PROXIMITY
PROXENSE
TECHNOLOGIES

truprox™ TOUCH TECHNOLOGY

John Giobbi
689 NW Stonepine Dr.
Bend, OR 97701

Confidential

The information provided in this document is the exclusive property of Proxense, LLC. Recipient hereby acknowledges that such information is confidential and privileged, and will not be disclosed, copied, distributed or used without the express written consent of Proxense, LLC.

MICROSOFT 1010

Background:

Optimizing sales transactions, providing secure access to physical & digital assets, and uniquely identifying individuals, are challenges faced by many businesses and organizations. Ensuring these processes are safe, efficient and simple is important to merchants, providers, users and consumers alike. Well known technologies such as magnetic cards (credit & debit cards, employee badges, etc.), and more recent developments such as contactless cards or tokens (designed to be waved near compatible readers), are examples of attempts to address these needs.

While these technologies *have* improved transaction-processing and access-control ("transactions"), they have inherent problems and shortfalls. In particular, none directly address one critical concern, knowing an individual attempting to perform a transaction is who they claim to be, and is actually authorized to do so. And the problem is worsening as Internet-based sales continue their rapid growth. In general, this shortfall has become a serious problem in need of a solution. And it is critical that the "solution" does not significantly increase the complexity, risk, or speed of processing such transactions.

Common attempts to address this issue involve using PINs or passwords in conjunction with account numbers. While these options do help combat fraudulent use/access, they also go against the desired goal of not adding complexity and delay to transactions ... and they are often defeated. Quite simply, in attempts to deal with an ever-growing need to memorize PINs and passwords, individuals often resort to using the *same*, simple phrase to *protect* many items, or worse, write the phrases on notes kept in their purse/wallet or stuck to their computer. Neither is a *best practice* ... but both routinely occur, and highlight some of the shortfalls inherent in current methodologies.

A technology *capable* of addressing the underlying issue, *authenticating users*, is biometrics. On the surface, biometric authentication (for example, comparing an individual's fingerprint to a known sample) is a logical solution. Yet, it too suffers from significant problems. The primary being it potentially exposes the participating parties - the entities administering the authentication ("controlling-entities"), and the individuals being authenticated ("users") - to serious liabilities, risks, and inefficiencies. Biometric authentication techniques in use today nearly always require users to release their most personal, private and <u>unchangeable</u> (biometric) data to the controlling-entity, or a third-party relied on by the entity, exposing that data to the possibility of theft and fraudulent use. And correspondingly, controlling-entities must either assume the risks & liabilities of storing such data in their databases, or trust (or expect their users/customers to trust) the data to a third-party's care.

And though the above highlights the *primary* problems with today's biometric options, another critical problem also exists. As today's biometric options generally function by accepting an individual's fingerprint "sample" (at the time of a transaction), and then comparing the sample to ones retrieved from a database, it is clear that at some point prior to the transaction, the individual was required to submit a "sample" for storage within the database. This "enrollment" process is time-consuming, risky, error-prone, and considered intrusive by many individuals. And highlighting the scope of this issue is the realization that currently, the process must be performed <u>for each individual for every intended use</u>. For example, if a user intends to enroll for biometric authentication with their company (e.g. for secure access to digital files or the business' facilities), and also with merchants utilizing various biometrically-based security technologies, the individual will likely need to repeat the enrollment process for each entity, *and* be comfortable with their personal biometric data being stored on <u>each</u> of those entities' databases. This issue alone is enough to prevent many people from ever considering these options.

While at first glance, one alternative, having individuals agree to store their biometric data in a shared centralized database, appears logical and simple, it too suffers from significant problems/issues. These include: theft and privacy risks/exposures (similar to the above options), inherent search & transaction delays (due to the need to provide a secondary form of identification in order to initiate a transaction), and importantly, the need to be "on-line" to take advantage of <u>any</u> of the security capabilities (making the option inappropriate for many "internal" business needs such as protecting digital or physical assets).

In summary, the above-defined issues represent serious roadblocks to the widespread deployment & acceptance of currently-available biometric authentication options. There is uncertainty as to whether the benefits will eventually outweigh the negatives, but (minimally) unless the identified deficiencies are addressed, the full potential of biometric solutions will never be realized. Therefore, a new technology, one fully capable of addressing these needs, is likely to be positively embraced, and have the potential to gain widespread acceptance.

Introduction - *The TruProx™ Touch Technology*:

Building on the TruProx™ proximity-based, multi-layered security technology, the invention, herein referred to as the TruProx™ Touch Technology ("Touch", "Touch technology", "Touch model"), defines a biometrically-authenticated security technology/system. Touch authentication addresses applications where it is important to ensure a specific individual is authorized to perform a given task/transaction. Examples of such transactions include: enabling secure financial dealings, providing secure access to physical and/or digital items, and simple user ID & age verifications.

NOTES: For clarity in this document, the biometric option discussed & used in examples, is that of fingerprint sensing/comparison. The reader should note, however, Touch technology is not limited to fingerprint-based options. Nearly any biometric authentication technology - including retinal scan, facial recognition, palm recognition, etc. - could be utilized by the model.

Model Overview:

The underlying premise of the Touch technology is that of enabling users to carry on their person a wireless, uniquely-identifiable device (in TruProx™ terminology, a "Personal Digital Key", or "PDK") containing *their* personal biometric data. This PDK, when needed, can prove beyond question that the biometric data it contains is that of the individual attempting to utilize it. This capability, when applied as defined by the Touch model, provides users/customers and merchants/businesses/organizations with unparalleled security, ease & efficiencies of use, and risks & liabilities substantially lower than comparable options. *It should be noted, that while PDKs referred to in this document are (for simplicity sake) described as simple, stand-alone devices, in practice they may take many different forms. Some examples include: direct integration into commonly carried items such as cell phones & PDAs, attached to/replacing employee ID tags, and even incorporated into jewelry items such as watches, rings or bracelets.*

To implement the Touch model, many new concepts, processes and components have been defined. These include: 1) special hardware devices (such as PDKs containing biometric-equivalent profile storage able to be written to only once), 2) the concept of an Authorized TruProx™ Notary, 3) a biometric user setup process that is easily verified, audited & trusted, and importantly, only needs to be performed once, and 4) a flexible PDK & user verification process, enabling multiple levels of authentication (applicable as needed). The levels ranging from simple local verification of a PDK as an authentic TruProx™ device, through secure lookup of a PDK's background & status in a Centralized Registry managed by a trusted third-party.

The Touch model defines a complete, highly-efficient and safe transaction processing model. Illustrating an example use/transaction, and assuming a user and their PDK have been properly setup (see below), to complete an in-store purchase, the user simply places their finger on the merchant's Touch Reader device (see below) for a quick scan. Once read, the Reader and the user's PDK, utilizing a secure wireless communications channel, automatically & invisibly perform an instantaneous, yet exhaustive & comprehensive authentication involving multiple levels of validation. When completed, the device then requests a credit card account number (or similar) from the PDK, and either directly or indirectly conducts a standard account number validation check. And assuming a valid account number, the transaction is complete. From the user's standpoint, even though a complex authentication & authorization has occurred, it appeared as if the entire transaction includes nothing more than a quick swipe of their finger. No credit cards or tokens were handled, no signatures were needed, and no PINs, passwords, or search codes had to be remembered or entered. The entire process was highly efficient, extremely safe, and required no participating parties to accept additional risks or liabilities.

Couple the capabilities defined in the above scenario with the fact that this *same* PDK also provides the user with an elegantly simple & efficient, biometrically-protected, digital & physical access/use "key" and personal ID system, and the value of the model's underlying concept and technology becomes obvious. The sections that follow describe important aspects of the TruProx™ Touch Technology.

Note: While the Touch model addresses many needs/uses, because financial transaction processing best illustrates its capabilities and features, most examples herein relate specifically to this use. Some of the models other intended needs/uses include: digital automation/access-control, physical/device automation/access-control, basic & biometric ID/Access systems, as well as, in-store, on-line and vending-based transaction processing.

Setup:

ATN Overview

The concept of an Authorized TruProx™ Notary ("ATN") is a critical component of the Touch technology trust & audit system. An ATN can be conceptually thought of as an enhanced Public Notary. That is, as a trusted third-party providing verification that an individual's identification has been properly authenticated prior to the execution of a transaction. In the case of a Public Notary, a typical transaction includes witnessing an individual signing a legally-binding document. An ATN performs the substantially identical function, except that instead of witnessing a signature being given, an ATN witnesses the acquisition of an authenticated user's biometric data. In Touch model terminology, this is referred to as (biometrically) *initializing* PDKs. In short, an ATN accepts responsibility for ensuring a person's ID and biometric data comply with, and have been acquired & processed according to, defined security protocols.

In addition to initializing PDKs, ATNs are also responsible for adding them to registries. In Touch model terminology, this is referred to as *registering* PDKs. The model defines the concepts of private and central registries. Private registries are, as their name implies, private to a particular controlling-entity. For these registries, the controlling-entity is responsible for selecting its administrative ATN(s). The Central Registry (there is only one) is managed by a single trusted party/organization. The trusted party is solely responsible for selecting ATNs to administer its registry. These ATNs (which may also be responsible for administering private registries) are required to pass extensive background checks prior to acquiring the accreditation and associated rights.

Importantly, every function an ATN performs, from initializing & registering new users/PDKs, to updating registry data, leaves an audit trail which includes the ATN's unique personal & PDK identifiers. An example of this trail is found inside every initialized/registered PDK, where the PDK ID of the ATN(s) who performed the processes is permanently stored, along with the user's data. This audit data can be retrieved from the PDK's memory (by authorized individuals/hardware) at any time. The utilization of ATNs, and the model's established processes & permanent audit system, establish the trust, credibility, and confidence underlying the Touch model.

Initialization Overview

The purpose of the initialization process is to load biometric data from the owner/holder of a PDK (the "owner") into the PDK's permanent biometric profile storage. An initialization, which is administered by an ATN using a specialized Touch device ("TouchProgrammer", "Programmer"), can only be performed once *per type* per PDK. *Type* is defined within the TruProx™ model as a combination of the biologic metric (i.e. fingerprint, retinal scan, etc.) and the specific protection scheme/version securing the profile. While the data can be validated again at any time, as an element of the model's "trust", it becomes technically unable to be over-written, deleted, etc. *Note: While performing initializations in-person with an ATN is the preferred method, utilizing specialized hardware, and technologies such as video conferencing, performing the process remotely via PCs, public kiosks, or similar is an option. And depending on need, it may also be acceptable to utilize initialization procedures not including ATNs.*

Summarizing a fingerprint-based (biometric) initialization example, the process includes a TouchProgrammer performing various ATN & PDK-related status checks, the owner providing fingerprint samples (usually of each finger but as few a single finger print or single biometric indicia) via the TouchProgrammer, and the Programmer writing the data, along with the ATN's unique PDK ID, to the owner's PDK. As a result of this process, the ATN's PDK ID becomes a permanent element of the Touch audit system, and can be traced from any transaction in which the owner's PDK is used. Below are more detailed descriptions of these steps.

To begin establishing the model's "trust", the TouchProgrammer first performs status checks of the ATN's and owner's PDKs against the Central Registry. This occurs by the ATN inserting his/her personal PDK, as well as the owner's, into openings in the Programmer. Once inserted, the device executes a Central Registry validation on both PDKs (and indirectly, therefore, on the ATN) to: 1) ensure the ATN and the ATN's PDK are registered and in good-standing, and 2) ensure the owner's PDK is in good-standing (meaning it has not been reported as stolen, lost, or similar ... or has simply never been registered).

Next, assuming the above checks were successfully completed, the TouchProgrammer begins the actual initialization. This involves the owner scanning each (desired) finger on the Programmer, one at a time. If needed, the Programmer allows (or requests) re-scans during the process to ensure valid reads of each print are captured. When the ATN and TouchProgrammer are satisfied all desired fingerprints have been adequately acquired, the ATN signals the Programmer to *write* the data to the owner's PDK. The TouchProgrammer then computes mathematical hashes of the data (or similar) and instructs the owner's PDK to accept/store the new bio-equivalent data, as well as the ATN's PDK ID, and the Programmer's ID, to its permanent *biometric* profile storage. If desired, the PDK can now be registered. Importantly, when either PDK is removed from a TouchProgrammer, the device automatically clears its own memory.

Registration Overview

The purpose of the registration process is to enable enhanced authentication (i.e. additional layers) when processing standard/ongoing transactions (see below). As PDK's can only be initialized a single time per type, and only ATNs can perform the registration process, an initialized/registered PDK effectively becomes a public, "trusted" device, with verifiable rights and status. Once registered, a PDK's rights and status can be fully verified by any Touch device in communications with the appropriate registry. It should be noted that any PDK, whether or not it has been (biometrically) initialized, can be registered. The rights of a given PDK, however, correspond to the type of initialization & registration it has undergone. If desired, though, a PDK can always be re-registered to add additional bio-profiles, modify its rights, etc.

In practice, registries are securely-accessed databases comprising, among other items, PDK, ATN, and Touch device information ... but no user biometric, bio-equivalent, or highly-personal/critical data. There are two basic registry types: private registries and the TruProx™ Central Registry. Private registries are established & administered by their controlling-entities (usually to manage specialized/independent needs). The Central Registry, in contrast, is a single, highly-secured, centrally-located database run by a trusted third-party entity/organization. To administer (add, modify, delete records) *any* registry, an ATN is required (and must be recorded & in good-standing in the Central Registry). ATNs wishing to administer only private registries, however, do not need to complete the extensive background checks, etc. required of those administrating the Central Registry.

While a PDK is typically registered immediately following a standard initialization process, it does not *have* to be. And regardless of when performed, the end result is identical. Summarizing, the registration process generally includes an ATN validating a PDK's biometric profiles(s) as that of its owner, positively authenticating the owner's identification, and adding/updating a record in an appropriate registry. While performing initializations in-person with an ATN is the preferred method, utilizing specialized hardware, and technologies such as video conferencing, performing the process remotely via PCs, public kiosks, or similar is an option. And depending on need, it may also be acceptable to utilize initialization procedures not including ATNs.

A typical PDK registration session begins by validating the PDK's initialization process. This is preferably accomplished by the ATN having just witnessed/completed the process. If, however, the initialization process was performed at an earlier time, the ATN must re-validate each previously-stored bio-profile. This comprises (using an example fingerprint bio-profile) the ATN placing the owner's PDK into a TouchProgrammer (along with their own which, as always, is verified by the Programmer against the Central Registry before proceeding), and the owner subsequently placing one finger at a time on the TouchProgrammer. The Programmer (or optionally the PDK, a separate hardware and/or software processor, or some combination therein) then compares the newly-acquired prints to what should be their equivalents stored in the PDK. If each is successfully matched, the PDK's biometric data is considered authentic, and its initialization valid. It should be noted that PDKs can be registered without their biometric data being validated. These PDKs, however, cannot successfully authenticate transactions requiring biometric validation (many do not).

Next, the ATN manually authenticates the owner's identification. This generally comprises the ATN reviewing/validating a defined number of publicly-available/accepted forms of personal identification. These may include: a valid driver's license, passport, social security card, or credit card. The specifics of this process can change from time-to-time as the managing parties (those defining the model's "trust") determine/refine what is "acceptable".

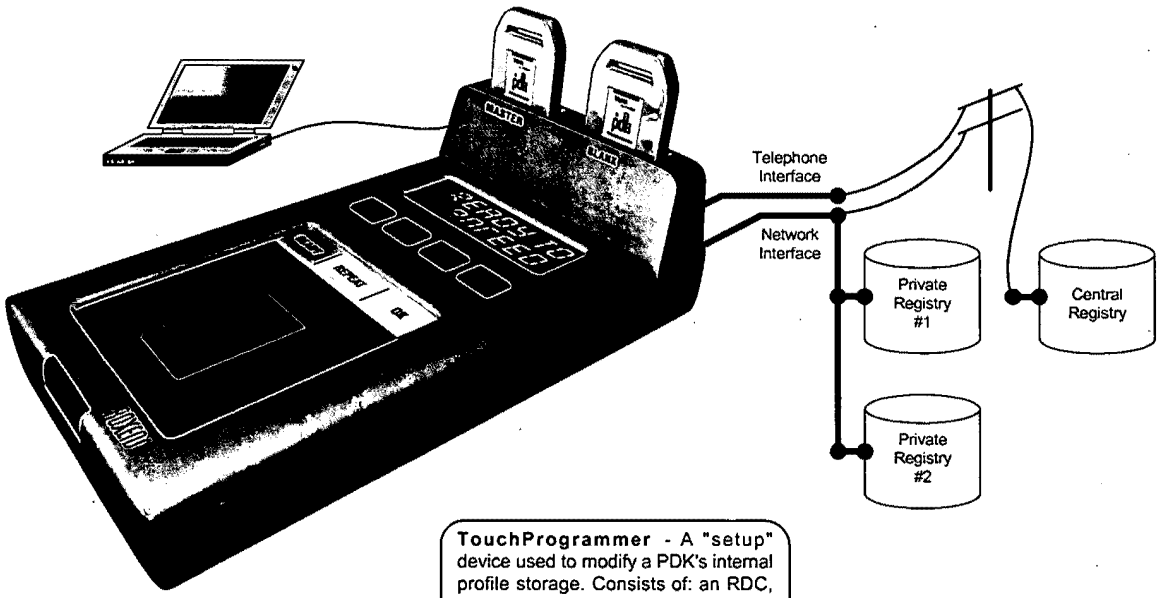
With the owner's identity successfully validated, the ATN commands the TouchProgrammer to add/update a record in the appropriate registry's database (the ATN must, of course, be recognized as a valid administrator of the registry to proceed). The TouchProgrammer then automatically updates certain fields in the record such as the owner & ATN's unique PDK IDs, while other elements are manually entered by the ATN via a PC/terminal connected to the registry. These elements may include the user's name, address, phone number, and date of birth, as well as, optional items such as auto-expiration date/time (where the registry automatically "expires" a PDK at a certain point in time).

The final step in the registration process is for the TouchProgrammer to update various fields in the newly-registered PDK's internal profile storage. These fields include: the PDK's rights information, the registering ATN's ID, and the TouchProgrammer's ID. These audit items, as always, are intended to enhance the underlying "trust" of the Touch model by being traceable in the event of fraudulent use. The registered PDK can now, depending on its established rights, satisfy private and/or Central registry authentications (as defined below).

NOTE: Throughout the initialization and/or registration processes, no actual biometric data is ever stored or maintained anywhere. And bio-equivalent data is stored only in the owner's PDK. And importantly, when either PDK is removed from a TouchProgrammer, the device automatically clears its own memory.

TouchProgrammer & System

To eliminate the possibility of unintended PDKs becoming involved in a programming session, the intended PDKs must be placed in very close proximity (e.g. in the openings shown) of the Programmer in order to properly communicate with the device.



TouchProgrammer - A "setup" device used to modify a PDK's internal profile storage. Consists of: an RDC, biometric-reader, status LEDs & display, and various I/O ports.

PDK Conceptual User-Bio Profile Data Format

Registry Code	(initializing) ATN ID	(registering) ATN ID	Programmer ID	User Bio-Data (including up to 10 fingerprint hashes)

00 - No Reg | 01 - Private Reg | 10 - Central Reg | 11 - Multi-Reg

See following page for a step-by-step review of TruProx™ Touch Technology Setup Procedures

Setup: Step-by-Step

The ATN Role & Designation Process

- To become an ATN, an individual completes a detailed application (possibly including biometric data, and indicating their willingness to assume certain legal obligations), and submits it to the ATN approval committee (members to be determined). When/if approval is granted, the individual is provided a PDK if needed, and their application data & unique PDK ID are permanently added to the Central Registry (and updated as needed to indicate changes in status, violations incurred, etc.).
- If an ATN does not have access to a TouchProgrammer ("Programmer"), he/she is provided one. Each programmer's unique ID is recorded in the Central Registry at issuance.
- Any ATN in good-standing may conduct user (biometric) initializations. For audit purposes, the unique IDs of the ATN, the ATN's PDK, and the TouchProgrammer utilized in the process, are permanently stored in the memory of an initialized PDK.
- To register an initialized PDK (registering non-initialized PDKs is allowed, but such PDKs are unable to satisfy biometric authentications) an ATN designated as an active administrator for the intended registry, is required. ATNs are designated as follows:
  - For a private registry, the owner of the registry may designate (or withdraw) ATN(s) of their choosing.
  - For the Central Registry, only Proxense (or a selected third-party, such as the ATN approval committee) may designate ATNs (who must successfully complete a stringent approval process).

(Biometrically) Initializing PDKs

- Before a new user's PDK can be initialized (have its owner's biometric data permanently stored in it), the TouchProgrammer's ID, and the ATN's PDK ID must be validated against the Central Registry as active & in good-standing. If all validate, and the ATN has properly conducted the initialization process (see below), the new user's PDK is permanently programmed with their new personal bio-profile data. Once written, this data is "physically" unable to be over-written, modified, or deleted, but can be re-validated by an ATN if needed. The PDK is now (biometrically) initialized. Following this process, a PDK is typically registered (added to a registry). This is not mandatory though, as ATNs can re-validate (then register) a PDK at any time.
- The initialization process:
  - A new user's PDK <u>and</u> an ATN's PDK are inserted into the TouchProgrammer.
  - The ATN completes a standard biometric authentication to validate their (personal) presence.
  - The ATN's PDK ID and TouchProgrammer's ID are authenticated against the Central Registry. Assuming both validate, the Programmer becomes temporarily enabled (though times-out if not utilized within a certain period of time).
  - The ATN then instructs the user to scan their fingerprints into the TouchProgrammer. The Programmer allows the user to perform each scan as many times as needed to ensure valid data has been captured.
  - When all prints are input & validated, the ATN instructs the Programmer to permanently write the new bio-profile data to the user's PDK. Once completed, this procedure can never be redone, though the profile can be re-validated.
  - When either PDK is removed from the TouchProgrammer, the Programmer's memory is automatically erased.

Registering PDKs

- To add a PDK to a registry, or "register" it, two basic validations must be successfully completed (regardless of the registry type - private or Central). The first is to confirm the PDK being registered is properly initialized. The second is to confirm the user's personal identification is correct. This generally consists of the ATN manually authenticating a pre-defined quantity of approved personal identifiers (e.g. driver's license, passport, social security card, credit card, etc.) provided by the user. If the validations are successfully completed, the ATN enters the following into a database record permanently added to the registry:
  - The initializing ATN's personal PDK ID
  - The registering ATN's personal PDK ID
  - The user's PDK ID
  - The TouchProgrammer's ID
  - The site ID
  - The registration date & time
  - Certain user data items (typically publicly-available items such as an address, phone number, date of birth, etc.)
  - Optional data items such as auto-expiration date/time
- Finally, the appropriate biometric profile in the user's PDK is updated to indicate the current Registry Code, as well as various other identifiers enabling future audits (see "PDK Conceptual User-Bio Profile Data Format" on previous page).

General Use:

Authentication

The Touch model's critical "trust" elements - the role of ATNs, and the initialization & registration processes - come together in the (transaction) authentication process. The "trust" established by the previously-described setup processes enables an extremely efficient, secure and elegant, yet powerful and scalable authentication process. At the very core of the Touch model, *and* every transaction protected by it, the authentication process builds on, and takes advantage of the foundation they provide.

The Touch model's efficiencies begin with the need to perform the model's setup process only once per user. When an ATN has completed a user's setup, that user is *automatically* able to utilize their PDK for *any* Touch-based application. This is very significant in that, while *users* clearly benefit by not needing to continually "re-enroll", *controlling-entities* (merchants, account issuers, etc.) similarly benefit by not needing to conduct massive customer enrollments when migrating to the technology, as any properly-setup user/PDK *is* "enrolled". Similarly, both parties greatly benefit from the model's specifications for the storage of sensitive biometric data. As a user's biometric data is *never* stored anywhere except within *their own* PDK, they are never required to put the data at risk by allowing it to be stored in merchant or third-party databases ... and merchants, correspondingly, are never required to handle, store, or maintain this sensitive data, or expect their customers to trust a third-party to do so. Summarizing, the combination of the Touch model's *one-time setup* design and its data storage specifications, provide the basis for the model's extremely efficient, low-risk and scalable protections.

The primary hardware component users interact with during authentication is the Touch Reader. Two general versions are defined (though others are envisioned), the simplest of which is a device called a TouchPad. A TouchPad generally has a bio-reader (a fingerprint scanner in these examples), a standard TruProx™ Reader/Decoder/Circuit (an "RDC",), a network connection (wired or wireless), and some form of communications (I/O) port (typically USB or serial). TouchPads can be thought of as signature-replacement devices, as they are commonly configured as supplemental components to credit card terminals. In this role they replace the signature pads typically attached to these terminals with the Touch model's wireless digital user/PDK authentication process. The other basic Touch Reader is a device called a TouchTerminal. TouchTerminals are simply TouchPads with *integrated* credit card terminals, and are intended to *replace* standard credit card terminals. But regardless of the Touch Reader, the underlying user/PDK authentication process is identical to the point where credit card authorization takes place.

Illustrating a typical in-store check-out scenario with a merchant employing TouchPads at its checkout counters, and a customer wishing to utilize their (properly initialized & registered) PDK to complete the purchase: The customer presents the items to be purchased to a clerk who scans/rings-up the items, and informs the customer of the amount due. To then complete the transaction, the customer simply presses a finger to the TouchPad ... and from their standpoint, the sale is complete. No signatures, passwords, PINs, or search codes required, no fumbling with credit cards/tokens needed ... a simple fingerprint scan *completes* the process.

Behind the scenes however, utilizing core TruProx™ technologies (see related TruProx™ patent filings), the customer's PDK and merchant's TouchPad have performed an instantaneous, yet exhaustive & comprehensive authentication process involving multiple levels of validation. And importantly, the levels performed were chosen by the merchant. As the model's levels are scalable - the higher the level used, the greater the authentication protection - merchants can select an appropriate level of authentication for any given transaction. *Note: This is generally accomplished in one of two ways. A merchant either specifies certain levels for particular transaction types (e.g. sales less than $50 do not require biometric authentication, those $50 or greater do), or they simply establish a default level in each Touch Reader to be applied to all transactions processed by the device.*

Assuming the customer's PDK satisfies the required authentications, the TouchPad requests the PDK to transmit to it the appropriate credit card number to which the charge should be applied (the ability to securely store/retrieve items such as credit card numbers is defined in related TruProx™ patent filings). If the customer has chosen to maintain more than one credit card account, the device simply provides a list enabling them to select which to use. Once received, the TouchPad notifies the attached credit card terminal a valid "signature" has been obtained, and then forwards the customer's credit card number to it for standard processing. The customer simply awaits the authorization, takes the receipt and goes. *Note: Had a TouchTerminal been used in this example, the only difference would have been in which device performed the credit card validation (the TouchTerminal versus the standard credit card terminal).*

Authentication (continued)

Summarizing, with the simple press of a finger to the TouchPad, the customer has completed an extremely secure, biometrically authenticated, financial transaction ... in only seconds, and without requiring any additional steps, account numbers, PINs, passwords, search codes or signatures.

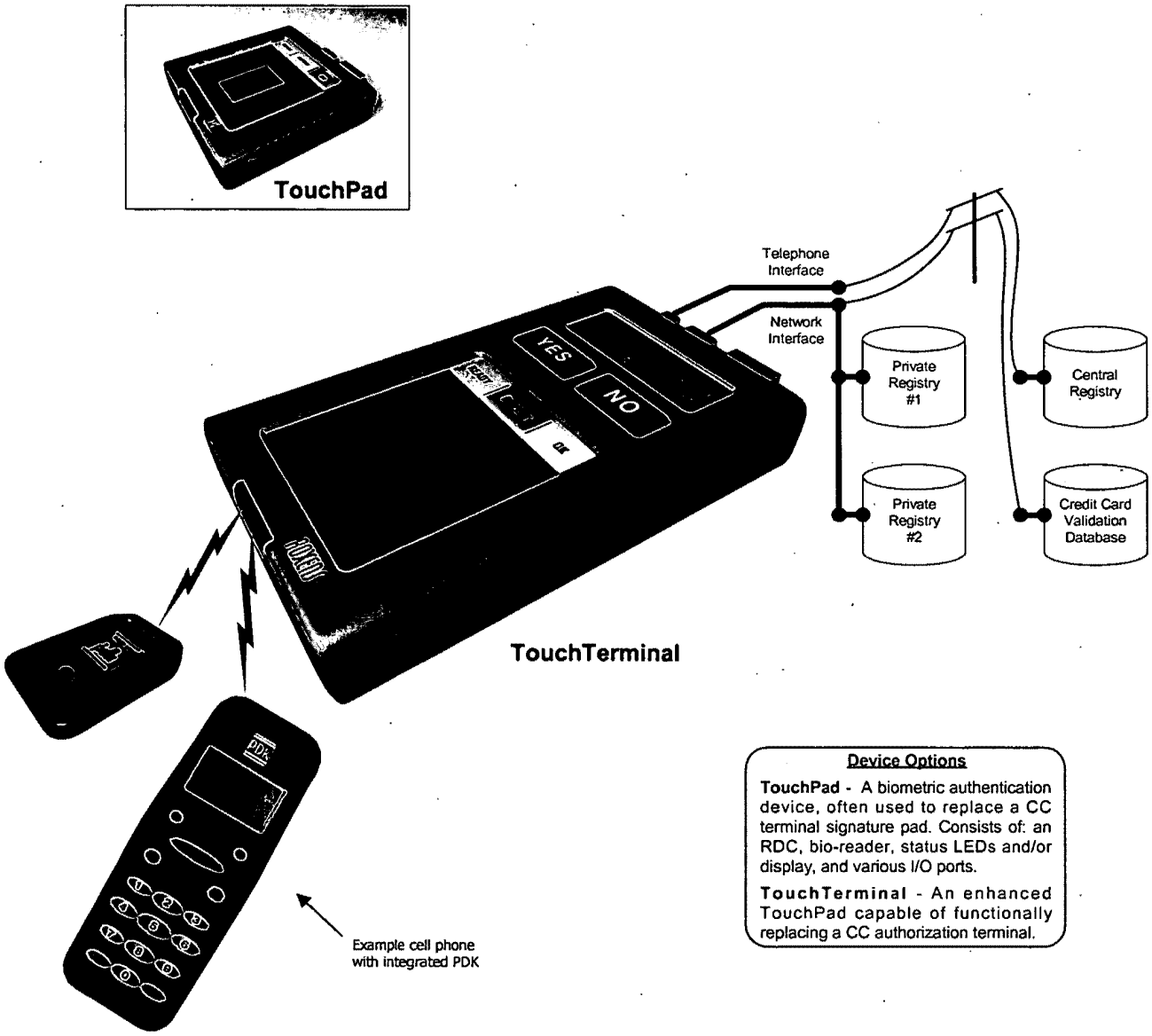
Note: A critical step occurring in the above process - one unique to the TruProx™ Touch Technology - is the TouchPad's ability to automatically determine which PDK in its vicinity is associated with biometric data it has just acquired. This step is a primary enabling factor in the Touch model's overall ability to function via pure-proximity/bio-scan, as it enables users to initiate (and complete) transactions without requiring them to specifically identify themselves or their PDKs. See section "Authentication: Step-by-Step" for details. This capability enables "one touch" validation of transactions, where the only action required of users is to input their bio-equivalent data (such as a scanned fingerprint) to initiate and complete at transaction.

In comparing the use of a TouchPad for providing secure access-control (e.g. to physical doors or digital files) to its use in the above-described financial transactions, the similarities of the steps involved (and therefore the underlying consistency of the Touch model) become apparent. The only differences noted concern the steps after which user/PDK authentication has been completed. Where a TouchPad handling financial transactions would signal an attached device to process a credit card transaction, a TouchPad providing access-control instead sends a signal to a door lock or digital filing system to authorize access. *Note: In the case of digital files, other TruProx™-based technologies (as defined in related TruProx™ patent filings) may also be utilized to further enhance and simplify the user experience.*

Similarly, to utilize the technology for simple user ID and/or age verification purposes, the process is even less involved. As part of a Level 3 or 4 authentication, a simple check of the user's ID and/or date of birth fields in the registry record, followed by the sending of a return code to the requesting device, is all that's required.

Regardless of the application, however, the exceptionally efficient and simple to use Touch technology enables a simple biometric scan to *initiate & complete* extremely secure transactions ... from the most simple, to the most complex.

Touch Readers & System



Device Options

TouchPad - A biometric authentication device, often used to replace a CC terminal signature pad. Consists of: an RDC, bio-reader, status LEDs and/or display, and various I/O ports.

TouchTerminal - An enhanced TouchPad capable of functionally replacing a CC authorization terminal.

See following page for a step-by-step review of TruProx™ Touch Technology Authentication Procedures

Authentication: Step-by-Step

Level 1 - Local PDK Authentication:

1. When a PDK comes into proximity of a Touch Reader, the Reader requests the PDK to conduct a Local PDK Authentication, and check-in ("register") with it. This process consists of:

   a. Completing a standard TruProx™ PDK-to-RDC authentication (ensuring the type & validity of the devices) and establishing a secure communications channel.

   b. The PDK transmitting its unique secret ID & encrypted bio-profiles to the RDC (the RDC automatically selects the appropriate bio-profile to use).

   c. The RDC temporarily buffering the received data, and notifying the PDK it is communicating with a Touch device (versus a simple RDC).

   NOTE: *The RDC maintains metrics for each "registered" PDK, including: signal strength, clarity of signal, and time in vicinity. To minimize the quantity of PDKs "registered" at any given time, a Touch Reader typically maintains a small diameter (approx 3-4') proximity zone.*

Level 2 - Local Biometric Authentication:

2. When the Touch Reader detects biometric contact (e.g. from a user's finger), Local Biometric Authentication begins. This consists of it performing a biometric scan, and comparing/testing the resulting data against all buffered PDK biometric profiles (prioritized by accumulated metrics) until a match is found. *Optional implementations may specify the compare/test processing be performed by the PDK, a separate hardware and/or software processor, or some combination therein,*

   NOTE: *If instead a PDK BioKey was utilized (versus a standard PDK) in the transaction, whichever device detected the biometric data (the BioKey or TouchPad) would initiate the step, allowing the processing of the data to take place as always (as defined by the specific implementation).*

3. Assuming a match is found (completing Local Authentication), the RDC determines which additional authentication levels to perform (none, Private Registry and/or Central Registry). If none (only Local was specified), the authentication process is complete (skipping Levels 3 & 4). Otherwise, the RDC looks at the PDK's buffered biometric profile Registry Code field to determine if further validation against desired registry(s) *can* be performed. Assuming *yes*, Levels 3 and/or 4 are performed next.

   NOTE: *The choice as to which level(s) of authentication to perform is determined by the Touch Reader's setup parameters, or software commands received via the device's I/O ports. It is acceptable to specify multiple private registries and/or the Central Registry for validation.*

Level 3 & 4 - Private/Central Registry Authentication:

4. To conduct Registry Authentication, the RDC establishes a secure channel (typically via a network connection) with the appropriate registry, and transmits a packet typically including the following: PDK ID, ATN IDs, TouchProgrammer ID, site ID, and time-stamps.

5. The registry's controlling software compares the received data against the registry's database to determine the PDK's status (Valid, Inactive, Expired, Lost, Stolen, etc.), while recording a complete audit record. If needed, the process is repeated for any additional registries until finished. Assuming successful validation(s), the audit record is completed, and a "Valid" status is returned to the RDC.

   NOTE: *Variations of **Level 4** and **Transaction** (below) processing may include combining the processes together in various fashions. One example is to enable a credit card (CC) validation facility to directly request Level 4 Authentication from the Central Registry (versus having the request initiated from the merchant-based terminal equipment), as part of the Transaction Validation step. This could be accomplished by the Level 4 request data being packaged in the Transaction Validation data sent to the CC validation facility, with the facility then parsing the Level 4 data and passing it directly to the Central Registry for authentication. This variation represents one of many options which could be utilized to enhance efficiency and/or simplify process-integration with CC validation facilities.*

Transaction Validation:

Assuming all levels of authentication are satisfactorily completed, the RDC notifies the Touch Reader the PDK is "Valid", approving the underlying transaction for processing. Depending on the type of Touch Reader in use, one of the following occurs:

TouchPad - The RDC notifies (via its I/O ports) the controlling device that approval has been granted (and typically forwards an account number or similar).

TouchTerminal - The RDC conducts a standard remote credit card ("CC") authorization/transaction.

NOTE: ***TouchPads** can be viewed as signature-replacement devices, and **TouchTerminals** (which include CC terminal hardware), as CC terminal replacements.*

Unique Design Elements/Capabilities:

Trusted Local-Biometric Authentication with Centralized Vehicle (PDK) Verification

The Touch model is unique in its ability to provide trusted local biometric-authentication of an individual (via the individual's PDK and any Touch Reader/RDC), by coupling remote, real-time, validation of the status of the biometric storage *vehicle* (the individual's PDK) containing the individual's biometric data. Under the model, the only location an individual's biometric data is ever maintained is in that individual's personal PDK. This fundamental and critical design feature enables any controlling-entity to biometrically authenticate individuals without assuming the liability and risk of storing, maintaining and protecting such sensitive (biometric) data themselves, or relying on a third-party to do so. Summarizing, under the Touch model, individuals *always* manage their own biometric data, and are therefore never expected/forced to trust another party's ability to protect this sensitive information. Correspondingly, controlling-entities *always* know an individual performing a transaction is who they claim to be, and authorized to do so. And importantly, the entities never need to ask their customers/users to part with what is considered by many to be an individual's most private and personal data.

One-Time User Setup

An item important to establishing the Touch model's efficiencies is its user-setup requirements. Regardless of how many separate uses and/or controlling-entities an individual may wish to utilize, only a single setup (initialization & registration) is ever required. This results in controlling-entities never needing to perform this time consuming process themselves, and users only needing to complete the process once. Additionally, due to the model's fundamental data storage design (see paragraph above), risks and liabilities that would otherwise be assumed by controlling-entities (in acquiring & maintaining such sensitive biometric data) are eliminated. And correspondingly, users enjoy the peace of mind of knowing their private biometric data is stored only in *their* PDK (versus the databases of every controlling-entity they may utilize) ... *and* in knowing that even if their PDK is ever lost or stolen, its data remains fully protected. Summarizing, controlling-entities can migrate to the Touch model without assuming additional data-storage-related risks and liabilities, conducting massive customer "enrollment" programs, or requiring their customers to trust a third-party to protect their most-private data; and by completing only a single setup session, an individual can utilize their PDK in any Touch-based transaction, and importantly, remain in *total* control of their personal biometric data. Finally, the Touch model's ability to easily co-exist with any current transaction processing system, further simplifies the migration process.

One-Touch Transactions

One of the most basic, yet powerful components of the entire Touch model, in particular from a user's viewpoint, is the ability to initiate & complete entire transactions with nothing more than a single touch of a finger to a Touch Reader. No card swipes, passwords, PINs, search codes, or similar, are required. While this feature is implemented via a number of other unique Touch capabilities (see next paragraph as an example), the One-Touch Transactions capability is itself a critical benefit/feature of the Touch model, as it significantly simplifies and enhances the user-experience of every intended application (from digital & physical asset control, to financial transaction processing).

Bio-Scan to PDK Auto-Association

The ability of a Touch Reader/RDC to automatically discern which PDK in its proximity is the one to which a just-acquired biometric scan belongs, is a primary enabling factor of the Touch model's One-Touch feature, and more generally, its true-proximity functionality.

RDC PDK-Metrics Eavesdrop-Resistant & Transaction-Optimization

To minimize the possibility of eavesdropping (and related fraudulent use), and to optimize transaction processing speed, Touch Reader RDCs maintain a suite of metrics for each PDK currently in vicinity, including: signal strength, clarity of signal, and time in vicinity. Touch Readers utilize these metrics to make educated guesses as to which PDK is most likely to be the one to which a newly-acquired biometric scan belongs (minimizing time wasted analyzing incorrect PDK's biometric data). Additionally, to reduce the quantity of PDKs "registered" with a Touch Reader at any given time, the devices typically maintain small diameter (typically 3-4') proximity zones. These features/capabilities combine to optimize authentication procedures, speeding up transactions, and minimizing opportunities for theft and fraud.

Unique Design Elements/Capabilities (continued):

Integrated Use/Fraud Detection & Audit Model

The Touch model defines a simple, consistent and persistent mechanism for inherently establishing a use localization & audit trail. Every ATN, Touch device, and PDK is assigned a unique ID, typically at the time of manufacture, authorization or first-use. Every PDK permanently stores the IDs of the ATN(s) & Touch device(s) utilized in its setup (initialization & registration) to its internal profile storage. When needed, the Touch model can access this information, allowing it to trace every transaction in which the PDK was used. And importantly, all registry-based transactions (private or Central) support this audit function. The audit model is based on the simple fact that the IDs of the ATN, Programmer device, and site (where the initialization/registration took place) are all permanently recorded right in the each user's PDK profiles. Therefore, the entire initialization/registration information is available at each transaction, and can accordingly be traced back to the sources.

Multi-Use, Variable-Protection PDK Profiles

The PDK *profile* mechanism supports the following unique features, enabling seamless PDK use in the Touch *and* other TruProx™-based models:

- While all profiles are accessed in a standardized and consistent manner, only one profile *per type* can store a user's biometric data. *Type* is defined as a combination of the biologic metric (i.e. fingerprint, retinal scan, etc.) and the specific protection scheme/version securing the profile. RDCs automatically select which type to use.
- Once written, a biometric profile becomes permanent (unable to be modified or overwritten).
- Each profile can utilize a unique encryption/protection scheme to protect the data it contains, including schemes where even the PDK does not "understand" the stored data (useful for storing data such as credit/bank account numbers), effectively acting only as a secure pass-through vehicle.
- Individual profile-types can mandate specific Touch or TruProx™ devices be used to update/modify/read their contents (e.g. only TouchProgrammers can modify a biometric profile, but an individual's personal RDC can be used to modify another profile, such as one containing an account number).

Real-Time, Scalable Security/Levels

Currently, up to four levels of user/PDK authentication can be performed for a given transaction:

Level 1	(*Local PDK Auth*)	- Confirms PDK (and RDC) are authentic TruProx™ hardware devices.
Level 2	(*Local Biometric Auth*)	- Confirms PDK biometric data is that of the individual attempting to use it.
Level 3	(*Private Registry Auth*)	- Confirms status of PDK via private registry(s) remote inquiry.
Level 4	(*Central Registry Auth*)	- Confirms status of PDK via Central Registry remote inquiry.

Which level(s) are performed is determined by the item/transaction, default Touch device configuration, or the PDK (as selected by the appropriate controlling-entity). All PDKs are capable of *performing,* though not necessarily *satisfying,* any authentication level. The ability to scale up/down the required protection to fit a given application's security needs enables a consistent, scalable and secure model, able to address nearly any concern. And, as needed, the number of available levels, the security defined by each level, and the interoperability between levels can be modified/enhanced.

Flexible Bio-Readers Location Support (on PDK and/or Touch Reader)

The Touch model supports standard, bio-*capable* PDKs (as described in this document), as well as PDK BioKeys, (which include *onboard* biometric readers - see related TruProx™ patent filings). While standard PDKs are fully capable, and generally-preferred under the Touch model, in certain circumstances it may be desirable to utilize PDK BioKeys. The Touch technology seamlessly integrates & fully supports both options, providing a unified model and consistent user experience.

Unique Design Elements/Capabilities (continued):

Low-Power, True-Proximity, Networkable, Biometrically-Capable Touch Devices

Touch Readers, each uniquely-identifiable, require relatively little power, include various I/O ports, and of course, fully support the Touch model specifications (such as registry interaction) and core feature set (including CRDC synchronization, tiered client access, dual transceiver, and dynamic cell-size variation - see related TruProx™ patent filings). The devices are also capable of supporting wired & wireless network communications standards, and include I/O ports enabling secure (encrypted) communication with external devices. These features make it possible for Touch Readers to assume many roles, including: directly controlling/triggering hardware or software access-control devices, replacing or working in conjunction with legacy equipment such as credit card authorization terminals, etc. TouchProgrammers are similar to Touch Readers, while including modifications such as very-close-proximity PDK openings (slots), firmware enabling the devices to command PDK profile modifications, the need for an ATN's PDK to be inserted in order to function, and an auto memory clear feature (triggered by either PDK being removed).

Compact Design, Low-Cost, Low-Maintenance, Low-Power, True-Proximity, Biometrically-Capable PDKs

Standard PDK design specifications intentionally define a low-cost, extremely power-efficient & compact circuit, capable of supporting multiple profiles (as described in this document), wireless biometric authentication with Touch Readers, the complete TruProx™ core feature set (including CRDC synchronization, tiered client access, dual transceiver, and dynamic cell-size variation - see related TruProx™ patent filings), and optional items such as battery-condition monitor/announce, power on/off switch, and use-specific interface buttons. These features, in part, enable a versatile, uniquely-identifiable, PDK circuit, to wirelessly, and without direct physical contact, conduct biometric authentication with Touch Readers, opening up vast opportunities for innovative new devices. Some examples include: Cell phones & PDAs with integrated PDKs, PDK-embedded employee ID tags, and PDK-embedded jewelry items such as watches, rings and bracelets. Quite simply, the ability for a user to conduct biometrically-authenticated/protected transactions via their cell phone (or similar device, as mentioned above) - without needing to even touch the device - represents an obvious advance in convenience and simplicity over any currently-available alternative. Therefore, the underlying PDK circuitry design is itself a critical component in the Touch model, greatly improving its potential to become widely adopted across broad markets.

25000/01000/DOCS/1621020.1

PROXIMITY
PROXENSE
TECHNOLOGIES

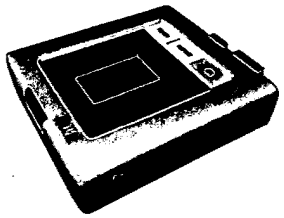
truprox™ TOUCH TECHNOLOGY

An Introduction & Overview

truprox™ TOUCH TECHNOLOGY

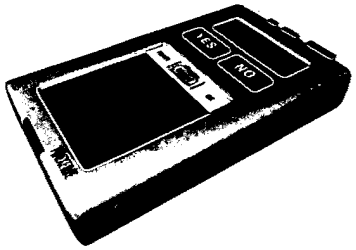
What is TruProx™ Touch Technology?

A powerful extension to the core TruProx™ technology where a simple touch of a finger is all that's needed to conduct and complete a biometrically-protected transaction.



Select an item for purchase, Touch a finger ... and go

No plastic cards	Nothing to swipe
No passwords	Nothing to remember
No PINs	Nothing to lose



Security, Convenience, Ease of Use, Personal Privacy

PROXIMITY PROXENSE TECHNOLOGIES

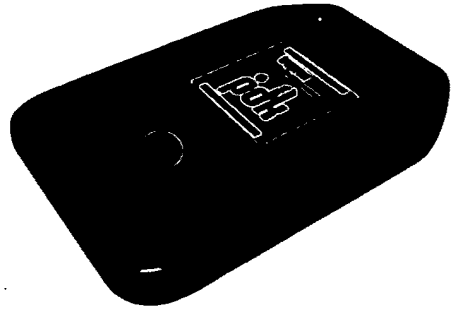
truprox™ TOUCH TECHNOLOGY

What makes TruProx™ Touch unique?

A user is never required to give up their biometric data to any individual or entity. The data resides only on the personal PDK carried in their pocket.

Merchants and businesses wishing to utilize the technology never need to "register" new customers ... or accept the liability of maintaining their biometric data.

The technology is fully scalable. The *appropriate* level of security can always be applied as *needed*. This results in a consistent and extremely cost-effective model ... and user experience.



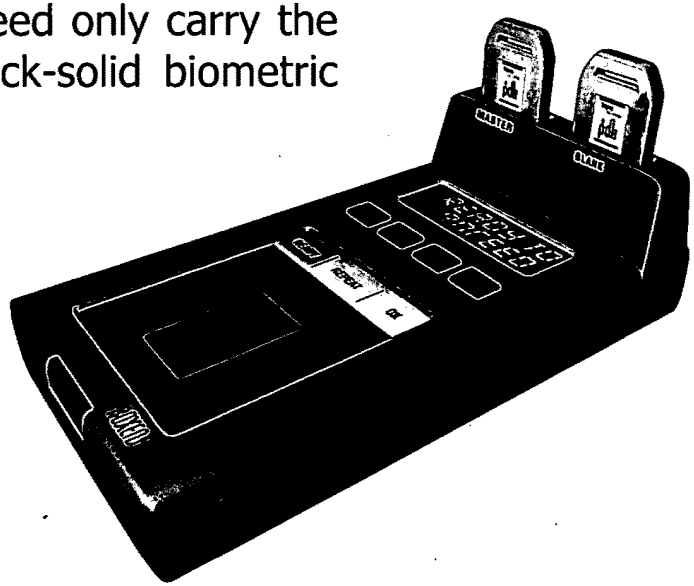
PROXIMITY PROXENSE TECHNOLOGIES

truprox™ TOUCH TECHNOLOGY

How is it used?

A one-time initialization - performed by an authorized representative - permanently, and extremely securely, stores an individual's fingerprints in their personal digital key (PDK).

Utilizing any TruProx™ PDK, users need only carry the device in their pockets to enable rock-solid biometric authentication whenever needed.



PROXIMITY PROXENSE TECHNOLOGIES

truprox™ TOUCH TECHNOLOGY

How is it used?

Illustrating with the scenario of an individual wishing to purchase an item from a store:

Once initialized, other than simply carrying their PDK on their person, a user need only touch their finger to the merchant's Touch device ... and from their perspective, the transaction is complete.

Behind the scenes however, the PDK & Touch devices perform an instantaneous, yet exhaustive & comprehensive authentication process involving multiple levels of validation. Assuming these processes conclude as expected, the individual's credit card information is securely transmitted to the appropriate issuer, and the transaction is allowed to complete.

PROXIMITY PROXENSE TECHNOLOGIES

truprox™ TOUCH TECHNOLOGY

Who / what can benefit from the technology?

Any sales / financial transaction.
An individual can complete an entire purchase with one quick touch of their finger. Fast, simple, secure.

Anywhere secure access to a device, space, or transaction is desired.
The low-cost PDKs enable wide-spread, ultra-secure, extremely low-maintenance protection.

Anywhere simple user authentication is needed.
Extremely fast, simple, rock-solid identification is now possible.

Any individual already utilizing PDKs elsewhere.
Many other uses of the technology are available or in development resulting in a single key (PDK) providing multiple capabilities.

truprox™ TOUCH TECHNOLOGY

Technology Highlights:

Extremely secure, multi-layered protection.

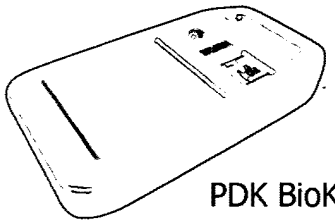
Low-cost PDKs enabling wide-spread use (and all PDKs are compatible with the system - including PDK BioKeys).

Touch devices incorporating proprietary TruProx™ Reader/Decoder Circuit (RDC) technology - providing unparalleled proximity services and wireless communications security.

Applicable to closed (e.g. known-user/private business) and open (e.g. anonymous-user/general sales) environments.

truprox™ TOUCH TECHNOLOGY

The Components ...

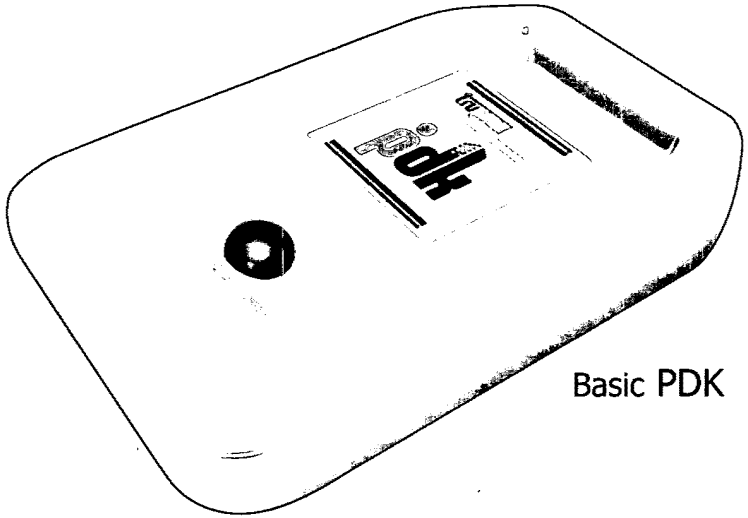


PDK BioKey

Any Personal Digital Key (PDK)

Any/all PDKs support full functionality.

PDK BioKeys (basic PDKs with on-board biometric readers), though not required, are fully compatible with Touch devices.



Basic PDK

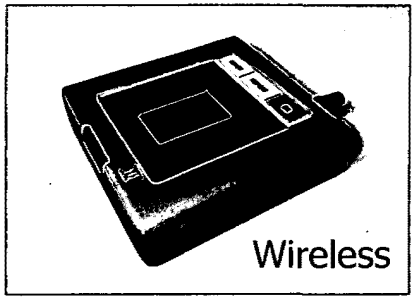
PROXIMITY PROXENSE TECHNOLOGIES

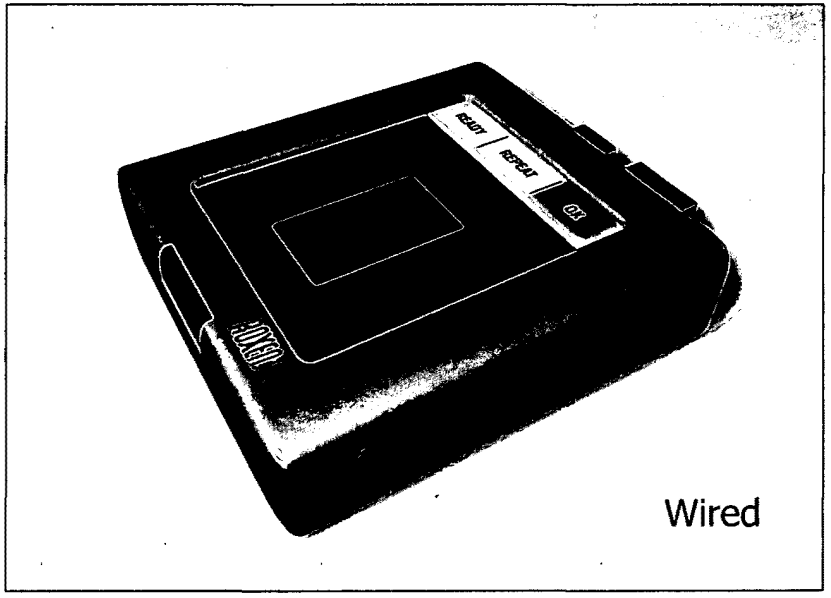
truprox™ TOUCH TECHNOLOGY

The Components ...

TouchPads (wired & wireless versions – PC card versions also likely)

Commonly used for simple authentication / access control needs, or credit card terminal signature device replacements.





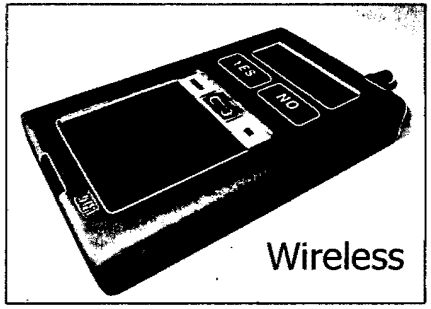
PROXIMITY PROXENSE TECHNOLOGIES

truprox™ TOUCH TECHNOLOGY

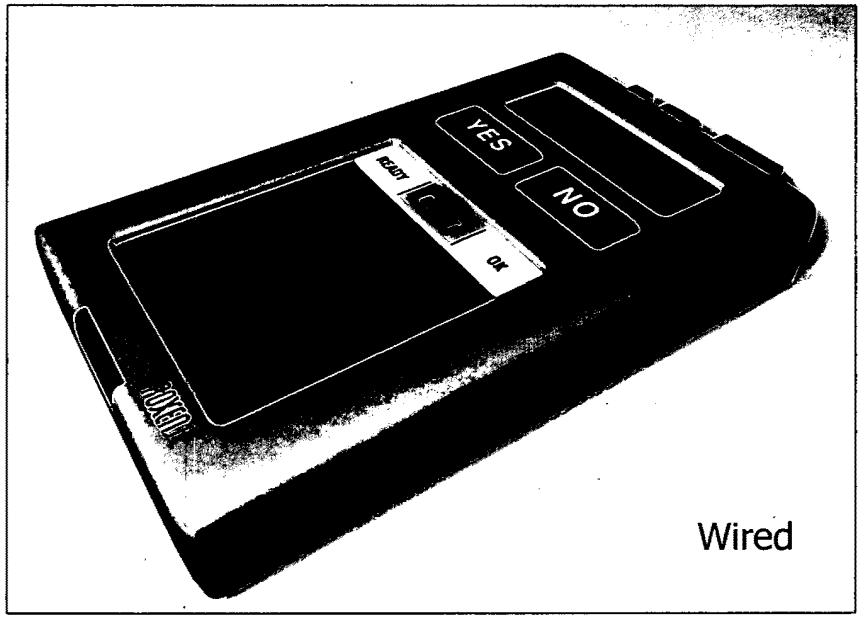
The Components ...

TouchTerminals (wired & wireless versions)

Complete credit card terminal replacements.



Wireless



Wired

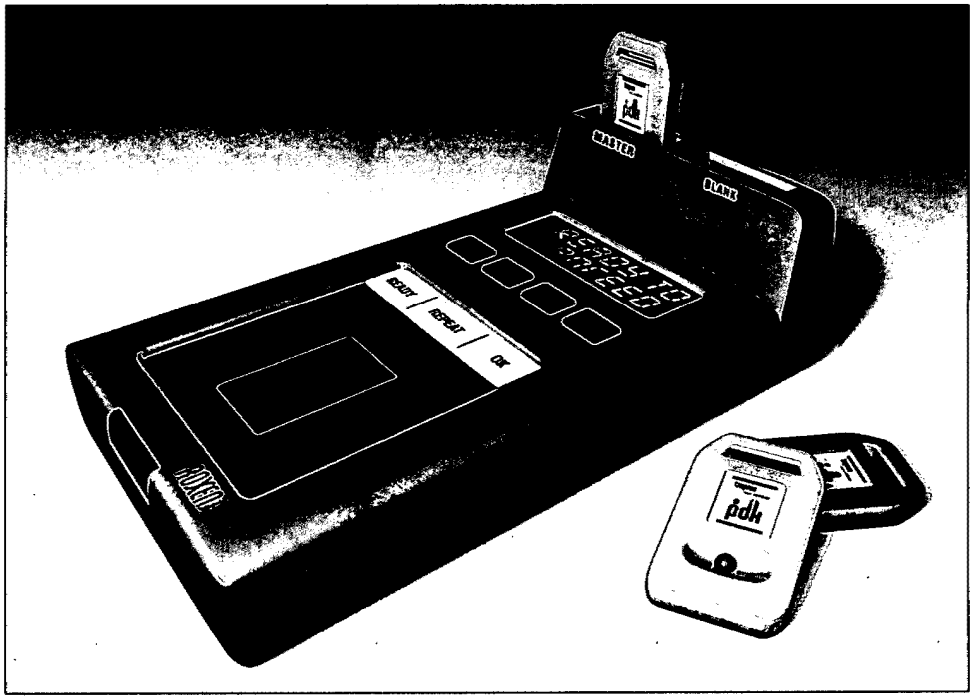
PROXIMITY
PROXENSE
TECHNOLOGIES

truprox™ TOUCH TECHNOLOGY

The Components ...

TouchProgrammer

Specialized devices utilized by Authorized TruProx™ Notaries (ATNs) to initialize & register PDKs.



PROXIMITY PROXENSE TECHNOLOGIES

The Components ...

Central Registry access

A centrally-run software system (accessible from any authorized Touch device) providing various remote authorization services.

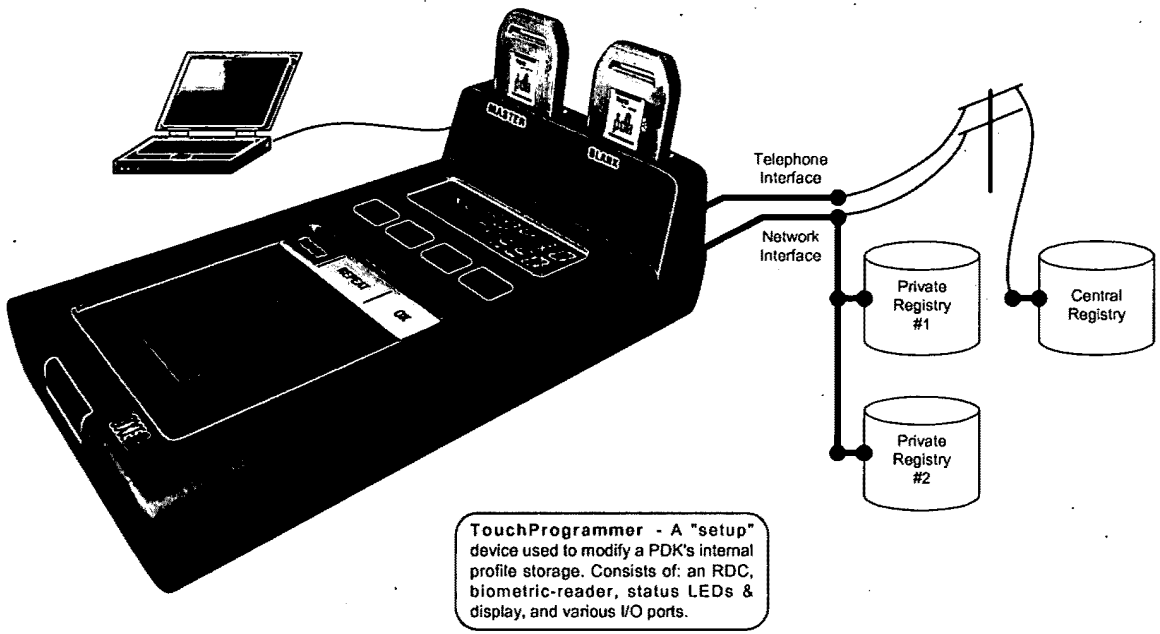
Private Registry package

A server-based software application providing services similar to that of the Central Registry, but for local/private concerns.

truprox™ TOUCH TECHNOLOGY

ATNs / PDK Initialization & Registration

step-by-step



PDK Conceptual User-Bio Profile Data Format

Registry Code	(initializing) ATN ID	(registering) ATN ID	Programmer ID	User Bio-Data (including up to 10 fingerprint hashes)

00 - No Reg | 01 - Private Reg | 10 - Central Reg | 11 - Multi-Reg

PROXIMITY PROXENSE TECHNOLOGIES

The ATN Role & Designation Process

- To become an ATN, an individual completes a detailed application (possibly including biometric data, and indicating their willingness to assume certain legal obligations), and submits it to the ATN approval committee (members to be determined). When/if approval is granted, the individual is provided a PDK if needed, and their application data & unique PDK ID are permanently added to the Central Registry (and updated as needed to indicate changes in status, violations incurred, etc.).
- If an ATN does not have access to a TouchProgrammer ("Programmer"), he/she is provided one. Each programmer's unique ID is recorded in the Central Registry at issuance.
- Any ATN in good-standing may conduct user (biometric) initializations. For audit purposes, the unique IDs of the ATN, the ATN's PDK, and the TouchProgrammer utilized in the process, are permanently stored in the memory of an initialized PDK.
- To register an initialized PDK (registering non-initialized PDKs is allowed, but such PDKs are unable to satisfy biometric authentications) an ATN designated as an active administrator for the intended registry, is required. ATNs are designated as follows:
  - For a private registry, the owner of the registry may designate (or withdraw) ATN(s) of their choosing.
  - For the Central Registry, only Proxense (or a selected third-party, such as the ATN approval committee) may designate ATNs (who must successfully complete stringent approval processes).

(Biometrically) Initializing PDKs

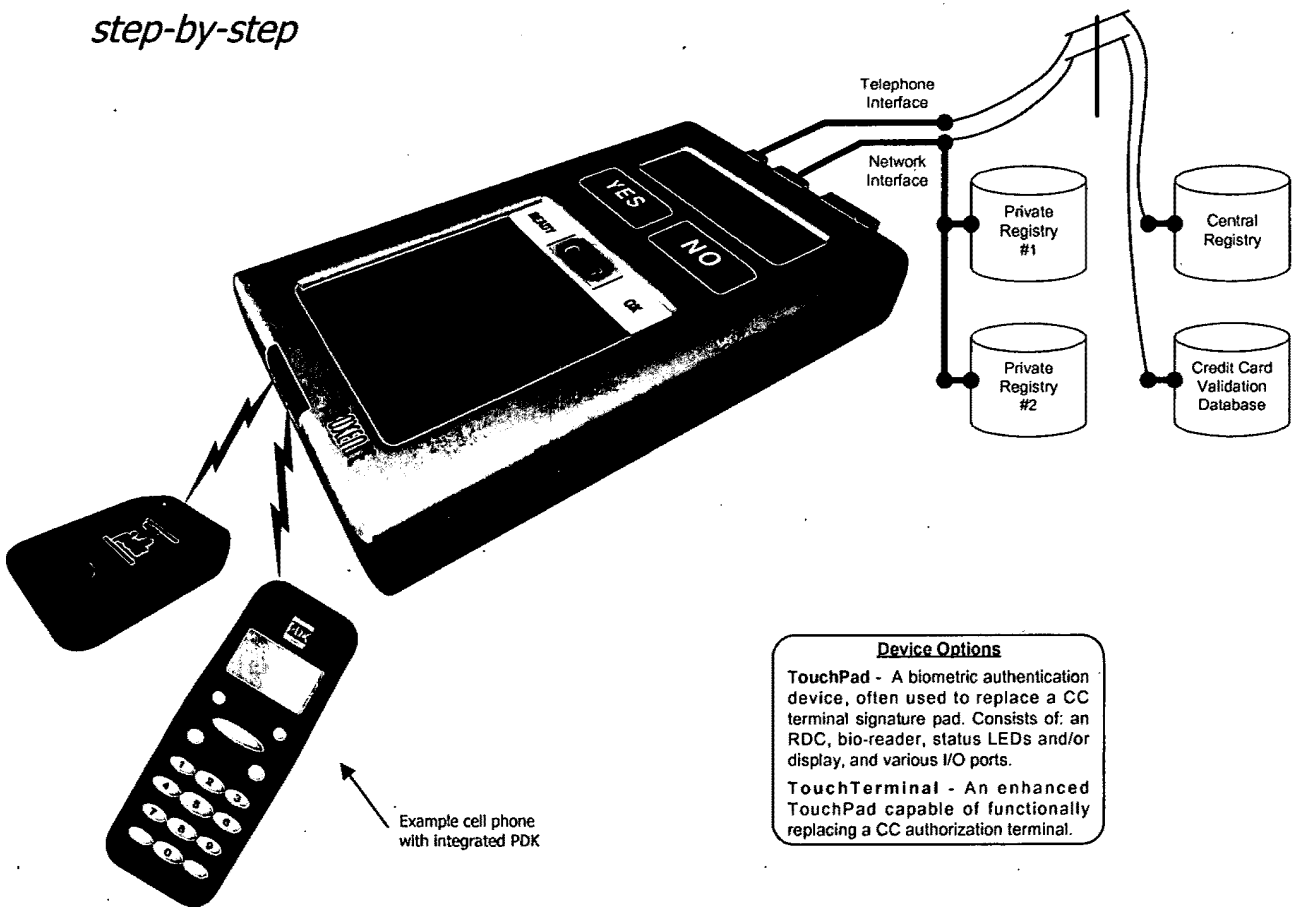
- Before a new user's PDK can be initialized (have its owner's biometric data permanently stored in it), the TouchProgrammer's ID, and the ATN's PDK ID must be validated against the Central Registry as active & in good-standing. If all validate, and the ATN has properly conducted the initialization process (see below), the new user's PDK is permanently programmed with their new personal bio-profile data. Once written, this data is "physically" unable to be over-written, modified, or deleted, but can be re-validated by an ATN if needed. The PDK is now (biometrically) initialized. Following this process, a PDK is typically registered (added to a registry). This is not mandatory though, as ATNs can re-validate (then register) a PDK at any time.
- The initialization process:
  - A new user's PDK <u>and</u> an ATN's PDK are inserted into the TouchProgrammer.
  - The ATN completes a standard biometric authentication to validate their (personal) presence.
  - The ATN's PDK ID and TouchProgrammer's ID are authenticated against the Central Registry. Assuming both validate, the Programmer becomes temporarily enabled (though times-out if not utilized within a certain period of time).
  - The ATN then instructs the user to scan their fingerprints into the TouchProgrammer. The Programmer allows the user to perform each scan as many times as needed to ensure valid data has been captured.
  - When all prints are input & validated, the ATN instructs the Programmer to permanently write the new bio-profile data to the user's PDK. Once completed, this procedure can never be redone, though the profile can be re-validated.
  - When either PDK is removed from the TouchProgrammer, the Programmer's memory is automatically erased.

Registering PDKs

- To add a PDK to a registry, or "register" it, two basic validations must be successfully completed (regardless of the registry type - private or Central). The first is to confirm the PDK being registered is properly initialized. The second is to confirm the user's personal identification is correct. This generally consists of the ATN manually authenticating a pre-defined quantity of approved personal identifiers (e.g. driver's license, passport, social security card, credit card, etc.) provided by the user. If the validations are successfully completed, the ATN enters the following into a database record permanently added to the registry:
  - The initializing ATN's personal PDK ID
  - The registering ATN's personal PDK ID
  - The user's PDK ID
  - The TouchProgrammer's ID
  - The site ID
  - The registration date & time
  - Certain user data items (typically publicly-available items such as an address, phone number, etc.)
  - Optional data items such as an auto-expiration date/time-period
- Finally, the appropriate biometric profile in the user's PDK is updated to indicate the current Registry Code, as well as various other identifiers enabling future audits (see "PDK Conceptual User-Bio Profile Data Format" on previous page).

truprox™ TOUCH TECHNOLOGY

Authentication
step-by-step



Device Options

TouchPad - A biometric authentication device, often used to replace a CC terminal signature pad. Consists of: an RDC, bio-reader, status LEDs and/or display, and various I/O ports.

TouchTerminal - An enhanced TouchPad capable of functionally replacing a CC authorization terminal.

Touch Technology Authentication Process

Level 1 - Local PDK Authentication:

1. When a PDK comes into proximity of a Touch Reader, the Reader requests the PDK to conduct a Local PDK Authentication, and check-in ("register") with it. This process consists of:
   a. Completing a standard TruProx™ PDK-to-RDC authentication (ensuring the type & validity of the devices) and establishing a secure communications channel.
   b. The PDK transmitting its unique secret ID & encrypted bio-profiles to the RDC (the RDC automatically selects the appropriate bio-profile to use).
   c. The RDC temporarily buffering the received data, and notifying the PDK it is communicating with a Touch device (versus a simple RDC).

   NOTE: *The RDC maintains metrics for each "registered" PDK, including: signal strength, clarity of signal, and time in vicinity. To minimize the number of PDKs "registered" at any given time, a Touch Reader typically maintains a small diameter (approx 3-4') proximity zone.*

Level 2 - Local Biometric Authentication:

2. When the Touch Reader detects biometric contact (e.g. from a user's finger), Local Biometric Authentication begins. This consists of it performing a biometric scan, and comparing/testing the resulting data against all buffered PDK biometric profiles (prioritized by accumulated metrics) until a match is found. *Optional implementations may specify the compare/test processing be performed by the PDK, or distributed between the devices.*

   NOTE: *If instead a PDK BioKey was utilized (versus a standard PDK) in the transaction, whichever device detected the biometric data (the BioKey or TouchPad) would initiate the step, allowing the processing of the data to take place as always (as defined by the specific implementation).*

3. Assuming a match is found (completing Local Authentication), the RDC determines which additional authentication levels to perform (none, Private Registry and/or Central Registry). If none (only Local was specified), the authentication process is complete (skipping Levels 3 & 4). Otherwise, the RDC looks at the PDK's buffered biometric profile Registry Code field to determine if further validation against desired registry(s) *can* be performed. Assuming *yes*, Levels 3 and/or 4 are performed next.

   NOTE: *The choice as to which level(s) of authentication to perform is determined by the Touch Reader's setup parameters, or software commands received via the device's I/O ports. It is acceptable to specify multiple private registries and/or the Central Registry for validation.*

Level 3 & 4 - Private/Central Registry Authentication:

4. To conduct Registry Authentication, the RDC establishes a secure channel (typically via a network connection) with the appropriate registry, and transmits a packet typically including the following: PDK ID, ATN IDs, TouchProgrammer ID, site ID, and time-stamps.

5. The registry's controlling software compares the received data against the registry's database to determine the PDK's status (Valid, Inactive, Expired, Lost, Stolen, etc.), while recording a complete audit record. If needed, the process is repeated for any additional registries until finished. Assuming successful validation(s), the audit record is completed, and a "Valid" status is returned to the RDC.

Transaction Validation:

Assuming all levels of authentication are satisfactorily completed, the RDC notifies the Touch Reader the PDK is "Valid", approving the underlying transaction for processing. Depending on the type of Touch Reader in use, one of the following occurs:

TouchPad - The RDC notifies (via its I/O ports) the controlling device that approval has been granted (and typically forwards an account number or similar).

TouchTerminal - The RDC conducts a standard remote credit card ("CC") authorization/transaction.

NOTE: *TouchPads can be viewed as signature-replacement devices, and TouchTerminals (which include CC terminal hardware), as CC terminal replacements.*

PROXIMITY PROXENSE TECHNOLOGIES

PROXIMITY
PROXENSE
TECHNOLOGIES

truprox™ TOUCH TECHNOLOGY

Doc#1620241

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☑ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.