FAQs – Entersekt Multi-factor Authentication Digital Banking

1. What is multi-factor authentication?

Multi-factor authentication is a concept used in the security industry to establish the identity of a user by requiring the user to present three identifying factors:

1. Knowledge factor — something that the user knows such as a username and password.

2. Possession factor — something that the user has such as a token or mobile device (e.g. mobile phone or tablet) that may be used to generate a one-time password.

3. Inherence factor – something that the user is, such as a fingerprint or face scan, confirming the identity of the user

By presenting these factors, the receiver of the information can have a high level of confidence that the user is in fact who he or she claims to be because the probability that someone else would be able to present both factors is very small.

2. What is evolved authentication and push notifications?

Enhanced multi-factor authentication security technology enabling you to authenticate your Internet banking transactions in real-time using your mobile device by means of a simple accept or reject response to an authentication request.

We will replace the current one-time password (OTP) system. In future, when you perform a high-risk Internet banking transaction, you will receive an interactive pop-up message on your banking application on your mobile device providing the details of the transaction and requesting you to click either Accept or Reject the transaction. This is called a Push notification request. If a transaction is not legitimate, you can simply reject it by clicking the Reject button displayed in the authentication request and the transaction will not be processed, stopping the attempted fraud in its tracks. Please make sure your push notifications are enabled for your banking app. Push notifications are important because it gives you full overview and control of all transactions on your account.

3. What is biometric authentication?

Biometric authentication is a security process that relies on the unique biological characteristics of individuals to verify they are who they say they are. Biometric authentication systems compare physical traits to stored, confirmed, authentic data in a database. If both samples of the biometric data match, authentication is confirmed. The advantages of biometric authentication are its convenience and security. Since biometric authentication uses unique characteristics for verification, they are difficult to replicate. Traditional methods, such as usernames, passwords or ID cards, are not as secure because they can be stolen or guessed easily.

For this new way of authentication, enabling biometrics is not mandatory, but it is recommended for a better user experience.

4. What is out-of-band?

Out-of-band authentication is a type of two-factor authentication that requires a secondary verification method through a separate communication channel along with the typical ID and password. Out-of-band authentication is often used in financial institutions and other organizations with high security requirements. Out-of-band helps improve cybersecurity because it makes hacking an account more difficult due to two separate and unconnected authentication channels that would need to be simultaneously compromised for an attacker to gain access. This new authentication utilizes out-of-band authentication via a push notification.

5. Why were one-time passwords replaced?

The new method provides a much more secure means of authentication because it allows you to accept or reject transactions directly via your mobile phone — you, as the account owner, remain firmly in control of every high-risk transaction because you accept or reject each transaction on your phone before the transaction is processed. Whenever a high-risk Internet banking transaction is being performed, you will receive a pop-up message on your banking application on your mobile device (push notification authentication request). This message will contain the details of the transaction being attempted and will allow you to choose whether to continue with the transaction or stop it. Because your response to the authentication request is sent to the Credit Union using a separate mutually encrypted connection directly between your mobile device and the Credit Union, instead of an OTP code being entered on your computer (where phishing and other cyber-attacks may get a hold of it), phishing and other cyber-attacks are prevented.

6. What are the risks associated with using one-time passwords?

One-time passwords (OTPs) can be intercepted by fraudsters employing cyber-attack techniques referred to as “phishing” or “man-in-the-middle”. Fraudsters lure unsuspecting users into entering their Internet banking credentials (username and password) on a site that mimics the real banking site. The unsuspecting user, seeing the familiar visual layout of the banking site, enters his or her login information on this fraudulent site, effectively giving it to the fraudster. The fraudster relays the captured information to the real banking site in real-time. This results in the user receiving an OTP on their mobile device. The fraudster then mimics the real Credit Union by asking the user to enter the OTP on the fraudulent site. Since the unsuspecting user again enters this OTP on the fraudulent site, the fraudster now has everything he needs.

At this point the fraudster has the power to do what he wants on the Internet banking site without any further user interaction. By the time the user realizes what has happened, the fraudster has already cleared out the bank account. Because we make use of the separate mutually encrypted connection directly between the bank and the user’s mobile device to send the Authentication Requests and responses to it, it does not require any information to be retyped on your computer, and thus the fraudulent site never gets all the information required to transact on behalf of the user, which means your account is safe.

7. What is considered a high-risk transaction?

Each Credit Union has a different definition of which transactions are considered high risk but the following are considered high risk by most banks:

- One-time payments

- Recurring payments
- Future-dated purchases
- Prepaid purchases
- Adding beneficiaries

Most banks will require two-factor or multi-factor authentication if you initiate one of these transactions.

8. Will this authentication work on my phone or tablet?

The app is available for all devices running iOS (iPhones and iPads), BlackBerry, Android, and Windows Phone operating systems. There is also a version of the application that runs on most feature phones. If your phone has a color screen, a browser, and can run common applications (e.g. Mxit or Facebook), it should be able to support the authentication.

9. Will I still be able to perform online banking if I do not have my mobile device with me?

Authentication is required only for high-risk transactions. If you do not have your mobile device with you, you will still be able to perform transactions that are not considered to be high-risk transactions.

10. If I perform bundled payments, will I have to authenticate each of the payments?

When performing multiple or bundled payments, you will receive only one message for authenticating the bundled transaction. The message will contain a figure showing the total value of the bundled transactions and the number of transactions being performed. You then have the choice to either accept or reject the bundled payment.

11. Will it cost me money to authenticate?

The only costs associated with using are for the GPRS, EDGE, 3G or Wi-Fi data transmitted. These costs will depend on what data package you have with your mobile operator or Internet service provider, but the authentication messages are small (roughly 1KB per message), which should be negligible in terms of data costs.

12. Will the authentication still work when I travel abroad?

If you travel abroad, the authentication will work wherever you have Wi-Fi Internet connectivity. It will also work if you have roaming data connectivity (GPRS, EDGE, 3G etc.) but you may incur roaming data charges when authenticating in this case, even though it uses a very small amount of data.

If you have no Internet connectivity, your bank will fall back to requesting you to enter an OTP in order to transact. The application has the built-in functionality to generate an OTP on the device when it has no mobile communication.

13. How long does it take on average for a message to appear?

Authentication request messages should appear on your mobile device within 5 to 10 seconds (on average) if the application is not open and has to be woken up. If the application is already open, the authentication request message should appear almost instantaneously. Traffic on the mobile network

may affect the time that it takes for the message to appear on your mobile phone. The quality of coverage that your mobile operator provides in your location may also impact delivery times.

If messages do consistently take too long to reach your mobile phone, you should contact your bank's call center for assistance.

14. What does it mean when a message times out on my mobile phone?

A timeout occurs when the authentication request message takes longer to reach your mobile device than the Credit Union allows for you to respond to the message, or if you take longer to respond to a message received on your phone than the bank allows for the response.

If this happens, click the Resend button (this will be implementation specific) on the Internet banking screen on your computer to send another message. If timeouts occur repeatedly, contact your bank's call center for assistance.

15. What happens if I end a call on my mobile phone while an authentication request message is on my phone?

If you press the cancel (red) button to end a call while an authentication request message is displayed on your mobile device, the system will recognize that you cancelled the authentication request message. A message will appear on your Internet banking screen informing you that the transaction was cancelled via your mobile device. The Internet banking screen will then prompt you to click either the Resend or Cancel buttons on screen.

16. What should I do if I receive an authentication request message when I did not initiate the transaction?

If you receive an authentication request message for a high-risk transaction on your account that you did not initiate, you should click the Reject button to reject the transaction. This will prevent the transaction from being processed. It is also advisable to inform the bank of the situation so that they can immediately take action to stop the fraudster from attempting the same thing again.

17. How do I manage my devices?

With this new way of authenticating, devices can be added to your account and identified as a 'trusted device'. All authentication requests will then be routed to this trusted device to approve – this creates a trusted environment which increases safety without increasing friction.

To register a trusted device:

- First time: automatic registration takes place which will give you the option to also enable your biometrics on your trusted device if the device has biometric capabilities.

- Adding additional devices: go to settings > device list > add a new device > follow the easy prompts to identify and register another device to be linked to your account. If the device has the capabilities, you will again be to activate the biometrics if you wish to.

- 18. What should I do if I lose my device?

- You can call your Credit Union call center who will be able to manually remove the device in question from your trusted devices list to ensure no fraudulent activity can take place.