Automated Energy Data

Interface Design

Energy Comparison

Presented by
Ian Banner
ian.banner@bigagilityinstitute.com
+447734606555

Contents

1 Introduction and Context
2. Key Points Summary
3 Technical Approach
3.1 Overview
3.2 Application Flow
3.3 Using OAuth2
3.3.1 Setup and Registration
3.3.2 Identity and Authentication
3.4 Consideration of NFRs
4 User Interaction - Principles and Patterns
4.1 Consumer Interactions – Principles & Design Patterns
5 Data Considerations
5.1 Payload Information Specification
5.2 Payload JSON Specification
5.3 Payload Patterns
Transport (HTTPS)
REST Services
End point
Protocol
Access token
5.4 Flow and Examples
Data Provider Endpoints and Versioning
Resource: supply-details
Responses
6 Out of Scope

1 Introduction and Context

The Ministerial Roundtable on 29 October 2014 reviewed recommendations for how to implement energy data access to third parties with consumer consent, for consumer benefit. The roundtable confirmed the scope of the data to be accessed, and agreed an additional item of work to iterate the detailed definition of how a consumer would be identified to their energy provider during the customer journey.

The purpose of this document is to format the design recommendations from the Data Access In Energy Recommendations Report, updated for the Roundtable review, into a document that each energy supplier can use as the basis for individual internal designs.

The key items agreed at the roundtable, and how they are addressed in this document are as follows:

Firstly, to enable energy suppliers to reuse elements of their current online account creation/logon solutions to enable consumer identification whilst minimising friction by doing so in such a way that does not require the customer to sign up to full online account management.

To enable the balance of flexibility and user experience, a design pattern rather than a detailed design is specified in this document.

Suppliers will be asked to agree to the design pattern, and then implement to the pattern reusing individual current solutions. The customer identification process pattern will allow suppliers appropriate flexibility in how they choose to identify their customers. The design pattern is defined in Section 5.

The **second key agreement** was to exclude the requirement for energy suppliers to include usage estimates for customers with less than 12 months tenure. The API design specification in section 6 has been updated to reflect this agreement.

Whilst no other areas of the design have been changed, further clarity has been provided in Section 4 following additional feedback from technical teams during the production of this document. For clarity also, whilst these have not changed, non-functional requirements have been included to reflect the discussions held during the impact assessment phase.

The overall objective of this document is to specify in enough detail, the parameters and information flow for the data access to enable energy providers and third parties with the necessary information to carry out individual detailed designs, build and testing for the creation of live services to specified production volumes.

2. Key Points Summary

This document builds on and clarifies the design statements made in the paper 'Automated Energy data report for IA' - all readers should ensure they have a copy of that paper available for reference

The requirements that this service needs to meet are described with the following user story

User Story	How will we know this is done?	Notes
AS AN energy user **I WANT** to be shown energy tariff options and recommended cheapest tariffs based on accurate information about my usage **SO THAT** I can make an informed choice on the best tariff for me.	User clicks to an energy tariff comparison website User indicates current energy provider Eligibility checks take place User is passed to energy provider portal where Energy Provider validates user and passes the required data to energy tariff site User is shown options for where to move to and savings available	Delivery of the service affects both energy supplier and 3rd party switching websites.

Design patterns and principles have been established to clarify the Roundtable agreement for flexibility in user authentication. This design pattern is contained in section 4. The key summary of these is:

1. User interaction is atomized.
2. It is not mandatory to complete a full online account set-up to authorise a midata payload to a comparison site.
3. User should, when handed off to the Data Provider, be shown only the screens necessary to identify themselves and authorise a payload transfer. (This is an extension of point 1 above)

The JSON specification has been improved to indicate when certain items will appear and names of data items has been improved for clarity. This includes the agreement on estimating for less than 12 months.

Non Functional requirements, previously available on the shared space, Basecamp, have been included for clarity.

3 Technical Approach

3.1 Overview

The solution uses a standard OAuth application flow but with the options of a modified context to improve consumer convenience and openness.

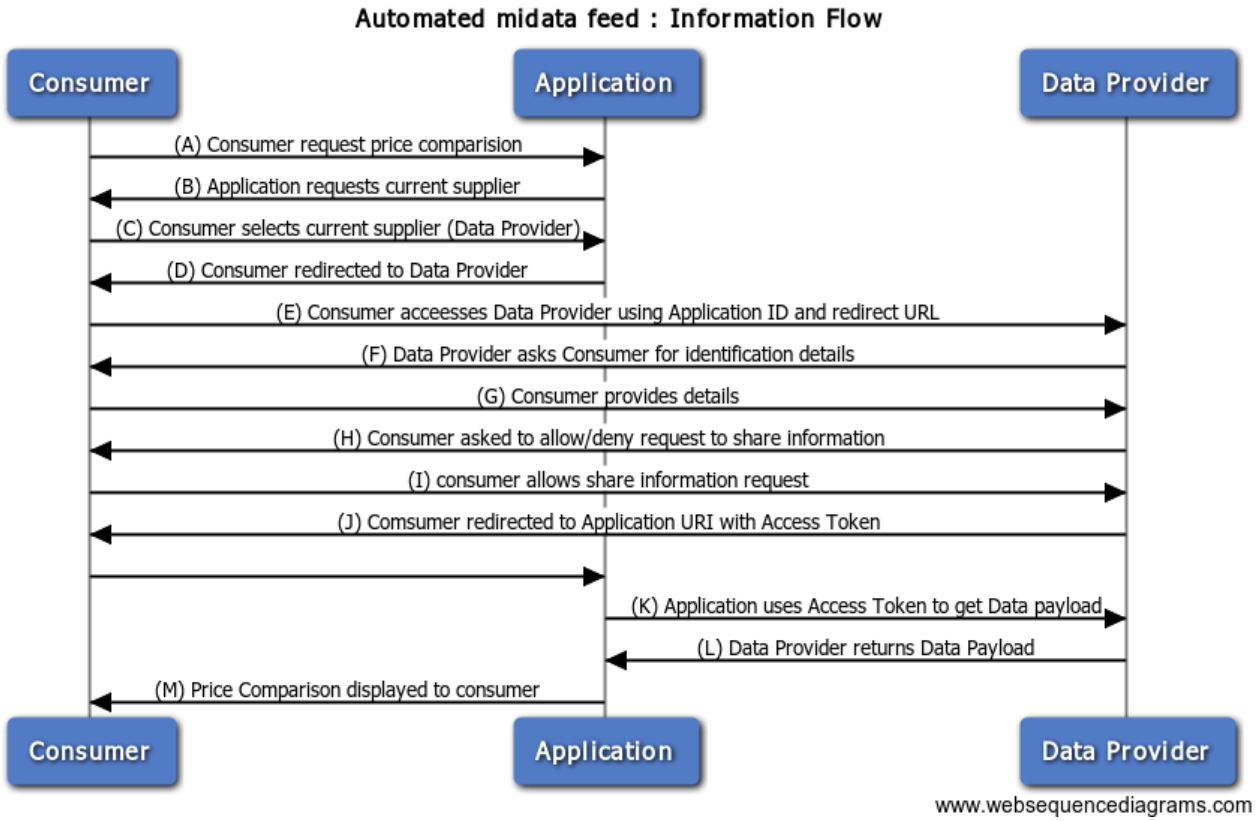
Solution builds on on commonly available technologies (OAuth, JSON, HTTPS) to support minimum development time. These standard technologies are supported in most utility and switching companies.

3.2 Application Flow

The diagram below describes a standard use of OAuth2 to ensure that a secure, transient trust relationship can be established between 3 entities to transfer data from the Provider to the Application. Importantly the Consumer remains in control of the transfer at points

- Consumer Provides details
- Consumer asked to allow/deny request to share information
- Consumer allows share information request

As part of the governance framework there is a requirement to create a registration between the application and Data Provider pair. This assumption is noted below



3.3 Using OAuth2

The security model suggested uses OAuth2 and has 3 distinct lifecycle phases:

1. Setup and Registration
2. Identity and Authentication
3. De-registration

Full details of the Outh2 specification are available at http://oauth.net/2/

3.3.1 Setup and Registration

Data Provider: Before the service can be deployed and made accessible the Data Provider must configure the OAuth2 framework for the service. This involves:

1. Preparing the OAuth2 authorisation services and authentication schemes
2. Preparing the supply-details endpoint
3. Defining the OAuth2 scope for the supply-details endpoint

Application (for framework choices A & C only): Before using the API, the Application

developer must obtain a client id. To do this they must register the Application with the Data Provider and provide the Application's callback URI.

The Data Provider supplies the Application developer with a client_id and a valid scope for interacting with the API.

3.3.2 Identity and Authentication

The OAuth2 specification details four flows (RFC 6749). The flow referred to in this document is the Implicit (simplified flow).

1. The Application redirects the Consumer to the Data Provider.
2. The Consumer signs-in and authorises access to supply details.
3. The Data Provider sends an Access Token to the Application.
5. The Application uses the Access Token to access supply details.

It should be noted that:
1. The Consumer never reveals security information to the Application.
2. The Access Token only allow access to the Consumer's supply details. No other information can accessed.

3.4 Consideration of NFRs

The table below summarises the design discussions with the project on the shared space, Basecamp. These are included here for summary purposes are indicative of volumes, the full design response should indicate these can be met.

Requirement	How will we know this is done?	Notes
Volume transactions of this service will be low. No more than 30 transactions per hour peal. Daily Average total will be 100 transactions	Review of solution by Design Authority Current live web services demonstrated to be unaffected Peak performance test carried out in Unit and Integration test cycles	It is assumed that all transactions moved to this service for energy providers will come from other business traffic and therefore no changes need to be made to current SLAs for transaction for live service, nor systems and software/hardware that these services are delivered upon.
SLA for service to match current web service of providers	Review of solution by Design Authority	This means if your web service is available 24/7, then this service should be available the same. Necessary down times for maintenance and upgrades are accepted. It is agreed that this service will be part of energy providers standard web services and will therefore be affected by issues that affect other live services in the same category

4 User Interaction - Principles and Patterns

The following list of agreed principles and patterns have already been agreed as part of the round table discussions, these are stated for clarity

4.1 Consumer Interactions – Principles & Design Patterns

Principle 1 - Customer interaction should be atomized.

This means the transaction interaction described above is seen as a single simple transaction to the consumer, the identification of themselves in a relevant way to the Data Provider is a simple steps within an entire transaction serviced by the user story.

Consequence of this principle is that the user is not presented during this interaction with a need to register for full online account management to collect the data, nor is the user moved to a retention interaction by the Data Provider and not returned to the comparison site.

Principle 2 - The interaction should be described as seen by the user as simple, straight forward and fast.

Principle 3 - It is not mandatory for the consumer to register for full online account management in order to authorise the payload to be passed to the 3rd Party application.

Two options for customer identification:

Principle 4 - If the user is already registered as an online user with the Data Provider, they can use the user ID and password already registered, although it is not mandatory to use it.

Principle 5 - The user can alternatively identify themselves by providing the information that the data provider currently uses as part of online account set-up.

To do this, an example of this fact matching approach could be to use:

- Account Number or Payment Card details
- Last Name
- Post Code

However, the decision on the final fact matching data set rests with the individual data provider.

Note that Principle 5 is based on the agreement at the most recent Roundtable summarised by Jim Poole from EDF that it is important that consumers could do this in one seamless transaction. Jim proposed and the Roundtable agreed that a work around was allowing the customer to notionally create an online account from a three facts combination. However, from the

perspective of the consumer this would be no different to a simple three facts authentication process. "

Principle 6 - Information/communication provided to consumers about the data they are sharing (how long this will be kept, how often it will be accessed, what period of time it will be accessed for) should be clear, simple and informative .

Principle 7 - The data provider site should be recognisable as the data provider, but the necessary interaction required to fulfill the user story should be clearly available.

This means the user could complete a sign on process if they are already identified as an online customer of the data provider, but the response to the sign on process should not be the standard screens. It should be only a screen to give authority for the data package share.

Principle 8 : Both price comparison and data provider screen designs should follow best of class design interactions.

Most price comparison and energy suppliers will have web standards, including areas such as:

1. Responsive design vs mobile specific design (either is valid)
2. Consistent appearance across operating systems (iOS, Android, OSX and Win 8)
3. Consistent appearance across browsers (e.g. Safari 10.6 onwards, IE8, Chrome, Firefox)

In the detailed design the energy supplier should indicate and reference their design standards in this area

5 Data Considerations

5.1 Payload Information Specification

The application flow is described above in section 4.2

The information specification of fields in the payload (taken from 'Automated Energy data report for IA)) is as follows **(shown here for context)**

Fields Specified in the midata Specification

Field Name (field reference in payload)	**Description**
Post Code (postcode)	Postcode of the customer property where the energy is provided.
Current Provider (currentProvider)	Name of the current energy supplier
Current Electricity Tariff (currentTariffName)	Name of the current electricity tariff the consumer is on
Current Gas Tariff (currentTariffName)	Name of the current gas tariff the consumer is on
Current Electricity Payment Method (currentPaymentMethod)	Current method of electricity bill payment
Current Gas Payment Method (currentPaymentMethod)	Current method of gas bill payment
Meter Point Admin No. (MPAN) (mpan)	MPAN of the electricity meter
Meter Point Reference No. (MPRN) (mprn)	MPRN of the gas meter
Annual Electricity Usage (historicAnnualConsumption)	Historical electricity usage in kWh over the previous 12 months of data creation date. **NOTE:** Only available after a consumer has been with the current energy supplier for over 12 months. Empty otherwise.
Annual Gas Usage (historicAnnualConsumption)	Historical gas usage in kWh over the previous 12 months of data creation date.

	NOTE: Only available after a consumer has been with the current energy supplier for over 12 months. Empty otherwise.
Start Date (startDate)	Start date of the contract with the current energy supplier

From the original IA:

Additional Fields Need for Comparison[1]

Field Name (field reference in payload)	**Description**
Payload Creation Date (payloadCreationDate)	Date when the payload message was created. i.e. usually this is the date of the payload request and reply
Last Updated Date (lastUpdatedDate)	Date the data was last updated. e.g. For a monthly tariff customer this would be the last bill date. For a Pre-pay it could be the last (annual) account summary. The intention is to give some indication of how up to date the information is provided.
Estimate Annual Consumption - Gas (estimatedAnnualConsumption)	Future looking estimate of projected annual consumption in kWh for the Consumer. **NOTE:** Where a consumer has been with the current energy supplier for less than 12 months, this field may not contain any data.
Estimate Annual Consumption - Electricity (estimatedAnnualConsumption)	Future looking estimate of projected annual consumption in kWh for the Consumer. **NOTE:** Where a consumer has been with the current energy supplier for less than 12 months, this field may not contain any data.
Estimated Annual Cost - Gas (estimatedAnnualCost)	Future looking estimated of project annual cost to the consumer including VAT. **NOTE:**

[1] Agreement to add these to the information was made at the last round table meeting

	Where a consumer has been with the current energy supplier for less than 12 months, this field may not contain any data.
Estimated Annual Cost - Electricity (estimatedAnnualCost)	Future looking estimated of project annual cost to the consumer including VAT. **NOTE:** Where a consumer has been with the current energy supplier for less than 12 months, this field may not contain any data.
Contract End Date - Gas (contractEndDate)	Date the current contract is coming to an end
Contract End Date - Electricity (contractEndDate)	Date the current contract is coming to an end

5.2 Payload JSON Specification

The basic structure of the Payload

{
"midata": {
"energy": {
"comparison": {
"payloadCreationDate": "20140827",
"gas": {....},
"electricity": {....}
},
}
}
}
	• It is assumed each customer has no more than one gas or electricity supply with any energy provider
	• It is assumed that an energy provider could only be providing gas or electricity, in which case the relevant data section will not appear.
	• All dates are in YYYYMMDD format
	• All costs are provided to 2 decimal places, including decimal

Fuels
Each fuel is described in a similar way with a couple of exceptions. For gas, the MPRN is provided whereas for Electricity it is the MPAN. Example :

"gas": { "lastUpdatedDate": "20140801", "postcode": "XY123Z",	• mprn attribute is only valid for gas and is a string representation of the

<table>
<tr>
<td>


```
   "currentProvider": "British Gas",
   "currentTariffName": "Fixed April 2016 Direct
Debit ebill",
   "startDate": "20140115",
   "contractEndDate": "20160430",
   "currentPaymentMethod": "DD",
   "mprn": "0000000002",
   "historicAnnualConsumptionKwh": 13500,
   "estimatedAnnualConsumptionKwh": 14400,
   "estimatedAnnualCostincVatPounds": 415.35
}
```


</td>
<td>

industry service endpoint identifier

- postcode will be the postcode of the service and not the postcode of the consumer which can be different
- consumption is always providing in kwh not volume (m3 or cft3) for gas
- currentTarrifName is the desription of the Tarrif as it appears on the customer bill.
- historicAnnualConsumptionKwh is provided if the customer has been with the supplier for 12 months or more. Otherwise not provided.
- estimatedAnnualConsumptionKwh is provided if the customer has been with the supplier for 12 months or more, and should match the data used for RMR personal projections
- estimatedAnnualCostincVatPounds should include standing charge and is inc Vat. Calculation should be to agreed industry guidelines for customers leaving fixed period tariffs in the next 12 months
- Possible currentPaymentMethod values are "DD","CC","PP", "CQ" and "OT"
- These represent
  - DD = Any form of Direct Debit
  - CC = Credit Card
  - PP = Prepayment
  - CQ = Cheque or Cash
  - OT = Other

</td>
</tr>
</table>

An example for an electricity supply:

<table>
<tr>
<td>


```
"electricity": {
   "lastUpdatedDate": "20140801",
   "postcode": "XY123Z",
   "currentProvider": "British Gas",
   "currentTariffName": "Fixed April 2016 Direct
Debit ebill",
   "startDate": "20140115",
   "contractEndDate": "20160430",
   "currentPaymentMethod": "DD",
   "mpan": "00000000000001",
   "historicAnnualConsumptionKwh": 3200,
   "estimatedAnnualConsumptionKwh": 3090,
   "estimatedAnnualCostincVatPounds": 516.35
}
```


</td>
<td>

Design Notes

- All notes above for Gas supply apply here
- mpan attribute is only valid for electricity

</td>
</tr>
</table>

5.3 Payload Patterns

Transport (HTTPS)

The Data Provider and Application must have a valid SSL certificate which is not self-signed.

REST Services

End point

The endpoint at the Current Energy Supplier will be RESTful web service at the URL https://<...>/midata/v1/supply .

It will be available on the internet behind a firewall only accessible to third party providers with pre--registered credentials.

The REST web services endpoint will implement only the GET HTTP method.

The endpoint shall be considered:

1. Open to the extent that it is REST based, uses HTTPS for transport, has payload in JSON format and be available over the Internet.
2. Secure and Authorised to the extent that Third party Providers will have to register with energy provider to be approved for access to the endpoint.
3. Protected to the extent that only authorised Third party Providers can successfully access the endpoint. The Energy Supplier will deny unauthorized access to the endpoint to any request from non declared third parties.

Protocol

Oauth 2.0 will be the tripartite protocol used to gain consent from the consumer and transfer midata from the current energy supplier to the third party provider.

The third party provider is considered the client application, while the current energy supplier is considered the resource server. The consumer is the resource owner and the protected resource is the midata. The authorization server (possibly part of the resource server) is controlled by the current energy supplier and resides at their premises.

The resource owner (consumer) initiates interaction with the client (third party provider). The client redirects the resource owner to the authorization server (current energy supplier) to authenticate the resource owner. Once authenticated, the authorization server sends an access token to the client. The client uses that access token to query the resource server (current energy supplier) for the protected resource (midata). The protected resource is sent to the client over a secure channel.

Access token

Access tokens should be granted in accordance with RFC6749 and will consist of a random 128 bit hexadecimal string created as an MD5 hash of a string of 255 alphanumeric characters. e.g. e4d909c290d0fb1ca068ffaddf22cbd0. The access token shall be valid for 30 minutes from the time of issue wherein a third party provider can request the consumer's midata once with this token.

Additional requests, or requests outside the 30 minute period will require a new access token.

5.4 Flow and Examples

Implicit Flow: Obtaining an Access Token
To obtain an Authorisation Code, the Data Provider will redirect the Consumer to the Data Provider.

Example URL

```
https://dataprovider/api/oauth/authorize?client_id=ApplicationID&
response_type=token&redirect_uri=http%3A%2F%2Fapplication%3A8090%2Fauth%2Fredirect.jsp&
scope=supplydetails
```

In order to get a valid response the Applications client_id, redirect_url and scope will have to match the Data Providers configuration.

The application key and token are not to be passed in the query string.

If successful the Data Provider will respond with a redirect for the Consumer's browser to the Data Provider's authentication (sign-in) page. After the consumer is successfully authenticated and subsequently authorises access to their supply details, an access token is returned in a second redirect response `redirect_uri`, e.g:

```
HTTP/1.1 302 Found
     Location: http://example.com/cb#access_token=2YotnFZFEjr1zCsicMWpAA
               &state=xyz&token_type=example&expires_in=3600
```

After the Application has obtained the Access Token, it will be able to access resources on

the Data Provider by using it as a Authorization: Bearer header, for example:

```
GET /midata/energy/v2/supplydetails HTTP/1.1
Authorization: Bearer 123345678abcdefg
Host: dataprovider
```

Path	GET	PUT	REPLACE	DELETE
/midata/energy/v2/…				
supply-details	Y	N	N	N

Data Provider Endpoints and Versioning

- Data Providers will be responsible for publishing valid service resource location
- Applications will be responsible for maintaining a valid map of all of the service locations across all supported Providers
- In general it is proposed that the service URI will follow the general form:
  - /midata - represents the root node for all midata APIs
  - /midata/energy - represents those API specific to the energy sector
  - /midata/energy/v2 - the version of the API
- Specific data provider URI will obviously contain DNS/Host and port references that will differ between Providers

Resource: supply-details

path: /midata/energy/v2/supply-details

This supply-details resource provides a summary of a consumers energy supplier information.

Design Notes

1. Importantly there is no resource identifier provided in the URL structure as this is injected through the security context. This hides the identity of the consumer which should in turn discourage "grazing" attacks.

Responses

200 - returns a valid payload (below) in JSON format
401 - not called within a valid security context, or unable to identify consumer
404 - no valid information available for authorised consumer
500 - exceptions causing failure for any other reasons
503 - service unavailable

Design Notes

1. 401 should only be returned if authentication fails using anyone of the allowed authentication schemes that will be defined over time. Initially it is thought that all data providers should provide a "fact-matching" scheme. However suppliers may also want to allow authentication by existing online credentials or social media credentials linked to their online accounts.
   a. importantly consumers who are pre-ssd or post-sed can be authenticated by the security layer.

See 404 as to why this is significant.

2. 404 should only be returned if there is no valid data on file for the authenticated consumer. For this service, this may be because either the consumer is too new or has left the supplier or if there is an open dispute about the consumption data on file.
3. All error conditions may contain a plain text narrative to help problem diagnosis which should be logged by the application and the data provider. We have avoided trying to provide structured error codes as the effort required to agree a standard model across all suppliers outweighs the value that would be added to the primary use case. This can be reconsidered as part of a future revision.

6 Out of Scope

For the avoidance of doubt , the following are outwith the scope of this interface design

1. Any work on establishing a Trust Charter for the UK energy Industry
2. The registration of comparison sites, along with secure URL redirects.
3. The 'code' or 'catalogue' of tariffs and price points across the industry
4. Comparison of energy performance across similar properties
5. Ways to become more efficient in your energy consumption
6. Proposals for implementation of the system, including test phases and timelines
7. On going central support role for point 6 above
8. Period Billing Assessment and the effect this has on data quality of usage or future usage predictions.
9. No understanding of potential cancellation fees as part of the price comparison. This will need to be developed in further iterations of this standard.
10. Complex customers with more than one account, therefore holding several properties with fuel agreements
11. Customers with more than one mpan or mprn at a single supply address.