SET

Other important protocol this is important for ecommerce industry and it is really important protocol fro me and it come with very good technology called dual signature, it is open encryption and security specification , it is used to protect internet credit and transactions look at who developed it master and visa cards ,but unfortunately we don't use it , when we buy some thing from internet we use SSL protocol and we use ssl protocol and it's a quite complex and lot of complex things are going on behind the scenes so today's e commerce application are when you go to NSI to buy something you are giving your credit card info and when you buy something with credit card you are in secure form and you are putting trust on the seller thinking that seller is not going to use that credit card for something else and then the other this is this, the seller knows the detail of yours , as is said he or she may use it later on or she may use for something else they are going to inform your bank saying that this guy bought this thing and you are going see it in your statement so bank will know what you are buying ,so is there any way from which I can hide what im buying from the bank and at the same time I want to hide info of my credit card form the seller if im able to do that then it will be perfect environment to buy something on internet if the seller misuse the trust that you are putting on him what is the protection mechanism you have ,for example you bought something on internet and you didn't receive the goods you are telling the seller that you dint buy and all but they charged you what are you going to do?..call the credit card company so that you can get the money back form the company only three times because credit company ,imagine this, you have received the goods but still you are calling saying that you didn't receive the goods i mean you can abuse the credit card company all the time , you cant do it all the time they keep you profile record over there and they will check how many times you did those kind of claims they will check whether you did true claim or false claim, generally they are not going to do that asking company and all , because the credit card that you got is insured, the credit company is not paying the money they are not spending any thing but insurance company will, because when they give you credit he insurance company, but you cant call all the time ,we need a better security environment ,we want to hid e credit card info from the seller and we want to hide payment info from the bank, SET does that , In today's world ,when you buy something you are going to put your details, address and everything and when you put credit card info to the order that credit card info is the payment, OI is the order info and PI is the payment info im going to make this OI and PI in such a way that it is unforgable in other words when the seller gets the OI and PI he cannot get the same for other orders im trying to avoid the some criminal activities this way I will be able to buy ,im planning to bind PI to OI and then im going to encrypt the PI so the server cannot see it but it sees that this order is connected to this PI so this going to scrap the PI and send the PI part to the bank , bank can see your PI but cannot seethe OI so to that they came up with the idea with dual signature , Im not going to go into details, so we are going to just focus on dual signature they are going to proived confidentiality of info, integrity of data ,cardholder account authentication merchant authentication ,

SET components

Here is the is sure and he issues the card, here is the acquirer do you guys know who is acquirer , there is a card holder that is you one internet you are buying some good s, payment gateway is connected to the acquirer and merchant is going to go to acquirer and acquirer will go to bank and check your credit

whether those things are available or not over here you are going to approved or not, you are in the store and you are in the payment section you swap your card and you are waiting and that communication is coking form merchant acquirer and they are checking whether you have enough money in your account and they are going to bank account and check your account and if there is money and they are come back to merchant saying that it is approved then you will say the recipient will be printed this acquirer are third party come in they are the most richest companies in the world and you don't even know there names that kind of company for every transaction they charge a fee, for example when you use your credit card then that card has 2 or 3 % more price on it that 2 or 3 5 goes t this acquirer when you buy gas which ever on the gallon 2 or something dollars but when you go and buy the marco with the check card the price will be 2 or 3 cents more than what you saw but they are going to charge transaction fee, when you are using your debit card for some they processing you money and they are spending your money or when you are buying some concert ticket form ticket master the price o f the ticket is 50$ and interest 60$ that 60 will become along with tax will become 80 or 90 these guys are big guys and they are handling millions of transaction per second in US I worked in one of the company they use aes signature as rsa signatures are quite slow for those stuffs ,they whatnot handle more transaction so they are looking alternative for rsa so ecc was candidate os we used ecc than rsa, so they finally dint get convince any ways so they are looking for alternative for handling it, if in other counter is you will see lot of card readers it is not just one in US its just one ,because in those counter is there is not acquirers in the bank only they will handle it that's why you are going to see 3 or 4 devices and then you are going to use one device corresponding to your bank bu t in US you are not going to see that you see only one post machine because all other transactions are done by this acquirer so that important so the is the is the SET company and it ahs CA and it wil have certificate so lets have a look how we are going to hide info from bank and merchants ,im not going to go over the details you a know the is you open a account and bank will come to know your money that you send on your purchase that is by using visa or master card they have the agreement and the merchant will open the account and the payment info it is going to be checked by the acquirer and its approved it will ship the good to you and its going to send the PI and its going to send it from your bank account to the merchant account this is the way

Dual signature,

Customer created dual signature OI to merchant and PI to bank this credit card info this the thing that you buy from the internet neither party want s to know the details as a use r you don't want the bank to know OI in found you don't want merchant to know PI info and you are going to use Dual signatures and they must be linked in other words called unforgebale links and we are going to use this , we aer going to have concatenated info OI and PI info signed by you something like this , you prepare Pi and Oi and take the hash of payment info and OI , pimd and oimd and concatenate and append he catch other and the result it pomd and they arew signed and is called dual signature and this K_{rc} is the customer signed private key so how am i going to use these things ,im going to pass this guys and there is PI and Oi and this is the dual signature of packet and its going to be transmitted to merchant from you so as I said merchant will not see the pi info from you so there is your pi and what you are doing is you are calculating hash of OI and hash of PI and concentrate and hash and you will get pOMD and encrypt rhten

with private key and you will get dual signature and append them with oimd and everything is going to be encrypted with the session key and it will be encrypted with the public key of the merchant, not the merchant but the bank because merchant will not see the content but bank will see ,this is digital envelop that means session key is encrypted with the public key info of the bank and PIMdD and Oi and dual signature and cardholder info this whole this is sent to destination it means merchant when merchant receives this one it will do , forward that encrypted part to bank but they must know that there is some PI related to OI how is going to dot hat there is dual signature and a cardholder info is also transferred so card holder info is known by merchant so its going to append that dual signature and what is contains.?.hash of OI , appended of hash of PI this is hashed and then signed, when I try ot verify this im going to use the public key of card holder and I have pimd , this one and this is oimd from OI the merchant can calculate the OIMD, PIMD already transmitted and ti is going to do the same calculation and the hash and the result is same to this DS, that the verification of signature , so the merchant knows that the corresponding payment info is in this part and think that this merchant is a bad guy , hew wasn't tot use this PI to another OI and lets say you bought 1 cd and he will say you bought 100 cd so what will happen.. he is playing with the content of oimd , he is trying to change the dual signature but it is transmitted to bank as well so bank will not pay anything for any changed to OI info , that's im not paying anything to cardholder so then no one can change the OI and no one can user this part of info for any other order , what about bank side, bank will receive this part, by using the private key of the bank it will recover the key and by recovering it receiver dual signature and oimd it doesn't have oi info but hve OIMD to verify its going to do hash of PI and concatenate this one and take the has changed result is inside the signature and if that is the case that means this is the order seen by bank , but bank doesn't see this one it will see the digest of the order info and the merchant doesn't see the payment it will see the payment MD info so this way im hiding pi form merchant and oi from the bank ,so bank don't know what you bought for that money , so is nt it neat , its really nice technology but not using in today's technology but big banks are using it now so what I said it is this is the verification merchant hs the OI and from that OI its going to calculate the hash of the order oimd and there's pimd append them and use again hash and the result si POMD and get the cardholder of the signature and decipher the signature and the result is pomd and this pomd and other should be same if its same then pI is related t to that oi ,no one can change the info, this is dual signature then this will go to bank and do lot of things , im not going to go into details ,as I said is the most important for us is dual signature this way im hiding PI from merchant and OI from the bank .