Revue du Projet 86 :

Démonstrateur pour un protocole de liaison et de révocation de certificats pseudonymes et dans les réseaux de transport intelligents.

Réalisé par : Houssam ROUGA, Youssef NABIL

Encadré par : Badis HAMMI et Nesrine KAANICHE

1-Vue d'ensemble :

Contexte Général

Dans le domaine des communications véhiculaires (V2V et V2I), la préservation de la vie privée et la sécurité sont des enjeux cruciaux. En effet, les véhicules échangent des informations sensibles qui, si elles étaient interceptées ou analysées de manière malveillante, pourraient compromettre l'anonymat et la sécurité des usagers de la route. Pour répondre à cette problématique, les normes européennes ETSI TS 102 867 et américaines SAE J2735 préconisent un changement régulier des pseudonymes (certificats de pseudonymat) utilisés par les véhicules, générés grâce à la collaboration de plusieurs entités. Ces normes recommandent respectivement un renouvellement des certificats pseudonymes toutes les 5 minutes ou toutes les 120 secondes (ou tous les 1 km), afin de limiter toute possibilité de traçabilité. Pour maintenir cette cadence de changement, chaque véhicule doit disposer d'un stock de certificats pseudonymes valides.

Cependant, la gestion de ces certificats soulève un défi particulier. Pour protéger la vie privée, il est impératif que les différents certificats d'un même véhicule ne puissent pas être liés entre eux. Ainsi, dans ce cadre, seul le certificat pseudonyme utilisé au moment de l'infraction est révoqué, sans pour autant invalider l'ensemble des certificats du véhicule. Or, cette solution permettrait à un véhicule malveillant de continuer à utiliser ses autres certificats valides.

Pour concilier ces exigences contradictoires, un protocole cryptographique permet d'associer de manière contrôlée et sécurisée les certificats d'un véhicule, garantissant ainsi qu'en cas de révocation, seule l'instance compromettante est affectée, tout en préservant la confidentialité globale du réseau.

Objectif du Projet

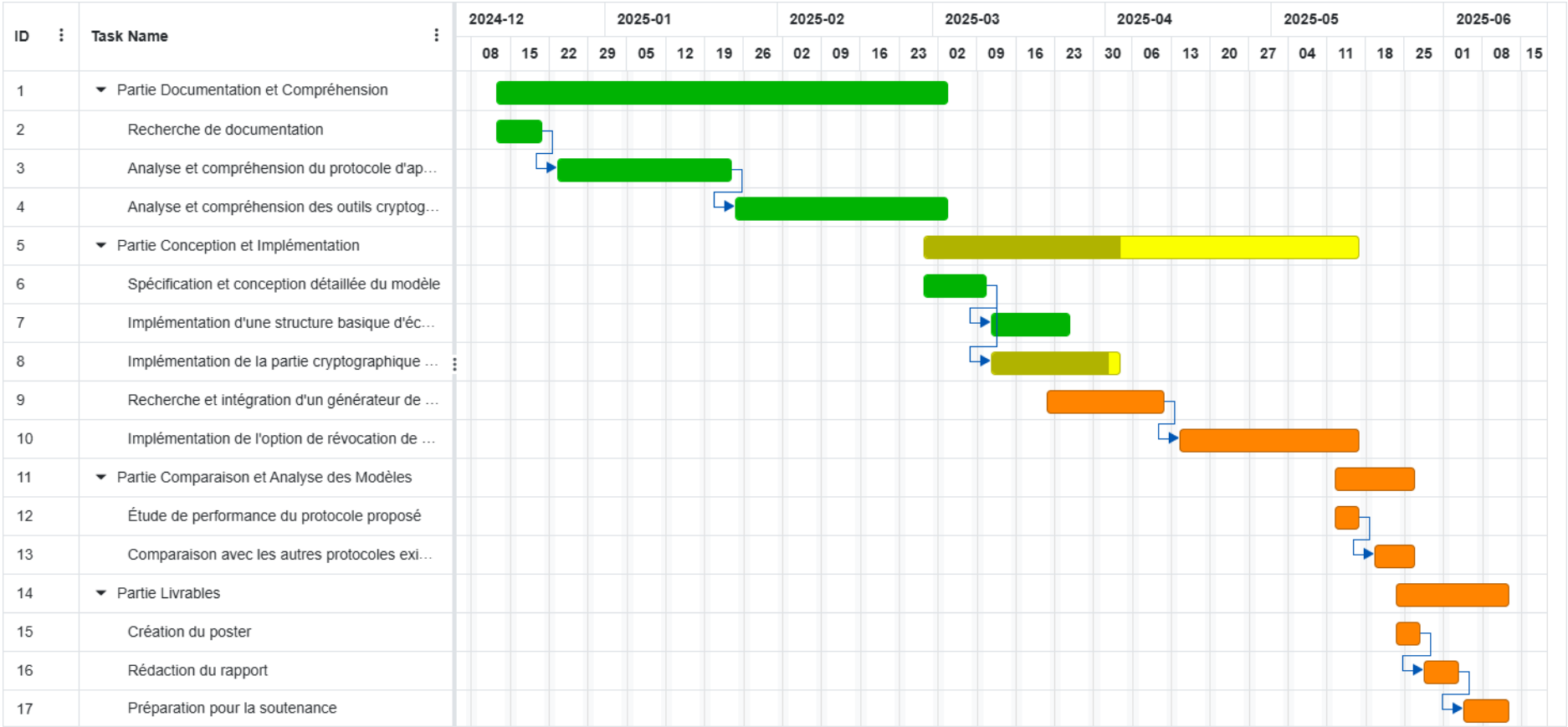
Dans ce contexte, le projet consiste à :

- **Implémenter le protocole cryptographique** : Réaliser une version pratique du protocole développé, permettant de tester et de valider son fonctionnement.
- **Choix technologique** : L'implémentation se fera en Python.
- **Étude et comparaison** : Une étude sera menée pour identifier les capacités et les limites du protocole, afin de pouvoir le comparer avec d'autres protocoles existants.

2-Planning du Projet :

Phase Documentation et Compréhension	**12/12/2024**	**27/02/2025**
Recherche de documentation ***(Terminée)***	12/12/2024	20/12/2024
Analyse et compréhension du protocole d'approvisionnement des certificats pseudonymes ***(Terminée)***	20/12/2024	22/01/2025
Analyse et compréhension des primitives cryptographiques : chiffrement basé sur les courbes elliptiques et fonction de hachage caméléon. ***(Terminée)***	22/01/2025	27/02/2025
Phase Conception et Implémentation	**27/02/2025**	**10/05/2025**
Spécification et conception détaillée du modèle. ***(Terminée)***	27/02/2025	10/03/2025
Implémentation d'une structure basique d'échange de messages entre les entités. ***(Terminée)***	10/03/2025	24/03/2025
Implémentation de la partie cryptographique (chiffrement du trafic et création des fichiers de records). ***(En cours)***	10/03/2025	31/03/2025
Recherche et intégration d'un générateur de certificats.	01/04/2025	17/04/2025
Implémentation de l'option de révocation de certificats et raffinement du programme.	17/04/2025	10/05/2025
Phase Comparaison et Analyse des Modèles	**10/05/2025**	**23/05/2025**
Étude de performance du protocole proposé.	10/05/2025	16/05/2025
Comparaison avec les autres protocoles existants.	16/05/2025	23/05/2025
Phase Livrables	**23/05/2025**	**10/06/2025**
Création du poster.	23/05/2025	27/05/2025
Rédaction du rapport.	27/05/2025	01/06/2025
Préparation pour la soutenance.	01/06/2025	10/06/2025

Gantt Chart



Complétée

En cours

A faire