Alina Consultants Inc, Project 'R' One pager

Genesis

- Client R[1] is a well-known public company that sells digital products on an ecommerce, 'direct to consumer' model.
- R was on a legacy ecommerce system that had grown organically over a period of more than ten years to service rapid business growth.
- A large percentage of R's orders were from repeat consumers. Credit card numbers were persisted in the legacy clients for single click type functionality.
- The legacy commerce system presented an insurmountable challenge for security best practices and PCI compliance as the clients persisted raw credit card numbers.
- The core client for R's ecommerce system was deployed on a very well known licensed invoicing system. This product stores credit cards in clear text by default. Add on packages are required in order to implement DSS controls.
- R approached AC[2] with a desire to build a service to interact with front end systems (Website, ERP) and accept credit card requests in a secure and PCI compliant manner.
- AC began the architectural design and implementation of the system on Feb 15th, 2014.
- Distributed team comprising of one Payments Expert & Senior architect and one Senior Java engineer.
- Go live tracking for May 15th 2014.

Application Details

- The application exposes encryption as a service. The service persists PANs, ibans, payment information using strong encryption.
- The solution involves minimal changes within clients.
- Client systems are not required persist payment data.
- No downstream vendor lock in. It is possible to replace R's payment provider with minimal changes in the core commerce system.
- Architecture makes it possible to meet all DSS control objectives.

Architecture

- Creation of a library service that persists PANs using strong encryption.
- Implemented as a library, however can be offered as a webservice via JSON/XML as the data exchange format

[1] Name of client not divulged for confidentiality reasons.
[2] Alina Consultants, Inc

- Robust horizontally scale-able architecture that works in a multi-threaded / distributed manner
- The service supports the business logic for authorization & settlement.
- NO changes are required for legacy clients through innovative[3] application design.
- Charge clients do not need to store PANs, they merely store a pointer to the PAN.
- Extensible design to plug-in custom encryption needs for key management
- Implemented using JEE components with AES128-bit encryption however, the design as such does not bind to any particular encryption methodology

Results

- In line with security best practices
- PCI footprint reduced by 90%
- Legacy clients out of scope for PCI compliance.
- R no longer needs to file compensating controls for PCI audit.
- Cost of PCI compliance reduced dramatically (more than 50%).

[3] Methodology is not being disclosed.