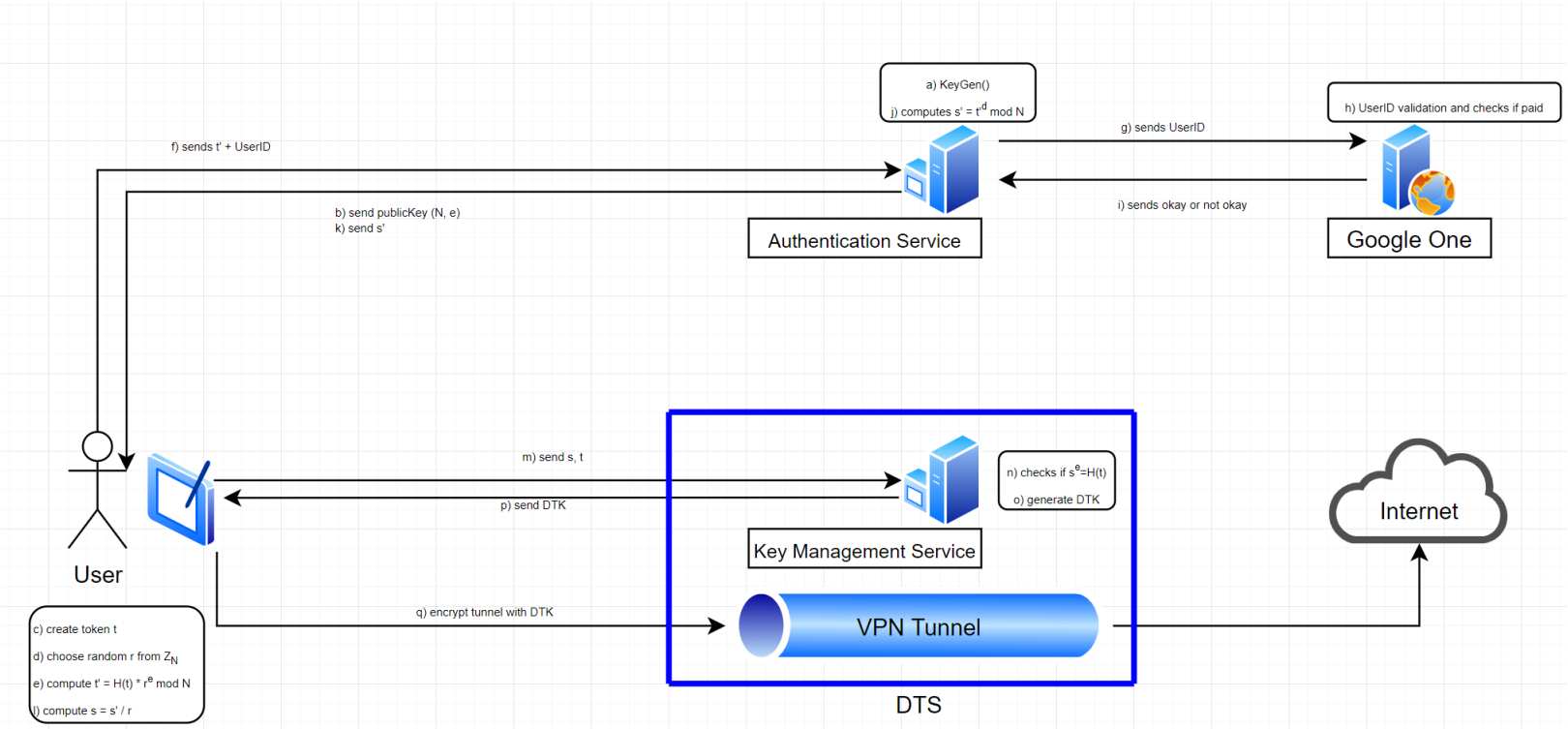
16-124-836
Marcel ZAUDER

3.1 Privacy in the Google-One-VPN



The client gets the public key from the authentication service, with which he can encrypt his token, by using any random number that he has chosen and a full-domain-hash-function. This so blinded token is then sent to the Authentication Service together with the user's ID, which is needed for checking the validity of the acoount and whether the user has paid for the VPN or not. If everything is correct the AS sends a blinded signature back to the user, which can then be unblinded by him/her. With the unblinded signature and the created token the user can then ask the Key Management Service to create DTKs for him. This will happen after the KMS has checked the signature token pair for validity. After that the user can use the DTK to access the VPN.

Scope and lifetime of RSA public/private key:
The RSA key pairs can have a long lifetime because they are only used to encrypt a token from any user so it can be sent to the authentication service (AS). Therefore the public key has a global scope so anyone would be able to send his/her token to the AS. Only in the AS the UserData are checked for validity and the signature is created using the private key, therefore only itself knows about the private key and given there is no data leak it could be used indefinately (given DLP is hard), but in practice those would be recreated in a set time interval.

Scope and lifetime of DTK:
DTK keys are like session keys, which are valid as long as the user is connected to the VPN, after logging out or a long time of inactivity these keys become invalid to ensure that a user cannot connect to the VPN with old DTKs (especially if their subscription already expired). Additionally those DTK keys should not be accessible from other clients.