SCRAG/6 WP/10
16/09/05

SADIS COST RECOVERY & ADMINISTRATIVE GROUP (SCRAG)

SIXTH MEETING

(Paris, 21st and 22nd November 2005)

Enhancements to SADIS FTP Service - Budgetary Estimate

(Presented by the United Kingdom)

REFERENCES

SADISOPSG Conclusion 10/18 - Enhancements to the SADIS FTP Service

That the SADIS Provider State be invited to prepare:

a) an implementation plan for consideration by the SADISOPSG/11 Meeting of the proposed enhancements to the SADIS FTP Service; and

b) a budgetary estimate for presentation to the SCRAG/6 Meeting.

1. INTRODUCTION

1.1 During September 2004 the SADIS Provider had contracted an independent information technology security specialist to review the current service practice employed for delivering the FTP Service. The review had concluded that the current security measures were considered appropriate for the provision of the service as a back-up source of data, but further enhancements would be beneficial for those users accessing the service as their primary source of WAFS and OPMET data. A summary of enhancements recommended by the SADIS Provider was reviewed by SADISOPSG/10. The meeting agreed that implementation of these enhancements should be endorsed, in principle, since an increasing number of users were known to derive their OPMET and WAFS data from the FTP service. The SADIS provider informed the meeting that the implementation of some of the suggested enhancements may require considerable effort and therefore it was recommended that further work to study their impact be undertaken by the SADIS Provider State.

2. SADISOPSG/10 formulated Conclusion 10/18 (see reference above for text) which invited the SADIS provider State to prepare a budgetary estimate for implementing the enhancements to the SCRAG/6 Meeting. This working paper is the response to part (b) of this SADISOPSG Conclusion.

2. DISCUSSION

2.1 A summary of the recommended enhancements are provided below:-

1. Implement Public Key Infrastructure (PKI);
2. Issue digitally signed products;
3. Employ an audit trail for distributed products;
4. Provide service on dual servers (perhaps located at different sites);
5. Implement Network Intrusion Prevention System (NIPS);
6. Implement Host Intrusion Prevention System (HIPS).

These enhancements are considered highly desirable, and essential to maximise resilience and security, and to ensure integrity of data transmitted between host and user. There are synergies and interdependencies between some of these enhancements, particularly between items 1-3.

2.2 A number of these features require implementation at an enterprise (i.e. organisational) level as opposed to at the level of the host servers which are actually delivering the service. Implementation at an enterprise level ensures that a common approach can be taken to implement a technology that is appropriate to a large number of services. Such an approach is most likely to benefit from economies of scale and minimise on-going support costs. Transparent allocation of costs will be provided to ensure that each service which benefits from a particular technology is charged its appropriate proportion of the total costs.

2.3 The SADIS provider has already commenced a project to investigate implementation of a PKI across a virtual private network (VPN). Implementation of this project will prove and deliver a number of important capabilities which are required prior to establishing a full PKI capability. Full PKI capability is required for enhancements 1-3 listed above. These enhancements are expected to be complex and technically involved. The current PKI project already underway is being funded through the UK National Meteorological Programme (NMP) and consequently costs associated with this limited scope work will not be passed on to the SCRAG.

2.4 Table A (below) includes *budgetary* costs for implementing a prototype PKI infrastructure that meets the requirements of enhancements 1-3. It is proposed that this prototype is proven with a small number of remote users. Expenditure involved in this prototype will include licenses, hardware, engineer and project management expenses. The majority of this expenditure will be transferable to implementing a PKI solution in an operational environment. In other words, *significant* extra spend to bring the prototype into an operational capability is not anticipated, though some extra cost is likely.

2.5 It is expected that a new project will commence during 2006 to implement NIPS at an enterprise level. This project will also be funded centrally via the NMP and it is not expected that the SCRAG will be burdened with additional cost. However

the SADIS FTP Service will benefit from this new technology as will all internet based services delivered by the SADIS provider.

2.6 Consideration is being given to initiating a further project that would be subject to NMP funding. This project would address enhancement 4 (service provided on dual servers) under a generic FTP Rationalisation Project. However agreement has not yet been reached on whether the NMP would support this initiative. Consequently budgetary costs for implementing this enhancement solely for the SADIS service are provided in Table A.

2.6 Enhancement (6) is unique to the SADIS FTP Service and therefore it can be expected that the full implementation cost would need to be borne by the SCRAG.

Table A - *Budgetary* Costs for Implementing Preferred Enhancements to SADIS FTP Service

Enhancement	Budgetary Implementation Cost	Explanation of cost	Implementation timescale
1. PKI - including digital certificate management and digitally signed products **(Enhancements 1 & 2)**	• preliminary proof of concept (PKI across VPN), capital investment NIL • capital investment for prototyping £20,000 to £35,000 • setup cost £32,000 • annual maintenance costs currently unknown	Hardware and licenses necessary to prototype the digital signing of products will be transferable to operational service. Setup cost includes the cost of a trial at a remote site.	Proof of concept across VPN already complete. Detailed analysis of implementation risks and costs complete by SADISOPSG/11. Roll-out to SADIS following review by SADISOPSG/11. Could be complete by 2007 or 2008. Cost recovery expected to commence from year 2006.
2. Employ audit trail **(Enhancement 3)**	• capital investment £15,000 • setup cost £16,000 • annual maintenance costs currently unknown	It may be necessary to procure additional hardware to deploy at remote user sites to validate the creation and transmission of receipts	Roll-out to SADIS following review by SADISOPSG/11. Could be complete by 2007 or 2008. Cost recovery expected to commence from year 2006.
3. Service on dual servers **(Enhancement 4)**	• capital investment £10,000 • setup cost £5000	Provides increased resilience of SADIS FTP	Implementation for SADIS could commence following review by

	• annual maintenance £10,000	Service	SADISOPSG/11. Could be complete by 2007/08. Cost recovery expected to commence for year 2007 or 08 costs, however there is a small probability that this project may be financed by the NMP.
4. NIPS & HIPS (Network & host protection) **(Enhancements 5 & 6)**	• capital investment £5000 (NIPS will be NMP funded) • setup cost £8000 • annual maintenance £5000	Improved protection of SADIS FTP Service	Enterprise level project for NIPS due to commence 2006, project costs recovered through NMP. Roll-out both technologies to SADIS following review by SADISOPSG/11. Could be complete by 2006/07. Cost recovery expected to commence for year 2006 costs.
TOTALS (assuming *minimum* NMP finance) Capital Expenditure (hardware, software, licenses) £65,000 Manpower (engineer support, consultancy, project management) £61,000 Annual Maintenance £15,000 excl. PKI maintenance costs (to be determined)			

3. TOLERANCES

3.1 The costs shown in the Table A are the expected maxima for each activity. However there are some variables that are currently unknown. In the event of work proceeding the SCRAG is requested that the SADIS provider be given control over the operation of the budget, so that money allocated to one activity might be split with another activity if this better satisfies the objective of providing all enhancements within the budgeted total.

3.2 Software licenses and any hardware acquired as a result of activities 1-3 would be owned by the SADIS provider and could be used in the deployment stage once the operational solution has been agreed upon. As the purpose of activities listed under items 1 and 2 in Table A is to prototype solutions, it should be anticipated that some further software and/or hardware will be required in order to create a full operational capability, though these costs should be modest.

4. IMPLEMENTATION SCHEDULE

4.1 Implementation of the enhancements can be achieved by running a number of concurrent projects, or a single project with a larger number of deliverables. Cost of capital can be spread over 5 years though it should be appreciated that a significant proportion of the budget relates to staff resource which would be recovered in budget cycle. The expected duration of full PKI capability (enhancements 1-3) implies that staff resource for this work could be recovered across two or three years (2006-08).

4.2 Implementation of the enhancements could be staggered across a number of years to further assist budgeting. In addition this will build in some flexibility to the implementation time scale (outlined below) which may be desirable bearing in mind that existing knowledge within the SADIS provider about some of the technologies to be deployed is limited. Implementation of technologies associated with delivering a full PKI capability (enhancements 1-3) are likely to prove the most demanding tasks. However by the time of SADISOPSG/11 the SADIS provider should have a more comprehensive overview of the risks associated with implementing these technologies, and a clearer description of the implementation path.

1. Full PKI implementation (enhancements 1-3) Year 2006/07/08
2. Implement NIPS at an enterprise level (NMP funded) Year 2006/07
3. Implement HIPS locally on SADIS servers Year 2007/08
4. Implement SADIS service on dual servers Year 2008/09

4.3 If a staggered implementation schedule such as the one outlined above is preferred it should be noted that implementation of an NMP funded NIPS and service provision on dual servers may occur outside of any timescale specified by the SCRAG or SADISOPSG. Table B has been prepared to illustrate for budgeting purposes the extra costs to the SCRAG for implementing the enhancements over the proposed schedule.

Table B - Budget Schedule

	2006	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**
Capital	£10K	£11K	£13K	£13K	£13K	£3K	£2K
Staff resource	£12K	£32K	£17K	0	0	0	0
Total	**£22K**	**£43K**	**£30K**	**£13K**	**£13K**	**£3K**	**£2K**

Note 1 Assumes that staff costs associated with enhancements 1-3 are recovered in the following manner (1/4 costs in 2006, 1/2 costs in 2007 and 1/4 costs in 2008).

Note 2 Assumes highest budgeted cost for implementing full PKI capability, i.e. £35K.

Note 3 Assumes that the SCRAG finances implementation of service on dual servers (enhancement 4) as opposed to the NMP.

4.4 SADISOPSG/10 has requested that consideration is given to hosting the SADIS FTP Service on physically separate duplicate servers. This is perhaps the ideal solution to maximise levels of availability and to also minimise the impact of a denial of service (DoS) attack against the Internet connection used by the SADIS provider.

However implementation of such a topology is likely to be technically complex and expensive for the following reasons.

- a new service will need to be built at a third party site;
- the new service will need to duplicate the structure of the existing service to ensure seamless compatibility;
- all user sites will need to be issued with a separate set of login information (ftp address and perhaps, username and password);
- all user systems will need to be re-configured to ensure that they can access the remote server in the event of problems,
- or, if load sharing between servers is to be achieved this has to be implemented across a wide area network;
- for the duplicate server to fully replicate the primary server and provide a fully redundant service, populating data would need to be sourced from WAFC Washington;
- this adds additional communication costs (resilient links will be required) and will require a certain amount of pre-processing of the data to be carried out to ensure that it is made available on the new server in the same format and structure as the primary host.

4.5 For these reasons it is recommended that this option is not pursued at present. It is recommended that the SADISOPSG is informed at its next meeting with a view to seeking further guidance. Perhaps consideration should be given to implementing this "holy grail" solution when all of the other initiatives have been rolled-out and proven.

5. ACTION

5.1 The SCRAG is invited to review the budgetary costs outlined in table A and the proposed expenditure schedule in Table B.

5.2 The SCRAG is invited to consider adopting the following Conclusion.

SCRAG Conclusion 6/x Enhancements to SADIS FTP Service

In view of the increasing use of the SADIS FTP Service as a primary source of operational data the SCRAG approves in principle the budgetary costs presented by the SADIS provider State and included in Appendix x to the report. The SCRAG invites the SADIS provider to complete a detailed implementation plan in time for SADISOPSG/11 and to advise SCRAG/7 as to whether any amendments to the budgetary figures are required.

Annex 1 - Explanatory Information about Recommended Enhancements

PKI

PKI (Public Key Infrastructure) can be used for the following purposes:

1. Authentication of SADIS users;

2. Authentication of the Met Office as a supplier of SADIS services;

3. Digitally signing of SADIS products to ensure integrity of the product, and to provide non-repudiation that the product was supplied by the Met Office.

4. Digitally signing of receipts by the SADIS user to ensure that the SADIS product was successfully received and verified by the user at a particular date and time.

For digital signatures to be effective it is necessary to employ significant physical security of the CDs, the equipment and the keys which allow changes to be made.

Digital Signing of Products

The normal way to digitally sign a product is to ”wrap” a digital signature around a file or embed the signature in the file. However, if this was done for the SADIS products, it might require all users of the system would have to change the way they handled the data. To ensure that existing users are unaffected by digitally signing products, it is possible that a separate file is created for each product (file) which contains the digital signature. In this way, existing users do not need to change

Audit Trail

An Audit Trail is required in a trusted service to provide a guarantee that the product was successfully received by the recipient at a specified time.

To better meet the requirements of life critical products, the SADIS user could be required to send back a digitally signed receipt confirming the products that have been received and verified. Verification of the products requires checking the signature of the products that have been digitally signed.

Duplicate Servers

The SADIS provider currently provides the SADIS FTP service via a clustered server. While this is perfectly appropriate for the backup service, it is less appropriate for delivering SADIS data as a primary service over the Internet. To achieve the appropriate levels availability, the following changes would have to be implemented.

- Two servers, one in each Computer Hall. The servers may be shared with other services, provided that the availability and performance can be guaranteed (this is difficult to achieve with a clustered server).

- Delivery of products will have to be duplicated – i.e. both SADIS servers receive the same information.

Backup Supplier

The main threat to providing a time critical service (i.e. one suitable for delivery of products to aircraft in-flight) is a DoS (denial of service) attack against the Met Office Internet connection, or against the SADIS server. The provision of a backup service via another authorised supplier (e.g. UK National Air Traffic Services) would ensure SADIS products could still be accessed from the Internet should the Met Office suffer a serious outage of the service.

NIPS (Network Intrusion Prevention System)

NIPS is appropriate for defending against various types of network attacks, such as DoS (denial of service) and DDoS (Distributed Denial of Service) attacks.
NIPS devices work by inspecting every IP packet that arrives from the Internet and preventing the illegal packets from entering the rest of the network. The response that the NIPS device can do are:

- Send a TCP reset packet back to the sender, forcing the sender to re-establish a TCP session.
- Drop the IP packet
- Log any suspicious IP packets.

While NIPS can protect systems residing in a DMZ from receiving malicious IP packets, and will allow legitimate traffic to pass through, however, bandwidth will still be consumed by the attacker. Thus NIPS can lessen the effects of a DoS or DDoS attack, but can not eliminate it all together.

HIPS (Host Intrusion Prevention System)

HIPS is software that resides on a server to provide protection to that system. HIPS works by inspecting all potentially dangerous system calls (such as write and delete). A properly configured system will prevent the deletion or writing to system files, and have provided proven protection against new worms. For example Entercept (a HIPS application) provided protection against Code Red worm before the worm had been identified and any other protection available (e.g. anti-virus software).
HIPS could be deployed on the WAFS ftp server to ensure that only legitimate ftp services are provided and deny all other actions.