UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat d'Informàtica de Barcelona

Sistema per l'emissió, validació i signatura electrónica de consentiments informats per aplicació clínica

GEP #1: Abast del projecte i contextualització

Autor:
Marc Juberó Silva

Director:
Oscar Flores Guri

Ponent:
Toni Cortés Rosselló

27 de setembre de 2016

Índex

1 Context

Aquest Treball de Final de Grau (d'ara en endevant **TFG**) en modalitat B, es desenvolupa a l'empresa Made of Genes [1] com a pràctiques curriculars de l'estudiant.
Per entendre el perquè d'aquest TFG, cal tenir en compte tres coses. Primerament, l'empresa en la qual s'ha desenvolupat el projecte.
Segon, s'ha de tenir clar el terme de *consentiment informat* i, finalment, ser conscient de les metodologíes més emprades actualment per la signatura electrònica de documents.

1.1 L'empresa, Made of Genes

Made of Genes és una empresa que ofereix un servei de genòmica personalitzada que posa a l'abast dels usuaris la seqüenciació del seu genoma i guardar-ne la informació de forma segura i de per vida.
Per altre banda, l'empresa ofereix una plataforma online que actua com a *marketplace* on es poden comprar aplicacions de terceres parts basades en el genoma. Aquestes aplicacions estàn disponibles per que aquelles persones que hagin contractat el servei de seqüenciació puguin treure partit de les dades enmagatzemades.

La compra d'aquestes aplicacions/serveis, però, implica que les dades genòmiques dels usuaris són cedides a tercers, i que aquests, amb les dades respondràn als serveis contractats pels usuaris.
Per assegurar que aquest porcés sigui lícit, el pacient ha de ser conscient de què és el que està contractant i què implica la contractació del esmentat servei. Per això es fa ús del consentiment informat.

1.1.1 Rols a la plataforma

- **Pacient**: L'usuari final, aquella persona que compra el servei de seqüenciació juntament amb una o varies aplicacions sobre les dades del genoma.
- **Professional sanitari**: El professional que facilitarà la informació, tant la relativa al consentiment informat com la dels resultats del servei adquirit, a l'usuari final. Farà d'intermediari entre l'analista i l'usuari.
- **Analista**: Aquell professional sanitari que farà ús de les dades cedides per l'usuari, en realitzarà els anàlisis i presentarà al professional mèdic un informe dels resultats.

1.2 Consentiment informat

En l'àmbit mèdic, rep el nom de ***consentiment informat*** el procediment a través del qual es garantitza que un pacient expressa de forma voluntària la intenció de participar en una investigació o tractament, havent prèviament comprès la informació que se li ha facilitat sobre l'estudi o tractament a realitzar, així com els beneficis, posibles riscos i alternatives i els seus drets i deures.

En ocasions, i en contextos poc rellevants com podria ser un exàmen físic, aquest consentiment es pot arribar a sobreentendre i no requerir la presencia d'un document. No obstant, en procediments invasius, que impliquin cert nivell de risc o bé amb alternatives, el consentiment informat s'ha de presentar per escrit i ha de ser signat pel pacient.

[1] http://www.madeofgenes.com

Aquest document, serveix per autoritzar a les organitzacions, metges o professionals sanitaris en general, a dur a terme les operacions necessàries amb la seguretat de que el pacient, o la persona sobre la qual recaigui l'efecte del tractament o investigació, n'és conscient.

1.3 Sobre signatures

La llei 59/2003 article 1, paràgraf 1, defineix:

> *La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.*

Alhora, en defineix també 3 modalitats:

- **Signatura electrònica**: Correspon literalment a la definició anterior.
- **Signatura electrònica avançada**: és aquella signatura que permet identificar al firmant alhora que permet identificar qualsevol canvi en les dades del signant. Aquesta signatura ha estat generada amb mètodes que el signant pot mantenir sota el seu control exclusiu.
- **Signatura electrònica reconeguda**: Correspon a la signatura avançada però en aquest cas, basada en un certificat reconegut i generada mitjançant un dispositiu segur de creació de signatures.

La anterior llei també estipula, en el quart paràgref del mateix article, que la signatura electrònica reconeguda té el mateix valor que la signatua manuscrita.

Prenent la tercera tipología de signatura electrònica, la que estipula una signatura creada mitjançant dispositius segurs, i amb la creixent necessitat de garantir la validesa i legalitat de tràmits de diferents tipus a Internet, neix el concepte de tercer de confiança.

El tercer de confiança, intentant buscar un paral·lelisme cotidià, es podria entendre com un notari que certifica que en un document, o en el seu defecte un tràmit, es va expedir (o efectuar) en un moment i amb un contingut determinats, però en aquest cas, el notari és una entitat que es troba a l'altre costat del cable de xarxa.

Aquestes entitats, fortament regulades per la llei, conten amb certificats totalment vàl·lids i reconeguts xpedits per una entitat certificadora superior, que juntament amb un segell de temps, poden garantir el no repudi del documents signats, així com oferir mètodes per tal de que els usauris en puguin validar la integritat.

1.4 One Time Password

Rep el nom de *One Time Password*, o còdi únic, aquell còdi generat en un moment concret i que té una validesa relativament curta que oscil·la entre els escassos minuts i les hores. Un cop expira aquest lapse de temps, cal generar-ne un de nou.

Per tal de generar aquests codis únics, el sistema es basa generalment, existeix un segon mètode de generació via algorismes matemàtics, en el càlcul de codi prenent com a base l'instant de temps en el qual s'ha fet a petició i en un "secret"per cada usuari; l'esmentat "secretçorrespon a una cadena de caràcters aleatoris que serà diferent per a cada

usuari, garantint d'aquesta manera, que per un instant de temps i un usuari concret, el codi generat serà únic.

El sistema de OTP és un sistema bastant extès dins de les entitats certificadores que permeten signatura online.

1.5 Blockchain

Blockchain és un concepte o tecnología aparegut en els darrers anys que neix de forma conjunta amb el concepte de les criptomonedes. És una tecnología totalment distribuïda, i que recentment està trobant aplicacions en diferents sectors; un dels quals és el de la verificació de documents mitjançant la publicació del hash d'aquests a la *blockchain*.

Al llarg del document s'explorarà amb més profunditat aquest concepte, així com els usos.

2 Formulació del problema

Atès a la informació presentada a la secció anterior, i donada la tipología del servei ofertat per l'empresa, és de vital importància dotar a la plataforma d'un mètode per a poder gestionar tot el cicle de vida d'una pètició, des de que el client decideix, un cop seqüenciat el genoma, adquirir un servei i així cedir les seves dades genòmiques, fins que el professional sanitari presenti l'informe final de resultats, i dotar a tot aquest procés de la legalitat necesària.

Com s'ha mencionat anteriorment, tot aquest procés de cessió de dades ha de quedar reflectit en un procés de consentiment informat on l'usuari manifesti que ha entès què és el que cedeix, per a què ho cedeix i a qui ho cedeix i culminant amb la firma d'un document on s'explicita tot lo anterior.

Aquest procés de consentiment i posterior signatura, ha de ser efectuat i gestionat de forma telemàtica, alhora que es garanteix la completa legalitat, integritat i accessibilitat del mateix.

3 Abast

El projecte conta amb un abast totalment definit; s'ha de desenvolupar el mòdul de firma de consentiments informats que compleixi amb els requisits legals i funcionals per a posteriorment integrar-lo a la plataforma.

S'espera que al finalitzar el període de pràctiques a l'empresa, el mòdul quedi perfectament integrat i testejat amb la plataforma, amb l'objctiu de que sigui plenamet funcional i que es pugui fer servir sense dificultats en les ocasions que així ho necessitin.

Com a possibles obstacles, queda la investigació sobre les diferents metodologíes i tecnlogíes per a dotar al procés de firma del consentiment informat de validesa legal i jurídica, així com satisfer les necessitats de demostrar la inmutabilitat del document.

4 Estat de l'art

El consentiment infortmat, tal i com s'indica en apartats anteriors, és un procediment, que, tret de contades ocasions, és d'obligada presència en l'àmbit mèdic.

El procediment actual consisteix en un professional sanitari que informa al pacient de tots els possibles riscos, alternatives al tractament o anàlisis, així com dels possibles beneficis o resultats finals, de forma presencial. Un cop acabada la sessió informativa el pacient rep un contracte on, amb la seva signatura manuscrita afirma, amb ple ús de les seves facultats i sempre de forma totalment voluntària, haver rebut la informació, haver-la comprès i estar-ne d'acord.

Un altre mètode de donar validesa legal, és la signatura electrònica, descrita amb anterioritat. Amb el temps i l'avanç de la tecnología han aparegut empreses que busquen oferir serveis de certificació i firma electrònica tant a ususaris com a empreses.
Empreses com *Lleida.net*[2] o *Logalty*[3] operen dins d'Espanya oferit serveis de certificació electrònica a través de la seva plataforma particular o a través d'una API que ells mateixos ofereixen.

El consum dels serveis ofertats per aquestes empreses, les posiciona dins del rol de tercer de confiança, una entitat que actua com un notari online i que, mitjançant un certificat digital i un segell de temps certifiquen que un document ha estat emés en un moment i amb un contingut determinats.
Aquest procés, reconegut davant la llei, certifica la integritat del document, així com n'assegura el no repudi.

L'ús de dispositius que capturin traç i pressió també està reconegut per la llei. El principal inconvenient d'aquests dispositius és, deixant de banda la pèrdua de la capacitat d'operar telemàticament, que el seu preu és molt alt, i la seva amortització resulta complicada.

Finalment, a Espanya es disposa de sistemes de certificació com per exemple, el DNI electrònic, que ofereix als usuaris un certificat digital vàl·lid per a autenticar-se i per a signar electrònicament.
Alternativament, des de ja fa un temps com a complement al esmentat e-DNI, existeix *Cl@ve*, un sistema que busca facilitar la identificació dels usuaris devant de l'Administració, alhora que permet signatura electrònica mitjançant certificats.

Els mètodes d'autenticació permesos al sistema *Cl@ve* són mitjançant certificats (e-DNI) o bé mitjançant el que anomenen *Cl@ve PIN*.
Aquest segon mètode, és el que s'anomena contrassenya única o en anglès, *One Time Password* (d'ara en endevant **OTP**). L'ús d'aquest mètode es basa en una contrassenya generada a partir de l'instant de temps en el que es sol·licita i, generalment, una clau privada i única de l'usuari, assegurant que per cada usuari i instant de temps, la contrassenya és única, garantint així, la identitat.

[2] https://www.lleida.net/
[3] https://www.logalty.com/en/

5 Metodología i rigor

5.1 Organització de l'equip

Per al desenvolupmanet del projecte s'adoptaràn les metodologíes emprades a l'empresa, que en aquest cas, són el que s'anomenen metodologíes àgils; conretament l'anomenada *Scrum*[4].
Scrum es basa en la realització d'iteracions durant el procés de desenvolupament que reven el nom d'*sprints*. Les esmentades iteracions es composen d'un seguit de tasques que s'han de completar al llarg de la durada dels *sprints*; que acostuma a oscil·lar entre una setmana i un mes.
Els objectius a assolir durant l'*sprint* es fixen en unes reunions que es duen a terme l'inici anomenades *Sprint Planning Meeting*.
Per altre banda, durant l'exercici de l'*sprint* es realitzen reunions periòdiques anomenades *Daily Scrum Meetings*, on es tracta de respondre a les següents preguntes:

- Què vaig fer ahir?
- Què faré avui?
- Quins impediments he trobat fins ara?

Les anteriors preguntes intenten donar una visió el més àmplia possible de l'estat del projecte a tots els memebres de l'equip, així com permetre la resolució col·laborativa dels diferents problemes que vagin apareixent al llarg del desenvolupament.
Scrum permet reaccionar de forma àgil a les diferents alteracions que poden sorgir al llarg del desenvolupament i que els desenvolupadors realitzin els canvis pertinents.
Al tractar-se d'un equip de desenvolupament reduït on la comunicació entre membres és constant, el seguiment de la filosofía *scrum* resulta a vegadas un tant òbvia. Tot i això, es respecten les *daylies* a l'inici de cada jornada i els *sprint plannings* a l'inici de cada iteració.

5.2 Codi i control de versions

El desenvolupament del codi del projecte es divideix en dos parts clarament diferenciades:

- **Backend**: desenvolupat amb Symfony, un dels frameworks PHP més extesos dins de la comunitat PHP per la seva versatilitat i potència.
- **Frontend**: desenvolupat amb AngularJS, un framework suportat per Google i que recentment ha alliberat la release final de la versió 2. Actualment, es postula com un dels principals frameworks

Pel control de versions es fa ús de *Git*, un sistema de control de versions desenvolupat primerament per Linus Torvalds (creador del kernel de Linux) i que gràcies a plataformes com *GitHub* o *Bitbucket* s'ha convertit en un dels sistemes de control de versions més emprat en el món del desenvolupament de software.

Per altre banda, per tal d'organitzar el flux de treball dins del repositori, s'ha decidit seguir un esquema com és *Gitflow*[5].

[4] http://scrummethodology.com
[5] http://nvie.com/posts/a-successful-git-branching-model/

A mode de resum, *gitflow* proposa una organització dins del repositori molt clara i estructurada.

La estructura bàsica del repositori contarà amb dos branques principals:

- **Master**: en termes més autòctons, la branca de producció. En aquesta branca del repositori sols hi ha codi plenament funcional i testejat. El codi que aqui es troba, està preprat per a ser publicat en qüalsevol moment.
- **Develop**: aquesta és la branca que es destinarà al desenvolupament del còdi pròpiament dit. El codi que aqui es trobi, també haurà d'estar testejat i ésser funcional, però el grau de rigurositat d'questa branca és menos que master.

Un cop definit el punt de partida, es crearàn branques a partir de la branca desenvolupament per a les diferents funcionalitats, aquestes rebràn el nom de *feature* seguit del codi de la tasca a desenvolupar. D'aquesta manera les branques queden etiquetades i vinculades amb la tasca.
Un cop acabada una tasca, es farà *merge* de la branca *feature-X* cap a la branca de desenvolupament i així successivament.
Un cop acabat l'*sprint*, es farà *merge* de la branca desenvolupament cap a la branca *master*. Aquest procediment l'anomenarem *release*.
Per a possibles correccions d'última hora, *gitflow* proposa una quarta branca anomenada *bugfix*. Aquesta surt directament de la branca *master*, i està pensada per a correccions de codi ràpides.

Per tal de mantenir el repositor el més net possible, cada cop que s'acabi una *feature* o un *bugfix* s'ha de tancar la branca creada.

5.3 Software de suport

Com a suport per a la gestió d'*Scrum* i del control de versions, així com de documentació interna, es disposa de llicència de la suite d'*Atlassian*[6], que ofereix diferents aplicatius:

- **Jira**: per a la gestió d tasques i planificació de les iteracions.
- **Confluence**: per a la documentació interna del projecte.
- **Bitbucket**: com a repositori de control de versions.

Per altre banda, també es fa servir *Jenkins*[7] per a la integració contínua.

[6] https://www.atlassian.com
[7] https://jenkins.io/