

# **Serrure Biométrique**

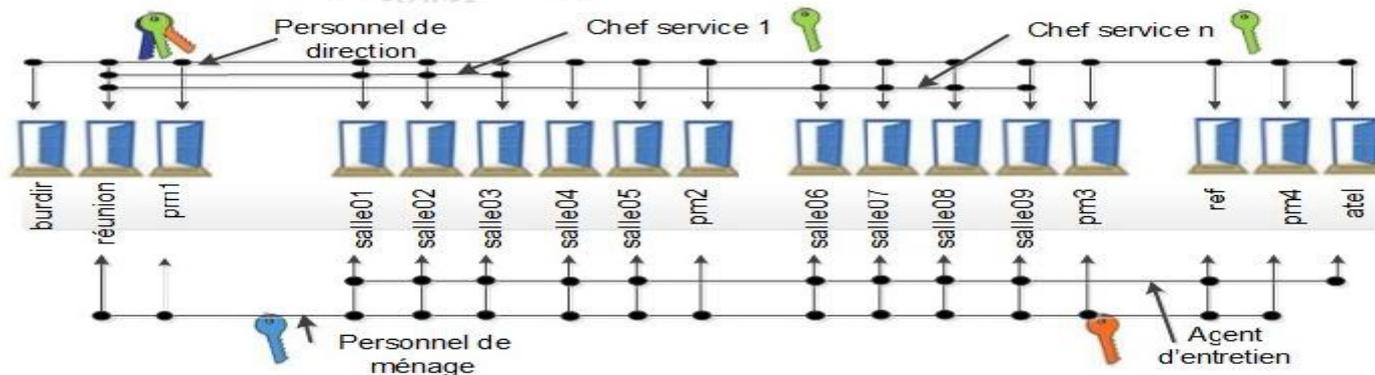
## **PCST 1 - Définition des besoins des parties prenantes**

# Besoin initial

Diagramme de Contenu 0\_Expression du besoin initial [ Besoin initial ]

## Besoin initial

Dans les grands parcs de clés traditionnelles qui permettent un certain contrôle des accès aux locaux, la gestion et le suivi de celles-ci induisent des coûts importants en temps et en frais de remplacement suite à des pertes ou des dommages. Ainsi dans l'organigramme partiel présenté ci-dessous, la perte d'une clé au niveau du personnel de ménage peut induire le remplacement de l'intégralité du parc. De plus l'emploi d'une clé classique n'assure pas de l'identité réelle de l'utilisateur.



Les contacts avec des clients ont permis au bureau d'étude de la société, de cerner les demandes qui portent sur une diminution des coûts de gestion des parcs de clés, sur une fiabilisation des autorisations d'accès et vers une évolution de la prise en compte de plages horaires avec possibilité de tracer l'historique des accès.

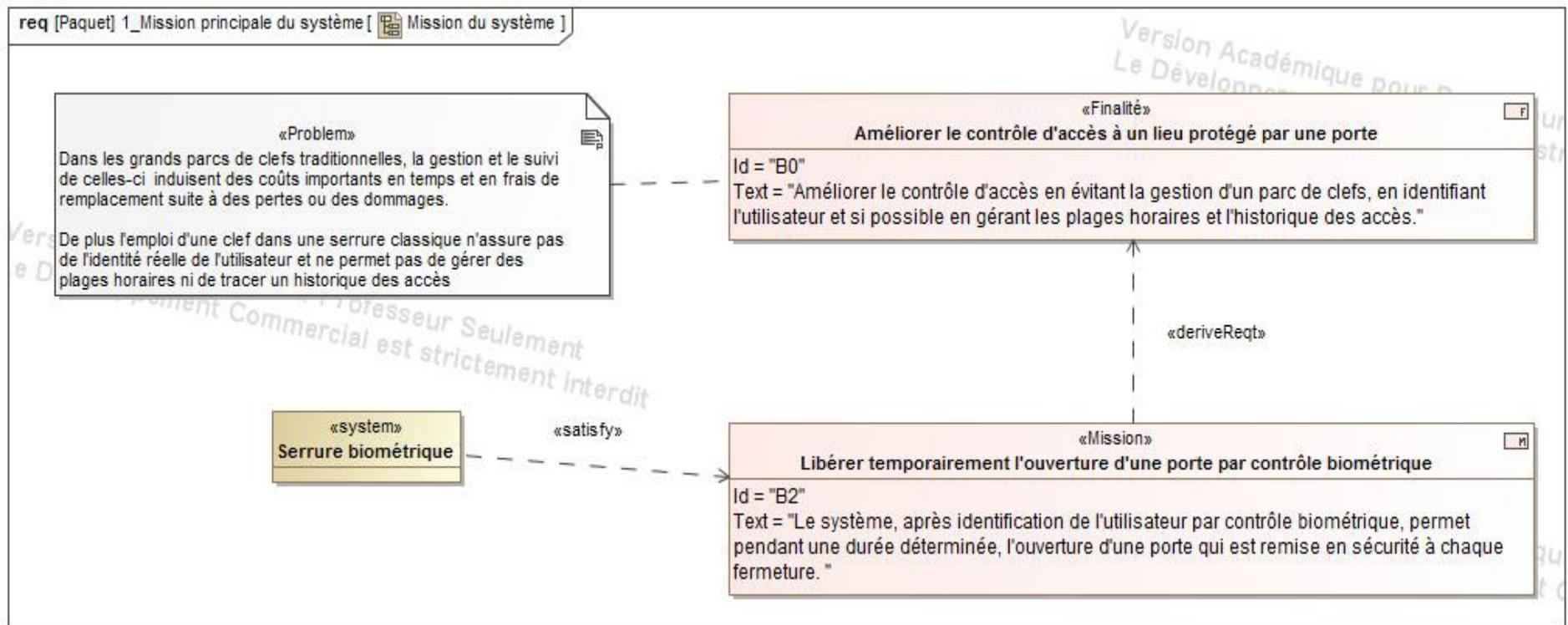
La veille technologique montre que l'orientation vers une identification biométrique digitale est envisageable. Les dernières informations recueillies indiquent :

- une miniaturisation de la taille des lecteurs,
- des taux de non reconnaissance et de fausse acceptation largement acceptables pour un emploi courant,
- la connexion possible du lecteur dans un réseau intégré de sécurité,
- un coût d'achat devenu intéressant.

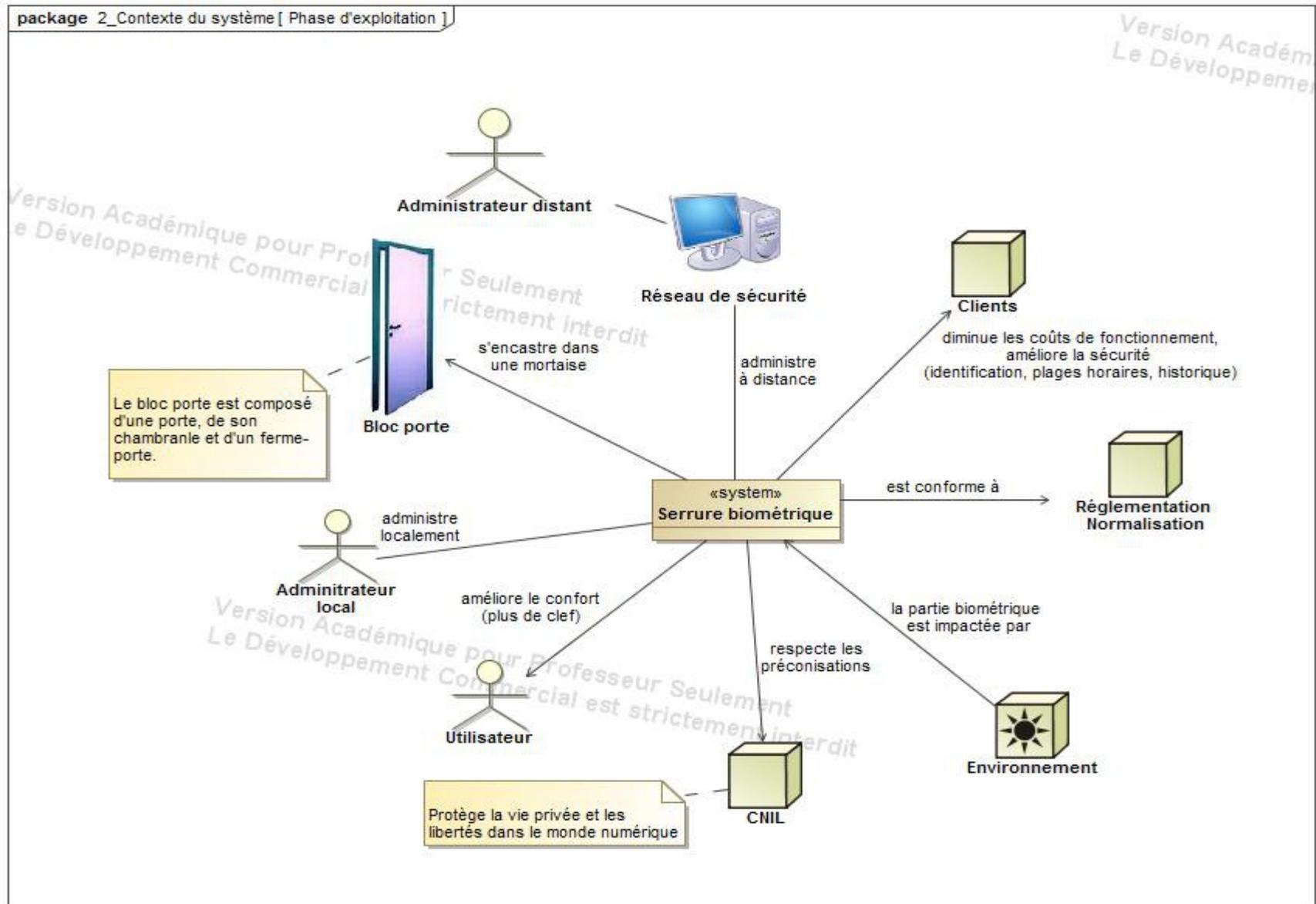
Si de plus, cette serrure pouvait, sans gros travaux de menuiserie, se monter sur les portes existantes équipées de serrure à encastrer de format standard, le marché de la rénovation pourrait offrir des débouchés non négligeables.

Devant l'intérêt marqué par les clients potentiels de ce futur produit, la société a décidé de concevoir le système.

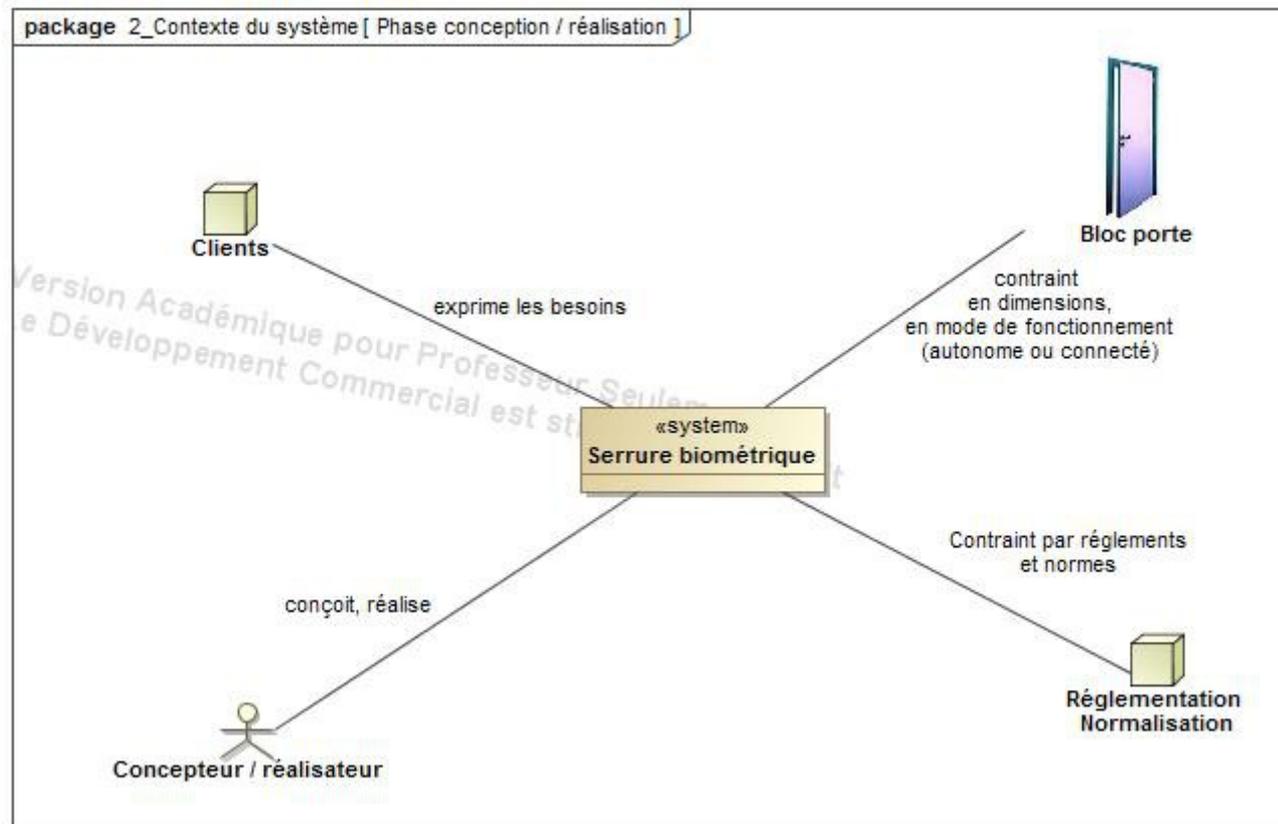
# Mission du système



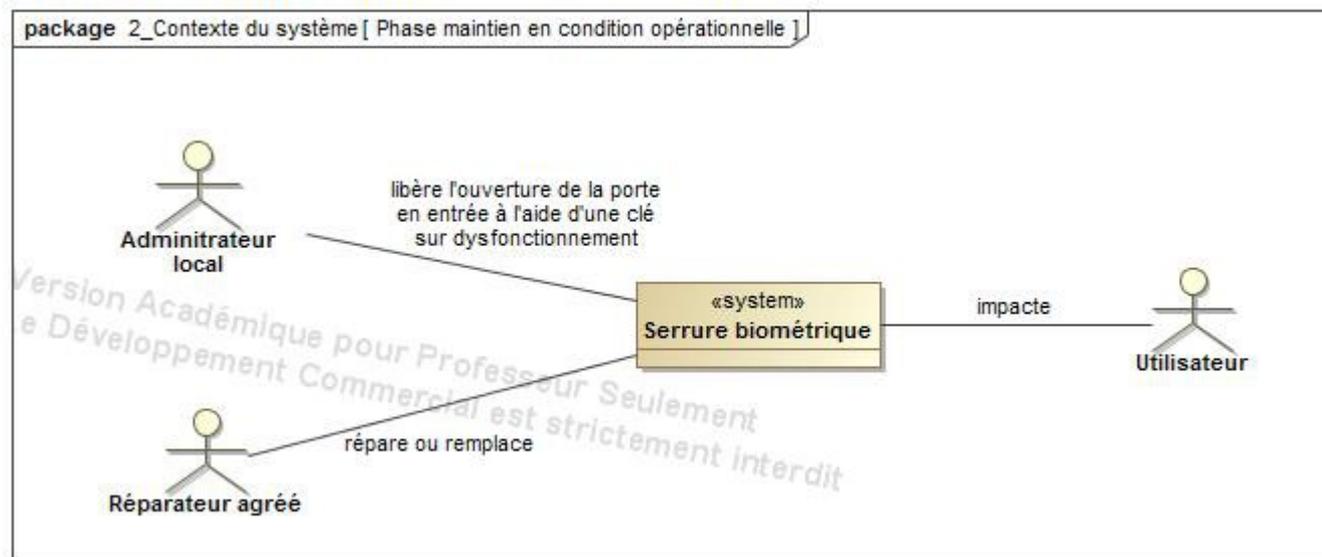
# Phase d'exploitation



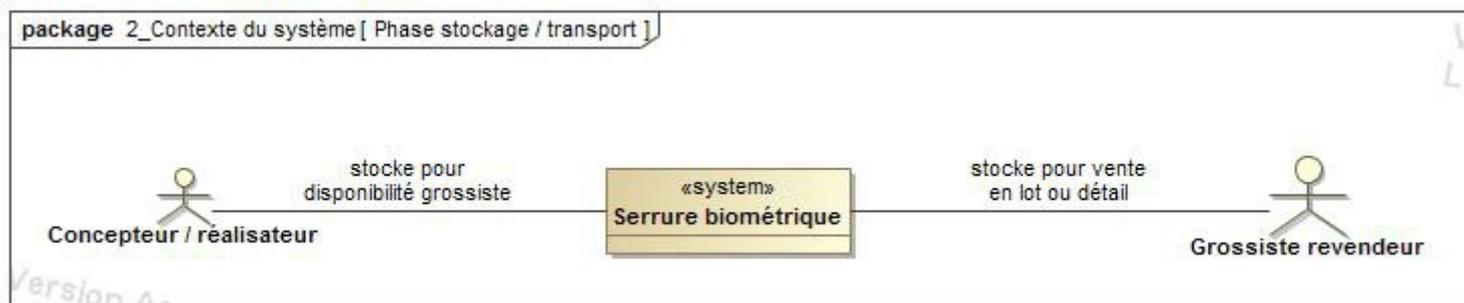
# Phase conception / réalisation



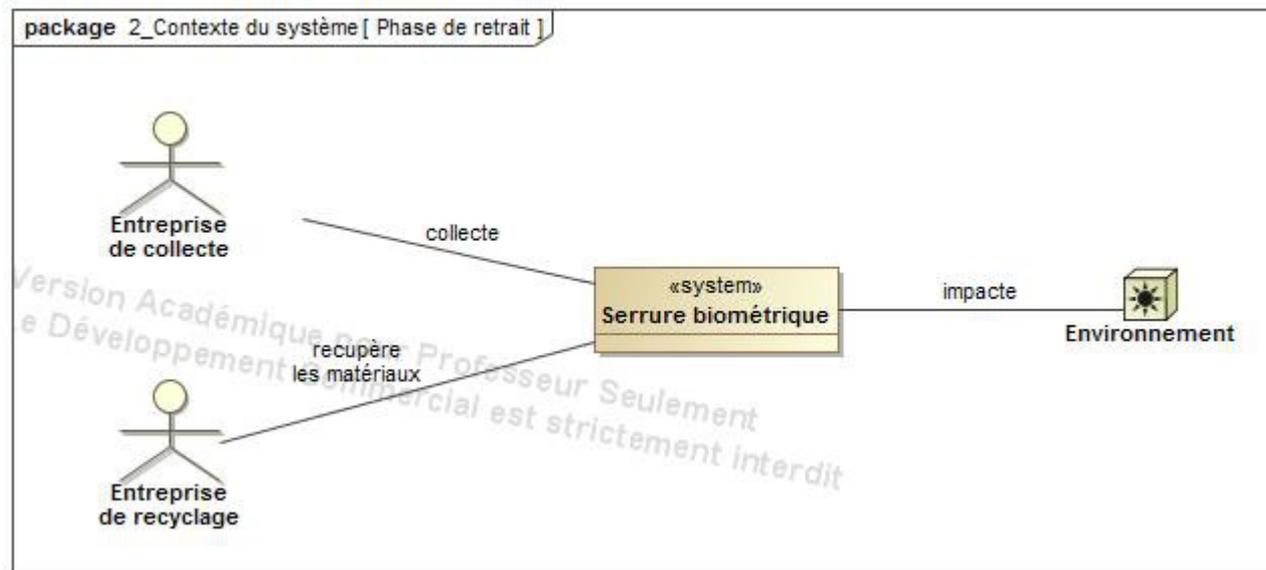
# Phase maintien en condition opérationnelle



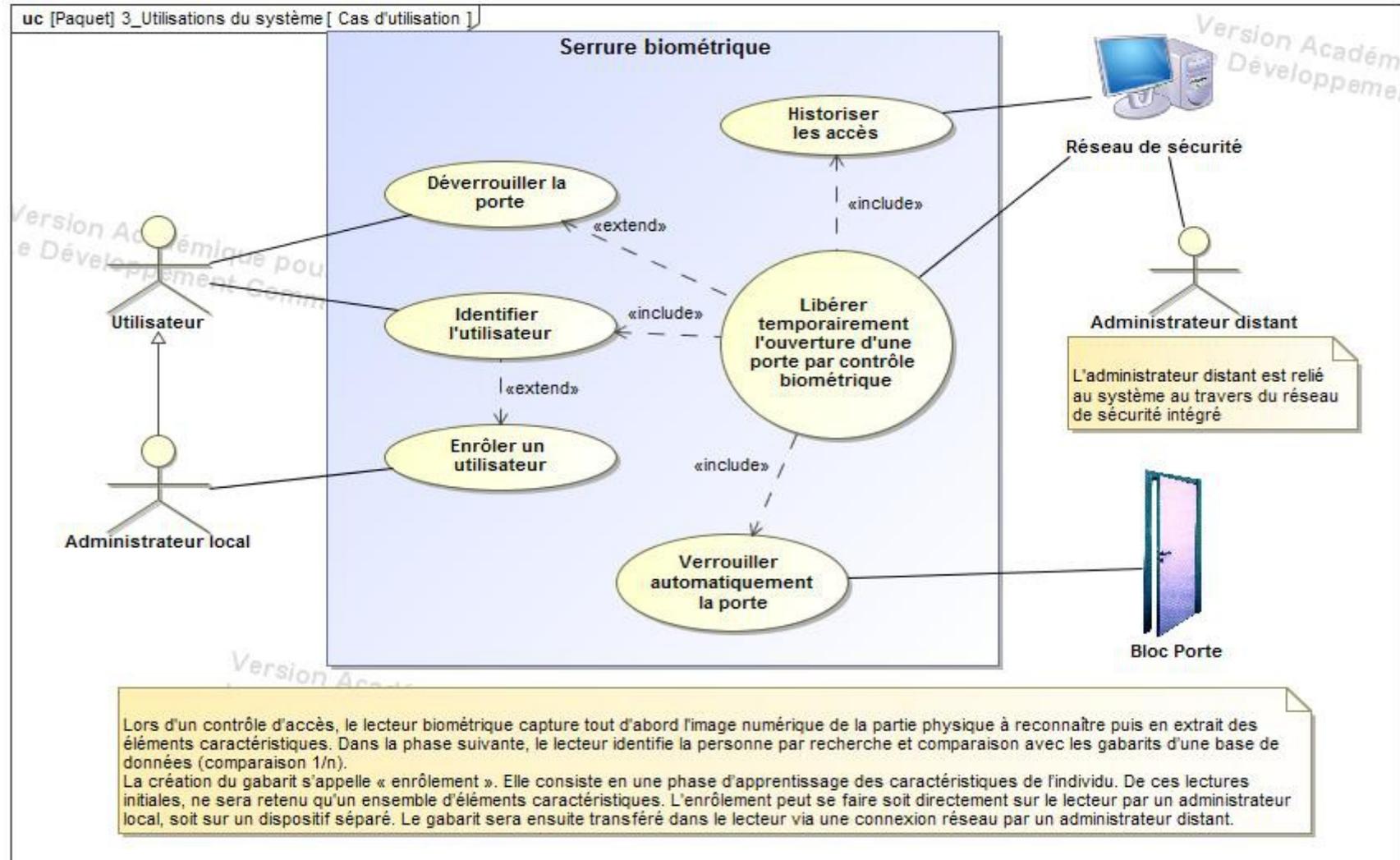
# Phase stockage / transport



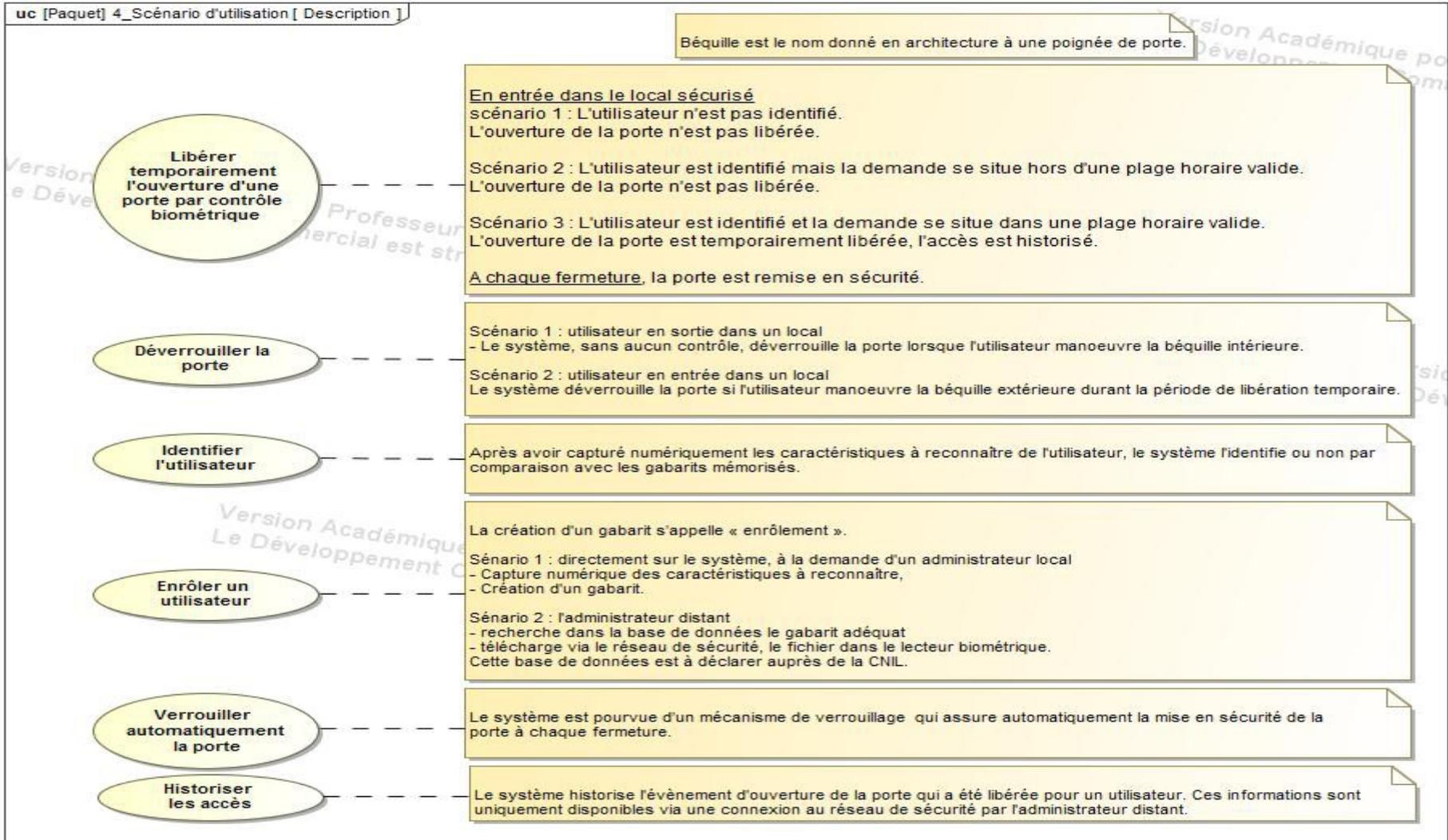
# Phase de retrait



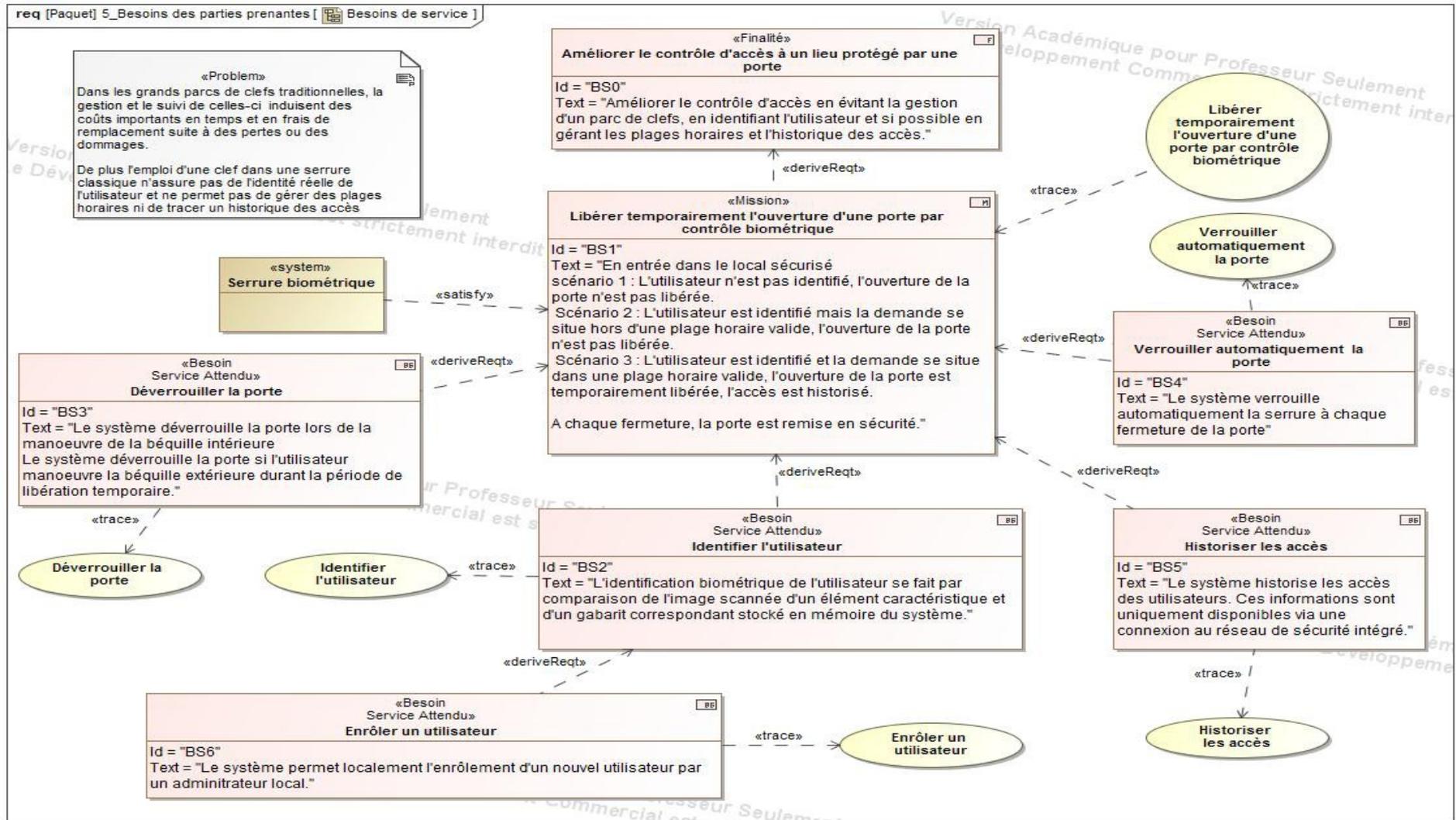
# Cas d'utilisation



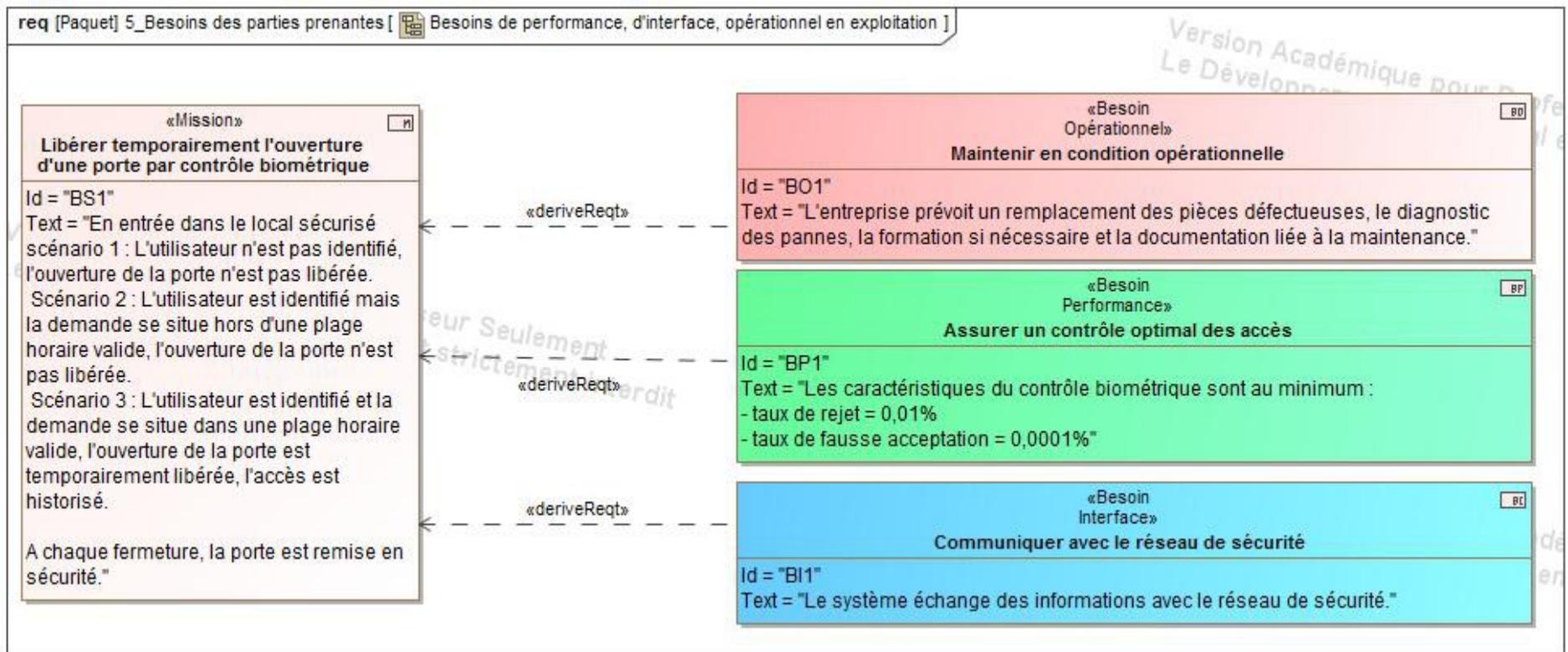
# Description



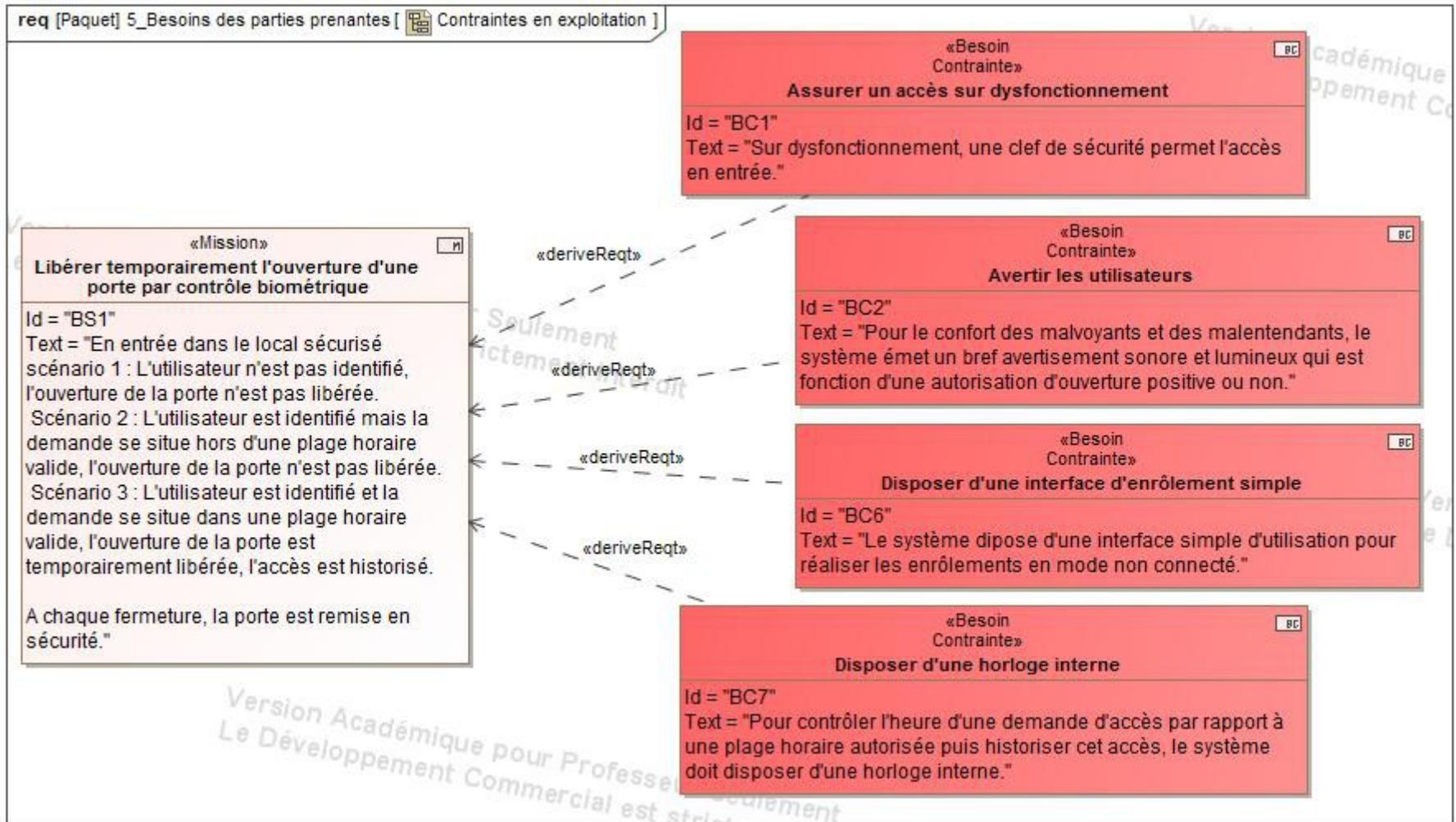
# Besoins de service



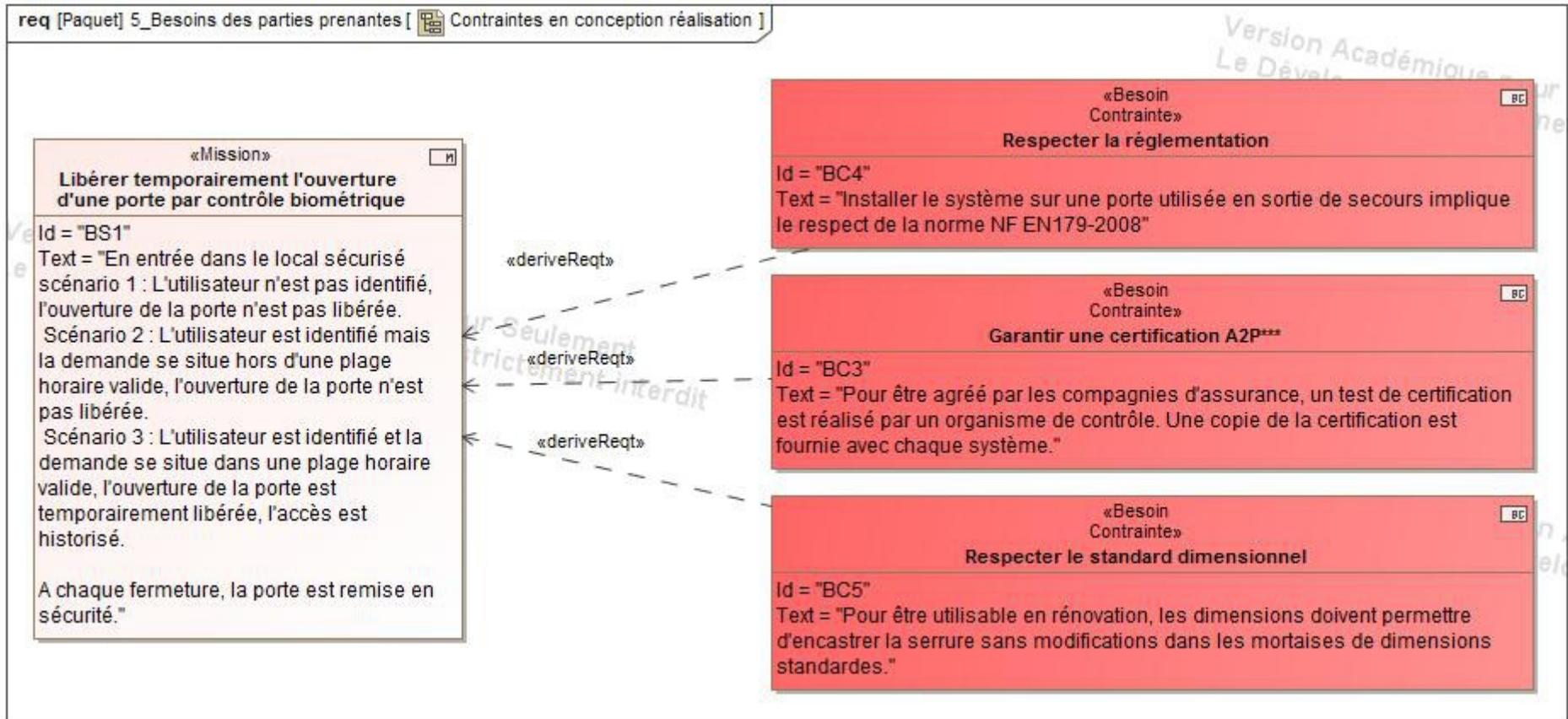
# Besoins de performance, d'interface, opérationnel en exploitation



# Contraintes en exploitation



# Contraintes en conception réalisation



# Liste des besoins

#	ID	Name	Text
1	BS0	Améliorer le contrôle d'accès à	Améliorer le contrôle d'accès en évitant la gestion d'un parc de defs, en identifiant l'utilisateur et si possible en gérant les plages horaires et l'historique des accès.
2	BS1	Libérer temporairement l'ouver	En entrée dans le local sécurisé scénario 1 : L'utilisateur n'est pas identifié, l'ouverture de la porte n'est pas libérée. Scénario 2 : L'utilisateur est identifié mais la demande se situe hors d'une plage horaire valide, l'ouverture de la porte n'est pas libérée. Scénario 3 : L'utilisateur est identifié et la demande se situe dans une plage horaire valide, l'ouverture de la porte est temporairement libérée, l'accès est historisé.  A chaque fermeture, la porte est remise en sécurité.
3	BS2	Identifier l'utilisateur	L'identification biométrique de l'utilisateur se fait par comparaison de l'image scannée d'un élément caractéristique et d'un gabarit correspondant stocké en mémoire du système.
4	BS3	Déverrouiller la porte	Le système déverrouille la porte lors de la manoeuvre de la béquille intérieure Le système déverrouille la porte si l'utilisateur manoeuvre la béquille extérieure durant la période de libération temporaire.
5	BS4	Verrouiller automatiquement la	Le système verrouille automatiquement la serrure à chaque fermeture de la porte
6	BS5	Historiser les accès	Le système historise les accès des utilisateurs. Ces informations sont uniquement disponibles via une connexion au réseau de sécurité intégré.
7	BS6	Enrôler un utilisateur	Le système permet localement l'enrôlement d'un nouvel utilisateur par un administrateur local.
8	BI1	Communiquer avec le réseau c	Le système échange des informations avec le réseau de sécurité.
9	BC1	Assurer un accès sur dysfoncti	Sur dysfonctionnement, une def de sécurité permet l'accès en entrée.
10	BC2	Avertir les utilisateurs	Pour le confort des malvoyants et des malentendants, le système émet un bref avertissement sonore et lumineux qui est fonction d'une autorisation d'ouverture positive ou non.
11	BC3	Garantir une certification A2P*	Pour être agréé par les compagnies d'assurance, un test de certification est réalisé par un organisme de contrôle. Une copie de la certification est fournie avec chaque système.
12	BC4	Respecter la réglementation	Installer le système sur une porte utilisée en sortie de secours implique le respect de la norme NF EN179-2008
13	BC5	Respecter le standard dimensio	Pour être utilisable en rénovation, les dimensions doivent permettre d'encastrier la serrure sans modifications dans les mortaises de dimensions standard.
14	BC6	Disposer d'une interface d'enrô	Le système dispose d'une interface simple d'utilisation pour réaliser les enrôlements en mode non connecté.
15	BC7	Disposer d'une horloge interne	Pour contrôler l'heure d'une demande d'accès par rapport à une plage horaire autorisée puis historiser cet accès, le système doit disposer d'une horloge interne.
16	BP1	Assurer un contrôle optimal de:	Les caractéristiques du contrôle biométrique sont au minimum : - taux de rejet = 0,01% - taux de fausse acceptation = 0,0001%
17	BO1	Maintenir en condition opératio	L'entreprise prévoit un remplacement des pièces défectueuses, le diagnostic des pannes, la formation si nécessaire et la documentation liée à la maintenance.

