Enterprise Security and Management Of Hardware-Based Encrypted USB Devices

White Paper by QuikProto Team

INTRODUCTION

With the BYOD movement, IT has a golden opportunity: serve the productivity needs of a fast-evolving, USB data storage strategy, while simultaneously providing data protection expected by corporate leaders. Great news: you can meet these requirements today by leveraging technology that is secure, manageable and cost effective. Learn how.

Organizations and agencies struggle to remain ahead of constantly evolving threats to the security of their data. Not only is news of data breaches increasingly being reported; the threats are escalating and risks are many:

- Intellectual property representing years of R&D falling into the hands of competitors
- Sensitive corporate records leaked to hackers, hacktivists and malicious governments
- Data breaches involving customers personally identifiable information about finances or health records, and the resulting damage to brands and customer loyalty
- Fines and other costs associated with failure to comply with data security mandates
- Pre-release of product content or trade secrets spoiling market opportunity.

Many organizations in financial services, Healthcare, government and other regulated industries implement data security policies because they are required to. Meeting compliance regulations is important, but even the strictest compliance requirements still can leave sensitive data vulnerable to malicious parties capable of breaking into encrypted USB storage devices and extracting confidential data from them.

Now more than ever , the need to move beyond just compliance should be on the forefront of an organizations data security and protection strategy. To help organizations and agencies answer the question, “is secure enough”, really enough? , When compliance alone may not offer the protection needed to prevent data breaches that can cost millions of dollars, inflict untold damage to corporate brands and customer relationships, and invite weeks or months of negative publicity.

Portable storage devices are a popular way to transport files between computers and to backup important information. However, the ubiquity of these devices heightens the security concerns of carrying confidential data. It is important to prevent confidential information from falling into the hands of unauthorized users should a device be lost or stolen. Encryption can be an effective way to protect the privacy of sensitive corporate and personal data.

While software encryption programs can help protect data and provide a good first line of defense, they are vulnerable to a number of decryption attacks. Hardware-based encryption offers a stronger defense against the same threat models, and is now available on a new generation of portable data security and authentication devices from QuikProto. This paper examines Genesis's data encryption capabilities, compares the competing software and hardware-based approaches, and analyzes their effectiveness against various threat models

75% of Fortune 1000 companies fell victim to data leakage in 2006, with an average recovery cost of $5,000,000.

QuikProto TrustedIcon represent one of the most secure and easy-to-use solutions to the problem of physical USB device security. However, physical security of USB flash drives is only one issue IT managers face. With thousands of flash drives being used in an organization, managing the usage and policies of devices presents an equally significant challenge.

Common Concerns Among Enterprise Security Managers

Figure 1: visually represents common areas of concern that are unique to enterprise management of portable data devices

Today's enterprise IT administrators face a number of challenges in managing an enterprise's portable data devices.

Figure 1. Management Requirements of Portable Data Devices in Enterprises

Endpoint Security

The data on portable storage devices should ideally be protected from a myriad of known attacks, regardless of whether the device is being used correctly by its assigned owner or being tampered with by an intruder. The devices must also integrate easily with endpoint security software that authorizes which devices can be safely integrated with the existing network or PC.

Security Policy Adherence

Portable devices must reside under and support the organization's existing security policy umbrella. This means that data access must be controlled by the same password policies and external devices must be subject to the same on-the-wire security policies.

Secure Device Recovery

Even if an enterprise's portable devices have been secured against a multitude of potential attacks, a forgotten password to a specific device could render the device inaccessible and result in loss of critical company information if there is not a secure means for device recovery. Examples also include accessing data on the device when an individual is no longer with the organization and changing the device owner's password for repurposing the device.

Forgotten passwords (more than 30% of all help desk requests5) could result in data loss if the password was to an encrypted flash drive.

Since forgotten passwords constitute upwards of 30% of all help desk requests5, data loss due to a forgotten password is a potentially significant problem for enterprise IT managers. However the ability to recover forgotten passwords carries its own set of security risks, and ensuring proper authentication, authorization and access are crucial. For example, even with military-grade device security, a disgruntled insider could gain access to the data on all of an organization's flash drives if the passwords are stored in a central database for administrators

Flexible Configuration

How endpoint devices may be used needs to be subject to policies and processes unique to a specific organization. Security managers must be able to control what software can be used on specific devices, how that software is configured for use. Equally important, the IT organization must control who is allowed to administer which policies on which devices

Consistent, Centralized Management

IT administrators need to balance system configuration with ease-of-use, cost, and consistent policy enforcement.

The flip side of flexible configuration is consistent management, and the two sides represent a balance of competing needs:

- The need to ensure that a minimum set of security standards can be established and automatically enforced across an entire group of portable devices.
- The need to allow flexible implementation to conform to the policy of a specific user group.

With multiple groups using portable devices throughout an organization (e.g. divisions, departments, teams), consistency of device policies becomes a critical concern. If a company has a seven character minimum for password length, then an enterprise administrator must be capable of enforcing that policy across all departments within their span of control.

Another aspect of consistent management involves cost. Consistent management is ineffective if the cost of administration is too high to make it practical. With hundreds or thousands of devices in a given user group, device management must have a centralized control console. Provisioning cannot be practically handled by already overburdened IT staff. Simple, yet secure self-provisioning of devices by

Defining the level of security

When evaluating security options, it is important to identify the impact to your business associated with the information you are protecting and the threats from which you are protecting them. Remember, too that security is a moving target and the threats continue to escalate to both the data and the device itself. As revealed at black Hat 2014, BadUSB is the first USB malware designed to attack the device itself instead of attacking the data on the device. The attack changes the firmware that controls the behavior of the USB hardware, allowing the USB device to become a host that can subsequently infect other computers and USB devices.

The Best protection against BADUSB is to use code signing for firmware updates. If the signed firmware is modified, the device cannot authenticate the firmware and simply will not operate. TrustedIcon protect against BADUSB malware. Our leadership in security, including our use of digital signatures in all controller firmware, makes QuikProto product immune to this threat.

Compliance Vs. Security

Secure, more secure, and most secure. Security levels for storage devices can be described as "secure," "more secure," and "most secure. To understand the level of security your organization needs, you first must take inventory of your reasons for implementing a secure data strategy. You must also always evaluate the need to move beyond compliance.

IT managers frequently cite one of three primary drivers:

1. **We need to be compliant with data security requirements.** When compelled to implement a data security strategy, organizations frequently fail to see a direct relationship between adding security and achieving improved efficiencies across their operations. Their goal is to simply be secure enough that if a breach occurs, they can show that they followed "industry standard and best practice," thus avoiding the cost of fines from government oversight bodies. In other words, the organization needs to get a passing grade in a security audit but does not see any pressing reason for security investments outside of this objective.

2. **Our workforce deals with information that is highly sensitive and cannot fall into the wrong hands.** In this case, a loss of critical proprietary or confidential information could have severe or even catastrophic consequences to a business; organizations tend to choose a security level that keeps the data secure from even the most aggressive and well-capitalized hackers, such as foreign governments and identity theft cartels.

3. **The storage device must survive the harshest of environments while being secure and accessible for long periods of time.** Most organizations don't subject their data devices to challenging physical conditions. But for those that do – including government, military, first responders, and hospital workers in sterilized environments – keeping data secure is a matter of more than data security. It can be a matter of national security or public safety.

Understanding your needs and the potential impact that exposures may have on your organization or business will help pinpoint your tolerance for data breaches. The greater the potential damage, the greater the need for the highest levels of security.

With all the security breaches today, being good enough isn't suitable.

Understanding What keeps data safe

It's one thing to pinpoint why you need security. It's another to understand the options available to you to help you meet those needs. This requires digging into the technology, architecture, physical composition, and management of storage devices. The more you know, the more it becomes clear why some solutions protect data more persistently than others, and why those solutions can cost more.

Encryption and Authentication. These are the common denominators for all systems regardless of the security level.

- **Encryption** transforms the data on the storage device so that an intruder cannot decipher the information.
- **Authentication** controls access to the information by requiring users to provide passwords or biometric identification (such as a fingerprint). Some devices require multiple forms of authentication.

Encryption comes in many forms and different algorithms, but all are designed around a fundamental premise: To create an algorithm with so many permutations that it would take thousands of years to solve them, even when using the most advanced current computing power. To ensure that this is true, current encryption algorithms use long encryption (or crypto) keys that make them exponentially more difficult to crack than shorter ones.

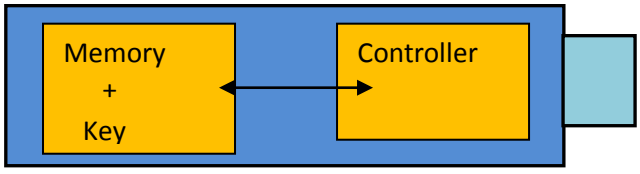

Figure 1: Drives that store encryption keys in the clear make it easier for hackers to read the key and steal the data stored on the device.

Hardware design. The way a device's security is implemented is just as important as the encryption technology utilized within it. Some devices store the crypto key in clear readable text in the flash memory itself, while others store the crypto key on a separate secure cryptographic module.

- **Readable clear text in the flash.** This means the crypto key is stored in the flash memory or hard drive built into the device, which makes it easier to read by people trying to get to the stored data. **Many devices that meet the FIPS 140-2 Level 2 security standard store their crypto key in this manner, or they obfuscate it using a key derived from the password.** In either case, the key is usually stored in the same memory area as the rest of the data. It is a lower-cost approach that offers less protection than devices with a cryptographic module. (*See Figure 1.*)

- **On a chip.** More secure systems keep the data encryption key out of the main device memory and store it on a separate cryptographic module, commonly used in smart cards. The chip is shielded in a tamper-resistant environment. **Devices that meet the more stringent FIPS 140-2 Level 3 security standard store their encryption key on a cryptographic module in this manner.** (*See Figure 2.)*

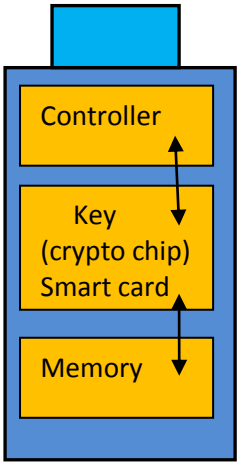

Figure 2.
Drives that store encryption keys in a separate tamper-resistant cryptochip module are significantly more difficult to compromise. They tend to feature unique defenses, such as a metal mesh cladding and self-destruct function in case of physical attacks.

TrustedIcon: Enterprise Edition

To deal with these issues, QuikProto has developed the TrustedIcon: Enterprise Edition , which provides an easy-to-use, scalable and secure solution for enterprise IT managers to customize the TrustedIcon devices for their organizations. Available as a managed security service, it reduces deployment costs and enables global rollout to anyone with or without Internet access.

Unique Features of the TrustedIcon: Enterprise Edition

The TrustedIcon: Enterprise Edition includes all the security features of the standard edition of the TrustedIcon Secure Flash Drive, and more.

QuikProto developed the TrustedIcon Enterprise Edition to specifically address the concerns IT managers have about managing TrustedIcon USB drives, potentially deployed in hundreds of locations around the world. The Enterprise Edition builds on top of the core feature set of the Secure Flash Drive, which includes:

- **Hardware Encryption of Flash Drive Data.**
  SecuDrive have high-speed hardware AES encryption that protects all data stored on the device. No software or drivers need to be installed and no local administration rights are required.
- **Hardware-Based Device Password Verification**.
  To unlock an TrustedIcon device, the user must enter their device password. This is verified in hardware by the SecuDrive. If a user enters the incorrect password too many times, the device self destructs by erasing all the user's encrypted data.
- **On-Board Cryptographic Authentication**.
  TrustedIcon is pre-configured with a unique cryptographic key that is pre-installed during manufacturing. This can be used for strong authentication to enterprise websites. Developers can also access the device's cryptographic functions for custom applications by using PKCS#11

The Enterprise Edition introduces the following new technologies

- **Creation & Enforcement of Corporate Password Policies on the Device**. TrustedIcon Enterprise Edition allows you to configure policies for device password strength through the Admin Console.
- **Configuration of TrustedIcon Applications and Services**.
  You may configure which on-board TrustedIcon applications and services are enabled for your users. You can allow or prohibit the use of the on-board Mozilla Firefox web browser, the TrustedIcon Password Manager, TrustedIcon's Secure Sessions (secure web surfing service)services.

- **Creation and Enforcement of Self-Destruct Policies**.

TrustedIcon: Enterprise Edition allows you to configure the number of times a pass- word can be entered incorrectly before the self-destruct feature is activated.

- **A Secure yet Practical Method for Unlocking Employee Devices**.

TrustedIcon: Enterprise Edition provides you with a secure mechanism for recovering device passwords for regulatory compliance or in the case of termination.

- **Integration with Endpoint Security Systems**.

TrustedIcon: Enterprise Edition has been designed to integrate seamlessly with many of the industry's leading endpoint security software products. Additionally, every TrustedIcon has a unique serial number and product ID, making it easy to manage and apply usage policies within endpoint security solutions.

TrustedIcon Device Recovery

Unlike systems that rely on backdoor passwords to recover devices, QuikProto services rely on strong, proven cryptographic algorithms.

The ability to securely access and recover your organization's devices is one of the strongest benefits of TrustedIcon: Enterprise Edition. Other devices on the market use backdoor passwords (a common password that will unlock all devices) to gain access to a device when the user has forgotten the primary password for that device. But backdoor passwords represent a number of unwarranted security risks:

- Backdoor passwords can be guessed and brute-force attacked.
- Securely managing a database of backdoor passwords is difficult – one or more administrators have easy access to every device's password.
- Backdoor passwords make it difficult to revoke administrator privileges because the password remains valid regardless of whether an administrator has been terminated or not.
- Backdoor passwords are subject to password replay attacks.

TrustedIcon has taken a unique and much more secure approach. TrustedIcon: Enterprise Edition uses a special recovery tool and patent-pending PKI-based device recovery to ensure that devices can be recovered without using a backdoor password or allowing anyone other than the device's owner to see the device password. Moreover, administrators can gain access to an TrustedIcon from their organization that has been abandoned (e.g. by a former employee who is no longer available) or previously lost.

TrustedIcon Device Recovery removes the threats associated with revoked administrators and backdoor passwords.

To do this the Enterprise Edition strongly encrypts the device password is such a way that only that specific enterprise can decrypt it. Additionally, it encrypts it again so that only an approved administrator's TrustedIcon can decrypt it. That way, unlocking a device requires that you:

1. Are an active administrator with appropriate privileges in the correct enterprise .
2. Have full access to an approved administrator's TrustedIcon

This approach removes the threats associated with revoked administrators, backdoor passwords, and other forms of unauthorized access to user passwords.
Additionally, this technique maintains TrustedIcon standard for ensuring that QuikProto and its employees cannot access your enterprises' devices.
This entire process has been designed to be the most secure way for administrators to recover their users' secure flash drives. It leverages the power of the TrustedIcon Cryptochip for hardware encryption and relies on the integrity of known, trusted and proven cryptographic algorithms, including AES, RSA, and SHA.

The Benefits of a the Managed Security Service

TrustedIcon enterprise services can ease the burden on IT staff without straining end-users with complicated software

The TrustedIcon: Enterprise Edition allow administrators to manage their devices without having to install and integrate complex enterprise software. The benefits of device management as a service include:

- **Easy to Trial and Deploy.**
  There is no complex enterprise software to purchase and install. TrustedIcon: Enterprise Edition's device management is straightforward to pilot, test and roll-out.
- **Scalability**.
  TrustedIcon: Enterprise Edition scales as your organization grows and changes. It is equally well suited for large enterprises as it is for small and medium businesses.
- **Reduced Cost of Ownership**.
  GQuikProtoT staff ensures that the service is online 24x7**. They are constantly managing network performance and availability. The team also manages service upgrades and the rollout of new features. All of this reduces the burden of IT administrators and the total cost of ownership of the managed solution.

The Security Architecture of the Enterprise Managed Service

The TrustedIcon: Enterprise Edition has been designed from the ground up with security in mind:

The TrustedIcon: Enterprise Edition has been designed from the ground up with security in mind (*secure by design*).

- **Network Security of the Service**.

  TrustedIcon enterprise services have been designed by security architects with a background in managing the security of banking and payment systems. Best practices are used in firewalls, IPS, event monitoring and cryptographic key management. All access to the systems is through two-factor authenticated encrypted communications.

- **Hardware Cryptographic Authentication of Devices to the Service**.

  All user and administrator TrustedIcon devices authenticate themselves to the management service with on-board hardware encryption. This allows the service to ensure that administrators and users are authenticated and have the appropriate permissions.

Secure Device Recovery is designed so that there is no way for QuikProto or its employees to unlock your enterprise's devices.

- **Encryption of All Communications with the Service**.

  All communications with the service are encrypted and strongly authenticated to mitigate spoofing, man-in-the-middle, phishing and pharming threats.

- **Anti-Phishing Technology**.

  User and administrator accounts have the latest anti-phishing technologies to authenticate users, including two-factor cryptographic mutual authentication, shared secret images, shared secret questions and device fingerprinting.

- **Cryptographic Architecture of Secure Device Recovery**.

  Unlike "backdoor password" systems, the TrustedIcon device key recovery system uses strong public-key cryptography to encrypt and recover device passwords.

Conclusion

The security experts at QuikProto have gone to extreme lengths to ensure that the TrustedIcon: Enterprise Edition meets the common security, deployment, and usability/maintenance needs of IT managers demand, while maintaining the overall security of the TrustedIcon enterprise services at the same unmatched level as the TrustedIcon hardware.

Hardware-based encryption, when implemented in a secure manner, is demonstrably superior to software-based encryption. That being said, hardware-based encryption products can also vary in the level of protection they provide against brute force rewind attacks, offline parallel attacks, or other cryptanalysis attacks.

TrustedIcon devices address the threat models described in this whitepaper. Password brute force guessing is prevented, and a variety of two-factor authentication protocols are provided. The physical security features of the devices protect against disassembly, rewind attacks and offline parallel attacks. TrustedIcon devices provide fast, strong, and always-on encryption that mitigates the security concerns of transporting confidential data.

If you should need more technical information than is provided in this whitepaper, please contact your QuikProto representative.

Find more information about TrustedIcon at:
www.quikproto.com
QuikProto Research Labs Pvt. Ltd
info@quikproto.com

References

1. Unworth, Joseph. "Forecast: USB Flash Drives, Worldwide, 2001-2011", Boston: Gartner/Dataquest, October 2007.

2. Pointsec as quoted in *Outlaw News,* June 13, 2005.

3. 2006 CSI/FBI Computer Crime and Security Survey, *http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf*

4. Ponemon Institute, 2006 Cost of Data Breach Study, *http://www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf*

5. Marianne McGee, "The Top Reason Users Call the IT Help Desk", InformationWeek, March 1, 2007, *http://www.informationweek.com/news/showArticle.jhtml?articleID=197700628*. Also ContactCenterWorld, January 15, 2003.

6. Bruce Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, 2nd Ed, 1996, John Wiley & Sons, Inc.

7. FIPS PUB 140-2 Federal Information Processing Standards Publication – Security Requirements for Cryptographic Mod- ules, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

8. FIPS PUB 197 Federal Information Processing Standards Publication – Announcing the Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

9. Joan Daemen, Vincent Rijmen, The Design of Rijndael: AES – The Advanced Encryption Standard, 2002, Springer-Verlag Berlin Heidelberg.

10. Niels Ferguson, Bruce Schneier, Practical Cryptography, 2003, John Wiley & Sons. Secure Encryption Challenged by Internet-Linked Computers, Oct. 22, 1997, http://distributed.net/pressroom/56-PR.html

11. Bellare, Mihir. "Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements." Springer Berlin Heidelberg, 2000. Page 1

12. https://security.berkeley.edu/content/data-encryption-transit-guideline

13. Robert Richardson, 2008 CSI Computer Crime and Security Survey at 19.i.cmpnet.com

14. Fiber Optic Networks Vulnerable to Attack, Information Security Magazine, November 15, 2006, Sandra Kay Miller