Claims

1. A method for managing user identity, the method comprising:

establishing a connection secured with Transport Layer Security (TLS) from a client device to an Identity Registration Protocol (IRP) server;

authenticating, at the IRP server, user login via the client device, with Strong Client Authentication (SCA) or Username/Password Authentication (UPA);

upon request from the client device via the secured connection, registering or retrieving at the IRP server user identity information comprising user information, and an Internet Protocol (IP) address of the client device;

upon request from the client device via the secure connection, registering or retrieving at the IRP server one or more digital certificate;

sending as part of a request from the client device to the IRP server a certificate signing request via the secured connection;

upon request from the client device via the secured connection, returning a signed digital certificate from the IRP server to the client device via the secured connection;

sending as part of a request a PKCS#12 package from the client device to the IRP server via the secured connection;

upon request from the client device via the secured connection, returning a PKCS#12 package from the IRP server to the client device via the secured connection;

upon a request for certificate validity status or revocation status of the digital certificate from the client device via the secured connection, determining at the IRP server a user identifier from a user's digital certificate;

determining at the IRP server a domain name of a second IRP server from the user identifier;

performing at the IRP server a Domain Name Server (DNS) SRV look up based on the domain name of the second IRP server;

obtaining from the DNS SRV look up a hostname of the second IRP server at the IRP server;

establishing a connection secured with TLS from the IRP server to the second IRP server;

authenticating at the second IRP server user login via the IRP server;

forwarding from the IRP server the request for certificate validity status or revocation status of the digital certificate to the second IRP server;

sending the certificate validity status or revocation status of the digital certificate from the second IRP server to the IRP server; and

sending the certificate validity status or revocation status of the digital certificate from IRP server to the client device.

2. The method as claimed in claim 1, wherein messages exchanged between the IRP server and the client device via the secured connection are semantically defined in Extensible Markup Language (XML) format.

3. The method as claimed in claim 1 or 2, wherein the method comprises:

sending as part of a request from the client device to the IRP server a request to revoke a digital certificate.

4. The method as claimed in claim 1, 2 or 3, wherein the method comprises:

upon request from the client device via the secured connection, sending validity status or revocation status of a digital certificate from the IRP server to the client device via the secured connection.

5. The method as claimed in any one of the preceding claims, wherein the method comprises:

if the SCA is unsuccessful, enabling UPA at the IRP server upon request to allow authentication of the user login via UPA.

6. The method as claimed in any one of the preceding claims, wherein the method comprises:

disabling UPA at the IRP server for user authentication when a digital certificate for SCA is obtained by the client device from the IRP server.

7. The method as claimed in any one of the preceding claims, wherein the method comprises:

enabling UPA at the IRP server for a predetermined time period; and

disabling the UPA at the IRP server after the predetermined time period.

8. The method as claimed in claim 6 or 7, wherein the method comprises:

encrypting a password used for the UPA when the UPA is disabled; and

decrypting the password used for the UPA when the UPA is enabled.

9. The method as claimed in any one of the preceding claims, wherein the method comprises:

upon a request for user identity information from the client device via the secured connection, determining at the IRP server a user identifier from the requested user identity information;

determining at the IRP server a domain name of a third IRP server from the user identifier;

performing at the IRP server a Domain Name Server (DNS) SRV look up based on the domain name of the third IRP server;

obtaining from the DNS SRV look up a hostname of the third IRP server at the IRP server;

establishing a connection secured with TLS from the IRP server to the third IRP server;

authenticating at the third IRP server user login via the IRP server;

forwarding from the IRP server the request for user identity information to the third IRP server;

sending the user identity information from the third IRP server to the IRP server; and

sending the user identity information from IRP server to the client device.

10. The method as claimed in any one of the preceding claims, wherein the method comprises:

obtaining at the IRP server a list of Certificate hierarchies on a Certification Authority; and

obtaining at the IRP server Certification Authority certificates.

11. An apparatus for managing user identity, the apparatus comprising:

one or more processors configured to execute program codes to control the apparatus to:

establish a connection secured with Transport Layer Security (TLS) from a client device to the apparatus;

authenticate user login via the client device, with Strong Client Authentication (SCA) or Username/Password Authentication (UPA);

upon request from the client device via the secured connection, register or retrieve user identity information comprising user information, and an Internet Protocol (IP) address of the client device;

upon request from the client device via the secure connection, register or retrieve one or more digital certificate;

receive as part of a request from the client device a Certificate Signing Request (CSR) via the secured connection;

upon request from the client device via the secured connection, return a signed digital certificate to the client device via the secured connection;

receive as part of a request a PKCS#12 package from the client device via the secured connection;

upon request from the client device via the secured connection, return a PKCS#12 package to the client device via the secured connection;

upon a request for certificate validity status or revocation status of the digital certificate from the client device via the secured connection, determine at the IRP server a user identifier from a user's digital certificate;

determine at the IRP server a domain name of a second IRP server from the user identifier;

perform at the IRP server a Domain Name Server (DNS) SRV look up based on the domain name of the second IRP server;

obtain from the DNS SRV look up a hostname of the second IRP server at the IRP server;

establish a connection secured with TLS from the IRP server to the second IRP server;

authenticate at the second IRP server user login via the IRP server;

forward from the IRP server the request for certificate validity status or revocation status of the digital certificate to the second IRP server;

send the certificate validity status or revocation status of the digital certificate from the second IRP server to the IRP server; and

send the certificate validity status or revocation status of the digital certificate from IRP server to the client device.

12. A non-transitory computer-readable medium storing a program causing a computer to execute a method for managing user identity, the method comprising:

establishing a connection secured with Transport Layer Security (TLS) from a client device to an Identity Registration Protocol (IRP) server;

authenticating, at the IRP server, user login via the client device, with Strong Client Authentication (SCA) or Username/Password Authentication (UPA);

upon request from the client device via the secured connection, registering or retrieving at the IRP server user identity information comprising user information, and an Internet Protocol (IP) address of the client device;

upon request from the client device via the secure connection, registering or retrieving at the IRP server one or more digital certificate;

sending as part of a request from the client device to the IRP server a Certificate Signing Request (CSR) via the secured connection;

upon request from the client device via the secured connection, returning a signed digital certificate from the IRP server to the client device via the secured connection;

sending as part of a request a PKCS#12 package from the client device to the IRP server via the secured connection;

upon request from the client device via the secured connection, returning a PKCS#12 package from the IRP server to the client device via the secured connection;

upon a request for certificate validity status or revocation status of the digital certificate from the client device via the secured connection, determining at the IRP server a user identifier from a user's digital certificate;

determining at the IRP server a domain name of a second IRP server from the user identifier;

performing at the IRP server a Domain Name Server (DNS) SRV look up based on the domain name of the second IRP server;

obtaining from the DNS SRV look up a hostname of the second IRP server at the IRP server;

establishing a connection secured with TLS from the IRP server to the second IRP server;

authenticating at the second IRP server user login via the IRP server;

forwarding from the IRP server the request for certificate validity status or revocation status of the digital certificate to the second IRP server;

sending the certificate validity status or revocation status of the digital certificate from the second IRP server to the IRP server; and

sending the certificate validity status or revocation status of the digital certificate from IRP server to the client device.