PATROLL Winning Submission

U.S. Patent 7,669,236

U.S. Patent 7,669,236 ("*Biogy*" or the "patent-at-issue") was filed on April 6, 2005 and claims an earliest priority of December 20, 2004. Claim 1 of the patent-at-issue is generally directed to an electronic security method that involves a registration process wherein, after completion, a machine receives a temporary user-generated passcode. Subsequently, upon receiving this passcode, an automated administrator on the machine generates a temporary administrator-generated passcode. This is achieved by encrypting a current passcode generator derived from retrieving a prior passcode generator from storage, perturbing it based on a prior access attempt, and saving the results as the current passcode generator associated with the user. The method then determines the permissibility of a current access attempt by checking if the user-generated passcode matches the administrator-generated passcode, granting access if the two codes align.

A primary reference, U.S. Patent App. 2003/0172272 ("*Ehlers*"), was filed on May 23, 2001, and claims a priority date on May 24, 2000. The patent application is directed to an authentication system designed for verifying the identity of a user seeking access to a secure service facility. This system employs three distinct communication channels: a network channel facilitating communication between the user and the facility, a channel for communication between the facility and an authentication server and a channel facilitating communication between an authentication server and the user. The process involves the user sending user information to the secure facility. The facility then generates a confirmation request for the user's identity, sent to the authentication server. Subsequently, the authentication server generates a passcode, and transmits the passcode to both the user's device and the facility. Upon receiving the passcode, the user provides it to the secure facility, which compares it with the passcode received from the authentication server. Access to the desired service or facility is granted if the two codes match.

A primary reference, U.S. Patent 7,613,919 ("*Bagley*"), was filed on October 12, 2004 and claims priority on the same date. The patent pertains to systems, computer program products, and methods for authentication using a one-time password. In a system consisting of a client, a service provider, and an authentication service, the authentication service generates an authentication service identifier for the client, typically in the form of an arbitrary number of characters. The client provides a client moniker (e.g., a username) to the authentication service. Subsequently, the authentication service sends a one-time password to the client for accessing the service provider. Upon receiving a one-time password from the service provider, the authentication service sends the authentication service identifier for the client to the service provider for client authentication if the received one-time password matches the one sent to the client.

A secondary reference, the PCT application published as Publication WO2003093923 ("*Eryou*"), was filed on April 30, 2003, claims a priority date of April 30, 2002 and is published on November 13, 2003. The patent application is directed to a mobile biometric device or biotoken, and a server enabling biometric validation. A person initiates the biotoken and communicates

generated codes to a server via a secure or unsecured channel. The biotoken captures biometric information, hashes part of the information, and generates a code using a clock value, random number, secure hash function, and a counter. The server initializes the biometric device, stores key values upon initialization, and validates codes during future use following a validation request. Additional features include creating a secure, auditable, and private application space on a device like a computer or cell phone.

A secondary reference, U.S. Patent App. 2005/0273866 ("*Brown*"), was filed August 8, 2005, and claims a priority date on July 6, 1998. The patent is directed to a rule-based biometric user authentication method and system within a computer network environment. Multiple authentication rules coexist in the network, including a default system-wide rule and rules linked to specific users, remote computers, user groups, or system resources. An established order of precedence among these rules is utilized to authenticate the user, allowing for flexible and context-specific authentication processes based on various factors such as user identity, remote location, group affiliations, and resource access requirements.

A secondary reference, U.S. Patent 7,725,926 ("*Karp*"), was filed on August 23, 2004, and claims priority on the same date. The patent is directed to a method for authentication in a client computer and a remote computer. The process involves obtaining a client base value chosen by the user for a first usage purpose and a client integer chosen by the user for a second usage purpose. These values are then combined to create a client combination, which is further hashed to generate a client password. This approach enhances security by incorporating user-selected values into the authentication process, providing a personalized and adaptable method for authenticating users between a client computer and a remote computer.

A sample claim chart comparing claim 1 of *Biogy* to *Ehlers, Bagley, Eryou, Brown,* and *Karp* is provided below.

US7669236 (“*Biogy* ”)	**A. US20030172272** (*“Ehlers”*) **B. US7613919** (*“Bagley”*) **C. WO2003093923** (*“Eryou”*) **D. US20050273866** (*“Brown”*) **E. US7725926** (*“Karp”*)
1. A method comprising: **after a registration process is complete**, **receiving at a machine a request for access from a user**, the **request including a user-generated passcode** that is **valid temporarily**, and that is **generated by applying at least one function at least one time to information associated with the user**;	**A. US20030172272** “The process commences with **the user** 12 **requesting access from his or her computer** 18**, via the IP network** 20**, to the desired service** 16 that in turn is a subscriber to the authentication system of the invention, by sending his or her username or number to the IP server 14 via the IP network 20. The user may optionally add additional information, such as account details and amounts during a commercial transaction, for example, as part of the request for access to services. This step is shown in general by 30. The IP server 14 then **generates a request for confirmation of the user's identity, which it then sends to the authentication server**, as indicated by 32. The request includes the username and server name or address as well as any extra information the user may have offered.” *Ehlers* at par. 0049 1. An authentication system for **authenticating the identity of a user wishing to access a facility, the system comprising** . . . **passcode generating means for generating a passcode**, the passcode generating means being controlled by the control means . . . *Ehlers* at Claim 1 “In one form of the invention, the passcode is a random number. Alternatively, **the passcode is a cryptographic digest of a message sent by the user to the facility**, the system thereby also allowing authentication of the message sent by the user.” *Ehlers* at par. 0022 “The same passcode, session number, as well as a confidence level are sent to the IP server 14, as shown by 38. However, **a different passcode is used for every new access attempt, with the passcode only being valid for a limited period of time**.” *Ehlers* at par. 0051 “. . . **prompting the user to provide the facility with user identification information** . . .” *Ehlers* at par. 0027

(cont.) 1. A method comprising: **after a registration process is complete**, **receiving at a machine a request for access from a user**, the **request including a user-generated passcode** that is **valid temporarily**, and that is **generated by applying at least one function at least one time to information associated with the user**;	2. An authentication system according to claim 1 wherein the control means, **the database that includes user identification information** and the **passcode generating means are situated at a centralized authentication server**." *Ehlers* at Claim 2 "The **authentication server** 22 **then generates a random number or computes a cryptographic digest, based on the information offered by the user, with either the random number or the cryptographic digest being referred to as a passcode, as well as a session number**." *Ehlers* at par. 0050 **B. US7613919** "In general, a **client requests or accesses, and a service responds or provides**. A client in one operation therefore, may be or act as a service in another operation, and vice-versa." *Bagley* at col. 7:45-48 "As described in more detail below, **authentication service** 120 **provides one-time passwords for client** 110 **to use when authenticating to service provider** 130. **Authentication service** 120 **also confirms that a one-time password received from service provider** 130 **corresponds to client** 110." *Bagley* at col. 7:51-55 "The **client accesses** (212) **the authentication service in order to obtain a one-time password**. **The authentication service requests (214) a client moniker or proxy password from the client. The client moniker identifies the client to the authentication service and is analogous to a username**. In response, the client sends (216) the client moniker to the authentication service." *Bagley* at col. 8:3-11 "For **a valid one-time password, the authentication service sends** (258) the authentication service identifier for the client to the service provider and discards (262) the one-time password so that it is no longer valid. **One-time passwords also may have expirations to limit the amount of time they are valid**. As a result, **one-time passwords may be valid for relatively short periods of time or relatively long periods of time**, depending on the needs and preferences of a particular implementation." *Bagley* at col. 9:19-27 **C. WO2003093923** "The CAS-LDAP-Proxy 310 is preferably an LDAP/S protocol compliant proxy that is **a front-end listener and communicates with clients that communicate using LDAP**

(cont.) 1. A method comprising: **after a registration process is complete**, **receiving at a machine a request for access from a user**, the **request including a user-generated passcode** that is **valid temporarily**, and that is **generated by applying at least one function at least one time to information associated with the user**;	**protocols**. For example, **this proxy would be responsible for accepting requests from the CAS Server** 205. The CAS-LDAP Proxy 305 and CAS-Engine 310 are preferably running on a single physical machine. **This proxy** 310 **does not need to implement relaying of requests to 3rd party LDAP Servers will preferably only service requests that are meant for CAS-Engine** 310." *Eryou* at p.10 "**The processor 120 is used to generate the code based on an initialization and verification process and may also be used to apply secondary authentication means**, such as a PKI certificate." *Eryou* at p.8 "GenerateKey() - This function could be called from EncryptPassword and DecryptPassword function. This function preferably gets the username or userid from the calling function and **generates a symmetric key based on the userid or username**. The symmetric key is returned to the calling function." *Eryou* at p. 14 **D. US20050273866** 1. **A method of controlling access to a computer resource in a computer environment, comprising:** **receiving a user identification of a user** . . . *Brown* at Claim 1 "**The keys may be typed in by the user**, or automatically generated by, for example, the swipe of an employee ID card through a card reader. **Based on a set of enterprise security policies SAFsite then challenges the user for the appropriate biometric credentials, such as finger-image, voice print, or facial image**. **The user's biometric is captured, individual characteristics are extracted from the biometric, and a digital representation of the characteristics are sent to the SAF Server 220 for authentication**." *Brown* at par. 0045 8. A method of controlling access to a computer resource in a computer environment, **comprising:** **using a first order of precedence as between at least first and second authentication rules for a first set of conditions pertaining to a user desiring access the resource** . . . *Brown* at Claim 8 "Authenticate( )—The authenticate function **provides a single function call verifying a users identity**. **The server**

(cont.) 1. A method comprising: **after a registration process is complete**, **receiving at a machine a request for access from a user**, the **request including a user-generated passcode** that is **valid temporarily**, and that is **generated by applying at least one function at least one time to information associated with the user**;	**performs authentication based upon the stored rule**." *Brown* at par. 0063 **E. US7725926** "In an illustrative example, a remote computer 160 functioning as a web site server may establish a requirement for the **user** 110 **to go through a registration procedure**, in order to obtain access to password-protected areas of the web site." *Karp* at col. 5:45-49 "In FIG. 3, the disposition of a **request** 310 **by the user** 110 **for the desired access to a resource** is illustrated according to an embodiment of the invention. An exemplary resource is the remote computer 160. The **request** 310 **includes the client password** 270 and the client integer 230. The request 310 is submitted by the user 110 to the remote computer 160." *Karp* at col. 5:33-38 "The **user** 110 **selects a client base value** 210 for at least a first usage purpose 220, **and a client integer** 230 for at least a second usage purpose 240." *Karp* at col. 3:29-31 "The **client base value is combined with the client integer to obtain a client combination. The client combination is hashed to obtain a client password**." *Karp* at col. 2:8-10
in response to the receiving the user-generated passcode, **generating, via the machine, which runs an automated administrator, an administrator-generated passcode that is valid temporarily**	**A. US20030172272** "The **authentication server** 22 then **generates a random number or computes a cryptographic digest**, based on the information offered by the user, with either the random number or the cryptographic digest being referred to as a passcode, as well as a session number." *Ehlers* at par. 0050 "**The same passcode, session number, as well as a confidence level are sent to the IP server 14, as shown by 38. However, a different passcode is used for every new access attempt, with the passcode only being valid for a limited period of time**." *Ehlers* at par. 0051 **B. US7613919** "For **a valid one-time password, the authentication service sends** (258) the authentication service identifier for the client to the service provider and discards (262) the one-time password so that it is no longer valid. **One-time passwords also may have expirations to limit the amount of time they are valid**. As a result, **one-time passwords may be valid for**

(cont.) in response to the receiving the user-generated passcode, **generating, via the machine, which runs an automated administrator, an administrator-generated passcode that is valid temporarily**	**relatively short periods of time or relatively long periods of time**, depending on the needs and preferences of a particular implementation." *Bagley* at col. 9:19-27 **C. WO2003093923** "**Set Auto Admin**() - This function could be called from within WlxWkstaLockedSAS and WlxLoggedOutSAS. **The main purpose is to make an entry in the registry thereby informing the windows that a logon box has been displayed to the user and there is no need for the windows to display its traditional logon box to the user**." *Eryou* at p. 13 **D. US20050273866** "The extended **User Manager** 240 and **Server Manager** 260 can communicate with the SAF Server 220 using NT RPC. **All data is encrypted**." *Brown* at par. 0030 "Extensions to WINDOWS NT's standard **User Manager and Server Manager provide enrollment and maintenance functions used by a systems administrator to register userIDs, passwords, BIRs, and workstation information into the SAF Server's database**." *Brown* at par. 0030 **E. US7725926** "However, if the client integer 230 is larger than the stored integer 330, the **remote computer** 160 **combines the stored base value** 320 **with the client integer** 230 **to obtain a remote combination** 340. The stored base value 320 and client integer 230 may be combined by the remote computer 160 in the same way that the client computer 120 combines the client base value 210 with the client integer 230 to obtain the client combination 250. The **remote computer** 160 **then hashes the remote combination** 340, such as by passing the remote combination 340 through the hash function 260. The **resulting hash value is the remote password** 350." *Karp* at col. 6:25-36

wherein **the administrator-generated passcode is generated by the automated administrator encrypting a current passcode generator derived by the automated administrator retrieving a prior passcode generator from a storage area of a storage unit and**, in response to a prior attempted access being permitted,	**A. US20030172272** "**The same passcode, session number, as well as a confidence level are sent to the IP server 14, as shown by 38. However, a different passcode is used for every new access attempt, with the passcode only being valid for a limited period of time**." *Ehlers* at par. 0051 **C. WO2003093923** "**EncryptPasswordO** - This function could be used to **encrypt the password before storing in the registry. The function used to store the value is called from PutPrevNamePassword**." *Eryou* at p. 13 **D. US20050273866** 2. The method of claim 1, further **comprising receiving the password**. *Brown*, Claim 2 3. The method of claim 2, **further comprising comparing the received password to a stored password associated with the user identification**. *Brown*, Claim 3 "In the exemplary embodiment, **communications between client workstations and the SAF Server 220 is via Remote Procedure Calls (RPC) and is encrypted**. A **different encryption key is used for each session between a client and the server. If a strong encryption version of the WINDOWS NT operating system is used, 128-bit keys are generated**." *Brown* at par. 0027 "If the verification server 222 verifies that the user is authorized to log on, **the server will retrieve the user's password from the database 221 and send the user's password back to the workstation where the log-on will be completed**, at step 319, via the GINA DLL 255. The completion of the log-on procedure is transparent to the user." *Brown* at par. 0035 **E. US7725926** "However, if the client integer 230 is larger than the stored integer 330, the remote computer 160 combines the stored base value 320 with the client integer 230 to obtain a remote combination 340. The stored base value 320 and client integer 230 may be combined by the remote computer 160 in the same way that the client computer 120 combines the client base value 210 with the client integer 230 to obtain the client combination 250. The **remote computer** 160 **then hashes the**

(cont.) wherein **the administrator-generated passcode is generated by the automated administrator encrypting a current passcode generator derived by the automated administrator retrieving a prior passcode generator from a storage area of a storage unit and**, in response to a prior attempted access being permitted,	**remote combination** 340, such as by passing the remote combination 340 through the hash function 260. The resulting hash value is the remote password 350." *Karp* at col. 6:25-36
applying at least one function at least one time to perturb the prior passcode generator, and saving results of applying of the at least one function as the current passcode generator, the current passcode generator being the prior passcode generator being associated with the user; and	**C. WO2003093923** "EncryptPasswordO - **This function could be used to encrypt the password before storing in the registry. The function used to store the value is called from PutPrevNamePassword**." *Eryou* at p. 13 "**PutPrevNamePassword**() - This function could be called from WlxLoggedOutSAS function. After successful logging in of the user and before exiting from WlxLoggedOutSAS function the PutPrevNamePassword is called. **The usemame and the password is passed to this function and this function calls the write registry functions and makes the corresponding entry in the registry. This function calls encrypt password before writing it on to the registry**." *Eryou* at p. 13 **E. US7725926** "The client integer 230 may, in some embodiments, be updated by the user 110 on a regular, irregular, or periodic basis, or whenever it is determined that too much spam has been delivered to the inbox 520 using that client integer 230. The value of the client integer 230 may be maintained and incremented manually or automatically; for example, by the user 110, by the client computer 120, or by a software application. The **client integer** 230 **may be incremented by one each time it is updated, or may be incremented by a larger number**. If desired, only one client integer 230 need be updated for any number of client base values 210." *Karp* at col. 8:29-40

determining whether a current attempted access is permitted, based on whether the user-generated passcode and the administrator-generated passcode match, and if the user generated passcode matches the administrator generated passcode granting the request for access.	**A. US20030172272** 10. An authentication system according to any one of the preceding claims that includes session number generating means for generating a session number, the session number being sent to both the facility and the user via the second and third communications networks respectively, so as to **allow the facility and the user to match the received passcode with the correct authentication session**." *Ehlers* at Claim 10 "Once the user 12 receives the passcode by his or her mobile communication device 28, he or she offers it, via the IP network 20, as a passcode to gain access to the secure service offered by the IP server 14. This is shown at 40. The passcode, which is typically in the form of a random number or a cryptographic digest, is generated in a cryptographically secure manner, and is used only once for a single, unique login session. The **IP server** 14 **then compares the passcode that was offered by the user via the IP network** 20 **with the passcode that was generated for that particular login session by the authentication server** 22. **If the two codes are the same, it is concluded that the user** 12 **is in possession of the authentication token**, typically the GSM SIM card, **and can therefore positively be identified as the user whom he or she claims to be**. If a cryptographic digest was computed, this digest, when logged, forms a signature, which can be used to confirm the authenticity of the information offered by the user. If, however, the numbers do not match, or if a response is not received within a certain time interval, access is denied." *Ehlers* at par. 0052 13. An authentication method for authenticating the identity of a user wishing to access a facility, the method comprising the steps of: . . . the **facility comparing the passcode received from the user to the passcode received from the control means**; and **allowing access to the facility in the event of there being a match between the two passcodes**. *Ehlers* at Claim 13 **B. US7613919** "After receiving the authentication service identifier for the client, the credit card registration service matches (268) the authentication service identifier for the client against previously received authentication service identifier for the client. **If the received authentication service identifier for the client matches the previously received authentication service identifier for the client, i.e., is valid** (272), **the logon**

(cont.) **determining whether a current attempted access is permitted, based on whether the user-generated passcode and the administrator-generated passcode match, and if the user generated passcode matches the administrator generated passcode granting the request for access.**	**service allows** (276) **access**, such as by associating the new registration information provided by the client, registering the credit card for use, etc." *Bagley* at col. 13:4-13 **C. WO2003093923** "**If a match is successful 1290, then the authentication request** (or other process request) **is validated and is sent for processing, i the case of a certificate request, a key fetch protocol is invoked 1295 which creates a secure channel with the user could be used to transmit a private code, a PKI certificate, a private key, or other sensitive information that can be used by the person requesting validation to perform other tasks**. **This might include transmission of encrypted messages on a public computer, digitally signing documents, or any number of other activities that require authentication of the user prior to processing**. A slowchart illustrating the DCTP is provided in Figures 13 and 14." *Eryou* at p. 29 **D. US20050273866** 3. The method of claim 2, further comprising **comparing the received password to a stored password associated with the user identification**. *Brown* at Claim 3 4. The method of claim 3, further comprising **granting access to the resource if the received password corresponds to the stored password**. *Brown* at Claim 4 5. The method of claim 2, wherein **receiving the password further comprises receiving a password typed in by the user**. *Brown* at Claim 5 **E. US7725926** "If the remote password 350 does not match the client password 270 that was received as part of request 310, the request 310 is rejected, and a status 370 is set to indicate that authorization has been denied. **If the remote password** 350 **matches the client password** 270 that was received as part of request 310, **the request** 310 **is accepted, and a status** 370 **is set to indicate that authorization has been granted.**" *Karp* at col. 6:37-43