Securing the Future of Payments

PCI Security Standards Council®

What does PCI Security Standards Council Produce?

Standards, Best Practices & Services

Payment **Equipment**

Payment **Software**

Merchant & Payment Service Provider **Environments**

Validation & Qualification – Equipment, Service Providers, Assessors, Investigators

Training – Assessors, Acquirers, Integrators

Growing Cybercrime

58% of Brazil's 200 million citizens are connected to the internet.

The number of cyberattacks grew by **197%** in 2014, and online banking fraud spiked by **40** percent.

Cybercrime causes **95%** of losses for Brazilian banks.

Growing Diversity of Attacks on Payments

- Criminal techniques are becoming less detectable
- POS Malware Growing at Staggering Rate
- ‘Low-tech’ attacks circumventing confidentiality

Future Threat Landscape

- Increasing card not present fraud
- Contactless payments vulnerabilities
- Account takeover
- Extortion

E-commerce growth rate at 25%, with credit cards handling 60% of digital transactions in Brazil.

Card not present fraud already accounts for 80% of fraud in Brazil.

User base for mobile payments in Brazil is predicted to reach 80 million by 2018.

Ultimate Goal

- EMV
- Tokenization
- Point-to-Point Encryption

Devalue Data
make it useless for criminals

PCI DSS is the Foundation

- ✓ Keep the bad guys out
- ✓ Set up your systems properly
- ✓ If you must have data then protect it
- ✓ If you must send data then encrypt it
- ✓ Protect yourself against malware and other attacks
- ✓ Build your software properly and securely
- ✓ Keep access to the card data to a minimum
- ✓ Make sure people are who they say they are
- ✓ Physical security is just as important
- ✓ Track who goes where and what they do
- ✓ Test and check everything is working correctly
- ✓ Make sure everyone knows what is required

PCI DSS 3.2 Update – April 2016

Market drivers:

- Threat and Payment Landscape
- SSL/TLS Updates to v3.1

Key changes:

- Multi-Factor Authentication
- Service Provider Updates
- SSL/TLS Sunset Dates

The Council updates PCI Standards to continue to protect against existing exploits, while also addressing new attacks on cardholder data.

Protecting Internet Payments

Stolen credit card information is one of the main concerns of internet payment users in Brazil.

Man-in-the middle attacks is one of biggest threats during online transactions.

Small e-commerce merchants in Brazil are highly vulnerable to attack.

- SSL/early TLS migration
- Development of safe e-commerce practices
- Evaluation of PCI DSS requirements for specific environments
- Simplified guidance for small e-commerce merchants

Best Practices for Safe e-Commerce

2016 Special Interest Group project to provide guidance for merchants, third parties and assessors

Guidance will be update to 2012 Special Interest Group information supplement on e-commerce

Topics covered will include use of encryption and digital certificates and questions to ask e-commerce solution providers

PCI Point-to-Point Encryption (P2PE) v2

- Consolidated the P2PE version 1 standards
- New function-specific domains to support P2PE component providers
- Introduced merchant-managed solutions (MMS)

P2PE for Merchants

PCI Point-to-Point Encryption (P2PE) Solutions for Merchants

Protecting your customers and your corporate brand continue to be the biggest challenges faced by IT executives. To meet that challenge, we've worked with a P2PE service provider to adopt a PCI-validated P2PE payment solution across all our stores in a simplified and cost effective way.

Bill Bolton, VP of Information Technology, The HoneyBaked Ham Co.

- **Lab-tested products and providers guarantee the strongest encryption protections**
- **Simplifies the PCI DSS compliance process**

How Criminals Hack Phones

- Cellular (e.g., Stingray or Cloning)
- Wi-Fi
- Proximity Capture
- Malware
- Side-channel/Data Leakage

Protecting the MPOS

Tokenization

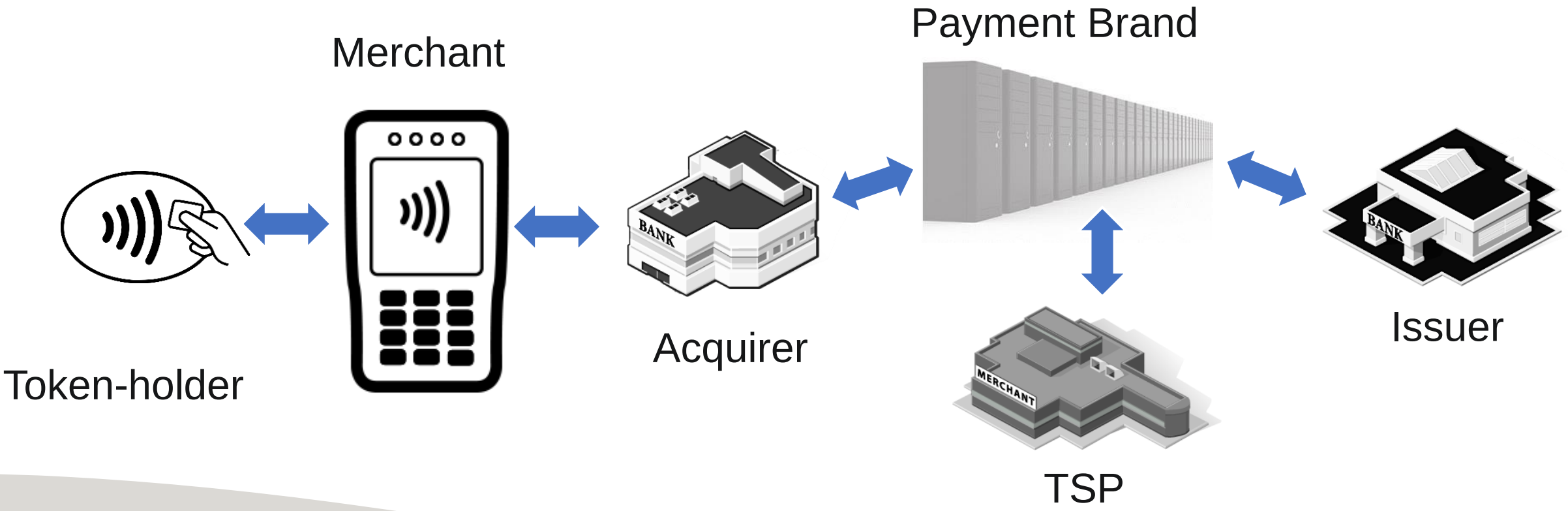
Apple Pay

Samsung Pay

Mobile Wallets

New Token Service Provider Standard

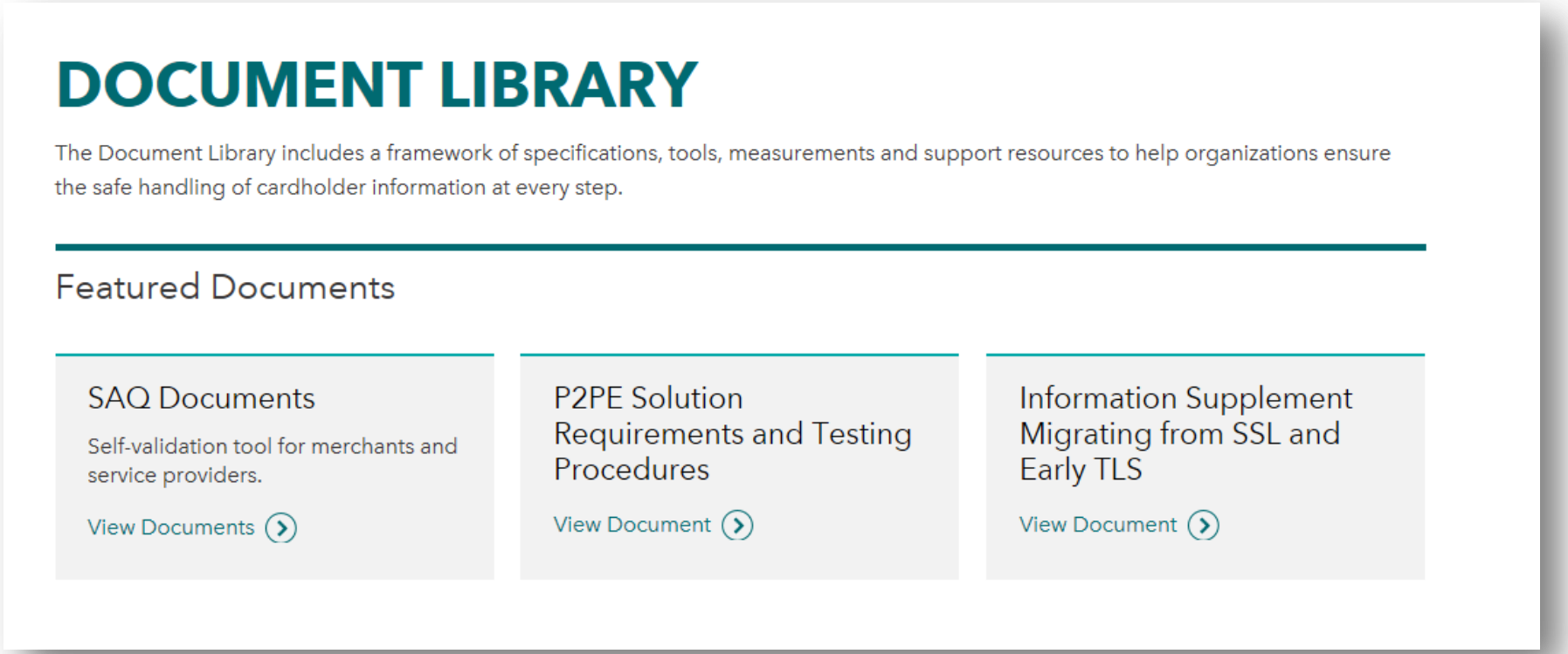
Released new standard December 2015 to address Token Service Provider environments



Securing the Future - Mobile

- ✓ Continue evaluation of PIN-entry use for mobile consumer devices
- ✓ Complete new requirements for over-the-air provisioning
- ✓ Complete support documents for Token Service Provider standard
- ✓ FAQs and promotion of payment tokens and P2PE for use in mobile payments

Resources



Check Our Document Library for New Resources

www.pcisecuritystandards.org

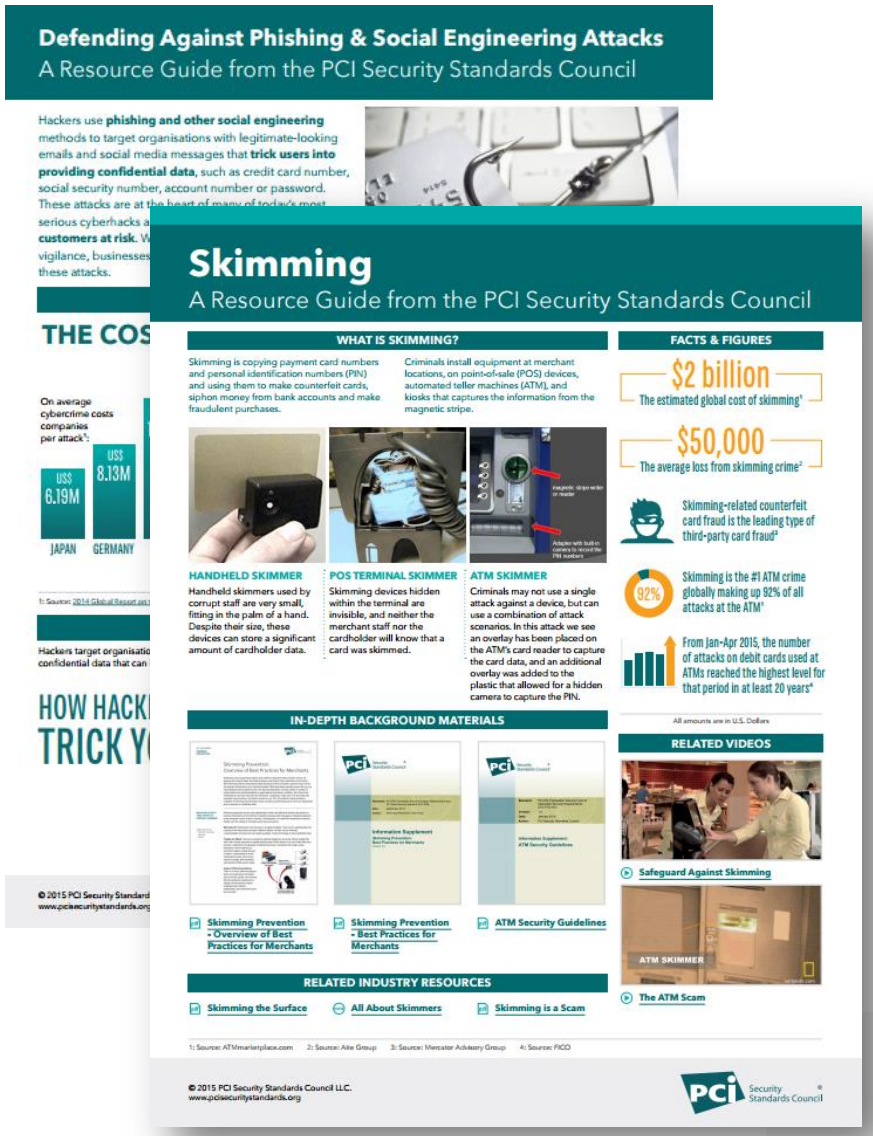
Portuguese Translations

- Now available!
  - PCI DSS Version 3.2 Summary of Changes
  - PCI DSS Version 3.2 Self-Assessment Questionnaires (SAQ)

Available at: www.pcisecuritystandards.org/document_library

- Translation partners needed!
  - Contribute translations for PCI DSS 3.2, PA-DSS 3.2 and supporting documents

PCI Guidance and Best Practices



- Protecting against malware
- Skimming prevention
- ATM security guidelines
- Defending against phishing attacks
- Working with third parties
- Building a security awareness program
- Accepting payments with a mobile phone
- PCI DSS compliance in the cloud

Available at: www.pcisecuritystandards.org

Acquirer Resources

Acquirer Training

- For acquirers and processors who don't perform assessments themselves, but need to understand the compliance process for their merchant clients
- Any acquirer can benefit – no previous PCI knowledge is required
- Eight training modules cover all of the relevant information about PCI DSS and related programs
- Available as instructor-led and eLearning

Acquirer Checklist

- Optional
- Developed by Assessor Quality Management
- Basic version
- Detailed version

www.pcisecuritystandards.org/program_training_and_qualification

Training and Education

Personal PCI training is essential to keep on top of emerging threats

PCI training by the Council is the most effective, targeted way to accelerate mastery and stay current

Validation proves your value to your employer and sets you apart from so-called “experts”

To learn more, visit: www.pcisecuritystandards.org/program_training_and_qualification

Partner with the Council

We Need You!

Save $1500 USD / 5078 BRL on a PCI Participating Organization membership

PCI PO Discount Code: Brazil16

Join us: www.pcisecuritystandards.org/get_involved/participating_organizations

Participating Organization Benefits

- Advance review of standards and supporting materials before release, with the opportunity to provide feedback
- Complimentary attendance at annual **Community Meetings** hosted by the Council
- Substantial training discounts; courses are offered in instructor-led and eLearning formats
- Nominate and vote for representatives to stand for election to the Council's **Board of Advisors**
- Drive the **Special Interest Groups (SIGs)** that provide the Council with understanding and guidance on particular topics or technologies

Join us: www.pcisecuritystandards.org/get_involved/participating_organizations

Mark Your Calendar
2016 Community Meetings

North America
Las Vegas, NV, USA
20 - 22 September

Europe
Edinburgh, Scotland
18 - 20 October

Asia-Pacific
Singapore
16 - 17 November


Please visit our website at
www.pcisecuritystandards.org