

Secure Proxy Solution

Substitutes alternative numbers for actual customer data.
A highly reliable, cost effective distributed enterprise solution.
Surpasses encryption with multiple security characteristics.



The Payment Card Industry (PCI) data security standards were created by MasterCard and adopted by the four major credit card companies, with regulations taking effect in June of 2005. This move was in response to a growing onslaught of cybercrime, with increasingly sophisticated thieves able to extract credit and debit card information from even ostensibly secure databases.

The five leading payment brands have jointly formed the PCI Security Standards Council, an independent entity, to manage the ongoing evolution of PCI Standards as a means of securing payment account data in a globally consistent manner. Failure to comply with these PCI security standards results in high fines, restrictions, or in some cases, expulsion from card acceptance programs.

PCI hurdles in the legacy environment

Many organizations still require legacy and/or proprietary operational applications to run their business and interface with partners, customers and other entities. Important functionality now required that may be missing from these systems include:

- encryption capabilities protecting cardholder data
- strong support for authentication and implementing access controls
- alternatives to embedded passwords to build and maintain secure networks
- logging capabilities for regular monitoring and testing

The challenge: complexity, demanding timeframe

The challenge to build an end-to-end enterprise solution for PCI compliance was brought to Cigital, Inc. by a worldwide hospitality company with sales exceeding \$11 billion from lodging properties in the U. S. and over 60 other countries and territories.

The client's goals included meeting PCI compliance with a universal system for protecting credit card data throughout the organization's credit card handling applications, preferably in a timeframe of 18 months to avoid incurring fines. The system needed to be dynamic, highly secure and easily usable across the diverse platforms, technologies and programming languages of 2800 locations.

The solution needed to provide access to network resources for employees, customers and partners. Drivers included:

- Enterprise-wide customer credit card data protection
- Safe aggregation of sensitive data for advanced marketing analytics
- Support of partners' B2B interface policies
- Seamless support of legacy systems with current security controls
- Controlling increase of maintenance costs
- Integration of security architecture with other enterprise efforts

Meeting cost expectations vs. other approaches

The full solution development involved planning, design, development, testing, legacy integration and migration, support and training of the client staff—at a total cost dramatically lower than alternative, application-oriented approaches that were considered.

Secure Proxy Solution Summary

- Secure multiple integration points across the enterprise
- Minimize impact to existing legacy apps and db schemas
- Ability to integrate with CRM, Financial, B2B partners
- Integrate with existing enterprise authentication scheme
- Supports PCI logging requirements for credit card access
- Supports central and distributed environments
- Robust access controls, concepts of "least privilege" or "need to know"
- Accelerated deployment via
 - Pre-built software components
 - Implementation templates
 - Extensible set of APIs
 - Highly trained security experts
- Benefits of a proxy number, which can serve the same function of a credit card number:
 - Protected at rest or in transmission
 - Remains a proxy until business case authorizes access
 - Less processing intensive, less unprotected usage
 - Fits data constraints of existing business systems
 - Supports separation of privileges; generates/reverses proxy based on need



Delivery of a Cigital Secure Proxy Solution

Cigital has proven methodologies that help organizations protect their most valuable assets: company information and customer data, customer confidence, brand, shareholder value.

The process that has been developed for delivery of a Secure Proxy Solution includes the following, some of which are optional depending on the precise needs of your enterprise:

ROADMAP	Initial assessment, plan analysis and project design, migration or change management. Business process improvements are defined for key rotation, certificate management, access and role definition.
DEVELOPMENT	Design modifications to core software and legacy application integration components. Depending on the requirements, significant cost savings may result from using a dual development approach with the expert staff of Cigital India. Software security is built into the Proxy Solution code through secure architecture/design and code review for vulnerabilities. Independent quality assurance is conducted with full life cycle artifact examination and risk-based testing.
DOCUMENTATION, TRAINING & SUPPORT	Provide complete documentation, training for staff on APIs and software. Develop training programs for legacy teams and Proxy Solution administration teams.

Cigital's PCI Standards Credentials

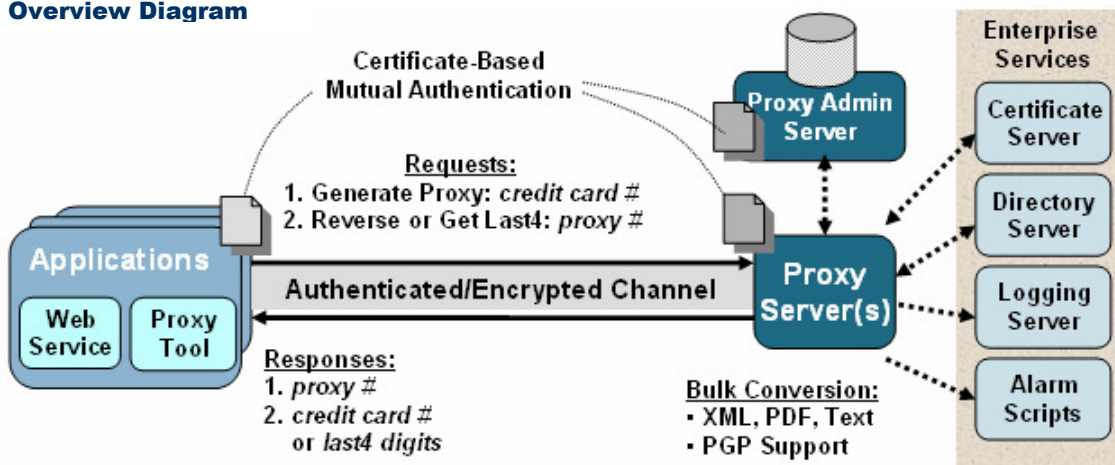
Cigital has worked with both VISA and MasterCard on payment systems security assurance, testing and on specific needs for PCI standards requirements. We continue to work with MasterCard, for example, augmenting the standards that are being written for wireless networks. We perform due diligence on MasterCard internal processes and act as subject matter experts to the people who write the policies – to identify any gaps. We provide advice to the auditors who perform quarterly penetration testing.

About Cigital

The growing demand for ubiquitous connectivity throughout the enterprise, for universal access to information and communications creates new, unforeseen vulnerabilities. Founded in 1992, Cigital is a leading consulting firm specializing in software security and quality. Our experience has demonstrated that the right solutions are built in, not “bolted-on.”

Cigital’s experts mitigate software-induced business risks and identify performance issues that have business consequences. We assure the reliable delivery and deployment of software that organizations build, buy and integrate. Cigital is headquartered near Washington, D.C. with offices in Boston, New York, and Los Angeles.

Conceptual Overview Diagram



Software confidence. Achieved.