11.2 Response

No.	Field	Description
1.	responseCode	Numeric response from CAS (refer Response Code)
2.	companyName	Full name of requested company.

3.11.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
97	Invalid required input
98	System is current not available

3.12 Update Company Name (`wsUpdateCompanyName`)

Update Company Name is an administrative function. It is used to update the company name based on the requested companyID. It is used by bank administrator during company name update is required at 3rd party application administration. The event will return a response to 3rd party application. Each field will be explained in greater detail during its sub chapter.

3.12.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	companyID	AN	Y	10	-
4.	companyName	ANSCP	Y	35	-
5.	applicationID	ANSC	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: companyID **Required**
This field describes the corporate ID to be updated. It may contain alphabets or numbers without white space.

Field: companyName **Required**
This field describes the corporate name to be updated. It may contain alphabets or numbers without white space.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.12.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (Refer Response Code)

3.12.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
97	Invalid required input
98	System is current not available

3.12.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soapenv:Body>
        <wsUpdateCompanyNameResponse xmlns="http://upass.cas.ws.my">
            <wsUpdateCompanyNameReturn>0</wsUpdateCompanyNameReturn>
        </wsUpdateCompanyNameResponse>
    </soapenv:Body>
</soapenv:Envelope>
```

3.13 Query Company Profile (`wsQueryCompanyProfile`)

Query Company Profile is an administrative function. It is used to obtain the company name based on the requested companyID. It is used by bank administrator during company creation at 3rd party application administration. The event will return the company profile of the request companyID or blank if company is not available. Each field will be explained in greater detail during its sub chapter.

3.13.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	companyID	AN	Y	10	-
4.	applicationID	ANSC	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: companyID **Required**
This field describes the corporate ID to be used in the query. It may contain alphabets or numbers without white space.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.13.2 Response

No.	Field	Description
<msg>		
<msgHeader>		
1.	<responseCode>	Numeric response from CAS (refer Response Code)
</ msgHeader >		
<msgBody>		
1.	<companyName>	Full name of requested company.
2.	<companyAddr1>	Company address line 1
3.	<companyAddr2>	Company address line 2
4.	<companyAddr3>	Company address line 3
5.	<companyAddr4>	Company address line 4
6.	<companyAddr5>	Company address line 5
7.	<companyPostCode>	Company postcode
8.	<companyState>	Company state
9.	<companyCountryCode>	Company 2 digit country code
10.	<companyContactNo>	Company contact number
11.	<companyFaxNo>	Company fax number
</msgBody>		
</msg>		

3.13.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
97	Invalid required input
98	System is current not available

3.13.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soapenv:Body>
        <wsQueryCompanyProfileResponse xmlns="http://upass.cas.ws.my">
            <wsQueryCompanyProfileReturn>
                <msg>
                    <msgHeader>
                        <responseCode>0</responseCode>
                    </msgHeader>
                    <msgBody>
                        <companyName>SMART CORPORATION</companyName>
                        <companyAddr1>67,JALAN BISTARI</companyAddr1>
                        <companyAddr2>MENARA BISTARI</companyAddr2>
                        <companyAddr3 />
                        <companyAddr4 />
                        <companyAddr5 />
                        <companyPostCode />
                        <companyState>Putrajaya</companyState>
                        <companyCountryCode />
                        <companyContactNo>0000000000</companyContactNo>
                        <companyFaxNo />
                    </msgBody>
                </msg>
            </wsQueryCompanyProfileReturn>
        </wsQueryCompanyProfileResponse>
    </soapenv:Body>
</soapenv:Envelope>
```

3.14 Query Company Profile Map (`wsQueryCompanyProfileMap`)

Query Company Profile is an administrative function. It is used to obtain the company name based on the requested companyID. It is used by bank administrator during company creation at 3rd party application administration. The event will return the company profile of the request companyID or blank if company is not available. Each field will be explained in greater detail during its sub chapter.

3.14.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	companyID	AN	Y	10	-
4.	applicationID	ANSC	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: companyID **Required**
This field describes the corporate ID to be used in the query. It may contain alphabets or numbers without white space.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.14.2 Response

No.	Field	Description
1.	responseCode	Numeric response from CAS (refer Response Code)
2.	companyName	Full name of requested company.
3.	companyAddr1	Company address line 1
4.	companyAddr2	Company address line 2
5.	companyAddr3	Company address line 3
6.	companyAddr4	Company address line 4
7.	companyAddr5	Company address line 5
8.	companyPostCode	Company postcode
9.	companyState	Company state
10.	companyCountryCode	Company 2 digit country code
11.	companyContactNo	Company contact number
12.	companyFaxNo	Company fax number

3.14.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
97	Invalid required input
98	System is current not available

3.15 Update Company Profile (wsUpdateCompanyProfile)

Update Company Profile is an administrative function. It is used to update the company related details based on the provided companyID. It is used by bank administrator during company profile update is required at 3rd party application administration. The event will return a response to 3rd party application. Each field will be explained in greater detail during its sub chapter.

3.15.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	companyID	AN	Y	10	-
4.	companyName	ANSCP	Y	35	-
5.	companyAddr1	ANSCP	Y	30	-
6.	companyAddr2	ANSCP	Y	30	-
7.	companyAddr3	ANSCP	O	30	-
8.	companyAddr4	ANSCP	O	30	-
9.	companyAddr5	ANSCP	O	30	-
10.	companyPostCode	N	O	15	-
11.	companyState	A	O	60	-
12.	companyCountryCode	A	Y	2	-
13.	companyContactNo	N	Y	20	-
14.	companyFaxNo	N	O	20	-
15.	applicationID	ANSC	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: companyID **Required**
This field describes the corporate ID to be updated. It may contain alphabets or numbers without white space.

Field: companyName **Required**
This field describes the corporate name to be updated. It may contain alphabets or numbers without white space.

Field: companyAddr1 **Required**
This field describes the corporate address to line 1 to be updated. It may contain alphabets, numbers and special characters with white space.

Field: companyAddr2 **Required**
This field describes the corporate address to line 2 to be updated. It may contain alphabets, numbers and special characters with white space.

Field: companyAddr3 **Optional**
This field describes the corporate address to line 3 to be updated. It may contain alphabets, numbers and special characters with white space.

Field: companyAddr4 **Optional**
This field describes the corporate address to line 4 to be updated. It may contain alphabets, numbers and special characters with white space.

Field: companyAddr5 **Optional**
This field describes the corporate address to line 5 to be updated. It may contain alphabets, numbers and special characters with white space.

Field: companyPostCode **Optional**
This field describes the corporate post code to be updated. It may contain numbers only.

Field: companyState **Optional**
This field describes the corporate state to be updated. It may contain alphabets only.

Field: companyCountryCode **Required**
This field describes the corporate 2 digit country code to be updated. It may contain alphabets only.

Field: companyContactNo **Required**
This field describes the corporate phone number to be updated. It may contain number only.

Field: companyFaxNo **Optional**
This field describes the corporate fax number to be updated. It may contain number only.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.15.2 Response

No.	Value	Description
2.	Response Code	Numeric response from CAS (Refer Response Code)

3.15.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
97	Invalid required input
98	System is current not available

3.15.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soapenv:Body>
        <wsUpdateCompanyProfileResponse xmlns="http://upass.cas.ws.my">
            <wsUpdateCompanyProfileReturn>0</wsUpdateCompanyProfileReturn>
        </wsUpdateCompanyProfileResponse>
    </soapenv:Body>
</soapenv:Envelope>
```

USER MAINTENANCE

3.16 Update User Profile (wsUpdateUserProfile)

Update User Profile is an administrative function. It is used to perform user details update based on input fields. It is used by bank administrator to perform user update via 3rd party application administration. The event will allow CAS to update fields that are request and returns a response to 3rd party application. Each field will be explained in greater detail during its sub chapter.

3.16.1 Request

No.	Field	Data Type	Required	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	userID	AN	Y	10	-
4.	userName	AN	O	-	-
5.	userIdentification	AN	O	40	-
6.	email	ANSC	O	100	-
7.	mobileNo	N	O	40	-
8.	countryCode	A	O	2	-
9.	autoSendIndi	A	O	1	B or R or P or N
10.	companyID	AN	Y	10	-
11.	applicationID	N	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: userID **Required**
This field describes the userID to be updated. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: userName **Optional**
This field describes the full name to be updated. It may contain alphabets, numbers or symbols with white space. This field will be stored as updatable information. This field will not be updated if left blank.

Field: userIdentification **Optional**
This field describes the I.C number or passport number to be updated. It may contain alphabets or numbers. This field will be stored as updatable information. This field will not be updated if left blank.

Field: email **Optional**
This field describes the valid email address to be updated. It may contain alphabets, numbers or symbol (specifically '@'). This field will be stored as updatable information and to be used for notification services. This field will not be updated if left blank.

Field: mobileNo **Optional**
This field describes the valid mobile number to be updated. It may contain numbers. This field will be stored as updatable information and to be used for notification services. This field will not be updated if left blank.

Field: countryCode **Optional**
This field describes the country of origin to be updated. It may contain alphabets only. This field will be stored as updatable information. This field will not be updated if left blank.

Field: autoSendIndi **Optional**
This field describes Auto sending mode of SMS or email to be updated. This feature will trigger an SMS or email send service to notify the success of user creation. If 'R' is used, CAS will trigger an SMS and email send. If 'B' is used, CAS will keep this record to be placed as a pending activation item in CAS Administration. If 'N' is used, no services will be triggered. If 'P' is used, CAS will keep this record to be placed as a pending item to be printed out in Pin Mailer system. It may contain alphabets only. This field will be stored as updatable information. This field will not be updated if left blank.

Field: companyID **Required**
This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.16.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (Refer)

3.16.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
6	User not found
97	Invalid required input
98	System is current not available
99	System is current not available
206	Invalid user auto send mode dependency (refer 3.1.4)

3.16.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soapenv:Body>
        <wsUpdateUserProfileResponse xmlns="http://upass.cas.ws.my">
            <wsUpdateUserProfileReturn>0</wsUpdateUserProfileReturn>
        </wsUpdateUserProfileResponse>
    </soapenv:Body>
</soapenv:Envelope>
```

3.17 Change Authentication Mode (`wsChangeAuthenticationMode`)

Change user authentication mode is an administrative feature. It is used to change an external user authentication mode from Static to Token and vice versa. It is used by bank administrator via 3rd party application administration. The event will allow CAS to change the authentication mode and returns a response. Each field will be explained in greater detail during its sub chapter.

3.17.1 Request

No.	Field	Data Type	Mandatory	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	userID	ANSC	Y	10	-
4.	authMode	A	Y	1	T or S
5.	companyID	AN	Y	10	-
6.	applicationID	N	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: userID **Required**
This field describes the userID to be queried. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: authMode **Required**
This field describes authentication mode to be changed. This feature will identify the authentication mode of either Static or Token. Static mode is represented by ‘S’ while Token mode is represented by ‘T’. It may contain alphabets only. This field will be stored as updatable information.

Field: companyID **Required**
This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.17.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (Refer Response Code)

3.17.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
6	User not found
97	Invalid required input
98	System is current not available
99	System is current not available

3.17.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <soapenv:Body>
                <wsChangeAuthenticationModeResponse xmlns="http://upass.cas.ws.my">
                        <wsChangeAuthenticationModeReturn>97</wsChangeAuthenticationModeReturn>
                </wsChangeAuthenticationModeResponse>
        </soapenv:Body>
</soapenv:Envelope>
```

3.18 Remove User Application Access (`wsRevokeUserAccess`)

Remove user application access function is an administrative function. It is used when 3rd party application tries to delete the user at their end and CAS will remove the application access to that particular application. This feature is used by bank administrator via 3rd party application administration. The event will allow CAS to remove the access rights and returns a response. Each field will be explained in greater detail during its sub chapter.

3.18.1 Request

No.	Field	Data Type	Mandatory	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	userID	ANSC	Y	10	-
4.	companyID	AN	Y	10	-
5.	applicationID	N	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: userID **Required**
This field describes the ID belongs to the user. Access right to this application will be removed from this ID. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: companyID **Required**
This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**
This field describes application ID to be removed from the user which is similar to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.18.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (Refer Response Code)

3.18.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
6	User not found
97	Invalid required input
98	System is current not available
99	System is current not available

3.18.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soapenv:Body>
        <wsRevokeUserAccessResponse xmlns="http://upass.cas.ws.my">
            <wsRevokeUserAccessReturn>97</wsRevokeUserAccessReturn>
        </wsRevokeUserAccessResponse>
    </soapenv:Body>
</soapenv:Envelope>
```

3.19 Revoke VASCO Token (`wsRevokeVASCOToken`)

Remove VASCO Token function is a token management function. It is used to remove the token being assigned to the specified user. It is used by bank administrator via 3rd party application administration. The event will allow CAS to remove the token ownership from the request userID and returns a response. Each field will be explained in greater detail during its sub chapter.

3.19.1 Request

No.	Field	Data Type	Mandatory	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	userID	ANSC	Y	10	-
4.	companyID	AN	Y	10	-
5.	applicationID	N	Y	3	Provided

Fields Description

Field: adminID **Required**

This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**

This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: userID **Required**

This field describes the ID belongs to the user. Token will be unassigned from this ID. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: companyID **Required**

This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**

This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.19.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (Refer Response Code)

3.19.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
9	VASCO Token not found
97	Invalid required input
98	System is current not available
99	System is current not available

3.19.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <soapenv:Body>
                <wsRevokeVASCOTokenResponse xmlns="http://upass.cas.ws.my">
                        <wsRevokeVASCOTokenReturn>97</wsRevokeVASCOTokenReturn>
                </wsRevokeVASCOTokenResponse>
        </soapenv:Body>
</soapenv:Envelope>
```

3.20 Change Password (`wsChangeStaticPassword`)

Change Password function is user function. It is used by user to change his/her password. The event will allow CAS to change the existing password to the new password and returns a response. Each field will be explained in greater detail during its sub chapter.

3.20.1 Request

No.	Field	Data Type	Mandatory	Max Length	Remarks
1.	userID	AN	Y	10	-
2.	newPassword	ANSC	Y	-	-
3.	oldPassword	ANSCS	Y	-	-
4.	companyID	AN	Y	10	-
5.	applicationID	N	Y	3	Provided

Fields Description

Field: userID **Required**
This field describes the ID belongs to the user. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: newPassword **Required**
This field describes the new static password to be used to login. It must have a minimum length of 5 characters and may contain alphabets or numbers or symbols without white space. This field will be checked for password complexity rule and history list during the change password process and will be used as the new login password via login portal of each 3rd party application.

Field: oldPassword **Required**
This field describes the existing valid static password to be used to login. It must have a minimum length of 5 characters and may contain alphabets or numbers or symbols without white space. This field will be checked for password complexity rule during the authentication process and will be used as the login password via login portal of each 3rd party application.

Field: companyID **Required**
This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.20.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (Refer Response Code)

3.20.3 Response Code

CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
1	Wrong user ID or password
2	Exceeded maximum login attempts
3	Password has been previously used
96	Password does not contain a combination of upper case, lower case, number and special character
97	Invalid required input
98	System is current not available
99	System is current not available

3.20.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <soapenv:Body>
                <wsChangeStaticPasswordResponse xmlns="http://upass.cas.ws.my">
                        <wsChangeStaticPasswordReturn>0</wsChangeStaticPasswordReturn>
                </wsChangeStaticPasswordResponse>
        </soapenv:Body>
</soapenv:Envelope>
```

3.21 Reset Password (`wsResetStaticPassword`)

Reset Password function is an administrative function. It is used to reset other user's password and used by bank/corporate admin. The event will allow CAS to reset password based on provided userID and returns a response. If userPassword is blank, CAS will triggers a system generated password and send SMS to notify user. Each field will be explained in greater detail during its sub chapter.

3.21.1 Request

No.	Field	Data Type	Mandatory	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	userID	AN	Y	10	-
4.	userPassword	ANSC	O	-	-
5.	companyID	AN	Y	10	-
6.	applicationID	N	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: userID **Required**
This field describes the ID to be reset. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: userPassword **Optional**
This field describes the existing valid static password to be used to login. It must have a minimum length of 5 characters and may contain alphabets or numbers or symbols without white space. This field will be checked for password complexity rule during the authentication process and will be used as the login password via login portal of each 3rd party application.

Field: companyID **Required**
This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.21.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (Refer Response Code)

3.21.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
3	Password has been previously used
6	User not found
96	Password does not contain a combination of upper case, lower case, number and special character
97	Invalid required input
98	System is current not available
99	System is current not available

3.21.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soapenv:Body>
        <wsResetStaticPasswordResponse xmlns="http://upass.cas.ws.my">
            <wsResetStaticPasswordReturn>97</wsResetStaticPasswordReturn>
        </wsResetStaticPasswordResponse>
    </soapenv:Body>
</soapenv:Envelope>
```

3.22 Verify Token OTP (`wsVerifyTokenOTP`)

Verify Token OTP function is a re-auth function. It is used as a 2nd factor authentication feature whereby it is common among maker checker approach. This function is used by approver in approving transactions initiated by the maker. Each field will be explained in greater detail during its sub chapter.

3.22.1 Request

No.	Field	Data Type	Mandatory	Max Length	Remarks
1.	userID	AN	Y	10	-
2.	companyID	AN	Y	10	-
3.	tokenOTP	N	Y	8	Device Generated
4.	applicationID	N	Y	3	Provided

Fields Description

Field: userID **Required**

This field describes the ID belongs to the token holder. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: companyID **Required**

This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: tokenOTP **Required**

This field describes the dynamic OTP generated by VASCO token held by the user. It must have a length of 6 digits and contain numbers only. This field will be checked for validity during authentication process and will be used as the 2nd factor authentication of each 3rd party application.

Field: applicationID **Required**

This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.22.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (Refer Response Code)

3.22.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
6	User not found
30	Invalid OTP
31	Exceeded max attempts of OTP
32	OTP has been previously used
33	Invalid token status
97	Invalid required input
98	System is current not available
99	System is current not available

3.22.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soapenv:Body>
        <wsVerifyTokenOTPResponse xmlns="http://upass.cas.ws.my">
            <wsVerifyTokenOTPReturn>97</wsVerifyTokenOTPReturn>
        </wsVerifyTokenOTPResponse>
    </soapenv:Body>
</soapenv:Envelope>
```

3.23 Enable User (`wsEnableUser`)

Enable User is an administrative function. It is used to enable CAS user if the status is Disabled, Dormant and by bank/corporate admin. The event will allow CAS to change the CAS user status to Active if it was an active user or New if it is a first time user based on provided userID and returns a response. Each field will be explained in greater detail during its sub chapter.

3.23.1 Request

No.	Field	Data Type	Mandatory	Max Length	Remarks
1.	adminID	AN	Y	10	Provided
2.	adminPassword	ANSC	Y	-	Provided
3.	userID	AN	Y	10	-
4.	companyID	AN	Y	10	-
5.	applicationID	N	Y	3	Provided

Fields Description

Field: adminID **Required**
This field describes the ID to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: adminPassword **Required**
This field describes the static password to be used as authentication purpose. Since the function is an administrative feature, authentication of system ID and system password is required in order to proceed. It is provided by CAS.

Field: userID **Required**
This field describes the ID to be reset. It may contain alphabets or numbers without white space. This field will be used as the login ID via login portal of each 3rd party application.

Field: companyID **Required**
This field describes the corporate ID belongs to the user. It may contain alphabets or numbers without white space. This field will be checked for referential integrity during the creation process.

Field: applicationID **Required**
This field describes application ID belongs to the application that sends this service. It may contain numbers only. It is provided by CAS.

3.23.2 Response

No.	Value	Description
1.	Response Code	Numeric response from CAS (Refer Response Code)

3.23.3 Response Code

This service requires system authentication which has additional response codes as per System Authorization Response Code Mapping. CAS will return a response code for this service as per below:

Response Code	Description
0	Successful
6	User not found
97	Invalid required input
98	System is current not available
99	System is current not available

3.23.4 Sample Response

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <soapenv:Body>
                <wsEnableUserResponse xmlns="http://upass.cas.ws.my">
                        <wsEnableUserReturn>0</wsEnableUserReturn>
                </wsEnableUserResponse>
        </soapenv:Body>
</soapenv:Envelope>
```

4 Appendix

4.1 System Authorization Response Code Mapping

Response Code	Description
1	Wrong user ID or password
2	Exceeded maximum login attempts
5	Invalid user status
6	User not found
10	Invalid access to application
96	Password does not contain a combination of upper case, lower case, number and special character

4.2 Data Type Legend

Field	Description	Remark
AN	Alphabet and numeric	Either type that is present
ANSC	Alphabet, numeric and symbols	Allowable symbols: !@#$%^&*()_+<>?
ANSCS	Alphabet, numeric and SSO symbols	Allowable symbols: !@#$%^&*()_+-=<>,.?/:;[]{}|
ANSP	Alphabet, numeric and spaces	-
ANSCP	Alphabet, numeric, symbols and spaces	-
N	Numeric only	-
A	Alphabet only	-