

Etude 4



Etude sur la sécurité de la
plateforme.



Sommaire

Considérations préalables.....	2
Accès sécurisé à la plateforme de télémedecine.....	3
Dispositions générales.....	6
Document de sécurité.	7
Confidentialité de la Salle Virtuelle.	11
Conclusions	13
Références	14

CONTRÔLE DE VERSIONS			
Lecture	Auteur	Date	Motif
1	José Criado SICBRAIN EUROPA SL	27/12/2011	Première version de l'Etude 4.

Etude 4. Etude sur la sécurité de la plateforme.

L'étude suivante a pour but d'identifier les standards que se doit de respecter la plateforme RESATER, tel que l'expose le dossier réalisé par SICBRAIN EUROPA SL pour ce projet, en réalisant un suivi et une auto-évaluation des mesures développées afin de garantir la confiabilité de cette "voie de communication". Pour cela, nous évaluerons le système d'autorisations ACL (Access Control List) utilisé lors de l'implémentation de la plateforme, nous identifierons les différentes possibilités d'accès et nous réaliserons une réglementation de prévention et sécurité conformément à l'usage qui va être fait par les utilisateurs, dans un environnement de transfert de connaissances international.

Considérations préalables.

Comme il a été exposé dans l'Etude 1 intitulée "Etude de faisabilité, adaptation des applications et services à la plateforme", dans la section *Analyse de la sécurité associée à la Plateforme de Télémédecine*, nous avons envisagé tout d'abord la possibilité d'implanter un algorithme cryptographique RSA. Nous avons vu que cette méthode permettait de doter la plateforme d'une forte sécurité et résistance mais nous avons décidé d'écarter cette option car ces mesures nous semblaient excessives pour l'espace de collaboration du partenariat RESATER, elles auraient en effet été pénalisantes pour une utilisation quotidienne de la part des professionnels, provoquant une forte baisse du rendement attendu. Le caractère pratique de cette proposition repose sur un environnement fiable et sécurisé et le fait de ne pas inclure cet algorithme permet d'augmenter la productivité des ressources associées.

Nous avons également cité dans ladite étude, la gestion des risques associés: " La protection de la plateforme se doit d'être à la hauteur des risques". Cette phrase résume l'implémentation qui a été développée pour l'élaboration des autorisations d'accès et la dimension des catégories attribuées, en fonction du rôle d'entrée à la plateforme. Une bonne gestion ainsi que le respect des législations européennes concernant la protection des données et la gestion des fichiers associés à une base de données de ces caractéristiques permet d'augmenter la confiabilité de la plateforme RESATER.

L'étude juridique réalisée pour cette plateforme nous a permis d'identifier les lois principales qui régissent ce type de traitement:

- Loi Organique 15/1999 du 13 Décembre sur la Protection des Données à Caractère Personnel (LOPDGP). - Espagne
- Loi N° 78-17 du 6 janvier 1978, relative à l'Informatique, aux Fichiers et aux Libertés. - France
- Loi N°41 du 18 août (Traitement de données à caractère personnel et protection de la vie privée à l'égard des Communications Electroniques). - Portugal

Le développement du logiciel réalisé respecte la législation en vigueur et assure à tout moment la confiabilité et confidentialité des données enregistrées, suivant toute une série de mesures pour l'utilisateur final, mesures qui seront décrites par la suite.

Accès sécurisé à la plateforme de télémédecine.

Pour la validation des utilisateurs du partenariat RESATER (et des différents rôles) nous avons développé un système de contrôle d'accès à travers un *framework* de langage PHP dénommé CakePHP. Vous trouverez ci-dessous une description des caractéristiques principales de cet environnement de développement:



Compatible avec PHP4 y PHP5	CRUD intégré pour l'interaction avec la Base de Données
Support d'application (scaffolding)	Architecture Modèle-Vue-Contrôleur (MVC)
Validation intégrée	Composants d'e-mail, cookie, sécurité, session et gestion des sessions
Listes de contrôle d'accès flexibles	Cache flexible
Serveur de distribution (dispatcher)	Localisation

Figure 1. Caractéristiques principales du framework CakePHP

Le développement du système d'accès à la plateforme est orienté aux professionnels du partenariat RESATER. Pour cela, afin d'accéder aux organismes et/ou centres, il faut réaliser une première validation en tant que professionnel associé à la plateforme.

La séparation réalisée par la logique du fonctionnement du système concernant la couche d'application est un des aspects clés de la sécurité implantée. Cela signifie que les utilisateurs et professionnels sont séparés dans la base de données.

Création d'un utilisateur associé.

Lorsqu'un profil professionnel est créé, la création d'un utilisateur associé se fait automatiquement. On peut observer ci-dessous les différentes étapes réalisées:

1. Vérification de l'identifiant. Il doit s'agir d'un nom unique dans le système.
2. Attribution du premier mot de passe: il s'agira du courrier électronique fourni.
3. Génération d'un champ codifié pour valider le compte.
4. Lorsqu'un utilisateur a été créé, celui-ci reçoit un courrier électronique sur son e-mail avec un champ codifié indiquant la démarche à suivre pour valider son compte. Les données reçues sont les suivantes:
 - a. Identifiant.
 - b. Mot de passe (le courrier électronique fourni initialement).
 - c. Code de validation de compte (chiffrée).
5. Confirmation de compte: une fois que l'utilisateur est rentré dans le système (avec son identifiant et mot de passe initial), il est redirigé vers une fenêtre de confirmation de compte. Il doit introduire dans cette fenêtre le code de validation reçu dans l'e-mail initial.
6. Demande de changement du mot de passe: une autre mesure renforce la sécurité de ce système d'accès, il s'agit de la demande obligatoire de changement de mot de passe.
7. Validation finale: une fois que le changement de mot de passe a été correctement réalisé (le code de validation coïncide avec celui qui a été généré lors de la création

de compte), l'utilisateur devient actif et est associé à un professionnel et peut alors accéder à l'information et aux services exposés.

The figure illustrates the process of creating an associated user on the RESATER platform. It consists of three main screenshots:

- Top Screenshot:** A screenshot of the 'Entidad' (Entity) management page. It shows a table with columns for 'Entidad', 'Responsable', 'Idioma', 'Actualizado', and 'Operaciones'. The 'Operaciones' column includes links like 'Añadir centros a Entidad', 'Añadir nuevo tipo de centro', 'Asociar servicios verticales a centros', 'Asociar profesionales a Entidad', and 'Añadir nuevo tipo de profesional'.
- Middle Screenshot:** A screenshot of the 'Añadir Profesional' (Add Professional) form. It includes fields for 'Nombre', 'Apellido', 'Email', 'Contraseña', 'Tipo de profesional', 'Entidad a la que pertenece', 'Asociar centros al profesional', 'Nivel de permisos del usuario', and 'Correo electrónico'.
- Bottom Screenshot:** A screenshot of the 'Registro' (Registration) page. It shows a welcome message and a registration form with fields for 'Nombre de usuario', 'Contraseña de primer ingreso', 'Código de validación', and 'Para acceder a la plataforma pulse aquí'.

Figure 2. Le processus de création d'un utilisateur associé

Lors de la création des mots de passe, la codification est réalisée à travers un *hash* propre de CakePHP. Une chaîne d'information privée est utilisée pour cette compression, sans savoir à utiliser des méthodes classiques telles que base64 ou encode/decode. Ce système

permet de fournir à la plateforme un excellent niveau de sécurité et de confiabilité lors de la création de nouveaux utilisateurs qui pourront alors avoir accès à l'information contenue dans les modules existants.

Le système d'autorisations utilisé pour les fonctions des différents services de la plateforme entre les ACOs et AROs créés sont appelés ACL (lorsqu'un ARO peut accéder à un ACO). ACO (Access Control Object) est l'objet que l'on souhaite contrôler et ARO (Access Request Object) est celui qui sert à contrôler quelque chose. Ce système permet de structurer les utilisateurs en groupes puis on définit quelles sont les actions que peut exécuter chaque groupe. La sécurité implicite bloque les utilisateurs qui n'ont pas les privilèges suffisants pour réaliser une opération. Cette gestion des autorisations garantit donc la sécurité quant à l'accès des utilisateurs selon les restrictions définies lors de la création et selon la législation existante concernant la confidentialité des données.

Dispositions générales.

Cette Etude 4 aborde, entre autres, la réglementation qui spécifie les mesures d'organisation et d'ordre technique nécessaires afin de garantir la sécurité des fichiers échangés entre professionnels du partenariat RESATER, ainsi que les bases de données générées.

Les mesures de **“caractère basique”** touchent les fichiers contenant les données à caractère personnel. C'est à dire, tous les champs enregistrés par les professionnels, organismes et centres recueillis dans les formulaires correspondants. Ceux-ci seront stockés dans le serveur Linux de la plateforme, qui est pourvu des mesures de sécurité correspondantes afin de garantir leur propre confiabilité. Le partenariat RESATER peut prendre la décision de nommer un ou plusieurs responsables de cette information.

Les mesures de **“niveau intermédiaire”** ont une influence plus importante car elles regroupent l'information financière ou administrative permettant d'évaluer les professionnels en termes de “situation personnelle”, ce qui logiquement n'est pas l'objectif de la plateforme. Son utilisation est restreinte, dans un premier temps, à l'échange d'information et à l'espace collaboratif créé à travers la Salle Virtuelle, et aux différents outils de *chat* et transfert de fichiers habilités.

Il existe un troisième groupe de mesures, dites de “**niveau élevé**”, qui ne sont pas applicables à cette plateforme, tel qu’il a été évoqué dans l’Etude 1, page 11, car elles sortent du cadre de la plateforme de télémédecine.

Ce type de dispositions nous amène à conclure que le propre partenariat RESATER se doit de nommer les responsables de ce type d’information, et SICBRAIN EUROPA SL s’engage de son côté à céder l’information de façon claire et précise, garantissant à tout moment le stockage des données réalisé et le support logiciel qui le gère.

Document de sécurité.

Un document de sécurité est un outil d’évaluation qui permet d’informer une personne autorisée sur le maintien de la sécurité associée à la plateforme de télémédecine. Le responsable des fichiers et dossiers doit noter, en fonction de la réglementation interne, tout type de modification qui lui semble importante. Ce type d’incidences doit respecter à tout moment la législation européenne concernant la protection des données et garantir totalement leur confidentialité. Nous citerons en référence les considérations de l’**Agence Espagnole de Protection de Données**, car ses réglementations sont d’ordre général et similaires aux lois des Etats français et portugais.

DOCUMENT DE SÉCURITÉ

CHAPITRE 1: CHAMP D’APPLICATION.

Le présent document s’applique aux fichiers contenant des données à caractère personnel qui se trouvent sous la responsabilité du partenariat RESATER.

Les mesures de sécurité sont fixées sur trois niveaux et peuvent se cumuler entre elles (basique, intermédiaire et élevé) en fonction de la nature de l’information traitée et du degré de garantie de confidentialité souhaité et de l’intégrité de l’information.

CHAPITRE 2: MESURES, NORMES ET PROCÉDURES DESTINÉES À GARANTIR LES NIVEAUX DE SÉCURITÉ EXIGÉS.

Identification et authentification: Mesures et normes relatives à l'identification et authentification des professionnels du partenariat RESATER autorisés à avoir accès à la plateforme.

- × Identification des utilisateurs de façon pertinente et personnalisée, en vérifiant leur autorisation. Le mot de passe permet de garantir la confidentialité et l'intégrité, et il est recommandé de le changer au moins une fois par an.

Contrôle d'accès: Le système de création d'un nouveau compte utilisateur inclut une première validation, moyennant l'insertion préalable d'un "code de validation de compte" que l'utilisateur reçoit sur son e-mail personnel.

Les utilisateurs accèdent aux données et ressources dont ils ont besoin pour réaliser leurs fonctions. Le responsable du fichier établit des mécanismes afin d'éviter qu'un utilisateur de la plateforme RESATER puisse accéder à des ressources non autorisées.

Le super-administrateur sera le seul à pouvoir concéder, modifier ou annuler l'accès autorisé, en veillant à tout moment à la sécurité de la plateforme et la gestion des ressources disponibles sur celle-ci.

Registre d'accès: Sauf demande expresse du partenariat RESATER, l'identification de l'utilisateur, la date, l'heure, le fichier consulté ou le type d'accès réalisé ne seront pas enregistrés.

Gestion des supports et documents: Les supports contenant des données à caractère personnel doivent permettre d'identifier les type d'information contenu et être répertoriés; ils sont stockés sur le serveur Linux, lieu d'accès restreint auquel seul le personnel habilité a accès pour cela, dépendant toujours du super-administrateur.

Copies de sécurité: les copies de sécurité seront réalisées chaque jour. Les données remontant à sept jours en arrière peuvent être restaurées de façon presque immédiate (en deux heures de temps). Elles contiennent les fichiers enregistrés ainsi que les bases de données sous-jacentes du logiciel de la couche d'utilisateur de la plateforme RESATER. Les procédures établies par les copies de sécurité permettent de les reconstruire tels qu'ils étaient avant leur perte ou destruction, ainsi que n'importe quelle version de copie de sécurité réalisée durant les sept jours précédents.

Responsable de sécurité: Un responsable de sécurité est désigné à l'intérieur du partenariat RESATER, ou le cas échéant, le super-administrateur du système, qui est chargé généralement de coordonner et contrôler les mesures définies dans ce document de sécurité.

CHAPITRE 3: PROCÉDURE GÉNÉRAL D'INFORMATION DES UTILISATEURS.

Afin de s'assurer que l'ensemble des utilisateurs ait connaissance des normes de sécurité concernant l'exercice de leurs fonctions, ce document peut être visible ou diffusé à travers la propre plateforme RESATER ou l'Observatoire créé à cet effet.

CHAPITRE 4: FONCTIONS ET OBLIGATIONS DES UTILISATEURS.

Tous les utilisateurs accédant à la plateforme du partenariat RESATER se doivent de prendre connaissance et de respecter les mesures, normes et procédures ayant trait à leurs fonctions.

Tous les utilisateurs se doivent de respecter la confidentialité et le secret professionnel des données à caractère personnel dont ils prennent connaissance lors de l'exercice de leur fonction.

CHAPITRE 5: PROCÉDURE DE NOTIFICATION, GESTION ET RÉPONSE LORS D'INCIDENCES.

Le non-respect de la législation évoquée dans ce Document de Sécurité, ainsi que tout type d'anomalie affectant ou pouvant affecter la sécurité des données à caractère personnel des professionnels associés au partenariat RESATER sont considérés comme des "incidences de sécurité".

CHAPITRE 6: PROCÉDURES DE RÉVISION.

Le Document de Sécurité est révisé par le responsable de sécurité désigné de façon périodique au moins une fois tous les 30 jours. Une feuille de contrôle “manuel” est alors établie afin de contrôler les registres et les incidences occasionnées, qui est sans cesse actualisée. Il doit, de fait, être révisé chaque fois que des changements importants se produisent dans le système d’information, dans le contenu de l’information des fichiers ou suite aux contrôles périodiques réalisés.

Tabla 1. Document de sécurité –Réglementation.

Les feuilles à renseigner doivent présenter le format suivant. On décrira le type d’incidence (dans le cas d’une révision périodique, choisir “notification périodique” dans la case correspondante), le numéro de révision, le type d’utilisateur qui est à l’origine de l’incidence (pour identifier le rôle d’accès à la plateforme) et son nom, ainsi que la date de l’incidence et le motif de la révision réalisée, de façon plus détaillée que dans le titre initial.

Type d’incidence:				
Révision	Type d’utilisateur	Nom	Date	Motif

Table 2. Rapport de sécurité (à renseigner)

Grâce à ce suivi des incidences et des professionnels ayant accès à la plateforme du partenariat RESATER, nous obtiendrons une évaluation constante du rendement et de l’utilisabilité qu’offre cette plateforme.

Le responsable de sécurité élaborera une liste des utilisateurs (incluant leur différent type d'autorisations) qui sera actualisé lors de chaque changement ou nouveauté ayant une incidence sur la liste des personnes ayant accès à la plateforme.

Confidentialité de la Salle Virtuelle.

La salle virtuelle de la plateforme RESATER est un des modules qui composent cette plateforme de professionnels. On peut à travers elle, établir des vidéoconférences et des *chat*. Elle permet à l'ensemble des utilisateurs de participer dans un espace de collaboration international, leur offrant ainsi une interopérabilité et permettant à ces professionnels d'améliorer leur prestation de services.

La confidentialité que possède cette salle est en accord avec le reste des mesures de sécurité adoptées dans l'environnement de la plateforme des professionnels. Ci-dessous le fonctionnement de celle-ci:

1. Les professionnels associés à la plateforme peuvent établir une vidéoconférence et envoyer des invitations aux professionnels possédant un identifiant et mot de passe pour accéder à la plateforme et également aux professionnels externes qui recevront alors par courrier électronique, une url de validation d'accès.
2. Lorsque les invitations à une session de vidéoconférence sont envoyées, les professionnels internes peuvent voir cette invitation dans leur "vue de vidéoconférences" et activer cette dernière afin d'y avoir accès.
3. La sécurité de ce système fait en sorte que le créateur de la vidéoconférence soit le premier à y avoir accès. Les utilisateurs invités y ont accès après avoir effectué leur validation. Le système possède en interne trois niveaux d'accès afin de vérifier les autorisations de chaque utilisateur.
4. Lorsqu'un utilisateur invité a accès à la vidéoconférence, un "token" vérifie (sur un niveau inférieur) que cet invité se trouve bien dans la base de données de la vidéoconférence. S'il n'a pas encore réalisé sa connexion à la vidéoconférence, un message le lui indiquera.
5. Dans le cas où un "intrus" arrive à avoir accès à l'url de la vidéoconférence, mais que celui-ci n'a pas été invité par le créateur de la vidéoconférence, une fenêtre

apparaît sur son écran lui montrant sa non-inclusion dans la base de données et l'accès lui sera refusé. Ce type de protection vient compléter la sécurité de l'accès à la salle virtuelle, en empêchant les actions malveillantes.

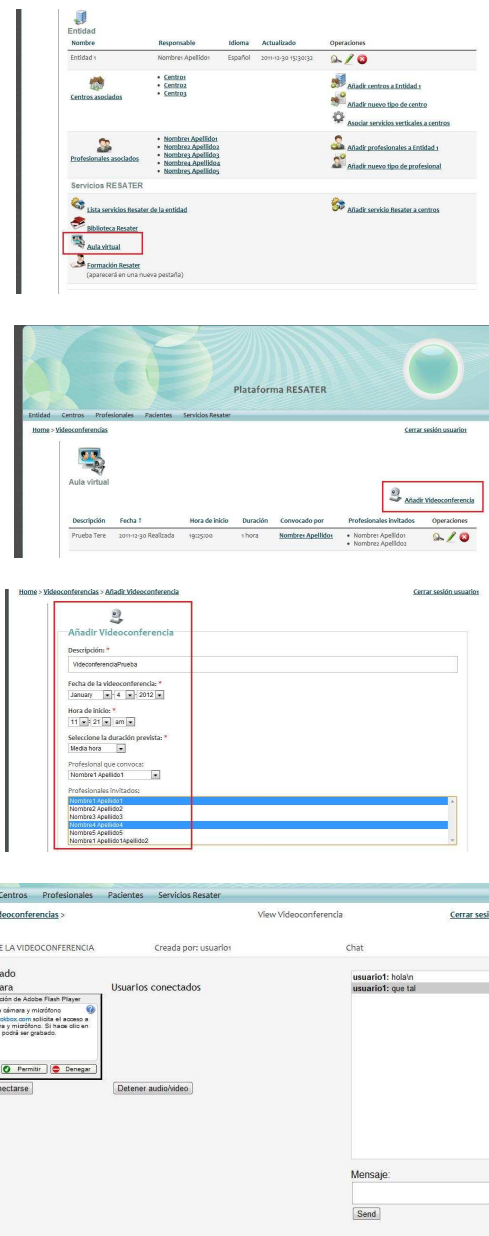


Figure 3. Accès à une vidéoconférence du module Salle Virtuelle

Conclusions

La sécurité associée à la plateforme de télémédecine du partenariat RESATER est un des points clés pour sa correcte implémentation. Elle respecte pleinement le cadre juridique de la législation européenne en matière de systèmes de communication online et de traitement de données à caractère personnel qui s'applique en Espagne, en France et au Portugal. L'accès aux bases de données et à l'information dite "sensible" est limité et soumis au contrôle des utilisateurs enregistrés et à leurs autorisations correspondantes.

Le système d'accès à la plateforme est validé dans un premier temps par un "code de validation de compte" reçu par messagerie électronique, confirmant l'adhésion du nouvel utilisateur à la base de données du système. Cette procédure de sécurité est créée par un *hash* de l'environnement de développement CakePHP; on obtient grâce à elle, une grande confiabilité dans la sécurité implicite du logiciel de la plateforme. Le système d'autorisations qui est utilisé pour ce faire, se dénomme ACL et se charge de mettre en relation les ACOs et AROs créés, qui classent les utilisateurs en différents groupes, possédant chacun un ensemble de privilèges déterminé.

En ce qui concerne les mesures d'organisation et d'ordre technique existantes, relatives à la sécurité des fichiers échangés et les bases de données créées, nous avons envisagé trois types de niveaux: basique, intermédiaire et élevé. Le premier prend en compte les données à caractère personnel, enregistrées dans les formulaires initiaux de renseignements. Le niveau intermédiaire se charge de l'identification personnelle de l'utilisateur à travers l'information enregistrée, la majorité des utilisateurs y ont accès. Enfin, les mesures de niveau élevé, n'ont pas lieu d'être dans cet espace de collaboration car leur nature ne correspond pas à l'usage et à la finalité de la plateforme du partenariat RESATER.

Le document de sécurité (et sa réglementation) prétend identifier une série de procédures afin que tous les utilisateurs et le/les responsable/s de la documentation enregistrée respectent les directives établies. Ils s'agit de mesures basiques qui permettent de renforcer la sécurité garantie par le propre logiciel, pour actualiser et améliorer le fonctionnement de la plateforme, offrant un environnement dynamique et fortement scalable s'adaptant aux changements demandés.

Enfin, la confidentialité de la Salle Virtuelle de la plateforme prévient les utilisations malveillantes de ses ressources, permet aux personnes non associées au partenariat RESATER (mais qui ont été autorisées par un professionnel interne) d'avoir accès aux vidéoconférences

dans une fenêtre parallèle et vérifie continuellement les accès à travers les bases de données identifiant les utilisateurs invités à cette session.

Références

- [1] <http://cakephp.org>
- [2] <http://www.aepd.es>
- [3] <http://www.tokbox/opentok/>
- [4] Etude 3. “Etude juridique de la plateforme RESATER”