SecureConnect™: A Major Leap In The Cordless Desktop Experience

Cordless mice and keyboards – the cordless desktop – vastly improve the computing experience. They look great and eliminate desktop clutter. They even free people from their desks, allowing users to lean back in a chair and place the keyboard on their laps. And there's no longer a mouse cord to push around or get snagged when navigating the screen.

But setting up a cordless desktop hasn't always been easy. Getting the tiny radio transmitters inside the mouse and keyboard to communicate with the receiver that's plugged into the computer doesn't always work. Computer users want their new cordless mouse and keyboard to be pre-synchronized, pre-encrypted and work immediately, right out of the box, without a finicky setup process. Whether a product uses 27 MHz radio frequency (RF) or 2.4 GHz RF, making that initial connection can be a challenge. For cordless desktops that use the open-standard Bluetooth® transmission technology, the connection process is even more complicated, due to the need to enter passkeys to connect the components to the receiver.

Until now.

Introducing Logitech SecureConnect™

Following two years of research and development, Logitech has introduced SecureConnect, the best possible cordless desktop connection experience a computer user could ever ask for. SecureConnect is yet another in a long line of industry firsts from Logitech, following Logitech's introduction of the world's first cordless mouse in 1992, first optical cordless mouse in 2001, and first cordless mouse with laser optics in 2004.

With Logitech's new SecureConnect technology, the cordless keyboard, mouse and receiver are all pre-synchronized and pre-connected during manufacturing. They're ready to go right out of the box, with a secure link and without the hassle of a manual connection process. Simply insert the batteries and go. And to assure security, encryption of keyboard activity is enabled by default.

A Logitech Bluetooth cordless desktop with SecureConnect eliminates the need to enter a passkey during installation; it's done during manufacturing. The result is installation that is faster and easier than ever before. And keyboard encryption is already enabled, too.

In addition to offering the highest possible level of encryption for 27 MHz cordless desktops, users are forever freed from a finicky setup. The process of establishing encryption is now done at Logitech's factory. Without SecureConnect, users need to perform several steps, including installing software and then activating encryption by entering a string of characters into the cordless keyboard.

Bluetooth users are certain to appreciate Logitech's "Bluetooth done right" strategy. Logitech was the first company to launch a Bluetooth desktop that didn't require people to have an existing corded keyboard in addition to their new one to complete the setup process. Previously, people had to use a corded keyboard to input a passkey to connect the new cordless Bluetooth keyboard to a PC. The new SecureConnect technology takes Bluetooth plug and play to an entirely new level by completely pre-configuring encryption and eliminating the need to enter a passkey.

Under The Hood

Every Logitech cordless desktop consists of at least three hardware components: the mouse and keyboard, each of which contains a miniature battery-powered transmitter, and the receiver, which plugs into the computer. The Logitech® diNovo™ Media Desktop™ product adds a fourth component: the MediaPad™, a numeric keypad with an integrated LCD display panel that incorporates a calculator along with time, date, and temperature displays.

Unlike a television remote control, which uses infrared (IR) technology and requires a direct line of sight to work, Logitech cordless devices use RF data-transmission technology. With RF, there's no line-of-sight requirement, allowing the receiver to be placed in a convenient, unobtrusive location, perhaps tucked behind a monitor or behind the computer itself.

But in order for the receiver to "hear" the mouse and keyboard – whether they're transmitting at 27 MHz, 2.4 GHz, or through a Bluetooth hub – the devices must be synchronized, ensuring that they are transmitting and receiving on the same channel, like being on a conference call together.

Because most Logitech cordless devices can transmit on more than one channel, synchronization is crucial. Having multiple channels minimizes interference, ensuring that cordless users who work near each other won't find their on-screen cursors moved by someone else's cordless mouse. For that reason, a Logitech cordless mouse or keyboard operating nominally at 27 MHz can actually transmit signals at 27.045 MHz or 27.145 MHz.

In the Bluetooth world, transmissions are a bit different. All Bluetooth devices operate at 2.4 GHz, the same frequency band used by Wi-Fi networks, cordless telephones, and other devices. To avoid transmission collisions among these devices, each uses multiple channels simultaneously, randomly hopping from channel to channel every time data is transmitted. Once a great idea, with so many different products now operating at 2.4 GHz, collisions are more common. However, this is not a problem for the Logitech Bluetooth cordless desktop.

Logitech Bluetooth cordless desktops incorporate the advanced technique of Adaptive Frequency Hopping (AFH). With AFH, the Logitech device identifies sources of interference and adapts to this environment by excluding those channels from the list of available channels.

Synchronization ensures that each device communicates on the same channel, in the same way a remote control on a garage door opener communicates with the receiver mounted on the motor housing. Until now, it has always been the user's responsibility to press the connect buttons on the receiver, mouse, and keyboard, initiating the synchronization process.

With SecureConnect, that's no longer necessary. Logitech's engineers developed a way to pre-synchronize cordless desktops at the factory so that people don't have to manually connect their desktop components. They were able to do this thanks to the rapidly evolving technology of Radio Frequency Identification (RFID).

RFID Steps Up

First developed to identify friendly aircraft in World War II, the use of RFID has skyrocketed in recent years. No bigger than a grain of rice and costing just a few cents apiece, RFID tags typically contain data that allows nearly any item – an engine in an automobile factory, a case of razor blades, or keyboards and mice – to be uniquely, and securely, identified. Think of it as an electronic replacement for a printed barcode label.

Usually containing no power source of their own, RFID chips spring to life only when they are in close proximity to an electromagnetic field from a reader device. The highway tollbooth transponder mounted on the inside of a car's windshield is one example. Inside is an RFID tag programmed with data that identifies your vehicle. The tag serves up that information only when driven through a toll plaza equipped with a compatible reader. In the world of retail, the use of RFID tags to track inventory through manufacturing, shipping, and distribution channels, is becoming increasingly popular.

In a Logitech cordless desktop with SecureConnect, the mouse, keyboard, and receiver each contain an embedded RFID tag. The tags are programmed with data to make sure the devices are properly configured and have the necessary identification information to ensure they work together right out of the box.

Because the three tags contain the same data, the installation process is seamless. In addition, the identifying data for each cordless desktop set has to be unique. After all, two sets with identical identifiers might cause interference, especially if two users with identical identifiers work within a few feet of each other.

For the user, it's essential that the mouse, keyboard, and receiver in the carton have RFID tags with matching data. But in the manufacturing process, surprisingly, it's not at all important what's on those tags when the products go into the box. How can this be?

Though writing matching identifying data to a mouse, keyboard, and receiver before they are packaged seems logical, Logitech developed a better method, one that guarantees 100-percent accuracy. The RFID tags are programmed only after the products are packaged and the box is sealed. This method eliminates the need to keep matched devices together throughout the manufacturing process. And since mice,

keyboards, and receivers are manufactured on different assembly lines producing thousands of units each day, making sure matched devices get packed in the same carton would be a nearly impossible undertaking.

How is it possible to program the RFID tags after the carton is sealed? It can be done, and the solution is the result of lengthy development and testing by Logitech engineers.

An assembly line technician places a sealed, packaged carton into a "pairing station." The station consists of several components: a rectangular loop antenna a bit larger than the retail package, a computer running a custom application to assign identification numbers and other data, and specialized RFID circuitry to power the antenna.

When a carton is placed in the station, the process begins automatically. For 27 MHz and 2.4 GHz sets, a unique identifier, encryption key, and other connection information are sent to the rectangular antenna, writing the data to the RFID tags in the mouse, keyboard, and receiver simultaneously. For cordless desktops using Bluetooth wireless technology, a Bluetooth address, PIN code, and other data are written to the RFID tags. The process takes just seconds. In a quality control step, the tags in each package are read and then secured to protect against possible corruption or modification. From there, the sealed packages are shipped to customers.

Easy, Secure User Experience

When a user opens a Logitech cordless desktop with SecureConnect, the installation process is as simple as inserting the batteries and plugging in the receiver. For Bluetooth devices, the RFID tag contains the Bluetooth address and PIN for the mouse, keyboard, and receiver. As soon as it's plugged in, the receiver starts the low-level device pairing process automatically, using the provided PIN. The connection process is completely automatic and secure.

SecureConnect assures complete user security. Critical information, including the cordless desktop's identifying data and Bluetooth PIN code, is not accessible via RFID. Even if it were possible to listen in on keyboard and mouse activity, a snoop's eavesdropping equipment would need to sit within three feet of the cordless desktop, the maximum communications range of the built-in low-power transmitters.

SecureConnect technology eliminates the hassle of configuring a cordless desktop.

Though the benefits of cordless mice and keyboards became clear years ago, now it can be said that technology has fully delivered on the vision. The improved user experience introduced by Logitech with SecureConnect technology delivers the most satisfying cordless experience possible.