Card Information Flow (PCI PA-DSS 3.2.1)

OFFICE

Workstation

Database

Web Services

Authorization

1. Typed/Swiped Card saved temporarily in memory
2. Card is edit checked and errors given to user
3. Authorize card (data sent via https: to service provider)
4. Service provider returns result to Theatre Manager
5. If declined, user given option to enter another card
6. If accepted, payment data is sent to database
   a. If schedule D: card is encrypted first, then stored
   b. If schedule C: card is shredded before storing
7. Window closed and temporary data cleared

Settlement

1. Batch totals inquiry sent to Processor
2. Batch is settled via https command
3. TM shreds cards per customer retention settings

Processors

Credit Card Processors

- Paymentech Orbital
- Authorize.net
- Moneris
- Worldline
- Elavon

+ support for merchant profiles

SSL (TLS 1.2 or better)

DMZ

NGINX

REMOTE BOX OFFICE

VPN

Remote Computer

1. VPN session established –or-
2. User connects to 2022 Terminal Services or Citrix ISA Server
3. All subsequent data flow same as for office computers

INTERNET

Customers Web Browser

SSL (TLS 1.2 or better)

Note: TM does not allow online purchaser to use a previously saved card. The card must always be typed by the patron.

1. User contacts ‘https://tickets.myserver.com’
2. SSL session established to NGINX 1.21.6 or later
   a. TLS 1.2 or better
   b. Let’s Encrypt - SHA-256 with RSA Encryption Certificate
3. Browser talks to NGINX which talks to Web Listener
4. User adds items to cart and shops
5. At checkout, patron types card and CVV2; sent to Web Listener
6. Data encrypted into field and sent back to client to confirm
7. Web Listener (behind firewall) does all *authorization* steps as above
8. Confirmation displayed and emailed to user with card masked

© 2022 Arts Management Systems Ltd. Confidential