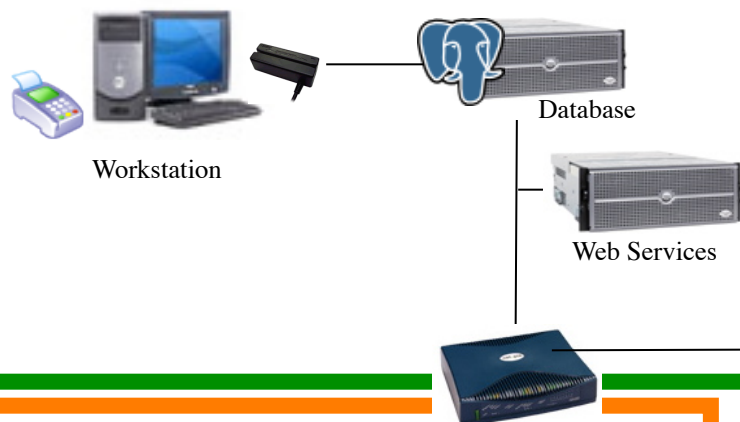




Card Information Flow (PCI PA-DSS 3.1)

OFFICE



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
 1. If schedule D: card is encrypted first
 2. 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

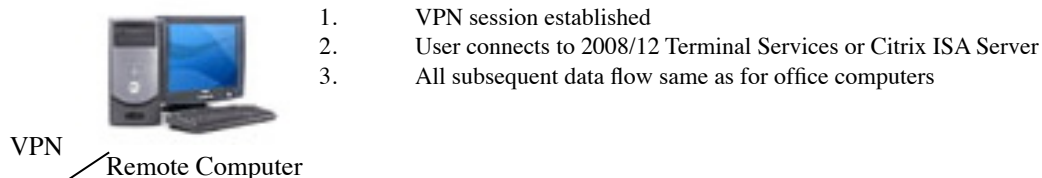
- Paymentech Orbital
- Authorize.net
- Moneris
- Beanstream 
- Elavon 



DMZ



REMOTE BOX OFFICE



1. VPN session established
2. User connects to 2008/12 Terminal Services or Citrix ISA Server
3. All subsequent data flow same as for office computers

INTERNET



SSL (TLS 1.2 only)

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 Apache 2.4.16
 1. TLS 1.2 only (no SSL or TLS 1.0, or TLS 1.1)
 2. GEOTRUST Premium 2048 bit/SHA2 certificate
3. Browser talks to Apache 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