



Bluetooth Proximity-based Access

One of the big tradeoffs enterprises encounter when trying to protect data on handheld wireless devices is balancing usability with security. CREDANT Mobile Guardian offers a number of key usability enhancements to improve the user experience, including Bluetooth[®] Proximity-based Access. This feature allows a Microsoft[®] Windows Mobile device to “sense,” or recognize, whether the authenticated user is within proximity of the handheld and if so, keeps the user’s handheld active—a unique and very elegant solution to a perennial problem of how a protected handheld device “knows” if the authorized user is still around.

Normally, if a user hasn’t touched the device keyboard or screen for 5 or 10 minutes, the security software on the device must assume that the user is no longer active, and it logs the user off. But what if the user is just in “read only” mode and possibly looking at driving directions, reading an email, etc? This scenario can be dangerous for a user in a moving vehicle, and is extremely irritating because the user must re-authenticate frequently while they are driving or otherwise using the device.

OVERVIEW

Handhelds are typically “always on” devices — once a user is logged in, they remain so indefinitely in order to receive calls, etc., even if the device powers down to conserve power. This capability can be disastrous if the device is lost or stolen, enticing anyone to immediately access the device’s data. Therefore, if the device remains inactive for a period of time, any good security software will log-off the user and encrypt the data. Once the device is locked down, the user must re-authenticate to access their email or check the Internet for directions. This is great for security, but what if the user is working with a handheld application that doesn’t require hands-on interaction, such as a GPS tool that runs while the user is driving?

CREDANT Technologies designed its Bluetooth Proximity-based Access capability for Windows Mobile handhelds to overcome a common usability feature of secured handhelds: the imposed device time-out for user inactivity. A trusted user, if in confirmed proximity to the device, should be able to remain logged in to that device, indefinitely, with the application remaining on and the data on the device remaining secure.

CREDANT Bluetooth Proximity-based Access uses Bluetooth to detect whether a second, trusted Bluetooth device is in range of the CREDANT-protected handheld. The trusted device can be the user’s Bluetooth headset or even a Bluetooth-enabled car. When the CREDANT-protected handheld “sees” the trusted device, it knows that the authenticated user is also nearby and automatically signs them in. As soon as the trusted Bluetooth connec-

BLUETOOTH HISTORY

Bluetooth is a short range (<10M) wireless standard originally proposed by Ericsson to eliminate wire clutter in homes. Its development is now managed by the Bluetooth SIG (Special Interest Group) where 400+ members ensure it remains an open standard, uninfluenced by any one manufacturer.

Initially aimed at wireless headsets, Bluetooth is now built-in to an installed base of well over 250M devices and growing at 3M devices/week.

BLUETOOTH SECURITY

For two Bluetooth devices to communicate, the user has to ‘Pair’ the devices by placing one into ‘Discoverable’ mode, and the other to ‘Discover’. Any Bluetooth radio in range and in ‘Discoverable’ mode will respond, and the user can select the device he or she wishes to ‘Pair’, or connect to. Although the ‘Discoverable’ mode is essential for pairing, it allows the device to be ‘seen’ and connected to by other devices — an apparent Bluetooth vulnerability. Unfortunately, this mode is the default mode for many devices, especially mobile phones. It is best to configure a Bluetooth device to be ‘Hidden’ or ‘Non-Discoverable’, making it impossible for any unknown device to pair with the unit without the owner’s permission.

Another safeguard is to force users to enter a matching 4-digit PIN on the respective devices. However, some devices without a keyboard (a headset for instance) use a default PIN of “0000” which cannot be changed.

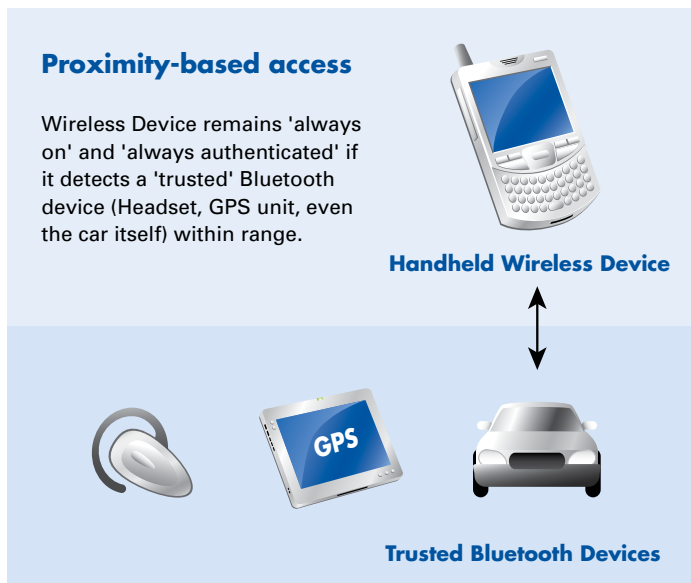


Bluetooth Proximity-based Access

tion is broken, the device immediately locks down access and secures all data. As with all CREDANT features, the System Administrator has complete control and can specify which user or user groups have access to this feature. CREDANT policies also allow the administrator to control how the device behaves when the feature is in use.

HOW IT WORKS

CREDANT Mobile Guardian's Bluetooth Proximity-based Access works on Windows Mobile PocketPC devices. It requires either the Microsoft or Widcomm® (Broadcom®) Bluetooth stack, both of which are used on the vast majority of Bluetooth devices.



Bluetooth Proximity-based Access is controlled by the Administrator via three CREDANT policies. As with all policies, these settings can be applied to everyone, groups or individual users:

Enable Proximity Based Access turns Bluetooth Proximity-based access on or off; valid values are True or False.

Proximity Based Authentication Attempts Allowed determines how many times the user's device can attempt to

discover its trusted Bluetooth device before the user is forced to manually authenticate; valid values are 0–10 attempts.

Proximity Based Access Max Security Timeout determines the maximum amount of time a user can use a device without being forced to manually authenticate, even if the trusted Bluetooth device is present; valid values are 0–120 minutes.

After these policies have been established and downloaded to the user's device, the user follows these three steps to complete the configuration:

1. **Pair with the Trusted Bluetooth Device:** CREDANT Shield will use this trusted device to determine whether access to the user's device should be granted. The user must use the device's Bluetooth Manager to initiate and complete the Pairing process. The Pairing process can be specific to an individual device, so the user should consult the device's User Guide.
2. **Create the Trusted Relationship:** After re-entering their CREDANT Shield PIN/password, the user simply selects the paired device that they want to use for Proximity Access. The CREDANT Shield menu flow looks like this:



Although a Bluetooth device identifier is generic ("Jabra headset" for instance), CREDANT collects information unique to that device to ensure that only that paired device is valid, not just any "Jabra headset".

(Important: CREDANT highly recommends that the user place all Bluetooth devices into 'Non-Discoverable' mode once paired. This action will greatly reduce the risk of hacking the devices via Bluetooth radio.)



Bluetooth Proximity-based Access

3. **Proximity-based Access in use:** Once the device has been configured, the first time a user uses the Bluetooth Proximity-based Access feature, the user will be forced to authenticate using the standard PIN or Password (Manual Authentication):



Thereafter, each time the trusted Bluetooth device is in range and powered off then on, or when it performs a soft reset, the handheld automatically authenticates the user, if policy allows. It will also keep the handheld from timing out through the CREDANT Idle Timer.

CREDANT Mobile Guardian Bluetooth Proximity-based Access contains built-in safeguards, including:

- If the “Number of Attempts” value is “0”, then each time the device is turned on or off, the user will be forced to manually authenticate, irrespective of whether or not the trusted Bluetooth device is present.
- Even while the trusted Bluetooth device is in range of the protected PPC, CREDANT will force the user to manually authenticate once the value specified in the “Proximity Based Access Max Security Timeout” policy is reached. This ensures that data is secure even if the trusted Bluetooth and PPC devices are lost together.
- The PPC and trusted Bluetooth device are allowed only a limited number of attempts to automatically authenticate before the user is forced to manually authenticate using their PIN/Password. This limitation prevents a thief from trying multiple Bluetooth devices or hacking unique device information.

(Note: the Bluetooth Proximity-based Access feature does not override the power management settings on the device. For instance, the handheld device may be set to power off after 15 minutes of inactivity, which will still occur, so users will need to change those settings as appropriate.)

SUMMARY

CREDANT Mobile Guardian’s Bluetooth Proximity-based Access provides a unique solution to the problem of devices timing out due to apparent inactivity. This feature leverages Bluetooth technology that is widely available in a very wide range of devices to provide a proximity access solution that is secure, configurable, and very flexible. In most instances, it can use Bluetooth devices already available to a user for a very low-cost, and highly usable solution that allows for easier end user adoption of handheld security.