REALVNC

PCI DSS and the VNC SDK

May 2017

What is PCI DSS?

PCI DSS (Payment Card Industry Data Security Standard) compliance is mandated by many major credit card companies, including Visa, MasterCard, American Express, Discover and JCB, to ensure the safe handling of credit card information. To achieve PCI compliance, your business must adhere to the following security requirements:

Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security

How does the VNC SDK enable PCI compliance?

With the VNC SDK, you can build remote access capabilities into your product without sacrificing PCI 3.2 compliance.

Note: No single aspect of your product makes it PCI-compliant. To achieve PCI compliance, your product must adhere in full to the security policies outlined in the table above; your choice of remote access SDK is merely one aspect of that.

Here’s how the VNC SDK meets each of the guidelines above:

Build and maintain a secure network

1. **Install and maintain a firewall configuration to protect cardholder data**
    a. The VNC SDK does not require any inbound firewall configuration, meaning your existing PCI-compliant firewall need not be changed. If you wish to connect via the cloud (and outbound rules are in place), certain domains must be whitelisted.
2. **Do not use vendor-supplied defaults for system passwords and other security parameters**
    a. The developer can configure the Server app to request a username/password before an incoming connection is accepted. No default password / security parameter is provided, and no connection is accepted by default.
    b. The VNC SDK supports two connection types: cloud and direct. The developer can choose to disable either of these.

Protect cardholder data

3. **Protect stored cardholder data**
    a. It is possible to transmit credit card information via the VNC SDK (e.g. via remote control or by copying and pasting between the Viewer and Server apps). These features are disabled by default and must be explicitly enabled by the developer, who can then limit their use to certain users.
    b. Keys used to secure encrypted remote access sessions can be stored and protected according to your requirements.
4. **Encrypt transmission of cardholder data across open, public networks**
    a. The VNC SDK uses the RFB 5 protocol, which mandates the use of modern cipher suites and uses strong cryptography throughout. Developers can use the VNC SDK’s logging functionality to verify cipher suites in use.
    b. All connections are protected by at least 128-bit AES-GCM encryption.
    c. All connections have perfect forward secrecy, ensuring they cannot be decrypted now or in the future.
    d. Access to the VNC Developer online portal is protected by mandatory TLS. We follow best practices for secure web development, and our website is graded A in the Qualys SSL Labs test.

Maintain a vulnerability management program

5. **Use and regularly update anti-virus software on all systems commonly affected by malware**

   a. The VNC SDK is compatible with your existing PCI-compliant firewall/anti-virus software.

   b. Our own online infrastructure is similarly protected from malware.

6. **Develop and maintain secure systems and applications**

   a. We release free security updates for the VNC SDK as and when new threats emerge. Any new code is subject to a security review. These security updates are available on the VNC Developer website.

   b. Our technical operations team monitors our online infrastructure 24 hours a day, 365 days a year. These systems are regularly patched. Any critical vulnerabilities in upstream dependencies are assessed and patched outside our regular patch schedule.

Implement strong access control measures

7. **Restrict access to cardholder data by business need-to-know**

   a. For VNC Cloud connections, access control lists regulate who can attempt to connect. For direct TCP connections, the developer can filter connections by IP address to achieve the same effect.

      For either connection type, the developer can grant permissions based on the authenticated user ID of the person connecting (certain users can be denied access entirely). The developer can look up appropriate permissions using a mechanism of their choice.

   b. Developers can ensure successful and failed connection attempts are appropriately recorded in audit logs.

8. **Assign a unique ID to each person with computer access**

   a. The developer can configure the VNC SDK to require an authenticated user ID before remote access is established. Without this configuration, all connections are rejected by default.

   b. The developer can tell the VNC SDK where to find an up-to-date list of authorized user IDs. This ensures unauthorized users do not gain access. It can also restrict users to access during certain times.

   c. Developers have full control over how many authentication failures a connecting user can make before being locked out, or how long a session may remain idle before the connected user is automatically disconnected.

   d. Public versions of the VNC SDK allow authentication by user ID and password/passphrase.

      Pre-release versions of the VNC SDK additionally include APIs to allow multi-factor authentication by a range of different mechanisms.

   e. Developers can configure the VNC SDK to meet any password length/complexity requirements, and to enforce any password change policy.

9. **Restrict physical access to cardholder data**

   a. Out of scope for a remote access SDK.

Regularly monitor and test networks

10. **Track and monitor all access to network resources and cardholder data**

   a. You can configure the VNC SDK to audit any quality of logging, to any destination you choose.
   b. If your VNC Developer account’s security settings (e.g. its password) are altered, an email is automatically sent confirming these changes.

11. **Regularly test security systems and processes**
    a. Out of scope for a remote access SDK.

Maintain an information security policy

12. **Maintain a policy that addresses information security**
    a. The features and functionality detailed above should help you complete the appropriate portions of your information security strategy. If you require any more details, please contact RealVNC.

RealVNC's remote access and management software is used by hundreds of millions of people worldwide in every sector of industry, government and education. Our software helps organizations cut costs and improve the quality of supporting remote computers and applications. RealVNC is the original developer of VNC remote access software and supports an unrivalled mix of desktop and mobile platforms. Using our software SDKs, third-party technology companies also embed remote access technology direct into their products through OEM agreements.

www.realvnc.com