



# **Government Gateway Release 2.2**

## **Feature Overview**

# GG 2.2 Feature Overview

- **Delegated Rights Management**
- **Strong Authentication**
- **SSOP Enhancement**
- **Disaster Tolerance**

# Delegated Rights Management

- **Allow Organisations and Agents to use their own “access rights” model within their Corporate Systems**
- **Agent users only able to access online services for the clients they have been assigned within their organisation**
- **GG Single Sign On site brokers interaction with corporate systems**
- **Used for Transaction and View Account type Services**
- **Common implementation for use by all Organisations**
- **Existing functionality remains unchanged**

# Strong Authentication

## Registration Authority and Authentication

- **Strong Authentication using Chip & Pin**
- **Extension of Identity Services and integration with 3<sup>rd</sup> party CAS/HSM component**
- **Extending the Common Authentication Portal**
- **Extending the SOAP Admin interface and enhancing existing methods**

# SSOP Enhancement

- **Identity Services**
  - Extend Portal Objects
  - Extend Resource Schema
- **Common Authentication Portal**
  - Extend session model
  - Extend Identity Orchestration
  - Extend sign-out handler
  - Implement keep alive handler
  - Enhance sign in handler

# Disaster Tolerance

- **Additional Layer of Disaster Tolerance**
- **Gateway to Hold Transactions**



# Gateway Delegated Rights Management

Technical Overview

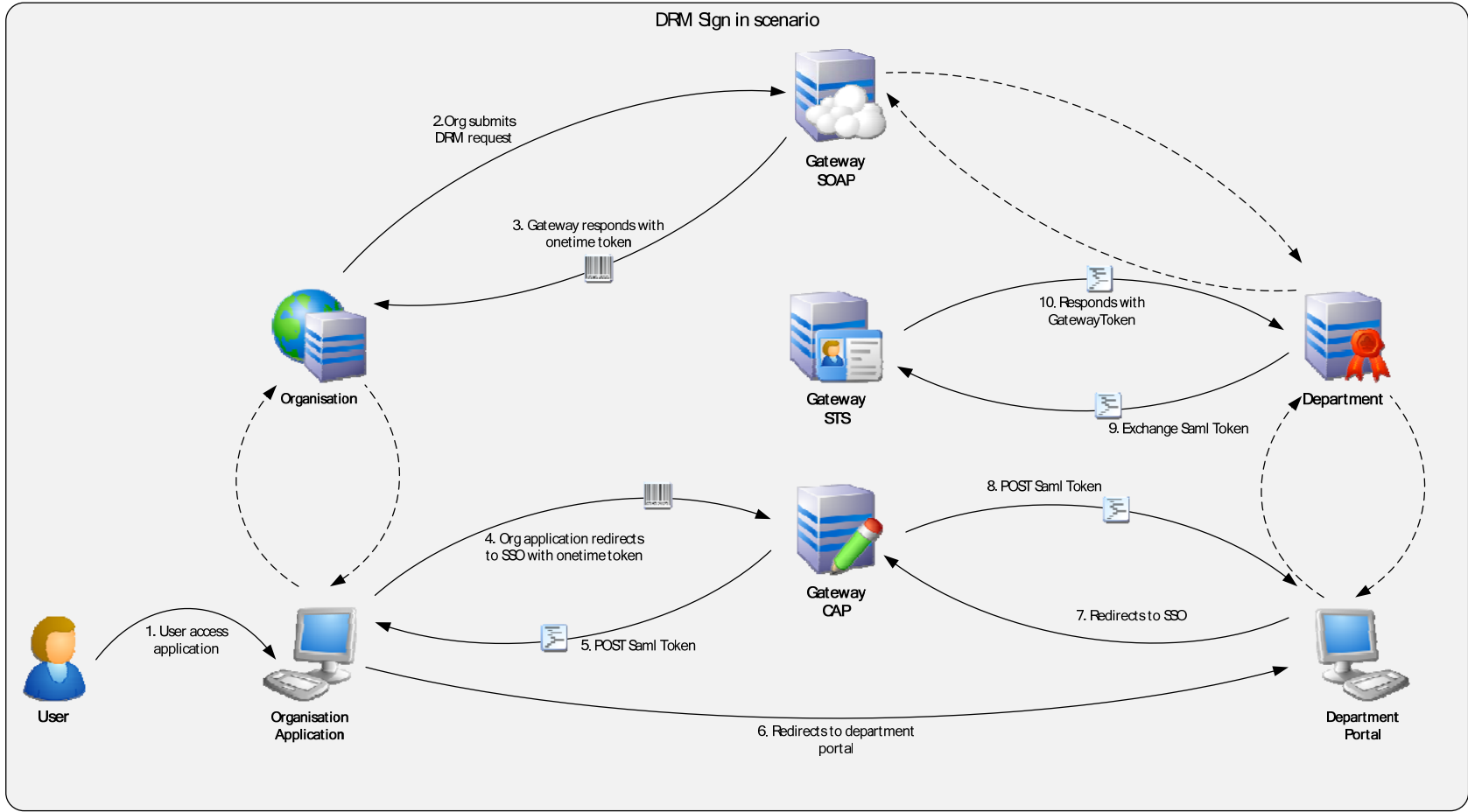
# Technical Overview

## Objectives

- Understand High level architecture
- Understand how to set up a DRM admin user
- Understand how to delegate rights
- Authenticating through the Common Authentication Portal

**NB – Please feel free to ask questions as we go.**

## High level architecture



## High level architecture

- Key areas of functionality
  - Public SOAP API
  - Common Authentication Portal
- DRM Admin user created on <http://www.gateway.gov.uk>
- Delegating rights results in a onetime token
- Onetime token then used to authenticate user on CAP

# Technical Overview

## Setting up DRM admin users

- What does a DRM admin user do?
- How many can be created?
- Using <http://www.gateway.gov.uk>

## DRM “Home Page”

**Government Gateway**

- Services
- Your details
- Your assistants
- Manage users
- Manage DRM users
- Help
- Log out

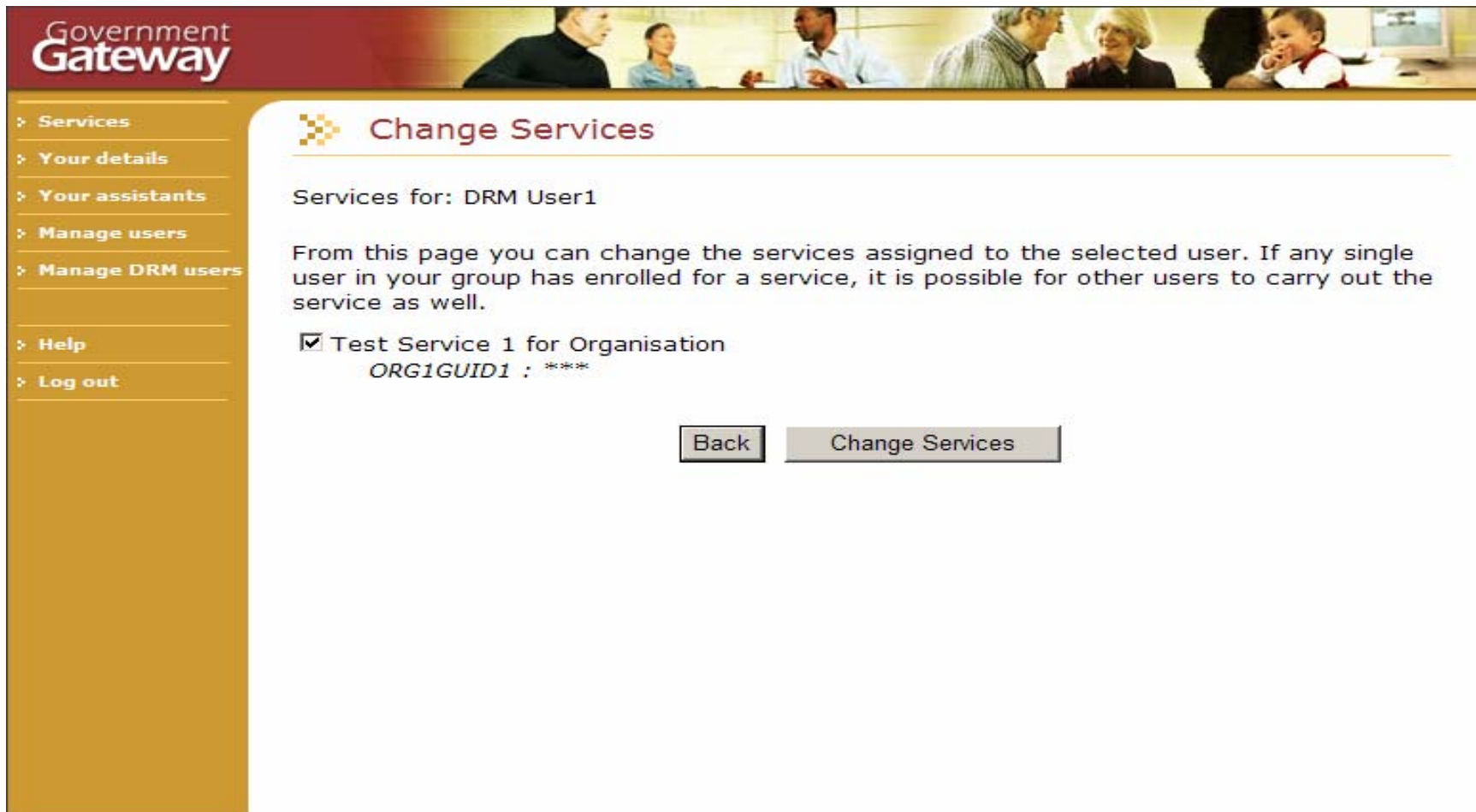
### Manage DRM Users

This page lists the DRM Users in your organisational group. You can view more details about each user, by clicking on their name.

Name	Additional Info	Services	Actions
<a href="#">DRM User1</a>	A DRM User	1	<a href="#">Change services</a>
<a href="#">DRM User2</a>	Second DRM User	0	<a href="#">Change services</a>

- [Add a new DRM UserID/Password user](#)
- [Add a new DRM certificate user](#)
- [Services list](#)

## Managing assignments for a DRM admin user



The screenshot shows the 'Change Services' page in the Government Gateway. The page has a dark red header with the 'Government Gateway' logo on the left and a photograph of a group of people on the right. A gold sidebar on the left contains a navigation menu with the following items: Services, Your details, Your assistants, Manage users, Manage DRM users, Help, and Log out. The main content area is white and features a gold header with a checkmark icon and the text 'Change Services'. Below this, it says 'Services for: DRM User1'. A paragraph explains that users can change services assigned to a selected user. A checkbox is checked for 'Test Service 1 for Organisation' with the identifier 'ORG1GUID1 : \*\*\*'. At the bottom, there are two buttons: 'Back' and 'Change Services'.

Government Gateway

Change Services

Services for: DRM User1

From this page you can change the services assigned to the selected user. If any single user in your group has enrolled for a service, it is possible for other users to carry out the service as well.

Test Service 1 for Organisation  
ORG1GUID1 : \*\*\*

Back Change Services

## Delegating rights

- New method GsoDelegateRights has been added to the endpoint <https://secure.gateway.gov.uk/soap/2007/02/delegatedrights>
- This method uses WS-Security and requires a WS-SecurityToken in the header.
  - In addition to the security token, the method uses an IRMark style hash of the body as the nonce for the security token.
- Requests must contain at least one valid direct enrolment or one valid client allocation. Requests not meeting the minimum criteria will have a SOAP fault returned.
- Requests that contain at least one valid direct enrolment or client allocation and one or more invalid enrolments will result in a delegated session being created and the following returned:
  - Onetime token
  - List of invalid direct enrolments or client allocations

## Authenticating using the Common Authentication Portal

- New endpoint  
[https://authenticate.gateway.gov.uk/protocols/\[Protocol\]/delegaterights.aspx](https://authenticate.gateway.gov.uk/protocols/[Protocol]/delegaterights.aspx)
- In addition to standard protocol semantics the endpoint requires the following two parameters:
  - token – the onetime token issued by GsoDelegateRights
  - signOutUrl - the URL to redirect the browser to, when SSO sign out is complete
- If the CAP successfully authenticates using the onetime a protocol specified SAML assertion is returned.
  - Applications using WS-Federation can chose to use the generic target resource <http://www.gateway.gov.uk/2008/02/delegated>. The SAML assertions returned for the generic TR cannot be used for Gateway Authentication.
  - SAML and Liberty ID-FF will need to create specific target resource
- If the CAP is unable to authenticate a protocol specified error is returned.

# Technical Overview

Questions?