Card Technology versus Cloud

For Retail Payments - SPA's Position

November 2013

1. Introduction

In this paper SPA provides an opinion on present and future trends for retail payments based on a comparison between the use of hardware-based card solutions and software-Cloud retail payment solutions, and their respective pro's and con's.

Cloud computing usually refers to the delivery of computer processing infrastructure, applications and data storage facilities over Internet. Yet there is a lack of a common understanding on the scope of the concept and their practical implications. It follows that heterogeneous IT solutions are being marketed as "Cloud Computing" ones. At present we observe a consensus in the industry that the Cloud represents a promising new IT paradigm for the provision of online services, including retail payments. The idea of storing personal data in a "Cloud" ubiquitously accessible and potentially shareable by authorized person is no doubt an appealing one. Now it remains the question of whether the technology is suitable for the storage and access of any type of data. For retail payments services, the question SPA explores is whether the Cloud constitutes a short-term realistic alternative to the card technology or whether the coexistence of both technologies constitutes a preferable option.

2. Retail payments, security and innovation

In their different paper positions, SPA has made clear that for many reasons, only very safe innovation technology is acceptable for the retail payment market. With this regard, the Cloud is challenging from the security and data privacy point of view. The Cloud is a driver for innovation in the security industry. But from the financial industry prospective, the technology for access to payment account must be safe now, not in the near future. Financial institutions are liable for any financial loss resulting from unauthorized access to the payment accounts of their clients. Moreover security breaches may have a devastating impact on the reputation of banks and other payment service providers. With this respect, SPA reminds that with Chip & Pin technology, fraud has been tackled down to negligible figures. With Chip & PIN technology, highly secure cloud-based computing infrastructures can be offered right now.

Retail payments is mass business. Payment systems are only profitable when they process a sufficient number of transactions (billions !) and fraud is negligible. Generating transactions requires adoption of interoperability standards, because retail payments is a two-sided market. The card is a highly standardized & safe payment instrument. As such, the card technology generates revenue for banks: it is accepted as a payment means everywhere because it is interoperable, and the number of transactions made has no impact on the risk of the next transaction. In addition, users have very good experience when paying with cards. Again that contributes to the security of the payment system, because it makes unlikely that a cardholder makes a wrong manipulation when using its card leading to a financial loss.

Security, interoperability, good user experience and a robust business model for the card issuer, constitute therefore four key advantages for the card technology. Let's concentrate in the two technical aspects of security and interoperability.

3. The lack of standards for cloud interoperability

The Cloud is an innovative promising business prompting many proprietary solutions. We are in the stage where competitors try to win the battle and become the "di-facto standard". Progress on international standardization is therefore not that obvious.

Now, the Cloud paradigm can be summarized in three points (1) access to services, personal data and applications in the Cloud, is ubiquitous using different devices, personal or not (2) the owner of data stored in the Cloud may in turn grant access rights to a third and (3) the user of a Cloud service is enrolled by the Cloud Service Provider. In addition, agreements between Cloud Service Providers are inevitable for business development in a networked world for cross-servicing purposes. These business requirements are highly demanding in terms of interoperability.

Standards endorsed by the most significant Cloud players are inevitable to develop large-scale Cloud services. A period of time will be required for Cloud common standards to be agreed and adopted. Moreover because of the specific security issues raised by the Cloud, proprietary solutions are marketed with their own security provisions. In the end, for the sake of interoperability both functional and security standards for the Cloud will be needed.

To illustrate that point, in the payments industry three recent hints are significant:

- ISO 12812, first international standard on mobile payments, recognizes the coexistence of mobile financial services provided by either locally resident applications or remote hosted ones
- The European Payments Council white paper on Mobile Wallets provides insight for local wallets as well as cloud resident ones
- The recent announcement by Visa, MasterCard and Amex on their workings for a new standard for a payment tokenization solution for internet commerce, let's the door open for implementations which could be outsourced in the Cloud

SPA outlines that the card technology already allows the ubiquitous access to a card payment account: First because the high level of interoperability between the card and the payment terminals accepting cards and second because the payment applications are now stored and executed in the secure elements and therefore benefit of the connectivity features of the mobile devices (Mobile Network, NFC and wireless network access).

4. The security of the Cloud and the card payment services

SPA analysis focuses on four security aspects in order to better understand the challenges raised by the implementation of security mechanisms to protect financial data stored in the Cloud:

4.1. The complex security policies required to deploy Financial Cloud Services

Cloud computing raises a number of cybercrime and security risks that do not exist in traditional card payments, where data transactions are transmitted through networks under the control of financial institutions. For instance, Cloud computing accounts can be created or existing accounts compromised for criminal purposes. New cloud computing accounts may be created with stolen access credentials and payment card details, by anonymous attackers difficult to track down the source of the attack, particularly when jurisdictions are crossed. These vulnerabilities arise because at the difference with card payment networks, well demarcated network security border is not fixed in Cloud systems.

These risks have to be addressed by deploying new security policies in order to detect, prevent and mitigate their impact by users and providers of Cloud services. These security responsibilities have to be properly assigned and communicated in the contract for Cloud Services, meaning that specific clauses addressing financial data integrity, confidentiality and the access management to account payments or payment applications have to be clearly understood and agreed by the user.

4.2. Authentication challenges for access to Cloud Payment accounts

Customer payment card data stored in the Cloud constitute a highly sensitive asset. Unauthorized access to cloud computing systems may occur when for instance a personal identifier has been obtained without authorization. To mitigate the risk of unauthorized access to personal card data stored in the cloud, these data should be encrypted. However, lack of specific regulation, encryption by the Cloud Service Provider can potentially be weakened or broken if insecure or obsolete.

In the card, data are securely stored because the card is a tamper resistant device duly certified. Leakage of information from card is useless for impersonation purposes and the card and the terminal proceed to an independent evaluation of the risk associated to a particular transaction, and then decide how to proceed to authorize the transaction. In addition, payment cards comply with EMV specifications. Meaning, the cryptographic mechanisms put in place are annually reviewed, the lengths of the keys updated when necessary and any academic theoretical published attack is carefully evaluated and countermeasures adopted. Migration timelines are decided so that security crypto-mechanisms considered obsolete be phased out.

Moreover, card payment data are under the control of the cardholder in a personal device. In the Cloud this direct control is lost, the data availability may be compromised. More fundamentally, at any time the data owner may require from the Cloud Service Provider evidence proving the integrity and the availability of its stored data.

.

Other than remote storage and processing, the Cloud is interesting because of the possibility to delegate to a third certain access rights to personal data. Even if in the payment domain the use cases are not obvious, because payment instruments are strictly personal, there may be scenarios for delegation. In that case two scenarios may be differentiated:

1. Either the delegation of rights may be granted directly by the owner of the data or
2. This delegation is to be authorized by the Cloud Service Provider upon the owner request; this could be the case when this delegation is for instance temporary and/or apply to a certain number of access.

In the case of payments, a delegation may be provided to a retailer in order to get access to payment account data stored in the cloud in order for the retailer or its agent to generate for instance an authorization request for a payment. If the retailer is unknown by the user, it must be known and trusted by the Cloud provider. This problem is not far away from the security issues raised by e-commerce. In the case of the Cloud an Identity management system is required at least:

- to authenticate legitimate data owners, at the enrollment and during access to Cloud,
- to control the validity of the delegation tokens issued by an enrolled customer.

That makes the design of the Cloud access system complex compared with traditional payment systems and even more complex card based internet payments. Complexity out of certified components adds vulnerabilities to any system.

The former is true even when using well-proven cryptographic primitives as those used to protect card transactions. The functional requirements at the core of the Cloud Computing model bring about security concerns specific to the Cloud, for which specific adapted cryptographic mechanisms have been designed but not sufficiently proven by the financial industry (homomorphic encryption, group signature).

In any case, the direct access to encrypted data in the Cloud by the owner himself of by an authorized third person, raises specific challenges in terms of key management. As a minimum, Cloud sensitive data must be encrypted in transit and the keys required to decrypt the content must be made available to the final user of the data.

Because of the variety of possible scenarios:

- For the encryption policy of the Cloud Service Provider
  - the Cloud Service Provider encrypts directly the data they store using its own keys and algorithms and then the Cloud Service Provider has to provide guarantees in the technology used to protects its encryption keys or
  - the Cloud Service Provider accepts data already encrypted
    - either directly by the owner of the data or
    - by a third trusted party having contracted with the data owner
- For the person granting access to protected financial data
  - the owner of the data or
  - a third having delegated rights

the key management system is necessary complex to achieve a level of security for financial data comparable to the protection in certified card payment systems. Because of this complexity, it will be expensive to implement and operate. Proper monitoring and audit of the Cloud Service Provider practices for the security management of keys should be required. With this particular respect, ISO JTC1 SC27 is discussing a new work item for the implementation of cloud security controls based on a set of high level controls in ISO/IEC 27017. If approved, this international standard should include

Cloud provider's declaration of security conformity. It remains, that the security policy this declaration should conform to is not yet agreed.

5. The security certification of components participating in Cloud payment infrastructures

The card uses both symmetric and asymmetric cryptography for authentication, data confidentiality and data integrity purposes. As a tamper resistant device, the card securely stores private signing keys and associated public key certificates useful to strongly authenticate the user or to generate a non-repudiable proof of consent. Protection profiles for cards and terminals used in different acceptance contexts are available and card products are certified against well proven security evaluation processes that include testing of product resistance against a permanently updated list of card targeted attacks.

In that sense, at present there is not a comparable formal Certification process for a Cloud Computing system. That does not mean than individual components of the Cloud infrastructure cannot be certified against PCI-DSS or a set of security requirements for HSM as the one defined by Book 4 of the Volume Book of Requirements v 7.0 (to be published by the European Payments Council early in 2014) . With this regard PCI has released a document containing Guidelines for PCI-DSS application to Cloud Computing. That's a good starting point.

6. The Data protection of Cloud users

Data protection for Cloud challenges may at first sight not be different from those raised by other remote access to financial services. But in the Cloud data centers are distributed. From the outside world there is no guarantee in the internal security mechanisms applied to move data, nor where the data physically lies and therefore the jurisdiction applicable to the data protection. As mention, the user has no visibility on whether its data are stored into the Cloud security perimeter.

On the other hand, the user decides to store payment account data in the Cloud because they can be accessed anywhere anytime either by himself or by a designated third person by connecting to a secure server under the control of the Cloud Service Provider. Yet in the Cloud, data are distributed meaning that:

- The access server must be able to execute queries looking for the card data required by the user
- These queries should be authorized by one authority verifying the access rights to this query
- This authority should also guarantee that even by cross-checking these queries, the conformity to the applicable data protection law is ensured

As it is the case for security, data protection specific concerns derive from the Cloud functionalities. With this regard, the SPA outlines that card specific frameworks for data protection have been released by standards bodies (Global Platform, CEN TC224 European Citizen Card) and are under discussion in financial standardization bodies (EMVCo, ISO TC68 SC7).

The need to address data privacy in the Cloud has been recognized by ISO and ISO JTC1 SC27 is working on a new standard for the privacy in the Cloud, ISO/IEC 27018. This standard should provide guidelines to protect Personally Identifiable Information for the public cloud computing environment in accordance with the privacy principles set forth in ISO/IEC 29100.

7. Conclusion: On the coexistence of Cloud and Card technologies for payments

As discussed, a secure Cloud system needs to address the four issues identified in this document: security policy, strong user authentication, certification and data protection. Cloud security services may well be implemented using a payment and/or identification card communicating with a remote infrastructure. The mobile wallet is an innovative concept enabling the coexistence of payment and authentication applications. In that sense, the Cloud represents an unprecedent business opportunity for the digital security industry. Not surprisingly, the draft white paper released by the European Payments Council addresses card as well as "cloud" implementations for the mobile wallet understood as stored in a secure server but accessed using a mobile device.

Future wallet business models may leverage these emerging efforts by combining the strong device-level security (a characteristic specific to the smart card) with cloud-based technologies, driving improved efficiencies and innovation for user experiences, while standardizing the back-end Cloud computing protocols for interoperability, ubiquity, and enhanced security.

It is therefore very likely that in the medium/long term, the coexistence of the card and the Cloud technologies will may rise to new payment infrastructures and instruments that will combine the best features of both technologies.