Hauteskunde unibertsal eta askeak telematikaren eskutik?

Maider Huarte, Iñaki Goirizelaia, Juanjo Igarza eta Joserra Etxebarria

Bilboko Ingeniaritza Goi Eskola Teknikoa
Urkixo Zumarkalea 48013 Bilbo (Bizkaia)
Tel.: 94 601 3991
e-posta: maider.huarte@ ehu.es)

Laburpena: Informazio eta Komunikazio Teknologia (IKT) berriek, demokraziaren kontzeptua asko hobetu dezakete, gizartearen partaidetza moduak areagotuz. Hauteskunde prozesuak dira partaidetza modu horien artean zabalduenak, hiritarren iritziak zuzenean jasotzeko erabiltzen direnak. Azken hamarkadetan, hauteskunde prozesuak IKTekin hobetzen dituzten sistema berriak proposatu dira; telematika arloan erronka berriak ekarri dituzte sistema horiek.

Edozein hauteskundek, demokratikotzat joko bada, unibertsaltasun-, berdintasun-, askatasun- eta sekretu-printzipioak betetzen dituen boto-sistema erabili behar du.

Gure ikerketa, Internet sarearen erabilera egiten duten «Boto-Sistema Elektronikoa» deiturikoen analisiarekin hasi genuen. Analisi horren ondorioz, gaur egungo Internet Darabilten Boto-Sistema elektronikoetan, gehienbat berdintasun- eta sekretu-printzipioak helburu dituzten propietateak betetzen direla ikusi genuen.

Hortaz, unibertsaltasun- eta askatasun-printzipioak ere besteak bezain garrantzitsuak izanik, horietarako beharren azterketa eta proposamenak landu ditugu.

Unibertsaltasun eta askatasunaren azterketa eta proposamen horiek berdintasun eta sekretu-printzipioak ahaztu gabe egin behar direnez, Internet Darabilen Boto Sistema Elektroniko oso bat zehaztu dugu. Gure proposamenen balioa erakusteko, Europar Kontseiluak Boto-Sistema Elektronikoetarako aurkeztutako segurtasun helburuak betetzearen azterketa egin diogu diseinatutako sistemari. Azterketa horren sakontasuna, sistemaren telekomunikazio-protokoloaren egiaztapenarekin osatu dugu, Internet erabiltzearen arriskuak gainditzeko. Ondorioz, beste edozein zerbitzu telematiko bezain seguru edo arriskutsua den Internet Darabilen Boto Sistema Elektronikoa definitu dugu eta bertan beste hainbatetan ere erabil daitezkeen unibertsaltasun eta askatasunerako proposamenak batu ditugu.

Abstract*:* New Information and Communication Technologies (ICT) can greatly improve democracy, with new participation methods. Elections, which are used to directly gather citizens' opinions, are the most widespread of those methods. Last decades, new ICT improved voting systems have been introduced which arouse new challenges in computer science.

Any election to be considered democratic is said to use a voting system that fulfills universality, equality, freedom and secrecy principles. Our research began analyzing Electronic Voting Systems that use Internet. That analysis let us know, that nowadays Internet based Electronic Voting Systems mostly comprise equality and secrecy related properties. Hence, being universality and freedom necessary too, we performed a study of their requirements and approaches, which are resumed in this paper.

As those universality and freedom requirements and approaches are to be considered along with equality and secrecy principles, we have specified a complete Internet based Electronic Voting System. We validated it also, analyzing the accomplishment of the security objectives introduced by the Council of Europe for Electronic Voting Systems. That analysis was complemented with the formal validation of the communication protocol, to overcome Internet usage threats. Therefore, we defined an Internet based Electronic Voting System that results as secure or risky as any other Internet service, providing universality and freedom integrated approaches that can be used in any other such voting systems.

1. **SARRERA**

Hauteskunde demokratikoen printzipioak Nazio Batuen Erakundeak zehaztu zituen 1966. urtean [1]. Printzipio horiek unibertsaltasuna, berdintasuna, askatasuna eta sekretua dira; hots, hautesle guztiek botoa baldintza berdinetan emateko aukera izan behar dute, bakoitzak boto bakarra eman ahal du, botoaren bidez iritzia askatasunez adieraziko da eta boto bakoitza nork eman duen jakitea ezinezkoa izango da.

Artikulu honetako tesia Internet Darabilten Boto-Sistema Elektronikoen (iBSE) azterketarekin hasi zen, hau da, hautesleen botoak Interneten bidez urruneko makinetan gorde eta zenbatzen dituztenen analisiarekin. Horietan gehienbat berdintasun- eta sekretu-printzipioak zaindu direla ikusirik, unibertsaltasuna eta askatasuna neurri berean lor daitezkeela erakutsi nahi izan da, ildo horretan ikerketa berriak bultzatzearekin batera.

2. **iBSE MOTAK**

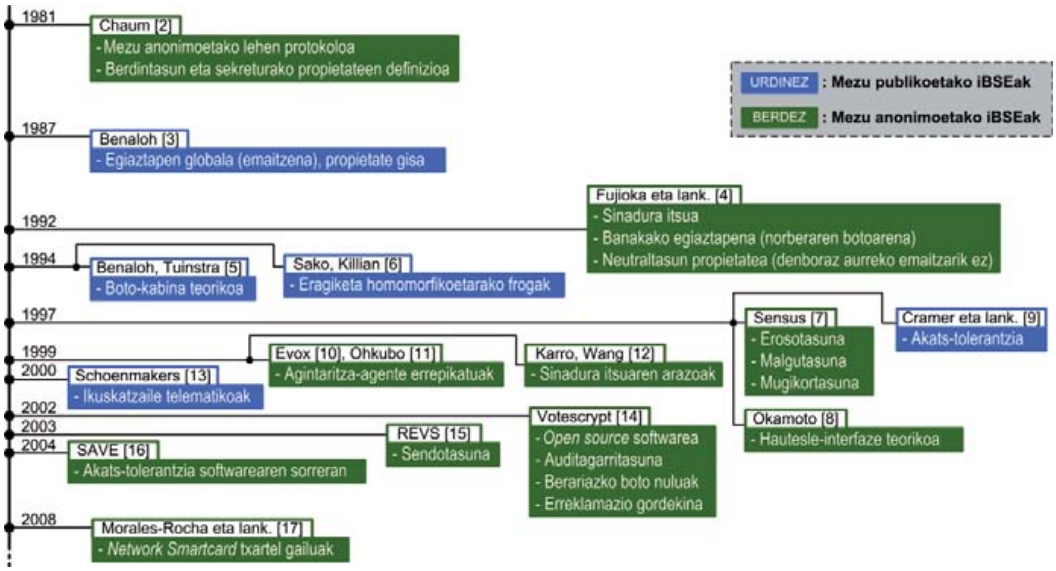
Interneten oinarrizko kriptografia erabiltzen da mezu seguruak bidaltzeko. Horrekin lor daitezke mezu konfidentzialak (hartzaileak bakarrik ireki ditzakeenak) edo sinadura kriptografikoak (mezua egile jakin batek prestatua dela ziurtatzen duten elementuak).

Oinarrizkoaz gain, hautesle eta agintaritzaren arteko protokoloa baldintzatu duten kriptografia teknika konplexuagoak erabili dira iBSE-etan. Horrela, protokoloen arabera, bi iBSE mota bereizten dira:

— **Mezu publikoetako iBSEak**: kriptografia homomorfikoari esker, hautesleek bidalitako botoak ireki gabe lor daitezke hauteskunde-emaitzak. Hautesle bakoitzak bere boto digital itxia gako sekretu eta eragiketa homomorfikoekin prestatu eta agintaritzari bidaltzen dio, bere identitatearekin batera. Emaitzak lortzeko erabiliko dituen mezu guztiak (boto itxi eta hautesle-identitateak) argitaratzera behartuta dago agintaritza. Beraz, edozeinek egiazta dezake hauteskunde-emaitzak benetan hautesle direnen botoekin lortu direla, berdintasun-printzipioa betez. Emaitzen kalkulua botoak ireki gabe egiten denez, sekretu-printzipioa ere babestuta dago.

— **Mezu anonimoetako iBSEak:** hauetan, hautesleak bere identitatea bidaltzen dio agintaritzari mezu seguru batean, botoa emateko baimena lortzeko. Agintaritzaren erantzuna prozesatuz, hautesleak baimena sortzen du, eta mezu anonimo batean (bere identitatea azaldu gabe) bidaltzen dio agintaritzari, boto itxiarekin batera. Baimena osatzeko, sinadura itsuko kriptografia erabiltzen da; horrekin, agintaritzak identifikatu ahalko du baimena eskatzen duen hauteslea, baina boto itxiekin iritsitako baimenetatik ezingo du jakin botoak zein hauteslerenak diren.

Azken urteotan, iBSE eskema teoriko zein praktiko desberdinak plazaratu dira. Horietako garrantzitsuenak 1.1. irudian adierazi ditugu:



1. irudia. iBSE-en bilakaera historikoa eta ekarpen nagusiak

3. HELBURUAK

Gaiaren bilakaera-azterketarekin egiaztatu dugunez, iBSE-etan hainbat propietate lortzeko asmoak egon dira. Ondoko taulan bildu ditugu aipagarrietan aipagarrienak (eskema guztietan bilatutakoak hizki lodiz markatu ditugu):

1. taula. iBSE-etan bilatutako propietate garrantzitsuenak

UNIBERTSALTASUNA	BERDINTASUNA	ASKATASUNA	SEKRETUA
Mugikortasuna	**Onargarritasuna**	**Egiaztagarritasuna**	**Pribatutasuna**
Sinpletasuna:	**Zehaztasuna**	Fidagarritasuna	
— Erosotasuna		Malgutasuna	
— Erabilterraztasuna		Neutraltasuna	
— Egokitasuna			

Agerian dagoenez, iBSE-etan berdintasun- eta sekretu-printzipioen propietateak bilatu dira gehienbat. Haiek bezain garrantzitsuak dira unibertsaltasuna eta askatasuna eta beraz, horietarako beharren azterketa eta proposamenak hartu ditugu helburu.

— Askatasun-printzipioari buruzko helburuak:

- Fidagarritasuna hobetzea, borondatezko partaidetza suspertzeko eta, ondorioz, emaitza zehatzagoak lortzeko.
- Malgutasuna handitzea, botoaren formatua eta zenbatze-metodoak mugatzen ez dituen proposamenarekin iritziak ahalik eta zehatzen adieraztea ahalbidetzeko.

— Unibertsaltasunaren inguruko helburuak:

- Hautesleriaren gaitasun-heterogenotasuna kontuan hartzen duten gizaki/makina interfazea definitzea.
- Hautesleen mugikortasuna erraztea, protokoloen segurtasunean eraginik izan gabe.

4. UNIBERTSALTASUN- ETA ASKATASUN-PRINTZIPIOETARAKO ELEMENTUAK

Erabilitako protokolo mota bakoitzak nabarmen baldintzatzen ditu lortu ahal diren propietateak eta, ondorioz, bete beharreko printzipioak; zehazki askatasuna eta unibertsaltasuna mugatzen ditu, berdintasuna eta sekretua maila berean lortuz.

2. taula. Protokolo motak eta propietateak

PROPIETATEA	DEFINIZIOA	Homomorfismoa	Sinadura itsua
UNIBERTSALTASUN-PRINTZIPIOA			
Sinpletasuna	*Guztientzat erabilerraza eta erosoa.*	Eraginik ez	Eraginik ez
Mugikortasuna	*Botoa edozein lekutatik eman ahal izatea.*	Eraginik ez	Eraginik ez
BERDINTASUN-PRINTZIPIOA			
Onargarritasuna	*Zenbatu beharreko botoak zehazten dira ([7]):* *Egiaztatutako hautesleenak.* *Hautesle bakoitzeko boto bakarra.*	Maila berean	Maila berean
Zehaztasuna	*Boto onargarriak bakarrik zenbatzen dira, dagokien balioarekin..*	Maila berean	Maila berean
ASKATASUN-PRINTZIPIOA			
Neutraltasuna	*Botoa emateko fasean zehar ezin dira bitarteko emaitzarik lortu.*	Bai	Bai
Malgutasuna	*Edozein boto-formatu eta zenbatze-metodo erabil daitezke.*	Batere ez	Bai
Egiaztagarritasuna	*Sistemaren funtzionamendu zuzena egiaztatu daiteke:* *Globala: edozeinek egiazta dezake emaitzak boto onargarri guztiekin lortu direla.* *Banakakoa: hautesle bakoitzak bere botoa ondo zenbatu dela egiazta dezake.* *Auditagarritasuna: edozeinek egiazta dezake sistemaren funtzionamendua egokia izan dela.*	*Globala* bakarrik	Bai
Fidagarritasuna	*Sendotasuna: erasoak jasateko gaitasun teknikoa.* *Gardentasuna: sistema ulergarria edo gutxienez ikuskagarria da.* *Erreklamazio-seguruak egin daitezke.*	Sendotasuna bakarrik	Bai
SEKRETU-PRINTZIPIOA			
Pribatutasuna	*Hautesle bakoitzak emandako botoa jakiterik ez dago.*	Maila berean	Maila berean

Eskema homomorfikoetan egiaztapen *globala* bakarrik lor daiteke (erdietsiriko emaitzak argitaratutako boto itxiekin kalkulatu direla, alegia); *banakakoa* egiterik ez dago (hau da, norberak ezin du jakin bere botoa nola zenbatu den). Batere gardentasunik ez duten eragiketa homomorfiko konplexuak egin behar dira. Malgutasuna, berriz, lor ezin daitekeen propietatea da, botoek formatu jakina behar baitute homomorfikoki zenbatuak izateko.

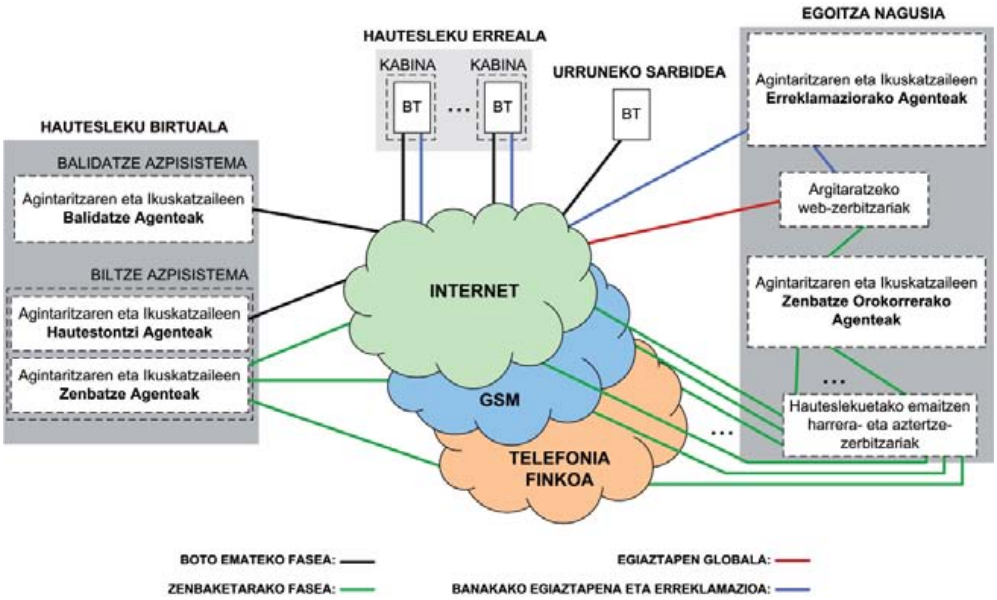
Sinadura itsuko eskemetan propietate gehiago lortzeko aukera izan arren, bestelako osagai batzuk beharrezkoak dira horiek ziurtatzeko.

Hortaz, printzipio guztiak bete ahal izateko, oinarrizko hiru osagai zehazten ditugu:

— **Sinadura itsuko protokolo segurua**: berdintasun- eta sekretu-printzipioak ziurtatzeaz gain, malgutasuna, egiaztagarritasun osoa eta fidagarritasuna lortzeko.
— **Hautesle-interfaze egokiak**: sinadura itsuko eskemek mugikortasun-, sinpletasun- eta pribatutasun-propietateetan dituzten hutsuneak betetzeko.
— **Ikuskatzaileak**: ohiko hauteskundeetan bezala, fidagarritasuna eta egiaztagarritasun osoa indartzeko. Emaitzetan interes kontrajarriak dituzten taldeak izango dira ikuskatzaileak. Hauteskundean garrantzitsuak diren erabakietan parte hartuko duten agenteak sortu eta exekutatuko dituzte, akats-tolerantziako teknikak [18] jarraituz. Teknika horiei esker, akatsekin ere lanean diharduten aplikazio sendoak sortzen dira; horrelako oinarririk gabe, segurtasun-neurriak gehitzeak ez luke balio handiegirik, zimendurik gabeko etxea egitea bezala bailitzateke. Erabilitako software guztia (agente-programak barne) *open-source* modukoa izan beharko da, gardentasuna ziurtatzeko. Egiaztagarritasun osoa lortzeko, egiaztapen global eta banakakoa ahalbidetzeaz gain, auditoria-arrastoen bilketa ere egin beharko dute.

5. SISTEMAREN DESKRIBAPENA

Azaldutako osagaiak erabilita, hurrengo irudian azaltzen dira gure proposamenak biltzen dituen agenteak eta komunikazioak



2. irudia. iBSE proposamena

Hautesleek, erabilpen-ingurune eta gaitasun guztietara egokitutako interfaze-tresneria erabiliko dute, botoa eman edo banakako egiaztapena eta erreklamazioa egiteko.

3. taula. iBSE interfaze-tresneria

	Itsuak/ Irakurtzen ez dakitenak	Gorrak/ Ezintasun gabekoak	Mugitze-ezintasuna dutenak
Periferikoak	**Datu-irteera**: Entzungailuak **Datu-sarrera**: Audiozko sagua	**Datu-irteera**: Pantaila **Datu-sarrera**: Teklatu birtuala pantaila ukigarrian	**Datu-irteera**: Pantaila **Datu-sarrera**: *Quadriplegic* sagua [19]
Boto-kabina	Audiozko argibideak	Idatzitako argibideak	Gurpil-aulkirako lekua
Urruneko sarbidea	*Multiple-casting*[1] edo *ingurune pribatua*[2]		

[1] *Multiple-casting:* botoa behin baino gehiagotan bidaltzea ahalbidetzen duen teknika, beti ere azken bertsioa zenbatzen delarik.

[2] *Ingurune pribatua:* hauteslekuetako boto-kabinetan bezala, hautesleak bere botoa emateko interfazearekin egiten dituen eragiketak beste inork ez ezagutzeko moduan egiteko beharrezko elementuak kontuan hartzen dituen kontzeptua, beste proposamenetan zehazten den *ingurune kontrolatu* kontzeptuari kontrajarria [21].

Interfaze-tresneria horrez gain, bi *smartcard* [20] txartel erabili beharko dituzte hautesleek. Smartcard gailuak, gaur egun oso zabalduak eta erabiliak dira; hala nola, sakelako telefonoetako SIM txartelak edo banketxeetako diru-txartelak dira smartcard adibideetako bi. Txartel hauek funtsean konputagailu osoak dira, eta ahalmena dute sorreran grabatutako sistema eragilea eta programak exekutatzeko. Honelakoetan oso abantailatsua da lortzen den exekuzio-ingurunea, hau da, sistemei ez diete eragiten konputagailu arruntetan hain arazo larria diren birus-erasoek, eta gainera gai dira sekretuak guztiz gordetzeko eta kriptografia-eragiketak egiteko.

Gaur egun gero eta memoria-ahalmen handiagoa dute, boto-sistema baten hautesle-programak beharrezko software guztia gorde eta exekutatzeko gai direlarik.

Gure iBSEan, esan bezala, hautesle bakoitzak bi smartcard erabili beharko ditu aldi berean. Bata Nortasun Txartela da (NT) eta hauteslea identifikatzeko balio du; besteak beste, herritar-identifikatzaile bakuna eta komunikazio digital seguruetarako kriptografia gakoak ditu. Bestea berriz, Boto Txartela da (BT), hauteslearen boto-programa edo agente-lana egiten duena. Hautetako bakoitzak ere, identifikatzaile bakuna du, kasu honetan bID (botoemate IDentitatea) deitu duguna; komunikazio seguruetarako kriptografia gakoak ere baditu. BT bakoitza, zein hautesleri egokitu zaion jakitea ezinezkoa izateko moduan banatuko da, eta ezertarako erabili baino lehen, NTrekin pertsonalizatu beharko du hautesleak. Horrela jakingo dugu BT hori pertsonalizatu zuena dela BT une horretan erabiltzen ari dena. Izan ere, iBSE agintaritzak ere herritar hori zehaztu ezin duelarik, kanal anonimoak jatorritik segurtatu behar dira.

Hautesleei baimenak banatu eta haien botoak gordetzeko, hainbat Hautesleku Birtualeko azpisistema batzuk daude. Botoa emateko fasean, (marra beltzeko komunikazioak), hautesle bakoitzaren BTak (hautesleekuko kabina edo urruneko sarbide batetik), lortuko du bere baimen-eskaera dagokion Hautesleku Birtualeko Agente Balidatzaileek egiaztatu eta itsuki sinatzea.

Baimen-eskaera hori NT txartelak sinatuta bidaltzen du, Balidatzaileei hauteslearen nortasuna ziurtatzeko; eskaera horretan bertan, hauteslea erabiltzen ari den BTaren bID identifikatzailea ere bidaltzen da, baina kriptografikoki *ezkutatuta*. Balidatzaile bakoitzak, hauteslearen nortasuna egiaztatuta, bere adostasuna adierazteko, ezkutatutako bIDa sinatuko du; ezkutatzeko erabiltzen den babes kriptografikoari esker, benetan zein bID sinatzen ari den ezingo du jakin, eta hortaz, ezingo ditu hautesleak eta BTak erlazionatu ere.

Hauteslearen BT txartelak Balidatzaileen sinadurak daramatzan erantzuna jasoko du, eta berau prozesatuz, edozeinek zuzen gisa egiazta dezakeen boto-baimena lortuko du.

Prozesamendu horretan, bID sinatuei ezkutatze-babes kriptografikoa kentzen die, sinadurak mantenduz. Boto-baimenak, egokitzat har dadin, Balidatzaile gehiengoaren bID berean egindako sinadurak eduki beharko ditu. Gure sisteman, Balidatzaileek, sinadura hautesleari dagokion hautesmahaiaren arabera egiten dute sinadura, eta beraz, lortzen den baimenak hautesleak parte hartu ahalko duen galdeketak ere zehazten ditu.

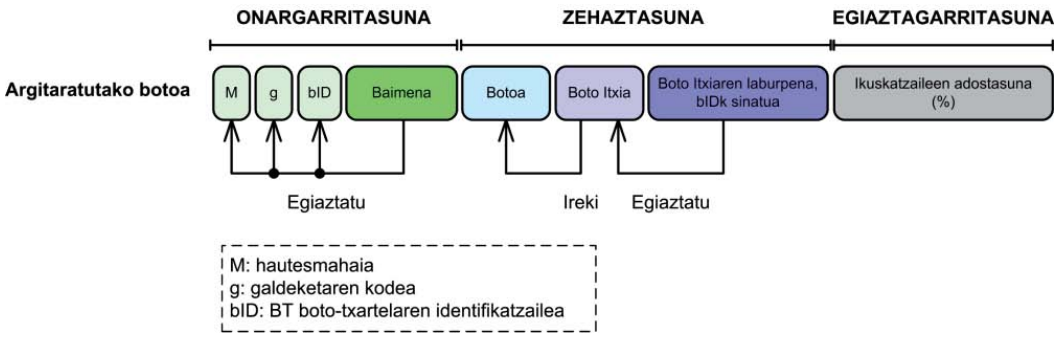
Baimena lortu ondoren, mezu anonimo batean (bID identifikatzailearekin bakarrik erlazionatu ahalko den mezu batean), baimena bera, galdeketa kodea eta kriptografikoki babestutako boto itxia bidaliko ditu hauteslearen BTak Hautestontzietara, eta horrela haietatik bere botoa gorde dutela adierazten duen gordekina lortuko du. Agente horiek, boto-baimena, galdeketa eta BTren boto itxia duen sinadura egokiak ote diren egiaztatuko dute eta horrela den kasuetan, bakoitzak bere datu-basean gorde eta erantzuneko gordekina eratzeko ekarpena sortuko du. Ekarpen horiez osatutako gordekinari esker, bere botoa ondo zenbatu den egiaztatu ahalko du hautesleak (banakako egiaztapena) argitaratzeko fasean eta ados ez egotekotan, erreklamatu ahalko du. Banakako egiaztapena eta erreklamazioa segurtasun osoz egin ahal izateko, botoa emateko fasea amaitutzat jo baino lehen hauteslearen BTak jasotako gordekina Erreklamazio Agenteek bakarrik erabiltzeko moduan babestuko du, kriptografiaren bidez.

Zenbatzeko fasean (marra berdeak), Biltze Azpisistemetan Hautestontzien datu-baseetako botoak zenbatzen dira, agintaritza eta ikuskatzaileen Zenbatzaileen artean. Ohiko hauteskundeetan bezala, esparru/galdeketa jakinetako emaitzak, Zenbatzaileen arteko adostasunez lortzen dira; iBSE honetan, eragiketa matematiko eta kriptografikoekin egiten da. Biltze Azpisistemetako tarteko emaitzok sare ezberdinetatik bidaltzen dira Egoitza Nagusira, datu-fitxategi handi horien garraioa akats-tolerantziarekin eginda.

Bertan, azken emaitzak Zenbatze Orokorreko azpisisteman kalkulatzen dira, berriz ere agintaritza eta ikuskatzaileen artean.

Argitaratzeko fasean web-zerbitzarien bidez plazaratzen dira emaitzak, hainbat eragiketa egiteko moduan:

— Edozeinek egiaztapen globala egin ahal du (marra gorria), boto bakoitzeko argitaratutako datu hauei esker:



3. irudia. Argitaratutako botoen datuak

— Hautesle bakoitzak, bere botoaren banakako egiaztapena eta erreklamazioa egin ahal ditu boto-kabinetatik (marra urdinak), Egoitza Nagusiko Erreklamazio Agenteekin. Eragiketa hauek segurtasunez egiten dira, lehen esan bezala, agente horiek bakarrik ireki dezaketen gordekin babestuan baitago beharrezko informazioa. Erreklamazioaren kasuan, informazio horrek, adieraziko du zenbatutako botoa eta hautesleak bidalitakoa bat ez datozela bakarrik, hauteslearen benetako aukera zein izan zen agertu gabe, eta pribatutasun propietatea ziurtatuz.

6. **PROPOSAMENEN BALIOA**

Gure proposamenetan oinarrituta eraikitako sistemak hauteskunde demokratikoak aurrera eramateko balio duela erakusteko, bi froga mota egin ditugu:

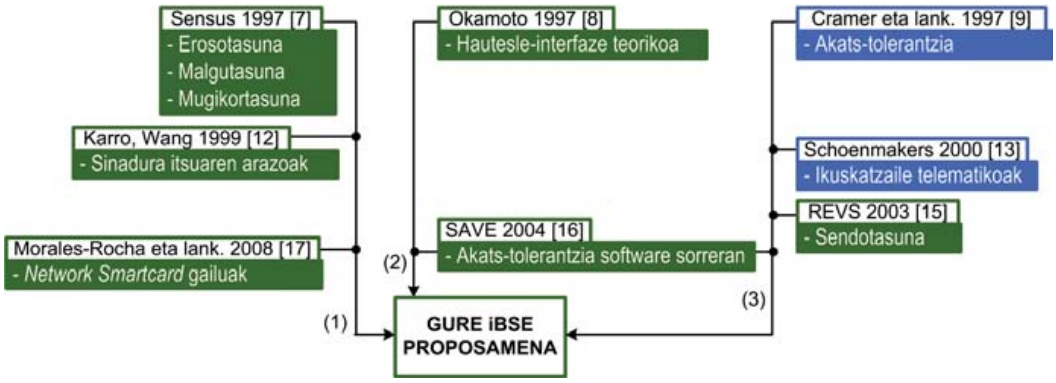
— *Common Criteria* [22] estandarrean iBSE-etarako zehaztutako segurtasun-helburuen betetze maila aztertu dugu. Mota honetako sistemetarako arau bakarra denez, gaur egun edozein iBSEren diseinua, gutxienez, horretan oinarritu behar da.
— Beste eskemetan egiazkotzat hartu den protokolo-zuzentasuna ere agerian utzi dugu. Horretarako, protokolo telematikoen analisirako metodologia erabili dugu; gure protokoloaren deskribapen formaletik abiatuta, egiaztatu dugu ProVerif izeneko *eredu-aztertze* aplikazioak [23] ezin duela erasorik kalkulatu.

7. **ONDORIOAK**

Informazio eta Komunikazio Teknologiek (IKTek) modu askotan hobetu ditzakete hauteskundeak demokraziaren erroetara hurbiltzeko, hots, herritarrei euren buruak gobernatzeko boterea emateko. Azken urteetan, hauteskundeak IKTekin hobetzen dituzten sistema asko proposatu dira; sistema hauek, erronka berriak ekarri dituzte telematika arloan.

Internet Darabilten Boto Sistema Elektronikoek historia mamitsua izan dute azken 30 urteotan. Proposamen garrantzitsu asko agertu dira epe honetan guztian, baina inplementazio praktiko gutxi, batez ere segurtasun, eskalagarritasun eta gizartearen onarpen faltarekin zerikusia duten arrazoi batzuengatik.

Gure proposamena ondoko irudi honetan adierazitako eskemetan oinarritu dugu:



4. irudia. Gure iBSE proposamenaren kokapena

Aurreko irudian, zenbakien bidez adierazi ditugu gure ekarpen nagusiak:

1. Sinadura itsuko eskemetako baimen errepikatuak eragotzi [12] eta mezu anonimo seguruak egiteko modua zehaztu dugu.
2. Botoa emateko hautesle-interfaze unibertsalaren eta urrunerako ingurune pribatuaren definizioa egin dugu.
3. Interes kontrajarrietako ikuskatzaileak erabili ditugu sendotasuna eta gardentasuna lortzeko eta beste eskemetan sortutako arazoak konpontzeko.

Egindako frogekin, erakutsi dugu telematikaren eskutik posible dela gaur egungo beste edozein Boto Sistema Tradizional eta Sistema Informatiko Banatu bezain seguru edo arriskutsua den iBSE unibertsal eta askea egitea. Gizarteak erabaki beharko luke ordea, hori nahikoa den, iBSE-ek eskain ditzaketen partaidetza mota berriak ustiatu ahal izateko.

ERREFERENTZIAK

[1] UNITED NATIONS. 1966 (1976tik indarrean). *International Covenant on Civil and Political Rights* 25. art. b atala. http://www.hrweb.org/legal/cpr.html

[2] CHAUM, D. 1981. «Untraceable electronic mail, return addresses, and digital pseudonyms». *Communications of the ACM* 24, 84-90.

[3] BENALOH, J. 1987. *Verifiable secret-ballot elections*. Dokt. Tesia, Yale University (AEB).

[4] FUJIOKA, A., OKAMOTO, T., OHTA, K. 1993. «A Practical Secret Voting Scheme for Large Scale Elections». *AUSCRYPT'92, LNCS* 718, 244-251.

[5] BENALOH, J., TUINSTRA, D. 1994. «Receipt-Free Secret-Ballot Elections (Extended Abstract)». *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, 544 - 553.

[6] SAKO, K., KILIAN, J. 1994. «Secure Voting Using Partially Compatible Homomorphisms». *Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology, LNCS,* 839, 411-424.

[7] CRANOR, L. F., CYTRON, R. K. 1997. «Sensus: A Security-Conscious Electronic Polling System for the Internet». *Proceedings of the Hawai`i International Conference on System Sciences,* 561-571.

[8] OKAMOTO, T. 1997. «Receipt-Free Electronic Voting Schemes for Large Scale Elections». URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.30.287 (2010eko maiatzean ikusia).

[9] CRAMER, R., FRANKLIN, M., SCHOEMAKERS, B., YUNG, M. 1996. «Multi-authority secret ballot elections with linear work». *Advances in Cryptology – EUROCRYPT'96, LNCS* 1070, 72-83.

[10] DURETTE, B. W. «Multiple Administrators for Electronic Voting». 1999. Bachelor's thesis, MIT (USA). URL: http://groups.csail.mit.edu/cis/theses/DuRette-bachelors.pdf (2010eko maiatzean ikusia).

[11] OHKUBO, M., MIURA, F., ABE, M., FUJIOKA, A., OKAMOTO, T. 1999. «An Improvement on a Practical Secret Voting Scheme». *LNCS* 1729, 771.

[12] KARRO, J., WANG, J. 1999. «Towards a Practical, Secure, and Very Large Scale Online Election». *Proceedings of the 15th Annual Computer Security Applications Conference* (ACSAC), 161-169.

[13] SCHOENMAKERS, B. 2000. «Fully Auditable Electronic Secret-Ballot Elections». URL: http://www.xootic.nl/magazine/jul-2000/schoenmakers.pdf (2010eko maiatzean ikusia).

[14] CARRACEDO, J., GÓMEZ, A., MORENO, J., PÉREZ, E. 2002. «Votación electrónica basada en criptografía avanzada (Proyecto VOTESCRYPT)». URL: http://vototelematico.diatel.upm.es/articulos/articulo_venezuela_revisado.pdf (2010eko maiatzean ikusia).

[15] JOAQUIM, R., ZÚQUETE, A., FERREIRA, P. 2003. «REVS- A Robust Electronic Voting System». *Proceedings of IADIS International Conference e-Society* 2003 , 95-103.

[16] SELKER, T., GOLER, J. 2004. «The SAVE system – secure architecture for voting electronically». *BT Technology Journal*, 22, 89 - 95.

[17] MORALES-ROCHA, V., SORIANO, M., MARTÍNEZ-PELÁEZ, R., RICO, F. 2008. «New multi-channel voting scheme: towards remote e-voting over the internet». *International Journal of Electronic Governance* 1, 155-173.

[18] AVIZIENIS, A. 1995. «The methodology of N-version Programming». *Software Fault Tolerance*, 23-46.

[19] MENG, L.F. 2004. «Applications of Computer Access Approach to Persons with Quadriplegics». *ICCHP 2004, LECTURE NOTES IN COMPUTER SCIENCE* 3118, 857-864.

[20] VEDDER, K., WEIKMANN, F. 1998. «Smart Cards – Requirements, Properties, and Applications». *COSIC'97 Course, LECTURE NOTES IN COMPUTER SCIENCE* 1528, 307-331.

[21] KRIMMER, R., TRIESSNIG, S., VOLKAMER, M. 2007. «The Development of Remote E-Voting Around the World: A Review of Roads and Directions». *VOTE-ID 2007, LECTURE NOTES IN COMPUTER SCIENCE* 4896, 1-15.

[22] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK. 2008. *Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products; BSI-CC-PP-0037*.

[23] BLANCHET, B. ProVerif. URL: http://www.proverif.ens.fr/ (2010eko maiatzean ikusia).