PGP key management

Last time we discussed that how we are signing the message with pgp and how we are encrypting the message with pgp, and we realized that key management will be big idea so that we are signing the message ,so if we are signing the message then im sending the key id of public key of the sender, that is actually the corresponding public key to the signature basically, for the encryption of the message we are encrypting with the session key of destination so im sending key id of destination public and we also mentioned that we will be having two key rings public key ring and private key ring, in pubic key ring im going to keep all the information of the people I know and it is indexed y using key id and the other one was private key ring im keeping my own public and private key ring , but the private key store as encrypted entity and the encryption done by hash of passphrase was a key to encrypt as private key ,but as far as id 's are concerned id's are only private keys ,we don't have ids of any private keys, private keys are secret ,we are not revealing any secret on private key, id s are only you are using but the problem is how we are going to distribute public key in pgp ,remember last time when we spoke about pgp we spoke about x509 certificates and we said that x509 will be used to distribute the public key of the user ,what was the reason we selected x509 remember you have a public key and you posted in some kind of user and I want to send you a encrypted information and I want to go to your public directory and I go to your public directory and I do find your public key from that public key directory , so what is the problem if I find you public key from there?. I don't know whatever actually that public key belongs o you or someone else we have to bring the public key in such a way that it is going to be unforgable in other words we are going to bind that crypto graphical so that we use x509 certificate ,so that it binds the owner in means of DS, so we use digital signature so that no one can forget it basically so it was a good way to bind the public key if you post that x509 certificate and I know that , that public key belongs to you ,because else ca sign that certificate like that, you may even b your own ca or you may create you own certificate you may not want to go to third party but unfortunately in pgp we re not going to use this beat able technology , pgp will come with its own idea, in pgp every user is a CA, what is wrong being CA in x509 concept?..why we need a third party in x509 certificate?..if the signature is valid I can verify the signature ,because verification needs only your public key information , I can impersonate your identity and post it in your directory so then everyone believing that certificates are real good name to byte the key they will accept that that public key is legitimate for that user to accept to avoid that kind fo stuff you have trusted third party like verisign kind of stuff , you have to prove your identity so that they can prove your certificate so that everyone using the verisign certificate can think that verisign is doing a truthful job so that they identify the user based on that id, they created the certificate so it is dangerous having you own CA they impersonate other set ,in ppg it doesn't like any third party as you are putting trust on the third party, imagine that big brother has relation ship with that company and they can generate some key s for some people which you are not aware of that then they can create a message or they can recover the session key ,hat is used for the encryption session key is the encryption version of the public key so in other words there could be some attacks possible if there is some relation ship between big brother and company, but here pgp doest not like those kind of stuffs..pgp says that you can create your own and you can sign your own keys and you can sign keys for your users if you know the user directly you are going to sign that key directly remember the trust keys that I was talking ,if you sign the keys of any user that you know that key will be legitimate key for you ,if

someone trust you still that key is legitimate for those guys , you see I don't need any third party like verisign kind of company ,so that's why I have web of trust , here trust key are sign in other words trusted key are signed by the people that you may trust or not the point over here is the keys are signed by there people and we assign trust values for the people ,if I don't know then im not going to give any trust value at all but im going to find some other guy I can trust and they know the unknown guy that I know and they sign the key for the unknown guy, I can accept the key of the unknown guy as a trusted key , for me ,we need somekind of relationship among the user ,so this is going to work well ,to know new people to trust them and to accept keys and so on and so for this what they are doing is pgp has central key server when you generate your keys you are going to there server and generating your keys so if I need your pgp public key then I can go to that server and I can write your name get the key ica n access those registered key, register your keys tot the server there are some central servers where you can access, in US you have to go to this server , in Europe to this server , so when you install the pgp when you do the lab you are going to register your key to the server so you don't need that kind of stuffs so web of trust is the main thing ,so we can trust the keys if we have the chain of signature more than one people might check the keys pgp will show it to you ,you are not going to decipher the keys all the time when you look the pgp key trays and you will get to know what is your key and based on the user it will assign the keys to you , and then key ring will improve the trust indicator , remember key legitimacy, owner trust , owner trust fields and I said that key legitimacy will be calculated using owner trust and signature trust anyways will talk about it later, and also users a can revoke their keys, remember in x509 revocation was done everyone an revoke the keys but ca is going to keep the list in CR L and that list is unforgable if one thing is there in that key then its there, they are using digital signature for the list we a can have those kind revoke keys here , so we can have that kind of revocation lets have look a t the details, first of all lets have a look at the use of trust fields in the public key ring.

The use of trust

We are going to have owner trust field and signature trust field ,these two are enough to calculate the key legitimacy field and pgp is going to do this along in other words is going to be user transparent all you have to do is there will be trust meter and you have to arrange the trust meter that is actually behind the implication in owner trust field we will be having some parameters ,undefined trust ,unknown user ,usually not trusted to other keys ,usually trusted to sign other keys and if there is this key is present in the trust field that means that its you public key if there is this bit up and that key up is appeared In the secret key ring as I said that means that is you public key info, those kind of parameter will be there but if you are the owner of the key here is unlegitimate trust, and look at the signature , undefined trust , undefined trust , usually not trusted to sign other key and usually are ,when you get the public key it is going to be signed by someone else other, if it is signed by then it ultimate trust by entering this parameters to those fields the –pgp us going to message, it is a trusted case and in that situation you rare going to sign that key if you sign that key you are changing the key legitimacy field you assigning ultimate legitimacy to these tow field so them so then key legitimacy will be ok and pgp will allow to use that key ,don't forget that and after that dont send me a email

saying ,I could do this. But pgp cannot do that because ppg dint receive the trust value tot hat key by the owner and also for the signature so you have to you are not for the meter and you are going to changing the volume of of something but moving the button up and down you are going to assign the trust value when you sign those things these hi. What we have to know is if we sign the key s ,if you are owner of the keys then you are key legitimacy will be ultimate trust ,s o this field will bin owner trust and signature trust field, as

PGP trust model example.

This symbol x and y means x is signed by lets say that this is public key and it is singed by y .so lets have a look this is you and you know some people abcdef and they are all pgp users you have 1% trust on the e and f so what ever the key you receive signed by the e and f is trustworthy for you , key of m ,key of n, most probably you don't know that guy , you need the public key information of m , if you receive the public key information of m signed by e that public key is valid for because you have 100% trust on e, if lets say L ,you know L and q you don't know that means q key can be used by you ,what about if I receive q by this way q keys signed by m you don't have any trust , you are going to be use that key , you may chain of signature you may have more that one signature on your keys, m signed q you don't have trust but q sends m that means that means you have a trust use the key of m if you have trust of m then you can use the key of q basically , but look at this guy , I know this guy but I dont trust this guy its in my public key ring but im not showing any trust to that guy but that guy is singing the key of I j and k ,you don't have any valid signature that m and you are not be able to use I j k you dont know p ,you are not going to use it because you dont have any signature reaction on signature , don't trust , you don't trust these guys so that you dont validate the put the trust on the p public key but look at the definition if there is a dot then key is legitimate by you , these guys you cant make it legitimate ,,but these guys if you go this way then you can make it legitimate and I do find that l also signed the key of p so I have full trust on l that means I can actually use this key as long as I have the signature of l, again this is going to depending on your relation ship, most probably you are going to ask this guy that you have the key of p if they have then they will give , you are not going to go to people you don't know and say that I need the key of p most probably this side it will not happen, you don't trust p but you can make it trustworthy by signing the key yourself ,if you sign the key yourself you can use the key ,if you don't , you will ask some people who knows p, not necessarily that p know the people I trust , what you know is you receive the p public key and you are looking for some kind of trust and you are telling your friend saying I got this key from p ,do you guys know p ,and D or l will reply saying I know it , and they sign it and you will receive it they are not going to say I know this guy and all they are going to sign the key and send in signed form but this is going to take time ,during the time the web of trust is going to go bigger , the problem is new user when there is new user he doesn't know anyone and he cant get the signed message , so if you sign that key then you make that key of the guy legitimate for you , if it is legitimate for you then it is legitimate for all the people who trust you so it is kind of living entity it is a dynamic thing and not static thing, you are not going to pull anyone , you are jus add some one if you know someone and add the key and if someone asks the keys of that guy form you are going to sign the key and send it to that guy and thats how that guy will accept the key that guy will have the trust in you this guy will go to register in the key server if you get the key form the server you will assign immediately, let

have a look you don’t trust e and you trust m ,lets say that is the case what will l happen the signature f key will not be accepted by me , that means m’s key will not be accepted by me but I havent the trust for m, if I have the trust for m then im not going to look at the signature anyways I have full trust and accept m’s key s it is and q signed by m will be ok form as I have 100% trust on m so if I get keys signed by entities I don’t have trust I jus will ignore and signed myself by making it trust worthy , we are talking about full trust, this dot says that they are waiting for legitimate for me, if this is valid then this key is legitimate or trust worthy for you .