



TRANSPOWER

Transpower House, 96 The Terrace,
PO Box 1021, Wellington,
New Zealand
Telephone +64-4-495 7000
Facsimile: +64-4-495 7100
www.transpower.co.nz

Richard Fletcher
richard.fletcher@transpower.co.nz

19 March 2010

Lisa DuFall
Electricity Commission
PO Box 10041
WELLINGTON

Dear Lisa

Re: Discussion Paper – Security, Web Services, and EIEP Data Exchange

This is Transpower New Zealand Limited's submission on the Electricity Commission's 17 February 2010 discussion paper *Security, Web Services, and EIEP Data Exchange*.

While the scope of the discussion paper is confined to the Registry and the EIEP Data Exchange, we are concerned that the proposals in this paper appear in isolation from broader security considerations.

Broader security considerations should be addressed by a security policy and recommended security standards, which would provide the context and basis for the provision of all secure services and information exchanges. The proposals as outlined should not be considered to be precedent setting beyond the scope under consideration.

Attached to this letter are responses to the questions posed by the discussion document. If you have any questions about the detailed responses, could you please address these in the first instance to Alun Evans, ph. 495-7134, e-mail AlunFrancis.Evans@transpower.co.nz.

Yours sincerely

Richard Fletcher
Regulatory Strategy Manager

APPENDIX – Security, Web Services, and EIEP Data Exchange

	Question	Response
Q1.	Do you agree with the risk assessment of the current unsecure FTP data transfer mechanism? Please give reasons for your view.	<p><u>Partially agree:</u></p> <p>The risk assessment in this paper does not appear to state what the risks are to the service as a whole, only that the FTP service is insecure from an interception point of view. It is unclear how the upgrading of FTP to an encrypted protocol will be used to ensure the security of the reconciliation process (Section 2.1.2).</p> <p>The advantage of FTP is that it is simple and easy to implement across a wide range of different types of computer systems environments. However, secure FTP tends to be problematic unless both the party sending data and the party receiving data are using exactly the same Secure FTP software application on a similar computer system.</p> <p>Standard FTP data transfer is very insecure for unencrypted data exchange. It has a number security issues, such as:</p> <ul style="list-style-type: none">• authentication in clear text;• in certain transfer modes it can permit the scanning of internal networks;• certain server implementations have a history of security failures that can lead to increased server privileges. <p>As a result, it is normal to deploy a FTP service with care. Typical methods include:</p> <ul style="list-style-type: none">• choosing a FTP server application with a good security history and maintaining (patching) it;• placing the service in an isolated demilitarised zone (DMZ) with strict firewall rules preventing access from the server to internal networks;• monitoring of brute force attacks against FTP server accounts;• monitoring of usage of the system and the type of files transferred;• if confidentiality or integrity is required this would normally be applied at the file level and consequently implemented outside the FTP protocol.

	Question	Response
Q2.	Do you agree with the risk assessment of the current browser and thin client data transfer mechanism? Please give reasons for your view.	<p><u>Partially agree:</u></p> <p>It is important to note that the paper does not define a security policy for this service that all parties can assess the security against. Security considerations for the Registry and EIEP data exchange services need to be framed in a security policy.</p> <p>The security of thin client and secure browser depends on the practices of the organisations implementing this service. Most systems use a public/private key or security certificate mechanism to set up an encrypted virtual “tunnel” or connection between the two parties exchanging information over the network. Such implementations in other businesses have been compromised in the past either by an oversight or lapse in secure practices by the company offering the data, or by a highly knowledgeable “attacker” exploiting various loopholes in the secure solutions. Generally these solutions are good, but they can never be claimed to be 100 per cent secure.</p> <p>The risk assessment does not include:</p> <ul style="list-style-type: none">• what happens to the data at rest;• how secure reconciliation is to be met;• how the service is to be maintained and monitored;• What happens if the internal security of one party is breached, e.g. can they affect this system by, for example, placing malformed/incorrect data into the registry? <p>Also, paragraph 2.1.9 refers to password based access to the registry. Will this password based access be accessible from the internet? If so, it may vulnerable to brute force attacks which are common for ssh/sftp. Later in the paper it states that certificate based authentication is to be used which will eliminate this risk, but this will introduce a certificate management overhead? e.g. what happens when a private key is lost?</p>

	Question	Response
Q3.	Do you agree with the proposed business requirements for the registry secure file transfer mechanism? Please give reasons.	<p><u>Agree:</u></p> <p>These requirements should add a minimal overhead on the end user of the service. Depending on how seamless the adopted solution is, end-users of it may even be unaware that the security of the solution has been hardened.</p> <p>However, in practice there may be an overhead in the security management of the service.</p>
Q4.	Do you have any additional business requirements for the registry secure file transfer mechanism? Please supply details.	<p>The solution must:</p> <ul style="list-style-type: none">• provide an audit trail for both parties (service provider and service client) to ensure data arriving at a site is from an authorised source, and the sender is transmitting data to a legitimate recipient;• ensure one authorised user cannot corrupt data entering the system. The statement in paragraph 2.3.4 which delivers data to the intended recipient based on file name format is not regarded as good security practice as it seems to permit the sender to masquerade as an arbitrary sender. (Permitting the free format of data from the client side is never a good idea.);• include report timestamping (again this is free format data on a file name);• detail how disputes to be adjudicated;• state the retention time for both the data transmitted and the logs recording the transmission. <p>In conjunction with this, parties exchanging information are responsible for preventing Malware, such Trojan horse type viruses. Any such system should be detailed in the system security policy and probably be on a best efforts basis.</p>
Q5.	Do you agree with the proposed characteristics for Web Services? Please give reasons.	<p><u>Note:</u> There is an assumption within this solution that the data being exposed do not offer competitive advantages to the competing participants using these data.</p>
Q6.	Would you propose any additional characteristics for Web Services? Please provide details.	No.

	Question	Response
Q7.	Do you agree with the proposed characteristics for EIEP data exchange? Please give reasons.	<p><u>Disagree:</u></p> <p><u>Ideally</u>, the characteristics provided should provide a simple and easy to implement file exchange system.</p> <p>However, the proposal in paragraph 2.3.4, which delivers data to the intended recipient based on file name format is not regarded as good security practice as it seems to permit the sender to masquerade as an arbitrary sender, permitting the free format of data from the client side. This is made especially risky as:</p> <ul style="list-style-type: none">• the concept in paragraph 2.3.7, which states that participants could exchange other files provided the file naming convention was adhered, runs the risk of automated data exchanges becoming complex and hard to maintain;• no policy is proposed with respect to how the system should be managed and monitored. <p>While the proposals provide for a convenient service (the identified risk notwithstanding) for some participants, use of this service should not be mandatory. Alternatively, participants should have the option to use alternate secure data exchange mechanisms that comply with a security policy for EIEP data exchange.</p>
Q8.	Do you recommend any additional characteristics for EIEP data exchange? Please supply details.	The (mandatory) requirements for secure EIEP data exchange should be provided as a basis for participants establishing peer-to-peer mechanisms.
Q9.	Would your organisation use the optional email/mobile text notification function for EIEP data exchange?	<p>In some instances yes, but not in others, e.g. frequent automated data feeds.</p> <p>This would be an extra security management overhead.</p>
Q10.	Which option does your organisation prefer for the registry secure file transfer mechanism? Please give details including specific costs and benefits that will be used in a cost benefit analysis.	No comment.

	Question	Response
Q11.	Are you aware of any problems that would make moving to FTPS or SFTP infeasible for your organisation? Please give details.	Regardless of which option Transpower selects, our existing FTP file transfer solution would need a redesign and update to fully support SFTP or FTPS. However, this has already been identified as a Transpower requirement.
Q12.	Do you support a phased approach allowing some participants to retain their current unsecure FTP processes until they have time to make the change (i.e. by implementing the explicit form of FTPS of option 2)? Should there be a published cut-off date?	<p>A phased approach would be more acceptable to most participants.</p> <p>Some participants are not as technically agile as others, and those with more complicated IT architectures would need additional time to design and deploy any new solutions to support the secure FTP options proposed.</p> <p>There should be a cut-off date of 18-24 months as a driver to encourage all participants to move from “unsecured” data transmission to “secured”.</p>
Q13.	Are there any other practicable options that should be considered for the registry secure file transfer mechanism? Please give details.	<p>The presented options cover the best available solutions for data exchange across varying requirements.</p> <p>However, as stated above, a defined security policy for this service is required.</p>
Q14.	Do you agree with the comments on the costs and benefits section? If not, please give reasons and alternate values that you consider more representative.	Agree.
Q15.	Will your organisation be seeking to implement Web Services with the registry in the near future as a registry tool? What is your organisation’s timeframe? Please give details and expected costs and benefits that will be used in a cost benefit analysis.	No comment.

	Question	Response
Q16.	Does your organisation see any business benefits in implementing all the registry interfaces in Web Services? Please give details and expected benefits.	No comment.
Q17.	With respect to the proposed web service function A (address search), do you have any issues with the proposed implementation or do you prefer that the suggested alternative is adopted instead? Do you recommend a different solution? Please give details.	<u>As a general comment across all data sharing solutions</u> , Transpower is in a unique position being in possession of SCADA and market data across all participants. As such, Transpower must be very careful about what data are released to ensure release does not result in an unfair competitive advantage by making one participant privy to another participant's sensitive information via the registry. With respect to the address search – this is a service of use to lines company participants rather than Transpower.
Q18.	With respect to the proposed web service function B (individual ICP list), do you have any issues with the proposed implementation or do you prefer that the suggested alternative is adopted instead? Do you recommend a different solution? Please give details.	No comment.
Q19.	With respect to the proposed web service function C (ICP query), do you have any issues with the proposed implementation?	No comment.

	Question	Response
Q20.	With respect to the proposed web service function D (ICP snapshot query), do you have any issues with the proposed implementation? Would your organisation use this particular service?	No comment.
Q21.	How would you rate (High/Medium/Low) the priorities for implementing: <ul style="list-style-type: none">• function A address search,• function B individual ICP list,• function C ICP query, and• function D ICP snapshot query.	No comment.
Q22.	Are there any other functions that should be considered for implementation via Web Services in the first phase? Please give reasons.	No comment.
Q23.	Do you agree with the assessment against the objectives in table 8? If not, please give reasons and alternate values that you consider are more representative.	Agree.
Q24.	Do you agree with the costs and benefits noted? If not, please give reasons and alternate values that you consider are more representative.	No comment.

	Question	Response
Q25.	Do you agree with the conclusion that an EIEP data exchange should be developed in the registry? Please give details including specific costs and benefits that will be used in a cost benefit analysis.	No comment.
Q26.	Are there other options that have not been considered for EIEP data exchange? If yes, please provide details.	There needs to be the option for participants to establish alternate secure peer-to-peer EIEP data exchange mechanisms that comply with an established security policy for this data exchange. All comments relating to the security risks identified previously apply and need addressing.
Q27.	Do you agree with the costs and benefits noted? If not, please give reasons and alternate values that you consider are more representative.	No comment.