VASCO
THE AUTHENTICATION COMPANY

DIGIPASS

DIGIPASS for Mobile using Blackberry Enterprise Server

Leveraging Blackberry Enterprise Server for mobile authentication deployment

DIGIPASS for Mobile leverages Blackberry Enterprise Server to facilitate the deployment of two-factor authentication in enterprises wanting to secure their remote access to the corporate network and business applications and mainly use Blackberry as their mobile platform.

DIGIPASS for Mobile provides two-factor authentication for enterprises wanting to secure the access to their SSL VPN for remote workers, extranets and business applications. The solution offers one-time password (OTP) and e-signature technology, allowing end users to use their Blackberry as their authentication device. With DIGIPASS for Mobile enterprises are able to counter unauthorized access to corporate networks and resources and prevent data theft.

DIGIPASS for Mobile using Blackberry Enterprise Server has been developed for enterprises wanting to deploy two-factor authentication to their employees on mobile phones and where Blackberry is the main mobile platform being used throughout the company.

With DIGIPASS for Mobile using Blackberry Enterprise Server, the deployment of the application to the employees' devices is centrally managed. Employees do not to take any action to obtain the authentication application, it will simply pop up on their Blackberry where the employee will need to activate it.

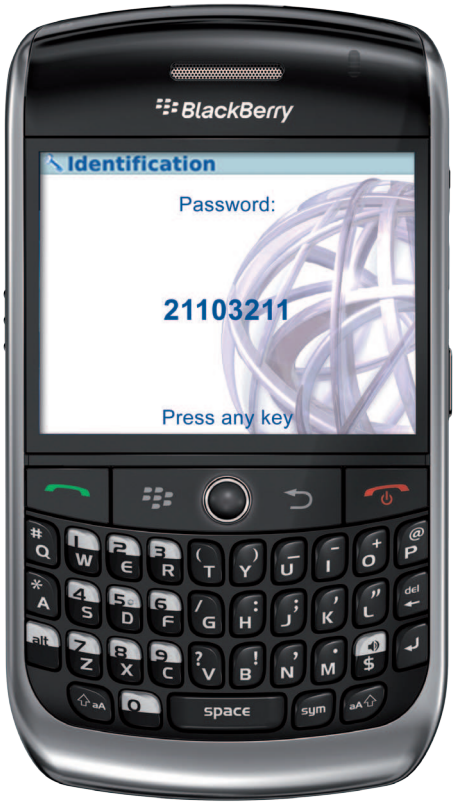
HOW DOES IT WORK?

IT administrators will configure an application folder and index the application. Furthermore they will create a software configuration and create an application control policy. Once this is done, they will assign an application control policy and assign the software configuration to the Blackberry devices. The DIGIPASS for Mobile application will be pushed to the devices over the wireless network within four hours.

End users will find the authentication application on their Blackberry and will be asked to activate it by choosing a PIN. The PIN will be asked every time the end user wants to generate an OTP.

HIGH END USER ACCEPTANCE

Employees will be able to securely do business from their mobile device or laptop while travelling anywhere in the world. They do not need to carry additional authentication devices; they simply use the Blackberry already in their pocket to authenticate. DIGIPASS for Mobile is self explanatory; it requires no end user training. The end user is asked to activate the authentication application by choosing a PIN. Once activated, an OTP is simply generated after PIN insertion.



VASCO
THE AUTHENTICATION COMPANY

DIGIPASS

CENTRAL DEPLOYMENT AND MANAGEMENT

IT administrators are able to centrally manage the deployment by themselves. They make use of their Blackberry Enterprise Server to transparently push the authentication application to the employees' Blackberry devices.

Employees do not have to do anything to get the application. It will pop up on their Blackberry and they will be asked to activate it.

COST-EFFICIENCY

DIGIPASS for Mobile makes use of the Blackberry Enterprises Server to deploy the authentication application to employees. It requires no additional infrastructure investments. Furthermore, no SMS or downloads are required to install the application on end user devices, thus reducing deployment costs.

A demo of DIGIPASS for Mobile is available on:
dp4mobile.demo.vasco.com

TECHNICAL SPECIFICATIONS

Response Only	Event-based or Time + Event-based DES/Triple DES Encryption Algorithm Response : 6 to 16 Decimal/Hexadecimal Check Digit 256 seconds Time Step
Host Confirmation Code	DES/Triple DES Length from 4 to 10 Decimal/Hexadecimal (1 to 10 in challenge response mode)
Challenge/ Response	Event-based or Time + Event-based DES/Triple DES Encryption Algorithm Challenge length from 4 to 15 Decimal Response length from 6 to 16 Decimal/ Hexadecimal Check Digit 256 seconds Time Step
MAC/signature	Event-based or Time + Event-based DES/Triple DES Encryption Algorithm Length from 4 to 16 Decimal/Hexadecimal Up to 8 customizable data fields Data field length from 4 to 15 digits 256 seconds Time Step
PIN management	PIN length options: no PIN or 6 to 9 digits Max number of wrong entries from 1 to 9 On wrong PIN: Invalid password generation or reset PIN check options : Checksum/Hashcode/None PIN change option

About VASCO

VASCO designs, develops, markets and supports patented DIGIPASS®, DIGIPASS PLUS, VACMAN®, IDENTIKEY® and aXsGUARD™ authentication products for the financial world, remote access, e-business and e-commerce. With tens of millions of products sold, VASCO has established itself as the world leader in Strong User Authentication for e-Banking and Enterprise Security for blue-chip corporations and governments worldwide.

www.vasco.com

BRUSSELS (Europe)
phone: +32.2.609.97.00
email: info-europe@vasco.com

BOSTON (North America)
phone: +1.508.366.3400
email: info-usa@vasco.com

SYDNEY (Pacific)
phone: +61.2.8061.3700
email: info-australia@vasco.com

SINGAPORE (Asia)
phone: +65.6323.0906
email: info-asia@vasco.com