

Digipass[®] Family of Authentication Devices

White Paper

Digipass[®] Family of Authentication Devices

Contents

Overview	2
The Problem	2
Concept	4
Technical Description	5
Response Only Mode	6
Challenge/Response Mode	8
Electronic Signature Mode	10
System Components	11
System Requirements	11

Digipass[®] Family of Authentication Devices

Overview

This paper describes the Digipass[®] Family of handheld security devices manufactured and marketed by VASCO. Digipass security devices (tokens) were originally developed as an alternative to common, and easy-to-compromise, security solutions such as static passwords and PIN codes.

Digipass products are designed to address what experts agree are significant issues for the IT industry:

- Incorrect authentication is the single largest threat to any computer system
- User-managed passwords are the single largest cause of incorrect authentication.

In this paper, we provide an overview of the “authentication device” security concept; the capabilities of our Digipass family devices, and the algorithms that can be used to protect specific areas within your application or environment.



Figure 1. From left to right the Digipass 250, 300, 600, 700 and 800

The Problem

Most security experts agree: Static passwords are not a safe way to protect vital systems. They prefer a “strong authentication” approach to system security. What is “strong authentication”?

Simply put, “*Authentication*” means verifying that people are who they say they are, before they’re entrusted with access to your sensitive data. And “*Strong Authentication*” means raising the ante on security, by preventing unauthorized users from simulating a legitimate user’s identity.

“Authentication” is easy in a face-to-face conversation: You can do a quick visual check, to confirm the identities of your speaking partners. And if you require a strong authentication, you can ask them to produce a passport, driver’s license or other form of ID.

Unfortunately, this scenario cannot be replicated in most electronic forms of communication. Instead, we ask our remote “speaking partners” to provide a password, pass phrase or PIN code to serve as their positive identification. Since passwords generally are user-managed, they can lead to security breaches: Passwords that aren’t changed frequently, for example, or that are based on easy-to-guess parameters (names of family members, pets, birth dates, etc.). These shortcomings make static passwords easy to compromise. Hackers can employ any number of techniques (like dictionary attacks, password readers, etc.) to detect static passwords and gain access to your sensitive information.

Some types of communications – such as commercial transactions, money transfers and other intrinsically valuable data transfers – require a higher level of security than most electronic messages. Without strong authentication, these high-value transactions can be subject to theft or malicious attacks – and in most cases, the identity and location of the hackers can be very difficult to trace. That’s why bulletproof security is imperative in banking or e-commerce environments, to guarantee the integrity of consumer and commercial transactions conducted over public (and, therefore, insecure) channels.

VASCO’s Digipass Family of products is specifically designed to deliver the exceptional authentication performance that your valuable electronic transactions require.

In *Applied Cryptography* (2nd Edition, 1996) security expert Bruce Schneier writes: “The world’s most secure algorithm won’t help much if the users habitually choose their spouse’s names for keys (passwords) or write their keys on little pieces of paper in their wallets.”

Cheswick & Bellovin comment in *Firewalls and Internet* (1994): “No security expert we know of regards passwords as a strong authentication mechanism. One can achieve a significant increase in security by using one-time passwords.”

Concept

The Digipass concept incorporates solutions that specifically target the weakest links in common approaches to data security.

A Digipass-based strategy eliminates the shortcomings of a “static password” approach, by delivering dynamic passwords through a device that is highly portable; easy to integrate into any computing environment; and inexpensive. In short, the Digipass solution provides “strong authentication” in a way that maximizes flexibility and minimizes the total cost of ownership.

What is a Digipass device?

Digipass products are handheld devices designed to perform two basic security functions:

- Calculate dynamic passwords, or One-Time Passwords (OTP), to provide positive authentication of a user on a remote system.
- Calculate electronic signatures, or Message Authentication Codes (MAC), to protect electronic transactions and guarantee the integrity of their contents.

Digipass products calculate these OTPs and MACs based upon the publicly available Data Encryption Standard (DES) algorithm. The DES algorithm is the industry’s leading encryption technology, accepted by security experts worldwide. Digipass products also support the Triple DES (3DES) algorithm, to provide an even higher level of security when required.

In general, “Strong Authentication” security can be based on three factors:

1. What you have (a token such as the Digipass device)
2. What you know (a PIN code, required to activate the Digipass)
3. Who you are (biometrics, voice, retina scan, fingerprint, etc.)

For most users, the third option is impractical, because the biometrics industry is still in its infancy stage, and biometric products tend to be extremely expensive. That’s why the Digipass Family is based on the first two security options.

Under the Digipass model, to enter a remote system or to digitally sign data, you need both:

- The hardware device (or token), and
- The PIN code, allowing you to access the applications stored inside the token.

Both factors contribute to increased security, by helping to ensure that an actual person is authenticating or signing the message, rather than a computer or another electronic device. At the same time, Digipass devices are designed to be extremely portable, so that you can use them to protect your transactions and systems “anytime, anywhere and anyhow”.

Technical Description

This technical description summarizes the three most frequently used modes for implementing the 3DES algorithm in conjunction with the Digipass Family. These modes are:

- Response Only
- Challenge/Response
- Electronic Signature

To start, we will describe the set-up sequence for the Digipass device usage. This illustration highlights the typical process in common applications.

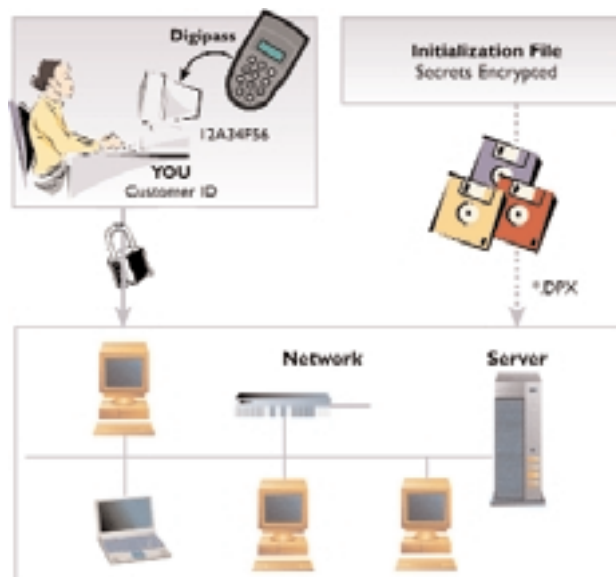


Figure 2: General concept for the Digipass Family hardware device usage

Step One: Digipass devices are initialized (at the factory) with a unique set of secrets and keys per device. These secrets and keys are encrypted and stored on files which are provided to the application owner (e.g. IT department, security department), as a way of safely transporting the data to the host computer. These files are used to read all the necessary secrets and keys from the portable Digipass devices into the application owner's database.

Step Two: The application owner assigns a distinct set of Digipass secrets to various end-users. Through this assignment process, the serial number of the Digipass device is linked to a particular end-user. The Digipass is then shipped to the end-user, together with a short manual and a protected PIN-code (using a secure PIN-mailer). Once the device is received by the end-user, it can be put into service.

Step Three: The Digipass device is used each time a connection is made to the host (server) computer. The user sends a Digipass Dynamic Password or electric signature to the host computer, which then retrieves all the necessary encryption information from the database. The OTP or MAC is checked against the database, to determine the validity of the password or signature. Then, the host computer responds to the remote location, either providing access or denying it, depending on the validity of the password or electronic signature received from the device.

This overall principle of device usage is employed for all three of the most frequently used implementation modes.

I. Response-Only Mode

In this mode, the Digipass device delivers a dynamic password (OTP) upon request by the end-user. The following illustration highlights the Digipass 300 usage flow.

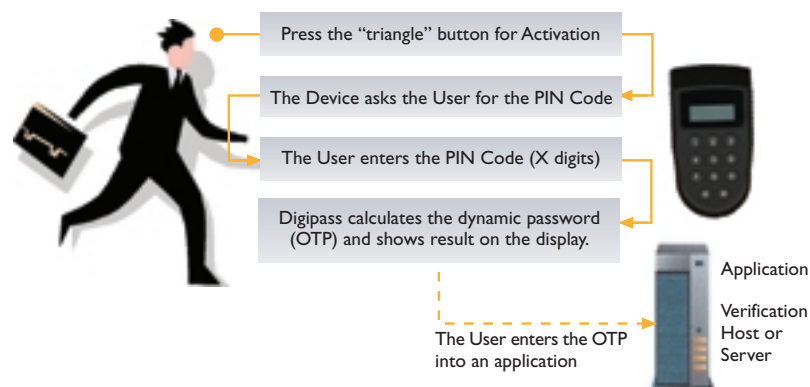


Figure 3: Usage for Digipass 300 (Response Only Mode)

How is a “Response Only” dynamic password generated?

Inside the Digipass device, a 3DES engine automatically calculates passwords and signatures. 3DES uses secret keys or “seed values” (3DES keys, offset, initial vectors, etc.) to perform this encryption. All these secrets are stored inside the Digipass itself and permanently saved into the device at initialization. Seed values are never exposed during the actual use of a Digipass device.

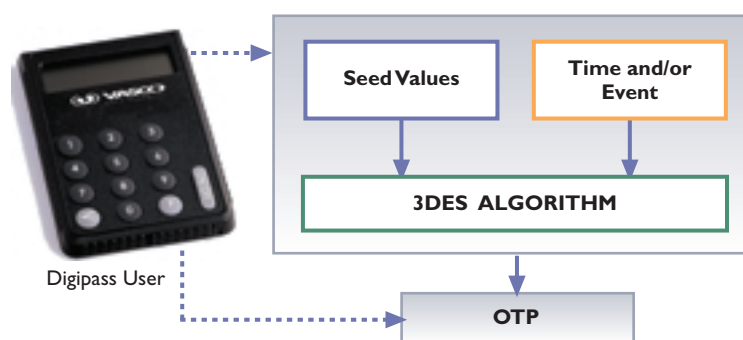


Figure 4: OTP calculation in “Response Only” mode, time and/or event based.

The Digipass device is designed to calculate OTPs on request. The Digipass uses the previously initialized seed value, and the current time and event data, to generate the dynamic password. (The device automatically generates time or event inputs for the 3DES algorithm, without end-user involvement.)

When a time-based “Response Only” mode is chosen, time data is internally derived from the Real Time Clock (RTC). The RTC cannot be altered from outside the device.

In event-based “Response Only” mode, the event code (i.e., a unique incremental number generated at the start of every new OTP calculation) is produced by the device itself to prevent outside inputs.

These two inputs (time and event) are key features in creating dynamic passwords. Because the inputs change each time the Digipass is used, the DES calculation automatically produces a unique password.

The end-user can select time-based, event-based, or a combination of both time and event, to generate the dynamic password in the “Response Only” mode.

Once the dynamic password is calculated by the Digipass, the password must also be verified by the host machine. The DES is a symmetric algorithm; therefore, DES keys and other secret information must be present on both the host machine and the Digipass device. This secret data can be imported into a database system through a variety of applications – either custom programs developed by VASCO Partners, or off-the-shelf applications. Both custom and off-the-shelf verification applications can successfully complete the verification functions required by the Digipass system.

2. Challenge/Response Mode

This mode provides an extra level of security for authentication. When the Challenge/Response mode is selected, the end-user must provide additional input before the dynamic password is calculated. This extra user input is called the “challenge.”

In this mode, an application running on the host computer generates a challenge at random each time the logon sequence is begun. The challenge is then sent over the communication line to the end-user. The user enters the “challenge” data into the Digipass and obtains a dynamic password (a number of x digits) based, among other parameters, on the challenge delivered by the application on the host system. As a result, the dynamic password is based on more than the end-user’s input alone. It requires extra information from the host system. The next illustration shows how the Challenge/Response mode is used on a Digipass 300.

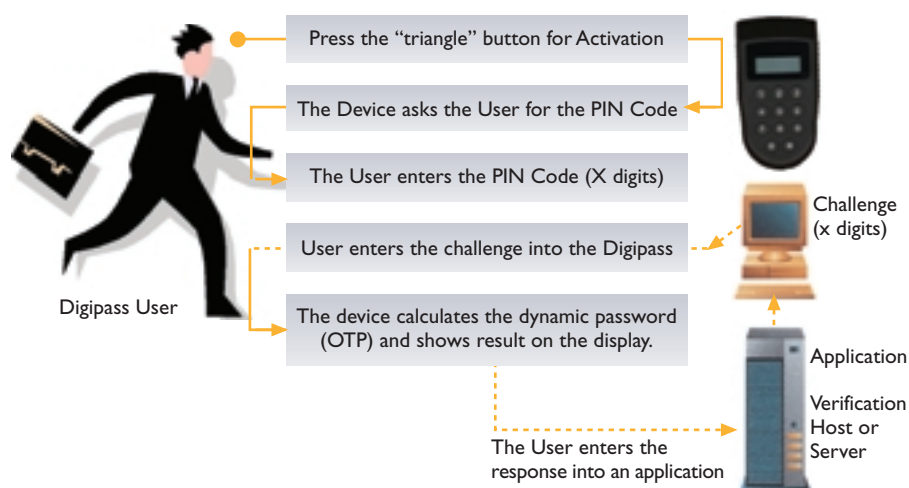


Figure 5: Usage of the Digipass 300 (Challenge/Response Mode)

Although both the “Challenge/Response” mode and the “Response Only” mode both are used to generate dynamic passwords, security is increased with the Challenge/Response mode because extra user input is required before a valid password can be calculated.

This two-way communication between the Digipass user and the host application helps to ensure that only authorized users (i.e., those who understand the challenge/response process) are granted access to system.

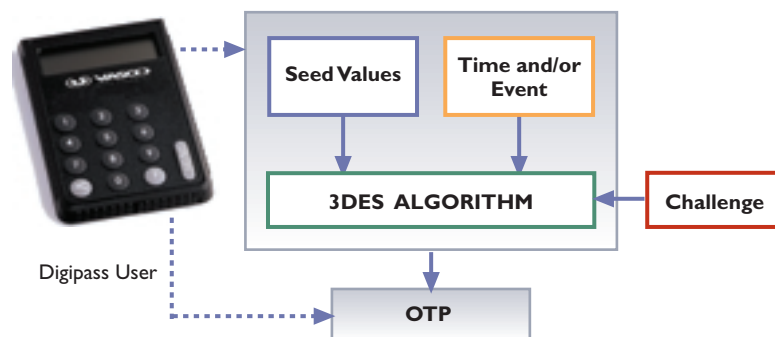


Figure 6: OTP calculation in Challenge/Response mode, time or event based

After the challenge/response has been entered, the Digipass calculates a dynamic password in exactly the same manner as in the “Response Only” mode. The Digipass device is pre-initialized to use a unique set of secrets and keys to generate the password. In addition, time and event inputs can be used to calculate dynamic passwords. Time and event inputs are generated in the exact same way for the “Challenge/Response” mode as they are for the “Response Only” mode.

The verification process, conducted at the host computer (server), is somewhat different in the “Challenge/Response” mode. In addition to applying the DES-generated verification units, the server must also temporarily memorize the challenge sent to the end-user; and then check the response against the challenge that was issued.

3. Electronic Signature Mode

The “Electronic Signature” mode (also called “Message Authentication Code” [MAC]) provides the most versatile form of token-based security. It acts not only in an authentication mode (i.e., verifying that users are who they say they are), but also serves to secure the contents of an electronic transaction.

This illustration shows how the Digipass device is used to apply electronic signatures to a transaction.

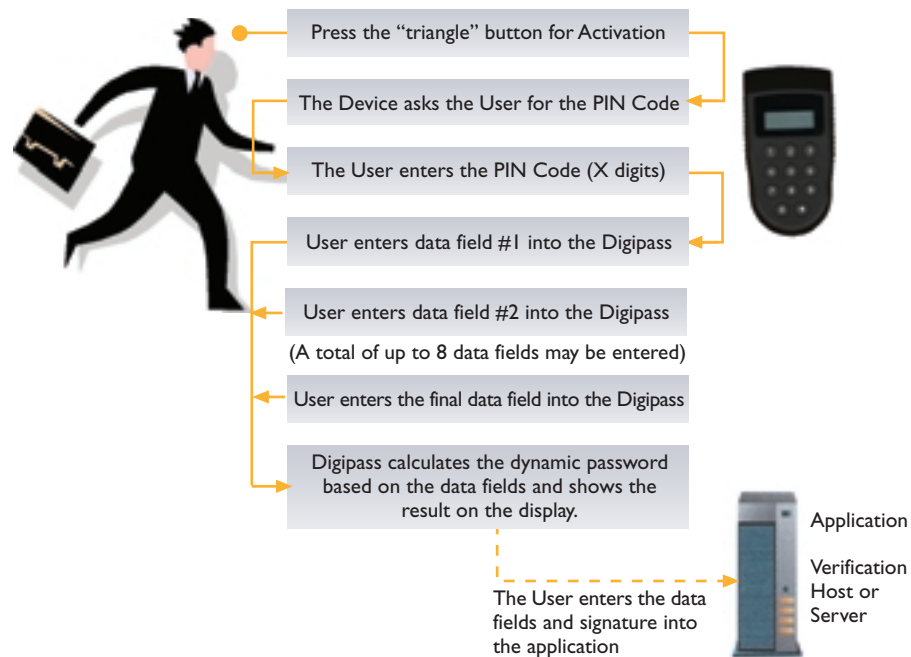


Figure 7: Usage of the Digipass 300 (Electronic Signature Mode)

In this mode, the Digipass can calculate a signature and apply it to a number of data fields created by the end-user. To digitally sign a wire money transfer, for example, the end-user may choose to protect data fields such as the bank account number of the sender; the bank account number of the recipient; and the amount of money to be transferred. These data fields are then sent, together with the electronic signature, to the host server for verification.

The electronic signature is not simply an authentication mode. It protects the contents of a given transaction, by generating a MAC on the values entered in specific fields in the message. With these MACs in place, hackers or eavesdroppers may be able to detect that an electronic transaction is under way, but they will not be able to alter it in any way. The electronic signatures guarantee the integrity of the transaction, just as it was sent by the end-user.

At the host end of the transaction, the server can check to determine whether the rightful owner of the Digipass actually performed the calculation of the electronic signature, and thereby verify the integrity of the data included in the transaction. This ensures that the transaction is highly secure, so that the bank or financial institution can execute the transaction while limiting its exposure to fraud or liability issues.

The data fields can be user-defined or application-defined: The application automatically provides the necessary fields to input transaction values and to calculate the electronic signature. Once this data is entered, the transaction can be sent to the host computer. At that point, the electronic signature is validated – and the host computer sends a message confirming both the signature and the execution of the transaction.

System Components

- All members of the Digipass Family (Digipass 250, 300, 600, 700, and 800).
- Recommended / Optional: VACMAN Controller for integration into applications.
- Recommended / Optional: PKA library for integration into a PKI environment.

System Requirements

Digipass security devices (hardware tokens) are self-contained, and do not require any specific hardware or software platform to operate.

VASCO's integration libraries (VACMAN Controller, PKA) are platform independent, and can be installed on practically any computing platform.

For more technical information on the above-mentioned products, please refer to the corresponding technical white papers of these products or contact VASCO.

About Vasco

VASCO secures the enterprise from the mainframe to the Internet with infrastructure solutions that enable secure e-business and e-commerce, protect sensitive information, and safeguard the identity of users. The company's Digipass® and VACMAN® product families offer end-to-end security through strong authentication and electronic signature, true and secure single sign-on, access control, and web portal security, while sharply reducing the time and effort required to deploy and manage security. VASCO's customers include hundreds of financial institutions, blue-chip corporations, and government agencies in more than 50 countries. More information is available at www.vasco.com.

For regional offices or to learn more about us, visit our web site at www.vasco.com



AMERICAS HQ

VASCO Data Security, Inc.
1901 Meyers Road, Suite 210
Oakbrook Terrace, Illinois 60181, USA
phone: +1.630.932.8844
fax: +1.630.932.8852
e-mail: info_usa@vasco.com

EMEA HQ

VASCO Data Security nv/sa
Koningin Astridlaan 164
B-1780 Wemmel, Belgium
phone: +32.2.456.98.10
fax: +32.2.456.98.20
e-mail: info_europe@vasco.com

APAC HQ

VASCO Data Security Asia-Pacific Pte Ltd.
#15-03 Prudential Tower, 30 Cecil Street
049712 Singapore
phone: +65.232.2727
fax: +65.232.2888
email: info_asia@vasco.com

All trademarks or trade names are the property of their respective owners. VASCO reserves the right to make changes to specifications at any time and without notice. The information furnished by VASCO in this document is believed to be accurate and reliable. However, VASCO may not be held liable for its use, nor for any infringement of patents or other rights of third parties resulting from its use.