

## **SmartWatch SecurePass Wireless Biometric Authentication of Vehicle Occupants**

### **ABSTRACT**

The purpose of this white paper is to provide a functional description of the integration of commercially available products from Privaris, Inc. and TransCore, LP. that allow for automatic identity of registered vehicles approaching an access gate and the simultaneous biometric authentication of the vehicle occupants via a secure, wireless connection. This solution eliminates the need to stop the vehicle at the access gate and present a picture ID and addresses many of the potential technical and value added benefits associated with fulfillment of the integration of the two technologies.

### **THE PROBLEM**

For many years, the Government and Private Industry have been investigating new technologies to assist security forces personnel in ways to reduce the work force requirements for vehicle gates and entrances to Government facilities. In the interest of better traffic management, Government facilities management has expressed the desire to identify not only a pre-authorized vehicle and its driver and/or occupants but also to do so without requiring the vehicle to stop.

Enhanced identification methods, including biometrics identification, bar codes, RFID vehicle tags, and electronic scanning of license plates and DoD decals have been implemented. Many of these methods still require the vehicle to stop and validate the identity of the driver and its occupants. In addition, none of the current technologies address the need to adjust dynamically the identity document requirements for personnel should an incident occur that raises the threat condition for a given facility.

Isolating vehicles in multiple lanes, identifying occupants within specific vehicles, delivering various identity documents including photographs and signatures and preventing tampering or spoofing of information transmitted in the lanes are all issues addressed by the integration of the Privaris BPID™ Security Solution and the TransCore SecurePass and eGo™ products.

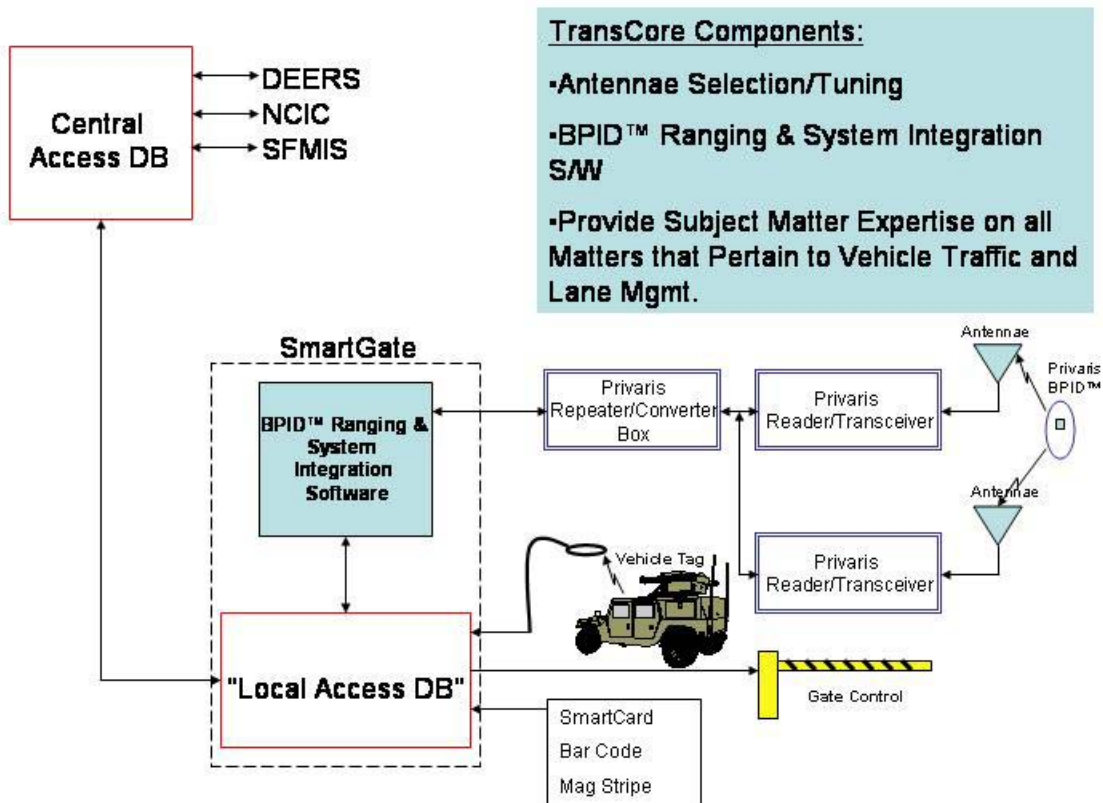
## PRIVARIS/TRANSCORE PRODUCT DESCRIPTION

The Privaris/TransCore Secure Gate Solution is comprised of the Privaris BPID™ Security Device issued to each user, Privaris networked Transceiver Modules, multiple customized antennae, Privaris Converter/Repeater Modules, Privaris Enrollment Software, the TransCore eGo™ RFID family of tags and readers and TransCore SecurePass gate management software system.

The TransCore eGo™ family of tags and readers combined with other vehicle lane hardware provides a high performance vehicle management system using single chip passive RFID tags that have been fully qualified to meet the rigorous performance demands for toll collection applications, including open road tolling. The eGo™ windshield sticker tag operates in the 902-928MHz radio frequency band, and is an RF-programmable device that does not require a battery or connection to the vehicle's electrical system. It is in the form of a flexible sticker much like a vehicle registration sticker. The windshield sticker tag is designed to withstand extreme temperatures, sunlight, humidity, and vibration. The tag can include a tamper-resistant option. Unique control numbers and markings may be etched on the outside of each tag.

The Privaris BPID™ Security Device uses fingerprint biometrics to authenticate the identity of the owner of the device prior to authorizing the release of any encrypted information stored within its memory. Upon the successful verification of the user's enrolled fingerprint(s) by the device, this information is wirelessly transmitted to receiving antennae located in or near the traffic lane. The wireless transmission uses the IEEE 802.15.4 protocol in the 2.4GHz radio frequency band and employs a "challenge-response" methodology using AES 256 to secure the data and provide a high degree of difficulty for spoofing or replay attacks.

The Privaris BPID™ Security Device performs all fingerprint processing, including capture, template generation, storage and matching, on the device. No database of biometric information is needed. It is possible for authentication to occur with a pre-configured stand alone PC at the vehicle access gate or to handheld devices in the vehicle lane should the infrastructure or the network be disabled or compromised. Furthermore, the device transmits only the required credential, not the fingerprint image or template. The user's biometric information never leaves the device. This solution strongly supports personal privacy concerns. Users need not be concerned about their fingerprint being compromised.



**PROPOSED PRIVARIS/TransCore SOLUTION**

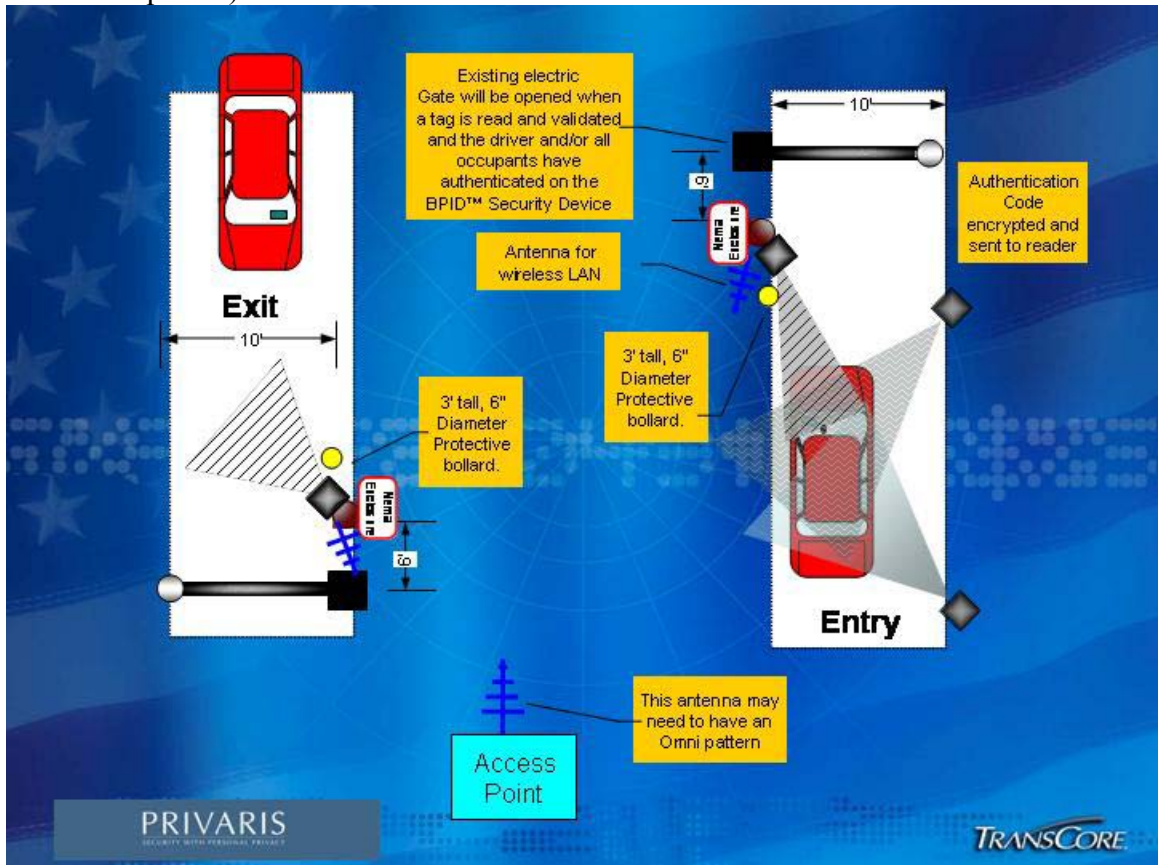
The Privaris/TransCore gate solution is easily integrated into the existing vehicle registration process used today at many Government facilities.

**ENROLLMENT:** A driver's identity is verified by the Issuing Authority of the customer's choice and is enrolled in a Privaris BPID™ Security Device. During this issuance process, the user and the Issuing Authority validate the biometric enrollment and storage of a private key onto the device. This key will be used to authenticate this particular user's identity and device at the vehicle access gate.

Additional credentials may also be added to the BPID™ Security Device and the Local Access Database for use in real-time authentication by the gate access system. A sample of other credentials could be any combination of PIN, Drivers License, Military or Government ID number, photograph, signature, security clearance information, travel documents, etc.

**OPERATION:** For purposes of discussion, it is assumed that a single lane for authorized vehicles entering a Government facility is equipped with the TransCore eGo™ vehicle tag system, automatic gates, ground loops, etc.

Before entering this vehicle lane, the driver is instructed via traffic light, message board or other means to power ON their BPID™ Security Device and authenticate. The driver placing his /her enrolled finger on the fingerprint sensor located on the BPID™ Security Device accomplishes authentication. The scanned image is matched to the stored template and results in a green indicator light illuminating on the device. As the vehicle passes into the range of strategically placed antennae, the eGo™ system develops a communications channel with the BPID™ Device and sends a challenge (randomly generated number sequence) to the device.



After the BPID™ Device receives the random number challenge from the eGo system it uses its private key to encrypt the challenge, add its own unique identifier code, and transmits this response to the TransCore SecurePass™ gate system. This response could include any additional credential that was placed on the BPID™ Device at time of issuance.

After receiving the response from the BPID™ Device, the eGo system uses the identified BPID device key from the Local Access Database to decrypt the response. The result is matched against the original challenge, and any credentials that were included in the response are matched against the Local Access Database. A positive match and a correct response to the challenge would authorize the system to open the vehicle gate and allow this vehicle to pass. A failure to match or an incorrect response to the challenge would cause the vehicle

lane to divert this particular vehicle to a guard house or other controlled entry point.

The eGo™ system, utilizing the customized antennae and Privaris electronics in the vehicle lane is provided with BPID™ Device position data. Combining BPID™ Device positioning with the eGo™ vehicle tag allows the system to determine the exact position of the driver, match this driver to the correct vehicle and eliminate the possibility of falsely accepting an authentication of a driver using another BPID™ Device in a different vehicle. The robust structure of the IEEE 802.15.4 protocol standard utilized by the BPID™ Device improves reception in the difficult and varying conditions encountered when transmitting through windshield glass and surrounded by various materials found in vehicles.

**THREAT LEVELS:** Under normal threat conditions, subsets of the total credential delivered by the BPID™ Device can be used to validate the driver's identity. Under higher threat conditions, a more strict security policy can be enforced that utilizes transmitted photographs and other human forms of credentials for physical guards to visually verify the authentication of vehicle drivers.

**SECURITY:** Both the SecurePass vehicle gate system and the BPID™ Device must possess the symmetric private key for that single device that was generated or loaded during BPID™ Device issuance. The gate system uses random information in each challenge to a BPID™ Device and employs 128 bit encryption technology. This approach enables the gate system to detect and defend against any replay attacks. Additionally, all credentials placed on the device at the time of enrollment may be optionally encrypted and/or digitally signed so their authenticity can be delivered and validated manually under increased threat conditions when vehicles may or may not be required to stop.

## CONCLUSION

The most significant immediate benefits of the proposed solution are the ability to reduce the number of personnel required to operate gates and entrances to Government facilities while at the same time provide secure, biometrically authenticated identity documents with a detailed audit trail. The system will also support the delivery of more detailed credentials that may be required at the gate under high threat conditions. Additional benefits include:

- Eliminate the need to stop vehicles to authenticate occupants.
- Eliminate the need for a central biometric database.
- Integrated system utilization since the BPID™ device is multi-functional and can be used for facility access control, operating with existing infrastructures such as HID®, Indala, Kantech..
- Increased individual privacy.
- Multiple layers of security including RFID transponders, BPID™ devices, optional guard interface with the system, authorized users' photos, vehicle information and other important information.
- Increased security since only the enrolled individual can use the BPID™ device.
- Devices can be erased and reissued.
- Increased security by biometrically authenticating the identity of drivers and pairing drivers to specific vehicles.