IS4231 T8

Security Management Models

Group 5
Lee Yang Peng
Liu Zhuohao
Lye Jun Wei Ananda

Table of contents

01

Warm-up Questions

Regarding PCI-DSS requirements & EAL

02

Target Data Breach

Revisiting Target's Data Breach (Tutorial 3) with new perspective

03

Common Criteria

Discussion of the Information Security evaluation model

04

PP Compliance

Comparison against EAL system

Lee Yang Peng

01

Warm-Up Questions

(Personally, the trickiest warm-up questions in tutorial for me so far)

Lee Yang Peng

PCI-DSS Compliant but insecure

Considering why a certain information system/infosec program could be PCI -DSS compliant but not secured, which of the following is a potential reason?

https://pollev.com/anandalye391

Reasonings and Discussions

A)

The effectiveness of self - assessment compliance is with doubt

B)

Typically, QSAs may only review a sample of system components

C)

The system could be compliant at the examination point but failed to keep compliant along the way

D)

QSA's professionalism may be with doubt

When poll is active, respond at **pollev.com/anandalye391**

Text **ANANDALYE391** to **+65 8241 0042** once to join

Considering why a certain information system/infosec program could be PCI-DSS compliant but not secured, which of the following is a potential reason?

- The effectiveness of Self-assessment compliant is with doubt.
- Typically, QSAs may only review a sample of system components.
- The system could be compliant at the examination point but failed to keep compliant along the way.
- QSA's professionalism may be with doubt.

Tc 0

Powered by Poll Everywhere

When poll is active, respond at **pollev.com/anandalye391**

Text **ANANDALYE391** to **+65 8241 0042** once to join

Considering why a certain information system/infosec program could be PCI-DSS compliant but not secured, which of the following is a potential reason?

The effectiveness of Self-assessment compliant is with doubt.

Typically, QSAs may only review a sample of system components.

The system could be compliant at the examination point but failed to keep compliant along the way.

QSA's professionalism may be with doubt.

Poll locked. Responses not accepted.

Considering why a certain information system/infosec program could be PCI-DSS compliant but not secured, which of the following is a potential reason?

The effectiveness of Self-assessment compliant is with doubt.

Typically, QSAs may only review a sample of system components.

The system could be compliant at the examination point but failed to keep compliant along the way.

QSA's professionalism may be with doubt.

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Reasonings and Discussions

Perspectives	Discussion Points			
Self -assessment doubtful	Self assessment only one part of the assessment criteria	Failing in self assessment might make it difficult to get certified	Organisations only motivated to pass the examination	Requires a Qualified Security Assessor (QSA) to certify
Limited inspection by QSA	Assessments are limited by time and resources	Previously PCI-compliant organisation might discover newly unidentified gaps	Difficult for QSA to trace all locations of cardholder data storage	Depends on the experience of the QSA
Compliant during examination but fail to keep compliant	Organisation focuses on passing annual assessments and obtaining certifications	Deficiency of a mature compliance standard for protection and security measures	Failing to apply continuous monitoring efforts of security controls	Limited security awareness of PCI-DSS with organisation's stakeholders
Unprofessional or Unqualified QSAs	Poor methodology to conduct PCI-DSS assessments	"Lax", not accurate, "glaring with errors", poor quality	QSA's low level of proficiency	Unfamiliar with hacking techniques, lack of expertise

Theoretically, which of the following merchants do not need to comply with PCI standards?

A) Starbucks

B) Square POS

C) FavePay

D) None of the above

When poll is active, respond at **pollev.com/anandalye391**

Text **ANANDALYE391** to **+65 8241 0042** once to join

Theoretically, which of the following merchants does *not* need to comply with PCI standards?

- Starbucks
- Square POS
- FavePay
- None of the above

Tc 0

When poll is active, respond at **pollev.com/anandalye391**

Text **ANANDALYE391** to **+65 8241 0042** once to join

Theoretically, which of the following merchants does *not* need to comply with PCI standards?

- Starbucks
- Square POS
- FavePay
- None of the above

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

🔒 **Poll locked.** Responses not accepted.

Theoretically, which of the following merchants does *not* need to comply with PCI standards?

Starbucks

Square POS

FavePay

None of the above

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Considering the seven EALs, which of the following products may be more likely to get itself examined against EAL 7?

A) Commercial Firewall

B) Chips for military usage

C) Digital Signature Solution

D) Key Management System

When poll is active, respond at **pollev.com/anandalye391**

Text **ANANDALYE391** to **+65 8241 0042** once to join

Considering the seven EALs, which of the following products may be more likely to get itself examined against EAL 7 (i.e. Formally Verified Design and Tested) requirements?

- Commercial Firewall
- Chips for military usage
- Digital signature solution
- Key management system

Tc 0

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

When poll is active, respond at **pollev.com/anandalye391**

Text **ANANDALYE391** to **+65 8241 0042** once to join

Considering the seven EALs, which of the following products may be more likely to get itself examined against EAL 7 (i.e. Formally Verified Design and Tested) requirements?

Commercial Firewall

Chips for military usage

Digital signature solution

Key management system

Poll locked. Responses not accepted.

Considering the seven EALs, which of the following products may be more likely to get itself examined against EAL 7 (i.e. Formally Verified Design and Tested) requirements?

Commercial Firewall

Chips for military usage

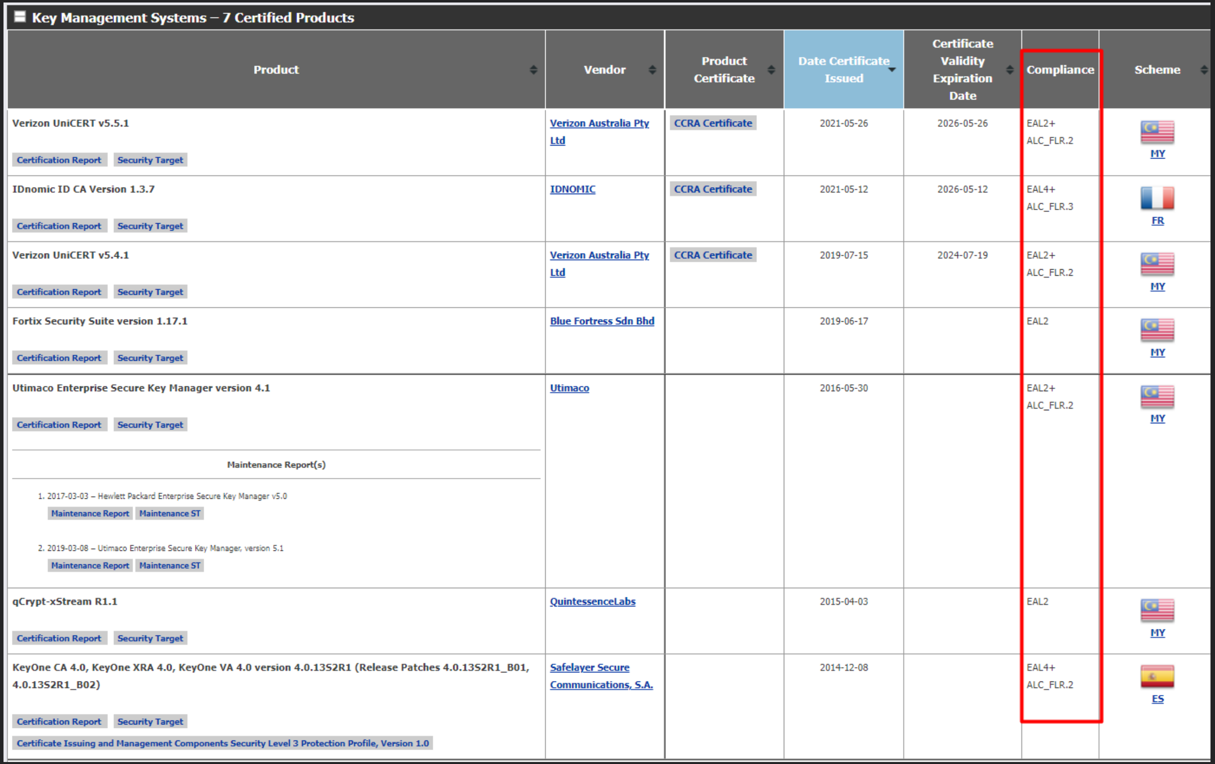
Digital signature solution

Key management system

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

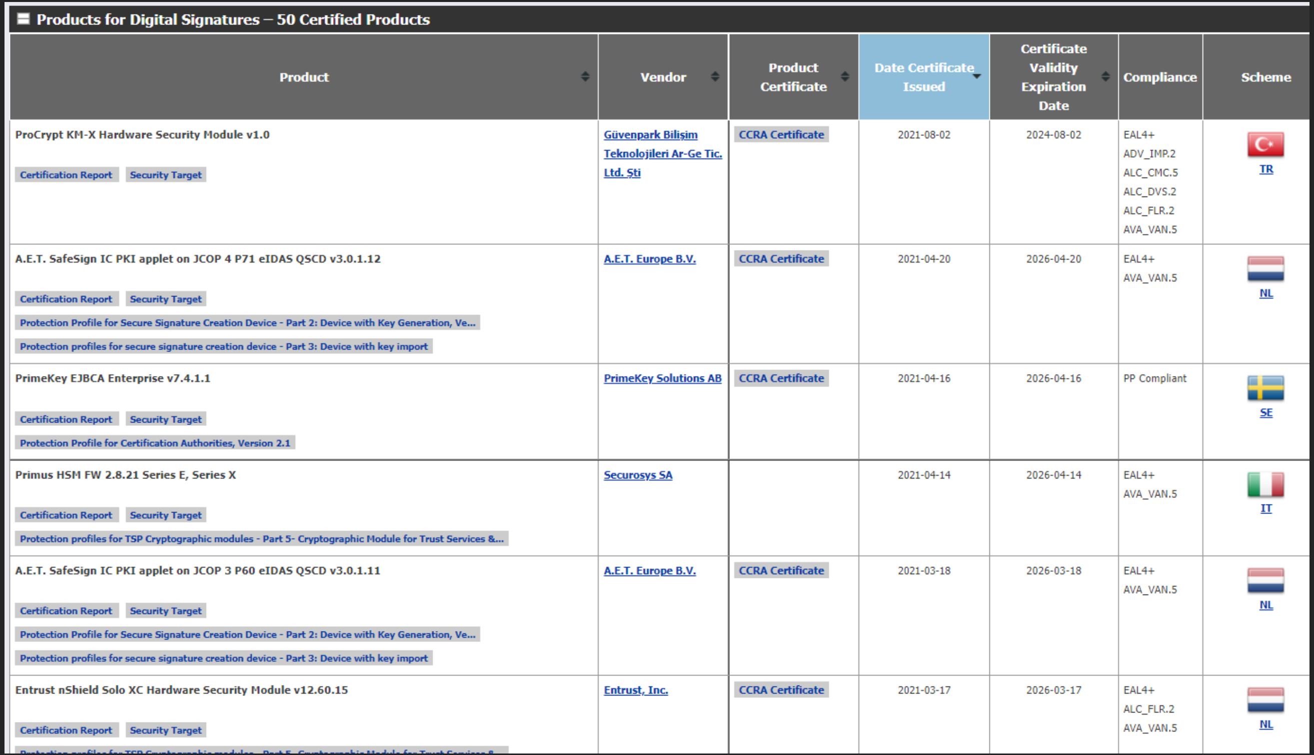
Considering the seven EALs, which of the following products may be more likely to get itself examined against EAL 7?



Key Management Systems – 7 Certified Products

Product	Vendor	Product Certificate	Date Certificate Issued	Certificate Validity Expiration Date	Compliance	Scheme
Verizon UniCERT v5.5.1 Certification Report Security Target	Verizon Australia Pty Ltd	CCRA Certificate	2021-05-26	2026-05-26	EAL2+ ALC_FLR.2	MY
IDnomic ID CA Version 1.3.7 Certification Report Security Target	IDNOMIC	CCRA Certificate	2021-05-12	2026-05-12	EAL4+ ALC_FLR.3	FR
Verizon UniCERT v5.4.1 Certification Report Security Target	Verizon Australia Pty Ltd	CCRA Certificate	2019-07-15	2024-07-19	EAL2+ ALC_FLR.2	MY
Fortix Security Suite version 1.17.1 Certification Report Security Target	Blue Fortress Sdn Bhd		2019-06-17		EAL2	MY
Utimaco Enterprise Secure Key Manager version 4.1 Certification Report Security Target Maintenance Report(s) 1. 2017-03-03 – Hewlett Packard Enterprise Secure Key Manager v5.0 Maintenance Report Maintenance ST 2. 2019-03-08 – Utimaco Enterprise Secure Key Manager, version 5.1 Maintenance Report Maintenance ST	Utimaco		2016-05-30		EAL2+ ALC_FLR.2	MY
qCrypt-xStream R1.1 Certification Report Security Target	QuintessenceLabs		2015-04-03		EAL2	MY
KeyOne CA 4.0, KeyOne XRA 4.0, KeyOne VA 4.0 version 4.0.13S2R1 (Release Patches 4.0.13S2R1_B01, 4.0.13S2R1_B02) Certification Report Security Target Certificate Issuing and Management Components Security Level 3 Protection Profile, Version 1.0	Safelayer Secure Communications, S.A.		2014-12-08		EAL4+ ALC_FLR.2	ES

Considering the seven EALs, which of the following products may be more likely to get itself examined against EAL 7?



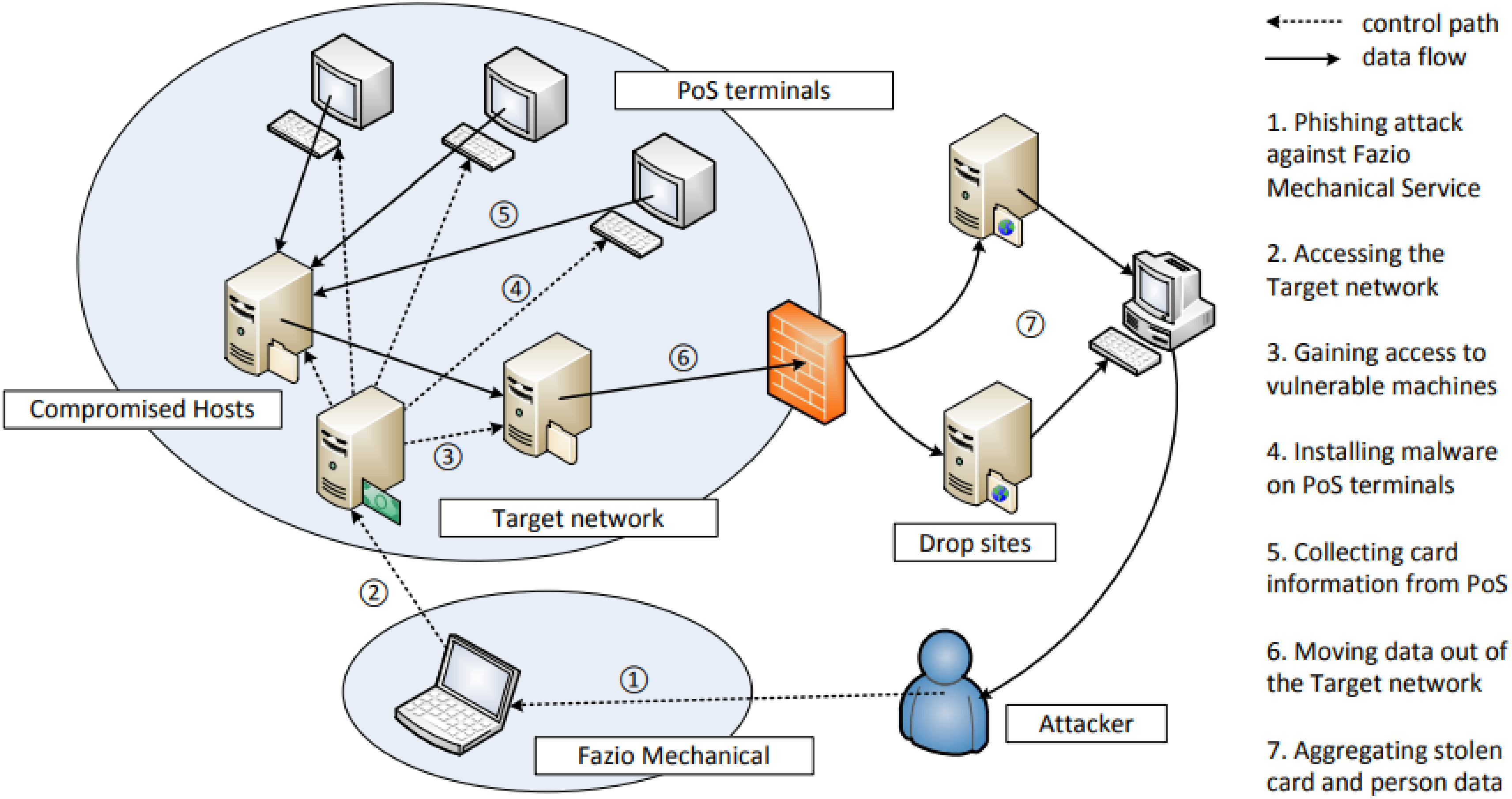
Products for Digital Signatures – 50 Certified Products

Product	Vendor	Product Certificate	Date Certificate Issued	Certificate Validity Expiration Date	Compliance	Scheme
ProCrypt KM-X Hardware Security Module v1.0 Certification Report Security Target	Güvenpark Bilişim Teknolojileri Ar-Ge Tic. Ltd. Şti	CCRA Certificate	2021-08-02	2024-08-02	EAL4+ ADV_IMP.2 ALC_CMC.5 ALC_DVS.2 ALC_FLR.2 AVA_VAN.5	TR
A.E.T. SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD v3.0.1.12 Certification Report Security Target Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation, Ve... Protection profiles for secure signature creation device - Part 3: Device with key import	A.E.T. Europe B.V.	CCRA Certificate	2021-04-20	2026-04-20	EAL4+ AVA_VAN.5	NL
PrimeKey EJBCA Enterprise v7.4.1.1 Certification Report Security Target Protection Profile for Certification Authorities, Version 2.1	PrimeKey Solutions AB	CCRA Certificate	2021-04-16	2026-04-16	PP Compliant	SE
Primus HSM FW 2.8.21 Series E, Series X Certification Report Security Target Protection profiles for TSP Cryptographic modules - Part 5- Cryptographic Module for Trust Services &...	Securosys SA		2021-04-14	2026-04-14	EAL4+ AVA_VAN.5	IT
A.E.T. SafeSign IC PKI applet on JCOP 3 P60 eIDAS QSCD v3.0.1.11 Certification Report Security Target Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation, Ve... Protection profiles for secure signature creation device - Part 3: Device with key import	A.E.T. Europe B.V.	CCRA Certificate	2021-03-18	2026-03-18	EAL4+ AVA_VAN.5	NL
Entrust nShield Solo XC Hardware Security Module v12.60.15 Certification Report Security Target Protection profiles for TSP Cryptographic modules - Part 5- Cryptographic Module for Trust Services &...	Entrust, Inc.	CCRA Certificate	2021-03-17	2026-03-17	EAL4+ ALC_FLR.2 AVA_VAN.5	NL

Liu Zhuohao

02 Target Data Breach

Revising Target’s compliance of PCI DSS



1. Phishing attack against Fazio Mechanical Service

2. Accessing the Target network

3. Gaining access to vulnerable machines

4. Installing malware on PoS terminals

5. Collecting card information from PoS

6. Moving data out of the Target network

7. Aggregating stolen card and person data

PCI DSS Requirements

#	Requirement Description
01	Install and maintain a firewall configuration to protect cardholder data
02	Do not use vendor -supplied defaults for system passwords and other security parameters
03	Protect stored cardholder data
04	Encrypt transmission of cardholder data across open, public networks
05	Use and regularly update anti -virus software or programs
06	Develop and maintain secure systems and applications

PCI DSS Requirements

#	Requirement Description
07	Restrict access to cardholder data by business need to know
08	Assign a unique ID to each person with computer access
09	Restrict physical access to cardholder data
10	Track and monitor all access to network resources and cardholder data
11	Regularly test security systems and processes
12	Maintain a policy that addresses information security for all personnel

Poll locked. Responses not accepted.

What are the requirements in PCI DSS v3.2.1 that Target might have failed to comply with before the breach?

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 5: Use and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

Requirement 7: Restrict access to cardholder data by business need to know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security for all personnel

🔒 **Poll locked.** Responses not accepted.

What are the requirements in PCI DSS v3.2.1 that Target might have failed to comply with before the breach?

Requirement 1: Install and maintain a firewall configuration to protect cardholder data	✓0%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	
Requirement 3: Protect stored cardholder data	✓0%
Requirement 4: Encrypt transmission of cardholder data across open, public networks	
Requirement 5: Use and regularly update anti-virus software or programs	✓0%
Requirement 6: Develop and maintain secure systems and applications	
Requirement 7: Restrict access to cardholder data by business need to know	✓0%
Requirement 8: Assign a unique ID to each person with computer access	✓0%
Requirement 9: Restrict physical access to cardholder data	
Requirement 10: Track and monitor all access to network resources and cardholder data	✓0%
Requirement 11: Regularly test security systems and processes	✓0%
Requirement 12: Maintain a policy that addresses information security for all personnel	

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

What rules did Target break?

What are the requirements in PCI DSS v3.2.1 that Target might have failed to comply with before the breach?

#1 - Install Firewall

1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

The paper (Page 3) mentioned …

> *2.1.2 Phase II: PoS Infection*
>
> *Due to Target's poor segmentation of its network, all that the attackers needed in order to gain access into Target's entire system was to access its business section. From there, they gained access to other parts of the Target network, including parts of the network that contained sensitive data.*

#3 - Protect Cardholders’ Data

3.1 Limit cardholder data storage and retention time to that which is required for business, legal, and/ or regulatory purposes, as documented in your data retention policy. Purge unnecessary stored data at least quarterly.

3.2 Do not store sensitive authentication data after authorization (even if it is encrypted). See table below. Render all sensitive authentication data unrecoverable upon completion of the authorization process. Issuers and related entities may store sensitive authentication data if there is a business justification, and the data is stored securely.

From Trustwave Lawsuit (Page 24) ...

> *Target kept credit and debit card data on its servers for six full days before hackers transmitted the data to a separate web server outside of Target's network … hackers were able to take 40 million Payment Card records, encrypted PINs, and 70 million records containing Target customer information over the course of two weeks*

#5 - Antivirus Program

5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

The paper (Page 4) mentioned …

> *Target did not investigate into the security warnings generated by multiple security tools, e.g., FireEye, Symantec, and* ***certain malware auto-removal functionalities were turned off***

#7 - Access Control

7.2 Establish an access control system(s) for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.

The paper (Page 4) mentioned …

> *Target did not apply proper access control on varieties of accounts and groups, especially the ones from third party partners [17]. The failure resulted in the initial break - in from the HVAC company Fazio Mechanical Services Inc.*

#8 - Remote Access

8.3 Secure all individual non-console administrative access and all remote access to the cardholder data environment using multi-factor authentication. This requires at least two of the three authentication methods described in 8.2 are used for authentication. Using one factor twice (e.g. using two separate passwords) is not considered multi-factor authentication. This requirement applies to administrative personnel with non-console access to the CDE from within the entity’s network, and all remote network access (including for users, administrators, and third-parties) originating from outside the entity’s network.

#10 - Track Network Activity

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.

10.8 Service providers must implement a process for timely detection and reporting of failures of critical security control systems

The paper (Page 4) mentioned …

> *Target did not investigate into the security warnings generated by multiple security tools, e.g., FireEye, Symantec …*

From Trustwave Lawsuit (Page 17) …

> *Reedum transmitted its first payload of stolen payment card information to a hijacked internal Target network server on December 2, 2013. The hackers later harvested "scraped" stolen payment card information from the Target server by sending it* ***over the Internet*** *to a computer in* ***Russia****. They repeated this process* ***numerous times over the next two weeks****.*

#11 - Regular PenTest

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. Address vulnerabilities and perform rescans as needed, until passing scans are achieved ...

11.3 Develop and implement a methodology for penetration testing that includes external and internal penetration testing at least annually and after any significant upgrade or modification ...

11.4 Use network intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date

SAQ Applicable to Target?

Considering the business model of Target, if Target planned to conduct self - assessment for compliance purpose, which Self - Assessment Questionnaire (SAQ) Target should use to do self-assessment?

Target’s Business Model?

Physical Store

Like how we buy grocery from Fairprice, it accepts **card - present payment**.

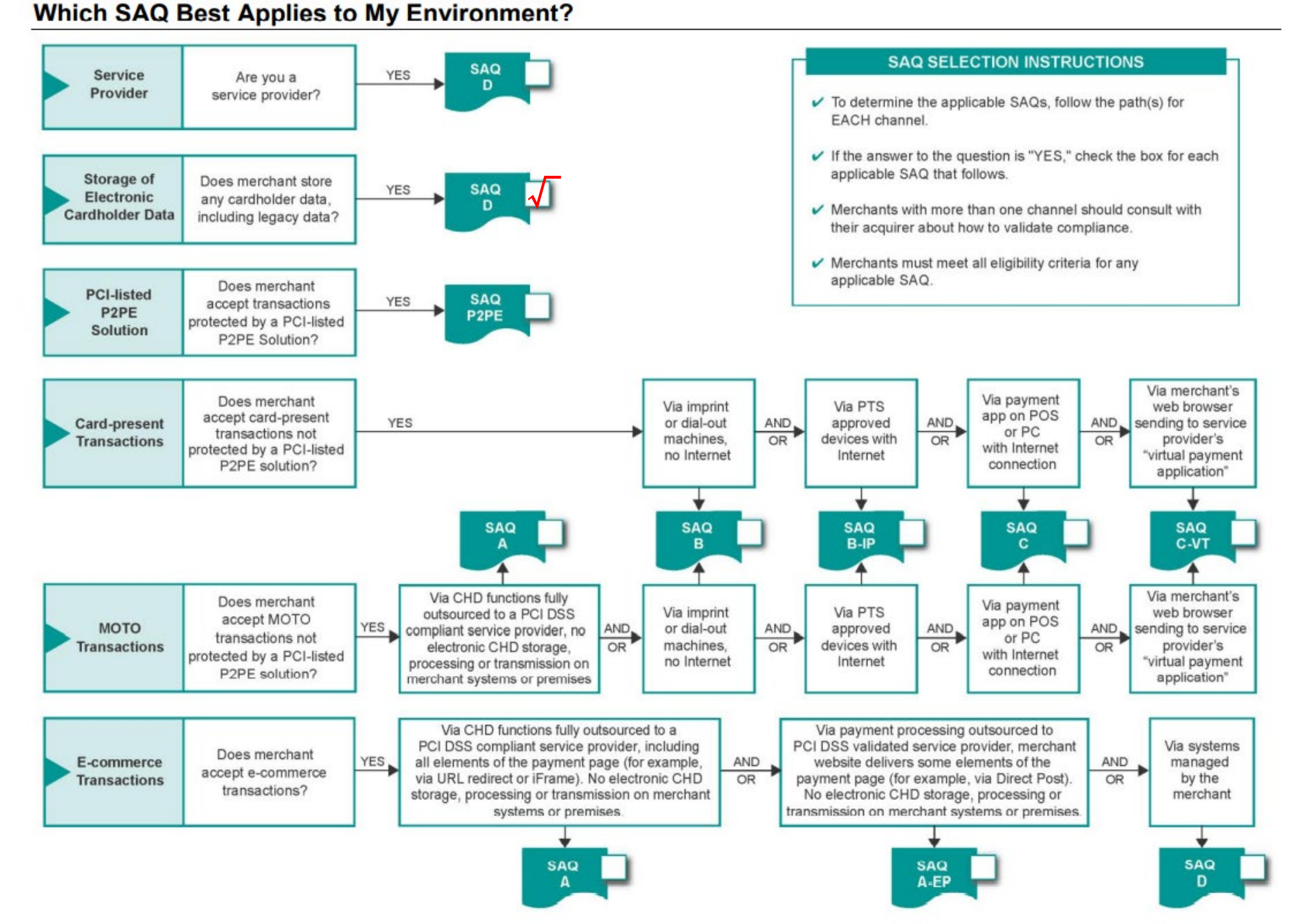
Also, Target’s POS system has connectivity to the Internet.

Online Store

Credit/debit card number and **Name** are collected as stated in their Privacy Statement.

Card number, or Primary Account Number (PAN) is considered Cardholder Data under PCI DSS.

Same for Cardholder’s Name.



Which SAQ Best Applies to My Environment?

Service Provider — Are you a service provider? — YES → SAQ D □

Storage of Electronic Cardholder Data — Does merchant store any cardholder data, including legacy data? — YES → SAQ D ☑

PCI-listed P2PE Solution — Does merchant accept transactions protected by a PCI-listed P2PE Solution? — YES → SAQ P2PE □

Card-present Transactions — Does merchant accept card-present transactions not protected by a PCI-listed P2PE solution? — YES → Via imprint or dial-out machines, no Internet (→ SAQ B □) AND OR → Via PTS approved devices with Internet (→ SAQ B-IP □) AND OR → Via payment app on POS or PC with Internet connection (→ SAQ C □) AND OR → Via merchant's web browser sending to service provider's "virtual payment application" (→ SAQ C-VT □)

MOTO Transactions — Does merchant accept MOTO transactions not protected by a PCI-listed P2PE solution? — YES → Via CHD functions fully outsourced to a PCI DSS compliant service provider, no electronic CHD storage, processing or transmission on merchant systems or premises (→ SAQ A □) AND OR → Via imprint or dial-out machines, no Internet (→ SAQ B □) AND OR → Via PTS approved devices with Internet (→ SAQ B-IP □) AND OR → Via payment app on POS or PC with Internet connection (→ SAQ C □) AND OR → Via merchant's web browser sending to service provider's "virtual payment application" (→ SAQ C-VT □)

E-commerce Transactions — Does merchant accept e-commerce transactions? — YES → Via CHD functions fully outsourced to a PCI DSS compliant service provider, including all elements of the payment page (for example, via URL redirect or iFrame). No electronic CHD storage, processing or transmission on merchant systems or premises. (→ SAQ A □) AND OR → Via payment processing outsourced to PCI DSS validated service provider, merchant website delivers some elements of the payment page (for example, via Direct Post). No electronic CHD storage, processing or transmission on merchant systems or premises. (→ SAQ A-EP □) AND OR → Via systems managed by the merchant (→ SAQ D □)

SAQ SELECTION INSTRUCTIONS

- ✓ To determine the applicable SAQs, follow the path(s) for EACH channel.
- ✓ If the answer to the question is "YES," check the box for each applicable SAQ that follows.
- ✓ Merchants with more than one channel should consult with their acquirer about how to validate compliance.
- ✓ Merchants must meet all eligibility criteria for any applicable SAQ.

SAQ D for Merchants

SAQ D for Merchants applies to SAQ -eligible merchants not meeting the criteria for any other SAQ type.

Examples of merchant environments that would use SAQ D may include but are not limited to:

- E-commerce merchants who accept cardholder data on their website;
- **Merchants with electronic storage of cardholder data** ;
- Merchants that don't store cardholder data electronically but that do not meet the criteria of another SAQ type;
- **Merchants with environments that might meet the criteria of another SAQ type, but that have additional PCI DSS requirements applicable to their environment** .

Ananda Lye

03

Common Criteria

Evaluation Assurance Level

Recap I - Common Criteria

Common Criteria is an international standard for computer security certification

Products are certified under the Evaluation Assurance Level (EAL) scheme

- with levels from 1 to 7,
- higher level indicating that it has gone under the **higher level of testing**

Evaluation is **documentation centric**

Certification process can be **lengthy, costly, not timely**

When poll is active, respond at **pollev.com/anandalye391**

Text **ANANDALYE391** to **+65 8241 0042** once to join

Two products under the same category have different EALs awarded - Product A has EAL3 & Product B has EAL2. Is Product A definitely more secure than Product B?

Yes

No

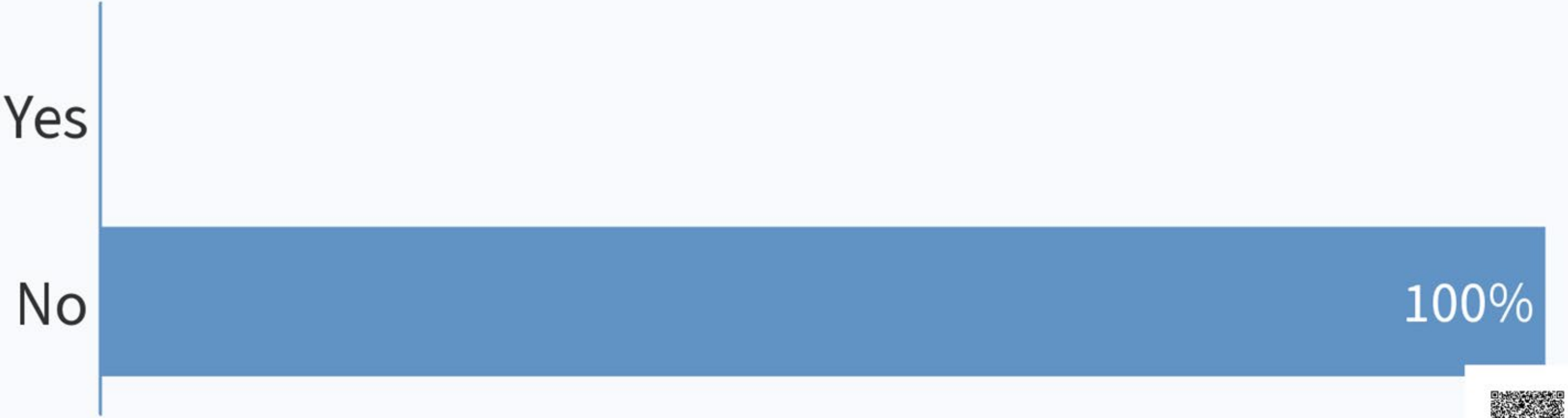
Tc 1

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Poll locked. Responses not accepted.

Two products under the same category have different EALs awarded - Product A has EAL3 & Product B has EAL2. Is Product A definitely more secure than Product B?

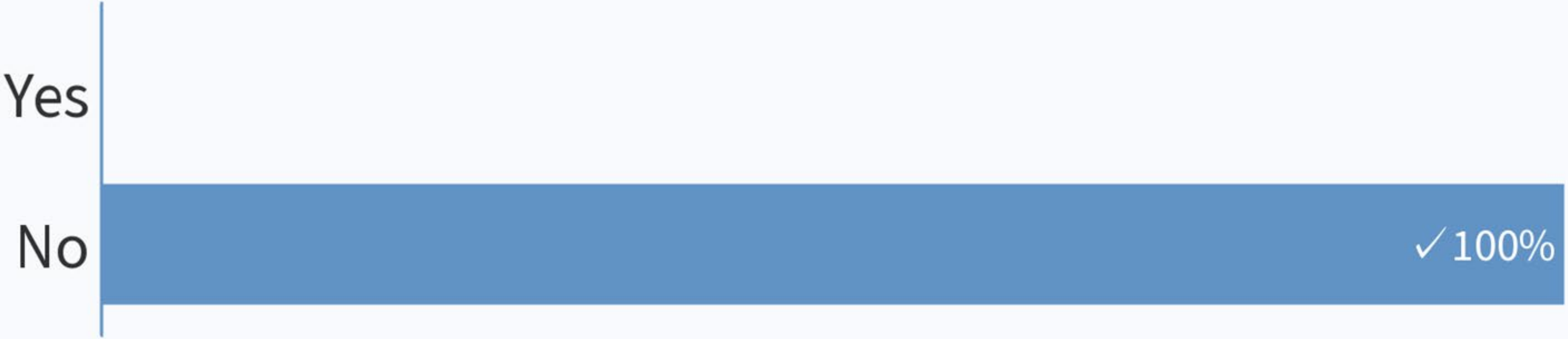


Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Poll locked. Responses not accepted.

Two products under the same category have different EALs awarded - Product A has EAL3 & Product B has EAL2. Is Product A definitely more secure than Product B?



Recap II - Terminologies

Protection Profile (PP)	Provides **customer** desires, needs, and requirements: "What is wanted". **User-generated** specification for security requirements
Security Target (ST)	Indicates how the above will be satisfied by **suppliers**: "What will be provided". Describes the system’s security properties to be met.
Target of Evaluation (TOE)	The supplier's physical manifestation of above. The system to be evaluated under EAL scheme

Under the EAL evaluation scheme, the **TOE** is evaluated based on the fulfillment of the **ST** provided.

Respond at **pollev.com/anandalye391**

Text **ANANDALYE391** to **+65 8241 0042** once to join, then **A or B**

Can products in the same category, have the same PP, but different ST and TOE?

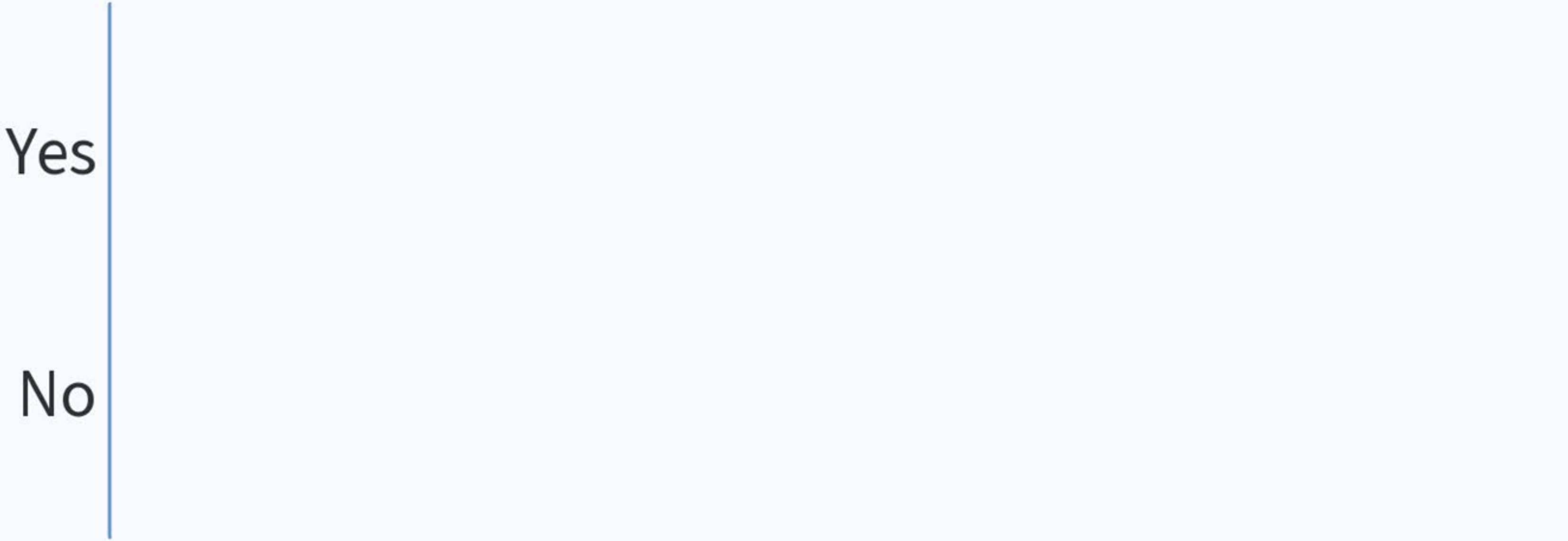
Yes

No

Tc 0

Poll locked. Responses not accepted.

Can products in the same category, have the same PP, but different ST and TOE?

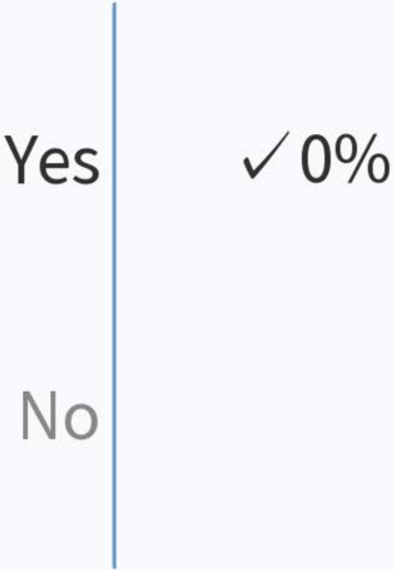


Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Poll locked. Responses not accepted.

Can products in the same category, have the same PP, but different ST and TOE?



Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Ananda Lye

NIAP - PP Compliant

04

Newer Certification – PP Compliant

The National Information Assurance Partnership (NIAP), who manages CC evaluation in the US, created and accepts a new certification – "**PP Compliant**"

NIAP **no longer accepts EAL-based evaluations**

Transitioned to evaluations with exact compliance to **technology-specific Protection Profiles (PP)**

Under PP-Compliant, there are **no levels**

Qn: What are some of the benefits of Protection Profiles (PP) oriented evaluation?

When poll is active, respond at **pollev.com/anandalye391**

Text **ANANDALYE391** to **+65 8241 0042** once to join

What are some benefits of Protection Profiles (PP) oriented evaluation?

All vendors within the same product type must adhere to the same security requirements

Customers can better compare across different products and vendors

Each vendor can individually choose which security requirements to claim for evaluation

Standardised threat models and security functional requirements across vendors

Tc 0

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Poll locked. Responses not accepted.

What are some benefits of Protection Profiles (PP) oriented evaluation?

All vendors within the same product type must adhere to the same security requirements

Customers can better compare across different products and vendors

Each vendor can individually choose which security requirements to claim for evaluation

Standardised threat models and security functional requirements across vendors

What are some benefits of Protection Profiles (PP) oriented evaluation?

All vendors within the same product type must adhere to the same security requirements	✓0%
Customers can better compare across different products and vendors	✓0%
Each vendor can individually choose which security requirements to claim for evaluation	
Standardised threat models and security functional requirements across vendors	✓0%

References

- *Compliant but not Secure: Why PCI-Certified Companies Are Being Breached*: https://csiac.org/articles/compliant-but-not-secure-why-pci-certified-companies-are-being-breached/
- Target & Trustwave Lawsuit: https://www.wired.com/images_blogs/threatlevel/2014/03/Trustwave-suit.pdf
- Research Paper - *Breaking the Target: An Analysis of Target Data Breach and Lessons Learned*: https://arxiv.org/pdf/1701.04940.pdf
- PCI DSS v3.2.1 Quick Reference:https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf
- Target’s Privacy Policy: https://www.target.com/c/target-privacy-policy/-/N-4sr7p#Type
- NIAP PP-Compliant Reference: https://www.niap-ccevs.org/Ref/FAQ.cfm

All images produced in this presentation are from the Internet, including screenshots from the above mentioned documents.

IS4231 Group 5

Thanks!

Do you have any questions?

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik