Q. Who can avail Mobile OTP as second factor of authentication?

Any internet banking user can avail Mobile OTP as second factor of authentication.

Q. What User has to do once he has opted for Mobile OTP?

User has to download **ArcotID OTP** application from his mobile App. Store or download desktop version of application if your mobile OS is not supported. After installing the application, user has to add account in it by using provisioning details sent on his registered mobile number. Desktop version of application is available at our website i.e. www.unionbankonline.co.in.

Q. Can I have Software token and Mobile OTP simultaneously?

Yes. Retail Internet banking users can have Software token and Mobile OTP simultaneously.

Q. Can I have Hardware token and Mobile OTP simultaneously?

Yes. Corporate Internet banking users can have Hardware token and Mobile OTP simultaneously.

Q. What if Software token is locked and Mobile OTP is active?

If Software token is locked, Mobile OTP will also get locked and vice-versa. Please contact our customer care number i.e. 1800222244 to get your account unlocked.

Q. What if Hardware token is locked and Mobile OTP is active?

If Hardware token is locked, Mobile OTP will remain active and vice-versa. Please contact our customer care number i.e. 1800222244 to get your account unlocked.

Q. What if I delete my account from Mobile/Desktop Application?

Once you delete your account from Mobile/Desktop Application, you can add your account any time. For that we have provided links to resend provisioning details again.

Q. Whether I have to set Secured PIN separately for Software Token and Mobile/Desktop Application?

No. PIN set for Software Token will work as PIN for Mobile/Desktop Application and vice-versa.

Q. If I change Secured PIN for Software Token, will the new PIN work for Mobile/Desktop Application?

No. User has to delete the account from Mobile/Desktop Application and add it again. For that user has to resend provisioning details by clicking the links provided.

Q. How a retail / corporate user can add account in Mobile/Desktop Application?

When a retail user opts for Mobile OTP, he will receive provisioning details on his registered mobile number. Provisioning details have Server URL, User ID and Activation Code values. User has to install Mobile/Desktop Application and add an account by using these details. Corporate users have to enter CorporateID-UserID as their user ID value. Life of Activation Code is of 3 minutes. A user guide has been provided on our website for that.

Q. On which platforms Mobile/Desktop Application is supported?

Mobile/Desktop Application is supported on most of the platforms available these days. A compatibility matrix is provided at our web site for that.

Q. What is the minimum and maximum length for PIN?

For PIN minimum length is one character and maximum length is 32 characters. PIN can be numeric, alphabets or combination of alphabets and numeric characters. Keep PIN strong enough so that no one can guess it easily.

Q. What if user machine is crashed or formatted?

If a user machine is crashed or formatted then user has to install and add account in a fresh application. To resend provisioning details links have been provided at appropriate places.

Q. What if a user's Mobile is lost or stolen?

If user's mobile is lost or stolen then user can install application and add account on new mobile or desktop. If stolen mobile comes into the possession of someone then correct OTPs can't be generate until correct PIN is provided. To resend provisioning details links have been provided at appropriate places.

Q. Can we add multiple accounts in same mobile/desktop application?

Yes. Multiple accounts can be added in the same mobile/desktop application.

Q. Does user require having internet connection while installing or using Mobile/Desktop application?

Internet connection is required while installing and adding the account in the application. After this activity no internet connection is required.

Q. How Secure is Mobile OTP solution as second factor of authentication?

Mobile OTP is quite secure. The keys are generated randomly and are protected by patented cryptographic camouflage technology. So no one will be able to guess any patterns.

Q. Does user need any extra security measures with ArcotID OTP application?

ArcotID OTP application is secured in itself as the seed is encrypted and protected by our patented technology. But for more security, it is recommended to download application only from app stores like Google Play, Apple Store etc and also recommends user have latest anti-virus and anti-malware installed on their mobile devices. Other applicable good practices like locking the smartphone with password are always good to follow.