Most secret management tools are designed to store exactly one of these types of secrets, and while you could try to force it to store the other types, that's rarely a good idea from a security or usability standpoint. For example, the way you store passwords that are infrastructure secrets is completely different from how you store passwords that are customer secrets: for the former, you'd typically use an encryption algorithm such as AES (Advanced Encryption Standard), perhaps with a nonce, as you need to be able to decrypt the secrets and get back the original password; on the other hand, for the latter, you'd typically use a hashing algorithm (e.g., bcrypt) with a salt, as there should be no way to get back the original password. Using the wrong approach can be catastrophic, so use the right tool for the job!

The Way You Store Secrets

The two most common strategies for storing secrets are to use either a file-based secret store or a centralized secret store.

File-based secret stores store secrets in encrypted files, which are typically checked into version control. To encrypt the files, you need an encryption key. This key is itself a secret! This creates a bit of a conundrum: How do you securely store that key? You can't check the key into version control as plain text, as then there's no point of encrypting anything with it. You could encrypt the key with another key, but then all you've done is kicked the can down the road, as you still have to figure out how to securely store that second key.

The most common solution to this conundrum is to store the key in a *key management service* (KMS) provided by your cloud provider, such as AWS KMS, GCP KMS, or Azure Key Vault. This solves the kick-the-can-down-the-road problem by trusting the cloud provider to securely store the secret and manage access to it. Another option is to use PGP keys. Each developer can have their own PGP key, which consists of a *public key* and a *private key*. If you encrypt a secret with one or more public keys, only developers with the corresponding private keys will be able to decrypt those secrets.