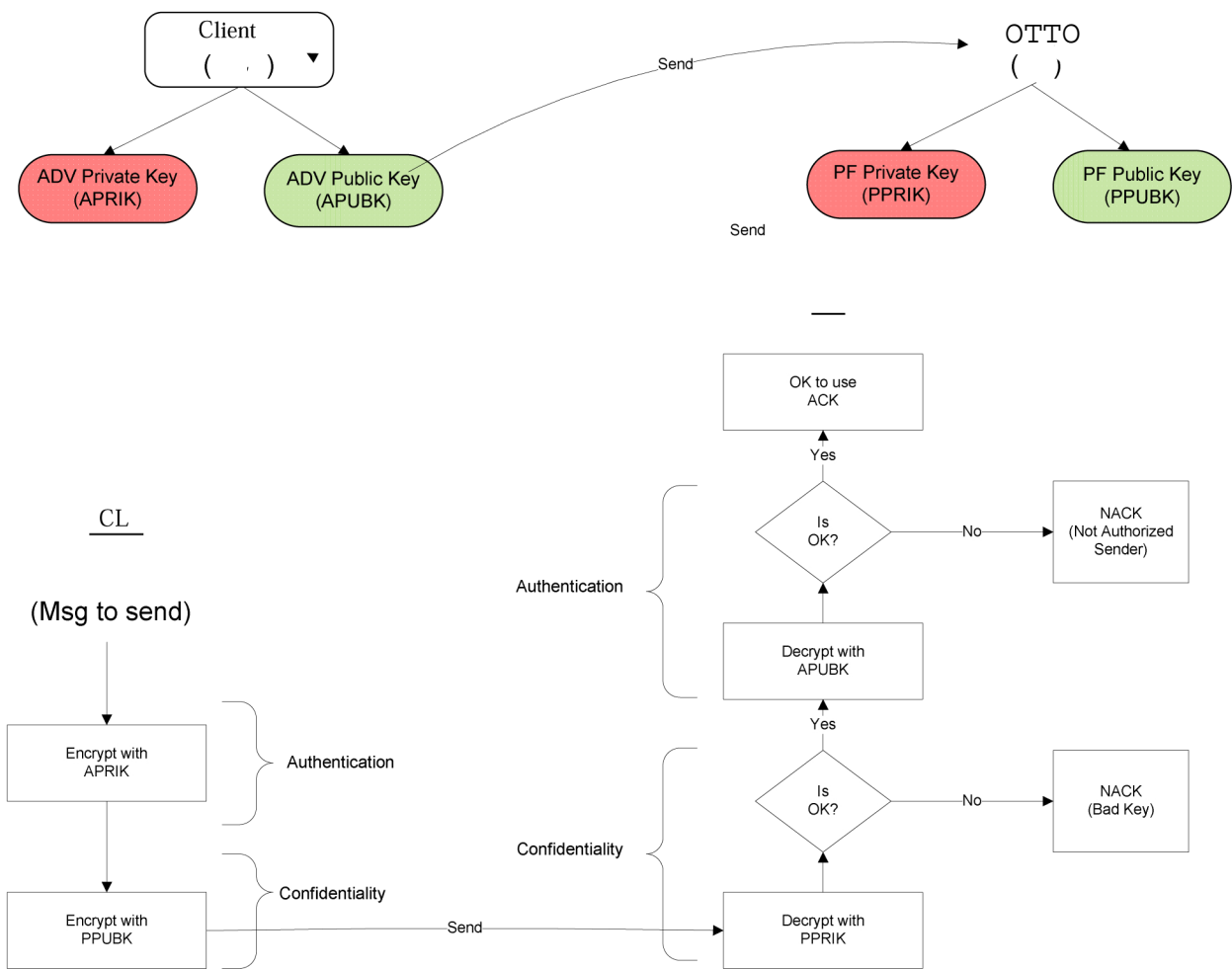# Security

Due to HIPAA regulations, all communication must be secure. To that end, all communication will be through a SSL encrypted interface. In addition, public/private key pairs will be used to issue session tokens that will be used in any transaction requiring information to be held confidential or guarantee the sender's identity. The use of public/private key encryption at various stages and content will ensure the following.

1. Confidentiality – By encrypting content (i.e. member information) with a receiving party's public key, it ensures it can only be decrypted with the receiving party's private key.
2. Authentication – By encrypting the content (i.e. a session token) with a sending party's private key, the receiving party can guarantee the sender's identity by using the sender's public key to decrypt the content.

Some or all of the message's parameters will require one or both of these levels of encryption. Below is a diagram that outlines the concept.
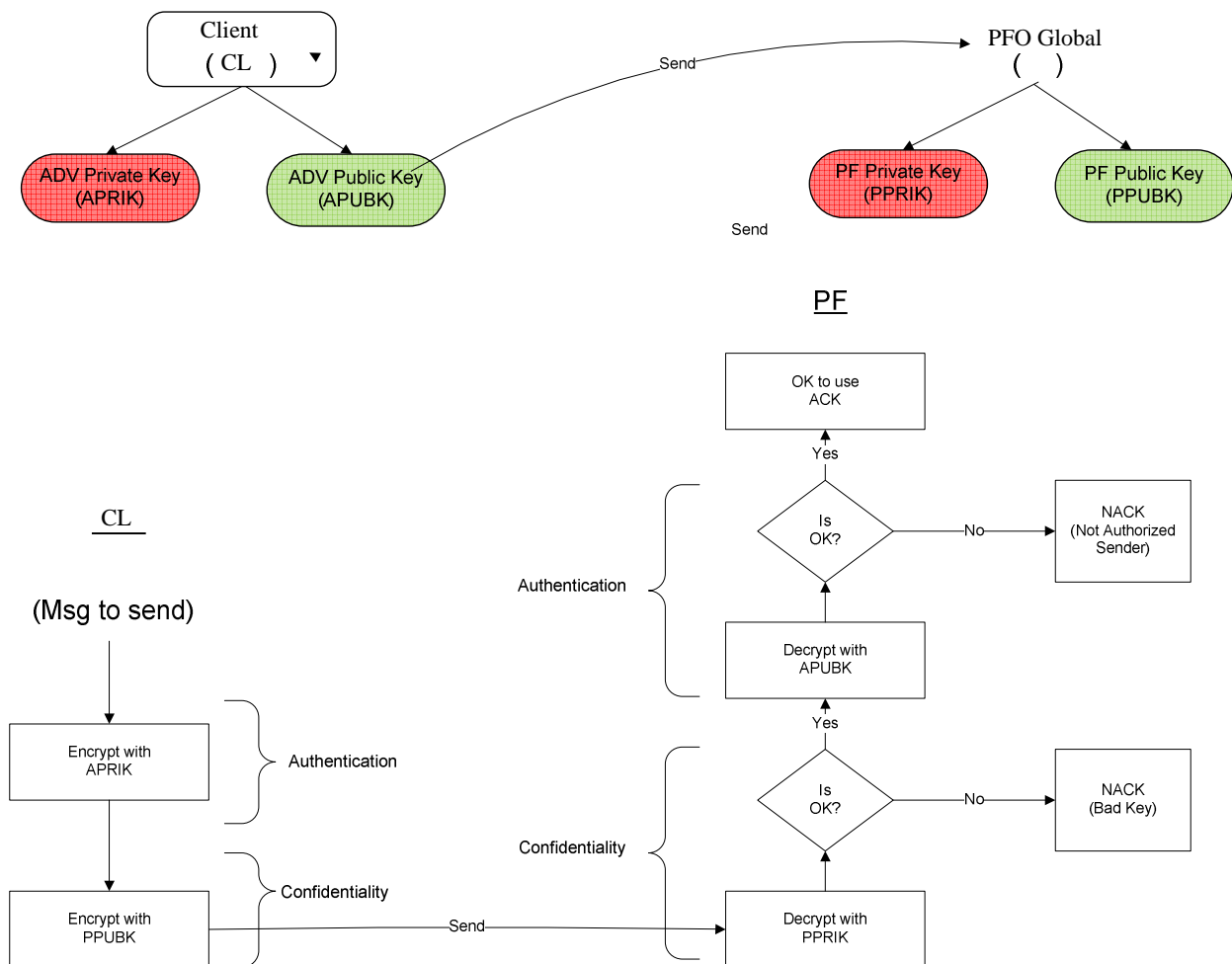
Security

Due to HIPAA regulations, all communication must be secure. To that end, all communication will be through a SSL encrypted interface. In addition, public/private key pairs will be used to issue session tokens that will be used in any transaction requiring information to be held confidential or guarantee the sender's identity. The use of public/private key encryption at various stages and content will ensure the following.

1. Confidentiality – By encrypting content (i.e. member information) with a receiving party's public key, it ensures it can only be decrypted with the receiving party's private key.
2. Authentication – By encrypting the content (i.e. a session token) with a sending party's private key, the receiving party can guarantee the sender's identity by using the sender's public key to decrypt the content.

Some or all of the message's parameters will require one or both of these levels of encryption. Below is a diagram that outlines the concept.

Client
(CL)   ▼

PFO Global
(   )

Send

ADV Private Key
(APRIK)

ADV Public Key
(APUBK)

PF Private Key
(PPRIK)

PF Public Key
(PPUBK)

Send

PF

OK to use
ACK

Yes

CL

Is
OK?   ——No——   NACK
(Not Authorized
Sender)

Authentication

(Msg to send)

Decrypt with
APUBK

Yes

Encrypt with
APRIK   Authentication

Is
OK?   ——No——   NACK
(Bad Key)

Confidentiality

Confidentiality

Encrypt with
PPUBK   ——Send——   Decrypt with
PPRIK

Sessions

All web based interactions will maintain state. To accomplish this, a session token will be issued prior to any initiation of the ordering process. There are two ways to issue a session token. One is by requesting a token via the RequestToken() API call. Another is in the initiation of an order via the InitiateOrder() API call.

Return Block

All APIs will implement a serialized return block that facilitates returning status and one or more classes of information.