

PKA™ Private Key Access

Technical White Paper

PKA™ Private Key Access

Technical White Paper

Contents

Contents	2
Overview.....	3
Problem Description	4
Concept.....	5
System Components.....	7
For more information.....	8
About VASCO Data Security	9
Corporate Overview	9

Overview

In this white paper we describe the use of VASCO Data Security's Private Key Access (PKA™) concept. PKA™ is a concept in which the Private Key, used in PKI environments with a public and private key pair, is stored in an encrypted manner on the hard disk of a user's PC. In fact, any key on a hard disk that has to be encrypted, can be protected this way.

PKA™ enabled applications use a DIGIPASS® PRO 300, PRO 600 or PRO 700 and a small client plug-in software. The DIGIPASS® will produce a dynamic password each time the Private Key needs to be used. As such, it uses the strong authentication capabilities of the DIGIPASS® family.

Strong authentication is based on two-factor security:

- Something the user knows (the PIN code to activate the DIGIPASS®)
- Something the user possesses (the DIGIPASS® itself)

Without having these two factors at the same time, the correct dynamic password can not be generated and it is impossible to fake or guess one. Therefore the Private Key can not be accessed even if this is stored on the hard disk.

Please refer to the "DIGIPASS® – a Family of Tokens - Technical White Paper" for more detailed information on strong two-factor authentication devices.

Fig 1. From left to right the PKA™ capable devices: DIGIPASS® PRO 300, DIGIPASS® DESK 300C, DIGIPASS® PRO 600 and DIGIPASS® PRO 700.



Problem Description

Today everyone is talking about Public Key Infrastructure (PKI). This is a concept in which asymmetric key pairs are created via the RSA algorithm and then distributed to the users. Such a key pair consists of a Private Key and a Public Key (RSA Algorithm for encryption). This key-pair owner can now distribute or publish his Public Key but guards his Private key with great care. Without going into detail on the rest of the concept of a PKI, the goal is that anybody can now encrypt a message with this public key and send it to the owner of the Private Key. The message can be intercepted but not decrypted because this can only be done with the Private Key. This means that only the real addressee can decrypt and read the message. Vice versa, the key-pair owner can encrypt a message with his Private Key and send it to somebody who has his Public Key. If the addressee can decrypt the message he knows that he holds a message sent to him by the right person.

It is obvious that the security level of such a system stands or falls with the way this Private Key is safeguarded.


The two most common safe storage techniques today are either: (1) on a smart card that can be inserted into the PC anytime the Private Key is needed, (2) to store the Private Key on the PC's hard disk and use a static password or pass phrase to decrypt it. Since static passwords are easy to compromise and can be broken into in no time, this method lacks security. PKA™ is the answer to this lack of security because it will replace that static password with a dynamic password generated by a DIGIPASS®.

Concept

The concept is explained by means of two visual representations. The first one shows how the dynamic password is generated on the DIGIPASS® side. The second one shows a representation of the way the dynamic password is verified by the application running on the client's PC.

Fig 2. The initialization parameters for PKA™ in a DIGIPASS® PRO 700.





While the DIGIPASS® gets initialized, the special secret key. K2 is generated by the initialization software as well as the normal key Kdp. Once the key is generated it will be programmed into the DIGIPASS®. This secret key K2 is the primary element to the usage of PKA™. It is this K2 that will be regenerated by the PKA™ verification software on the client PC, to encrypt and decrypt the Private Key of the RSA key pair.

In order to verify this dynamic password on the PC side there are a few things to do. One is to import the DIGIPASS® secrets into the application's database. In normal DIGIPASS® enabled applications, you would need to use a DIGIPASS® import file (*.DPX format) in order to store the necessary DIGIPASS® secret keys into the database system of the application. This import file would then be read by the application software to import the initialized Digipasses into its database in an encrypted format.

In order to keep the total cost of ownership for the application as low as possible, instead of using an import file you now can use a simple activation code. This activation code will be sufficient to activate the usage of a unique DIGIPASS® for PKA™ usage into your client PC application. The initial time you use the application, the software will ask you to enter this activation code and will then ask you for a PKA™ dynamic password twice. This double dynamic password is used to check whether you have received the right activation code for this DIGIPASS®. If you have received the right activation code, the application software will immediately encrypt your Private Key. From that point on, you will need a PKA™ enabled DIGIPASS® to be able to decrypt your Private Key.

In the next scenario you can take a look at the way the dynamic password is used to protect the Private Key is verified on the client PC.

Fig 3. The verification process of a PKA™ dynamic password on a client PC.

INPUT

RESULT



If you compare Fig. (2) with Fig. (3) you will see that there are two fields that have switched positions between the input and the result side. The dynamic password is now an input field and this is because it needs to be verified, and the Secret Key (K2) has become the result of the calculations performed by the PKA™ library integrated into the application. In fact, it looks as if the secret key K2 has been exported out of the DIGIPASS® into the application. As mentioned before, the secret key K2 is the key element of PKA™. This means that the encryption and decryption of your locally stored Private Key can be performed based on this secret key K2 that is never stored on your hard disk. Since we now reached the point where a locally stored Private Key (or any other piece of information that is stored) can be encrypted and decrypted by means of a dynamic password, we finalized the concept of the Private Key Access possibilities of a DIGIPASS® security device.

System Components

- Following members of the DIGIPASS® Family of tokens support PKA™:
- DIGIPASS® PRO 300
 - DIGIPASS® PRO 600
 - DIGIPASS® PRO 700

- The usage of VASCO's Private Key Access Toolkit.
- This toolkit contains all routines (native C source code) needed to convert an existing or new application into an application that uses dynamic passwords in combination with an encryption protection for your private information stored on your system.
- The toolkit is an integration tool for the client PC application. It serves both the purposes of initializing the application with a PKA™ dynamic password, as well as, verifying the PKA™ dynamic passwords generated by a member of the DIGIPASS® Family of Tokens.

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

Or visit our corporate web site on: <http://www.vasco.com>

About VASCO Data Security

Corporate Overview

VASCO designs, develops, markets and supports patented “Identity Authentication” products for e-business and e-commerce. VASCO’s Identity Authentication software is delivered via its Digipass security products, small “calculator” hardware devices carried by an end user, or in a software format on mobile phones, other portable devices, and PCs. For user access control, VASCO’s VACMAN products guarantee that only designated Digipass users get access to the application. VASCO’s target markets are the applications and their several hundred million users that utilize fixed passwords as security. VASCO’s time-based system generates a “one-time” password that changes with every use, and is virtually impossible to hack, or break. With 10 million Digipass sold and shipped, VASCO has established itself as a world-leader for strong Identity Authentication with 200 international financial institutions, approximately 1000 blue-chip corporations, and governments representing more than 60 countries.

Corporate Mission:

Be The Authentication Company worldwide, anyhow, anywhere, anytime.

Some facts about VASCO

- **Structure**
A public corporation traded on NASDAQ under the symbol VDSI.
- **Founded**
1997
- **Products**
VASCO's family of Digipass® and VACMAN® products offer end-to-end security through strong authentication and digital signature, while considerably reducing the time and effort required to deploy and manage security.
- **Customers**
Almost 200 financial institutions worldwide, several hundreds of corporations and government agencies including many members of the Fortune 500.
- **Users**
More than 10 million people worldwide use VASCO's security products.
- **Geographic Reach**
VASCO has customers in more than 60 countries.

- **Employees**

80

- **Locations**

Headquarters in Chicago and Brussels with operations in Bordeaux (France), Brisbane and Sydney (Australia), and Singapore.

- **Partners**

VASCO's Partner Alliance includes notable partners such as Novell, Europay-Mastercard, Entrust, Telindus, Ubizen, Polizer & Haney, Cisco, Checkpoint, Lucent and Microsoft.