

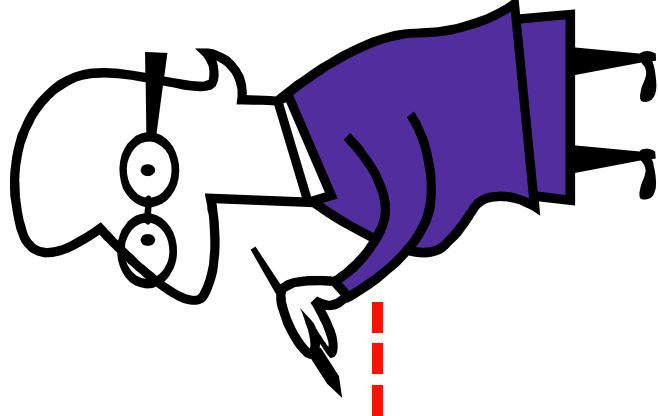
Who's Reading My E-mail?

**A Sane Approach to Choosing an
Encrypted E-mail Solution
(or not)**

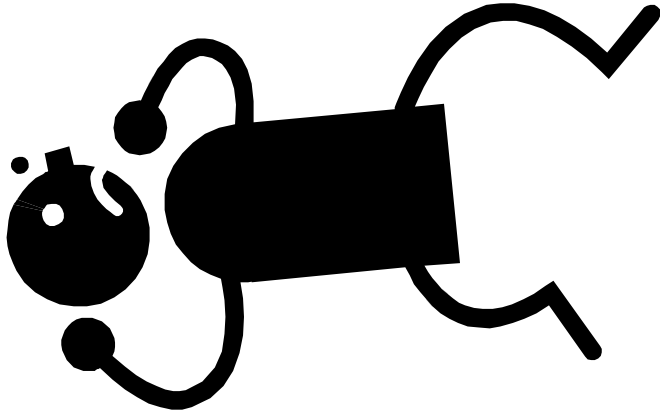
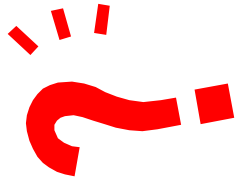
**Donald McKillican
donald.mckillican@bell.ca
Bell Canada Corporate Security
ISSA, Vancouver
May 18, 2006**

Disclaimer

- This is not a technical presentation.
- The information is not drawn from any single project, nor from any single company.
- This presentation deals with e-mail encryption, not viruses, spyware or other problems.



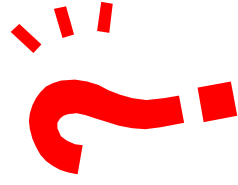
Why Should I Encrypt My E-mail?



Possibly because:

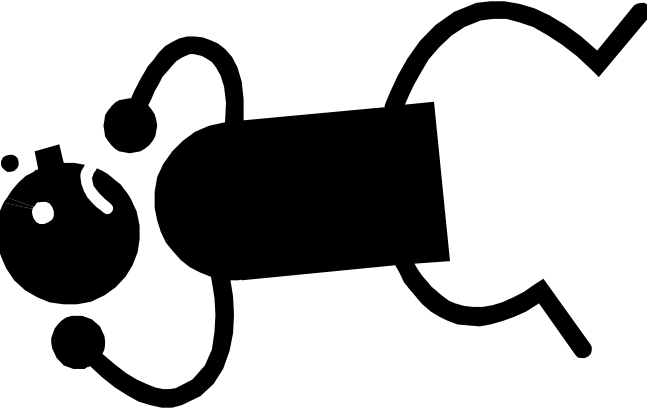
- ❑ “Cleartext e-mail is like a postcard”
 - Well, sort of ...

Why Should I Encrypt My E-mail?



Possibly because:

- ❑ “Cleartext e-mail is like a postcard”
 - Well, sort of ...



More Likely:

- ❑ Your auditors (or lawyers) are telling you to do it
- ❑ Your customers are telling you to do it
- ❑ Or you think they’re about to tell you to do it

The Wish List: Features

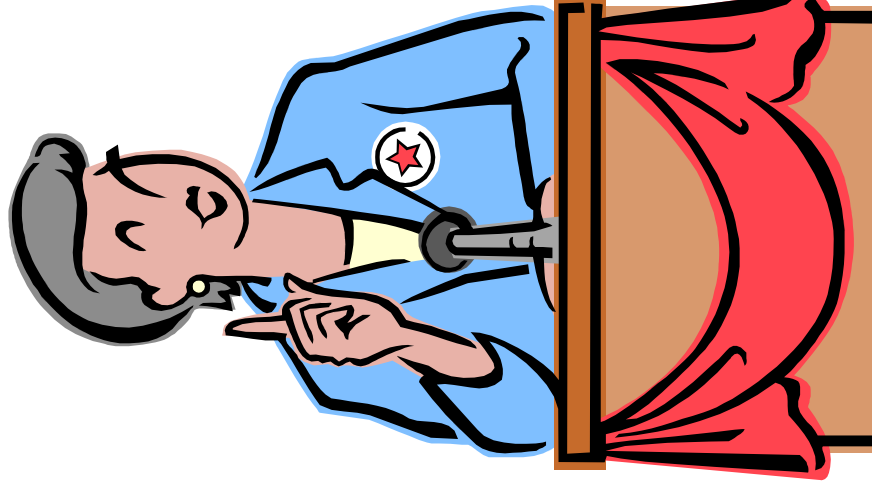
- ❑ Compatible with partner software
- ❑ Low Impact on e-mail flow
- ❑ Encrypts body and attachments
- ❑ Built-in for common client s/w
- ❑ Supports centralized virus and content scanning
- ❑ Ease of audit-proofing
- ❑ Provides desktop-to-desktop encryption
- ❑ Supports Roaming Users

The Wish List: Costs

- ❑ Low Infrastructure Costs
- ❑ Low Per User Installation Costs
- ❑ Low User Training Costs
- ❑ Low Administration Support Costs
- ❑ Low Interoperability Support Costs

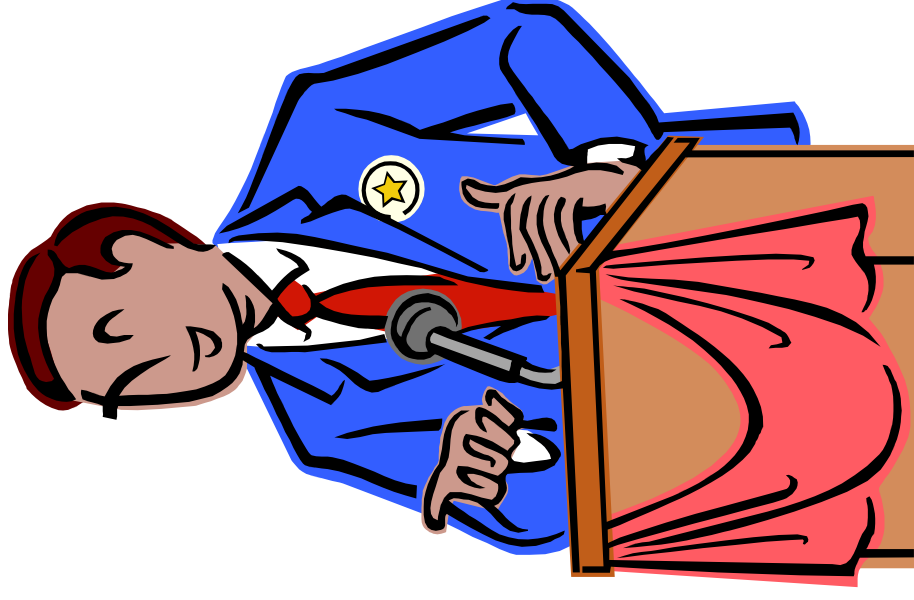
The Candidates

- ❑ Corporate S/MIME CA
- ❑ Outsourced S/MIME CA
- ❑ Corporate S/MIME Gateway
- ❑ Corporate Webmail Gateway
- ❑ Corporate IBE









The Candidates (continued)

- Personal S/MIME certificates
- Personal PGP
- Corporate PGP
- Personal Encryption tools
- SMTP-TLS
- Dabra



Corporate S/MIME CA

-  Very mature technology, built-in to all common e-mail clients
-  No impact on existing e-mail flow
-  Magnet for auditors
-  High user training costs
-  High cost to support interoperability
-  Centralized virus/content scanning usually not possible

Outsourced S/MIME CA

- 👍 Simplifies the CA solution by letting someone else do a lot of the work 😊
- 👎 Audit proofing easier, but still needs work
- 👎 Same user support issues as in-house CA
- 👎 Virus/Content scanning still not possible
- Depends *heavily* on the costs of the outsourcing contract

Corporate S/MIME Gateway

- 👍 Simplifies the PKI solution by taking it out of the hands of the user, so no user support costs of any kind
- 👍 Supports centralized virus/content scanning
- 👎 Will have some impact on e-mail flow, perhaps significantly (perhaps not)
- 👎 Interoperability problems still there, but restricted to e-mail server admins

Corporate Webmail Gateway

- 👍 User not involved in encryption decision, so no user support costs of any kind
- 👍 Supports centralized virus/content scanning
- 👎 Could have a heavy admin burden, and will certainly be resisted by business partners
- 👎 Will have some impact on e-mail flow, perhaps significantly (perhaps not)

Corporate IBE

- 👍 Simplifies the PKI solution by making the e-mail address the public key
- 👍 No audit issues, no impact on e-mail flow
- 👍 Supports roaming users
- 👎 Low take-up in industry, not built-in to any e-mail clients
- 👎 Limited support for centralized virus scanning

Personal S/MIME Certificates

- 👍 All of the benefits of PKI (almost) with no infrastructure costs or audit problems! 😊
- 👍 No impact on existing e-mail flow
- 👎 Can *only* be used to encrypt attachments
- 👎 Centralized virus scanning not possible
- 👎 Same user and interoperability support issues as in-house CA






Personal PGP

- 👍 No impact on e-mail flow, no interoperability problems (or audit issues)
- 👍 No infrastructure to purchase or administer
- 👎 **Very** geeky end user interface, not ideal for non-technical managers or executives
- 👎 Can **only** be used to encrypt attachments
- 👎 Centralized virus scanning not possible

Corporate PGP

- Provides both gateway and keypair recovery facilities
- 👍 Can be used for both message body and attachments
- 👎 Same geeky interface (in desktop mode), some impact on e-mail flow (in gateway mode)
- 👎 Centralized virus scanning possible (in gateway mode only)

Personal Encryption Tools

-  No infrastructure costs, no impact on e-mail flow
-  Provides end-to-end encryption.
-  Serious issues with key management, especially for multiple correspondents
-  Unlikely to be acceptable to large business partners
-  Can only encrypt attachments

SMTP-TLS

- Just a normal e-mail gateway plus a TLS (SSL) certificate
 - 👍 Takes encryption entirely out of the hands of the end user, so no user support.
 - 👍 Supports centralized virus scanning
 - 👍 No audit issues
 - 👎 Will have some impact on e-mail flow, perhaps significantly (perhaps not)

Dabra

- Uses a central server for key negotiation and special writer and reader plug-ins
- 👍 No infrastructure costs (pay per message), minimal impact on e-mail flow
- 👍 Provides legal-strength acknowledgement when the message is decrypted.
- 👎 Unknown to business partners
- 👎 User installation and support needed.

So Which One is Right For You?

- First step: evaluate how well each solution meets your requirements
- Second step: weight each requirement according to its importance



Example Evaluation

| Technology Features | Corporate S/MIME CA | Outsourced S/MIME CA | Corporate S/MIME g/w | Corporate Webmail g/w | Corporate IBE | Personal S/MIME certs | Personal PGP | Corporate PGP | Personal Encryption tools | SMTP-SSL | Dabra |
|---|---------------------|----------------------|----------------------|-----------------------|---------------|-----------------------|--------------|---------------|---------------------------|----------|-------|
| Compatible with Partner s/w | 10 | 10 | 10 | 0 | 0 | 10 | 5 | 5 | 0 | 8 | 0 |
| Low Impact on E-mail Flow | 10 | 10 | 5 | 0 | 10 | 10 | 10 | 10 | 10 | 5 | 10 |
| Encrypts Body, Attachments | 10 | 10 | 10 | 10 | 10 | 0 | 10 | 10 | 0 | 10 | 10 |
| Built-in for Common Client s/w | 10 | 10 | 10 | 10 | 0 | 10 | 5 | 5 | 0 | 10 | 0 |
| Supports centralized virus and content scanning | 3 | 3 | 10 | 10 | 7 | 0 | 0 | 3 | 0 | 10 | 4 |
| Ease of Audit-Proofing | 0 | 5 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| Provides End-to-End Encryption | 8 | 8 | 0 | 0 | 10 | 8 | 9 | 5 | 10 | 0 | 10 |
| Supports Roaming Users | 0 | 0 | 10 | 10 | 10 | 0 | 0 | 0 | 0 | 10 | 0 |
| Infrastructure Costs | 0 | 4 | 2 | 0 | 5 | 10 | 10 | 5 | 10 | 3 | 10 |
| Per User Installation Costs | 7 | 7 | 10 | 10 | 0 | 7 | 5 | 5 | 5 | 10 | 0 |
| User Training Costs | 0 | 0 | 10 | 10 | 5 | 0 | 0 | 0 | 0 | 10 | 5 |
| Administration Support Costs | 0 | 3 | 3 | 0 | 4 | 10 | 10 | 7 | 10 | 9 | 10 |
| Interoperability Support Costs | 0 | 0 | 3 | 10 | 8 | 0 | 10 | 10 | 10 | 10 | 10 |

Example Features Weighting

- 5: Compatible with partner s/w
- 5: Low Impact on e-mail flow
- 1: Encrypts body and attachments
- 2: Built-in for common client s/w
- 2: Supports centralized virus and content scanning
- 2: Ease of audit-proofing
- 1: Provides desktop-to-desktop encryption
- 1: Supports Roaming Users

Example Costs Weighting

- 2: Low Infrastructure Costs
- 2: Low Per User Installation Costs
- 2: Low User Training Costs
- 2: Low Administration Support Costs
- 2: Low Interoperability Support Costs

Example Weighted Evaluation

| Technology | Score |
|------------------------------|-------|
| Corporate S/MIME CA | 199 |
| Outsourced S/MIME CA | 223 |
| S/MIME Gateway | 241 |
| Webmail Gateway | 170 |
| Corporate IBE Gateway | 219 |
| Personal S/MIME Certificates | 234 |
| Personal PGP | 220 |
| Corporate PGP | 209 |
| Personal Encryption Tools | 190 |
| SMTP-TLS Gateway | 280 |
| Dabra | 220 |

Summary

- First decide *whether* you need encrypted e-mail, and be clear about why.
- Evaluate the different technologies and products
- Pick the one that best meets your needs.



Thank You!

Donald McKillican

donald.mckillican@bell.ca

Bell Canada Corporate Security