

MLL Telecom Ltd

Secure Cloud Services Platform (SCSP)

Service Definition



Date: January 2026

MLL Ref: G Cloud 15 - RM1557.15

Secure Cloud Services Platform (SCSP) - Service Definition

About MLL

MLL Telecom is a leading provider of managed Wide Area Networks and telecommunication services including LAN, Unified Communications (UC), Wi-Fi, and Security to the UK public sector. Our services are provided through our MLL's UK based support teams and engineering service and selected partners. Formed in 1991, MLL has established a reputation for customer-focused service delivery and agility.

Service Overview

MLL's Secure Cloud Services Platform (SCSP) is a network solution that MLL uses to deliver cloud services to Buyers in a secure fashion. It forms the basis of all cloud integrations for not only our own cloud services, which include Cloud Network Management, SaaS, IaaS and SASE offerings, it also connects Buyers to other cloud platforms including, but not limited to, Cloud Service Providers, (Amazon, Google, Microsoft, Sophos, Cisco etc), as well as the Internet and other private / semi-private cloud solutions including, HSCN, PSN and Janet. Key features include:

- Secure Software defined networking
- Direct access to Cloud Service providers
- Cloud managed and integrated national and regional connectivity solutions
- Other cloud-based solutions – Internet, HSCN, PSN, Janet, etc.



SCSP is a flexible cloud and cloud enablement solution, providing security and resilience to Buyers. It allows MLL to deliver our own cloud offerings, as well as swiftly integrating third party cloud solutions. More importantly, the SCSP delivers cloud services in a manner that brings end users, regardless of

their physical location, closer to the applications, data and services they need to use, thereby ensuring the best possible experience.

The service is fully supported by MLL's UK based 24x7x365 NOC and field engineering services.

Service Description

Secure Cloud – Cloud Managed SD-WAN / Zero-Trust Networking

MLL delivers cloud security to end users by employing encryption and traffic examination / remediation using SD-WAN and Zero trust networking principles. This is provided as a managed service overlay to the cloud, with self-service options also available.

The SCSP has the orchestration, reporting, management and self-service elements built into it, which Buyers simply need to join to be protected.

Buyers take advantage of the investment MLL has made in these cloud platforms, greatly reducing cost of migration and therefore the cost of a next generation security implementation.

All traffic from these cloud platforms and between the Buyer's sites and users is encrypted and passed through full 7-layer unified threat protection services. This is all performed in a hardware accelerated environment and therefore has almost zero effect on latency and absolutely no adverse effect on end user experience. In fact, the end user experience is usually greatly improved, not only from the architecture of the SCSP itself but through the application-aware nature of the service.

The software defined solution can identify over 5,000 known applications and custom applications can be added if needed. This in turn allows for traffic steering over multiple paths, with prioritisation at both the network layer and the software layer. Costs can be reduced by aggregating multiple lower cost paths. The security layer is regularly updated with updates being generated from a lab environment that receives telemetry from more than 5.8m devices under management.

The lab uses powerful AI algorithms to provide protection from emerging threats through behavioural analysis and is regularly updated to remain compliant with all emerging regulatory requirements. Self-service portals provide up to the minute information on network and application status with clear KPI and SLA driven dashboards. It will also allow Buyers to make changes in real time, providing safe and timely network interaction as needed.

Network Infrastructure

The SCSP Secure networking options are network agnostic. They can be delivered on private or public networks either through MLL or a third party, if necessary.

The SCSP can be delivered directly to the Buyer's sites as a private MPLS solution, which can lower initial security costs and allow for a staged implementation, as required.

MLL can also deliver this as Direct Internet Access (DIA) or a hybrid of both. This does require a greater degree of security overlay.

Optional Products / Services

To facilitate direct access to the SCSP MLL offers optional services:

Connectivity

Connectivity is built directly into the SCSP, this is an instrumental factor in providing the best end user experience.

Buyers have access to the following connectivity through MLL's SCSP cloud environment:

- National carrier networks
- Alternative Network providers (Altnets)
- National infrastructure partners
- National network aggregators

Through the investments MLL has made in these partnerships we are able to bring innovative, cost-effective, and secure solutions to Buyers. It should be noted that while pricing is included for all of these providers, connectivity choices are influenced by location. MLL's solutions team will be able to determine what is available to your sites, as a free of charge service.

Our pricing schedule includes the following data connectivity options.

- Full fibre Ethernet services from 100Mbps through to 10Gbps.
- Superfast and Ultrafast broadband solutions, including SOGEA, FTTP and FTTP equivalents.
- Traditional broadband solutions, including DSL service and MPF delivered services.
- 4/5G cellular data services.
- Low Earth Orbit satellite connectivity.

This connectivity offers a plethora of options for failover and resilience, from a simple 4G / broadband failover, through carrier diversity and in-life managed full fibre path diversity. MLL believes that one size fits all approaches are rarely the best answer. Our Sales and Solution Architects will provide free consultative services to deliver the best answer tailored specifically to the Buyer, ensuring best value for the Buyer's organisation as well as the best end user experience.

CPE

To facilitate the connectivity to the SCSP, Customer Premise Equipment (CPE) is often required to route traffic between the SCSP and the Buyer's LAN environment.

The MLL pricing schedule includes diverse hardware providers ranging from ultra low-cost options, fuller featured mid-market options, through to hardware accelerated secure networking devices.

MLL's architects work with a wide range of Buyers, all at different stages in their IT development, often with widely different plans. In using this service offering, Buyers will be able to take full advantage of MLL's expertise free of charge to bring about the best outcomes.

Other Service offerings

The MLL SCSP can incorporate other G-Cloud service offerings to provide more encompassing solutions. It ties together these offerings in one cloud solution. Buyers can therefore order other MLL G-Cloud Service Offers, which are seamlessly integrated into the SCSP, under one call off using the SCSP Service offer. These include:

Gateway Services

MLL provides a range of Gateway services though connectivity to the MLL core network including:

- Internet access
- Health and Social Care Network (HSCN)
- Public Services Network (PSN)
- Public Clouds services including:
 - Amazon Web Services
 - Microsoft Azure
 - Google Cloud
 - IBM Cloud
 - Oracle Cloud
 - VMWare Cloud

IP Addressing (Public)

MLL provides public IP address subnet ranges which can be used to aid connectivity to the internet from inside the local network.

MLL DDoS Mitigation & Protection

This service offer detects anomalous traffic from public sources and reroutes the traffic through a cloud-based scrubbing solution, returning only the desired traffic and protecting the Buyer's online presence.

Cloud based firewalls and Firewall as a Service

This service offering covers managed and comanaged firewall services, including dedicated and multitenant options. This also includes client VPN end-point solutions allowing the SCSP to be extended to almost any device, in any location. It also includes identity management solutions.

Standards based delivery

MLL will use industry standards for project and service delivery as summarised in the table below:

Delivery and Service Management	Industry Standard
Service Management	ITIL

Project Management	PRINCE2
Quality Management	ISO 9001
Security Management	ISO 27001 and Cyber Essentials Plus
Environmental Management	ISO 14001
Health and Safety Management	ISO 45001
NHS Digital	Data Security and Protection Toolkit

Delivery

MLL provides Buyers with an Implementation Coordinator for small-scale SCSP solution deliveries, for example SD networking for fewer than 20 sites with existing MLL underlay connectivity, or an MLL Project Manager for large scale/ complex deliveries. The scale of the solution required, and therefore the MLL delivery team required to manage the implementation of the Buyer's requirements, including engineers, will be determined during the MLL team's assessment of the initial enquiry from the Buyer.

MLL follows an ISO 9001 audited delivery process and maintains an ISO 27001 audited configuration and change management process for customer hosting infrastructure. MLL's Project Managers are PRINCE2-qualified and, where assigned, will be MLL's stakeholder to manage the project delivery. MLL's Solutions Architects, Technical Design Authorities, and Technical Engineers, including our NOC and Field Engineers, are skilled across the range of technologies used in MLL's network deliveries, including Fortinet, Juniper, Cisco and HPE Aruba.

MLL uses PRINCE2 methodologies to deliver projects, typically employing the following 4 stages of project delivery:

- Internal project set-up (including contract award, team assignment, etc)
- Project Initiation (Kick-off meeting, risk assessment, technical discovery, technical workshop, project and technical documentation)
- Project Delivery (solution delivery, risk and issue management, change management, progress reporting, escalation management, governance, progressive handover to MLL's Business as Usual (BAU) team, etc)
- Project Handover (complete handover to MLL's BAU team, project review, lessons learnt, project closure, etc)

The lead time to deliver small scale SCSP services in this offer is expected to take between 20 and 40 working days. The lead time to deliver a complex SCSP delivery is entirely dependent on the Buyer's overall requirements and will be assessed and advised during the scoping of the project requirements, prior to award.

MLL's team will undertake regular project reviews with the Buyer to an agreed frequency. For larger projects, governance will be provided through a project board comprising senior sponsors from MLL and the Buyer.

Support

Monitoring and Reporting

- MLL will monitor all in scope Secure Cloud Services Platform (SCSP) 24x7x365 for availability, utilisation and performance.
- Any failure which appears will be analysed and where appropriate raised as an Incident with MLL's Service Desk and the Buyer's Service Desk will be notified.
- Incidents will be managed using MLL's Incident Management Service through to resolution.
- The Buyer will be provided with quarterly reports showing performance of the Secure Cloud Services Platform (SCSP) as agreed within the Order Form.
- MLL will provide access to the MyMLL service portal and through this access to the performance monitoring service.

Service Desk

MLL's Network Operations Centre is based in Marlow, Buckinghamshire, supporting buyers on a 24x7x365 basis.

The NOC and Service Desk undertakes the following functions:

- Receives Incident or Service Requests by agreed contact methods – telephone, email or via MyMLL portal.
- Records Incident or Service Requests on the Service Management System.
- Allocates a Call to Severity 1, 2, 3 or 4 and where relevant manage the Incident through to Resolution in accordance with the Service Levels.

Support Model

MLL's service support model is based on ITIL compliant processes with clearly defined roles and responsibilities, supported by industry recognised systems and tools. This model will be used to monitor the Service in order to meet the Service Level.

Incidents will be raised either proactively by MLL or reactively by the Buyer and logged in MLL's IT Service Management system.

MLL utilise the following Severity Definitions for Incident Management:

Category	Definition
Severity 1	The Services are Unavailable across the entire Buyer's estate
Severity 2	The Services are Unavailable at one of the Buyer's sites
Severity 3	The Services are Unavailable to an individual user

Severity 4	All other Incidents, including any Incidents raised initially at a higher Severity Level that were subsequently deemed to be attributable to the Buyer or in any other way not attributable to the Supplier.
------------	--

MLL will ensure that Incidents are resolved within the Incident Resolution Time, based on the Severity Level of the Incident.

Service Hours

Monday – Sunday (including Bank Holidays) - 00:00-23:59, (24 hours per day, 7 days per week)

Service Levels

Incident Resolution – Secure Network Overlay

Where MLL do not provide the underlying circuit connectivity, only the SD-WAN overlay service will be monitored and supported by MLL reactive Incident Management.

Service	Severity 1; and Severity 2	Severity 3	Severity 4 (Indicative Only)
Secure Network Overlay Only	5 hours (from time Incident is raised to MLL)	End of next Working Day (from time Incident is raised to MLL)	10 Working Days (from time Incident is raised to MLL)

Incident Resolution – Underlay Connectivity

Site Connectivity	SLA	Severity 1	Severity 2	Severity 3	Severity 4 (Indicative Only)
National Carrier – RAO2	Standard	4 Hours	4 Hours	40 Hours	10 Working Days
National Carrier – Fibre Ethernet	Standard	6 hours	6hours	End of next Working Day	10 Working Days
National Carrier – FTTP	Standard	40 Hours	40 Hours	3 Working Days	10 Working Days
National Carrier – FTTP	Enhanced	20 Hours	20 Hours	End of next Working Day	10 Working Days
National Carrier – FTTP	Express	7 hours	7 hours	End of next Working Day	10 Working Days
National Carrier – FTTC/SOGEA	Standard	40 Hours	40 Hours	3 Working Days	10 Working Days

National Carrier – FTTC/SOGEA	Enhanced	20 Hours	20 Hours	End of next Working Day	10 Working Days
National Carrier – FTTC/SOGEA	Express	7 hours	7 hours	End of next Working Day	10 Working Days
National Carrier – ADSL	Standard	40 Hours	40 Hours	3 Working Days	10 Working Days
National Carrier – ADSL	Enhanced	20 Hours	20 Hours	End of next Working Day	10 Working Days
Altnet – Fibre Ethernet	Standard	6 Hours	8 Hours	2 Working Days	10 Working Days
Altnet – FTTP	Standard	8 hours	8 hours	End of next Working Day	10 Working Days

Availability - Overlay

Service	Availability
SD-WAN Management Platform	99.99%

Availability – Underlay Connectivity

Connectivity Type	Availability
Fibre Ethernet	99.90%
Ethernet FTTP	99.70%
Ethernet FTTC	99.50%
FTTP	99.70%
FTTC	99.50%
ADSL	99.50%

Service Credits

Service Credits will be calculated and reported by MLL through the Service Report and reviewed with the Buyer. This will include a summary of any service credits accrued within the previous period.

Overlay

Service	Coefficient (m)	Service Level Threshold % (a)	Service Failure Threshold % (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
SD-WAN Management Platform	5	99.99%	95.99%	5%	25%

Underlay Connectivity

Connection Type	Coefficient (m)	Service Level Threshold % (a)	Service Failure Threshold % (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
Fibre Ethernet	5	99.90%	95.90%	5%	25%
Ethernet FTTP	5	99.70%	95.70%	5%	25%
Ethernet FTTC	5	99.50%	95.50%	5%	25%
FTTP	5	99.70%	95.70%	5%	25%
FTTC	5	99.50%	95.50%	5%	25%
ADSL	5	99.50%	95.50%	5%	25%
EFM	5	99.50%	95.50%	5%	25%

Incident Resolution

Number of Incidents per Service Period	Coefficient (m)	Service Level Threshold (a)	Service Failure Threshold (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
39 or fewer	Not applicable	No more than 2 Incidents are Resolved in excess of the max Incident Resolution Times	5 or more Incidents are Resolved in excess of the max Incident Resolution Times	2.5% (payable when 3 Incidents breach the Service Level Threshold in any Service Period)	5% (payable when 4+ Incidents breach the Service Level Threshold in any Service Period)
40 and more	0.25	95%	85%	2.5%	5%

Social Value

MLL is committed to providing social value as part of its contractual deliverables which will be agreed with the Buyer and detailed in the call-off contract. Key social value themes for MLL include:

Fighting Climate Change - Underpinned by MLL's existing ISO 14001 environmental management system and published carbon reduction plan with a net zero target date of 2040.

Tackling Economic Inequality - We will deliver tailor-made offers to support the communities and citizens in the localities in which we serve our customers.

Equal Opportunity - This is a fundamental principle of our business and the basis of our customer relationships.

Company Information

Company Details

MLL Telecom Limited

Marlow International, Parkway, Marlow, England, SL7 1YL

Company No: 02657917

Date of incorporation: 28th October 1991

VAT No: 203558428

Switchboard: 01628 495400

Website: www.mlltelecom.com

Contacts

Name: Ellie Coome

Position: Bid Manager

Tel: 01628 495 400

Email: gcloud@mlltelecom.com

Copyright

All rights reserved. © MLL Telecom 2026