

➤ Information Security Decisions



PCI Guidance Check-In – Where are We Now?

A close-up photograph of a computer keyboard key featuring a white padlock icon on a dark blue key. The background is a dark, blurred image of other keyboard keys.

Diana Kelley
diana@securitycurve.com
[@securitycurve](#)

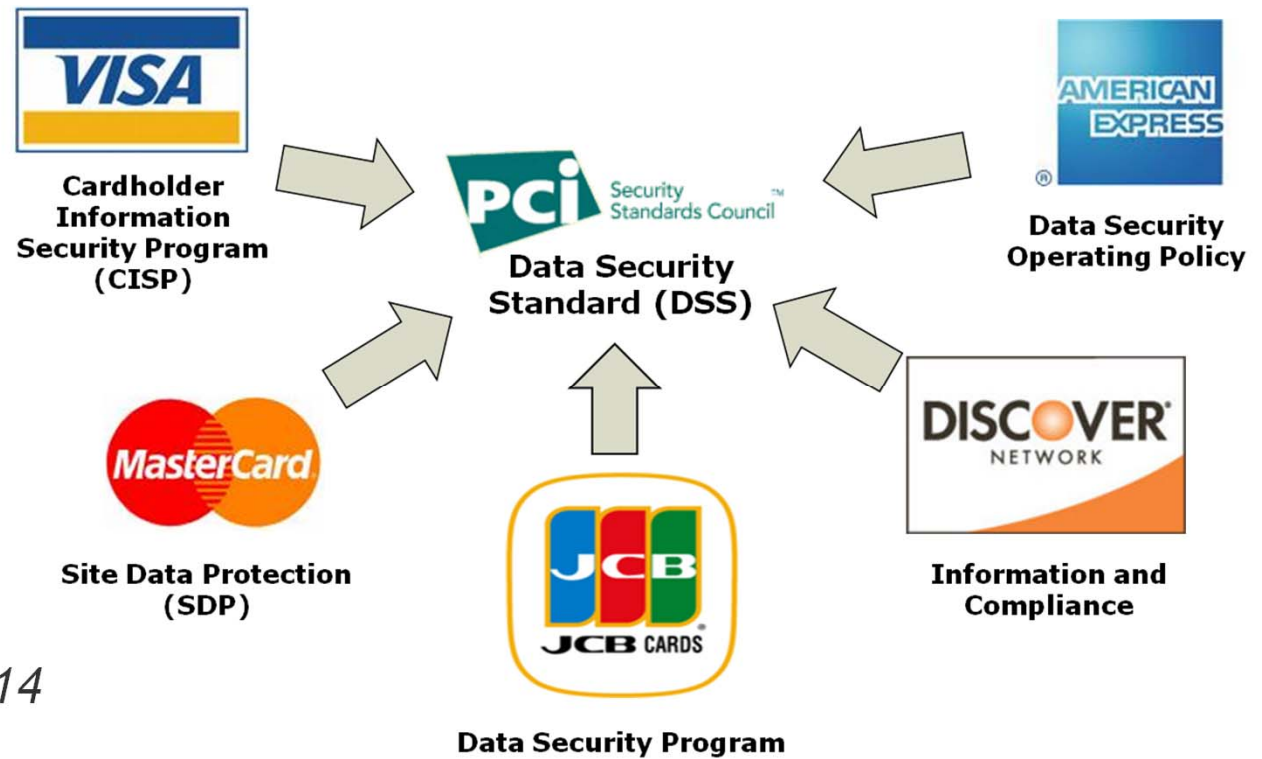
A horizontal dotted line, composed of small teal dots, is located at the bottom of the slide.

Agenda

- Quick PCI DSS level-set
- Changes in PCI DSS v2.0
- Published SIGs
- 2012 SIGs
- Other Documents

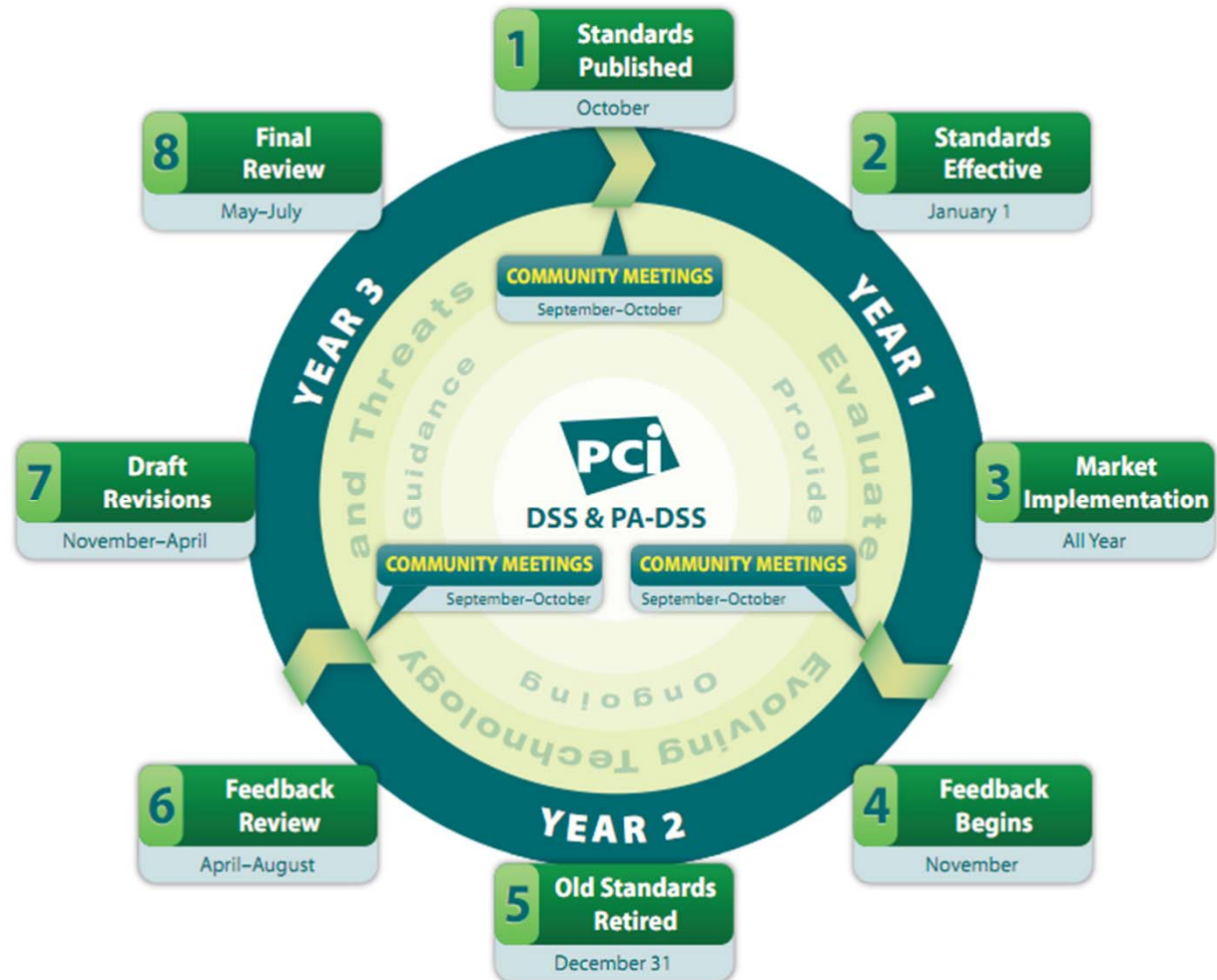
PCI DSS History

- Pre-2004
 - 5 separate programs
- PCI DSS
 - 5 separate programs
 - 1 standard
- Revisions
 - v1.0 – 12/04
 - v1.1 – 9/06
 - v1.2 – 10/08
 - v2.0 – 1/11
 - EST: v3.0 – 1/14



PCI DSS 3 Year Lifecycle

- Council publishes and maintains technical standards
- Incorporates review and feedback from outside
- Results in new version after review
- Initiates new version
- Rinse and repeat



Source: *Lifecycle for Changes to PCI DSS and PA-DSS*
https://www.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_dss_and_padss.pdf

Feedback: Next Steps

1	Feedback reviewed and categorized (April '12 – August '12)
2	Feedback shared with PCI community (August – September '12)
3	Feedback presented at 2012 Community Meetings (September '12 – October '12)
4	Revisions drafted for PCI DSS and PA-DSS (November '12 – April '13)
5	Final Review Period (May '13 – July '13)
6	Standards Published (October '13)

PCI DSS v2.0 – Evolution

- Recent (2.0) changes are mostly minor
 - The standard is gaining maturity
 - 3-year cycle means more time it'll stay “live”
 - But emerging technologies are not incorporated
- Changes were community driven
 - Merchants/Processors
 - Special Interest Groups (SIGs)
 - Participating Organizations
 - QSAs

Revision 2.0 – Change Types

Clarifications

“Clarifies intent of requirement. Ensure that concise wording in the standards portray the desired intent of requirements.”

3.2.1 Replaced “*contained in a chip*” to “*equivalent data on a chip*” for consistency.

Additional Guidance

“Explanations and/or definitions to increase understanding or provide further information...”

General *“Added detailed paragraph to clarify that the first step of a PCI DSS review is to accurately determine the scope”*

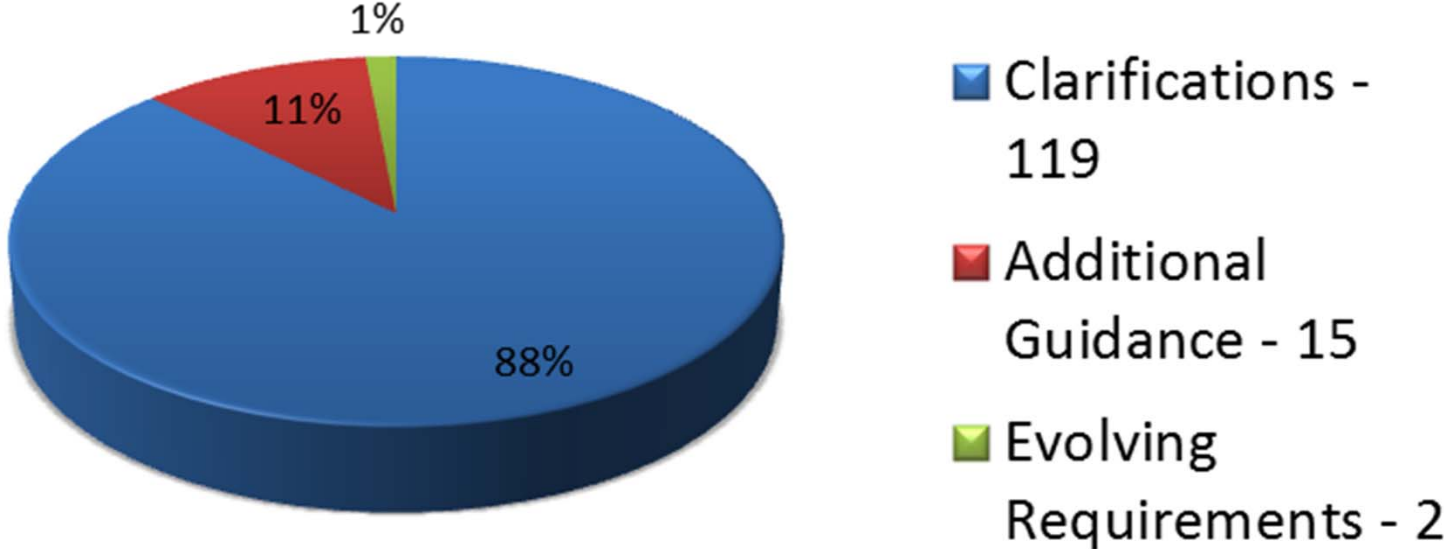
Evolving Requirement

“Changes to ensure that the standards are up to date with emerging threats and changes in the market.”

6.2 *Risk rankings should be based on industry best practices. [Ex] criteria for ranking “High” risk vulnerabilities may include a CVSS base score of 4.0*

Breaking Down the Changes

Changes in PCI DSS v2.0



General Changes of Note

- AOCs (Attestation of Compliance) – moved from appendix to separate documents
- Scoping awareness highlighted and expanded
- “*Virtualization*” included in definition of “*system components*”
- Clarified that using a PA DSS compliant app does not make the organization compliant

Why Scope is a Big Deal

- New section in v2.0
 - Pages 10 through 13
 - Flow chart on scoping/sampling in Appendix D
- The scope of the compliance *must include* the entirety of the cardholder data environment (CDE)
- Cardholder data environment is:
 - Any system that stores, processes or transmits credit card information
 - Any machine(s) not separated from those machines
- This means, unless you strategize, *the whole network is in scope*

1.1.5 Requirement Clarification

- Pre v2.0
 - Documentation and business justification for use of all services, protocols and ports allowed, including documentation of security features implemented for those protocols considered to be insecure
- v2.0 Addition
 - *“Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP”*
- Why it Matters
 - Organizations using the ports/services they had not deemed “insecure” must now document and implement security features

6.2 Evolving Requirement

- Pre v2.0
 - Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet)
- v2.0 Change
 - *“Risk rankings should be based on industry best practices*
 - *The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement”*
- Why it Matters
 - Must have a way to rank vulnerability risks
 - NB: Can use CVSS (Common Vulnerability Scoring System, <http://www.first.org/cvss/>) scores and vendor rankings

Other Standards



PTS - PIN Transaction Security

- PIN Security Requirements
- Hardware Security Module (HSM)
- Point of Interaction (POI)

PA-DSS – Payment Application Data Security Standard

PCI P2PE (Point to Point Encryption)

Other Updates of Notes



SAQs (A-D)

- All updated May 19, 2011

SAQ OACs (A-D)

- All updated May 20, 2011

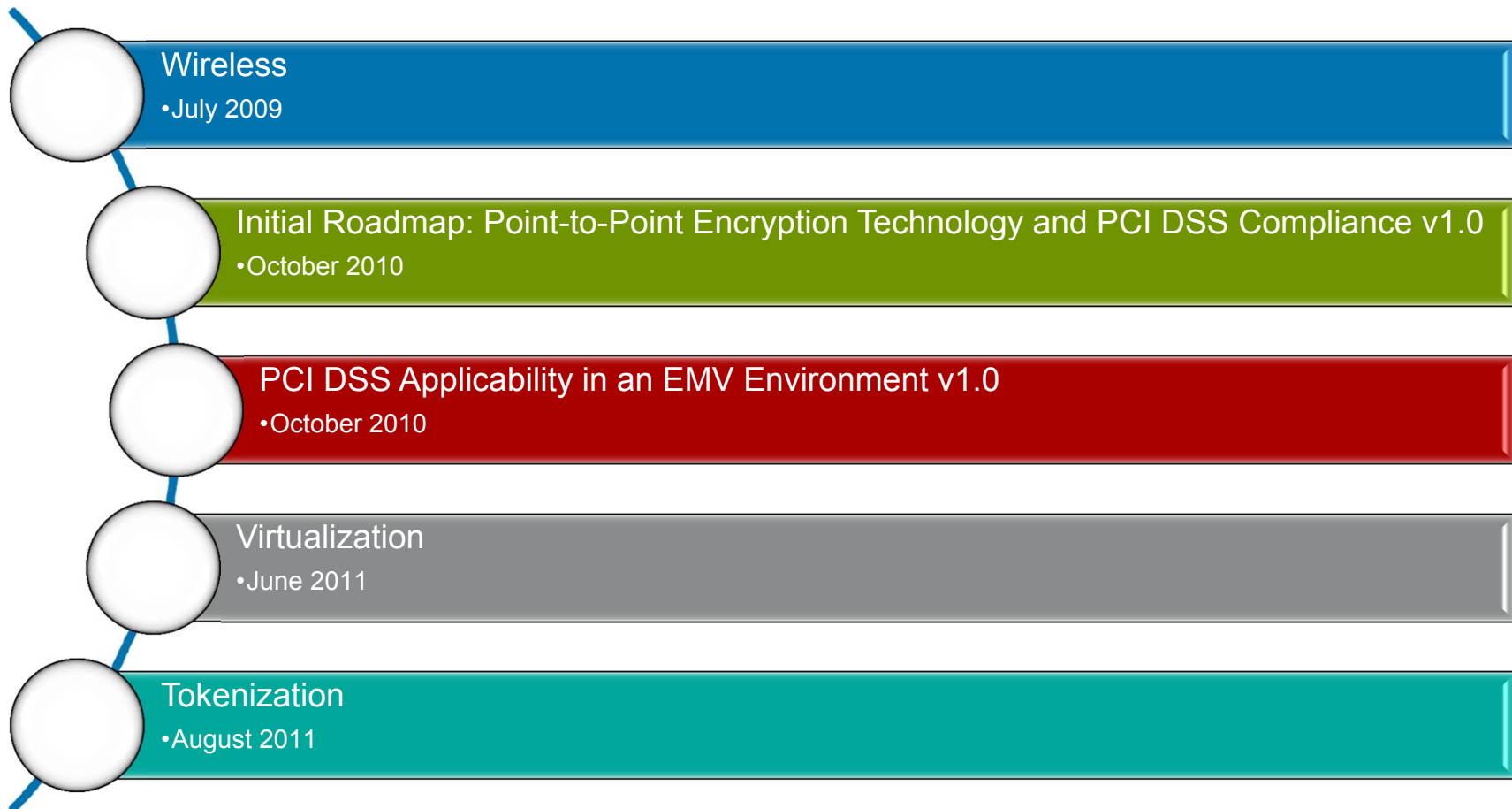
PA-DSS

- Program Guide and AOV 1/12
- Mobile Apps FAQ 6/11

PCI – Special Interest Groups

- Participating Organizations (POs) and the Council work together on guidelines
- Useful because DSS is on 3 year refresh cycle
 - May address emerging technology
 - Ex: Virtualization
 - Or clarify covered technology
 - Ex: Wireless

Special Interest Groups – Completed Guidelines





Wireless

- Section 3

Generally applicable (in and out of CDE)

- “These are requirements that all organizations should have in place to protect their networks . . . regardless of whether the wireless technology is a part of the CDE or not.”

- Section 4

CDE and PCI DSS specific

- “(S)pecific to the usage of wireless technology that is in scope for PCI DSS compliance, namely the Cardholder Data Environment (CDE).”

Quote source: edited from original:

https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

Wireless

- Wi-Fi LANs (802.11 networks) only
 - Not covered?
 - Bluetooth
 - 2G and 3G (GPRS, EDGE, etc)
- Be Aware
 - Hybrid wireless devices are increasingly common
 - If you are using hybrid devices
 - Turn off any non-WiFi communications
 - Or enable equivalent data protections on all channels



Wireless

In Scope

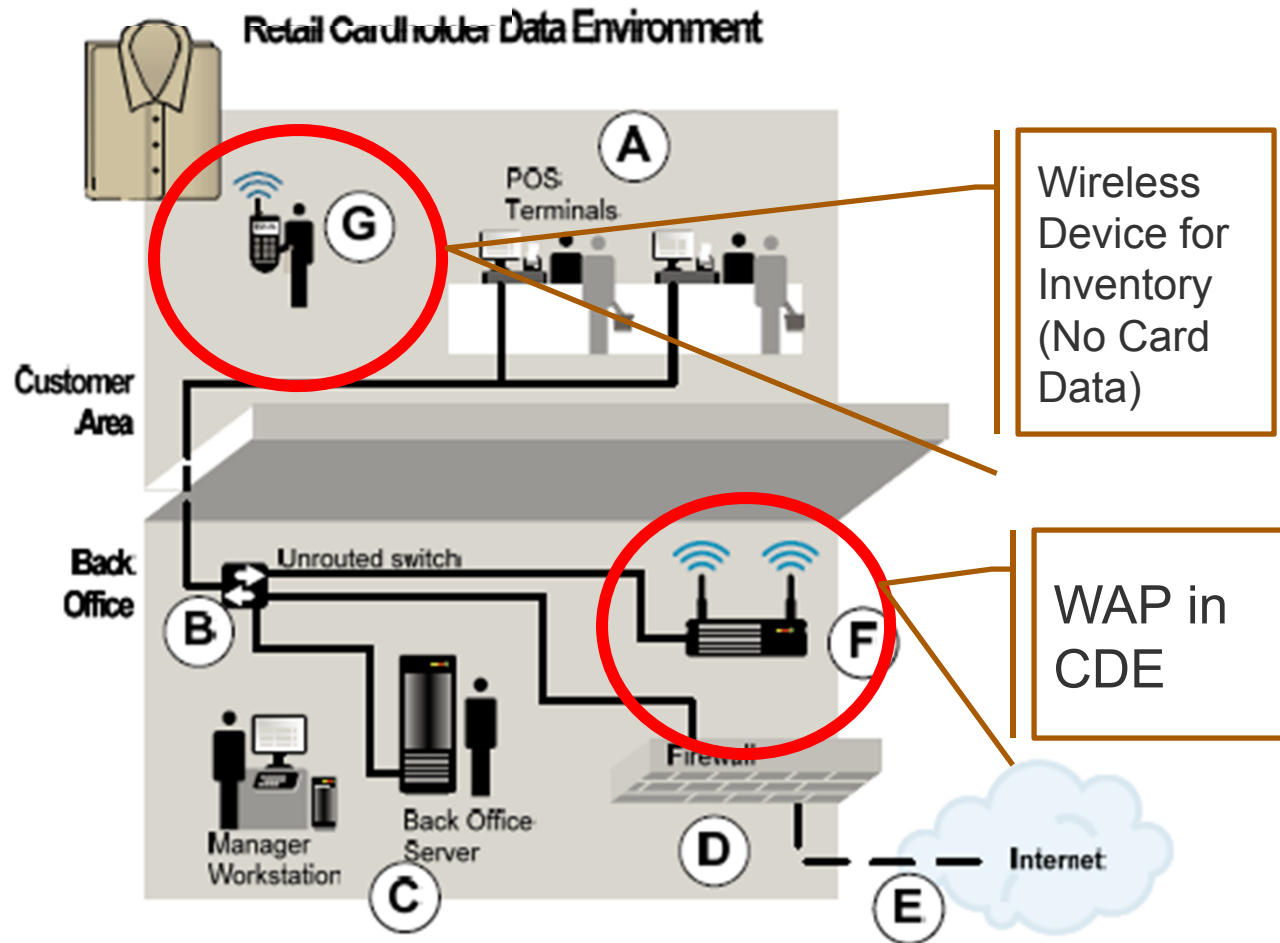
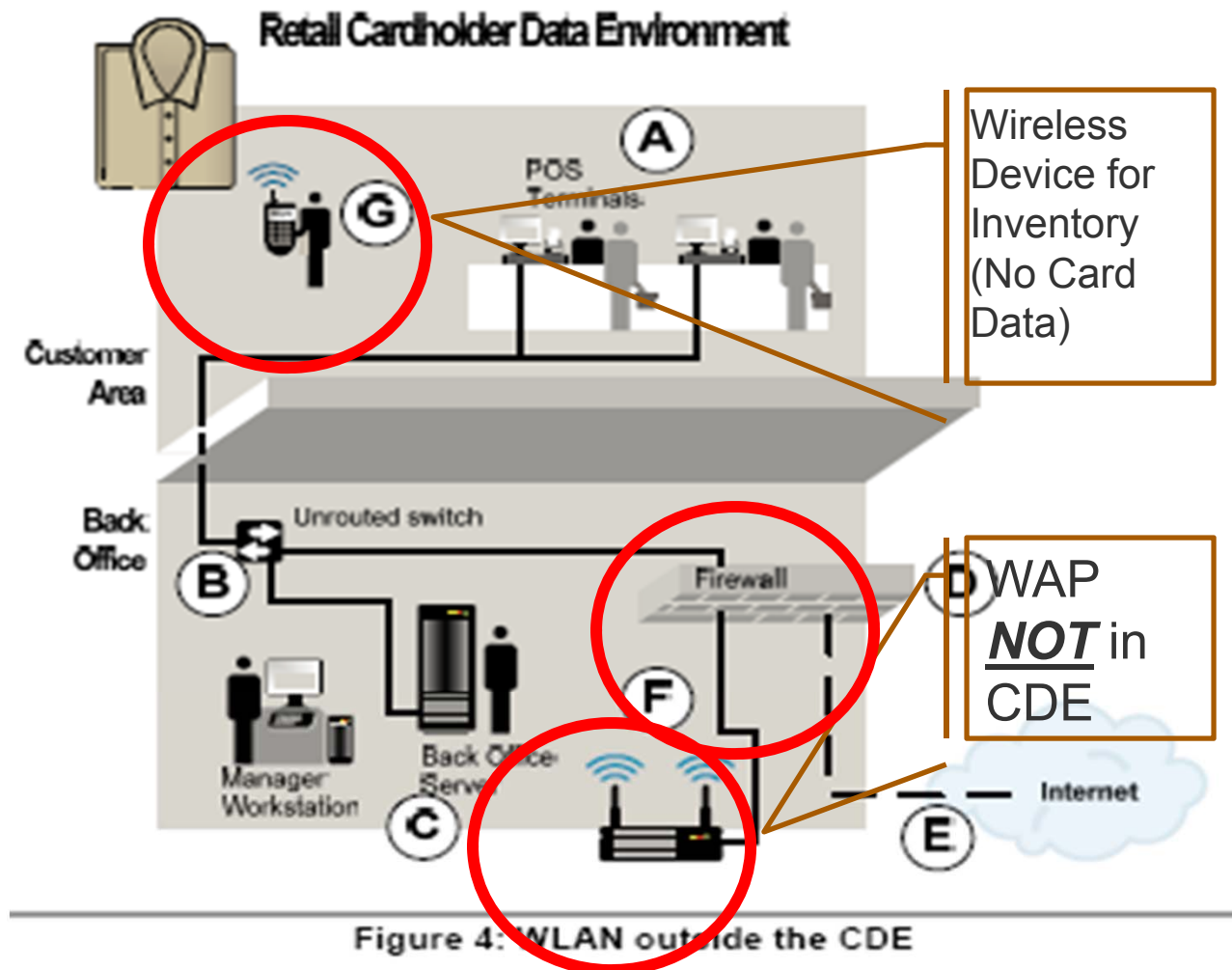


Figure 3: A CDE with an added WLAN

Wireless

Not in Scope





Virtualization

- Pages 1-14 general overview of security risks associated with virtualization
- Recommendations begin on page 15
 - Includes mention of cloud
 - NB: Cloud SIG due in 2012
- For VirtSec gurus
 - Focus on the Appendix
 - This maps “virtualization considerations” to the PCI DSS requirements
- Example Requirement 1 - firewalls and connections from the outside/public networks to servers and systems in the CDE
 - “Do not locate untrusted systems or networks on the same host or hypervisor as systems in the CDE”

Original Source: https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf



Virtualization

- Pages 1-14 general overview of security risks associated with virtualization
- Recommendations begin on page 15
 - Includes mention of cloud
 - NB: Cloud SIG due in 2012
- For VirtSec gurus
 - Focus on the Appendix
 - This maps “virtualization considerations” to the PCI DSS requirements
- Example Requirement 1 - firewalls and connections from the outside/public networks to servers and systems in the CDE
 - “Do not locate untrusted systems or networks on the same host or hypervisor as systems in the CDE”

Original Source: https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf



Virtualization

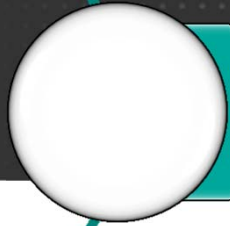
- VMs running on top of single hypervisor are in a similar trust zone and all of them can be considered as inside the CDE
 - “if **any component** running on a particular hypervisor or host is in scope for PCI DSS, it is recommended that **all components** on that hypervisor or host be **considered in scope as well.**”
 - Keep the same security level for all server VMs on a single hypervisor a
 - “**virtual component requiring higher security could unintentionally be exposed to additional risk if hosted on the same system or hypervisor as a virtual component of lower security.**” Original Source:

https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf



Virtualization

- Issues with inter-VM monitoring
 - If traffic stays in the hypervisor
 - May be a blind spot for traditional netmon tools
- Guidelines suggest
 - “firewalls and routers could be embedded within the hypervisor”
- Use of virtual desktop infrastructures (VDIs) and applications
- These systems are in scope if
 - “they are involved in the processing, storage, or transmission of cardholder data, or provide access to the CDE.”
 - Re-assess the architecture to ensure PCI audit scope is correctly defined
 - Additional segmentation or even limiting access to certain devices may be required



Tokenization

No PAN, No Scope

(Know PAN, Know Scope)

- From the council:

- *“These data elements must be protected if stored in conjunction with the PAN. ...PCI DSS, however, does not apply if PANs are not stored, processed or transmitted.”¹ [emphasis mine]*

- What if there were no PANs?

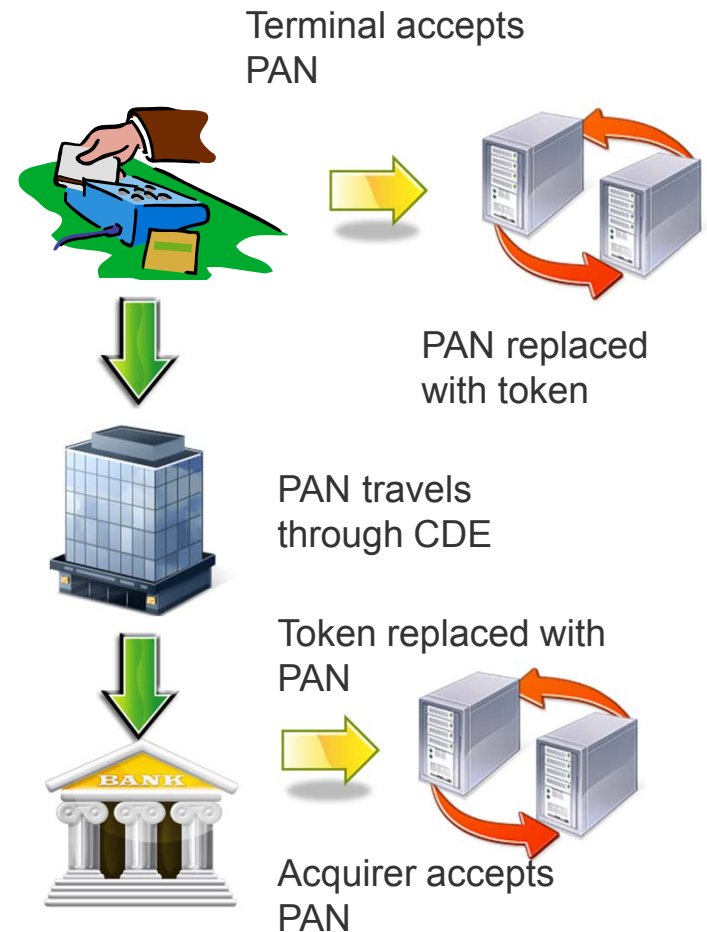
- Or stored/processed/transmitted only in very small zones?
- Doing this, you could create areas where PCI DSS does not apply
- You'd still need to enforce segregation between the places where PANs did still exist, but everything else wouldn't matter (at least for PCI)

- Goal: reduce scope by limiting PANs

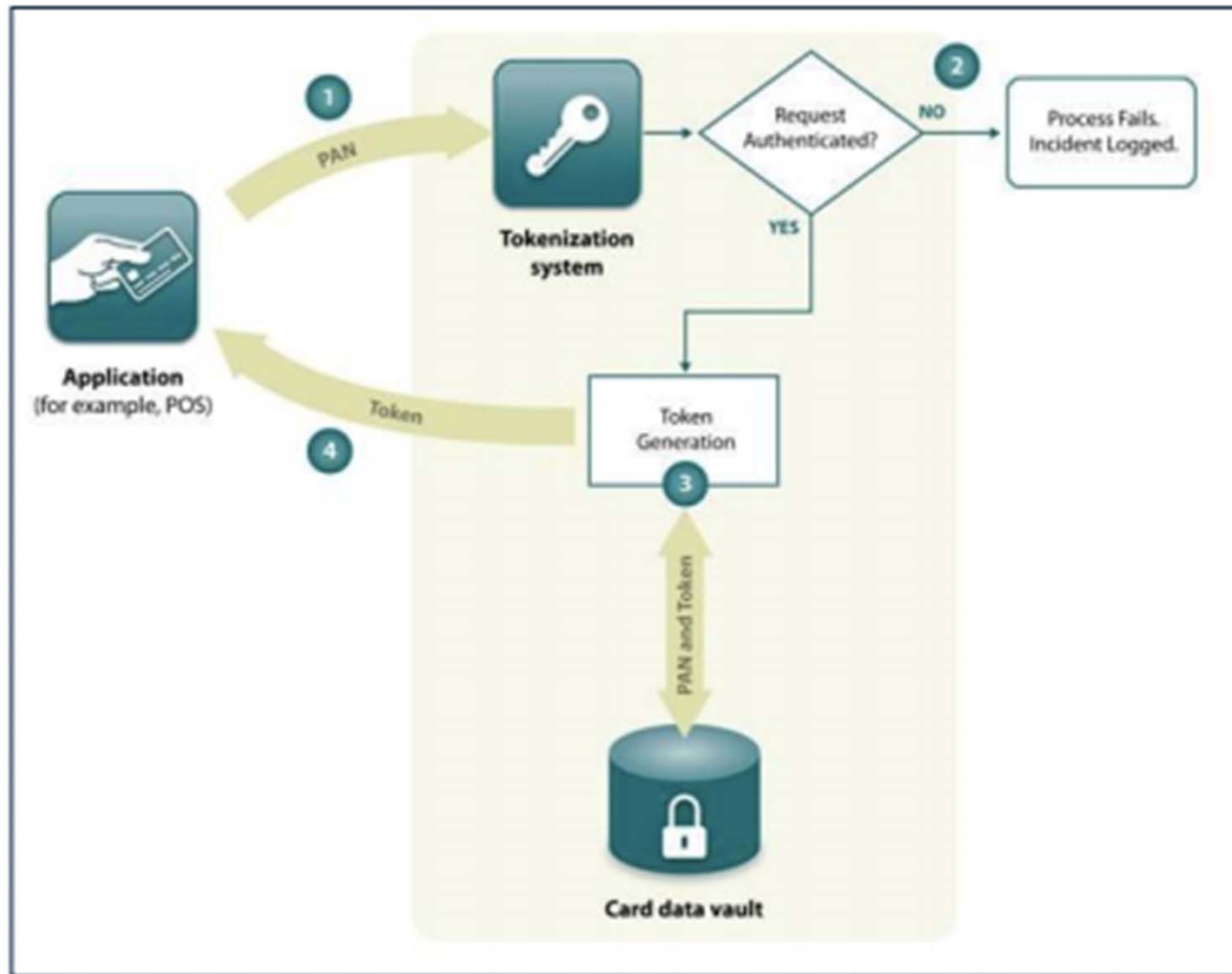
¹“PCI Quick Reference Guide” (https://www.pcisecuritystandards.org/documents/pci_ssc_quick_guide.pdf)

Tokenization

- Not an auth token!
- Replaces PAN
 - A “token” that represents the PAN in a transaction
- Usually done at (or near) payment locality
 - At the POS
 - At eCom transaction point



Tokenization



https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

Figure 1: High-level example of a tokenization process

Tokenization

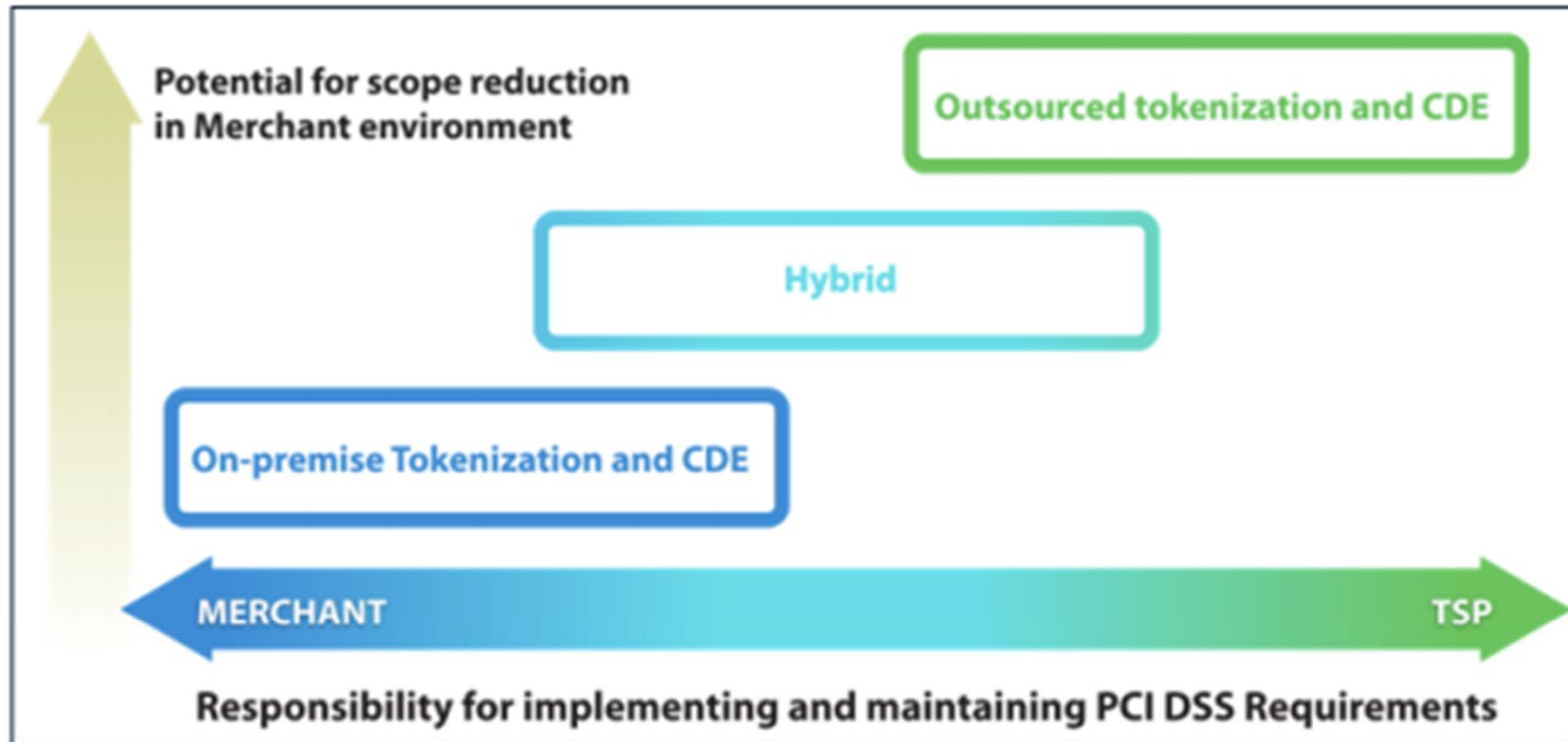


Figure 3: Example of how merchant and TSP responsibilities may be assigned for on-premise, hybrid, and outsourced solutions



Tokenization

What's Not in the Guidance

- Assessment standard for TSPs
 - Certification program for TSPs
 - Merchants and providers must do this themselves
 - Definition of a token
 - Not all tokens are created equal
 - Reversibility v. de-tokenization
-

2012 Special Interest Groups

*IS
End of
2012*

Cloud

- Explore architectures
- Identify risks
- Provide clarification

*IS
End of
2012*

eCommerce Security

- Examine threats
- Discuss roles and responsibilities
- Discuss best practices

*IS
Middle of
2012*

Risk Assessment

- Guidance on documenting risk and potential impact
- Implementing risk-management methodologies

Protecting Telephone-based Payment Card Data

• March 2011

● Call Centers

- *“This call may be monitored or recorded for training purposes.”*
- *“The Contact Center as Police State”*
- QSA recommended
 - *Raise cube walls*
 - *Wall off areas of the center where agents handle credit cards*
 - *Badge agents with different colors based on access levels*

<http://strategiccontact.com/blog/2012/02/the-contact-center-as-a-police-state/>

Lori Blocklund



Other Documents



Skimming Prevention: Best Practices for Merchants

• August 2009

Requirement 6.6 Application Reviews and Web Application Firewalls Clarified v1.2

• August 2009

Requirement 11.3 Penetration Testing v1.2

• August 2009

Protecting Telephone-based Payment Card Data

• March 2011

https://www.pcisecuritystandards.org/security_standards/documents.php

Point-to-Point Encryption



2012 Target Deliverables

General Requirements

- *P2PE Hardware encryption and hardware decryption*
- *P2PE "Hybrid" Hardware encryption and hardware decryption, with transaction keys in software at decryption*
- *P2PE next phase*

Point-to-Point Encryption

- P2PE Assessor Qualification Requirements released
- Testing Procedures now available!
- Program Guide, SAQ and P2PE Assessor training coming soon
- Solutions listing for Fall 2012

Sign up for P2PE Training today:
administration@pcisecuritystandards.org

Mobile Update



2012 Target Deliverables

Guidance and Best Practices

- *Mobile Transactions Using SCR & P2PE for Merchants*
- *Mobile Transactions Using SCR & P2PE for Vendors and Assessors*
- *Mobile Acceptance Best Practices*

Mobile Payment Acceptance Security


- Key areas of focus include:
 - Devices
 - Applications
 - Service Providers

v.3.0?

- Still very early to tell
 - Stage 2: Feedback Begins
 - Stage 3: Feedback Review
- May incorporate some of the SIGs
- Stay tuned to the PCI Council Site and outcomes from the Community Meetings

Conclusions

- DSS is on a 3 year cycle
- But the Council remains active
 - And new SIGs are being published annually
- Recent SIGs of note
 - Virtualization (w/some Cloud recommendations)
 - Tokenization
- To Watch for in 2012
 - Cloud
 - eCommerce
 - Risk Assessment



Diana Kelley
diana@securitycurve.com
@securitycurve



Featured Member of the
TechTarget Editorial
Speaker Bureau