Photo Seal Security Overview

"If what they wished to build was an unusual summer resort for people of moderate incomes - as they had announced - then they should realize that the worst curse of poverty was the lack of privacy..."

Ayn Rand*, The Fountainhead, Copyright © 1971*

Disclaimer

RealProven, LLC accepts no responsibility for how you choose to use Photo Seal. While every effort has been made to ensure this product functions correctly, the only way to enjoy impenetrable security is to have nothing worth stealing. RealProven, LLC makes no guarantees, implicit or otherwise, that through some future technical advance or unintended consequence of its implementation, your content protected by Photo Seal will always remain private. If you wouldn't send the same message without Photo Seal, you should reconsider whether you should do so with it.

Summary

The only purpose of Photo Seal is to protect your privacy.

Before we discuss some of the features that make it unique, please understand that this app will *never communicate* any of our personal information without your explicit consent. Furthermore, no one other than those people you choose will know for sure that you're using Photo Seal. Everything here has been carefully designed with these basic principles in mind.

From this foundation, Photo Seal combines reliable encryption with convenient secrecy to update a technique that protected the communications of royal families for hundreds of years. In the past, a king's wax seal was used to prevent unauthorized access to private messages. Any letters endorsed in this way could only be read by its intended recipient. It was the appearance of the seal that maintained their privacy.

This model works in much the same way.

Components

Photo Seal begins with an image. Just like with the king's seal, your seal will have a unique appearance unlike anyone else's. This image serves two purposes. First of all, it allows all your friends to identify your private messages quickly because they know what your seal looks like. Secondly, it offers the first level of protection against unauthorized access.

When you send any photos in your communications, your seal image will be used to scramble the colors of the photo before any other encryption is applied. The reason for this first step is to make your messages as future-proof as possible. Nearly all

modern security relies on the use of very large numbers to encrypt communication. The principle is that by using values such as these, modern computers can't possibly guess them, even if they took the next billion (literally) years trying to figure it out. As computers get faster, however, older security that was too complex for older computers, can now be broken. It is a constant race between computers and your private information.

By using your seal to scramble the colors in your message photos, it makes it less likely that a computer in the future will be able to decode its contents. The colors in photos don't follow any rules, and at the moment, only a human would even know if the photo was accurately descrambled.

Next, your seal is attached with two different kinds of secure encryption keys, a symmetric, Advanced Encryption Standard (AES) 128-bit key, and a 2048-bit public/private key pair. The symmetric key will encrypt every message between you and all of your friends. The public/private keys will be used by them to know the message only came from you and to allow them to respond privately back only to you.

In other words, your seal allows you to securely send a message to more than one person, but when you reply to someone else's message, even others with the same seal can't read it.

Finally, once your message has been securely encrypted, it is embedded *inside* a copy of another photo using steganography. What this means is that your message will be hidden inside a decoy image that you can upload to a very public web site or send through e-mail and while everyone else sees the container, Photo Seal will be able to see what is really inside.

All of this allows you to hide your private communications in plain sight. Because there are no user-identifying features to a sealed message, only those people with your seal will be able to read it.

The Vault

While secure messaging is the essence of Photo Seal, if yours and other peoples' seals are not carefully managed, its privacy would be compromised. This management is accomplished with your seal vault.

The seal vault coordinates with the security subsystem on your iOS device to reliably store your encryption keys and ensure that all data saved is also encrypted on disk. This means that even if your device is compromised, unless the attacker has your password, your vault cannot be opened. No one, including the makers of Photo Seal, has the key to the vault except you.

Additionally, the application integrates with the vault in such a way that allows the owner of a seal to decide when to revoke access. It is your choice, at any time, to

send a message to any of your seal holders that directs Photo Seal to erase your seal from their vault. Without that seal, none of the messages you previously sent can ever be opened or read again.

The bottom line is that when you send messages under protection of your seal, you always own that content and you always own that seal. Ownership comes with the privilege of restricting access even to past content, if you decide to do so.

Conclusion

In this new era of globally-connected social technology, it is becoming increasingly difficult to realize experiences whose value comes from their intimacy between people. Whether that comes from a private joke between friends or when reliving memories with family, there is always a need for personal, unshared exchanges. There was a time that to ‘know someone socially’ meant a casual relationship, but that definition has been slowly lost.

Casual has its place, but not everywhere and not at all times. Cultivate the anti-social.