Public key certificate classes

We will have different class certificates one is called class 1, this is automated and we give name address and stuff we give and this is for the identity of the user so when some one asks this question how will identify the users, because what you are saying is this ,im bla this is my email address , I want public key and this is my certificate , how will VeriSign know that you are the one who sent that info to VeriSign ,im not standing over there, im just clicking on that thing and getting digital id and there form appears and there I will write my name, and every details and my public key will get automatically updated, in the system so how do you know that you are actually using your name ?.., that's why they ask your email id, as they send the second portion of steps to recover that certificate via email ,if you are giving the correct email you must be the one who can recover those certificates from the second part of email , I know you are not clear, what they are doing is they are using the email account and sending a confirmation about your application and they send the second part of the email, if you are one who has the email account then that is the identity verification for the VeriSign it is not high level high security system , you may fool them by saying you created a dummy account with a dummy name ,go and get a digital id and use it for your friend and you can use someone see name and there is not high security in clas1 so most of the application do use this one, in other words when you use class 1 you know disadvantages of class1 , so that's why you are using class1 where you don't need very high level of security ,it is quite enough that not enough security is needed, it will cost you not enough money , it will cost you 10 or 15$ for trial version so its not that costly that's why it doesn't have too much security what about the private key is protected in VeriSign and that protection mechanism is PCA, which is VeriSign permission certificate authority and ca actually stored there private key If it is in ca it is transfer the site software and hardware they are tamper proof hardware that the protection is high level they may also use software to protect there private keys they are all class1 and they are used in web browsing and other application ,its is not a big deal as far as security is concerned , in class 2 we are going to improving the security, they are going to improve the security by providing email security + automated information check and automated address check and some other steps so that you can see the recovery mechanism certificates from the mail not the email , they are going to ask for you address so its your physical address or company address that's provide little bit better verification, they go through pca and ua private key authority application include ,online subscription ,web browsers like I said there are lot of high level applications , but if you are looking for more high level security then you can use class 3 , in this it is different it uses class 1 plus class 2 and id checking and it will check the id the person having the certificate and then you have tot show the company details that means you have to show your details that is for the class 3 as you to go there class 3 certificate and this is very highlevel and they are protecting there hardware and application of high level things, what about your private what happend to your private key that you have ?. it will go to the encryption level recommended by SMIME and for windows environment they are supported by many application but you don't have nay control on it, for class it ,encryption software pin protected and encryption software along with hardware token recommended , so in other word you can carry smart card to access the key when you need to create your private key or your own key , system may ask smart card from you, you have to put smart card into your reader so that you can work on it ,things are clear?. In the lab exercise you will use the class 1 file and you can see how you can check how class 1 files are used and you can see how VeriSign can use that

stuff any email client to send the encrypted message or send the SMIME message this is the end of chapter 5.