X509 certificates

There are three versions version 1 ,2 and 3, and certificate serial number and signature id and parameter and subject name and if you are using this for email then this subject can also for email addresses. In the past we didn't had anything else, right now it could be email address or something, issuer email id and issuer email address in the past these information were not useful for us ,companies with same name or different name ,we have to make this unique, so that I will use another identifier to make this thing unique extension field in version 3, it is generally related to key ,like this key is used for encryption and these keys are used for email security and those kind of usages, we will see the details we are just look at the basic part , and look at this part here ,the last part is going to be very important here along with the signature public key info box ,it contains signature field, algorithm and key what I am going to do in the signature part is im going to calculate the hash of all these fields ,lets say im using sha1 algorithm, I am going to use sha1 algorithm to calculate the hash of the all these parameters ,and im going to put in the last part and it will be encrypted with the CA private key, and that is the signature and I said this is the binding with usage, and where is the binding?..in the algorithms itself like?.imagine that you are an hacker and you want to change the subject name to something and you are changing the public key to corresponding private key and use some one else name and then whoever wants to secure something to that name ,so how can you change the public key and im using the signature over here, signature means when we hash the parameters here the last parameters will receive the hash of the messages and when you sign it with private key , no one can sign it that way if you change the name here then the verification is going to change what is the verification ,we are going to use public key of hash to get this CA and im going to get the hash and if it matches then im going to added to the signature field here. And I am going to use this public key for this user ,signature means encrypting the hash with the private key ,so no one can forget this one if they know the CA's private key lets have a look at the creation of the certificates ,what you are doing is ,its called digital id by the way and you are going to go to verisign site and its going to ask some questions and most probably you will get certificates for email security ,and your subject name and your crypto api of your operating system will generate public key and private key pair , and it was going to send the public key info along with modulus to verisign and verisign will calculate all the steps and sign it and encrypted it send it back and verisign doesn't have any idea about your private key ,if verisign knows your private key then forget this one that's means that you are revealing your secret to the company that you trust and private key will be trusted and you are not going to say that this Is your public key ,then private key and things like that save it that place and these are done by crypto api of the operating system automatically by the way and sending the messages does help the authentication as well ,you are going to see in email security ,you are going to get the lab exercises , public key and private key ,you are going to go to verisign and sign it send it and so on and so forth and you will have the experience and you will see lot of standards like PKI standard to get this things ,how you are going to store the keys in smart cards each one will be a standard anyways we will se the details ,binding is this signature , so any certificate ,when you check the certificate and when you verify the signature you can say that it is valid key for the user and lets have a look at real certificate , let see in my computer. these are the certificates I have now and lets have a look at individual , it says that my certificate has expired that I had in last quarter , it was issued to me , and issued by remember the field verisign class 1 valid form this date to this date , 1 month , when you know

so I have this to use but it expired and you have the parity and lets have a look at the details so that you can see all the detail now we said that version 3 ,every certificate has the serial number , this is the serial number and every credit card is valid for visa not for master card, some body may have same credit card number from the different companies so there is that kind of possibilities so this is unique and we have to specify which algorithm we have to use using signature algorithm to sign the service hash is going to be calculate d with sha1 and encryp4ted with RSA and the other option is DSA and they are using DSA , and issuer is verisign ,as I said they are all x500 names , they say organization verisign, country US , org unit ,and many stuffs that defines x500 names of the issuer , and then lets go to valid to ,valid ,subject name is my email address and be careful if you have gmail account and if you include someother address then you cannot use the certificate for gmail account you must provide gmail account address .this is my x500 name it same org is this, CN is my name and email address is this one and email Is also option in x500 they are defining me in x500 structure and RSA key and the modulus size of the RSA is 1000 bits they are not providing 2048 bits , this is the key in hex format and the modulus you can see that this is correspond to modulus and public key and size is 1024 bit ,these are valid constraints in version 3 and I will explain later on certificate policy it say what type of certificate we are using and this shows that this key is used for encryption or DS and there is another option enhance email land it is for secure email and client authentication and they defined that way and other imp thing is , if this is not valid anymore how do you know this is not valid and they are keeping the list of invalid certificates and it is called certificate revocation list , so if one certificate and serial number will go to any ,everytime I will be checking crl list im not going to use it as may be only dates are valid and thumb print is the hash algorithm and this Is the hash of the message right here, encrypted because this is the DS this is the real certificate you are going to use and to distribute the public keys of the user and that’s why we use it, and I don’t know which key belongs to whom kind of stuff, but when we look at pgp, it will solve these things in a different way but this is very widely used application and this is the certification path , it will give the verification of the address and the important question Is how do I know the public key of verisign to verify the certificate to verify the certificate to you are going to go through the verification process ,it means decipher the signature with the public key of ca and how do you know it?..lets have look at this part trusted root certificate by this operating system these are the companies they are working like ca and accepted by so and this guys verify so relieved by this user and the public key verified but the company which are listed here ,you are going to get the warning message ,it will say that this certificate is not a trusted one ,are you still want to accept this one if you say yes then the path over there , by using the certification path they are going to recover the CA and verify the signature and that s going to be the idea otherwise it is done by the OS it is going to be handled by the OS asi was talking about revocation list this is the revocation list ,signature id and parameters updates of this list and next updates and revoke certificates ,it is the certificate defined by the serial number and date if some one finds the certificate serial number in the crl list you are not be able to use the list and the mechanism you are using in PKI and this is also be signed by CA, why is that?..if some changes it ,it should be unforgable ,whoever is maintaining that one will change the things with those updates users will not be able to update , if you want to change some body else then just put the serial number over there and that certificate is going to be revoked and again you may cause mahem ,its not going to work properly ,if you do those kind of stuffs in the industry ,so we are going to have lot of complex issues this is not a easy job and this pki is quiet a complex thing.

Obtaining a certificate,

Any user with access to CA can get any certificate with it ,only the CA can modify the a certificate this is unforgable and certificates canbe placed in public directory that’s why we said it is a part of x500 ,so it will be x500 global directory.