FSA Modernization Partner

Electronic Mass Mailings Whitepaper: Recommendations by the ASG

Version 1.0

AWG Support Group &
Business-Technology Alignment

Document Revision History

Version No.	Date	Contributors	Revisions Made
1.0	June 26, 2002	Sponsor: Martin Renwick Author: Bill Malyszka Contributors: Karen Anderson, Wayne Chang, David Elliot, Milton Thomas, Brenda Ware	White paper describing the proposed email policy for FSA to address testing, operations, and message design

Contents

Introduction **4**

Context **4**

Investigation *4*
FSA Electronic Mail Architecture *4*
Issues *5*

Scope **6**

Assessing Need **6**

Descriptions of Possible Solutions **7**

Technical Recommendations **7**

Basis For Recommendation **8**

Implications of Recommendations **8**

Existing Systems *8*
New Systems *9*

Appendixes **12**

Introduction

Federal Student Aid's (FSA's) Business-Technology Alignment (BTA) framework utilizes a pragmatic, "just-in-time" approach to the development of technical architecture standards. The approach is to develop and recommend technical standards on an as-needed basis for the specific project need while taking an enterprise perspective. Thus, when a need for a FSA technical standard is identified by a project, an effort is initiated to identify options, conduct the necessary analysis and make recommendations driven by the needs of that particular project, but based on the most appropriate benefits and tradeoffs from a FSA-wide perspective. This focuses the effort and the limited resources where they are most needed and will make the greatest impact, while continuing to populate FSA's technical standards guide.

This document describes the issue triggering the need for establishing standards for electronic mass mailing including message construction, message routing, and mail system testing. Then, recommendations are made based on an analysis of the options. This analysis does not address the data security needs for electronic mail transmission. Nor does it address the electronic mail receipt verification that is required when sending financial information. Individual projects will develop security and receipt verification policies for electronic mail. These may be considered for generalizing to enterprise policies if the need arises.

Context

Investigation

The need for sending electronic mass mailings has triggered this investigation and recommendation for establishing enterprise architecture standards. The necessity for standards stems from several projects that implement communication with customers through electronic mail. The FSA Architecture Working Group (AWG) has requested the AWG Support Group (ASG) to recommend standards and guidelines for electronic mass mailing design, testing, and operations. The investigation will include an inventory of what email services are currently implemented or planned. This request follows the procedures of the Business Technology Alignment (BTA) framework developed by FSA.

FSA Electronic Mail Architecture

The FSA electronic mail architecture is used to relay messages to FSA customers. Electronic mail messages to customers are constructed by system applications within either the Virtual Data Center (VDC) or other Application Service Provider (ASP) systems. Within the VDC, electronic mail messages are relayed through the Integrated Technical Architecture's (ITA's) mail framework or through non ITA mail relay systems. All mail relayed from the VDC is routed to Department of Education (ED) mail servers which then relays it to recipient mail servers via the internet. Electronic mail relayed from the ASP systems goes through the internet directly to recipient mail servers.

The illustration below provides a logical portrayal of the FSA email architecture.

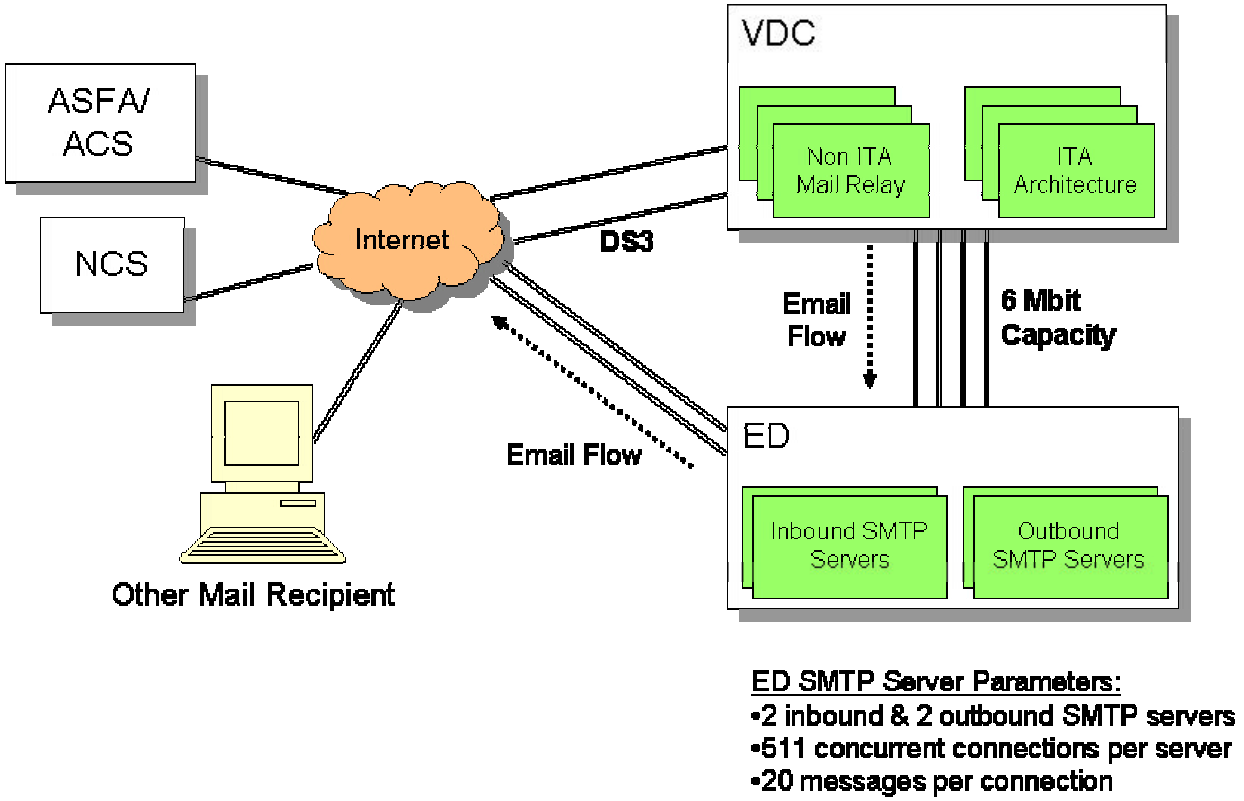

Figure 1 FSA Email Architecture Logical Model

The ED mail server parameters are listed in Figure 1 FSA Email Architecture Logical Model. The constraints of the ED server are imposed on other servers that initiate a connection. This is negotiated through server-to-server communication when the connection is initiated. Application systems using ITA for mail handling, are responsible for message construction, message size, and the attachment of files to the message. ITA does not impose limitations on the construction of messages or the number of messages sent. It is merely a conduit for applications systems to relay messages to the ED servers.

Issues

There are three issues which surround the relaying of electronic mass mailing. These relate to the three components of the scope of this investigation.

First, as organizations increasingly use electronic mail to communicate with customers, a side effect has emerged which is Unsolicited Bulk Email (UBE) or “spam”. UBE is commercial communication sent to recipients who have not intentionally given permission for their email addresses to be included on a mass mailing list. UBE is seen by many Internet Service Providers (ISPs) as electronic mail abuse, and they have taken steps to filter out UBE. The filters rely on characteristics of the email header or body to determine whether an email message should be treated as UBE. The filtering logic can result in a false positive in which a message is deemed to be

UBE when it is not. FSA can minimize the probability of an ISPs UBE filter labeling an FSA message as "spam" by employing best practices in constructing the message header.

The second issue involves mail relay capacity within the Department of Education. As all electronic mail generated from the VDC is relayed through ED mail servers, the capacity of both FSA and ED servers must be considered when electronic mass mailing is added to the electronic mail already used for other business functions. The risk is that the electronic mass mailing sent to customers will exceed the ED and FSA mail server capacity and result in interruptions to other business processes that rely on the mail servers. The capacity of FSA and ED mail servers can be impacted by both production and testing systems that are generating email messages.

The third issue is testing. One of the events that prompted the AWG to investigate electronic mass mailing was a testing incident that resulted in the "ed.gov" domain being rejected by Hotmail. The incident report and follow up meeting notes are attached as Appendix A. In short, the cCampus Based testing team set up a Hotmail account to test the email relay services in their system. They sent several thousand emails to one account on Hotmail during this test. Hotmail perceived a Denial of Service (DoS) attack and rejected the "ed.gov" domain in response. FSA testing guidelines can prevent this type of incident.

Scope

FSA system managers and application developers require standard procedures to design, test, and operationalize the transmission of electronic mass mail employed to meet their overall business needs. This document provides proposed recommendations for:

- The construction of an electronic mail message which will minimize the likelihood of triggering UBE filtering.
- The scheduling of electronic mass mailing in production which will minimize the impact on other FSA and ED email communication.
- The setting of email relay testing guidelines which will prevent DoS incidents.

This document does not address the following, which represent future topics to be addressed by the Architecture Working Group:

- The secure transmission of Privacy Act data through electronic mail.
- The tracking and verification of receipt of financial documents transmitted through electronic mail.

Assessing Need

The Technical Lead of an FSA system application employing electronic mail to communicate with external customers or partners will need to assess the impact their application will have on the FSA and ED email architectures. The assessment should include:

- Construction of the message header
- Size and contents of the message body
- Frequency with which messages will be relayed (number of messages per period of time)
- Peak and average email relay volume

Descriptions of Possible Solutions

The following are solutions for the construction, relaying, and testing of electronic mass mailing performed by FSA systems:

1) When a system application constructs an email message, only one recipient email address will be placed in the "To:" line. No other recipients will added to the "CC:" or "BCC:" lines..

2) When testing electronic mass mailing, a maximum of 100 email messages will be sent at one time. The testing team will notify the system administrator of the server that will receive the test messages before testing.

3) FSA system applications will send email to customers during nonbusiness hours. Normal business hours for FSA are 8 a.m. EST to 6 p.m. EST.

4) Outsourcing the SMTP relaying services for sending electronic mass mailings. This will reduce the impact on capacity made by electronic mass mailing.

5) Subscribe to an electronic mail service that specializes in capability testing. This will eliminate the need to establish a "dummy" account to receive the test messages. The service may also provide performance measures that can be used to optimize the application system.

Technical Recommendations

Below are recommended solutions for the construction, testing, and operations of electronic mass mailing by FSA systems.

1) *Construction of message* When a system application constructs an email message, only one recipient email address will be placed in the "To:" line. No other recipients will added to the "CC:" or "BCC:" lines. The message body will contain either plain text or HTML. No file attachments will be sent through a system application constructed message intended to be sent to a customer.

   ***Rationale*:** Multiple recipients in a message header may trigger UBE filters resulting in the message not being rejected. Using one recipient's email address in the header will prevent UBE filters from rejecting the message. File attachments significantly increase the size of a

message. This places a great strain on the email infrastructure. Other protocols such as HTTP or FTP can be used to transfer files to customers.

2) *Electronic Mass Mailing Testing* When testing electronic mass mailing, a maximum of 100 email messages will be sent at one time. The testing team will notify the system administrator of the server that will receive the test messages before testing.

   Rationale: Notifying the system administrator of the recipient system before testing will assure the system test will not result in the originating domain being perceived as launching a Denial of Service (DoS) attack on the recipient machine.

3) *Electronic Mass Mailing Operations* FSA system applications will send email to customers during nonbusiness hours. Mail will be sent before 8 a.m. EST or after 6 p.m. EST.

   Rationale: Sending email during nonbusiness hours will prevent email sent by FSA system applications from consuming server connections resulting in poor email performance. Email sent during nonbusiness hours will task the email servers during off peak times.

Although these recommendations are suitable in the majority of instances, an application may have a specialized need for an alternative electronic mass mailing implementation. Such alternatives will be reviewed by the ASG for recommendation to the AWG as an FSA enterprise standard on a case-by-case basis.

Basis For Recommendation

Emerging project needs require capabilities that do not currently have architecture standards defined to support them. There are several projects (for example, eCampus Based and Consistent Answers) that have the requirement to communicate with customers or partners through electronic mail. The ASG has conducted the necessary research to identify electronic mass mailing procedures that follow industry best practices and standards, while satisfying federal and FSA policies, as well as, technical constraints. The analysis conducted was used as a basis for the recommendations in this document.

Implications of Recommendations

Existing Systems

Current FSA systems are constrained by the present email architecture parameters. To maintain the electronic mail server capacity necessary for business processes, these recommended guidelines will be adopted by all existing systems. All business processes using email services rely on the ED SMTP servers to relay email messages. Also, message construction and email services testing that does not follow the recommended guidelines in this document may result in false positive UBE filtering or a perceived DoS attack. These risks and the subsequent consequences are outside FSA's control.

New Systems

New system applications, not already in production, will meet all recommended guidelines for electronic mass mailing testing and operations found in this document and adopted by the AWG. If a project team requires an exception to these guidelines, the AWG will review and determine if the exception is warranted based on business or technical case for granting the exception.

Option	Description	Implementation Alternatives	Costs	Benefits	Cons
One recipient per email message, no file attachments	When a system application constructs an email message, only one recipient email address will be placed in the "To:" line. No other recipients will added to the "CC:" or "BCC:" lines.. No file attachments will be included in electronic mass mailing messages.	Constrain message construction in the application system, in the ITA framework for systems using the ITA framework, or at the server.	Existing systems would need to comply with the message construction constraints adopted to minimize risk.	• Will prevent false positives from ISP UBE filter • Will minimize the impact a message will have on the email architecture	• Existing systems will need to redesign the message construction capabilities
Limit the number of test messages	When testing electronic mass mailing, a maximum of 100 email messages will be sent at one time. The testing team will notify the system administrator of the server that will receive the test messages before testing.	No limiting the number of test messages may result in a perceived Denial of Service (DoS) attack and blocking of the "ed.gov" domain.	No cost	• Will minimize the probability of being perceived as launching a DoS attack • Will reduce the burden that testing email relaying will have on the ED and FSA email capabilities	• Performance testing of relaying a large number of messages will not be feasible.
Electronic Mass Mailing will be sent during off business hours	FSA system applications will send email to customers during nonbusiness hours. Normal business hours for FSA are 8 a.m. EST to 6 p.m. EST.	Sending email during off business hours will reduce the impact on other business related email. This is implemented by application systems.	No cost	• Will reduce impact on other business email • Will minimize the impact of electronic mass mailing on the ED and FSA email architecture	• Constrains when mass customer communication can occur
Outsourcing email relay services	Outsourcing the SMTP relaying services for sending electronic mass mailings. This will reduce the impact on capacity made by electronic mass mailing.	Implementation alternatives include managing email traffic to minimize the impact of electronic mass mailing on	Cost to vendor	• Administration of services is done by vendor • Can purchase necessary capacity	• Present email infrastructure has no significant associated cost compared to outsourcing to a vendor

Option	Description	Implementation Alternatives	Costs	Benefits	Cons
Subscribe to email testing service	Subscribe to an electronic mail service that specializes in capability testing. This will eliminate the need to establish a "dummy" account to receive the test messages. The service may also provide performance measures that can be used to optimize the application system.	An alternative is to coordinate with an existing FSA Modernization Partner email server for testing.	Cost to vendor	• Administration of test server is completed by vendor • Can purchase the testing services required and not incur cost of system when idle. • Vendor may provide specialized performance testing not available through no cost alternatives	• Cost to vendor when there are no cost solutions available

Appendixes

Appendix A: eCampus Based Incident Report

Appendix B: Unsolicited Bulk Email: Mechanisms for Control