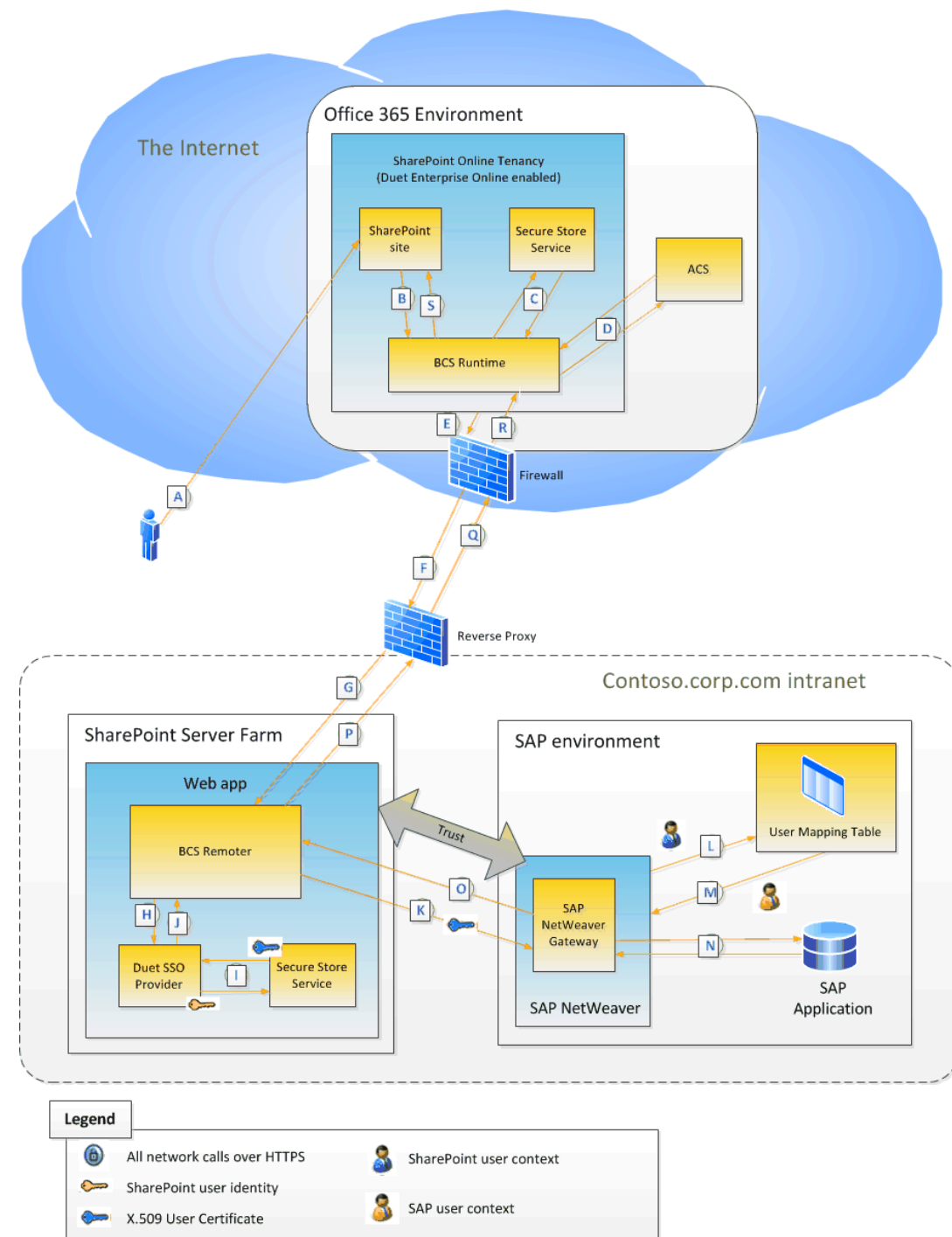


Duet Enterprise Online Authentication - Forward Flow

This illustration shows a high-level view of how authentication works in a Duet Enterprise Online environment when the end user is pulling data from the SAP system. This is also known as forward flow.



The following list describes the steps shown in the illustration.

- A user logs on to Office 365 and accesses a Duet Enterprise Online enabled website.
- Because the site surfaces data that is in SAP, the request is sent to the BCS Runtime.
- The BCS Runtime gets a remote proxy certificate from the Secure Store Service.
- The BCS Runtime gets a service to service OAuth token (also known as a JWT token) from ACS. This token identifies the following:
 - SharePoint Online Identity
 - SharePoint tenant calling the SharePoint on-premise farm
 - End user's ACS Identity
- The BCS Runtime sends the request along with the remote proxy certificate and OAuth token to the firewall.
- The firewall forwards the request to the reverse proxy server.
- Because the reverse proxy server trusts the remote proxy certificate that is included in the request, the reverse proxy server forwards the request with the OAuth token to the Duet Enterprise 2.0 enabled web application on the SharePoint farm. Before the request arrives at the BCS Remoter, SharePoint swaps the ACS credentials in the OAuth token for SharePoint on-premise credentials (credentials stored in AD DS on the intranet).

Note: The BCS request is addressed and sent to a particular web application in the SharePoint farm. Because a trust relationship was created between the SharePoint Server farm and ACS in the Office 365 environment during hybrid configuration, the SharePoint Server farm trusts ACS.
- The BCS Remoter invokes the Duet OData Extension Provider.
- The Duet OData Extension Provider gets the DuetRoot certificate from the Secure Store Service.
- The Duet OData Extension Provider uses the DuetRoot certificate to create an X.509 user certificate and sends the user certificate to the BCS Remoter.
- The BCS Remoter sends the request with the user certificate to SAP NetWeaver in a request packet.
- Because SAP NetWeaver trusts the DuetRoot certificate that was used to create the user certificate, SAP NetWeaver can authenticate the user and look up the SAP user who is mapped to the SharePoint user identified by the certificate.
- The SAP user account that is mapped to the SharePoint user is returned to SAP NetWeaver.
- SAP NetWeaver uses the SAP user account to request access to the requested information in the SAP system; and, if the user is authorized to access the information, the requested information is sent to SAP NetWeaver Gateway.
- SAP NetWeaver Gateway sends the response to the BCS Remoter on the on-premise SharePoint farm.
- The BCS Remoter sends the response to the reverse proxy.
- The reverse proxy sends the response to the Office 365 firewall.
- The Office 365 firewall sends the response to the BCS Runtime.
- The BCS Runtime sends the response to the end user. In this case, to the website in SharePoint Online that the end user has accessed.