# Pippin Authentication

**version 003**

*Abstract*: Pippin CD-ROMs require “authentication” in order to boot a Pippin Power Player. This technical note describes the Pippin authentication process.

Please send questions and comments via e-mail to pippindev@apple.com.

# 1 Introduction

In order for Pippin CD-ROMs to run on a Pippin Power Player, they must first go through a Pippin authentication process. The authentication process is about applying an Apple-approved RSA signature, in the form of an electronic encrypted key, onto a Pippin CD-ROM.

# 2 RSA's Authentication Software Library

Apple has licensed RSA for their public key authentication software library. The foundation of this library is non-reversible (i.e., one-way) mathematical algorithms based on using large prime numbers as keys to encrypt messages. With RSA's public key authentication system, keys are generated in pairs. One key is held privately by its owner, and the other key, the public key, is given out to be used by others to decrypt the owner's generated "keyed" messages. Public keys cannot be interchanged or swapped, and a message encrypted with a private key can *only* be decrypted with its corresponding matching public key.

Encrypted messages make very good electronic signatures since they can only be decrypted by a public key which is registered to a specific person (or company). Knowing a person's public key, however, will never offer any clue as to what that person's private key might be. Since only private keys can create an encrypted message, the system is secure.

# 3 Authenticating a Pippin CD

For Pippin, the "message" to be encrypted is the entire contents of the CD. Since this typically is a lot of data, and the algorithms are slow, the CD contents are first "digested" by a hashing algorithm which produces a small digest of the CD contents. The digest later can be used to test that the current CD content matches what it was when the digest was first created and than signed (encrypted).

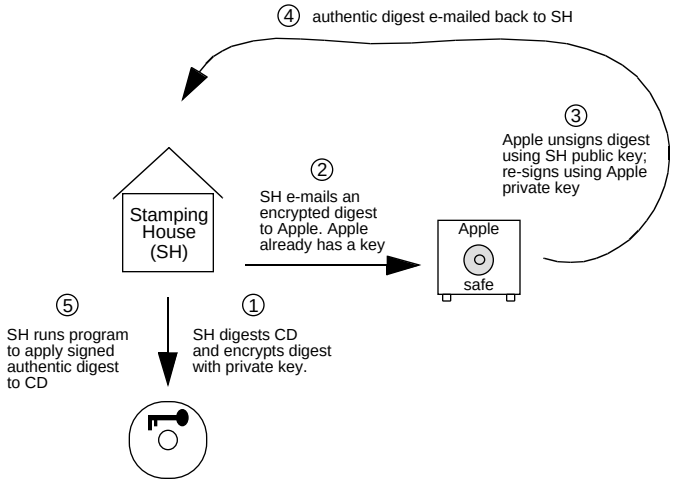
To create a Pippin-authentic CD requires two sets of key pairs. Each authorized CD stamping house has a public pair and private pair. Apple also holds both a public pair and private pair. Apple's private key is on a computer locked inside a safe which is connected to an internet mail system. Apple's public key is inside every Pippin ROM. The stamping house's private key is inside a "digesting" program at the stamping house and their public key is on file with Apple inside the safe.

The authentication process steps are as follows:

1. An authorized CD stamping house digests the CD content, then signs the digest (on the CD) by encrypting it with their private key.
2. The stamping house then emails the signed digest encrypted with their private key to Apple's computer in the safe.
3. Apple's "safe" computer unsigns the digest using the stamping house's public key, and then re-signs it using Apple's private key.
4. The digest, which has now been effectively signed by Apple's private key, is then e-mailed back to the stamping house.
5. Back at the stamping house, a program is run to apply the signed authentic digest onto the CD.

Figure 1 illustrates the flow of the Pippin authentication process.

**Figure 1** The Pippin Authentication process




Through this process, private keys never have to be revealed to anyone and the only data which leaves the owner's facility, via e-mail, is encrypted with a private key.

After the stamping house applies the signed authentic digest to the CD, the CD is Pippin-authentic. During the boot process, the Pippin ROM creates a temporary digest using the same algorithm as was used to make the original, then unsigns the digest on the CD to compare the two. Only an exact match will allow the boot process to continue.

---

☞ Pippin disks are not exactly encrypted since they still will mount on a Macintosh just fine. However, the still have a signature applied to them which can be read and tested.

---