How to make sure a Lock is authentic

Here's the problem: unless someone has given you his/her Lock in person by displaying it as a QR code that you've read with your smartphone (from his/her screen or printed on a business card) or some other direct way, how do you know that a Lock really belongs to this person? If you have obtained the Lock by copying it from an email signature or downloading it from some online source, it is perfectly possible that an enemy may have replaced the genuine Lock with another that actually locks items for him/her/it to read. Then you might end up sending messages to this enemy, who in turn is relaying whatever he/she/it wants to your intended recipient. This is the classical "man-in-the-middle" problem, the Achilles's heel of any public-key cryptography system.

Many solutions have been proposed over the years to get around this problem. PGP encourages users to only use public keys that have been signed by other users, and thus establish a "Web of Trust" that will convince others that the keys are genuine. S/MIME also relies on signing, but not just by everyone, but by specially trusted Certification Authorities. Both schemes have worked well enough to encourage users to entrust their credit card and banking information to web pages, but there are flaws.

The first is that the signed public keys are large and unwieldy, and get even larger and unwieldier with additional signatures and certifications. Users are forced to rely on software to assign an appropriate level of trust to each key, and to do so automatically and accurately. The experience of PGP users in this respect, however, is that the scheme doesn't work without an inordinate amount of personal knowledge and attention.

The second is that Certification Authorities and other trusted Internet actors, such as web hosts, have been known to betray the trust placed on them when pressured by government agencies or hacked by fourth parties. Security-minded websites are increasingly using self-signed SSL certificates, for this very reason.

Against this backdrop of betrayed trust, PassLok proposes a radically simpler alternative: trust only material that you have checked personally. So that a user can hope to achieve this daunting task previously reserved to computers, PassLok makes the checking process as simple and painless as possible. It can be used to authenticate public keys (Locks, in PassLok language), as well as the program itself. Here's how you would authenticate someone's Lock: I'm showing you an easy way, which is also good for authenticating the program, and there's a harder way that can be used if the easy one is not possible.

The easy way:

1. When you make your Lock, click the More button on PassLok so the Lock's ID is displayed above the window. Copy this ID.

2. Go to a device with a camera and make a video of yourself reading this ID. For better security, have some music playing in the background as you read the ID. For good measure, I also like to show to the camera the piece of paper where I've written the ID. The video should be about one minute long. Then post the video on a public online page.

3. When you post your Lock so that people can use it to lock messages for you, post also the address of the video. People wishing to authenticate your Lock can generate the ID as in step 1, and then they can compare it with the ID they see you reading on the video. If they know your face and your voice, they will be assured that the Lock is authentic.

Here's an example, where I am reading my Lock's ID. I made it directly from YouTube's Upload command, using my laptop's camera without any additional software. @@

My hope is that anyone that has met me will be assured that my Lock is actually mine. For people that I've never met in person, my hope is that they have formed a sufficiently complete picture of me from other sources, so that they can identify me on the video. The main feature here is that no "trusted" third party is involved in the authentication. YouTube makes no claim concerning my identity; their role is simply to host a video, which I've taken pains to make as hard to fake as possible.

Variations of this method: (1) Make it a recording rather than a video. Perhaps your voice is enough to authenticate the Lock. (2) Make it live rather than recorded. In other words, call the Lock's owner and ask him/her to read the ID to you. The live call makes it pretty much impossible for a sophisticated interloper to make a doctored recording.

The harder way:

Let's say that making a video or a recording is out of the question, and you cannot establish a live conversation. Then you can use the interlock protocol to detect whether there is a man-in-the-middle between you and the Lock's presumed owner. If you are communicating exclusively by email, you'll send this person the following email, or something like it:

Dear So-and-So:

I just obtained your PassLok Lock from (cite source), but I still wonder if it is authentic since I am unable to view the authenticating video. Therefore, I ask you to help me authenticate it through the interlock protocol. Here's what I want you to do:

1. *Write me a message asking me to take a picture of myself doing something of your choice. Lock it with my Lock, which is at the bottom of this message, but don't send it*

back to me just yet. Instead, save it and display the locked message's ID, and send me that.

2. *When I receive your ID, I will also write a message asking you to do something in a picture, which I'll lock with your Lock. But I'll send you the ID first. When you get it, go ahead and send me the locked message containing your instructions.*

3. *When I get that, I'll check that the ID matches and then I'll take a picture according to your instructions. I'll send it to you right away, along with my locked request. Expect to receive it within half an hour of your message.*

4. *When you get it, please make sure it matches the ID I sent you earlier, and that my picture is what you wanted. If everything is okay, go ahead and take the picture of yourself that I requested and send it back to me as soon as possible, within half an hour if you can. Then I'll know that your Lock is authentic.*

Many thanks. Your friend This-and-That

Alternatively, you can ask the other person to split the locked message in two, and send you first one half, then the other half (PassLok has a built-in function to split messages securely). Instead of a picture, which does not need to be locked before it is emailed, you can request a recording or a video. Only the instructions for the pictures need to be locked and transmitted with a two-step process.

Let's see how this protocol thwarts the man-in-the-middle. His troubles begin in step 2. Since he doesn't know the contents of the other person's locked instructions but knows you should get an ID or everything stops, he must make up some instructions, lock them, and send you that ID. He cannot send you the original ID because when he gets the actual message containing the instructions and unlocks it (using a Key that is not actually yours, but which the other person believes to be authentic), he must then re-lock it for your real Key to unlock it, and then the ID won't match. The chances that he will guess what the other person has asked you to do are minimal, and so he won't be able to produce a picture of yourself that will convince the other person to send you the final confirming picture in step 4. This is especially true if you give a time limit to the exchange, so he won't have time to fake yours or the other person's picture using image editing software.

If you know the other person really well, you may ask each other questions whose answer only the other person knows, but this has two disadvantages: (1) if someone is actually listening, you are going to reveal some private stuff; (2) you may not know the other person well enough for this kind of exchange, but hopefully you know how he/she looks or sounds like. Obviously, if there is no way whatsoever that you can identify the other person, the protocol will fail because then the man-in-the-middle will be able to

impersonate him/her. But then, who'd want to communicate secretly with a perfect stranger?