sysnet® | Cyber Risk

base

Base Commerce CypherPay™ Whitepaper

Sysnet Global Solutions works in partnership with **Base Commerce** providing assistance and advice to their customers to help them meet their regulatory and cyber security requirements.

Prepared by: **Greg Kraft**

Report issue date: **May 31, 2019**

Table of Contents

Distribution List

Company	Name	Project Role
Sysnet Global Solutions Cyber Risk Services 1st Floor, Block 71a, The Plaza, Park West Business Park, Dublin, 12, Ireland	**James Devoy**	Head of Consulting
	Greg Kraft	Document Author
	Jeff Montgomery	Regional Manager – Americas
Base Commerce	**Brian Bonfiglio**	CEO
	Zachary Walker	Primary Project Contact

Revision History

Rev	Date	Description
0.7	01 April 2019	QA
0.8	06 April 2019	Technical Review
1.0	31 May 2019	Final Release

1. Executive Summary

1.1. Introduction

Base Commerce have tasked Sysnet Global Solutions' Cyber Risk Services to perform an assessment of controls and control reduction testing against the CypherPay™ solution offered to service providers and merchants. The scope of the assessment has been provided by the client and is detailed in section 3.1. Assessment of the controls related to PCI DSS 3.2.1 in addition to PCI P2PE V2.0 Rev 1.1 were tested for the scope of this assessment, in order to align the understanding of the Base Commerce solution and how this benefits the applicable control reductions for service providers and merchants using the intuitive CypherPay™ solution designed and implemented by Base Commerce.

The findings detailed within this report reflect the environment at the time of testing, this may not necessarily reflect the current environment, or custom implementations by service providers, and does not constitute a formal assessment of compliance.

The tests were carried out onsite over a 5-day period with the Base Commerce development, operational, cryptographic key management and technical teams at the Base Commerce headquarters in Arizona, USA, in accordance with the best practice methodologies of NIST 800-57 for cryptographic key management, in addition to applicable PCI DSS V3.2.1 controls and applicable P2PE V2.0 rev1.1 control requirements. Vulnerability assessments against the infrastructure and systems were conducted using Kali, Nessus and forensics tools such as Autopsy. Both, automated and manual techniques were used to evaluate the security posture of the target systems.

Forensic information was gathered by traffic analysis and system image snapshots via FTK to ascertain the state of transient data, in relation to industry best practice standards for securing data in transit and securing communication mechanisms in use.

Validation of controls in the form of coding practices, and systems implementation and deployment are additionally covered by an annual PCI DSS assessment as a foundation to this assessment on Base Commerce systems.

1.2. Introduction to Base Commerce

Founded in 2008, Base Commerce is a leading provider of advanced payment processing solutions. Headquartered in Phoenix, AZ and expanded to Jacksonville, FL, the company is a powerhouse in fin-tech, with stakeholders in the payments ecosystem relying on the company's comprehensive suite of technology and services to ensure that payments are processed securely, efficiently, and cost-effectively.

The company started in the world of payments by solely focusing on ACH and electronic check processing. As the company matured, they identified an opportunity to provide a more comprehensive solution by incorporating card payment processing into their strategy. In addition to adding services, Base Commerce continues to grow through the acquisition of smaller processing companies and innovating their own technology solutions for the payments industry.

For over a decade, Base Commerce has been perfecting payment acceptance with a simple, fast, and secure platform that supports all payment type acceptance through a single connection. The company continues to experience impressive year-over-year growth, an ever-expanding portfolio, and one of the most tenured and innovative teams in the industry. The company is driven and focused on successfully collaborating with their partners and using advanced technology to facilitate lasting value. Base Commerce has continuously proven throughout the years that innovation is at the forefront of their philosophy, as they have pushed to create solutions that break the mold.

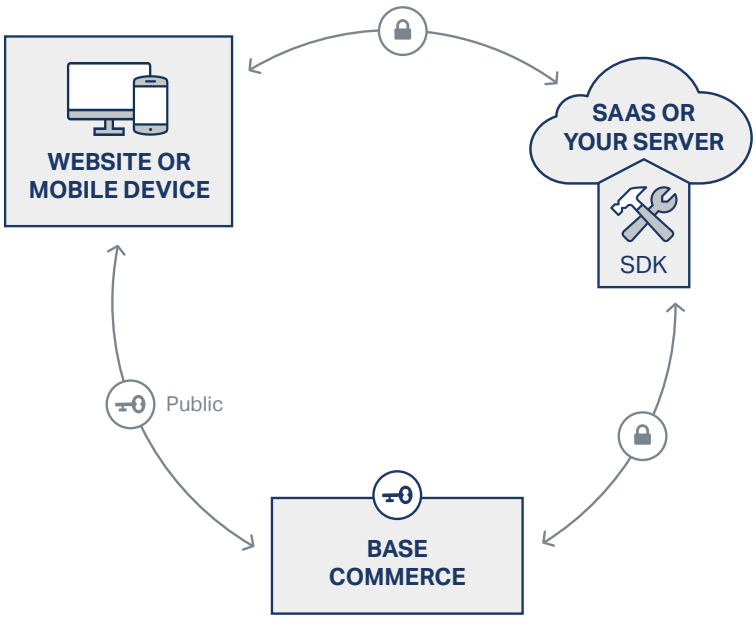
Armed with an experienced team focused on the customer experience and developing mutually beneficial relationships to support growth and success, Base Commerce continues to pave a new path in the payments space by focusing on solutions that provide their customers with the right tools to accelerate their business.

1.3. CypherPay™ Overview

The Base Commerce CypherPay™ (CypherPay™) E2EE solution is a framework accessible through our Prebuilt SDKs that removes all cardholder data from a client's environment. By encrypting cardholder data and banking data at the point of entry and producing a unique public key for each transaction, Base Commerce can ensure that the software and technology environment is never exposed to any unencrypted data. And, clients maintain complete control of the user experience.

The complete removal of cardholder data through a QSA-approved CypherPay™ solution means client applications get a significant PCI compliance scope reduction and merchants can become PCI compliant by answering three simple questions in the Base Commerce Merchant Portal. This means that you have less to worry about when it comes to data security and PCI compliance rules and can spend more time building the best application in your market.

See a simple diagrammatic explanation below:



1.4. Summary of Findings

We present below a summary of findings related to this technical review to provide pertinent elements for consideration.

Sysnet Global Solutions have presented these findings as follows:

- **Scope reduction**
  - Scope reduction is achievable by correct implementation of the CypherPay™ solution as data is not accessible to the service provider or merchant environment.
  - Service providers are able to complete assessments with minimal requirements applicable, yet it allows service providers to manage maintain their clients effectively.
  - Merchants are able to complete an assessment with significantly less requirements, once they are making use of a correctly implemented CypherPay™ solution.
- **Cryptographic data elements**
  - The cryptographic data elements were found to be strong making use of a PKI (Public Key Infrastructure) 2048 bit public / private key pairs. PKI allows for the secure distribution of cryptographic mechanism, as the public key allows for the encryption of data elements that are only deciphered at the decryption point within the Base Commerce secured infrastructure.
  - The data is further secured by making use of a process that generates a new PKI key pair per transaction session, ensuring that keys are managed in a secure manner for each transaction vastly increases the security of data transmitted, as it allows the use of a specific PKI keypair for a single transaction session, and significantly eliminates the ability to compromise a single key.
- **Cryptographic transport elements**
  - Cryptographic transport makes use of strong mechanisms, using TLS 1.2 (4096 bit) via a trusted certificate authority, ensuring that communications are encrypted using industry accepted best practices and protocol strengths.
- **General findings**
  - When CypherPay™ is implemented correctly it significantly reduces the risk of PCI related data compromise, as cardholder data would not be present in the client environments, Base Commerce handles the sensitive information on the client's behalf and provides a secure manner to manage their business through a PCI DSS validated solution.

2. PCI DSS Applicability to Control Reduction

The Payment Card Industry Security Standards Council (PCI SSC) is the owner and author of the PCI suite of standards and as such is responsible for designating the applicable controls for compliance across the suite of standards. The standards are primarily focused on assuring the protection of card holder data and sensitive authentication data as described below:

Cardholder Data (CHD):

- **Primary Account Number (PAN)**
- **Cardholder Name**
- **Expiry Date**
- **Service Codes**

Sensitive Authentication Data (SAD):

- **PIN**
- **PIN Blocks**
- **CAV2/CVV/CVC2/CID**
- **Track 1/2 Magstripe Data**
- **IC Chip Data**

Within this paper, our attention is focused on the control reduction of PCI DSS V3.2.1 controls, when correct implementation of the CypherPay™ solution is undertaken.

The PCI SSC makes various guidance documents available on a regular basis to assist in the guidance of merchants and service providers understanding the applicability of PCI DSS controls within their environment. Please see the reference on scoping guidelines to gain a better understanding of what scope pertains to in regard to PCI DSS V3.2.1

https://www.pcisecuritystandards.org/documents

Guidance for PCI DSS Scoping and Network Segmentation V1.1 released May 2017, provides related information of what constitutes an in-scope element of validation and also provides various mechanisms for minimizing the scope of validation, such as segmentation (isolation of sensitive systems), tokenization (devaluing of data), and removal of data not required by systems in order to remove those systems from scope entirely.

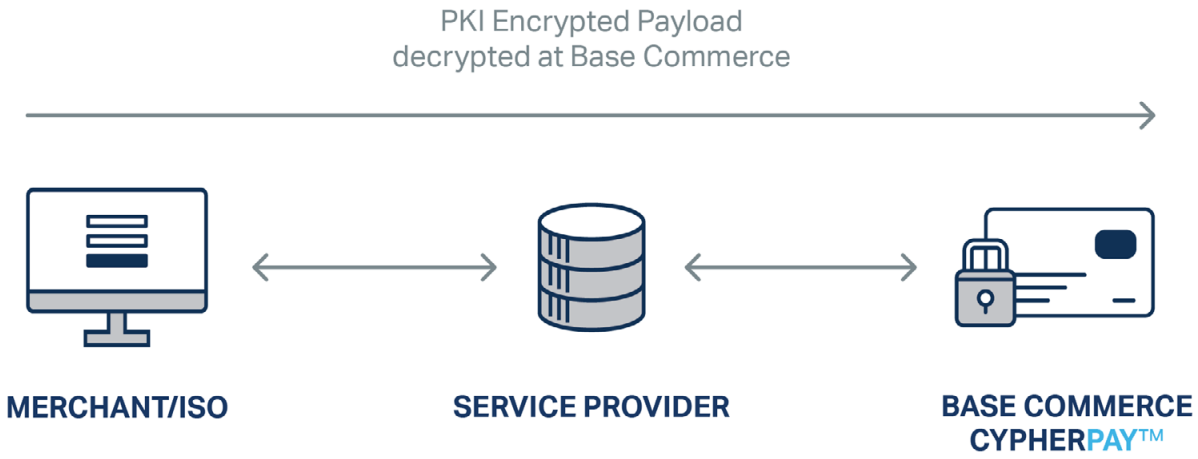
Our focus within this document is not concerned with the reduction of scope, but rather the applicability of the controls to systems that do not ever see the unencrypted data, or have the capability of decrypting the data at all and only act as a conduit for securely transporting the entire encrypted payload to a secure location where it is handled by a certified, validated partner.

The specific verbiage from the guidance document we will focus our attention on is provided in section 2.1 of the document and reads as follows:

> *"If an entity outsources in-scope functions or facilities to a third party, or utilizes a third-party service that impacts how it meets PCI DSS requirements, the entity will need to work with the third party to ensure the applicable aspects of the service are included in scope for PCI DSS either for the entity or the service provider. It is also important for both parties to clearly understand which PCI DSS requirements are being provided by the service provider and which are the responsibility of the entity using the service."*

What this outlines within the context of this document is that if a payment provider such as Base Commerce is able to secure the information at a point of entry, such as the merchant, and covers those services as part of their annual PCI DSS validation, then a third party provider which is present would have a massive reduction in the applicable scope of their validation in turn.

Please see the diagram below illustrating this principle:



By implementation of the Base Commerce CypherPay™ solution a client would be able to understand their applicability of required controls to meet PCI DSS Version 3.2.1 and ascertain a clear understanding of their responsibilities in achieving compliance. It should be clearly understood that by implementing the CypherPay™ solution, a client would not be excluded from compliance, but rather be able to demonstrate a significantly reduced scope for assessment, as is detailed in the requirements matrix in Appendix 5.1. Please scroll down and view the appendix to have a clear understanding of the requirement that would still form part of the responsibilities of a client.

Once implemented, a client would significantly reduce the associated risk of loss of cardholder data, as they would not have any access to clear text data containing any sensitive information, and to that end, they would also heavily mitigate the risk of cardholder data compromise.

Regardless of the reduction in PCI controls to the client environment, clients should still be aware that they should continue to maintain an information security posture, and ongoing information security governance, in order to avoid the ongoing risk of data compromises.

In summary, a client should be able to make use of this paper, as guidance to their QSA, to effectively demonstrate the applicability of controls and provide assurances that the client has no access to sensitive information, and that the controls they are responsible for are addressed in the appropriate manner. This in turn can be used to demonstrate to acquirers and payment brands that the client has addressed their responsibilities in securing the payment channels effectively and has addressed their responsibilities of their reduced scope effectively. The Major benefit of implementing CypherPay™ would be as follows:

- **Reduction in applicable control deployment to the client solutions.**
- **Reduction in efforts and cost of compliance programs.**

3. Assessment Criteria

3.1. Scope

The infrastructure and architecture of systems are built around the following:

CypherPay™ components, which include the elements below are validated under PCI DSS Version 3.2.1 and have an AOC (Attestation of Compliance) dated within the last 12 months.

List BC Elements here:

- **Fortinet Firewalls with IDS/IPS**
- **Apache Web Servers**
- **Unix based Application and Database Servers**
- **Luna HSM's**

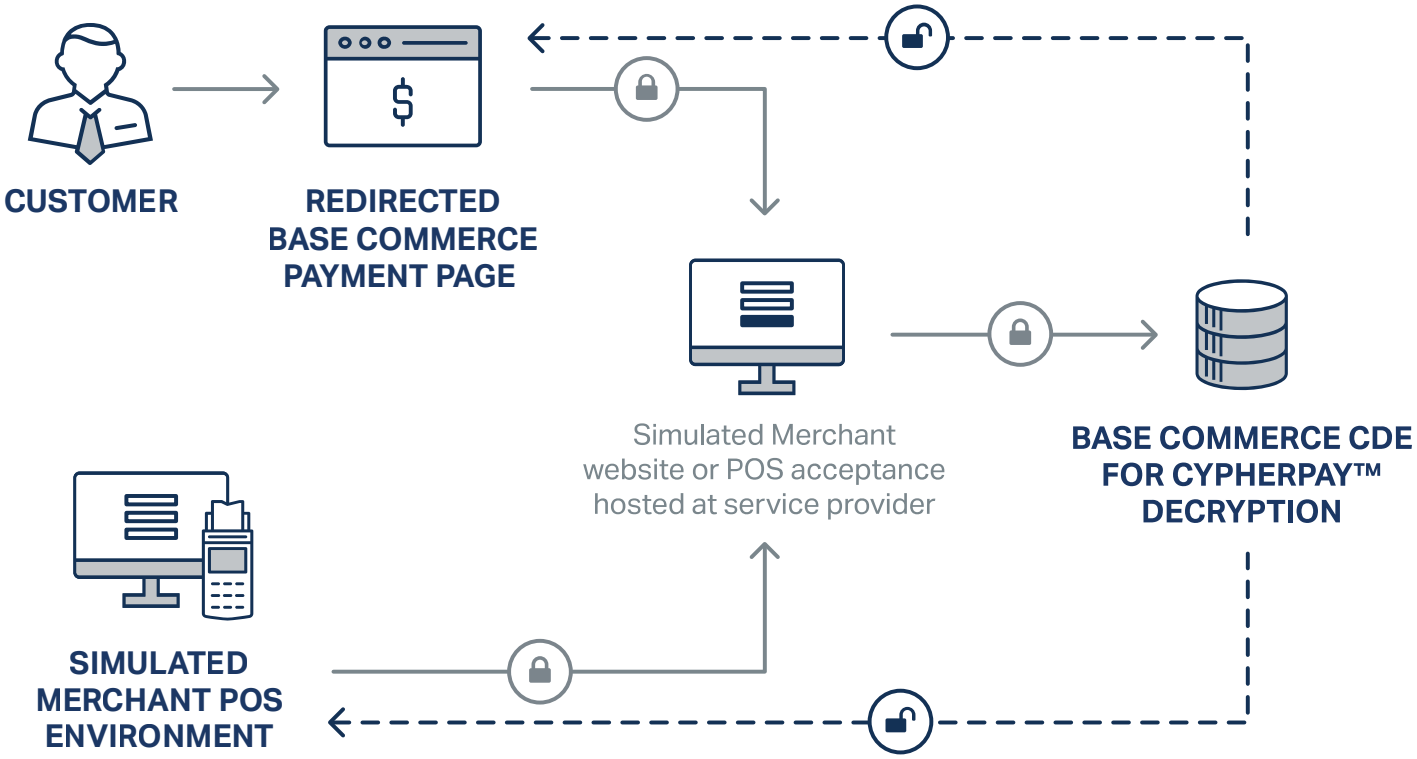
Simulated end points, including the following:

- **Windows workstation with FTK Imager and Wireshark, to simulate merchant environment for e-Commerce and POI based transactions and capture relevant images and data transmission.**
- **POI devices as below:**
  - ID Tech – Secure Mag
  - Ingenico – IPP 350
  - Ingenico – IPP 320
  - Ingenico – ICT 250
  - Ingenico – ICT 220
- **Base Commerce CypherPay™ decryption environment, capturing transmissions via Linux TCPDump, into pcap format for analysis on Wireshark.**

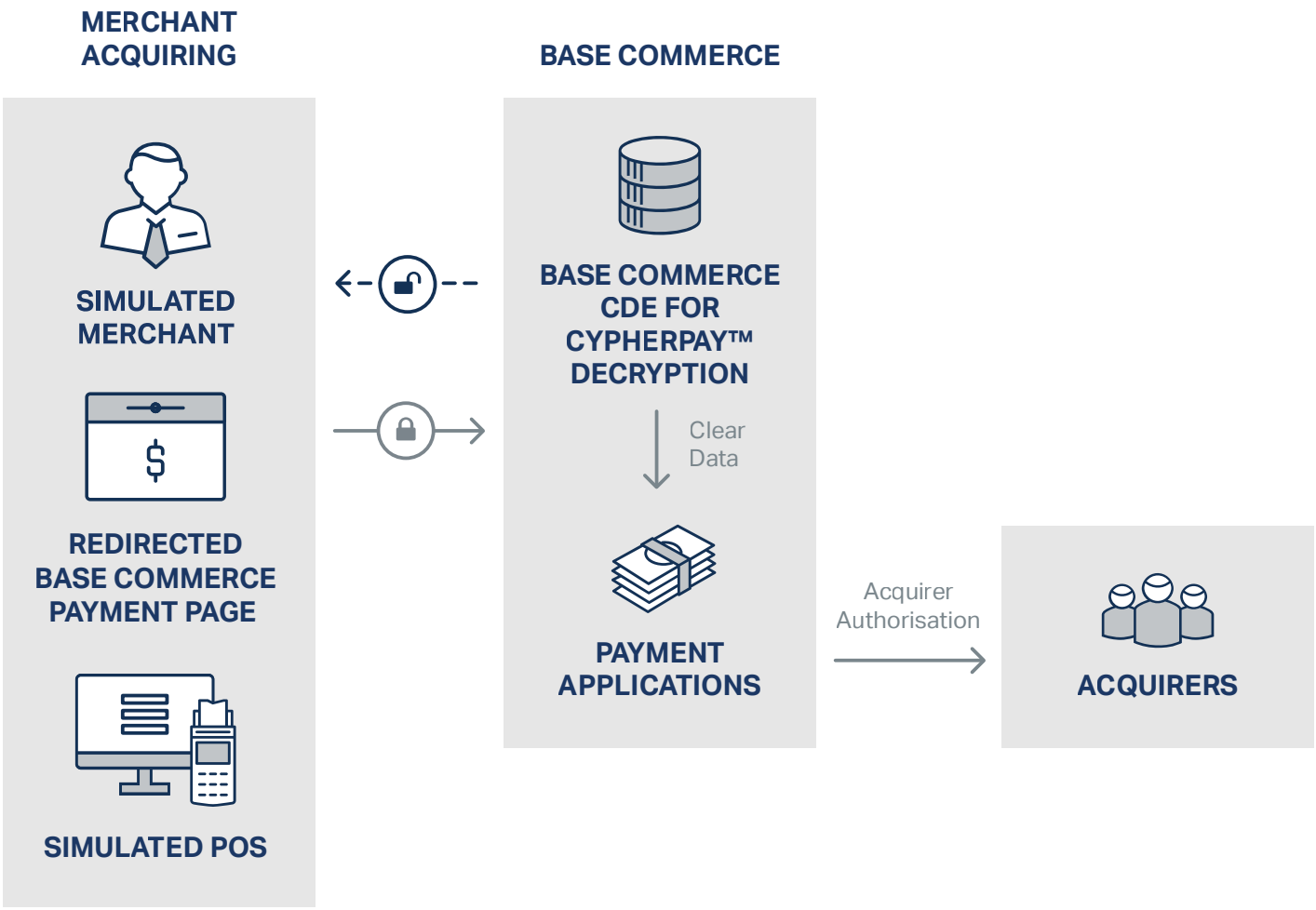
CypherPay™ implements an encryption methodology that enables end point devices to negotiate, via SDK, a unique PKI based key (public) per session which is held in the CypherPay™ suite database under strong encryption (TDES 168) for decryption (Private Key) after which the keys are removed from the database and discarded. The entire payload is encrypted using the PKI public key, which is then transmitted across a secured TLS 1.2 channel, while traversing the service provider infrastructure as per the below environment and dataflow diagrams.

See below diagrams depicting the environment for testing:

Testing environment



Dataflow

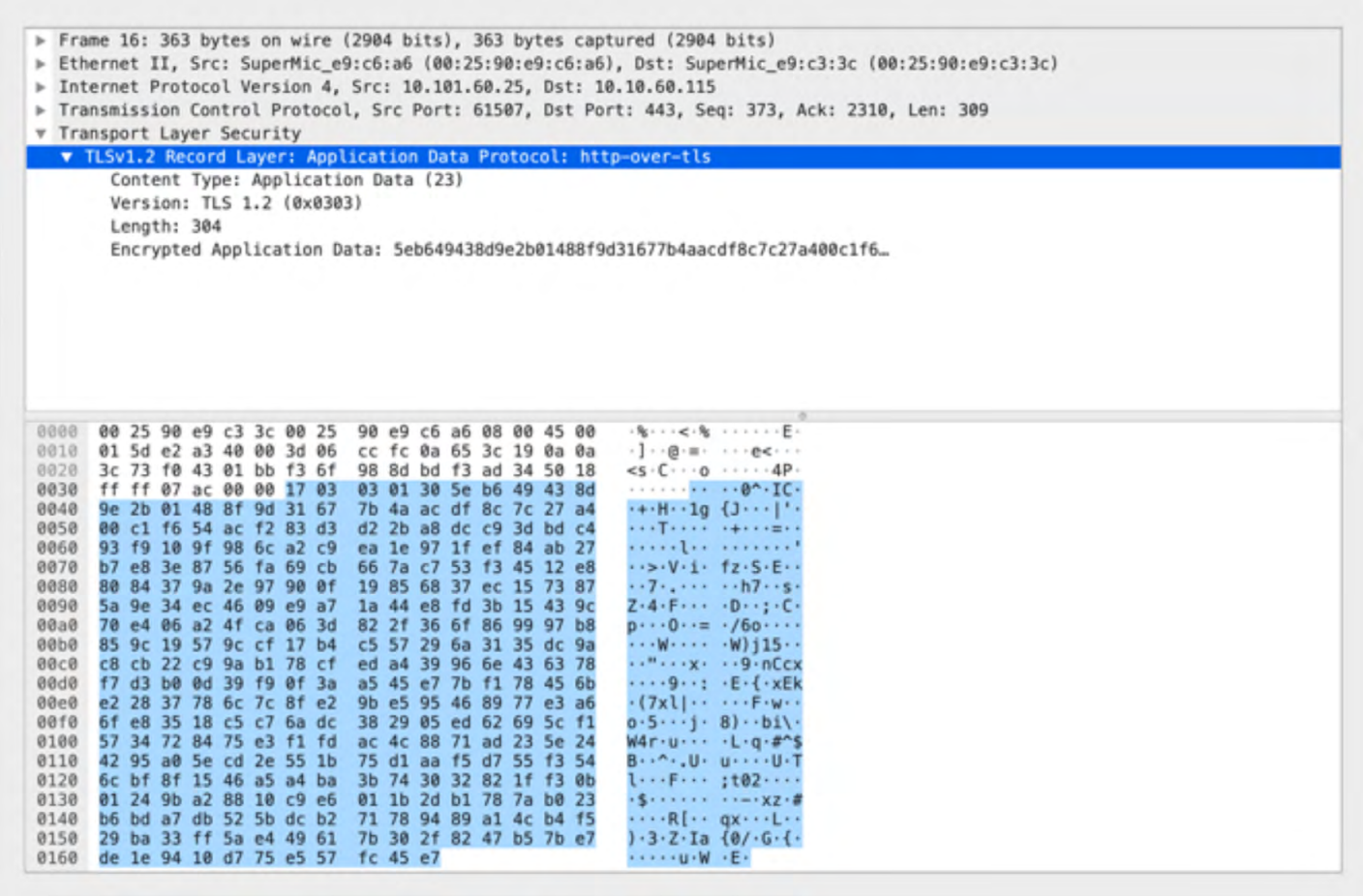


The assessment focuses on the following:

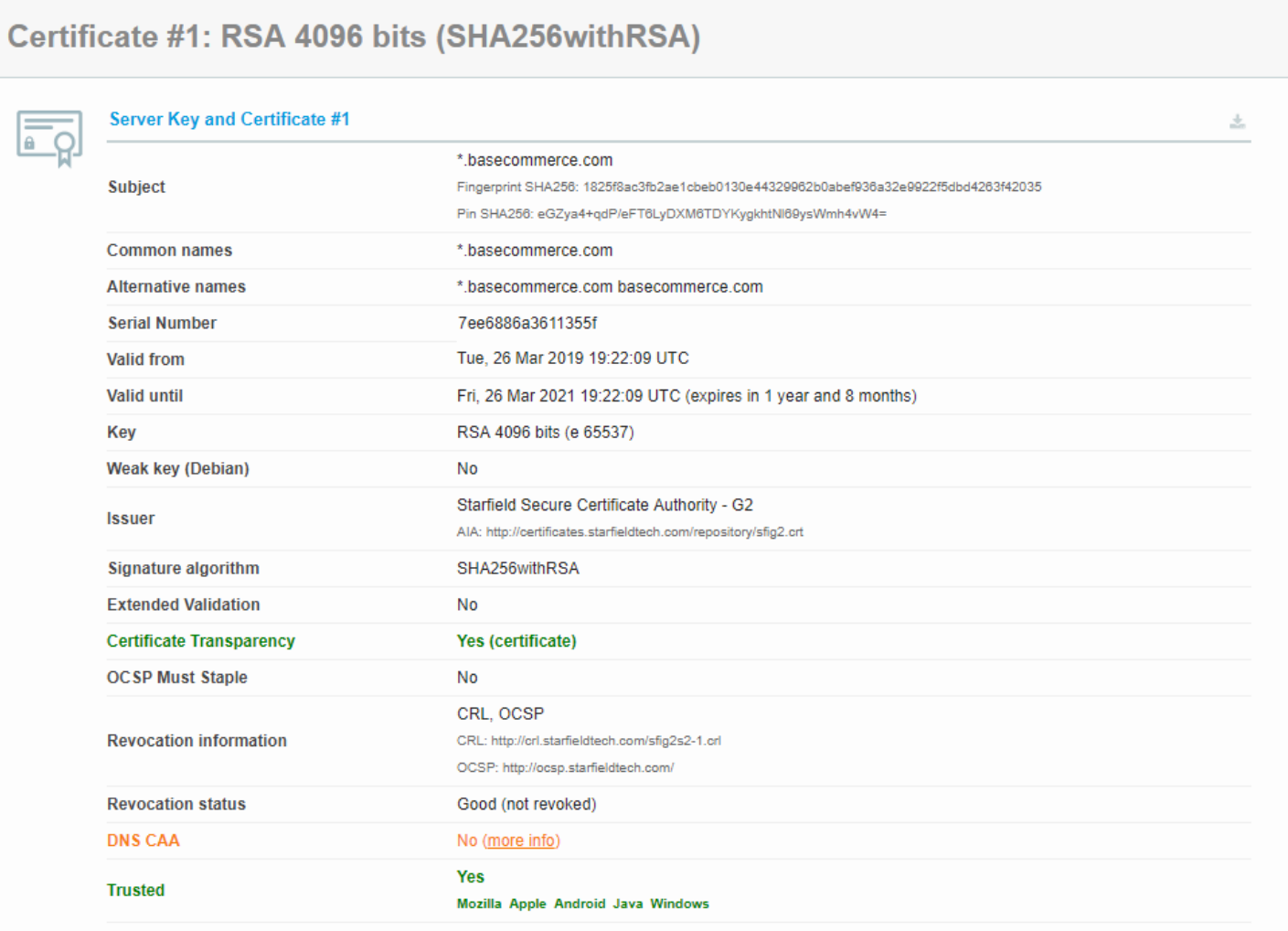
- Validation of the encryption mechanisms from encryption endpoints to the Base Commerce CDE decryption environment and any messages returned to the merchant environment depicting status of the transaction or any resultant error codes.
- Cryptographic key management principles in alignment with NIST 800-57, and PCI SSC P2PE version 2.0 rev1.1.
- The implementation of PKI for payload encryption and decryption.
- The implementation of secure communication channels using TLS 1.2.
- Forensic investigation of end point systems, via FTK and Autopsy to determine the existence of any latent cardholder data or sensitive authentication data post authorization of transactions.
- Performing transactions for each of the envisaged payment channels to include:
  - POS, as per POI list
  - e-Commerce based transactions

3.2. Validation of data in transit

Validation of the data in transit was undertaken making use of Wireshark to assess traffic in transit in addition to the validation of certificates used within the CypherPay™ solution, to ensure verifiable certificates are used, and generated to the correct strength and algorithms as per the relevant PCI DSS, NIST and P2PE programs. The image below confirms the use of TLS 1.2 (4096) in communication channels, in addition to verification of the Base Commerce certificates used within the production environment being tested against SSL Labs for confirmation of correct verification mechanisms and algorithm strength.



SSL Labs verification:



Certificate #1: RSA 4096 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.basecommerce.com Fingerprint SHA256: 1825f8ac3fb2ae1cbeb0130e44329962b0abef936a32e9922f5dbd4263f42035 Pin SHA256: eGZya4+qdP/eFT6LyDXM6TDYKygkhtNl69ysWmh4vW4=
Common names	*.basecommerce.com
Alternative names	*.basecommerce.com basecommerce.com
Serial Number	7ee6886a3611355f
Valid from	Tue, 26 Mar 2019 19:22:09 UTC
Valid until	Fri, 26 Mar 2021 19:22:09 UTC (expires in 1 year and 8 months)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	Starfield Secure Certificate Authority - G2 AIA: http://certificates.starfieldtech.com/repository/sfig2.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.starfieldtech.com/sfig2s2-1.crl OCSP: http://ocsp.starfieldtech.com/
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

3.3. Payload and application environment validation

Validation of the Payload data was undertaken making use of the FTK Toolkit, Autopsy and Wireshark to analyze the payload for cardholder data. FTK was used to take image snapshots of the environment to ensure no latent cardholder data existed in the systems post authorization, and data inspection undertaken by autopsy to check through payload data and system data for clarification of non-existence of cardholder data and sensitive authentication data.

Specific details of the test card used for POI transactions was searched across the images gathered for each transaction type, and was found to be unavailable, as payload was encrypted, and systems images showed that the relevant programmatic methods used to clear the data from any storage mechanisms, both disk based and memory based were enforced.

Full track data used in search:

```
025201801F422800009BA5FC9AC38FA8CE610B5F3D6B3D9A137B82ED03CC3E32B11D7A39098E8A
F74E620024A9F452CC9457E9C6B2514DF930AF12107A2A81F47A12175607F56ACAA736DFE9255E4
67D5E3CBE41216C26A134096F7C3568405362224EE9AC877F3166AEE643B32800A9EC543A1BF6A
6311379A2D56FC87F947DFDC59AAF7F32ACC632B71F70529FCF938C6FD049E86F930A862C72B42
1B10C83845BFFFF8880015009A000120BE503
```

Card Details used in search:

Card Number: 47**********8893

Card Expiration Month: 01

Card Expiration Year: 2021

3.4. Cryptographic Key Management

As part of the validation criteria cryptographic key management principles were evaluated against the NIST 800-57 standards in addition to P2PE Version 2.0 rev 1.1 and encompassed the following elements.

Cryptographic Key Management policies and procedural documentation, for Key Custodians, Key Generation, Key Traversal, Key Destruction for higher level keys, as application calls to the HSM are made to generate per session keys as required.

Verification of HSM's to PTS / FIPS validations and ensuring HSM are deployed as per the accompanying security policy and managed in a secure manner as per the cryptographic policies and procedures and verified to be validated under the PCD DSS program.

3.5. Conclusion

CypherPay™ provides a unique solution to merchants and services providers alike by implementing a secure mechanism for the transmission of transaction information over secured channels and further enhancing the security robustness of transactions by implementing a per session key methodology.

The solution makes use of industry best practices in cryptographic key management and strong secure algorithms to accomplish encryption processes that remove visibility of any cardholder data from the service provider and merchant environments, allowing for significantly simpler validation against industry recognised standards.

The solution also affords clients the opportunity of reducing risk within their environment of cardholder data compromise, as the client does not have access to the information, but rather relies on the validated services provided by Base Commerce.

For further information please reach out to Base Commerce for more information on implementation of the CypherPay™ solution.

https://www.basecommerce.com/cypherpay/

4. References

- **PCI Security Standards Council:** https://www.pcisecuritystandards.org/
- **Base Commerce:** https://www.basecommerce.com/
- **NIST Cryptographic Standards:** https://www.nist.gov/
- **SSL Labs:** https://www.ssllabs.com/

5. Appendices

5.1. Appendix A: PCI DSS V3.2.1 Control reduction mappings

Requirement	Control reduction description
1	Controls would be reduced moderately; related connectivity requirements would need to be addressed.
2	Controls significantly reduced / negligible, as these become a third-party requirement.
3	Controls significantly reduced / negligible, as these become a third-party requirement.
4	Controls significantly reduced / negligible, as these become a third-party requirement.
5	Controls significantly reduced / negligible, as these become a third-party requirement.
6	Controls significantly reduced / negligible, as these become a third-party requirement.
7	Controls significantly reduced / negligible, as these become a third-party requirement.
8	Controls significantly reduced / negligible, as these become a third-party requirement.
9	Controls would need to be met for physical security and access to sensitive systems.
10	Controls significantly reduced / negligible, as these become a third-party requirement.
11	Controls significantly reduced / negligible, as these become a third-party requirement.
12	Controls would need to be met for policy and process and third-party management.

5.2. Appendix B: Tools Used

Tool	Description
Kali OS https://www.kali.org/	Is a penetration testing operating system as provided by Offensive Security.
Nessus http://www.tenable.com/	Nessus is a commercial vulnerability scanner.
Burp Suite http://portswigger.net/burp/	Burp Suite is an integrated platform for attacking web applications.
Wireshark https://www.wireshark.org/	The Wireshark application is a packet capture tool to analyze data in traversal over various mediums.
Metasploit http://www.metasploit.com/	An exploitation framework with auxiliary modules used also for manual testing.
TCPDump https://www.tcpdump.org/	A packet capture utility for linux based systems.
FTK Toolkit https://accessdata.com/products-services/forensic-toolkit-ftk	A forensic framework to provide deep data analysis.
SSL Labs https://www.ssllabs.com/	A toolset to verify the certificates used by public facing services.

sysnet® | Cyber Risk

base

Require Cyber Security and Compliance Solutions?

If you would like to find out more about our **Cyber Security and Compliance Solutions**; then please send an email to cyber-risk@sysnetgs.com and a member of staff will contact you.

About Sysnet

Established in 1989, **Sysnet Global Solutions** provides payment card industry, cyber security and compliance solutions that help businesses to improve security and acquiring organizations to reduce risk.

Specializing in data security and PCI DSS compliance validation solutions, Sysnet offers a range of services, including its award-winning, proprietary, cyber security and compliance management solution **Sysnet.air®**, to a wide variety of businesses including acquirers, ISOs, international banks, payment service providers and merchants.

Headquartered in Dublin, Ireland, Sysnet has **clients in more than 60 countries worldwide**.

Call us now

Ireland +353 (0)1 495 1300
UK +44 (0) 207 868 1630
India +91 (0)4 06 713 5336
USA +1 404 991 3110
Poland +48 61 631 1230
South Africa +27 (0) 83 629 7514

sysnetgs.com
cyber-risk@sysnetgs.com

Let's stay connected