

NIH Primary Email Address V1.0

Status of this Memo

This document specifies a standard for the National Institutes of Health (NIH) and requests discussion and suggestions for improvements. Distribution of this memo is unlimited. This NIHRFC specifies a National Institutes of Health (NIH) standard for NIH primary email addresses. This standard, defined in Sections 3 and 4 of this document, was approved by the NIH Architecture Review Board (ARB) on March 25, 2009. This standard supersedes the description of Primary Email in Table 1 of NIHRFC0002: Person Name.

Table of Contents

1	Introduction.....	1
2	Background.....	1
2.1	Security Risk.....	1
2.2	S/MIME Compatibility.....	2
2.3	Creation and Portability.....	2
3	Standard NIH Email Naming Convention.....	3
3.1	Given Name.....	3
3.2	Surname.....	3
3.3	Numeric Qualifier.....	3
3.4	Order of Name Construction.....	4
3.5	Examples.....	4
4	Implementation.....	4
4.1	The Use of Email Aliases.....	5
4.2	Required Use of Primary SMTP Email Address.....	5
4.3	Persistence of NIH Email addresses.....	5
5	References.....	5
6	Contact.....	6
7	Security Considerations.....	6
8	Changes.....	6
9	Author's Address.....	7
	Appendix A: Author's Response to Comments.....	8

1 Introduction

This NIHRFC defines a standard syntax for the primary SMTP email address (default reply-to) for a person as represented by Central Email Service (CES) at NIH. The use of this proposed syntax will:

- Improve IT security
- Facilitate the use of S/MIME (Secure / Multipurpose Internet Mail Extensions) for public key encryption and digital signing of e-mail
- Simplify the creation and portability of NIH Personal Identity Verification (**PIV**) ID badges issued under Homeland Security Presidential Directive 12 (**HSPD-12**), Policy for a Common Identification Standard for Federal Employees and Contractors¹.

2 Background

IETF RFC 2822, Internet Message Format², defines an email address as a locally interpreted string followed by the at-sign character (“@”) followed by an Internet domain (i.e., local-part@domain-part). NIHRFC0002, Person Name³, sets the local-part of the primary email address to be identical to the Active Directory (AD) system account name (sAMAccountName). At NIH, the domain-part of the email address varies by IC and usually appears as either mail.nih.gov or <ic>.nih.gov (e.g., sAMAccountName@nhlbi.nih.gov).

As documented in the following sections, the current NIH email address standards have a number of problems, including: 1) it raises a slight IT security risk, 2) it creates S/MIME interoperability issues and 3) it complicates the issuance and portability of PIV ID badges. The alternative standard proposed by this NIHRFC mitigates these concerns.

2.1 Security Risk

The current standard, which sets the local-part of the email address to the user’s sAMAccountName (AD account name), presents an IT security risk in that it publicizes the user’s account name and the domain can be easily ascertained. Displaying and/or publicizing the user’s account name are contrary to NIST security recommendations⁴.

2.2 S/MIME Compatibility

S/MIME mail encryption and digitally signed email (S/MIME) is dependent upon the email address specified in the public key infrastructure (PKI) issued digital certificate. Most email clients will not permit a user to send an encrypted email to an email address that is different from the one specified in the digital certificate used to encrypt the email. Likewise, email clients will not validate a digitally signed email that was received from an email address that is different from the one specified in the signer's digital certificate.

To insure S/MIME compatibility, this standard requires that the user's reply-to address always match the primary SMTP email address defined by this standard. Furthermore, the primary SMTP email address must be the only address that can be obtained electronically by email clients from an externally facing directory.

2.3 Creation and Portability

HSPD-12 mandates that all Federal staff receive a new smartcard ID badge. This ID badge, known as the PIV card, contains PKI digital certificates that support user authentication and encrypted and digitally signed email. At NIH, the issuance of PIV cards is a component of the staff induction process (i.e., new hire process) supported by the NIH Enterprise Directory (NED), the HHS Identity Management System (IDMS) and a number of other related IT systems. To create a PIV card, NED must pass the primary SMTP email address of the person who is being issued the PIV card, to the HHS IDMS.

Having an individual's email address linked to their PIV ID badge raises two issues:

- 1) The PIV badge may be issued before the individual receives a NIH email account; and
- 2) When an individual transfers to another IC their email address may change requiring the individual to obtain new digital certificates for their PIV card.

A uniform syntax for the NIH primary SMTP email address, as proposed by this standard, simplifies the creation of an individual's email address (even before their email account is established). The use of a NIH-wide common domain-part of the email address, as proposed by this standard, ensures that as long as an individual's PIV card remains valid; their email address will not change regardless of their IC. (Note: a legal name change requires the issuance of a new PIV card).

3 Standard NIH Email Naming Convention

The standard syntax for the primary SMTP email address for all NIH staff represented in the NIH Central Email Service will be:

[givenName.Surname\[numeric-qualifier\]@nih.gov](#)

The local-part of the NIH email address is constructed from the mailbox owner's given name (first name) and surname (last name), separated by a period character (ASCII value 46). In the event of a name collision, a numeric qualifier will be appended to the surname. The domain-part of the email address will always be set to *nih.gov*. The rules for constructing the local-part of the NIH email address are detailed in the sections below.

3.1 Given Name

The mailbox holder's givenName, used to construct the local-part of their email address, is defined in accordance with NIHRFC0002: Person Name³ and may be either the common (preferred first name) or legal first name of person. The first name may contain hyphens and apostrophes; however, in accordance with RFC 2822, spaces (ASCII value 20) are not permitted.

3.2 Surname

The mailbox holder's Surname, used to construct the local-part of their email address, is defined in accordance with NIHRFC0002: Person Name³ and may be either the common (preferred last name) or legal last name of person. The last name may contain hyphens and apostrophes; however, in accordance with RFC 2822, spaces (ASCII value 20) are not permitted.

3.3 Numeric Qualifier

A numeric qualifier will be appended to the last name when the combination of the user's first and last names fails to produce a unique NIH primary SMTP email address (i.e., name collision with a pre-existing NIH email address). The numeric qualifier will consist of one or more digits ("0" – "9", ASCII values 48 – 57), with no leading zeros. The numeric qualifier will be assigned sequentially, starting with the digit two (2), and continuing (i.e., 2, 3, 4 ...) until a unique NIH email address is generated.

3.4 Order of Name Construction

The local-part of a mailbox holder's email address may be constructed from either the mailbox holder's preferred or legal names (assuming that they are different). The use of the preferred vs. legal name will be applied in the following order until a unique NIH email address is derived:

- 1) Preferred givenName + preferred Surname; then
- 2) Preferred givenName + legal Surname (if different); then
- 3) Legal givenName + preferred Surname (if different); then
- 4) Legal givenName + legal Surname (if different); then
- 5) Preferred givenName + preferred Surname + numeric qualifier

3.5 Examples

Following this standard, the sequential processing of the following individuals would yield the associated NIH primary SMTP email addresses:

1. Mary C. Martin -> Mary.Martin@nih.gov
2. Rose Marie Smith -> RoseMarie.Smith@nih.gov
3. Peter O'toole -> Peter.O'toole@nih.gov
4. Peter Pan-Cook -> Peter.Pan-Cook@nih.gov
5. Mary D. Martin -> Mary.Martin2@nih.gov

4 Implementation

All new NIH primary SMTP email address shall be assigned in accordance with the standard NIH email naming convention rules defined in Section 3. It is recommended, but not required that existing (legacy) NIH email addresses be converted to the new format.

4.1 The Use of Email Aliases

This standard does NOT prohibit the use of email aliases that contain a local-part and/or domain-part that does not adhere to this standard. However, the alias may not appear in outgoing SMTP email address fields (e.g., reply-to address) or be electronically distributed to email clients (e.g., via an electronic LDAP directory inquiry). Email aliases may appear in electronic and/or printed media (e.g., publications, business cards, etc.) and may be distributed through other informal means (e.g., provided verbally).

4.2 Required Use of Primary SMTP Email Address

This standard requires that all NIH staff use their primary SMTP email address (as defined by this standard) for their reply-to address. This standard also requires that the primary SMTP email address must be the only address that can be obtained by email clients from an externally facing NIH electronic directory.

4.3 Persistence of NIH Email addresses

NIH Email addresses need to be persistent (i.e., an email address, once assigned, must not be assigned to another individual). While the rules governing email address persistence are beyond the scope of this standard; this standard supports persistence through the use of the numeric qualifier defined in Section 3.3.

5 References

1. Bush, George W., President of the United States of America. Homeland Security Presidential Directive/HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors. <http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>. August 27, 2004.
2. Resnick, P., RFC 2822: Internet Message Format, <http://www.ietf.org/rfc/rfc2822.txt>, April 2001.
3. Sharp, J., NIHRFC002: Person Name, <http://enterprisearchitecture.nih.gov/NR/rdonlyres/B6CC7AE9-A6AA-44E7-8452-51D20B8E1AA1/0/NRFC0002.pdf>, January 2007.

4. Souppaya, Murugiah; Kent, Karen and Johnson, Paul. NIST Special Publication 800-68: Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist. October 2005.

6 Contact

To contact the NRFC Editor, send an email message to EnterpriseArchitecture@mail.nih.gov.

7 Security Considerations

1. The primary SMTP email naming convention proposed by this standard mitigates the security risk associated with publicizing a user's login account name (i.e., sAMAccountName)
2. The primary SMTP email naming convention proposed by this standard mitigates S/MIME issues with (email encryption and digital signatures) associated with mismatched email addresses.
3. The Primary SMTP email convention proposed by this standard will mitigate potential problems with the creation and portability of NIH Personal Identity Verification (**PIV**) ID badges issued under Homeland Security Presidential Directive 12 (**HSPD-12**), Policy for a Common Identification Standard for Federal Employees and Contractors.

8 Changes

Version	Date	Change	Authority	Author of Change
1.0	5/29/08	Original Draft	NRFC0001/BCP0001	Mark Silverman
1.1	6/16/08	Incorporated suggested changes from NED team.		Mark Silverman
1.2	7/01/08	Incorporated suggested changes from EMIB.		Mark Silverman
1.3	10/20/08	Incorporated edits from IT Architect; added order of name		Mark Silverman

		construction.		
1.4	11/20/08	Added legacy email		Mark Silverman
1.5	12/30/08	Minor Edits		Mark Silverman
0.7	03/19/09	Re-numbered the versions to ensure they start with v0.1		Anja Holovac – NIH OCITA
0.8	03/19/09	Created Appendix “Author’s response to comments” and added comment responses from NIH Portal	NIHRFC0001	Anja Holovac – NIH OCITA
1.0	03/25/09	Approved by the ARB. Updated version number to 1.0	NIHRFC0001	Anja Holovac – NIH OCITA

9 Author’s Address

Mark Silverman
 National Institutes of Health
 10401 Fernwood Road
 MSC 4806
 Bethesda, Maryland 20817
 Phone: 301-435-8190
 Email: Mark.Silverman@nih.gov

Appendix A: Author's Response to Comments

Comment 1: Removing the IC from the name of the standard degrades the "branding" value of the various Institutes. This may seem like a small point, but in correspondence with colleagues this could be seen as a diminishment of the independence and unique value of each IC.

Response: NIHRFC0034 permits the use of email aliases, which allows the unique IC "brand" to still be prominently displayed as part of a published email address (e.g., journal articles, business cards, etc.). Removing the IC label from the primary SMTP email address (i.e., default from/reply-to email address) eliminates problems people could face in transferring between ICs. NIH staff will soon receive a new HSPD-12 ID badge that contains PKI digital certificates that assert their logical identity (i.e., email address). When someone changes their email address (e.g., by transferring to a new IC) their digital certificates can no longer be used to send that individual an encrypted email or enable that individual to digitally sign an email. As a result,

- a) the person must go through a process to verify their "new" logical identity and load new digital certificates onto their badge;
- b) everyone the person communicates with, must update their own local contacts list (since the contact information and certificates for that person have changed); and
- c) the person must update every (non-NIH) LISTSERV that they are subscribed to (since their new email address will not allow them to post to those LISTSERVs).

Having a standard, NIH-wide email address eliminates this burden placed on NIH staff that move from IC to IC which, in my opinion, more than offsets the loss of the IC brand from an automated (as opposed to published) email address.

Comment 2: A security point has been raised that documents that are encrypted using the PIV cards while in the employ of a specific Institute should not necessarily be available to that employee once they leave the Institute. Thus by "breaking" the encryption by including the IC in the email address it would be a defacto management control for IC specific sensitive data.

Response: PKI digital certificates enable a third party to send an encrypted email to a certificate holder. When a person's certificate becomes invalid (e.g., the email address changes), that individual can no longer receive encrypted email. However, as long as the individual has the private key associated with the digital certificate, they can still read previously encrypted email. Therefore, breaking encryption through an email address change provides no management control over previously encrypted data; it only imposes a technical burden on the individual and everyone who needs to securely communicate with them.

Comment 3: The use of numerical augments to the email names may provide a means of creating more uniqueness, however increased uniqueness likelihood could also be achieved by the addition of the IC in the address.

Response: Email addresses must be unique. Using a person's name to construct an email address will inevitably lead to a name collision; the addition of the numerical qualifier ensures

the email address is unique. Including the IC as part of the email address may reduce, but does NOT eliminate the risk of a name collision. This risk is particularly high at NIH since NIH has a policy of providing an email address for life (e.g., an email address published in a journal will always be associated with the author, even if the author is no longer affiliated with NIH).

Comment 4: A concern about the costs that would be incurred by requiring users to update their PIV cards when changing ICs is valid, however based on my discussions this is a cost that would be overall modest per year, and readily agreeable to ICs to achieve the value outlined above.

Response: I agree that key issue behind NIHRFC0034 is the tradeoff between having the IC name in the automated email address vs. the burden (i.e., cost) incurred when an individual moves to a new IC. While the monetary cost associated with the physical badge is minimal to non-existent, the inconvenience and labor costs associated with the time it will take people to update their PIV cards and deal with the email change (e.g., notify correspondents, update LISTSERVs, etc.), coupled with the labor cost of the NIH staff needed to assist those individuals, could be quite significant. I believe that most ICs will find these "costs" unacceptable, especially when it is incurred by an IC that does not brand its email addresses (i.e., someone transfers from a "branded" IC to an IC using the common NIH email domain)

Comment 5: Encryption options have been available for some time at NIH, however the routine use of this facility is rare, thus the likely "breaking" of encryption when moving to another IC is a small issue when compared to the value of including the IC name in the standard.

Response: I agree that current PKI use at NIH is limited to less than 4000 subscribers. One objective of HSPD-12 is to provide all Federal staff with digital certificates. OMB and HHS are already indicating that the use of these certificates will soon become much more widespread (i.e. required). Given the "cost" of updating an email address imbedded in a HSPD-12 ID badge, we cannot wait until after NIH has issued 40,000+ badges to see if the "breaking" problem becomes a major issue.

Comment 6: What do you do with people who go by their middle names rather than their first names such as C. Everett Koop or J. Edgar Hoover?

Response: NIHRFC0034 gives priority to use of the preferred name (as opposed to legal name) in composing the email address. Using your example, the email address would be Everett.Koop@nih.gov.

Comment 7: Using "Numeric Qualifiers" to differentiate identical names has caused serious problems at NIMH on at least two previous occasions with regard to the payroll and personnel systems. Numeric Qualifiers cause user and system email errors and should be avoided, if at all possible. Perhaps adding the IC to the "local-part" as a preferred order of construction prior to adding a "Numeric Qualifier" would suffice.

Response: I am perplexed as to why a number in a person's email address would affect how a person's name is stored in the payroll or personnel systems. RFC2822, Internet Message Format (Section 3.4.1) allows the email address to be constructed with any ASCII character in the range

D33-D90, D94-D126 (excluding the "@" character which is used to separate the local-part of the email address from the domain). Therefore the use of numeric qualifiers should work with any RFC2822 compliant email system/client. As noted in my response to question 3, the use of the IC label does not eliminate the risk of name collision.