Authentication and Trust: Turning the Cloud inside out

Christian Brindley

Regional Technical Manager, EMEA – VeriSign Europe
2nd Floor, Chancellors Road, London W6 9RU, United Kingdom
cbrindley@verisign.com

Abstract

There is no doubt that enterprises of all sizes are moving more of their critical business applications into the cloud, relying on services such as Salesforce.com, Google Apps and Amazon Web Services to organise and protect their core business data.

It is also true to say that very few enterprises base their entire infrastructure in the cloud. There is almost always a part of the IT core which is managed and protected in house, leading to a hybrid approach to cloud computing.

In any given enterprise, the split between in house and in cloud infrastructure speaks volumes about that organisation's perception of the cloud. Often, the single part of the enterprise IT infrastructure to be retained in house is the authentication and identity management system.

This paper puts forward the argument that authentication and identity management should in fact be the first element of an enterprise infrastructure to be moved into the cloud. Only then will the cloud model realise its full potential of zero footprint in house, finally setting organisations free to focus on their core business.

1 Introduction: Shaking things up

Cloud computing is a disruptive technology: it falls nicely into Gartner's definition of “causing a major change in the accepted way of doing things” [CECL08]. In fact, back in 2008, Gartner included cloud computing as one of the top ten disruptive technologies for 2008-2012 [CECL08], and few would disagree that this position holds fast today.

Disruption brings with it the opportunity to apply new approaches to old problems. This is particularly true of the opportunity offered by cloud computing to rethink our approach to security.

Unfortunately, security is often perceived as a barrier rather than a driver for adoption of the cloud model. There are a number of surveys run by various organisations to test CIO/CSO appetite for the cloud: each survey takes a different approach and has different motivations, but a common slant is to present security as a negative.

As a typical example, one survey [RELI08] asks participants to choose from the following reasons to use the cloud:

- Performance
• Cost Savings
• Rapid Deployment
• Uptime/High Availability
• Consumption-Based Pricing
• Scalability
• Capacity

And from the following reasons not to use the cloud:
• Security
• Support
• Integration With Existing Systems
• Vendor Lock-In/Portability
• Consumption Pricing
• Performance/Availability Concerns
• Speed to Activate
• Regulatory/Compliance Concerns

This is a common approach. Various surveys swap reasons from one list to the other, but the majority put security in the list of potential barriers to cloud services.

Of course, security is always going to be at the forefront of an executive's considerations when moving to the cloud. However security should be seen as a benefit of the cloud rather than a drawback.

According to NIST, the benefits of cost and agility determine why to migrate to the cloud, and the issues of security determine how. The argument presented here is that security should determine both how and why.

2 What do we mean by Security in the Cloud?

The phrase “Security in the Cloud” introduces two vast topics: both security and the cloud are broad and subjective terms, which need to be limited in scope for the purposes of any meaningful analysis.

2.1 The Cloud

NIST [MEGR09] define cloud computing as

"a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

Note that this does not dictate whether the cloud services are located within the enterprise, or with a third party. Well known provisioning models for cloud computing include:
• **Private Cloud**
  This is an architectural model where services are compartmentalised and usually virtual-