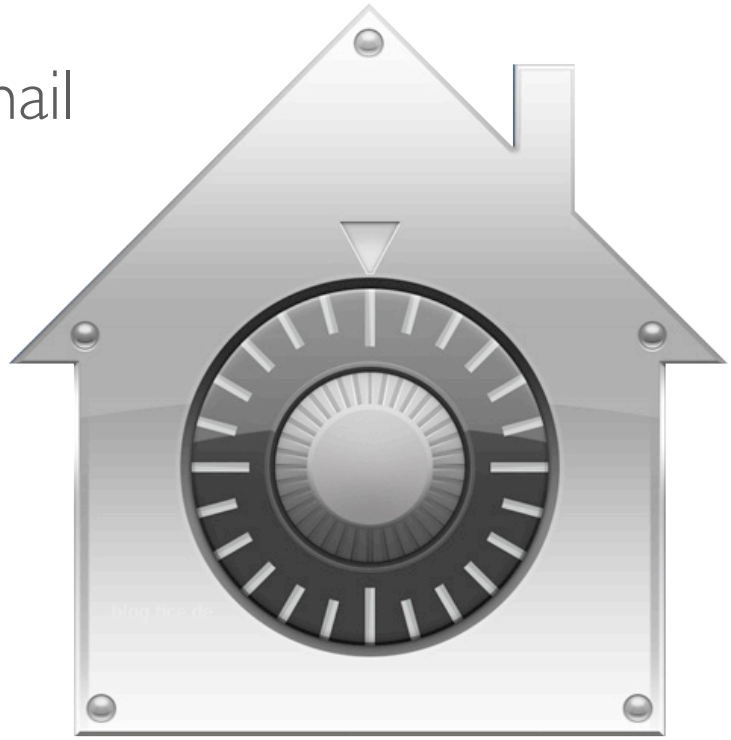
MACTECH BOOTCAMP MINNEAPOLIS, MN

James Alcasid

ENCRYPTION

- FileVault2
- S/MIME Certificates for email
- Encrypted Zip Files
- Encrypted Disk Images
- Cost/Benefit
- Impact on Performance



FILEVAULT 2

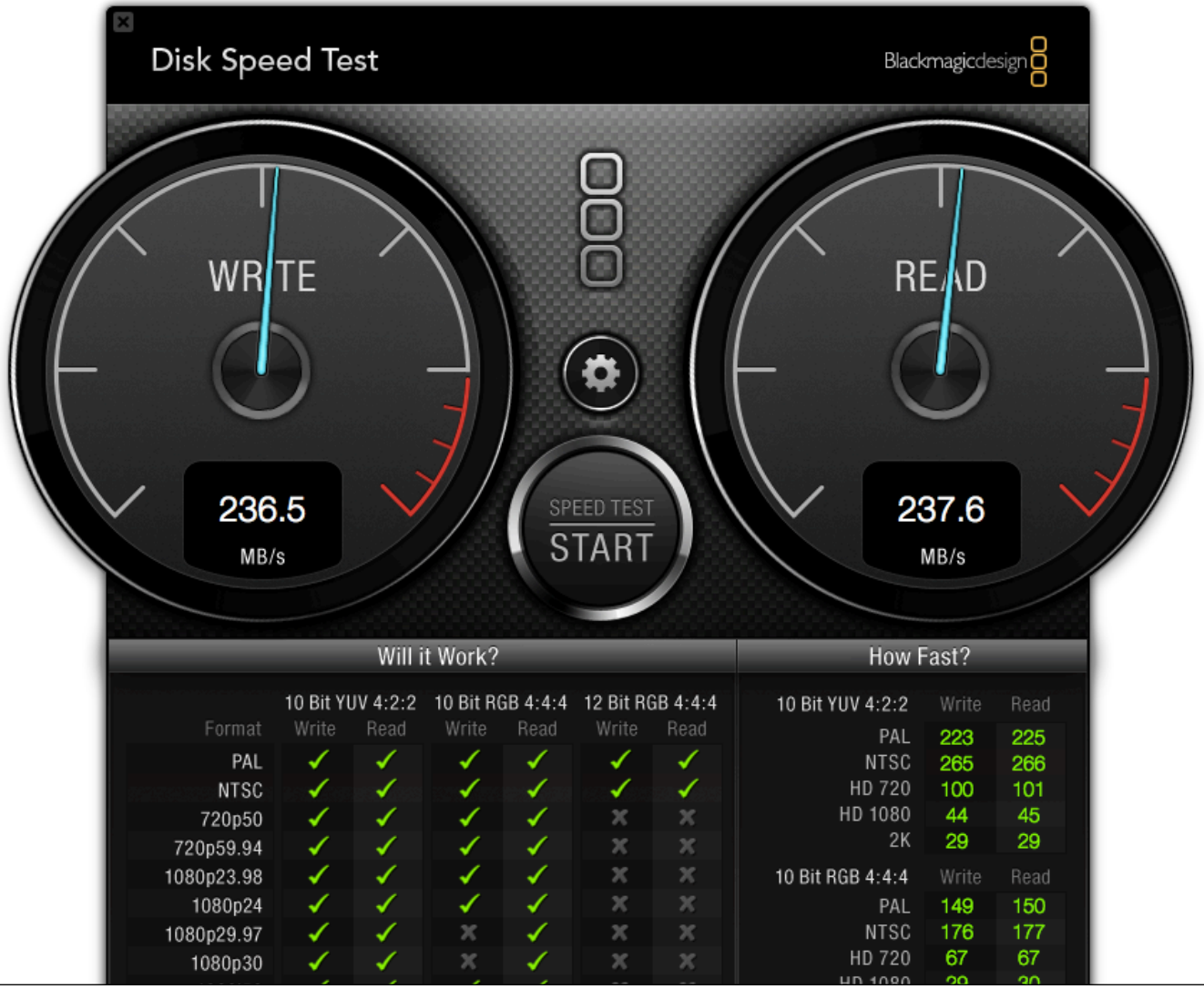
- Full-disk encryption
- Make a Backup & Encrypt the backup!
- Almost FIPS 140-2 data protection but you still need a strong password
- Apply all Software Updates and do maintenance before enabling FileVault 2 and Backup!
- Tradeoffs with performance on standard HDs
- For most users it is best to escrow recovery keys with Apple
- Apple and JAMF can manage FV2 in the enterprise

FILEVAULT 2


Security & Privacy
Show All
General
FileVault
Firewall
Privacy
FileVault secures the data on your disk by encrypting its contents automatically.
Turn Off FileVault...
FileVault is turned on for the disk "Macintosh HD".
A recovery key has been set.
Click the lock to make changes.
Advanced...
?

FILEVAULT 2

- The performance trade-off on SSD, negligible!

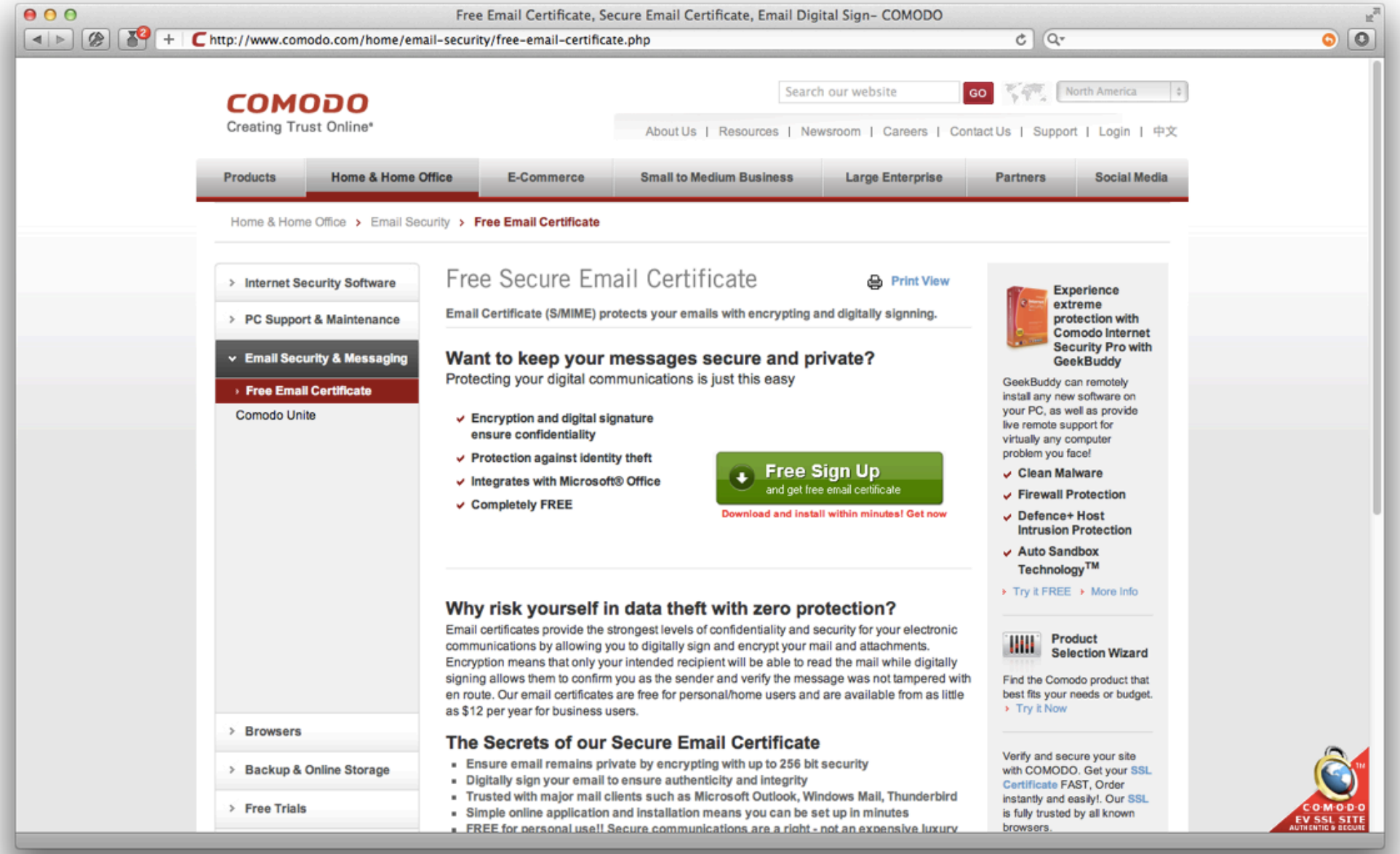


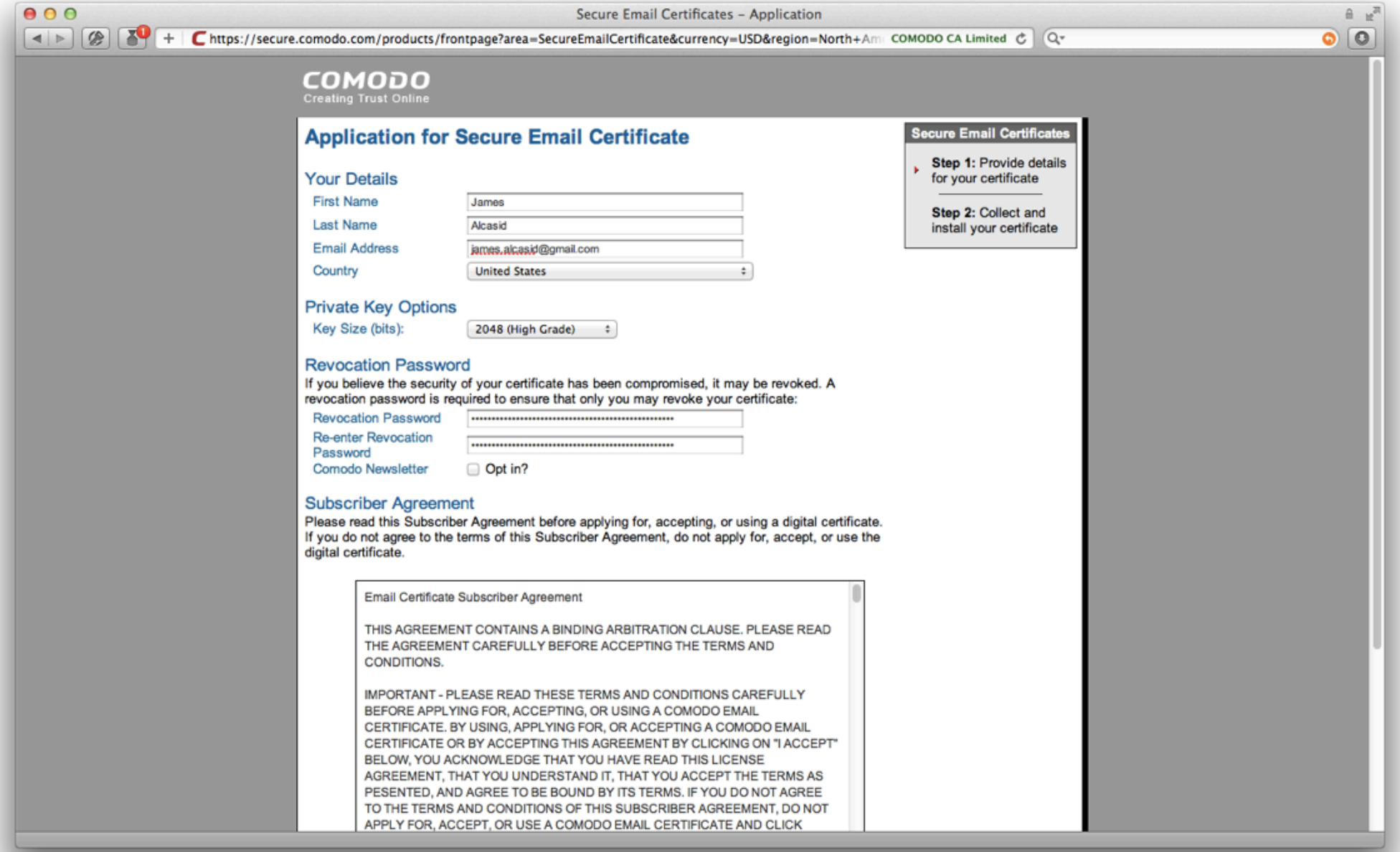
S/MIME MAIL CERTIFICATES

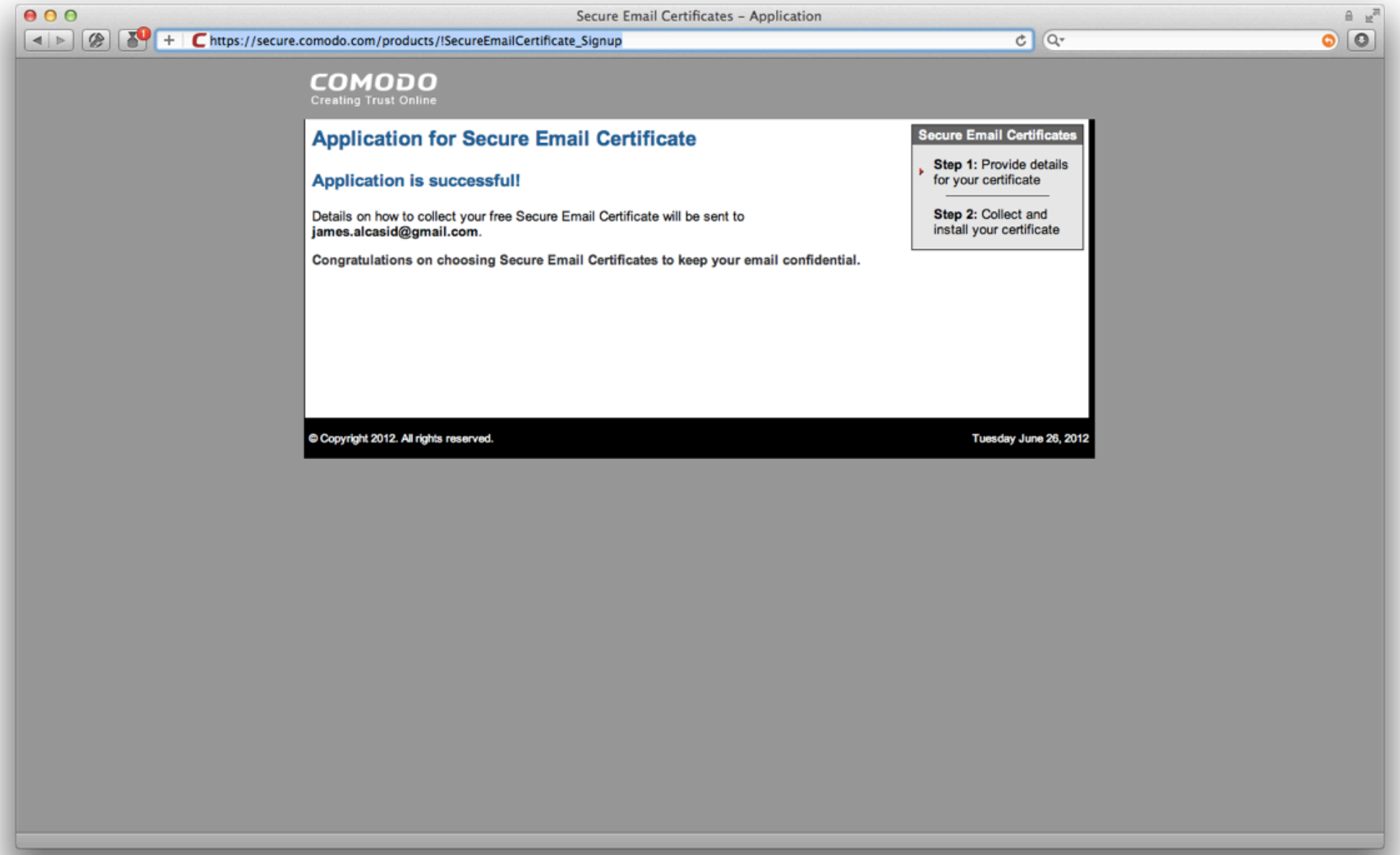
- Secure/Multipurpose Mail Extension
- Digitally Sign and Encrypt Email
- Used with an email client such as Apple Mail
- Low impact but an effective layer of security
- The sender and receiver must both use S/MIME certificates for mail encryption

S/MIME MAIL CERTIFICATES & APPLE MAIL

HTTP://WWW.COMODO.COM/HOME/EMAIL-SECURITY/FREE-EMAIL-CERTIFICATE.PHP




Secure Email Certificates – Application
https://secure.comodo.com/products/frontpage?area=SecureEmailCertificate&currency=USD&region=North+Am
COMODO CA Limited
COMODO
Creating Trust Online
Application for Secure Email Certificate
Secure Email Certificates
Step 1: Provide details for your certificate
Step 2: Collect and install your certificate
Your Details
First Name
James
Last Name
Alcasid
Email Address
james.alcasid@gmail.com
Country
United States
Private Key Options
Key Size (bits):
2048 (High Grade)
Revocation Password
If you believe the security of your certificate has been compromised, it may be revoked. A revocation password is required to ensure that only you may revoke your certificate:
Revocation Password
Re-enter Revocation Password
Comodo Newsletter
Opt in?
Subscriber Agreement
Please read this Subscriber Agreement before applying for, accepting, or using a digital certificate. If you do not agree to the terms of this Subscriber Agreement, do not apply for, accept, or use the digital certificate.
Email Certificate Subscriber Agreement
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS.
IMPORTANT - PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A COMODO EMAIL CERTIFICATE. BY USING, APPLYING FOR, OR ACCEPTING A COMODO EMAIL CERTIFICATE OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, THAT YOU ACCEPT THE TERMS AS PESENTED, AND AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE A COMODO EMAIL CERTIFICATE AND CLICK


Secure Email Certificates – Application
https://secure.comodo.com/products/!SecureEmailCertificate_Signup
COMODO
Creating Trust Online
Application for Secure Email Certificate
Application is successful!
Details on how to collect your free Secure Email Certificate will be sent to james.alcasid@gmail.com.
Congratulations on choosing Secure Email Certificates to keep your email confidential.
Secure Email Certificates
Step 1: Provide details for your certificate
Step 2: Collect and install your certificate
© Copyright 2012. All rights reserved.
Tuesday June 26, 2012

Your certificate is ready for collection! — Inbox

From: **Certificate Customer Services <secureemail@comodogroup.com>**
Subject: Your certificate is ready for collection!
Date: June 26, 2012 2:04:23 PM EDT
To: James Alcasid

Hide

14 Attachments, 51 KB Save Quick Look

COMODO

Tel Sales : **+1 888 266 6361**
Fax Sales : **+1.201.963.9003**

Your Comodo FREE Personal Email Certificate is now ready for collection!

Dear James Alcasid,

Congratulations - your Comodo FREE Personal Secure Email Certificate is now ready for collection! You are almost able to send secure email!

Simply click on the button below to collect your certificate.

Click & Install Comodo Email Certificate

Note:- If the above button does not work, please navigate to https://secure.comodo.net/products/!SecureEmailCertificate_Collec2 Enter your email address and the Collection Password which is

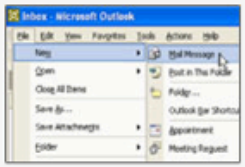
Your Comodo FREE Personal Secure Email Certificate will then be automatically placed into the Certificate store on your computer.

Click "Yes" if you see a "Potential Scripting Violation" window asking "Do you want this Program to add Certificates now?"

How to encrypt mail

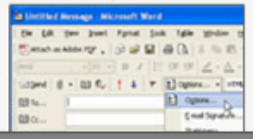
Step 1

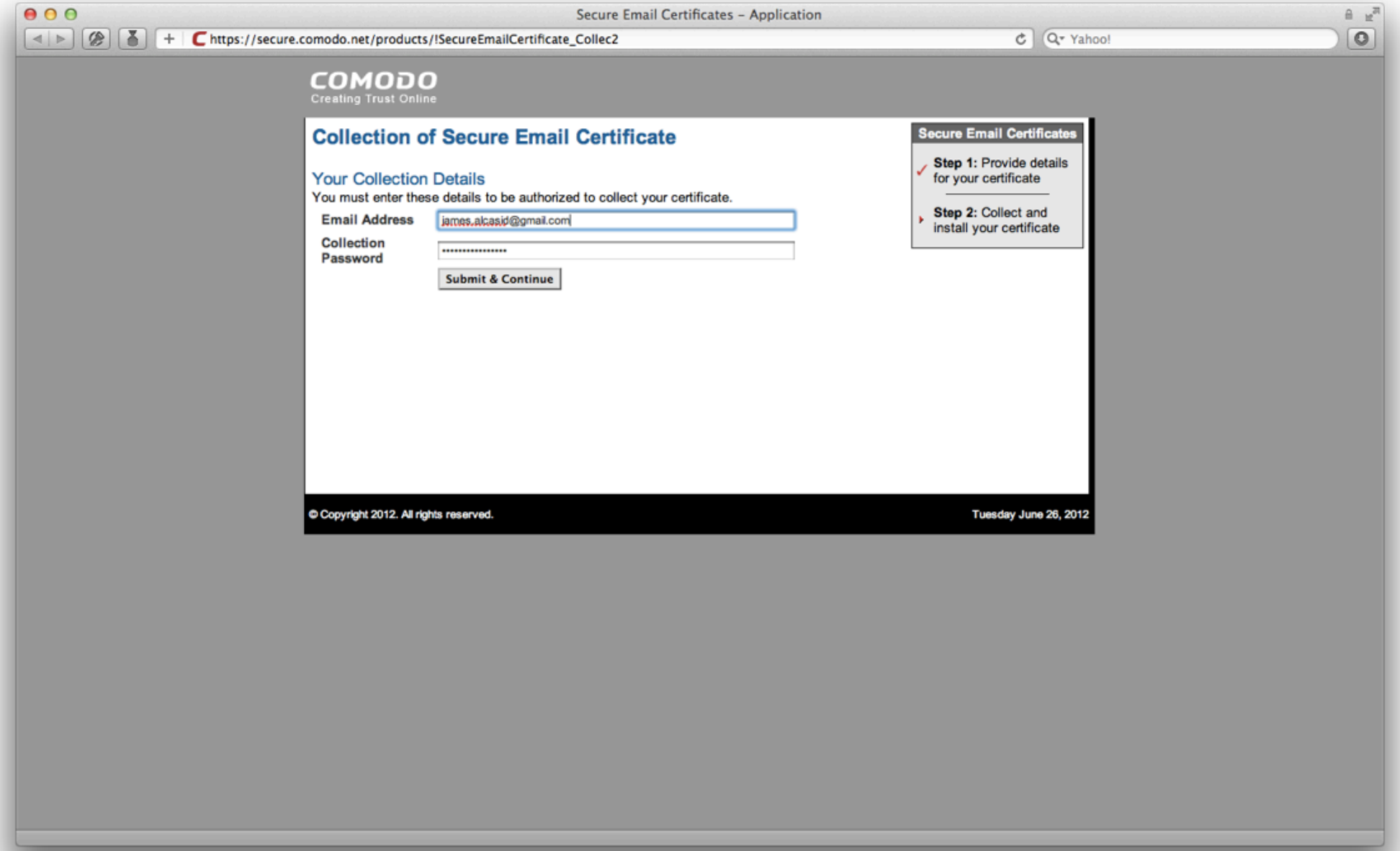
Create a new Mail



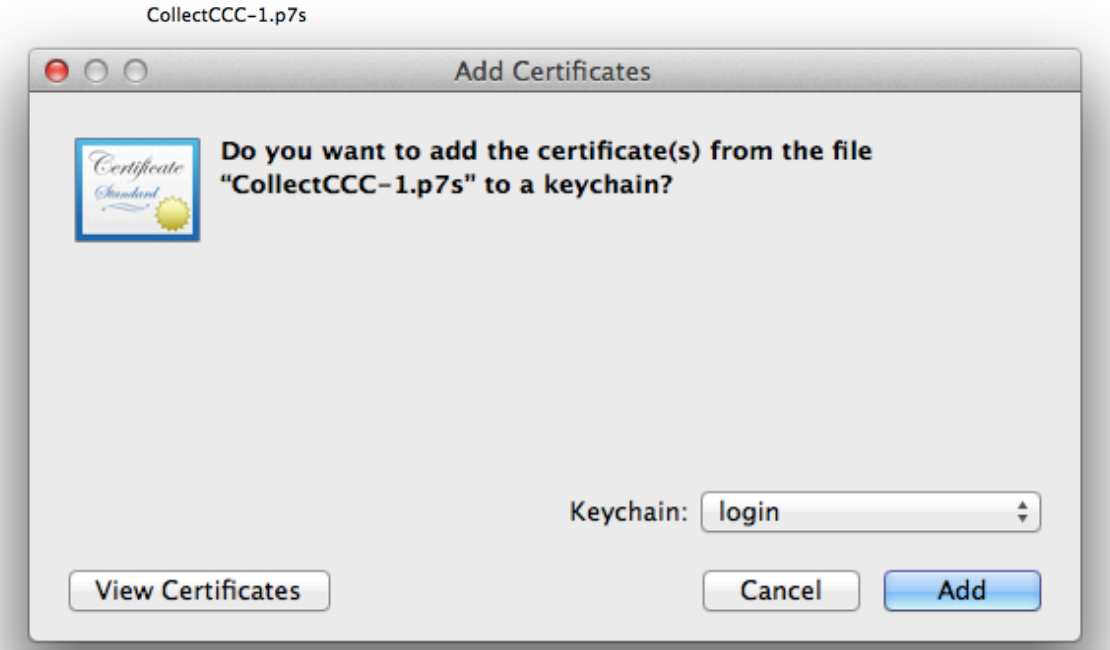
Step 2

Chose the Options button



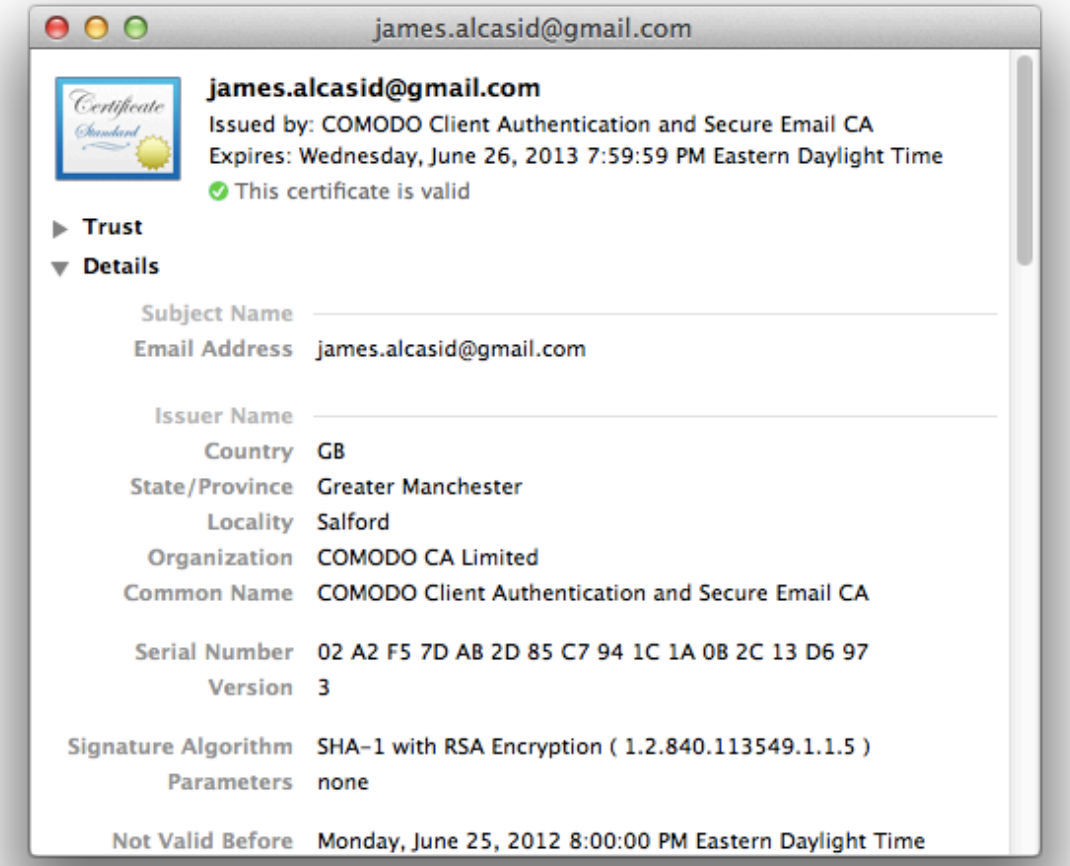

Secure Email Certificates – Application
https://secure.comodo.net/products/!SecureEmailCertificate_Collec2
Yahoo!
COMODO
Creating Trust Online
Collection of Secure Email Certificate
Your Collection Details
You must enter these details to be authorized to collect your certificate.
Email Address
james.alcasid@gmail.com
Collection Password
Submit & Continue
Secure Email Certificates
Step 1: Provide details for your certificate
Step 2: Collect and install your certificate
© Copyright 2012. All rights reserved.
Tuesday June 26, 2012

The downloaded file containing the certificates. Double-click to install.

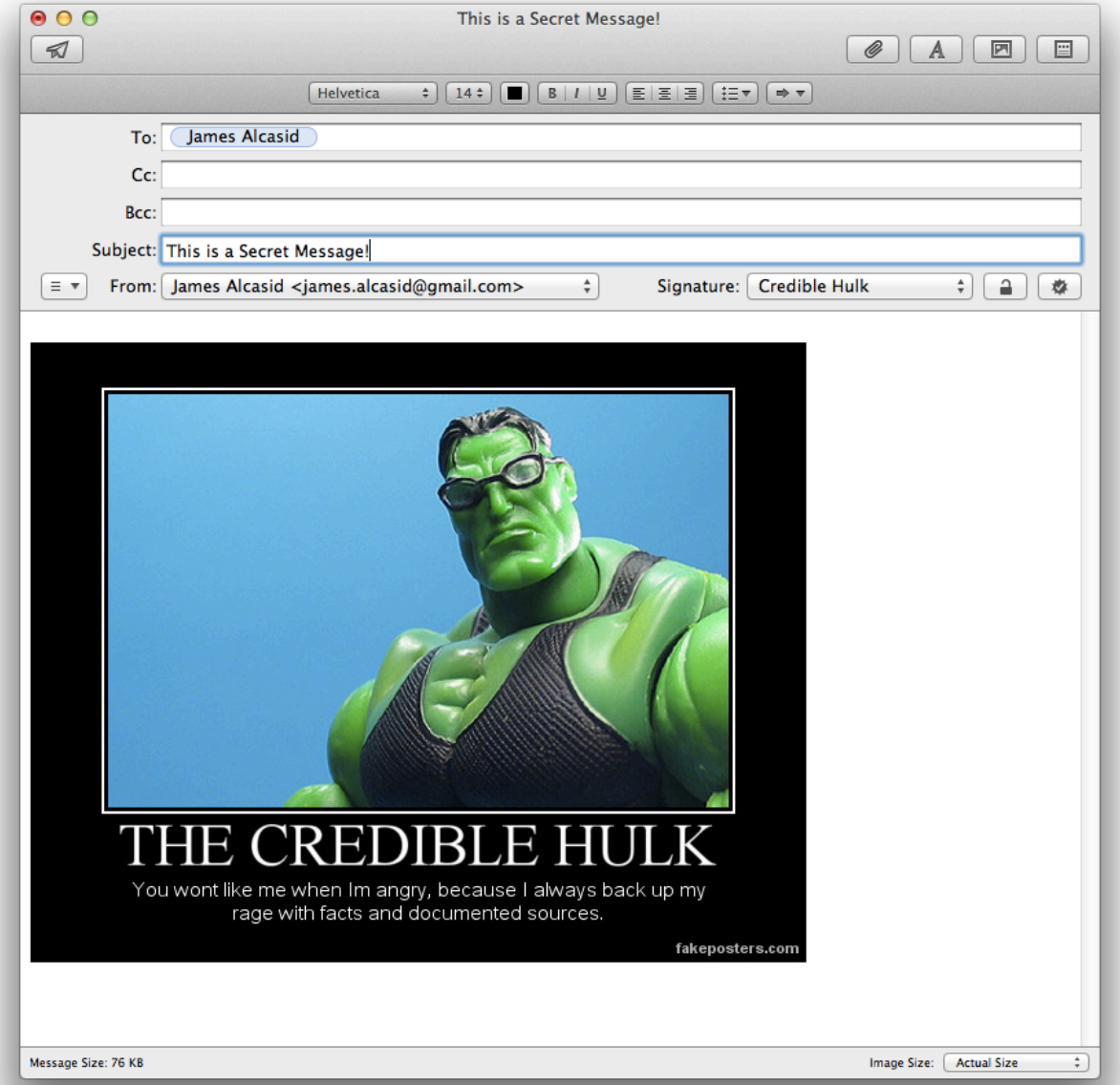


Click 'Add' to add certificates to Keychain.

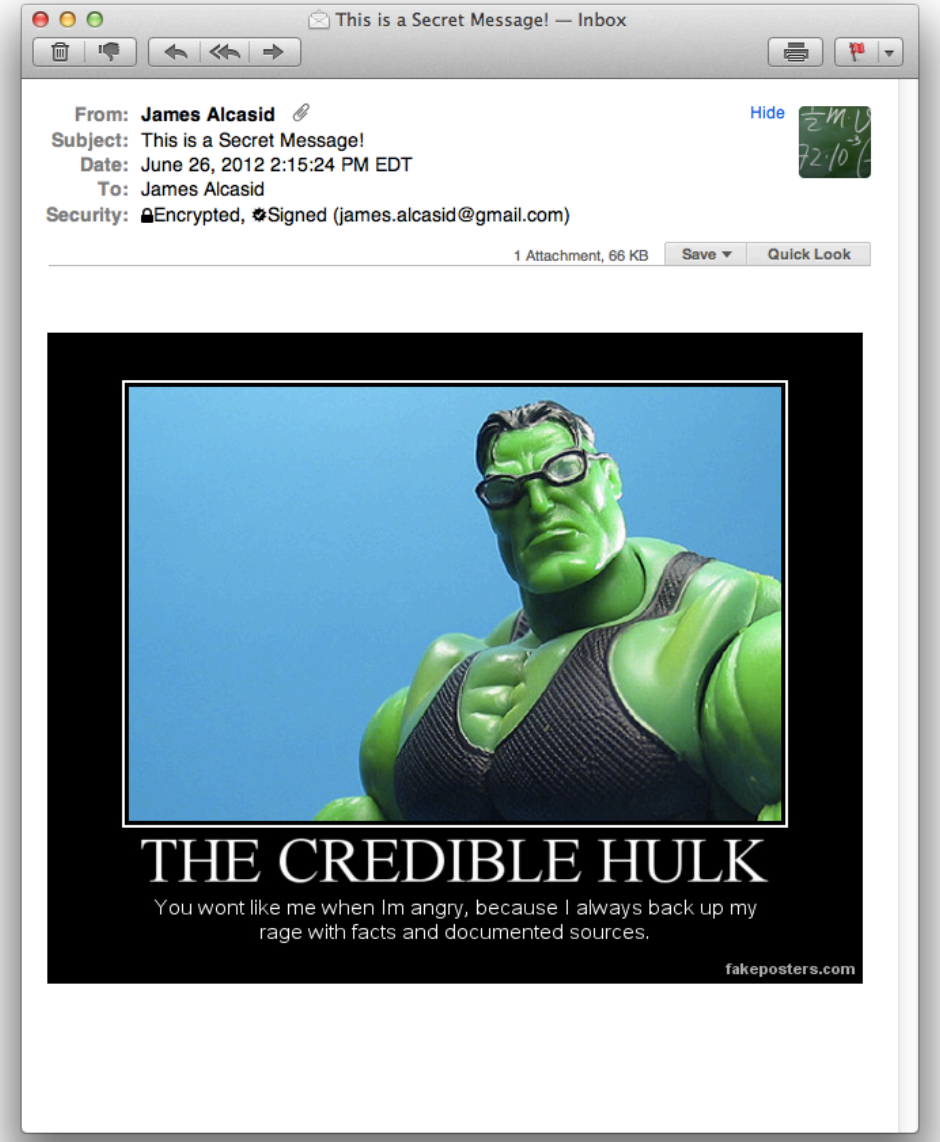
CHECK OUT YOUR CERTIFICATE!



THE TEST


This is a Secret Message!
Helvetica
14
To: James Alcasid
Cc:
Bcc:
Subject: This is a Secret Message!
From: James Alcasid <james.alcasid@gmail.com>
Signature: Credible Hulk
THE CREDIBLE HULK
You wont like me when Im angry, because I always back up my rage with facts and documented sources.
fakeposters.com
Message Size: 76 KB
Image Size: Actual Size

THE RESULT

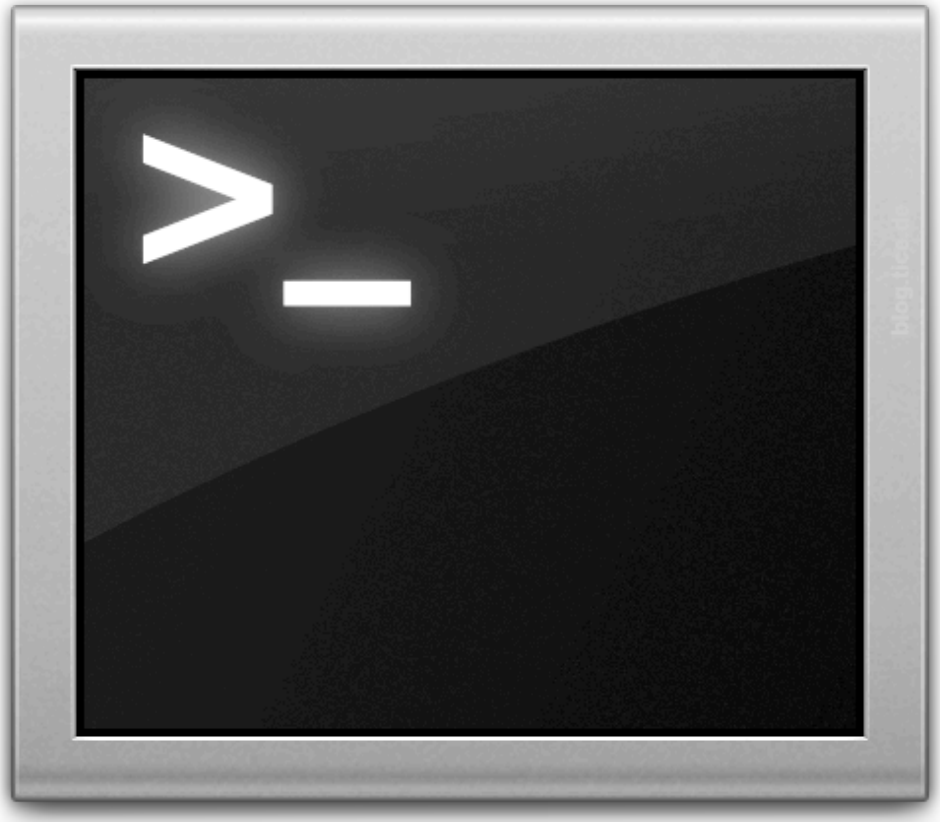

This is a Secret Message! — Inbox
From: James Alcasid
Subject: This is a Secret Message!
Date: June 26, 2012 2:15:24 PM EDT
To: James Alcasid
Security: Encrypted, Signed (james.alcasid@gmail.com)
Hide
1 Attachment, 66 KB
Save
Quick Look
THE CREDIBLE HULK
You wont like me when Im angry, because I always back up my rage with facts and documented sources.
fakeposters.com

S/MIME MAIL CERTIFICATES & APPLE MAIL DEMO

PASSWORD PROTECT ZIP FILES

- Mac OS X and Windows compatibility
- Executed from Terminal
- $ zip -e encrypted_filename encrypted file

PASSWORD PROTECT ZIP FILE DEMO



ENCRYPTED DISK IMAGES

- Mac OS X only
- Executed from Disk Utility or Terminal
- Useful as a secure container for sensitive data

ENCRYPTED DISK IMAGE DEMO

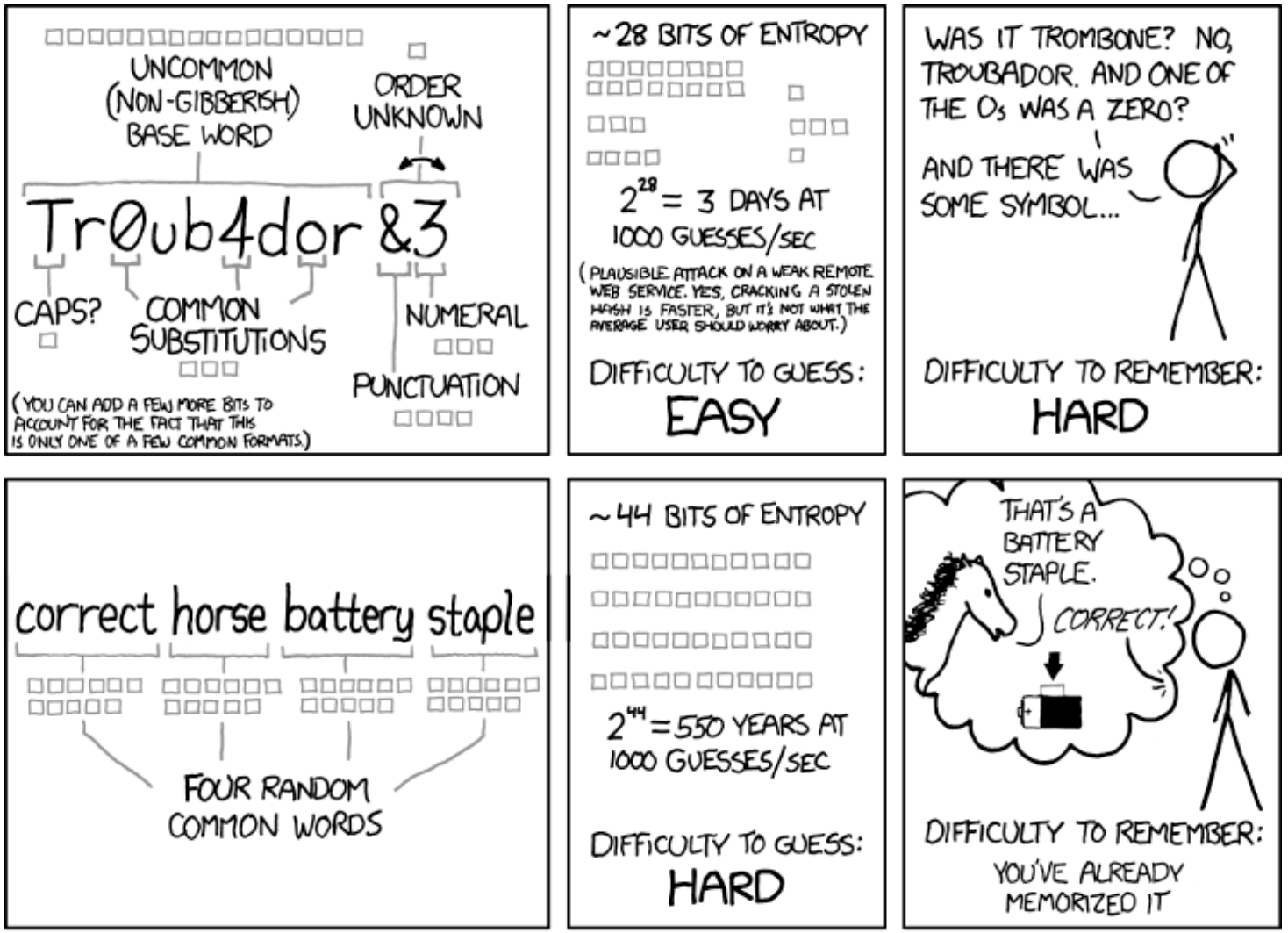
ICLOUD SECURITY

	Encryption		
Data	**In transit**	**On server**	**Notes**
Calendars	Yes	Yes	A minimum of 128-bit AES encryption
Contacts	Yes	Yes	
Bookmarks	Yes	Yes	
Reminders	Yes	Yes	
Photo Stream	Yes	Yes	
Documents in the Cloud	Yes	Yes	
Backup	Yes	Yes	
Find My iPhone	Yes	Yes	
Find My Friends	Yes	Yes	
iCloud.com	Yes	N/A	All sessions at iCloud.com are encrypted with SSL. Any data accessed via iCloud.com is encrypted on server as indicated in this table.
Back to My Mac	Yes	N/A	Back to My Mac does not store data on iCloud. Data retrieved from other computers is encrypted with SSL while in transit.
iTunes in the Cloud	Yes	N/A	Purchased or matched music files are not encrypted on server because they do not contain any personal information
Mail and Notes	Yes	No	All traffic between your devices and iCloud Mail and Notes is encrypted with SSL. Consistent with standard industry practice, iCloud does not encrypt data stored on IMAP mail servers. All Apple email clients support optional S/MIME encryption.

PASSWORDS

- Hard to remember passwords decreases security
- Backup your Keychain
- Substitution does not improve password strength
- Excessive password rotation decreases security
- Increasing password entropy does improve password strength

HTTP://XKCD.COM/936/



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

THANK YOU!

james.alcasid@gmail.com
twitter@jamesalcasid