NEC PAYMENTS

Delivering Secure Transaction Processing in the Public Cloud

Andrew Sims, Chief Executive Officer
andrew.sims@necpayments.com

30th December 2016

Delivering Secure Transaction Processing in the Public Cloud

The deployment of secure processing technology environments is an arduous and costly process. With legacy transaction processing still mainframe-based; and even relatively recent processing technologies burdened down with hardware security, key management and encryption devices; deploying or scaling quickly - or even just changing anything infrastructure-related - is something not to be undertaken by the faint hearted.

When you place these restrictions into the context of the dramatic and wholesale changes that are occurring in the approach to procurement and management of technical infrastructure in other industries, you can begin to better understand the negative effect that the current position has on the agility and efficiency of payments products, and the operating costs of financial institutions and other businesses operating in the payments space.

The rulebook has been re-written with the advent of public cloud infrastructure. Imagine what financial institutions and payments businesses would be able to achieve if they could leverage the significant benefits that cloud deployment brings?

For example:
- creating or replicating a secure environment on another continent within a matter of hours;
- scaling-up or down volume handling capacity, and the associated costs, on demand;
- building and deploying new products for beta testing without any worries about the cost and availability of technical infrastructure resources; or

- being able to mitigate disaster recovery and business continuity planning risks at a fraction of the cost of traditional techniques without compromising on recovery time or recovery point objectives.

All of these things are now possible - right here and right now - using public cloud technologies. However, driving the transformation of the payments industry requires not just infrastructure to be available; it also requires cloud-ready technologies that are agile, flexible, secure, and ready to harness the benefit that cloud infrastructure can offer.

It is the ground-breaking approach that independent software vendors like NEC Payments – working closely with its global technology partner Microsoft - are taking to building security and agility by design into its software products; coupled with the power, scalability and speed of the Microsoft Azure cloud that is enabling true digital transformation and delivering new deployment options into an industry segment that has been static for a considerable period.

This transformation was manifested at the GITEX event held in Dubai during October 2016 where NEC Payments and Microsoft jointly announced the availability of NEC Payments' MasterCard and PCI-DSS compliant suite of transaction processing technologies in Microsoft Azure.

"NEC Payments not only completed the technical aspects of the project in a short period of time, but also aligned its product offering with Microsoft's objective of helping its customers drive Digital Transformation and use the power and scale of the Microsoft Azure Cloud to enable payments transaction processing".

Chief Innovation Officer, Microsoft Gulf. October 2016

By leveraging a purely virtualised software and security design that is built using .net framework and SQL technologies, NEC Payments has been able to create a flexible and agile processing solution that is native to the Microsoft platform and to Azure.

Utilising the Microsoft platform, and re-engineering the design of the processing engine from scratch, has enabled NEC Payments to build a technology product that is compliant with the most recent thinking in cyber security and that provides the flexibility to cope with current and future market and product developments. Its virtual account-based hierarchy is fully tokenised and compatible with multiple external transaction and integration channels via a set of secure and flexible open-APIs. This enables external networks and payment devices, such as MasterCard EMV or contactless cards, core banking and EFTS; to be seamlessly handled alongside other more innovative channels like external digital wallets or cryptocurrency accounts; or integrations with the latest CRM and ERP solutions built on Microsoft Dynamics 365 or other business process platforms.

Additionally, virtualisation has been achieved – whilst maintaining PCI-DSS L1 v3.2 security requirements – through the development of a highly innovative Software Security Module (SSM). The SSM is deployed into a segregated virtual machine that operates in a high security zone and performs the secure processing operations that are in most cases handled by a HSM. These operations include multi-level encrypted key storage; multi-custodian key injection, key generation and check sum validation; and a processing service that manages keys and cryptographic work during operational flows and communications with other platform components.

As well as opening-up a broader range of deployment and scalability options; the SSM also increases processing capacity through the simultaneous handling of multiple cryptographic operations - for example as seen in an incoming authorisation from a payment scheme - resulting in higher performance and volume handling capability than many traditional HSMs.

These, and other innovative features of NEC Payments software product, when coupled with Azure's powerful, highly-scalable, resilient and secure infrastructure, facilitate deployment at a significantly faster pace than traditional on-premises

environments, and enable NEC Payments to offer its customers the widest range of deployment options in the industry.

1. **Pure cloud infrastructure**
    Fully redundant production and DR environments hosted in Microsoft Azure can be deployed and scaled-up or scaled-down, in a matter of minutes, in any of Microsoft's regions globally. These environments can be operated on a SaaS basis by NEC Payments as a Microsoft Cloud Services Provider, or can be installed as a licensed product and managed by customers themselves under Azure accounts that they operate with Microsoft.

2. **Hybrid infrastructure**
    Azure environments can be created for use as disaster recovery and business continuity planning resources linked to traditional on-premises environments, with near to zero recovery point and recovery time objectives, and at a fraction of the expected usual costs.

3. **On-premises**
    NEC Payments recognises that in some situations there remain regulatory and policy challenges to running secure workloads or hosting sensitive data in the cloud. In addition to its Azure public cloud capabilities, NEC Payments has engaged with Huawei as an Enterprise Partner and has built a fully redundant on-premises data centre in Bahrain. Through this partnership a standardised high-performance, low-foot print hardware, network and security design has been created, founded upon Huawei enterprise servers and networking appliances. This standardised design can be replicated into client or co-location data centres as a private cloud to satisfy scenarios where on-premises hosting – or hosting within specific geographies- is a mandatory corporate policy or compliance requirement of a regulator.

The standardised hardware, network and security design that has been developed by NEC Payments to run within its on-premises private cloud and Microsoft Azure public cloud environments provides the highest levels of security and protection for data and network traffic, and has been audited and certified as being compliant with PCI-

DSS L1 v3.2 – the most recent version of the highest level of the ultra-stringent international Payment Card Industry Data Security Standard.

The design uses a multi-zoning approach to create and group virtual LANs that are dedicated to particular types of data, processing operations, security levels and access requirements. Strict access controls are implemented to restrict traffic across zones, and permissions for connections between software components is managed - using rules specific to each software module and virtual instance - to block unknown or non-standard network traffic. All internal network traffic is encrypted using TLS1.2.

Administration of the platform is managed according to the highest levels of security by segregating production and administration network traffic across physically and logically separate networks. External access into processing environments for administration purposes is only allowed across VPNs that are protected using two-factor authentication. Dedicated network monitoring; logging and event management; data replication, virtualisation and back-up; patching; and intruder detection and prevention systems; are deployed to maintain control and audit trails.

In addition to its use as a production resource, NEC Payments has also found cloud infrastructure to be a valuable and effective resource to supplement its internal development and testing environments; and to provide a flexible, always-there, scalable resource for prototyping and user acceptance testing.

Using a similar approach that it took to creating a standardised network and security design; NEC Payments has also developed a standardised template for its Azure resources. The template can be copied within the same Azure region, or into any region globally, to spin-up and roll-out copy processing environments in a matter of minutes. The resources can be used to create new environments – for example, a segregated user acceptance testing environment dedicated for a specific customer, project or testing scenario - and can also be used for prototyping and piloting new products or variants without impacting the on-going operation of mature products and work flows. The deployment capability is near-immediate and provides virtually unlimited capacity for development, prototyping and testing operations.

Microsoft Azure flexible pricing model means that the creation and use of these environments are charged for by actual processing consumption only, meaning you only pay for the time that the environment is up and running. It's simple, highly-available, and economical.

However, working within the financial services industry requires risk assessments to be performed and decisions to be made taking account of many factors in addition to technical and economic benefits. For this reason, establishing and maintaining the trust of clients and the security of data and solutions is critical; and security, risk management and compliance must be at the front and centre of everything that organisations like NEC Payments do.

NEC Payments have embraced these regulatory and compliance challenges; and in addition to technical security, they place a high value on governance and the strength of business policies, processes and procedures. As an Ancillary Services Provider licensed and regulated by Central Bank of Bahrain, they are required to build and maintain robust compliance, risk management, and corporate governance frameworks.

They have implemented and are in pre-audit operation of an Integrated Management System that meets ISO 9001 Quality Management and ISO27001 Information Security Management standards, and are also currently in the process of preparing for a SOC1 audit to ISAE3402 standard. The ISAE3402 standard tests the control mechanisms that are put in place by service organizations that are engaged by clients to perform sensitive data or transaction processing functions and covers the functional capabilities from a technical perspective and the business policies, procedures and control mechanisms that are deployed.

NEC Payments' approach echoes that taken by its partner Microsoft, who are also passionately committed to security, privacy and creating a trusted environment in the Azure cloud. Microsoft Azure cloud infrastructure is independently audited and compliant with PCI-DSS, as well as more than 50 other international security and regulatory standards. Microsoft have a privacy and data protection policy that prohibits data hosted in the Azure cloud from being accessed or used and which

compiles with ISO27018. There are separate legal terms and conditions that specifically govern Microsoft's commitments to Financial Institutions using Azure.

With the development of its software, and its ground-breaking deployments in the Microsoft Azure public cloud, NEC Payments is making a significant contribution to the digital transformation of the Middle East payments industry. However, it recognises that the financial services industry that it serves is conservative and risk adverse, and as such views the significant investment in time and resources necessary to also lead the way in the adoption of standards and compliance frameworks as fundamental to the creation of trusted relationships with its customers, partners and the regulator.

For further information about NEC Payments, its technologies and infrastructure deployment options please contact:

Nissrin Damdam, Business Development Manager
E: nissrin.damdam@necpayments.com
T: +(973) 1720 3000 x107
M: +(973) 6660 0400

NEC Payments B.S.C(c)
32 Classic Tower, Building 869
Road 3618, Block 436
Seef, Kingdom of Bahrain