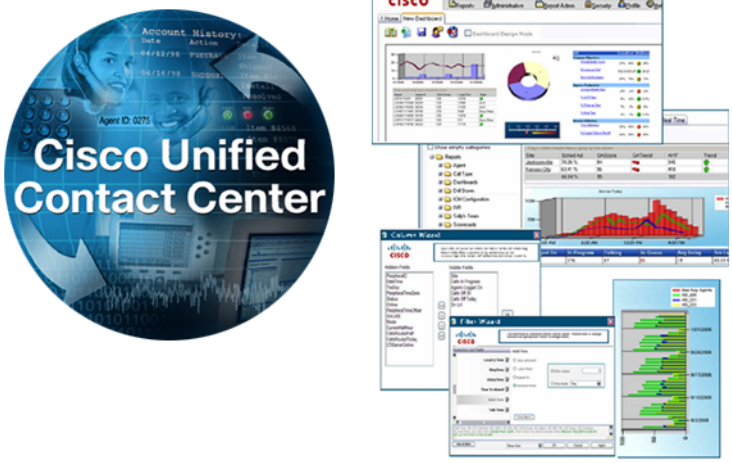
Credit Card Secure Architecture for Interactive Voice Response (IVR) Applications



What You Will Learn

This whitepaper describes how to meet the Payment Card Industry Data Security Standard (PCI DSS) for securing credit card information while using the Cisco® Unified Customer Voice Portal (CVP). Cisco CVP is an interactive voice response (IVR) product with a unique architecture that lends itself to safe, secure deployment for applications taking credit cards for payment or verification. This document describes the architecture for a Cisco Unified CVP deployment that provides a recommended architecture for credit card safety and security.

Cisco Unified CVP may be used in self-service applications that involve the verbal or electronic entering of credit card information as part of a credit card approval transaction. The security of this credit information needs to be considered as part of any PCI-compliant implementation.

This document looks at Cisco Unified CVP in the context of a secure architecture design for PCI. It discusses how Cisco Unified CVP would be deployed in that model and how its components would map to the components of the PCI standard. Cisco PCI design guides are available at http://www.cisco.com/en/US/docs/solutions/Verticals/PCI_Retail/PCI_Retail_DIG.html

What is the Payment Card Industry (PCI) Data Security Standard (DSS)?

The Payment Card Industry (PCI) Data Security Standard (DSS) applies to all businesses, large and small, in any industry, that process, transmit, or store credit card transactions and cardholder information. The goal of the PCI DSS is to increase protection of credit card information and related transactions. Any product that processes, stores, or transmits cardholder data falls under PCI DSS and is subject to a PCI audit.

PCI DSS includes a set of data security requirements as outlined in Table 1.

Table 1. Addressing PCI DSS Requirements

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to 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

Cisco offers numerous technology solutions and advanced services to help companies address their PCI DSS requirements. Because PCI covers many parts of the network, no single product or technology meets all of the PCI technology requirements.

Cisco PCI solutions address many of the 12 PCI DSS requirements. They go beyond just the requirements—for example, with newer technologies such as virtualization—and provide comprehensive best practices for securing sensitive information. Cisco PCI solutions can strengthen a company's overall security posture and help customers satisfy their PCI DSS requirements in a cost-effective and efficient manner.

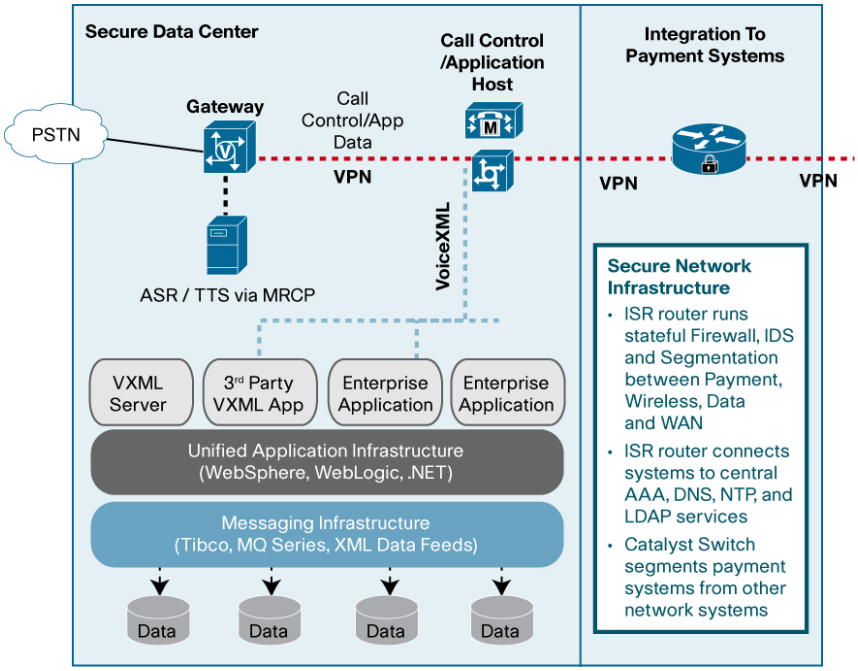
PCI DSS is applicable to a self-service IVR that is accepting credit card transactions. The merchant (that is, the owner/host of the self-service IVR system) is responsible for getting audited to achieve PCI compliance.

Cisco Unified CVP Architecture

The network plays a critical role in achieving PCI Compliance. PCI requirements can be broken down into the 2 key areas: 1) Addressing security requirements through technology (firewalls, etc.); and 2) Establishing and maintaining business policies.

Because Cisco Unified Customer Voice Portal (CVP) is a network-based IVR architecture, credit card security can be achieved via Cisco Technology Solutions.

Figure 1. Cisco Technology Solutions Overview



Cisco Unified Customer Voice Portal (CVP) resides within the Cisco Secure Network Infrastructure, and uses these infrastructure components to provide voice ingress as well as security. The following are the Cisco Secure Network Infrastructure components:

- Cisco Integrated Services Router (ISR) runs stateful firewall, as well as intrusion detection system (IDS) and segmentation between payment, wireless, data, and WAN.
- ISR router connects systems to central authentication, authorization, and accounting (AAA), Domain Name System (DNS), Network Time Protocol (NTP), and Lightweight Directory Access Protocol LDAP) services.
- Cisco Catalyst switches segment payment systems from other network systems.

Applying PCI DSS Standard to Cisco Unified CVP Deployment

The following table lists Cisco Solution and Unified CVP products and technologies that help to address PCI requirements.

Table 2. PCI Requirements to Cisco Solution Mapping

Solution Feature	PCI Value	Cisco Unified CVP Implication
Requirement 1: Install and maintain a firewall configuration to protect cardholder data		
Cisco Firewall Services Module (FWSM), Cisco ASA 5500 Series Adaptive Security Appliances	Network security (firewall segmentation/filtering), stateful filtering	Install Cisco Unified CVP in the protected cardholder data environment.
CiscoWorks LAN Management Solution (LMS) and Network Compliance Manager (NCM), Cisco Security Manager	Configuration management/secure configurations	
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.		
Cisco Unified CVP Server	Default passwords changeable Non console encrypted administrative access	Change passwords on Cisco Unified CVP servers, use AAA for administrative access.
Requirement 3: Protect stored cardholder data		
Cisco Unified CVP	Protect the data by only storing it where necessary, and only transmitting it in an encrypted form	Cisco Unified CVP applications should be written to not store sensitive information at all, and encryption points (VPN) should be used when transmitting data out of the secure data center. Logging of Cisco Unified CVP application data should also be disabled.

Solution Feature	PCI Value	Cisco Unified CVP Implication
Requirement 4: Encrypt transmission of cardholder data across open, public networks		
Cisco Unified CVP	Data protection	Use VPN when transmitting data out of the data center. This may be implemented by putting a secure VPN-enabled device between the Cisco Unified CVP Server and the egress to the payment network.
Requirement 5: Use and regularly update anti-virus software or programs		
Third-party anti-virus	Anti-virus protection, malware/spyware protection, alerting	Anti-virus is recommended for all Windows-based Cisco Unified CVP servers.
Requirement 6: Develop and maintain secure systems and applications		
Cisco Unified CVP Server	Capable of being patched and updated	Cisco releases Cisco Unified CVP security patches on http://www.cisco.com.
Requirement 7: Restrict access to cardholder data on a business need-to-know basis		
Cisco Unified CVP servers	Least-privilege, role-based access	Use AAA and Active Directory to provide role-based authentications. Cisco Unified CVP Operations, Administration, Maintenance, and Provisioning (OAMP) servers also support role-based access.
Requirement 8: Assign a unique ID to each person with computer access		
ISRs, Cisco 7200 VXR Series Routers, Cisco FWSM, Cisco ASA 5500 Series, switches, wireless controllers, CiscoWorks (LMS), Cisco Security Monitoring, Analysis, and Response System (CS-MARS), Cisco Secure Access Control Server (CS-ACS), Cisco Wireless Control System (WCS), RSA applications and NRC Advanced Checkout Solution (NCR-ACS), Cisco Unified CVP servers	Unique user IDs, authenticated access, encrypted passwords, no group/shared IDs/passwords	Cisco Unified CVP provides these features.
ISRs, Cisco 7200 VXR Routers, Cisco FWSM, Cisco ASA 5500 Series, switches, wireless controllers, CSA Manager, Cisco Security Manager, CiscoWorks (LMS), CS-MARS, CS-ACS, WCS, RSA applications and NCR-ACS, Cisco Unified CVP servers	Password strength requirements	Cisco Unified CVP supports password strength requirements.
ISRs, Cisco 7200 VXR Routers, Cisco FWSM, Cisco ASA 5500 Series, switches, wireless controllers, CSA Manager, Cisco Security Manager, CiscoWorks (LMS), CS-MARS, CS-ACS, WCS, RSA applications and NCR-ACS, Cisco Unified CVP servers	Account lockout requirements	Cisco Unified CVP provides account lockout capabilities.
Requirements 9: Restrict physical access to cardholder data		
All servers and database storage	Physical access requirement	Cisco video surveillance and monitoring systems can be implemented to meet this requirement.
Requirement 10: Track and monitor all access to network resources and cardholder data		
ISRs, Cisco 7200 VXR Routers, switches, wireless devices, WCS, CS-ACS, CiscoWorks (LMS), RSA applications, NCR Applications, Cisco Unified CVP servers	Audit trails, time synchronization	Cisco Unified CVP supports audit trails and time synchronization.
CiscoWorks (LMS and NCM)	Centrally archive audit log records	Cisco Unified CVP audit logs can be centrally stored away from the Cisco Unified CVP Server.
Requirement 11: Regularly test security systems and processes		
Cisco Integrated Services Routers, Cisco ASA 5500 Series, Cisco Intrusion Prevention System (IPS) Sensor, Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) (sensor), Cisco Security Manager (policy, signature updates—a part of the Cisco Unified CVP environment)	Network IDS	Networking best practice.
Requirement 12: Maintain a policy that addresses information security for employees and contractors		
Cisco Advanced Services can help with the creation of this policy.	Creation and maintenance of security policy	Cisco Unified CVP deployment implementation and operation should be factored into your overall security policy.

Conclusion

This document describes Cisco Unified Customer Voice Portal (CVP) in the context of a PCI deployment. Intended as a summary of Cisco's PCI best practices, it is not a standalone document that covers PCI architectures in general.

Cisco® Validated Designs are a critical element of Cisco's PCI solution portfolio. Built and tested in Cisco labs, these designs have been evaluated by a PCI QSA, who then provided a report on compliance (ROC) outlining how each solution addresses PCI DSS technology requirements. The Cisco Validated Designs for PCI can be downloaded from http://www.cisco.com/go/pci. The independent ROCs for Cisco's PCI solutions are also available for viewing at this address. At this time, the PCI audit of the Cisco Unified CVP solution is pending.

Cisco also offers **Cisco Payment Card Industry Compliance Services**. These services help network directors, security managers, and directors who process payment card transactions achieve and maintain PCI compliance by identifying and remediating compliance gaps.

Each enterprise network deployment is unique. For detailed architectures and security discussions, please contact your Cisco account team.

For More Information

For more information on Cisco PCI solutions, please visit http://www.cisco.com/go/pci, or http://www.cisco.com/go/retail. More information about PCI DSS compliance and standards is available at: https://www.pcisecuritystandards.org/

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-604236-00 05/10