ID Assurance
Attribute Provider
Service Definition

Prepared by: Richard Mardling
Date: 23rd September 2013

For enquiries regarding this document, please contact:

**European Head Office:**
Olympian Trading Estate, Cayton Low Rd
Scarborough, North Yorkshire, YO11 3BT
www.aurionpro.com
Contributors

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Telephone</th>
<th>E-mail Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Richard Mardling</td>
<td>Strategic Business Director</td>
<td>0844 800 1985</td>
<td><a href="mailto:richard.mardling@aurionpro.com">richard.mardling@aurionpro.com</a></td>
</tr>
<tr>
<td>Steve Ford</td>
<td>Principle Consultant</td>
<td>0844 800 1985</td>
<td><a href="mailto:steve.ford@aurionpro.com">steve.ford@aurionpro.com</a></td>
</tr>
<tr>
<td>Robbie Cruickshank-Sutton</td>
<td>Account Manager</td>
<td>0844 800 1985</td>
<td><a href="mailto:robbie.cruickshanks@aurionpro.com">robbie.cruickshanks@aurionpro.com</a></td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date Issued</th>
<th>Status</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>17th Sept ‘13</td>
<td>Draft</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>23rd Sept ‘13</td>
<td>Release</td>
<td></td>
</tr>
</tbody>
</table>

This document will be kept under revision control

Intellectual Property Rights

The material contained in our response, and any material or information disclosed during discussions of the proposal, represents the proprietary, confidential information pertaining to Aurionpro Solutions’ services, methodologies and methods. Other products and brand names may be trademarks or registered trademarks of their respective owners.

By accepting this response, [client name] agrees that the information in this proposal will not be disclosed outside the organization and will not be duplicated, used, or disclosed for any purpose other than to evaluate this proposal. This proposal is subject to a mutually approved agreement or contract specifying full terms and conditions.
# Contents

Executive Summary.................................................................................................................. 1

1.1 Overview of Identity (ID) Assurance Attribute Provider.................................................. 1

1.2 Overview of Aurionpro Solutions plc.................................................................................. 1

1.3 Investment Summary........................................................................................................... 2

Project Definition....................................................................................................................... 3

1.4 Overview of ID Assurance Attribute Provider.................................................................... 3

1.5 Use of Open Source.............................................................................................................. 5

1.6 Capacity ............................................................................................................................ 5

1.7 Test Environment................................................................................................................ 5

1.8 Information assurance......................................................................................................... 6

1.9 On-boarding processes....................................................................................................... 6

1.10 Off-boarding processes.................................................................................................... 6

1.11 Service Management details........................................................................................... 6

1.12 Service Levels................................................................................................................... 9

Pre-requisites............................................................................................................................ 10

1.13 Technical requirements.................................................................................................... 10

1.14 Details of any trial service available.................................................................................. 10

Investment Details...................................................................................................................... 11

1.15 Pricing............................................................................................................................... 11

1.16 Limitations of the Test Service......................................................................................... 12

1.17 Example calculations......................................................................................................... 12

1.18 Ordering and invoicing process......................................................................................... 13

Commercial Notes.................................................................................................................... 13

1.19 Financial recompense model ........................................................................................... 13

1.20 Termination terms.............................................................................................................. 14
Executive Summary

1.1 Overview of Identity (ID) Assurance Attribute Provider

The identity attributes that are provided by an IdP are not always sufficient for the purposes of the Service Provider. Attribute Providers and Service Provider Matching Services can be used to either enhance the SAML assertion or confirm the presence of a local record.

Aurionpro Solutions plc's (Aurionpro) Identity (ID) Assurance Attribute Provider:
- Receives and processes SAML 2.0 Attribute Query messages as issued by the Hub
- Undertakes a search to provide extra attributes or confirms a match
- Returns values using the SAML 2.0 Response messages allowing the Hub to undertake identity enrichment (claims transformation)
- Logs transactions within an open source MySQL database

The interface with the local identity store may require some integration work, the scope of which will need to be defined on a per installation basis.

1.2 Overview of Aurionpro Solutions plc

Aurionpro Solutions plc (Aurionpro) provides Advisory, Implementation and Managed Services Consulting in the Identity and Access Management domain to both public sector and corporate organisations in the UK. We offer complete lifecycle services in this area including strategy, architecture, custom development, implementation, project management and managed support. Our UK based team of dedicated consultants hold manufacturer and industry recognised accreditations including CISSP, ITIL, SSCP and HM Government clearances.

Placing emphasis on delivering business benefit by improving user satisfaction and on cutting costs through increased operational efficiency, we provide solutions to public sector organisations that: reduce Service Desk calls, facilitate information sharing within partnerships, secure remote access, streamline the User Lifecycle Management process and enable user self service for administrative functions.

With an Identity and Access Management division established since 1998, we are both a Microsoft Gold Identity and Security Partner and an Oracle Gold Partner, specialized in Identity Administration and Analytics. The prestigious Oracle partner awards we have won are testament to our expertise in delivering a range of different identity and security projects. These include multi-year TITAN Award Winners, Oracle Technology Specialist Partner of the Year and the Oracle Partner Network Specialized Middleware Partner of the Year Award for EMEA.
1.3 Investment Summary

<table>
<thead>
<tr>
<th>Bandings - based upon cumulative transactions per AtP per quarter</th>
<th>Charge per transaction - Basic Managed Support</th>
<th>Charge per transaction - Enhanced Managed Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;=10,000</td>
<td>£0.0400</td>
<td>£0.0500</td>
</tr>
<tr>
<td>&lt;=50,000</td>
<td>£0.0320</td>
<td>£0.0400</td>
</tr>
<tr>
<td>&lt;=100,000</td>
<td>£0.0256</td>
<td>£0.0320</td>
</tr>
<tr>
<td>&lt;=1,000,000</td>
<td>£0.0205</td>
<td>£0.0256</td>
</tr>
<tr>
<td>&lt;=10,000,000</td>
<td>£0.0164</td>
<td>£0.0205</td>
</tr>
<tr>
<td>&gt;10,000,000</td>
<td>£0.0132</td>
<td>£0.0165</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup fee per Attribute Provider instance</td>
<td></td>
</tr>
<tr>
<td>- Level One organisation</td>
<td>£21,000</td>
</tr>
<tr>
<td>Setup fee per Attribute Provider instance</td>
<td></td>
</tr>
<tr>
<td>- Level Two organisation</td>
<td>£28,500</td>
</tr>
<tr>
<td>Setup fee per Attribute Provider instance</td>
<td></td>
</tr>
<tr>
<td>- Level Three organisation</td>
<td>£46,000</td>
</tr>
<tr>
<td>Minimum Quarterly Transaction Charge</td>
<td>£600</td>
</tr>
<tr>
<td>Charge to connect an additional federation hub to the Attribute Provider</td>
<td>£2,500</td>
</tr>
<tr>
<td>Provision of an individual Test Service</td>
<td>£20,000</td>
</tr>
</tbody>
</table>

**Organisation definition**

<table>
<thead>
<tr>
<th>Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level One</td>
<td>&lt;= 1,000 employees</td>
</tr>
<tr>
<td>Level Two</td>
<td>&lt;= 10,000 employees</td>
</tr>
<tr>
<td>Level Three</td>
<td>&gt; 10,000 employees</td>
</tr>
</tbody>
</table>

For full details, please see section 1.15. Please see also Aurionpro Solutions plc SFIA Rate Card Lot 3.
Project Definition

1.4 Overview of ID Assurance Attribute Provider

The core attribute provider is built around Oracle technologies running on a Linux platform and provides a modular and scalable mechanism for a federation hub to request additional attributes from an identity store in order to enrich the SAML assertion. MySQL is used as a logging repository and the primary source of service status information. It is fully SAML 2.0 compliant to ensure maximum compatibility with existing federation solutions.

The solution as described does not prescribe a hosting environment or deployment platform. The solution may be hosted in any IL3-certified environment assuming that the technical pre-requisites are met and can be deployed on either physical or virtual hardware. The required hardware specifications are dependent on the expected user load and the number of connected federation hubs and will be determined prior to implementation. Provision of suitable hardware is not included as part of the solution.

At a high level the architecture looks like this:

1. A user requests access to a cloud-hosted Service Provider.
2. The Service Provider requires authentication and redirects the request to the Federation Hub using a SAML2.0 Authentication Request.
3. The Hub checks to see which Identity Providers are trusted by the Service Provider. If more than one IdP is trusted, the user is prompted to choose which one they'd like to use. Note that the external Policy Store could also be used to determine the correct IdP on a per-user or per-Service Provider basis at this point.
4. A SAML 2.0 Authentication Request is sent to the selected Identity Provider.

5. IF the user has previously authenticated in the same session, the user is NOT required to re-authenticate and a new authentication token is issued. If no valid authentication session exists, the user is prompted to provide their username and password (or whatever credentials are required by the selected IdP).

6. The user’s credentials are checked against the Identity Store and a new authentication token is generated.

7. The token is returned to the Hub as a SAML2.0 Authentication Response.

8. The Hub checks the (internal) Policy Store to determine whether the Service Provider requires additional user attributes. If not, go to step 12.

9. A SAML2.0 Attribute Query request message is sent to the Attribute Provider.

10. The required user attributes are retrieved from the Attribute Store.

11. The attribute assertion is returned to the Hub in a SAML Response message and incorporated into the authentication assertion.

12. A SAML2.0 Authentication Response returns the token to the service provider which performs whatever internal functions are necessary.

13. The user is granted access to the service.

Internal architecture of the ID Assurance Attribute Provider:

![Figure 2: ID Assurance Attribute Provider Internal Architecture]
The Attribute Provider receives and processes SAML 2.0 Attribute Query messages as issued by a federation hub. It then undertakes a search according to the agreed policy of an external identity store in order to retrieve additional attributes or confirm a match. Any additional attributes are returned to the federation hub using the SAML 2.0 Response messages. The federation hub is then able to undertake identity enrichment (claims transformation). The external identity store can be a user directory e.g. Microsoft Active Directory, a virtual directory, a database or a MDM.

1.5 Use of Open Source

The ID Assurance Federation Hub (adjust as appropriate) uses a number of Open Source components, namely:-

- Linux operating system
- MySQL for the Accountancy database
- Java for scripting within the Hub / Attribute Provider

1.6 Capacity

The ID Assurance Attribute Provider as specified with a single gateway and given sufficient resource headroom on the host server is capable of handling approximately 50,000 I/O transactions per second subject to the specification of the hosting environment. Incorporating additional workflow activities may significantly reduce this number depending on the additional steps a request must pass through. The service can be easily scaled up to support additional workload through the deployment of additional Gateway components (all of which can share the same configuration/policy) with load-balancing technology at the point of access.

Aurionpro will customise a capacity management plan for your requirements based on the applications deployed and the environmental constraints placed on the system. The plan will include details for up/down scaling of your environment as needed. Ideally you have information about the levels of activity that components of the application are expected to meet, such as:

- The anticipated number of and size of requests from the federation hub(s).
- The number of concurrent sessions.
- The number of SSL connections required.
- The amount of data and its consistency.
- Determining your target CPU utilisation.

Performance objectives are limited by constraints, such as:

- The configuration of hardware and software such as CPU type, disk size versus disk speed, sufficient memory and network throughput.
- The ability to interoperate between domains, use legacy systems, support legacy data.
- The security requirements and use of SSL. SSL involves intensive computing operations and supporting the cryptography operations in the SSL protocol can impact the overall performance.
- Development, implementation, and maintenance costs.

1.7 Test Environment

Test environments can be provided by Aurionpro, please see section 4.1 for further details.
1.8 Information assurance

The Hub service as described in this document does not store any information which might be considered to be privileged under the Government IL specifications.

1.9 On-boarding processes

During the initial setup process the ID Assurance Attribute Provider will be configured to interoperate with a customer nominated federation hub. The customer will need to provide the following details pertaining to their federation hub:

- Sign-in URL – the federation hub server
- A copy of the Signing certificate
- A copy of the Encryption certificate (if used)
- A unique Realm identifier
- The metadata URL for the relevant federation hub

1.10 Off-boarding processes

Due to the overall design of a federation infrastructure, on and off-boarding components do not require data extraction / removal processes. Once a customer no longer requires the use of the ID Assurance Attribute Provider, then the server instance, along with the Accounting Database will be destroyed using the hosting organisation’s removal tools.

1.11 Service Management details

Aurionpro offer Basic and Enhanced Managed Support, with the price per user varying to reflect the increased level of service:

- Basic covers normal business hours.
- Enhanced covers 24/7 hours for priority 1 support issues.

Aurionpro will provide problem analysis and technical break fix managed support for the ID Assurance Attribute Provider as defined in section 1.4. The service is limited to the Attribute Provider and does not include any components provided by the hosting organisation. Our service provides customers with peace of mind by ensuring 24x7x365 monitoring and management, service desk and sustaining engineering capabilities.

Our SLA driven service consists of:

Service Availability Management – Daily health checks, maintaining BAU.

Break-fix Support– Offers the route and framework through which a defined selection of updates to the system could be delivered, providing a break/fix service based on a agreed to schedule.

Incident and Change Management – Receiving and recording issues/incidents/service tickets, defining severity levels and triage, investigation and analysis, resolution and recovery, closure.

**Account Management** – Maintaining the client relationship and providing regular analysis on all activities, identifying areas for service improvement.

**Service Functions**

The table below defines the relationships between Aurionpro and the customer’s representatives:

The Relationship Manager and SLA Manager are our nominated team members with specific responsibility for liaising with your organisation.

- The Relationship Manager is responsible for strategic governance of the service management, effectiveness of the service delivery and customer satisfaction. This function is delivered from the same location as that of the customer organisation.
- The SLA Manager is responsible for maintaining the defined service levels and in turn manages the support team to ensure overall delivery of the service.

**Managing Incidents and Service Requests**

The highlights of this process are:

- ITIL compliant, ISO9001 certified managed support desk manned by industry accredited engineers.
- Receiving and Recording of Incidents/Service tickets. These can be raised via telephone, email or through a self-service portal.
- The incident logging system is also available online for customers to view, raise and update incidents.
- Classification of severity levels and initial support
- Issue Investigation/ Initial Analysis
- Resolution and recovery, as required
- Ticket closure, with feedback from client

This process enables us to track, monitor and communicate progress on the issues and service tickets that are reported to our service desk. After a ticket has been raised has been reported, Aurionpro will work within the defined SLAs to close the ticket.

During this period a pre-agreed representative from the customer organisation may be requested to carry out tasks in order for progress to be made – this must be carried out within a reasonable time and feedback given to the Aurionpro Managed Support team as soon as possible.
response times will be suspended whilst waiting for the response back from the customer.

Aurionpro may need remote access to the customer’s hosting environment in order to effect investigations and resolutions. The customer organisation must ensure that secured remote access is made available to Aurionpro in order for this work to be carried out.

The following illustrates a typical workflow for ticket allocation and management.
1.12 Service Levels

<table>
<thead>
<tr>
<th>Standard</th>
<th>Enhanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>• P1 calls 09:00-17:30</td>
<td>• P1 calls 24x7x365</td>
</tr>
<tr>
<td>• P2 calls 09:00-17:30</td>
<td>• P2 calls 09:00-17:30</td>
</tr>
<tr>
<td>• P3 calls 09:00-17:30</td>
<td>• P3 calls 09:00-17:30</td>
</tr>
<tr>
<td>• P4 calls 09:00-17:30</td>
<td>• P4 calls 09:00-17:30</td>
</tr>
<tr>
<td>• 2 Authorised Customer Contacts</td>
<td>• 4 Authorised Customer Contacts</td>
</tr>
</tbody>
</table>

1.12.1 Severity Levels and Response Times

<table>
<thead>
<tr>
<th>Criticality</th>
<th>Initial Response</th>
<th>Incident Update</th>
<th>The Companies Action To Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority 1</td>
<td>Within one (1) hour.</td>
<td>At least every four (4) hours.</td>
<td>The Company to work continuously both within and outside Working Hours, until problem resolved.</td>
</tr>
<tr>
<td>Priority 2</td>
<td>Within four (4) Working Hours.</td>
<td>At least every Working Day.</td>
<td>The Company to work continuously within Working Hours, until problem resolved.</td>
</tr>
<tr>
<td>Priority 3</td>
<td>Within twelve (12) Working Hours.</td>
<td>Last Working Day of each week.</td>
<td>The Company to use all reasonable efforts to resolve problem within ten (10) Working Days.</td>
</tr>
<tr>
<td>Functionality Enhancements</td>
<td>Within 1 week</td>
<td>Last Working Day of each month (or as agreed between the Company Support and Customer at time of incident logging)</td>
<td>The Company to provide a time and cost estimate to customer within 2 weeks of Incident being raised.</td>
</tr>
</tbody>
</table>

Priority 1 - Customer is unable to do production work or production is jeopardized and a Workaround is not available or is generally unacceptable.

**All Priority 1 incidents must be raised by telephone**

Priority 2 - A major Software function is inoperable but production work can continue.
Priority 3 - Loss of a function which does not seriously affect operation

Priority 4 - Functionality Enhancements (These are passed to Manufacturer and costs may apply)

* On any occasion where no immediate configuration enhancement or data change can affect the issue raised by the client, it may be necessary to introduce a temporary work-around whilst a resolution is investigated, tested, and implemented. This ‘work-around’ will be designed to ensure that functionality continues to be available whilst the issue is resolved, but may involve changes to the implementation of manual processes at the client site. This work-around will be tested and verified in a local test environment before applying to the Production environment. Where such a work-around is proposed by Aurionpro, projected completion date for the implementation of the resolution will be given. With regards to achievement of Service Level, a temporary workaround will be deemed as satisfactory.

** In the event that any P1/P2/P3 issue is reported during the same time as a P4 (Query/Admin request) request, the Query/Administrative request will be attended to only when the P1/P2/P3 issue(s) are resolved; the P4 SLA response time in such cases may vary from what is stated in the above table.

*** All Testing, UAT and development environment issues will be treated as P4 issues.

All support and monitoring services are located, staffed and managed entirely within the UK.

1.13 Technical requirements

Any federation hub that will be exposed to the ID Assurance Attribute Provider must be capable of issuing and receiving SAML 2.0 Attribute Query messages for the purposes of identity matching and enrichment.

1.14 Details of any trial service available

No trial versions are currently available.
Investment Details

1.15 Pricing

Please see also Aurionpro Solutions plc SFIA Rate Card_Lot 3.

<table>
<thead>
<tr>
<th>Bandings - based upon cumulative transactions per AtP per quarter</th>
<th>Charge per transaction - Basic Managed Support</th>
<th>Charge per transaction - Enhanced Managed Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;=10,000</td>
<td>£0.0400</td>
<td>£0.0500</td>
</tr>
<tr>
<td>&lt;=50,000</td>
<td>£0.0320</td>
<td>£0.0400</td>
</tr>
<tr>
<td>&lt;=100,000</td>
<td>£0.0256</td>
<td>£0.0320</td>
</tr>
<tr>
<td>&lt;=1,000,000</td>
<td>£0.0205</td>
<td>£0.0256</td>
</tr>
<tr>
<td>&lt;=10,000,000</td>
<td>£0.0164</td>
<td>£0.0205</td>
</tr>
<tr>
<td>&gt;10,000,000</td>
<td>£0.0132</td>
<td>£0.0165</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup fee per Attribute Provider instance</td>
<td>£21,000</td>
</tr>
<tr>
<td>- Level One organisation</td>
<td></td>
</tr>
<tr>
<td>Setup fee per Attribute Provider instance</td>
<td>£28,500</td>
</tr>
<tr>
<td>- Level Two organisation</td>
<td></td>
</tr>
<tr>
<td>Setup fee per Attribute Provider instance</td>
<td>£46,000</td>
</tr>
<tr>
<td>- Level Three organisation</td>
<td></td>
</tr>
<tr>
<td>Minimum Quarterly Transaction Charge</td>
<td>£600</td>
</tr>
<tr>
<td>Charge to connect an additional federation hub to the Attribute Provider</td>
<td>£2,500</td>
</tr>
<tr>
<td>Provision of an individual Test Service</td>
<td>£20,000</td>
</tr>
</tbody>
</table>
Organisation definition

<table>
<thead>
<tr>
<th>Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level One</td>
<td>&lt;= 1,000 employees</td>
</tr>
<tr>
<td>Level Two</td>
<td>&lt;= 10,000 employees</td>
</tr>
<tr>
<td>Level Three</td>
<td>&gt; 10,000 employees</td>
</tr>
</tbody>
</table>

1. The setup fee includes:
   a. the establishment of the Attribute Provider within the chosen hosting environment
   b. connection to a single federation hub that is able to issue SAML2.0 Attribute Query messages
2. An instance of an Attribute provider is defined as one single Attribute Provider (according to the size of organisation – see table above) within a single data centre.
3. Charged on usage per quarter per Attribute Provider (in arrears) according to the appropriate banding and support levels with a minimum Quarterly Charge of £600.
4. A transaction (for chargeable purposes) is defined as the receipt and processing of a SAML2.0 <AttributeQuery> request message from an authorised federation hub. The transaction is denoted as being completed when the Attribute Provider issues a SAML2.0 <Response> message to the federation hub. A completed transaction could be either when the Attribute Provider is able to retrieve the requested attributes or it retrieves none of the requested attributes.
5. The setup and user fees do not include any integration with local or external identity stores. If such integration is required then please see Aurionpro Solutions plc Single Sign On service (refer to Aurionpro Solutions plc Single Sign On Service Definition document).
6. Support is provided to the contracting organisation i.e. the purchaser of the Attribute Provider and not the end user.
7. The setup and user fees do not include any hosting charges. This allows the customer to choose their own hosting provider and therefore utilise existing arrangements for their economic advantage.
8. A connecting federation hub will need issue SAML2.0 compliant <AttributeQuery> request message.

1.16 Limitations of the Test Service

1. It cannot be used for production purposes
2. Only connections with test / development instances of federation hubs and identity stores, will be permitted.
3. All Service Management calls will be classified as P4, unless otherwise agreed
4. Functionally identical to a production Attribute Provider
5. If any professional services are required to support integration or testing of the Test Attribute Provider then these can be purchased via Aurionpro Solutions plc Single Sign On service (refer to Aurionpro Solutions plc Single Sign On_Service Definition document).

1.17 Example calculations

For example calculations, please see Aurionpro ID Assurance Attribute Provider Rate Card.
1.18 Ordering and invoicing process

Aurionpro Solutions plc must receive a signed copy of a purchase order before any order can be accepted and processed. Any expenses to be charged must be detailed on a separate line. Purchase orders should be issued to “AURIONPRO SOLUTIONS PLC” and can be sent by post, fax or e-mail. Details are as follows:

**By post:**
Unit 4-5 Olympian Trading Estate
Scarborough
Y011 3BT
United Kingdom

**By fax:**
Fax number: 0844 800 3018 FAO: Sales

**By email:**
uksales@aurionpro.com
Format: pdf

---

Commercial Notes

1.19 Financial recompense model

The maximum unplanned service downtime shall be 43 minutes per calendar month for a planned availability of 99.9%.

Availability of the service is measured by the ability of the PSIIF Federation Hub to deliver a federation hub to the PSN.

The factors that will be excluded from any unplanned service downtime calculations are:

- End user accessibility caused by the their local network
- Unplanned downtime by the hosting organisation’s infrastructure e.g. servers, network, load balancers, storage
- IdP unplanned downtime / Identity Store unplanned downtime / SP/RP unplanned downtime

The Aurionpro Help Desk shall be used as the source of information for calculating Availability.

Availability will be measured and reported according to the following formula:

\[
\text{Availability} \% = \frac{(UT - DT) \times 100}{UT}
\]

Where:

UT: Total number of minutes in the relevant calendar quarter, excluding Planned Downtime
DT Total number of minutes of Unplanned Downtime in the relevant calendar quarter (excluding periods of scheduled maintenance)

Where service provision falls below the 99.9% availability level, the following service credits will become payable.

<table>
<thead>
<tr>
<th>Uptime Achieved</th>
<th>Applicable Service Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>98.90% to 90.00%</td>
<td>5.0% of User fee/ Transaction charge</td>
</tr>
<tr>
<td>89.99% to 75.00%</td>
<td>15.0% of User fee/ Transaction charge</td>
</tr>
<tr>
<td>74.99% to 00.00%</td>
<td>30.0% of User fee/ Transaction charge</td>
</tr>
</tbody>
</table>

Aurionpro shall not be obliged to reimburse the Customer more than once in respect of a Fault or Failure.

1.20 Termination terms

By consumers
90 days notice required prior to the anniversary

Minimum contract – 12 months

By the Supplier
90 days notice required prior to the anniversary