VASCO Digipass® Family of Authentication Devices
Technical White Paper

Overview

The Digipass Family is the name VASCO uses to describe the family of handheld security devices that VASCO manufactures and markets.
The Digipass are security devices (tokens) that were originally developed as an answer to easily compromised static passwords and PIN codes, because:

- 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 will provide an overview of what you can do with our Digipass family members. You will also learn more about the concept of an authentication device and the specific algorithms used to protect specific areas within your application or environment.

Fig. 1 from left to right the Digipass 300, Digipass 500, Digipass 600, Digipass 700 and Digipass 800

Problem Description

An expert opinion by Bruce Schneier in 'Applied Cryptography', 2nd Edition 1996 states: "The worlds 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 wrote in 'Firewalls and Internet' in 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."

Security experts' statements confirm that static passwords are not safe. (See left).
They also use the term "strong authentication".

What is "strong authentication"?

We need to split this term into two parts.

"Authentication" means that you verify that people are who they say they are, before you can trust them with your sensitive data and before they can do harm to that data.
"Strong" means preventing people from simulating other users' identities.
In a face-to-face conversation, your speaking partners can see who you are by running a visual check on your identity. If they want to identify you 'strongly' (e.g. police) they will ask you for your passport or any other positive ID.

This scenario can not be imported into the remote telecommunications world, where people are communicating without knowing who their conversation partners really are and what they look like. In the telecommunications world a password, pass phrase or PIN code is still often used as the positive identification for a person. Since passwords are static and managed by their owner, he can change it at free will and can choose any password he wants (usually names of family members, pets, birth dates,…). These passwords are easy to compromise. Hackers have several techniques for quickly detecting static passwords (like dictionary attacks, password readers, etc.) which allow them to access your sensitive information.

Another risk in the telecommunication world is making sensitive transactions - like money transfers - over a communication line. If these transactions are not strongly protected against attacks from malicious people, they can be easily changed to the benefit of the hacker and it is very hard to trace (post hoc) the identity and location of this hacker. In a Banking or E-commerce environment, security is imperative to guarantee the integrity of the commands and orders issued through public and, by nature, insecure channels.

For authentication and electronic transaction problems, VASCO delivers appropriate solutions by means of the Digipass Family.

Concept

In the Digipass concept we have implemented cures for the weak areas of authentication and data integrity.
To avoid the static nature of passwords, we needed a device that delivers dynamic passwords, is highly portable and flexible to integrate into any environment, and in addition, is not expensive. In other words: we needed to implement strong security with a maximum of flexibility and a minimal total cost of ownership. We considered security to be a trade-off between: security, flexibility, price and ease of use and therefore developed the Digipass.

What is a Digipass device?

A Digipass device is a handheld device that calculates dynamic passwords, also known as One-Time Passwords (OTP), for the positive authentication of a user on a remote system. Moreover, it is able to calculate digital signatures, known as electronic signatures or Message Authentication Codes (MAC), to protect electronic transactions and guarantee the integrity of the contents of these transactions.
The calculation of these OTP's and MAC's is based upon the publicly available Data Encryption Standard (DES) algorithm. The DES algorithm has proven itself to be strong in numerous fields of application by renowned institutions and industry leading companies. To provide an even higher level of security the Triple DES algorithm is supported as well.
Security has three factors:

1. What you have (the Digipass device itself)
2. What you know (the PIN code to activate the Digipass)
3. Who you are (biometrics, voice, retina scan, fingerprint, …)

Since the biometrics industry today is still not completely developed and products in this area tend to be extremely expensive, we based the Digipass Family on the first two factors of the list. In order to enter a remote system or to digitally sign data you need:

- The hardware device itself (factor 1): if you do not physically have the device, you will never be able to log on to the system.
- The PIN code for the device (factor 2), to be able to use the applications stored within it.

Both these factors help to make sure that a physical person is authenticating or signing instead of a computer or another device.
These factors also enable extremely high portability: you can use a Digipass "Anytime, Anywhere and Anyhow".

Technical description

In this technical description, we will elaborate on the three currently most frequently used implementation modes of the DES algorithm in conjunction with the Digipass Family. These modes are the "Response Only" mode, the "Challenge/Response" mode and the "Digital Signature" mode.
First we will start with the complete application cycle of the Digipass device usage.

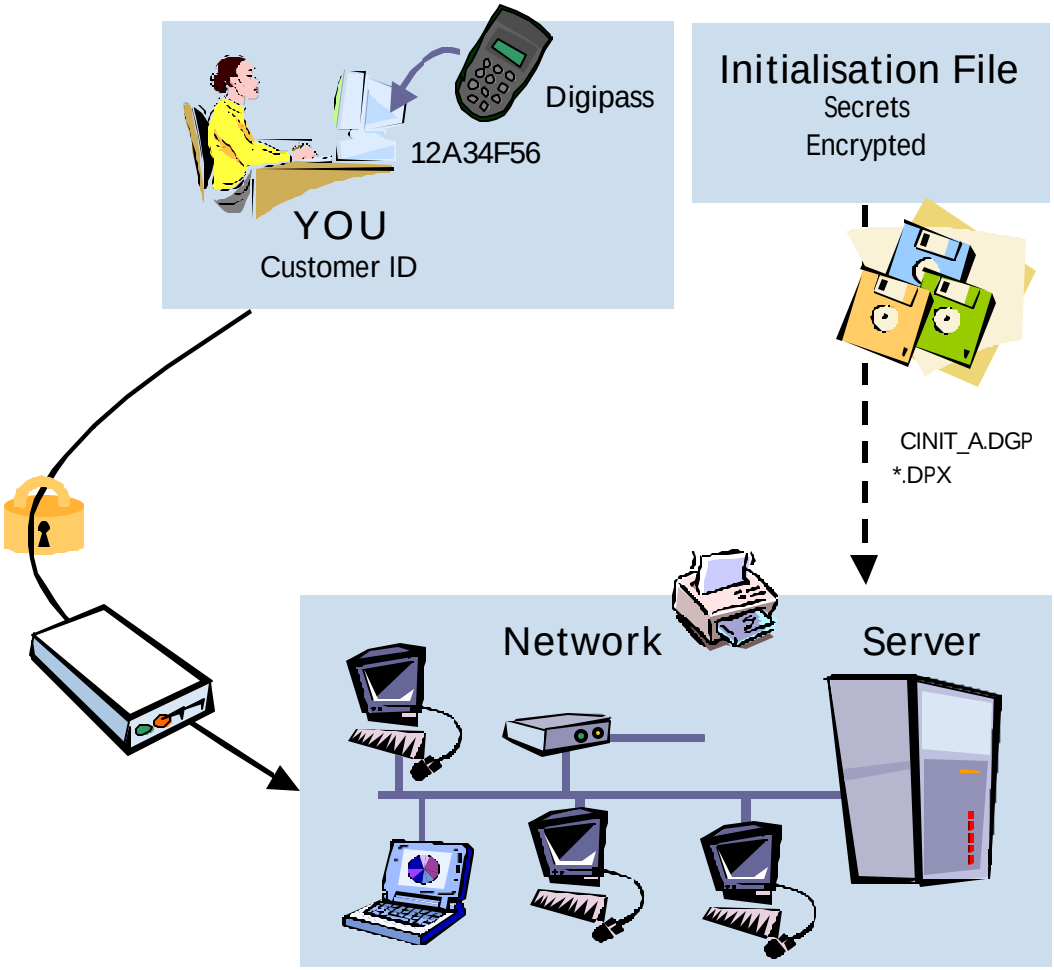

Fig 2. General concept for the Digipass Family hardware device usage

The above illustration shows you step-by-step the global flow on device usage.
In the first step the devices are initialized with their unique set of secrets and keys per device. These secrets are stored in an encrypted way on a diskette that is sent to the application owner (e.g. the IT manager in a company or the security department of a bank). These floppy disks are a way of safely transporting the Digipass secrets to the host computer.

The files on the floppy disks will be used to read all the necessary secrets and other data from the delivered Digipass devices into a database.
Then the application owner will assign those Digipass secrets to the end-users. This assignment is based on the serial number of the Digipass device and the name of the end-user.
The Digipass is then shipped to the end-user together with a manual and the protected PIN-code on a secure PIN-mailer.
Once the device is received by the end-user, he can start using it.

To use a Digipass, you need a connection to the host (server) computer that knows the secrets of the end-user's Digipass. Every time the user sends a dynamic password or digital signature to the host computer, the computer will retrieve all the necessary information from the database and will check the validity of the password or signature. After the host has checked the validity of the dynamic password or signature, it will notify the end-user of the correctness or incorrectness of the validity check.

Since we now know the overall principle of device usage, we can explain the three most frequently used implementation modes of the (Triple) DES algorithm in combination with Digipass hardware security devices.

1. Response Only Mode

As the term indicates the "Response Only" mode on a Digipass delivers a dynamic password (OTP) upon request by the user. The following illustration describes the Digipass 300 usage flow.

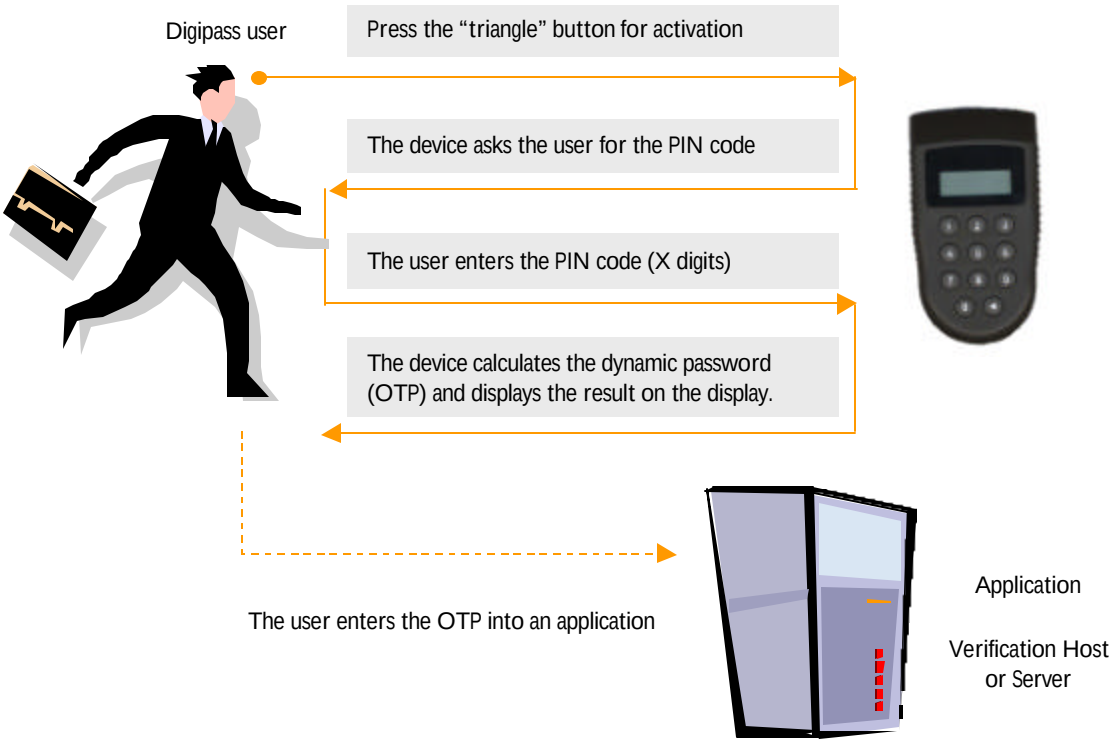

Fig 3. Usage for Digipass 300 (Response Only Mode)

As you can see in the example for the Digipass 300 above, the interface for the device is intuitive.
How is a "Response Only" dynamic password calculated?

Inside the Digipass device a DES engine takes care of the calculation of the passwords and signatures. DES uses secret keys or "seed values" (DES keys, offset, initial vectors, etc.) to perform this encryption. All these secrets are thus stored inside the Digipass itself and saved into the Digipass at initialization. By consequence they are never exposed while using a Digipass.

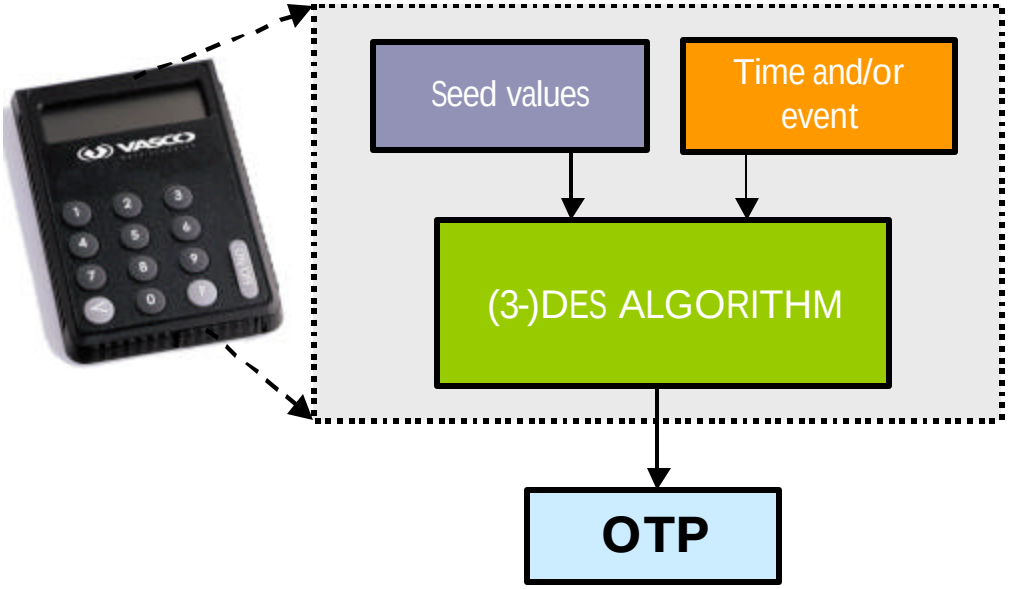

Fig 4. OTP calculation in "Response Only" mode, time and/or event based.

Upon usage the Digipass will start calculating OTP's on request.
This happens as shown in the above illustration: the Digipass uses the pre-initialized seed value and the input from time and event to generate the dynamic password.
The device itself generates the time or event inputs for the DES algorithm. When a time-based "Response Only" mode is chosen, the time is internally derived from the Real Time Clock (RTC) which can not be altered from the outside of the device. In the case of an "Event Response Only" mode, the event (= a number that is incremented at every new calculation of an OTP) is generated by the device itself to prevent untrustworthy third party inputs.
These two inputs (time and event) are the key features for the creation of dynamic passwords. Without them the result of the DES calculation would always be the same and therefore unsafe.
In the "Response Only" mode, time and event can be combined or can exist separately but you need at least one of them to calculate a dynamic password.
Once a dynamic password is calculated by the Digipass, the password needs to be verified for correctness. This typically happens on a host machine. Since DES by nature is a symmetric algorithm (secret information and DES keys need to be known by the verifying unit as well) the DES keys and other secret information needs to be present on the host machine. The secrets are imported into a database system by an application. Such an application can be tailor-made (e.g. one of the VASCO Partner applications) or can be available off-the-shelf (e.g. Shiva Access Manager). Both these types of verification applications have implemented the verification functions VASCO delivers in the form of the AAT (Advanced Authentication Technology) Libraries. Please refer to the "Technical White Paper on the AAT Libraries" for more information.

2. Challenge/Response Mode

This mode is also used for authentication purposes but works in a different way. The Challenge/Response mode demands an extra user input for the calculation of a dynamic password. This extra user input is called "the challenge".

If we put this theory into practice, we see that the challenge is generated at random at every logon trial by the application running on the host computer, and is then sent over the communication line to the user. The user puts the challenge into the Digipass and obtains a dynamic password (a number of x digits) that is based, among other parameters, on the challenge delivered by the application on the host system (server). The result, the dynamic password, is now based on more than the user's input alone. It needs extra information coming from a third party.
In the next illustration you will see a representation of the Challenge/Response mode usage on a Digipass 300.

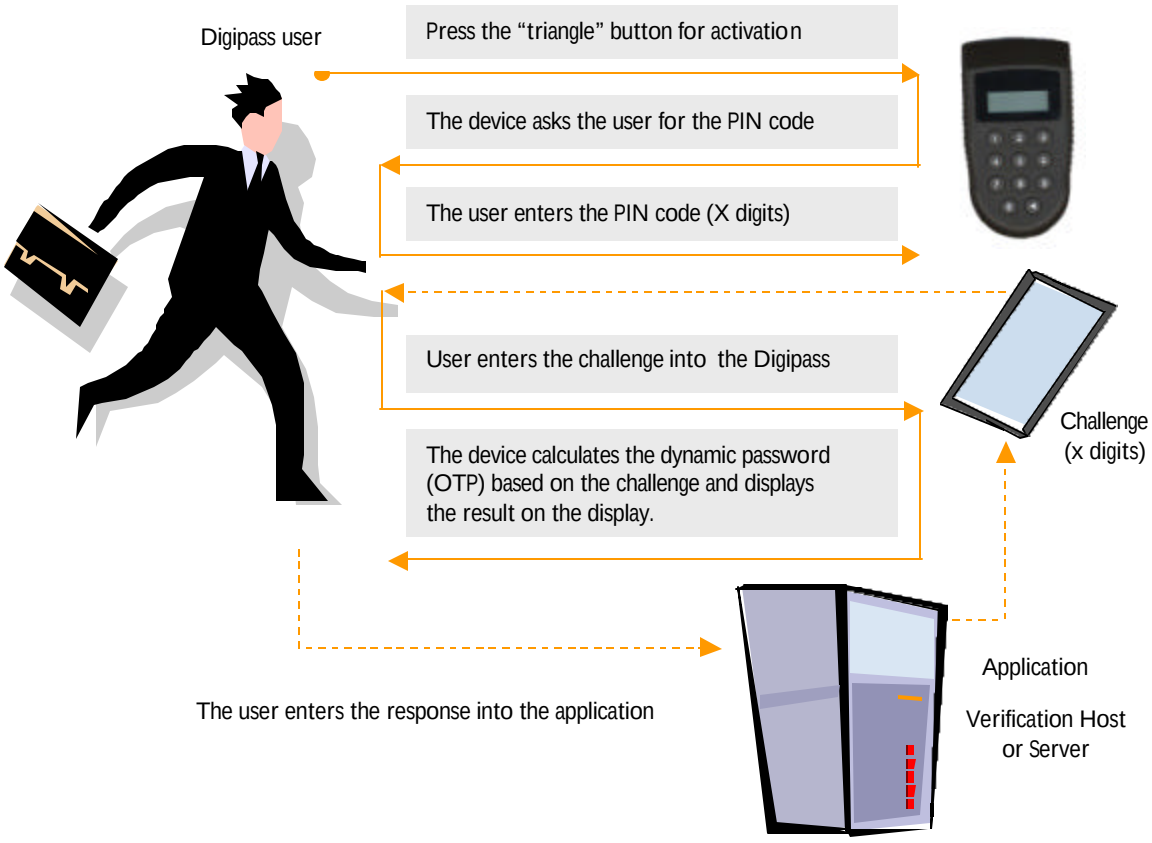

Fig 5. Usage of the Digipass 300 (Challenge/Response Mode)

The difference with the "Response Only" mode is that there is now an extra user input into the device.

The final result remains that a dynamic password is generated, but based on a different set of parameters, enabling a two-way communication between the Digipass user and the host application.

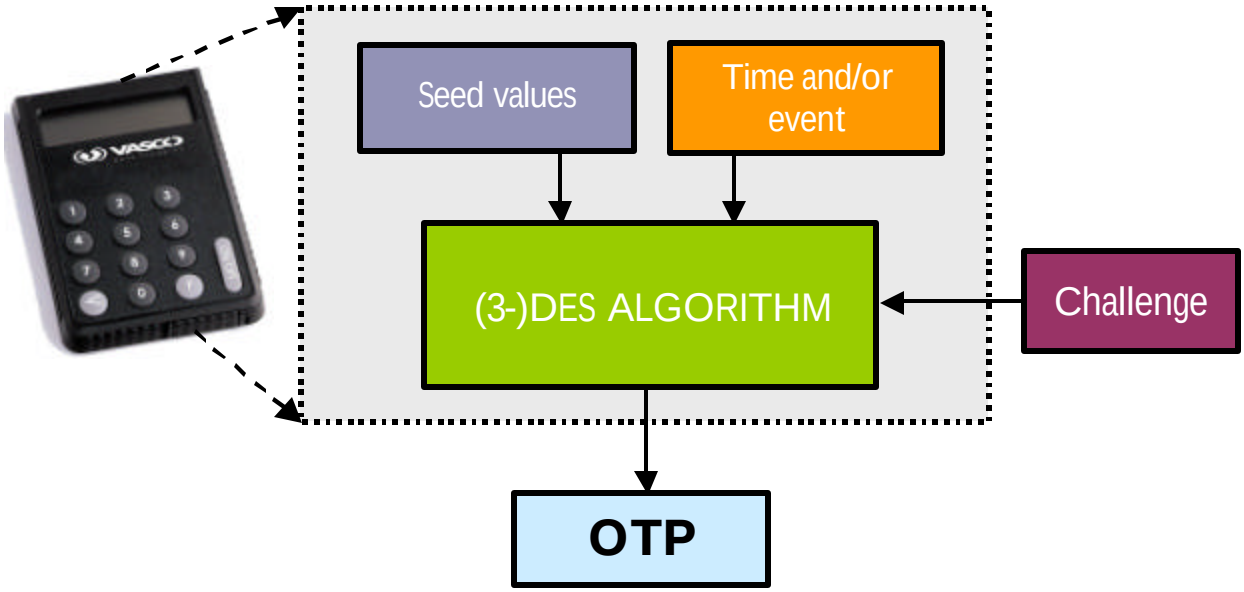

Fig 6. OTP calculation in Challenge/Response mode, time or event based

In the same way as in the "Response Only" mode the Digipass will calculate dynamic passwords as described in the above illustration. Digipass devices are pre-initialized in the same way as before, but now run an application that needs input (the challenge) coming from outside the device (the application/verification server). If time or event inputs are used they are generated in exactly the same way as they are for "Response Only" devices.
For the verification of the "Challenge/Response" dynamic passwords the treatment on the server side is a little different. The verification units are the same but the server memorises the challenge that he sent to the individual user and verifies whether the response that is given by the user matches the challenge that was issued for this user.
For more information on the implementation and integration of VASCO's AAT Libraries, please refer to the "Technical White Paper on the AAT Libraries".

3. Digital Signature Mode

The "Digital Signature" mode also known as "Electronic Signature" or "Message Authentication Code" (MAC) is not only an authentication mode (people are who they say they are) but is also as a way to secure the contents of an electronic transaction.
The Digipass can calculate a signature based upon a number of data fields created by the end-user and not by the server software. If someone wants to protect or sign a wire money transfer, he could protect data fields like, for example, the bank account number of the originator, the bank account number of the recipient and the amount of money he wants to transfer. The data fields, together with the signature, are then sent to the application/verification server to be checked for the validity of the digital signature. The digital signature is not an authentication mode as such; it protects the contents of the transaction by generating a MAC

(Message Authentication Code) on it. This means that if somebody is eavesdropping on the communication line and detects an electronic transaction, he cannot alter it in his favor. Digital signatures guarantee the integrity of the transaction that is sent.

On the application/verification server the signature is checked for the right person. This means that the server can check whether the rightful owner of the Digipass performed the calculation of the signature, and the data integrity of the transaction. In this manner the transaction is highly secured and the bank or financial institution can execute the transaction without worrying about safety issues. In the next illustration you will find a visual representation of the device usage for digital signatures.

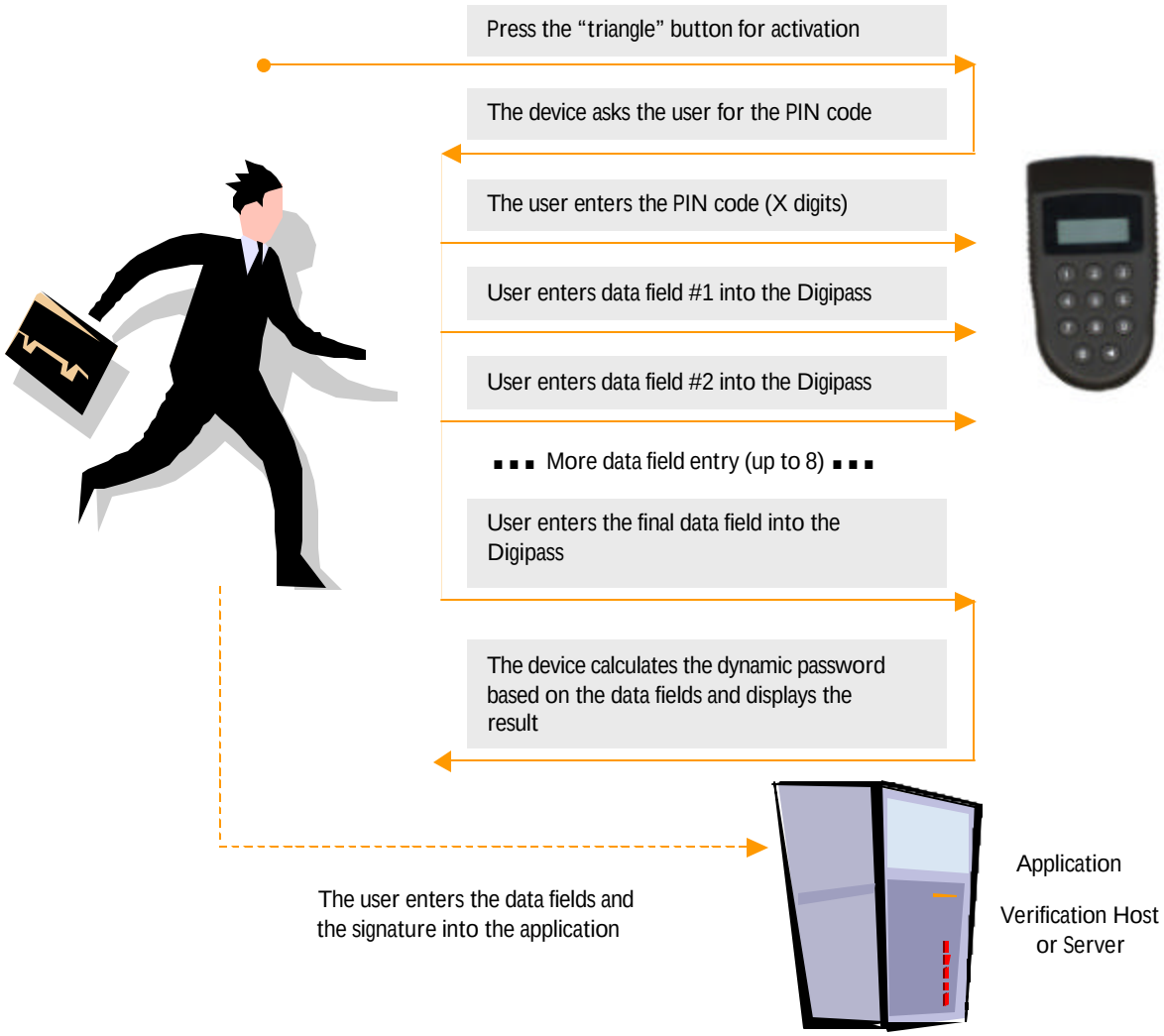

Fig 7. Usage of the Digipass 300 (Digital Signature Mode)

The data fields for the digital signature calculation are user and/or application defined: the user decides what the values for the data fields are going to be and that the application provides the user with the necessary fields to input the values

and the digital signature. Once the values are known, the signature can be calculated and the transaction can be sent. On the host side, the digital signature will be validated and a message stating the validity of the signature and the execution of the transaction will be sent to the user.

System Components

- All members of the Digipass Family (Digipass 300, 500, 600 and 700).
- Possible usage of the Advanced Authentication Libraries for integration into applications. (For more information please refer to VASCO's "Technical White Paper on AAT Libraries").
- Possible PKA library usage for integration into a PKI environment (For more information please refer to VASCO's "Technical White Paper on PKA")
-

System Requirements

Digipass security devices (hardware tokens) do not require any specific hardware or software platform since they only interact with human beings.
Integration libraries (AAT, PKA) can be used on practically any platform because of the platform independence of these VASCO products.
Shiva Access Manager for remote access runs on a Windows NT platform.
For more technical information on the above-mentioned products, please refer to the corresponding technical white papers of these products or contact VASCO.

For more information

VASCO U.S. Headquarters at:
1.800.238.2726 or e-mail your information requests to
info_us@vasco.com
VASCO Europe Headquarters at:
+32 2.456.98.10 or e-mail your information requests to
info_europe@vasco.com
VASCO Europe Headquarters at:
+33.557.19.11.00 or e-mail your information requests to
info_france@vasco.com
Or visit our corporate web site on: http://www.vasco.com

About VASCO

VASCO Data Security, a US corporation, helps organizations rapidly and effectively secure their e-business and e-commerce applications and services. The company's family of Digipass® and SnareWorks™ products offers end-to-end security through PKI, strong user authentication, true Single Sign-On, Web access control, enterprise management, and encryption solutions that also sharply reduce the time and effort required to deploy and manage them. The company has more than 100 employees in headquarters and development centers in the US, Europe, and Asia.