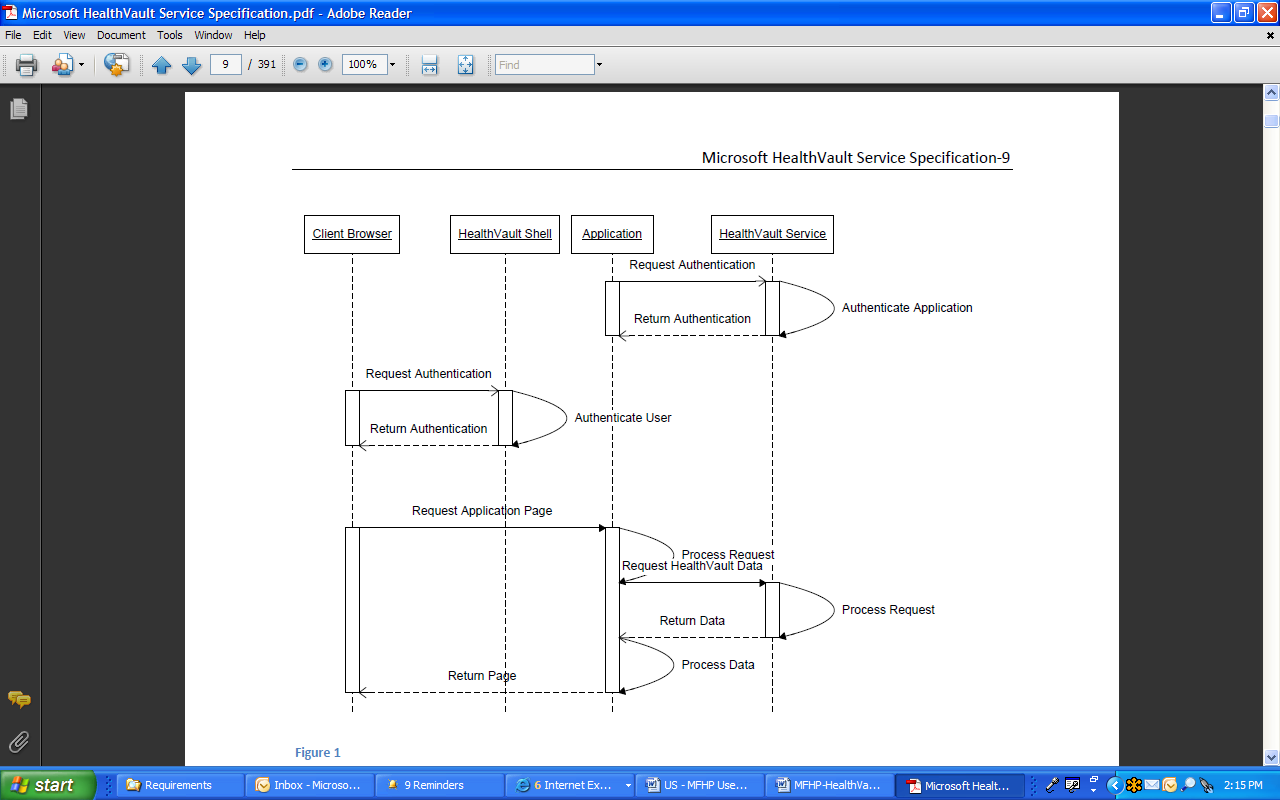
**Summary of My Family Health Portrait(MFHP) - HealthVault Authentication**

My Family Health Portrait (MFHP) will use a 2-point online authentication process to access HealthVault. MFHP first establishes an “application session” with HealthVault Service (Point 1), and then it creates a “user session” (Point 2) by having the MFHP user authenticate with the HealthVault Shell. At each point, valid credentials must be supplied.

The HealthVault Service consists of the HealthVault Platform and the HealthVault Shell. Microsoft defines the HealthVault Service as an online environment that provides consumers with ownership and choice around their own health-related information and activities. The environment enables external applications to add/modify items within individual records, creating a comprehensive suite of functionality. It defines the HealthVault Platform as the web-based API layer that provides health data and infrastructure services upon which all HealthVault applications are built. Microsoft defines the HealthVault Shell as an application that provides a consumer experience for the HealthVault Platform, allowing for an account management and record manipulation. It is also the key middleman for web-based authentication and authorization.

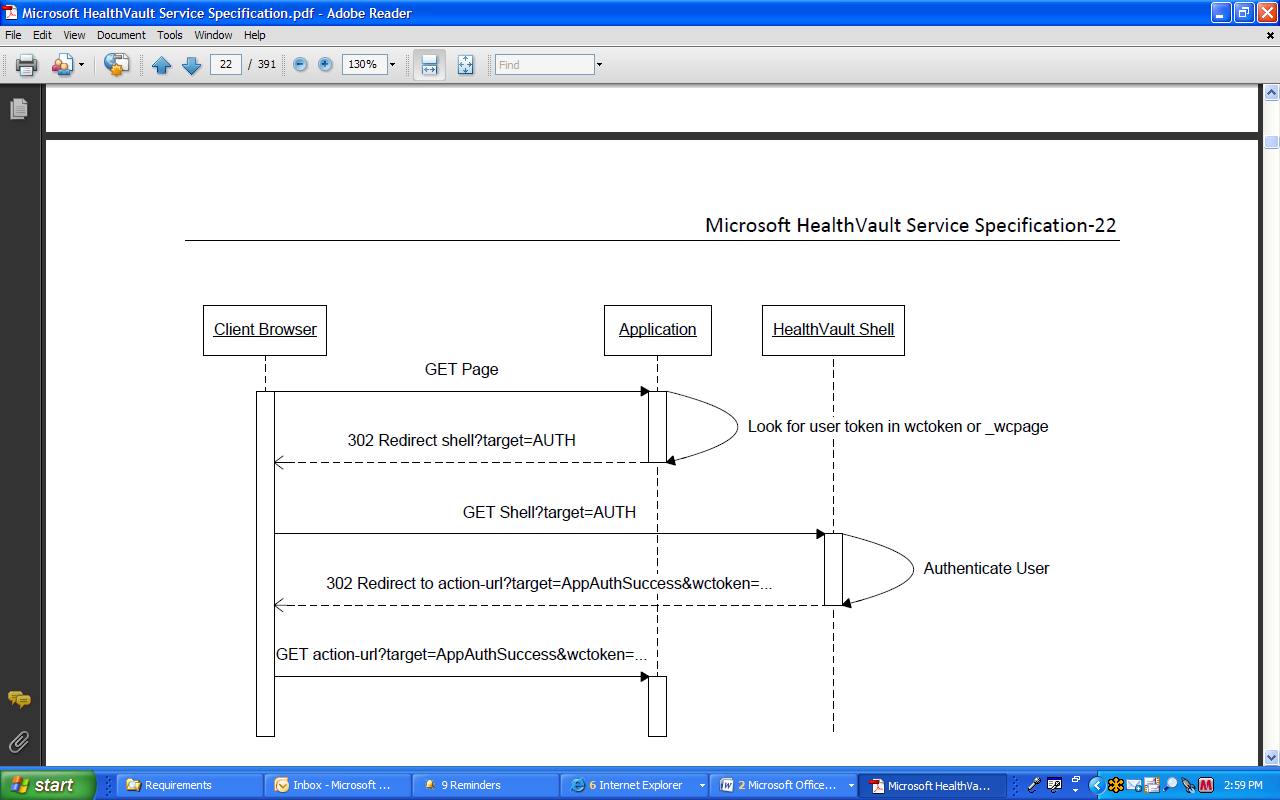
For an application session, MFHP will prove its identity by signing a x-509 certificate with RSA Digital Signature Verification using a private key.[[1]](#footnote-2) HealthVault verifies that identity using the public key which has been registered for MFHP with HealthVault prior to the application session. After HealthVault verifies the identify of MFHP, MFHP requests a session toke with the *createauthenticatedsessiontoken* message. The application session process, in generic form, is presented in Figure 1 below.

**Figure 1: Application Session Process**



For a user session, MFHP will redirect the client to the HealthVault Service for authentication. HealthVault offers the user a choice of authentication – WindowsLive ID (traditional username/password combination), or OpenID. OpenID is provided by 3rd parties, such as Verisign, and enables second-factor authentication using, for example, physical devices; image-based techniques similar to SiteKey; Windows Cardspace; or one-time-passwords through a mobile phone. With either one of these credentialing options, an MFHP user will provide his/her HealthVault credentials to the HealthVault Service, and, upon successful match, the HealthVault Service returns a token for use by the User for the duration of the user session. The user session process, in generic form, is presented in Figure 2 below.

**Figure 2: User Session Process**



All communication between MFHP and HealthVault will be secured at multiple layers. The transport itself is encrypted with HTTPS. Communication is doubly-encrypted using a shared secret that will be negotiated on a per-session basis between MFHP and HealthVault. All further communications are verified for authenticity via an encrypted token comprising an application ID, session ID, and a person ID.

Both the application session and the user session are timed-out at pre-determined intervals as specified by MFHP. If the response is an invalid token then MFHP and/or the MFHP User must submit a request to the HealthVault Service for a valid authentication token.

For more detail about authentication and other HealthVault specifications, see http://www.microsoft.com/downloads/details.aspx?FamilyID=721eed65-4758-4b0e-8c02-68b0e321f31b&displaylang=en

1. An RSA Digital Signature Verification (RFC3447) comprises the application ID, the public key and the x-509 certificate. [↑](#footnote-ref-2)