



SIDES : examens sur tablettes (retour d'expérience)

Pascal AUBRY
DSI de l'université de Rennes 1



Le projet SIDES

- **Système Informatisé et Distribué d'Évaluation en Santé**
- **Objectif : passage de l'ECN sur tablettes en mai 2016**



- **Examen très sensible**
 - ECN = Examen Classant National
 - 6^e année de médecine, choix de la spécialisation
 - Enjeux financiers, risques juridiques



- **Richesse de nouveaux médias**
 - Images, bandes sonores, vidéos, ...
- **Progressivité des examens**
 - Impossibilité pour les candidats de voir une question tant qu'ils n'ont pas répondu aux questions précédentes
- **Réduction des temps/coûts de correction**
- **Réutilisation des sujets**
 - À l'aide de bases de connaissances
- **Meilleure discrimination des étudiants**



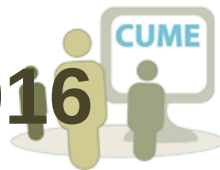
- **Les informaticiens en première ligne**
- **Maîtrise d'OuvrAge**
 - Le service de scolarité de l'UFR Médecine
- **Maîtrise d'Œuvre**
 - Les informaticiens de la DSI
- **Utilisateurs**
 - Les enseignants et les étudiants
- **Aspects sécurité**
 - Groupe RSSI (RSSI et suppléants)
- **Importance de l'Assistance à Maîtrise d'Ouvrage**
 - Coordination de tous les acteurs



- **Ingénieurs Système/Réseau**
 - Conception d'une architecture robuste et fiable
- **Architectes du Système d'Information**
 - Mise en œuvre les procédures d'inscription
- **Informaticiens de proximité**
 - Exploitation d'un nouveau parc
 - Exigence de disponibilité



- **Calendrier très contraint**
 - Septembre 2013 : remontée du projet à la DSI
 - Décembre 2013 : prise en charge par la DSI
 - Mars 2014 : mise à niveau de l'infrastructure Wifi
 - Mai 2014 : tests
 - Juin 2014 : examens blancs
 - Novembre 2014 : examens facultaires
 - Janvier 2015 : examens facultaires
 - Juin 2015 : audit CNG
 - Novembre 2015 : pré-labellisation
 - Avril 2016 : labellisation
- **Passage de l'ECN sur tablettes : mai 2016**



Les tablettes

- **iPad Retina**
 - RAM 16Go, 802.11a/b/g/n
 - Non choisies par la DSI
 - Apple seul constructeur homologué



Gestion des tablettes

- **Configuration**

- Bridage au strict nécessaire
 - Connexion automatique au réseau SIDES
 - Navigateur avec onglets
 - Gestion de l'alimentation

- **Outils**

- Aujourd'hui avec iConfigurator
 - Génération d'un master
 - Déploiement « en masse » (par USB)
- Demain avec JamF (Casper suite)
 - Enrôlement sur un serveur Apple
 - Définition de politiques

- **Utilisation**

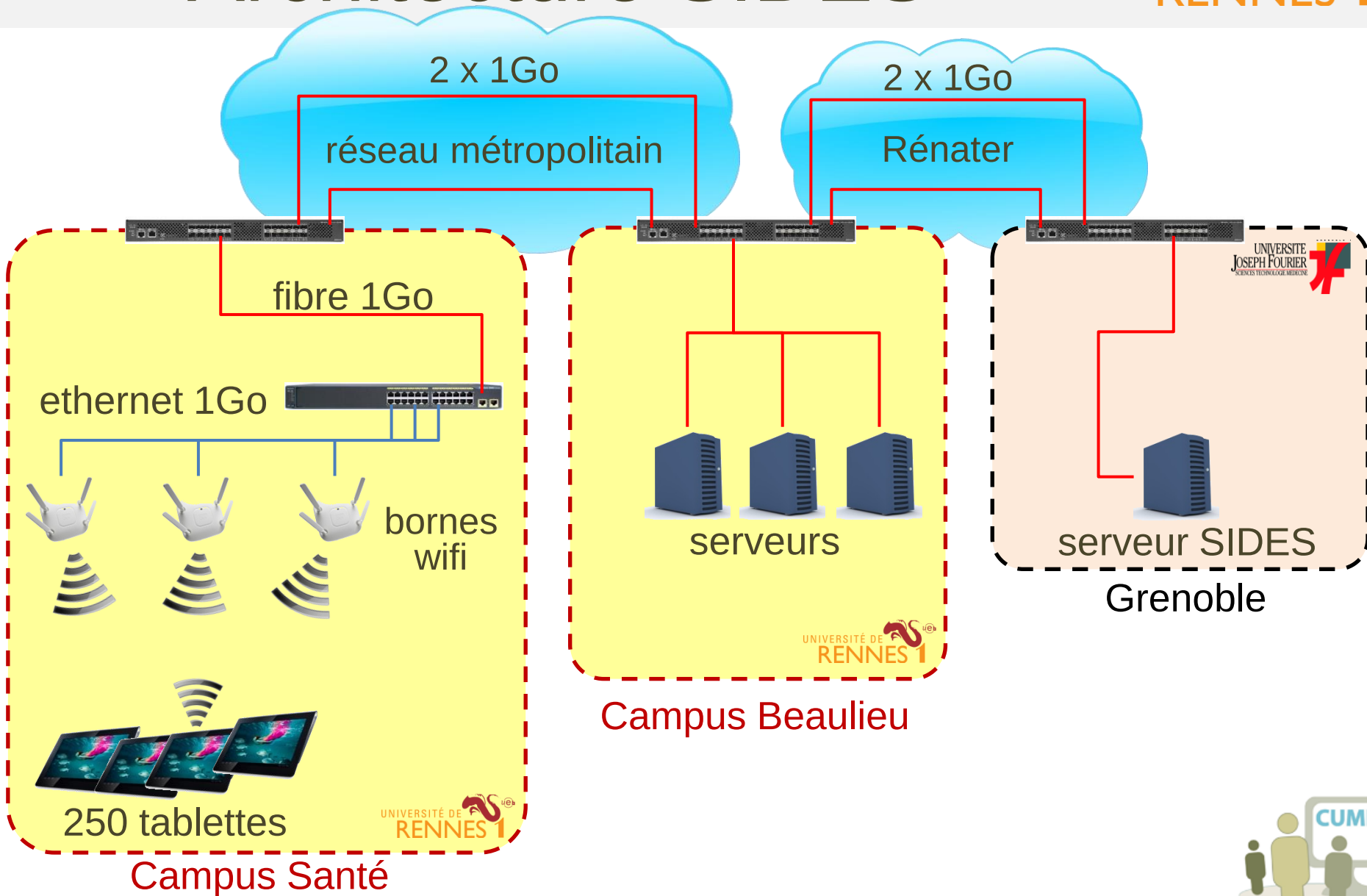
- Mise en charge
- Distribution



- **Le projet doit satisfaire...**
 - La PSSI propre au projet SIDES
 - Connaissance en cours de mise en œuvre
 - La PSSI de l'établissement
 - Le RGS (Référentiel Général de Sécurité)
 - S'applique à tout télé-service de l'administration
 - La PSSIÉ (de l'État)



Architecture SIDES



- **Malveillances**
 - Piratage, triche, ...
- **Sinistres**
 - Incendie, pannes, ...
- **Erreurs**
 - Mauvais comportements,



Appréciation du risque

- **Disponibilité**
 - Les examens doivent se tenir, dans le temps et le lieu imparti
 - Identification des SPOF (Single Point Of Failure)
- **Intégrité**
 - Non modification des flux et des données
 - Imputabilité et non répudiation des actions
 - Avant les examens (procédures administratives d'enregistrement des acteurs, préparation des sujets, ...)
 - Pendant les examens (composition des étudiants)
 - Après les examens (correction)
- **Confidentialité**
 - Sécurisation des échanges
 - fuite au-delà du « besoin d'en connaître » = invalidation
- **Preuve**
 - Traçabilité des actions des utilisateurs



Appréciation du risque

	D isponibilité	I ntégrité	C onfidentialité
Validation du contenu des épreuves (sujets et corrections) par le Jury et le Conseil Scientifique	3 - Critique (entre 4 et 24h)	4 - Intègre / Exacte (Aucune erreur n'est tolérée)	4 - Secret / Privé
Déroulement des épreuves	4 - Vitale (moins de 15 min)	4 - Intègre / Exacte (Aucune erreur n'est tolérée)	3 - Confidentiel / Réserve
Phase de correction automatique et semi-automatique	3 - Critique (entre 4 et 24h)	4 - Intègre / Exacte (Aucune erreur n'est tolérée)	3 - Confidentiel / Réserve
Gestion des résultats et production du classement	3 - Critique (entre 4 et 24h)	4 - Intègre / Exacte (Aucune erreur n'est tolérée)	3 - Confidentiel / Réserve

Source : cabinet Solucom – présentation SIDES 27 mars 2015

Disponibilité

- **Un seul être nous manque...**
- **Pannes, malveillances, erreurs**
- **Continuité de service**
- **Performances optimales**
- **Doivent être disponibles**
 - Fluides
 - Equipements
 - Services



- **Connectivité réseau**
 - De bout en bout...
 - Présence et non saturation
- **Électricité, refroidissement**
 - Redondance des équipements
 - Redondance des sources
 - Contrôle des équipements de secours



- **Réseau filaire, fibre, wifi**
 - Accessibilité, partage, redondance, exposition
- **Équipements réseau, bornes, contrôleurs**
 - Redondance, disponibilité de spare
- **Tablettes**
 - Protection physique (vol)
 - Mise en charge préalable
 - Correction du déploiement



- **Configuration des tablettes**
 - DNS, DHCP
- **Authentification des utilisateurs**
 - CAS, LDAP
- **Piratage, déni de service**



- **S'assurer que seules les tablettes d'examen composent, dans le temps imparti, sans aide extérieure**
- **Contrôle temporel**
- **Contrôle géographique et matériel**
- **Limitation de l'accès**
 - À des sources de connaissances externes



- **S'assurer que personne ne compose en dehors du temps imparti**
- **Délégation au serveur SIDES à Grenoble**
 - Code secret donné en début d'épreuve
 - Clôture manuelle de la prise en compte des réponses



- **S'assurer que seules les tablettes dédiées permettent de composer**
- **Limitation de l'accès au serveur SIDES à une tranche IP**
 - Configuration de l'examen sur la plateforme SIDES
 - Deux classes C
- **Routage des IPs dédiées**
 - Autorisation de sortie du réseau Wifi SIDES aux seules IPs dédiées
 - Interdiction de sortie des autres réseaux depuis les IPs dédiées
- **Contrôle de l'accès au réseau wifi SIDES**
 - Par clé WPA2
 - Inaccessible aux utilisateurs des tablettes
 - Procédure stricte de mise à jour



- **S'assurer que les tablettes ne permettent pas de se connecter à d'autres ressources**
- **Par routage**
 - Rapide à mettre en œuvre
 - Sensible aux modifications d'adressage
- **Par filtrage (mandataire)**
 - Plus coûteuse et complexe
 - Meilleur traçage
 - Plus complexe (sinon SPOF)
- **Et toutes les mesures d'un examen classique...**



Contrôle d'identité

- S'assurer que chaque candidat compose pour lui-même

- **Contrôle classique d'identité**

- L'utilisateur assis est bien celui prévu



- **Contrôle visuel**

- L'utilisateur connecté est bien celui prévu



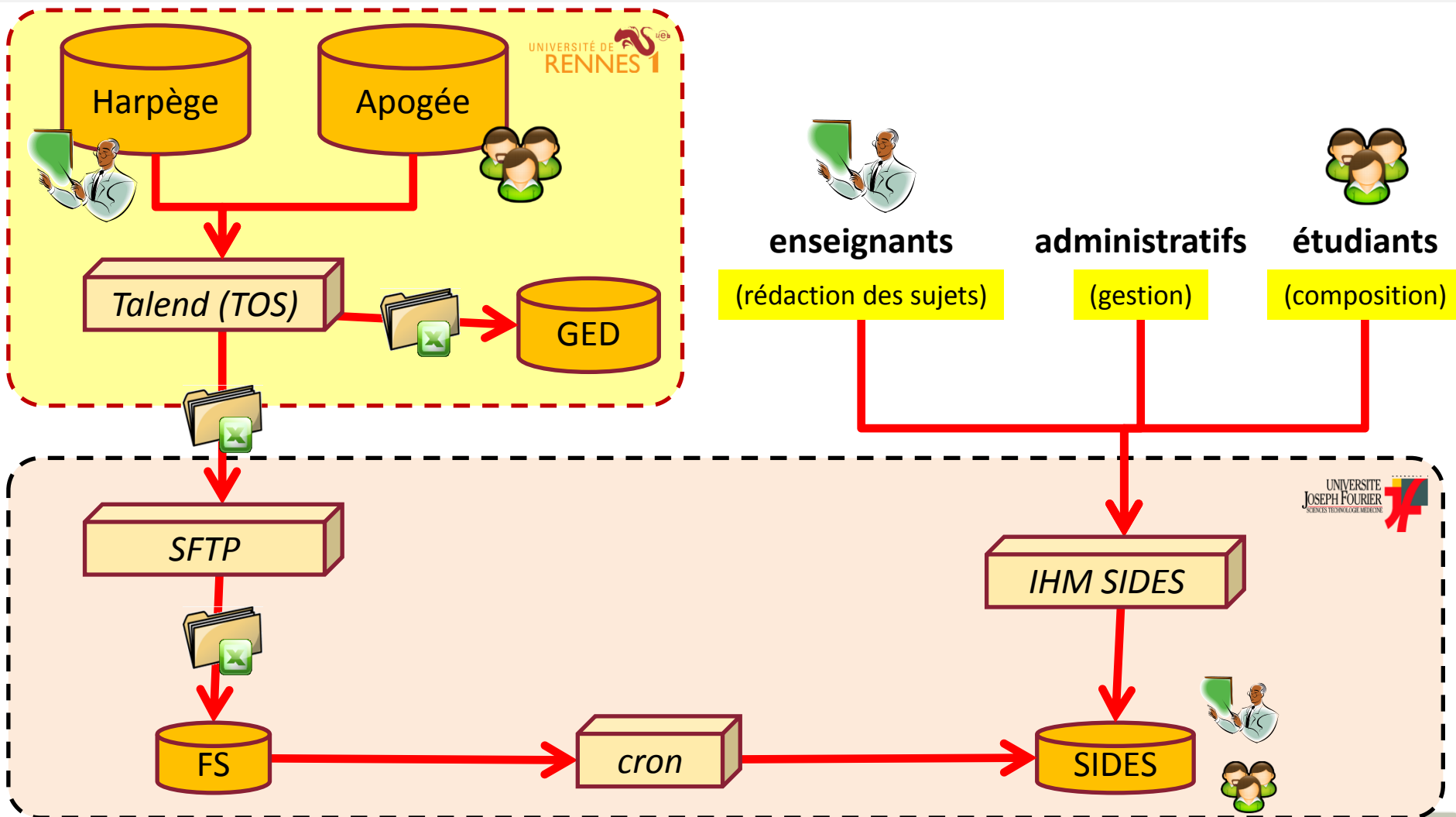
**Emplacement 183
DUPONT CLAIRE**

- **Contrôle en temps-réel des connexions « louches »**

- Plusieurs utilisateurs sur une même tablette
- Un même utilisateur sur plusieurs tablettes



Provisioning et deprovisioning



• **Déclaration CNIL en cours**

- **Le refus des risques n'est pas possible**
- **Ils doivent être minimisés**
 - Chiffrement de toutes les communications,
 - Renforcement de l'architecture réseau existante,
 - Séparation logique des réseaux,
 - Contrôle physique des personnes,
 - Développement d'outils de contrôle en temps-réel
 - Détection des tentatives de fraudes
 - Mise au point de procédures d'alertes
 - éviter tant que faire se peut l'annulation d'examens



- **Transmission du risque résiduel**
 - À la Maîtrise d'OuvrAge
- **Acceptation du risque résiduel**
 - Par la Maîtrise d'OuvrAge



Questions ?

