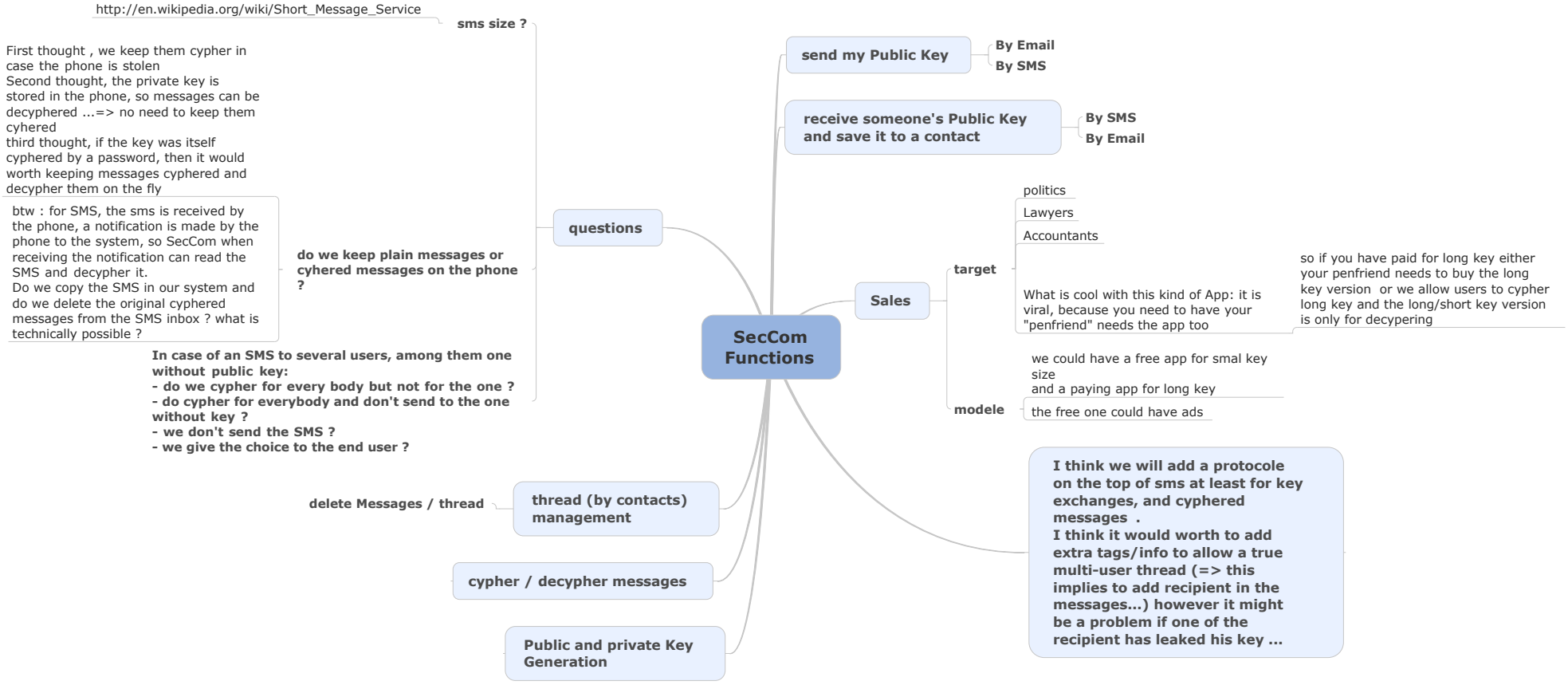
SecCom Functions
questions
sms size ?
http://en.wikipedia.org/wiki/Short_Message_Service
do we keep plain messages or cyhered messages on the phone ?
First thought , we keep them cypher in case the phone is stolen
Second thought, the private key is stored in the phone, so messages can be decyphered ...=> no need to keep them cyhered
third thought, if the key was itself cyphered by a password, then it would worth keeping messages cyphered and decypher them on the fly
btw : for SMS, the sms is received by the phone, a notification is made by the phone to the system, so SecCom when receiving the notification can read the SMS and decypher it.
Do we copy the SMS in our system and do we delete the original cyphered messages from the SMS inbox ? what is technically possible ?
In case of an SMS to several users, among them one without public key:
- do we cypher for every body but not for the one ?
- do cypher for everybody and don't send to the one without key ?
- we don't send the SMS ?
- we give the choice to the end user ?
send my Public Key
By Email
By SMS
receive someone's Public Key and save it to a contact
By SMS
By Email
Sales
target
politics
Lawyers
Accountants
What is cool with this kind of App: it is viral, because you need to have your "penfriend" needs the app too
so if you have paid for long key either your penfriend needs to buy the long key version or we allow users to cypher long key and the long/short key version is only for decypering
modele
we could have a free app for smal key size
and a paying app for long key
the free one could have ads
I think we will add a protocole on the top of sms at least for key exchanges, and cyphered messages .
I think it would worth to add extra tags/info to allow a true multi-user thread (=> this implies to add recipient in the messages...) however it might be a problem if one of the recipient has leaked his key ...
thread (by contacts) management
delete Messages / thread
cypher / decypher messages
Public and private Key Generation