



Digipass for Mobile C4C User Guide

Version 2.0

21 Nov 2014

Table of Contents

1 Document Control.....	3
1.1 Amendment Record.....	3
2 Introduction	3
3 Software Digipass Activation.....	4
3.1 Software Digipass Type.....	4
3.2 Pre-requisites.....	4
3.3 Digipass for Mobile	5
3.3.1 Installation and Activation	5
3.3.2 How to Use Digipass for Mobile	5
3.4 Lost/Faulty Digipass	7
3.5 Common Error Messages.....	7
Glossary	10

1 Document Control

1.1 Amendment Record

Version	Date	Status	Author	Comment
0.1	27-10-2014	Draft	Goh Cheng Sze	Initial Draft
2.0	20-11-2014	Draft	Kylie Wong	Changes made to cater for C4C service

2 Introduction

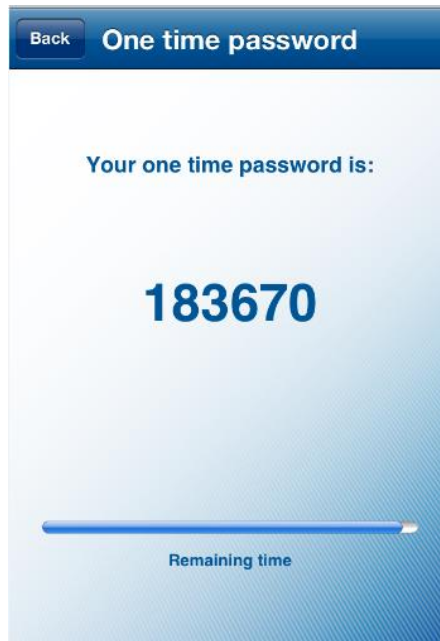
This document contains information for users on how to use the VASCO software digipass which provide 2-factor authentication to the Identikey Server.

2-factor authentication is a security process in which the user provides two means of identification, one of which is typically a digipass, and the other typically something memorised, such as a security PIN. In short, it is commonly spoken of as *something you have* and *something you know*.

To achieve this goal, users will need to have a digipass to be able to log on the services using 2-factor authentication.

A digipass is a device that provides a One Time Password (OTP) to a user for logging into the secure system. This document focuses on Digipass of Mobile, a type of Vasco digipass used in the Shell environment all of which can be ordered from [MyRequest](#):

- a. **Digipass for Mobile** - software digipass installed onto a user's mobile phone that runs on selected operating systems, such as iOS, Android, Blackberry and Windows. A user accesses the Digipass for Mobile application to obtain a six-digit OTP, as shown below:



3 Software Digipass Activation

Note: This Section is only applicable for users who are ordering a software digipass.

3.1 Software Digipass Type

A software digipass is an application installed onto a Microsoft Windows-based client machine, iOS, Android, Blackberry or Windows mobile devices. A user accesses the software digipass application to generate an OTP in the same way as a physical hardware digipass device. Digipass for Mobile are one types of software digipass available within Shell:

Digipass for Mobile is supported by selected mobile platforms as follow:

- iPhone and iPod Touch (iOS version 4.1 and later)
- Android OS version 2.2 and later
- BlackBerry device (OS version 5.0 and later)
- Windows Mobile 6.x

3.2 Pre-requisites

To use a software digipass, you first need to install and activate your digipass on a supported client device before you can use it to generate an OTP. Please note:

- the client device must be running on a supported platform as stated in [Section 3.1](#)
- the client device must be connected to the Internet to be able to download the required software to the client device
- the user must have the administrator rights to install the software on the client device
- the user must have obtained all relevant details about the software digipass. If you have not receive any software digipass details, you may contact your Shell focal point or place an order yourself in [MyRequest](#).

Note: The software digipass details will be protected with password using Winzip application and send in email to you. The password to un-zip the software digipass details will be sent to you in the second email. You must have Winzip application to un-zip the software digipass details using the password in the second email.

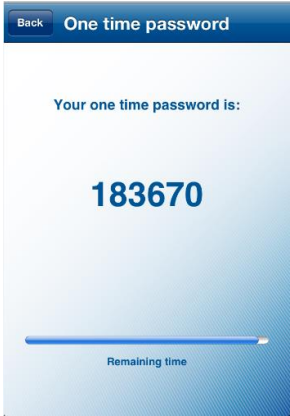
3.3 Digipass for Mobile

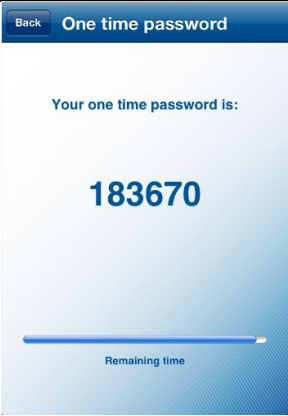
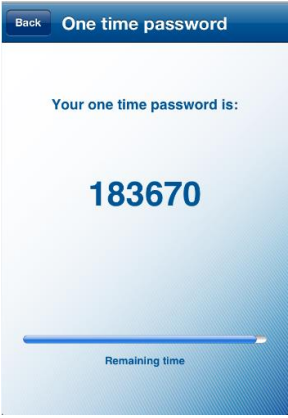
3.3.1 Installation and Activation

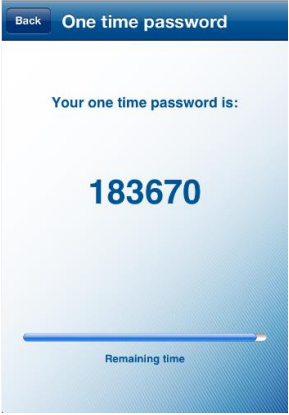
Follow these steps to perform the Digipass for Mobile installation and activation:

1. For an iOS platform mobile device, download and install **DIGIPASS for Mobile Enterprise Security** (version 4.x) from AppStore.
2. For Android platform mobile devices, download and install **DIGIPASS for Mobile Enterprise Security** (version 4.x) from PlayStore.
3. For BlackBerry platform mobile devices, download and install **DIGIPASS for Mobile Enterprise Security** (version 4.x) from App World.
4. For Windows platform mobile devices, download and install **DIGIPASS for Mobile Enterprise Security** (version 4.x) from the Windows Mobile Download Center.
5. Select **Manual Activation** mode.
6. You will be prompted for your Serial Number and a 20-digit Activation Code of the digipass. The Serial Number refers to the last 7 digits of a 10-alphanumeric digipass serial number that has been assigned to you. For example, enter 0134950 into the Serial Number field if you have been assigned with the digipass serial number VES0134950.
7. An One Time Password will be generated if Digipass for Mobile is activated successfully.

3.3.2 How to Use Digipass for Mobile

<p>How do I generate a new One Time Password (OTP) after activation?</p>	<ol style="list-style-type: none"> 1. Tap the Digipass for Mobile Enterprise Security application on your mobile device. 2. The OTP will be displayed on the screen, for example: 
<p>How do I re-synchronize my Digipass for Mobile if I have any concerns with my mobile device's date/time configuration?</p>	<ol style="list-style-type: none"> 1. Tap the Digipass for Mobile Enterprise Security application on your mobile device. 2. The OTP will be displayed on the screen, for example:

	 <ol style="list-style-type: none"> 3. Tap the Back button on the screen. 4. Tap the Settings button on the screen. 5. To synchronize your Digipass for Mobile date time settings, select Automatic time synchronization. If you prefer to set the date/time manually, then select Manual time synchronization. Enter the current date and time based on GMT, tap OK button to update the date/time settings.
<p>How do I view my digipass information (i.e. my digipass serial number and time data)?</p>	<ol style="list-style-type: none"> 1. Tap the Digipass for Mobile Enterprise Security application on your mobile device. 2. The OTP will be displayed on the screen, for example:  3. Tap the Back button on the screen. 4. Tap the Settings button on the screen. 5. To view your digipass information, tap the DIGIPASS Information button.
<p>How do I view my digipass' provider information (i.e. Digipass for Mobile software version details)?</p>	<ol style="list-style-type: none"> 1. Tap the Digipass for Mobile Enterprise Security application on your mobile device. 2. The OTP will be displayed on the screen, for example:

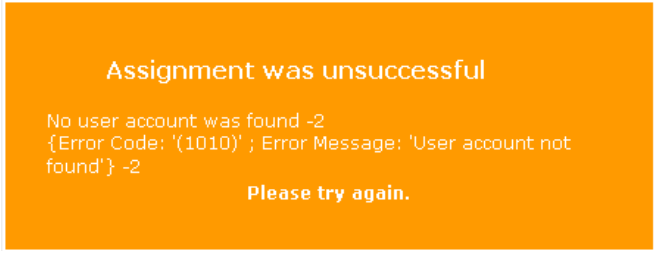
	 <p>3. Tap the Back button on the screen.</p> <p>4. Tap the Settings button on the screen.</p> <p>5. To view your digipass' provider information, tap the Provider Information button.</p>
<p>How do I re-activate my digipass if the Digipass for Mobile software is uninstalled or crashed on my mobile device?</p>	<ol style="list-style-type: none"> 1. Un-install the Digipass for Mobile Enterprise Security from your mobile device. 2. Repeat the steps in Section 3.4.1 to activate the digipass on your mobile device.

3.4 Lost/Faulty Digipass

If you lose or damage your digipass, you must request a replacement yourself or from your Shell focal point. Until the replacement arrives, request a Windows Password every seven days from your Shell focal point/Helpdesk.

1. Follow the procedure in the [Section 3.3.1](#) to install/activate the digipass for mobile.

3.5 Common Error Messages

Error Message	Reason	Action Required
<p>No user account was found -2</p> 	<p>You have mistyped your User Name.</p>	<p>Re-type your User Name.</p>
<p>No DIGIPASS was found for the given Serial Number -2</p>	<p>You have mistyped the digipass Serial Number.</p>	<p>Re-type your digipass Serial Number.</p>

<p style="text-align: center;">Assignment was unsuccessful</p> <p style="text-align: center;">No DIGIPASS was found for the given Serial Number -2 Please try again.</p>		
<p>Back-end authentication failed with supplied password -2</p> <p style="text-align: center;">Assignment was unsuccessful</p> <p style="text-align: center;">Back-end authentication failed with supplied password -2 {Error Code: '(1326)'; Error Message: 'Incorrect Windows user name or password.'} -2 Please try again.</p> <p style="text-align: center;">Synchronization was unsuccessful</p> <p style="text-align: center;">Back-end authentication failed with supplied password -2 {Error Code: '(1011)'; Error Message: 'Incorrect static password'} {Error Code: '(1326)'; Error Message: 'Incorrect Windows user name or password.'} -2 Please try again.</p>	<p>You have mistyped your Windows Password.</p>	<p>Re-type your Windows Password.</p>
<p>Back-end authentication failed with stored user password -2</p> <p style="text-align: center;">Your Digipass test login was unsuccessful</p> <p style="text-align: center;">Back-end authentication failed with stored user password -2 {Error Code: '(1326)'; Error Message: 'Incorrect Windows user name or password.'} -2 Please try again.</p>	<p>You have recently changed your Windows Password and the new password has not synchronised with the password stored in the Vasco database.</p>	<p>Contact your Shell focal point/Helpdesk to update your password stored in the the Vasco database.</p>
<p>The One Time Password failed validation -2</p> <p style="text-align: center;">Your Digipass PIN change was unsuccessful</p> <p style="text-align: center;">The One Time Password failed validation -2 {Error Code: '(-13)'; Error Message: 'Failed to get search results: LDAP returned 'No Such Object (32)'} {Error Code: '(-13)'; Error Message: 'Failed to get next paged results'} {Error Code: '(1)'; Error Message: 'Validation Failed'} {Er -2 Please try again.</p>	<p>You have mistyped the Digipass Response or the combination of PIN + Digipass Response.</p>	<p>Re-type the Digipass Response or the combination of PIN + Digipass Response.</p>

<p>Your Digipass test login was unsuccessful</p> <p>The One Time Password failed validation -2 {Error Code: '(1)'; Error Message: 'Validation Failed'} {Error Code: '(1012)'; Error Message: 'Serial VES0134958 Application AUTHENTICATE OTP Incorrect - Validation Failed'} {Error Code: '(1)'; Error Message: 'Validation Failed'} {Error Code: '(1)'; Error Message: 'Validation Failed'} -2</p> <p>Please try again.</p>		
<p>Assignment was unsuccessful</p> <p>The One Time Password failed validation -2 {Error Code: '(1)'; Error Message: 'Validation Failed'} {Error Code: '(1012)'; Error Message: 'Serial 0086702683 Application GO3DEFAULT OTP Incorrect - Validation Failed'} -2</p> <p>Please try again.</p>		
<p>The user accounts is locked -2</p> <p>Assignment was unsuccessful</p> <p>The user account is locked -2 {Error Code: '(1007)'; Error Message: 'Digipass User account is locked'} -2</p> <p>Please try again.</p>	<p>You have entered either the Digipass Response or the combination of PIN + Digipass Response incorrectly more than six times.</p>	<p>Contact your Shell focal point/helpdesk to un-lock your Digipass User Account.</p>
<p>Code Replay Attempt</p> <p>Your Digipass test login was unsuccessful</p> <p>The One Time Password failed validation -2 {Error Code: '(201)'; Error Message: 'Code Replay Attempt'} {Error Code: '(1008)'; Error Message: 'Serial 0086702683 Application GO3DEFAULT OTP Incorrect - Code Replay Attempt'} {Error Code: '(1)'; Error Message: 'Validation Failed'} {Error Code: '(1)'; Error Message: 'Validation Failed'} -2</p> <p>Please try again.</p>	<p>You have used the same Digipass Response for more than twice.</p>	<p>Generate a new Digipass Reponse from your hardware or software digipass and re-type.</p>

Glossary

One Time Password (OTP)

OTP is a combination of your digipass PIN and digipass response. Digipass PIN is a 6 digit number that you set when you register your digipass. The digipass response is a 6 digit number but is generated from the hardware or software digipass. The digipass response can only be used once and changes every (approximately) 20 seconds.

Two-Factor Authentication

Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a digipass, and the other is typically something memorized, such as a security PIN. In short, it is commonly spoken of as *something you have* and *something you know*.