International Civil Aviation Organization

SADISOPSG/13-WP/21
1/4/08

WORKING PAPER

SATELLITE DISTRIBUTION SYSTEM OPERATIONS GROUP (SADISOPSG)

THIRTEENTH MEETING

Dakar, Senegal, 27 to 29 May 2008

Agenda Item 6: Development of the SADIS
6.5: SADIS Internet-based FTP Service

ENHANCEMENTS TO THE SADIS FTP SERVICE

(Presented by the SADIS Provider State)

SUMMARY

This working paper provides a progress report on the implementation of enhancements to the SADIS FTP service, details some of the difficulties encountered by the SADIS Provider State to progress since SADISOPSG/12, and offers solutions to move the project forward.

1. INTRODUCTION

1.1 The group will recall that it formulated Conclusion 11/19 calling for the SADIS Provider State to proceed with the implementation of enhancements to the SADIS FTP service in accordance with the detailed plan presented to the SADISOPSG/11 Meeting. Moreover, the group will also recall that it formulated Conclusion 12/19 calling upon the SADIS Technical Development Team to review updated material prepared by the SADIS Provider State in relation to the enhancements to the SADIS FTP service.

1.2 This paper details some of difficulties encountered by the SADIS Provider State, since the last meeting, regarding the implementation of enhancements to the SADIS FTP service. Furthermore, this paper will outline SADIS Provider State recommendations aimed at fulfilling all of the aspects of SADIS FTP enhancements which the group has previously endorsed.

1.3 The SADIS Provider State provided a report to the SADIS Technical Development Team on 6 March 2008, detailing all of the following discussions.

2. DISCUSSION

2.1 The group will recall that, in the majority of cases, SADIS FTP was to be the beneficiary of a wider-range of enhancements that the UK Met Office (SADIS Provider) was implementing on its internet-based services. As such, progress of work in relation to SADIS FTP enhancements was dependant on a number of variables, some beyond the immediate control of the SADIS Provider.

2.2 The original proposal for SADIS FTP enhancements was four-fold. Namely, the implementation of:

a) Public Key Infrastructure (PKI);

b) Network Intrusion Prevention System (NIPS);

c) Host Intrusion Prevention System (HIPS); and

d) Dual server capability.

2.3 During 2006 and the first half of 2007, the Met Office had been running a project to implement the PKI technology. Following the SADISOPSG/12 Meeting, the PKI project ran into a number of technical difficulties with the ENTRUST software used for VPN tunnelling. Furthermore, issues arose with the UK certification authorities, limited in-house technical expertise, and the future need to use external contractors.

2.4 A number of options to move the project forward were considered by the PKI Project Board. However, since SADIS FTP was one of the few services requesting the PKI technology to be implemented within the Met Office, a clear steer was required on the preferred way forward.

2.5 By September 2007, due to the high cost of the project to date (borne by Met Office Core costs and not passed onto the SADIS community), and on-going issues with the immaturity of the technology and certification process, the decision was taken by the Met Office to close the PKI Project Board. The Secretariat was made aware of these difficulties and supported a recommendation that the SADIS Provider should evaluate alternative ways of moving the project forward with a view to completing the work within budget and to the original timescale. ICAO and the SADIS Provider were aware that any methodology adopted to move forward must cater for the provisions in the ICAO *Guidelines on the Use of the Public Internet for Aeronautical Applications* (Doc 9855).

2.6 In respect of the implementation of the Network Intrusion Prevention System (NIPS), the Met Office made some progress towards fulfilling this task during the first half of 2007. NIPS was installed and passed acceptance tests in March. By August, a Secure Collaboration Project (encompassing the initial elements of NIPS) had closed, having completed its activities in a Climate Research network environment of the Met Office. Further work on NIPS implementation is still being evaluated in view of more wide-ranging enhancements that the Met Office is making to its general levels of IT network security. One of the recommendations of future work is that a process for monitoring NIPS on a 24/7 basis, and reaction to alarm events, be implemented.

2.7 In respect if the implementation of Host Intrusion Prevention System (HIPS) and dual server capability, little, if any, work was carried out in 2007 – primarily in response to difficulties encountered to move the SADIS FTP enhancements project forwards.

3. NEW PROPOSALS FOR SADIS FTP ENHANCEMENTS

3.1 During the latter stages of 2007 and early 2008, the Met Office reviewed alternative ways to fulfil the obligations of the SADIS FTP enhancements project detailed at previous meetings, paying due consideration to: Doc 9855; the timescales and costs already endorsed by the SADISOPSG; and the impact that any changes in approach would have on end-users.

3.2 By early-March 2008, the Met Office determined that the SADIS FTP service could be improved in two stages (or phases). Firstly, to gain enhanced service resilience by making use of recently-developed infrastructure within the Met Office (Phase 1). Secondly, to develop a secure version of SADIS FTP with the required security enhancements (Phase 2).

3.3 Phase 1 entails a rebuild of the existing SADIS FTP application onto the Met Office's resilient operational internet FTP server (called FTPOPS). The Met Office has already initiated a policy of moving its IT systems away from a reliance on HP-UX – the Unix servers that are currently used to host SADIS FTP. Existing systems are being migrated to a 'supported architecture' – such as Linux-based PC-server platforms running recommended software. Once built, a network address translation change (so-called "NAT'ing") to the Met Office firewall would re-direct all existing users to the new system/server. Here, users would find the same data layout and have available their usual access methods and user-login procedure. No "migration" of users to the new system would be necessary, and the change would be largely transparent. Furthermore, the newly resilient platform would encompass cross-IT hall capability (i.e. service resilience), using tried-and-tested components such as an automatic file distributor.

3.4 The automatic file distributor (AFD) provides a framework for very flexible, non-stop delivery of a random number of files to multiple recipients or locations. AFD has been in operation at DWD in Germany for over 10 years, and the Met Office has utilised this technology with tremendous success in recent years. In respect of SADIS FTP, AFD would be used to deliver the OPMET, GRIB and SIGWX data to the appropriate directory/file locations in the most efficient manner.

3.5 The Phase 1 work is considered to be low risk, with easily implemented work packages that would attract little additional cost to support. The total set-up cost of the Phase 1 system is considered to be less than £5,000, and (subject to endorsement) could be launched as an operational service by January 2009 at the latest.

3.6 Phase 2 would involve building a *security-enhanced* version of SADIS FTP, requiring software and hardware architecture technologies – both of which are beyond the expertise of the support team maintaining the FTP servers. Preliminary discussions with relevant design authorities in these areas indicated that most of the security enhancements recommended by the SADIS FTP enhancements proposals (and reflected in 2.2 above) could be provided as part of a properly-managed project. However, the hardware architecture required, the development and application of IT security techniques, and the use of project-management and support team resources, implies a substantial cost to implement and maintain in the long term. There would be an initial set-up cost in the order to £30,000, plus project, development and licensing costs.

3.7 Nevertheless, this secure service is viewed, at least by the SADIS Provider State, as the "holy grail" solution to aspire to for SADIS FTP in future years – notably taking into account the future ICAO provisions for the use of the public internet in aeronautical applications (applicable in November 2010). Should the group endorse the Phase 2 proposals, the Met Office believes that they could launch SADIS FTP Secure as an operational service by November 2010.

3.8 Further details on the proposals of Phase 1 (SADIS FTP Enhanced) and Phase 2 (SADIS FTP Secure) are provided in the Appendix to this working paper.

4. ADVANTAGES AND DISADVANTAGES OF THE PROPOSALS

4.1 Phase 1 – SADIS FTP Enhanced

4.1.1 The advantages of progressing with Phase 1 include:

a) low-risk, with easy to implement work-packages utilising existing Met Office systems to support the service;

b) hardened resilient platforms;

c) virus scanning capabilities;

d) captive accounts;

e) system monitoring;

f) dual server capability across IT Halls which will ensure that there is a guaranteed level of performance and availability for users;

g) testing and implementation transparent to end users, with a dedicated test environment available to perform end-to-end tests before any changes are implemented on a live system;

h) existing SADIS FTP usernames and passwords will work on the new service, and users will still be able to access the existing SADIS FTP IP address – since the Met Office will use network address translation ("NAT'ing") techniques to route IP calls to the new servers;

i) existing users will not have to update their SADIS workstations to access the service once operational, since the directory structure will be unchanged.

4.1.2 The disadvantages of progressing with this Phase 1 include:

a) some procurement and set-up costs will be incurred – although these are not expected to be considerable;

b) lack of security features – e.g. digital signing is unlikely to be available.

4.2 Phase 2 – SADIS FTP Secure

4.2.1 The advantages of progressing with Phase 2 include:

a) enhanced security features (including encryption and digital signing), and opportunity to improve security features through the life of the service;

b) hardened resilient platforms;

c) virus scanning capabilities;

d) captive accounts;

e) system monitoring;

f) dual server capability across IT Halls will ensure that there is a guaranteed level of performance and availability for users;

g) implementation can occur at any time after completion of Phase 1. The SADIS FTP Secure service could be introduced as a parallel service with the pre-existing service. This would afford users the opportunity to migrate to the secure service at their convenience during a parallel running period;

h) testing will be not impact existing SADIS FTP users, as it would be developed as a new "stand-alone" service;

i) a dedicated test environment would be available to perform end-to-end tests before any changes are implemented on a live system; and

j) conformance with the requirements/recommendations of Doc 9855.

4.2.2 The disadvantages of progressing with Phase 2 include:

a) moderate to high-risk strategy, with new/emerging technologies and external expertise required to implement;

b) considerable cost initial cost to initially set-up, plus project, development and licensing costs;

c) potential for significant costs to maintain and support the system;

d) longer-term timescale to implement;

e) requirement for new user login credentials – i.e. existing SADIS FTP usernames and passwords would NOT work on the new service, and users would be expected to migrate from the pre-existing service to the secure service during a parallel running period; and

f) existing users will be need to update their SADIS workstations to access the new service, since login credentials and directory structure will not be the same at the traditional service. This however, could be built into the normal workstation update lifecycle, should the parallel running period be long enough.

5. IMPLEMENTATION TIMESCALES

5.1 Phase 1 is considered considerably more straightforward (and less expensive) to implement compared to Phase 2. Much of the SADIS FTP Enhanced system (phase 1) will utilise pre-existing IT architecture that the Met Office utilises for its internet based services. Subject to endorsement by this group, the Met Office expects that they would be able to launch a Phase 1 system by January 2009 at the latest.

5.2 Understandably, Phase 2 involves considerable more work. In view of this, the Met Office considers that 12 to 18 months would be required to deliver a SADIS FTP Secure service. If the SADISOPSG were to endorse further details and recommendations at the next meeting (circa May 2009), the Met Office would expect to be able to deliver the secure FTP service by November 2010. This timescale would be consistent with ICAO Annex 3 amendment proposals. The SADIS Provider State would recommend a parallel running period (of at least 12 months) to allow existing users to migrate to the SADIS FTP Secure service. All new users would be immediately invited to utilise the secure service. After the parallel running period, it is envisaged that the original service (SADIS FTP Enhanced) would be withdrawn.

6. CONCLUSION

6.1 In view of moving the project forwards, the group is invited to formulate the following draft conclusion:

Conclusion 13/.. — SADIS FTP enhancements

That, the SADIS Provider State, in co-ordination with the SADIS Technical Development Team, be invited to:

a) progress with the development and implementation of a SADIS FTP Enhanced service (to be referred as “Phase 1”), for introduction by SADISOPSG/14 at the latest; and

b) provide further information (including costs, scope and timescales) to the SADISOPSG/14 meeting relating to a SADIS FTP Secure service (to be referred as “Phase 2”).

Note 1.— Both services will be expected to benefit from dual server capability and network address translation, as a minimum.

Note 2.— The SADIS FTP Secure service will be expected to incorporate security enhancements in accordance with ICAO Doc 9855, Guidelines on the Use of the Public Internet for Aeronautical Applications.

7. ACTION BY THE SADISOPSG

7.1 The group is invited to:

a) note the information in this paper; and

b) decide on the draft conclusion proposed for the group's consideration.

— — — — — — — —

APPENDIX

SADIS FTP ENHANCEMENT PROPOSALS

1. PHASE 1 – SADIS FTP ENHANCED SERVICE

1.1 Platform

1.1.1 The Met Office has recently developed a network of Linux-based server pairs to manage traditional general-purpose data transfers across its internal production systems, and beyond to its external customer and partners' networks. Internet partners are served from a server-pair located within an Internet-facing de-militarized zone (DMZ), called 'FTPOPS'. The DMZ is replicated across two resilient, largely-independent, computing halls. The servers are hardened to limit potential user mal-practice and virus-scan all files written there, though host-intrusion detection is not currently employed.

1.1.2 A secure FTP package is used to ensure users are captive and have read-only access to their data area. Two component packages are used to (a) mirror designated data areas (b) automatically fail-over the data-transfer application in the event of a problem.

1.1.3 The servers present a single service address which is directed to the active server. The second server's disk system is mirrored to reflect the current state of the active server. Its applications are quiesced (i.e. made quiet) and a monitoring process listens on a dedicated heart-beat connection. If the heartbeat ceases, the second server activates a list of applications and assumes the service address with minimal disruption. The service can also be manually 'failed over' transparently for preventative maintenance purposes, if needed. The servers are monitored by a Tivoli agent reporting back to support teams via GUI warning displays and the automatic raising of Incident reports.

1.2 Data Provision

1.2.1 Currently data is supplied from the Met Office message switch (Frost) as a series of files of batched WMO bulletins. The SADIS FTP application resides on a resilient HP-UX cluster, which is not replicated in another computing hall.

1.2.2 The Perl application performs the actions of de-batching files into individual bulletins, and writes these to a hierarchical directory structure. Other housekeeping functions aggregate files over time and purge to maintain the agreed data lifetime.

1.2.3 The existing platform 'FTPOPS' has an extensive customer-base of users and has its own file-transfer and data-management application. It has an allocated bandwidth to the Internet using packet-shaping technology applied upstream. Including the SADIS FTP automatic file distributor (AFD) application and its associated user base on FTPOPS is within its operating capability.

1.2.4 Figure A1 below indicates the proposed configuration of the SADIS FTP Enhanced service (Phase 1).

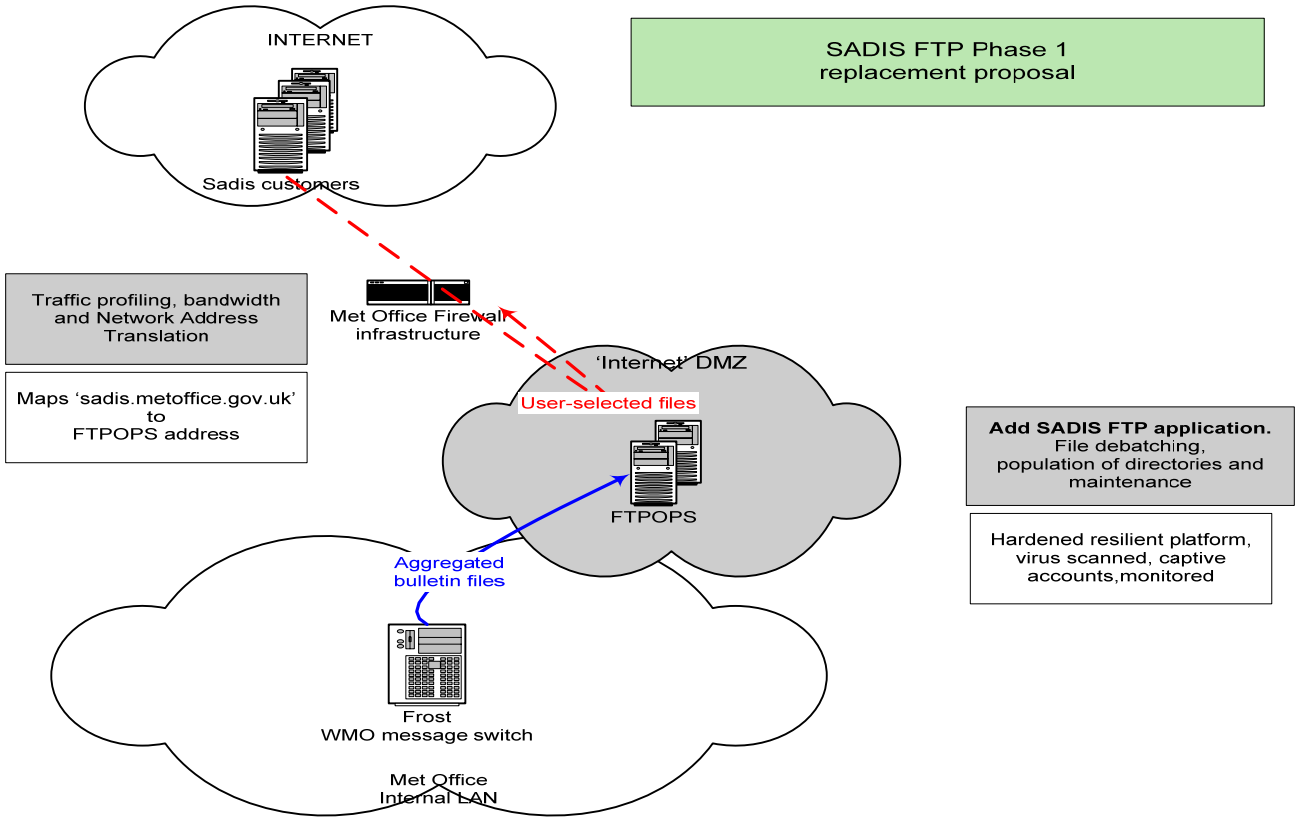

Figure A1 – SADIS FTP Enhanced proposal (Phase 1)

2. PHASE 2 – SADIS FTP SECURE

2.1 To achieve the security levels deemed appropriate to meet the user and ICAO requirement, it is considered necessary that the secure functions should be split between platforms in the secure internal Met Office LAN (where file-encryption and digital signing is performed) and the Internet facing DMZ (where the 'FTP' server platform is especially hardened to prevent intrusion, and also performs PKI certification functions). Third party certification facilities could be used to complete this activity.

2.2 Virtual-server technology is suggested to provide a managed, resilient platform in each location.

2.3 In view of the enhanced capability of this service, it would be important to provide users a period of parallel phase 1/phase 2 running to facilitate changeover to end-user workstations.

2.4 Figure A2 below indicates the proposed configuration of the SADIS FTP Secure service (Phase 2).

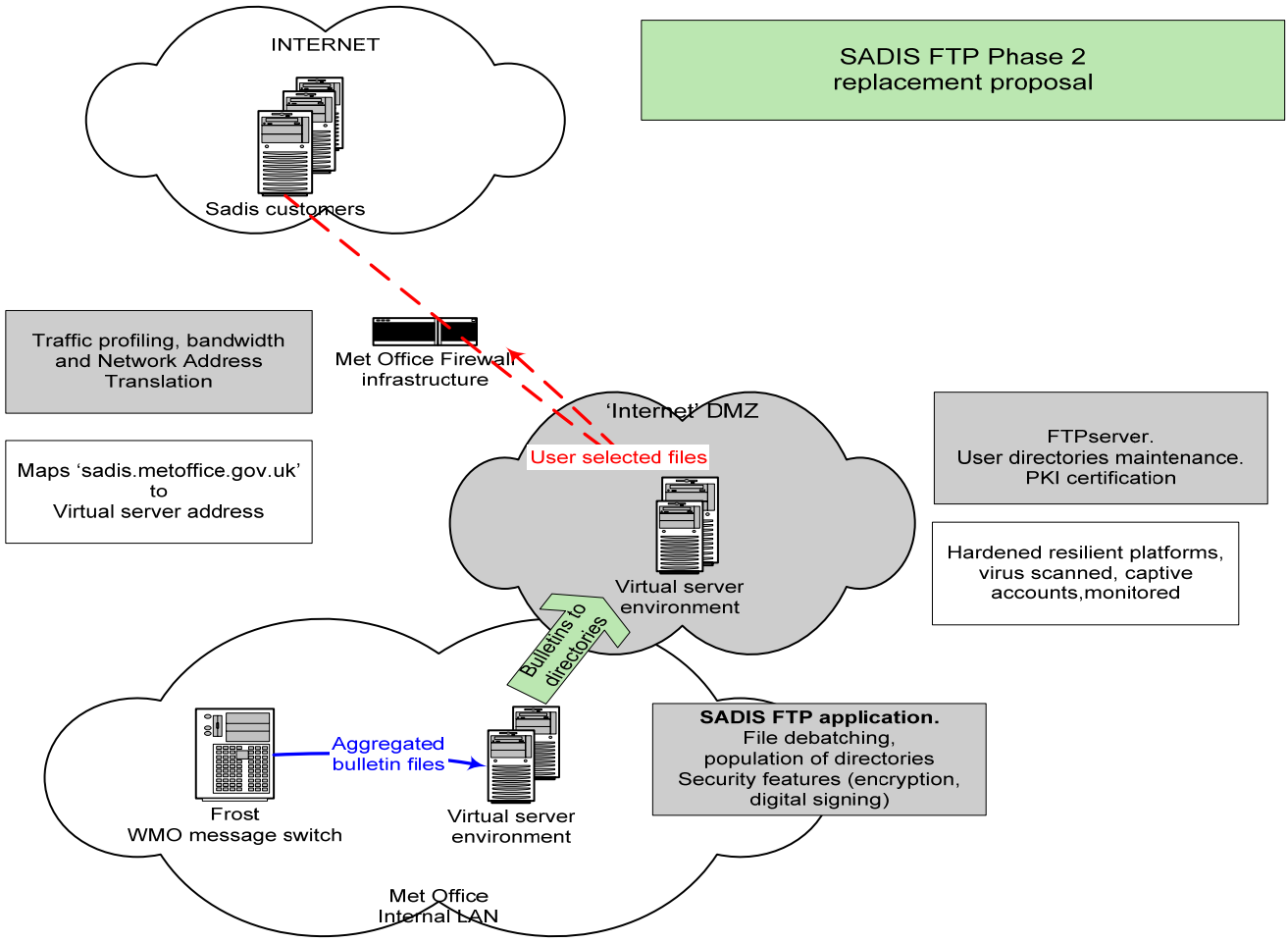

Figure A2 – SADIS FTP Secure proposal (Phase 2)

— END —