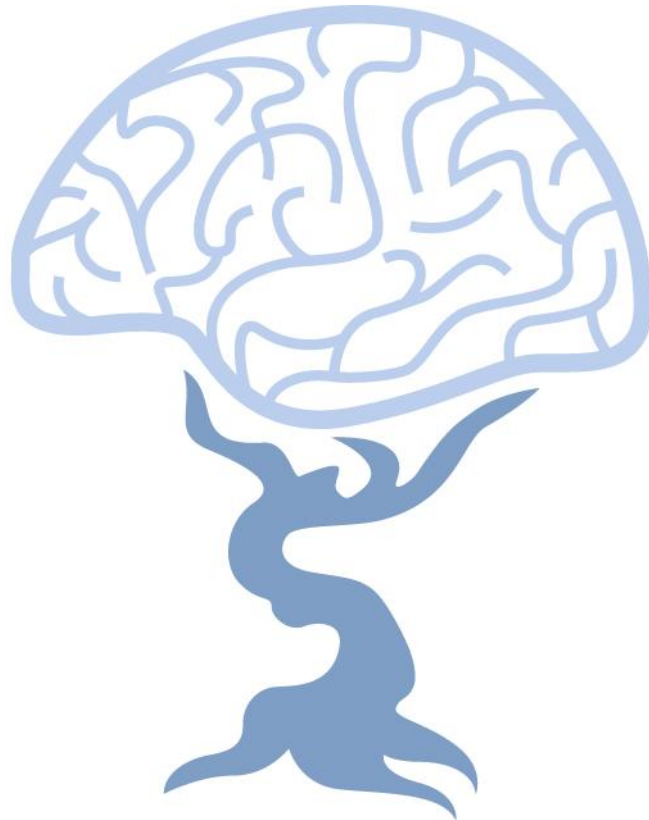


Introduction to the Roozz security model



roozz[®]
makes software grow

April 2011

Still under construction

Introduction:

This document describes the Roozz security model. The document is intended for end users, customers, developers and decision makers.

Roozz plugin is a product that allows end users to run standard desktop applications in the web browser and then it includes several attractive features. When comparing the Roozz plugin to other browser plugins on the market today the primary advantages are that:

1. it can run CPU and GPU intensive applications much better than for example Flash Player and Silverlight.
2. the developer efforts to web enable an legacy .exe application is very small for most legacy applications.
3. the security model has several advantages over standard ActiveX plugins, both with regards to the end user and to the company which distribute the application.
4. the Roozz Platform offers a new payment model that allow rental and micropayment with very few click by the end user and reduce the transaction fee overhead to a minimum.

ActiveX security

Today it is a well known fact that there is a security risk when installing ActiveX plugins on the end users computer. Basically ActiveX plugins (as well as plugins for FireFox, Chrome, Opera, Safari, etc. In the following they are all referred to as ActiveX plugins) run directly on the users CPU and the programmer can do almost anything with the end users computer like logging passwords, erase the harddisk, etc. Thus end users are advised never to install ActiveX plugins from parties they don't know and trust and if in doubt don't install at all. But it is also a well known fact that most computer users around the world have install Acrobat Reader and Flash Player on their computer, which are examples of two ActiveX plugins which most users trust.