**Partie 1:**

**1. Décrire le rôle de chaque entité « Reader et Tag »**

**Partie 2:**

**1. Décrire le rôle de chaque entité « Reader et Tag »**

**Notation :**

* S et T : L'entité S représente le Tag, et T pourrait faire référence à une autre partie du protocole ou à un paramètre spécifique au Tag.
* Ps et Pt : Ce sont les clés publiques utilisées dans le processus d'authentification. PsP\_sPs​ est probablement une clé publique associée au Tag, tandis que PtP\_tPt​ pourrait être la clé publique associée à un lecteur ou une autre entité.
* SND et RCV : Ce sont les canaux de communication :
* SND représente le canal de transmission (lorsque le Tag envoie des messages).
* RCV représente le canal de réception (lorsque le Tag reçoit des messages du Lecteur).

**Rôle du «Reader» (Lecteur) :**

Le **Lecteur** est l'entité qui initie la communication et demande une authentification à l'étiquette (Tag). Son rôle est principalement de :

* **Générer des valeurs aléatoires** : Le Lecteur génère un nombre aléatoire r1r\_1r1​ qu’il utilise dans ses calculs pour interagir avec l'étiquette.
* **Envoyer un message au Tag** : Le Lecteur envoie une valeur calculée, comme R1R\_1R1​, à l'étiquette pour démarrer le processus d'authentification.
* **Vérifier les réponses** : Après avoir reçu la réponse du Tag, le Lecteur vérifie si les informations reçues (comme M1M\_1M1​) sont correctes avant de procéder à l'étape suivante.
* **Calculer et envoyer un second message** : Si la vérification est réussie, le Lecteur calcule et envoie un message supplémentaire M2M\_2M2​, destiné à prouver qu'il est bien le Lecteur légitime.

**Rôle du Tag (Étiquette) :**

Le **Tag** joue un rôle crucial dans l'authentification et la sécurisation de la communication. Voici ses actions et responsabilités :

* **Génération de valeurs aléatoires** : Le Tag génère un nombre aléatoire r2r\_2r2​ qu'il utilise pour ses calculs.
* **Réception du message du Lecteur** : Le Tag reçoit R1R\_1R1​, envoyé par le Lecteur, via le canal de communication RCVRCVRCV (réception).
* **Calcul et vérification de l'authenticité** : Le Tag calcule un message M1M\_1M1​ basé sur R1R\_1R1​, r2r\_2r2​, et d’autres paramètres comme la clé publique PsP\_sPs​. Ce message M1M\_1M1​ sert à authentifier le Lecteur.
* **Réponse au Lecteur** : Le Tag renvoie {R2,M1}\{ R\_2, M\_1 \}{R2​,M1​} au Lecteur pour permettre la vérification de l'authenticité.
* **Vérification de l'authenticité du Lecteur** : Le Tag, après avoir reçu M2M\_2M2​, le compare avec le message calculé M1′M\_1'M1′​ pour authentifier le Lecteur. Si l'authentification est réussie, la communication peut continuer. Sinon, le Tag arrête le processus.