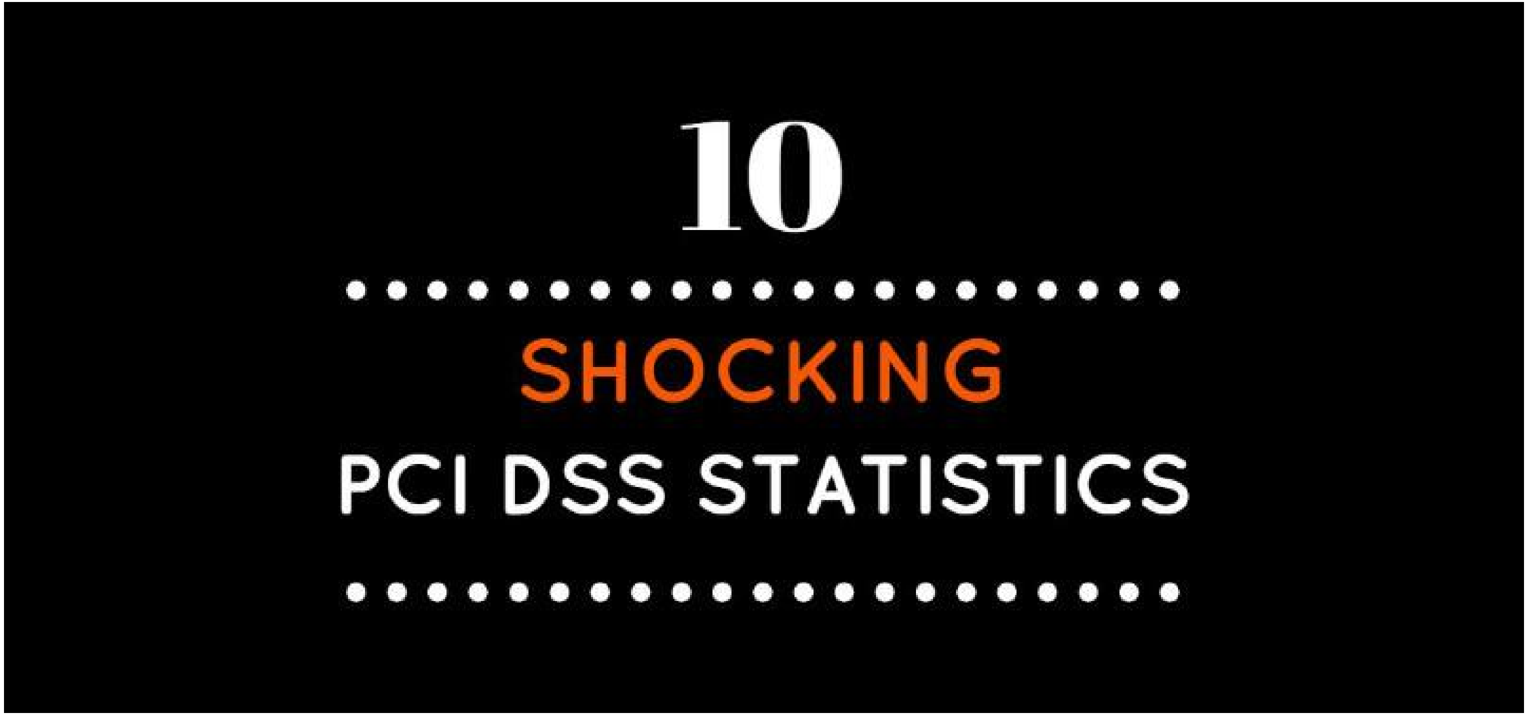
Olivier Yiptong / Nov 2017 / TPAC Burlingame

Encrypted Card

PCI DSS Compliance Horror Stories, BuzzFeed style



10

SHOCKING

PCI DSS STATISTICS

PCI DSS Compliance Horror Stories, BuzzFeed Style

https://www.goanywhere.com/blog/2017/02/03/8-shocking-pci-compliance-statistics

1. PCI DSS compliance has increased by 167% since 2012
2. 80% of organizations are still not compliant
3. Only 26% of news media executives feel confident their businesses are compliant
4. Only 29% of companies are compliant a year after validation
5. You could pay $100,000 a month for being non-compliant...or much more
6. None of the companies breached during Verizon’s investigations were fully compliant
7. 39% of organizations were breached through insecure remote access
8. The average total cost of a data breach is $4 Million
9. 69% of consumers would be less inclined to do business with a breached organization
10. The average merchant, at the time of data compromise, wasn't compliant with at least 47% of PCI DSS requirements

Key Takeaways

- Security is hard 😓
- □ Hard to become compliant, hard to stay compliant 😫
- 🤯 Bad for brand, bad for business, bad for bank account 💸💸💸

Conclusions on PCI Compliance

- Compliance is a helpful assessment
- Reduce Scope we must: the least exposure the better it is

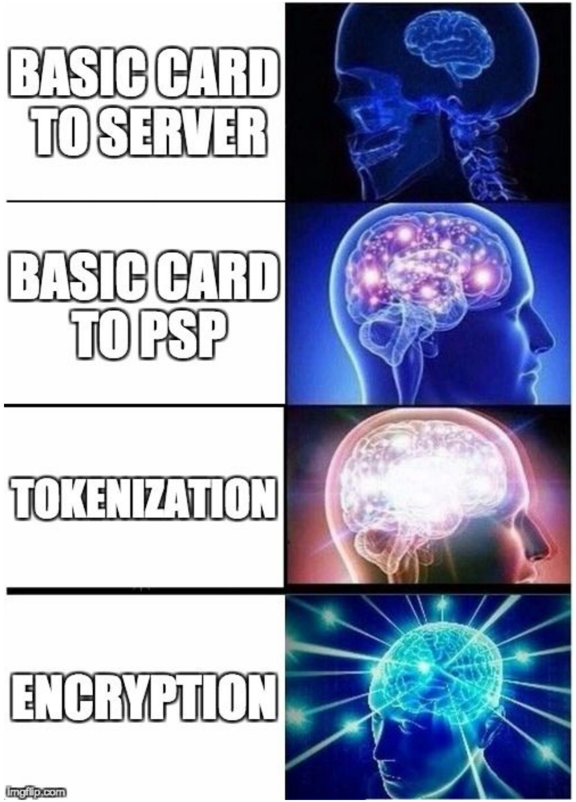
PCI DSS 3.2 SAQ Validation

Validation Type	Eligibility Criteria	ASV Scan 💵	Penetration Test 💰💰💰	# of questions 😠
A	* Card-not-present * Fully outsourced processing (iframe, redirect) * No storage	No	No	22
A-EP	* E-commerce * Fully outsourced processing (iframe, redirect, in-page API) * No storage * Elements from merchant site	Yes	Yes	191
D		Yes	Yes	329

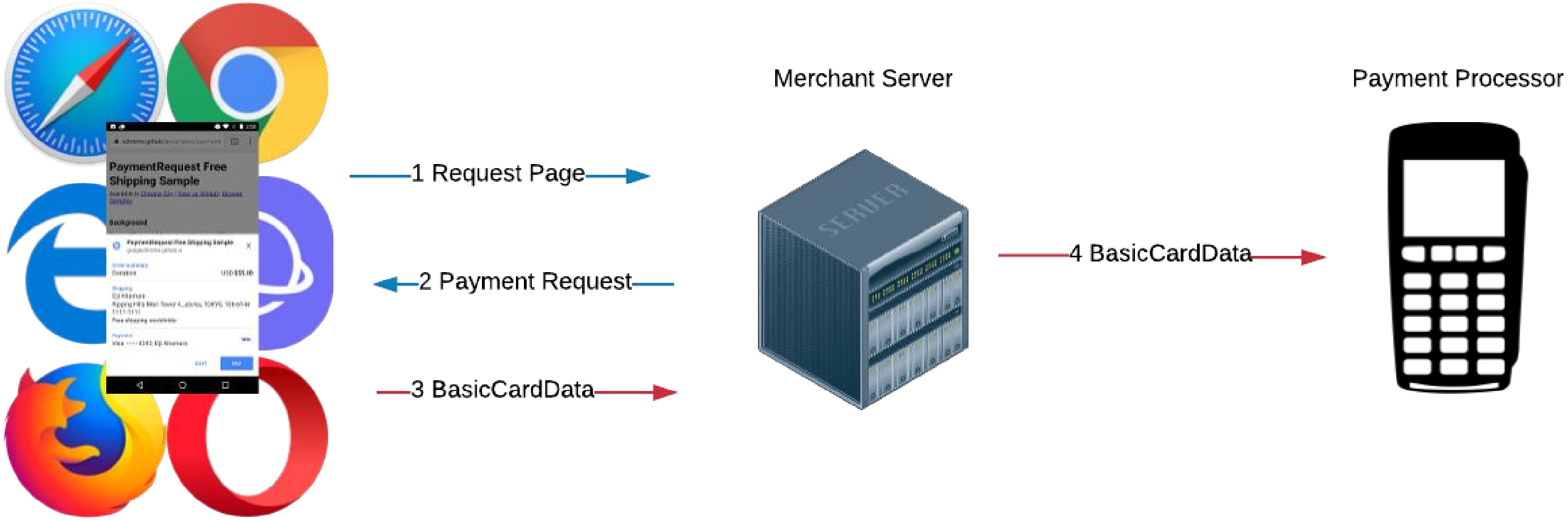
Payment Request API

- BasicCard usage requires SAQ A-EP at minimum
- Possible to pass SAQ-A using payment handlers

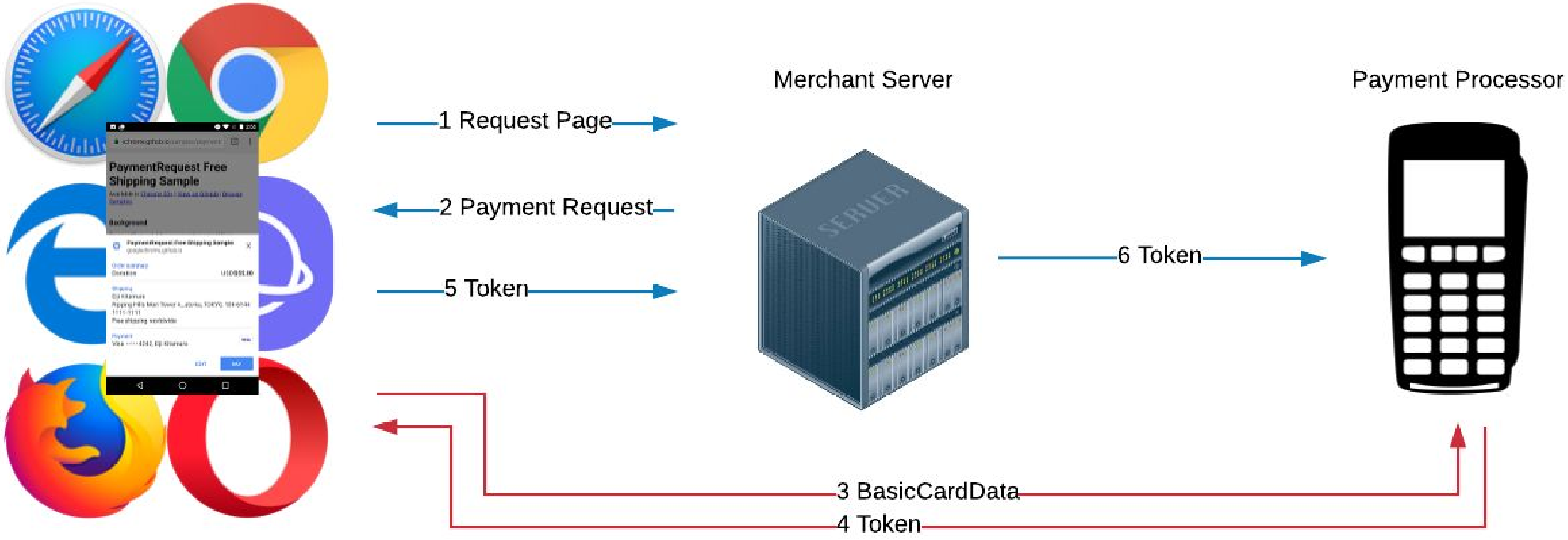
Journey


BASIC CARD TO SERVER
BASIC CARD TO PSP
TOKENIZATION
ENCRYPTION
imgflip.com

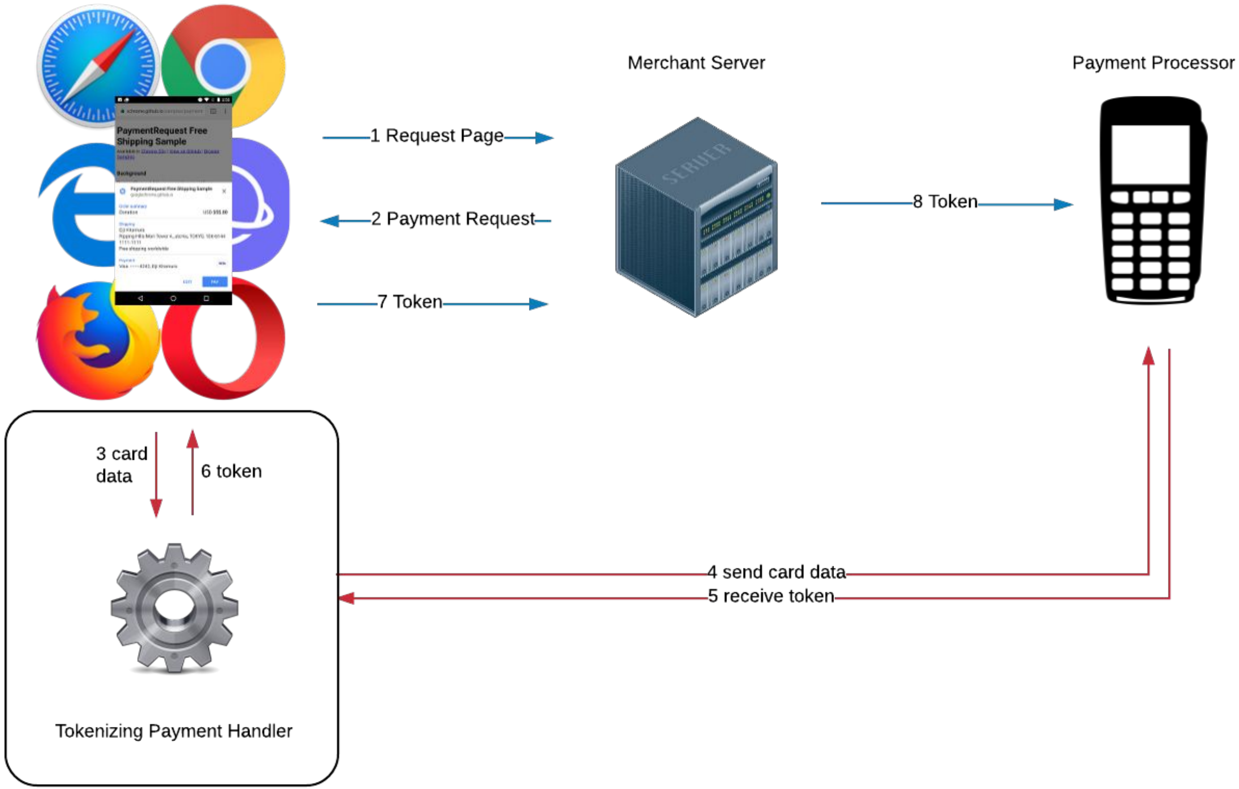
BasicCard To Server



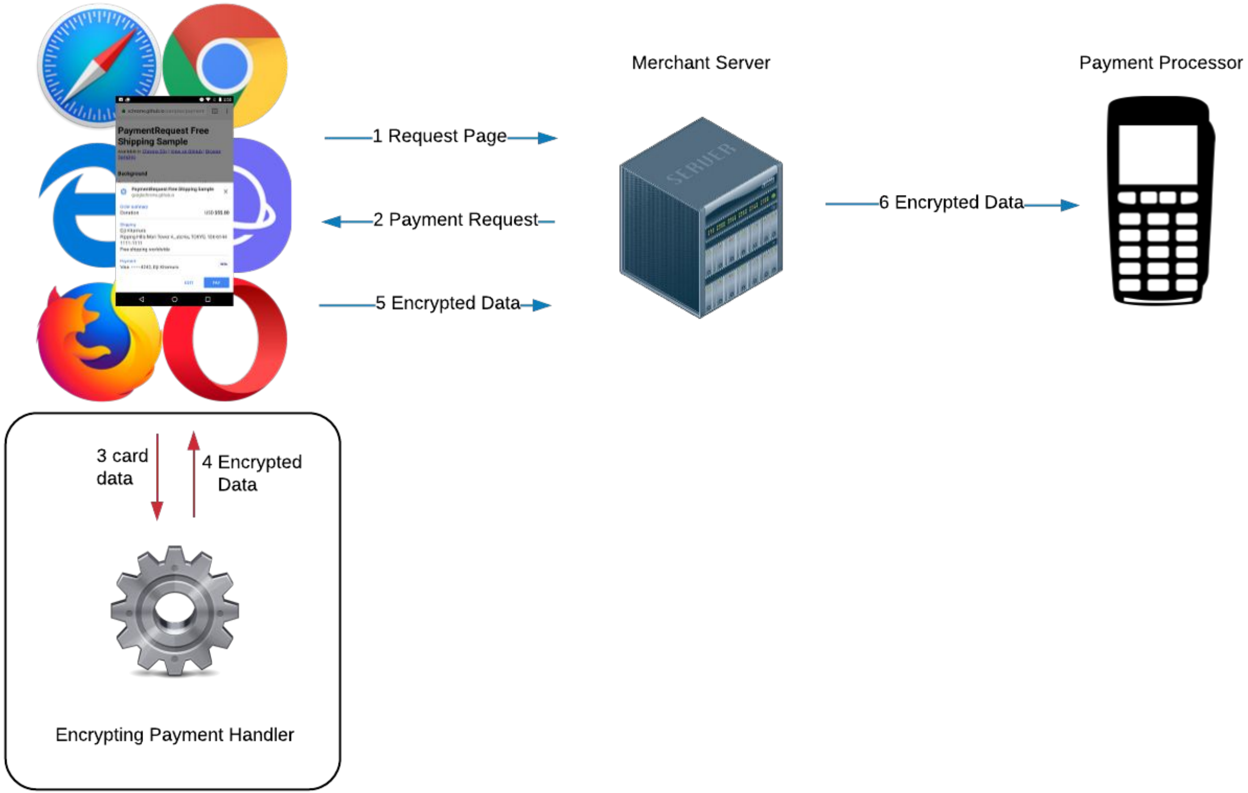
BasicCard To PSP



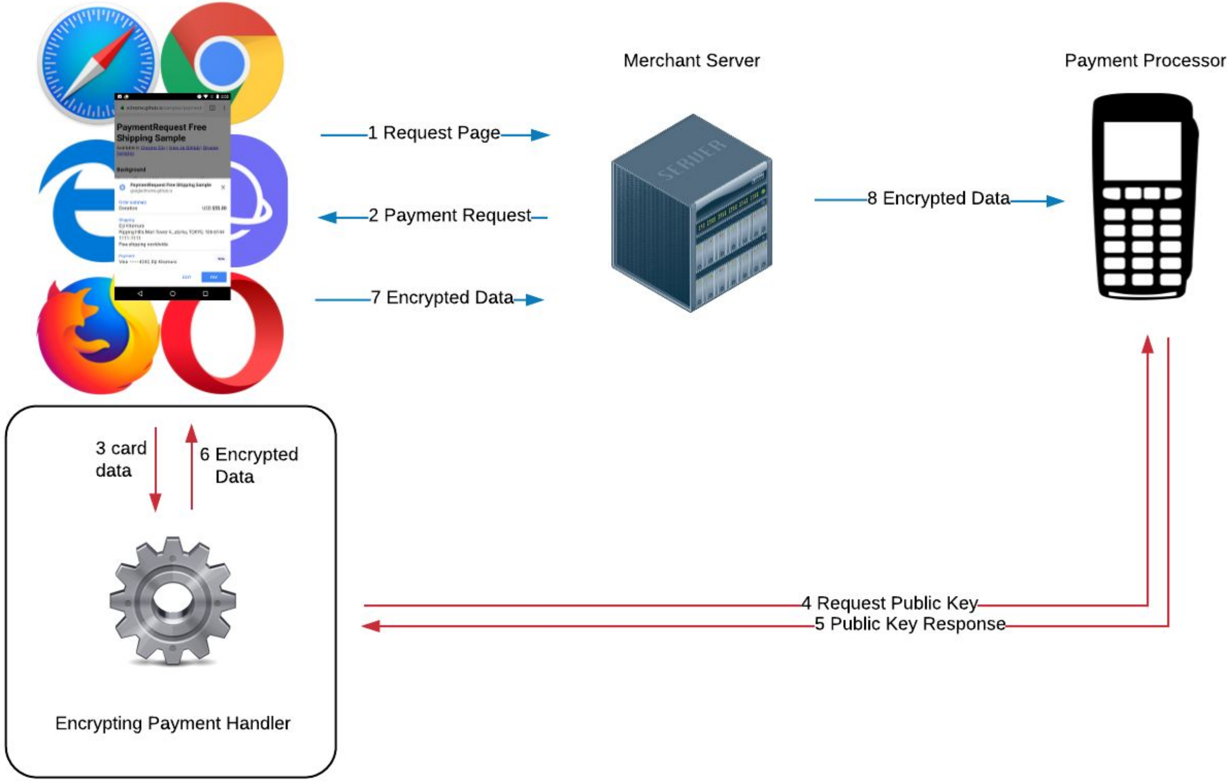
Tokenization



Encryption


PaymentRequest Free Shipping Sample
Background
Merchant Server
Payment Processor
1 Request Page
2 Payment Request
5 Encrypted Data
6 Encrypted Data
3 card data
4 Encrypted Data
Encrypting Payment Handler

Encryption with Server PK Load



Live Demo

Encrypted Card Proposal in a gist

- Reduced PCI Scope: SAQ-A
- Cheap to implement
- Low merchant activation cost for PaymentRequest
- Returns an encrypted payload containing BasicCardResponse’s data
- Market Adoption 🚀🚀🚀

Next Steps

- Deserves BasicCard treatment
  - Autofill
  - First class support
  - Availability
- Links:
  - https://oyiptong.github.io/payment_handler_demo/handler/
  - https://github.com/w3c/webpayments-methods-tokenization/wiki/encrypted_card