AllWebID Identity Manager

Online 2-Factor Identity Authentication Solution

AllWebIDiOS SDK
Manual

Version 1.1

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

Introduction

The purpose of this document is to briefly explain the iOS AllWebID Identity Manger Software Development Kit (SDK). This SDK will help developers to quickly integrate AllWebID Identity Manager Application Programming Interface (APIs) with their iOS applications, and to offer Multi-Factor Identity Authentication to their clients/ end users

Overview

The APIs provided in the SDK are used to enable secure data exchange between the servers hosting the mobile application and AllWebID cloud based servers. The APIs are organized in groups which are triggered in a particular sequence to accomplish different tasks of the Identity Manager solution, and enable the end users to conveniently use 2-factor authentication (2FA). Following are some of the key processes which can be integrated in android applications to enable AllWebID 2-factor authentication service:

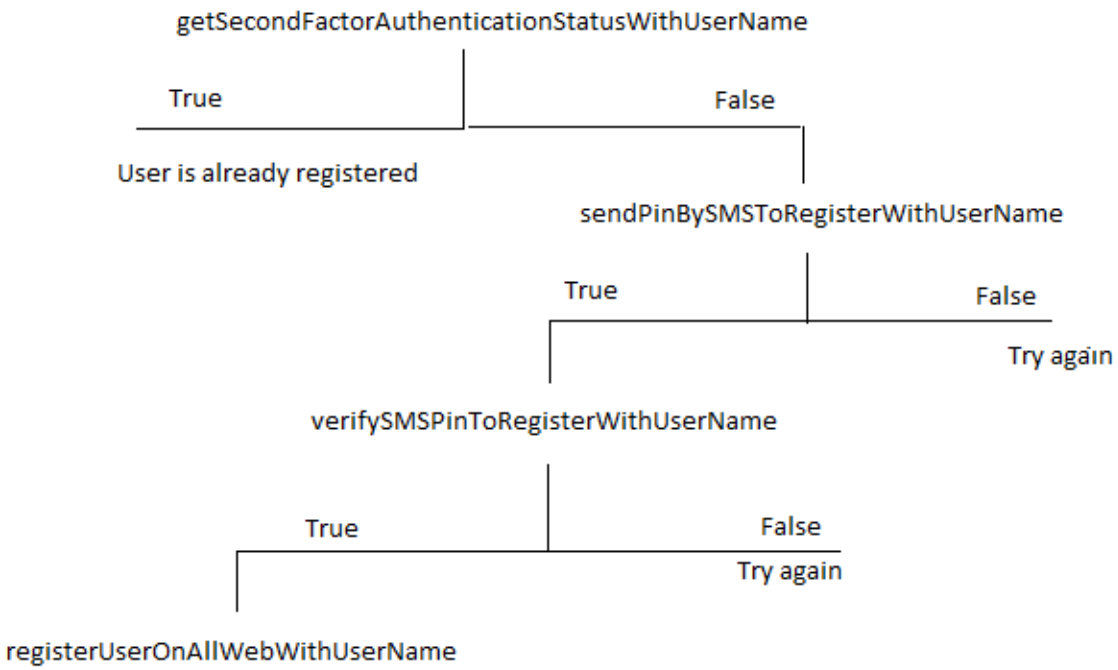
1. 2nd Factor Authentication Login
2. Registration with AllWebID
3. Enable / Disable 2FA
4. Fingerprint Linking / De-Linking with current device.
5. SMS Authentication for verification
6. SMS Authentication for Cell Phone registration
7. Fingerprint Authentication
8. Enable / Disable trusted device
9. Make current device trusted

Register user for second factor authentication through SMS

To register a user for second factor authentication, following steps are recommended

- First invoke "getSecondFactorAuthenticationStatusWithUserName" method of API to make sure the user is not already registered.
- Check the received response. If it returns "disabled", verify the phone number provided by the user by invoking "sendPinBySmsToRegisterWithUserName" method to send pin code on phone.
- To check if pin code entered by user is correct, invoke "verifySMSPinToRegisterWithUserName" method.
- If pin code entered by user is correct, invoke "registerUserOnAllWebWithUserName" method to register user for second factor authentication.

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

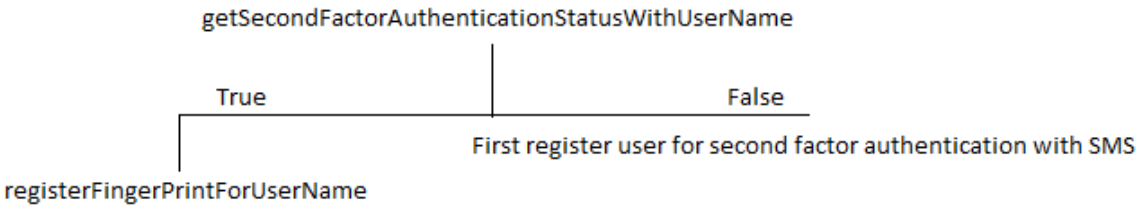


Register user for second factor authentication through SMS

Register user for second factor authentication through Fingerprint scan

- To register user for second factor authentication with finger print, user must have already registered for SMS authentication(second factor authentication through SMS).
- It can be checked if user has already registered for SMS authentication by invoking API method "getSecondFactorAuthenticationStatusWithUserName"
- If user second factor status returned by above API method call is "SMS", invoke "registerFingerPrintForUserName" to register user for second factor authentication with fingerprint.

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

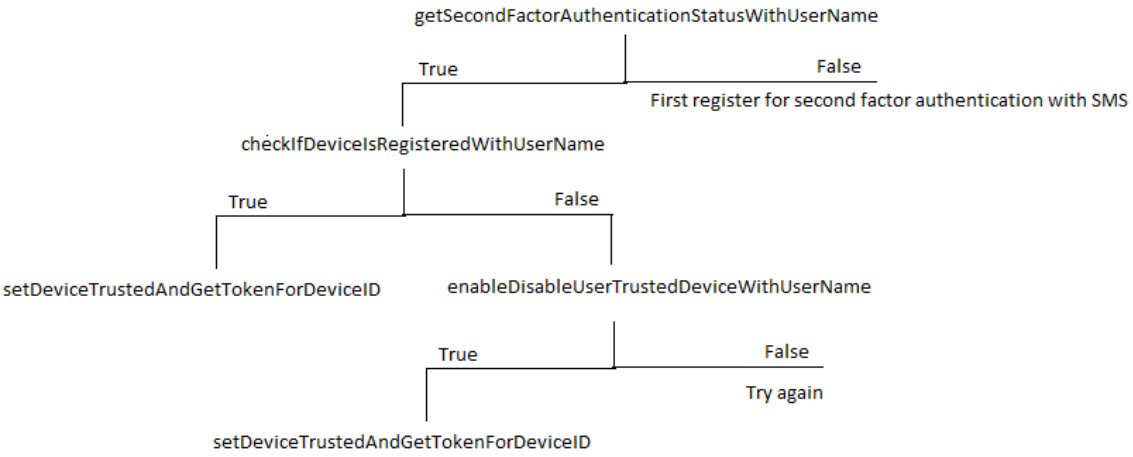


Register user for second factor authentication through Fingerprint scan

Make Device Trusted

Note: This is an optional feature.

- If user has registered for second factor authentication with fingerprint, user can also be allowed to make device trusted so that user doesn't need to scan finger print on his trusted device, instead a generated token is used to authenticate user.
- To make device user trusted, it is pre-requisite that user has registered for second factor authentication with fingerprint, user has enabled the trusted device feature.
- Enable user trusted device feature by invoking API method "enableDisableUserTrustedDeviceWithUserName" and pass "true" in the parameter which is of type Bool.
- Make user device trusted by invoking method "setDeviceTrustedAndGetTokenForDeviceID".



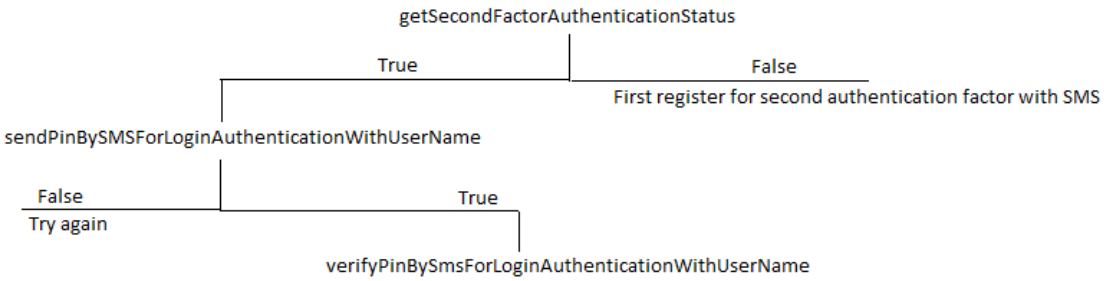
Make Device trusted

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

Login

- To authenticate user with AllWebID second factor authentication mechanism, it is required that user has enabled second factor authentication.
- Invoke "getSecondFactorAuthenticationStatusWithUserName" method to check if user has enabled second factor authentication.

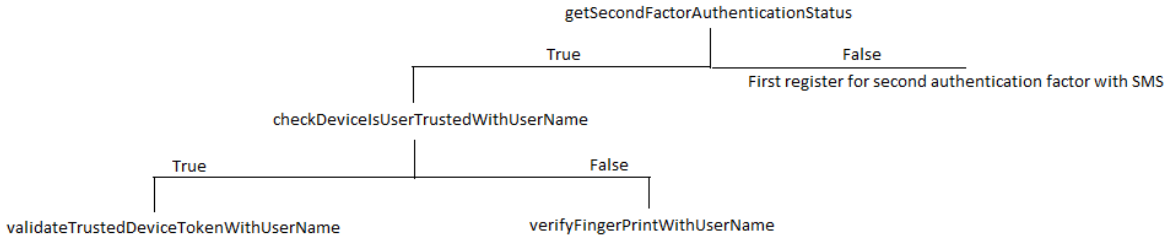
    - **Authentication with SMS**
        - Invoke method "sendPinBySmsForLoginAuthenticationWithUserName" to send pin code to user phone.
        - Verify pin code entered by user by invoking method "verifySMSPinForLoginAuthenticationWithUserName"



Authentication with SMS

    - **Authenticate with fingerprint**
        - To authenticate with fingerprint user must have registered for second factor authentication with user name
        - Invoke method "checkIfDeviceIsUserTrustedWithUserName" to check if user has set the device as trusted
        - If the user device is set as trusted, invoke method "validateTrustedDeviceTokenWithUserName" to validate token, if token is validated, user is authenticated.
        - If user device is not set as trusted, invoke method "verifyFingerPrintForUserName" to authenticate user by scanning finger prints.

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com



Authenticate with fingerprint

A normal iOS app with insecure single factor (password only) based access, and one enabled with AllWebID 2FA solution are illustrated in figures 1 and 2.

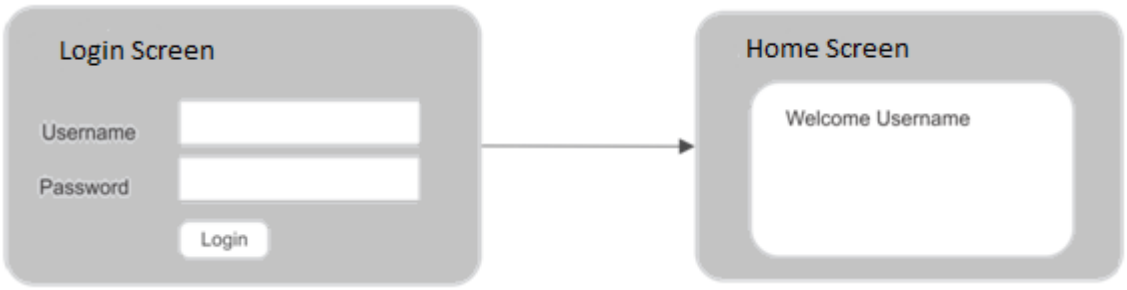


Figure 1: Normal iOS app operation without AllWebID2FA

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

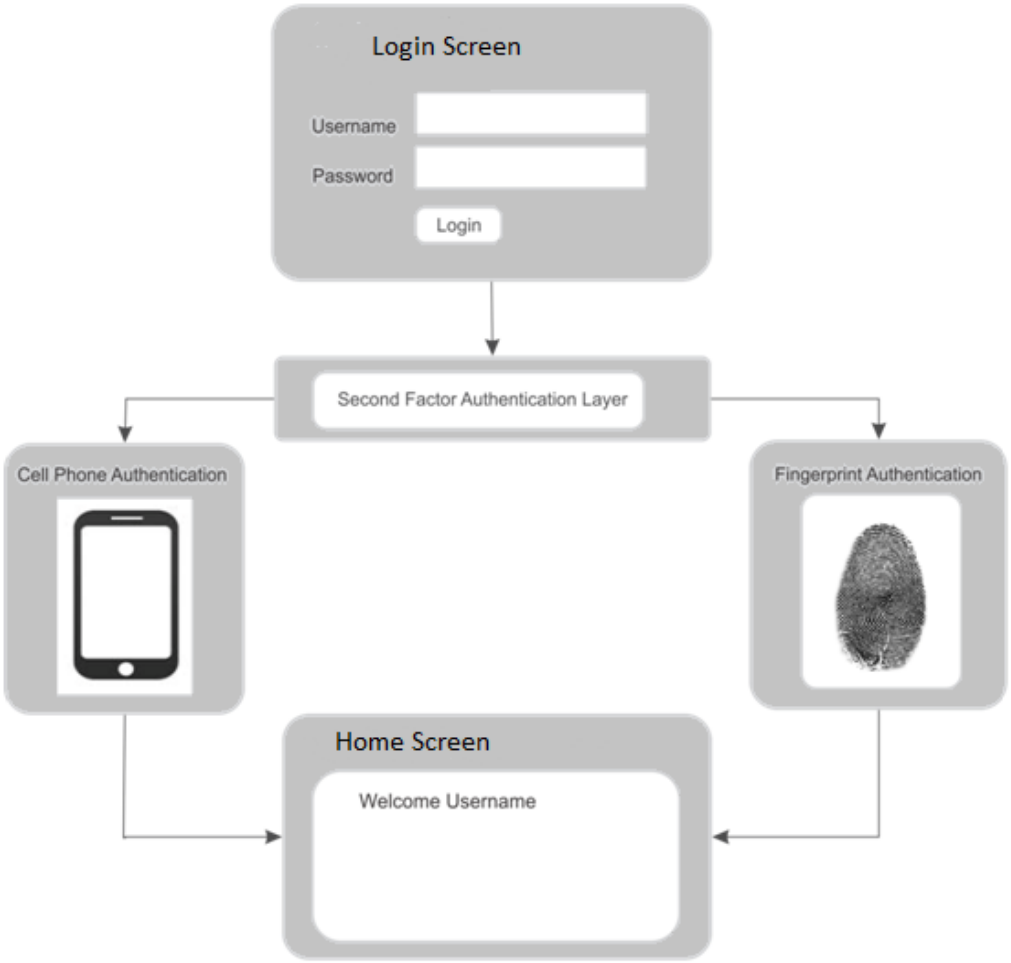


Figure 2: iOS app login process with AllWebID2FA

How does iOS SDK work?

As part of the deployment, your iOS App is integrated with SDK,which communicates withAllWebIDservers for second factor authentication. You will continue to manage your end users' passwords without disclosing them to AllWebID. The whole setup of adding 2FA is done by integrating the AllWebIDIdentity Manager API SDK, along with some relevant changes to your appuserinterface. The deployment is illustrated in figure 3.

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

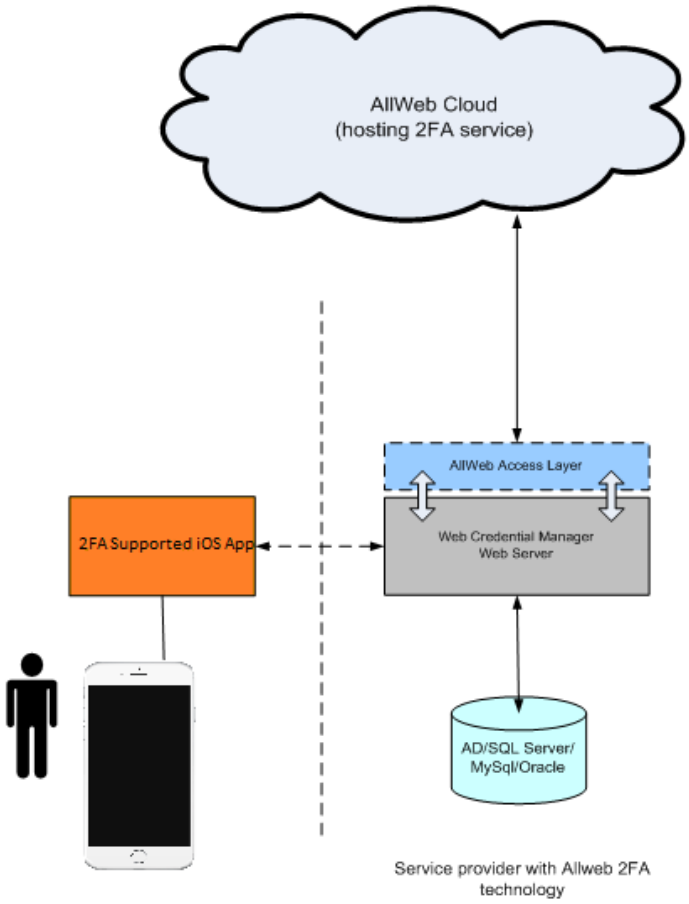


Figure 3: Allweb enabled 2FA eco-system

Integration of iOS SDK and API method list

- Include AllWebId2FAService.framework file into your xCode project.
- Import AllWebId2FAService.h in header of class where you want to call API methods like #import<AllWebId2FAService/AllWebId2FAService.h>
- Create property of AllWebId2FAService class in header like
- @property(nonatomic, strong) AllWebId2FAService *secondFAService;
- Update your header file interface like this
- @interface yourViewController : ParentViewController<AllWebId2FAServiceDelegate>

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

- In .m file of your class, write following code in viewDidLoad method _second2FAService =[[AllWebIdService2FAService alloc] init];
- _second2 FAService.delegate = self;
- Call any API method on _second2FAService object and it will return you result in its respective delegate method.

List of API methods and their respective delegates is given in below Table 1a.

API Function	Parameters	Response	Delegate Method
getSecondFactorAuthenticationStatusWithUserName	username:NSString, apiKey:NSString	success/fail, SMS/FP/Disabled/None	delegate_SecondFactorAuthenticationStatusReceived
sendPinBySmsForLoginAuthenticationWithUserName	username:NSString, apiKey:NSString	success/fail	delegate_PinSentBySMSForLoginAuthentication
verifySMSPinForLoginAuthenticationWithUserName	username : NSString, pinCode : NSString, apiKey : NSString	success/fail	delegate_SMSPinVerifiedForLoginAuthentication
registerFingerPrintForUserName	username : NSString, deviceID : NSString, apiKey : NSString	success/fail	delegate_FingerPrintRegistered
setDeviceTrustedAndGetTokenForDeviceID	username : NSString, deviceID : NSString, apiKey : NSString	True/False/Token	delegate_DeviceSetTrustedAndTokenReveived
enableDisableUserTrustedDeviceWithUserName	username : NSString isEnabled : BOOL apiKey : NSString	True/False/Token	delegate_UserTrustedDeviceEnabledOrDisabled
deleteUserDeviceWithUserName	username : NSString, deviceID : NSString, apiKey : NSString	success/fail	delegate_UserDeviceDeleted
deactivateSecondFactorAuthenticationWithUserName	username : NSString, apiKey : NSString	success/fail	delegate_SecondFactorAuthenticationDeactivated
sendPinBySmsToRegisterWithUserName	username : NSString, cellNumber : NSString, apiKey : NSString	success/fail	delegate_PinSentBySMSToRegister
verifySMSPinToRegisterWithUserName	username : NSString, pinCode : NSString, apiKey : NSString	success/fail	delegate_PinVerifiedBySMSToRegister
registerUserOnAllWebWithUserName	username : NSString, secondFactorMode : NSString	success/fail	delegate_UserRegisteredOnAllWeb

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

	secondFactorStatus : BOOL cellNumber : NSString apiKey : NSString		
activateSecondFactorAuthenticationWithUserName	username : NSString, mode : NSString, apiKey : NSString	success/fail	delegate_SecondFactorAthenticationActivated
checkIfDeviceIsUserTrustedWithUserName	username : NSString, apiKey : NSString	True/False	delegate_UserTrustedDeviceStatusChecked
validateTrustedDeviceTokenWithUserName	username : NSString, token : NSString, deviceID : NSString, apiKey : NSString	True/False	delegate_TrustedDeviceTokenValidated
verifyFingerPrintForUserName	username : NSString, deviceID : NSString, apiKey : NSString	success/fail, error	delegate_FingerPringVerified
getApiKey	-	success/fail, ApiKey	delegate_APIKeyreceived
checkDeviceIsRegisteredWithUserName	username : NSString, deviceID : NSString, apiKey : NSString	success/fail	delegate_UserRegistrationWihDeviceChecked
Destroy	-	-	-
getUserPhoneNumberWithUserName	username : NSString, apiKey : NSString	success/fail, phoneNumber	delegate_UserPoneNumbereReceived
verifyOOBPin	pin : NSString username : NSString apiKey : NSString	Success/ fail	Delegate_OOBPinVerified

Table 1a: Integration Steps and List of APIs used to integrate AllWebID 2FA solution

API Function	Description
getSecondFactorAuthenticationStatusWithUserName	To get user's second factor authentication status i.e. enabled, SMS, FP
sendPinBySmsForLoginAuthenticationWithUserName	To send pin on user's registered cell phone number for login authentication via SMS.
verifySMSPinForLoginAuthenticationWithUserName	To verify if pin entered by user for login authentication is correct or incorrect.
registerFingerPrintForUserName	To register user's finger print and device for login authentication for user registered on AllWebID.
setDeviceTrustedAndGetTokenForDeviceD	To make user's device trusted, so that token is used to authenticate user instead of user's finger print. To make device trusted, user must enable finger print authentication first.

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

enableDisableUserTrustedDeviceWithUserName	To enable or disable user's trusted device.
deleteUserDeviceWithUserName	To deactivate login authentication via finger print.
deactivateSecondFactorAuthenticationWithUserName	To disable second factor authentication feature provided by framework.
sendPinBySmsToRegisterWithUserName	Send pin on user's provided cell number while user registration with AllWebID.
verifySMSPinToRegisterWithUserName	Verify pin entered by user while registering on AllWebID is correct or incorrect.
registerUserOnAllWebWithUserName	Register user on AllWebID.
activateSecondFactorAuthenticationWithUserName	Activate second factor authentication.
checkIfDeviceIsUserTrustedWithUserName	To check if user has made device trusted.
validateTrustedDeviceTokenWithUserName	Validate token for user trusted device for login authentication with token instead of user's finger print.
verifyFingerPrintForUserName	For login authentication via finger print.
getApiKey	To get API key.
checkDeviceIsRegisteredWithUserName	To check if user has registered device/ his finger prints on AllWebID.
destroy	Call destroy method when AllWebIf2FAService object is no more needed.
getUserPhoneNumberWithUserName	To get user's registered phone number on AllWebID.
verifyOOBPin	To verify pin/ passcode entered by user for authenticaion

Table 1b: Integration Steps and List of APIs used to integrate AllWebID 2FA solution

Parameter	Description
deviceID	Unique hardware ID of device where application is installed.
apiKey	API key is an Integration key which an integrator can get for creating integration
userName	Username(Email used to login) of the user using AllWebID 2FA service
cellNumber	Cell phone number of the user of using AllWebID 2FA service
secondFactorMode	Defines 2nd factor authentication mode: • SMS

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

	• SMS+ Fingerprint
secondFactorStatus	Defines 2nd factor authentication status: • True • False
pinCode	PIN code entered by the user/ sent to user on his mobile phone
Token	An identifier to keep track of the trusted device

Table 2: List of parameters and their description

Data parameters shared between AllWebID Cloud &ClientCredential Manager:

Below are scenarios and data parameters in which data will be gathered and shared by Client Credential Manager withAllWebIDCloud.

1. User enrollment for 2FA:

When a user enrolls for 2FA, following parametersaregathered and communicated tothe AllWebID cloud by App Credential Manager.

1. User's email address
2. 2FA status
3. 2FA mode
4. Cell number

2. Login through 2FA:

When a user logs into anapp integrated with AllWebID 2FA solution, a token is generated and shared between AppCredential Manager and AllWebID Cloud to keep track of the authentication process.

API Methods Response

Response	Description
True/ successful	API Call successful or input return result is true

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com

False / fail	Input result is false
ERROR_CODE_100	Authorization failed
ERROR_CODE_101	Empty value
ERROR_CODE_103	Website disabled
ERROR_CODE_104	User not found
ERROR_CODE_105	Data expired
ERROR_CODE_106	Network error
ERROR_CODE_107	Fingerprint initialization failed
ERROR_CODE_200	Server Not Responding
ERROR_CODE_201	Invalid Result

Please contact us if you have any questions.

Email: support@allwebid.com

Website: http://allwebid.com/IdentityManagerFAQs.aspx

Allweb Technologies Inc.
211 Warren Street, Suite 1019, Newark, NJ 07103, USA
Ph: +1 908 333 3447
e-mail: sales@allwebtechnologies.com