Scytl

Innovating Democracy

Preguntes freqüents (FAQs)

Sobre el proveïdor de la solució tecnològica i seguretat del sistema de vot

Eleccions als Òrgans de Govern del
Col·legi d'Arquitectes de Catalunya 2018

COAC

1 Sobre el proveïdor de la solució tecnològica

1.1 Qui és el proveïdor dels sistemes?

Scytl Secure Electronic Voting (Scytl). És una empresa de software especialitzada en el desenvolupament de solucions segures de vot electrònic. Scytl ha desenvolupat protocols avançats per dotar al vot electrònic d'un major nivell de seguretat, privacitat i confiança. A més, Scytl ofereix la primera solució completa i proporciona el màxim nivell, actualment disponible, en els estàndards de seguretat i transparència.

1.2 Quins són els antecedents de Scytl?

Scytl es va fundar l'any 2001 a partir d'una spin-off d'un prestigiós grup d'investigació de la Universitat Autònoma de Barcelona (UAB), pioners en la cerca de solucions de seguretat per al vot electrònic des del 1994. Aquest grup científic va produir les dues primeres tesis doctorals a nivell europeu sobre seguretat per al vot electrònic, així com diverses publicacions internacionals en el camp de la criptografia a nivell d'aplicació i del vot electrònic. Els innovadors protocols criptogràfics de Scytl deriven d'aquests anys d'investigació en el sector del vot electrònic.

1.3 On està Scytl?

Scytl és una societat anònima espanyola, amb seu a Barcelona i amb oficines als Estats Units, Brasil, Canadà, Grècia, Hong Kong, Corea del Sud, Perú, Mèxic i Austràlia.

1.4 Quins són els accionistes de Scytl?

Scytl és una societat anònima privada. Els accionistes de Scytl són diversos fons de capital risc, alguns espanyols: Spinnaker SCR i Nauta Capital, i altres d'internacionals: Vulcan Capital, Sapphire Ventures, Industry Ventures LLC, Adams Street Partners i Balderton Capital. A més, d'un grup de persones que inclou els fundadors de Scytl i els membres del seu equip directiu. En compliment de l'estricta neutralitat política de Scytl, cap dels seus accionistes o directius està afiliat a cap partit polític.

1.5 Quins són els productes de Scytl?

Scytl ha desenvolupat una família completa de solucions de vot electrònic al voltant d'un nucli comú de seguretat. Scytl ofereix productes de vot electrònic per dur a terme tot tipus d'eleccions en el sector públic i productes especialment dissenyats per a les necessitats específiques de les eleccions en el sector privat.

1.6 La tecnologia de Scytl està protegida per patents?

Scytl ha presentat múltiples patents PCT internacionals per protegir les característiques diferencials de la seva tecnologia de seguretat per al vot electrònic. Scytl també ha protegit la seva tecnologia i software amb copyright.

1.7 Ha rebut Scytl algun premi?

Scytl ha rebut diversos premis internacionals per la seva tecnologia innovadora per al vot electrònic com l'ICT Award atorgat per la Comissió Europea, el premi RedHerring 100 o el premi Global Innovator atorgat per Guidewire Group. Per veure la resta de premis que ha rebut Scytl pot consultar la següent pàgina web http://www.scytl.com/ca/premis/

1.8 On puc trobar més informació sobre Scytl i la seva tecnologia?

Pot trobar més informació visitant la pàgina web de Scytl: http://www.scytl.com

2 Sobre la seguretat del sistema

2.1.1 Com puc verificar la firma digital de l'aplicació de vot?

Quan accedeixis a la pàgina de vot, se't mostrarà una finestra indicant si confies en el certificat de la pàgina web. Aquesta finestra indica si el certificat ha estat verificat per una entitat de confiança o no. Si ho desitges, pot visualitzar més detalls seleccionant "Més informació..."

2.1.2 Com puc verificar que estic accedint al portal de vot real, és a dir, no hi ha phishing, intents d'obtenir informació privada com el nom d'usuari, la contrasenya, etc.?

Quan s'accedeix al portal de vot s'utilitza una connexió HTTPS, la qual implica que el servidor s'autenticarà amb un certificat digital davant el teu navegador web. Si tot és correcte, podràs accedir al portal de vot sense cap notificació d'error i el navegador normalment mostrarà un cadenat tancat o una icona similar per indicar-ho.

D'altra banda, si apareix una finestra d'alarma al navegador indicant que el certificat digital del lloc no coincideix amb la direcció on es connecta (o missatges similars) és possible que estiguis accedint a un portal fals. En aquest cas, contacta amb l'equip de suport per notificar-ho.

2.1.3 Com proporciona Scytl seguretat "extrem-a-extrem" a un procés de votació?

La solució de Scytl proporciona seguretat extrem-a-extrem (*end-to-end*), des de votants individuals fins la Mesa Electoral, evitant així el risc d'atacs interns per part dels administradors de sistemes. Els vots es xifren i se signen digitalment pels votants als seus dispositius de vot (ordinadors) abans de ser emesos. La clau privada per desxifrar els vots està dividida en fragments que es distribueixen entre els membres de la Mesa Electoral abans de l'inici de l'elecció. Al final de l'elecció, un número mínim prèviament definit de membres de la Mesa Electoral ha de reunir-se per reconstruir la clau privada i desxifrar els vots.

2.1.4 Amb la solució de Scytl, el control de l'elecció està en mans dels administradors de sistemes?

La solució de vot per Internet de Scytl posa el control del procés electoral exclusivament en mans de la Mesa Electoral, tal com passa en les eleccions tradicionals en paper. Els membres de la Mesa Electoral són els únics que poden reconstruir la clau privada que permet desxifrar i comptar els vots. Els

administradors de sistemes, o qualsevol altre actor amb privilegis al sistema, no tenen accés a la clau privada i, per tant, no poden veure ni modificar els vots.

2.1.5 Com garanteix Scytl la privacitat dels votants?

Els vots són xifrats als dispositius de votació dels votants abans de ser emesos. Només la Mesa Electoral —mitjançant la col·laboració dels seus membres— pot reconstruir la clau privada i desxifrar els vots. Aquest procés es realitza en un servidor aïllat i físicament segur, aplicant una tècnica de *mixing*, que trenca la correlació entre la identitat dels votants i els vots desxifrats per garantir la seguretat.

2.1.6 Com protegeix Scytl la integritat dels vots?

Els vots emmagatzemats als servidors de vot estan protegits de forma segura —xifrats i signats digitalment— en tot moment, i per tant, ningú els pot manipular, ni tan sols els administradors dels sistemes amb accés privilegiat.

2.1.7 Com evita Scytl la incorporació de vots falsos?

Una vegada xifrats, els vots són signats digitalment pels votants. Els certificats digitals usats pels votants per signar digitalment els seus vots xifrats poden ser certificats digitals preexistents o certificats digitals generats ad-hoc per aquesta elecció específica. Abans de desxifrar els vots, la Mesa Electoral verifica que les signatures digitals dels votants pertanyin als votants validats. Els vots amb una signatura digital no vàlida són apartats per a una auditoria posterior.

2.1.8 Poden verificar els votants que els seus vots han estat inclosos en el recompte final?

Pots imprimir un rebut de vot amb un identificador únic que consisteix en un codi alfanumèric generat de forma aleatòria al teu dispositiu de vot i que, per tant, només el coneixeràs tu.

Aquest identificador únic es xifra amb el vot en un sobre digital al dispositiu de vot abans que el vot s'emeti. Només la Mesa Electoral pot obrir el sobre digital —una vegada reconstruïda la clau privada— i recuperar el vot així com l'identificador únic. Uns dies després de la proclamació de resultats, la Mesa Electoral farà pública la llista d'identificadors únics recuperats i podràs verificar que el teu vot ha arribat a la Mesa Electoral i es comptabilitza.

2.1.9 El rebut de vot de Scytl facilita la coerció o la venta de vots?

El rebut de vot de Scytl és un codi alfanumèric que no revela les opcions de vot seleccionades pel votant, i per tant, no permet ni la venta dels vots ni la coerció dels votants.

2.1.10 La solució de Scytl és auditable?

Scytl considera que la transparència és una part integral de la seguretat. Per això, proporciona l'accés al codi font de la seva solució a les autoritats electorals i a terceres parts designades per les autoritats electorals. Una vegada auditat el codi font, les autoritats electorals poden signar-lo digitalment per assegurar-se que la solució auditada és la mateixa que s'implementa durant l'elecció.

2.1.11 Les autoritats electorals poden auditar els resultats de l'elecció?

La solució de Scytl genera registres per a cada acció realitzada durant l'elecció. Aquests registres s'encadenen de forma xifrada —cada vegada que es genera un nou registre— per prevenir qualsevol manipulació. Aquests registres inalterables permeten una auditoria precisa dels resultats de l'elecció per part de les autoritats electorals (i de terceres parts) al final de l'elecció.

Innovating Democracy