

User Pays User Group

8th September 2008

This presentation covers

- Contractual approach
- IAD Enhancements
- Operational update

Contractual Approach

- There is a strong desire of the UPUC to develop a proposal enabling a dual governance approach to the contract
 - Terms and conditions governed by the User Pays Contract Expert Group
 - Service Schedules governed by the User Pays User Committee
- xoserve needs to ensure that it is not exposed to unacceptable risks from the proposed governance approach
- Following the actions from the previous meeting (UPUG 0031 to 0034) xoserve has developed a proposed approach to move the contracting issues forward which we believe satisfy both of the above criteria – ie
 - Enables dual governance
 - Provides xoserve with adequate risk mitigation

What risks are xoserve potentially exposed to?

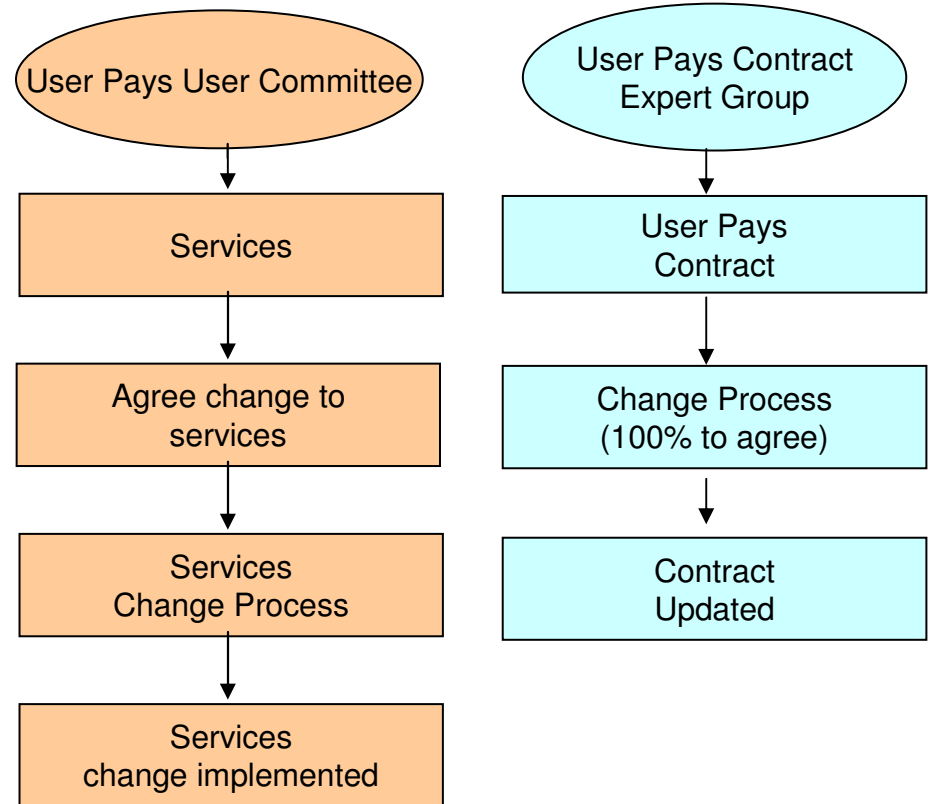
Action UPUG 0031

- Key risks to xoserve of separately governed Service Schedules

Area	Risk	Proposed Mitigation
Legal / Regulatory/ existing contractual obligations	There is a risk that xoserve may be asked to carry out a service that puts it breach of the law, regulatory obligations or risks putting it in breach of existing contractual obligations	Paragraph covering this in the main User Pays contract
Financial	There is a risk that xoserve may be exposed to financial risk as a result of: <ul style="list-style-type: none">■ Being required to deliver services for which demand is less than forecast/agreed■ Development costs being incurred can not be recovered	Change process
Operational	There is a risk that services requested may be outside of xoserve's key capabilities or may result in prioritisation issues around delivery of services	Change process
Systems	There is a risk that services requested may put undue strain or demand on systems or may result in system reliability issues if the necessary capacity does not exist	Change process

The Vision

- Customers made clear their support for the two tier approach
 - Contract - UPCEG
 - Services – UPUC
- Contract change process has been developed by Contract Expert Group and agreed in principle
- xoserve action to draft a change process for services
 - This included exploring other examples of contracting approaches with separately governed Schedules, notably the electricity arrangements for ECOES.



Electricity Model

Action UPUG 0034

- Review of the MRA, MRASCO, GEMSERV and C&C contractual arrangements has been undertaken
 - Service Schedules are subject to separate governance but are part of the overall contract
 - Key differences to the operating and contracting model are summarised below:

	Owner of licence obligations	Customers	Service Delivery
Electricity	Distribution and Supplier companies	Distribution and Supplier companies	Gemserve (owned by Distribution and Supplier Cos) via C&C
Gas	Distribution Networks	Shippers	xoserve (owned by Distribution Networks)

Owners and customers are the same entities

Commercial entity

Owners and customers are different entities

Cost + 6%

Electricity Model continued

- The process management of change also differs as summarised below:

	Agreement of change	Delivery of change	Management of contractual change
Electricity	MRASCO (D+S)	Gemserv (D+S)	MRASCO (D+S)
Gas	UPUC (Shippers)	xoserve (GDNs)	UPCEG (xoserve and shippers)

Electricity Model

Conclusions from the Review

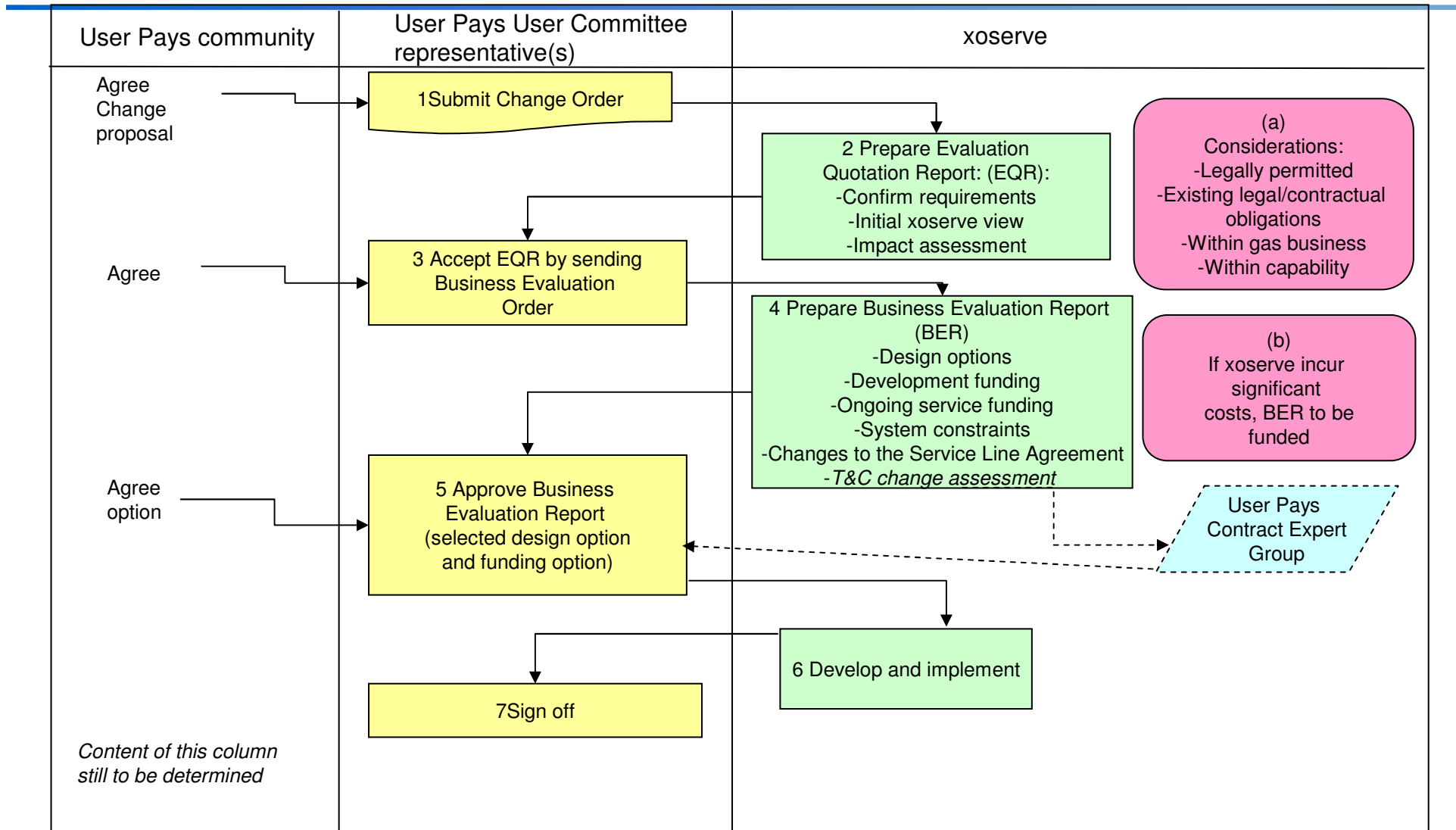
- There are some key differences in the electricity ECOES contracting model. A direct copy is therefore not possible
- Some aspects may work for User Pays and we have reflected these in the proposed approach outlined in the following slides

Service change proposal

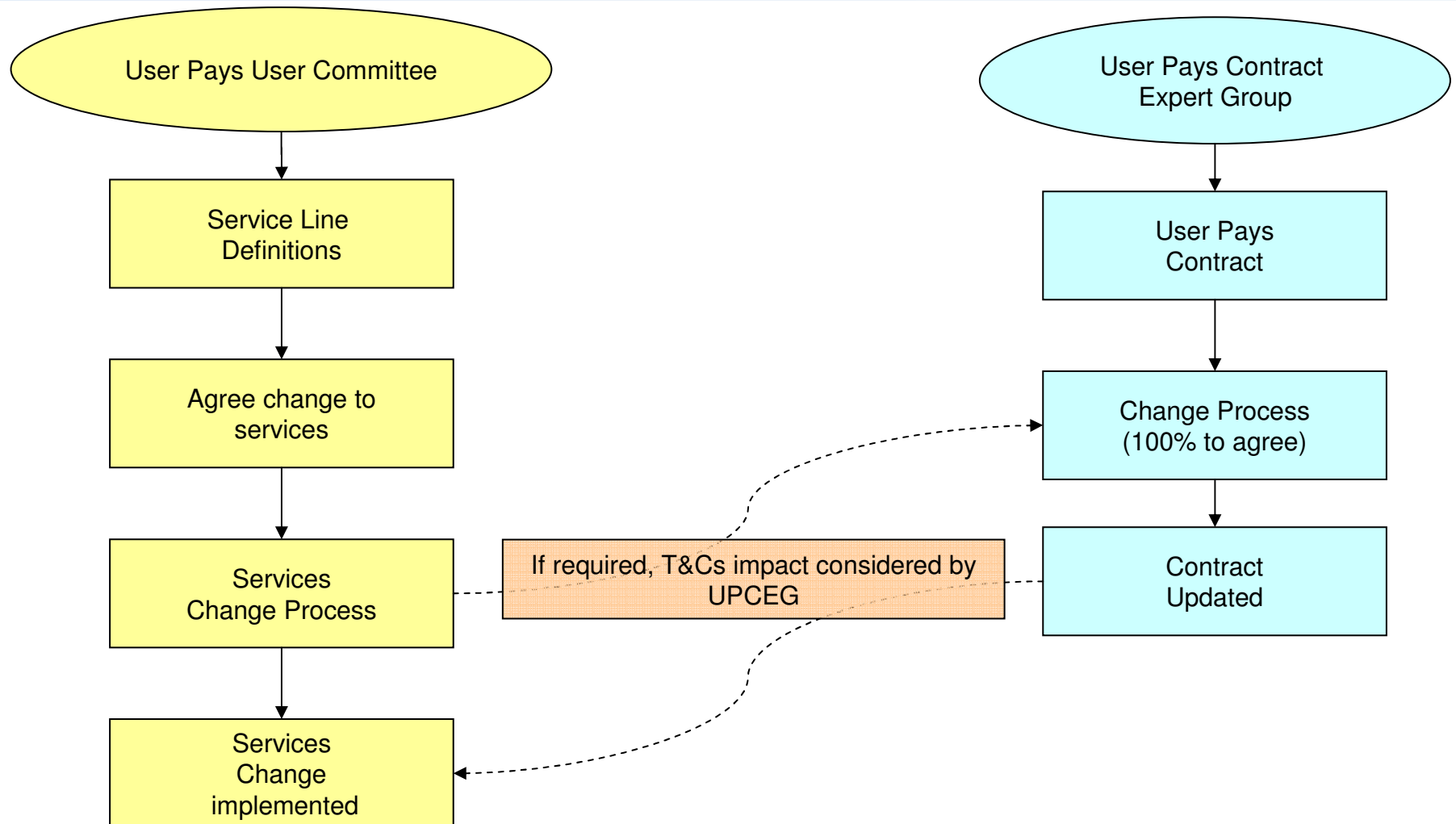
Action UPUG 0032

- The proposal is based on the two tier approach:
 - UPUC manages the service lines
 - UPCEG manages the contract
- Changes to the services lines will be made by following a change process
 - Proposed change process based on other change processes we manage (notably UNC)
 - Assumption is that, to mitigate the risks outlined previously, xoserve has a voice in the service change process regarding feasibility of proposed change but not a vote

Proposed Service Change Model



How does this look?



What does this mean?

- xoserve is supportive of separating out service schedules if a robust change process is in place
- Service Schedules become Service Line Definitions (SLDs) to be published in separate document to main contract and will be cross referenced in the contract
- Service Line Definitions to sit with UPUC
 - Terms of Reference for UPUC required, including voting arrangements for the change process
- Contract sits with UPCEG
 - Terms of Reference to be finalised
 - UPUC SLD change process to be defined in main contract

Next Steps

Appendix

- More detailed description of change process steps on following slides

A guide to each stage of the proposed change process

Stage 1 - Following agreement between customers, a Change Order is submitted to xoserve. xoserve will review and evaluate based upon defined criteria. xoserve may also raise a change order.

Stage 2 - xoserve prepare an Evaluation Quotation Report (EQR). The EQR is xoserve's understanding of the Change Order, and xoserve's assessment of what analysis work is required in order to develop the Business Evaluation Report (BER). The EQR is a quotation for the analysis work. In the EQR xoserve will have determined if it needs to recover the costs of completing the BER phase, and how this will be done and the feasibility of the request.

Stage 3 - The customers will need to agree and approve the EQR before work commences on the BER. This may include agreement of the funding of the work necessary to complete the BER.

Stage 4 - Assuming the EQR is approved, xoserve will commence work on the BER. The BER is the analysis and design work. The BER contains the various options for how a service may be delivered (including timescales) and the development and ongoing costs/price (and cost recovery) of each option. xoserve and the customers will define how the development work is to be funded. Customers will need to estimate the demand for the service when evaluating the options.

A guide to each stage of the proposed change process

Stage 5 - The customers will review the BER and determine the next steps – selection of an option or ending the Change Order at this point.

Stage 6 - If the BER is approved, and there are no changes to the T&Cs, xoserve will commence work on the chosen design solution. If the BER is approved and supporting changes to the T&Cs are required, these will be progressed at the User Pays Contract Expert Group. When agreement is reached, xoserve will commence work on the chosen design solution. Ongoing progress reports will be provided for each change as it progresses, this will include performance against planned timescales and budgets.

Stage 7 - The Change will be implemented. Customers will final sign-off completion of the Change Order.

Stage 8 (not shown on diagram) - xoserve will complete a Post Implementation Appraisal and provide a report to the Customers.

Note: the arrangements under which the User Community determine and approve changes is not included within this Change process.

IAD Enhancements

Timeline for September 2008

- xoserve -

- Publish LSO managed organisation template on xoserve web site
w/c 1st September
- Validate data received from LSO managed organisations. Identify and communicate any data issues to appropriate organisation
w/c 15th September
- Agree reconciliation process for IAD account creations and deletions.
w/c 15th September
- Develop UAT test cases and execute UAT
work in progress
- Publish User Guides
w/c 15th September

Timeline for September 2008

- Shippers -

- Populate LSO managed organisation template and submit to xoserve for xoserve to validate. 15th – 22nd September
- Brief all Users within own organisation of the changes asap
- Arrange for new LSO's to be registered asap

IAD Enhancements

Implementation of IAD Service Changes

- Proposed Outage - 10th October (22.00) - 13th Oct (06.00)
- Contingency Outage - 17th October (22.00) - 20th Oct (06.00)

IAD Service changes implemented will include:

- Single Log-on – restrict to one User able to access account
- Forced logout functionality - Idle time set to 30 minutes
- User or LSO password reset / retrieval functionality

IAD Enhancements

- All project activities are on track and the project is at a Green status.
- The Design Stage of the project has been completed.
- Currently developing the solution and completing both System and Performance testing.
- xoserve business users are developing test cases to perform user acceptance testing.
- xoserve are liaising with IAD users for organisations that wish to be LSO managed to confirm timescales of when information needs to be supplied to xoserve.

User Password Reset Functionality

Day 1

- Users logging into the IAD Service post implementation will be navigated to 'Create Profile' screen.

xoserve Internet Applications - Microsoft Internet Explorer

Monday August 25th, 2008 at 11:30:11

xoserve

Create Profile

Profile does not exist for X3CM001 in IAD.

Please answer the 3 security questions to create your profile

What is your/LSO email address?

What is your/LSO name?

What is your/LSO security password?

Note:

1)Users belonging to LSO Managed Organisation will need to contact the LSO to undertake the password reset.
2)The answers for the above 3 security questions are not case sensitive.

Please enter a new Password
to access your IAD account

Confirm New Password

Note: Please ensure to follow the below password criteria while setting up the New IAD Password:

- 1.Password should begin with a alphabetic character(Upper or Lower case letters).
- 2.At least one digit from 0-9.
- 3.At least one special character i.e (\$/#/_ are allowed).
- 4.Password should have minimum length of 6 and a maximum of 30 characters.

User Password Reset Functionality

Day 1

- In addition to creating their Security Profile Users will also be requested to reset their passwords.
- Please note that due to controls within the IAD Service users will be unable to reset their password to one that has been used within the previous 365 days.
- There is also a restriction on special characters with only the \$, # and _ being recognised.
- Once users have created their Security Profile and reset their password they will be navigated back to the front screen and will need to log in using their new password.
- Users can only retrieve or reset of their password by answering their security questions.

LSO User Password Reset Functionality

Day 1

- LSO managed organisations will have to supply answers to the following questions to xoserve for all IAD accounts within their organisation:
 - What is the LSO's e-mail address?
 - What is the LSO's name?
 - What is the LSO's IAD Administration password?
 - The IAD account password that each User will input when logging into IAD post implementation.
- Please note that post implementation the password that has been provided to xoserve by the LSO will be the live password for the IAD account.
- This password will supersede any password resets that have occurred in the period between the submission of the account details and implementation of the changes to the IAD Service.

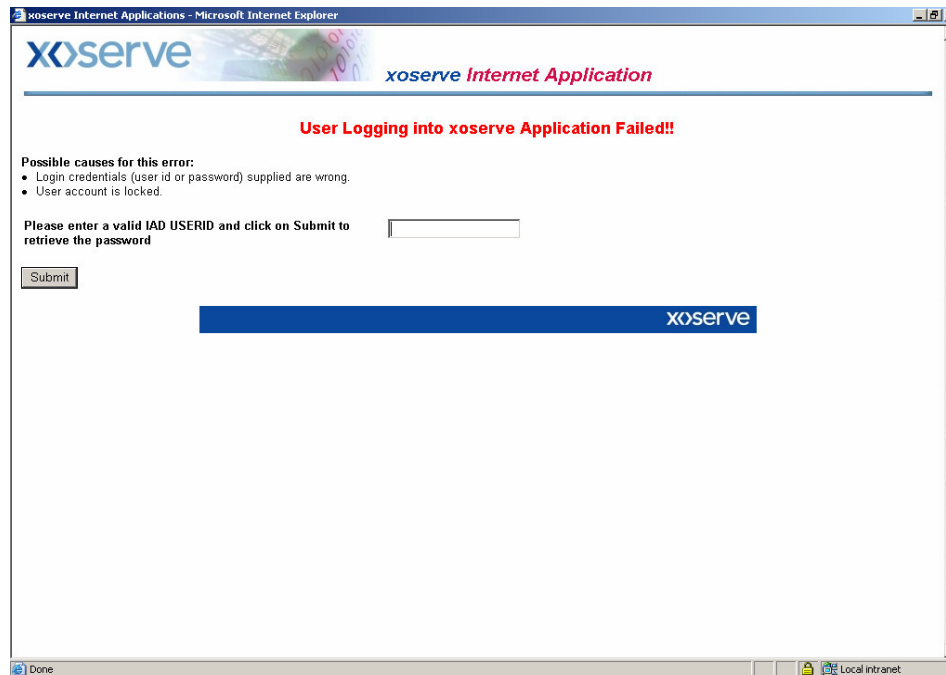
LSO User Password Reset Functionality

Day 1

- Post implementation users in an LSO managed organisation will log into the IAD Service in the usual way by inputting their user name and **new** password.
- All IAD account password retrieval or resets will be managed by the designated LSO.
- The 365 rule does not apply to the Security Profile answers.

IAD – Login Failure Screen

- Users who input their password incorrectly 3 times into the IAD System will be automatically navigated to the following screen:



- For an LSO managed organisation once a user is navigated to this screen they must contact their LSO to retrieve their password on their behalf.

IAD – Login Failure Screen

- For a User Managed organisation the user will need to input their user id and click the submit button. They will then be navigated to the Security Profile screen where they will have to answer all 3 questions correctly.



The screenshot shows a web browser window titled "xserve Internet Applications - Microsoft Internet Explorer". The address bar shows "Monday August 25th, 2008 at 12:18:27". The page header includes the "xserve" logo, a "MENU" button, and the title "Security Profile". Below the header, there is a navigation bar with links: "Back", "Forward", "Refresh", "Stop", "Print", and "Logout". The main content area contains the instruction "Please answer the following Security Questions to modify your password." followed by three questions, each with a text input field:

- What is your/LSO email address?
- What is your/LSO name?
- What is your/LSO security password?

At the bottom of the form, there are two buttons: "Submit" and "Clear".

IAD – Login Failure Screen

- Once the user/LSO has input the answers and clicked on the submit button they will be navigated to the following screen:



- For user managed organisations they will need to click in the Re-login link where they will be navigated back to the IAD front screen to log into the IAD Service.
- For LSO managed organisations the LSO will need to contact the individual to advise them of their IAD account password.

LSO Managed Organisation

- **SCENARIO 1**
- Need to reset password because.....
 - a) want to re-allocate an IAD account to a new User
 - b) a User has locked their account – 3 failed attempts to input password
 - c) want to stop the account being accessed by somebody who has left
 - d) protect access to systems being compromised (ad-hoc / routine)
 - e) the User (who is part of an LSO Managed Organisation) has tried to answer the 3 Security Profile questions 3 times *

LSO Managed Organisation

Scenario 1 ~ a) – d)

LSO enters the relevant IAD account using that User's Log-on I.D. and password

LSO enters their own LSO Security Profile details

LSO enters new password

Note : can't be a repeat of one used in last 365 days

Confirm the password

Note: the password must conform to a prescribed format



LSO issues the account to the allocated User and notifies of new password

LSO Managed Organisation

- SCENARIO 2
- Need to change the Security Profile because.....
 - a) it is routine business practice to change passwords
 - b) the name changes or an e-mail address changes
 - c) change of LSO – new LSO takes on associated set of IAD accounts
 - d) an LSO, who is privy to a fellow LSO's security profile details, leaves
 - e) Forgotten or locked the Security Profile
 - f) A User has tried to answer the security profile questions three times *

Create Security Profile screen

xoserve Internet Applications - Microsoft Internet Explorer

xoserve   **Create Profile**

Tuesday September 2nd, 2008 at 13:25:03

Profile does not exist for XBUS002 in IAD.

Please answer the 3 security questions to create your profile

What is your/LSO email address?

What is your/LSO name?

What is your/LSO admin password?

Note:
1)Users belonging to LSO Managed Organisation will need to contact the LSO to undertake the password reset.
2)The answers for the above 3 security questions are not case sensitive.



















Please enter a new Password

to access your IAD account

Confirm New Password

Note: Please ensure to follow the below password criteria while setting up the New IAD Password:

- 1.Password should begin with a alphabetic character(Upper or Lower case letters).
- 2.At least one digit from 0-9.
- 3.At least one special character i.e (\$/#/_ are allowed).
- 4.Password should have minimum length of 6 and a maximum of 30 characters.

Start |      >> |  I...  C...  t...  M..  q...  u...  six  F...  M..  1...  X...  X...  5:52 PM

LSO Managed Organisation

Scenario 2 ~ a) – e)

LSO to contact xoserve.userpays@xoserve.com
to request a datafix of the security profile answer(s)

Note: need to provide the full set of associated IAD accounts

Change Request to be raised specifying the requirements of the request

Copy of the Change Request to be sent to originator for validation and authorisation

Approved Change Request passed to Applications Support Team to action
Originating LSO contacted when datafix undertaken

Note: there is a lead time of 10 business days from approval of CR

LSO Managed Organisation

Scenario 1 ~ e) and Scenario 2 ~ f)

LSO contacts the Helpdesk 0800 917 7111 to raise job to reset the security profile

Note: need to specify the answers to each profile question

Application Support team contacts the LSO to confirm that Security profile reset

LSO enters the relevant IAD account using that User's Log-on I.D. and password

LSO enters their own LSO Security Profile details

LSO enters new and confirmed password

Note : can't be a repeat of one used in last 365 days

LSO issues the account to the allocated User and notifies of new password

LSO Managed Organisation

- SCENARIO 3
- Need to re-assign set of associated IAD accounts (in part or in full) to another LSO because....
 - a) an LSO ceases to be an LSO and need to link associated IAD accounts to another LSO(s)
 - b) of a re-organisation
 - c) balance the workload

LSO Managed Organisation

Scenario 3 ~ a) – c)

LSO to contact xoserve.userpays@xoserve.com
to request a datafix of the security profile answer(s)

Note: need to provide the full set of associated IAD accounts

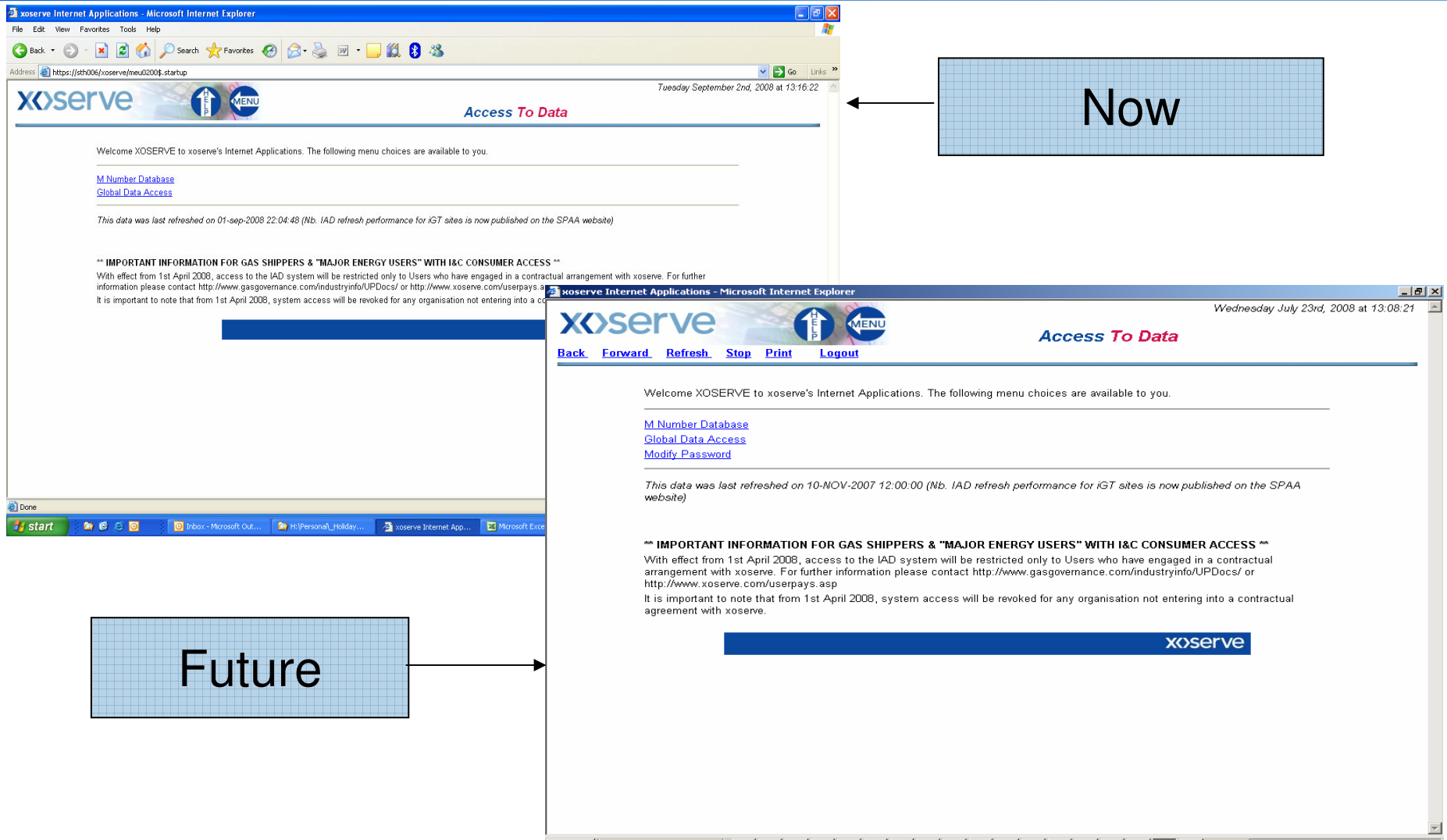
Change Request to be raised specifying the requirements of the request

Copy of the Change Request to be sent to originator for validation and authorisation

Approved Change Request passed to Applications Support Team to action
Originating LSO contacted when datafix undertaken

Note: there is a lead time of 10 business days from approval of CR

Screen Changes



Operational Update

Telephone Service Line

	No of calls	Service Availability (target 95% availability)	Call answering (target 90% within 30 seconds)
August	28,735	100%	91%
July	31,834	100%	90%
June	28,073	100%	95%

IAD Service Line

	Number of Accounts (original forecast 12,500, revised ACS average 13,900)	Availability (Target 95% availability during core hours)
August	14,100	100%
July	13,500	100%
June	13,400	100%

Email Report Service Line

	No. of email reports (forecast 150 per month)	Performance (2 and 5 business days)
August	91	100%
July	113	100%
June	96	100%

Portfolio Reports

	Reports sent in the month (forecast 80)	Performance standard
August	110	
July	108	
June	110	

AQ Enquiries

	Number of AQ Enquiries processed	Performance (Target process by end of second Business Day)
August	164,450	100%
July	1,610.954	100%
June	5,258	100%

IAD Account Transaction Volumes

	Accounts Created (normal process)		Bulk Password Resets	
	Number	Within 10 days	Number Requested	Completed within Month
August	590	86%	1,068	1,068
July	880	99%	150	1,200
June	695	97%	1,050	135
May	687	66%	135	0
April	556	85%	1,890	1,890
March	27	100%	0	0

- Ongoing close monitoring of performance in this area continues

October Portfolio Reports

- **REMINDER** : AQ 2008 data refresh planned 29 September to 2 October
- Reports scheduled to be run on these dates would contain out of date data if delivered as usual
- Impacted reports;
 - 'Registered User Portfolio Report'
 - 'Registered User Portfolio Statement'
 - 'Data Portfolio Snapshot'
- Industry wide effected report 'Registered User Portfolio Statement'
 - To provide accurate reflection of new AQ data we WILL run this report on 6 Oct and deliver to industry as per normal
- Users with other reports scheduled in this period are being contacted on individual basis