
# Championnat de protocoles

---

## Description du protocole (1re correction)

NoSafetyAssociation (NSA)

Encadrante :
Véronique Cortier
veronique.cortier@loria.fr

Bastien Del-Valle
bastien.del-valle@telecomnancy.eu

Louis Jacotot
louis.jacotot@telecomnancy.eu

Bruno Gomes Dos Santos
bruno.gomes-dos-santos@telecomnancy.eu

2020 – 2021

Le protocole se décrit de la façon suivante :

1. A $\rightarrow$ B : A, $\{K\}_{pub(B)}$
2. B $\rightarrow$ A : $\{\{B, N\}_{pub(A)}\}_K$
3. A $\rightarrow$ B : $\{N\}_{pub(B)}$

**Connaissances initiales :** Au début du protocole, on suppose que :
- L'agent $A$ connaît la clef symétrique $Kas$ ;
- L'agent $B$ connaît la clef symétrique $Kbs$ ;
- L'agent $S$ connaît la clef symétrique $Kas$ ;
- L'agent $S$ connaît la clef symétrique $Kbs$ ;
- L'agent $A$ connaît la clef publique $pub(B)$ ;
- L'agent $B$ connaît la clef publique $pub(A)$.

**Valeurs générées au cours du protocole :**
- $N$ est un nonce généré par $S$ ;
- $K$ est un secret généré par $A$.

**Description du protocole :**

A la deuxième étape, B chiffre B et son nonce N avec la clé publique de A puis chiffre de nouveau avec la clé envoyée par A. A vérifie ensuite qu'il parle bien à B et reçoit le nonce généré par B.

A la Troisième étape B vérifie que c'est bien son nonce qui est renvoyé. Si c'est le cas, il a fini ses actions

**Propriétés de sécurité :** À la fin de l'échange :
- Si $B$ a fini pensant avoir reçu une clef $K$ venant de $A$, alors $A$ a bien envoyé $K$ à $B$ ;
- Si $A$ a fini en ayant envoyé une clé $K$ à $B$ alors $B$ a bien reçu $K$ de la part de $A$ ;
- La clé $K$ est secrète entre $A$, $B$ et $S$.

**Poids du protocole : 69**

1. $1 + 1 + 1 + 1 = 4$
2. $10 + (1 + (50 + 1 + 1)) = 63$
3. $1 + 1 = 2$