Why No One Uses Encrypted Email Messages

With so much concern about government surveillance, corporate espionage, and everyday identity theft, it may seem surprising that so few people use encrypted email messages. Try using encrypted email and you'll find it to be difficult and complicated to use.

Encrypted emails are a headache to deal with. You may be able to deal with the complexity, but the people you want to communicate with also have to handle it.

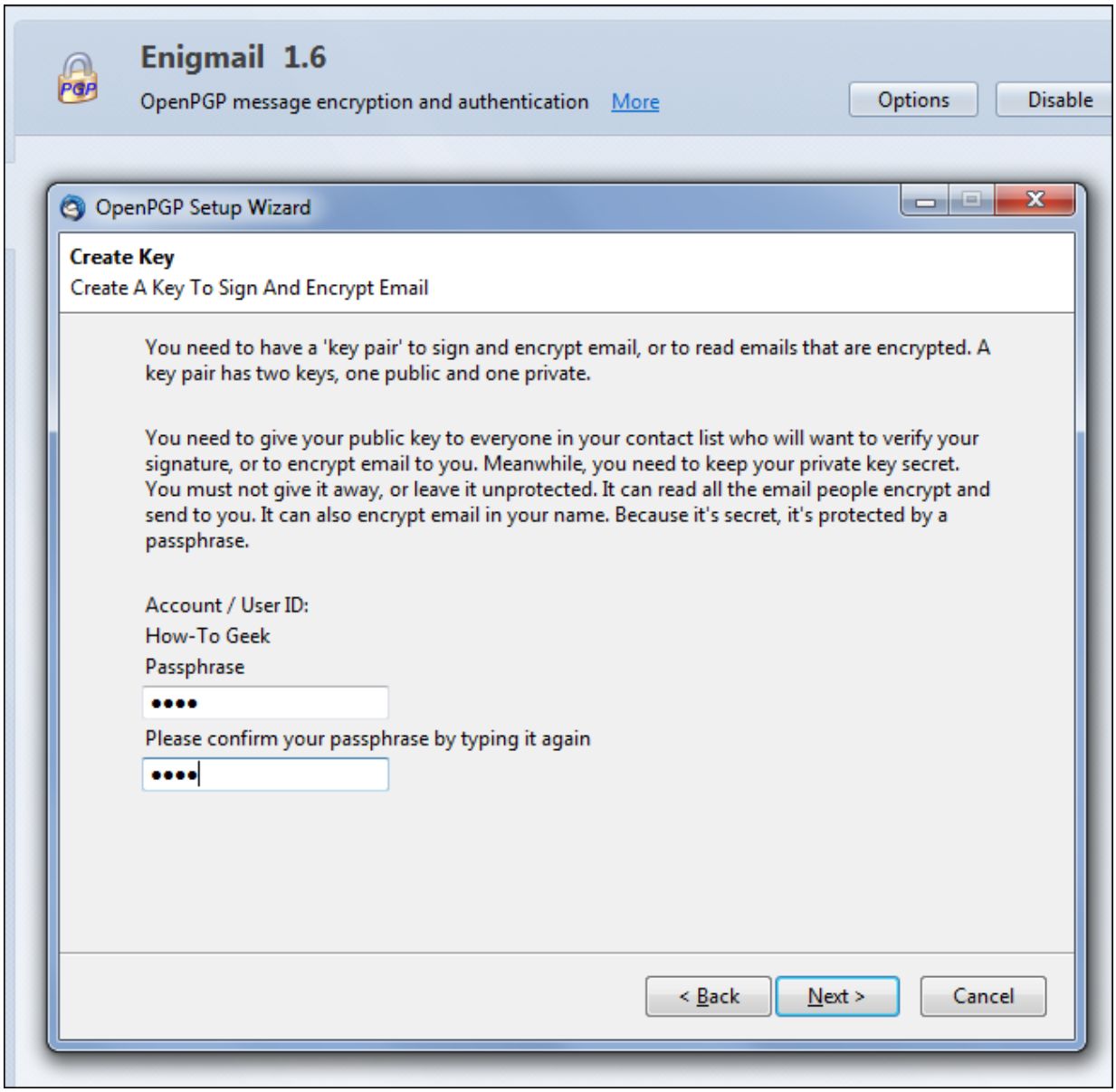
Encrypting Your Own Emails vs. Encrypted Email Services

RELATED: ***What Is Encryption, and How Does It Work?***

We're making a distinction between two types of email encryption here. There are some services that claim to offer easy encrypted email. They'll handle the encryption for you on their end, taking all the annoyance of managing encryption keys out of your hands. If you send encrypted emails between two accounts using the same service, the encrypted email messages will stay secure in the service itself.

This seems tempting, but it's opening up a big weakness. You're trusting the service to handle your encryption, and services like Lavabit have been forced by governments to allow access to their customers' encrypted email messages. The US government even demanded Lavabit's own private keys, allowing them access to all customers' encrypted emails.

If you really want to communicate privately and securely, you'll want to handle the email encryption yourself. This means generating your own encryption keys and safeguarding them instead of storing them with an encrypted email service.

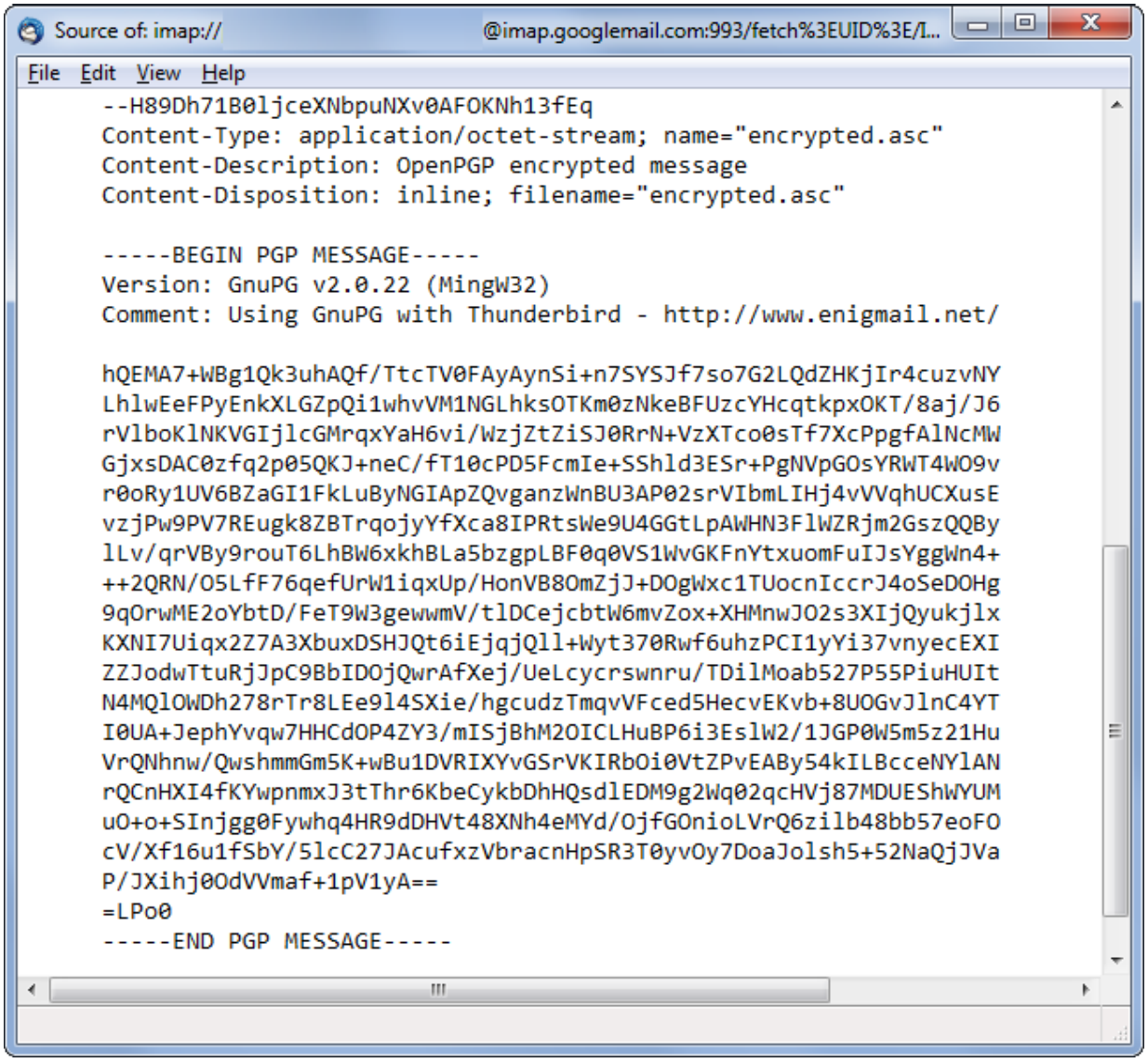


How Email Encryption Works

We typically think of PGP encryption when we think about encrypted email, but there are other standards like the S/MIME encryption feature built into Microsoft Outlook. When you use PGP, you have a public key and a private key. You give the public key to people who want to email you. They use the public key to encrypt their email, and you can only decrypt their email with your private key. So, to use PGP, you'll need to generate a public/private key pair, keep your private key secure, and give your public key to anyone who wants to email you. The person you're communicating with will also have to understand how to encrypt, send, receive, and decrypt encrypted email messages and will need their own key pair.

The contents of the email appear as random gibberish, just as the contents of an encrypted file appear as nonsensical, meaningless data until the file is decrypted.

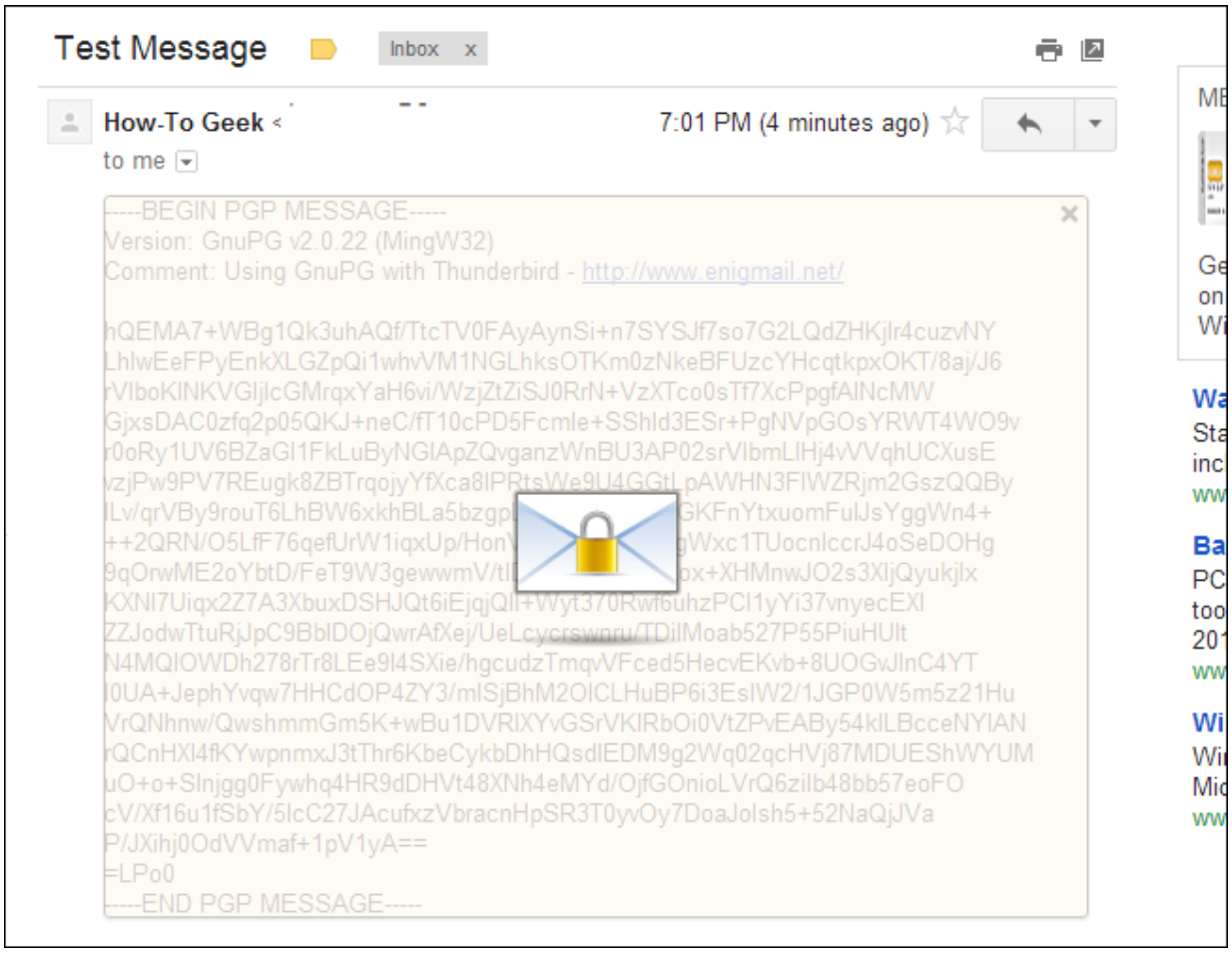
Note that much of an email is insecure even if you use encrypted email. The subject line, To, and From fields are generally sent unencrypted, so surveillance agencies monitoring Internet traffic can monitor who's communicating with who and even see each email's subject. Email encryption is a patch on top of an unencrypted system, encrypting only the message body.



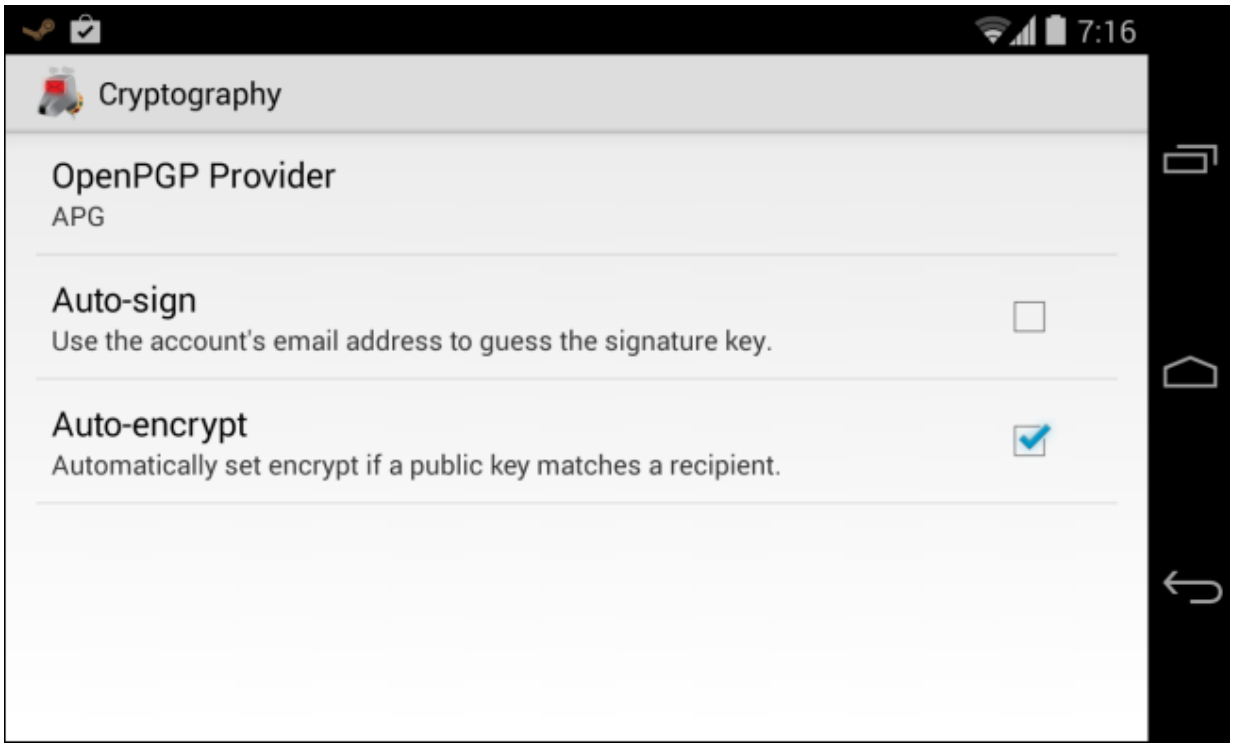
How You'd Actually Use Encrypted Email

Never mind the theory. Here's how you'd actually go about using encrypted email.

Most people tend to use web-based email services like Gmail, Outlook.com, and Yahoo! Mail. These services don't have this feature integrated (although Google is rumored to be working on PGP encryption integration in Gmail). You'll have to use a browser extension to do this. Mailvelope seems to work, offering PGP support that works on webmail sites like Gmail. You'll need it installed in your web browser to use email encryption.



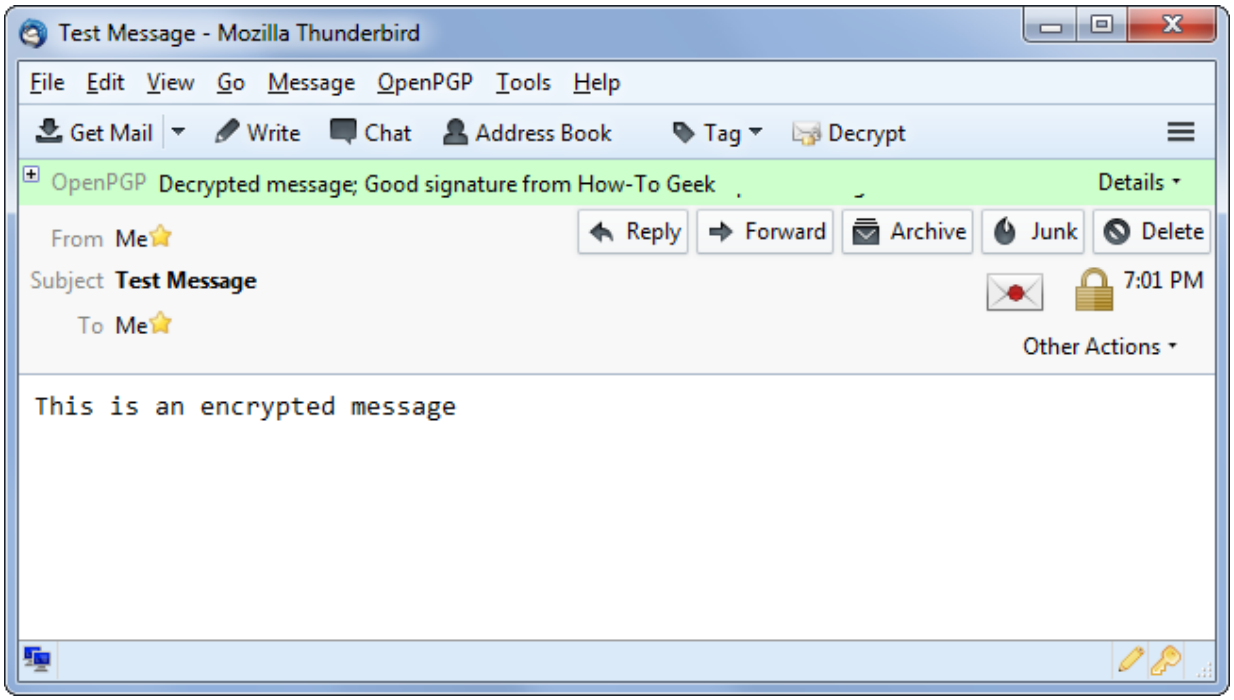
This feature also isn't integrated into the associated mobile apps. Sure, you can access that encrypted email message in your web browser with an extension, but how do you read it on your smartphone? You'll need a dedicated app to do so — you can't just use the Gmail app or the standard Mail app included with your phone. K-9 Mail offers PGP support on Android if you also have APG installed, for example.



Things are complicated even when it comes to desktop email clients that should be able to integrate this better. For example, Microsoft Outlook has a built-in feature to digitally sign and encrypt emails, but it uses S/MIME and isn't compatible with PGP.

The most popular utility to encrypt emails with is the Enigmail extension for Mozilla Thunderbird. Mozilla has stopped developing Thunderbird and may discontinue it one day, so this is hardly an ideal solution. The Enigmail extension integrates OpenPGP into the Thunderbird desktop email client, giving you the key generation, encryption, and decryption options you need. You'll have to install the GNU Privacy Guard (GnuPG) software separately.

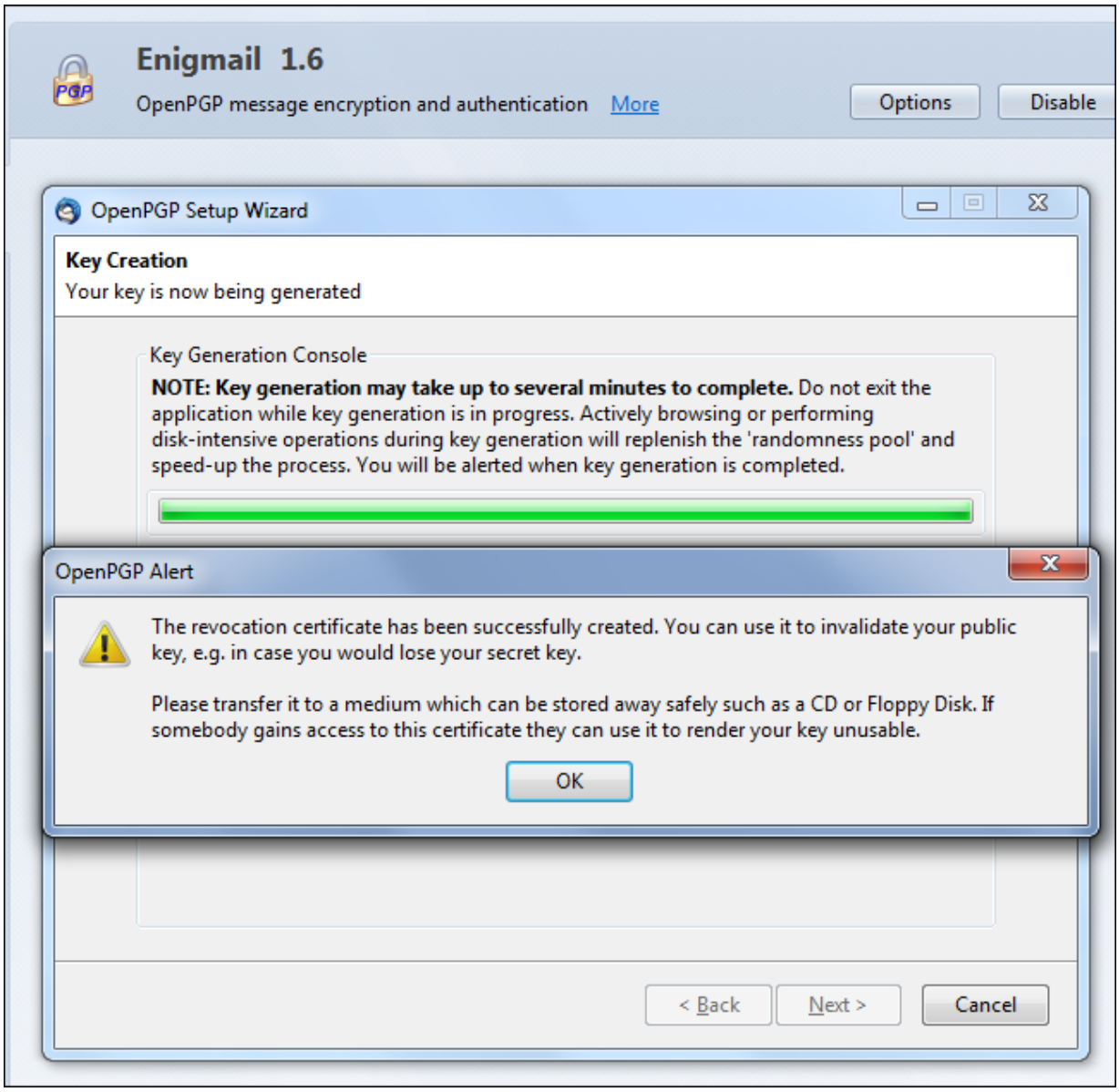
You'll only be able to use encrypted emails in a client that supports PGP. Even when using Thunderbird, you'll need to consider what you'll do if you need to access these emails in a web browser, on your smartphone, on your tablet, or on any system without your private key.



The Problems with Encrypted Email

Here's a quick summary of what you'll experience when using encrypted email:

- You need to understand the way public-private key encryption works, generate a key pair, and provide your public key to the person you want to communicate with.
- Other people you want to communicate with also need to understand and do all these things.
- Both people need to keep their private keys safe so they don't become compromised or lost — in which case you'd lose access to the emails. You also need to keep your revocation certificate as it can invalidate your public key if you ever lose your private key.
- Your private keys must be encrypted with a secure passphrase you have to remember, which is separate from your email account password.
- You need to ensure you're both using the same email encryption standard, whether its PGP or S/MIME or some other standard.
- You need to use a third-party solution — either a browser extension, smartphone app, or email client plugin. If you opt for the best-supported option, you'll need to install an email client, an extension, and an encryption software package separately.
- You need a mix of different smartphone apps and desktop solutions if you want to access your emails on all your devices.
- Even if you do all of these things, people will still be able to see who you're communicating with and what the subjects of your messages are.



With all this complexity — and so much information leaking out even if you use PGP properly — it's no wonder encrypted email is used so little. It's also no surprise that people choose to use services like Lavabit that seem to be a convenient way of making encryption easy-to-use, but are actually much less reliable than encrypting your own emails.