

ANNEX 4 TO APPENDIX D SPRINT DATA LINK PRODUCT

The following terms and conditions in this Sprint Data Link Product Annex ("Annex"), together with Contract DIR-TSO-3432 under which Customer is purchasing Sprint Data Link, govern Sprint's provision of Sprint Data Link to Customer. Terms not otherwise defined herein will have the meanings set forth in Contract DIR-TSO-3432.

1. DESCRIPTION

- 1.1.** Sprint Data Link requires a dedicated connection between the Sprint 3G Network or Sprint 4G Network and Customer's wireline network. Customer has three options for this dedicated connection: MPLS VPN, IP VPN or Frame Relay. A Wireless Data Connection Device, certified OEM (Original Equipment Manufacturer) data device or certified telemetry device is used to connect wirelessly to Customer's wireline network. Customer must have MPLS VPN, IP VPN or Frame Relay services under a separate wireline agreement with Sprint ("Sprint Wireline Agreement") or through another provider acceptable to Sprint from a technical and/or service level standpoint, in Sprint's sole discretion. Texas state agencies are not permitted to enter into a Sprint Wireline Agreement for the sole purpose of utilizing Sprint Data Link.
- 1.2.** Connection from the wireless device is established through a user name and password-protected login. Keying on the domain portion of the user name – for example, @yourcompany.com – the Sprint AAA (Authentication, Authorization and Accounting) Server proxies authentication to the AAA Server hosted by Sprint, or to the AAA behind Customer's firewall through a secure VPN tunnel or SprintLink Frame Relay PVC that's established between the Sprint 3G Network or Sprint 4G Network and the Customer's wireline network. Once the AAA Server completes device authentication, Sprint assigns an IP Address to the device. Wireless access to Customer's network is then available via the VPN or SprintLink Frame Relay PVC.

2. IMPLEMENTATION OPTIONS; USAGE

- 2.1.** Customer must choose either the Sprint Data Link via MPLS VPN, IP VPN or the Sprint Data Link via Frame Relay. If Customer purchases either of these connections from Sprint, Customer must execute the separate Sprint Wireline Agreement for that connection. Pricing and terms and conditions for Sprint provided MPLS VPN, IP VPN or Frame Relay are described under the separate terms of Customer's Sprint Wireline Agreement.
- 2.2.** Once the Sprint Wireline Agreement is executed, Sprint will start the implementation process designed to support the Sprint Data Link component of Customer's services. During this process, the Sprint Business Implementation Management team will work with Customer to develop an implementation timeline that will be jointly agreed to prior to the execution of the implementation process. This timeline will include target delivery dates for all service components. Customer may be responsible for implementation charges as outlined in Appendix C Pricing of Contract DIR-TSO-3432.

Option 1 - Sprint Data Link via IP VPN

This Service will allow Customer to connect its network with the Sprint 3G Network or Sprint 4G Network via IPSec VPN over the Internet. Sprint uses the IPSec protocol to encapsulate Customer's data in secure IP packets for transport across the Internet. Customer's data will also be encrypted using the 3DES encryption algorithm. Customer must have a VPN appliance that is capable of terminating IPSec protocol, and AAA Server running RADIUS, and Internet Access.

Option 2 - Sprint Data Link via Frame Relay

This Service will allow Customer to connect its network to the Sprint 3G Network or Sprint 4G Network by using a Frame Relay virtual circuit (PVC).

Option 3 - Sprint Data Link via MPLS VPN

This Service will allow Customer to connect its network to the Sprint 3G Network or Sprint 4G Network via a network based IP VPN across an IP/MPLS backbone.

- 2.3.** Use of Sprint Data Link requires certain certified devices and software that is capable of Sprint Data Link operation. Not all applications and services work, or work the same, on all Sprint Data Link enabled devices.
- 2.4.** In the standard implementation, Sprint Data Link is not available when roaming off the Sprint 3G Network or Sprint 4G Network. If Customer chooses to use the Sprint Data Link in a roaming environment, Customer is responsible for protecting its own information and for its own privacy. Sprint is not responsible for any lost Customer data, information, or materials while roaming in a non-Sprint network. The Customer agrees that Sprint is not responsible for any breach of corporate information while using Sprint Data Link when roaming.

2.5. Sprint is not responsible for any opinions, advice, statements, services applications or other information provided by third parties and accessible through Sprint Data Link. Neither Sprint nor its vendors or licensors guarantees the accuracy, completeness or usefulness of information that is obtained through Sprint Data Link. Sprint is not responsible for any lost Customer data, information, or materials. Customer is responsible for evaluating such content. Connections to the Internet via Sprint Data Link may result in the disclosure to others of the user's email address and other personal information. Customer is responsible for protecting its own information and for its own privacy and acknowledges that due to such disclosures, its users may receive advertising, warnings, alerts and other messages, including broadcast messages.

3. IP ADDRESSING OPTIONS; SPRINT HOSTED AUTHENTICATION SERVICE

3.1. **Customer Specific IP Addresses.** Customer can designate a range of private IP Addresses to be assigned to their mobile users. Sprint offers either static IP addresses or dynamic IP addresses.

- A. Static IP Address. Each time a Wireless Data Connection Device authenticates and connects to the Sprint 3G Network or Sprint 4G Network, the Sprint 3G Network or Sprint 4G Network will assign the same IP Address to the device from the designated range.
- B. Dynamic IP Address. Each time the Wireless Data Connection Device authenticates and connects to the Sprint 3G Network or Sprint 4G Network, the Sprint 3G Network or Sprint 4G Network will dynamically assign an IP Address to the device from the designated range. The IP address is released back to the customer specific IP Address pool upon disconnection from the Sprint 3G Network or Sprint 4G Network.

3.2. **Sprint Data Link - Hosted RADIUS Authentication Service.** Sprint's Hosted RADIUS Authentication service provides Customer a hosted username and password management solution for their remote access users. Remote users authenticate on one of two redundant Sprint AAA servers while remote access administrators facilitate username/password management, of multiple transports types, on a single Sprint hosted Remote Access Authentication System (RAAS) or tool. Authentication database – Native RADIUS, Active Directory, LDAP, any SQL-based solution.

- A. Redundant Sprint AAA servers are located in Lenexa, KS. and Lee Summit, MO. The RAAS application is Oracle based and is located in a highly secure strong DMZ environment in Lenexa, KS.
- B. Authentication administrators through the RAAS system will have the ability to:
 - (1) Change passwords for existing users
 - (2) Control the addition and deletion of users (up to the maximum limit purchased)
 - (3) Control RADIUS authentication via policy management and profile groups
 - (4) Reset forgotten passwords
 - (5) Sprint provides authentication administrators RAAS Tier 1 support for application questions
 - (6) Sprint maintains the server infrastructure providing both AAA RADIUS authentication and username/password management (RAAS)

4. **PARTIES' RESPONSIBILITIES.** In addition to the parties responsibilities outlined in Contract DIR-TSO-3432, the parties **commit** to the following:

4.1 Customer must:

- A. Provide a Customer-owned, ARIN-registered domain (e.g., acme.com) for designating routing through the Sprint 3G Network or Sprint 4G Network;
- B. If Customer does not subscribe to Sprint's Hosted RADIUS Authentication service, Customer must provide a AAA server that runs the RADIUS protocol and support RADIUS (UDP port 1812-auth and 1813-accounting) and MD5 CHAP AAA service must either utilize public IP addresses or NAT. Sprint Data Link must utilize either (i) public IP addresses or (ii) NAT;
- C. Provide and provision user profiles (usernames and passwords) on Sprint or Customer-provided AAA server. Customer will also be responsible for configuring their AAA server;
- D. Provide a VPN termination appliance or appliances that can support two IPSec connections (VPN Option only);
- E. Provide a connection from VPN appliance or appliances to the Internet (VPN Option only);
- F. Configure their VPN appliance or appliances to establish two IPSec tunnels to Sprint's redundant VPN gateways (VPN Option only);

- G. Configure their AAA server, internal routers, router(s), and firewall as part of the initial set up of Sprint Data Link. Customer will exchange AAA shared secret values with Sprint in order to set up proxy authentication between AAA servers;
- H. Provide a designated contact person(s) to meet with Sprint as needed to discuss issues relating to Sprint Data Link and appropriate subject-matter experts and/or administrators of the VPN appliance, Frame Relay Access Device ("FRAD"), the AAA server, internal router, and Customer firewall. Administrators will be readily available to assist Sprint in the setup and troubleshooting of any bugs or issues. If necessary, Customer will also be responsible for escalating to any vendor of Customer equipment in the case that Customer subject-matter experts are unable to configure a device or resolve an issue or bug;
- I. Make the appropriate subject-matter experts available and be responsible for providing contact information for those individuals; and
- J. Configure its network system to allow Sprint to authenticate the Wireless Data Connection Device, certified OEM (Original Equipment Manufacturer) data device or certified telemetry device to allow access to Customer's application systems to be wirelessly accessed by Customer's end-users.

4.2 Sprint will provide:

- A. SprintLink Frame Relay port and PVC or MPLS VPN port, local access and router (the routers will be available for lease or purchase), as needed and as agreed to in the Sprint Wireline Agreement unless Customer provides its own, Sprint-approved connection;
- B. Up to two appropriate resources for deploying and supporting Sprint Data Link;
- C. Issue tracking during implementation;
- D. Process for Customer to contact deployment and support personnel;
- E. Instruction and guidance on the configuration of the VPN appliance, FRAD, AAA server, firewall, and users; and
- F. A customized copy of the Sprint Connection Manager software.

5. [Intentionally Omitted]

6. CUSTOMER RESTRICTIONS

6.1 Customer will not:

- A. Modify, translate, adapt, reverse engineer, decompile, disassemble, or otherwise translate or create derivative works based on Sprint Data Link, SSV or SCM, except to the extent expressly permitted by applicable law (and then only upon advance written notice to Sprint).
- B. Use Sprint Data Link, SSV, or SCM to provide any facility management, time sharing, service bureau, or other similar services to third parties.
- C. Rent, lease or sublicense Sprint Data Link, SSV, or SCM to a third party. Any attempted rental, lease or sublicense in violation of this Annex will be void.

7. SPRINT DATA LINK SUPPORT MODEL

7.1 Customer Support (Tier 1)

- A. If a user of Sprint Data Link has a problem accessing the Customer's enterprise systems, that user must first contact the Customer's help desk or support group per the procedures outlined and communicated during initial rollout of Sprint Data Link.
- B. Customer will provide Tier 1 support for its users of Sprint Data Link including: taking the initial call, gathering critical information, and initiating the triage process. If triage is unsuccessful, then the designated help desk or support group should escalate via a phone call to the Sprint Tier 2 Technical Support group for additional support.

7.2 Sprint Customer Solutions Support (Tier 2)

- A. The Sprint Tier 2 Technical Support group will receive calls from the designated Customer Help Desk or support group personnel. This support model establishes a single point of communication and ensures customer Help Desk or support group personnel are aware of the status of any open issues and can implement any ad-hoc triage plans or processes. The Sprint Tier 2 specialist will act as a liaison to the technical support personnel who will work to resolve any and all open issues based on their assigned severity levels.
- B. If Customer's Help Desk or support group personnel experiences problems or are unable to triage any issues with the Sprint Data Link product, they will need to contact the Sprint Tier 2 Technical Support group via a

telephone call to communicate the issue and open a trouble ticket. Sprint Tier 2 Technical Support is available 24 hours a day, seven days a week for Sprint Data Link support at the Sprint-provided technical support contact numbers.

- C.** When Customer calls the Customer Service Center (CSC), the following information will need to be provided (at a minimum):
- (1)** What is Customer's name?
 - (2)** Is the caller available 24X7? If not is there an alternate contact?
 - (3)** Contact's phone number
 - (4)** What type of problem is the Customer having?
 - (5)** What Sprint Data Link, SSV, or SCM software version is the Customer using?
 - (6)** How many users are affected?
 - (7)** What error message is being described? If none describe symptom
 - (8)** Describe the troubleshooting steps taken
 - (9)** Is the activation greater than 36 hours?
 - (10)** Is the Customer trying to connect by pressing "Connect" or "Go" on the Sprint Data Link, SSV, or SCM software and the error then occurs? Or are they trying to log into a specific application after they have been connected and then receive the error?
 - (11)** What data activities were you able to perform?
 - (12)** Number of failed attempts?
 - (13)** Computer or device type?
 - (14)** Call direction – stationary or moving?
 - (15)** What is the user's realm? (information after the "@" sign)
 - (16)** What type of Wireless Data Connection Device, certified OEM (Original Equipment Manufacturer) data device or certified telemetry device are you using?
- D.** The Sprint Tier 2 Technical Support Specialist will provide Customer the assigned severity code for the issue, a ticket number, and information regarding when you will be contacted next and by whom. If the call is not your initial one, please have your existing trouble ticket number available for the Sprint Tier 2 Support Specialist.