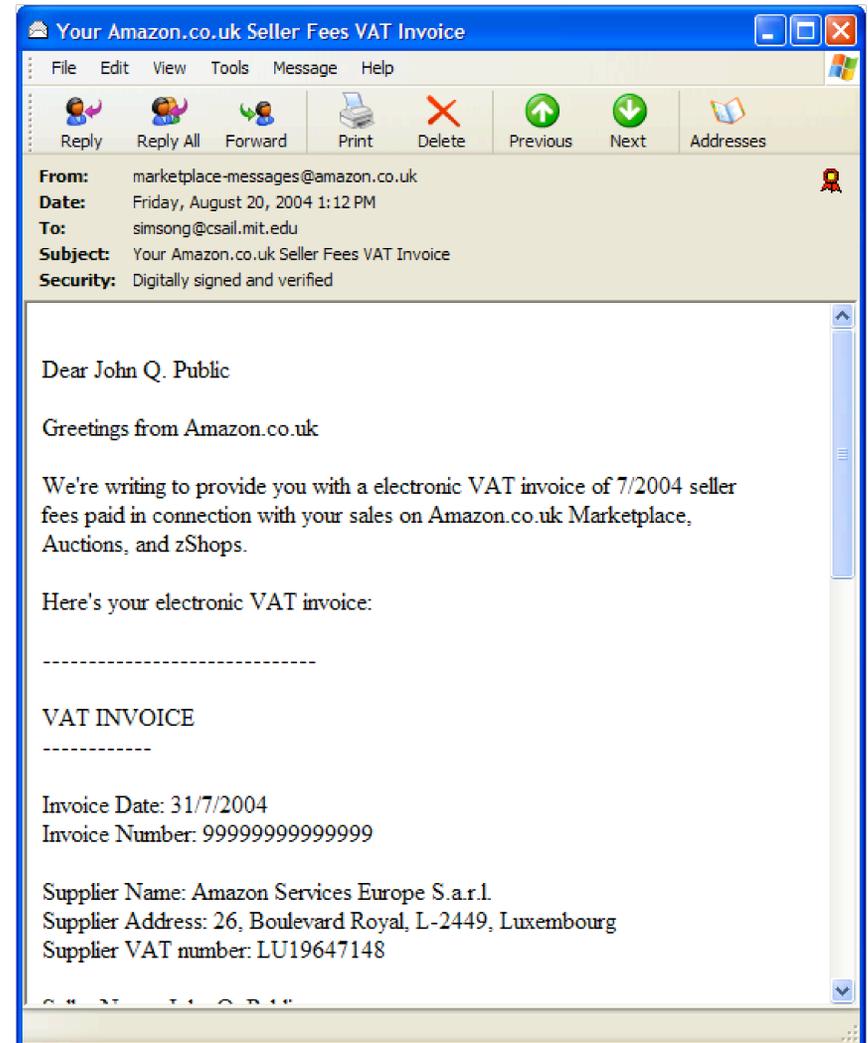


Views, Reactions and Impact of Digitally-Signed Mail in e-Commerce

Simson L. Garfinkel (MIT)
Jeffrey I. Schiller (MIT)
Erik Nordlander (MIT)
David Margrave (Amazon.com)
Robert C. Miller (MIT)



<http://www.simson.net/smime-survey.html/>

Secure Email: Where are we today?

- RFC 989: Privacy Enhanced Mail (1987)
- PGP (1992) has failed to gain market penetration.
- S/MIME (1998):
 - Support in Outlook, Notes, Apple Mail
 - Soon in Eudora (this year!)
 - No support in consumer web mail systems.
- A few other odd balls.

**After roughly 20 years of active work,
most mail sent over the Internet is not “secure.”**

If support for S/MIME is pervasive, why isn't *use* of S/MIME widespread?

There are really two options:

- Option #1: S/MIME is hard to use.
 - It's hard to seal mail for a recipient: You need their certificate.
 - It's hard to sign mail: You need your own certificate.
- Option #2: Secure email just isn't needed.

... But given the problems with spam and phishing, it's hard to argue that email security isn't needed.

Perhaps the problem is with this phrase, “email security.”

There are *many* ways that email could be “secured.”

- Disconnected email “islands.” (1980s solution)
- Filtering (today’s solution)
- Sender-certified or proof-of-sender
- Sender pays (financially or computationally)
- Proof-carrying messages

Email security seems to be one of the “grand challenges” of computer security.

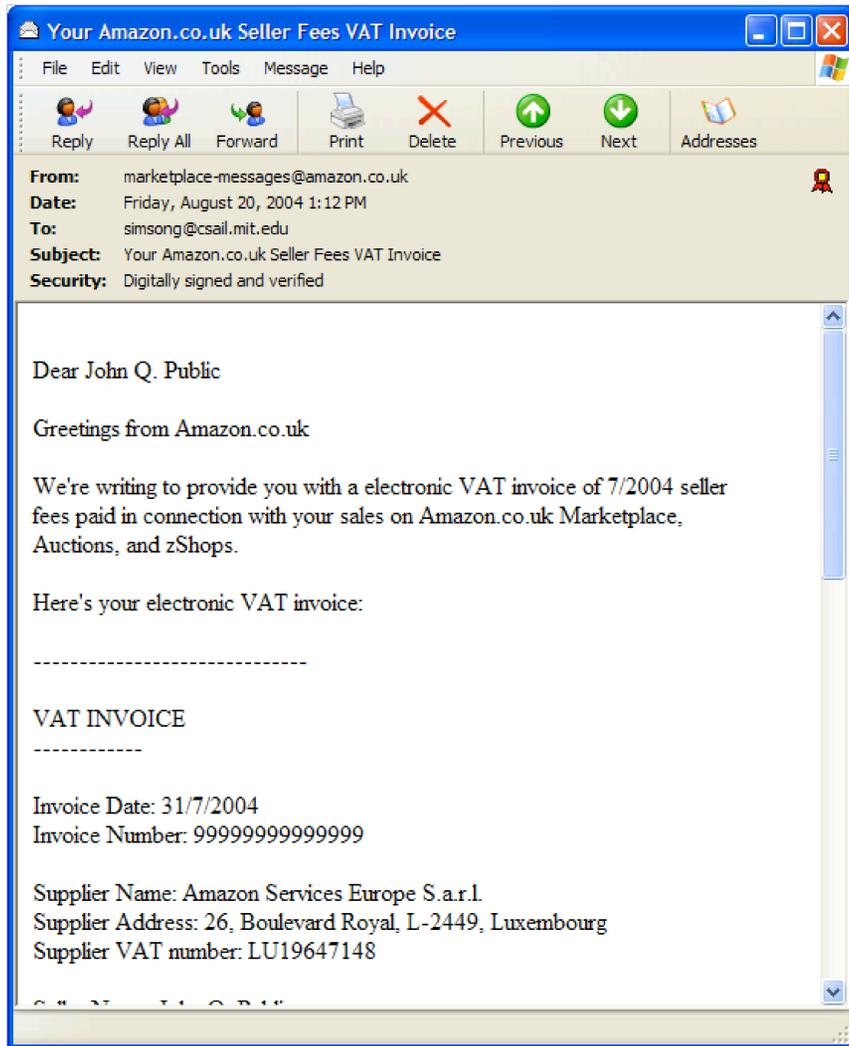
There are also *many* ways that an average person (like my mother) could “use S/MIME”



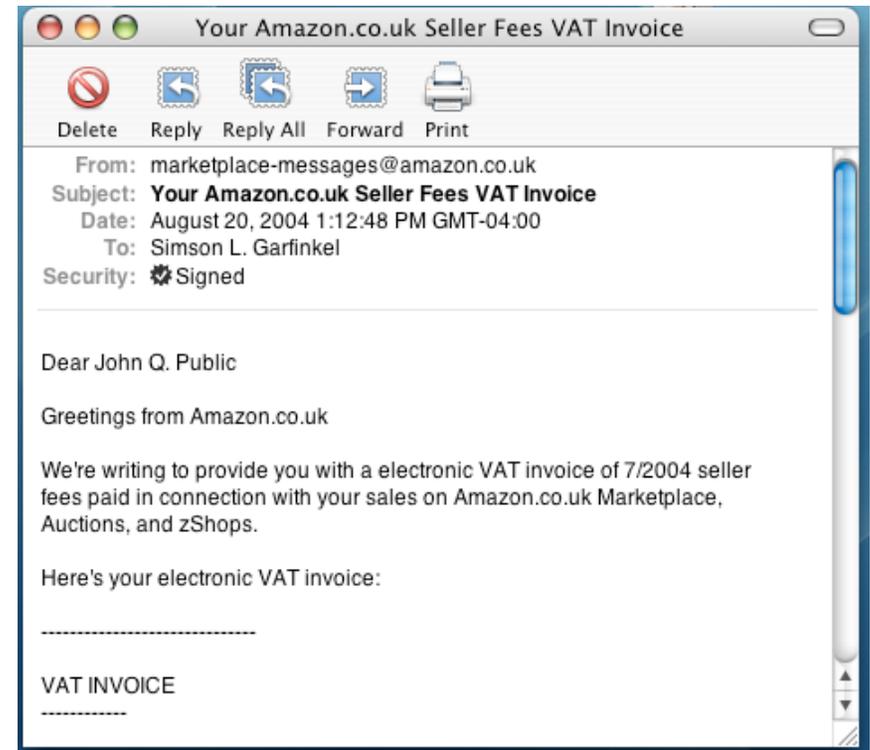
- To *send* S/MIME mail.
 - ✗ sealed mail: She needs the recipient’s certificate.
 - ✗ signed mail: She needs her own certificate.
- To *receive* S/MIME mail.
 - ✗ sealed mail: She needs her own certificate (and she needs to get it to the sender!)
 - ✓ signed mail: She need sender’s CA’s certificate. (S/MIME messages come with the certificate of the signer.)

Every S/MIME client ships with CA certificates for VeriSign, Thawte, and other well-known CAs.

Mail *signed* with an S/MIME certificate issued by a well-known CA will be verified by most email clients.



Outlook Express



Apple Mail

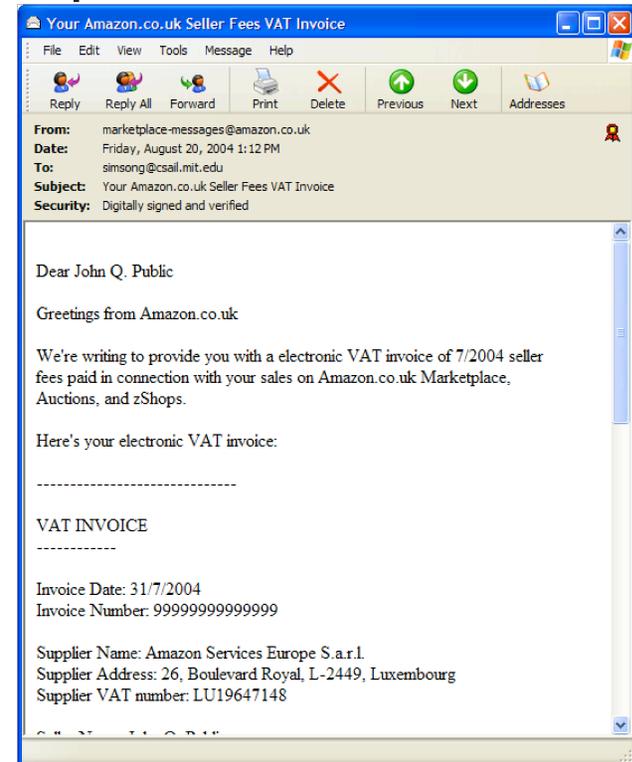
But few organizations are sending S/MIME signed mail.

Amazon.com: The S/MIME Leader!

In June 2003, Amazon.COM started using S/MIME to sign the VAT invoices sent to its European Marketplace Sellers .

EU Directive 99/93/EU calls for the use of “advanced digital signatures” for certain kinds of electronic messages.

Amazon sent signed mail to Europeans, but not to other merchants.



This created an excellent opportunity for survey research.

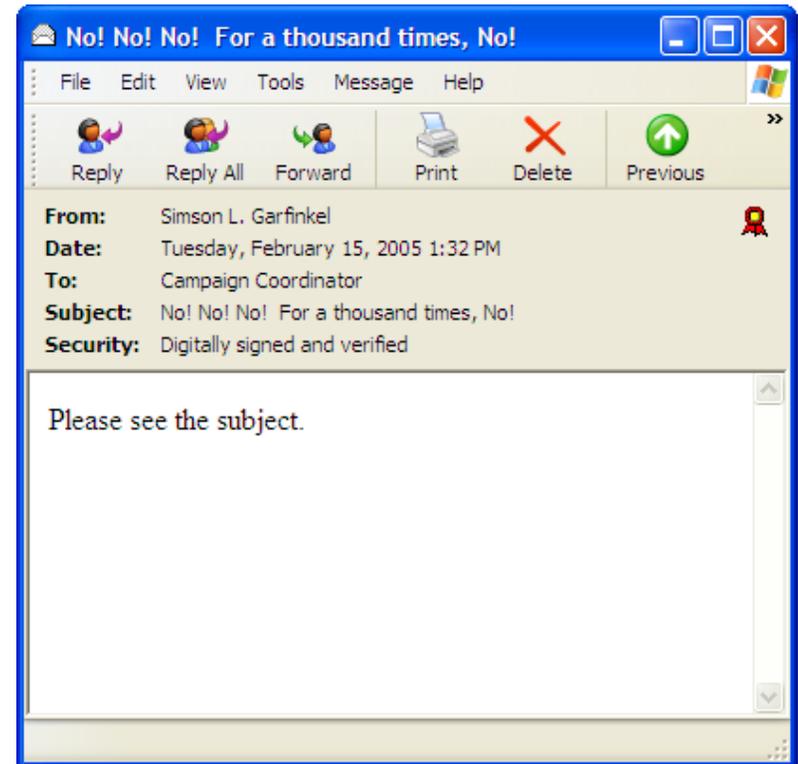
Research questions that we wanted to answer:

- Did people have software to automatically verify the signatures?
- Did they understand what the software told them?
- What did they think that a signature on a message *means*?
- How did receiving signed messages affect their attitudes?

These are open research questions.

There are many cases in which a signed S/MIME message has problems.■

- Exformation: “?” ... “!” ■
- “Digital Signatures and Electronic Documents: A Cautionary Tale”
[Kain, Smith & Asokan '02]■
- Do you digitally sign the email to your attorney with the contract that’s under review?■



S/MIME is a lousy signature standard, but it’s the signature standard that we have.

We created a web survey and posted links to it in the Amazon Sellers Forums:

- 5 web pages; 40 questions total
- 2 minutes to complete each page
- Different URLs for Europe vs. America

**Europe Sellers had received signed messages from Amazon.
US Sellers – had not received the messages**

Survey respondents:

- 1083 sellers clicked on the link
 - 470 submitted the first web page.
 - 417 (89%) completed all five pages.
- Very educated:
 - 26.1% advanced degree
 - 34.9% college degree
- Very computer literate:
 - 18% “very sophisticated” computer user
 - 67.7% “comfortable” using computers

Findings on Attitudes: Roadmap

1. Statistical Techniques
2. Passive Learning
3. Knowledge and Attitudes
4. “Savvy” vs. “Green”
5. What should be signed?
6. What should be sealed?
7. What do the respondents have?
8. Risks
9. Conclusions

Interesting partitions of the survey population:

Europe (93) vs. US (376)

“Savvy” (148) vs. “Green” (334)

Savvy:

- Rated their “understanding of encryption and digital signatures” a 1 (“very good”) or 2 on a 5-point scale. (23 and 53)
- Had knowingly received a signed message (104)
- Had knowingly received a sealed message (39)
- “Always” or “sometimes” send digitally signed messages (29)

Significance Test: Logistic Regression with χ^2 .

Not everything that’s significant is relevant!

(Highest education high school: 16% Europe, 5% US, $p < .01$.)

Most can automatically handle S/MIME-signed mail

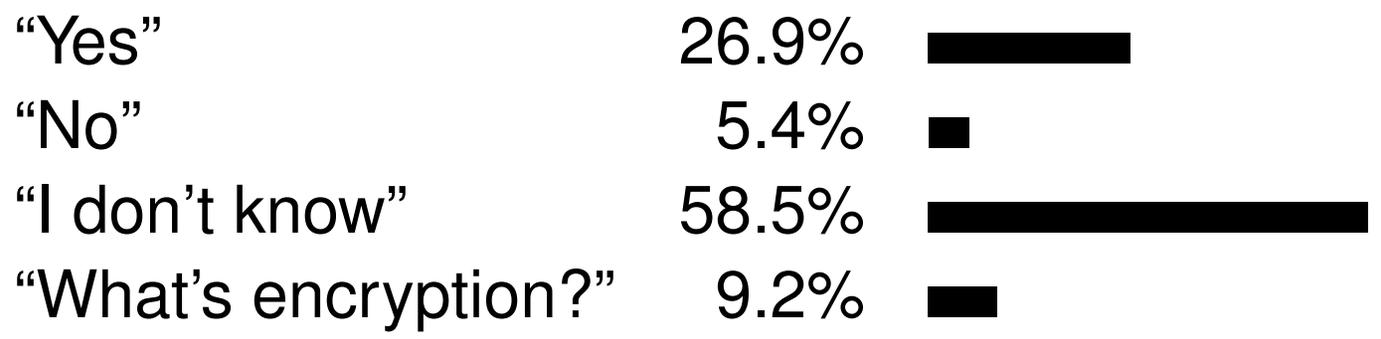
Which computer programs do you use to read your email?

Microsoft Outlook Express	41.8%	
Outlook	30.6%	
Netscape	10.1%	
<hr/>		
Any S/MIME compatible reader	81.1%	
<hr/>		
Eudora	6.9%	
<hr/>		
(Webmail)	13.1%	
<hr/>		

Fortunately, fixing the webmail problem doesn't require upgrading client software!

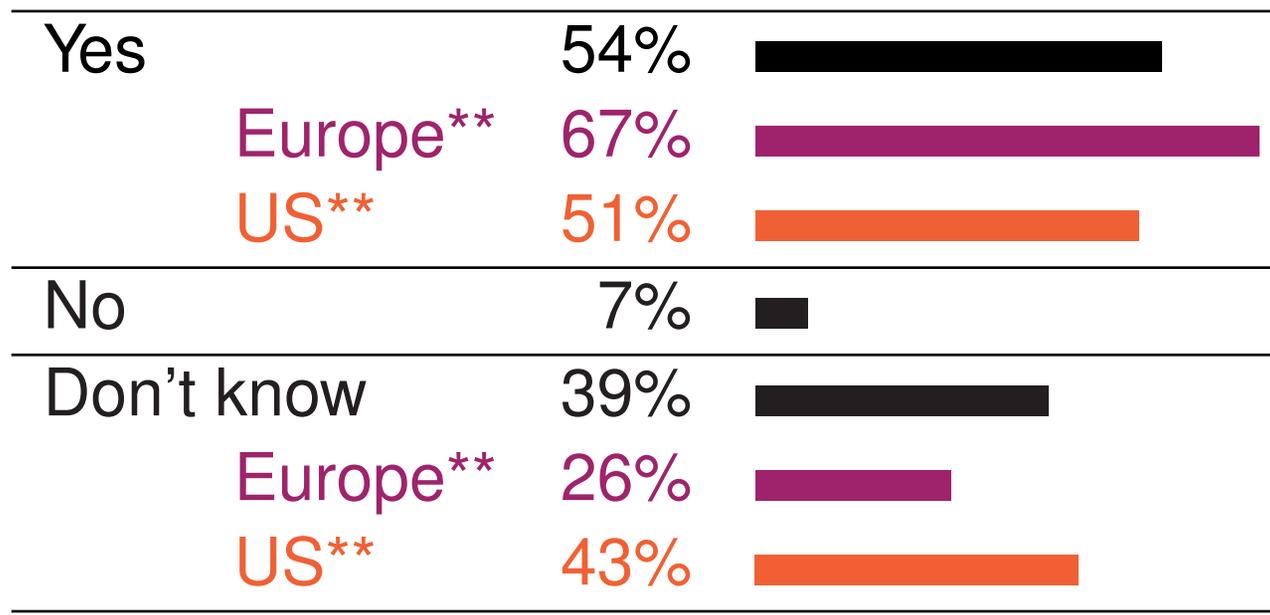
But most people who can receive S/MIME mail don't know it:

“Does your email client handle encryption?”



Passive Learning Works!

“Practically speaking, do you think that there is a difference between mail that is digitally-signed and mail that is sealed with encryption?”



** $p < .01$

Users who received S/MIME-signed mail know more about encryption than those who didn't.

Respondents thought that signatures should be used for financial matters.

What should be digitally signed? (E-Commerce)

Bank or credit-card statements	65%	
Receipts from online merchants	59%	
Questions to online merchants	33%	
Savvy*	26%	
Green*	36%	
Advertisements	17%	

* $p < .05$

Respondents thought that signatures should be used for financial matters.

What should be digitally signed? (General Email)

Tax returns or complaints to regulators	74%	
Personal mail sent or received at work	40%	
Personal mail sent or received at home	40%	
Mail to political leaders voicing opinion	38%	
Newsletters from politicians	22%	

Most thought that signatures should be used for financial matters, but not otherwise.

Likewise, most respondents thought that sealing should be used for financial matters.

What should be digitally sealed? (E-Commerce)

Bank or credit-card statements	79%	
Receipts from online merchants	47%	
Savvy*	39%	
Green*	51%	
Questions to online merchants	18%	
Advertisements	3%	

* $p < .05$

Interestingly, those who are more familiar with encryption thought that sealing was less important for receipts.

Likewise, most respondents thought that sealing should be used for financial matters.

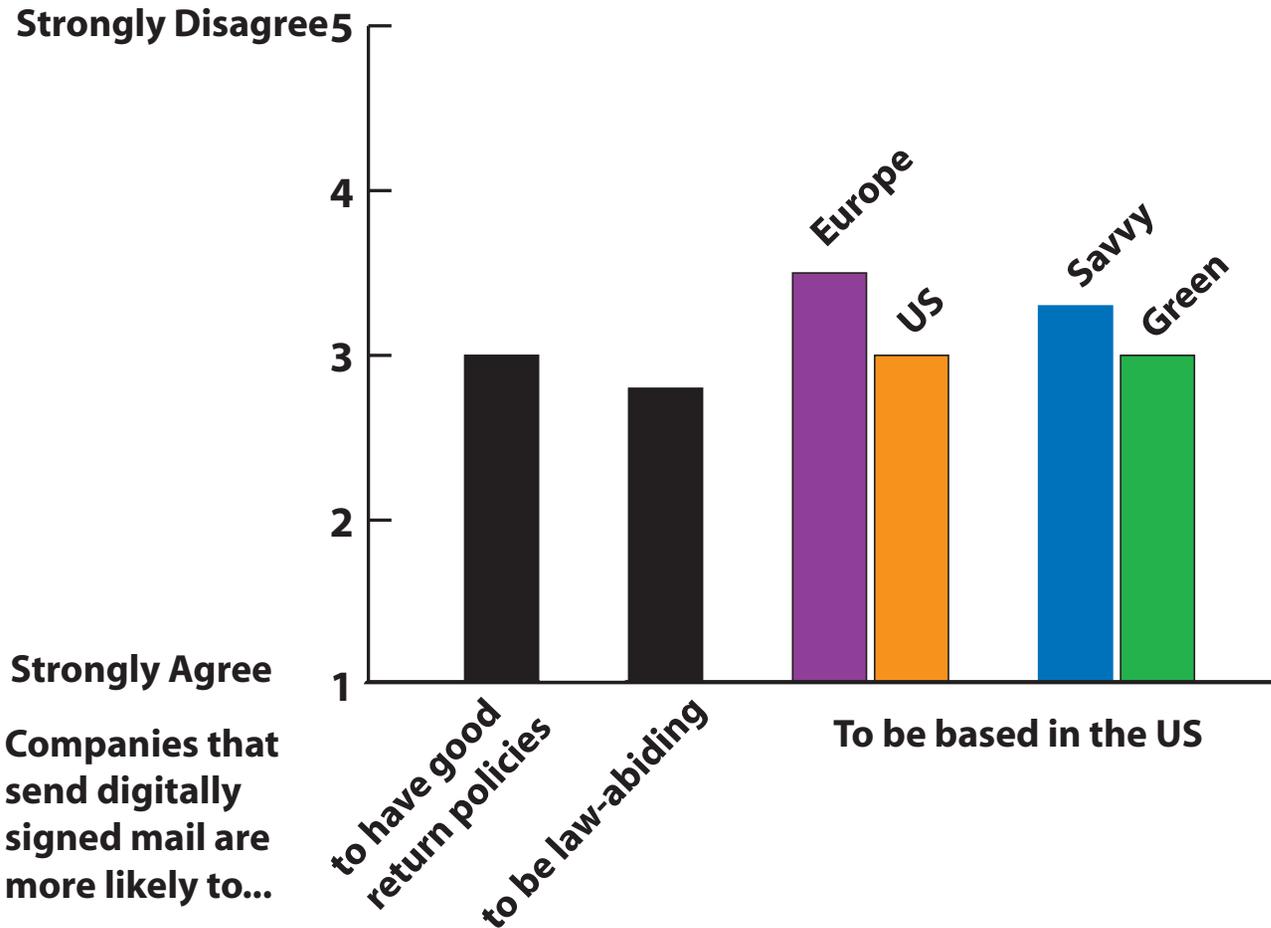
What should be digitally sealed? (General Email)

Tax returns or complaints to regulators	74%	
Mail to political leaders voicing opinion	38%	
Personal mail sent/received at work	38%	
Savvy ^{***}	26%	
Green ^{***}	44%	
Personal mail sent/received at home	31%	
Savvy [*]	25%	
Green [*]	34%	
Newsletters from politicians	3%	

* $p < .05$; *** $p < .001$

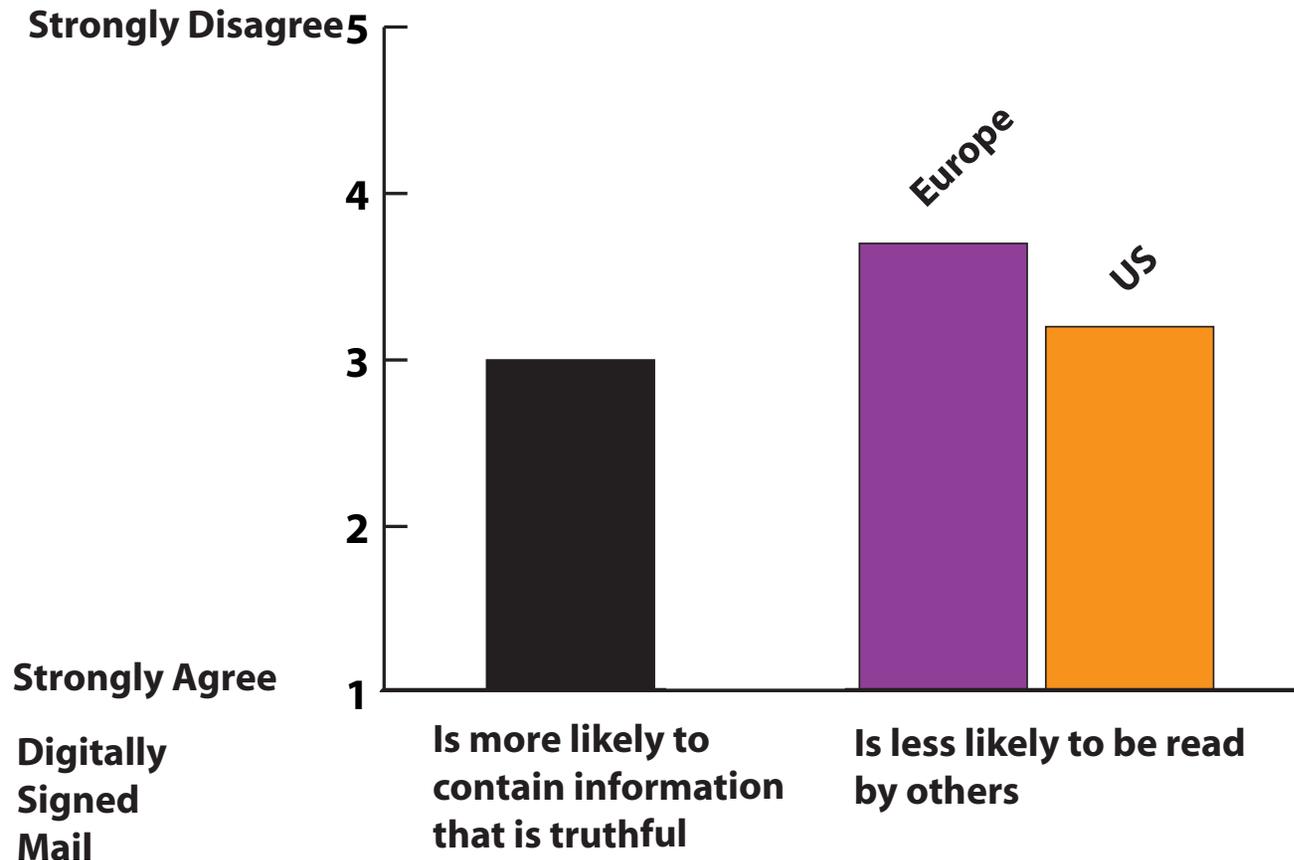
Companies that send digitally signed mail:

On a scale of 1 to 5, where 1 is “strongly agree” and 5 is “strongly disagree:”



Respondents don't think that sending digitally signed mail means that companies are better merchants

Digitally signed mail:



Respondents didn't think that digitally signed mail is inherently more truthful or less likely to be eavesdropped.

Free-Format Responses

Many respondents wished they knew more about email security:

“I wish I knew more about digitally-signed and sealed encrypted e-mail, and I wish information were more generally available and presented in a manner that is clear to those who aren’t computer scientists or engineers. “



“This is an interesting topic... I had not thought about the need to send/receive signed or sealed e-mail for other than tax info.”

Many respondents don't want any more complications!

“Most sellers do not care about digital signatures when selling on on-line marketplaces unless they are dealing in big sums of money in the transaction, even then I still do not care.”



“I think it a good idea, but I'm lazy and it's too much trouble to bother with.”



“I know it's necessary, but it shouldn't be complicated to handle.”

Conclusions: The Time for Signatures is Now.

- Even though most (58.5%) respondents didn't know that they could read S/MIME signatures, the vast majority (81.1%) could.
- People who have no interest in selling this technology believe that it should be used.
- Sending signed mail require zero training for recipients and zero keystrokes; but the results are visible!
- Amazon's out-of-pocket cost was trivial.
- Companies that send out email should probably sign it.

Questions?