1. GTR

GTR is Email encryption tool provides full deniability offline conversation with perfect forward secrecy. GTR is based on OTR protocol adapted for high - latency email environment.

Traditionally the autentification of participants in Email model is based on PGP PKI (identity of the participant to certify its public key). GTR uses PGP encryption as a transport for authentication only in two first messages: request for conversation and permit of it. This IKE is based on Abadi protocol and provides deniable private autentification of both parties. Following autentification procedure all regular GTR messages are encrypts and authenticates by GTR and can be sends directly using base64 encoding. Each regular GTR message includes encrypted user's text and some material for new Diffie-Hellman key agreement.

If suspects a leak one or both sides long-lived public keys parties can determine MitM attack using additional partially reliable communication channel (eg eavesdropping phone providing voice authentication). Proposed verification protocol also involves mutual untrusting of parties and prevented the possibility of compromise a participant. Also even if the acceptor and the initiator do not have a trusted public keys, they can start a conversation without authentication and then verify the identity of each other as described above. GTR also allows to create deniable signatures proving the identity of signed content to the other party but not third parties.

Example:

Alica creates such text:

"Hi! Sorry, but I suspects that our private keys could be compromised and want to check it. I know your voice, and I shall calls you by the phone, but I'll change my voice. I will utter the phrase: "I am salesman and want to offer you a vacuum cleaner." Please aforehand compute deniable signature of this phrase. You will get 6 letters. Compose any suitable response so that its words beginning with those letters. Remember the phrase and responce and be ready to issue the responce if you will hear the phrase on the phone. Since you will pick the response yourself, it does not compromise you. Please provide your phone number to call. Also you can pick and send me yours phrase for perform a similar check. My phone number is 1234567."

Bob receives message and decrypts it. After this Bob extracts Alica's autentification request phrase from message and computes deniable signature. The result is 6 letters: "s,f,d,r,n,s". Bob composes responce: "Sorry, fucking dillers rejected now, shit" and remembers both request and responce phrases.

Bob answers Alica:

"Hi! It's a good idea, my phone is 9876554 and I ready now. After your call I also will call to you. My secret phrase will be: "I am a member of Greenpeace and gather help endangered animals". Be ready to answer."

Alica receives message, decrypts it. After this Alica extracts Bob's autentification request from message and computes deniable signature using GTR in –m mode. The result is 6 letters: "i,g,l,r,c,b". Alica composes responce: "Idea generally looks really cool but..." and remembers both request and responce phrases.

Now Alice knows that Bob is ready to answer her call. She computes signature of own autentification phrase, remembers six letters and makes an anonymous call to Bob (eg, from a payphone), with changed own voice. Eva could change request sent by Alice. But in this case Bob can not hear the expected question and will not give an answer. In the case of MitM attack shared secret will be different and the first letters of the words of Bob's response will not match expected Alica. If Bob's answer matched given letters then Alice assured in the security of the communication session.

After Alica's call Bob also makes an anonymous call to Alica. Alice delivers a response only if her verification was successful. While receiving a response and making sure of its authenticity, Bob also believes that communication is secure.