VASCO showcases DIGIPASS for Mobile at MEFTEC

Oakbrook Terrace, Illinois, Zurich, Switzerland, April 20, 2010 - VASCO Data Security Inc. (Nasdaq: VDSI; www.vasco.com), a leading software security company specializing in authentication products, will showcase its DIGIPASS for Mobile authentication solution at MEFTEC (Bahrain International Exhibition Centre, 20th and 21st April, booth H301). DIGIPASS for Mobile is VASCO's authentication solution which leverages Internet enabled mobile phones for authentication purposes. DIGIPASS for Mobile can be used for two factor authentication and digital signature.

DIGIPASS for Mobile offers a solution to banks who want to secure multiple customer facing channels including e-banking, m-banking, phone banking using IVR and cash retrieval at the ATM.

An increasing number of banks protect their e-banking channels against fraud attacks, such as phishing and man-in-the-middle attacks, with two-factor authentication. Banks are also increasingly introducing m-banking for their generation Y customers or in regions where the mobile phone penetration is higher than the Internet penetration. M-banking is facing similar challenges as e-banking when it comes down to protecting user accounts. VASCO's DIGIPASS for Mobile can be used to protect both the e-banking and m-banking channels using a one-time password (OTP) to access the banking application and e-signature to sign online transactions.

Furthermore the use of DIGIPASS for Mobile can be extended to phone banking. Most phone applications use Interactive Voice Response (IVR) which allows the customer to access their bank via a touchtone telephone or voice recognition. These systems often use simple passwords like: who are you and what is your mother's name. This information can easily be retrieved online using social engineering techniques. As a result the use of dynamic authentication messages becomes more important to avoid impersonation. DIGIPASS for Mobile can easily be integrated in an IVR system: when calling the bank the IVR system would immediately recognize the customer who would be prompted for a user ID and OTP to further access the banking system.

The use of DIGIPASS for Mobile can also secure cash retrieval at the ATM. ATMs have always been subject to fraud. Nowadays skimming techniques and ghost ATMs are used to obtain card details and plunder accounts. DIGIPASS for Mobile strong authentication can be added without having to change the existing ATM network, PIN validation will simply be replaced by OTP validation. The bank customer will activate the authentication application on his phone using a PIN-code. On PIN-insertion an OTP will be generated which the banking customer will type on the ATM keyboard.

"We are using VASCO's DIGIPASS for Mobile for "Cep Şifrematik" which runs on a mobile phone. Our customers can access the Garanti Online/Mobile Branch using a one-time password generated by Cep Şifrematik. Since the mobile phone is used as authentication device, customers can access their bank account whenever and wherever considering that they have their authentication device always in their pocket. Whether they want to access their account

from somebody else's PC or in an Internet cafe they can do so in total security," says M.Feridun Aktaş, Chief Security Officer at Garanti Bank (Turkey).

"The use of strong authentication for online banking is mandatory by the Turkish Banking Association. Halkbank's *Şifrebaz* uses DIGIPASS for Mobile. It is very straightforward in use; simple and fast: we send the authentication application by SMS to our customers. They will download the application on their mobile phone and choose a password. Every time they want to use Şifrebaz they will enter their password to generate a one-time password to access the online banking application," says Cenk Niksarli, Chairman of IT from Halkbank (Turkey).

DIGIPASS for Mobile uses proven VASCO VACMAN® authentication technology and supports more than 400 types of mobile phones and operates on Java phones, Blackberry, iPhone and Windows Mobile and platforms such as NTT Docomo.

"The mobile platform not only is becoming more attractive to hackers as more and more mobile applications are introduced, the mobile phone is also a loyal companion never leaving our side. As a result it is an excellent platform for strong authentication. Since the mobile phone is always in our pocket it can be used for user authentication at the ATM or to access e- and m-banking applications anywhere and any time," says Jan Valcke, President and COO at VASCO Data Security.

About VASCO

VASCO is a leading supplier of strong authentication and e-signature solutions and services specializing in Internet Security applications and transactions. VASCO has positioned itself as global software company for Internet Security serving a customer base of almost 9,500 companies in more than 100 countries, including approximately 1,400 international financial institutions. VASCO's prime markets are the financial sector, enterprise security, e-commerce and e-government.

Forward Looking Statements:

Statements made in this news release that relate to future plans, events or performances are forward-looking statements. Any statement containing words such as "believes," "anticipates," "plans," "expects," "intend," "mean," and similar words, is forward-looking, and these statements involve risks and uncertainties and are based on current expectations. Consequently, actual results could differ materially from the expectations expressed in these forward-looking statements.

Reference is made to VASCO's public filings with the U.S. Securities and Exchange Commission for further information regarding VASCO and its operations.