

Report of Senior Service Development - Security

Report to Chief Information Officer

Date: 13th August 2015

Subject: Report to seek approval to waive contract procedure rule 8.1 & 8.2 entering into a contract for an Enterprise Agreement for Entrust SSL Certificate Renewal.

| | | |
|--|---|--|
| Are specific electoral Wards affected? If relevant, name(s) of Ward(s): | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| Are there implications for equality and diversity and cohesion and integration? | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| Is the decision eligible for Call-In? | <input type="checkbox"/> Yes | <input checked="" type="checkbox"/> No |
| Does the report contain confidential or exempt information? If relevant, Access to Information Procedure Rule number: Appendix number: Appendix A – Detailed cost breakdown | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No |

1. Summary of main issues

- 1.1. Leeds City Council (LCC) use Secure Sockets Layer (SSL) Certificates * to encrypt and secure HTTPS public facing services. Entrust have provided LCC with these certificates and a managed portal for a number of years.
- 1.2. The current support and maintenance contract expires 11th September 2015. A new agreement needs to be in place with a supplier to allow LCC to publish secured web content.

2. Recommendations.

- 2.1. The Chief Information Officer is recommended to approve the waiver of contract procedure rule 8.1 and 8.2 entering into a contract with Entrust Limited for the provision of an Enterprise Account to support and maintain LCC's SSL Certificates.

* SSL stands for Secure Sockets Layer. It provides a secure connection between internet browsers and websites, allowing you to transmit private data online. Sites secured with SSL display a padlock in the browsers URL and possibly a green address bar if secured by an EV Certificate. Reference <https://www.instantssl.com/ssl.html>

1. Purpose of this report.

- 1.1. The Chief Information Officer is recommended to approve the waiver of contract procedure rule 8.1 and 8.2 entering into a contract with Entrust Limited for the provision of an Enterprise Account to support and maintain LCC's SSL Certificates.

2. Background information.

- 2.1. LCC uses SSL Certificates to enable secure communications for external web services.
- 2.2. LCC currently use Entrust Limited to manage SSL certificates and this partnership has been in place for a number of years. Entrust provide a management suite and the ability to add / remove certificates as LCC needs throughout the year.
- 2.3. Certificates are needed for public facing HTTPS websites to encrypt and secure LCC data.
- 2.4. The current support and maintenance contract expires 11th September 2015.
- 2.5. The cost of SSL Certificates to LCC in the last 2 years was \$12,852 (£8,309.41 in today's exchange rate) and has historically increased each year in-line with inflation.

3. Main issues

Reason for contracts procedure rules waiver

- 3.1. Entrust are LCC's current provider of SSL Certificate services. Should LCC not award the contract to Entrust there will be a significant cost of change in monetary terms and would also create a resource pressure.
- 3.2. LCC currently uses 68 SSL, Unified Communications (UC) and Subject Alternative Name certificates. LCC must have an agreement in place with a certificate authority to issue these certificates.
- 3.3. No additional training required.
- 3.4. No migration charges in time and costs.

Consequences if the proposed action is not approved

- 3.5. If the existing contract is allowed to lapse a number of LCC published web services will be viewed as insecure when accessed via the internet.
- 3.6. Without an agreement in place there is a significant risk to availability and reliability of key internet published systems together with the potential to damage LCC's reputation.
- 3.7. Should the contract not be awarded to Entrust the Council would incur extra costs to migrate all the SSL certificates to a new provider.
- 3.8. Moving the service to another provider would lead to a number of staff needing to be retrained on a different SSL Certificate product range.

Advertising

- 3.9. No advertising was undertaken. Quotes were obtained and considered from four other providers.

4. Corporate Considerations

Consultation and Engagement

- 4.1. Consultation has taken place with key ICT stakeholders including ICT Service Development, Security team, Software Licensing and ICT Procurement.

Equality and Diversity / Cohesion and Integration

- 4.2. There are no Equality and Diversity / Cohesion and Integration issues associated with this decision.

Council Policies and City Priorities

- 4.3. The ongoing implementation of SSL Certificates underpins key elements of the Customer Access Strategy 2012-15. The Best Council Plan objective 6 for 2015/16 was to make LCC more efficient and enterprising. Secure web services offered through payments.leeds.gov.uk and functionality on www.leeds.gov.uk helps LCC to achieve these targets. SSL certificates are a key component of these services.
- 4.4. SSL Certificates are crucial in allowing secure communications with 3rd parties, present services to the public and for remote working. Examples of services which are dependent on the use of SSL certificates are Adult & Children Social Care systems, VPN, public access planning portal, email and mobile devices.

Resources and Value for Money

- 4.5. A detailed cost breakdown is included at Appendix A – Detailed cost breakdown.
- 4.6. Three alternative options are provided and have been considered.
- 4.7. Financial provision exists within the approved ICT Operational revenue budget to undertake the action proposed.
- 4.8. No additional resources are required to implement this decision.

Legal Implications, Access to Information and Call In

- 4.9. The decision is a Significant Operational Decision and is not subject to call in.

Risk Management

- 4.10. In the event of changing provider LCC would be exposed to a risk of certificates being incorrectly managed during the transition.
- 4.11. From April 2015 all SSL certificates will be limited to a maximum validity of 39 months (previously a certificate could have a 4 or 5 year validity). SSL certificates have limited validity periods so that the certificate's holder identity information is re-authenticated more frequently. It is best practice to limit the amount of time that any key is used, to allow less time to attack it. Quotes for 2 – 3 years have been considered in line with this directive. Further reading can be found here <https://www.globalsign.com/en/ssl-information-center/baseline-requirements/>

5. Conclusions

- 5.1. There is an ongoing requirement for LCC to publish content to the internet. A large proportion of this content is published using HTTPS websites. To validate this content the use of SSL certificates are required.
- 5.2. Agreeing a new contract with Entrust will lead to no extra training costs.
- 5.3. Agreeing a new contract with Entrust will lead to no migration costs.
- 5.4. Agreeing a new contract with Entrust will lead to no disruption to services.

6. Recommendations

- 6.1. The Chief Information Officer is recommended to approve the waiver of contract procedure rule 8.1 and 8.2 entering into a contract with Entrust for the provision of an Enterprise Agreement for the LCC's SSL Certificates.

7. Background Documents

- 7.1. Confidential Appendix A.