Encrypted Card
PCI DSS Compliance Horror Stories, BuzzFeed style
PCI DSS Compliance Horror Stories, BuzzFeed Style

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

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

<table>
<thead>
<tr>
<th>Validation Type</th>
<th>Eligibility Criteria</th>
<th>ASV Scan</th>
<th>Penetration Test</th>
<th># of questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>* Card-not-present&lt;br&gt;* Fully outsourced processing (iframe, redirect)&lt;br&gt;* No storage</td>
<td>No</td>
<td>No</td>
<td>22</td>
</tr>
<tr>
<td>A-EP</td>
<td>* E-commerce&lt;br&gt;* Fully outsourced processing (iframe, redirect, in-page API)&lt;br&gt;* No storage&lt;br&gt;* Elements from merchant site</td>
<td>Yes</td>
<td>Yes</td>
<td>191</td>
</tr>
<tr>
<td>D</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>329</td>
</tr>
</tbody>
</table>
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
BasicCard To Server

1. Request Page
2. Payment Request
3. BasicCardData
4. BasicCardData

Merchant Server

Payment Processor
BasicCard To PSP

1. Request Page
2. Payment Request
5. Token
3. BasicCardData
4. Token
6. Token

Merchant Server

Payment Processor
Tokenization

1. Request Page
2. Payment Request
3. Card Data
4. Send Card Data
5. Receive Token
6. Token
7. Token
8. Token

Merchant Server

Payment Processor

Tokenizing Payment Handler
Encryption

1. Request Page
2. Payment Request
3. Card Data
4. Encrypted Data
5. Encrypted Data

Merchant Server

6. Encrypted Data

Payment Processor

Encrypting Payment Handler
Encryption with Server PK Load
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