Sabre Red Apps Security Requirements

6 February 2018

Security Requirements for Red Apps

These requirements are organized as follows:

- **General security requirements** for all *Red Apps*
- **PCI-specific requirements** for *Red Apps* that handle cardholder and personal data

General Security Requirements

All *Red Apps* must comply with the following requirements:

- The application must not introduce a virus or other malicious malware.
- The application must not download or launch other executable code that is not included in the certification application.
- The application must not enable illegal file sharing.
- Local logging is required for authentication and payment information creation and access. *Sabre* administrators must have the ability to enable or disable local logging, and define the number of days to aggregate logs and the location of logging files. End-users cannot control logging.

IMPORTANT: Browser integration (if applicable) will support no less than the equivalent security features available in Internet Explorer (IE) 7 or greater.

PCI-specific Requirements

Red Apps that handle sensitive, cardholder, or personal data must comply with the following requirements:

- The Red App must be GDPR compliant.
- The Red App must not use FTP, Telnet, or any other protocol that displays clear text IDs and passwords used to transfer data or connect to other systems.
- The *Red App* source code must be reviewed by the *Red App* developer before submission for certification or release to production or customers in order to identify any potential coding vulnerabilities (including at least the OWASP Top 10).
- The PAN must be masked when displayed by the application.
- Audit trails must be implemented in the application to log security events and access (read, write, or modify) to cardholder or personal identifying data. You must have a process in place to review these on a daily basis and follow-up on any security exceptions. Audit trails must be retained for at least one year.
- The Red App must comply with all legal requirements in any location where they are made available to users. It is the *Red App* developer's obligation to understand and conform to all such applicable legal requirements.

  Example: If you make your *Red App* available to users in Holland, then your *Red App* must comply with Holland's legal requirements.
- The *Red App* must comply with PCI standards and laws in every region of the world.

- The *Red App* must not write sensitive data to disk, nor cache sensitive data, nor retain it. If sensitive data is encrypted, however, a *Red App* can retain it. When encrypting cardholder or other sensitive data, encryption standards include the following:
    - TLS 1.2 transmission encryption
    - Locally stored credentials and forms of payment are encrypted with 3DES or AES-128 or greater.
    - Only appropriate use of internet facing protocols (i.e., TCP port 80 and 443 are open, TCP and UDP ports closed, and file transfer protocols are prohibited).