

# Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

---



**John Elliott**

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire [www.withoutfire.com](http://www.withoutfire.com)



## Requirement 4

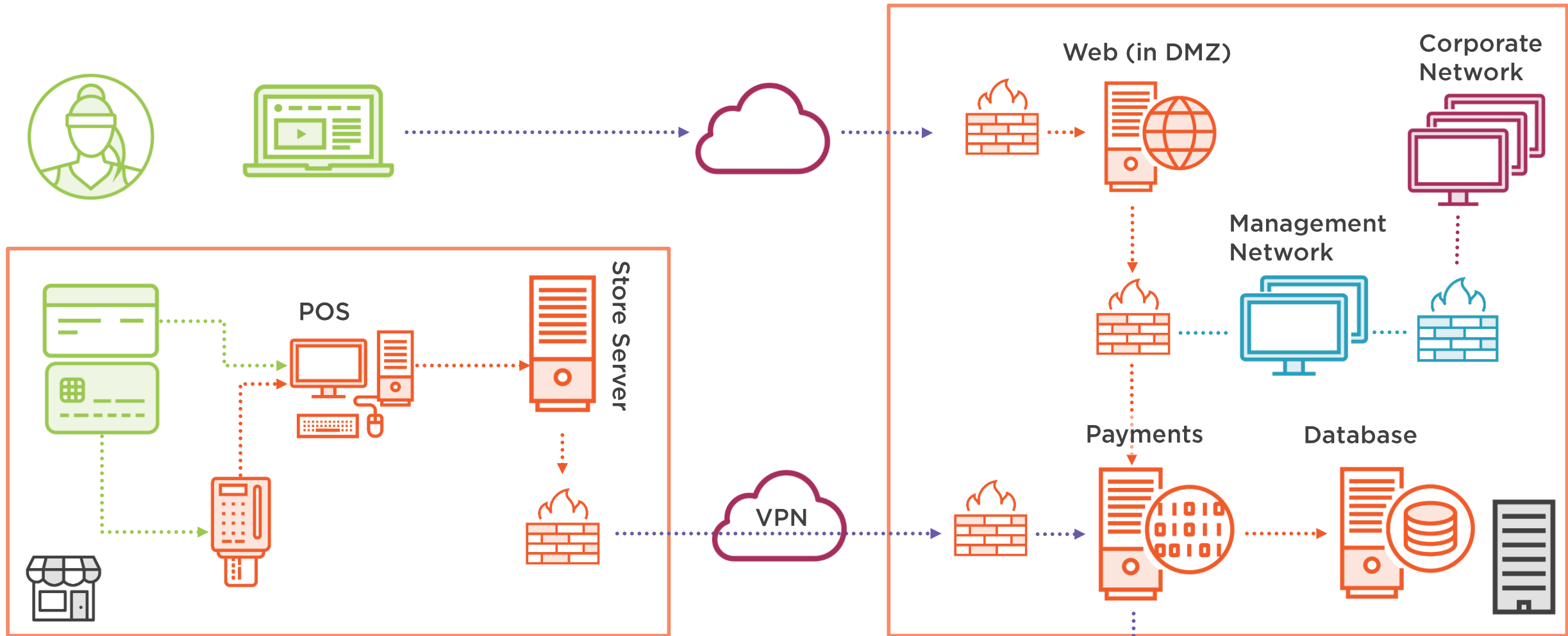


**Encrypt cardholder data**

**Secure PANs in messaging services**

**Have policies and procedures**

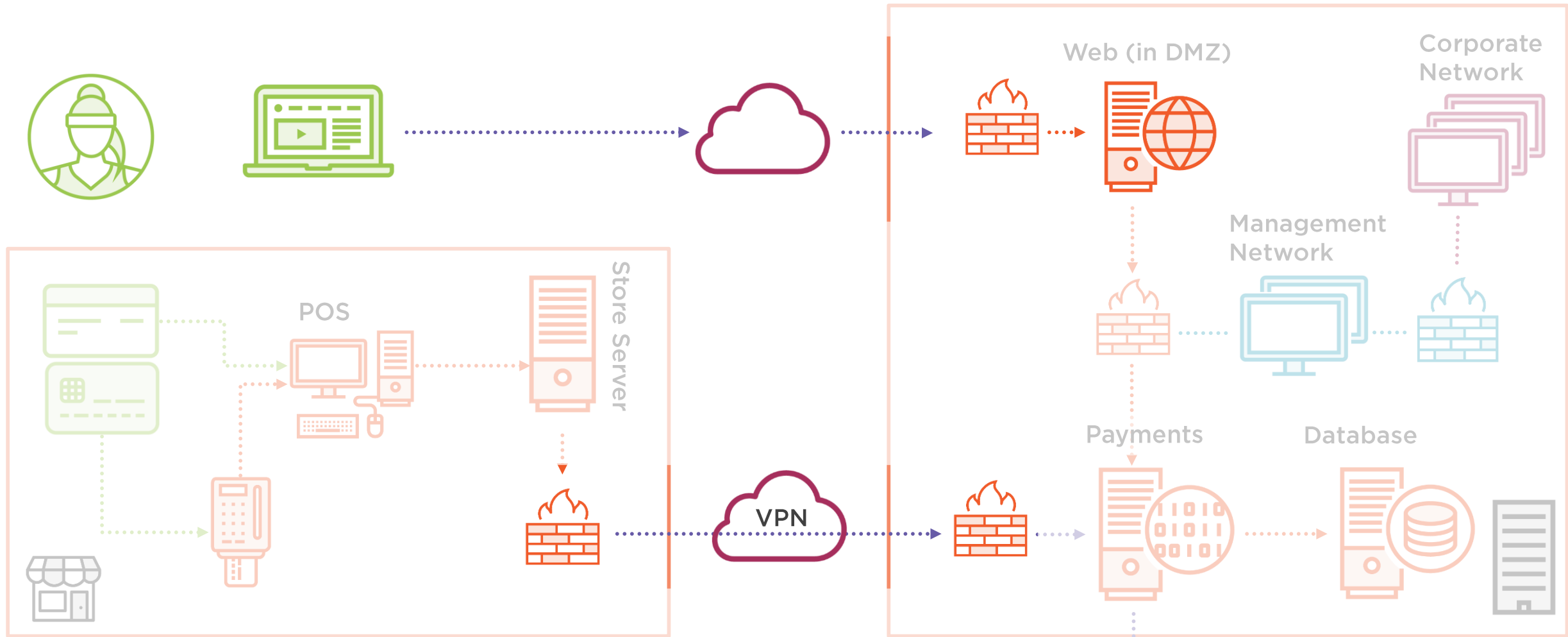




- Cardholder's card and systems
- Stores, processes or transmits
- Connected to or security affecting
- Out of scope of PCI DSS

- Unencrypted cardholder data
- Encrypted cardholder data
- Physical card read
- Management network
- Corporate network







# Requirement 4.1

Use strong cryptography



## Requirement 4.1

Use strong cryptography and security protocols to safeguard sensitive CHD during **transmission** over **open, public networks**, including the following:

- **Accept** only trusted keys and certificates
- Protocol in use only supports secure versions or configurations
- Appropriate encryption strength for the encryption methodology in use



## Requirement Guidance

- Secure transmission of CHD requires using trusted keys/certificates, a secure protocol for transport, and proper encryption strength to encrypt cardholder data. Connection requests from systems that do not support the required encryption strength, and that would result in an insecure connection, should not be accepted.
- Whichever security protocol is used, ensure it is configured to use only secure versions and configurations to prevent use of an insecure connection—for example, by using only trusted certificates and supporting only strong encryption (not supporting weaker, insecure protocols or methods).



# Open, Public Networks



**The internet**

**Anything wireless**

- WiFi
- Bluetooth
- Cellular – GSM, GPRS etc.

**Where there is shared access**

“Cryptography based on industry-tested and accepted algorithms, along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices”

## **Strong Cryptography**

[www.pcisecuritystandards.org/documents/PCI\\_DSS\\_Glossary\\_v3-2.pdf](http://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf)

*See: NIST Special Publication 800-57 Part 1*







## Requirement 4.1

Use strong cryptography and security protocols to safeguard sensitive CHD during **transmission** over **open, public networks**, including the following:

- **Accept** only trusted keys and certificates
- Protocol in use only supports **secure versions or configurations**
- Appropriate encryption strength for the encryption methodology in use



## Requirement Guidance

- Secure transmission of CHD requires using **trusted keys/certificates**, a **secure protocol** for transport, and **proper encryption strength** to encrypt cardholder data. **Connection requests** from systems that **do not support the required encryption strength**, and that would result in an insecure connection, **should not be accepted**.
- Whichever security protocol is used, ensure it is configured to use only secure versions and configurations to prevent use of an insecure connection—for example, by using only trusted certificates and supporting only strong encryption (not supporting weaker, insecure protocols or methods).



# What Is Safe?

SSL



TLS 1.0



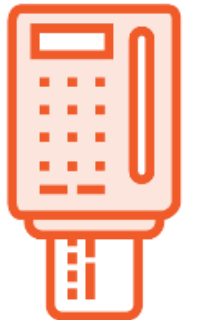
TLS 1.1



TLS 1.2



TLS 1.3



See Appendix 2



## 4.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Transmissions of CHD on open public networks, system configurations (TLS protocol suites) , keys and certificates</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Standards, policies and procedures</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 4.1.1

Strong encryption and protocols for all wireless networks



### Requirement 4.1.1

Ensure wireless networks **transmitting cardholder data** or **connected to the cardholder data environment**, use industry best practices to implement **strong encryption** for **authentication** and **transmission**.



### Requirement Guidance

- Malicious users use free and widely available tools to eavesdrop on wireless communications. Use of strong cryptography can help limit disclosure of sensitive information across wireless networks.
- Strong cryptography for authentication and transmission of cardholder data is required to prevent malicious users from gaining access to the wireless network or utilizing wireless networks to access other internal networks or data.



## 4.1.1 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Wireless networks, system configuration settings</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Standards</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 4.2

Encrypt PANs sent via  
e- mail, instant messaging, SMS, chat, etc.



## Requirement 4.2

Never send **unprotected PANs** by **end-user messaging technologies**.

(for example, e- mail, instant messaging, SMS, chat, etc.)



## Requirement Guidance

- E-mail, instant messaging, SMS, and chat can be easily intercepted by packet-sniffing during delivery across internal and public networks. Do not utilize these messaging tools to send PAN unless they are configured to provide **strong encryption**.
- Additionally, if an entity requests PAN via end-user messaging technologies, the entity should provide a tool or method to protect these PANs using strong cryptography or render PANs unreadable before transmission.





## 4.2 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>Y</b>	<b>Processes (watching users) Outbound transmissions</b>
<b>Examine documentation</b>	<b>Y</b>	<b>Policies</b>
<b>Examine records</b>	<b>-</b>	
<b>Interview people</b>	<b>-</b>	





## Requirement 4.3

Have policies and procedures





### Requirement 4.3

Ensure that **security policies** and operational **procedures** for encrypting transmissions of cardholder data are **documented, in use**, and **known to all affected parties**.



### Requirement Guidance

- Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis.

## 4.3 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	Y	Security policies and operational procedures
<b>Examine records</b>	-	
<b>Interview people</b>	Y	Responsible people and people who need to know



# That's Fine in Theory

