CA hierarchy Use

X509 and authentication thing requires for this CA hierarchy use and other important thing is for us was, this certificate revocation why we are doing ?

Certificate revocation

Certificates have periodic validity and user is not longer certified by verified by this CA and there are some information User private key CA private key and these are the reasons we are checking the list all the time ,so you don't have any option saying that first of all go and check the certificate from the crl and when you install any certificate from the crl ,that means that certificate has been checked by OS ,

Authentication procedure

There are three ways one way , two way and the three way both of them are using public key signature ,for example

One authentication

It is used to establish the identity of A and that message is from A ,and message is intended for and message is intact and it doesn't mean anything lets have a look at details , im going to send the timestamp and im going to send the random number and identity of b saying that I want to access b and I want to get it signed and I m sending a session key encrypted with the public key of b ,in other words key distribution ,what is the authentication over here?..where is the authentication ?..k_{ab} is the session key and im signing the data and all the se guys are hashed and encrypted with the private key of a and when b receives this one then it will receive the public key of a to verify this signature, so when the verification is successful the n verification can come from a ,because there is only one entity that can sign data like this must have the a's private key , so Authentication come from the certificate and that's why it is called x509 certificate ,this is my number and a authenticating with b and if we have the same parameter and b to a which going to be two ways ,now look at message 2 ,T_a , r_a , sign data used between b and a and for this direction one session and for the other direction other session key and you can vomit this part you can use it for this and why you are using t_a , r_a k_b ,one is t is timestamp r,is random number so im trying to measure or identify the freshness of the message so this way I have two way I have two way authentication and this way I have two way authentication but I don't know whether a is successful authenticated by b or b is trying to authenticated to a ,this r_a information so we are going to send it to a and this back to b so this way b knows a is successful authenticated a and this way is called authentication three way and this is this way and 3rd is just send a random number back to b and this way you have 3 way authentication and with x509 we have this kind of authentication , so we have only one r_b in this one you are right it should be r_a, because it was r_a I n the previous one it was r_b , are we clear with this authentication by signing the data you can have this authentication scheme Kerberos 1 was one authentication and the this is the second ,x509 and Kerberos we saw so far and so lets have a look at x509 version three .

X509 version 3

These are extension fields has been recognized that additional information is needed for that field and what is that additional information ,issuer name and sender name was important ,because they were not unique there could be another company it could be some other name and the user name could be something else we needed unique thing because the certificates in the email security the certificates will come to your email versign will issue the certificate to you email account and if you try to use it then its going to work with your email account and not with your other account and it will not allow you to send or encrypt later its going to be little bound email address that you provided when you created th certificate and that's one extra thing actually so in other words they can issue the certificate not jus for the name but for the users email addresses or url , sometimes you can get the certificate to t he department of the company and how ever is working in that dept will be able to use it and we could use it in the past as we dint had the url name ,url ,email addresses are going to give us those kind of extra things so what we doing if we are making more unique not only names but also these guys and for those unique guys most of the time this kind if x50 structure to define the user and to fine the company and extension consists of extension identifier ,criticality indicator and extension value im not going to too much details we are going to define the key policies in version 3 ,subject key identifier , key users. In that we will say that you are going to use this DS or for encryption for both it will be different if here are those kind of different things are available then you have to say that these kind of keys that are available is used for this purpose only , or private key usage period, so you can limit the private key usage or you can say this things are valid only upto this time , and the other one is policy mapping and what Is the category and so on these are the parameter s we are using for key policies and other one is subject automotive names and key automotive names and some application like ipsec may require to use different name sna id you are using certificate for ipsec protocol the names will be different and those names will be subject alternative and issue alternative names and if you going to carry x509 subject attributes what kind of attributes you are going to put? Telephone number office number ,department number and what ever you can include the attributes the o, c , and 1000 are available as a designer its upto you which kind of design you want to include in x500 directory in the certificate version 3, because when you get the certificate you are not jus going to verisign and saying I want certificate when you go there and request ,verisign is not giving you certificate immediately it will send you to the email address the instruction of how to get the certificate it will say that I received you application and here you this is the instruction but if you know the peoples password then you can fool the people, another time they will send to your home address this time its going to be hard copy of the instruction and its not going to be secure and increase the security level and this time it will ask you to go to verisign and show your id show your company doc and then they are going to give you certificate and they define the class and in our application we are going to use class 1 its going to come to you email then you aer going to follow and get your certificates these are version 3 information and with that information we are having really nice flexible certificates ,lot of extra info, as I said key and policy information and subject issue keys plus indicates policy and any attributes can be selected

Certificate extension

When I get the certificate and when I get to verify how am I get the public key info of the issuer?..how do I know verisign public key?..we create d this public key information and its not easy to assign public

key to the owner but how do you know that public key is verisign public key how are you going t o access and those access define certificate path constraint and so will do the math and user transparent and it will have all the certificates for the trusted CA ,if you receive any certificate outside ,it will warn you as I said before, finally it will follow that path to verify the certificate if verification successful then you can use it , if not then you cannot and that is the definition of those kind of things , so far we say Kerberos x509 certificate , one more thing is PKI ,PKIX and it is the last section in this chapter and it is architectural model it is the same model for any pki application and it Is not important for us if you understand the PKI structure and if you understand architecture it is available.