PRIVARIS®

plusID 90

Gate and Vehicle Solution

Based on plusID identity verification technology

Keep traffic moving while insuring the identity of drivers and vehicles

As the need for heightened security pervades every corner of society new challenges have been created for the movement of vehicles through gates. Whether it is a port, a military base, or a logistics center, vehicle traffic is slowed by traditional, manual methods of verifying driver identity at portals and gates impacting productivity and the flow of commerce.

Facility operators need to be able to quickly and reliably verify the identity of drivers and vehicles without imposing solutions that violate privacy, add substantial costs or create additional security risks for the organization.

An ideal approach would be to have a “fast lane” for drivers and vehicles that we “know”, enabling them to proceed through checkpoints without stopping. Conventional manual checks would still be used for the smaller population of drivers and vehicles that are not pre-qualified.

While it is possible to install RFID technology on a truck for remote identification of the vehicle, the challenge has been how to verify the identity of the driver. A known vehicle with the wrong driver could present as much, or more, of a risk than the presence of a completely unknown vehicle.

Until now it has not been possible to reliably verify driver identity without requiring a full stop for either manual inspection of identity credentials or for execution of a biometric verification at a fixed, mounted reader. The Privaris plusID Gate and Vehicle system changes that by offering the world’s first, wireless, personal, biometric identity verification solution.

A New Approach
Personal, Mobile Biometrics for Gate and Vehicle Security

- verifies driver identity without requiring vehicles to stop
- matches driver to vehicle
- works with commercially available physical access control systems for gate operation
- works with commercially available solutions for vehicle starting and locking
- cannot be shared, useless if lost or stolen

Personal biometrics

With Privaris plusID, drivers verify their identity by swiping their finger on their own key fob biometric device as they approach the gate. The device compares the live fingerprint to the fingerprint template securely stored inside their device and upon a match, wirelessly transmits encrypted credential information (not biometric data) to the gate control system which validates the access rights for that driver and vehicle.

Easy integration with physical access control systems

The Privaris gate system can be configured to output a Wiegand data stream – a standard communications signal that is compatible with virtually all access control systems.

Protecting privacy and minimizing corporate risk

The plusID unit eliminates the privacy concerns associated with conventional biometric systems. The user's biometric data is never collected or stored in a database. Users enroll directly into their own personal plusID unit where the data is encrypted and securely stored. It is never released or transmitted. Rather than delivering biometric data as an access credential, plusID uses it simply to "unlock" the transmission of standard identity credentials.

This unique approach eliminates employee concerns over the collection of personal data while eliminating the risk and expense of collecting, storing and protecting employees' sensitive personal information.

Convergence: combining physical and network security

plusID provides organizations the ability to use a single device to satisfy both their physical and logical (network) access needs, for convenient, secure access – everywhere it is required.

In addition to supporting long-range wireless communications over 802.15.4 for gate access, plusID also works with 125 kHz and 13.56 MHz contactless card readers from HID, Casi, and Indala for access to multiple buildings and facilities in place of standard access cards (such as Prox and iCLASS) – no coding, middleware or wiring required. Further, each plusID device can also be used for logon to computers and networks. It is out-of-the-box compatible with Microsoft Servers, no middleware required, for use in place of passwords and smart cards.

Technical overview: gate and vehicle application

As the vehicle approaches the gate, the driver swipes their finger across their plusID device. After verification of the driver's fingerprint, the plusID transmits credential data via 802.15.4, an IEEE standard for wireless communications operating at 2.4GHz. The data is received by the Privaris Long Range Transceiver, which decrypts the credential information and passes it to an external gate control system, which opens the gate. The entire transaction typically takes less than three seconds.

The plusID identity token supports wireless communication with the transceiver over distances of up to 100m (328 feet). With adequate lane design, vehicles can easily proceed through gates at moderate speed without having to stop the vehicle!

Verification and vehicle speed

Based on the speed of travel and the plusID's maximum transmission range of 100 meters* (328 feet), below is the amount of time available to turn on the device and successfully verify - while approaching the gate:

- At 10 miles per hour = 22 seconds to verify
- At 15 miles per hour = 15 seconds to verify
- At 20 miles per hour = 11 seconds to verify

*May vary by installation. Check with Enrollment Administrator for actual range.

Antenna Considerations

The following range testing was conducted with the 50 deg 10.5 dBi outdoor antenna from SMC; model number SMCANT-DI105, part number 751-5784. There are two other similar 10.5 dBi antennas from SMC which are the DI135 (36 deg) and the DI145 (26 deg) which are more

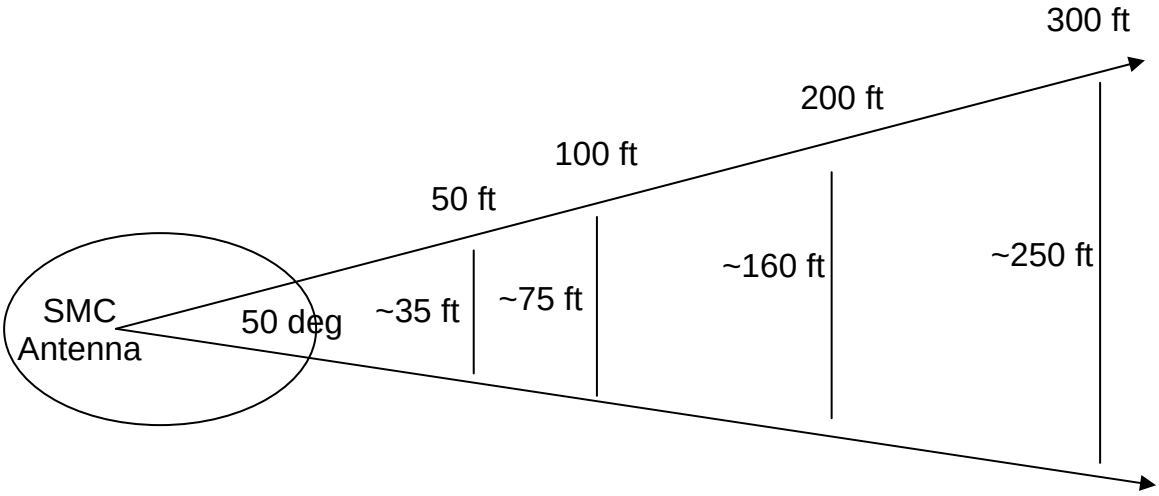
directional if this is needed. The 50 deg SMC antenna is recommended this for installations that are a “generic” single lane.

This antenna in a standard set up was able to communicate at about 25 degrees off center providing about a 50 degree cone of reception. Like all antennas, there are side lobes that allow you to communicate in about a 10 foot circle around the antenna with no attenuation. The approximate pattern is a 10 foot circle around the antenna with a 50 degree beam width beyond that. The test data was collected using the following criteria:

- In a car with all windows rolled up
- plusID device held in right hand above dashboard

The baseline was obtained using a standard set-up with no attenuation; the plusID 90 was held above the dash board at a 45 degree angle and communicated with the lane transceiver with a 2-3 second delay resulting in a confirmed maximum range of ~300 feet. At 300 feet there is approximately 250 feet of side to side range as shown in the diagram below. As the distance to the SMC antenna or attenuation decreases the plusID 90 becomes less orientation and position dependent as the signal strength increases and provides faster connections time (usually less than 1 sec).

* This is an approximation of a complex antenna pattern.



- With 10 dBi of attenuation there was not an appreciable reduction in performance when measured at the maximum range of 300 feet.
- With 16 dBi of attenuation the maximum range was reduced to 90 feet.
- With 20 dBi of attenuation the maximum range was reduced to 36 feet.

Based on these measurements it is estimated that 18 dBi of attenuation will give about 50 feet of range and 15 dBi of attenuation will give about 100 feet of range.