SERVICE DEFINITION

Fordway Cloud Identity Management Service
Why you need this?

_Fordway Identity and Authentication Management Service (IDAMS)_ is a cloud-based, user identity and authentication service which provides an authoritative source of identity to authenticate against corporate, PSN, Web, Cloud and hosted systems. This minimises the time and complexity of brokering authentication and access to cloud services, simplifying the user experience, while reducing security and compliance risks and user support costs.

Single sign-on has long been seen as a panacea for IT system access and administration. The growth of Cloud and other web based services would indicate that the situation will only become more challenging. Historically, bespoke solutions to solve this have come at a significant cost, both in terms of time and complexity.

_Fordway IDAMS_ solves the problem of every user requiring access to a proliferation of systems, many of which are no longer hosted internally, meaning more authentication requirements, multiple logons and more complex passwords. Allowing users to sign into all key corporate systems, once, provided suitable security controls are in place, has massive benefits to security and ease-of-use. One of the largest support costs in any organisation is user login and password issues. In the organisations Fordway has surveyed this can be in excess of 25% of all Service Desk calls logged.

_Fordway IDAMS_ offers pre-configured connectors for over 20 applications. These include Active Directory, LDAP, NIS and eDirectory; web services; ERP, CRM and databases including SAP, Oracle, PeopleSoft, SQL Server and Sharepoint; MS Office365, Salesforce, Service Now and Google Apps; IaaS and PaaS including Microsoft Azure, Amazon Web Services and Google’s App Engine. Custom connectors can be developed. _Fordway IDAMS_ can be configured to authenticate to almost any other system. It includes a self-service Client portal. Here the users or your administration staff can provision and update requirements for themselves, with custom authentication and provisioning workflows defined to allow staff and partners secure access to services.

Benefits

The key benefits of utilising Fordway’s Cloud Service Management are:

- **Access to any system** – all systems from any location are covered.
- **Map to business processes** – configurable workflows through the portal allow authentication and access processes to map to the way your organisation works.
- **Single set of credentials required** – no additional logon needed for accessing multiple applications.
- **Enhanced security** – every element is secured and encrypted.
- **Consistency of Approach** – as the login process is the same for anyone from anywhere it ensures less confusion about accessing services, reducing Service Desk calls.
- **User self-service** – staff and external users can self-maintain their credentials and administrators can simply provision new users from pre-configured templates and workflows.
- **24x7x365 Support** – The service is fully supported by Fordway with no requirement for your own staff to manage it – no more people phoning you in the middle of the night to access systems.
Service outline

The key characteristics of Fordway IDAMS are:

- **Single authoritative identity source for authentication to anything** – enables authentication against the vast majority of Cloud, hosted or in-house IT services available today, from any source.
- **Seamless authentication** – credentials are automatically supplied to target applications once approved.
- **User self-service** – all available applications and services are published to a portal which users can select and put into ‘shopping baskets’ for approval where required.
- **Integrated workflow and approvals** – this allows for automated provisioning of services and managerial authentication of available services.
- **Web portal** – all user and administrator functions are provided through a single web portal for identity management and authentication.
- **Self-service password reset** – users can optionally securely reset passwords without access to any service desk.
- **Multi-Factor authentication** – secure tokens or challenge response systems can optionally be incorporated for extra security.
- **Formal audit trail** – every authentication and service interaction is recorded for regulatory and compliance purposes.
- **Support for external users** – Fordway IDAMS offers a lightweight authentication service plus workflows for external, non-organisational users or extranets and other secure communities.
- **PSN service available** – the IDAMS service is available over the PSN, Fordway’s IDAMS service is PSNSP certified.
- **N3/HSCN service available** – our IDAMS service is also available to authenticate applications delivered over NHS N3 and the new Health and Social Care Network (HSCN).

Service diagram
Fordway IDAMS modules

Fordway IDAMS is a modular service which offers extended capabilities to meet every organisations’ requirements. The available modules are:

✓ **Base IDAMS service:** provides identity management, taking an authoritative data source for employees from a number of possible sources including direct input into IDAMS, CSV and other data files, HR systems, Active Directory and LDAP. This central account is used as the template to provision further accounts and roles into connected applications and services. The base module includes workflows for controlling user provisioning, role provisioning and group memberships of target systems. The base IDAMS service includes a number of standard application and service connectors which are detailed in the product notes below.

✓ **Specialist connectors:** IDAMS offers a number of additional connectors, detailed in the product notes below. Custom connectors can be configured or developed for applications which do not conform to one of the standard authentication methods.

✓ **Extended Web authentication:** SAML is supported as standard. This module allows credential pass through and seamless authentication between other Web authentication standards including SOAP, WS-Federation, LDAP, Kerberos, https, SPML, XACML and webforms authentication.

✓ **External community authentication:** provides secure authentication to trusted partners, third parties and extranet users. The Base external service provides the same authentication set as the Base IDAMS service. The Enhanced service provides the suite of Web authentication services to external users.

✓ **Automated password reset:** allows users to securely reset passwords without Service Desk input with customised, user defined challenges.

✓ **Multi-factor authentication:** available either as a standalone capability or integrated within IDAMS. This facility allows a variety of additional controls on authentication including OATH compliant hardware tokens, soft tokens for iPhone, Android, Windows Mobile and Blackberry, one time SMS messages for occasional users and web tokens with token self-registration.
Information assurance

All elements of the service are secured to ISO27001 under Fordway's certification, Fordway are Cyber Essential PLUS accredited, and all operational processes to deliver and manage the service are certified to ISO20001. *Fordway IDAMS* service is hosted and runs active/active across our two datacentres. The service is Pan Government Accredited (PGA) up to and including OFFICIAL and has the relevant controls in place to authenticate to OFFICIAL-SENSITIVE. Public Sector clients can access the service over the PSN; connectivity is resilient across Fordway’s two datacentres. *Fordway IDAMS* has also gained PSN Service Provider (PSNSP) certification. NHS clients can use IDAMS to authenticate to N3 and HSCN delivered applications and access the service through these networks.

As IDAMS is a directory service containing user accounts and access credentials for entire organisations. Fordway further restrict access via placing the environment in its own security environment with audited access and controls.

Data security

All information held within *Fordway IDAMS* is encrypted. Audit logs and other checks are in place to ensure the data can’t be modified, copied or removed without a trail being left. These logs are inspected on a regular basis, and the entire service plus process checks have undergone Pan Government Accreditation. Each client’s environment is securely segregated from others. The IDAMS databases for each client are automatically replicated between the two Fordway datacentres to ensure resilience in case of a failure.

Data backup

Multiple levels of backup are performed on the IDAMS environment for each client, based on regular system snapshots taken every 2 hours. The service runs across both Fordway datacentres active/active with real time data replication, connections are load balanced between them.
Pricing

Fordway IDAMS is priced as follows, the same pricing is applicable for both Standard (Internet and private client networks) and PSN/N£/HSCN Authentication, and can be configured to authenticate across both environments concurrently:

Volume discounts are offered for the IDAMS service, for the full base service users the volume discount breaks are at 1,500, 5,000, 10,000, 25,000, 50,000 and 100,000 users. External user price breaks are at 25,000, 50,000, 100,000, 200,000 and 500,000 users.

FORDWAY IDAMS SERVICE COSTS – PER USER

<table>
<thead>
<tr>
<th>Service Description</th>
<th>Monthly Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base service, comprising authoritative data source plus standard connectors and configured workflows</td>
<td>£2.95</td>
</tr>
<tr>
<td>Additional custom or specialist connector, per connector</td>
<td>£1.00</td>
</tr>
<tr>
<td>Internal user self-service password reset capability</td>
<td>£0.50</td>
</tr>
<tr>
<td>Web authentication service for internal user added to IDAMS service</td>
<td>£0.65</td>
</tr>
<tr>
<td>Two factor authentication for internal user added to IDAMS service</td>
<td>£3.50</td>
</tr>
<tr>
<td>Basic extranet/third party user authentication with SAML federation</td>
<td>£0.45</td>
</tr>
</tbody>
</table>

Product notes

- Standard connectors comprise: Active Directory, MS Exchange, MS Office 365, SharePoint, IBM Lotus Notes, LDAP, OpenLDAP, ODBC, ASCII flat file.
- Custom connectors, at additional charge, include: Oracle, SAP, PeopleSoft, IBM iSeries, IBM DB2, IBM zOS (Mainframe), Novell eDirectory, Google Apps, Amazon Web Services plus any custom connector development.
- Charging is per user identity within the IDAMS service.
- Third party users are those not employed or contracted to the contracting organisation who need access to hosted systems from the organisation Fordway IDAMS is configured for.
- Minimum service requirement is 500 users from a single organisation.
- Service design, initiation and user migration is done as a scoped engagement using Fordway Cloud Migration Services from within G-Cloud at defined SFIA rates.

Service levels

Fordway IDAMS is delivered from two load balanced UK datacentres. Application availability is 99.95% measured annually, 99.9% in any quarter. 24 x 7 telephone and web support are provided as standard. Clients have access to service availability information for each instance and overall service availability for their services through Fordway’s Client Portal plus have access to regular service reports.

Service monitoring

Availability monitoring is included as part of the standard Fordway IDAMS service and provides information of Instance availability, capacity and basic performance. Events and alerts from IDAMS can be forwarded to a clients’ systems monitoring tools or viewed through Fordway’s customer portal.
Fordway offers over 27 years' experience advising and delivering strategic IT infrastructure and IT service delivery change to complex enterprises. We've been providing this service in all iterations of G-Cloud since the first iteration in 2012 and it has been enhanced with each iteration to support market needs.

Fordway's consultancy helps inform your strategy and review the options relevant for your organisation. Our advice will be aligned to your business requirements. We then assist with the ongoing operational management and optimisation of the resulting cloud service, based on best practice defined by the ITIL service management framework.
Service Terms

Service management and reporting
Fordway’s Service Operations and Service Support teams maintain and continually monitor the IDAMS service, responding to any issues with the service. Utilisation and trending information on service performance and availability is included as part of the management service and is available through an online portal. This offers real-time service availability plus incident, change and service requests with standard online reports. IDAMS includes manned Service Desk support 7.00am to 7.00pm weekdays excluding statutory holidays. Priority 1 (service down or unavailable) incident escalation is provided 24 x 7, as standard. Clients receive consolidated monthly service level and highlight reports plus security incident reporting.

For higher levels of service and user support we offer Fordway Cloud Service Management. For Government clients this is under G-Cloud. In brief this provides a range of additional services including:

- Nominated Fordway Service Delivery Manager with scheduled service reviews
- Customised reporting to individual client requirements
- Integration of Fordway’s service management toolsets with client service management applications
- Additional service desk services including end user support and incident management for 3rd party suppliers
- Service reporting to include availability and performance of other Cloud and third party services where clients contract for Cloud Monitoring as a Service (G-Cloud Lot 2).
- Asset management of client devices and infrastructure

Service constraints
Fordway IDAMS service runs active/active across two datacentres. There is no requirement for planned downtime of the underpinning IDAMS infrastructure. Fordway IDAMS is available 24 x 7 x 365. Any updates or patches will be performed using spare capacity and reallocation of services between physical components. OS and application patching of instances may require server instance downtime but the service will not be affected. Due to operating a fully resilient and virtualised environment there is no requirement for planned downtime of the underpinning IaaS infrastructure. However, each quarter Fordway reserve the right to invoke a 4-hour maintenance window. A maximum of two of these can be invoked per datacentre in any rolling year.

Recompense for not meeting SLA’s
Service availability levels are calculated quarterly. The SLA guarantees 99.95% availability per year which equates to 8 hours downtime per year. For each hour of service unavailability in a year over this Fordway will recompense users of the service by providing a credit of 2.5% of the monthly service contract value for each working hour the service has not met the SLA up to a maximum of 20% of the monthly service charge.

Service connectivity
Users of this service require network connectivity to Fordway’s datacentres. Primary network connectivity is via secure SSL (https) or IPSec VPN connectivity over standard Internet links. Our datacentres also support MPLS and VPLS connectivity from major service providers. For Public Sector clients we offer PSN compliant network connections into our datacentres, the service is undergoing PSN Service Provider certification.

Trial of service
Due to the complexity of the solution it is not possible to offer a formal trial of the service. Prospective clients can access and evaluate a test and demonstration service which offers a range of standard connectors and pre-configured workflows.

Service initiation (on-boarding)
The requirements to commence Fordway IDAMS are as follows:

- Review of directory requirements and
services to authenticate

- Define authoritative source(s) and information flows
- Build/configure connectors
- Define and agree authorisation and authentication policies
- Define and create workflows
- Test the solution
- Migrate the directories
- Service goes live

Clients need to have administrator access to the target directories, applications and services for Fordway to configure and test IDAMS. Valid licences for all source and target services are the client’s responsibility. The monthly Fordway IDAMS user charge includes licences for all contracted elements of the IDAMS service.

Provisioning Fordway IDAMS is a managed design and on-boarding project and there is a correlation between the number of connectors and workflows to the time to deliver. Workflows include such features as self-service portal and joiners, multiple level approval processes plus movers and leaver’s processes. A number of standard workflows are included.

Service termination (off-boarding)
The requirements to terminate Fordway IDAMS are as follows:

- Fordway will receive formal notification from an authorised person
- Date and time of expiration of service will be agreed
- Details of when the workflow and directory synchronisation will cease will be agreed
- Authentication to all relevant systems and services will cease at the allotted time
- Any servers holding directory information will be wiped/deleted by Fordway and all connectors removed
- Standard Service termination charge is 50% of the average monthly Service Cost

Termination terms
Fordway require one month notification for termination of the service. Fordway reserve the right to terminate the service if improper usage of the system has been found, and reserve the right to impose penalties up to and including the full payment of the agreed contract, depending on the nature and severity of the breach.

Training
Fordway IDAMS workflows and client administration are configured as a joint project with each client. Formal training is provided remotely by Fordway to client IT staff with documentation as part of the service initiation. Onsite Fordway IDAMS training and portal/workflow training is also available and can be provided on request, this is normally chargeable.

Customer responsibilities
It is the responsibility of the customer to ensure the systems are used in a proper fashion, in accordance with English Law, the specified terms and conditions of service plus any procedures governing access and usage policies laid down by their organisation. Fordway will apply data access and other server security policies as mandated by the client for use of the service; these are defined and set up as part of the service initiation. If the customer cannot provide these the cost of setting these up will be charged as part of the migration onto the service.

As the service relies on processes defining authoritative data sources and procedures to ensure information is added via the correct interfaces, it is the customer’s responsibility to ensure that all their staff comply with these procedures. Any breach of IDAMS or issues caused by improper use of the systems or workflows are not the responsibility of Fordway.

Change management
Any required changes to the service are initiated and managed through Fordway’s Change Management process which customers will be given access to once the service is initiated. All Change Requests are reviewed and implemented where accepted against a published SLA which is provided as part of Service Initiation. The online customer portal also offers Service Requests for incidental elements, and authorised staff from the customer organisation can add or delete users.
Ordering

Fordway services can be ordered by contacting your Fordway account manager or other members of our team on 01483 528200, emailing sales@fordway.com or using the contact form on www.fordway.com.

Public Sector customers can order Fordway IaaS and other Fordway Cloud services through the G-Cloud Framework, please go to www.digitalmarketplace.service.gov.uk, search on Fordway and browse the catalogue.

Fordway Solutions Limited Hambledon House
Catteshall Lane
Godalming
GU7 1JJ

01483 528200