The Izzentek Licensor Process

Izzentek Licensor is based on the concept of *digital signatures*. The digital signatures used in Izzentek Licensor are based on RSA cryptography, using a *private-public* key pair. The private key is used to digitally sign a license file, while the public key is used to verify that the digital signature matches the license. If either the license file or digital signature is tampered with, then the digital signature will no longer match the license, and license validation will fail. As well, only the person or organization in possession of the private key can generate digital signatures that can be verified by the corresponding public key.

There are three components to Izzentek Licensor:

1. The License Key Generator
2. The License Signer
3. The License SDK

Each of these components are used at different stages of the licensing process. This white paper describes the different stages of the licensing process.

The License Key Generator

The License Key Generator is the software that is responsible for the generation of the private-public cryptographic key pair. The private key will be used for the generation of digital signatures for licenses. This private key must be kept secret and not be disclosed outside a trusted circle of people within an organization. The public key is used for verification of license signatures. This public key is not secret, and in fact, must be shipped with your software or license file so that the license can be verified when your own software is run by the end user.

You can choose to create one or multiple private-public key pairs. If you create one key-pair, you would use the single private key to sign all license files that you create, and ship the single public key with your software. Alternatively, you could create multiple private-public key pairs. In this scenario, you may choose to sign licenses with different private keys for different customers. However, there is more administrative overhead associated with this technique, as you must ensure that you ship the correct corresponding public key with the license file to your customers in order for their license validation to succeed.

The License Signer

The next step is to create an Izzentek Licensor XML license file that you would like to ship with your software. This license file can contain information such as the end user's name, an expiry interval, and feature restrictions, among others. The XML license file must be constructed in accordance to the Licensor Schema.

The License Signer is then used to digitally sign the license file. It takes the XML license file and the private key as input, and outputs a file containing the digital signature of the license. This digital signature file can then be distributed to the end user (along with the XML license file, if it has not already been distributed) so that the end user can run your software.

The License SDK

The License SDK is the Java software library that you embed and redistribute with your software. It provides an API that allows you to validate the license for your software, as well as check whether specific software features that you have defined are enabled or disabled by the license. This API is powerful in that it allows you to restrict features in your software based on the license. For example, you can distribute Trial, Standard, or Enterprise versions of your software using the exact same binary distribution, but providing different licenses for each version.