DATACOM

Payment Gateways

The Most Dangerous Game

Stephen Morgan
2021 AppSec New Zealand Conference

$ whoami

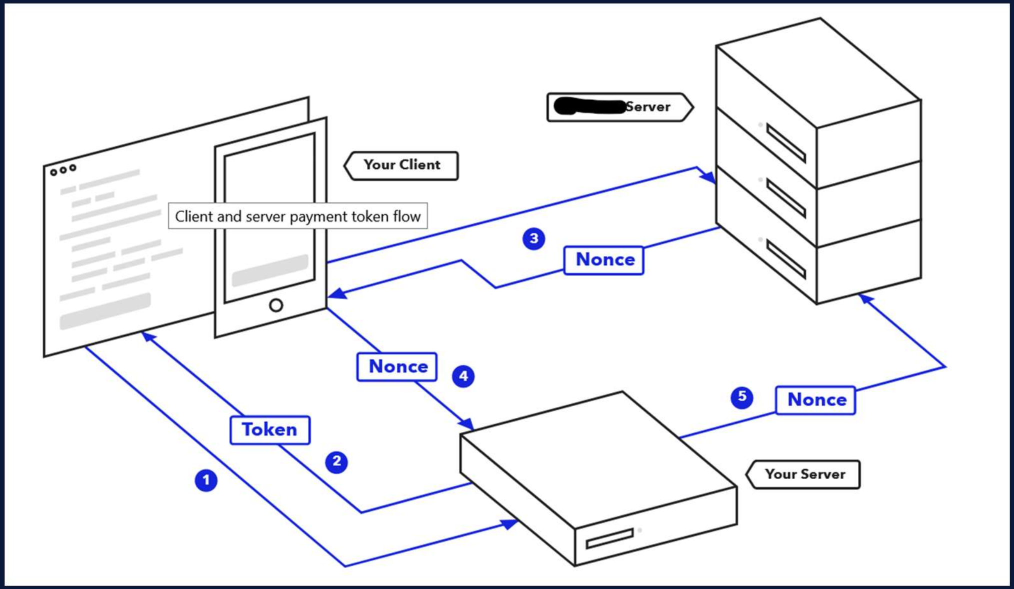
- Application Security Consultant @AppSec Datacom

- Background in Technical Security Consulting
    - Penetration Tester (OSCP circa 2016)
    - Dev(Sec)Ops Engineer
    - Security Architecture

- …and recent Consultant to a Payments Gateway

The Most Dangerous Game

- Important Concepts
- What are Payment Gateways?
- PCI Compliance
- Implementations
  - Recommended
  - Not recommended
- Summary



Important Concepts

Payment Gateways

- Don’t trust the client
  - Maintain integrity between services

- PCI Compliance is a pain
  - Lowing your compliance requirements

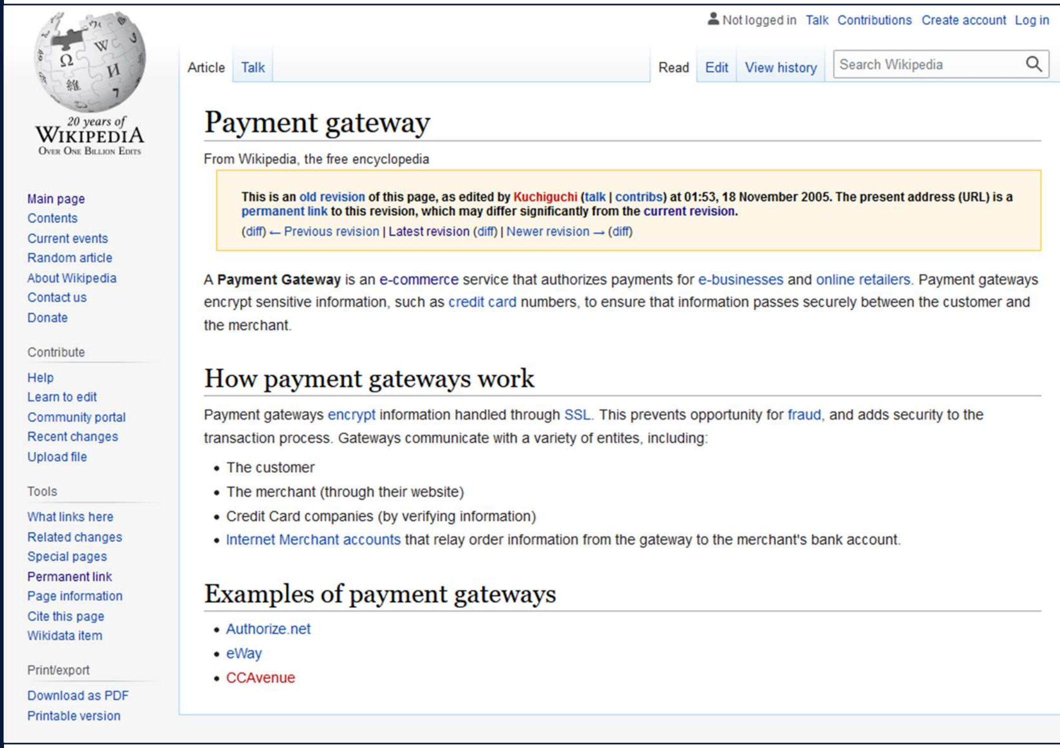
What are Payment Gateways?

- Accept payments so you don't have to

1. "add security to the transaction process"
2. Validate and charge payment method
3. Transfer funds to merchant

Involves:

- Customer (interweb)
- Merchant (you?)
- Payments Gateway
- Banking entity (via gateway)



Payment gateway

From Wikipedia, the free encyclopedia

This is an old revision of this page, as edited by Kuchiguchi (talk | contribs) at 01:53, 18 November 2005. The present address (URL) is a permanent link to this revision, which may differ significantly from the current revision.

(diff) ← Previous revision | Latest revision (diff) | Newer revision → (diff)

A **Payment Gateway** is an e-commerce service that authorizes payments for e-businesses and online retailers. Payment gateways encrypt sensitive information, such as credit card numbers, to ensure that information passes securely between the customer and the merchant.

How payment gateways work

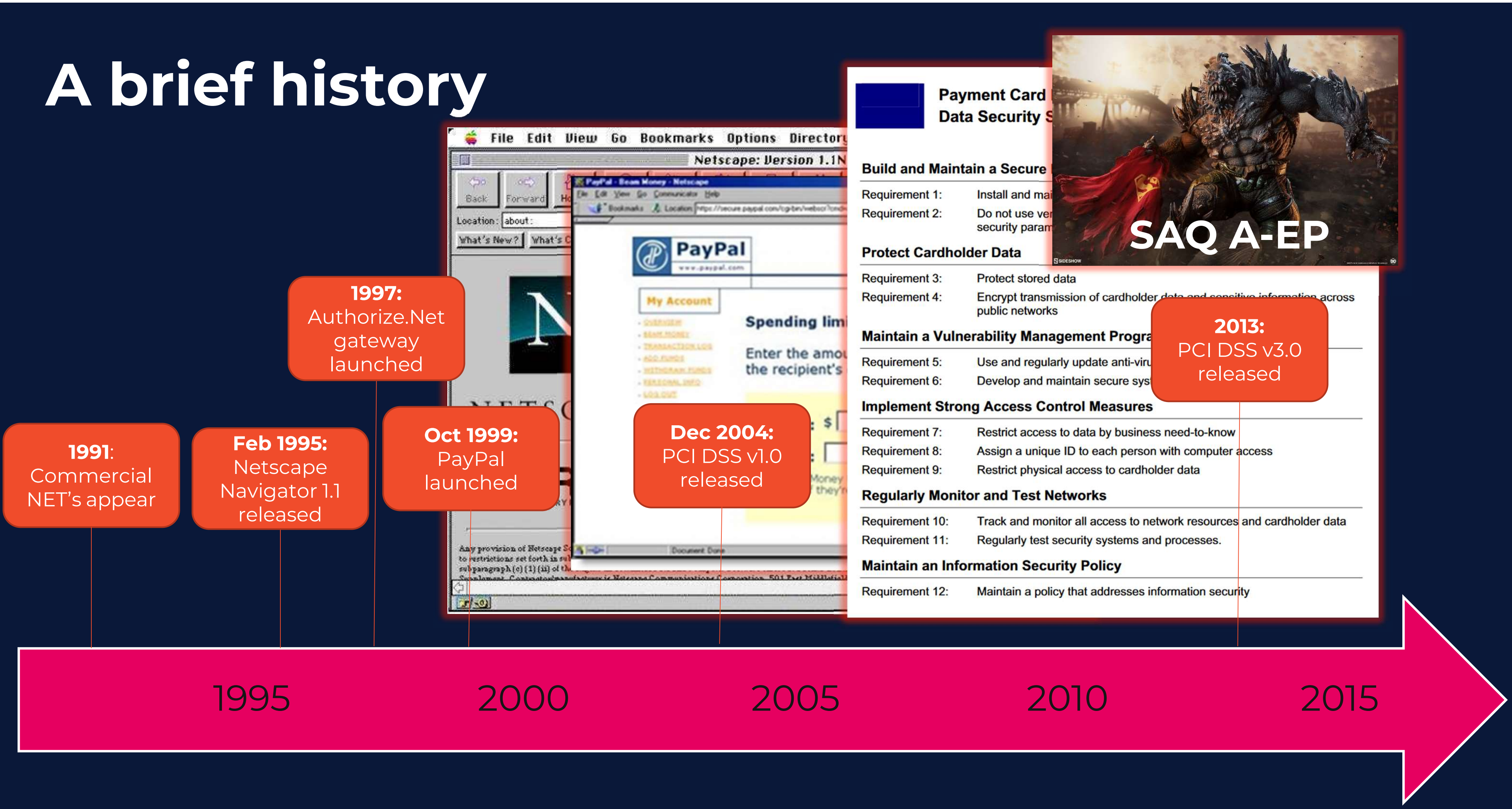
Payment gateways encrypt information handled through SSL. This prevents opportunity for fraud, and adds security to the transaction process. Gateways communicate with a variety of entites, including:

- The customer
- The merchant (through their website)
- Credit Card companies (by verifying information)
- Internet Merchant accounts that relay order information from the gateway to the merchant's bank account.

Examples of payment gateways

- Authorize.net
- eWay
- CCAvenue

A brief history



1991: Commercial NET's appear

Feb 1995: Netscape Navigator 1.1 released

1997: Authorize.Net gateway launched

Oct 1999: PayPal launched

Dec 2004: PCI DSS v1.0 released

2013: PCI DSS v3.0 released

Any provision of Netscape S… to restrictions set forth in su… subparagraph (c) (1) (ii) of th… Supplement. Contractor/manufacturer is Netscape Communications Corporation, 501 East Middlefield

Payment Card Data Security S

Build and Maintain a Secure

Requirement 1: Install and mai

Requirement 2: Do not use ver security param

Protect Cardholder Data

Requirement 3: Protect stored data

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Progra

Requirement 5: Use and regularly update anti-viru

Requirement 6: Develop and maintain secure sys

Implement Strong Access Control Measures

Requirement 7: Restrict access to 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

Regularly Monitor and Test Networks

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

Requirement 11: Regularly test security systems and processes.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

PCI Compliance and You

Scope

> *“Scoping involves the identification of people, processes, and technologies that interact with or could otherwise impact the security of Cardholder Data”*
>
> - Guidance for PCI DSS Scoping and Network Segmentation, 2016

PCI Compliance and You

Self-Assessment Questionnaire

SAQ A

14

REQUIREMENTS

- Ecommerce pages are delivered from Payment Service Provider

SAQ A-EP

139

REQUIREMENTS

- Partially outsourced ecommerce solution
- Merchants site controls pathway to payment (direct post)

SAQ D

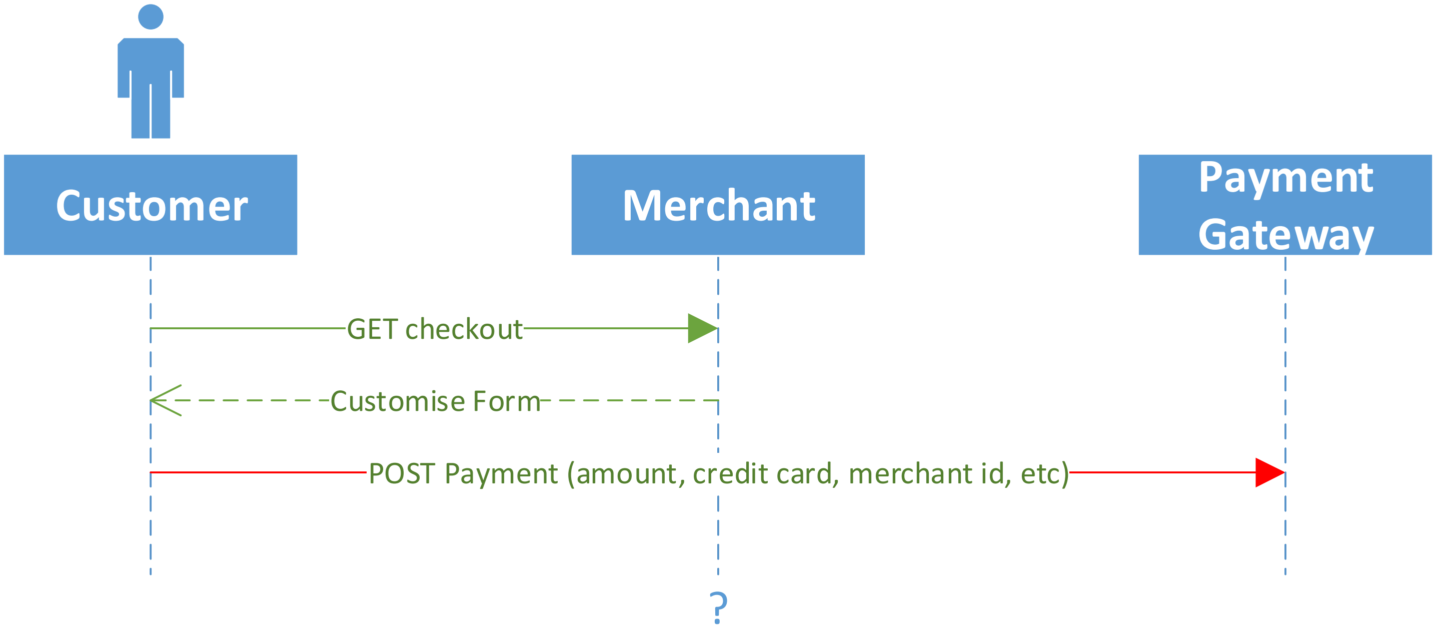
335

REQUIREMENTS

- Ecommerce merchant accepts payment directly on website

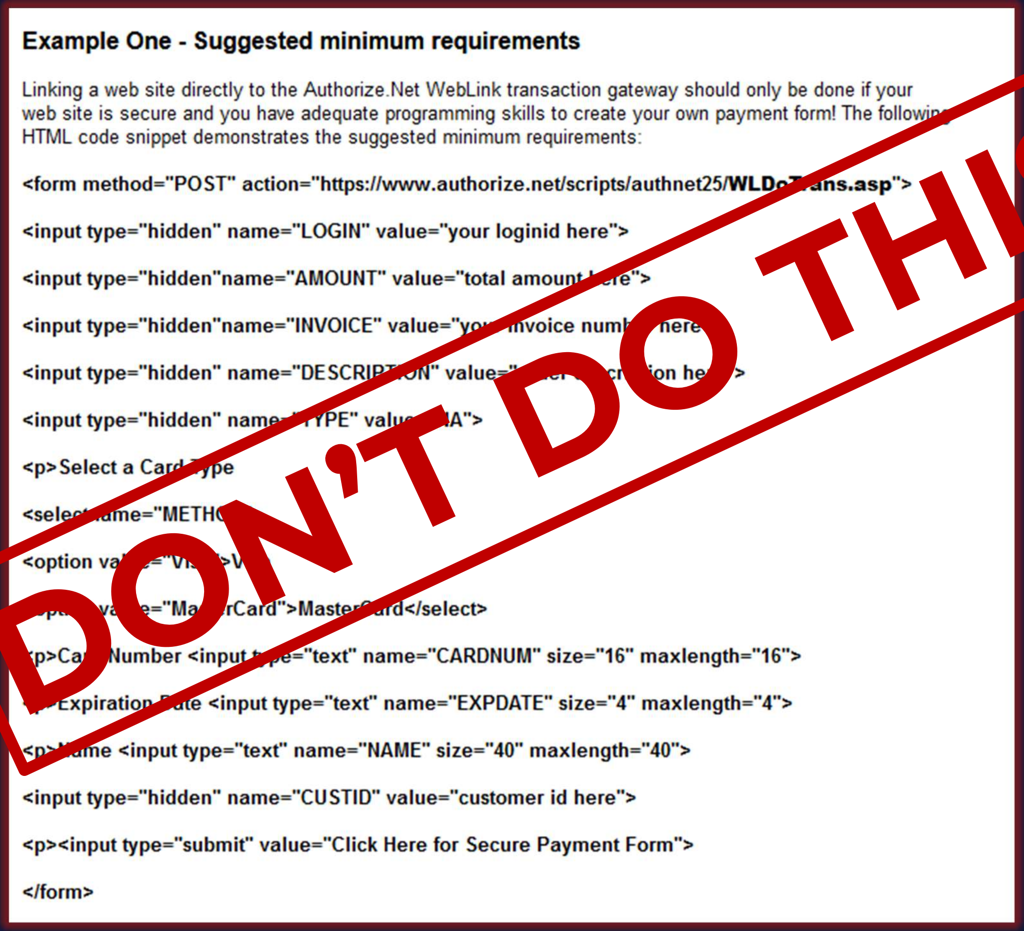
Integrations

Direct Post



Integrations

Direct Post



Example One - Suggested minimum requirements

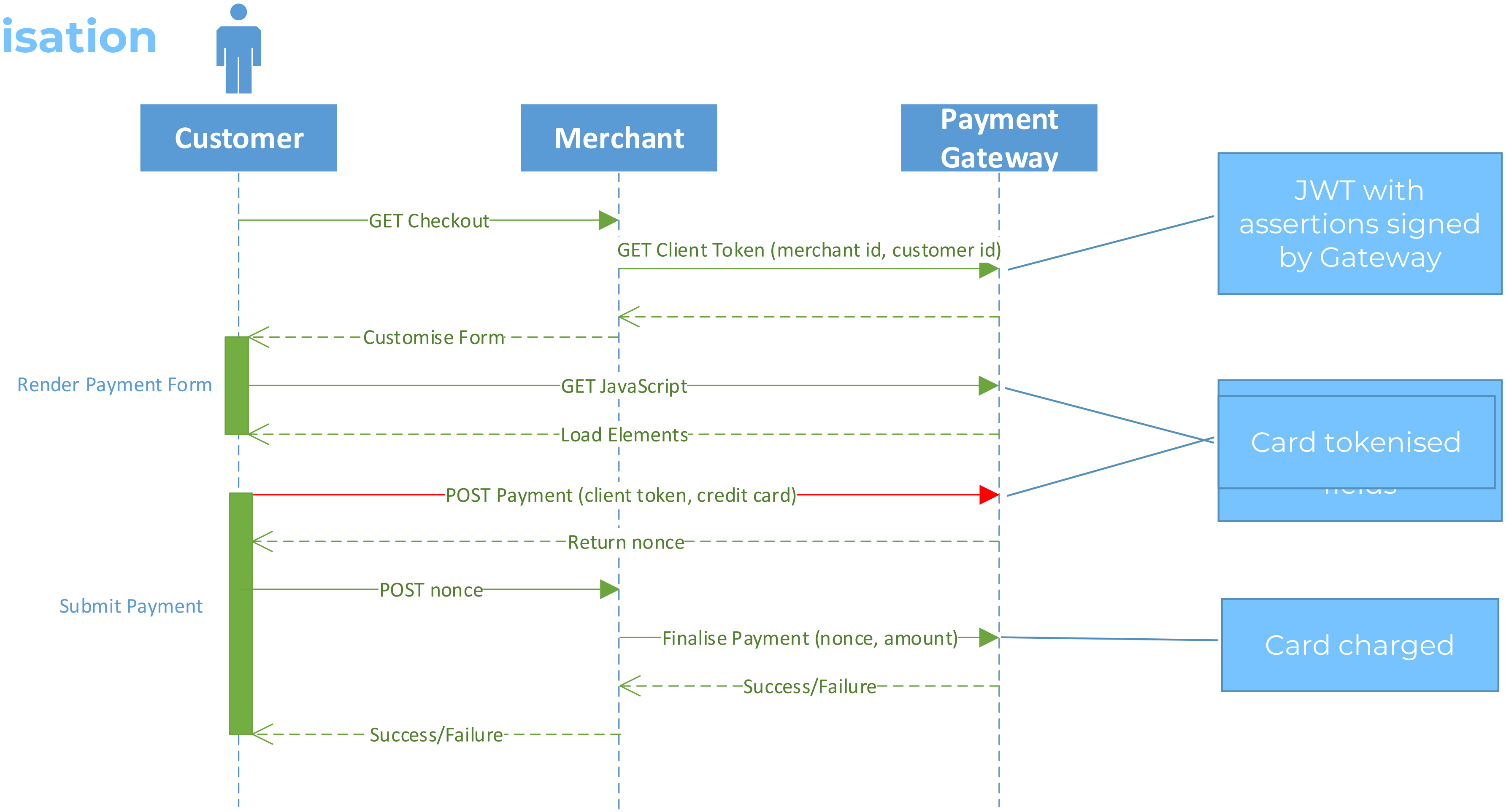
Linking a web site directly to the Authorize.Net WebLink transaction gateway should only be done if your web site is secure and you have adequate programming skills to create your own payment form! The following HTML code snippet demonstrates the suggested minimum requirements:

```
<form method="POST" action="https://www.authorize.net/scripts/authnet25/WLDoTrans.asp">

<input type="hidden" name="LOGIN" value="your loginid here">

<input type="hidden"name="AMOUNT" value="total amount here">

<input type="hidden"name="INVOICE" value="your invoice number here">

<input type="hidden" name="DESCRIPTION" value="[illegible] description here">

<input type="hidden" name="TYPE" value="[illegible]A">

<p>Select a Card Type

<select name="METHO[illegible]

<option value="VI[illegible]>V[illegible]

<option value="MasterCard">MasterCard</select>

<p>Card Number <input type="text" name="CARDNUM" size="16" maxlength="16">

<p>Expiration Date <input type="text" name="EXPDATE" size="4" maxlength="4">

<p>Name <input type="text" name="NAME" size="40" maxlength="40">

<input type="hidden" name="CUSTID" value="customer id here">

<p><input type="submit" value="Click Here for Secure Payment Form">

</form>
```

DON'T DO THIS

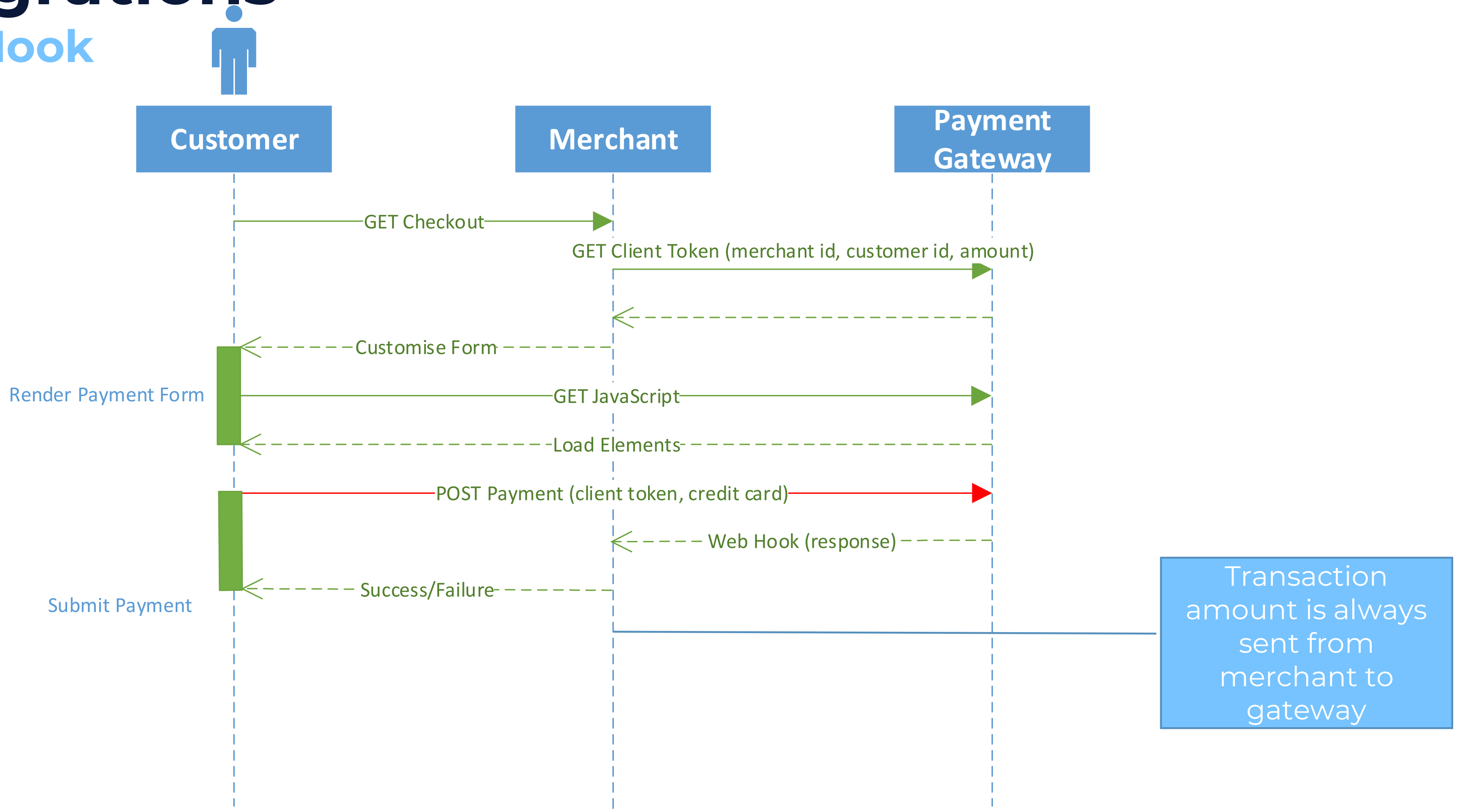
Implementations

Tokenisation



Integrations

Web Hook

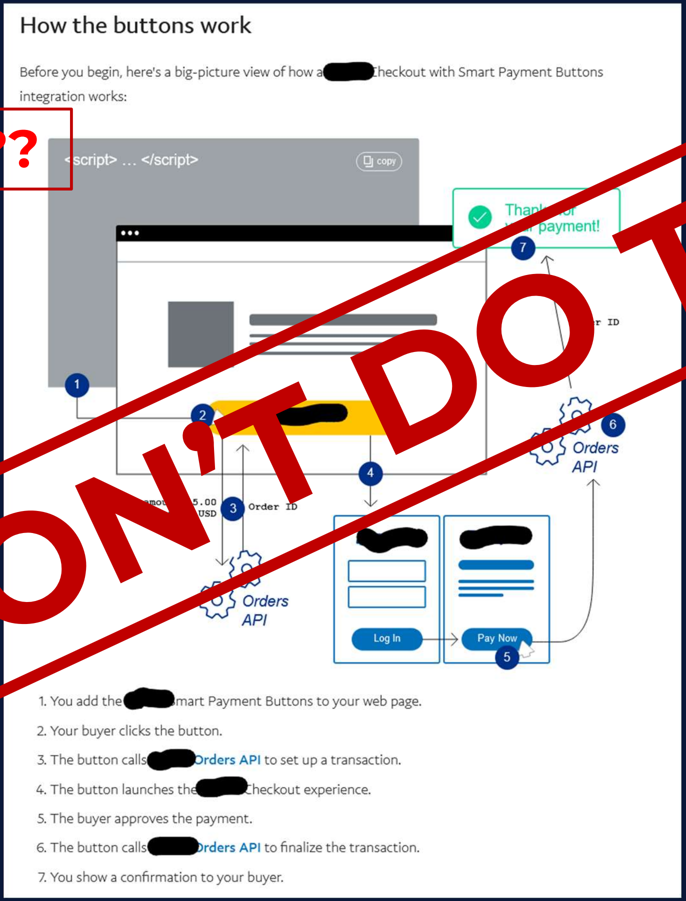


Transaction amount is always sent from merchant to gateway

Integrations

Dishonorable Mention

CLIENT ONLY SDK??



How the buttons work

Before you begin, here's a big-picture view of how a [redacted]heckout with Smart Payment Buttons integration works:

1. You add the [redacted]mart Payment Buttons to your web page.
2. Your buyer clicks the button.
3. The button calls [redacted]Orders API to set up a transaction.
4. The button launches the [redacted]heckout experience.
5. The buyer approves the payment.
6. The button calls [redacted]rders API to finalize the transaction.
7. You show a confirmation to your buyer.

DON'T DO THIS

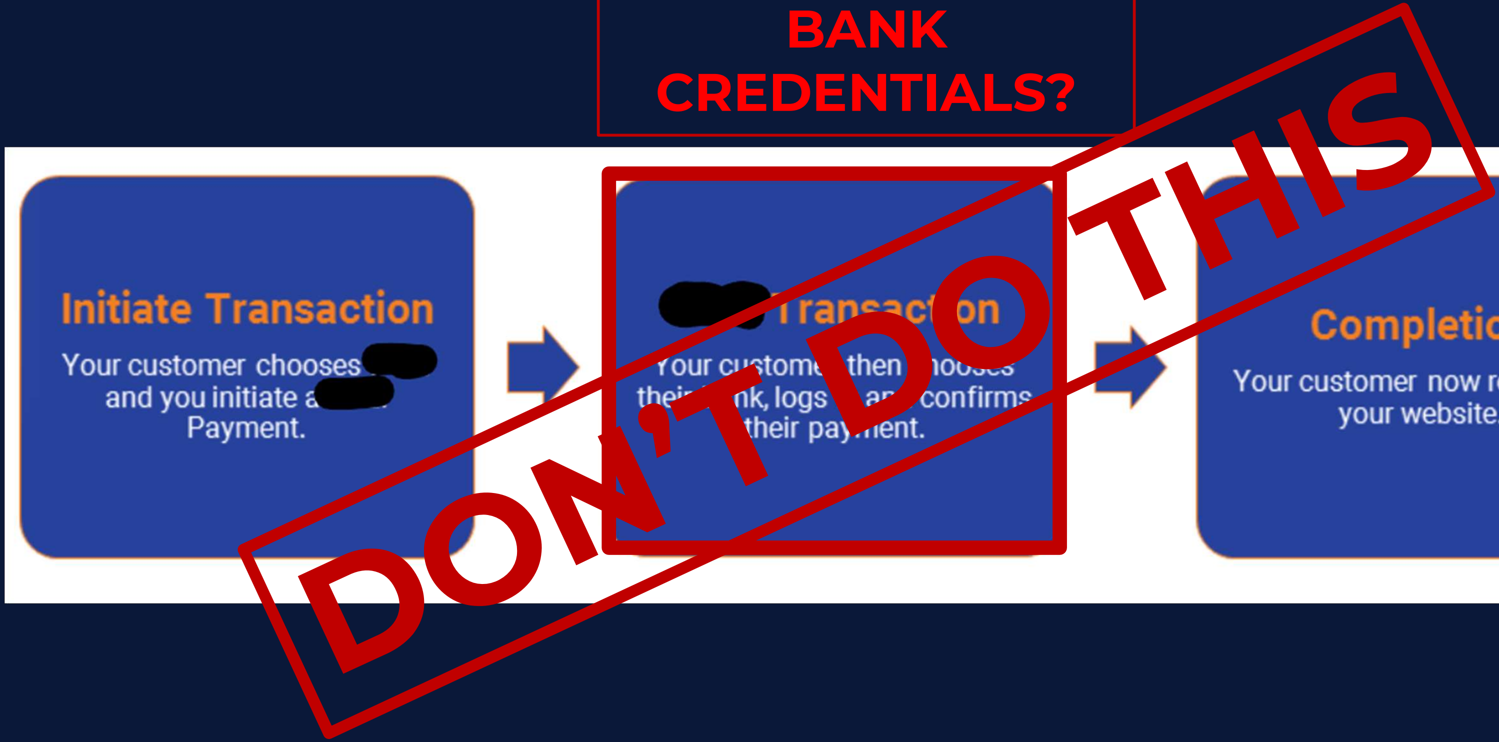
BURIED VALIDATION IN YOUR DOCUMENTATION???

© 2020 Datacom

Integrations

Dishonorable Mention

REQUIRE CUSTOMERS TO GIVE YOU THEIR BANK CREDENTIALS?



Initiate Transaction

Your customer chooses [redacted] and you initiate a [redacted] Payment.

[redacted] Transaction

Your customer then chooses their bank, logs in and confirms their payment.

Completion

Your customer now returns to your website.

Summary

Payment Gateways

1. Do not trust the client
2. Payment gateway fee < meeting PCI requirements
3. Not all gateways are created equal
4. Do not trust the client

Questions?