DOCTORATS INDUSTRIALS

EL PLA DE DOCTORATS INDUSTRIALS

# PROJECTE DE DOCTORAT INDUSTRIAL
# EXPEDIENT 2015 DI 030

## DADES DE L'EMPRESA I DE L'ENTORN ACADÈMIC

**Títol del projecte**
Sistemes de Vot Electrònic de Tercera Generació: privadesa a llarg termini.

**Empresa**
Scytl Secure Electronic Voting, SA

**Responsable de l'empresa**
Jordi Puiggalí Allepuz

**Universitat o Centre de Recerca**
Universitat Politècnica de Catalunya – Barcelona Tech

**Director/a de tesi**
Maria Paz Morillo Bosch

**Treballador/a de l'empresa i doctorand/a**
Nuria Costa Mirada

## BREU DESCRIPCIÓ DEL PROJECTE DE RECERCA

La proposta es basa en estudiar mecanismes de seguretat en els sistemes de vot electrònic que permetin enfortir la privadesa de la informació publicada al finalitzar una elecció.

Una part important de la verificació dins un sistema de vot electrònic consisteix en la publicació d'informació en un espai públic (bulletin board) que ha de permetre a qualsevol persona poder verificar el resultat de l'elecció. Per exemple, els votants han de poder verificar que el seu vot s'ha tingut en compte en el recompte final i un auditor ha de poder verificar que els vots han estat emesos per votants legítims. Tota aquesta informació utilitza diferents tècniques criptogràfiques per assegurar la privadesa del vot (el que es coneix en anglès com la propietat de hiding) i a l'hora assegurar que aquell vot ha estat utilitzat per obtenir el resultat final de l'elecció (propietat de binding). No obstant, per evitar que aquestes propietats no facilitin correlacionar els vots amb els votants, el sistemes es basen en l'acceptació de que hi ha problemes computacionals, com el logaritme discret o la factorització de nombres grans, que són difícils de resoldre. Però, podem assegurar que seguiran sent difícils d'aquí uns anys? És una realitat que la potència computacional dels dispositius d'avui en dia augmenta a una gran velocitat i que, per tant, el que avui en dia es considera segur i garanteix la privadesa dels vots i els votants, no ho farà en un futur. És per aquest motiu que s'estan començant a definir sistemes de votació electrònica amb el que es coneix com everlasting privacy, on l'objectiu consisteix en publicar informació de manera que les propietats de hiding i binding no es basin en la dificultat de resolució de problemes computacionals.

DOCTORATS INDUSTRIALS

EL PLA DE DOCTORATS INDUSTRIALS

El projecte començarà amb un estudi i anàlisi de les propostes actuals de protocols de vot electrònic fent èmfasi en aquells protocols amb mecanismes de verificació i que fan servir el bulletin board com un d'aquests mecanismes. També s'analitzaran les solucions proposades fins ara per obtenir privadesa a llarg termini i es detectaran possibles millores. L'estudi contemplarà tant sistemes de vot electrònic presencial com sistemes de vot electrònic remot.

L'objectiu principal del projecte és dissenyar i desenvolupar protocols criptogràfics de vot electrònic assolint el requeriments de seguretat del vot electrònic, proporcionant eines de verificació i, al mateix temps, proporcionant everlasting privacy.

La propietat intel·lectual que s'obtingui del projecte es patentarà i es farà servir en productes de la companyia.