# UI AND SERVICES ON DIFFERENT SERVERS A *cross-domain policy file* is an XML document that grants a web client—such as Adobe Flash Player (though not necessarily limited to it)—permission to handle data across multiple domains. When a client hosts content from a particular source domain and that content makes requests directed towards a domain other than its own, the remote domain would need to host a cross-domain policy file that grants access to the source domain, allowing the client to continue with the transaction. Policy files grant read access to data as well as permit a client to include custom headers in cross-domain requests.

The most common location for a policy file on a server is in the root directory of a domain with the filename crossdomain.xml (e.g. http://example.com/crossdomain.xml)—the default location that clients check when a policy file is required.

<?xml version="1.0"?>

<!DOCTYPE cross-domain-policy SYSTEM

"http://www.adobe.com/xml/dtds/cross-domain-policy.dtd">

<cross-domain-policy>

<site-control permitted-cross-domain-policies="master-only"/>

<allow-access-from domain="\*"/>

<allow-http-request-headers-from domain="\*" headers="SOAPAction"/>

</cross-domain-policy>

The site-control element here specifies that only this master policy file should be considered valid on this domain. Below that, the allow-access-from element specifies that content from any other domain can access any data within the current domain (the domain in which this policy file has been saved). Finally, the allow-http-request-headers-from element indicates that a SOAPAction header is also allowed to be sent with requests made to this domain.

(INSERT DIAGRAM)

Additional References:

<http://www.adobe.com/go/policyfiles>

<http://www.flexafterdark.com/docs/Flash-CrossDomain>