

International Email Addresses in X.509



Технический
Центр
Интернет



Технический
Центр
Интернет

International Email Addresses in X.509

Dmitry Belyavskiy
Technical Centre of Internet
ICANN 60 Tech Day, Abu-Dhabi
October 30, 2017



IETF EAI workgroup:

- *2007-2010: experimental RFCs*
- *2012: final RFCs 653x: SMTP*
- *2013: final RFCs 685x: POP/IMAP*



Group of RFC 653x (2012):

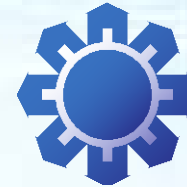
- *RFC 6530: Overview and Framework for Internationalized Email*
- *RFC 6531: SMTP Extension for Internationalized Email (SMTPUTF8)*
- *RFC 6532: Internationalized Email Headers*
- *RFC 6533: Internationalized Delivery Status and Disposition Notifications*
- *RFC 6783: Mailing Lists and Non-ASCII Addresses*



Group of RFC 685x (2013):

- *RFC 6855: IMAP Support for UTF-8*
- *RFC 6856: POP3 Support for UTF-8*
- *RFC 6857: Post-Delivery Message Downgrading for Internationalized Email Messages*
- *RFC 6858: Simplified POP and IMAP Downgrading for Internationalized Email*

EAI: adoption



Технический
Центр
Интернет

Servers: Postfix 3.0+, Exim 4.86+, Dovecot, Roundcube...

Mail clients: Microsoft Outlook 2016 for Windows, Apple iOS Mail, The Bat!, mutt...

Mail providers: Google Gmail...

Russian statistics: 1,3% MX-servers, 2,6% Domain zones

Source: <https://statdom.ru>

EAI: missing standards

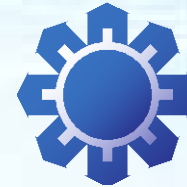


Технический
Центр
Интернет

EAI in EPP

EAI in X.509 – work in progress

Something else?



IETF WG Lamps

- <https://tools.ietf.org/wg/lamps/draft-ietf-lamps-rfc5280-i18n-update/>
Russ Housley
- <https://tools.ietf.org/wg/lamps/draft-ietf-lamps-eai-addresses/>
Alexey Melnikov
Weihaw Chuang

Source: <https://tools.ietf.org/wg/lamps/>



Set of patches to RFC 5280

X.509/CRL Profile

- IDNA 2008 compatibility
- CAs SHOULD ensure that IDNs are valid
- A-labels anywhere but EAI emails
 - *subjectAltName, issuerAltName...*
- Hostname in Smtputf8Mailbox
 - *Local part:*
 - ASCII? A-Label
 - Non-ASCII? U-Label

References to draft-ietf-lamps-eai-addresses

Internationalized Email Addresses in X.509 certificates



Технический
Центр
Интернет

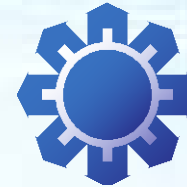
- Smtptf8Mailbox in GeneralName
 - *otherName*
- Comparison
 - *A-labels => U-labels*
 - *Lowercase ASCII labels*
 - *Compare strings octet-for-octet for equivalence*
- Name constraints
 - *Local-part NC SHOULD NOT be used*
 - *Apply domain-level NC (RFC 5280, 4.2.1.10)*
 - *CAs MUST use rfc822Name subject alternative names only*

EAI in X.509: implementation



Технический
Центр
Интернет

- Preliminary version of patch to OpenSSL
<https://github.com/openssl/openssl/pull/2560>
- Depends on LibIDN
- Needs more testing
- Waiting for the necessary OIDs



Questions?

beldmit@tcinet.ru

No, I do not have a EAI mailbox