



***tSecure<sup>®</sup> is a unique, tamper-resistant security device/methodology for disabling and/or controlling electronic and electronically controlled equipment almost anywhere***

### ***Abstract***

**tSecure is an antitheft system** for use in electronic and electronically controlled equipment. tSecure addresses a gap that existing security solutions do not, that is whether or not the equipment is, at the most basic level, operable.

**In addition to being a disabling component, tSecure** may also be used as an enabling technology, protecting equipment in transit; allowing it to be used only when activated at its intended destination or in the hands of authorized users.

**tSecure may be incorporated into various kinds of electronic equipment** specifically those that are micro-processor based and have as part of their start up, a Power On Self Test (POST) process. tSecure will deactivate the device into which it is incorporated on receipt of coded paging telemetry. This signal is initiated when it has been determined that equipment has been stolen or misplaced. When the tSecure device receives the deactivation code, software and circuitry within the electronic equipment causes the equipment to shutdown and become inoperative. To ensure the antitheft receiver is not removed or tampered with, internal validation takes place each time the system goes through any type of POST processing activity. If this internal authentication is not possible or is incorrect, the POST process assumes the tSecure antitheft device has been removed or tampered with and causes the equipment to become inoperative.

Any equipment in which the tSecure device is installed may be reactivated upon receipt of a properly coded telemetry signal.

tSecure is designed to be an integral part of the equipment it protects, this means it is built in during the manufacturing process. A major consideration in its design is one of minimal impact to existing processes (e.g. power consumption).

The purpose of the tSecure device/methodology is to render any equipment in which it is installed, *virtually useless*, should it be stolen. Further applications of the technology may include initiating tasks to thwart compromise of any of the equipment's internal components. Because the tSecure is activated via a paging signal broadcast, protection can be virtually global. Paging signals may be broadcast repeatedly if desired.

tSecure is envisioned to have a broad range of applicability, from laptop computers to military devices or specialized communications equipment containing some form of start up (POST) processing, as such can be a powerful tool for the management and control of technology assets.

***tSecure*** is different from other products/processes that address security issues in that the majority of these offerings require an internet connection to be effective, *tSecure* does not. As such, it can be used in equipment that does not connect to the internet. *tSecure* also operates at a very basic level, as part of the internal validation that the system goes through when it is turned on.

A custom design insures that tSecure will meet the needs of the application it is to protect or manage.

### ***Reference***

U.S Patent 5,966,081.

### ***Licensing***

tSecure is licensed through ***Tirraappendi, Inc.*** a Washington State Corporation. Any, and all licensing issues are processed through:

Tirraappendi, Inc.  
7250 Old Redmond Road, #147  
Redmond, Washington 98052

Email Frank Vlacil: [Frank@Tirraappendi.com](mailto:Frank@Tirraappendi.com)  
or  
Van Chesnutt at: [Van@Tirraappendi.com](mailto:Van@Tirraappendi.com)

### ***Legal Representation***

---

#### **Patent Attorneys:**

---

Rodney Tullett & Maria Culic  
Christensen, O'Connor, Johnson &  
Kindness, PLLC  
1420 Fifth Avenue  
Seattle, Washington 98101