January 2015

CitiDirect BE℠ Mobile Security

Frequently Asked Questions

1. Device and Application Security

1.1. Does a Mobile Phone require any software installation to run CitiDirect BE℠ Mobile?

No. CitiDirect BE Mobile is a mobile web application. This means that it is run within the device's Internet browser. It does not require the installation of any third-party software such as Java, Active-X, Flash, or any mobile phone specific installation.

1.2. Does CitiDirect BE Mobile save any data on the mobile device either via private storage or cookie?

No. CitiDirect BE Mobile is a server-side web application where it does not require to store any data on the mobile device or browser cache. Only an obfuscated cookie is used as a session token.

1.3 Does CitiDirect BE Mobile display all digits of the client account number as well as the beneficiary's account number?

Yes. Since CitiDirect BE Mobile is simply another channel to CitiDirect and uses the same secure Safeword card challenge/response system, users can view complete account numbers on the application. This ensures a seamless, consistent user experience across CitiDirect and CitiDirect BE Mobile.

1.4. Does CitiDirect BE Mobile have automatic timeout on the client's browser? If so, is it configurable?

Yes. CitiDirect BE Mobile has a five-minute inactivity timeout which is not configurable for clients.

1.5. Does the timeout synchronize with mobile phone screen lock?

No. It does not synchronize with the mobile phone screen lock settings.

1.6. If the mobile phone was stolen, for example, how will CitiDirect BE Mobile protect access to private information?

Since CitiDirect BE Mobile is a 100% server-side web application, it does not leave any footprint containing PII data of the client. Therefore even under an extreme circumstance like this, client information will not be visible. And moreover, even if the CitiDirect BE Mobile URL was hit by the thief, the multifactor login using external Safeword card will prohibit any mal-intent penetration to the solution.

1.7. Does any mobile phone virus or spyware impact the security of CitiDirect BE Mobile?

The risk is relatively small. Since CitiDirect BE Mobile is a browser-based thin-client web solution protected by a multifactor authorization (i.e., SafeWord) system, the application is secure to external attacks – including those originating from a virus or spyware on the client's mobile phone.

2. Mobile Phone Security

2.1. How is my mobile phone protected when using CitiDirect BE Mobile?

While Citi takes steps to protect the application, it is, however, the client's responsibility that the mobile device is protected from device-level viruses. We recommend the client take precautions to ensure appropriate security components are installed (e.g., anti-virus).

2.2. What are the OS, Browser, HTML, Javascript that CitiDirect BE Mobile supports at a minimum?

To use the application the phone's browser must, at a minimum, support XHTML-MP 1.0, JavaScript 1.5, CSS-MP 1.0 and allow cookies to set. These are standard client-side restrictions for secure Internet browsing.

2.3. Must a user use any corporate device? If not, can any personal device be used?

No. CitiDirect BE Mobile is a device-agnostic solution. Therefore, any corporate or personal devices can access CitiDirect BE Mobile as long as the mobile device meets the minimum requirements described in 2.2.

3. User Authentication and Entitlement

3.1. How does a user of CitiDirect get authenticated into CitiDirect BE Mobile?

A user of CitiDirect first needs to have a valid Citi-issued safeword card. After the user is entitled to have mobile access via the CitiDirect security manager function, then a user can be authenticated via CitiDirect BE Mobile using the same safeword card credentials. For security manager setup, please refer to the user guide.

3.2. How is the trustworthy authentication process organized?

CitiDirect BE Mobile provides a defensive, in-depth approach using multifactors. CitiDirect BE Mobile will extend the current security enablement with your existing Safeword card challenge/response system. By doing so, Citi will authenticate and authorize the user based on the very secure entitlement engine that CitiDirect currently employs. You will receive the benefit of this security feature by making sure that the person who is making the authorization has full responsibility of his/her actions while using a mobile device. Identical authentication mechanism is used by the desktop application, CitiDirect.

3.3. Must a user carry a separate safeword card to authenticate into CitiDirect BE Mobile?

Yes. Citi is investigating options for potential improvement of convenience under the strict guidance of corporate security officers – however, the SafeWord card is a secure, independent mechanism for secure access.

3.4. Can a user authenticate simultaneously into CitiDirect BE Mobile as well as CitiDirect?

Yes. As a result, the data displayed should be consistent. However, it does not share any pending state of data between multiple sessions.

3.5. Does a user inherit the same entitlement of CitiDirect?	Yes. Existing entitlement by CitiDirect is inherent to CitiDirect BE Mobile.
3.6. What are the different entitlement categories specific to CitiDirect BE Mobile only?	E-mail and SMS notification are unique to CitiDirect BE Mobile. Therefore, the security manager must set this up after giving mobile access to a user. For more information, please refer to the user guide.
3.7. Does CitiDirect BE Mobile display any failed login attempt?	Yes. CitiDirect BE Mobile displays # of failed login attempts at the main screen once correctly authenticated.
3.8. Does CitiDirect BE Mobile only show any accounts or transactions that a user is entitled to view?	Yes. Any accounts and transactions display is driven by the existing CitiDirect entitlement.

4. Network & Mobile Server Security

4.1. What is the encryption that CitiDirect BE Mobile supports?	CitiDirect BE Mobile only works under TLS with 128-bit RSA encryption model supported by most standard browsers of the mobile phones. For compatibility of your browser, please refer to your phone manufacturer's guide.
4.2. Can a user use any public WiFi or any public 3G network to access CitiDirect BE Mobile? If so, does it require a different security implementation?	Yes. A user of CitiDirect BE Mobile can use public WiFi or any 2G/3G/LTE network to access CitiDirect BE Mobile. It does not require any additional security implementation. CitiDirect BE Mobile will not be different from your connection on a laptop. It is the client's responsibility to protect their mobile device. The Citi Information Security Officer recommends any personal protection software that is suited for mobile phones.
4.3. Does CitiDirect BE Mobile use any public "Cloud" technology?	No. CitiDirect BE Mobile does not use any public or private "Cloud" technology to store client's data, both temporary and permanent.
4.4. Where is the CitiDirect BE Mobile server located?	The CitiDirect BE Mobile server is located in the PCI-compliant Citi data center in the United States. It is where the CitiDirect server is located.
4.5. How does monitoring and auditing take place on CitiDirect BE Mobile transactions?	Since CitiDirect BE Mobile is only a channel to CitiDirect, all existing monitoring and auditing is applicable to CitiDirect BE Mobile transactions and activities.

4.6. Does CitiDirect BE Mobile produce separate transaction reporting?

No. Since CitiDirect BE Mobile is only a mobile channel to CitiDirect, all reporting functionality remains with CitiDirect. Any authorizations performed via CitiDirect BE Mobile will be reported as "Mobile-Authorize" in the transaction report of CitiDirect.

5. Regulatory Approval

5.1 Does CitiDirect BE Mobile require separate internal/external approval for the client to start using it?

No. Since CitiDirect BE Mobile is only a mobile channel to CitiDirect, all security settings remain true from CitiDirect, meaning no separate approval is needed. However, we do recommend for client security officers to review.

5.2. What are the security and compliance reviews performed on this application?

The CitiDirect BE Mobile application has undergone and passed third-party Vulnerability Assessment testing.

5.3. What are the names of all countries where CitiDirect BE Mobile is approved?

Legal and Compliance teams on Regional, Country and Local levels were involved in a review that was carried out for each of the 91 countries where CitiDirect BE Mobile solution is live.

The countries that have gone live are: Algeria, Argentina, Australia, Austria, Bahamas, Bahrain, Bangladesh, Barbados, Belgium, Bolivia, Brazil, Bulgaria, Cameroon, Canada, Channel Islands, Chile, China, Colombia, Costa Rica, Cote d'Ivoire, Czech Republic, Democratic Republic of Congo, Denmark, Dominican Republic, Ecuador, El Salvador, Finland, France, Gabon, Germany, Greece, Guatemala, Haiti, Honduras, Hong Kong, Hungary, India, Indonesia, Ireland, Israel, Italy, Jamaica, Japan, Jordan, Kazakhstan, Kenya, Kuwait, Lebanon, Luxembourg, Malaysia, Mexico, Morocco, Netherlands, New Zealand, Nigeria, Norway, Pakistan, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Puerto Rico, Qatar, Romania, Russia, Senegal, Singapore, Slovakia, South Africa, Spain, Sri Lanka, Sweden, Switzerland, Taiwan, Tanzania, Thailand, Trinidad & Tobago, Tunisia, Turkey, Uganda, Ukraine, United Arab Emirates, United Kingdom, United States of America, Uruguay, Venezuela, Vietnam and Zambia.

5.4. Does a user need to accept any specific disclosure statement to be able to use CitiDirect BE Mobile?

Generally, current account conditions of CitiDirect cover the usage of CitiDirect BE Mobile except SMS notification. CitiDirect BE Mobile asks a user to accept an independent disclosure statement for SMS notification. However, each country may have their own specific agreement that the client must accept. For details, please check with your Citi representative. For the actual disclosure statement, please refer to the user guide.

5.5. Is there a limit on the amount to be authorized via CitiDirect BE Mobile?

No. There is no limit on the amount for transactions to be authorized via CitiDirect BE Mobile.

1281070 GTS05979 01/15