



Systeme P2P de sauvegarde sécurisé

Maryline Laurent-Maknavicius
TELECOM SudParis

01/11/2008

Projet DisPairse financé par la fondation TELECOM

- **Comment sécuriser un service P2P de sauvegarde ?**
- **Double objectif :**
 - Donner confiance aux utilisateurs
 - Facturer le service en fonction des ressources consommées

The diagram shows a circular network of 8 nodes, labeled Nœud 1 through Nœud 8, connected to each other. A user icon labeled 'Utilisateur' is connected to Nœud 1. The network is labeled 'Réseau P2P' in the center.





Fonctions de sécurité souhaitées

- **Protection des fragments P2P**
 - Intégrité, confidentialité, anonymat de l'utilisateur, respect de la vie privée
- **Contrôle d'accès au service de sauvegarde**
 - Limiter l'accès aux seuls abonnés
 - Limiter la participation au service des nœuds P2P voulus
- **Supervision du fonctionnement du service**
 - Détecter les comportements malveillants/égoïstes

Environnement Pastry



Structuration en fragments (pstore)

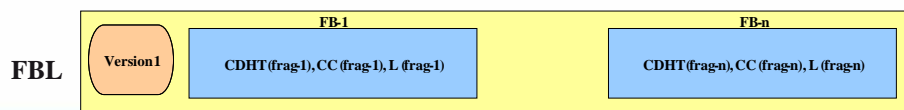
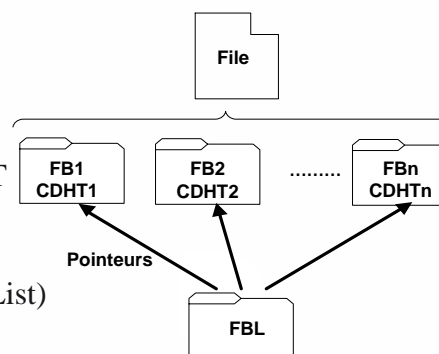
Chaque fichier est constitué de :

- un ensemble de fragments de données FB (File Block)

Identifié / localisé par une clé DHT

- un seul fragment FBL (File Block List)

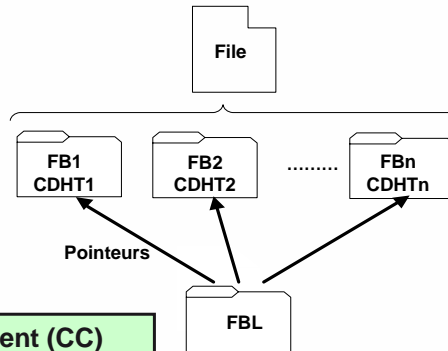
Identifié / localisé par une clé DHT





Protection des fragments

Intégrité, confidentialité,
anonymat de l'utilisateur,
respect de la vie privée

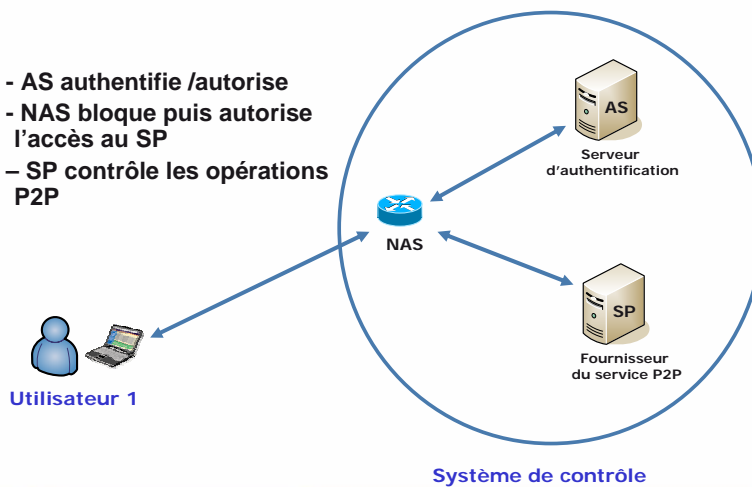


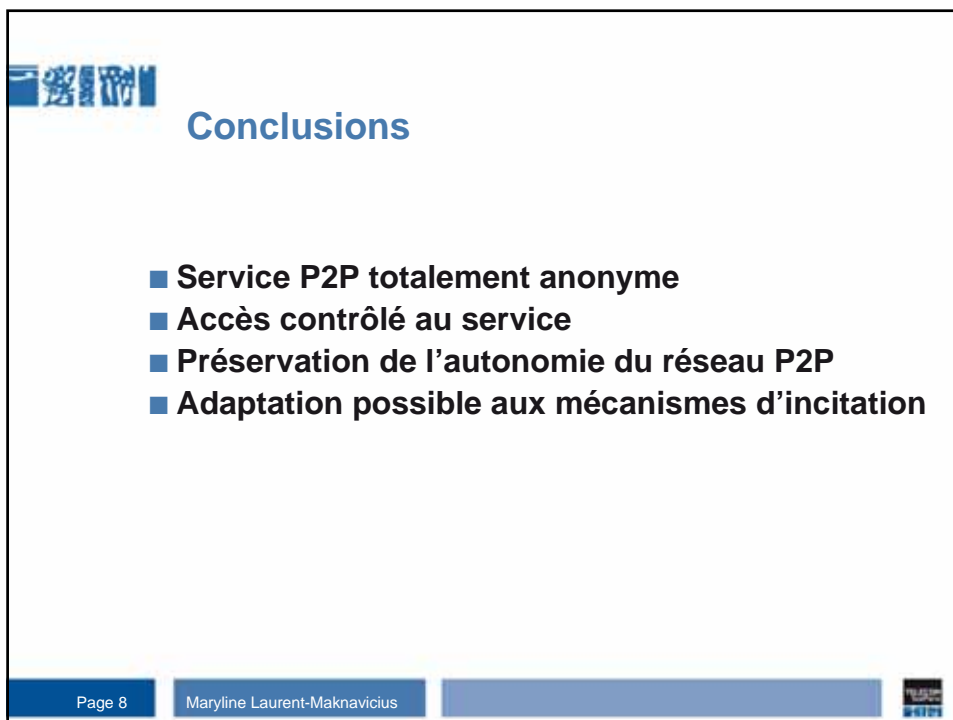
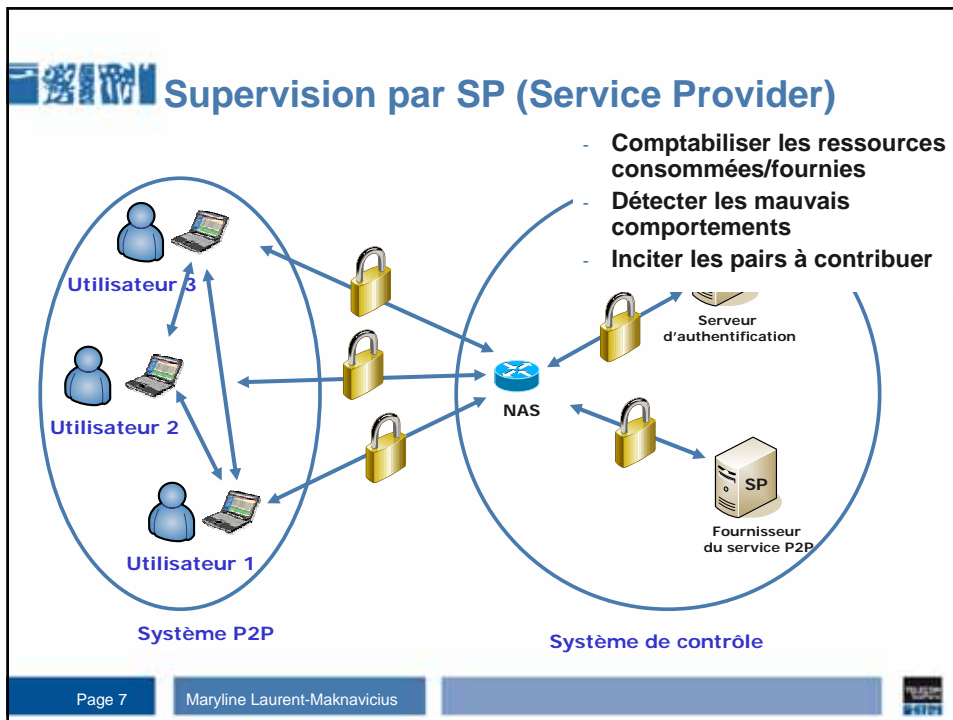
Ex de clé CDHT et clé de chiffrement (CC)
pour les FBL (File Block List) :

$$\text{CDHTFBL} = H(\text{secret} \text{ o pathname} \text{ o filename})$$
$$\text{CCFBL} = H(f(\text{secret}) \text{ o pathname} \text{ o filename})$$


Contrôle d'accès au service de sauvegarde à 3 niveaux par une architecture AAA

- 1 - AS authentifie /autorise
- 2 - NAS bloque puis autorise l'accès au SP
- 3 - SP contrôle les opérations P2P







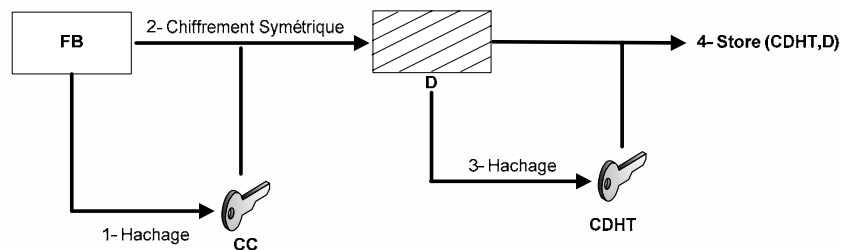
Plus d'informations...

- <http://www-lor.int-evry.fr/~maknavic>
- **1 brevet déposé :**
 - « Restauration facile, sécurisée et automatique de fichiers personnels sauvegardés dans un réseau Peer-to-Peer (P2P) », numéro d'enregistrement 08 52170, avril 2008
- H. Jarraya, M. Laurent-Maknavicius, " Système P2P de sauvegarde distribuée sécurisée ", 8ème Conférence Internationale sur les NOUvelles TEchnologies de la REpartition, NOTERE 2008, Lyon, FRANCE, Juin 2008, pp. 125-134



Protection des fragments FB

Convergent Encryption



➤ Confidentialité : $CC = H(\mathbf{FB})$

✓ Utilisation d'une clef de chiffrement CC dépendant du contenu

➤ Intégrité : $CDHT = H(\mathbf{FB-chiffré})$





Protection des fragments FBL

- Calcul de la clé DHT (pStore étendu)

$$\mathbf{CDHT}_{\text{FBL}} = \mathbf{H}(\text{secret} \text{ o pathname o filename})$$

- Confidentialité

$$\mathbf{CC}_{\text{FBL}} = \mathbf{H}(f(\text{secret}) \text{ o pathname o filename})$$



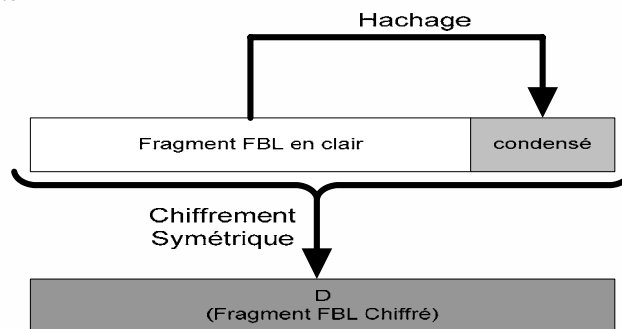
Secret : mot de passe, clé privée, f (login, mot de passe),...

Maryline Laurent-Maknavicius



Protection des fragments FBL

- Intégrité



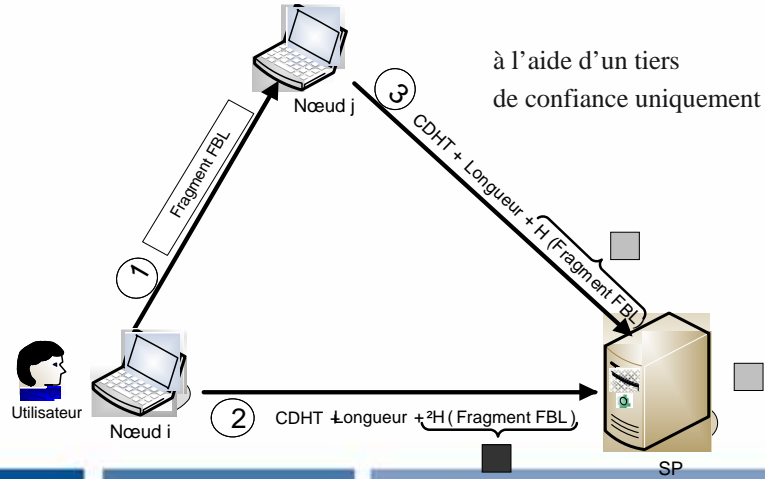
- Anonymat du propriétaire
- Seul le propriétaire est en mesure de vérifier l'intégrité du FBL

Maryline Laurent-Maknavicius



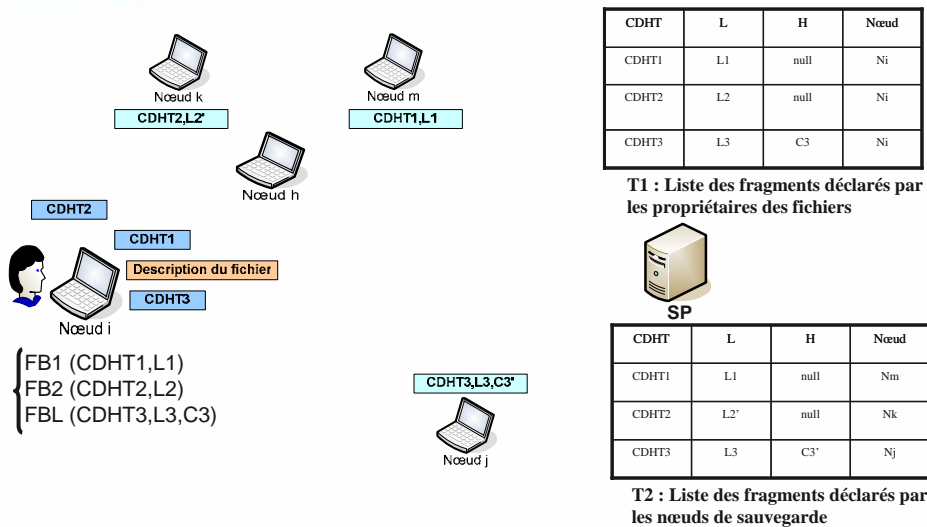
Protection des fragments FBL

> Vérification de l'intégrité par un nœud de sauvegarde



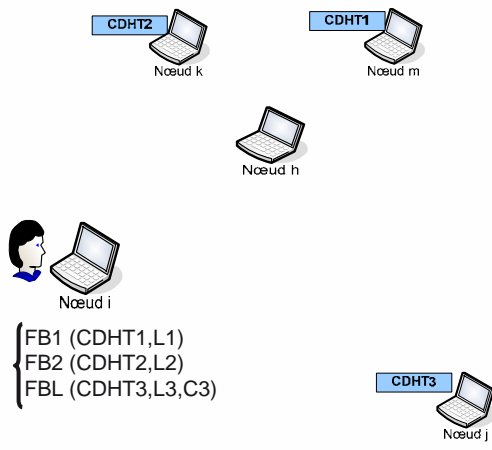
Maryline Laurent-Maknavicius

Sauvegarde d'un fichier



Maryline Laurent-Maknavicius

Sauvegarde d'un fichier



CDHT	L	H	Nœud
CDHT1	L1	null	Ni
CDHT2	L2	null	Ni
CDHT3	L3	C3	Ni

T1 : Liste des fragments déclarés par les propriétaires des fichiers



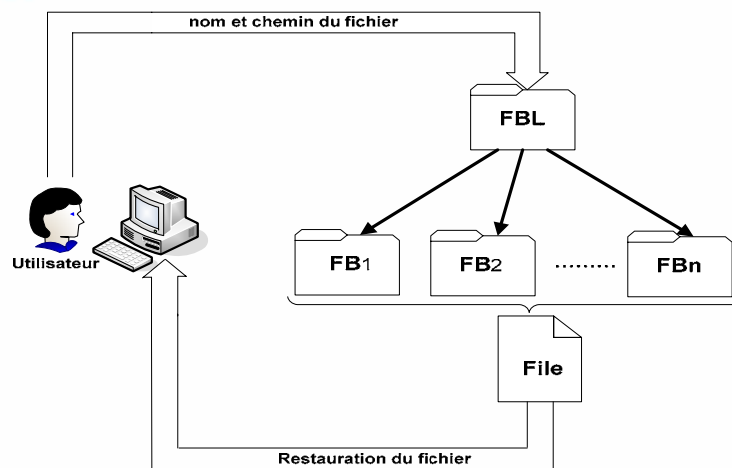
CDHT	L	H	Nœud
CDHT1	L1	null	Nm
CDHT2	L2*	null	Nk
CDHT3	L3	C3*	Nj

T2 : Liste des fragments déclarés par les nœuds de sauvegarde

Maryline Laurent-Maknavicius



Restauration d'un fichier



Processus de restauration d'un fichier

Maryline Laurent-Maknavicius

