

Digipass and PKI

A white paper on how Digipass®
enables your PKI environment



THE AUTHENTICATION COMPANY

Digipass and PKI

A white paper on how Digipass® enables your PKI environment

Contents

Contents	2
Introduction.....	3
PKI.....	3
Storing and accessing the private key	4
PKA	5
Digipass® enables private key stored on the local hard disk	5
Digipass® 850	5
Digipass® enables private key stored on a Smart Card.....	5
Server based PKI credentials	6
Digipass® enables private key stored on a central server	6
About VASCO Data Security	7
General	7
Digipass product range.....	8
VACMAN Product Range.....	9



Introduction

This document is intended for companies and financial institutions that are considering setting up a public key infrastructure (PKI) or those that already utilize Digipass® technology for authentication and secure transactions. This document explains the different ways Digipass® technology can be used to help resolve some of the common problems encountered when deploying or migrating to a PKI in an enterprise or banking environment.

This document assumes that the reader is familiar with the concept of two-factor strong authentication. If this is not the case, the reader is encouraged to refer to the “*Digipass – a family of tokens - Technical White Paper*” for more detailed information on two-factor strong authentication devices.

This document also assumes that the reader is familiar with the basics of PKI.

PKI

Every public key infrastructure (PKI) relies on the use of asymmetric cryptography. In contrast to symmetric cryptography (where the same secret key is used for encryption and decryption), in asymmetric cryptography two different but complementary keys are used for encryption and decryption. The two keys of such a pair of corresponding keys have the following properties. Any document that has been encrypted by one key of the key pair can only be decrypted by the other key of the key pair. And conversely, if it is possible to decrypt a document with one key of the key pair, then it automatically follows that the document must have been encrypted by the corresponding other key of the key pair and by no other key.

These two properties are behind the two major benefits of any public key infrastructure i.e. respectively secure communication between two parties that have never been in contact before (or have otherwise been unable to exchange a secret key), and non-repudiation of digital signatures.

In a public key infrastructure every participant has their own pair of keys. One of the keys is referred to as the private key and the other as the public key. Every participant makes their public key publicly available and jealously keeps their private key secret. To secure communications a sending participant uses the public key of the receiving participant to encrypt a document. Only the private key of the receiving participant can be used to decrypt the document. To make a digital signature, a participant uses their private key. Anyone can

then verify this signature by using the corresponding public key. To unambiguously link a public key to a specific identity, certificates are used.

A certificate is a formal statement linking a public key to an identity, which has been digitally signed by a trusted authority. It is assumed that every participant knows and trusts the public key of that trusted authority.

Storing and accessing the private key

Large scale deployments of public key infrastructures are being hampered by a number of issues regarding the deployment of client PKI credentials. Storage of and access to the private key raise major protection issues when deploying any PKI.

Obviously, the private key must be stored in a very secure way such that only the rightful owner can have access to it. On the other hand, using the private key must be convenient, and the total cost of the chosen solution must remain cost-effective. Commonly, private keys are stored on a smart card or on an end-user's local hard disk.

The local hard disk has the distinct advantage that it comes at no extra cost. Distribution of the keys and certificates is relatively simple as it is no different than installing a personalized piece of software. Its disadvantages are that, as a software solution, it is insecure (see below) and the end-user is tied to the PC on which the keys and certificates are located.

Smart cards by themselves are very secure. They are also more mobile than the local hard disk. A main disadvantage is that smart cards require a card reader that is physically connected to the end-user's device. Not only does this represent an additional, non-negligible cost, in practice it also can cause considerable deployment problems. Problems of incompatible drivers or connectors are unfortunately still quite common. This is especially the case in environments with a heterogeneous IT infrastructure such as in large companies or a bank's customer base. Furthermore, the use of smart cards with typical card readers presents security challenges addressed below. For PDA's and smart phones it might even be impossible to attach a smart card reader.

It is clear that, as with so many technological problems, the choice of storage medium for PKI data is a trade-off between convenience, security and cost. The following paragraphs explore ways in which Digipass® technology can be used to reduce the trade-offs.

PKA

Digipass® enables private key stored on the local hard disk

A public key infrastructure using the local hard disks as storage medium generally relies on static password derived encryption to protect the access to the PKI credentials. As is generally accepted, static passwords offer only a very low level of security as people tend to choose passwords which are easy to remember (and therefore easy to guess), or they write them down on post-it notes attached to the PC.

A much better level of security can be reached by replacing static passwords with dynamic or one-time passwords. This is exactly what VASCO Data Security's Private Key Access technology offers. PKA enabled applications use a Digipass® (whether this Digipass® is a hardware token, or a soft token installed on a PDA or mobile phone is of minor importance) 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, PKA uses the strong authentication capabilities of the Digipass® family. This dynamic password is used by the verification software on the client PC to regenerate the secret key that is used for the encryption and decryption of the private key.

For more information on PKA refer to “PKA – Private Key Access – Technical White Paper”. PKA has been incorporated into the PKI product suite of Entrust.

Digipass® 850

Digipass® enables private key stored on a Smart Card

If the PKI credentials are stored on smart cards, all client PCs, workstations and other devices from which these PKI credentials have to be accessed, must be equipped with smart card readers. In general, smart cards holding private keys protect access to these keys by means of a PIN. Using a smart card but accepting PIN entry via the inherently insecure PC keyboard and screen can give a false sense of security.

Indeed, it is quiet conceivable for some rogue piece of software to retrieve the PIN by monitoring the user's keystrokes. Once the PIN has been captured nothing prevents that rogue software from accessing the smart card's private PKI capabilities for its own nefarious or plainly unauthorized purposes without the end-user even realizing that their PKI smart card is being used. To prevent such a scenario one needs a smart card reader with local PIN entry capabilities. If carefully constructed, such a reader can guarantee that no software on the PC will ever be able to capture the PIN and that the private key can only be accessed if the PIN has been successfully entered on the reader itself.

VASCO's DP850 is a trusted smart card reader with local PIN entry and local PIN change capabilities.

The competitive edge of the DP850 (with respect to any other competing smart card readers with PIN pad) is that it can also be used in unconnected mode. In unconnected mode it emulates a traditional Digipass® **strong authentication token**. *It does not however contain any personalized data, but instead relies on the personalization of the inserted smart card.* This means that financial institutions and companies that already have invested in a Digipass® infrastructure can be given a smooth migration path when they decide to roll-out a smart card based PKI infrastructure.

Since the DP850 can also be used in an unconnected mode, it also offers an elegant fall-back option as users equipped with a DP850 can still conduct secure transactions even in an environment that doesn't support connected smart card readers (e.g. over the telephone, or for users on business trips, or in small companies with a not-so-up-to-date computer infrastructure).

Examples of PKI smart cards that can be used with a DP850 in this way include Datakey Model 330, Gemplus GPK and Proton Prisma.

Server based PKI credentials

Digipass® enables private key stored on a central server

Conventional PKI solutions often require the end-user to generate the key-pair, submit the public key for certification, and securely manage their private key, thereby pushing much of the security and management burden to the user or client application. It is argued that this is necessary to ensure that only the end-user has knowledge of, and access to, their private key. In some environments where a PKI deployment is considered, there is however a formal trust relationship governed by contracts between the end-users on the one hand and the issuer of PKI credentials on the other hand e.g. between a company and its employees or between a bank and its customers.

In such environments, a very interesting alternative is to store the PKI keys and certificates on a central server. As for any other centrally managed resource, access to these centrally stored PKI credentials is granted to the end-user only upon successful authentication. VASCO Data Security's Digipass® technology (in whatever form factor: hardware tokens, soft token, PDA, mobile phones, etc.) is ideally suited to secure this authentication process. The client application can then access the PKI credentials through a piece of software that often formally looks as if it were a smart card driver. The terms 'roaming certificates' or 'virtual smart card' are often used to label this kind of a PKI solution. From a security perspective, a clear distinction must be made between solutions whereby the private key never leaves the server and solutions whereby the private key is sent to the client when needed.

This approach has several appealing advantages. The mobility is considerably increased as the PKI credentials can be accessed from any client PC without requiring special hardware to be connected to the PC. If the private key never leaves the server and depending on the implementation details, the overall security can be similar or even better than that of smart cards based system, as all state of the art security technology (firewalls, hardware security modules, strong two-factor authentication, ...) can be used. The total cost can be kept relatively low as the existing authentication and authorization infrastructure can be leveraged. Finally, this solution makes it possible for banks and companies to centrally enforce policy, and to manage and control access to the PKI credentials they have issued, when dealing with the revocation and replacement of obsolete or compromised certificates.

Examples of companies that offer products that in one form or another use such a server based approach protected by Digipass strong authentication tokens include Cryptomathic, Authentidate and CyberSafe.

About VASCO Data Security

General

VASCO Data Security International, Inc. (VDSI) designs, develops, markets and supports open standards-based software and hardware security products, which manage and secure access to information and financial assets. Securing trust, securing value is the company's creed. VASCO's range of enterprise-wide products secure Internet, client/server, and mainframe-based applications, and provide end-to-end security through Radius, LAN and Web security, PKI and LDAP enablement, web portal and application security, strong user authentication, access control, user administration and encryption.

VASCO's products are used by more than 7 million users, by over 180 financial institutions and by hundreds of blue-chip corporations and governments, spanning over 50 countries.

VASCO is a global company with headquarters in the United States.

Company:	VASCO Data Security International
NASDAQ NM/NASDAQ EU.:	VDSI
Founded:	1997
Web:	www.VASCO.com
CEO	Ken Hunt
President and COO:	Jan Valcke
Employees:	80
Worldwide Headquarters:	1901 South Meyers Road, Suite 210, Oakbrook Terrace, Illinois, USA
European Headquarters:	Koningin Astridlaan 164, B-1780 Wemmel, Belgium

VASCO Product Range:

VACMAN: Authentication, Authorization, Administration, AAA Security
Digipass: Encryption, Remote Access, Corporate Access, Hard- & software tokens

VASCO's roots are in cryptography. It was the first company in the world to port the DES and RSA algorithms to a chip and also the first to develop a software product to authenticate and digitally sign e-banking and online brokerage services. Now, VASCO secures the enterprise from the mainframe to the Internet with infrastructure solutions that enable secure e-business and e-commerce, while protecting sensitive information and safeguarding the identity of users. The company's family of Digipass® and VACMAN® products offer end-to-end security through strong authentication and digital signature, enterprise Single Sign-On, and LAN security, while sharply reducing the time and effort required to deploy and manage security.

Digipass product range

DIGIPASS® provides financial institutions and companies with a secure means of customer or employee identification and authentication for remote access to their computer systems and networks.

Digipass stands for three ranges:

Digipass Pro:

Digipass Pro includes Digipass models for professional use, offering dynamic password and digital signature functionality.

- Digipass Pro 300 is ideally suited for large public banking applications such as telebanking, home banking, PC banking, phone banking and Internet banking where authentication and e-signatures are key requirements.
- Digipass Pro 550 combines strong authentication, e-signatures and a modern design with integrated hardcover.
- Digipass Pro 600 grants physical access to buildings as well as secure remote network access.
- Digipass Pro 700 offers sophisticated and yet user-friendly strong authentication services with extended digital signature capability.
- Digipass Pro 800 is used by several top tier banking institutions worldwide and is strongly appreciated by the banks and their clients for securing full access to financial applications on the existing banking network via an existing smart card, in a flexible, easy to use and cost-effective way.

Digipass GO:

Digipass GO can be used Anywhere, Anyhow and Anytime. It is e-security that fits in your pocket, clips on your belt, hangs around your neck, on a key ring.

- Digipass GO 1 is the first-born in the "GO" range. GO 1 is an ultra-portable, smoothly designed token that outsmarts all others and is much safer than any static password.
- Digipass GO 10 is a software Digipass for GSM's, integrated on the SIM card.

Digipass Desk:

The Desk-range contains highly user friendly Digipass models to be used on a professional's desk.

- Digipass Desk 300 is a large-scale security device designed for managers and executives. It features remote access and authentication features and its larger size makes it very suitable for use in the office.
- Digipass Desk 850 can future-proof an existing smart card system, increase a network's security and leverage investment in a public key infrastructure (PKI) solution. This advanced e-wallet/PKI device provides ultimate versatility and security, supporting strong authentication and e-signatures for the customers authorized to carry your smart cards.
- Digipass Desk 3000 is a software Digipass for laptop & desktop.

VACMAN Product Range

VACMAN Controller integrates smoothly into existing applications that require remote access.

VACMAN RADIUS Middleware enables strong authentication security without replacing or redesigning your remote access solution(s).

VACMAN Server is a cross platform authentication engine designed to provide strong and seamless user authentication and access control for remote, local and web-based users. The product supports RADIUS, LAN and Web functionality.

- *VACMAN Server for RADIUS* is a standard compliant server designed to provide AAA services.
- *VACMAN Server for Networks* provides strong user authentication and access control management for RADIUS and LAN environments in a fully integrated system.
- *VACMAN Server for Web* delivers access control to Web enabled applications, whether Internet , extranet or intranet based.