D-4.1.7 Technology and Communications Standards

Ofgem Switching Programme

Decision

Overview:

The Technology and Communications Standards for the End-to-End (E2E) Switching Arrangements is an important product deliverable of the Design Level Specification (DLS) Phase of the Ofgem Switching Programme. It defines a set of recommendations and guidance regarding the capabilities and attributes which the technology solution delivering the To-Be E2E Switching Arrangements should deliver.

Context

This document should be read in conjunction with DLS-4.1.5 E2E Solution Architecture.

Associated documents

References are shown in the following format: Ref. [09].

REF	TITLE	VERSION / DATE
1.	D-4.1.5 E2E Solution Architecture	1.0
2.	D-4.1.10 E2E Security Architecture	1.0
3.	D-4.1.4 E2E Switching Arrangements NFR	1.0
4.	D-4.1.6 E2E Operational Choreography	1.0
5.	D-4.1.9 E2E Switching Service Management Strategy	1.0
6.	Govt open standards https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles	N/A
7.	OWASP standards https://www.owasp.org/index.php/Main_Page	N/A
8.	National Cyber Security Centre https://www.ncsc.gov.uk/	N/A
9.	Centre for the Protection of National Infrastructure https://www.cpni.gov.uk/critical-national-infrastructure-0	N/A
10.	SANS Paper illustrating the principle of Defence in Depth https://uk.sans.org/reading-room/whitepapers/basics/defense-in-depth-525	1.2E
11.	SANS Reading Room – resources, guidance and information regarding information security best practice https://uk.sans.org/reading-room/	N/A
12.	D-4.1.2 E2E Detailed Design Models	Wave 3 baseline

Contents

Executive Summary **4**

2. Introduction **5**

Goals and Objectives 5

3. Technology & Communications Standards **7**

General 7

Availability & Resilience 7

Scalability 9

Supportability 10

Portability 10

Infrastructure 10

Networking & Communications 11

Data & Interfaces 12

Security 14

Management & Monitoring 16

4. Conclusion **18**

Appendix 1 – E2E Solution Architecture Glossary **19**

Executive Summary

1.1. The Technology and Communications Standards for the End-to-End (E2E) Switching Arrangements is an important product deliverable of the Design Level Specification (DLS) Phase of the Ofgem Switching Programme and defines a set of recommendations and guidance to architects, project managers, system administrators, developers, procurement personnel, industry stakeholders and others who require guidance and directions on the implementation of standardised technology and technology products for the design, development, integration, deployment and operations of Information, Communications and Technology (ICT) components of the new E2E Switching Arrangements.

1.2. It is not the intent of the Technology and Communications Standards to replace the individual set of standards and standard products employed by the various stakeholders throughout the E2E Switching Arrangements eco-system.

1.3. The Technology and Communications Standards is not intended as a comprehensive list of standard products in use within the E2E Switching Arrangements eco-system. It defines a set of requirements and guidance regarding the capabilities and attributes which the technology solution delivering the To-Be E2E Switching Arrangements, should deliver.

1.4. Additional background information and context for the Ofgem Switching Programme can be found in D-4.1.5.E2E Solution Architecture (Ref.[01]) and at the following link:

https://www.ofgem.gov.uk/electricity/retail-market/market-review-and-reform/smarter-markets-programme/switching-programme

1.5. For additional detailed information about Security for the E2E Switching eco-system – refer to the Ofgem Switching Programme D-4.1.10 E2E Security Architecture (Ref. [02]).

2. Introduction

2.1. The Technology and Communications Standards (TCS) for the End-to-End (E2E) Switching Arrangements is a companion product which should be read in conjunction with the DLS-4.1.5 E2E Solution Architecture.

2.2. Whereas the E2E Solution Architecture defines the logical business, application and data architecture required to deliver the To-Be switching arrangements, the TCS will provide additional guidance to architects, project managers, system administrators, developers, procurement personnel, industry stakeholders and others on the implementation requirements and attributes for the technical solution.

Goals and Objectives

2.3. The primary goal of the Technology and Communications Standards is to define a set of standards as a guide and reference to architects, project managers, system administrators, developers, procurement personnel, industry stakeholders and others who require guidance and directions on the implementation of standardised technology and technology products of Information, Communications and Technology (ICT) components for the DBT (Design, Build, Test) Phase of the Ofgem Switching Programme.

2.4. The Technology and Communications Standards addresses the fundamental technologies that comprise the ICT landscape, and focuses on standards that promote successful managed services within a reliable and secure environment. They try to balance and align industry-wide investments in ICT with the needs of the Ofgem Switching Programme and the Open Standards Principles of the UK Government.

2.5. Additional information on the UK Government – Open Standards Principles can be found on the link below:

https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles

2.6. The Technology and Communications Standards will not place specific restrictions on the individual technologies, platforms or toolsets which organisations use to build, test and deliver the components of the CSS solution. However, the Technical and Communications Standards document does aim to:

- Augment the logical system/application architecture defined in the E2E Solution Architecture with product selection & implementation guidance. In combination, these two products should provide guidance to assist with the final product selection exercise.
- Define the qualitative attributes and capabilities which the CSS solution (and its constituent components) are required to demonstrate.

- Reference relevant National guidance & industry recommended/best practices where these are applicable to the solution e.g. guidance papers from the UK National Cyber Security Centre (NCSC).
- Provide references to authoritative DLS design products where relevant.

2.7. Due to the broad scope of this document, there will be some overlap with the coverage of the following DLS products:

- D-4.1.10 E2E Security Architecture (Ref.[02])
- D-4.1.4 E2E Switching Arrangements NFR (Ref.[03])
- D-4.1.6 E2E Operational Choreography (Ref.[04])
- D-4.1.9 E2E Switching Service Management Strategy (Ref.[05])

2.8. The Technical and Communications Standards document will not attempt to define the following:

- The individual set of standards and standard products employed by Stakeholders or Service Providers within the E2E Switching Arrangements eco-system. These parties are expected to define their own standards as appropriate to their individual circumstances.
- While the TCS will describe the attributes which the solution must exhibit, it will not specify a list of approved technologies, platforms, vendors or suppliers from which the solution must be constructed.
- The methodologies which should be followed in the design, test, build, delivery of solution components outside of CSS. Participants are advised to adopt an approach which best suits their individual business model and capability.
- The methodology by which the operation of the associated Switching service is expected to be managed – refer to D-4.1.9 E2E Switching Service Management Strategy (Ref. [05]) for further information on this topic.

3. Technology & Communications Standards

General

3.1. The solution and the Service Operator's Target Operating model, must be responsive and flexible to change where change is required.

3.2. The solution must include automated mechanisms to minimise and control operational IT costs and provide real-time billing information.

3.3. System architecture should be modular and adaptable to changing regulatory requirements.

3.4. Technology roadmaps will be produced to support the strategic evolution and maintenance of the Switching technology solution. Roadmaps must facilitate the following activities:

- Planning and management of technology related change within the solution
- Identification of areas of risk within the technology solution
- Maintenance of a definitive software inventory for the technology solution
- Identification of the product lifecycle support status for all software components of the technology solution

3.5. Both Proprietary (Commercial Off The Shelf - COTS) and Open-Source products may be used within the solution.

3.6. Further guidance regarding the principles which should be applied to the selection and usage of Open Source software for UK Government initiatives, is provided in Ref. [06].

Availability & Resilience

3.7. As defined in Ref. [04] the CSS has a formal availability requirement of 99.75%, excluding agreed maintenance windows. This section will provide additional guidance as to how the CSS should handle failure, with that figure in mind.

3.8. The solution must minimise the impact of component failure to the operational switching service. A component could be one or more of the following:

- Hosting facilities (i.e. datacentres) and their associated utilities.
- Underlying physical hardware e.g. servers, storage, network & security infrastructure, power supplies.
- A server or an instance of an operating system.

- Applications, including web-servers, middleware [1].
- Databases and/or data stores.
- Management & monitoring tooling.

3.9. It must be possible to continue to receive incoming requests/messages even if the core CSS solution is not capable of processing them at that point in time. Situations where this may be applicable include:

- When the system is undergoing planned maintenance.
- If system is experiencing unplanned outages.
- If system demand is exceeding available capacity and no resources are available to service the processing of incoming requests.

3.10. To avoid overloading individual components the solution must be capable of distributing load across multiple, independent processing nodes, which may or may not be located in the same hosting facility.

3.11. The solution must respond dynamically to significant changes in volumes via configurable thresholds, which will allow:

- Automatic scaling out to meet spikes of increased demand within the agreed volumetric profile (see Ref.[04] for details).
- Automatic decommissioning of additional resources deployed through scaling operations, if continued utilisation drops below a configurable threshold.
- Non-disruptive scaling – it must be possible to perform a scaling operation (i.e. scaling out or in) without interruption to the Switching Service.

3.12. Protection against data loss & corruption is required. Service Providers must implement a backup regime which protects resources (data & other service critical resources such as customised server build images etc.) according to their criticality and data classification. This regime will:

- Contribute to minimising the overall data storage costs of the CSS by:
  - Minimising overall data storage volumes & redundancy.
  - Using automated lifecycle management to ensure that data is resident on the appropriate class of storage.
  - Use partial backups in favour of full backups where feasible.

[1] Middleware – a collection of software services which provide the capability for integration between heterogeneous, distributed systems.

  - Allow easy (automated) removal of backups which are no longer required.

- Support the encryption of backups.
- Provide secure archiving (& retrieval) facilities for data requiring long term storage.
- Provide the facility to restore data at various levels of granularity – i.e. restore or refresh an entire database, recover to a specified point-in-time or transaction.

3.13. If the Service Provider believes that the CSS service will not be operational for a period which exceeds the maximum (regulator defined) switching time window, alternative (i.e. Business Continuity / Disaster Recovery) facilities must be available to process the backlog within the required window. The Recovery Point Objective (RPO) & Recovery Time Objective (RTO) for the service are defined in Ref.[03].

3.14. The solution should support concurrent processing/receipt of requests from multiple participants.

3.15. For guidance, at the time of writing the service has an estimated daily (peak) volume of 31,000 switch requests and there are 93 Market Participants. Further detail and analysis of service related volumetrics is available in Ref.[03].

3.16. CSS must support synchronous and asynchronous processing as appropriate[2].

Scalability

3.17. The CSS solution must be capable of dynamically adapting to changing demands in workload. It should be possible to configure thresholds so that this behaviour can be driven automatically.

3.18. Network solutions should include the flexibility to accommodate increased network traffic without requiring bearer upgrades.

3.19. It must be possible to scale individual components of the CSS solution independently & in line with the specific demand on that component. For example, the load on message queuing services may be high at a given point in time, but database load may be low – in this situation it must be possible to increase available resources in the messaging component independently of database resources.

[2] See the following articles for an explanation of asynchronous and synchronous processing in computer systems:
https://technet.microsoft.com/en-us/library/cc978253.aspx
https://docs.oracle.com/cd/E17984_01/doc.898/e14729/sync_async_processing.htm
http://camel.apache.org/asynchronous-processing.html

3.20. The system should minimise costs wherever possible by deploying no more compute resources than required to process the mean hourly request volume, however it should also allow for automated dynamic (horizontal) scaling.

Supportability

3.21. All technologies deployed within the solution must be backed by an appropriate technical support capability, and/or vendor technical support agreements – at all times during the lifecycle of the solution.

Portability

3.22. The CSS solution must not be tightly coupled to a given Service Provider's existing business operations.

3.23. If deployment within a Service Provider owned datacentre is necessary then the chosen solution architecture must allow for a simple and timely transition to another Service Provider, or physical location.

3.24. The use of Proprietary data formats within any part of the Switching technology solution are discouraged, as these will inhibit its future portability.

3.25. Solutions must enable an easy transfer of operations to a secondary Service Provider

3.26. Where Proprietary (COTS) products are selected, the desired functionality should be capable of being delivered through product configuration or integration with other standard products. Customisation should be justified with a supporting business case, demonstrating that:

- The requested customisation is fully supported by the software Vendor
- Customisation of the product will not inhibit the future development or portability of the solution e.g. by tightly coupling it to a specific vendor, product or proprietary technology.
- The Vendor has formally agreed to merge the customisation into the software product's Main feature set – solutions requiring fully maintained, separate branch releases are not permitted.

Infrastructure

3.27. Requirements governing where the solution & its data can be geographically hosted are provided in Ref.[02].

3.28. Solutions should be able to demonstrate the following attributes:

- Automation

- Flexibility
- Portability
- Scalability
- Security
- Cost Effectiveness
- Time to Market
- Unified Management Capability
- Platform Evolution

3.29. A Hybrid hosting model will be considered if it can be demonstrated that it does not significantly constrain any aspect of the solution.

3.30. The hosting environment must support the automated build and deployment of resources from pre-defined templates.

3.31. To support optimisation of development, test and release management processes and the timescales associated with them, automated deployment of replica Production and Non-Production environments (either full scale or scaled-down) from templates must be possible.

3.32. Service Providers must have the capability to deploy & implement changes into the appropriate environment within minutes of approval.   Availability

3.33. The Service Provider must maintain a versioned catalogue of infrastructure resources deployed for the CSS.

Networking & Communications

3.34. A data communications network (the 'Switching Network') will be procured and commissioned to support the operation & management of the CSS. The specification and design this network will be finalised as part of CSS Detailed Design. The requirements listed in this section are appropriate to the Switching Network.

3.35. Systems participating and exchanging data as part of the E2E switching arrangements will require connection to the private 'Switching Network'.

3.36. The Switching Network will implement access control and authentication mechanisms in accordance with requirements laid out in Ref.[02] E2E Security Architecture.

3.37. Volumetrics detailing the total, average and peak number of switch requests which must be supported by the Switching Network are laid out in Ref.[04] D-4.1.4 E2E Switching Arrangements NFR. It is important to note that while each switch request is a single transaction between supplier and customer, this will involve the exchange of many messages between multiple systems, each of which will require connectivity to the Switching Network.

3.38. All communications between the CSS and other systems within the E2E Switching ecosystem will occur through the Switching Network.

3.39. The relevant governance instrument will be established which will lay out the baseline set of controls which Participants must comply with order to be granted connection to the Switching Network. These controls cover Technical, Procedural, Physical and People related areas.

3.40. Physical controls must be implemented to control the flow of data within the Switching Network. Examples of applicable controls may include a combination of network and application layer firewalls, host based firewalls and physical network segregation.

3.41. The approach to security should apply the principle of Defence in Depth to the Switching Network and the CSS solution. Ref.[10] provides practical examples of the application of Defence in Depth to 3 common scenarios.

3.42. A tiered network topology should be implemented, in which the tiers provide segregation between components according to the risk profile of the services they provide and the data which they manage. Appropriate controls must be in place to manage the flow of traffic into and out of each tier.

3.43. Systems management & administration access must be segregated from user access. This may include one or more of the following controls:

- A dedicated out-of-band management network or VLAN
- Separate network interfaces for administration and user traffic
- Separate user and administrative interfaces, operating on different network ports

3.44. Data/message flows between the CSS and other systems are defined in Ref.[02] (Switching Design Repository (Abacus)), with supporting information regarding their sequencing and coordination defined in Ref.[04] (Operational Choreography).

3.45. DLS 4.1.10 Security Architecture will define the data classification scheme which will apply to the Switching solution and the controls which must apply accordingly.

Data & Interfaces

3.46. The CSS solution will support both real-time and batch interface mechanisms, with selection of the appropriate mechanism being dependent on the characteristics and requirements of the specific process which that interface enables. For each interface, the mechanism and its associated interface pattern are defined in Ref.[01].

3.47. Loose coupling between components is preferred as this reduces the interdependency between functional components, in turn reducing the cost, complexity and timeliness of implementing change.

3.48. New interfaces within the E2E To-Be switching arrangements are characterised according to the following 4 types of interaction pattern:

- Outbound interfaces from CSS have one of the following message interaction patterns:
  - **Notifications** – a message between two systems that informs the recipient of an event and provides some related information in a structured form. CSS will issue a number of different types of Notification, which Recipients have no requirement to act on and may (or may not) choose to receive:
    - Switch request validated
    - Switch request confirmed (no objection raised)
    - Switch request secured (gate closure on D-1)
    - Agent update
    - Change of shipper
    - Change of domestic/non-domestic indicator
    - Initial registration
    - Switch Objected
    - Switch Withdrawn
    - Switch Annulled
    - Deactivate registration
  - **Enquiry** – a message between two systems that informs the recipient of an event and provides the recipient with an opportunity to respond in a structured form (within a fixed timescale). The response may or may not be mandatory, but confirmation of receipt is required.
  - **Synchronisation** – a formal mechanism designed to keep information shadowed in one Central Data Service in line with that mastered in other systems. A synchronisation may take place before (and after) an event/activity to ensure that all involved parties share the same information.
- Inbound interfaces to Central Data Services Systems follow the **Update** interaction pattern, defined as:
  - A mechanism to issue notifications of proposed changes to switching related master data which must be processed by Central Data Services (CSS, UK Link, MPRS, DSP, ECOES, DES). Acknowledgment of receipt is mandatory, and a formal response message may be required following processing, but is optional. The receiving (Central) data service must maintain a record of all Updates received and applied.

3.49. Both batch and real-time interfaces may employ Message Oriented Middleware or other B2B integration platforms, however no assumptions are made regarding the presence, capability or configuration of such systems.

3.50. The CSS switching application should be largely stateless – clients will send all data required to process a given request in isolation, regardless of previous interactions with the server.

3.51. All requests will be authenticated and authorised by the CSS service prior to execution.

3.52. Requests should be idempotent - a specific request should produce the same outcome however many times it is performed.

3.53. The CSS server is responsible for maintaining resource state by default – in that it is the only system which can directly manipulate the data (resources) managed by the service.

3.54. Within the Switching Design Repository, each interface specification will include a message schema definition which defines the required structure and content for the message body.

3.55. CSS will perform validation of the message structure and the format of individual data fields/elements against the appropriate message schema definition. Message schemas will be defined in the ABACUS Switching Design Repository (Ref.[12]) as part of the CSS Detailed Design phase.

3.56. For well-defined data elements the system will be capable of performing field validation against appropriate business rules. For example, it should be possible to validate a date field to ensure that a specified switch date is valid and does not occur in the past.

3.57. The CSS solution should allow for requests to be processed in First in First Out (FIFO) order if necessary.

3.58. All messages sent or received by the CSS must include a relevant timestamp – time will be defined in local time as defined in Ref.[04].

3.59. CSS will not perform any data transformation – the interface specifications will define the format for data supplied to / consumed by the service.

3.60. Where data is synchronised between systems within the E2E arrangements, an eventual consistency model will be assumed, in which secondary ('slave') systems are no more than 1 hour behind the master system. This figure should be taken as a guide and may be refined during subsequent detailed design.

3.61. It must be possible to throttle and/or limit incoming requests to the CSS solution.

Security

3.62. The solution should comply with acknowledged industry good practice in application security. The following web resources provide detailed information and guidance in the area of information systems security:

- National Cyber Security Centre (Ref.[08]).
- OWASP (Open Web Application Security Project – Ref.[07]).
- SANS Reading Room (Ref.[11]).

3.63. All Service Providers will have in place Identity and Access Management solutions to authenticate and authorise user access to resources.

3.64. All computer system User accounts, and those of service accounts, should be centrally managed and administered.

3.65. The Principle of Least Privilege should be applied to all accounts – no accounts should have any more privilege than is required to perform their business process.

3.66. Service Providers must demonstrate compliance with UK Government recommendations for password management and complexity, as laid out in Ref.[08] - https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach.

3.67. Guest accounts will be disabled and/or renamed as appropriate on all servers.

3.68. Generic, highly privileged super-user accounts such as the UNIX-like 'root' account, must not be used for routine administrative duties.

3.69. All system access, including administrative access must be audited and performed using named accounts.

3.70. The solution must be compatible with Public Key Infrastructure security protocols and mechanisms. Further requirements can be found in Ref.[02] E2E Security Architecture & associated security workstream DLS products.

3.71. All systems must undergo hardening to minimise their attack surface. Un-necessary services and software should be disabled or uninstalled, and communications only permitted on defined ports and protocols. Guidance for system hardening is available from the National Cyber Security Centre (Ref.[06]).

3.72. A layered approach to security management must be employed in which Service Providers can demonstrate compliance with the principle of Defence in Depth (see Ref.[10]) – no single component should assume 'responsibility' for protection the entire solution from malicious intent.

3.73. Anti-malware software must be installed & operational on all systems communicating within the Switching Network. Automatic updates must be configured on at least a daily frequency, with an emergency update process for applying critical updates immediately if required.

3.74. All software should be patched to the latest stable release unless it can be operationally justified otherwise.

3.75. Service Providers must have a Patch Management process for the validation, testing and deployment of software updates to systems. The process must define how the criticality of updates is established and the associated protocols for their deployment.

3.76. Routine vulnerability scanning will be performed on all systems connected to the Switching Network. A policy will be established which will define the protocols for treating the various categories of vulnerability (H/M/L).

3.77. The Service Operator must conduct independent Penetration Testing on the CSS technical solution on an annual basis.

3.78. All requests must be encrypted in transit and signed using an agreed security certificate. It may be necessary to encrypt certain data items at rest – if the security requirements identify this as a requirement, a solution will be identified during the CSS detailed design.

3.79. Message integrity checking, and content/field validation will be performed on message headers and bodies to ensure they have not been intercepted and tampered with in transmission.

3.80. Message headers and bodies will be validated against the defined specification for the specified message type. Validation should include structure of the message body and the content type of each field/element.

3.81. The solution must have the capability to perform Anomaly Detection and should dynamically respond to 'out-of-band' events such as unsolicited Brute Force attacks.

3.82. Host-based Intrusion Detection should be deployed to all servers and configured to monitor access to system resources.

3.83. Auditing must be enabled for Network and User access, with logs stored in a standard format (e.g. Syslog). Logs should not be stored on their originating system indefinitely and must be transferred to a secure location as soon as practical following log rotation.

Management & Monitoring

3.84. The CSS will require an appropriate operational systems management & monitoring capability, as defined in Ref.[05].

3.85. It should be possible to manage the operation and configuration of the CSS solution via UI and API driven interfaces.

3.86. Automation of routine CSS management and administration tasks must be possible – (common) management tasks must be able to be performed programmatically as well as via the management tool UI.

3.87. The solution must be able to collect CSS system metrics, logfiles and specified events for resources as required within the solution.

3.88. 'Single pane of glass' monitoring should be available, with system metrics for all components accessible through a single application.

3.89. It must be possible to configure alarms which will issue alerts to appropriate support personnel.

3.90. The management toolset must support customised dashboards

3.91. The solution must support the use of standard SYSLOG format logfiles.

4. Conclusion

The production description for this document posed the following questions, with responses in italics:

1. Which components of the solution architecture will be subject to communications standards? With an explanation of the reason.

   The document proposes that a private 'Switching Network' should be procured, through which all switching related communications must occur. This provides assurance by enabling a consistent baseline control set to be applied across Participants in the To-Be switching ecosystem.

   The controls will be defined in a governance instrument (not yet defined) which describes the Technical, Procedural, Physical and People controls Participants must demonstrate in order to be granted connection to the Switching Network by the CSS Service Operator.

   All Participants with service interfaces to CSS – barring those which receive Notifications only – require compliance with the controls laid out in the governance instrument. Participants receiving Notifications only, do not require the capability to send information into CSS and will only receive outbound communications from CSS, hence they do not require full compliance with the controls. However, they may still be required to demonstrate partial compliance.

2. Do any communication standards need to be approved before service procurement and or regulatory change(s)? With an explanation of why the desired approach is necessary/ appropriate.

   To promote innovation, it is necessary to avoid specifying products, technologies or methods by which systems will communicate. Even high-level specifications or lists of example options have the potential to constrain Bidders thinking and are therefore not included.

   Consequently, the document focuses on the requirements & attributes which system to system communications must meet – and which naturally take the form of NFRs. These should ideally reside in the D-4.1.4 E2E Non-Functional Requirements product to avoid fragmentation.

3. What are the performance standards that need to be met by the ICT (information and communication technologies) components?

   The performance standards which must be met by CSS as a whole and by individual components of the solution, should be defined in D-4.1.4 to avoid the potential for fragmentation and inconsistency of requirements across the DLS product set.

In conclusion, the early specification of technologies, products or methods as 'standards' will undermine the Programme's requirement for a solution neutral position which does not influence the shape of Request For Proposal responses or constrain innovation.

Therefore, it is not possible to define specific (technical or communications) 'standards' without compromising the Programme's stated objectives and this Product instead focuses on defining the attributes which a successful solution should demonstrate, and in providing supporting commentary where required. These attributes are more naturally expressed as NFRs and should reside in the D-4.1.4 product accordingly.

Appendix 1 – E2E Solution Architecture Glossary

Please refer to the Glossary within DLS-4.1.5 E2E Solution Architecture for a full definition of all terms.