COALFIRE LABS

HARDWARE SECURITY MODULE LEADERSHIP - HPE ATALLA HSM ANALYSIS

NICK TRENC, CISSP, CISA, QSA, PA-QSA

DAN FRITSCHE, QSA (P2PE), PA-QSA (P2PE)

Hewlett Packard Enterprise

Prepared For:

HPE Security - Data Security
1160 Enterprise Way, Floor 2
Sunnyvale, CA 94089

Prepared by:

Nick Trenc
ntrenc@coalfire.com
Senior Consultant

Dan Fristche
dfristche@coalfire.com
VP, Solutions Architecture

Date:

9/13/2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

As a recognized leader in IT security, governance, regulatory and compliance, Coalfire Systems, Inc. has been completing independent assessments of IT solutions for use in varying enterprise environments for over 15 years. Coalfire helps organizations comply with global financial, government, industry and healthcare mandates while helping build the IT infrastructure and security systems that will protect their business from security breaches and data theft. The company is a leading provider of IT advisory services for security in retail, payments, healthcare, financial services, higher education, hospitality, government, and utilities.

Coalfire professionals use a combination of IT experience, expertise, and intelligence to independently audit and evaluate your entire IT infrastructure to determine what your actual risks are, help you understand how to protect your business assets, and what resources you need to quickly identify and respond to security threats.

In partnership with Hewlett Packard Enterprise (HPE), Coalfire was engaged to review the HPE Atalla Hardware Security Module (HSM) solution for customer use within Payment Card Industry (PCI) environments, as well as to evaluate the competitive advantages provided by the HPE Atalla HSM solution.

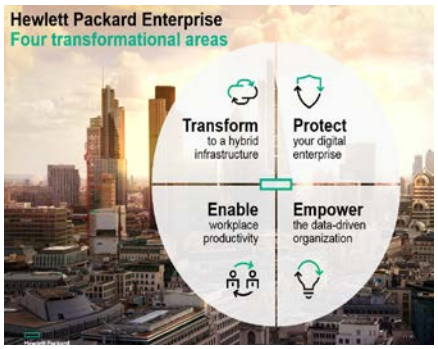
SUMMARY FINDINGS

As a part of this Coalfire assessment, the HPE Atalla HSM (Hardware Security Module) was found to contain several important key security benefits:

- **Security Certifications and Industry Standards:** The HPE Atalla HSM has been through several comprehensive certifications that validate an extra level of security assurance found throughout the solution. These certifications include Federal Information Processing Standard (FIPS) 140-2 Level 3 and Payment Card Industry (PCI) HSM 1.0. The devices have also been built to exacting industry standards such as the National Institute of Standards and Technology (NIST) 800-22 and ANSI X9F. Industry certifications and standards such as these provide an extra level of trust and assurance for HPE Atalla HSM end-users due to the thorough certification processes and validations that the device has undergone.
- **Industry Best Practices for Key Management:** The HPE Atalla HSM drives Industry best practices for security of encryption keys to include: strong security controls around key export, using strong encryption algorithms, supporting cryptographic key loading utilizing dual controls and audit logging of all key management activities.
- **Disaster Recovery Capabilities:** A robust backup and restore capability to prevent loss of data in case of disaster.
- **Superior Cryptography:** The HPE Atalla Key Block (AKB) for security assurance and performance of Triple Data Encryption algorithm (3DES) and Advanced Encryption Standard (AES) encryption implementations.
- **Robust Device Management:** The ability to securely and remotely manage the HPE Atalla solution which is ideal for lights-out data centers.

- **Range of Industry Usage:** The HPE Atalla HSM enables a wide range of uses for a PCI-compliant environment.
- **Validated Market Leadership:** The HPE Atalla HSM solution is one of the most established security hardware products and has achieved the highest 'Net Promoter Score' of any of the HSM appliance providers among their customers. Combined, these two factors provide HPE customers an extra level of security assurance, considering both the maturity and functionality of the HPE Atalla HSM solution.
- **Security Assurance:** The HPE Atalla HSM includes full "*Chain of Trust*" for its users. This is a critical, and sometimes overlooked, aspect of security. HPE ensures and validates that when someone receives an HPE Atalla HSM, they can be assured it has 'not' been tampered with and they are starting with a device that can be fully trusted.

ABOUT HPE



Hewlett Packard Enterprise (HPE)

HPE is dedicated to transforming the enterprise in new and innovative ways. HPE is doing this by focusing on four key areas that will help any size business' IT perform more efficiently and more securely: transformation, protection, enablement, and empowerment. By combining these four areas, HPE is seeking to enable customers to accelerate their businesses combining leading edge technology, while remaining focused on building in security for those assets that matter most to an enterprise … its data.

HPE Protecting Your Digital Enterprise

The key transformational area that this paper seeks to address is the secure protection of non-cash retail payment environments. Coalfire analysis was focused on confirming these security measures were comprehensive and supported enterprise needs for security and compliance standards.

As an expert in governance, regulatory and compliance with a focus on security, Coalfire Systems is uniquely poised to deliver an expert opinion on validating solutions protection for digital enterprises of all things information technology and security related.

HPE Security

The HPE Security - Data Security business has four security solution offerings in their portfolio, all of which deal with encryption and tokenization of data, through either hardware security modules (HSM) or software. HPE Atalla HSMs are essentially vaults that hold encryption keys. They are usually deployed behind firewalls and perform specialized functions triggered by discrete commands for each function. Sending minimal information in a command, and receiving minimal information in response, is a built-in security feature. That model of communication is used when verifying a payment card's Card Verification Value (CVV) number, an EMV chip card's authorization request cryptogram (ARQC), for tokenization, and

when Personal Identification Numbers (PINs) are sent to card issuers from automated teller machines (ATMs) and point-of-sale (POS) terminals.

HEWLETT PACKARD ENTERPRISE ATALLA HSM SOLUTION

The focus of this evaluation was on the HPE Atalla HSM (Hardware Security Module) or Host Security Module as defined by the ANS X9.24 definition. The industry uses a dual use of the acronym to distinguish secure hardware for use at the server (host) from hardware used for client purposes (i.e. PIN entry devices). The HPE Atalla HSM fits both definitions and includes the following key characteristics:

Figure 1 – HPE Atalla HSM

- 2U rack-mountable tamper-resistant security device which can be utilized for cryptographic and key management operations in:
    - PIN processing
    - Card verification
    - Card production and personalization
    - ATM interchange
    - EFTPOS (Electronic funds transfer at point-of-sale)
    - Data integrity
    - Chip-card processing
- Up to 1060 PIN translations per second per device when used with the Atalla Key Block feature
- Secure Configuration Assistant-3 (SCA-3) a tablet-based UI tool for secure local and remote management of the HPE Atalla HSMs
- Multiple HSMs can be utilized by host applications to handle growing transaction volumes, and higher speed HSMs are available for higher value transactions where such operations as PIN translations or verifications per second are critical for the business. HPE sells devices with varying levels of performance that can address even the most demanding customer's requirements. The HPE Atalla HSM devices are Secure Cryptographic Devices (SCDs) as defined by ANS X9.97. The HSM employs active zeroization of all the keys in the appliance and the whole device will shut down depending on the degree of attack.

AUDIENCE

This white paper will assist the following three audiences in evaluating the use of the HPE Atalla HSM for industry use.

1. The first target audience includes **merchants** evaluating the HPE Atalla HSM for deployment in their payment card environment for encryption and key management.
2. The second target audience is **acquirers (or payment processors), payment gateways and issuers (or banks)** that offer PIN verification, encryption, and key management, and EMV processing solutions for their merchant and service provider payment card environments.
3. The third target audience is the **Point-to-Point Encryption (P2PE) service providers** who are implementing a P2PE environment as part of payment card processing.

ASSESSMENT SCOPE

The scope of this assessment was to validate that HPE Security and the HPE Atalla HSM can provide specific security benefits for P2PE solution providers, issuers and acquirers, and merchants; as well as maintains thought leadership that end-users will benefit from when choosing this hardware security module solution.

The assessment testing focused on the following HPE Atalla HSM solution functional areas:

- Assessment of the HPE Atalla HSM solution and key functions:
    - Encryption capabilities
    - Key management
    - Secure Chain of Trust
- Atalla Secure Configuration Assistant-3 (SCA-3) with Atalla Secure Keypad (ASK)

METHODOLOGY

Coalfire has implemented industry and audit best practices in its assessment and testing methodologies. Coalfire completed a multi-faceted technical assessment process during the course of this project. Coalfire conducted all technical lab testing while connected remotely via virtual private network (VPN). Coalfire's assessment methodology also included a complete documentation review.

At a high level, testing consisted of the following tasks:

1. Technical review of the architecture of the full solution and any components.
2. Implementation of the Secure Configuration Assistant-3 (SCA-3) with the Atalla Secure Keypad.
3. Evaluation of detailed technical documentation.

4. Interviews with expert points of contact within HPE.
5. Detailed review of industry security best practices for the HSM's logical and physical security.

Figure 2 - HPE Secure Configuration Assistant-3 with Atalla Secure Keypad

ASSESSOR COMMENTS

Coalfire was provided VPN access to a single instance of the HPE Atalla HSM for configuration testing. Coalfire did not attempt any security testing to break encryption methodologies or otherwise subvert security controls. No sensitive or real world data was utilized as part of testing the solution.

For practical and security reasons, Coalfire performed limited technical testing of the HPE Atalla HSM configurations that might not simulate real world functionality for encryption management in an actual payment card environment. Data was reviewed and analyzed from validated processes, documentation, certifications and through subject matter expert interviews.

HPE ATALLA HSM SECURITY FEATURES

The following illustrates the key security advantages for utilizing the HPE Atalla HSM within a payment environment.

Certifications and Industry Standards

The HPE Atalla HSM has been certified by several security bodies to provide a level of assurance of security for HPE's customers. These include (but are not limited to) FIPS 140-2 Level 3 for physical security and PCI HSM 1.0 as part of the PIN Transaction Security (PTS) standard. Additionally, the HPE Atalla HSM is built in accordance with NISP SP800-90, which is the modern standard for random bit generation.

FIPS 140-2 Level 3 provides assurances that the certified device attempts to prevent unauthorized access to critical security parameters within the device via physical security mechanisms that have a high probability of detecting and responding to unauthorized attempts at physical access, and use or modification of cryptographic modules. With the HPE Atalla HSM, any attempts to physically access hardware or firmware within the security module automatically results in a zeroing of all critical security parameters.

A PCI HSM 1.0 certification under the Practical Test Standard (PTS) standard provides assurance for the use of the HPE Atalla HSM as part of PIN processing, card verification, card production, electronic funds

transfer at point-of-sale (EFTPOS), ATM interchange, cash card reloading, data integrity and chip card transaction processing within PCI environments including banks, merchants and service providers. The HPE Atalla Ax160 (**Hardware #**: A10160 [HW P/N AJ560A], A9160 [HW P/N AJ558A], A8160 [HW P/N AJ556A] with Firmware #: 1.21) is a PIN Transaction Security (PTS) approved device that is currently listed on the PCI SSC Approved PTS Devices website: https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

The NIST 800-22 industry standard provides guidelines that the random number generation features within the secure cryptographic module are truly random utilizing specific tests designed by the National Institute of Standards and Technology.

HPE Atalla Key Block

One of the other features that sets the HPE Atalla HSM apart is the use of a unique feature called the HPE Atalla Key Block for double and triple key-length 3DES implementations. This increases security within payment environments by providing assurance against key manipulation that could otherwise be destructive to the payment card industry.

Figure 3 – HPE Atalla HSM

The Atalla Key Block is a feature that adds a level of security to double and triple key-length 3DES implementations not available from other manufacturers. The HPE Atalla HSM provides a data structure for protecting cryptographic keys that ensures that key encryption is completed with proper key size and secure algorithms that the HPE Atalla HSM has sufficient information in order to determine that keys are being used correctly and that any manipulation of keys will be detected by the HPE Atalla HSM.

HPE Atalla HSM Use Cases

HSMs have been primarily adopted as part of card issuing and PIN verification within the payment card industry. However, they have a much broader use case than what they are typically used for in today's PCI environment.

They can be deployed in multiple use case scenarios such as the following;

- PIN validation and related processing – The HPE Atalla HSM Ax160 is developed and can be supported in accordance with the PCI HSM security policy that is required for PTS certification and can be found at the following: https://www.pcisecuritystandards.org/ptsdocs/HP%20Atalla%20Ax160%20PCI%20HSM%20Security%20Policy%201_1.pdf
- Card verification – The HPE Atalla HSM can be used to verify any number of security codes for card transactions by matching CVV codes from track data to the expected value during an authorization request.
- Card production and personalization – The HPE Atalla HSM can be utilized during card production for generation of smartcard keys, CVV/CVC/CSC values, PIN offsets, and other cryptographic tasks.

- EFTPOS – Similar to PIN validation, the HPE Atalla HSM can be utilized for verification of cardholder identity during PIN processing while requesting money during a debit transaction.
- Data integrity – The HPE Atalla HSM can be utilized to confirm message integrity for data sent over the public Internet or private networks.
- Chip-card transaction processing – The HPE Atalla HSM can be used for trusted authentication of Europay, MasterCard and Visa (EMV) transactions, both contact and contactless. Utilizing public key infrastructure (PKI), the HPE Atalla HSM can be used for trusted authentication of transactions.
- Cryptographic key generation – The HPE Atalla HSM can be utilized to simply generate and store cryptographic keys used during encryption processes
- Cryptographic key injection – As part of a P2PE issuing environment, the HPE Atalla HSM can be utilized to inject encryption keys into PIN Transaction Security (PTS) point of interaction (POI) devices otherwise known as PIN pads.
- Cryptographic authentication – The HPE Atalla HSM can also be used for cryptographically secure authentication purposes such as certificate authorities (CAs) and registration authorities (RAs) as part of generation, storage and handling of key pairs utilized as part of a PKI environment.
- P2PE certified secure decryption environments – The HPE Atalla HSM meets the core industry standard for PCI P2PE requirements for use in a PCI P2PE environment.
- Data Privacy – The HPE Atalla HSM supports both 3DES and AES encryption of arbitrary messages for data privacy.

Point-To-Point Encryption

Released in July 2015, the PCI P2PE standard version 2.0 Domain 5 - Decryption Environment requirement calls for the use of hardware security modules that are either FIPS140-2 Level 3 (or higher) certified or PCI PTS HSM approved. The HPE Atalla HSM is listed as HPE Atalla HSM Ax160 (**Hardware #:** A10160 [HW P/N AJ560A], A9160 [HW P/N AJ558A], A8160 [HW P/N AJ556A] with Firmware #: 1.21) is a PIN Transaction Security (PTS) approved HSM device that is currently listed on the PCI SSC Approved PTS Devices website. It can be found here:

https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

The use of HSMs can greatly reduce the current risk of payment card data compromise in a merchant or service provider environment if implemented properly. HSMs are now being used increasingly within PCI P2PE solutions to meet various requirements within the standards and automate tasks during the transaction process such as:

- Cryptographic authentication by the HSMs
- Cryptographic key injection and key-management functions (for hybrid decryption environments*)

The HPE Atalla HSM provides secure communication and access capabilities that are required to meet a high level of security. Memory access prevention, integrity assurance, and limiting exposure of

cryptographic keys are strengths of HSMs over software-based systems. The ability to quickly and securely complete tasks makes the use of a dedicated HSM an attractive proposal for P2PE solution providers.

Adopters of the HPE Atalla HSM solution can be assured that these devices will support their efforts to become a P2PE solution provider when utilizing the device as part of their hardware decryption needs.

*Hybrid decryption: This is where account data decryption can occur outside of an HSM in non-Secure Cryptographic Device (SCD) Host System. Host System is a combination of software and hardware components used for purpose of decrypting account data.

Additional Benefits

Best Practices: Basic security of the device is configured to support security best practices for encryption and key management. The HPE Atalla HSM Ax160 generated Master File Keys (MFKs – up to 10 per appliance), including those generated internal to the HSM are never exported, are at least double-length keys and can use the TDES algorithm (including parity bits) or the AES algorithm using a key size of at least 128 bits. Cryptographic key loading and administration can be accomplished via split knowledge and dual-control/split knowledge in a secure fashion, as prescribed by ANSI X9.24 part 1. TR39 is an audit standard that checks that you follow the requirements mandated in X924 and other standards. All cryptographic key administration activities are logged and can be audited for compliance purposes.

Net Promoter Score: For almost four decades, the HPE Atalla HSM is one of the most established security products on the marketplace and has been adapted to fit changing technologies and evolving security standards. HPE Atalla HSM customers have consistently given the HSM the highest "Net Promoter" score for HSM solution providers. The Net Promoter Score is calculated based on 0 – 10 point scale for answering a single question: *How likely is it that you would recommend it to a friend or colleague?*

Thought Leadership: In addition, HPE Security has continually invested in advancing payment security standards, through governing bodies such as ANSI X9. For example, the HPE Atalla Key Block (AKB), a key block structure intended to securely store and manage the use of encryption keys such as Triple DES (3DES) and RSA public and private keys, was the basis for what ultimately became the ANSI X9 TR-31 standard key block. In addition to the AKB, HPE has continuously made additional innovative contributions to ANSI standards, such as the AES PIN block (both original proposal and final design) and the AES Derived Unique Key Per Transaction (DUKPT) (drafted original proposal, instrumental in final design), as well as acted as technical editor for AES PIN verification. As a result, HPE Atalla HSM customers are well-positioned to ensure compliance with payments security standards and future compatibility for their existing HSM investments.

The HPE Atalla HSMs provide differentiated capabilities for the payments security market such as a flexible approach to HSM configuration and key management, robust backup/restore capabilities and ongoing innovation contributions to the payments Security Standards. These include:

Backup and Restore Capabilities: HPE Atalla HSM customers can enjoy a robust backup and restore capability because of the ability for the HPE Atalla HSMs to utilize a policy within the device that can be set to specify multiple smart cards (M of N) to be used as part of a restore operation. This adds an additional functionality that must be required for a restore instead of the single card set. The HPE Atalla HSMs specifically address this concern with a configurable policy that can be set to specify that multiple cards (M of N) must be required for a restore. This approach provides increased robustness and policy

control around the recovery of sensitive encryption keys and configuration data should a disaster occur in which a smart card is destroyed or worse.

Key Entry and Management: Another unique feature for the HPE Atalla HSMs is the ability to utilize the SCA-3 with the ASK (Atalla Secure Keypad) for remote key entry and management of the HSM. The HPE Atalla HSM solution uses a workflow model which allows each security officer to perform their job discretely and independently of each other. This approach allows for a secure way to manage encryption keys and methodologies even in today's modern lights out data centers where it is impractical or impossible to have all key custodians physically located at the same HSM terminal for management. This approach meets *PCI split knowledge and dual control requirements.* All HPE Atalla HSMs are shipped in a secure state, with tamper-reactive mechanisms enabled to prevent undetected tampering in transit.

Industry Validation: As a final key benefit, the HPE Atalla HSMs maintain a secure chain of trust and physical security from the time the device is manufactured to the time of receipt at the end destination. When Chain of Trust is purchased as part of the HSM solution, an organization receives an email containing the serial number of the Atalla Cryptographic Subsystem (ACS), the serial number of the hardware chassis, and the date it is shipped from HPE manufacturing. In order to validate that the device has not been tampered or swapped prior to arrival at an organization, the organization simply needs to compare serial numbers and the shipment date before installing the HSM solution and check the Security Status indicator (green LED) to ensure that the device has not been swapped or tampered with in any way.

TECHNICAL ASSESSMENT

ASSESSMENT METHODS

The primary assessment was completed utilizing documentation review and interviews. Limited technical testing of remote key management was completed utilizing an HPE provided SCA-3 including the ASK with VPN access to an HPE lab.

HPE ATALLA HSM COMPONENTS

The primary HPE Atalla HSM is made up of two main components:

1. **HPE Atalla HSM** – The actual security hardware device that manages encryption, payment data verification, tokenization or other general encryption needs. Other use cases include authentication, document/code signing, and PKI credential management.
2. **HPE SCA-3 Tablet with Atalla Secure Keypad (ASK) –** A purpose-built configuration tool with easy to use GUI for remote or local configuration of keys.

ASSESSMENT ENVIRONMENT

The technical assessment was completed using HPE SCA-3 and VPN connections to an HPE lab environment to test encryption key management functionalities as it relates to the HPE Atalla HSM use cases for PCI environments.

CONCLUSION

In short, Coalfire Systems Inc. believes that the HPE Atalla HSM solution provides merchants, acquirers, issuers, and third-party service providers the flexibility and the level of security mandated to meet necessary compliance regulations. HPE's thought leadership and continued investment in the robust capabilities of the HPE Atalla HSM solution ensures that it will be a solution that can meet enterprise needs for the foreseeable future. The breadth of use cases for a PCI environment make the HPE Atalla HSM solution a perfect fit for most environments seeking a balance between ease of use and rich security assurance.

For additional information on the HPE Atalla HSM solution, please visit HPE Security - Data Security at HPE.com/software/DataSecurity.

ABOUT THE AUTHORS

Nick Trenc (ntrenc@coalfire.com) is an Application Security Specialist with Coalfire. Nick has several years of experience working as a QSA and PA-QSA helping clients develop systems and software for use in PCI DSS environments and has authored and spoken on multiple security topics including mobile security, application security, virtualization, cyber risk management, secure software development, and PCI DSS and PA-DSS compliance. He holds a CISSP, CISA, QSA, and PA-QSA.

Dan Fritsche (dfristch@coalfire.com) is Vice President of Solution Architecture with Coalfire. He has two decades of experience in application and network security architecture and his team is responsible for translating requirements created by IT risk and compliance mandates into business-centric cyber solutions strategies. His experience covers a broad spectrum of security disciplines including payment security, vulnerability scanning, application security, penetration testing, mobile security, software development, encryption, compliance, anti-virus, and IDS/IPS. He holds a CISSP, QSA (P2PE and PA-QSA (P2PE).

ABOUT HPE SECURITY – DATA SECURITY

HPE Security - Data Security drives leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of expertise we protect the world's largest brands and neutralize breach impact by securing sensitive data-at-rest, in-use and in-motion. Our solutions provide advanced encryption, tokenization and key management that protect sensitive data across enterprise applications, data processing IT, cloud, payments ecosystems, mission-critical transactions, storage, and big data platforms. HPE Security - Data Security solves one of the industry's biggest challenges: simplifying the protection of sensitive data in even the most complex use cases. For more information, please visit: http://www.hpe.com/software/DataSecurity

ABOUT COALFIRE

Coalfire is the global technology leader in cyber risk management and compliance services for private enterprises and government organizations. Our professionals are renowned for their technical expertise and unbiased assessments and recommendations. Coalfire's approach builds on successful, long-term relationships with clients to achieve multiple cyber risk management and compliance objectives, tied to a long-term strategy to prevent security breaches and data theft.