Background

Security is an inherent part across the IaaS Trusted Public S5 platform and is applied as a key principle at all levels of the architecture. The platform is globally certified to the ISO/IEC 27001:2005 standard.

Within the UK, Fujitsu assert the TPSS platform as suitable for usage by the Public Sector for OFFICIAL & OFFICIAL-SENSITIVE dependent on any necessary associated controls required within the application running on the TPSS platform.

This document presents how IaaS trusted Public S5 provides protected, reliable, secure and highly available hosting environment for your key business applications and services.

Information Assurance

Fujitsu assert the TPSS platform as suitable for usage by the Public Sector for OFFICIAL & OFFICIAL-SENSITIVE, equivalent to strong commercial grade security. This is dependent on any necessary associated controls required within the application running on the TPSS platform and it is the responsibility of the customer to assess the platform in conjunction with Fujitsu based on their specific requirements and risk profile.

The Infrastructure

In designing the infrastructure for TPSS, Fujitsu have used the same attention to detail and best practice standards to ensure customers have the most secure and reliable platforms possible, to run their systems.

Reliable

Fujitsu hardware is world renowned for its build quality, durability, performance and energy efficiency. With a typical MTBF (Mean Time Between Failures) of 6 years and redundant, hot swap components, it was the natural choice for Fujitsu to use PRIMERGY servers and ETERNUS storage in this platform. The hardware however is only part of the story. The most reliable systems can become flawed if they are not built or managed correctly and this is where the platform comes into its own, with enterprise-class architecture and innovative management backing up the hardware.

Resilient

Resilience is built into every aspect of the platform. Built on a round-robin allocation and failover architecture, as new virtual machines are created they are stored sequentially on different physical servers.

In the rare event of a physical server failure, any affected virtual machines will be migrated to the next available server. This is done automatically with the minimum amount of downtime. It must be noted that during this failover stage, communication with that particular virtual machine will be lost. However, there are measures that can be architected to ensure that even though a virtual machine has failed, service availability is maximised and data loss is minimised. These are explained in the Virtual Systems section (see below).

A failure doesn’t even have to take place before a virtual machine is migrated. When there are indications of pending physical problems on a server, all virtual machines will be allocated to other servers. All services and any information in the virtual machine’s memory will be retained and the user will never know this has taken place.

A full inventory of spares is kept within the Technical Halls that are manned 24x7. If a hardware failure occurs, there is no need to request a parts delivery or call out for an external engineer – (eliminating a potential security breach). The hardware, spare parts and engineers are all in the same room. With so many components within the servers and arrays being redundant and hot swappable, repairs can take place without the need to power down the hardware.

Fujitsu have given the storage element of the platform as much consideration to ensure that data stored on the platform is safer than storing it in-house. All data stored in the cloud is in a RAID5 configuration. The data is mirrored to separate disk arrays before management software
uses "data-striping" to randomise data location. If a single disk, volume, disk tray or entire array is lost, a user’s data is still completely intact and accessible.

This level of excellence is not just reserved for the physical servers and storage, the whole infrastructure has been designed this way. VLAN technology controls the data path between the ETERNUS Storage Array and the PRIMERGY Servers with resilience throughout and no single points of failure. If a switch or router or cable fails, there will always be an alternative path in operation.

Secure
We have shown how reliable and resilient the physical infrastructure is. Now Fujitsu can demonstrate the excellent security measures in place.

Firstly, virtualisation technology ensures that IaaS Trusted Public S5 client accounts are separated. Users in one Contract can in no way access virtual systems or data belonging to another Contract. Likewise, users can be assured that their virtual systems and data are just as well protected. Systems and data CAN be shared between users WITHIN a Contract but even then it is governed by strict user roles and access privileges. This is covered in more detail in the next section.

One would expect all data stored to be encrypted and this platform is no exception. Fujitsu use a custom encryption level equivalent to AES 128bit. The ETERNUS Data Storage Array handles data encryption within the confines of the Storage Array. Data is encrypted when stored and decrypted when retrieved. This is performed automatically and transparently.

The platform guarantees data residency and Fujitsu does not move customer data to another location or country, unless specifically requested by the customer. This preserves customer ownership of their information and maintains regulatory compliance.

When a virtual machine or virtual disk is returned (deleted) by the user, zero overwriting is performed before it can be re-used. Likewise, when a physical disk fails, it is subject to the same process. No encryption keys are located outside of the array and no users have access to the keys. Even if an unauthorized user could remove a physical disk it would be impossible to decrypt and read the data on the disk.

The User
No matter how secure the platform buildings and infrastructure is, it is designed for customer use and controlling customer’s access and usage is arguably the biggest challenge of them all. In constructing the IaaS Trusted Public S5 Platform, Fujitsu has more than met these challenges and the security measures that have been put in place will ensure a safe and consistent user experience.

Trusted Community
The platform itself is not an open system that anyone can just sign up to; it is a ‘Trusted Community’ platform. Registration and acceptance to the platform is limited to registered companies, charities and public sector organisations. An IaaS Trusted Public S5 account is only activated after Fujitsu has ensured that registrants meet these criteria, and run a credit check. This means that members of the public and inappropriate organisations cannot use the platform, further protecting Fujitsu IaaS Trusted Public S5 customers from malicious activity.

Also, Fujitsu do not hold administrator privileges or access rights to customer virtual machines – unless it is specifically granted by that customer.

Secure Access
Initial access to the platform is done via a username and a password (with a minimum of 16 alphanumeric characters). During this first visit, a PKI certificate (256 bit encryption) is stored on the client’s workstation. Subsequent visits by the client to the Cloud can only be carried out from that workstation using the certificate.

Access Roles and Privileges
All users within a contract can see the different virtual systems created in that contract. However, they can only access those systems that they are authorised to.
By default the Central Administrator has access to all virtual systems within the contract. The administrator within an account has the ability to create new **Master Authorization Patterns** via the **Access Control: Central Management List** function of the portal. Through this function the Administrator can grant permissions or capabilities for portal users as shown below:

![Access Control: Central Management List](image1)

The simplicity is its strength. At the touch of a button, administrators can allow or deny access to any of the virtual systems in their contract. A particular user may need to be assigned more granular roles and access permissions within the Portal and this can be achieved quite simply by creating **Custom Authorization Pattern** via the **Access Control: Virtual System Management List** function of the Portal. This function provides a greater granularity of access control that that offered by the Master Authorization Patterns as shown below:

![Access Control: Virtual System Management List](image2)

Once Central and Custom Authorization Patterns have been created, these can be assigned on a per user, per vSYS basis via the **Access Control: Authorization List** function.
The Virtual System (vSYS)

Finally, there are the virtual systems themselves – the nucleus of the Trusted Public S5 Platform. Fujitsu have again incorporated stringent resilience and security measures in the composition of the virtual systems.

Secure

When each virtual system is created, a self-service Firewall is deployed. This is an automatic process carried out by the platform so virtual systems are immediately protected from the moment they are created. Furthermore, the default setting of the Firewall is ‘drop all’ so no traffic can enter or leave the virtual machine without the user configuring it.

SSL-VPN is used for all connections between the platform and Customer sites. The connection itself is bi-directional so the traffic flow is completely secure whether it is from the virtual machine to a client’s workstation or vice versa. Any connection to a TP55 physical server also uses SSL-VPN.

All data transferred between a virtual machine and a client is carried via HTTPS - the combination of HTTP with SSL/TLS protocols. HTTPS provides encrypted communication and secure identification typically used for online payment and sensitive corporate transactions.

The three tier segmented architecture (DMZ, Secure 1 and Secure 2) provides additional protection. In the same way you would configure hardware architecture, only servers in the DMZ can be accessed from the public internet. Application and database servers should be architected to be in the other two tiers and thereby sheltered from external access. The Firewall has to be configured to allow authorised users access to the servers in any segment.

Shared Services

Fujitsu have a number of shared services built into the TP55 Platform so users do not have to look externally for compulsory patches, updates, DNS or NTP services, thereby removing this common security risk. (There are common shared services that a typical architecture would require – Windows and YUM patches and updates, DNS and NTP servers. Such services would typically come from an external source. This inevitably leads to third party data entering the architecture – a definite security risk).

Enhanced Communication

The Intranet function provides communication between virtual machines within a virtual system. This function can further enhance the TP55 Platform by allowing the same levels of secure communication between a Customer’s virtual machines and their existing servers hosted in a Fujitsu Data Centre. Thus providing a hybrid style cloud architecture but in a completely secure and controlled environment.

Security is ultimately the client’s responsibility

While Fujitsu takes its responsibilities for providing a robust and secure infrastructure very seriously, it is ultimately a client’s responsibility to secure their business. Clients are responsible for installing, updating and running their own anti-virus (etc. etc.) and for configuring their firewalls to defend against possible malware attacks and unauthorised intrusions.

The Datacentre

Every Fujitsu Datacentre is designed and built to provide a highly resilient, highly secure environment that maximizes availability. In the UK, the Service is operated out of two Tier III Data Centres, providing a choice of geographical location with guaranteed UK data residency. In addition, the London North Data Centre is the first to be awarded Gold status by the Uptime Institute for both its Build and its Operational Sustainability. For more information, please refer to Fujitsu’s London North Data Centre and Fujitsu’s London East Data Centre.

Perimeter Defence

The UK&I Data Centres boast multiple internal / external CCTV cameras and on-site security with a dedicated 24x7 Security team. There are secure loading and delivery areas with pre-arranged loading and delivery times and electronically operated gates. All exterior doors have anti-ram protection and both entire site are protected by an electric fence.

Security

There is a dedicated 24x7 Site Operations Team monitoring access control and the environment at all times. Vehicle and pedestrian entry points are constantly controlled and secured. Each reception has turnstile access control to enter the DC and all Technical Halls have Biometric access. Each DC utilises Restricted Access Levels so employees can only enter areas relating to their roles. All other areas will be inaccessible.
Fire Protection
To safeguard against fire, both data centres are installed with smoke detection. All technical halls and electrical rooms have inert gas suppression systems in place. All mechanical plant rooms, DC Bridge and offices have fog, mist and sprinkler systems. All corridors and technical halls have "Very Early Smoke Detection Alarms" installed.

Power Resiliency
The DC has full N+1 redundancy on power distribution units (PDUs), generators, and air conditioning units. This means there is no single point of failure thus enabling Fujitsu to offer a high availability hosting service.

Furthermore, the London North Data Centre is amongst other Fujitsu sites listed by the UK Government as critical to National Infrastructure and therefore fuel supplies to these locations are prioritised in times of shortage or other issues.

Award Winning
Fujitsu has received widespread recognition for its achievements in service reliability, availability and energy efficiency. Through innovative solutions and best practice standards, Fujitsu have been short listed and successful across a number of specialist awards, including:

- 2008 – Tier III facility certification awarded by The Uptime Institute (first in Europe)
- 2011 – Gold Operational Sustainability certification awarded by The Uptime Institute (first in Europe)
- Most Sustainable Refurbishment - Winner - The Sustainable Building Services Award 08
- Innovation in the Mega Data Centre - Winner - Data Centre Awards 2008
- Green in the Data Centre - Finalist - Data Centre Awards 2008
- BP Environment Award - Finalist - BCS IT Industry Awards 2008
- Future Thinking & Design Concept - Winner - Data Centre Leaders Awards 2009
- Green Policy Solution category for Data Centre Energy Efficiency Programme - Winner - Fujitsu Group Environmental Contribution Awards 2010

The datacentre also has the following classifications:
- Information security rating AAA
- ISO 9001
- ISO 14001
- ISO/IEC 27001:2005

In Conclusion
This document provides an overview of how Fujitsu takes a pragmatic approach to security in IaaS Trusted Public S5.

Security is critical across the Fujitsu organisation and underpins the provision of comprehensive, robust, reliable and secure platforms and services for our private and public sector clients.

Security provision is subject to continual review and improvement and dedicated teams are in place to monitor, manage and react to any real or perceived threats to the hosted infrastructure and our client data, applications and services.