Apparatus And Method For Managing Digital Certificates

Abstract

An apparatus and a method for managing user identity, the method comprising: establishing a connection secured with Transport Layer Security (TLS) from a client device to an 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, 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, registering or retrieving at the IRP server one or more digital certificate; sending from the client device to the IRP server a Certificate Signing Request (CSR) via the secured connection; upon request from the client device, returning a signed digital certificate from the IRP server to the client device; sending a PKCS#12 package from the client device to the IRP server; and upon request from the client device, returning a PKCS#12 package from the IRP server to the client device.

Figure 2