L’architecture de l’espace de stockage

Groupe 2F – version 4.0 – 11 décembre 2003

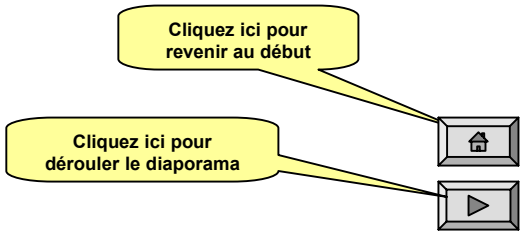


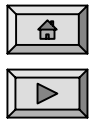
Table des matières

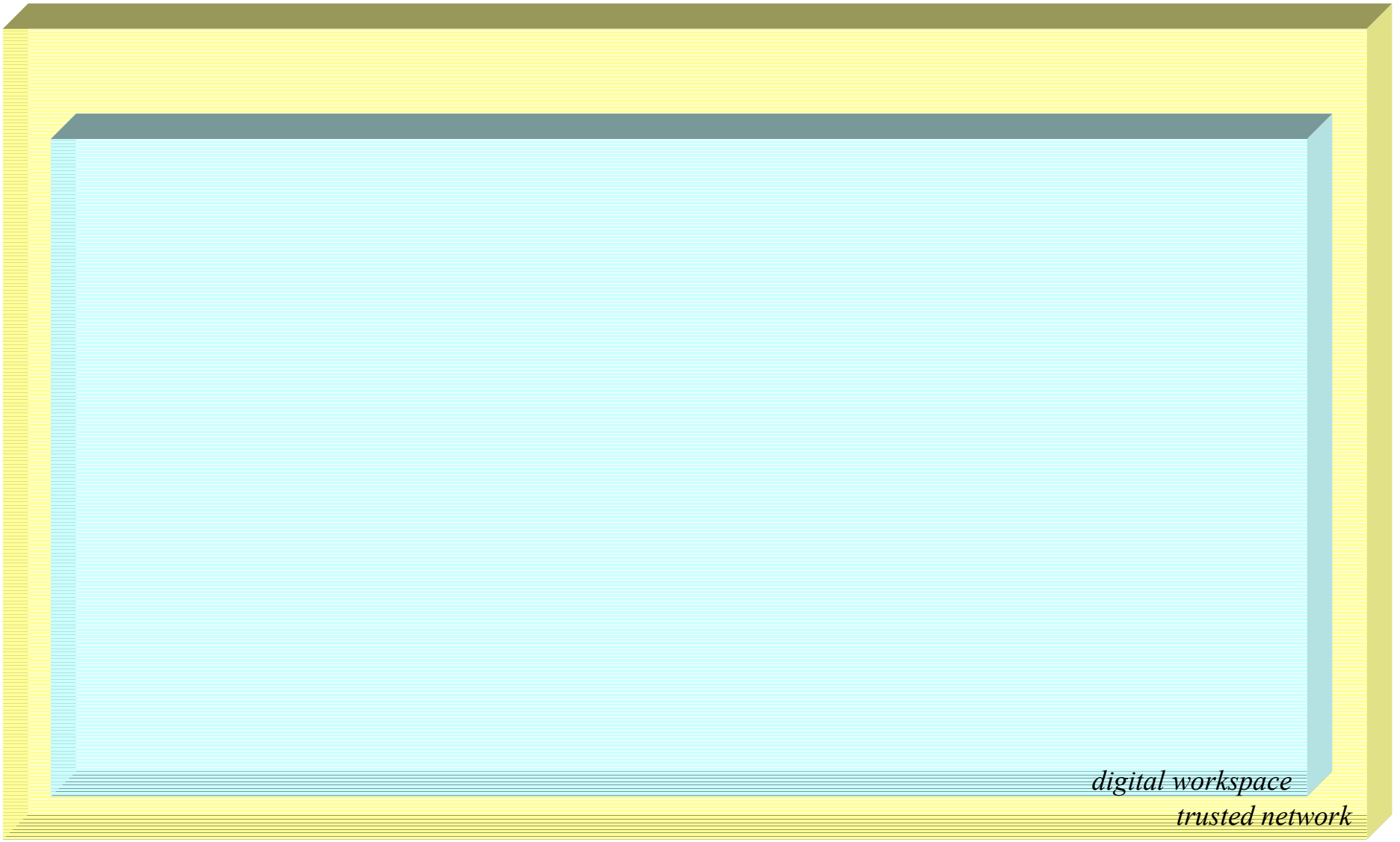
Statut de ce document

- Historique
  - 2003-12-11 – version 4.0
    - P. Aubry, J.-G. Avelin, R. Bourges, P. Gambarotto, V. Mathieu, J. Marchal, S. Qiang, B. Sor
      - Ré-organisation de la feuille de route
      - Principes de mise en œuvre de la version 1
  - 2003-12-03 – version 3.2
    - V. Mathieu :
      - Renumérotation des versions (V0 devient V1)
      - Ajout de la problématique des quotas
      - Modification de l'adressage logique des espaces utilisateurs (basé sur les identifiants)
  - 2003-11-12 – version 3.1
    - Les modules « authentification », « autorisation » et « système de fichiers » sont clairement indiqués comme étant des modules du serveur WebDAV (P. Gambarotto)
    - Ajouts de l'adressage logique de l'espace physique (P. Aubry)
    - Planification des versions (P. Aubry)
  - 2003-11-11 – version 3
    - Intégration de Access Control Protocol (B. Sor & P. Gambarotto)
  - 2003-11-06 – version 2
    - Intégration du gestionnaire de groupes et du système d'ACLs (P. Aubry, R. Bourges, V. Mathieu & A. Kermarrec)
  - 2003-10-04 – version 1 (P. Aubry)

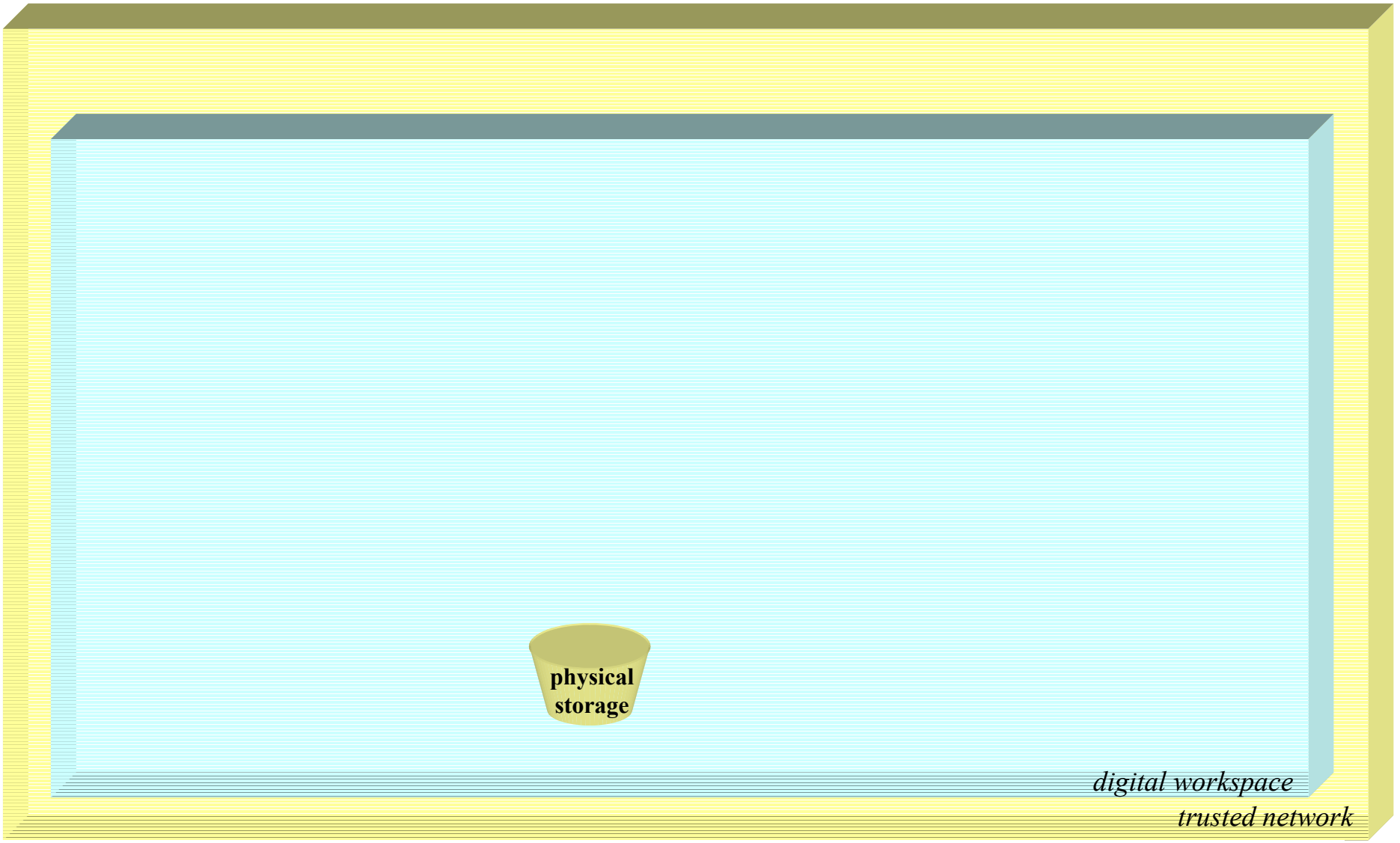
- Validation du document
  - au plus tard le mardi 16 décembre 2003
  - La version 4.0 est la dernière version des spécifications avant mise en œuvre de la version 1

- Planification des développements (feuille de route)

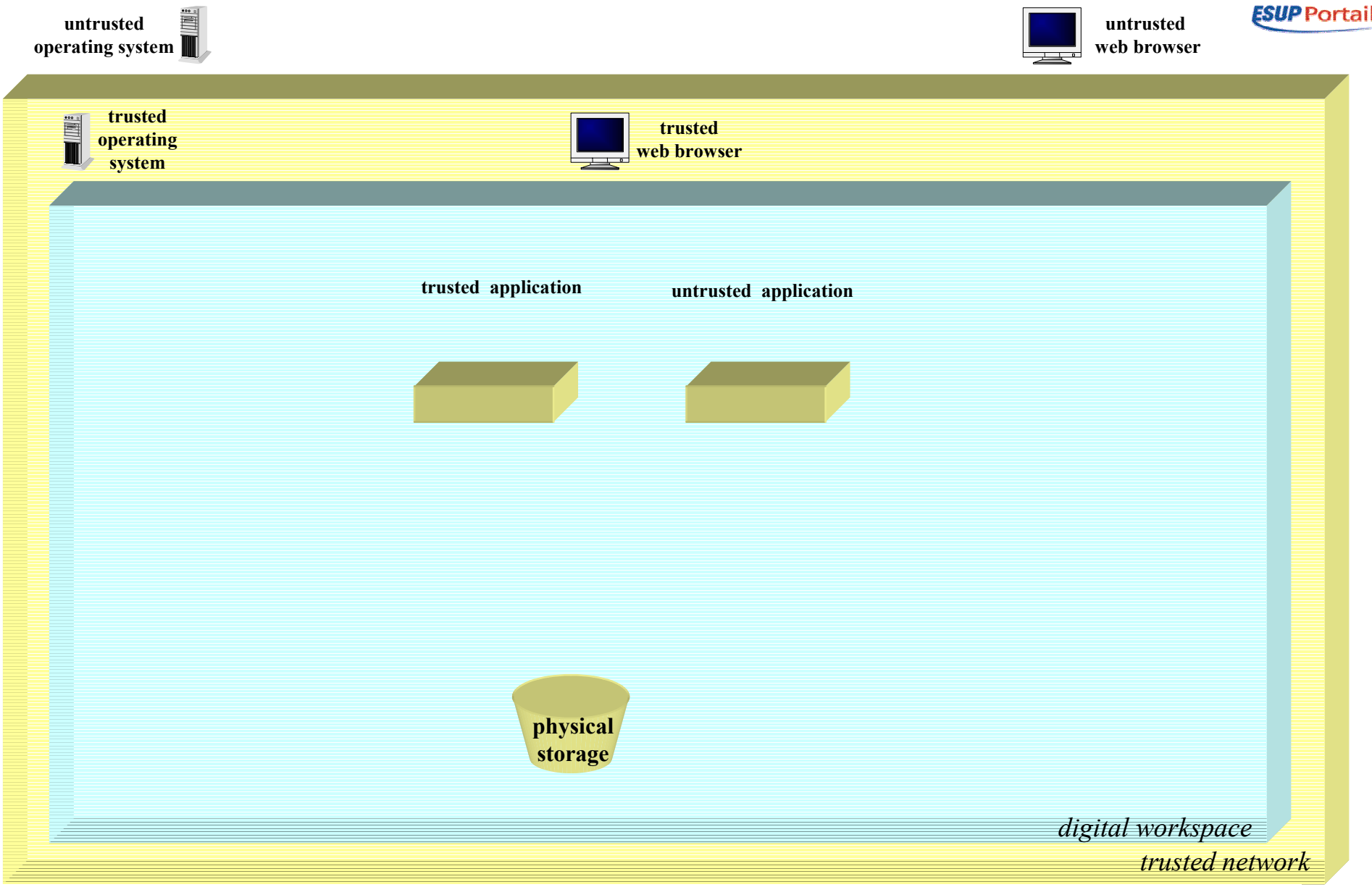




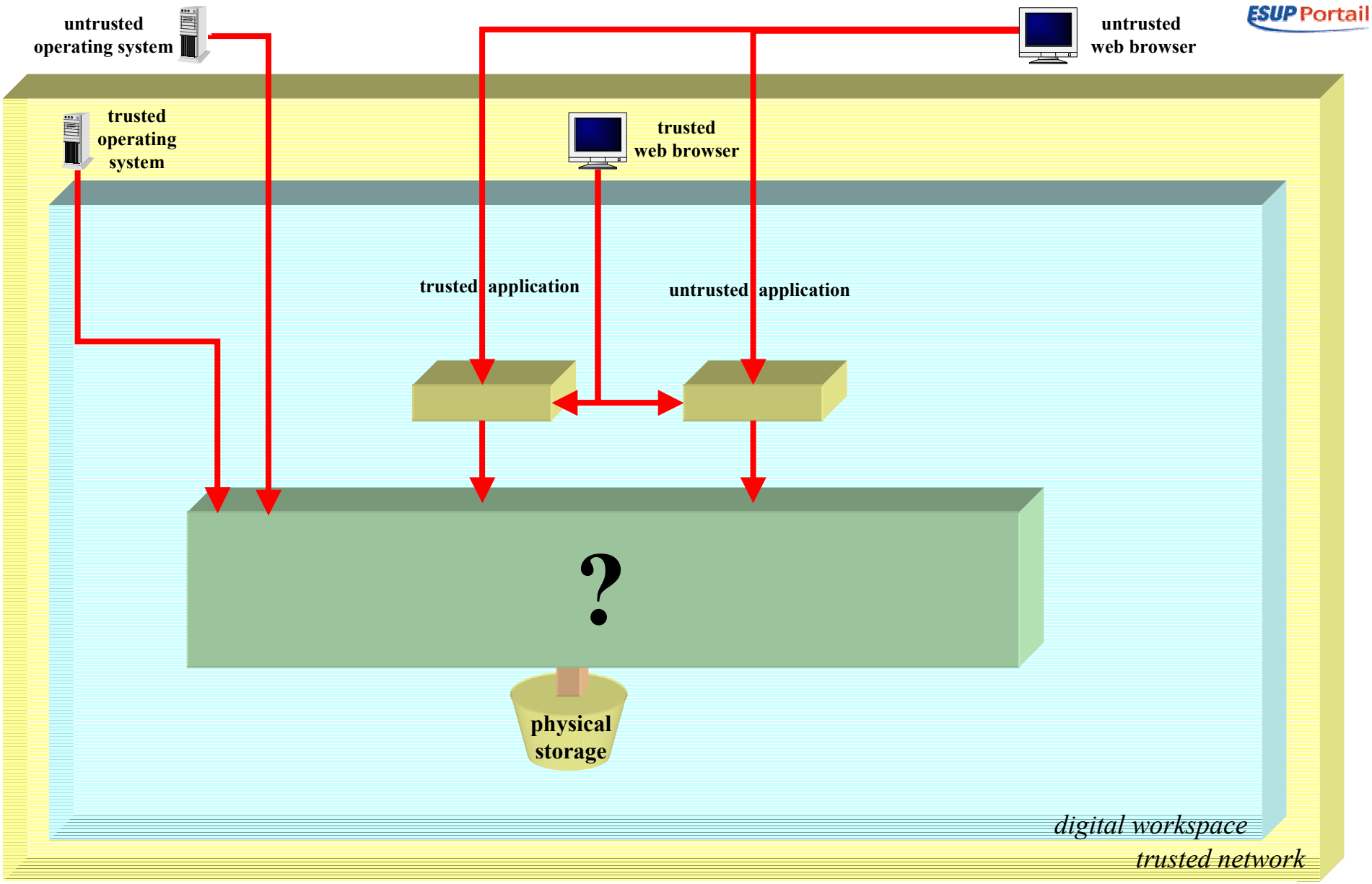
- Les zones en présences
  - En bleu : l'Environnement de Travail Numérique
  - En jaune : un réseau de confiance
  - En blanc : le reste de l'internet



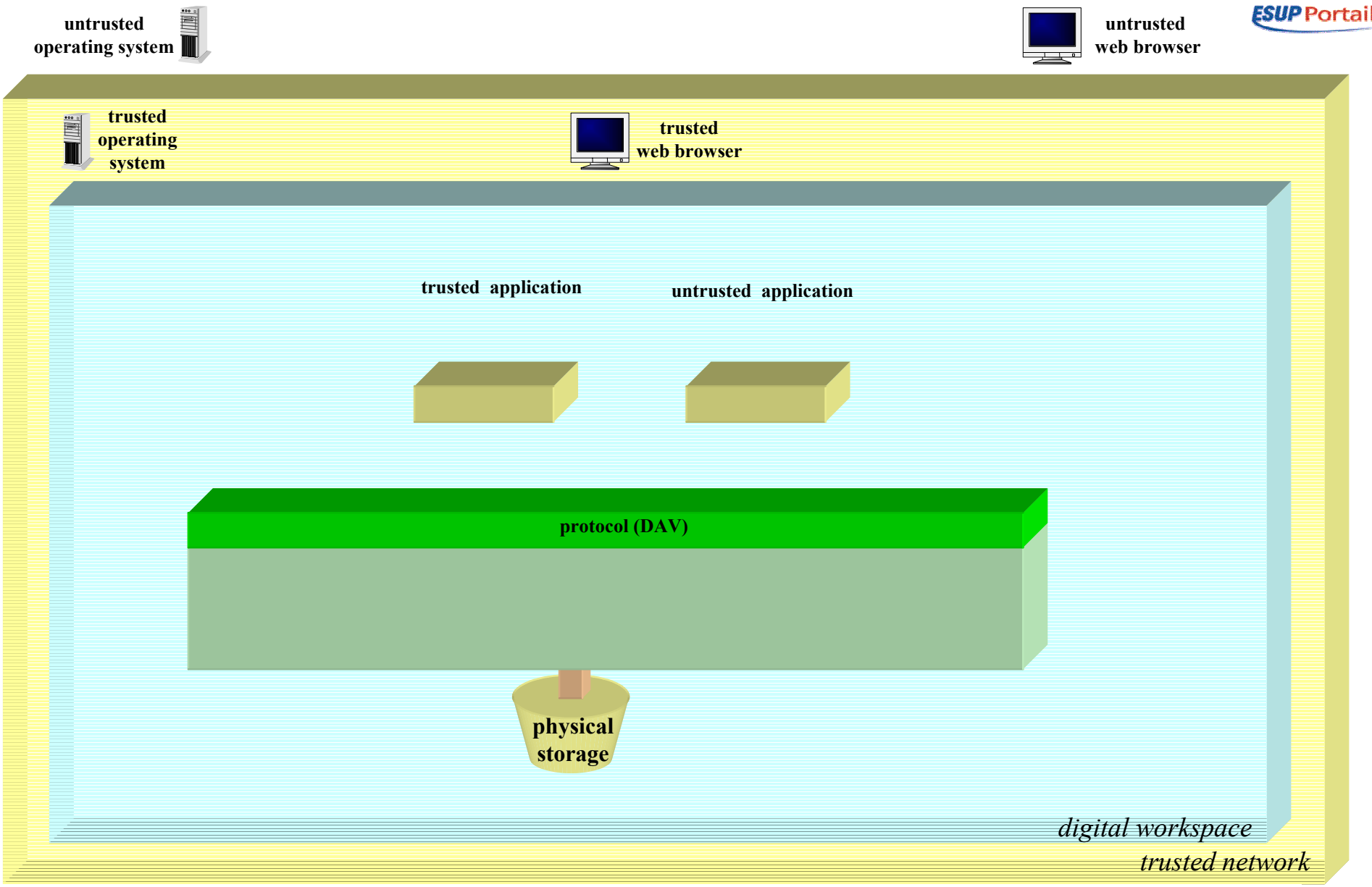
- Un espace de stockage physique, à propos duquel on ne fait pour l'instant aucune hypothèse



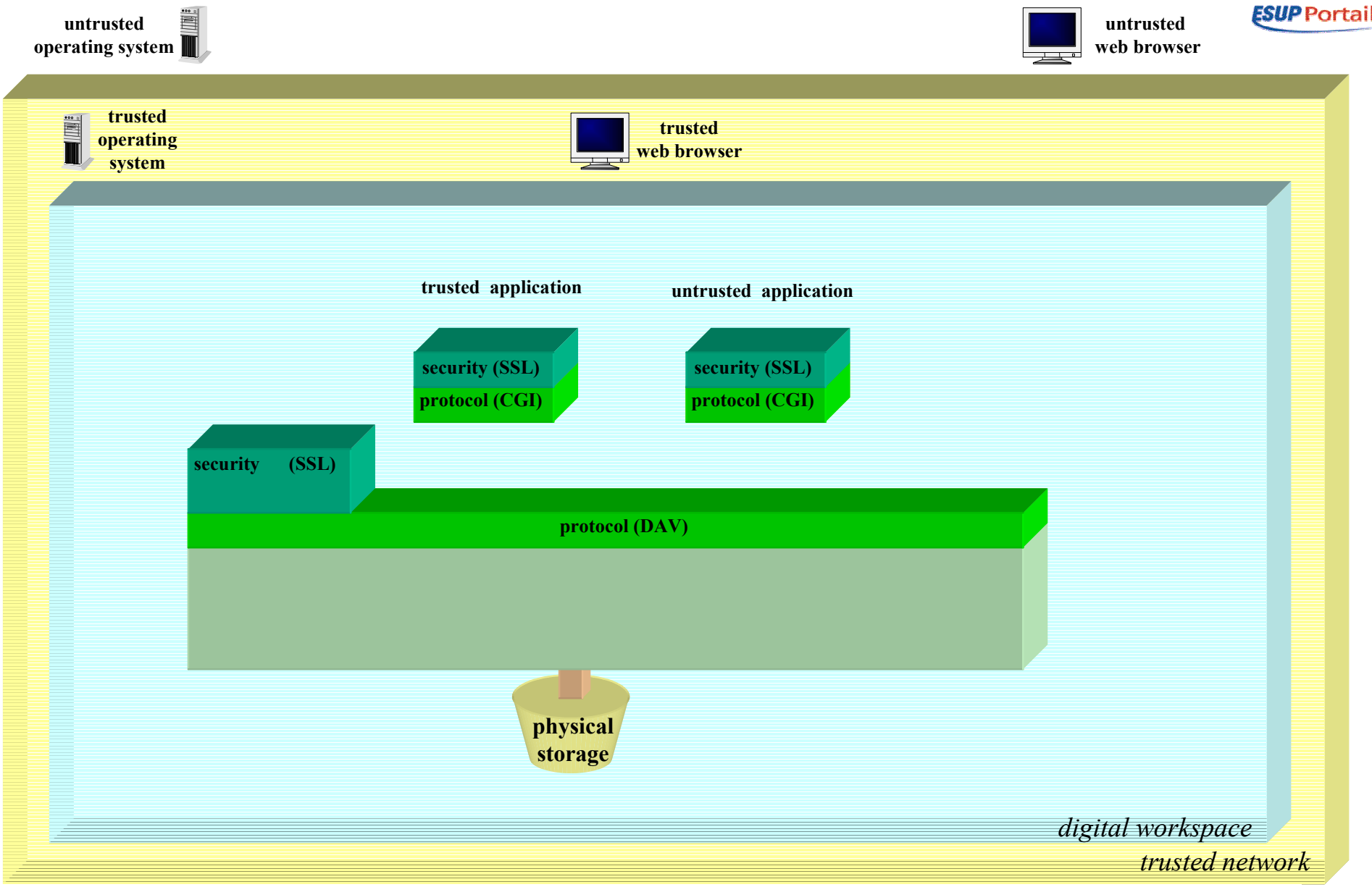
- Les clients de l'espace de stockage :
  - Des systèmes d'exploitation
  - Des navigateurs
  - Des applications



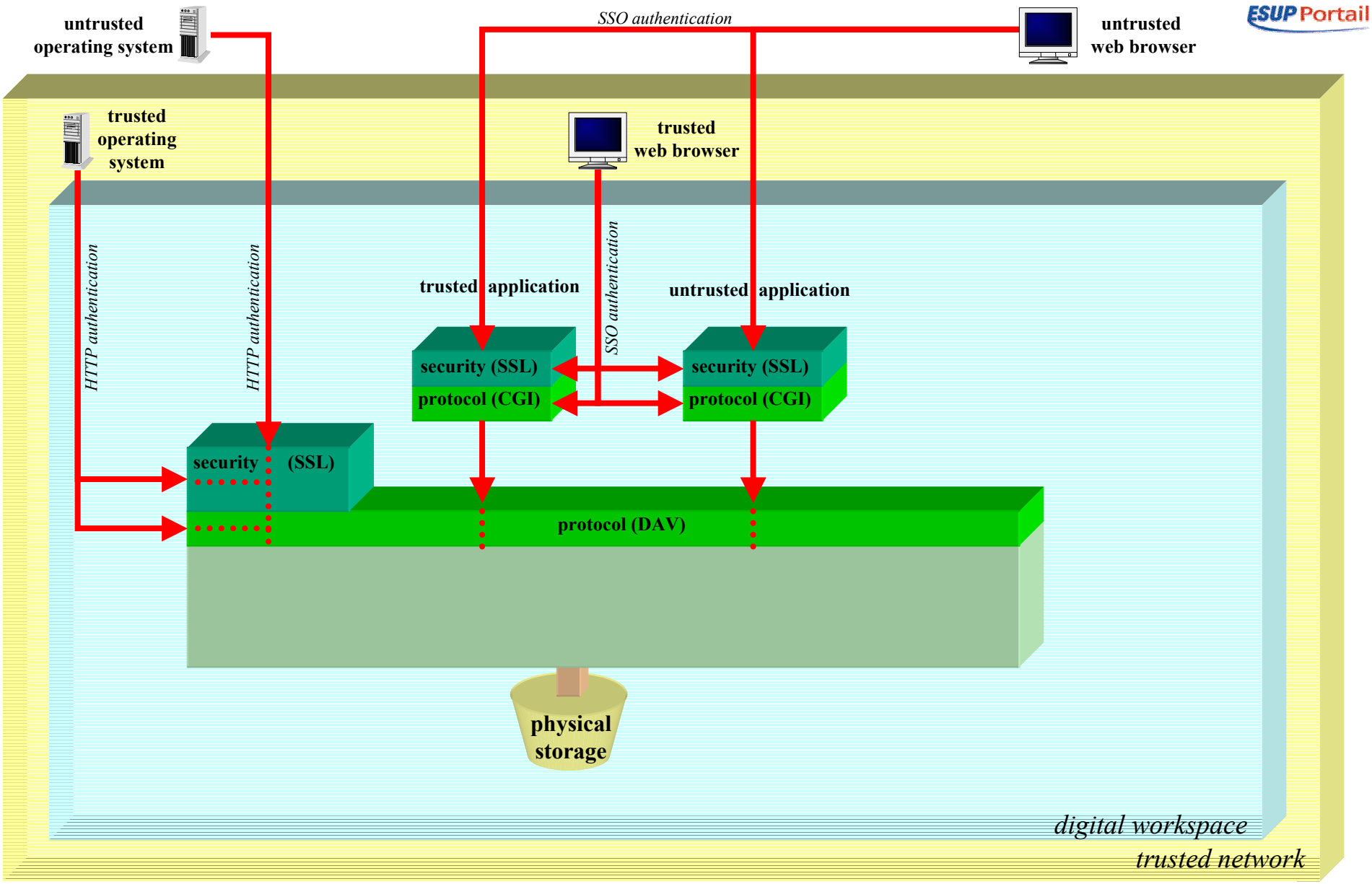
- Problématique
  - Que mettre en place pour que tous ces clients puissent accéder à l'espace de stockage ?



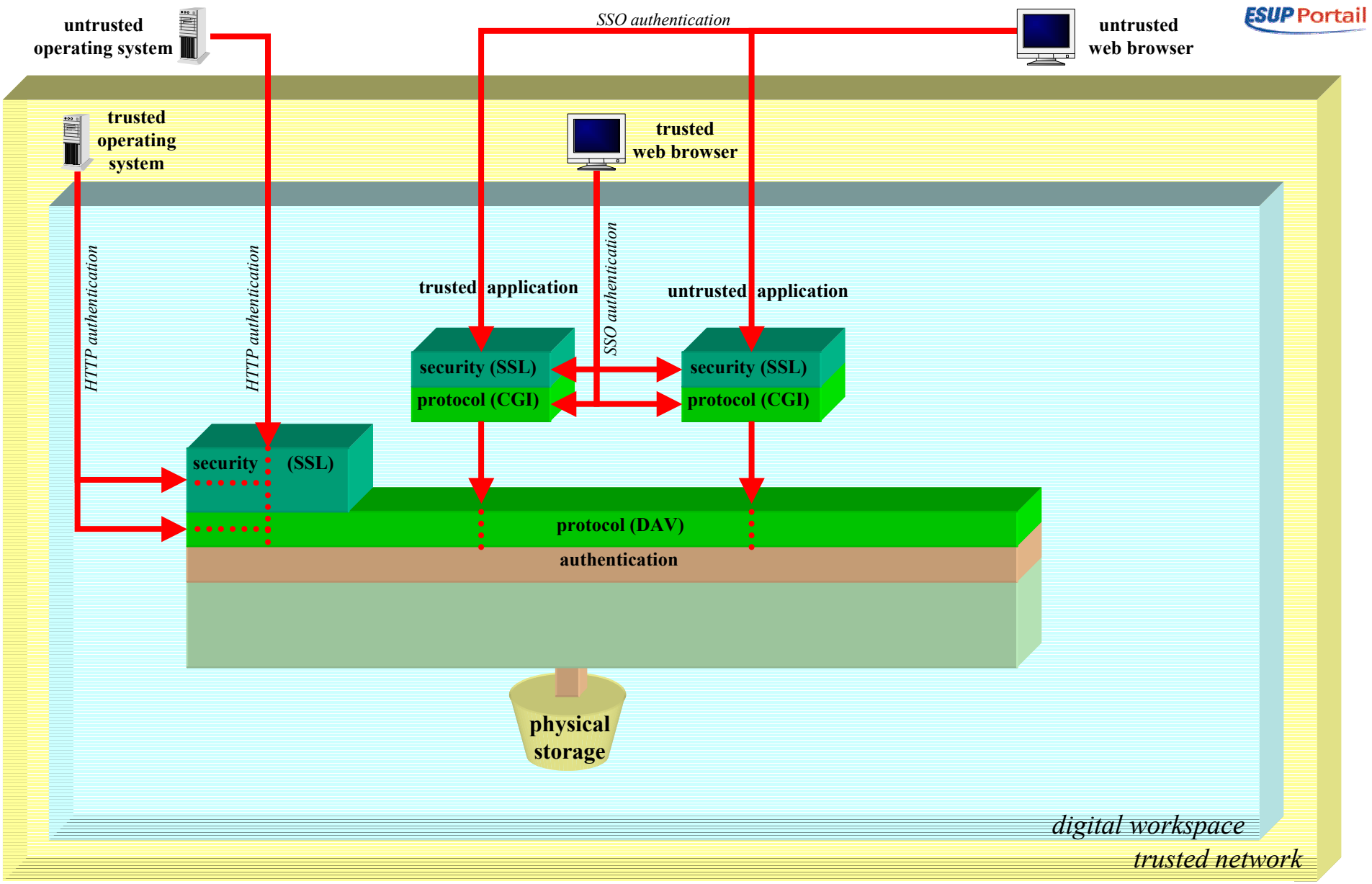
- Le protocole d'accès
  - L'espace de stockage devant être accédé depuis tout l'internet, on choisit WebDAV



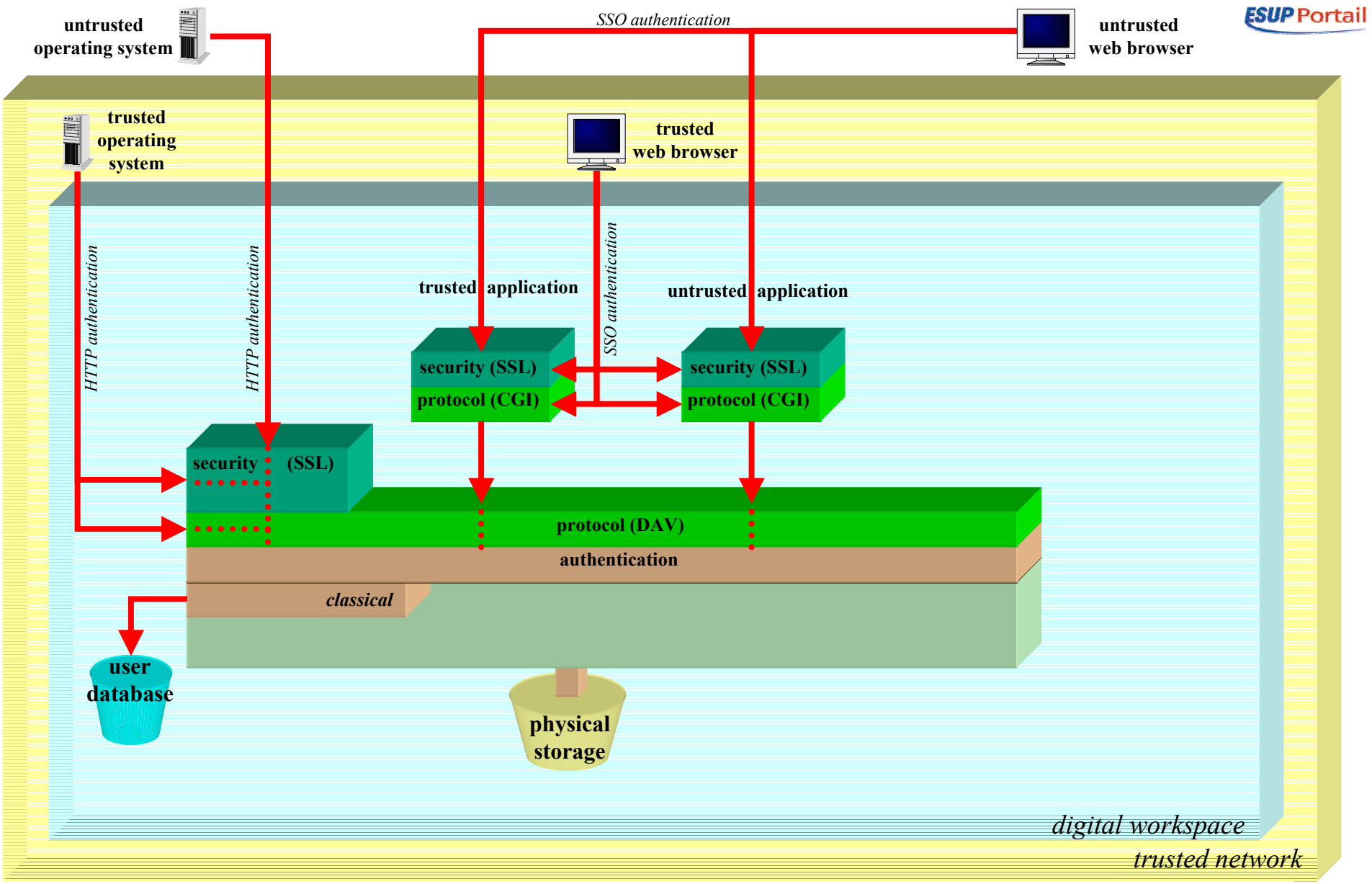
- Confidentialité
  - L'espace devant être accédé depuis n'importe quel point de l'internet, les échanges doivent être chiffrés (HTTPS pour les applications et WebDAV sur HTTPS pour les systèmes d'exploitation).



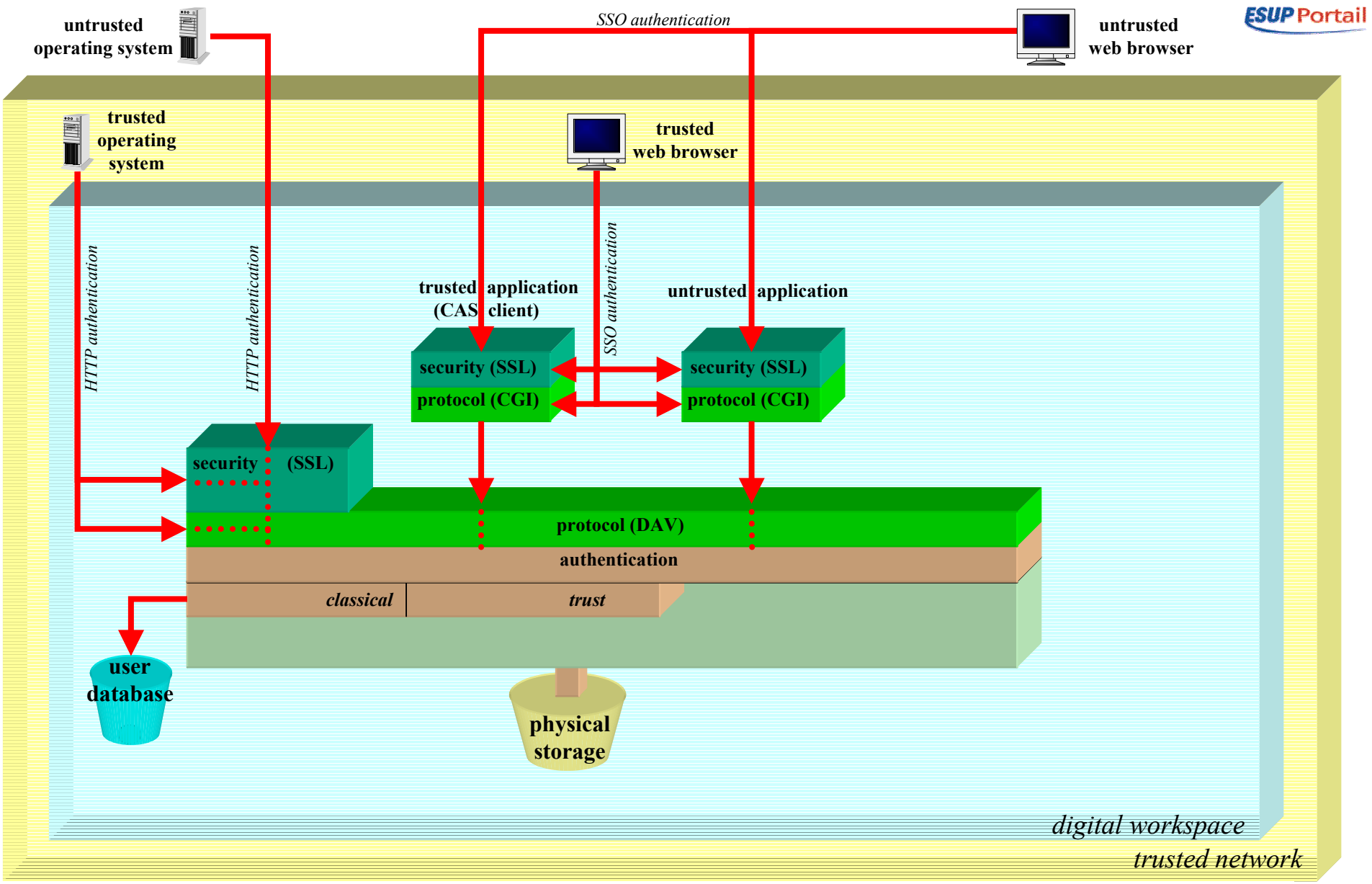
- Les applications s'appuient sur une authentification SSO
- Les systèmes d'exploitation s'appuient sur une authentification HTTP
- Note : Selon les politiques de sécurité des établissements, on peut ou non autoriser l'accès à l'espace de stockage de manière non sécurisée depuis un réseau de confiance.



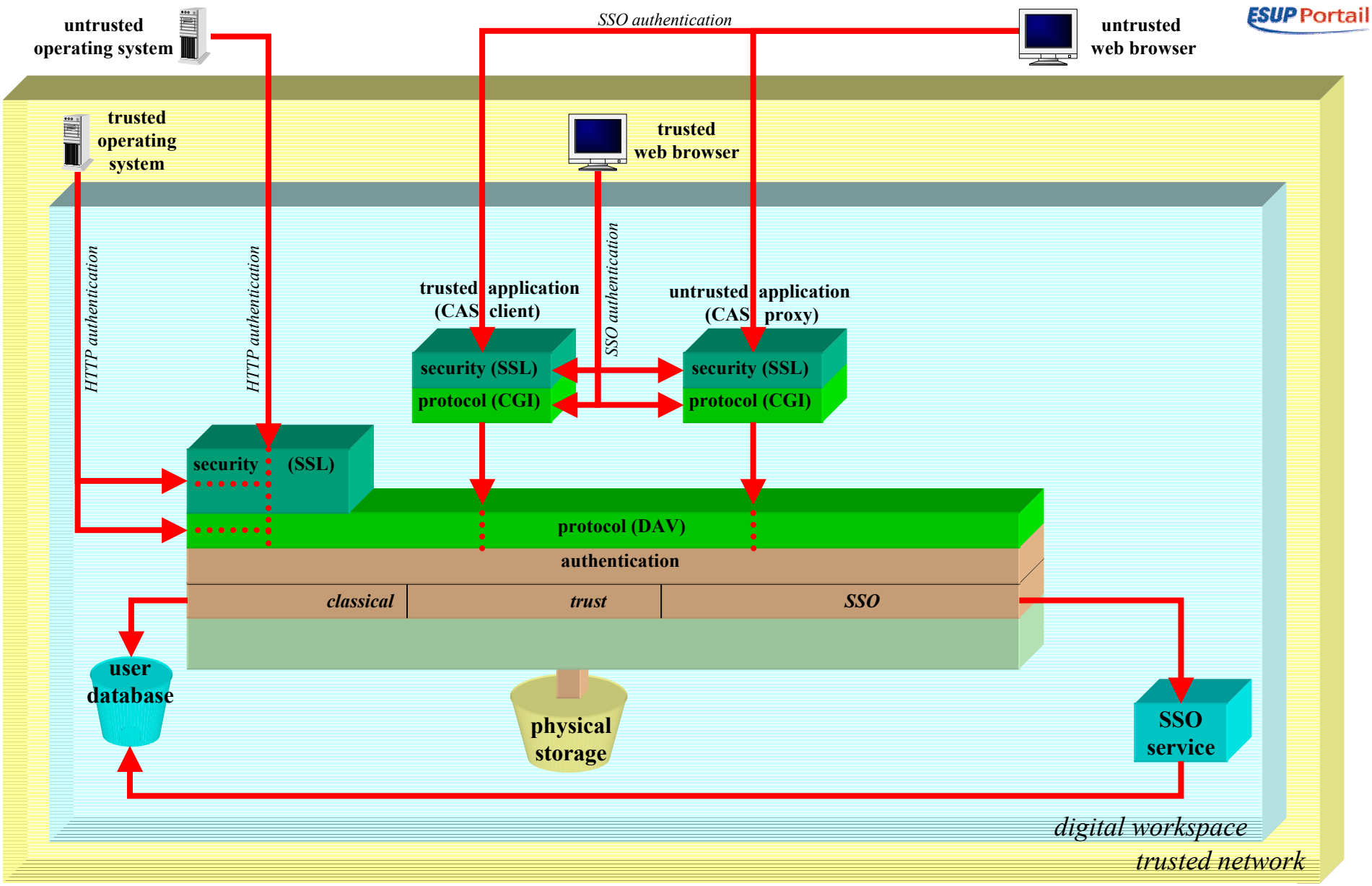
- Authentification
  - Le protocole WebDAV n'offre pas nativement d'authentification
  - Il faut donc l'implémenter en fonction de nos besoins



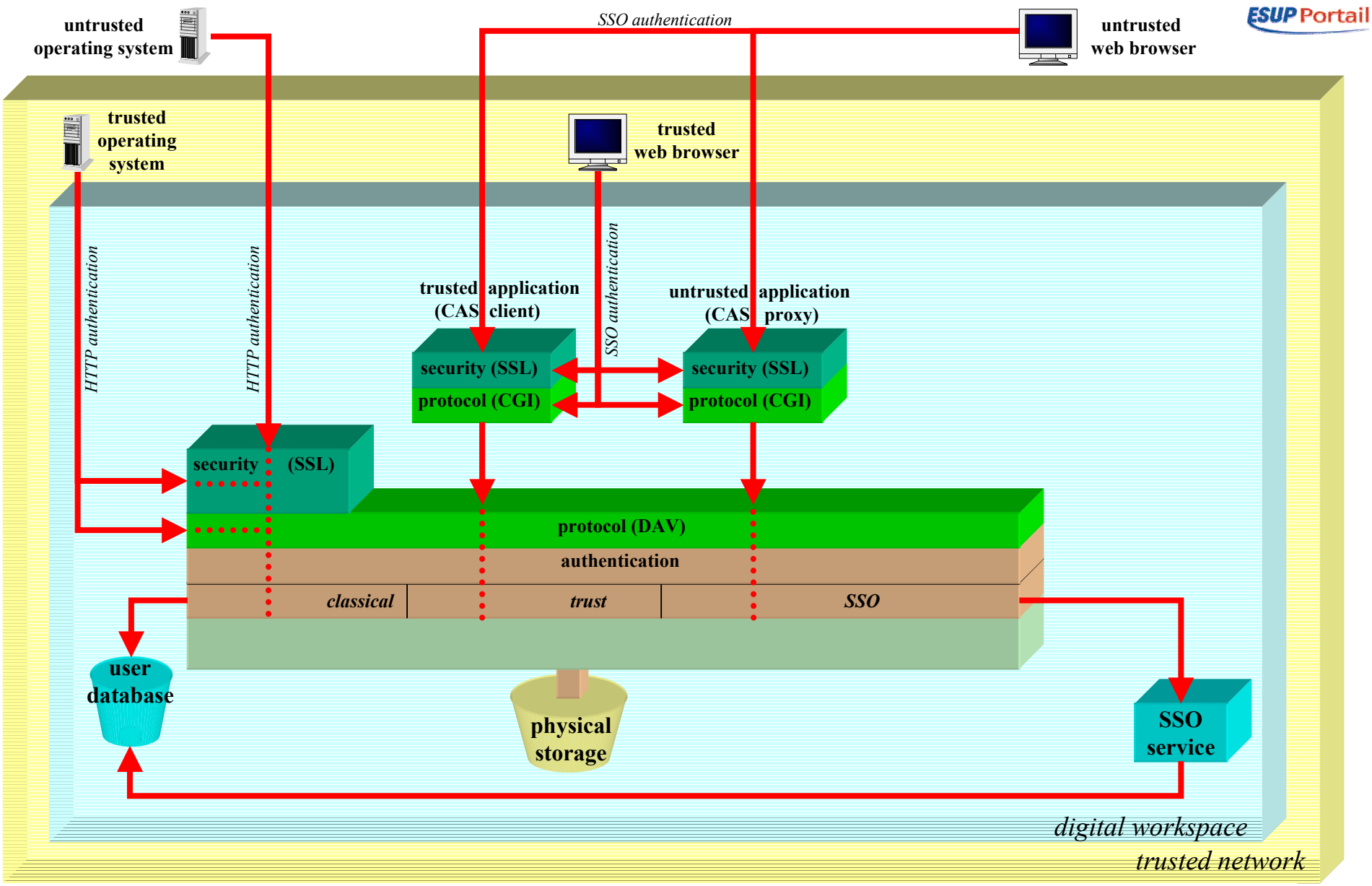
- Pour les systèmes d'exploitation
  - Puisqu'ils ne parlent pas SSO, il faut implémenter une authentification HTTP classique, en s'appuyant sur le référentiel utilisateur



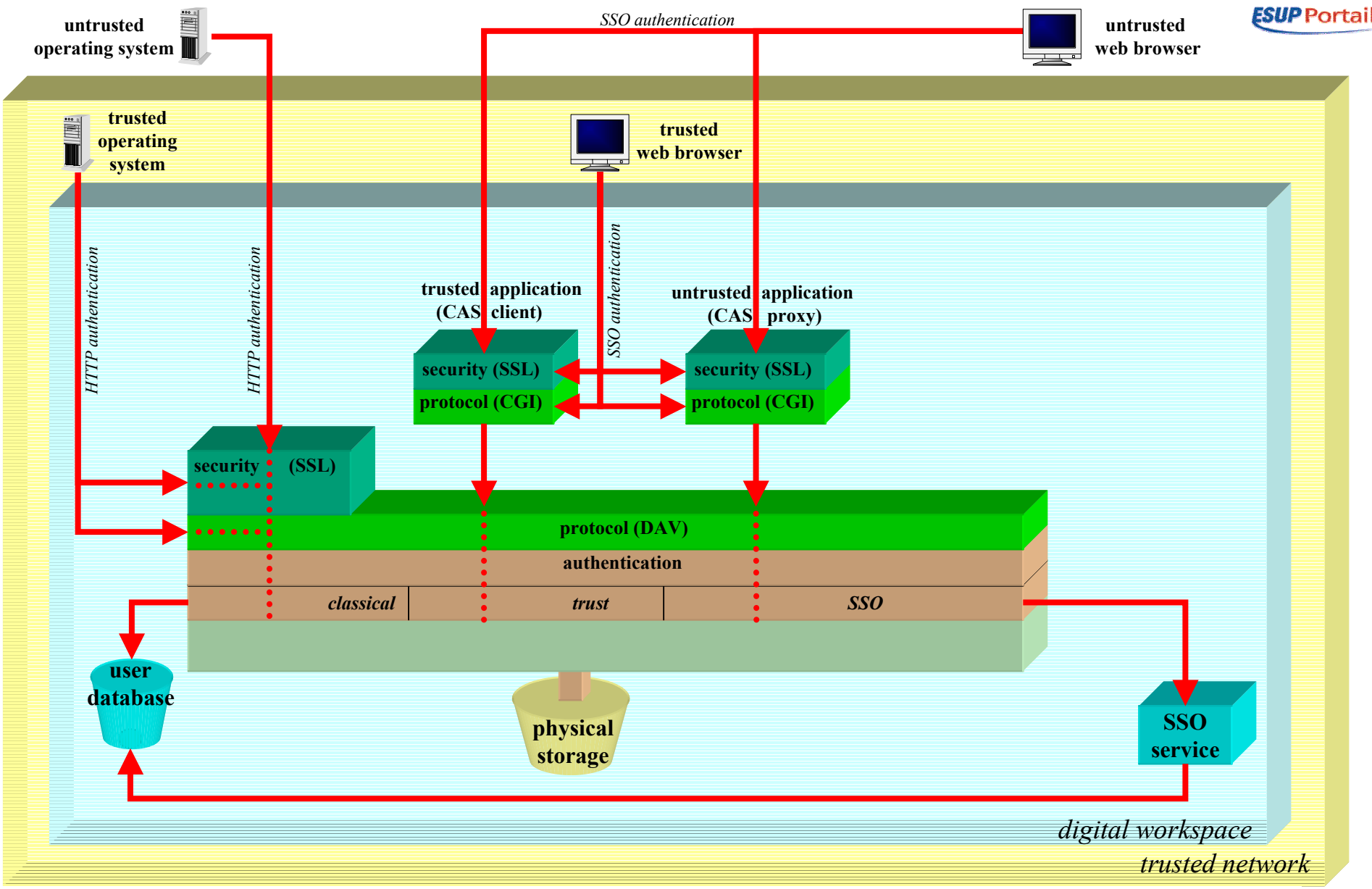
- Pour les applications de confiance
  - Puisque l'on peut leur faire confiance (clients CAS), on leur délègue l'authentification. Celles-ci doivent néanmoins indiquer à l'espace de stockage quel est l'utilisateur authentifié



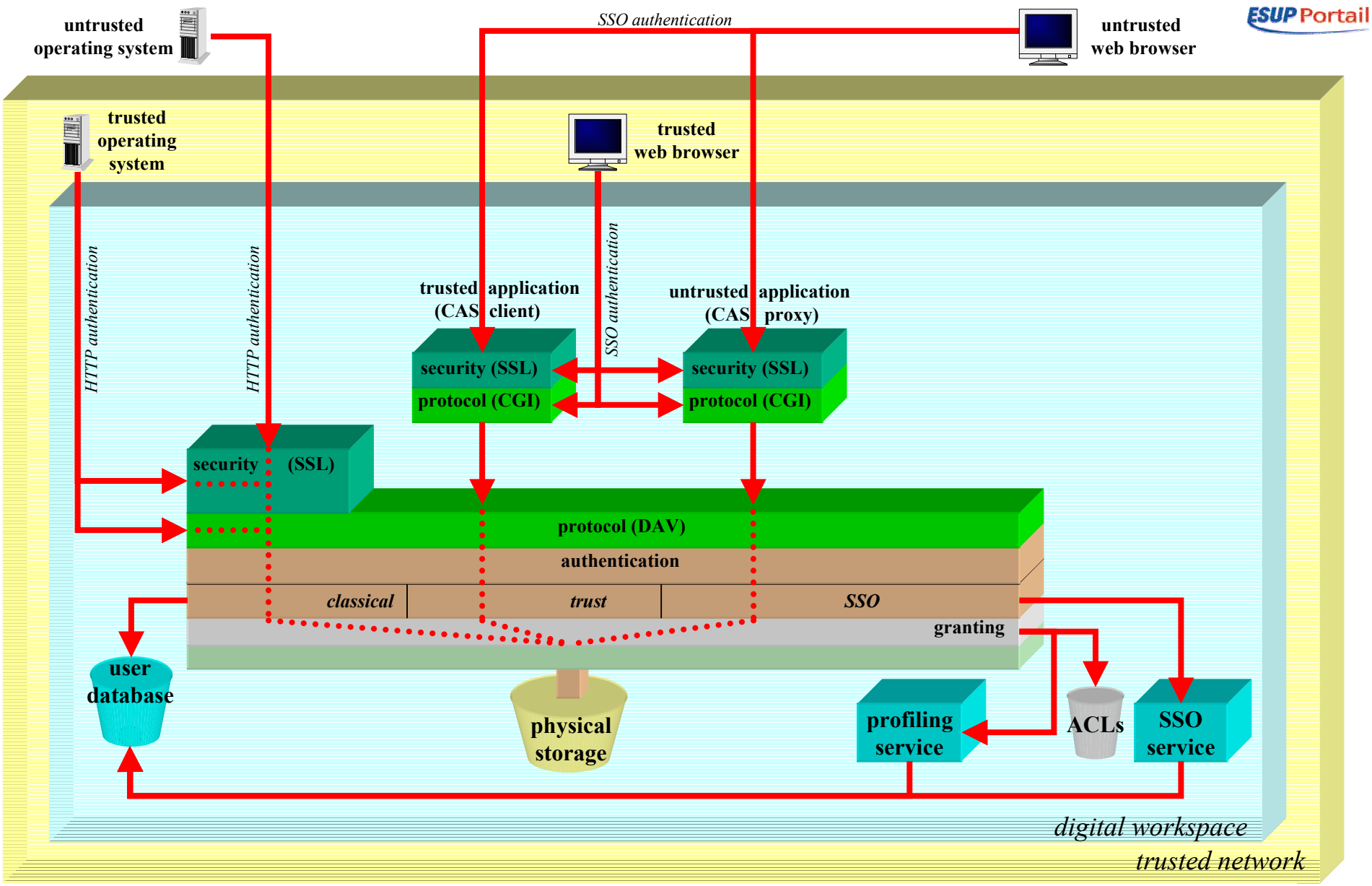
- Pour les autres applications
  - On s'appuie sur le SSO (les applications doivent alors être des mandataires CAS)
- Le service SSO est utilisé pour valider les tickets CAS fournis par les applications



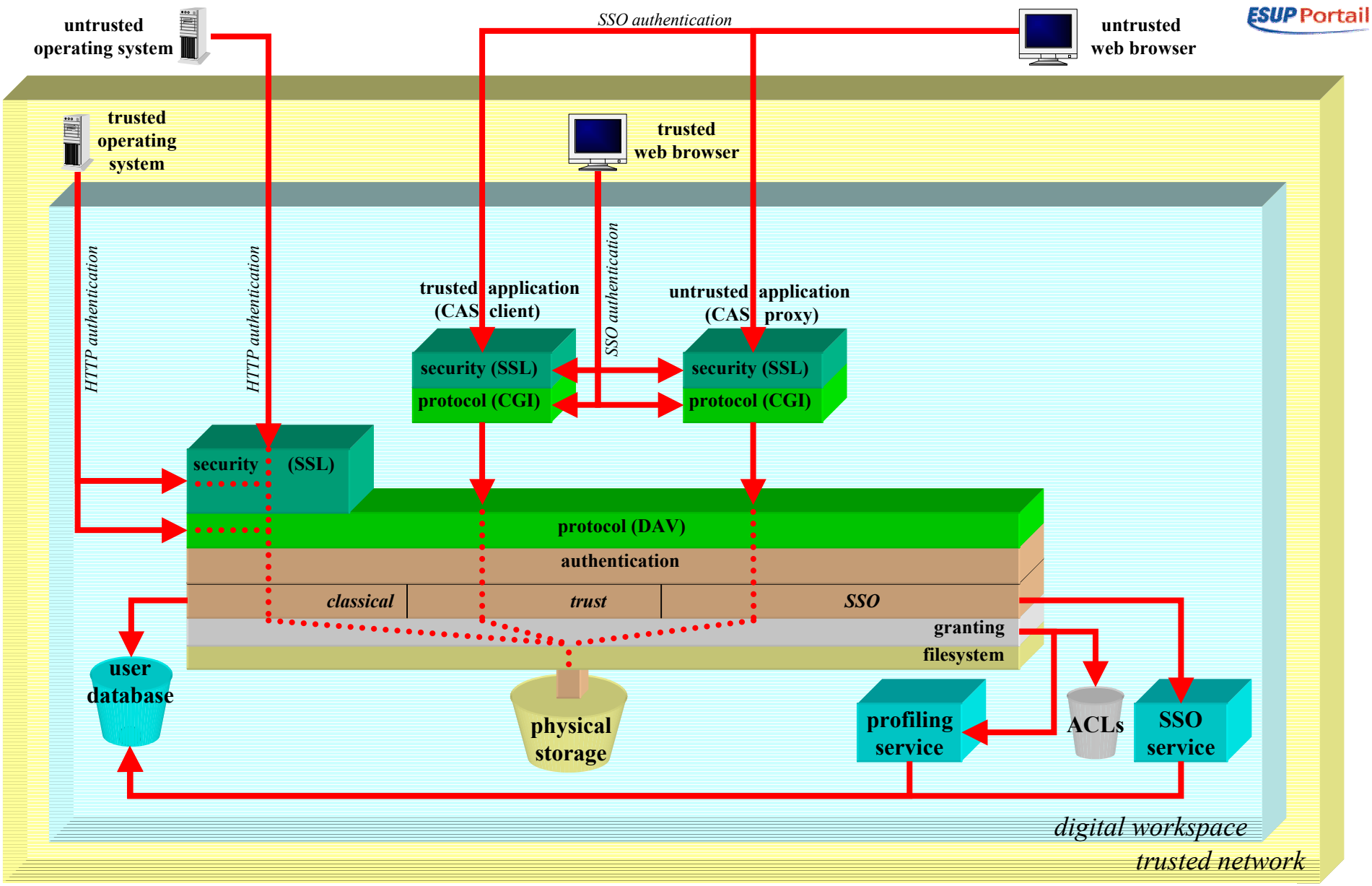
- L'authentification est une couche logique (module ou service) qui a pour unique but de répondre à la question suivante :
  L'utilisateur authentifié a-t-il le droit d'accéder à l'espace de stockage ?
  - En particulier, il ne dit pas ce que l'utilisateur authentifié a le droit de faire sur l'espace de stockage (cf plus loin).



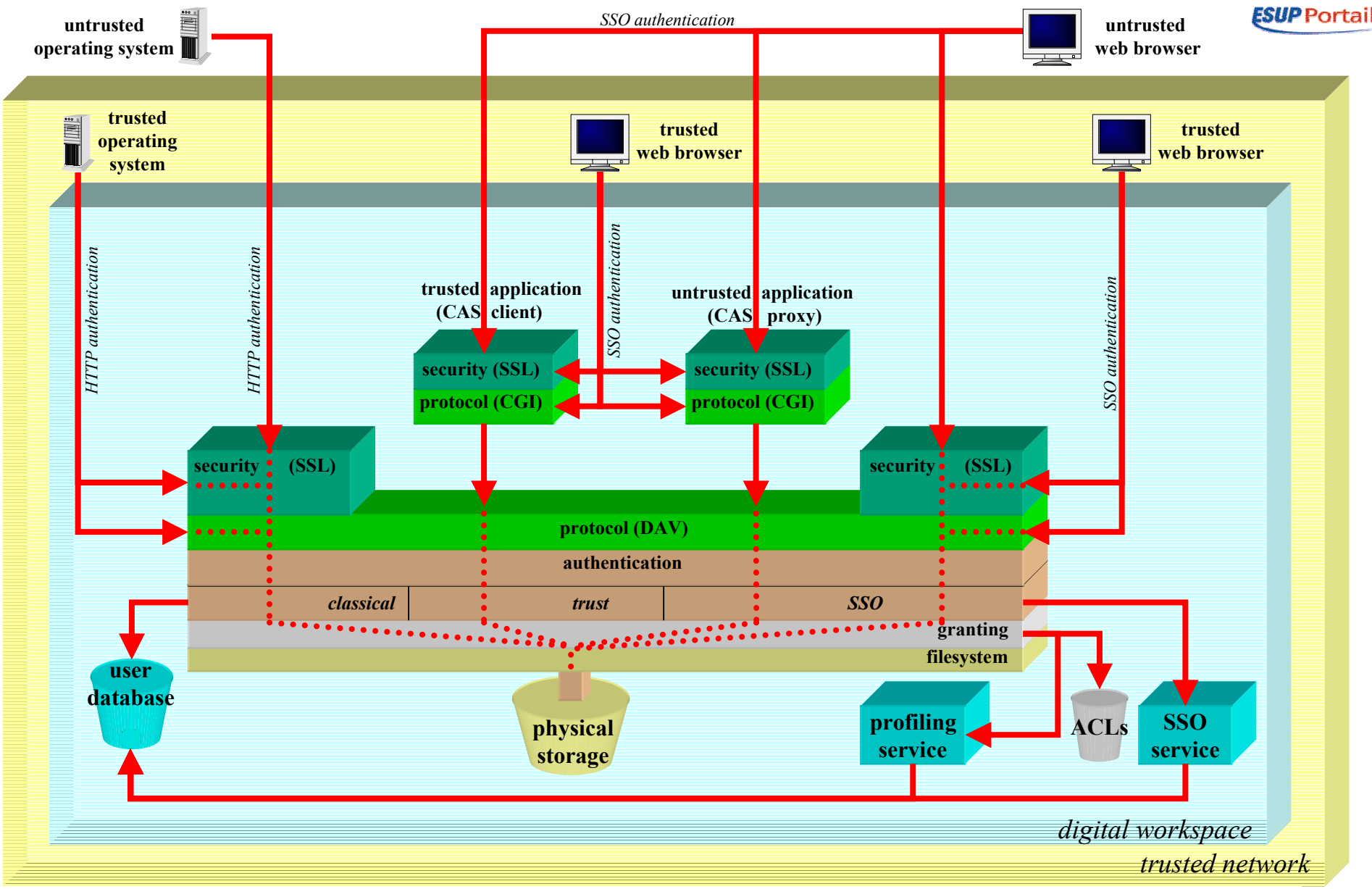
- L'authentification est gérée selon la provenance des requêtes
  - système d'exploitation
  - application de confiance
  - application autre
  - navigateur web (cf plus loin)



- L'autorisation est une couche logique (module ou service) qui a pour but de répondre à la question suivante :
  Tel utilisateur a-t-il le droit d'effectuer telle opération sur tel fichier/répertoire/volume ?
- Pour cela, il s'appuie sur un service d'ACL et un gestionnaire de profils (cf plus loin).

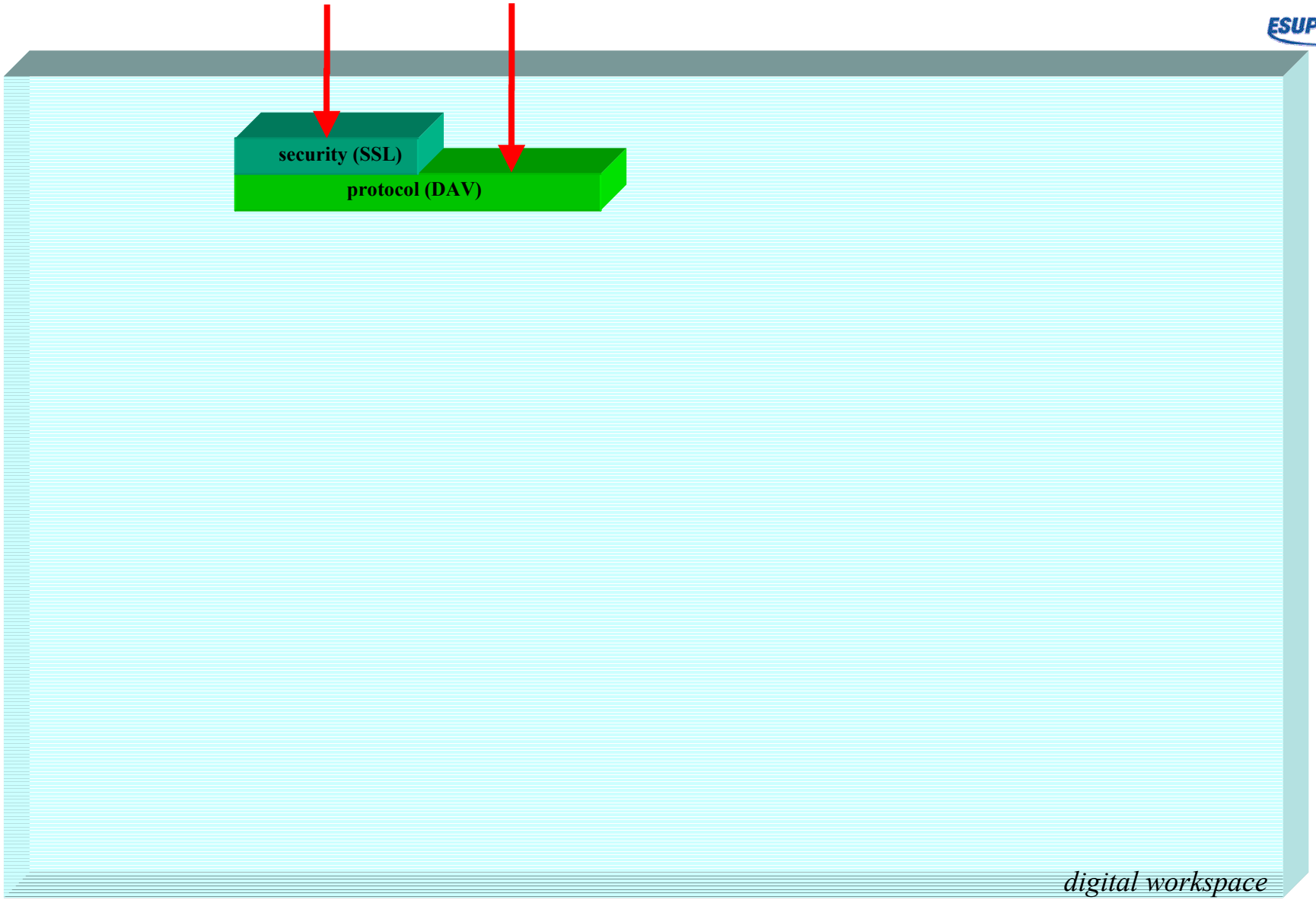


- Accès au système de fichiers
  - le système physique de stockage est abstrait par une couche logique qui permet de prendre en compte différents protocoles d'accès (NFS, CIFS, …)
  - L'accès au système de fichiers gère la problématique des quotas, en renvoyant l'erreur HTTP adéquate lors d'un dépassement de quota.

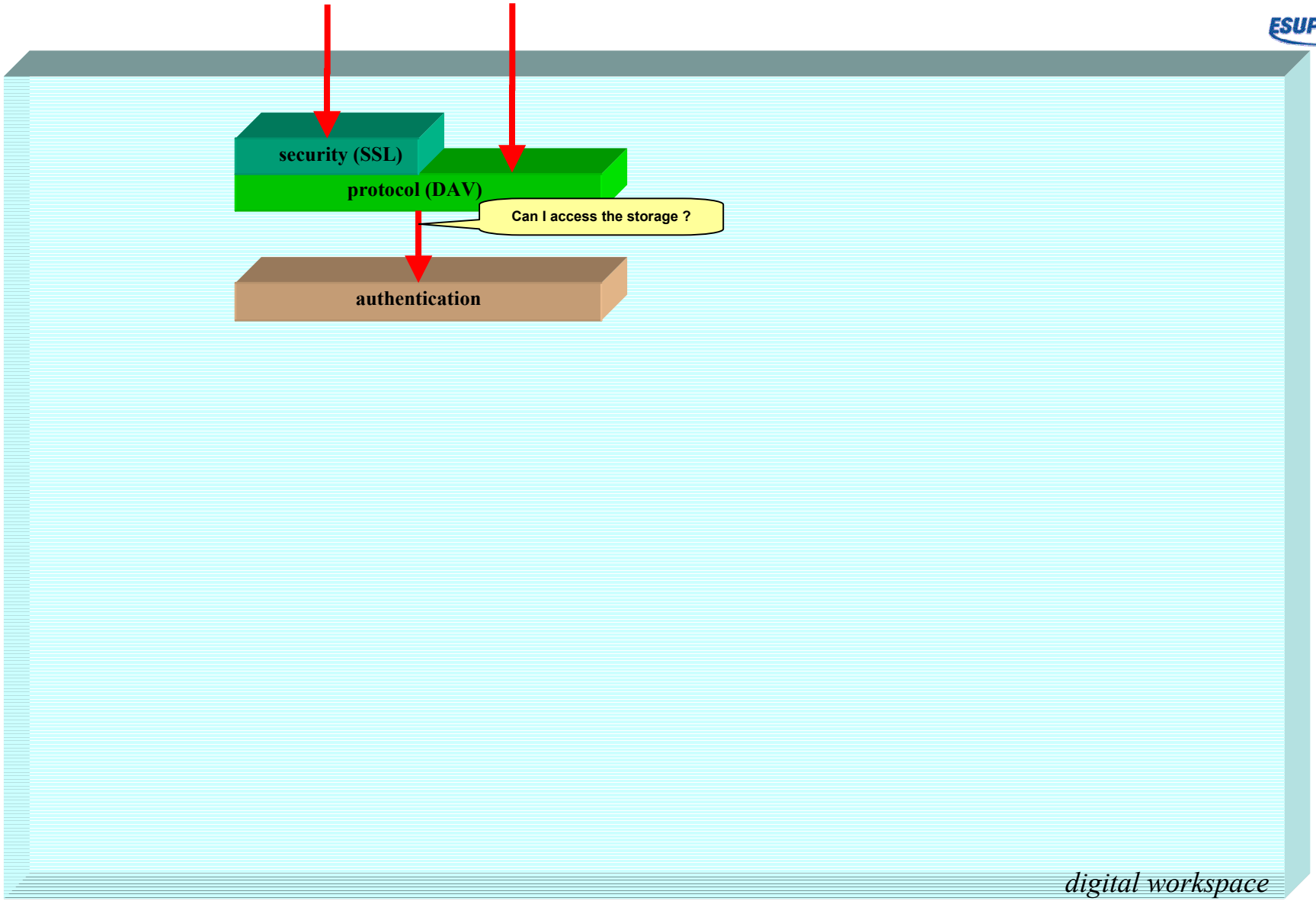


- Accès à l'espace de stockage depuis les navigateurs possible avec une authentification CAS
- Le schéma de l'espace de stockage est complet.

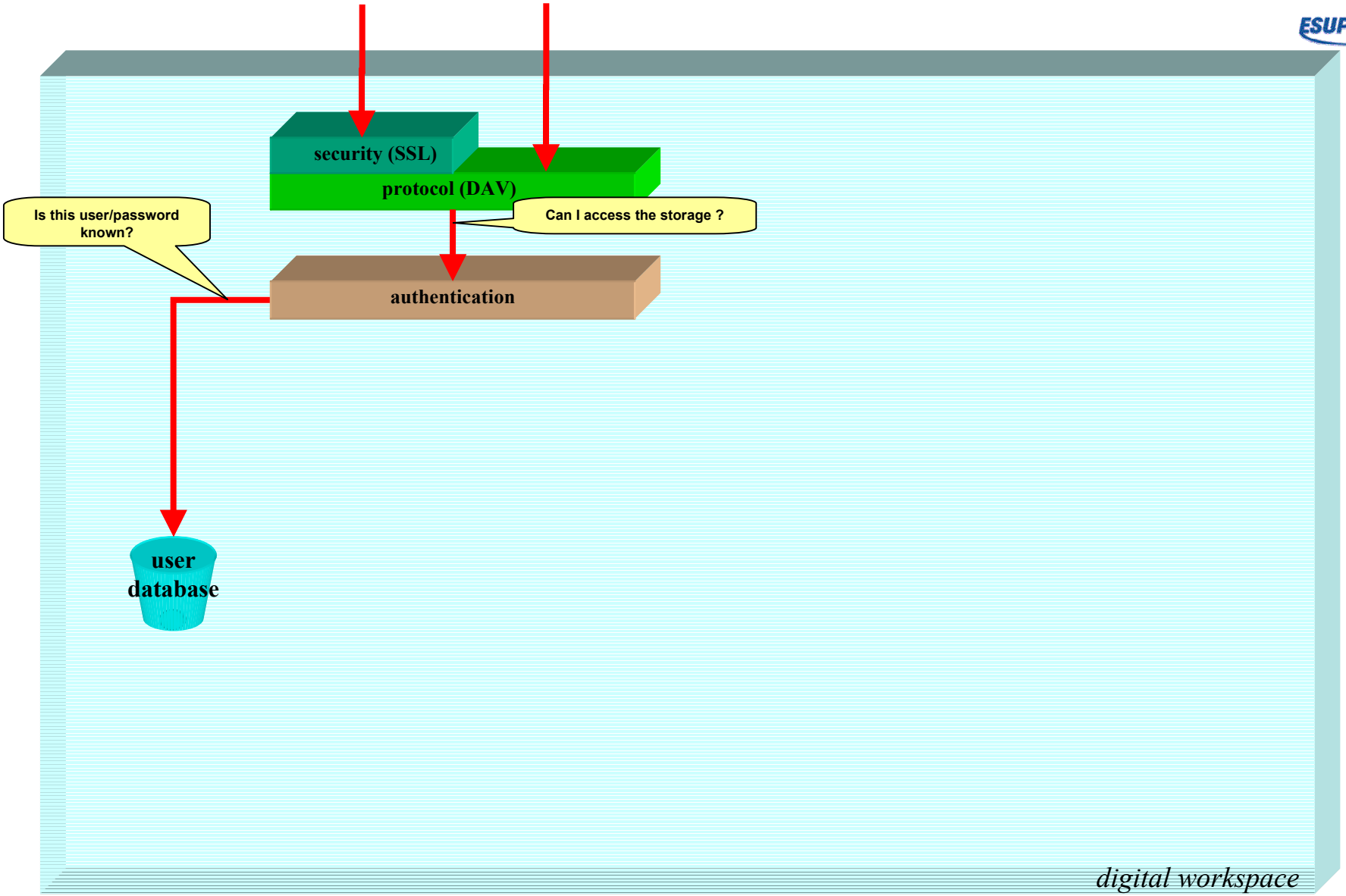
Voyons maintenant les interactions entre les différents blocs…



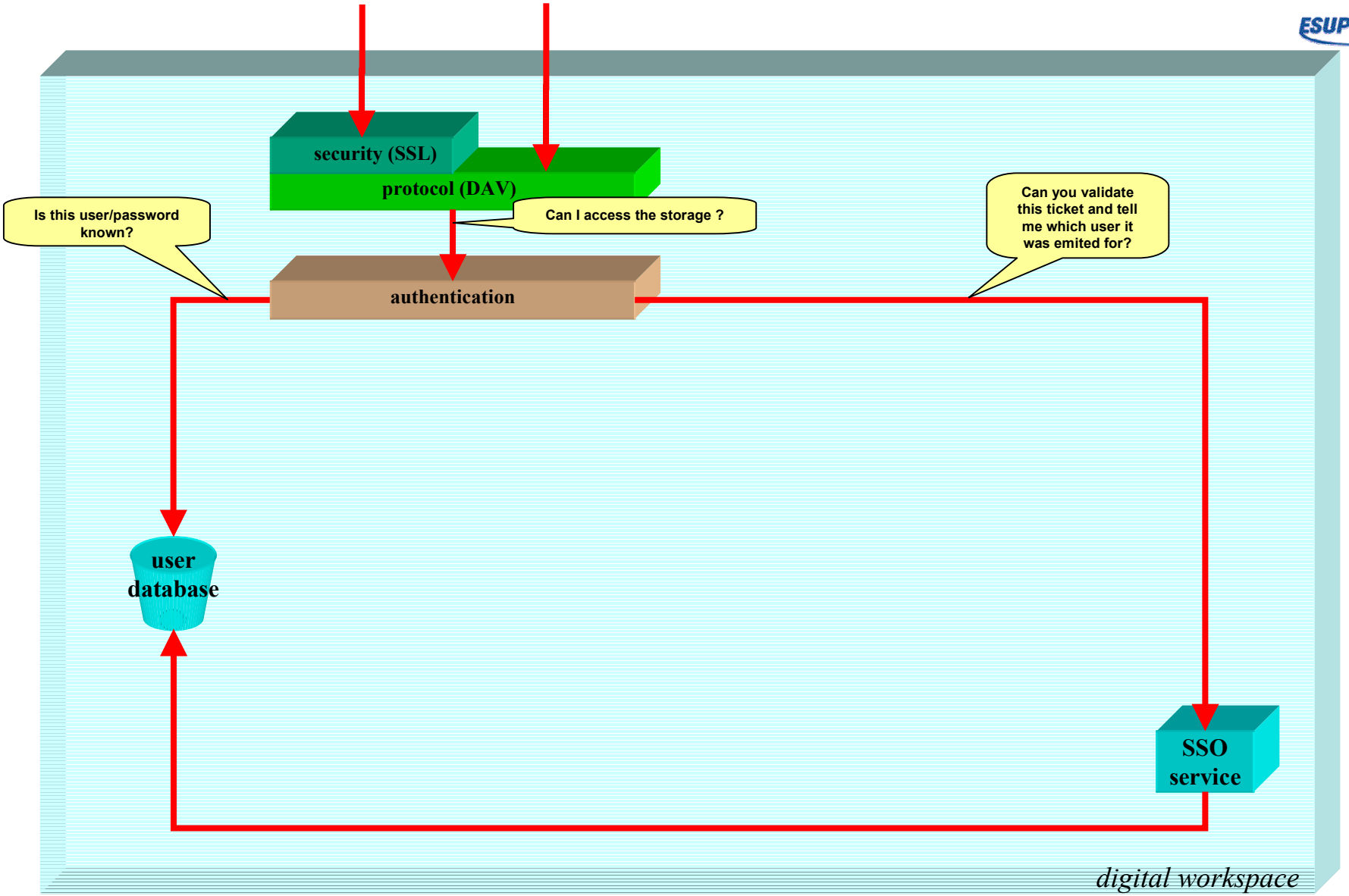
- La couche « protocole » est accédée par les navigateurs et les systèmes d'exploitation



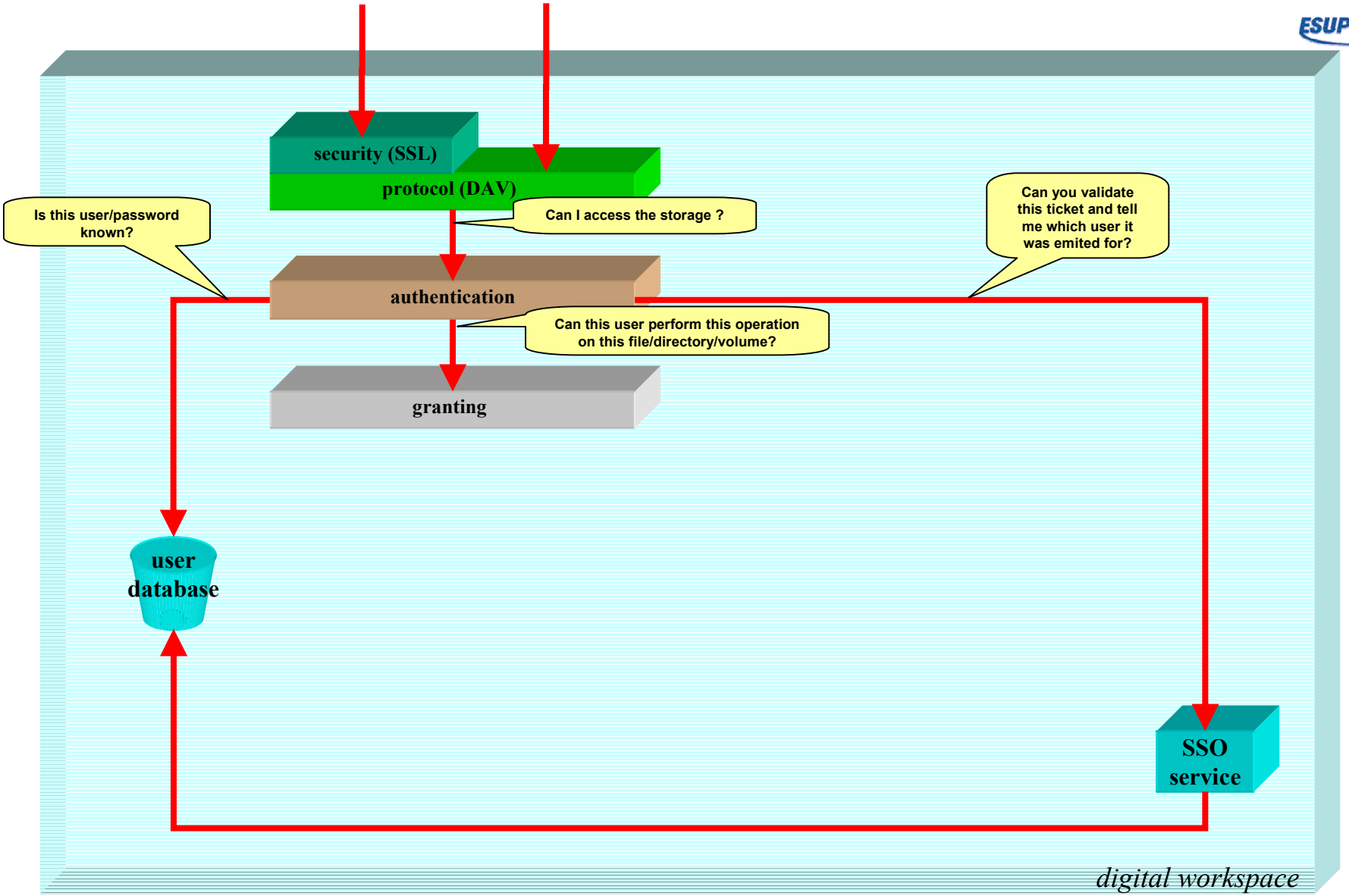
- La couche « protocole » s'appuie sur la couche « authentification » pour savoir si un utilisateur peut accéder à l'espace de stockage.



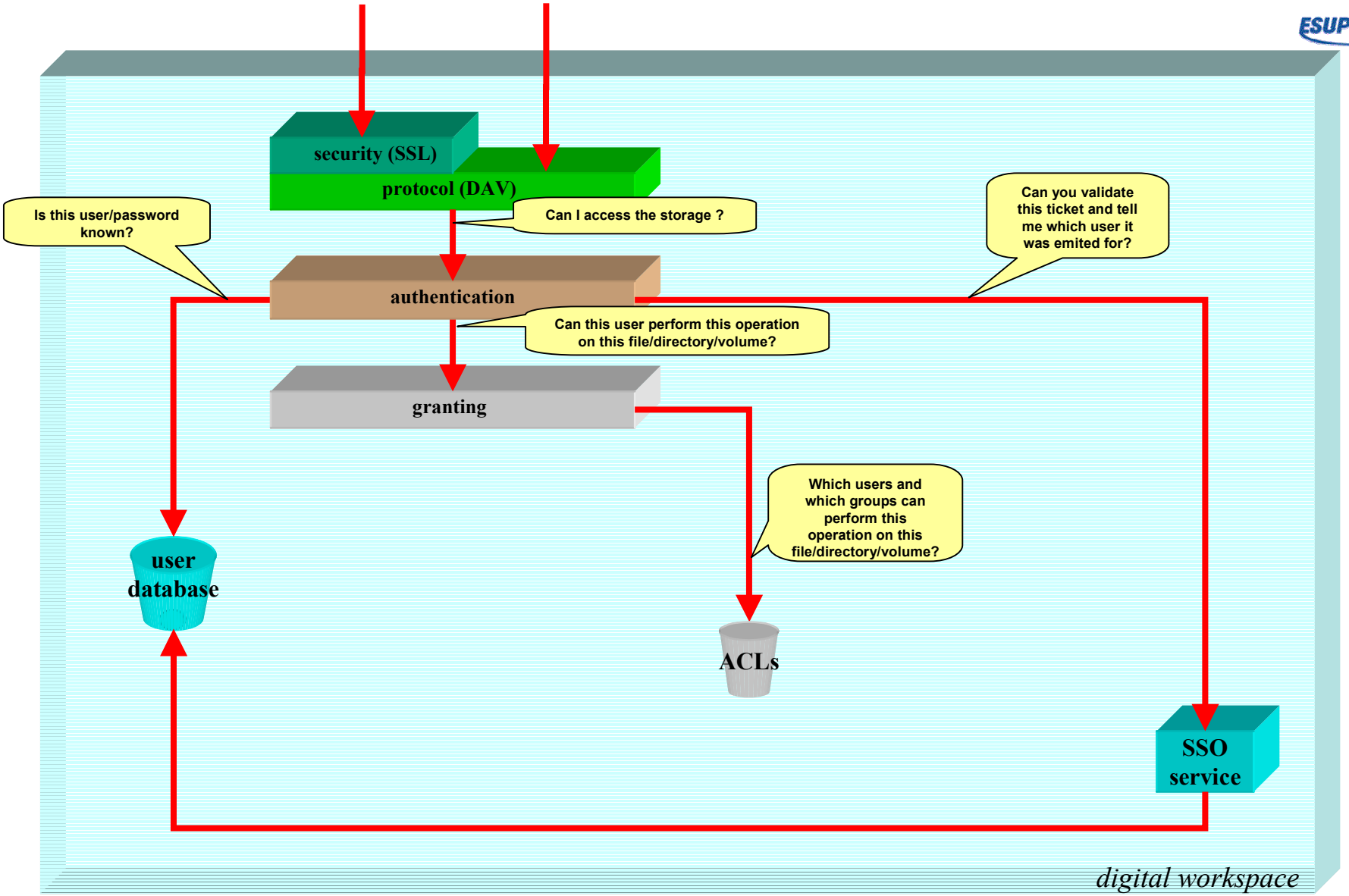
- La couche « authentification » s'appuie sur le référentiel utilisateur pour valider les accès des systèmes d'exploitation…



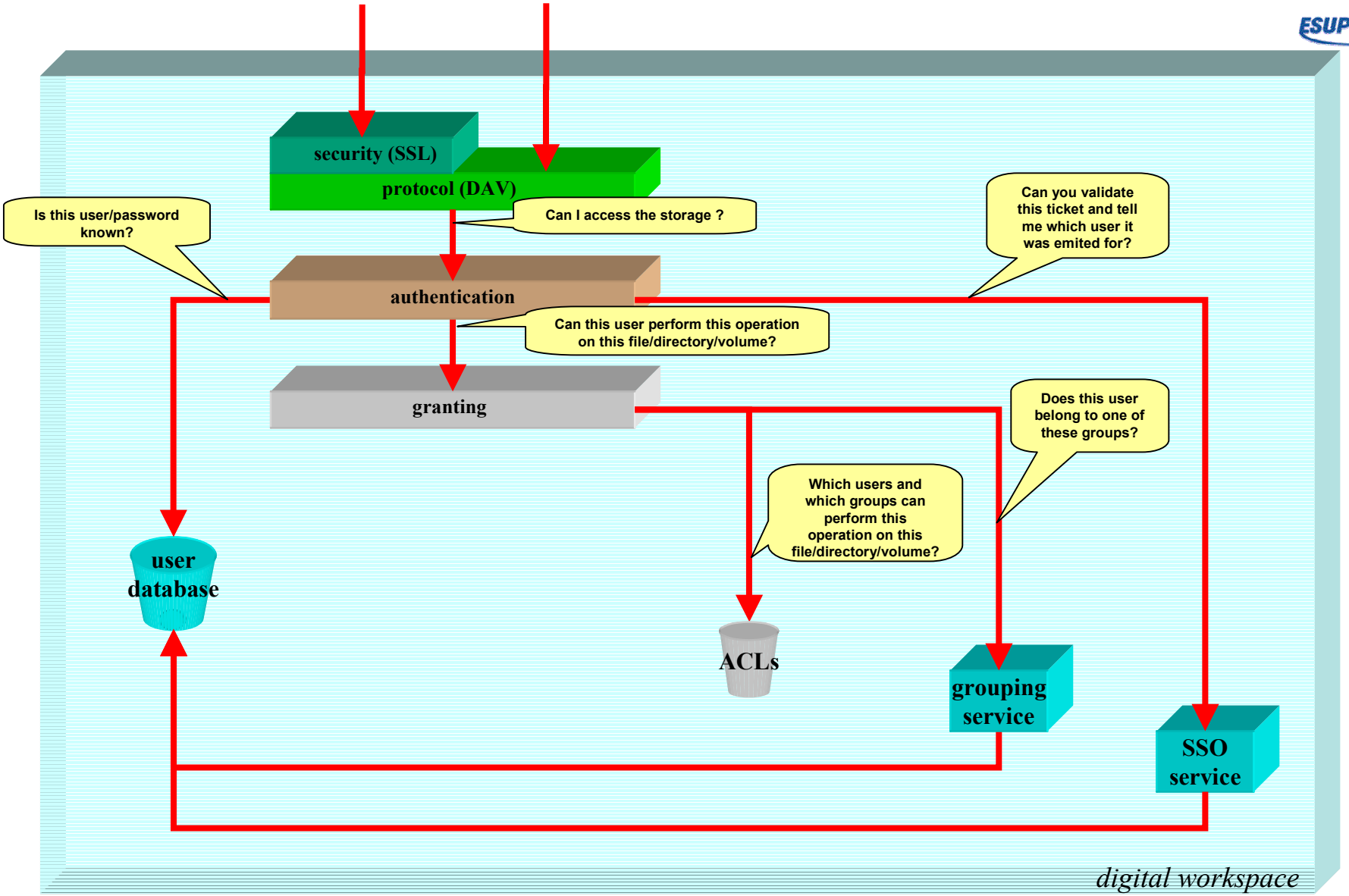
- …et sur le service SSO pour valider les tickets CAS des applications clientes et des navigateurs.



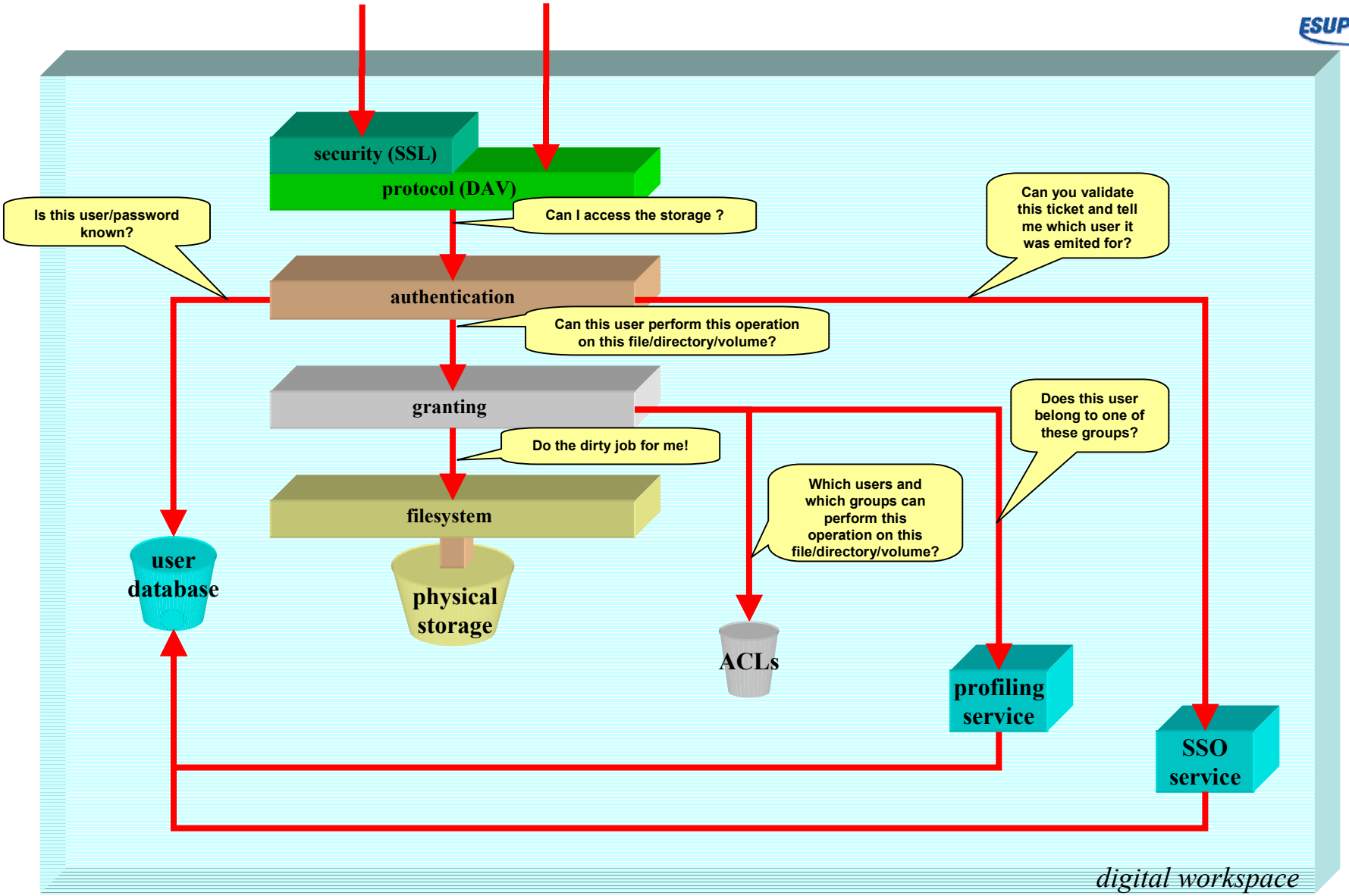
- La couche « authentification » s'appuie sur la couche « autorisation » pour déterminer si un utilisateur peut effectuer une opération sur un fichier/répertoire/volume particulier.



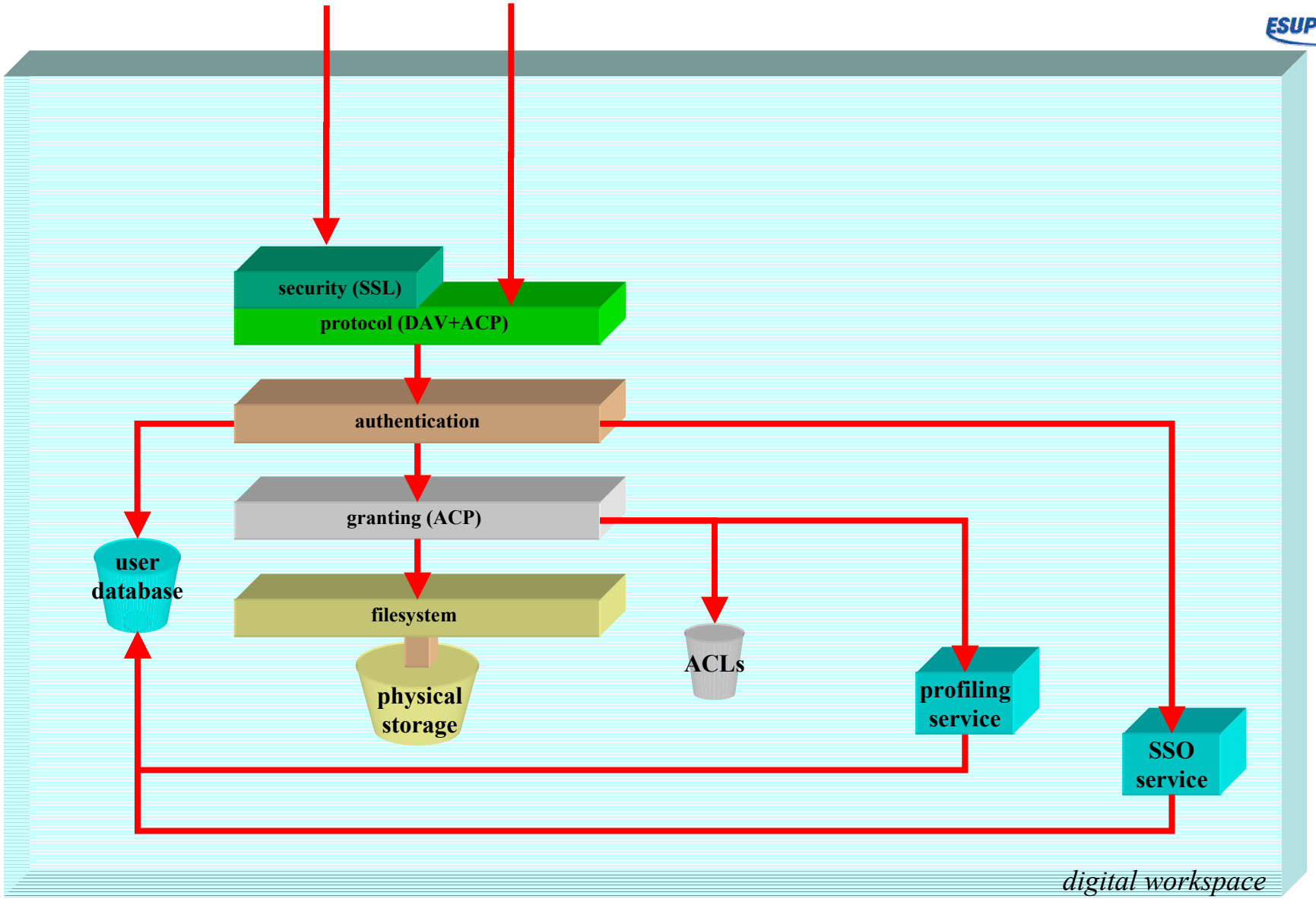
- La couche « autorisation » s'appuie sur un système d'ACL (Access Control List) pour déterminer quels utilisateurs/groupes d'utilisateurs ont le droit d'effectuer l'opération voulue sur le fichier/répertoire/volume voulu…



- … et sur un gestionnaire de profils pour déterminer si l'utilisateur connecté appartient ou non aux groupes autorisés.

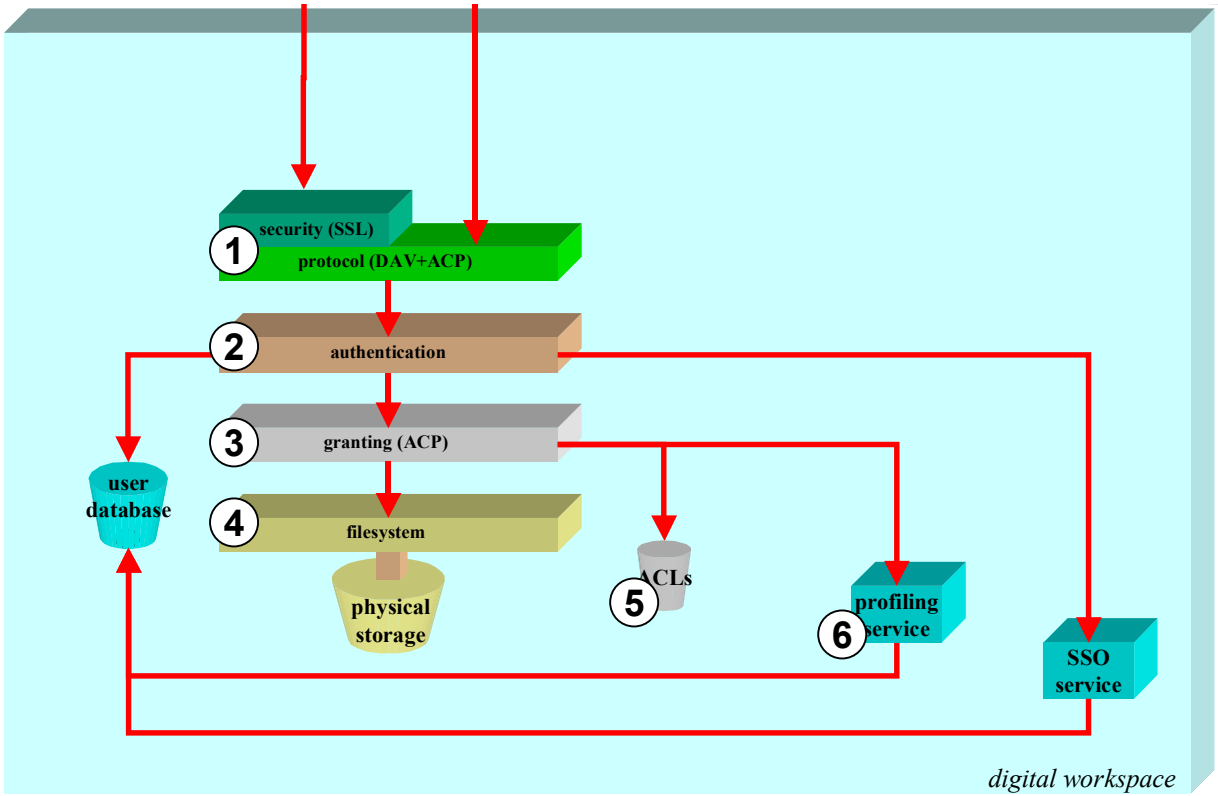


- Finalement, la couche « autorisation » s'appuie sur la couche « système de fichiers » pour lui laisser faire le sale boulot.



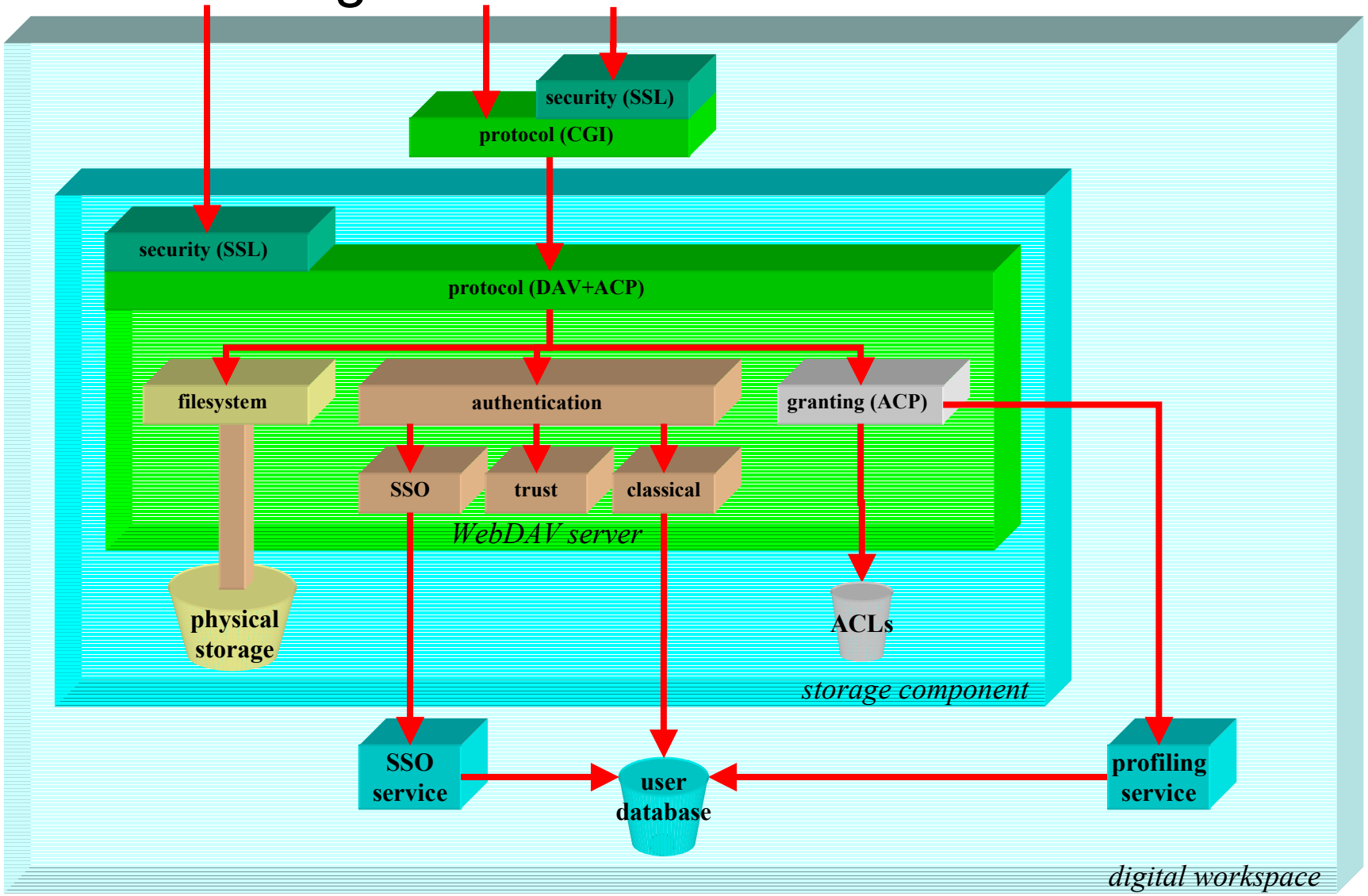
- On peut maintenant résumer tout ce qu'il faut pour mettre en œuvre l'espace de stockage.

Ce qu'il faut pour mettre en œuvre l'espace de stockage



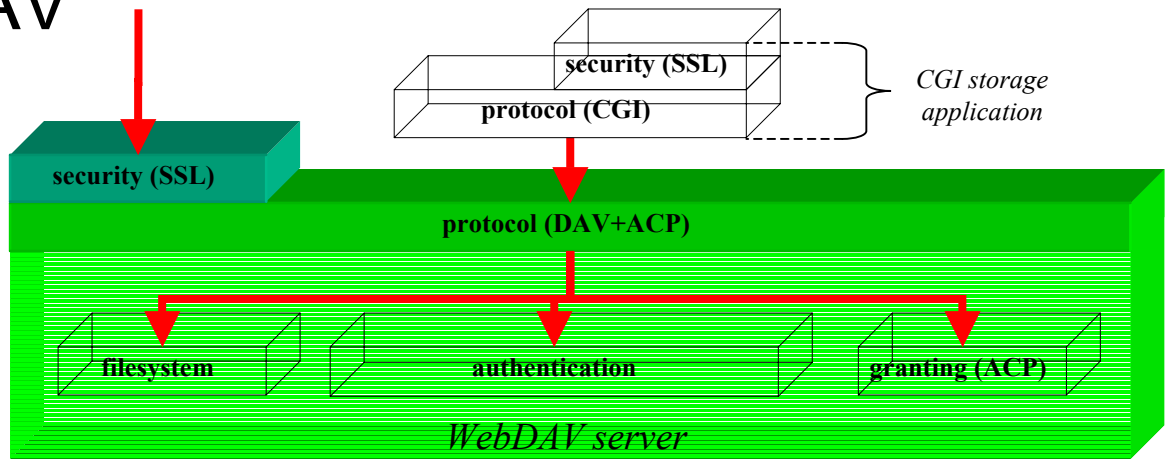
1. Un serveur WebDAV
2. Un module d'authentification
3. Un module d'autorisation
4. Une abstraction du système de fichiers
5. Un système d'ACL
6. Un gestionnaire de profils

Architecture logicielle



- Les blocs décrits dans les schémas précédents ne sont que des blocs logiques, décrivant essentiellement les flux d'informations au sein de l'espace de stockage
- Le schéma ci-dessus décrit l'espace de stockage en terme de briques logicielles
  - Les blocs « système de fichiers », « authentification » et « autorisation » sont à considérer comme des modules du serveur WebDAV
- Voyons maintenant en détail chaque brique logicielle

Le serveur WebDAV



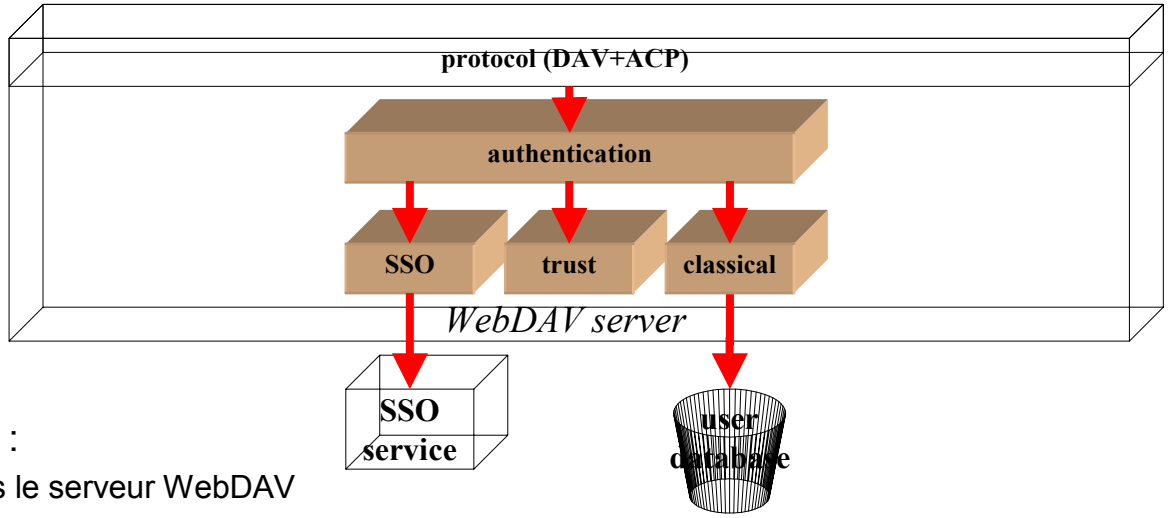
- Fonctionnalités attendues :
  - WebDAV (selon RFC 2518 pour pouvoir être compatible avec les systèmes d'exploitation et les navigateurs)
    - Note : les extensions de versioning (RFC 3253) ne seront très certainement pas prises en compte (cf http://www.webdav.org/specs/).
  - WebDAV ACP (Access Control Protocol, selon http://www.webdav.org/acl/)
  - SSL pour la confidentialité
  - Doit être suffisamment modulaire pour s'appuyer sur :
    - Un module d'authentification
    - Un module d'autorisation
    - Un module d'accès au système physique de fichiers
  - Doit pouvoir être distribué pour la montée en charge et la redondance

- Remontées d'erreur :
  - 500 (Internal server error) en cas d'incident ou erreur de protocole

- Pistes :
  - Un serveur J2EE existant

- Remarques :
  - Le serveur Webdav est nécessaire dès la première version

Le module d'authentification

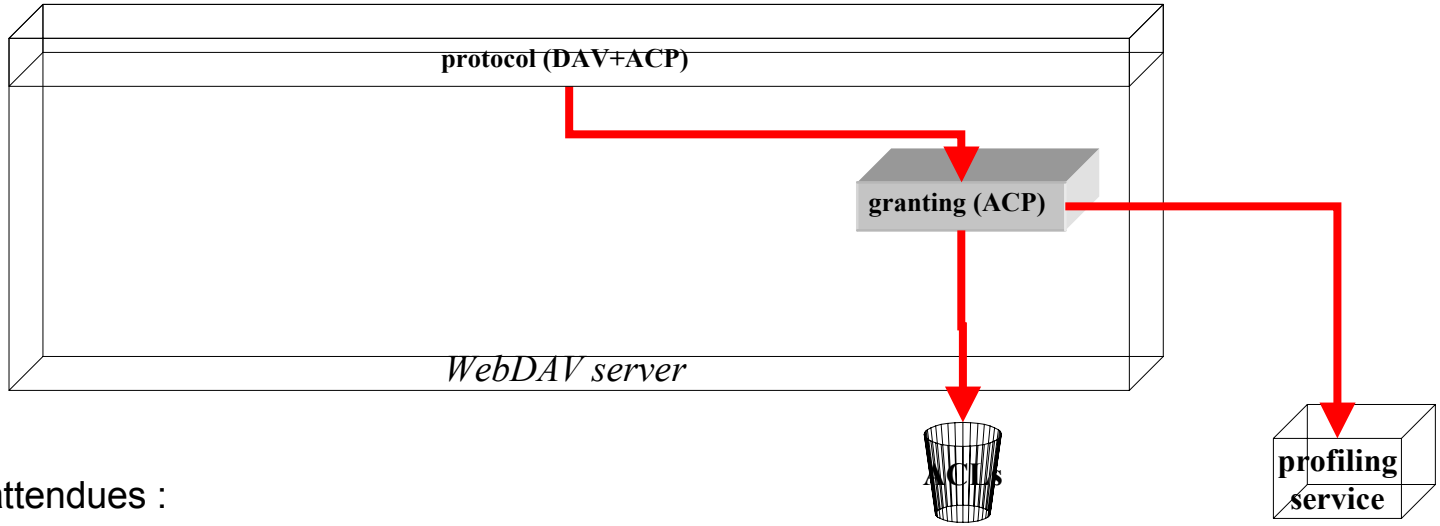


- Fonctionnalités attendues :
  - Doit être intégrable dans le serveur WebDAV
  - Doit répondre à la question « l'accès à l'espace de stockage est-il possible pour ce client ? »
  - Doit différencier les clients pour leur appliquer des contrôles différents pour :
    - Directement sur un référentiel utilisateur (login/password)
    - Sur un serveur CAS (ST ou PT)
    - Sans contrôle pour les applications de confiance
  - Doit s'appuyer sur :
    - Le référentiel utilisateurs pour les authentifications classiques (systèmes d'exploitation)
    - Le service SSO pour les authentification SSO (navigateurs)

- Remontées d'erreur :
  - En cas d'échec :
    - 401 (Unauthorized) pour les systèmes d'exploitation et applications
    - 302 (Found) pour les navigateurs (redirection vers le serveur CAS)
  - 500 (Internal server error) en cas d'incident
  - 503 (Service unavailable) en cas d'indisponibilité (du serveur SSO ou du référentiel utilisateur par exemple)

- Pistes :
  - PAM (pas forcément très facile à brancher sur du J2EE)

Le module d'autorisation

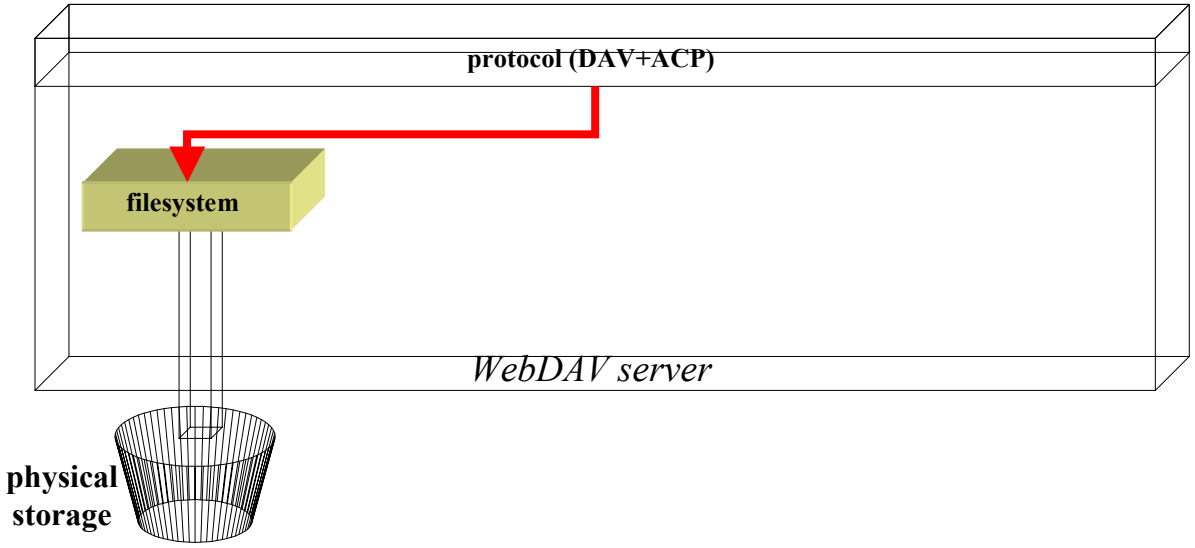


- Fonctionnalités attendues :
  - Doit être intégrable dans le serveur WebDAV
  - Doit, pour un utilisateur préalablement authentifié, répondre à la question « l'utilisateur authentifié a-t-il le droit d'effectuer une opération donnée sur un fichier/répertoire/volume ? »
  - Doit s'appuyer sur le gestionnaire de profils de l'ENT

- Remontées d'erreur :
  - 200 (OK) si l'opération est correctement effectuée
  - 403 (Forbidden) si les droits de l'utilisateur ne sont pas suffisants
  - 500 (Internal server error) en cas d'incident
  - 503 (Service unavailable) en cas d'indisponibilité (du système d'ACL ou du gestionnaire de groupes par exemple)

- Pistes :
  - S'appuyer sur un système d'ACL et un gestionnaire de groupes
    - Demande au système d'ACL « quels utilisateur ont-ils le droit d'effectuer telle opération sur tel fichier/répertoire/volume ? »
    - Demande au gestionnaire de profils, si nécessaire, « l'utilisateur authentifié appartient-il à un tel ou tel groupe ? »
    - Répond en fonction

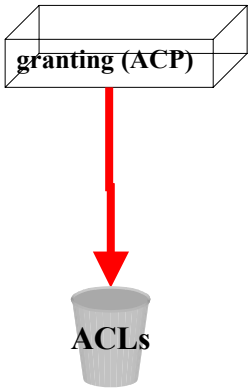
L’abstraction du système de fichiers



- Fonctionnalités attendues :
  - Doit s’intégrer dans le serveur WebDAV
  - Doit pouvoir effectuer sur un système de fichiers physique les opération de base permises par WebDAV (selon RFC 2518).

- Pistes :
  - Cette couche est essentiellement logique, car les fonctionnalités sont offertes par les systèmes d’exploitation contrôlant les ressources physiques (NFS, CIFS, …). Elle pourrait être de la responsabilité des établissements, avec un support minimal (NFS et CIFS par exemple).

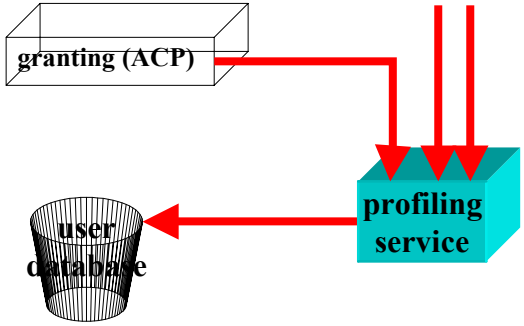
Le système d'ACLs



- Fonctionnalités attendues :
  - Doit être interrogeable par le module d'autorisation du serveur WebDAV
    - Doit répondre à la question « quels utilisateurs et quels groupes d'utilisateurs ont-ils le droit d'effectuer telle opération sur tel fichier/répertoire/volume ? »

- Pistes :
  - Si l'on veut des ACL assez riches et permettant le partage entre plusieurs utilisateurs, les droits classiques des systèmes de fichiers existants ne seront certainement pas suffisants.
  - On peut penser à une base de données contenant des entrées du type ALLOW|DENY action FOR USER|GROUP xxx ON file/directory/volume
  - La partie interrogation du système pourrait être mis en redondance

Le gestionnaire de profils

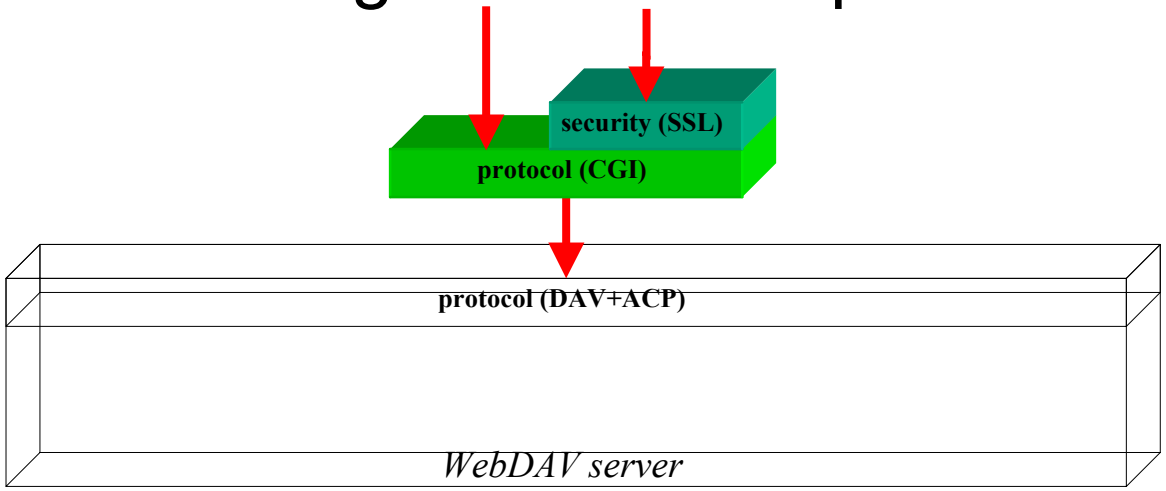


- Fonctionnalités attendues :
  - Doit répondre (au module d'autorisation de l'espace de stockage) à des questions :
    - « tel utilisateur appartient-il à tel groupe ? »
    - « tel utilisateur appartient-il à un groupe parmi plusieurs ? »
    - « à quels groupes appartient tel utilisateur ? »
  - S'appuie sur un référentiel utilisateurs (LDAP par exemple)
  - Doit pouvoir être interrogé par les autres briques de l'ENT (fonctionnalités à déterminer)

- Pistes :
  - Cette brique étant une des briques de base de l'ENT, la réflexion doit être menée au sein du projet ESUP.
  - La partie interrogation du gestionnaire pourrait être mis en redondance

- Remarque :
  - Le gestionnaire de profils fait l'objet d'une spécification indépendante.

L'application CGI de gestion de l'espace de stockage



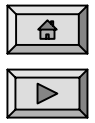
- Fonctionnalités attendues :
  - Doit accéder à l'espace de stockage à travers le protocole WebDAV
    - Fonctions traditionnelles de mise à jour de l'espace de stockage de chaque utilisateur
  - Doit implémenter les opérations de base du protocole ACP
    - Partage de fichiers entre utilisateurs, modification des ACLs, …

- Pistes :
  - Pas beaucoup pour l'instant…

Versions prévues

ESUP Portail

- Version 1 : espace de stockage personnel
  - Accès des utilisateurs à leur propre espace de stockage, à travers un canal uPortal
- Version 2 : diversification des accès
  - Version 2.0 : accès sécurisé par les systèmes d'exploitations, navigateurs et clients WebDAV à l'aide d'une authentification user/password basée sur le référentiel utilisateur (typiquement LDAP)
  - Version 2.1 : accès sécurisé par les navigateurs et les applications à travers une authentification SSO
- Version 3 : passage à une plate-forme J2EE
- Version 4 : partage de données
  - Version 4.0 : gestion d'ACLs pour des utilisateurs
  - Version 4.1 : gestion d'ACLs pour des groupes



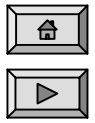
Version 1 (fonctionnalités)

- Clients
  - Seule une application CGI particulière (l'application de gestion de l'espace de stockage) est autorisée à accéder à l'espace de stockage
    - C'est une application de confiance, client CAS, partie de l'ENT, qui peut accéder à l'espace de stockage de manière non sécurisée
  - Les accès depuis d'autres applications CGI, les systèmes d'exploitation et les navigateurs ne sont pas autorisés

- Authentification
  - L'application des gestion de l'espace étant une application de confiance, s'appuyant sur le SSO, elle ne nécessite pas d'authentification
  - En conséquence, le service SSO n'est utilisé que par l'application CGI de gestion de l'espace de stockage, et plus par l'espace de stockage lui-même

- Autorisation
  - On s'appuie sur un gestionnaire d'ACLs basique
    - Un utilisateur a tous les droits sur son espace personnel
    - Un utilisateur n'a aucun droit sur le reste de l'espace de stockage
    - Les ACLs ne sont pas modifiables
  - En conséquence, le gestionnaire de profils n'est pas nécessaire, de même que le référentiel utilisateurs.

- Système de fichiers
  - On s'appuie sur un montage d'un système de fichiers physique (par NFS ou CIFS) sur lequel l'espace de travail :
    - A tous les droits
    - A un accès exclusif

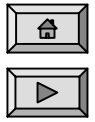


Version 1 (choix de mise en œuvre)

- La création et la destruction de l'espace de stockage est assurée en amont par les établissements.

- Client d'accès à l'espace de stockage
  - Comme prévu, la version V1 est minimale et permet aux utilisateurs de gérer leur propre espace de stockage, et pas plus.
  - La gestion de l'espace de stockage se fait par une seule application, un canal de uPortal. S'il se révèle impossible de récupérer un canal existant (cf plus loin), il faudra en développer un, ou à défaut une application CGI.
  - Ce canal est une application de confiance vis-à-vis de l'espace de stockage ; il lui transmet une identification (l'uid de l'utilisateur et un mot de passe bidon) par une authentification HTTP basique.
  - L'URL principale d'accès à l'espace de stockage est http://storage.univ.fr/users/uid pour se garder la possibilité d'utiliser d'autres URLs d'accès, par exemple http://storage.univ.fr/projects/project.

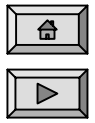
- Serveur de stockage
  - Les parties authentification/autorisation et accès WebDAV sont dissociées comme suit :
  - Un frontal Apache prend en charge l'authentification, le contrôle d'accès et la ré-écriture d'URLs, en utilisant :
    - mod_auth_anon pour l'identification (authentification anonyme, peut-être à modifier un peu pour qu'il accepte n'importe quel mot de passe) ;
    - mod_rewrite ou les .htaccess (gérés en amont par les administrateurs de l'espace de stockage à la création des espaces des utilisateurs) pour le contrôle d'accès ;
    - mod_user_dir ou mod_rewrite pour la transformation d'URLs, c'est-à-dire le mapping sur l'espace physique (/users/uid devient par exemple /users/u/ui/uid).
  - Les accès WebDAV proprement dits sont pris en charge par un serveur Apache couplé à mod_dav. Si les tests avec mod_dav ne s'avèrent pas fonctionnels (sans parler de performances), un autre serveur WebDAV pourra être envisagé, mais aucun obstacle n'est vu dans cette solution, rapide à mettre en œuvre.



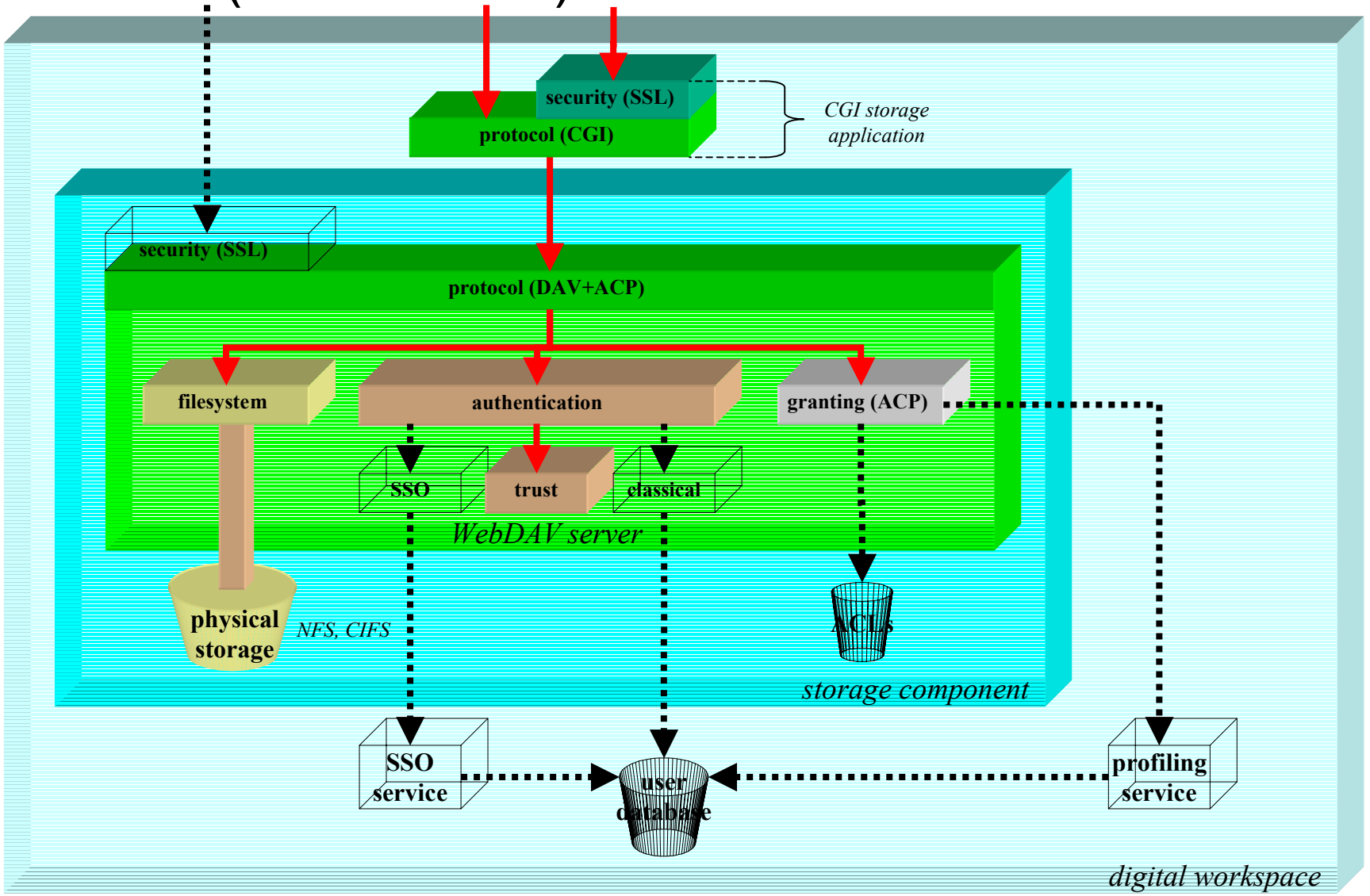
Version 1 (travail à réaliser)

- Client d'accès à l'espace de stockage
  - Prise de contact avec le développeur du canal WebDAV pour demander le droit d'utiliser et d'adapter dans le cadre d'ESUP-Portail
    - Shijia
  - Patch du canal WebDAV pour le faire coller à notre besoin en ne gardant, peut-être, que l'interface utilisateur
    - Pas de personne affectée, dépend du retour obtenu par Shijia
  - S'il ne nous est pas possible d'utiliser le canal WebDAV il nous faudra le développer totalement.

- Serveur de stockage
  - Test mod_auth_anon pour l'identification
    - Vincent
  - mod_rewrite ou .htaccess pour le contrôle d'accès (l'utilisateur requête bien son espace de stockage et pas celui du voisin)
    - Vincent (Pierre regarde aussi mod_rewrite)
  - mod_user_dir ou mod_rewrite pour la transformation d'URI : passer de /users/uid (répertoire virtuel) à /esup/storage/users/u/ui/uid (répertoire physique)
    - Vincent (Pierre regarde aussi mod_rewrite)



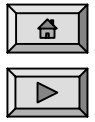
Version 1 (architecture)



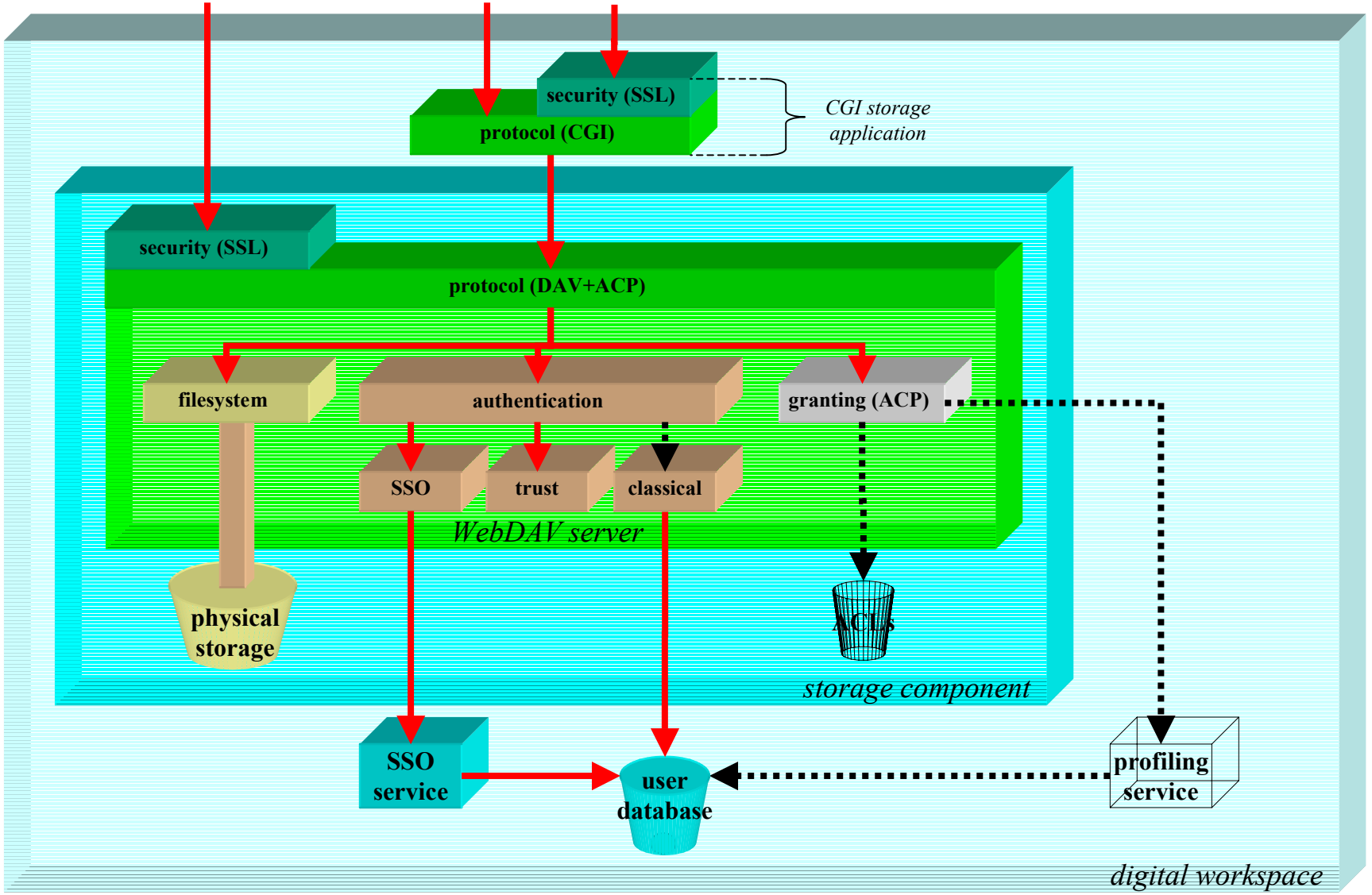
Version 2

ESUP Portail

- Nouvelles fonctionnalités
  - Accès sécurisé par les systèmes d'exploitations, navigateurs et clients WebDAV à l'aide d'une authentification user/password basée sur le référentiel utilisateur (typiquement LDAP)
  - Accès sécurisé par les navigateurs et les applications à travers une authentification SSO
- Travail à réaliser
  - CAS-ifier le serveur WebDAV (client CAS seulement)
  - Sécuriser le serveur WebDAV (SSL)



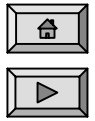
Version 2


security (SSL)
protocol (CGI)
CGI storage application
security (SSL)
protocol (DAV+ACP)
filesystem
authentication
granting (ACP)
SSO
trust
classical
WebDAV server
physical storage
ACLs
storage component
SSO service
user database
profiling service
digital workspace

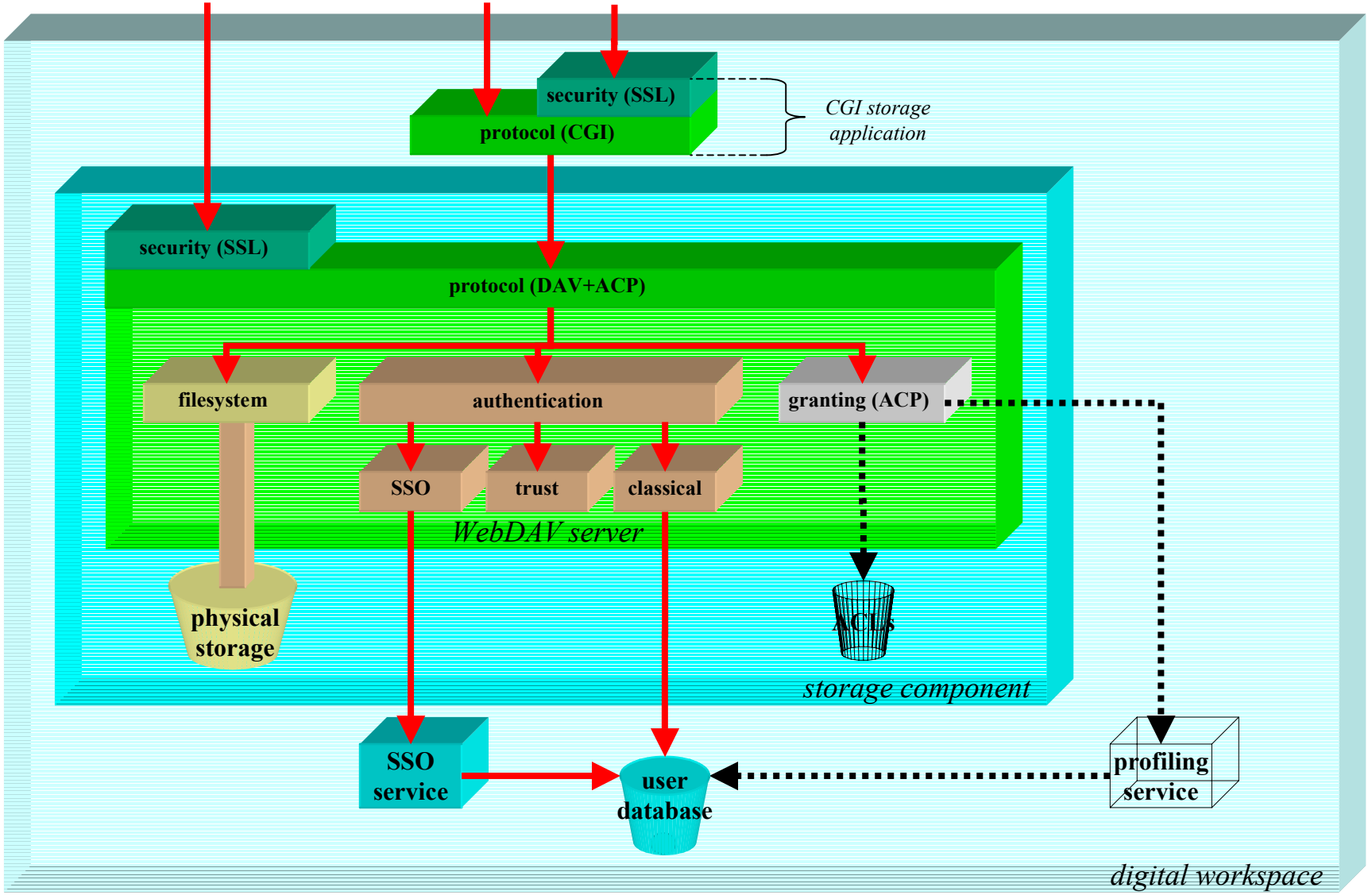
Version 3

ESUP Portail

- Nouvelles fonctionnalités
  - Aucune
- Travail à réaliser
  - Passer à un serveur WebDAV J2EE



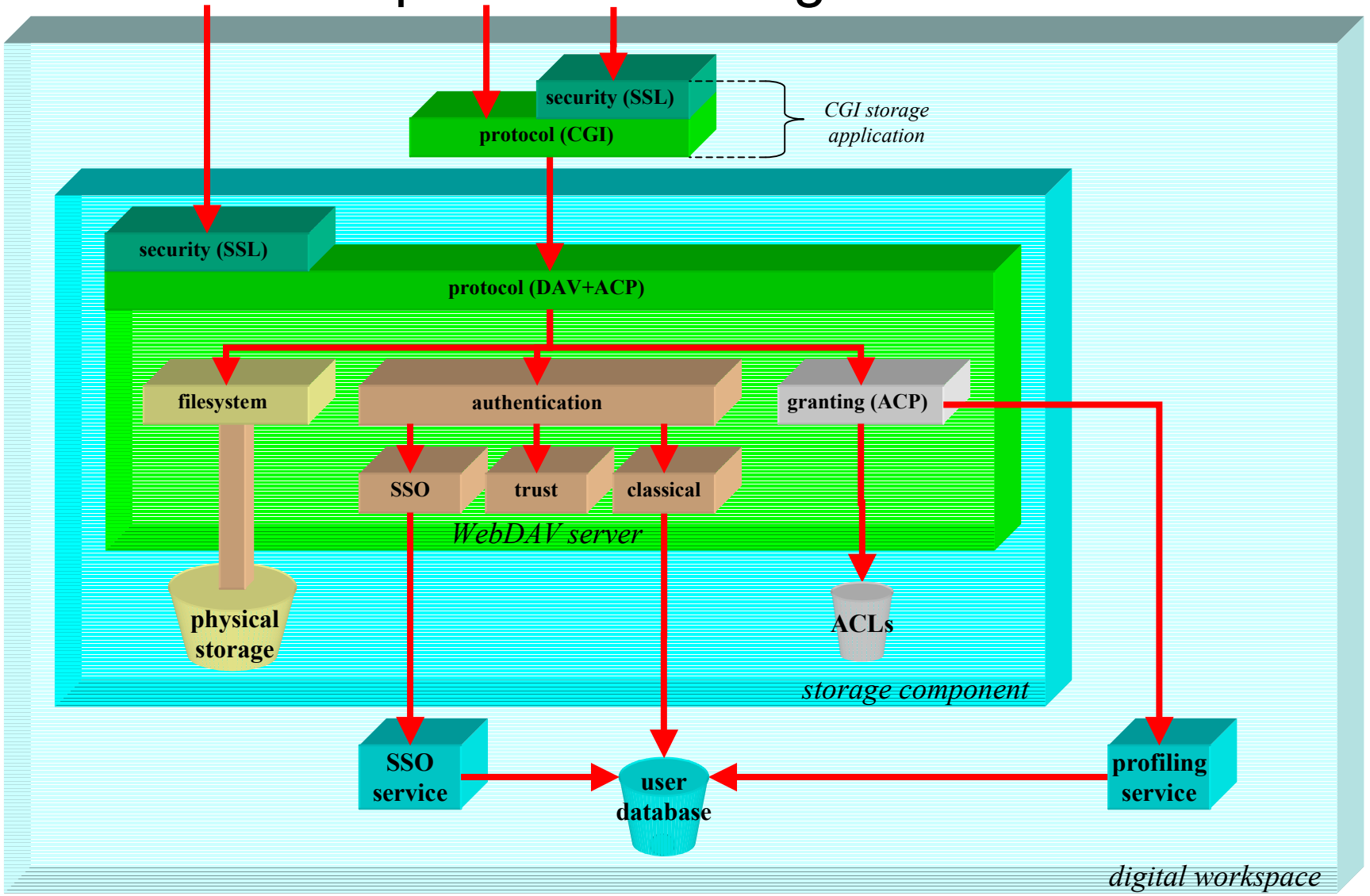
Version 3


security (SSL)
protocol (CGI)
CGI storage application
security (SSL)
protocol (DAV+ACP)
filesystem
authentication
granting (ACP)
SSO
trust
classical
WebDAV server
physical storage
ACLs
storage component
SSO service
user database
profiling service
digital workspace

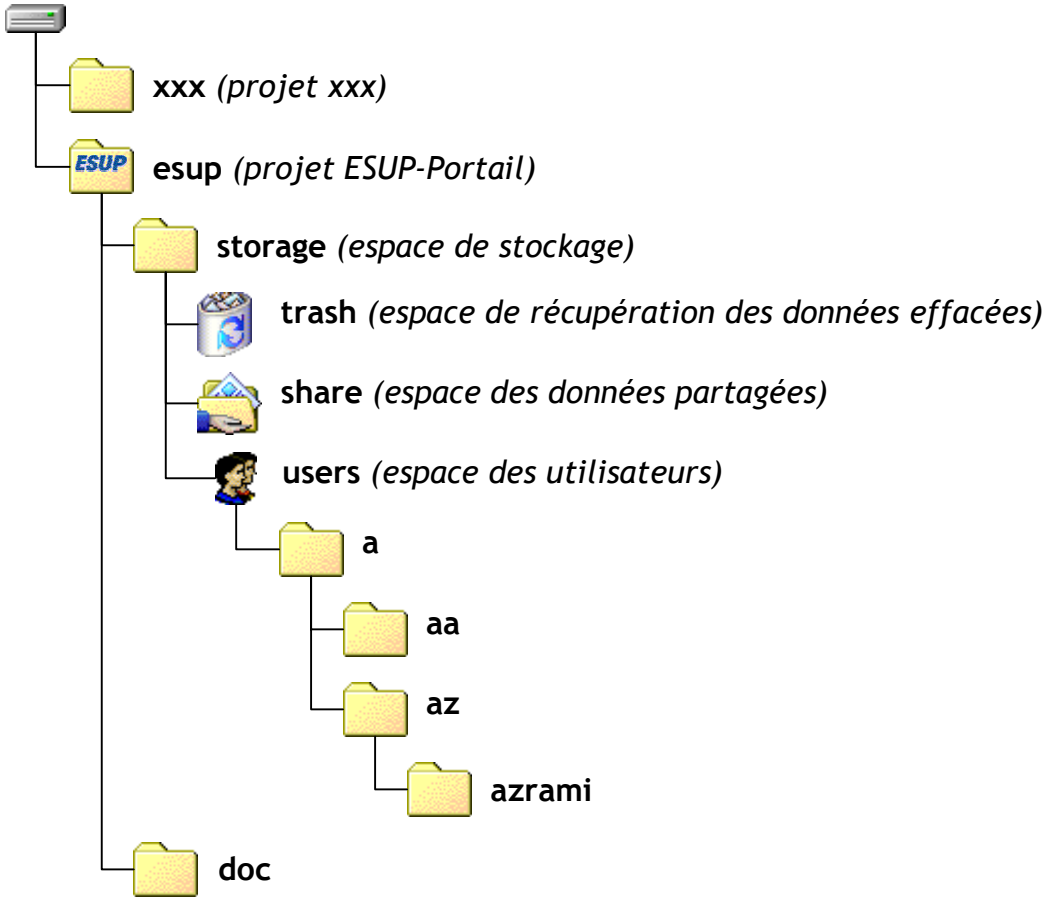
Version 4 de l’espace de stockage

- Nouvelles fonctionnalités
  - Prise en compte de la notion de partage
- Travail à réaliser
  - Ajouter le système d’ACLs
  - Connecter module d’autorisations sur le gestionnaire de profils et le système d’ACLs

Version 4 de l'espace de stockage



Adressage logique de l'espace physique de stockage



- Exemple d'adressage logique de l'espace d'un utilisateur : /esup/storage/share/users/a/az/azrami
- Accès WebDAV : http[s]://storage.univ.fr/users/azrami, ou http[s]://storage.univ.fr/~azrami

Ce qui pourrait être la feuille de route du groupe 2F

- Version 1 : espace de stockage personnel
  - Janvier 2004
- Version 2 : diversification des accès
  - Février 2004
- Version 3 : passage à une plate-forme J2EE
  - Avril 2004
- Version 4 : partage de données
  - Juillet 2004