WHITE PAPER

COMFORTE AG SECUREDPS

PCI DSS TECHNICAL ASSESSMENT

LYLE MILLER | CISA, CISSP, QSA, PA-QSA, PCI SSLCA, PCI SSA
NICK TRENC | PCI SSLCA, PCI SSA, CISSP, CISA, QSA (P2PE), PA-QSA (P2PE), QPA, CCSK

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Comforte AG (Comforte) engaged Coalfire Systems, Inc. (Coalfire), a leading independent industry provider of information technology (IT) security, governance, and regulatory compliance services, to conduct an independent technical assessment of their SecurDPS Enterprise Solution (SecurDPS) in support of the Payment Card Industry Data Security Standard (PCI DSS). Organizations accepting payment cards for purchases are subject to the requirements of PCI DSS.

Selected organizational and technical safeguards should align with the requirements and outcomes specified by PCI DSS including, among other things, data minimization, storage limitation, purpose limitation, accuracy, integrity, confidentiality, availability, and accountability. It is necessary to discover and identify the processing of cardholder data (CHD) to appropriately apply safeguards. The primary account number (PAN) is the defining factor for cardholder data. Organizations storing such data should understand the risks associated with such storage and processing.

This paper primarily focuses on possible available technical safeguards provided by SecurDPS that can be useful for the protection of PAN data in customer environments. Comforte requested that Coalfire determine the effectiveness of SecurDPS to support PCI DSS, principally for data protection. The solution submitted for review is positioned to enable visibility, insight, and control capabilities for the organizations subject to PCI DSS to help reduce risk and improve data security.

ABOUT SECURDPS ENTERPRISE SOLUTION

SecurDPS is a scalable and fault-tolerant enterprise tokenization and encryption solution. It enables organizations to achieve end-to-end protection of sensitive data, lower compliance costs, and significantly reduce the impact and liability of data breaches. SecurDPS provides a flexible integration framework that allows for multiple layers of data protection for new and existing applications. Change in existing applications may not be necessary to achieve the protection of data using SecurDPS.

SecurDPS provides protection layers ranging from fully protecting sensitive elements or files using various data protection methods to auditing user access of a specific database record. Additionally, key protection in Hardware Security Modules (HSMs) and dual custodian mechanisms further secure the data when configured. SecurDPS can be integrated with other enterprise data protection solutions and provides a comprehensive and mature set of capabilities that enable data-related risk reduction.

ASSESSMENT SCOPE

The scope of this assessment was to conduct an independent review of SecurDPS. The goals of the technical whitepaper aere to:

- Confirm that SecurDPS can support a consumer-facing enterprise's overall PCI DSS compliance efforts.
- Determine how SecurDPS can reduce the risk and the scope of data stores in the merchant's or enterprise's network PCI DSS compliance respoibilities and efforts.

In this report, Coalfire will explain SecurDPS architecture at a high level, delving into the technical aspects of the solution that are applicable to the compliance. The report will also assess the expected impact of the technology on audit scope using PCI DSS version 3.2.1.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

PCI DSS is an information security standard for organizations that handle branded credit cards from Visa, Master Card, Discover, American Express, and JCB. The PCI standard is mandated by the card brands but administered by the PCI Security Standards Council (PCI SSC). Version 1.0 of PCI DSS was published in 2004. This standard has undergone several updates; the current version is 3.2.1 and was released in May 2019.

PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit CHD or sensitive authentication data (SAD).

Compliance with PCI DSS for the above-named entities is mandatory. Organizations found to be out of compliance with PCI DSS may be subject to fines as assessed by the individual card brands.

PCI DSS is made up of 12 requirements, which can be grouped into six major control objectives:

OBJECTIVES	REQUIREMENTS
Build and maintain a secure network and systems	1. Install and maintain a firewall configuration to protect CHD. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect CHD	3. Protect stored CHD. 4. Encrypt transmission of CHD across open, public networks.
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update antivirus software or programs. 6. Develop and maintain secure systems and applications.
Implement strong access control measures	7. Restrict access to CHD by business need to know. 8. Identify and authenticate access to system components. 9. Restrict physical access to CHD.
Regularly monitor and test networks	10. Track and monitor all access to network resources and CHD. 11. Regularly test security systems and processes.
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel.

Table 1: PCI DSS High Level Requirement

PROTECTING DATA WITH SECURDPS

SecurDPS offers a data-centric security approach for the protection of sensitive data to help organizations meet reasonable data security protection measures to comply with privacy regulations, including General Data Protection Regulation (GDRP) and California Consumer Privacy Act (CCPA). The solution allows for control over sensitive data and protection of data using tokenization and encryption methods without significantly affecting the existing applications.

SecurDPS offers various options, such as encryption, tokenization, format-preserving hashing, and masking methods for protection of sensitive data. Strategy configurations and properties manage protection, which requires the input of a protection method, algorithm attributes, the format of the data, and a distinguishing method.

- **Tokenization**: SecurDPS offers a set of algorithms and random mapping techniques that can be customized to each sensitive data element that needs to be protected. It provides linearly scalable, high-performance tokenization while operating without states or vaults and free of collisions. As the tokenization mapping operations occur purely in memory and the central processing unit (CPU) without any disk input or output operations, the SecurDPS solution offers a secure approach for the protection of sensitive data.[1]

  The SecurDPS tokenization method is based on the static, table-driven tokenization scheme described in the American National Standards Institute (ANSI) X9.119-2 tokenization standard.

- **Encryption**: In classic encryption, the protected data element has completely different format properties from those of the underlying sensitive value. Classic encryption schemes (both symmetric and asymmetric) map values to a protected element that has a different length and typically contains values of a completely different alphabet. The change of the length of the value has a significant impact when it comes to the need to implement data protection. While this usually results in the need to deprotect sensitive data for application usage and processing, classic encryption has its use cases. Examples include data-in-transit protection for complete streams and full file or device encryption for unstructured data. SecurDPS has the ability to translate between protection methods (e.g., encrypted to tokenized data) in a secure fashion, helping to reduce the exposure of clear text data in the data life cycle to an absolute minimum and eliminating any intermediate storage on the server.[1]

- **Format Preserving Encryption (FPE)**: SecurDPS supports tokenization using Format Preserving Encryption (FPE) along with the static, table-based tokenization. The FPE key is kept isolated within the protection node and is not shared with external entities that meet the criteria for encryption-based tokenization.

- **Masking**: SecurDPS performs masking operations by replacing the sensitive data element with a series of masking characters.

- **Format-Preserving Hashing**: Classic hashes (e.g., SHA256), like classic encryption operations, do not preserve the format of the underlying sensitive values. The SecurDPS format-preserving hashing algorithm can be used to preserve irreversible protection with deterministic results in a way that maintains format properties.

INTEGRATING ENTERPRISE APPLICATIONS

SecurDPS offers two options for integrating existing and new enterprise applications with SecurDPS protection services, described below. Benefits of these options include shortened project time through integration capabilities and minimized service interruptions through development and deployment activities.

[1] SB_Enterprise_Tokenization_with_SecurDPS_201911.pdf

SecurDPS offers easy-to-use application programming interfaces (APIs) and integration without changing the record format of the original data:

- **SmartAPIs**: A comprehensive and easy-to-use software development kit (SDK) that consists of SmartAPIs for different programming languages.
- **Transparent Integration**: No application changes are required for this option. The transparency layers provided by SecurDPS inject the data protection options into the application. The underlying SecurDPS processing layer then identifies the sensitive data elements to be protected and performs a call out to the SmartAPI. This simplifies implementation to enterprise, hybrid, and cloud applications, including software-as-a-service (SaaS) environments.

AUDITING AND ANALYZING

SecurDPS has built-in audit and analysis capabilities to help different IT or security stakeholders. SecurDPS provides integration with existing security information and event management (SIEM) frameworks. SecurDPS offers audit trail details for the following areas:

- Status of the data protection system.
- The unique or distinct data elements being protected.
- Sensitive data elements accessed (e.g., how many social security numbers [SSNs] were accessed based on day or time frame selection).
- Specific sensitive data elements accessed and any peak in those activities.
- The application or services accessed including the data elements.
- Sensitive data elements being currently accessed by any users.
- The status of data protection system and the different components.
- The protection system behavior for both past and current occurrences and a comparison offered to show any unusual system behavior.
- Management console access login and details on who accessed data, how often it was accessed, and when it was accessed.
- The actual actions performed by system or users.

SECURDPS ARCHITECTURE REVIEW

ARCHITECTURE COMPONENTS

The Protection Cluster is the main component of SecurDPS and is a centrally managed, scalable, and fault-tolerant cluster of virtual appliances that performs the actual protection operations on the behalf of the enterprise applications. The Protection Cluster consists of the following sub-components:

- **Management Console (MC)**: The protection cluster is centrally administered through an MC. The MC is a hardened appliance that securely stores all configuration data, keys, and secrets required for the cluster operation.
- **Protection Nodes (PNs)**: Protection Cluster consists of multiple clustered soft appliances operating as PNs. Enterprise applications (EAs) connect to the PN to protect or reveal sensitive data elements using SecurDPS APIs or the transparent protection layer. PNs do not store any data on a local or network disk and perform all operations in memory.

- **Audit Console (AC)**: AC collects and displays metrics about usage of protection services by an EA, including the number of distinct sensitive data elements accessed by users in plain text, the number of protection operations per time interval, and the number of failed authentications. The AC can be run standalone or as a cluster on its own. The AC consists of multiple subcomponents and services as shown in Figure 1. Key components of the AC are:
  - **Kafka**: Kafka is a distributed streaming platform. It is used as the message broker and landing platform (LP) for all information from the protection node cluster.
  - **Elasticsearch**: Elasticsearch provides the data storage and analytics engine for Kibana (Dashboard).
  - **Logstash**: Logstash is a data processing pipeline. It is used to ingest data from Kafka into Elasticsearch.
  - **Kibana**: Kibana provides visualization in form of dashboards.
  - **Rsyslog**: Rsyslog is a log message forwarder that implements the syslog protocol. It is used to locally redirect the incoming log and audit stream from the PNs and the MC to Kafka.

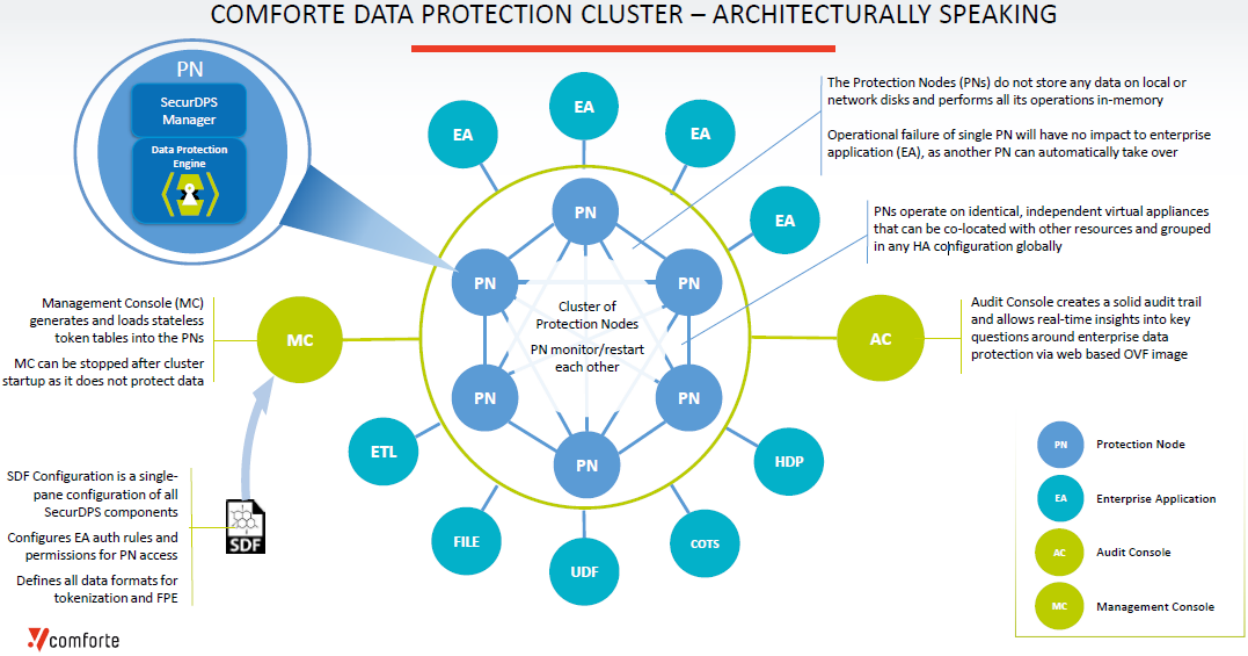

Figure 1: SecurDPS High-Level Architecture and Components

The goal of SecurDPS is to provide a secure architecture for management of the SecurDPS virtual appliance. However, the following aspects are also covered by the solution:

- Hardened operating system (OS) with restricted access – The SecurDPS OS is highly restricted and does not allow any shell or root access or for any software to be installed on the system. The sensitive data on the system is protected using the AES-256 encryption mechanism. Customers can optionally use either HSMs or secure cryptographic devices (SCDs) for the protection of keys if they require an additional layer of protection. The SecurDPS virtual appliance is considered a black box that operates securely by default.
- Single-purpose service user accounts – No user accounts exist for general use and service user accounts only provide the ability to perform activities needed for its purpose. SecurDPS provides strong authentication based on Secure Shell (SSH) public keys or enterprise instant messaging

(IM) based authentication with Kerberos combined with Lightweight Directory Access Protocol (LDAP) based group or role-based access control.

- Minimal external attack surface – SecurDPS virtual appliances only allow SSH connections for incoming network interface connections. SecurDPS supports the use of other protocols via developed components that include proxy capabilities and provide fault tolerance and performance features.
- Stateless protection nodes – The PN operates purely in memory and CPU and does not require permanent storage. The configurations are managed centrally via the MC, which allows for virtually unlimited scalability because no synchronization is needed. This reduces the potential attack surface. Sensitive data (e.g., tokenization secrets) is stored within the MC and PNs hold it in memory once seeded. Once a PN is shut down, the secrets do not exist in the PN.

DEPLOYMENT SCENARIOS

SecurDPS can be implemented using various deployment models, these models provide flexibility for deployment due to use of stateless virtual PNs. The PNs can be deployed everywhere and do not need to synchronize keys or tables. The PNs allow for the protection and deprotection of data everywhere, independent of the location or environment. Common deployment models are discussed in the subsections below.

Option 1: On-Premises Only Deployment

In this deployment option, the MC, AC, and PNs are deployed on-premises. The applications can talk to PNs in the local network in this scenario.

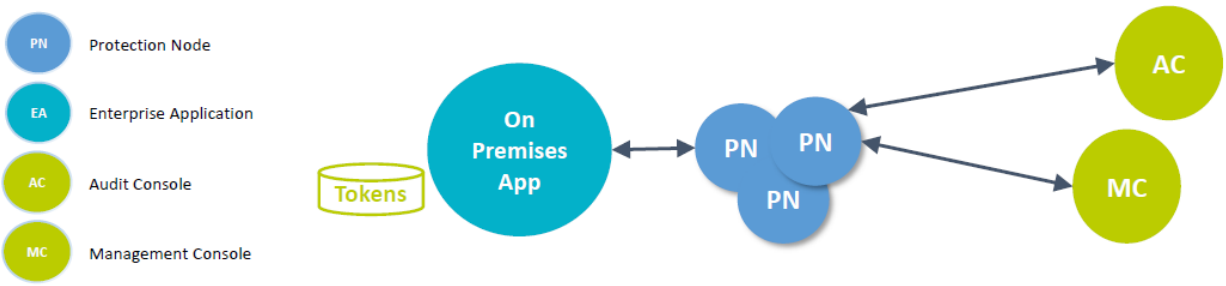

Figure 2: SecurDPS Deployment Model On-Premises

Option 2: Hybrid Deployment

In this deployment option, the MC and AC are deployed on-premises and can be used in conjunction with a PN cluster deployed on-premises or in the cloud. Even when PNs are deployed in the cloud, security-relevant information is never stored in the cloud and only resides in the memory of the PNs.

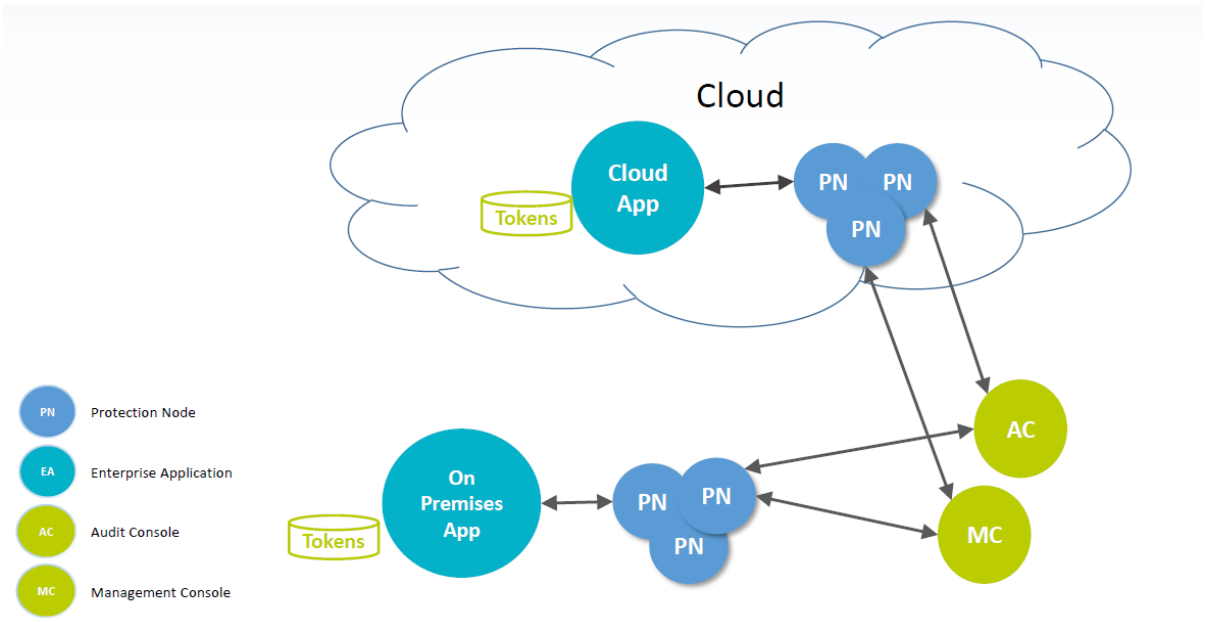

Figure 3: SecurDPS Deployment Model – Hybrid

Option 3: Hybrid Client Cloud Deployment

In this deployment option, all elements of SecurDPS are deployed on a client's cloud infrastructure. The PNs either connect to applications running in a cloud environment or on-premises.

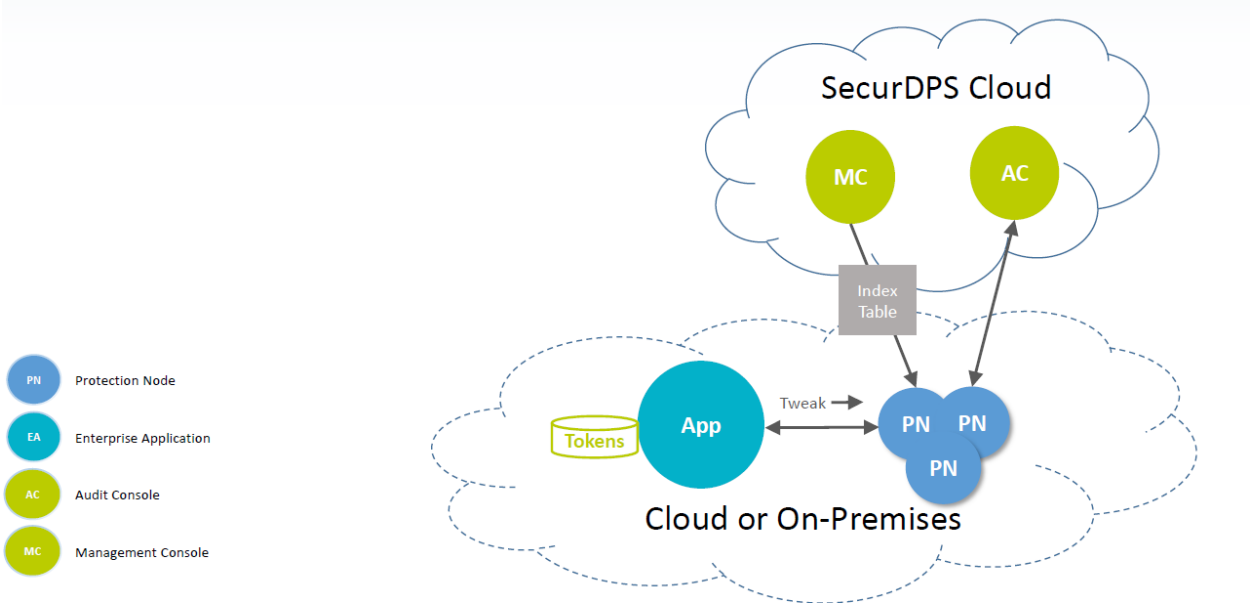

Figure 4: SecurDPS Deployment Model – Hybrid Client Cloud Deployment

ASSESSMENT METHODOLOGY

SecurDPS utilizes encryption, tokenization, and masking technologies for protecting data and requires the controllers to protect the encryption keys or tokenization secrets. SecurDPS allows for the solution to be implemented in the environment and secure implementation steps are outlined in guides and reference manuals provided by Comforte.

Coalfire validated the various protection strategies that can be configured for the protection of sensitive data elements. Strategies tested and their expected outcomes are displayed in Table 2 below.

Coalfire examined SecurDPS impact within a PCI DSS environment. The scope impact was evaluated at a granular level, examining each control. The results are summarized in the Coalfire Findings section.

ASSESSMENT METHODS

Coalfire conducted a technical analysis of SecurDPS by configuring the solution per the instructions outlined by Comforte. Deployment architecture using the MC or AC On-Premises and Hybrid Protection Node Cluster Deployment (Hybrid Deployment) scenario was set up for testing. The SecurDPS MC, PN instances, AC, and syslog server (Kiwi SIEM) were set up as virtual machines within the Coalfire lab.

A sample Java application to verify the file and stream filter integration provided by the vendor was tested on Windows platform with a Java runtime environment. The data was read from a source input stream, the data transformation actions (e.g. tokenization, encryption) were performed, and the modified data was written to a target output stream to a Windows file. The SecurDPS Virtual File System (SDFS) was mounted to a virtual folder to protect the sensitive data within the folder, and the file was available in tokenized format in the mapped folder.

Coalfire performed the following steps to confirm the functionalities offered to support PCI DSS requirements:

1. **Authorization**: The attributes were set with the Security Definition File (SDF) configuration file where the PNs authorized requests from Enterprise Applications (EAs) based on the incoming SSH user ID. The users were authorized based on the public/private key pair. The use of strong authorization algorithms was observed, as shown in Figure 5.

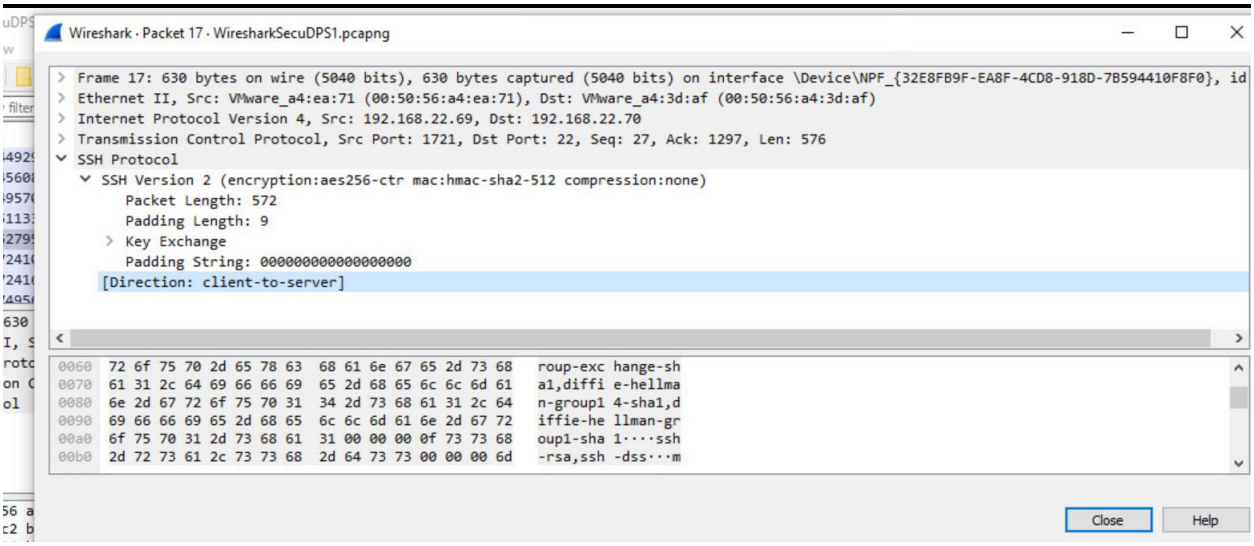

Figure 5: SecurDPS Public/Private Key Pair Authorization

2. **Vault configurations**: Various mechanisms were configured to verify data protection using SecurDPS. The mechanisms configured for data protection were cryptographic algorithms, format-preserving encryption, and stateless tokenization.
3. **Strategy configurations**: The “strategies” section of the SDF file specified how SecurDPS should perform the data protection operations associated with a distinct vault. Multiple strategies were tested with the supported vault type.

4. **Audit Logs**: The audit collector's format was configured to allow for information to be captured in specific audit log format. The log targets were configured to send logs to a syslog server.
5. **Audit Console**: The audit console virtual machine was configured to review the collected metric data about the usage of protection services by the applications.

Vaults and Strategies

Table 2 below depicts input and output data before and after protection mechanism operations have been executed. In the context of SecurDPS, a vault is an object that protects the protection secret used to map between plain data strings and their protected equivalent. The following combinations were validated with SecurDPS during the testing. The vault types supported with SecurDPS solution are:

- **Index Table Vault**: An index table is used by the SecurDPS internal tokenization engine to perform tokenization and detokenization. An index table vault will contain encoded random characters of the given alphabet, which are used to produce tokens with the tokenization algorithm developed by Comforte.
- **Format-Preserving Encryption (FPE) Vault**: An FPE vault is used by SecurDPS to perform FPE or decryption with the FPE algorithm developed by Comforte. An FPE vault will contain the encryption key generated during the initialization step if it is detected that the file specified as vault store does not exist.
- **Basic Masking Vault**: A basic masking vault is used by SecurDPS to perform masking operations where some portion of a sensitive data element is replaced by a series of masking characters.

VAULT TYPE	SECURDPS STRATEGY (SUPPLIED YAML CONFIGURATIONS)	INPUT DATA	OUTPUT RESULTS
FPE	Primary Account Number (PAN): Numeric, Preserve: First 6-Last 4 Alphabet: Distinguish (A-Z) Min-protection – 6 characters	5413330089020010	541333DHIDEB0011
FPE	ACCOUNT NUMBER: Alphabet: A-Z, a-z, 0-9	9001010267	mqoTYkeT0w
FPE	Government ID: Alphabet: A-Z, a-z, 0-9	M08833567	g3CG09Ep9 OR Vnn1oTKm4 OR KcaGwfPfz
FPE	PHONE: Alphabet: A-Z, a-z, 0-9	+44 20 7235 3457	+4U 1y yXC2 ksxZ
FPE	IPADDRESS: Alphabet: A-Z, a-z, 0-9	107.167.245.5	Uu7.TDC.VLd.w
FPE	Date of Birth: Numeric, Preserve: First 2 Alphabet: SQLDATE	3-Jun-07	17-Jan-75
FPE	EMAIL: Alphabet: A-Z, a-z, 0-9	joesmith@hotmail.com	1p6kz49f@8zAUFx5.aS3

VAULT TYPE	SECURDPS STRATEGY (SUPPLIED YAML CONFIGURATIONS)	INPUT DATA	OUTPUT RESULTS
FPE	ADDRESS: Alphabet- ISO8859	550 Larimer St Ste 784, Denver, CO 80021	BsB ik7LtTI Ji 2CL kvo, 2MRFOG, g0 y1frH OR 550 qkvMmQs ZQ tKx 784, xlPWMB, iu 80021
Masking	Primary Account Number (PAN): Numeric, Preserve: First 6-Last 4 Alphabet: Masked character "X" Min-protection – 6 characters	5413330089020010 4761739001010260	541333XXXXXX0011 476173XXXXXX0267
Masking	Numeric, Preserve: First 6-Last 4 Alphabet: Masked characters "A-Z" Min-protection – 6 characters	joesmith@hotmail.com	joesmiABCDEFGHIJ.com
Tokenization	First Name Last Name: Preserve-first 2 Alphabet: A-Z and a-z	John Smith David Smith	Jozr bcSzT Daiuu XYxiF
Tokenization	Primary Account Number (PAN): Numeric, Preserve: First 6-Last 4 Alphabet: Distinguish (A-Z) Min-protection – 6 characters	5413330089020010 4761739001010260	541333DHIDEB0011 476173IEIAIA0267
Tokenization	HOSTNAME: Alphabet: A-Z, a-z, 0-9	DESKTOP-PM76998	XKcCaYy-g6e4fgd

Table 2: SecurDPS Enterprise Solution Testing Results

These examples illustrate the way that the SecurDPS solution protects data. These are a combination of just a few strategies tested – refer to the SecurDPS guides for details on the configuration of strategies and the parameters for additional information. Properties of a strategy include the tokenization table, algorithm attributes, the token format (e.g., how many leading and trailing characters are left in the clear), and a distinguishing method (i.e., how plain values can be distinguished from tokens). Format-preserving tokens can be generated for credit card numbers, SSNs, and other Personally Identifiable Information (PII) such as names or email addresses.

Audit Logging

The SDF attributes and cluster configurations were able to display the log messages within the Kiwi Syslog SIEM as shown in Figure 5. A separate syslog server was configured to receive the log data from the SecurDPS components.

At no time was a submitted PAN found in clear text on the network. The SecurDPS architecture protects the CHD based on the configurations performed by the implementing organization.

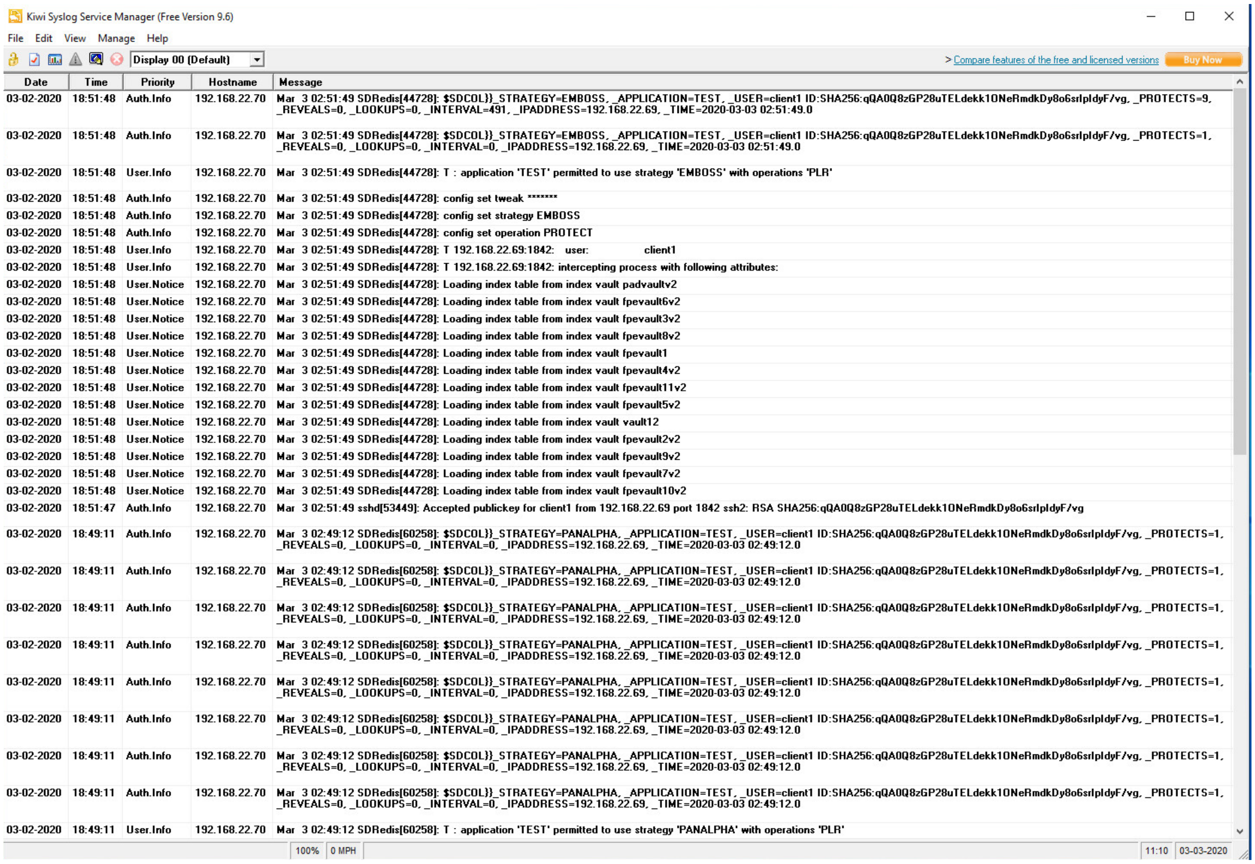

Figure 6: Syslog Messages from SecurDPS

SecurDPS Audit Console

The audit console dashboard can display log messages retrieved from the PNs and management nodes as seen in Figure 6. The SecurDPS audit console dashboard as seen in Figure 7 also provides statistical data represented in graph or pie chart format. The dashboard can provide visibility into the data protection that would be useful for risk assessment or incident response management within the organization.

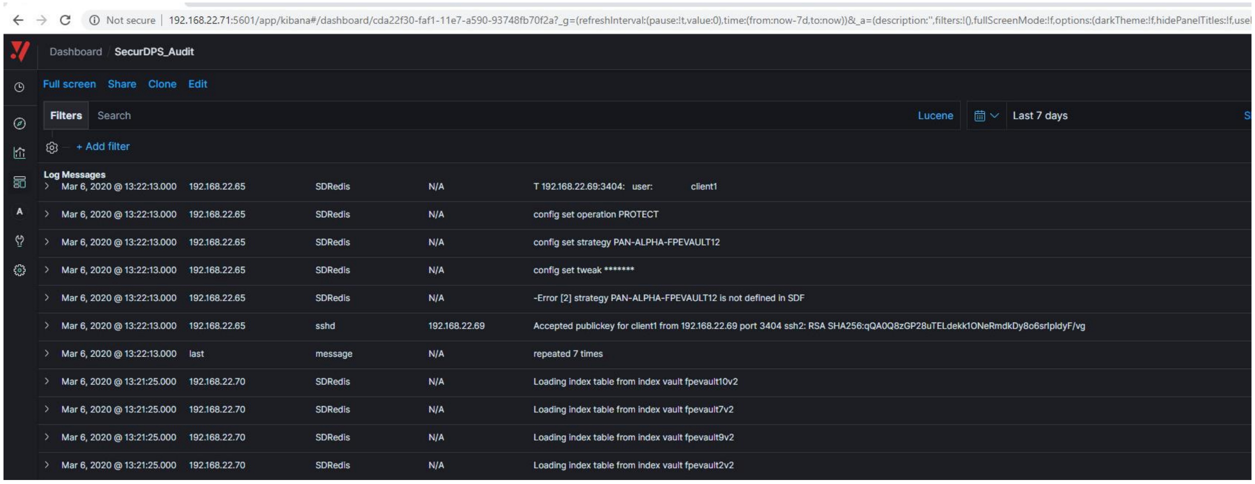

Figure 7: Aggregated Log Messages from SecurDPS Nodes

Figure 8: SecurDPS Audit Console Dashboard

COALFIRE FINDINGS

This paper's primary focus pertains to the use of SecurDPS for supplying technical safeguards that may be used to support an entity's PCI DSS. Coalfire identifies that the proposed solution could be suitable to be considered as part of an organization's technical security measures to ensure a level of security in support of data privacy initiatives. Though applicability of the solution with PCI DSS requirements is narrow, aspects of the proposed solution help to address several common threats associated with IT infrastructures that can pose a threat to data privacy if an organization's systems are compromised.

Principally, the concepts of application of security boundary protection mechanisms may be useful to limit exposure by minimizing accessibility to private data through the cloud infrastructure or application platforms.

Pertaining to applicability for PCI DSS outcomes, Coalfire has determined that narrow applicability can be found across several requirements as noted in the table below.

The following table provides more detail as to the alignment and capabilities of SecurDPS to support PCI DSS outcomes for payment card protection.

POTENTIAL IMPACT ON APPLICABLE CONTROLS TABLE

In this section, the SecurDPS methodology is evaluated against PCI DSS requirements at a granular level. It separates the major requirements in the previous table, providing the anticipated scope impact on each control. Where appropriate, assessor comments are included in the far-right column.

Key to Potential Impact on Applicable Controls Table

APPLICABLE CONTROL LEVEL	DESCRIPTION
✓	Properly implemented, the SecurDPS solution reduces, but does not eliminate, the applicability of this control. The QSA should determine to what extent the control applies.

APPLICABLE CONTROL LEVEL	DESCRIPTION		
✓	**PROPERLY IMPLEMENTED, THE SECURDPS SOLUTION REDUCES, BUT DOES NOT ELIMINATE, THE APPLICABILITY OF THIS CONTROL. THE QSA SHOULD DETERMINE TO WHAT EXTENT THE CONTROL APPLIES.**		
PCI DSS REQUIREMENT	SECURDPS CAN SUPPORT FOR CUSTOMER ENVIRONMENT	SECURDPS MEETS REQIUREMENT	SECURDPS SUPPORT DETAIL
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.			
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. **This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.**	✓		SecurDPS supports the merchant's PCI DSS compliance efforts through its ability to integrate with a customer's LDAP. SecurDPS provides instructions in the implementation guide about changing passwords for all system components that are part of the SecurDPS architecture.
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)	✓		SecurDPS supports the merchant's PCI DSS compliance efforts by implementing one primary function per server.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	✓		SecurDPS enables only the necessary services, protocols, daemons, and similar required by SecurDPS.
2.2.4 Configure system security parameters to prevent misuse.	✓		SecurDPS is accompanied by instruction on the proper and secure configuration of the solution.
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	✓		SecurDPS includes only the necessary functionality.
2.3 Encrypt all non-console administrative access using strong cryptography.	✓		SecurDPS uses SSH2 for non-console administrative access to its components.

APPLICABLE CONTROL LEVEL	DESCRIPTION		
Requirement 3: Protect stored cardholder data.			
3.1 Keep cardholder data storage to a minimum by implementing data retention and policies, procedures, and processes that include at least the following for all cardholder data storage: • **Limiting data storage amounts and retention time to that which is required for legal, regulatory, and business requirements.** • **Processes for secure deletion of data when no longer needed.** • **Specific retention requirements for cardholder data.** • **A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.**		✓	SecurDPS can be configured to utilize capabilities such as tokenization, encryption, masking, or format preserving hashing for the protection of CHD. The data stored on other systems protected with SecurDPS functions would not have access to CHD directly, minimizing the CHD storage with key access. The merchant must implement data retention and disposal policies. Remaining processes and procedures listed in this requirement must be administered by the merchant.
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see more than the first six or last four digits of the PAN.		✓	SecurDPS is configurable to display PAN in format-preserving encrypted, tokenized, or masked forms only. SecurDPS does not have the ability to display full PANs.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • **One-way hashes based on strong cryptography (hash must be of the entire PAN)** • **Truncation (hashing cannot be used to replace the truncated segment of PAN)** • **Index tokens and pads (Pads must be securely stored)** • **Strong cryptography with associated key-management processes and procedures**		✓	SecurDPS is configurable to display PAN in format-preserving encrypted, tokenized, or masked form only. SecurDPS does not have the ability to display full PANs.

APPLICABLE CONTROL LEVEL	DESCRIPTION		
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.		✓	SecurDPS stores configuration data, keys, and secrets required for the cluster operation on the MC.
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • **Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key.** • **Within a secure cryptographic device (such as a hardware [host] security module [HSM] or PTS-approved Point-of-interaction device).** • **As at least two full-length key components or key shares, in accordance with an industry-accepted method.**		✓	SecurDPS stores all secret and private keys on the management console (optionally if HSMs are used). SecurDPS programmatically handles the encryption and tokenization of data and no clear text key management is necessary. Merchants or customers should ensure that the management console with encryption keys or tokenization secrets are protected.
3.5.4 Store cryptographic keys in the fewest possible locations.		✓	SecurDPS meets this requirement by storing cryptographic keys on the MC.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	✓		SecurDPS includes instruction on encryption key management. However, customers must implement processes and procedures with support from SecurDPS.
3.6.1 Generation of strong cryptographic keys	✓		SecurDPS enables the creation of strong cryptographic keys (AES-128 or greater) based on the merchant's needs and preferences.
3.6.2 Secure cryptographic key distribution	✓		SecurDPS does not distribute encryption keys.
3.6.3 Secure cryptographic key storage	✓		SecurDPS stores all secret and private keys on the management console (optionally if HSMs are used).
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been Produced by a given key), as	✓		SecurDPS enables the retirement or replacement of cryptographic keys by modifying the Security Definition File (SDF).

APPLICABLE CONTROL LEVEL	DESCRIPTION		
defined by the associated application vendor or key owner, and based on industry best Practices and guidelines (for example, NIST Special Publication 800-57).			
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component) or keys are suspected of being compromised.	✓		SecurDPS enables the retirement or replacement of cryptographic keys by modifying the SDF.
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.		✓	SecurDPS does not use manual clear-text cryptographic keys.
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	✓		SecurDPS encryption keys only reside on the management console with restricted access, so there is no ability for users to modify the keys. If HSMs are used optionally for the management of keys, the appropriate vendor procedures will have to be followed.
Requirement 6: Develop and maintain secure systems and applications.			
6.2 Ensure that all system components and software are Protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	✓		SecurDPS systems are provided with the current version to customers. Updates are made available as needed.
6.3.1 Remove development, test, and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	✓		SecurDPS environment setup requires the password to be changed for systems, and customers are required to follow the implementation guides or manual to ensure that default passwords for systems are not used.
Requirement 7: Restrict access to cardholder data by business need to know.			
7.1 Limit access to system components and cardholder data to	✓		Access to CHD on the SecurDPS system is restricted to individuals as identified by the merchant.

APPLICABLE CONTROL LEVEL	DESCRIPTION		
only those individuals whose job requires such access.			
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.		✓	SecurDPS uses the principle of least privilege for all user IDs, limiting access to only those users that are needed to perform their respective job functions.
7.1.3 Assign access based on individual personnel's job classification and function.	✓		The merchant is responsible for assigning access to all individuals based on job classification and function.
7.1.4 Require documented approval by authorized parties specifying required privileges.	✓		The merchant is responsible for requiring and obtaining documented approval for all users' access privileges.
7.2 Establish an access control system(s) for system components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.		✓	The merchant is responsible for granting access to SecurDPS based on the users need to know.
Requirement 8: Identify and authenticate access to system components.			
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	✓		The SecurDPS system provides user authentication out of the box by default. By default, unique user IDs are required to access the system components.
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	✓		The SecurDPS AC provides user authentication out of the box by default. By default, SecurDPS includes a single user ID that is used to create, delete, or modify other user IDs, credentials, or other identifier objects. Permissions on the system to make these additions, deletions, or modifications are restricted to those with adequate permissions. Addition, deletion, and modification of user IDs, credentials, or other identifier objects for other system components (MC and PNs) are handled by the underlying OSs.
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	✓		The SecurDPS AC provides user authentication out of the box. The system can be configured to disable user accounts after a specified number of invalid logical access attempts. Customers must configure the lockout threshold on the system based on the requirements or regulations to which they are subject.

APPLICABLE CONTROL LEVEL	DESCRIPTION		
			User lockout threshold for other system components (MC and PNs) are handled by the underlying OSs and must be configured at that level.
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	✓		The SecurDPS AC provides user authentication out of the box. The system can be configured to set a lockout duration for accounts that have been disabled. Customers must configure the lockout duration on the system based on the requirements or regulations to which they are subject. User lockout duration for other system components (MC and PNs) are handled by the underlying OSs and must be configured at that level.
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	✓		The SecurDPS AC provides user authentication out of the box. The system can be configured to require re-authentication after a user session is inactive for a specified period of time. Customers must configure the session timeout value on the system based on the requirements or regulations to which they are subject. Lockout for sessions that have been idle for longer than 15 minutes for other system components (MC and PNs) are handled by the underlying OSs and must be configured at that level.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: **Something you know, such as a password or passphrase.** **Something you have, such as a token device or smart card.** **Something you are, such as a biometric.**	✓		The SecurDPS AC provides user authentication out of the box. The system requires logging in with a user ID and password by default. Configuring user authentication for other system components (MC and PNs) are handled by the underlying OSs and must be configured at that level. In addition to assigning unique user IDs to all users, customers are responsible for assigning a strong password based on the requirements or regulations to which they are subject.

APPLICABLE CONTROL LEVEL	DESCRIPTION		
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.		✓	SecurDPS provides secure transmission of authentication credentials by use of the SSH protocol by default.
8.2.2 Verify user identity before modifying any authentication credential — for example, performing password resets, provisioning new tokens, or generating new keys.	✓		This is a process-driven requirement. Customers must have a process in place to verify the identity of a user requesting a password reset, the provisioning of new tokens, or generation of any new keys.
8.2.3 Passwords/passphrases must meet the following: • **Require a minimum length of at least seven characters.** • **Contain both numeric and alphabetic characters.** **Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.**	✓		The SecurDPS AC can help customers meet this requirement by integrating the system into the customer's LDAP or Kerberos implementation. Password minimum length for other system components (MC and PNs) are handled by the underlying OSs and must be configured at that level.
8.2.4 Change user passwords/passphrases at least once every 90 days.	✓		The SecurDPS AC can help customers meet this requirement by integrating the system into the customer's LDAP or Kerberos implementation. Maximum password age of 90 days for other system components (MC and PNs), are handled by the underlying OSs and must be configured at that level.
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	✓		The SecurDPS AC can help customers meet this requirement by integrating the system into the customer's LDAP or Kerberos implementation. Preventing the reuse of the last four passwords for other system components (MC and PNs) are handled by the underlying OSs and must be configured at that level.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • **Generic user IDs are disabled or removed.**		✓	The SecurDPS AC does not support group, generic, or shared IDs. Customers are responsible to create unique IDs per individual for access and use of the system.

APPLICABLE CONTROL LEVEL	DESCRIPTION		
• **Shared user IDs do not exist for system administration and other critical functions.** • **Shared and generic user IDs are not used to administer any system components.**			Disallowing the use of group, generic, or shared user IDs for other system components (MC and PNs) are handled by the underlying operating systems and must be configured at that level.
Requirement 10: Track and monitor all access to network resources and cardholder data.			
10.1 Implement audit trails to link all access to system components to each individual user.	✓		SecurDPS includes log entries that link access to its components to individual users.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	✓		SecurDPS audit trails, when configured, can be used to support the merchant's environment.
10.2.1 All individual user accesses to cardholder data	✓		SecurDPS includes log entries for access to CHD.
10.2.2 All actions taken by any individual with root or administrative privileges	✓		SecurDPS includes log entries for actions taken by an individual with root or administrative privileges.
10.2.3 Access to all audit trails	✓		SecurDPS includes log entries for access to audit trails.
10.2.4 Invalid logical access attempts	✓		SecurDPS includes log entries for invalid logical access attempts.
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of Privileges—and all changes, additions, or deletions to accounts with root or administrative Privileges	✓		SecurDPS includes log entries for use and changes to identification and authentication mechanisms.
10.2.6 Initialization, stopping, or Pausing of the audit logs	✓		SecurDPS includes log entries for invalid logical access attempts.
10.2.7 Creation and deletion of system-level objects	✓		SecurDPS includes log entries for the creation and deletion of system level objects.
10.3 Record at least the following audit trail entries for all system components for each event:			
10.3.1 User identification	✓		SecurDPS log entries include user identification.
10.3.2 Type of event	✓		SecurDPS log entries include the type of event.
10.3.3 Date and time	✓		SecurDPS log entries include the date and time of the event.

APPLICABLE CONTROL LEVEL	DESCRIPTION		
10.3.4 Success or failure indication	✓		SecurDPS log entries include the success or failure of the event.
10.3.5 Origination of event	✓		SecurDPS log entries include the origination of the event.
10.3.6 Identity or name of affected data, system component, or resource.	✓		SecurDPS log entries include the name of the affected data or system.
10.5 Secure audit trails so they cannot be altered.		✓	SecurDPS audit logs are captured within management console and cannot be altered.
10.5.1 Limit viewing of audit trails to those with a job-related need.		✓	SecurDPS only permits authorized users with a job-related need to view audit trails.
10.5.2 Protect audit trail files from unauthorized modifications.		✓	SecurDPS audit logs cannot be altered.
10.5.3 Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.		✓	SecurDPS logs audit logging and audit console functionalities can be utilized to meet the necessary audit trail functions for SecurDPS components.
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.		✓	SecurDPS logs audit logging and audit console functionalities can be utilized to meet the necessary audit trail functions for SecurDPS components.
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	✓		The retention of logs will have to be configured by customer to ensure that they meet the necessary requirement.
Requirement 12: Maintain a policy that addresses information security for all personnel.			
12.3.2 Authentication for use of the technology	✓		The SecurDPS system provides user authentication out of the box by default. By default, unique user IDs are required to access the system components.

CONCLUSION

The features or capabilities offered by SecurDPS, such as tokenization, encryption, masking, hashing, logging, and monitoring, can be used towards implementing strong technical safeguards to comply with a subset of PCI DSS requirements. Features within SecurDPS can help enterprises protect CHD in their environment. Implemented properly per guidance documentation from Comforte, the SecurDPS solution can reduce the impact of data breaches. Also, if implemented properly per guidance documentation from Comforte and with limited storage of CHD, SecurDPS will support a customer's PCI DSS validation efforts.

The findings revealed that no clear text CHD is stored or processed within SecurDPS when it is deployed in a manner consistent with SecurDPS implementation guidance.

It is important to note that no one product, technology, or solution can address all security and compliance requirements. Security is a design principle that must be addressed through carefully planned and implemented strategies. Entities seeking compliance are best able to obtain it through its GRC program.

REFERENCES

- PCI SSC - Data Security Standard (https://www.pcisecuritystandards.org/document_library)
- SB_Enterprise_Tokenization_with_SecurDPS_201911.pdf
- SecurDPS_Enterprise_Protection_Cluster.pdf
- SecurDPS_Enterprise_Integration_For_Windows_Manual.pdf
- SecurDPS_Enterprise_Virtual_File_System_for_Linux_Reference_Manual.pdf
- SecurDPS_Enterprise_REST_API.pdf
- SecurDPS_Enterprise_SmartAPI_for_Java_Reference_Manual.pdf
- SecurDPS Audit Console Reference Manual.pdf

ABOUT THE AUTHORS

Lyle Miller | Principal

Lyle Miller is an application security specialist for the Solution Validation team at Coalfire. Lyle has over 19 years of experience in the IT security industry and over 9 years of experience working as a PCI Qualified Security Assessor (QSA) and Payment Applicationj-Qualified Security Assessor (PA-QSA), helping clients secure their systems and software for use in PCI DSS environments. He currently holds Computer Information Security Auditor (CISA), Computer Information Systems Security Professional (CISSP), QSA, PA-QSA, Secure Software Assessor (SSA), and Secure Software LifeCycle Assessor (SSLCA) certifications. As a lead PA-QSA, Lyle supports assessments for some of the largest payment software providers in the world, helping teams recognize the importance of secure code development and information security within their operational practices.

Nick Trenc | Director

Nick Trenc is the Director of the Solution Validation team at Coalfire. Nick has several years of experience working in information security and has an in-depth understanding of application, network, and system security architectures. He holds CISA, CISSP, SSA, SSLCA, QSA (P2PE), PA-QSA (P2PE), Qualified Pin Assessor (
certifications.

Published July 2020.

ABOUT COALFIRE

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit Coalfire.com.