

**Sprint PCS<sup>®</sup>**

# **Sprint PCS Business Connection<sup>SM</sup>**

## **Technical Information**



**Sprint PCS<sup>®</sup>**

## Introduction

### **Sprint PCS Business Connection<sup>SM</sup>: Empowering the Mobile Professional**

Until now, remote access to corporate data has been driven by corporate IT departments adopting and deploying new technologies. This model has suffered with the explosion of wireless-data access options, ranging from WAP-enabled wireless phones to laptops using airport and hotel 802.11 b wireless networking. In addition, each new wireless-data technology has introduced the need for product-specific training and subject matter expertise within the IT organization when supported using traditional EAI (enterprise application integration) practices.

Sprint PCS Business Connection empowers the mobile professional with secure and efficient remote access to corporate data, using the complete range of wireless computing options available today. The deployment of Sprint PCS Business Connection does not require additional training, support or infrastructure build-out by already overburdened corporate IT staff; the entire solution is driven by an easy-to-use Web interface, and is supported by Sprint PCS.

Sprint PCS Business Connection offers two methods of wireless data access: Sprint PCS Business Connection Enterprise Edition for managed deployments by the enterprise IT department, and Sprint PCS Business Connection Personal Edition for individual subscribers.

Sprint PCS Business Connection Personal Edition provides secure wireless access to enterprise data behind the corporate firewall via a specialized PC application. The application is quickly and easily installed on a PC, and maintains a secure outbound connection to the Sprint PCS Network. Connection-sharing technology allows users to share fixed PC resources, thus eliminating the need to keep their PC connected to the network while accessing data via a wireless device.

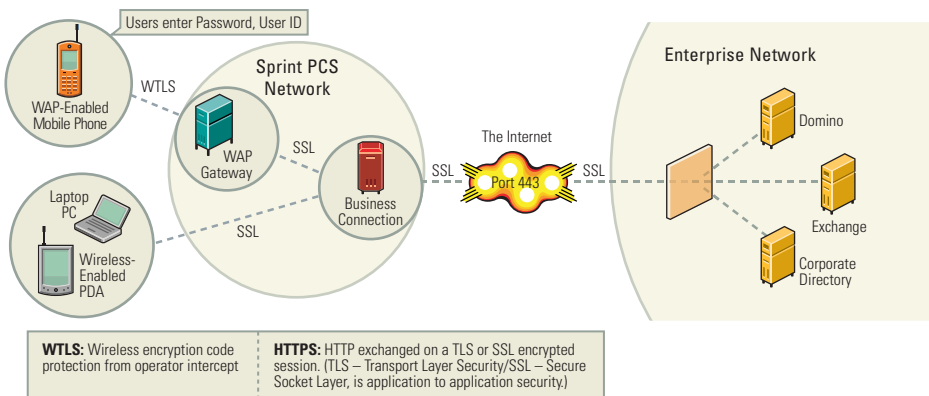
In contrast, Sprint PCS Business Connection Enterprise Edition is a managed solution that relies on an extranet relationship between Sprint PCS and the enterprise, and is secured using SSL application-level encryption. Additional connectivity options such as VPN and Frame Relay are available based on the needs of the enterprise. This extranet relationship is structured to permit appropriate levels of access to corporate messaging and directory resources by Sprint PCS. Each transaction is individually authenticated with the identity of the wireless user.

Unlike competing solutions, Sprint PCS Business Connection never replicates sensitive corporate data to the Sprint PCS Data Center. This critical difference means that Sprint PCS Business Connection users are not forced to trust Sprint PCS to safeguard data stored beyond their direct control.

## Sprint PCS Business Connection: Architectural Overview

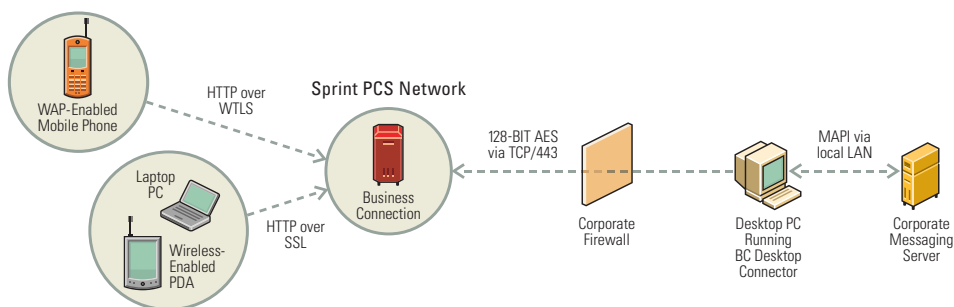
Sprint PCS Business Connection is a network-based application residing in a Sprint PCS Data Center. Wireless users may connect to Sprint PCS Business Connection using the full spectrum of wireless productivity devices available today, including WAP-enabled wireless phones, PDAs and PDA-based smartphones, and PCs. Access to Sprint PCS Business Connection services is delivered via an adaptive Web interface, which automatically optimizes the experience for the device being used.

### Sprint PCS Business Connection Enterprise Edition architecture:



As illustrated above, Sprint PCS Business Connection Enterprise Edition establishes on-demand, SSL-secured connections to enterprise resources. Users are required to authenticate to Sprint PCS Business Connection using a username, password and enterprise ID triplet known only to that user. 128-bit AES encryption, in conjunction with the user's secret password, ensures that enterprise credentials may only be unlocked when a user is correctly and fully authenticated. These credentials are then used to access resources requested by the user, e.g. the Inbox or Calendar views.

### Sprint PCS Business Connection Personal Edition architecture:



In the diagram above, the desktop PC running the Sprint PCS Business Connection desktop connector establishes an outbound connection to the Sprint PCS Network. The authorized user of that PC (and other co-workers who have been invited to share that PC's connection to Sprint PCS Business Connection) may then access corporate messaging and other resources via any of the wireless platforms or devices supported by Sprint PCS.

## Sprint PCS Business Connection Security

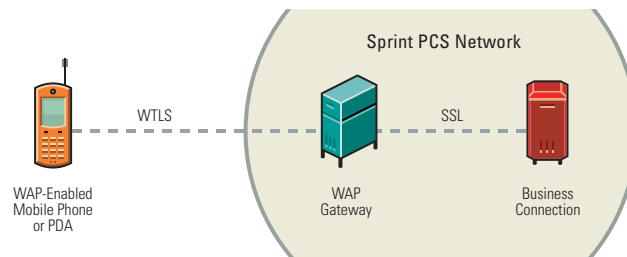
### Philosophy of Design

Every facet of Sprint PCS Business Connection design is governed by the following principles:

- Proven, advanced technologies are used to ensure confidentiality, integrity, and appropriate authorization at all points in the system.
- All components of Sprint PCS Business Connection have been designed using a “zero-trust” model. No part of Sprint PCS Business Connection design may ever rely solely on the security of the infrastructure in which it is deployed, and must instead include reliable and verifiable protective measures to safeguard all data handled by the system.

Infrastructure and application security measures are designed using the “defense in depth” model. No single failure or compromise may result in a loss of integrity within Sprint PCS Business Connection, and such events must be reported in a manageable, efficient fashion.

### Transport Security: Wireless Users to Sprint PCS Business Connection



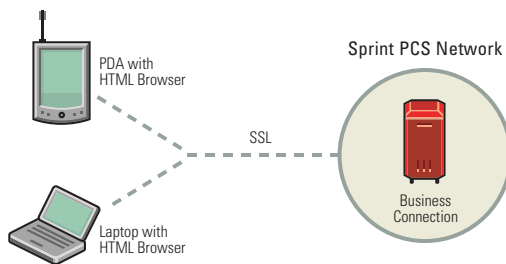
The specific security protocols used between a wireless user’s device and Sprint PCS vary depending on the capabilities of the device. The following examples illustrate the two major types of wireless connectivity to Sprint PCS.

WAP-enabled devices, by design, use an intermediary security and content adaptation server called a “WAP Gateway” to enable access to content and applications written for WAP devices. For secure sessions, a specialized protocol called WTLS (Wireless Transport Layer Security) is used to establish an encrypted connection to the WAP Gateway server. The WAP Gateway server then completes the connection to Sprint PCS Business Connection using Internet-standard 128-bit SSL.

WAP Gateways are tightly secured systems residing in the heart of the Sprint PCS network. Data flowing between WAP browsers and Internet sites via WTLS-SSL sessions is decrypted for only a few microseconds during the transition between the WTLS and SSL connections, greatly reducing or eliminating any opportunity to intercept data flowing across the WAP Gateway.

Users accessing Sprint PCS Business Connection with a WAP device are required to log in using a WML form protected by a WTLS-SSL connection. Users present their wireless credentials to Sprint PCS and are in turn authorized to access the various features and functions of Sprint PCS Business Connection.

Users may optionally choose to allow their session to persist across multiple connections, allowing easy resumption of work in progress after an interruption to connectivity. In the case of WAP devices, once the user is authenticated, a “cookie” with a fixed expiration time/date stamp is stored at the WAP Gateway. Return visits falling within the expiration period of the cookie are authorized by the presence of encrypted content within the cookie validating the identity of the user.



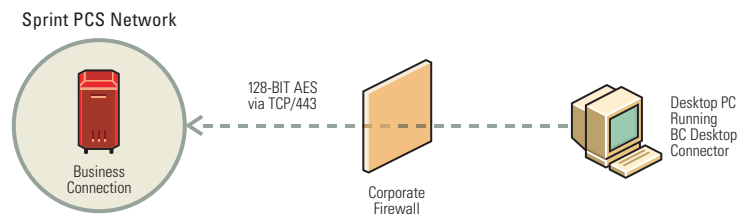
Platforms supporting native HTML browsers, such as PDAs and PCs, establish a secure session directly to Sprint PCS Business Connection using 128-bit SSL encrypted links. Users accessing Sprint PCS Business Connection with browser-equipped devices authenticate using an HTML form protected by an SSL connection. As with WAP-based connections, cookies may be used to enable users to return to bookmarked sessions within the expiration period of the cookie.

All transactions between remote clients and Sprint PCS Business Connection are protected using either pure SSL, or WTLS and SSL in combination. In either case, all connections use high-security 128-bit encryption to protect the confidentiality and integrity of all user data.

## Sprint PCS Business Connection Security (cont.)

### Transport Security: Sprint PCS Business Connection Personal Edition Desktop Connector to Sprint PCS

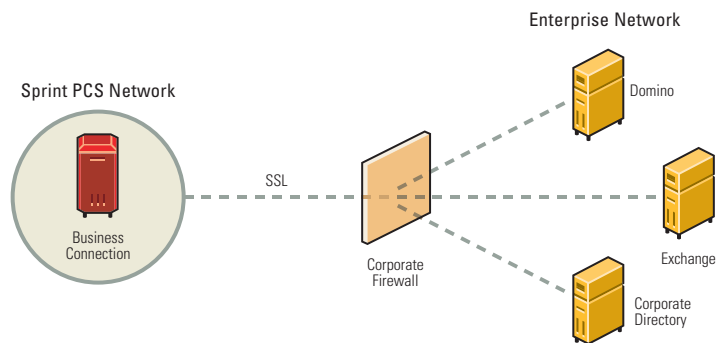
The Sprint PCS Business Connection Personal Edition desktop connector runs on a PC residing within the corporate network, and establishes an outbound connection to the Sprint PCS Data Center on port tcp/443 or applicable SSL port used by the enterprise. The desktop connector does NOT use SSL connection-layer encryption. Instead, when the desktop connector establishes a connection to Sprint PCS, it completes a cryptographic exchange, which results in a 128-bit AES secret key, valid for that session only. This key is then used to encrypt all communications between Sprint PCS and the desktop connector.



All transactions between Sprint PCS Business Connection and the desktop connector are encrypted using the 128-bit AES key negotiated as outlined above. Sprint PCS considers 128-bit AES keys to have a useful lifetime of 24 hours. At any time, an existing key may be gracefully discarded and the client required to reconnect and negotiate a new key. Please see the Appendix for additional information about AES and the strategic decision of Sprint PCS to use this particular encryption protocol.

### Transport Security: Sprint PCS Business Connection Enterprise Edition to Enterprise Servers

Sprint PCS Business Connection Enterprise Edition differs from Sprint PCS Business Connection Personal Edition in several ways, the most notable of which is the mechanism by which data is retrieved on behalf of authenticated wireless users. Instead of relying on individual desktop PCs to handle requests for user data, Sprint PCS Business Connection Enterprise Edition communicates directly to the enterprise application servers. Each user request for data residing at the enterprise (for example, a list of messages in the Exchange Inbox) results in a short-lived SSL connection being made to the application server at the enterprise.



All transactions between Sprint PCS and the enterprise are encrypted using 128-bit SSL, as shown in the diagram above. Additionally, Sprint PCS may choose to augment this security by offering IPsec-based VPN tunnels or Frame Relay between their data center and the customer's premises. While SSL provides completely satisfactory security for connections between Sprint PCS and the enterprise, VPN connectivity may be desirable for administrative or policy reasons, including reduced configuration requirements at the enterprise firewall.

### **Authorization, Credentials, and Encryption: Wireless Users**

Users sign up for Sprint PCS Business Connection accounts using a secure Web-based interface. During this setup process, they are required to select a unique Sprint PCS Business Connection user name, as well as a password meeting minimum requirements for length and complexity. Sprint PCS Business Connection Enterprise Edition users are also informed of their Enterprise ID during the setup process. The credentials created during this process are referred to as the user's "wireless credentials," and are separate and distinct from any account information used to access enterprise resources.

In the case of Sprint PCS Business Connection Personal Edition, the user must then successfully install and authenticate using the Sprint PCS Business Connection Personal Edition desktop connector. This step confirms that the user is, in fact, an authorized user of the corporate security domain in which their PC resides. Please see below for details of how the desktop connector authenticates to Sprint PCS.

Each user's Sprint PCS Business Connection password is irreversibly encrypted during account setup using an AES-compatible hash function, before being stored for future login verification. It is not computationally feasible to recover a password encrypted using a hash function. When a user attempts to log in at a later date using the wireless credentials previously established, Sprint PCS Business Connection validates the password input during the login sequence by encrypting the presented password and comparing the result to the encrypted password stored in the Sprint PCS Business Connection database. If the encrypted passwords are identical, the user is authorized for access.

In keeping with the Sprint PCS Business Connection security principle, user passwords are stored as outlined above: in a form that allows validation of presented credentials, without the possibility of accidental disclosure of a user's password. The only possible response to a lost password is a password reset, which can be initiated by the user or by Sprint PCS. The re-establishment of account access is accomplished by use of a one-time password sent as an email message to the user's registered account, or optionally, via a text-message-capable wireless device. Once the single-use password is presented to Sprint PCS Business Connection, the user is then required to register a permanent password before being permitted to use any feature of the service. Password resets can only occur after a user has responded correctly to a challenge question, that was established in the initial registration for the service.

## Sprint PCS Business Connection Security (cont.)

### **Authorization, Credentials, and Encryption: The Sprint PCS Business Connection Personal Edition Desktop Connector**

Each individual desktop connection is registered to a primary user. During the installation of the desktop connector software, the user is required to input his wireless credentials. Using these wireless credentials, the desktop connector then authenticates to Sprint PCS Business Connection and receives a cryptographic authorization token if the presented wireless credentials are valid. This token is then stored by the desktop connector and used for all subsequent connections, eliminating the need to store the wireless credentials on the host PC. The decision to store this token persistently is driven by user selection of the “remember my password” option in the desktop connector configuration.

Users may employ the Sprint PCS Business Connection Personal Edition connection sharing feature to enable uninterrupted access to corporate resources. A user may initiate a request to a co-worker to enable connection sharing, which is delivered to the co-worker’s email inbox. If the co-worker chooses to host the user’s connection as a result of this request, several things happen:

- The requesting user must submit their enterprise messaging credentials to Sprint PCS Business Connection Personal Edition to enable access to messaging services via connection sharing.
- The co-worker’s desktop connector is reconfigured to provide connectivity for both the co-worker and the user requesting connection sharing. This results in the creation of an additional authorization token on the co-worker’s PC for the hosted user.
- Each time the co-worker’s desktop connector connects and registers with Sprint PCS Business Connection, it retrieves the hosted user’s enterprise messaging credentials and stores them in memory. These credentials are never stored on disk, even in encrypted form, effectively preventing any possibility of recovery or accidental disclosure.

The enterprise messaging credentials stored within Sprint PCS Business Connection Personal Edition are protected using 128-bit AES encryption. Recovery of these credentials is only possible when a cryptographic authorization token is presented containing the correct key, in conjunction with other authorization information transmitted by the desktop connector. The net result is that the stored credentials are not accessible by users, and can only be recovered by an authorized desktop connector by means of a fully authenticated session.

## **Authorization, Credentials, and Encryption: Sprint PCS Business Connection Enterprise Edition Requirements**

In order to gain authorized access to enterprise resources on behalf of wireless users, each user must configure their Sprint PCS Business Connection Enterprise Edition account with the appropriate credentials. As a specific example, a user who desires access to their Microsoft Exchange 2000 mailbox must use the Sprint PCS Business Connection Web interface to configure their exchange username, password and domain information. This enterprise credential is then encrypted using that user's unique 128-bit AES key, which in turn can only be unlocked when that user is actively logged in.

Once again, this mechanism is structured according to the Sprint PCS Business Connection security policy. In essence, the enterprise is not required to trust the integrity of the Sprint PCS infrastructure or staff to ensure an appropriate level of data security. Instead, the enterprise may rely on the proven strength of the AES cryptographic standard to safeguard their user's stored credentials, and the use of the user's login credentials (never stored in recoverable form by Sprint PCS) to safeguard that same AES key.

## **Sprint PCS Business Connection Personal Edition Application Security**

Each feature or function of Sprint PCS Business Connection is carefully designed to maximize security while minimizing inconvenience to the user. Of particular interest to the IT administrator are the protections governing wireless access to documents via the desktop connector. Included among these protections:

- Wireless document access is read-only. Data stored at the enterprise cannot be modified in any fashion using Sprint PCS Business Connection.
- Retrieved documents are never stored within Sprint PCS Business Connection, but instead are passed directly through to the user for storage or viewing on the wireless device.
- Limitations on wireless access to documents – namely, which files may be accessed – include the following:
  - Access must be explicitly enabled to one individual folder selected by the user, and is subject to the additional restrictions below.
  - Designation of an entire drive for remote access is not permitted. The path to be enabled for remote access must be at least one folder below the level of the root directory of the host PC's disk volume.
  - The folder designated for remote access must not contain, or be part of, the active Windows directory (e.g. C:\WINDOWS or any subdirectory) on that PC. No assumptions are made about the actual name or specific location of the active Windows directory; instead, the desktop connector queries the Windows registry for this information.

## Sprint PCS Business Connection Security (cont.)

### Some of Sprint PCS Business Connection's additional security features include:

- Brute-force password guessing protection: automated attacks attempting to guess the password for a particular user are made impractical by the introduction of automatic delays after a certain number of failed password attempts.
- Strong validation of session tokens using cryptographic techniques: cookies and other authorization tokens used by Sprint PCS Business Connection Personal Edition include tamper-proof, forgery-resistant cryptographic signatures.
- Encryption of all communications between Sprint PCS Business Connection Personal Edition and the desktop connector using the AES cipher with a one-time 128-bit session key.
- Validation of every transaction between Sprint PCS Business Connection Personal Edition and the desktop connector using cryptographic signatures to ensure that man-in-the-middle attacks are impossible to execute against any part of Sprint PCS Business Connection.
- Encryption of all communications between Sprint PCS Business Connection Enterprise Edition and the enterprise using industry-standard SSL v2/v3.

### Conclusion

Sprint PCS Business Connection Personal Edition is a powerful, efficient solution for enabling the mobile professional with anytime access on the Sprint PCS Nationwide Network to corporate resources. With Sprint PCS Business Connection Personal Edition, the individual user gains the ability to securely access email, PIM, directory and file-based data via modern data devices, just as if they were sitting at their desktop.

Sprint PCS Business Connection Enterprise Edition provides an equally powerful IT-managed solution suitable for larger populations of end users. With the exception of wireless document access, every other feature in Sprint PCS Business Connection Personal Edition is present in Enterprise Edition, and in many cases performance is enhanced by the use of direct-to-server access protocols in place of the desktop connector.

The powerful and flexible features of Sprint PCS Business Connection are made possible within the bounds of good corporate security practices, and provide wireless users with an alternative to the risky practice of replicating sensitive data to easily lost devices such as PDAs and laptop PCs. Sprint PCS Business Connection combines unprecedented ease of access to corporate data via wireless devices with proven security technology – a combination that allows wireless users to be productive outside the traditional bounds of the enterprise network.

### AES: Strong, Scalable Encryption for User Data

On December 6, 2001 the United States federal government announced the approval of FIPS-197, the standards document for the new Advanced Encryption Standard (AES). This marked the culmination of a multi-year selection process during which the world's leading cryptography teams presented competing proposals for the crypto technology that was to become the AES.

The competition was fierce, and the peer-review process was merciless. At the end, several candidates survived the final round of analysis. The winning Rijndael algorithm, submitted by a pair of cryptographers from Belgium, was selected for its combination of resistance to attack, ease of implementation, efficiency, and scalable design allowing several encryption-key sizes.

In accordance with the Sprint PCS policy of using proven, tested security standards, and for the reasons above, AES was selected for use throughout Sprint PCS Business Connection. In the short term, using AES encryption on a per-transaction basis (encrypting each payload individually) allows radically more efficient use of server resources than SSL-based client connections, which are extremely CPU-intensive. The implementation of AES encryption at the application layer requires much less CPU time per new session startup, which translates directly to fewer connection servers needed for a given size user population.

Computational power per dollar continues to grow according to Moore's Law, doubling roughly every 18 months. Cryptography technologies must be able to compensate for this by allowing for the use of increasingly strong encryption keys over time. In the longer term, the use of the AES offers Sprint PCS Business Connection a growth path to increasingly larger key sizes without disruption to the basic security strategy. This is in contrast to end-of-life standards such as DES (reincarnated as Triple-DES, or 3DES), used in certain competing products despite the lack of a future growth path; AES is intended to replace DES and 3DES altogether in the next few years.

A good example of the strength of the AES cipher: If one were to build a specialized computer to attempt decryption of 56-bit DES encrypted data, and that computer were capable of trying all possible DES keys in 1 second, that same computer would take 149 trillion (1000 x 149 billion) years to try all possible 128-bit AES keys. In comparison, the universe is believed to be less than 20 billion years old.

Sprint PCS Business Connection is available on the Sprint PCS Nationwide Network and is not available while roaming. See online user guide available at <http://businessconnection.sprintpcs.com> for detailed information relating to the technical requirements, limitations, restrictions and available features of Sprint PCS Business Connection. Use of Sprint PCS Business Connection is subject to the License Agreement presented when registering. Copyright ©2002 Sprint Spectrum L.P. All rights reserved. Sprint, Sprint PCS, Sprint PCS Business Connection and the diamond logo are service or trademarks of Sprint Communications Company L.P. Architectural diagrams are property of SEVEN Networks, Inc.

**Get the whole Sprint PCS Clear Wireless Workplace® story at [sprintpcs.com](http://sprintpcs.com) – or contact your Sprint PCS Representative for more information.**

**Sprint PCS Clear Wireless Workplace.®**



**Sprint PCS®**