ICAP PATENT BROKERAGE

Mobile One-Time Password (OTP) – Authentication Token

Prism Technologies, LLC

Initial Bidding Guidance: Mid 6 Figures

The present invention provides a design for a remote authentication token using a smart card or a subscriber identity module (SIM card) in cell phones that an organization would issue to its customer, along with an interface device to display the one-time password. In a preferred implementation, the invention is used in combination with a remote authentication server for validation of the password. Many financial services are now issuing "smart" credit or debit cards which have already been personalized and securely delivered to the customer. Likewise, financial services companies and eCommerce companies are using the SIM cards in cell phones to secure online transactions with one-time passwords. These same organizations are offering online services that need effective user authentication to protect access to customer data as required by legislation. Consequently, for authentication purposes, use of a smart card that has already been delivered to the customer is cost-effective and will help to reinforce both the organization's brand and its commitment to security.

The technology is based on IETF Standards and is applicable to OATH (Open Authentication) Standards.

Forward Citing Companies: Netflix, Direct TV, Honeywell

Priority Date: 05-05-2002

Representative Claim: US 7,865,738 – Claim #1

A system for generating secure passwords for use by at least one authentication server in authenticating a user of an authentication token and an authentication token interface device, in response to the user seeking access to protected computer resources of at least one server, comprising: said authentication token interface device operable to interact with said authentication token to generate said secure passwords in response to input of a unique consumer code by the user into said authentication token interface device and upon authenticating of said unique consumer code by said authentication token; said authentication token interface device having; a processor, firmware, a user interface, an I/O interface compatible with said authentication token, and a dynamic variable generator; said authentication token having; a processor, firmware, an operating system, a data store, an I/O interface compatible with said authentication token interface device, a key generation algorithm, and a password application; said authentication token storing at least; (i) a secret key, (ii) a changing register value, (iii) a seed value and (iv) said unique consumer code; said password application generating said secure passwords by; (i) combining said changing register value with a dynamic variable generated by said dynamic variable generator to produce a payload, (ii) encrypting said payload with said secret key to produce an encrypted payload and, (iii) combining least significant bits of said encrypted payload with least significant bits of said dynamic variable to produce a new secure password; and said key generation algorithm: (i) generating a new secret key and a new seed value following the generation of a first of said secure passwords and of said new secure password, said new secret key being derived from said secret key, said changing register value, and said seed value, and said new seed value being derived from

TECHNOLOGY
PASSWORD AUTHENTICATION - TOKEN

NOVELTY
SYSTEM FOR PROVIDING A REMOTE AUTHENTICATION VIA A SMARTCARD ENABLED INTERFACE DEVICE

IMPORTANCE
STRATEGIC PORTFOLIO FOR FINANCIAL SERVICE PROVIDERS, ECOMMERCE PROVIDERS, AND ONLINE SECURITY VENDORS

NUMBER OF ASSETS
16

PATENTS (11)
US 7,865,738
US 8,375,212
US 8,688,990
CH 1504424
DE 60323483
DK 1504424
EP 1504424
FR 1504424
GB 1504424
IE 1504424
SE 1504424

APPLICATIONS (5)
US 14/229,045
AT 20030722850
AU 20030230010
GB 20020010692
PCT/GB03/02028

said secret key, said changing register value, and said seed value, (ii) replacing said secret key and said seed value with said new secret key and said new seed value in storage of said authentication token, and (iii) changing said changing register value by a change value to result in a new changing register value after generation of said new secret key and said new seed value; wherein, after generation of said first of said secure passwords and of said new secure password, said dynamic variable is changed to a new dynamic variable by said dynamic variable generator.

Contact:
For more information on the assets available for sale in this portfolio, contact Paul Greco.

Paul Greco
Senior Vice President
Paul@icapip.com
(212) 815-6692