

The Identity Landscape

A place where Mad Max would feel right at home

Very few things happen at the right time, and the rest do not happen at all: The conscientious historian will correct these defects.

Mark Twain



... once upon a time

cc:Mail
Banyan VINES
Internet Mail
UUCP
BITNET Mail
X.400
FidoNet

Build and Deploy Your Sendmail

4th Edition
Revised & Updated

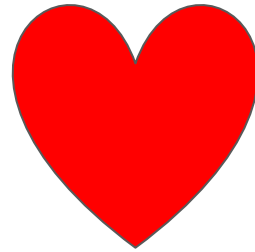
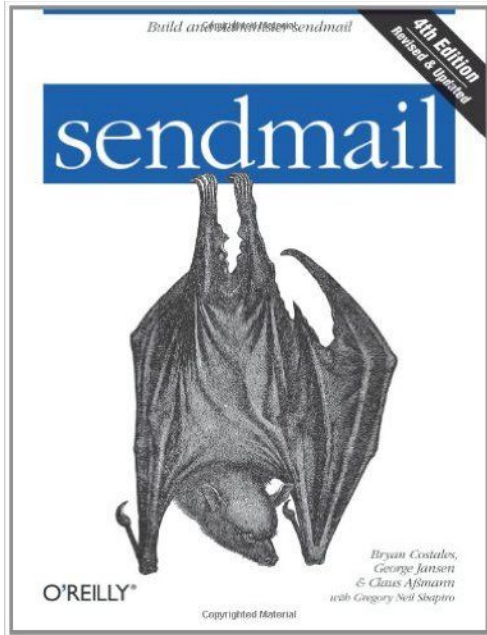
sendmail



O'REILLY*

Bryan Costales,
George Jansen
& Claus Aftmann
with Gregory Neil Shapiro

Copyrighted Material



cc:Mail
Banyan VINES
Internet Mail
UUCP
BITNET Mail
X.400
FidoNet

~~Interoperability~~

... the complete lack thereof

Build and Deploy Your Sendmail

4th Edition
Revised & Updated

sendmail



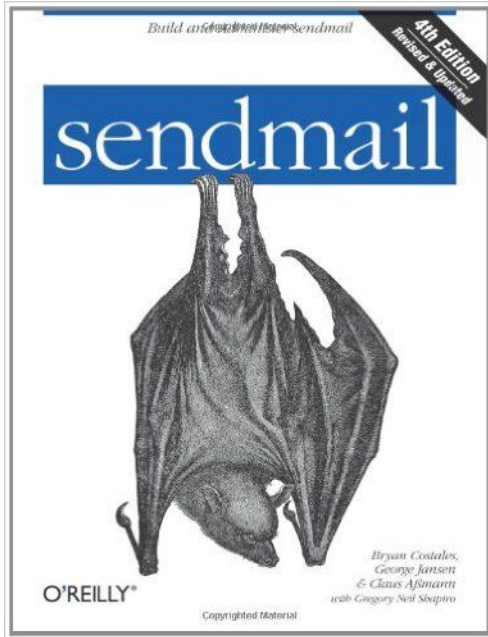
O'REILLY*

Bryan Costales,
George Jansen
& Claus Aftmann
with Gregory Neil Shapiro

Copyrighted Material

No message was ever
improved by a gateway

Internet Mail (RFC 822)



Email today...

(...which mostly works btw)

- Works for both sunet.se, cisco.com and google.com
- Straight forward to operated for small domains
- Multiple interoperating implementations

Identity “architecture”



You call that architecture?

- Trust Management
 - X509, SAML Metadata, webfinger+HTTPS, WS-Trust
- Identity Claims and Assertions
 - SAMLv1, SAMLv2, OpenID Connect, OpenID 1, OpenID 2.0, WS-Federation, McGyvered-JOSE, CBOR/COSE, OAUTH, OAUTH-over-JOSE
- ... and re-spin for IoT



Is OpenIDC the one?

Who Made OpenIDC?

...Google, Facebook, Microsoft....

... and also this guy!



Decisions are made by the
folks who show up

Is OpenIDC The one?

Is OpenIDC The one?

It depends...

OpenIDC works when...

- You have a very small number of IdPs
- You do “continuous deployment”

What is missing?

- Scalable trust management that doesn't tie us to the Web PKI
- "Sendmail" now (multiprotocol gateway) and then "Postfix" (simplification)
- A trusted solution to the discovery problem (accountchooser?)
- A way to make phishing much less attractive (FIDO?)

The Future

NEXT EXIT



Whats next?

- AL2 is becoming cheap
 - Vertical federations have to become either buyers clubs or provide AL3
- Passwords are (finally, maybe) not the only way to authenticate users
 - If you're not already integrating FIDO U2F/2.0 - start working on it

Support your SDO

Decisions are made by the folks who show up.