Case Study NAME:
Symantec Trust Network (STN)
Certification Practice Statement (CPS) Analysis

AUTHORS:
Symantec Corporation

STUDENT NAME:
Maxwell Farnga

DATE:
October 27, 2017

COURSE INFO:
AIT 612_101
Fall 2017

COURSE TITLE:
Information Systems Security
Vulnerability and Risk Assessment

ASSIGNMENT:
Case Study assessment

NAME OF INSTRUCTOR:
Prof. Arthur R. Friedman

Contents

Certification Practice Statement (CPS) Analysis

Assignment Requirements:

You are the security manager for a mid-sized company (3,000 to 5,000 employees). Your company has determined that confidentiality (or privacy) and data integrity are the security services you must provide to your work force. 10% of the work force handles company sensitive information, which requires additional security protection. The remainder of the work force must also protect their data, but not to the same level of protection or assurance.

Your assignment is to review the Verisign CPS and recommend the type of certificate(s) (e.g., Class 1) needed for your workforce. Provide a rationale with your recommendation. As the security manager, you also need to ensure cost is kept to a minimum. Even though the CPS does not include cost information, you can find cost data on the Internet. Additionally, you need to identify the security challenges of implementing a Verisign-based solution, as well as the security features provided by this solution.

You also need to identify the security features described in the CPS that support the security requirements for this company.

Hint: Use the Verisign CPS on Bb and select the technical capabilities and security services desired for a specific environment (e.g., financial institution, health care, etc.). Also identify the planning considerations using the CPS and your class notes. You do not need to include detailed cost information, estimates.

Note: Symantec purchased Verisign. Check their website for cost information.

Each student will submit their own response.

The assignment is due on Oct. 27, 2016 at 11:59 pm.

Case Study Summary

EMMAX Health Systems is one of the leading provider of urgent care services in the United States and we have 80 locations, including our corporation headquarters in Towson, Maryland. We have 4000 employees who work in these locations, and 400 or 10% of these employees handle more sensitive data than others, therefore they will need more security than the other 90%.
To accomplish our organization's goal of ensuring the confidentiality and Integrity of all our users and data, we have decided to evaluate some vendors who can provide the appropriate Cryptography services.

Objectives

In this paper we will do an analysis of the Symantec Trust Network (STN) Certification Practices Statement, and our goal is to solve the following concerns in the EMMAX Health Care System.

- Confidentiality
    - That our data, services, employees, and patients provide no useful information to any unauthorized entities or individuals
    - Because our data is HIPAA (Health Insurance Portability and Accountability Act) and ePHI (Electronic Protected Health Information) compliant, unauthorized disclosure is our top priority
- Integrity
    - That no unauthorized entities or individual have the means to temper with our organization's data assets which includes (PII, ePHI, Medical, HIPAA, Employees) and other important information required for our operations.
- Authenticity
    - That we will have the potential to verify that all assets are attributable to their authors and custodians both externally and internally
- Non-repudiation
    - That all content creators, custodians, owners, and contributors cannot deny that they are associated with their contents.

Certification Practice Statement overview

As the security manager of EMMAX Health Systems, below are my analysis from reviewing the latest Certification Practices Statement (CPS) of Symantec Trust Network (STN) formerly Verisign Trust Network:
This Symantec Trust Network (STN) Certification Practice Statement ("CPS") document states the practice of the Symantec Certification Authority ("Cas"), which provides certification services that include, issuing, managing, revoking, and renewing certificates in accordance with requirements from the Symantec Certificate Policies ("CP").

According to Symantec, "The CP is the principal statement of policy governing the STN. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the STN and providing associated trust services."

In addition to the CP, this CPS also confirms to Internet Engineering Task Force (IETF) RFC 3647 and the Symantec Cas also conforms to the current version of the CA/Browser Forum (CABF) requirements.

These requirements include:

- The secure management of Symantec core infrastructure
- How they issue, manage, revoke, and renew the STN Certificates
- Rules for issuing and managing Extended Validation (EV) Certificates
- Rules for issuing and managing Extended Validation (EV) Code-Signing certificates
- Basic requirement for issuing and managing Publicly-Trusted Certificates
- Most importantly, Symantec Certification Practice is audited annually, by KPMG

Certification Services:

Symantec currently offers three classes of certificates to its sub-domains and all certificate classes are managed by this CPS. These classes of certificates are issued to subscribers or End-users which may include: individuals, organizations, or infrastructure components like firewalls, routers, trusted servers, applications, and other devices used to secure the communications within an Organization.

In this analysis, we will focus on the certification process for organizations, such as EMMAX Health care systems.

Organizational certificate issuance:

According to Symantec, "Organizational Certificates are issued to organizations after authentication that the Organization legally exists and that other Organization attributes included in the certificate (excluding nonverified subscriber information) are authenticated e.g. ownership of an Internet or e-mail domain."

The assurance levels of certification:

Class one - Low assurance certificates:

- These certificates cannot be used for authentication or non-repudiation purposes. Their digital signature provides modest assurances that emails originated from a sender with certain email addresses. This class of certificate provides no proof of subscriber's identity.

Class two – Medium assurance certification:

- These certificates suitable for securing some inter and intra-organizational, commercial, and personal emails that require medium level of assurances of authenticity and non-repudiation of the subscriber. Symantec verifies the subscribers' identity but not the organization's authentication for the individual applicant.

Class three – High assurance certificates:

- These certificates provide high level of assurance of the identity of the Subscriber compared to Class 1 and 2

Class three – High assurance certificates with extended validation certificates:

- Class 3 certificates issued in conformance with the rules for Extended Validation Certificates

Certification repositories:

Symantec manages the certificate repositories and functions of its own Cas and the Cas of its Enterprise customers (Managed PKI customers). The publish the certificates issued to end-user subscribers in a repository in accordance with the CPS. Upon revocations, they also publish the revocation status in the repository called the CRLs (Certification Revocation List).

Symantec also maintains a web-based repository that permits relying parties to make online inquiries regarding revocation and other statuses called the Online Certification Status Protocol (OCSP).

Certificate information published in the web-based repository is publicly accessible in read only mode. Individual must agree to "Relying Party Agreement or CRL Usage Agreement as a condition to accessing Certificates, Certificate status information, or CRLs."

Trusted identity validation:

Symantec ensures that EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conforms to the CABF requirements. Class 2 and 3 end-user Subscriber Certificates contain names with commonly understood semantics to verify the individuals and organizations that owns the certificates.

Prove Possession of Private Key:

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to

the public key to be listed in the Certificate. According to Symantec, "the method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another Symantec approved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pre-generated keys are placed on smart cards."

Authentication of Organization identity:

Whenever a certificate contains an organization name, the identity of the organization and other enrollment information provided by Certificate Applicants is confirmed with the procedures set forth in Symantec's documented validation.

The minimum requirements to validate an organization include the following:

- Determine that the organization exists by using other third-party identity proofing service, organizational documentation issued by or filed with the applicable government agency or competent authorities.
- Confirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so, when the certificate includes individual names.

Certificate Type Additional Procedures include the following:

- Extended Validation (EV) Certificates
- Organization Validated (OV) and Domain Validated (DV) Certificates

- OFX Server IDs
- Hardware Protected SSL Certificate and Hardware Protected EV Code-Signing Certificate
- Managed PKI for Intranet SSL Certificate
- Authenticated Content Signing (ACS) Certificate
- Class 3 organizational e-mail signing Certificates
- Mozilla Verification Requirements for Organization Applicants
- Domain Validation

Identification and Authentication for Re-key and revocation request:

In other to perform routine re-keying for an end-user subscriber, the person or organization must go through the use of a Challenge Phrase or show proof of possession of the private key.

To perform re-keying after revocation is not permitted, if the revocation was due to violation of the Symantec CPS policies. Otherwise, the individual or organization requesting the re-keying need to be the actual subscriber with the original certificates and/or a challenge phrase.

Symantec verifies all revocation requests to ensure that the person or organization is the subscriber that approved the certificate application. Once the challenge phrase is accepted, the revocation is automatically granted.

Certificate Life-Cycle Operational Requirements:

Below is an overview of the certification live cycle management

Certificate Application

Describes the process and procedure to obtain an encryption / PKI certification from Symantec. This process includes the following: (Eligible applicants, Enrollment Process and Responsibilities, End-User Certificate Subscribers, CABF Certificate Application Requirements, and CA and RA Certificates)

Certificate Application Processing

The process of verify that all applicants and subscribers meeting the requirement for certificate issuance. The processing stage includes the following steps: (Certificate Application Processing, Approval or Rejection of Certificate Applications, Time to Process Certificate Applications, and Certificate Authority Authorization (CAA))

Certificate Issuance

Following the approval of an application, a certificate is created and issued to the organization or individual who submitted the application. The steps include: (CA Actions during Certificate Issuance, Notifications to Subscriber by the CA of Issuance of Certificate, and CABF Requirement for Certificate Issuance by a Root CA)

Certificate Acceptance

In this stage, the organizations accept the certification and applicable agreements, then Symantec publishes the Certificates to necessary repositories. The steps include: (Conduct Constituting Certificate Acceptance, Publication of the Certificate by the CA, and Notification of Certificate Issuance by the CA to Other Entities)

Key Pair and Certificate Usage

Describes how to abide by the terms, agreements, and best practice of using the certificate to stay in compliance with the CPS. Which includes: (Subscriber Private Key and Certificate Usage, and Relying Party Public Key and Certificate Usage).

Certificate Renewal

Certificate renewal is the issuance of a new certificate to the subscriber without changing the public key or any other information in the certificate. The following eligibility must be met: (Circumstances for Certificate Renewal, Who May Request Renewal, Processing Certificate Renewal Requests, Notification of New Certificate Issuance to Subscriber, Conduct Constituting Acceptance of a Renewal Certificate, Publication of the Renewal Certificate by the CA, and Notification of Certificate Issuance by the CA to Other Entities)

Certificate Re-Key

Re-keying refers to the processing of obtaining a replacement certificate. The process includes: (Circumstances for Certificate Re-Key, Who May Request Certification of a New Public Key, and Processing Certificate Re-Keying Requests).

Certificate Modification

Certification modification has to do with the application for a replacement certificate due to changes in the existing certificate information. This includes: (Circumstances for Certificate Modification, Who May Request Certificate Modification, Processing Certificate Modification Requests, Notification of New Certificate Issuance to Subscriber, Conduct Constituting Acceptance of Modified Certificate, Publication of the Modified Certificate by the CA, and Notification of Certificate Issuance by the CA to Other Entities)

Certificate Revocation and Suspension

The terms, condition and procedure for certification and suspension of a certificate. Which includes: (CABF Requirements for Reasons for Revocation, Who Can Request Revocation, Procedure for Revocation Request, Revocation Request Grace Period, Time within Which CA Must Process the Revocation Request, Revocation Checking Requirements for Relying Parties, CRL Issuance Frequency, Maximum Latency for CRLs, On-Line Revocation/Status Checking Availability, On-Line Revocation Checking Requirements, Other Forms of Revocation Advertisements Available, Special Requirements regarding Key Compromise, Circumstances for Suspension, Who Can Request Suspension, Procedure for Suspension Request, and Limits on Suspension Period)

Certificate Status Services

The process of providing the status of every subscriber's and CA's certification to ensure authenticity and non-repudiation are minimized. Example: (Operational Characteristics, Service Availability, and Optional Features)

End of Subscription

This describes the process of ending subscriptions by either refusing the renew or manually relocating.

Key Escrow and Recovery

This option is available to Enterprise customer who deploy Managed PKI key management services, they can escrow they CAs, RAs, and Private Keys. It also includes details for Key Escrow and Recovery Policy and Practices.

To guarantee that our keys are safe, Symantec has deployed the following security control which meets both ISO, SOX and NIST and other compliance standards for information security.

These security controls include: Facility, Management, and Operational Controls, Technical Security Controls, and Compliance Audit and Other Assessments

Facility, Management, and Operational Controls

Physical Controls

Symantec has implemented the physical security policies and controls which supports the security requirements in the CPS: These physical controls include: (Site Location and Construction, Physical Access, Power and Air Conditioning, Water Exposures, Fire Prevention and Protection, Media Storage, Waste Disposal, and Off-Site Backup)

Procedural Controls

The procedural controls cover the standards for all trusted and prospective employees who have access to or control Symantec's authentication or cryptographic operations. Examples include: (Trusted Roles, Number of Persons Required per Task, Identification and Authentication for Each Role, and Roles Requiring Separation of Duties)

Personnel Controls

"Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts". This includes: (Qualifications, Experience, and Clearance Requirements, Retraining Frequency and Requirements, Job Rotation Frequency and Sequence, Sanctions for Unauthorized Actions, Independent Contractor Requirements, and Documentation Supplied to Personnel)

Audit Logging Procedures

Symantec manually or automatically logs the following significant events: Examples: (Types of Events Recorded, Frequency of Processing Log, Retention Period for Audit Log, Protection of Audit Log, Audit Log Backup Procedures, Audit Collection System (Internal vs. External), Notification to Event-Causing Subject, and Vulnerability Assessments)

Records Archival

Symantec archives all audit data, application, documentations, life cycle and other information. Example of their archive criteria includes: (Types of Records Archived, Retention Period for Archive, Protection of Archive, Archive Backup Procedures, Requirements for Time-Stamping of Records, Archive Collection System (Internal or External), and Procedures to Obtain and Verify Archive Information)

Compromise and Disaster Recovery

Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: (Incident and Compromise Handling Procedures, Computing Resources, Software, and/or Data Are Corrupted, Entity Private Key Compromise Procedures, and Business Continuity Capabilities after a Disaster)

CA or RA Termination

Symantec makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination.

Technical Security Controls

Key Pair Generation and Installation

"CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys"

Private Key Protection and Cryptographic Module Engineering Controls

"Symantec has implemented a combination of physical, logical, and procedural controls to ensure the security of Symantec and Enterprise Customer CA private keys."

Other Aspects of Key Pair Management

This key pair management includes: Public Key Archival, and Certificate Operational Periods and Key Pair Usage Periods

Activation Data

"Activation data (Secret Shares) used to protect tokens containing STN CA private keys is generated in accordance with the requirements of the and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged." Examples: (Activation Data Generation and Installation, and Activation Data Protection)

Computer Security Controls

"Symantec performs all CA and RA functions using Trustworthy Systems that meet the requirements of Symantec's SAR Guide. Enterprise Customers must use Trustworthy Systems." These computer security controls include: (System Development Controls, Security Management Controls, Life Cycle Security Controls, Network Security Controls, and Time-Stamping)

Cost analysis for Certifications:

Symantec uses industry-leading SSL encryption across all products, with various solutions for website and server security.

No.	***SSL Certifications***	***COST / Yr.***	***Assurance level***	***Description***
1.	Security Site Pro with EV	$1499	Class 3 – High Assurance	Extended Validation (EV) SSL certificates will increase customers' confidence
2.	Security Site with EV	$995	Class 2 – Medium Assurance	Extended Validation (EV) SSL certificates will increase customers' confidence, except there is no ECC support

3.	Security Site Pro	$995	Class 2 – Medium Assurance	This product offer ECC encryption: strong security on a short key length.
4.	SSL Wildcard	$1999	Class 1 – Low Assurance	Protects multiple subdomains under one SSL certificate.
5.	Secure Site	$399	Class 1 – Low Assurance	Protects single subdomains under one SSL certificate.

Recommendations:

Given our need to provide Confidentiality and Integrity for our 4000 users in all locations around the country, we are recommending the below as the next steps.

- Purchase a Class 3 – Security Site Pro with EV for our 400 users who handle more sensitive information
- Purchase a Class 2 – Security Site Pro for our 3600 users who handle less sensitive information throughout the organization
- Signup for Symantec Managed PKI services for enterprise customers
- Invite Symantec to provide further details and clarity about their services

In addition to the fact that Symantec complies with all major regulatory standards, they meet all EMMAX Health System data security needs as listed below:

- Certificate Policies
- Certification Services
- Organizational certificate issuance
- Certification repositories
- Trusted identity validation
- Prove Possession of Private Key
- Authentication of Organization identity
- Certificate Life-Cycle Operational Requirements and others

We also believe that outsourcing our Data Security and Certification needs to Symantec will be the best decision, because they have all the necessary Security Controls for a safe Information Systems environment and it will be a cost-effective decision as well.

No.	**Internal Implementation and operational cost**	**Cost of Symantec Managed PKI services**
1.	Less costly	Cost over 5 times more
2.	Certification are trusted world wide	Limited trust in the global community
3.	Rely on Symantec's expertise	Train and/or find employees with skills is difficult
4.	Easy to distribute Certifications	Need a secured central server
5.	No new hardware required	Need to acquire new hardware Infrastructure
6.	Easy to deploy and use	Required Software and Database Infrastructure
7.	No intensive training Required	Extensive training required

- Pfleeger

Conclusion:

Based on our detailed review and analysis of the Symantec Trust Network (STN) Certification Practices Statement, we have found Symantec to be credible and trustworthy to provide EMMAX Health System's data security needs. Symantec is currently in compliance with all the major regulatory organizations, they perform regular security assessments and submit to external audit on an annual basis.

WORK CITED:

Pfleeger, Charles P. Security in Computing. Upper Saddle River. Prentice Hall, 2015. Print

Symantec Corporation. " Certification Practice Statement". Symantec Trust Network. 08 Sept 2017. Print

Symantec Corporation. "Compare and Buy SSL Certificates". Symantec. Oct 2017. Web. 26 Oct 2017. https://www.symantec.com/en/in/page.jsp?id=compare-ssl-certificates#