How to secure USB e-Token using VaultIC™ Security Modules?
Table of Contents

Introduction .......................................................................................................................... 5

1 Needs and Threats ........................................................................................................... 6
   1.1 Today’s needs ........................................................................................................... 6
   1.2 Threats .................................................................................................................... 6
   1.3 Software-based solutions are unsuited ................................................................. 7

2 The USB Token Solution .............................................................................................. 8
   2.1 Strong authentication ........................................................................................... 8
   2.2 Two-Factor authentication devices ........................................................................ 8
   2.3 The USB e-token solution ................................................................................... 9

3 VaultIC solution .......................................................................................................... 11
   3.1 What are the benefits of Smart-Card-based USB tokens? ............................... 11
   3.2 Strong Authentication application ....................................................................... 12
   3.3 Secure Storage applications .............................................................................. 19

4 Conclusion .................................................................................................................... 22

Definitions & Abbreviations ......................................................................................... 23

Revision History .............................................................................................................. 25
Today’s enterprises need new methods of developing trust in a virtual world. Wherever Internet access is available, business operations can occur. However, with expanded access to networks, enterprises are finding it increasingly difficult to authenticate who someone is. As well as being concerned about identifying authorized parties, enterprises are also becoming increasingly worried about ensuring and maintaining the security of proprietary information and privacy protection.

Easy-to-use and bringing a high level of security, USB tokens enable data protection and user authentication before any access to a network is granted. Using a multi-factor authentication, these tokens respond exactly to the enterprises’ needs.

VaultIC USB Security Modules - based on highly secure microcontrollers used in Banking or ID markets that need a high level of security - respond to these challenges, thanks to their embedded firmware which provides strong authentication mechanisms.

Depending on the size of the data which needs to be secured, the VaultIC USB Security Modules Family, composed of ATVaultIC420, ATVaultIC440 and ATVaultIC460 products, can provide an appropriately sized product.
1. Needs and Threats

Today’s enterprises have specific needs, briefly described below, however, unless appropriate protection is provided, meeting these needs may result in identity theft.

1.1 Today’s needs

1.1.1 Increasing productivity

In the business world, mobile workers are more and more numerous, and mobility is critical to business success. To avoid missing any business opportunity, enterprises want to allow their clients, partners or employees to access company’s resources and applications wherever they are (office, home, business trip...), by using high speed networks and public Wi-Fi hotspots.

Obviously everybody wanting to access these resources must first be authenticated.

1.1.2 Securing mobile data

Thanks to expanded mobile networks and mobile data storage possibilities (laptops that can reach 500 Gigabytes and above, USB keys...), workers are taking more sensitive data on the road with them. While mobile computing is a key to success, it poses considerable threats to corporate data. Indeed equipment such as laptops, PDAs, and memory cards are becoming more frequently stolen. On any mobile computing device, we can find private information (user identities complete with access information such as passwords and account numbers, social security numbers...) or sensitive information (financial data or email messages discussing sensitive projects...)

These data are confidential and must be protected from unauthorised access.

1.1.3 E-banking

For sensitive applications such as e-banking, security is obviously mandatory: for online banking operations or any online service offered by financial organizations, both parties need guarantees about who is on the other side. Indeed the major issue in these exchanges is identity theft, particularly by phishing. In this case, trusting the person you are speaking to requires mutual authentication.

1.2 Threats

1.2.1 Identity theft and phishing

ID theft is one of the biggest issue that plagues consumers, business and law enforcement. In particular, this is preventing financial institutions and their customers from achieving a secure world for online banking. Financial Insights estimates that in 2005 nearly 8% of American consumers, or 18 million people, have been victims of ID theft. Types of identity theft are represented in the figure below.
"Phishing is the criminal fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication" (source: Wikipedia). This fast-growing type of online fraud is called the "hottest, and most troublesome, new scam on the Internet" by the FBI. Banking institutions are the main target of the phishing attacks. To fight against phishing, government regulators and leading institutions worldwide are taking actions, such as introducing data protection laws and privacy legislations (HIPAA, FDA, Sarbanes-Oxley...). These regulations force organizations to safeguard personal data stored on their systems, or face stiff penalties.

1.2.2 It costs dearly!
In addition to the risk of stiff penalties, the company’s reputation can be damaged (customers must be notified of any data privacy breaches, and these breaches are reported publicly). The costs associated with breaches can be huge: bring in investigators, invest in new security, respond to lawsuits, not to mention costs to a company’s long-term competitive advantage if sensitive intellectual property is stolen (e.g. product roadmaps, design plans, financial information).

1.3 Software-based solutions are unsuited

1.3.1 Passwords
Nowadays, passwords are the main way of authentication, but passwords are weak because they are:

- Difficult to setup: Password formats are different across applications (case, numeric...), some passwords need to be changed periodically and others can last forever. Password overload is becoming a continual headache for network security administrators.
- Difficult to use and so not secure: Users today have an average of 15 password-protected accounts. So usually users choose the same passwords for several accounts, and they are...
usually easy to guess. When passwords are complex, de facto they are difficult to memorize. Thus users have to write them down, further compromising security.

- **Expensive**: Users that do not write their passwords often forget them, so call the helpdesk to reset them, consuming time and the cost of IT support.
- **Easily "crackable"**: Many efficient tools are available using "Brute Force" attacks to find passwords.

Concerned about these security issues, enterprises are looking for other ways of authentication.

### 1.3.2 Software tokens

The software encasing a user's private keys or a certificate is often called a software token. The user's private key is retrieved from the software token in order to sign or decrypt. The main problem with software tokens is that they rely on the integrity of the computer on which they reside, so they are exposed to threats such as physical access (laptop lost or multiple users working on the same machine), and malicious software (viruses, worms, trojan horses...). So security may be compromised.

### 2. The USB Token Solution

#### 2.1 Strong authentication

For high level security, the scheme must include a three-factor authentication: *something you have* (a hardware component), *something you know* (password, PIN...) and *something you are* (biometric feature). Using more than one factor is called strong authentication.

The most popular and effective solution of strong authentication is the two-factor authentication combining a token or smart-card with a PIN or a password, supported by a token lifecycle management system.

#### 2.2 Two-Factor authentication devices

Various types of two-factor authentication devices exist:

- **Smart-Cards**: They provide highly secure storage, and they are able to generate keys and perform cryptographic operations on-board without exposing the user's private key to the computer environment. But they require a dedicated reader.
- **USB Tokens**: Users are granted access upon plugging the token into a USB port and entering the token password.
- **Smart-Card-based USB Tokens**: They contain a secure microcontroller (built-in smart-card technology), so provide the same level of security as a smart card but with no need for a reader.
- **One-Time Password (OTP) Tokens**: They generate a password for one-time use. The user enters the one-time password appearing on the token and this value is compared to the value generated by the authentication server (usually used for VPN access from a PDA or a cellphone).
- **Hybrid Tokens**: They combine multiple types of authentication functionality on a single device: USB and OTP tokens for instance.
- **Software tokens**: They are software programs stored on a laptop for instance, that can generate a one-time password, for accessing online services or authorizing transactions. But they are not as secure as hardware tokens.
2.3 The USB e-token solution

An increasingly popular strong authentication method is a USB tokens which acts like keys, thanks to the cryptographic algorithm embedded in a plug inserted into the USB port. These tokens have a stronger authentication scheme than tokens generating one-time passwords, since they have digital certificates embedded within them and can also store data.

The figure below illustrates the comparison between tokens regarding Security and User Acceptance.

**Figure 2-1.** User Acceptance of various secure devices

Users authenticate themselves to their computer by simply plugging in the token into a USB port and enter their PIN or password. These tokens are very convenient for users since they can store credentials for an SSL or IPsec VPN access for instance, or multiple passwords to multiple applications to which the user has access over the corporate network. With these capabilities, users do not need to remember and handle all their passwords, they only need their token and one password to enter all their accounts.
2.3.1 Benefits of USB tokens

- Easy-to-use / user-friendly: plug and play simplicity, no software installation required.
- Users don’t have to enter passwords manually, so can use complex passwords.
- Hassle-free: no maintenance, never expires, no battery replacement required.
- Portable USB design: no reader needed
- Secure storage of users’ credentials, keys and sensitive data
- Lower Cost: no cost of maintenance and support of desktop-based clients
- High level of identity assurance: private keys are never exposed outside the token

2.3.2 Applications using USB tokens

- Secure log-on
- Secure access
- Banking environment / e-commerce
- Secure e-mail communications
- ...
3. VaultIC solution

VaultIC USB microcontrollers are Secure Microcontrollers that contain a turnkey firmware that supports PKCS#11-enabled applications and the Microsoft® Card Minidriver specification. They provide digital signature, encryption, key management functions and a full-speed USB 2.0 interface with a software stack. The integrated USB-CCID implementation makes these chips behave like a smart card reader with an emulated smart card inside. Therefore tokens using VaultIC microcontrollers can directly interface with common applications running on computers (Windows Logon, Mail clients, Web browsers...) through PKCS#11 libraries or Microsoft Cryptographic Service Providers (CSP). Moreover they support SSL and TLS protocols.

Because form factor is important for the integration in an embedded system, especially on a PCB, the VaultIC-based device is available in SOIC-8 (Small Outline Integrated Circuit, 8 pins) or QFN-44 (Quad Flat No leads, 44 pins). For more details about these packages, please refer to the technical datasheet of the VaultIC security modules.

3.1 What are the benefits of Smart-Card-based USB tokens?

Smart-Card-based USB tokens which contain a Secure Microcontroller chip inside (commonly called a Smart-Card chip) provide the functionality of both USB tokens and Secure Microcontrollers. They enable a wide range of security solutions and provide the abilities and security of a traditional Smart-Card without requiring a dedicated Smart-Card reader. VaultIC microcontrollers family are based on Smart-Cards.

The "Smart-Card" chip inside a USB token is a Secure Microcontroller specifically designed to protect against hacking techniques such as direct attacks (code injection, buffer overflow, external intrusions, spying bus...), SPA and DPA attacks (using "side channels" such as power consumption), fault injection (test mode activation, protection fuse bypassing easing reverse engineering, glitch attacks...), internal memories analysis.

In addition, Secure Microcontrollers contain dedicated hardware which enables fast and secure cryptography.

Security Certifications such as Common Criteria or FIPS 140 provide a commonly recognized level of confidence in information technology products so that they can be used without the need for further security evaluation.
For more details about Secure Microcontrollers in Systems, please refer to the document "Secure your Embedded Devices" (6528) available on the Inside Secure Web Site.

3.2 Strong Authentication application

The most famous strong authentication methods are One-Time Password authentication and authentication used in Public-Key Infrastructure (PKI). These and others, can be provided using VaultIC turnkey solutions.

3.2.1 Introduction to Public Key Infrastructure (PKI)

In cryptography, a PKI is the way that public keys are bound to user identities by means of a Certificate Authority (CA), a Registration Authority (RA) and a Validation Authority (VA). Indeed it is important to encrypt a message with the recipient’s key and not any other key, like the attacker’s key. Moreover it is important to be able to verify the identity of the signer for a signed document. For each user, the user identity, the public key, their binding, validity conditions and other attributes are made unforgeable in public key certificates issued by the CA.

The PKI architecture is detailed on the diagram below.
The first concept of a PKI is the Certification Authority (CA). The CA confirms who is the owner of the private key corresponding to the public key and fixes the correspondence between both. The CA issues and controls a so-called "electronic certificate" as the authorization of this correspondence. In particular, set up as an organization with responsibility for checking the certification of the key holder with the CA, the Registration Authority (RA) verifies the identity of the key holder in face-to-face manner. The RA might be or might not be separate from the CA.

As the second key concept in PKI, a Validation Authority (VA) is set. The VA is a body for checking the legality of electronic certificates; namely, whether a certificate is valid and whether that certificate was issued by a trustworthy CA. Since the PKI is a system to prevent spoofing, the procedure that checks the validity of the electronic certificate is said to be the most important among the PKI operations.

In short, a PKI is essentially a way of distributing public keys in a secure way, thus enabling users to securely exchange data and financial assets across networks and over the Internet.

VaultIC-based USB tokens add security and portability to PKI solutions by generating public keys and storing user digital certificates and keys: users only have to plug their tokens into any computer to use them. Moreover, unlike private keys normally located in a computer, and therefore susceptible to e-thieves, token-based private keys are generated on-board the token itself, where they are securely stored – always in the possession of the user and never exposed to the PC.
3.2.2 Example: Secure Web Browsing

Well known examples of PKI enabled applications are Internet browsers, such as Mozilla Firefox or Internet Explorer. They use the software modules Microsoft CSP and PKCS#11 which are able to use cryptographic security of hardware-security-modules like smart cards or tokens.

VaultIC-based USB tokens support PKCS#11-enabled applications and Microsoft card minidriver for Base CSP, creating a secure environment for PKI solutions (see Figure 3-3).

Figure 3-3. VaultIC-based USB tokens with Web browsers

VaultIC-based USB tokens are capable of generating and storing cryptographic keys and certificates securely, and signing data with these keys.
3.2.3 VaultIC family supports SSL / TLS protocols

For more flexibility, VaultIC chip supports Secure Sockets Layer (SSL) and Transport Secured Layer (TLS) protocols (TLS is the most recent version of SSL). These protocols are protocols on the layer between Transport and Application Layers, independent from the protocol used in the Application layer. So it means that it can be used to secure a Web transaction, send/receive emails, etc.

SSL is transparent for the user: for example, a Web user wanting to connect to an e-commerce site secured by SSL will send sensitive data with no additional step for securing it. All internet browsers support SSL protocol: Netscape Navigator and Microsoft Internet Explorer show a little padlock when connecting to a website secured by SSL. A Web server secured by SSL has a URL beginning by https:// ("s" means secured).

SSL uses public-key cryptography to secure the transmission on the Internet, opening a secure channel between the client and the server, as shown on the Figure 3-4.

**Figure 3-4.** Authentication in SSL/TLS

To use SSL/TLS, a Web server must acquire a server’s digital certificate (format x509) from a Certification Authority, a third-party organization that issues digital certificates. A digital certificate guarantees that the public key contained in it belongs to its owner so that the receiver of a digitally signed message can verify the authenticity of the signature. Contrary to the server's authentication which is mandatory, the client’s authentication is optional, but more and more web applications use client’s authentication thanks to TLS. Figure 3-5 shows the exchanges between client and server for a client SSL authentication.
Thanks to VaultIC chip embedded in a USB token where the client can store his certificate, it is possible to offer a mutual authentication between the client and the server, and therefore a strong authentication.

### 3.2.4 One-Time Password authentication (OTP)

A One-Time password is a password that changes after each login or after a set time interval. Passwords are generated from a secret shared key and using a complex mathematical algorithm (standardized HOTP algorithm). Each password is unguessable, even when previous passwords are known.

Time-based One-Time Password (TOTP) algorithm is an extension of one-time password algorithm HOTP to support time based moving factor. Thanks to its hardware Real Time Clock, the VaultIC family supports TOTP algorithms.

This authentication provides an access to a secure network using a single password and usable only once.
Figure 3-6.  TOTP-based USB Token

Figure 3-7 is an example of secure logging using OTP authentication.

Figure 3-7.  Secure Login using OTP authentication

VaultIC Family
3.2.5 Hybrid Token

Both authentication processes, OTP and PKI-based, can be combined in one token. In this case, the customer can access networks in different ways. For instance, the USB interface allows the user to plug directly into a USB port and gain access quickly and securely. However, sometimes USB connection is not available: in those cases, the OTP feature is perfect. At the push of a button, the token displays a one-time password on a small, built-in display. The OTP can be entered using the keyboard for secure access even from a public terminal like an airport internet kiosk, or from behind a firewall at a client site.

**Figure 3-8.** Secure Accesses using a USB e-token

3.2.6 Inside the token

A VaultIC Module can be considered as a secure box, storing secrets seamlessly and securely. To do this, the secret objects are stored in the secure EEPROM memory of the module, in the form of a dynamic file system. For USB tokens, the file system downloaded by the manufacturer in a VaultIC might be composed as follows:

- **Administrator data**: file system version, private keys.
  
  These data allow the Administrator to be authenticated to upgrade keys, change administration data, update software...

- **User data**: identifier, private keys, certificates.
These data allow the token user to be authenticated on a network or on a machine. For more security these data are unique per chip and per user.

- **Application data**: depends on the application.

Figure 3-9 shows examples of integration of a VaultIC microcontroller into a USB token.

**Figure 3-9.** VaultIC Solution Integration for Authentication applications

---

### 3.3 Secure Storage applications

Secure portable virtual desktops or applications, secure data storage, encrypted backup, password manager application... so many possible applications thanks to the VaultIC security modules. Some of these typical applications using VaultIC modules are described below.

#### 3.3.1 Secure Portable Virtual Desktop

When considering how to increase business opportunities while maintaining a high level of security, we can imagine a secure portable virtual desktop in a VaultIC-based USB token. The high level of security can be achieved thanks to the VaultIC device and a Flash memory can offer a large memory needed for a complete virtual desktop environment, both communicating through an SPI connexion for instance. The hardware encryption mechanisms of the VaultIC device, much faster than software encryption, make the virtual desktop setup transparent to end-users.

Employees can then carry and securely use their working environment, included applications, data, users preferences and passwords, wherever they go.
3.3.2 Password Manager

An application such as Password Manager installed on a VaultIC-based USB token increases significantly the level of security of the environment: all passwords are stored securely in the USB key, this avoiding the need for the user to remember them. Such an application will automatically fill all the required fields with the correct parameters (login, password). The fact that this kind of application is portable means also that all secrets are independent of the PC, avoiding cyber attacks such as key logging.

Keylogging is the practice of logging the keys struck on a keyboard in a covert manner so that the person is unaware that their actions are being monitored. Usually keyloggers, previously installed on the PC, are launched at the boot of the PC and then log all key strikes. If the PC is connected to the Internet, the hackers will email the log file to themselves. This may well be encrypted so even if the user discovers the file they will not know what it contains.

Figure 3-11. Example of Keylogger
Password Manager embedded in a VaultIC-based USB token prevents data and applications from malicious attacks such as keylogging.

Moreover, passwords stored in a Secure Portable Password Manager allow the user to use more passwords, and especially more complex passwords, thereby increasing their security.

### 3.3.3 Secure mass storage (secure companion)

In a mass storage application, the VaultIC can be considered as a secure companion for an external memory. In this configuration, the VaultIC device will store only sensitive data, such as private keys, credentials etc., whereas the external memory (a NAND flash for instance) will store the large data files. The link between both can be made using the SPI or I²C interface.

### 3.3.4 Inside the token

Thanks to its large EEPROM memory the VaultIC chip can store secrets such as credentials or private keys in numbers.

The file system downloaded by the manufacturer in a VaultIC might be composed as follows:

- **Administrator data**: file system version, private keys.
  These data allow the Administrator to be authenticated to upgrade keys, update users’ properties, change administration data, update software...

- **User(s) data**: identifier, private keys, certificates, credentials... for up to 7 different users.

- **Application data**: depends on the application.

Figure 3-9 shows an example of integration of a VaultIC microcontroller into a USB token for a storage application.

**Figure 3-12.** VaultIC Solution Integration for secure storage applications

![VaultIC-based USB e-Token for storage application](image)
4. Conclusion

Doing business in the virtual world means that many business operations require some form of authentication to ensure that only an authorized employee, customer, or partner is the one performing the operation. USB tokens, and particularly VaultIC-based USB tokens, provide secure solutions to trusted people accessing company's private resources, using PKI-based architecture or other strong authentication methods.

Travelling with secured portable data is another requirement for companies who want to keep their sensitive information protected from third parties. This is another application targeted by VaultIC which can store large size of sensitive data, along with a large memory chip, both in the same USB e-token.

For more details about the VaultIC Products Family please contact your local Inside Secure Sales office.
Definitions & Abbreviations

AES  Advanced Encryption Standard algorithm as defined in FIPS PUB 197.
APDU  Application Protocol Data Unit as defined in ISO7816-3.
API  Application Programmer’s Interface, set of functions that may be called by a program.
Authentication  An identification or entity authentication technique assures one party (the verifier), through acquisition of corroborative evidence, of both the identity of a second party involved, and that the second (the claimant) was active at the time the evidence was created or acquired. (From Handbook of Applied Cryptography).
CA  Certification Authority.
Cryptoki  Name of the API specified by the PKCS#11 standard. Pronounced crypto-key and short for cryptographic token interface, it follows a simple object-based approach, addressing the goals of technology independence (any kind of device) and resource sharing, presenting to applications a common, logical view of the cryptographic token.
DES/3DES  Data Encryption Standard algorithm as defined in FIPS PUB 46-3. Triple DES algorithm.
DSA  Digital Signature Algorithm as defined in FIPS PUB 186-2.
ECC  Elliptic Curves algorithm.
EEPROM  Electrically-erasable programmable read-only memory.
FDA  Food and Drug Administration (USA).
FIPS  Federal Information Processing Standards. FIPS140 specify requirements for cryptography modules.
HIPAA  Health Insurance Portability and Accountability Act, which help people keep their medical information private.
HOTP  HMAC-based One Time Password algorithm.
OTP  One-Time Password.
PCSC  Personal Computer/Smart Card. Workgroup defining a standard architecture for integration of smart cards in computers.
PDA  Personal Digital Assistant.
PIN  Personal Identification Number.
PKCS#11  Public Key Cryptography Standard #11. API defining a generic interface to cryptographic tokens.
PKI  Public Key Infrastructure.
RA  Registration Authority.
RSA  Rivest Shamir Adleman algorithm.
SPA/DPA  Simple Power-Analysis involves visually interpreting power traces, or graphs of electrical activity over time. Differential Power-Analysis is more advanced form of power analysis which can allow an attacker to compute the intermediate values within cryptographic
computations by statistically analyzing data collected from multiple cryptographic operations.

SSL  Secure Sockets Layer, cryptographic protocol that provide security for communications over networks, such as the Internet.

TLS  Transport Layer Security. Successor of SSL.

URL  Uniform Resource Locator, web address.

USB  Universal Serial Bus.

VA  Validation Authority.

VPN  Virtual Private Network.

WLAN  Wireless Local Area Network.
Revision History

Document Details
Title: How to secure USB e-Token using VaultIC™ Security Modules?
Literature Number: TPR0451BX
Date: 20Jan11

• Revision B - January 2011 :
  – Update for INSIDE template.
• Revision A - May 2010 :
  – First release.