CLAIMS

1. A method for assuring that a client device is authorized to receive information from a system, the system and the client device being in bi-directional communication over a network, the method comprising:

reading a network address of said client device on said network;

reading a predetermined piece of information from said client device pertaining to a hardware component incorporated in said client device;

using a cryptographic program to receive said network address and said predetermined piece of information as inputs, and to compute therefrom a registration identification (ID) hash code for said client device;

and wherein said registration ID hash code is not stored on said client device after said registration ID hash code is sent to said system;

using said client device to supply said registration ID hash code to said system when making a call to said system over said network;

using the system to provide the client device with a client-side key that is used by the client to digitally sign said registration ID hash code;

and

causing said system to generate a digital certificate having a component that is used by said system to validate a digital signature of said registration ID hash code that is provided by said client device to said system in future communications

for each subsequent call by said client device to said system, causing said client device to re-obtain said network address and said pre-determined piece of information as said inputs to said registration ID hash code, and to regenerate said registration ID hash code and to re-transmit said registration ID hash code to said system signing said registration ID hash code with said client-side key; and

further comprising using said client device to supply a pre-determined user name together with said registration ID hash code to said system.

2. The method of claim 1, wherein:

generating a digital certificate comprises generating a digital certificate having a system-side key; and

further comprising having said client device digitally sign its registration ID hash code with said client-side key before presenting said registration ID hash code to said system during a future call to said system; and

having said system use its said system-side key to compare to said digitally signed registration ID hash code when receiving a future call from said client device, to authenticate an identity of said client device.

3. The method of claim 1, wherein using a cryptographic program comprises using a cryptographic hash program stored on said client device.

4. The method of claim 1, wherein reading a predetermined piece of information comprises reading a volume serial number identification code of a primary partition of a mass storage device residing in said client device.

5. The method of claim 1, wherein reading said network address comprises reading a MAC address of a network card residing within said client device.

6. The method of claim 1, wherein using said client device to supply said piece of user identifying information comprises using said client device to supply a user name.

7. The method of claim 1, wherein using said client device to supply said piece of user identifying information comprises using said client device to supply a user password.

8. The method of claim 1, wherein using said client device to supply said piece of user identifying information comprises using said client device to supply a previously selected registration name for said client device.

9. The method of claim 8, further comprising using said system, upon receipt of said registration name from said client device, to check if another device using the same registration name as said client device is already in communication with said system.

10. The method of claim 8, further comprising causing said system to prohibit further communication with said system if said registration name is detected to be already in use by a device other than said client device.

11. The method of claim 1, further comprising storing said registration name and said registration ID hash code in a memory of said system.