Acme Corporation

Cryptography Assessment

TABLE OF CONTENTS

INTRODUCTION

The purpose of this assessment for Acme is to understand the laws, regulations, security controls gaps and policies that must be implement at Acme.

Acme executives want to understand the threat landscape what we are protecting our assets and our customers against.

From the legislation perspective there are two pieces of legislation that mandate the protection of sensitive data in the U.S. healthcare system are known as HIPAA (Health Insurance Portability and Accountability Act) and HITECH (Health Information Technology for Economic and Clinical Health Act).

In a bit more detail, HIPAA/HITECH is a U.S. law that applies to certain healthcare companies, including doctors' offices, hospitals, health insurance companies, and other companies involved in the healthcare industry that may have access to patient information (called Patient Healthcare Information or PHI). For a covered healthcare company to use a service provider like Microsoft or Amazon product and services, the service provider must agree to adhere to a minimum level of security and privacy and sign certain contractual provisions.

This document is segmented in the following areas:

- Executive Summary
- Logical Service Architecture
- Security Control Description
- Summary of Security Controls
- Final Considerations
- References

Needless to mention the importance of implementing the policies and security controls to our executives and provide a checklist that help Acme to move the needle from the security perspective taking Acme and our partners to the next level in terms of security while assuring compliance with ever changing laws and regulations.

1. EXECUTIVE SUMMARY

This assessment will help the executives of ACME organization to review all cryptography improvements for a large organization and its partners, which must comply technical requirements from Health Insurance Portability and Accountability Act (HIPAA).

Our mission is focused on key areas highlighted in the network diagram and employ the right encryption levels to ensure confidentiality, integrity and above all, address the required and go beyond the all controls shared in the HIPAA guidelines:

- Scalable security strategy and architecture.
- Reduce risk.
- Increase customer trust.
- Protect our data and from our customers.
- Stop bad actors.

This assignment will break the strategic goals in five major areas which are:

- Identify potential risks of violations to comply with the HIPAA and PCI DSS policy.
- Identify potential threats that could violate any cryptographic mechanisms.
- Proactively identify security controls to be implemented in the environment.
- Regulatory changes.
- Security education and awareness.

Proactively out of this assignment, we want to identify metrics that will help to keep track of the progress of company environment, customers, providers and remote workers. The executives and our overall security posture dashboard will track the following:

1. **100%** of communications with customers, providers, remote workers through secure channels.
2. **100%** of internal communications using highly secure channel leveraging technologies IPsec.
3. **100%** Critical Bugs being resolved vs assets.
4. **100%** Data encrypted.
5. **100%** Assets coverage by a TVM (Threat Vulnerability Solution).
6. **100%** Current of Assets with Security Updates.
7. **100%** Secure Development Lifecycle Assessment of Services.
8. **100%** Compliance of technical requirements with PCI-DSS and HIPAA.
9. **100%** of assets with secure monitoring.
10. **100%** of data at rest being heavily encrypted.

The scope of this assignment is limited to diagram in the logical service architecture.

2. THREAT LANDSPACE

What are we protecting our assets and customers against?

Fight against phishing

Phishing has continued to grow in scale and success. In 2016 more people clicked on phishing emails than ever before. 30% of Acme's phishing messages were opened by the target. An estimated 93% of all data breaches begin with a phishing campaign. Acme Corporation has been constant target for phishing. The goal is to gain an initial beachhead into the company and obtain a set of valid credentials. This threat vector will continue to be successful in more than 70% of the cases, so we need to make sure our environment is designed to prevent further lateral movement.

Decrease the vulnerability releases and backdoors

Over the past few years we've seen an increase in nation state created backdoors in major commercial products. These include both large companies such as Cisco and Juniper to smaller companies like Thales and UltraEdit. These issues pose a huge risk to Acme Corporation not just as a consumer of the technologies but as a potential next target for these attackers. Shadow Brokers is now offering a vulnerability as a service offering that dramatically increases our risk of zero-day attacks.

Continue rise of malware and ransomware

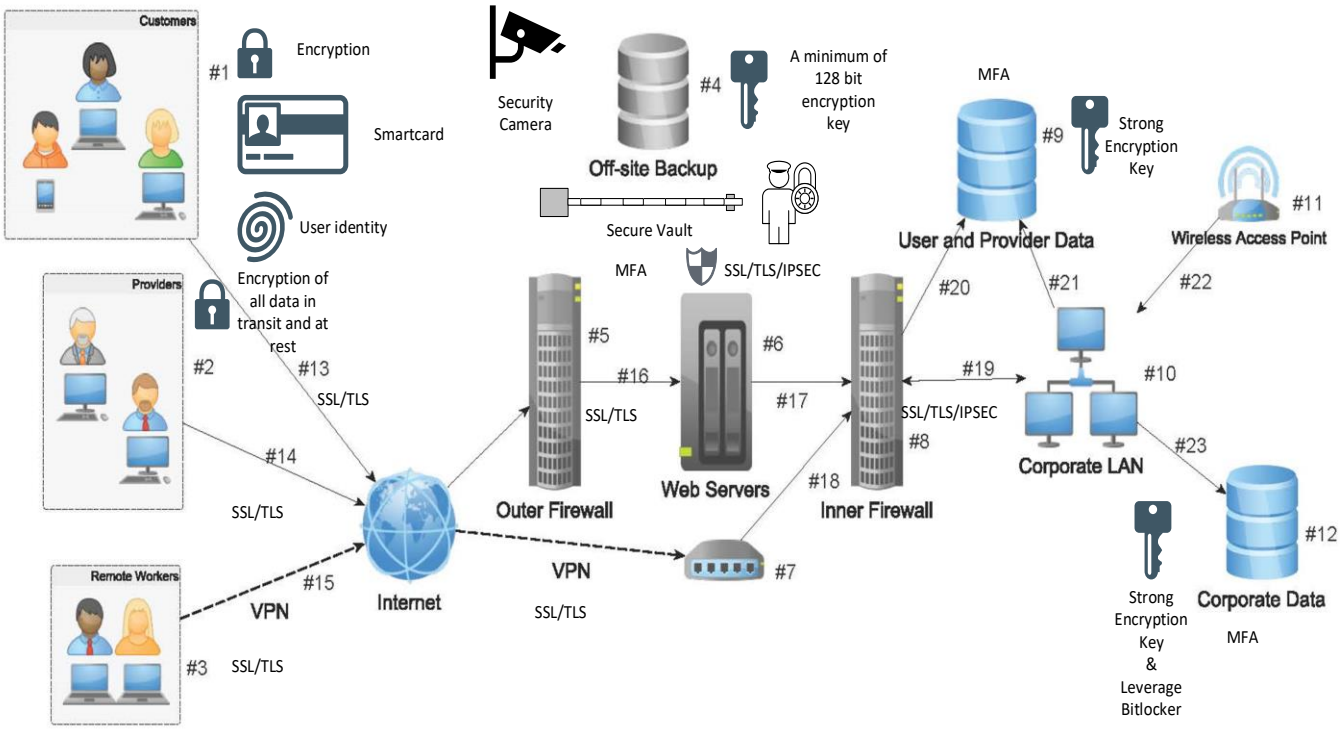
Malware has continued to evolve and this year we saw one of the largest destructive malware attacks in recent history. Ransomware grew 267% last year alone with over 400 active variants. We have seen outbreaks across industries. Memory resident malware is emerging as a significant threat, making detection difficult and mobile malware had an 83% increase in the second half of 2016.

Regulatory changes

This year will see several changes to the regulatory landscape. These include the enactment of the General Data Protection Regulation (GDPR) as well as the Peoples Republic of China Cybersecurity Law where Acme Corporation has been investing heavily in our manufacturing facility.

3. LOGICAL SERVICE ARCHITECTURE

The logical service architecture represents the architecture for the health insurance company mentioned in the assignment. Each component and interfaces are labeled with a corresponding number and have received the security controls. On the next section, every security control will have a detailed description that helps Acme to achieve a better security posture and consequently a better security relationship with remote workers, providers and ultimately protecting our most important asset, which is our customers and its data.



4. SECURITY CONTROLS DESCRIPTION

This section helps the executives of Acme to understand in detailed description the security that will be deployed across the corporate network, providers, remote workers and customers.

#1 Customers: In today's computing environment, there are many threats to the confidentiality of information stored on consumer devices. The primary security controls for restricting access to sensitive information stored on consumers devices are encryption and authentication. Our organization can recommend, educate the additional security controls, but cannot enforce these security controls, an education campaign will assist in the strengthen security posture of consumers. For consumers are complex passwords, personal identification numbers (PIN), cryptographic tokens, biometrics such as Windows Hello and smart cards. Another example rarely used for end-users(consumers) is the bitlocker available in the Windows, which can encrypt disk volumes as well. Devices leveraging Trusted Platform Module (TPM) where encryption keys can be stored. We must keep in mind; these end-users are not under the enforcement policy of our organization.

In summary the additional security controls would be recommended are:

- Windows Hello
- Windows Bitlocker
- Smartcards
- Endpoint Protection and response software
- Anti-virus

From the key distribution protocols standpoint, our primary reason for issuing smart cards is to increase the security of the remote access service. Additionally, the cards provide a platform increased mobility of certificates utilized by other applications. For scenarios where is not cost effect to issue smart cards, the focus will on the personal certificates leveraging a future implementation of PKI infrastructure. The PKI trust space is a collection of root and subordinate certificate authorities pushed down to all corporate clients.

Advantages: The use of smart cards for authentication is much more secure than the current model of usernames and passwords, which are subject to a variety of attacks.

Disadvantages: The current market for management systems to issue and track the smart cards is limited and the solutions are normally very expensive.

The main protocol leveraged will be **TLS** (Transport Layer Security) with **RSA** as a key exchange algorithm and the block cipher will be **3DES-EDE-CBC**.

It is important to highlight the RSA algorithm involves four steps: key generation, key distribution, encryption and decryption. In this case, due the scope of this assignment the focus will in the key distribution.

#2 Providers: For a provider, the recommended additional security control would be:

- Windows Hello
- Windows Bitlocker
- Smartcards
- Endpoint Protection and response software
- Anti-virus
- Secure communication channel using SSL/TLS

The main protocol leveraged will be **TLS** (Transport Layer Security) with **RSA** as a key exchange algorithm and the block cipher will be **3DES-EDE-CBC**. As mentioned in the previous section, in this section, we can also leverage smartcards using the same design and infrastructure.

#3 Remote Workers: Secure Sockets Layer (SSL) and virtual private networks (VPN) provide secure remote access to an organization's resources. A VPN is a virtual network, built on top of existing physical networks, that can provide a secure communications mechanism for data and other information transmitted between two endpoints. Because a VPN can be used over existing networks such as the Internet, it can facilitate the secure transfer of sensitive data across public networks. An SSL VPN consists of one or more VPN devices to which users connect using their Web browsers. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor, the Transport Layer Security (TLS) protocol. This type of VPN may be referred to as either an SSL VPN or a TLS VPN. ***(NIST, 2008)***

To enforce additional security controls for remote workers, the following additional controls must be leveraged:

- Windows Hello
- Windows Bitlocker
- Smartcards
- Endpoint Protection and response software
- Anti-virus
- Secure communication channel using SSL/TLS
- Privileged Access Workstation
- Identity Isolation

At this point, we will be locking down the traffic with our remote site and using IPsec protocol with **Diffie-Hellman 256-bit Elliptical Curve** or **384-bit Elliptical Curve**. These represents group **19** and group **20,** respectively. What is IPSec anyway? A security protocol in the IP layer that provides cryptographic security services and combinations of authentication, integrity, access control, and confidentiality.
Additionally, IPSec is used to connect the remote sites and drive all internal communications within our security architecture diagram, and we are leveraging Cisco routers, as an assumption for this assignment/project. While certificates are not currently utilized here, the necessary components are in place to issue off-line router certificates capable of IPSec.

Advantages: As an internet standard, IPSec should theoretically provide the most flexibility for systems interaction. IPSec can utilize both Kerberos and X.509 certificates in its implementation. Kerberos will be discussed in the future assignments.
Disadvantages: Lack of configuration flexibility and ability to effectively segment enterprise-scale networks.

#4 Off-Site Backup: Ensure that off-site backup is encrypted using a **strong key** a minimum of **256-bit encryption** and notification for:

- When a file is accessed
- When a file, system or device is backed up
- When a file is modified
- When a physical server is accessed and unusual network activity

Additional security controls feature to increase security posture are:

- Automated, unattended data backups with built-in notifications;
- Data security via 256-bit encryption – data is always compressed and encrypted; during transmission and storage;
- Data integrity controls with mutual authentication via just-in-time access;
- Restricted password access using password vaults;
- Off-site storage at highly secured data centers;
- Data is mirrored to secondary secure facilities for ultimate data availability;
- Data mirroring leveraging cloud storage;
- On-demand, exact copy data retrieval;
- DVD archives;
- Physical security controls such as cameras.

From the key distribution protocol perspective, we want to keep this offsite disconnected from our future PKI infrastructure, therefore keep a strong offline key to encrypt the data off-site.

#5 Outer Firewall: Essentially, you need to have firewalls fully implemented on your site. There are three basic types of firewalls: hardware firewalls, software firewalls, and web application firewalls (WAFs). Additional security controls feature to increase the security posture in the firewall are:

- Application Control;
- Intrusion and threat prevention;
- Internet Access and filtering;
- Identity and computer awareness;
- Data loss prevention.

We will be locking down the traffic with our remote site and using IPsec protocol with **Diffie-Hellman 256-bit Elliptical Curve** or **384-bit Elliptical Curve**. These represents **group 19** and **group 20**, respectively.

#6 Web Servers: The additional security controls feature to increase security posture are:

- Transport Encryption: Is always encrypted as it is transmitted over the Internet;
- Backup: Is never lost, i.e. should be backed up and can be recovered;
- Authorization: Is only accessible by authorized personnel using unique, audited access controls;
- Multi-Factor Authentication;
- Implementation Windows Defender Advanced Threat Protection in all servers;
- Storage Encryption: Should be encrypted when it is being stored or archived.

For web-servers, the main protocol leveraged will be **TLS (Transport Layer Security)** with **RSA** as a key exchange algorithm and the block cipher will be **3DES-EDE-CBC** and using S**HA** as message authentication algorithm.

#7 VPN: VPN devices that are to be used in FIPS-compliant applications must also use FIPS-compliant hash functions. Plain SHA-1 can only be used until the end of 2010 in FIPS-compliant systems13. The keyed hash message authentication code **(HMAC)** form of SHA-2. Since SSL VPN devices use **HMAC-SHA-2**. There are a couple of standards encryption protocols for VPNs other than SSL, IPSEC and GRE. For the IPSec communications will be using **AES 256 (256-bit AES-CBC) using HMAC** to ensure integrity.

For the VPN devices, will be locking down the traffic with our remote sites and using IPsec protocol with **Diffie-Hellman 256-bit Elliptical Curve** or **384-bit Elliptical Curve**. These represents **group 19** and **group 20**, respectively.

#8 Inner Firewall: Essentially inner firewall will require the same security controls described in the outer firewall section.

For inner firewall, the same rule will apply and we will be locking down the traffic with our remote sites and using IPsec protocol with **Diffie-Hellman 256-bit Elliptical Curve** or **384-bit Elliptical Curve**. These represents **group 19** and **group 20**, respectively.

#9 User and Provider Data: For user and provider will ensure the communications are encrypted using a strong key a minimum of **AES 256 (256-bit AES-CBC)** and **TLS** with **HMAC** built-in as mechanism to ensure integrity.

From the user and provider data perspective, IPSec will be used with **Diffie-Hellman Group (14)** for all internal communications **Encryption**: **AES-CBC-256 Integrity**: SHA-384.

#10 Corporate LAN: The corporate LAN must be using the following additional security controls:

- Use Windows Bitlocker in all servers and end-user computers;
- Use Smartcards to segregate identity to access high value assets;
- Install Endpoint Protection and response software;
- Install Anti-virus;
- Setup IPSec communications across all computers and devices;
- Leverage Privileged Access Workstation

- Leverage Identity Isolation
- Leverage Multi-Factor Authentication;
- Implementation of Windows Defender Advanced Threat Protection in all servers;
- Implementation of Advanced Threat Analytics to prevent lateral movement and escalation of privileges and protect identity

In the section, it is the core of what we are trying to protect, therefore all the communications will be using IPSec using with **Diffie-Hellman Group (14)** for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384.

#11 Wireless Access Point: The following additional security controls will be used on the Wireless Access Point across the organization:

- Leverage Intrusion Detection System (IDS);
- Disable unnecessary Wireless Access Point;
- Leverage Advanced Encryption Standard (AES) to encrypt wireless data;
- Use wireless authentication protocols that require mutual or multi-factor authentication;
- Conduct penetration access exercises from the parking lot.

Wireless Access Point will be leveraging IPsec using Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384. These secure tunnels will be allowing a more secure wireless connection into our core LAN infrastructure.

#12 Corporate Data: The same rule will apply: For internal communications, all devices will be communicating over IPSec using IPsec Rules and be using **AES 256 (256-bit AES-CBC).** In this aspect to keep the integrity, the policy will enforce and implement **TLS** which use **HMAC** algorithm using **SHA-256.** Corporate data will be using Multi Factor Authentication and password keys vault to generate random complex passwords.

All Corporate Data communication will be using IPsec using Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384. These secure tunnels will be allowing a more secure wireless connection into our core LAN infrastructure.

Amongst the interfaces will be using the secure channel communications decided in the previous assignments. All key distribution protocols will be summarized in a table by the end of this section.

#13 Customers to Outer Firewall: Generally, using **PGP**, **SSL**, or **AES** encryption of stored data can accomplish this very nicely and address the integrity part. For the certificates will be leveraging TLS certificates using RSA as key exchange/agreement. Block ciphers AES and the messaging **SHA256** hash function. In this aspect to keep the integrity, the policy will enforce and implement **TLS** which use **HMAC** algorithm using **SHA-256.** The key exchange algorithm will be **RSA**.

#14 Providers to Outer Firewall: Generally, using **PGP**, **SSL**, or **AES** encryption of stored data can accomplish this very nicely and address the integrity part. For the certificates will be leveraging TLS certificates using RSA as key exchange/agreement. Block ciphers AES and the

messaging SHA256 hash function. In this aspect to keep the integrity, the policy will enforce and implement **TLS** which use **HMAC** algorithm using **SHA-256.** The key exchange algorithm will be **RSA**.

#15 Remote Workers to VPN: Ensure the remote worker use **TLS** certificates using **RSA** as key exchange/agreement. Block ciphers AES and the messaging **SHA256** hash function. In this aspect to keep the integrity, the policy will enforce and implement **TLS** which use **HMAC** algorithm using **SHA-256.**

#16 Outer Firewall to Web Servers: For internal communications, all devices will be communicating over IPSec using IPsec Rules and be using **AES 256 (256-bit AES-CBC)**. In this aspect to keep the integrity, the policy will enforce and implement **TLS** which use **HMAC** algorithm using **SHA-256.**

#17 Web Servers to Inner Firewall: For internal communications, all devices will be communicating over IPSec using IPsec Rules and be using **AES 256 (256-bit AES-CBC)**. In this aspect to keep the integrity, the policy will enforce and implement **TLS** which use **HMAC** algorithm using **SHA-256.**

#18 VPN to Inner Firewall: For internal communications, all devices will be communicating over IPSec using IPsec Rules and be using **AES 256 (256-bit AES-CBC).** In this aspect to keep the integrity, the policy will enforce and implement **TLS** which use **HMAC** algorithm using **SHA-256.**

#19 Inner Firewall to Corporate LAN: For internal communications, all devices will be communicating over IPSec using IPsec Rules and be using **AES 256 (256-bit AES-CBC).** In this aspect to keep the integrity, the policy will enforce and implement **TLS** which use **HMAC** algorithm using **SHA-256.**

#20 Inner Firewall to User and Provider Data: For internal communications, all devices will be communicating over IPSec using IPsec Rules and be using AES 256 (256-bit AES-CBC). In this aspect to keep the integrity, the policy will enforce and implement **TLS** which use **HMAC** algorithm using **SHA-256.**

#21 Corporate LAN to User and Provider Data: For internal communications, all devices will be communicating over IPSec using IPsec Rules and be using AES 256 (256-bit AES-CBC). In this aspect to keep the integrity, the policy will enforce and implement **TLS** which use **HMAC** algorithm using **SHA-256.**

#22 Wireless Access Point to Corporate LAN: The same security controls described in the section Wireless Access Point.

#23 Corporate LAN to Corporate Data: For internal communications, all devices will be communicating over IPSec using IPsec Rules and be using AES 256 (256-bit AES-CBC). In this aspect to keep the integrity, the policy will enforce and implement **TLS** which use **HMAC** algorithm using **SHA-256.**

Additionally, two core security controls will help to strengthen the overall security of service and comply with HIPAA requirements. The first core will be Active Directory issuing the Kerberos tickets and the second will a Public Key Infrastructure (PKI).

From the Active Directory perspective, attackers also use the credentials to create ways to remain persistence and dormmate for months sometimes even years.

It is no small undertaking to rebuild and attempt to secure an entire existing Active Directory forest. You must defend every facet of your infrastructure; an attacker only needs to find enough flaws in your defenses to get to their desired goal.

For these reasons, it is recommended a more focused, targeted approach to secure the Active Directory forest. It is not anticipated any changes in the previous security controls mentioned to incorporate the Kerberos server (Active Directory).

It is important to highlight to the leadership the attack possibility that will contained by the previous security controls discussed later in the document, some of these attacks are:

- Kerberos Golden Ticket
- Pass the ticket attack
- Malicious replication of Directory Services

For more attack and its references are mentioned in the reference section under the following document Advanced Threat Analytics Suspicious Activity guide.

Based on the overall project goals, these will be parameters to be set from the PKI perspective:

- The PKI must be constructed around a minimum three tier hierarchy: Root; Policy; and Issuing certificate authorities.
- To provide the maximum security and integrity to the PKI, the Root certificate authority should be utilized as little as possible. The policy sub-tier of the hierarchy should be utilized to enforce policy on the issuing certificate authorities, be it internal vs. external, legal/contractual, or government mandated policy.
- Only issuing certificate authorities signed by policy certificate authorities should interact directly with end users.
- The PKI should utilize a self-signed root for issuance of certificates that are utilized only internal to Acme.
- Due to the large amount of certificates issued to internal Acme groups for testing, services and development, in addition to the overall trust placed in the PKI, internally verified user authentications and digital signatures should be issued from certificate authorities chaining to an internal self-signed root certificate authority.
- The PKI may utilize an external (3rd party) root certificate authority to sign portions of the PKI hierarchy where use of end-entity certificates signed by a commercial certificate authority.
- Provided acceptable contractual obligations can be met, the use of a third party to sign a policy or issuing certificate authority is acceptable. The potential cost benefit for self-

issuing 3rd party SSL certificates or the client compatibility achieved with 3rd party S/MIME certificates outweigh the potential complexity added to the PKI.

- A minimum of two enterprise certificate servers must be built for each enterprise certificate authority logical service.
- To provide maximum uptime for users in addition to permit necessary maintenance windows, two certificate servers should be built for each identified instance of a required enterprise certificate authority.
- The protection scheme utilized to secure and access the private keys of the Root and Policy certificate authorities must require a representative from both legal team and Acme IT be present.
- This principle is designed to ensure the legitimacy of all certificate authorities introduced in the PKI hierarchy
- All certificate authorities in the PKI must be in an Acme approved vault
- The Root CA will be offline and in a protected vault. It will be on, only during the cycle of checking CRLs
- The vault security needs to be protected against electromagnetism attacks, air gapped and prevent malware that could bridge the air gap (Guri, Mordechai, 2018 – Black Hat)
- Due to security considerations and concerns, a more descriptive definition of a vault will not be provided here. Legal Team, Facilities and Acme IT have an approved vault design and all certificate authorities must be in one of these facilities.
- All activity in the vault housing certificate servers must be logged.
- A minimum of two people must sign all log entries for work done in the vault. As a best practice, all parties present during vault operations should sign vault entries.
- Systems comprising a Root or Policy certificate authority must not be allowed to connect to a data network.
- All work done in the process of performing a signing operation from a root or policy certificate authority must be done at the system console to provide the maximum protection for certificate authority integrity.
- Key Lengths:
- The need to balance functionality with security requires that key lengths be long enough to be assumed secure over their lifespan, but not so long as to impede functionality by slowing cryptographic functions unnecessarily. The following key length principles assume end-entity certificates are valid for one year or less, issuing certificate authorities are valid for 2 years or less, and root and policy certificate authorities are valid for 16 years or less.
- The minimum key length for any end-entity certificate issued from the Acme hierarchy will be 2048 bits.
- The minimum key length for two-year certificate authority certificate issued from the acme hierarchy will be 2048 bits.
- The minimum key length for 16-year (or less) certificate authority certificate issued from the Microsoft corporate hierarchy must be 4096 bits.
- Distribute certificates for VPN services, webservers, end-users, smart cards and IPSec certificates

5. SUMMARY OF SECURITY CONTROLS

The table summarizes the additional security controls per area of the architecture diagram and the key distribution mechanisms per area.

What we are protecting	Policy Security Controls	Key Distribution and Protocols
#1 Customers	• Encryption • Smartcard • User Identity Protection	**TLS:** Protocol **RSA:** Key Exchange Algorithm **3DES_EDE_CBC:** block cipher **SHA:** message authentication algorithm
#2 Providers	• Windows Hello • Windows Bitlocker • Smartcards • Endpoint Protection and response software • Anti-virus • Secure communication channel using SSL/TLS	**TLS:** Protocol **RSA:** Key Exchange Algorithm **3DES_EDE_CBC:** block cipher **SHA:** message authentication algorithm
#3 Remote Workers	• Windows Hello • Windows Bitlocker • Smartcards • Endpoint Protection and response software • Anti-virus • Secure communication	**IPsec:** Diffie-Hellman **256-bit** Elliptical Curve or **384-bit Elliptical Curve**. These represents **group 19** and **group 20** respectively

	channel using SSL/TLS • Privileged Access Workstation • Identity Isolation	
#4 Off-site	• Strong Key with 256-bit encryption	Does not apply
#5 Outer Firewall	• Application Control • Intrusion and threat prevention • Internet Access and filtering • Identity and computer awareness • Data loss prevention.	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384
#6 Web Servers	• Transport Encryption: Is always encrypted as it is transmitted over the Internet; • Backup: Is never lost, i.e. should be backed up and can be recovered • Authorization: Is only accessible by authorized personnel using	**TLS:** Protocol **RSA:** Key Exchange Algorithm **3DES_EDE_CBC:** block cipher **SHA:** message authentication algorithm

	unique, audited access controls • Multi-Factor Authentication • Implementation Windows Defender Advanced Threat Protection in all servers • Storage Encryption: Should be encrypted when it is being stored or archived.	
#7 VPN	Does not apply	**IPsec**: Diffie-Hellman **256-bit** Elliptical Curve or **384-bit Elliptical Curve**. These represents **group 19** and **group 20** respectively
#8 Inner Firewall	Does not apply	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384
#9 User and Provider Data	Does not apply	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384
#10 Corporate LAN	• Use Windows Hello on the end-user machines	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**:

	• Use Windows Bitlocker in all servers and end-user computers • Use Smartcards to segregate identity to access high value assets • Install Endpoint Protection and response software • PKI • Domain Controllers (Kerberos Authentation) • Install Anti-virus • Setup IPSec communications across all computers and devices • Leverage Privileged Access Workstation • Leverage Identity Isolation • Leverage Multi-Factor Authentication • Implementation of Windows Defender Advanced Threat Protection in all servers • Implementation of Advanced Threat Analytics to prevent	AES-CBC-256 **Integrity**: SHA-384

	lateral movement and escalation of privileges and protect identity	
#11 Wireless Access Point	• Leverage Intrusion Detection System (IDS) • Disable unnecessary Wireless Access Point • Leverage Advanced Encryption Standard (AES) to encrypt wireless data • Use wireless authentication protocols that require mutual or multi-factor authentication • Conduct penetration access exercises from the parking lot	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384
#12 Corporate Data	• Encryption with IPSec	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384
#13	Does not apply	**TLS:** Protocol **RSA:** Key Exchange Algorithm

		3DES_EDE_CBC: block cipher **SHA:** message authentication algorithm
#14	Does not apply	**TLS:** Protocol **RSA:** Key Exchange Algorithm **3DES_EDE_CBC:** block cipher **SHA:** message authentication algorithm
#15	Does not apply	IPsec: Diffie-Hellman 256-bit Elliptical Curve or 384-bit Elliptical Curve. These represents group 19 and group 20 respectively
#16	Does not apply	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384
#17	Does not apply	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384
#18	Does not apply	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384

#19	Does not apply	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384
#20	Does not apply	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384
#21	Does not apply	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384
#22	Does not apply	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384
#23	Does not apply	**IPsec:** Diffie-Hellman Group (14) for all internal communications **Encryption**: AES-CBC-256 **Integrity**: SHA-384

6. FINAL CONSIDERATIONS

We are confident with the contrls

7. REFERENCES

HIPAA Journal. (2019, March 4). New HIPAA 2019 Regulations. Retrieved from:

https://www.hipaajournal.com/new-hipaa-regulations/

NIST Portal. (2008, July 8). Guidelines on Implementing an SSL/VPNs. Retrieved from:

https://csrc.nist.gov/publications/detail/itl-bulletin/2008/07/guidelines-on-implementing-a-secure-sockets-layer-ssl-virtual-/final

NIST Portal. (2007, November). Guide to Storage Encryption Technologies for End Users Devices. Retrieved from:

https://csrc.nist.gov/publications/detail/sp/800-111/final

NIST Portal. (2017, March 16). Microsoft Windows FIPS 140 Validation. Retrieved from:

https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3095.pdf

Microsoft Portal. (2019, April). Microsoft Trust Center. Retrieved from:

https://www.microsoft.com/en-us/TrustCenter/Compliance/HIPAA

Microsoft Portal. (2019, May 16). Understanding HIPAA Compliance with Azure. Retrieved from:

https://www.youtube.com/embed/6ptdye1LZ5k?autoplay=0

Microsoft Portal. (2017, February 2). Microsoft Azure HIPAA/HITECH Act Implementation Guide. Retrieved from:

https://gallery.technet.microsoft.com/Azure-HIPAAHITECH-Act-1d27efb0

Microsoft Portal. (2018, January 25th). Bitlocker. Retrieved from:

https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

Microsoft Portal. (2018, August 18th). Windows Hello biometrics in the enterprise. Retrieved from:

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise

Microsoft Portal. (2019, March 12th). Privileged Access Workstations. Retrieved from:

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations

Microsoft Portal. (2019, February 2nd). Active Directory administrative tier model. Retrieved from:

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Check Point Portal. (2018). Check Point Firewall Security Solution. Retrieved from:

https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/92746.htm

Microsoft Portal. (2019, March 4th). Windows Defender Advanced Threat Protection. Retrieved from:

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/windows-defender-advanced-threat-protection

Cisco Portal. (2002, Feb 22nd). IPsec Overview Part one: General IPsec Standards. Retrieved from:

http://www.ciscopress.com/articles/article.asp?p=25470

Microsoft Portal. (2019, Feb 24th). Configure a site-to-site VPN over ExpressRoute Microsoft peering. Retrieved from:

https://docs.microsoft.com/en-us/azure/expressroute/site-to-site-vpn-over-microsoft-peering

Microsoft Portal. (2017, May 30th). Active Directory Domain Services Overview. Retrieved from:

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Microsoft Portal. (2016, October 11th). Kerberos Authentication Overview

https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview

Microsoft Portal. (2019, April 2nd). Advanced Threat Analytics Suspicious Activity guide

https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide