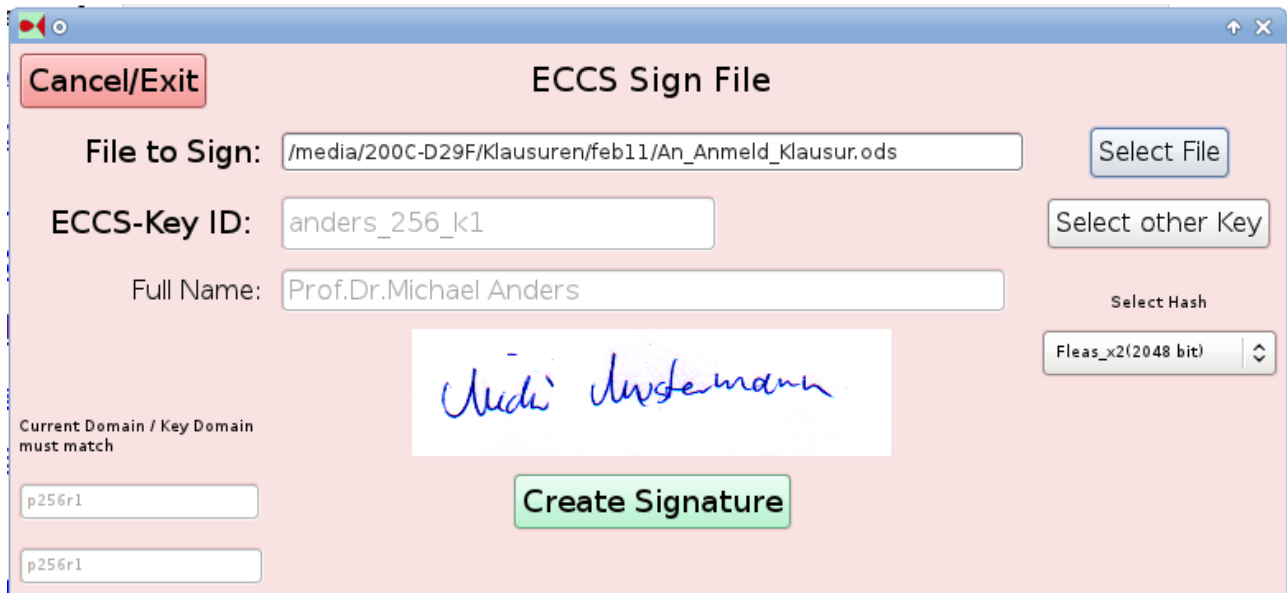


## Some Screenshots of Academic Signature

Academic Signature is dialog oriented and contains more than 20 different dialog windows. To give you an overview of what is to be expected during usage, I took some shots of core dialogs. The shots were taken from version b17.



*Illustration 1: ECDSA Signing Dialog. You select the file to be signed, the private key to be used and select which hash algorithm is to be used. Clicking "Create Signature" will produce the signature file sharing the path and name with the document file with the additional extension "ecsg". Note that the red background color indicates an operation involving the private key.*



*Illustration 2: Shot of the Verification Dialog after a successful signature proof. You select which file to prove and the public key to prove against. The public key can be set from internal protected storage(Button"Get Stored Pubkey"), from importing a human readable \*.pell file containing the key(Button "Import Pubkey from File") or can be simply pasted into the Text controls from any textual source in hex-notation. Upon signature acceptance, the green message appears at the bottom and an additional message box appears.*

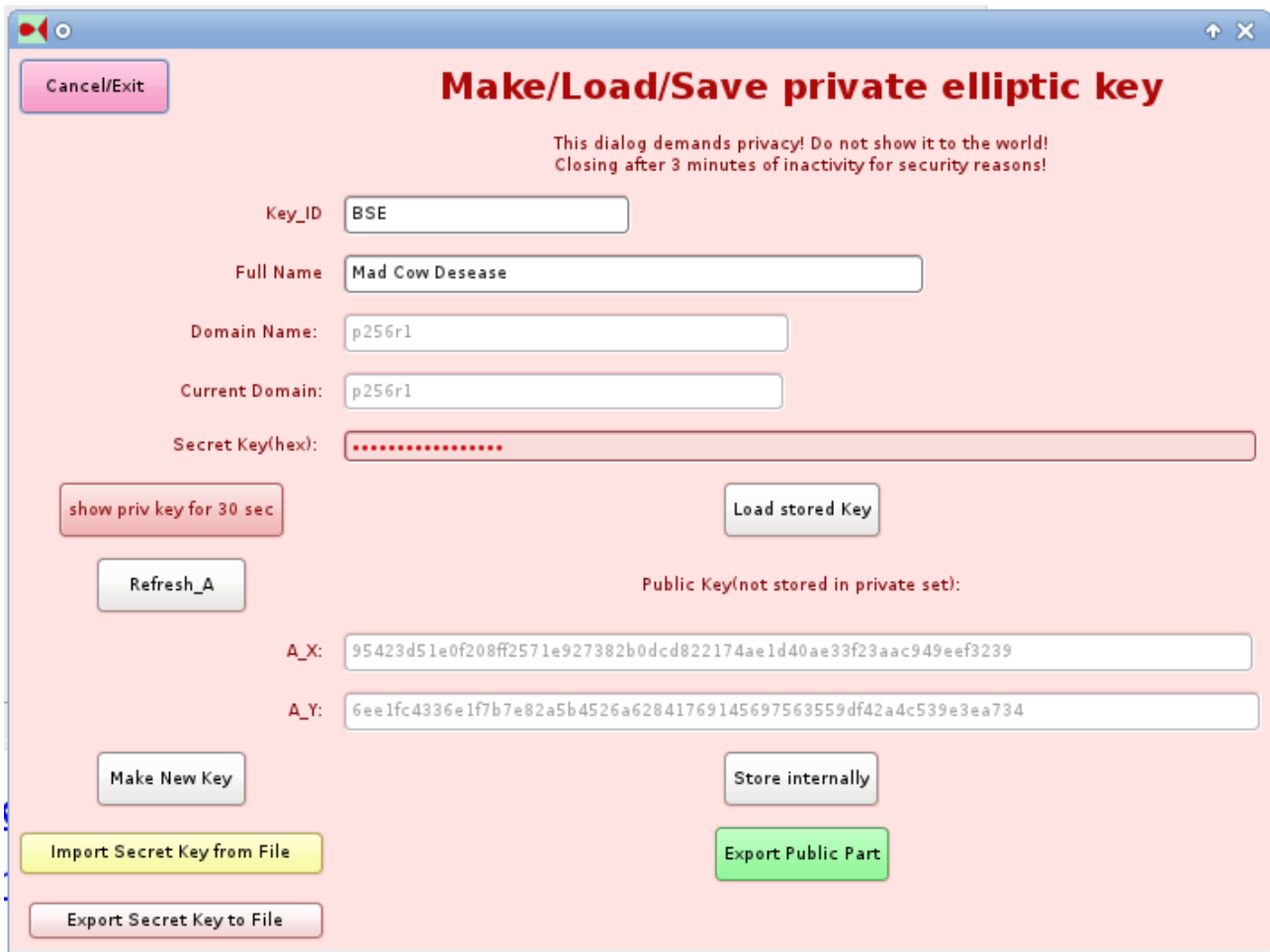


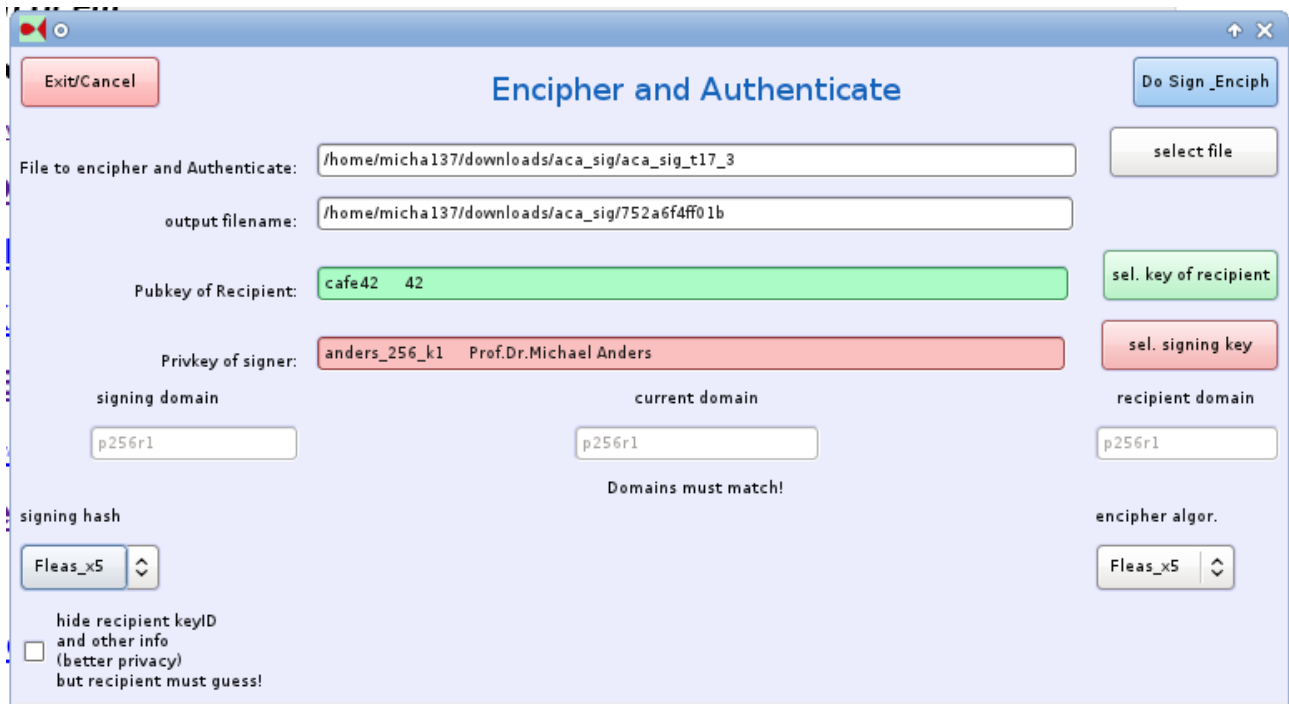
Illustration 3: Dialog for handling private key information.

Procedures and associated secondary dialogs accessible from this dialog are e.g. retrieve private key from internal storage ("Load stored Key"), produce new private public key pair ("Make New Key"), export public part to file, import private key from enciphered file or export private key to an enciphered file. Since this dialog has access to your personal "Fort Knox" of secrets it will close automatically if unattended for some time. Hinting to involvement of private keys, the background color is reddish.



Illustration 4: Dialog for dealing with and selecting public key information.

Again the public key can be set from internal protected storage (Button "Retrieve Locally"), from importing a human readable \*.pell file containing the key (Button "Import from File") or can be simply pasted into the Text controls from any textual source in hex-notation. The green background denotes that public keys are dealt with from here.



*Illustration 5: Dialog for combined authentication and encryption. Use this dialog to first sign a file with your private key (red text control), merge signature and original document and encipher the resulting compound file for the intended recipient using his/her public key (green text control). You may select any file name for the cipher and can choose from a wide array of hash and symmetric enciphering algorithms. The public key of the messages target may or may not be disclosed in the cipher for either comfort or added privacy, respectively.*

*Upon successful deciphering, the recipient will be informed about the file being a compound of document and signature and the file will automatically split into separate document and signature files.*