



Adaptable Secure Online Identification

- **Secure against man-in-the-middle attack (cryptographically robust)**
- **Personal token optional (works without it)**
- **Written PIN optional (works without it)**
- **Memorized PIN optional (works without it)**
- **Two or more simultaneous identification (if necessary)**
- **Risk-free distress signal (to handle forced online registration)**
- **Unburdensome login procedure (graphic, entertaining)**

The Internet forces us to identify ourselves through a string of bits, and nothing more. The temptation for hackers is just too great: if they pick someone's bit sequence they can steal that person's identity. Unfortunately, those egg-head academics that started this revolution called Internet for their own email needs put together an



A new PIN can arrive in the mail. No expensive hardware. PINpen can be used via a generic token or via your cell-phone

**Token-Free Implementation
Use Your Cellphone Only!**



incredibly flexible protocol IP/TCP, but one that is totally devoid of security consideration. Ever since, hackers were one step ahead of security

because the Internet is conducive to man-in-the-middle: a scheme in which a hacker positions himself between two conversing parties (say the bank and its customer), sends to each party the messages of the other, so that each thinks that he talks to the other, while in fact they both talk (and expose themselves) to the hacker: passwords, PINs, account numbers, etc.

The first generation of security solutions that offered an answer to the man-in-the-middle scheme is the now familiar time-dependent tokens: expensive, limiting devices that display a six digits number that changes every sixty second (e.g. RSA. VASCO). These tokens may be lost, may break, and are unfriendly to apply, but they provide security against man-in-the-middle attack.

The time has arrived for the new generation of solutions to make an entry, of which PINpen™ is



Serves all your remote identification needs!

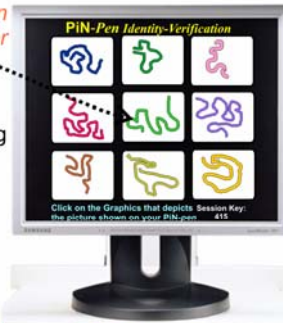
the most prominent. PINpen™ is PIN based (password like) but that PIN is never ever typed into the conversation. So the watchful hacker has no PIN to steal. Instead the two parties (say the bank and its customer) engage in a brief dialogue that proves to each of them that they talk to the other because that conversation could only have been conducted by someone who does have that PIN in his possession. With PINpen™ that conversation is even entertaining, it is based on a graphic selection.

Random PINs are easy to generate, they are

**Mutual Proof-Verification
bank-customer**



Online User proves his identity by clicking on the graphics that matches the display on his key-chain device. That display changes for every log-on session.



**PiN-pen™
Phishing Buster™**

Based on a personal PIN that is never ever typed in to a networked computer.

comfortably distributed, instantly replaced, and with PINpen™ they are readily concatenated.

Concatenation means that PINs or say sequences of digits can be added one behind the other to create a larger PIN. This concatenation offers remarkable implementation flexibility:

“Something you have, something you know”: This maxim has been enshrined in the hallways of security. The PINpen™ PIN can be electronically etched on a card (smart card or regular magnetic card), and it can be committed to memory. One PINpen™ implementation might use either mode, or combine them.

Suppose a traveler uses his PINpen™ card, taps in the memorized digits and thus gets online. The next day that traveler discovers that he lost his PINpen™ card. He would then log in using just his memorized pin, and notify the bank of the loss of the card. Without the card, the privileges of the customer are severely curtailed, per bank's policy, say only account visibility no money movement. And when later on the thief tries to log on with the stolen card, the bank is ready for him.

The Two Man-in-the-Middle Resistant Solutions



Vasco requires the user to copy a long random sequence



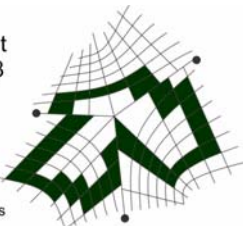
PINpen shows a picture for the user to recognize on his screen

The frustrated thief may become aggressive and force his victim to log in under some threat. The PINpen™ user is thus coerced to use his memorized portion of the PIN. But the victim fights back. When the bank equipped him with the PIN it also gave him a distress sequence that looks like the normal pin. The victim may apply the distress PIN without betraying that fact to the coerced. The bank would know that the customer is under duress, and it then activates a standard policy involving false assurance to the criminal that the



US Patent
6,823,068

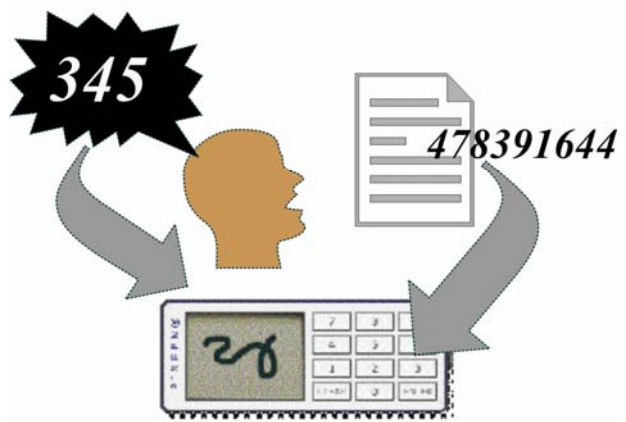
Data conversion patent is used to generate unique graphics from any size PIN. The PIN can not be reverse engineered from the graphics



bank executes his orders, while summoning the police to the scene.

Imagine an industrial situation where some action needs to be witnessed by two individuals; to report online they both may need to be present. PINpen™ then can be used in a way that both individuals will use their PINs without divulging them one to the other.

PINpen may be implemented via a simple memorized PIN, via a written down PIN, or via a built-in PIN -- or any combination thereto.



This flexibility offers both security and convenience

Parental control: do you want to keep tabs on your child's online activity? Let him or her bring to you the PINpen™ token for you to secretly type in your memorized pin, so that it generates a picture (different one each time) that your child would use to log in. The PINpen™ pin may be valid, for, say, a week, and must be mailed to you every Friday along with a list of your son's visited websites.

PINpen™ is phishing resistant, man-in-the-middle immunized; it is operationally flexible, allowing for a myriad of implementation protocols, it offers help in distress, and it is fun to use.

PINpen™ is being developed by
AGS Encryptions Ltd.

Amnon Samid, CEO.
+972 544 200 400
amnon@agsencryptions.com