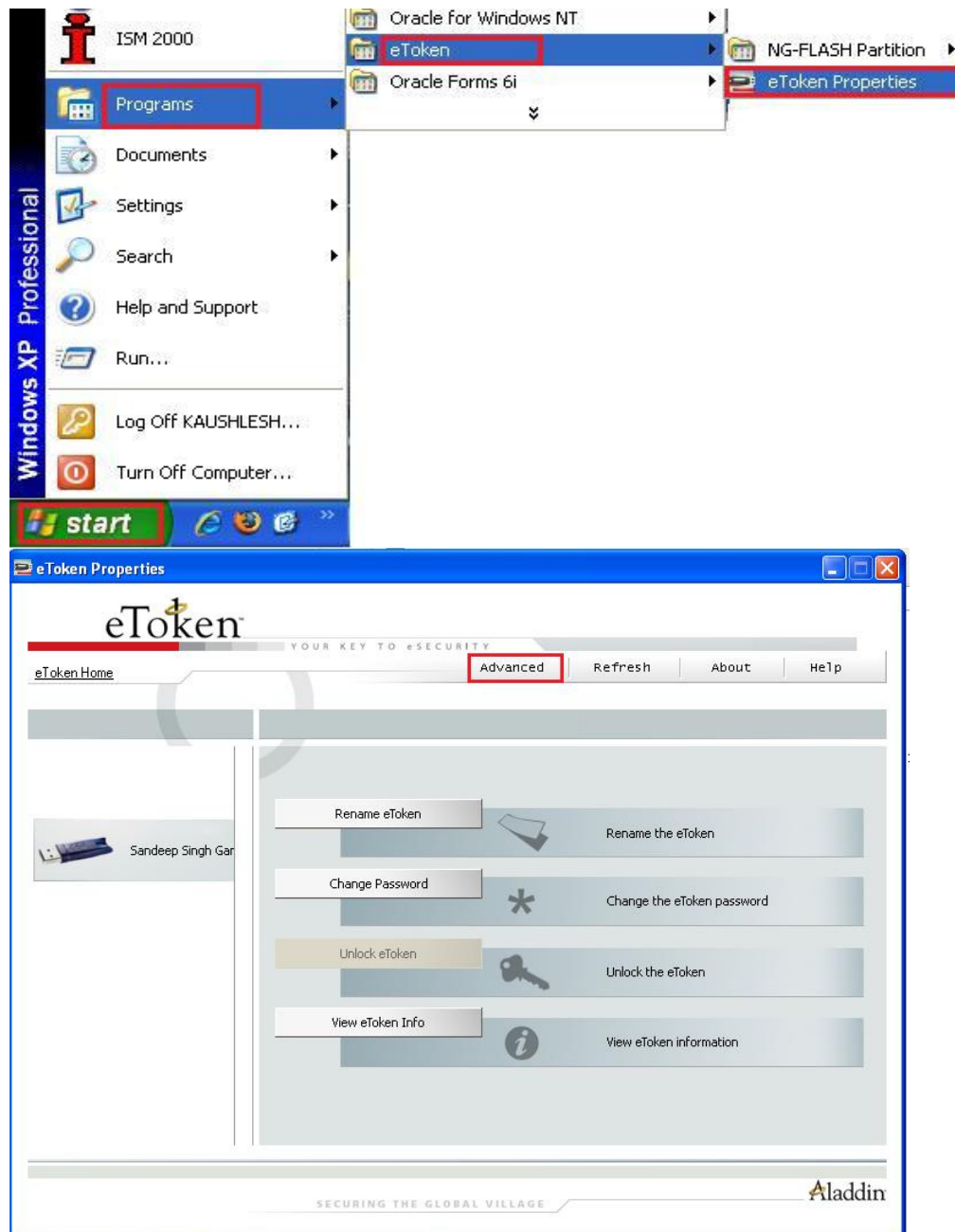


## Precautions for Safe use of e Tokens:

There are some settings by which Digital signature can be stored in client Machine. This is not secure and following action should be taken for safe and secure use of digital certificate.

If Driver and software of e-token installed properly, an interface of “**e Token properties**” can be opened as per procedure shown below.

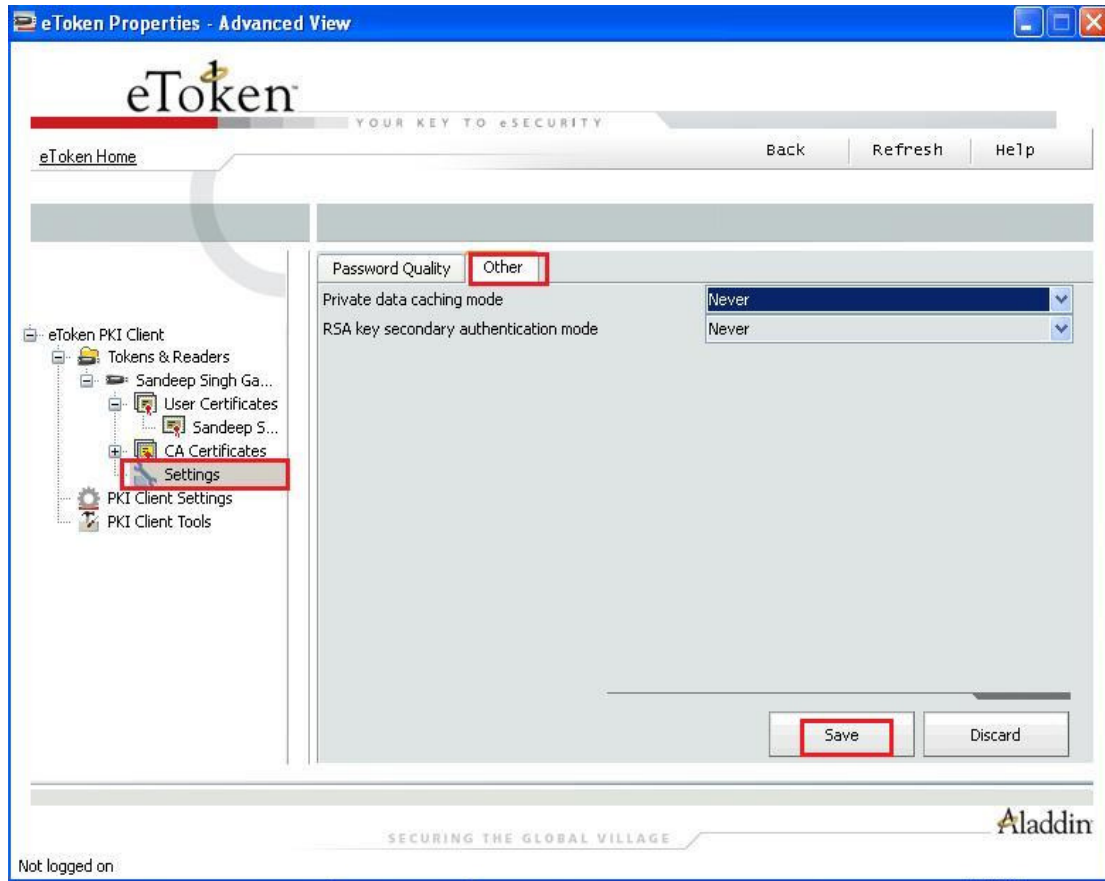
**Step 1:** Click on **Start > Programs > e Tokens > e Token Properties**, Then click on “**Advanced**” tab



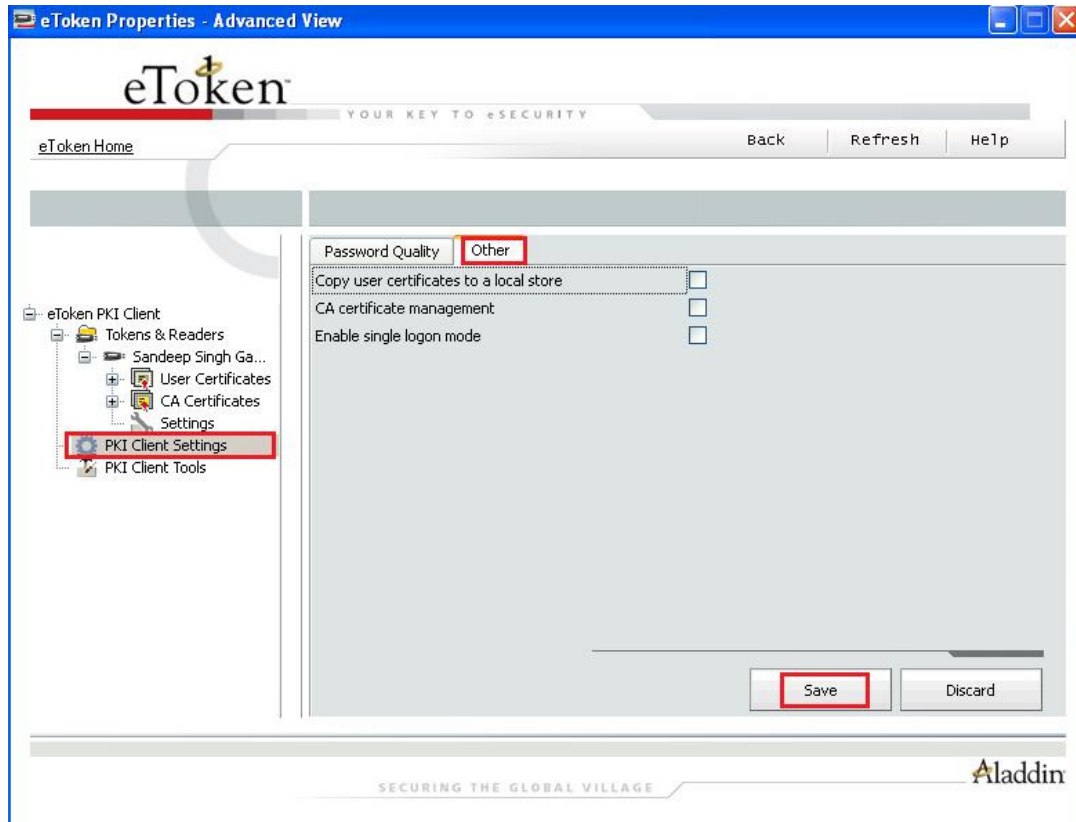
Then following window will appear,

**Step 2:** Click on “Settings” under eToken PKI Client >Token & Readers, then Click on “Other” tab,

There are two Options “Private data caching mode” and “RSA key secondary authentication mode”, select “Never” from dropdown menu for both options. Then click on **Save**.



**Step 3:** Click on “Settings” under eToken PKI Client >PKI Client Settings, then Click on “Other” tab, There are three check box for three options “Copy user certificates to a local store”, “ CA certificate management” and “enable single logon mode” . All checkbox should be **unchecked**. Then click on “Save”.



By adopting above procedure, it will be possible to remove the private data of digital signature certificate from client machine.