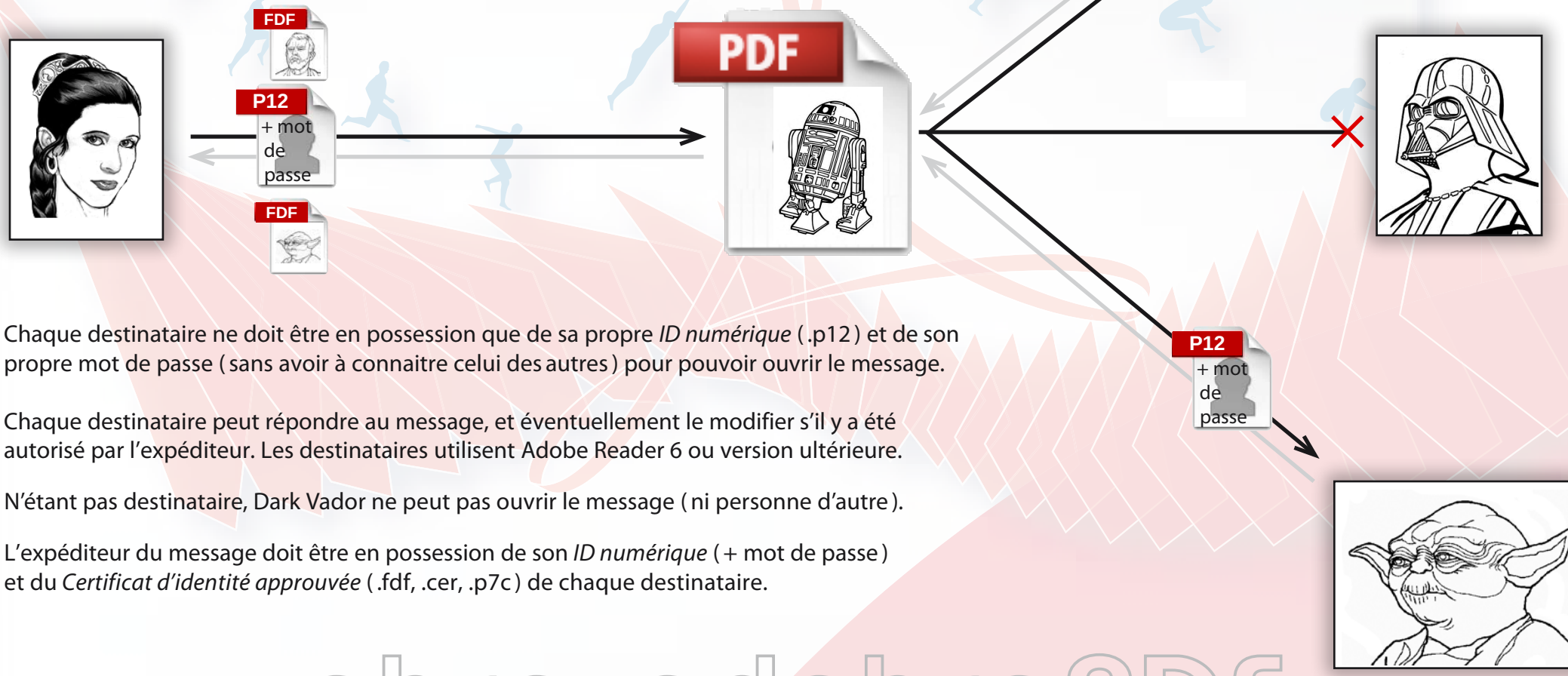
Principe de la Protection par Certificat
(ID numérique)

L'ID numérique utilise un cryptage de 1024 ou de 2048 bits (au choix) pour la clef privée, et de 512 bits pour la clef publique.

La princesse Leïa Organa doit faire parvenir des informations confidentielles à Obiwan Kenobi et à maître Yoda.

Elle crypte le message (fichier PDF) en utilisant son *ID numérique* (.p12) + son propre mot de passe, et utilise les *Certificats d'identités approuvées* (.fdf, .cer, .p7c) pour définir les destinataires ainsi que leurs droits respectifs.



Chaque destinataire ne doit être en possession que de sa propre *ID numérique* (.p12) et de son propre mot de passe (sans avoir à connaitre celui des autres) pour pouvoir ouvrir le message.

Chaque destinataire peut répondre au message, et éventuellement le modifier s'il y a été autorisé par l'expéditeur. Les destinataires utilisent Adobe Reader 6 ou version ultérieure.

N'étant pas destinataire, Dark Vador ne peut pas ouvrir le message (ni personne d'autre).

L'expéditeur du message doit être en possession de son *ID numérique* (+ mot de passe) et du *Certificat d'identité approuvée* (.fdf, .cer, .p7c) de chaque destinataire.