

## Why PCI Compliance is Important for Hotels

November 25, 2011 - by Ulf Mattsson, CTO of Protegrity

According to Verizon's 2011 Data Breach Investigations Report<sup>i</sup>, 40 percent of all 2010 data breaches occurred in the hospitality industry. Not unsurprisingly, the report also found that PCI compliance levels were down from the previous year; 89 percent of businesses surveyed were not validated compliant at the time of the breach.

Hotels of all sizes need to understand the risks and ensure their customer data handling and transaction processing meet PCI standards. Failure to do so will result in hefty fines, increased card processing fees, loss of ability to accept payment cards, bad publicity and brand devaluation.

### Your responsibilities

PCI compliance is the responsibility of the hotel, not the software vendors. You need to ensure that your business implements and maintains effective network security, cardholder data protection, vulnerability tracking, and system monitoring. The PCI Security Standards website<sup>ii</sup> offers plenty of easy-to-read guidance.

Compliance certification comprises two distinct steps:

1. **Self-Assessment:** All businesses are required to self-assess their IT and payment processing environment using the appropriate PCI Self -Assessment Questionnaire (SAQ).
2. **Vulnerability Scanning:** Depending on how you process payments and the Internet connection, network vulnerability scanning by an Approved Scanning Vendor (ASV) may also be required.

### Outsourcing

Outsourcing any part of the data handling process does not negate your security responsibilities. You must ensure any vendor with access to the data complies with your standards. Because controlling your service providers' handling of your data is not typically possible, you can mitigate the risk by controlling the form in which the data is stored. One approach that's gaining in popularity is tokenization, which can significantly reduce the burden of compliance without getting in the way of business.

### Tokenization Explained

At its basic level, tokenization simply replaces real customer data with fake data. The fake data is considered non-sensitive for PCI compliance purposes and thus falls outside of mandated protection requirements, regardless of whether you or a third party is storing that data.

### Basic vs. modern tokenization

There are two types of tokenization solutions on the market today.

Basic tokenization solutions are built around a large, dynamic table of token/credit card pairs. While this is a reasonable first step, the token lookup table can, over time, become so large that it's difficult and costly to manage, introducing performance, scalability, and availability problems.

Modern tokenization eliminates performance, scalability and availability issues by pre-generating static token tables that can be installed in multiple locations. Hospitality and retail businesses are often

widely distributed and need rapid access to large amounts of data and quick response times, so modern tokenization's ability to perform over 200,000 transactions per second is particularly appropriate.

One major retail chain in the US switched from encryption to tokenization to secure its customer data and realized a reduction in PCI audit time from seven months to three. The entire initial tokenization process took only 90 minutes, and transaction times met the merchant's required sub-second processing speed. A planned future extension of the system is expected to reduce the audit time to just one month, resulting in significant cost and resource savings.

### **Encryption**

Encryption has been the gold standard for data protection for many years, and has many strong points. However, it is technically complex and often difficult to implement. Unfortunately, some vendors have jumped on the tokenization bandwagon with a solution that is in reality an unproven encryption scheme. Such systems are vulnerable to both breach and catastrophic data loss, so if you're testing tokenization solutions and need to be sure you're working with the real thing and never, ever, test on a live system.

### **What's next?**

It's clear the hospitality industry needs to speed up its adoption of PCI standards to avoid remaining in the top position in future data breach surveys. Much of the problem lies with the widespread use of legacy software systems that don't have the ability to properly encrypt and secure sensitive card holder information. Tokenization holds significant potential for overcoming that particular issue, so if you're dealing with older systems, it's certainly worth looking into what it could do for your business.

Also keep an eye on Hotel Technology Next Generation (HTNG)<sup>iii</sup>, a newly-formed global trade association of hoteliers and technology providers whose mission is to facilitate technology developments in the hospitality industry. At least 16 hotel groups have expressed interest in developing an industry-wide solution, and are working with HTNG to create a credit-card security framework. That's an approach that makes more sense than the past efforts by individual hotel groups to develop their own data protection technologies.

The bottom line: to keep your customers happy and loyal to your brand, protect their data in the most secure way possible.

*Ulf Mattsson is the chief technology officer of Protegrity, a provider of enterprise data security management.*

---

<sup>i</sup> 2011 Data Breach Investigations Report, <http://www.verizonbusiness.com/go/2011dbir>

<sup>ii</sup> PCI Security Standards Council, <https://www.pcisecuritystandards.org/merchants/index.php>

<sup>iii</sup> Hotel Technology Next Generation, <http://www.htng.org/>