DDS Identity Federation Service

Sharing Identity across Organisational Boundaries

daemon DIRECTORY SERVICES

Executive Overview for UK Government

Identity Federation is an important service enabler for the Government's G-Cloud programme; it allows government agencies to seamlessly authenticate their users to external cloud based services without the need to maintain insecure secondary user accounts and passwords.

The DDS Identity Federation Service is an IL3 accredited, standards-based identity federation broker that meets this need. The DDS IFS manages trust relationships between government users and cloud service suppliers by interfacing with their agency's identity management systems (e.g.: Active Directory).

The service is scalable enough to meet the largest customers' needs and is open to any IL3 service supplier to join using DDS' easy-to-implement supplier service-joining package. The DDS IFS solution is fully compatible with other identity brokering solutions and fits into the government's broader plans for a future distributed identity management strategy.

Applications need to establish a user's identity whenever there's a need for users to have personalised service, which is almost always with modern web applications.

Establishing user identity is straight-forward when an application is run within the user's local network domain; the network Active Directory service[1] automatically makes the user's identity available to the application as needed.

But when the application is delivered as an external web service in the cloud, its server cannot be directly connected to the user's local Active Directory and so the user's identity is unavailable.

If the user needs a personalised service the traditional solution is to issue them with a secondary account with a separate username and password.

This may be an acceptable solution when a small number of users and external services are involved, but for an organisation aspiring to use multiple cloud-based services it simply doesn't scale – users would have to remember too many secondary accounts; they'd have to be separately on-boarded and off-boarded from each service and the multiple user identities wouldn't integrate on their the desktops.

Identity federation is modern technology that solves this problem. It does this by providing an 'identity broker' which a service application trusts to request users' identity credentials from different 'upstream' Identity Providers which it trusts.

Identity federation solves two problems for the cloud – service customers needing to access multiple services, and, service suppliers needing to support multiple customers.

Modern identity management solutions are now based on standard industry protocols (notably SAML 2.0, and WS*-Trust) which are supported by all the major authentication and identity management products.

The DDS Identity Federation Service (DDS IFS) is an identity brokering solution that supports these standards.

It has been developed from Microsoft's ADFS 2.0, operated from a secure resilient hosting platform, pre-accredited to IL3 (RESTRICTED) level, and available over GSi. This makes it ideal for government agencies intending to develop a G-Cloud service policy.

This paper explains how the DDS IFS works, the benefits it offers and how organisations and service suppliers can take advantage of it.

1. Almost all government networks now use Microsoft networking with Active Directory managing the network user identities

Company Profile

Daemon Directory Services Ltd. (DDS) is an application service provider supplying cloud services to the UK Government community.

DDS develops and deploys secure collaboration applications that can be used across organisation partnerships. The services include federated user identity management, departmental directories and multi-agency versions of collaboration software such as SharePoint and MS Dynamics CRM.

DDS specialises in working with UK Government agencies and is fully equipped to meet their security requirements.

DDS products have been used in Government for more than 15 years, in which time most of the central Government agencies have used one of more of DDS' products or services.

DDS was a founder partner of the first pan-Government shared hosting service – the Government Wide Service (GWS) delivered by Savvis.

DDS is a leading SME in the supply of IL3 accredited SaaS services to government, with 10 services in its G-Cloud portfolio.

Contact Details
DDS Ltd.
Gaston House
Gaston Street
East Bergholt
Colchester
CO7 6SD

Web Site: www.dds-labs.com
Email: info@daemon.co.uk
Tel: +44 (0) 1206 299288

Identity Federation – Why it is needed

Being able to establish a user's identity is a pretty standard requirement in a corporate IT environment; it 'personalises' the service and enables users to get to information that's protected by user permissions.

Establishing identity is not a problem within a local network; the user 'authenticates' themself to network when they first log in, and from that point will expect their identity to be recognisable by all the applications they fire up on their desktop; e.g.: MS Office, Outlook, the corporate intranet and so on.

In a Microsoft based network this is done by Microsoft's Active Directory service which manages network assets in the local network domain, including user sessions. The AD controller issues and maintains an 'identity token' for the user so long as they are logged in and passes this token to applications and web services operating within the network domain in a form they can recognise (see Figure 1 opposite).

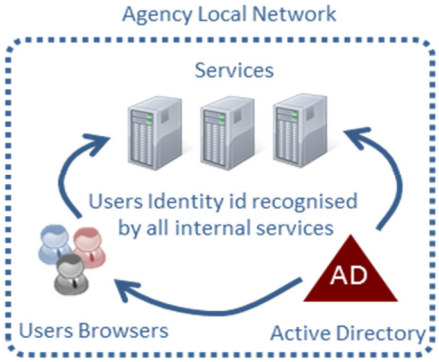

Figure 1 - Identity in a local network

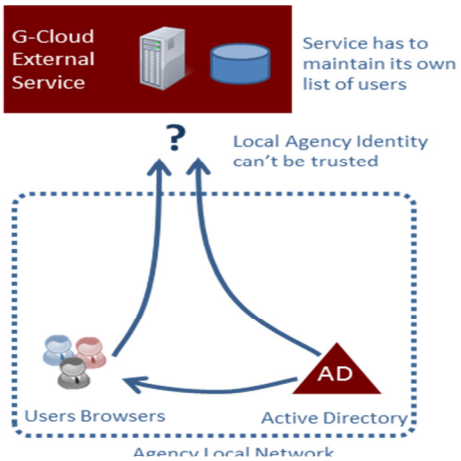

Figure 2 – Enter an External Service

Things get difficult when the user goes beyond their local network; i.e.: when they need to access applications on a partner's network or on an external 'cloud' service. The problem is that the identity tokens that are generated and understood on an internal network aren't valid to an external systems provider who's outside the network domain. Without their identity being recognised the user can only be granted anonymous access to the service, (see Figure 2 on left).

The old fashioned solution to this problem was to give users of the external service a secondary account and have them remember a separate login and password. However, that approach is now recognised as inefficient and insecure; there being significant account management overhead and additional security risks with users having secondary accounts. It's also recognised that this is impractical when dealing with multiple external services as would be faced by a government agency aspiring to adopt the G-Cloud strategy.

The modern solution uses federated identities to exchange user identity tokens beyond the boundary of the user's local network, there now being industry standard protocols for generating, encrypting, exchanging and interpreting identity information.

In order to exchange identity information a trust needs to exist between the identity provider and identity consumer. Trust relationships are 'one-way' in the sense that the service supplier needs to trust the service consumer's ability to provide the users' identities but there is no similar trust requirement in the other direction. The party providing the user's identity information is termed an 'Identity Provider' (IdP), and the party depending on this trust, the 'Relying Party', (RP). IdP and RP trusts use certificates to 'bind' the relationships, using the certificate keys to encrypt and decrypt fields in the identity tokens.

The need for identity 'broker' services arise as suppliers increase the number of consumers using their service and as consumers increase the number of services they consume. That would cause the number of trust relations and certificates to rise proportionally, creating the need for a trusted 'middle-man' between these parties, reducing the number of trust relationships needing to be established. That is the role provided by the DDS IFS broker service.

The identity broker server will decrypt and re-encrypt user identity tokens as they pass through it. It also provides the ability to 'map' identity credentials across the service boundaries to meet different configurations; e.g.: when a customer IdP provides a different set of identity claims (email, forename, surname, tell-number, role, etc.) to that needed by the RP service.

The IFS broker is illustrated in Figure 3 opposite.

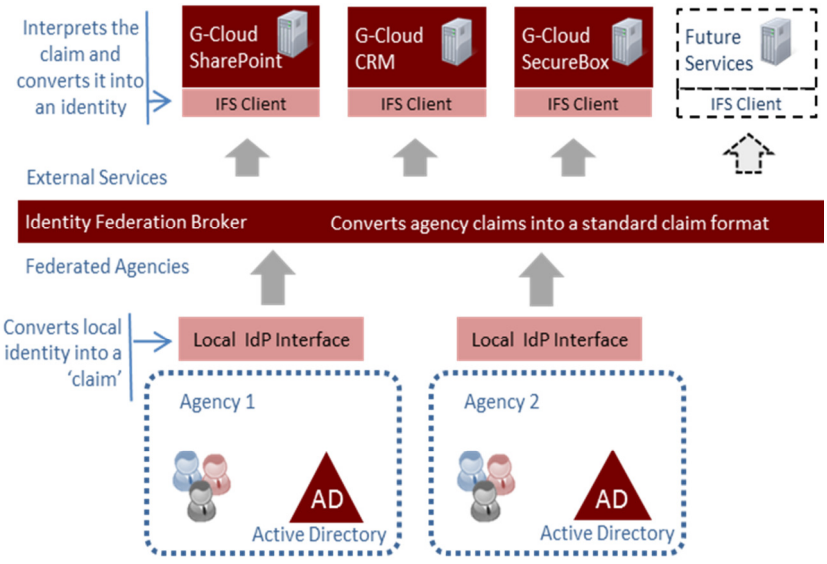

Figure 3 - the Identity Federation solution, brokering and converting

Identity Federation – How it Works

The overall process for identity federation has become known as 'Claims Based Authentication' (or CBA). CBA is supported by a wide range of products, all of which now comply with the two dominant Internet standards: SAML 2.0 and "WS-Trust". In the Microsoft world the key products are *Active Directory Federation Services* (*ADFS 2.0)* which converts an Active Directory domain into an IdP service and *Windows Identity Foundation* (*WIF*) which, when added as a authentication layer to an .NET application converts it into an RP. In the Oracle & Java world, there are similar products, e.g.: for IdP services - Oracle's *Identity Federation Manager or* IBM's *Tivoli* and for RP services, the open-source *Shibboleth plug-in for* Unix based web servers such as Apache.

Most government organisations run networks based on MS Windows and use Microsoft *Active Directory (AD)* and therefore would need to implement ADFS 2.0 to become an IdP in a federated identity environment[1].

It's helpful to work through the exchange of messages when an agency user federates to an external service, as shown in Figure 4 below where a user on a Windows network accesses an external (e.g.: G-Cloud) SharePoint service through a federation broker.

Certificates Set-up

The necessary certificates binding the trusts must first have been set up on all servers involved exchanging certificates. The SharePoint-DDS IFS server has a RP-IdP relationship as is the DDS IFS-organisation ADFS server relationship, (certificate relationships are shown as the dotted lines in Figure 4).

Communication by Browser Redirects

The three servers in Figure 4 do not communicate directly with each other. Instead the user's browser passes messages between the servers by being instructed to 'redirect' its web requests. This means there's no need to open firewalls for incoming messages into the agency network – something that would go against the agency's security policy.

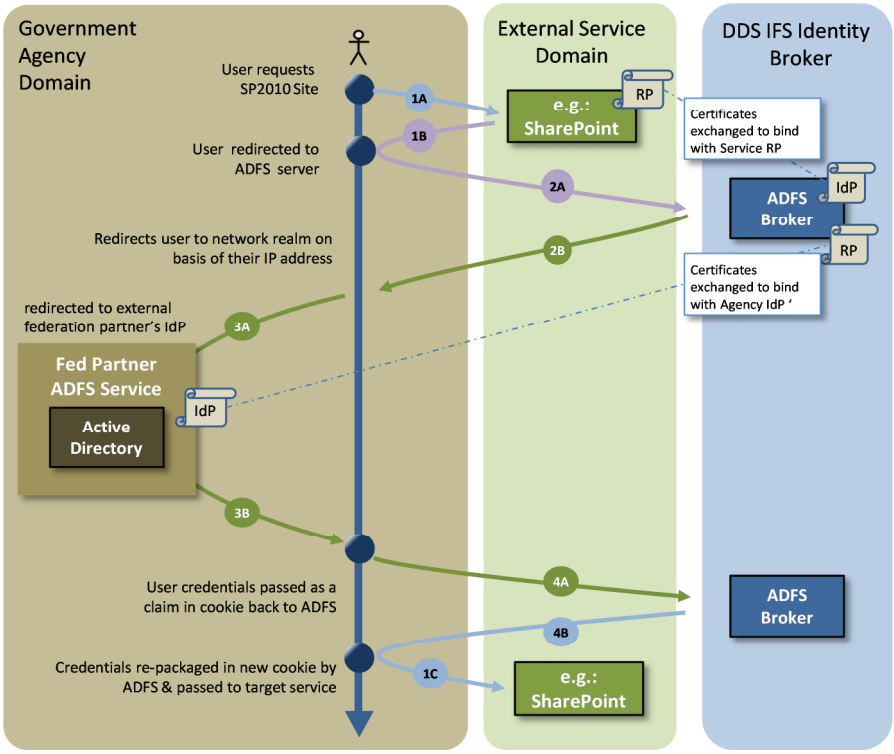

Figure 4 – Example showing how IFS works with DDS IFS Broker

1st Redirect - paths 1A, 1B and 2A

The user calls the SharePoint service as a standard URL from the browser. The call is intercepted by the web server's WIF plug-in and a check is made for an identity 'claim' cookie. The first time the session is opened there won't be such a cookie and so WIF redirects the browser to the DDS IFS Identity Broker to which it is bound to get one. On subsequent occasions the cookie will exist and this entire process will be skipped.

2nd Redirect – Paths 2B and 3A

The ADFS server is a broker and doesn't actually do any authentication, instead it redirects the request for an identity token it to the user's IdP server; the address of which it knows by checking the sub-net from of the incoming request against a lookup table of all bound IdP servers.

3rd Redirect – Paths 3B and 4A

The receiving ADFS server receives the redirected request from the DDS IFS server and builds a 'claim' cookie confirming the user's identity using information obtained from the AD server; cross-referencing the workstation that the current user has logged into it. The 'claim' token takes the form of a web response in XML, with sensitive fields encrypted, and returned as a redirected response to the DDS IFS Identity Broker.

4th Redirect – Paths 4B and 1C

When the DDS IFS Identity Broker receives the claim it decrypts it (using the certificate key shared with the agency ADFS server); remaps its attributes to those needed by the SharePoint server; then re-encrypts the re-mapped claim (this time using the certificate key shared with the SharePoint server) and returns it to the SharePoint server via a browser redirect. The SharePoint server WIF plugin receives the claim, de-crypts it using its part of the shared DDS IFS Broker certificate, and passes relevant claims attributes (i.e.: the user's ID) to the web server for the application to access (in Windows this is a web server 'IIS Session variable').

---

[1] DDS has a G-Cloud service for this - see http://www.dds-labs.com/g-cloud-services/cloud-management-services/g-cloud-identity-federation-services-ifs/

The DDS IFS Identity Broker Service

The DDS Service in Summary

The DDS IFS Identity Broker service has been accredited to IL3 (RESTRICTED) by the Home Office and is operated from a secure hosting centre run by SAVVIS. The service is designed to be resilient and scalable, and initially sized for 100,000 users. The service is available to government users over the GSi or similar secure networks.

The service is built on the Microsoft AD FS 2.0 platform and is capable of federating with any partner network that's compliant with the standard Internet identity protocols of SAML 2.0 or WS-Trust.

Service suppliers can connect to and use the service whether they use a Microsoft or Unix based web server (they'd use the *WIF* or *Shibboleth* server-side plug-ins respectively). The only condition is that the supplier's service needs to be IL3 accredited and be accessible via the GSi to connect to the DDS IFS.

It's straightforward to join, either as a service supplier or as a customer organisation – and to make the process easy, DDS has developed a set of implementation work-packages available as G-Cloud "Lot-4" special services[2].

Joining the Service – Government Bodies

A government organisation joining the DDS IFS Identity Federation service is require to first install Microsoft's ADFS plug-in as a service on a Windows server within the organisation's network domain, (this may be on the AD server itself) - this of course assumes the organisation is using Microsoft's networking (which almost all do).

With the ADFS service running, the customer requests and installs a certificate from the DDS IFS Identity Broker service and then configures in the information on the connection with the DDS IFS ADFS server.

N.B. - there is no need for firewall ports to be opened on the organisation's network, so there is minimal impact on the organisation's network security profile, greatly lessening the impact of implementing the service[3].

Joining the Service – Service Suppliers

Suppliers can join their service applications to the federation service to make them available to government agencies. Joining an application is similarly straightforward: If it is a Windows application then the supplier needs to install the (free) Microsoft WIF module on the server (already installed with WS2008R2). If it is a Unix/Java application then the supplier installs the Shibboleth plug-in.

Implementing the certificate 'contract' between the server and the federation broker and setting up the configuration is the same as for a customer agency.

All of these tasks are straightforward and have been templated by DDS in its work-package so that if an organisation's IT supplier is unfamiliar with this set of tasks DDS can readily help. The estimate on the amount of engineering time involved is measured in a few days, including testing.

DDS have also developed a virtual testing rig in Internet space so that customers and suppliers can test their environments before committing changes to their production systems[4].

Local Directory Services

DDS have recognised that there will be some organisations who will want to use services that use the DDS IFS but won't want (or be able to) join the federation service as IdPs. For such organisations the DDS IFS service includes a local directory capability through which local user accounts can be provided. These accounts work alongside fully federated accounts with the difference that they are secondary accounts that prompt the user for a user-name and password in order to generate a token.

Local Directory user accounts can be managed by the customer through an easy, self-serve administration module that's integral to the DDS IFS service. Of course, fully federated user accounts don't require any management.

---

[2] See the DDS web site www.dds-labs.com/g-cloud_services

[3] Microsoft publish a various guides to setting up ADFS – see this reference here for a list: http://technet.microsoft.com/en-us/library/adfs2-step-by-step-guides(WS.10).aspx. DDS also have a G-Cloud consultancy package that can supply this to an agency.

[4] See the DDS IFS entry on the G-Cloud CloudStore http://gcloud.civilservice.gov.uk/cloudstore/ and search for DDS.

Summary of DDS Identity Federation Service Functions

DDS IFS - Key benefits

DDS Identity Federation Service (DDS IFS) is a standards-compliant, single-sign-on solution that offers a security accredited, government-facing identity federation system for government bodies. It is designed to allow government customers and government suppliers to seamlessly pass their user identity credentials to G-Cloud provided IL3 accredited services.

DDS IFS is simple to implement, transparent to use, quickly deployable on an organisation's local network domain and procurable as a GWS SaaS service. The benefits to the organisation's management and users can be summed up as follows:

Benefits to Customers	
Wider access to G-Cloud services	The DDS IFS gives a government organisation a way of securely reaching G-Cloud services without the need for managing secondary accounts
Reduced management	Because administrative time and effort is saved by not needing separate on-boarding and off-boarding of users for each external service consumed
Improved security	Because there are no secondary user accounts to be managed - users don't have to memorise (or write down) additional usernames and passwords, and secondary accounts don't have to be cleared when users leave the system
More interoperability	Because identities are shared across partner networks, users can trust each other's user credentials for authentication and authorisation
Improved desktop integration	Because external applications and services can be more easily assimilated into the user's desktop when they are run under a single identity
No firewalling issues	Because the DDS IFS solution operates through the user's browser redirects over existing out-going HTTP and HTTPS ports and there is no need to change firewalling rules on the customer's local network
Saves money	Because the customer can access the cost effective competitive market of G-Cloud services seamlessly - as though they were local services
Future proofing	Because the DDS IFS leverages the customer's existing identity infrastructure whilst applying standards that will be used in the future
Accredited Security	The DDS IFS has been accredited to IL3 (RESTRICTED) level by Home Office Security and is available via a GSi network connection
Easy to Implement	The DDS IFS system is easy to connect to with DDS providing consultancy work-packages to assist customer IT support teams if they are unfamiliar with the technology; similar support packages and test environments exist for suppliers wishing to connect their services
Easy to Procure	The system is procurable as a pay-as-you-go SaaS service through the G-Cloud Framework and there are deployment packages available to build an IFS interface into the agency's local network.
Immediate Availability	The DDS IFS service has been operative since mid-2011 and is available to join now
Free Trial	DDS offer a free trial of the service, and if required free access to the DDS IFS test rig for customers to test the system in their own context

What Next?

You may want to

- Contact the DDS Government Directory Team
- Ask for a demonstration
- Discuss the business implications or talk through the technical architecture

See http://www/dds-labs.com
Contact info@daemon.co.uk

daemon DIRECTORY SERVICES
Gaston House
Gaston Street
East Bergholt
Colchester
CO7 6SD
01206 299288
info@daemonlabs.co.uk