Revised November, 2007

W.A.R.N. Passive Biometric ID Solution
Acquisition Specification Template

Scope of Product Specification

An access control, identification protection, and verification system, utilizing passive technologies, and one-time pad (or "1-to-1") biometric confirmation.

Deliverables

Individual Identification

The system shall employ an Identification Card containing Identification Information utilizing passive technology.

The Identification Card shall be optically-read, tamper proof, and impervious to

- a static or varying magnetic field
- static electric discharge of 18 KV
- Gamma and X-ray radiation of 35 Gy

The Identification Card shall survive accidental and deliberate exposure to energy from antennae, generators, and RF leaks.

The Identification Card shall employ an error-correcting methodology capable of reconstructing corrupted portions of corrupted data.

The Identification Card shall contain sufficient personal, permission level and forensic information to enable identity and access control decisions to be made without the need to access a remote database or utilize real-time network resources.

The Identification card shall contain forensic dada about the creation process, its validity and expiration dates.

The Identification Car raw stack shall cost no more than $0.50 per card.

Security shall be insured by the use of proven algorithms and cryptographic techniques.

The cryptography module shall have been validated by NIST and CSE for FIPS Publication 140-2 level 1 conformance.

The system shall allow multiple levels of secure storage within the Identification Information.

The Identification Information shall contain multiple sections of data, each individually protected by such techniques as described herein. One data section shall contain a fingerprint biometric of the cardholder.

Additional sections shall contain the various data specified in this section, including such cardholder identification data as is found on the face of the ID card. Additional data sections shall be available as needed for the private use of various entities and organizations that might need to utilize the Identification Card.

Total Identification bar code capacity must be a minimum of 3 Gig of data types.

Identification Information Creation

The system shall provide for the creation of secure documents and identification credentials across geographically dispersed, trusted intranets.

The system shall protect against unauthorized document and credential issuance while securing the identification data from unauthorized access, tampering, or spoofing.

The system shall provide monitoring and managing of the identification credential creation and validation events between cooperating agencies, regional centers, and local sites on a “need-to-know” basis.

Enrollment Process

The local Enrollment Process shall create and store Identification Record(s) for an individual.

Individuals shall register by providing proof of identity, having a photo taken, and presenting their lives forensic information.

The Identification record shall be passed to a Central Enrollment Process for further processing and checking.

The Local Enrollment Process shall locally maintain a detailed log of its activity and pass that log to a Central Enrollment Process.

The Central Enrollment Process shall maintain a detailed love of its activity and the activity of any downstream Local Enrollment Process(es).

The Central Enrollment Process shall set the capabilities of the Local Enrollment Process as dictated by an Authorization Process.

A Temporary ID Card, a Permanent ID Card, A Digital Seal Laminate to be used on a Permanent ID Card, and Digitally Sealed Documents shall be capable of being produced at the end of the enrollment process.

Both the Permanent ID card and the Temporary ID Card shall contain the particular cardholder's forensic and other identity information.

The system shall instantly distinguish between Temporary ID Cards and Permanent ID Cards.

The central Enrollment Process shall pass an image of the resultant Digitally Sealed image to the Local Enrollment Process.

Authorization

The Authorization Process shall be distributed and hierarchical.

The Authorization Process shall issue requests to the Central Enrollment Process to change the authorization.

The Central Enrollment Process shall determine if the authorization change request is valid.

Access Control

The system shall support manned or unmanned Access Control Points.

Access Control Points shall be capable of fully functional, stand-alone operation without reliance on a networked controller or database.

Access Control Points shall acquire and validate the Identification Information from the Identification Card.

Access Control Points shall acquire forensic information from the card holder.

The Identification Information shall be compared to a database of invalid cards maintained within the Access Control Point.

The Identity of the card holder shall be determined by comparing the live forensic information to the forensic information stored within the Identification Information.

The Access Control Point shall analyze the above information against locally maintained authorization to determine an appropriate Pass/Stop outcome.

The acquired forensic information and the determined Pass/Stop outcome shall be maintained within the Access Control Point and, when networked, passed to a Central Control Process.

The live forensic information shall be of a type acceptable for prosecution such as fingerprint image.

Unmanned Access Control Point

The Unmanned Access Control Point shall provide all of the capabilities listed in Section “Access Control” above.

The Unmanned Access Control Point shall consist of a self-contained unit.

As an option, the Unmanned Access Control Point shall provide internal battery backup capable of providing a minimum of 0.5 hours of operation.

Unattended operation shall be provided.

The Pass/Stop outcome shall be indicated via Green and Red LEDs, respectively, located on the Unmanned Access Control Point.

The Unmanned Access Control Point shall display prompts on an alphanumeric LCD display readable in either dim or bright environments.

Via an internal hardware interface, the unmanned Access Control Point shall be capable of controlling an electronic locking device to grant card holder access.

Manned Access Control Point

The Manned Access Control Point shall provide all of the capabilities listed in Section “Access Control” above.

The Manned Access Control Point shall communicate the Pass/Stop outcome to the operator via either a green bar or a red bar with the international NO symbol, respectively, displayed on a computer monitor.

Central Control

The Central Control Process shall monitor and update Access Control Points within its scope.

The Central Process shall continuously assess the activity and the status of the networked Access Control Points within its scope.

Any detected anomalies on the Access Control Points connecting hardware shall be logged and reported so that corrective action can occur in a timely manner.

The Central Control Process shall locally maintain a detailed log of its activity.

Activity Log Monitoring and Reporting

One or more monitoring stations shall be provided to view the various activity logs in near real time and historically.

Monitoring stations shall be constrained to view only those records for which authorization has been granted by the authorization process.