



## PLS - SECURE AUTHENTICATION

The following descriptions are derived from the U.S. Utility Patent for PLS provided to Card Logistics, and internally designated by Card Logistics as “Secure Authentication”. While these descriptions are not in the same order or exact text (the actual text is in ‘patent examiner language’) as listed within the Allowed Claims for this Patent, they summarize the intent of the Patent. There are actually 10 (ten) separate claims within the allowances, to include broad coverage of capabilities and options required for significant licensing opportunities within the various security and encryption markets. The Utility Patent for these claims was formally issued by the USPTO on 25 May 2010 and is Valid into 2027.

- Provision of high level and simultaneous “dual authentication” (mutual authentication) to allow for secure and encrypted communication between wired and wireless devices. The communication link is verified via consistent polling between the two sources, and information is only passed as long as the “dual authentication” is maintained.
- The “dual authentication” encryption communication link can be implemented either by embedded software on an existing CPU-based device or SIM Card, or a complete hardware implementation using currently available circuit technology or an application-specific processor-based Smart Card Chip for advanced capabilities.
- Secure access between the enabled devices (computers, cell phones, smart cards, computer-readable media devices, et al), whether direct or remote, is consistently polled to determine the previously approved secure link. If at any time the polling fails to establish the validation of the two devices for secure communication, the ‘information’ link (voice, data, et al) will be immediately disabled, protecting the parties involved.
- A biometric reader and/or ‘device’ implementation used to obtain unique authentication for the secure access to any information storage device, including computers, local or on-line disk storage, portable data storage devices, smart card chips, et al, whether directly connected to that information storage or via a wireless or remote connection.