Title: Bringing PCI Data Security Standard on the Cloud

Description

The PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.

PCI-DSS requirements apply to all players involved in electronic transactions with credit cards. Regulators (such as National Authorities) storing such information need to certify the PCI-DSS compliance of part of all their IT infrastructure thus it is a costly task *from both an economic and organization points of view*. PCI DSS data management requires, among the other things:

- Restrict any physical access to data or systems that house cardholder data and prevent the possibility of access and/or removal of devices, data, systems or hardcopies,
- Establish entry controls to limit and monitor physical access to systems in the cardholder data environment,
- Establish, publish, maintain, and disseminate a security policy that addresses all PCI DSS requirements, includes an annual process for identifying vulnerabilities and formally assessing risks. This includes a review at least once a year and whenever the environment changes,

Additionally such data could be accessed by other players than the regulator and this would imply PCI-DSS certification at both sites and of the communication channels making the thing economically not substainable.

The goal of the project is to make an assessment of moving PCI DSS data stored by authorities on o cloud or federation of clouds.

Objectives

State of the art

Provide a (small) overview of the PCI DSS focusing on the problem of PCI data management of stakeholders.

Gap Analysis and threat modeling

Identify possible gaps bringing PCI DSS compliant data on:

1. Private clouds;
2. Public clouds;
3. Federated public clouds

Design a Solution

Provide an initial design for a PCI DSS based on federated clouds pointing out how some of the PCI DSS requirements could be satisfied.

References

Use you favorite search engine and look for PCI DSS Systems.
https://www.pcisecuritystandards.org/security_standards/documents.php
http://www.juniper.net/us/en/local/pdf/solutionbriefs/3510278-en.pdf