En design av ett I-röstningssystem för riksval

LUDVIG FORSBERG
och HARRY LI

KTH Datavetenskap
och kommunikation

Examensarbete
Stockholm, Sverige 2012

En design av ett I-röstningssystem för riksval

L U D V I G F O R S B E R G
o c h H A R R Y L I

DD143X, Examensarbete i datalogi om 15 högskolepoäng
vid Programmet för datateknik 270 och 300 högskolepoäng
Kungliga Tekniska Högskolan år 2012
Handledare på CSC var Johan Boye
Examinator var Mårten Björkman

URL: www.csc.kth.se/utbildning/kandidatexjobb/datateknik/2012/
forsberg_ludvig_OCH_li_harry_K12027.pdf

Kungliga tekniska högskolan
Skolan för datavetenskap och kommunikation

KTH CSC
100 44 Stockholm

URL: www.kth.se/csc

Sammanfattning

Syftet med denna rapport är att designa ett röstningssystem där väljaren skickar sin röst hemifrån över Internet. För att åstadkomma detta redovisas först ett resonemang om vilka krav som bör ställas på ett sådant röstningssystem, som t.ex. bevarandet utav valhemligheten, hög användarvänlighet och korrekthet samt motiveringen för detta. Därefter redogörs dessa krav i en mer utförlig beskrivning där rapporten bland annat tar upp krav som att alla har rösträtt, väljarfrihet samt att det finns en öppenhet med systemet. Med hjälp av dessa krav utförs en analys runt de möjliga designval som behöver tas, som t.ex. beslut rörande transport utav data, verifiering utav data samt autentisering av väljare. Därefter framställs designen utifrån denna analys. Designen fokuserar framförallt på att ge väljaren möjlighet att verifiera sin valröst samt minska beroendet utav känsliga komponenter i systemet. Efter det diskuteras ett par attacker och svagheter hos designen. I slutet dras slutsatsen att tidigare nämnd typ av röstningssystem åtgärdar många av de största problemen med dagens röstningssystem men samtidigt introducerar nya problem.

Redogörelse av samarbete

Först identifierade vi ett par sektioner som vi ansåg nödvändiga för rapporten tillsammans. Därefter delade vi upp sektionerna emellan oss, samlade in information om varsin sektion och skrev slutligen det första utkastet av dessa med referenser. Texterna har vi sedan tillsammans gått igenom och korrigerat, förbättrat samt integrerat med resten de andra texterna. Vi har även utfört text- och dokument estetik, bilder och designkonceptet tillsammans.

Grov uppdelning utav sektioner:

Sektion	Ansvar för första utkast & referenser
1.1 Problemformulering	Harry
1.2 Krav på allmänna val	Harry
1.3 Krav och traditionella röstningssystem	Harry
1.4 Traditionella röstningssystem och I-röstningssystem	Ludwig
2.1 Analys av krav på ett I-röstningssystem	Ludwig
2.2 Krav på ett I-röstningssystem	Harry
3.1 Röstning i Sverige idag	Harry
3.2 I-röstning i Estland	Ludwig
4.1 Beslutsunderlag	Ludwig
5.1 Valprocessen	Ludwig
5.2 Identifiering och Autentisering	Ludwig
5.3 Säkerhetskopiering	Ludwig
5.4 Verifiering	Ludwig
5.5 Granskning	Ludwig
5.6 Alternativa röstningsmetoder	Ludwig
6 Diskussion	Ludwig
7 Slutsats	Harry

Innehåll

1 Introduktion

Demokrati har sedan urminnes tider varit problematisk att implementera. Att en grupp människor har en vilja är lätt att konstatera, att makten över en grupp människor bör ligga hos gruppen självt är en någorlunda vedertagen föreställning. Men hur fångar man upp denna vilja, hur mäter man den? Det är den praktiska frågan som röstningssystem försöker att lösa.

Dagens röstningssystem har i grunden hundra år på nacken samtidigt har tekniken som hanterar information, den teknik som demokrati i praktiken är fullkomligt beroende utav, gjort dramatiska framsteg. Vi anser därför att det är dags att på allvar undersöka vilka problem som kan lösas med ett röstningssystem byggd med dagens teknik.

1.1 Problemformulering

Syftet med den här rapporten är att identifiera krav som ett I-röstningssystem måste uppfylla samt designa ett I-röstningssystem som kan användas till riksval i Sverige. Ett I-röstningssystem är ett röstningssystem där någon kommunikation i systemet sker över Internet [1]. Det vanligaste fallet är att den kommunikationen som sker över Internet är den mellan väljare (röstberättigad person i det specifika valet) och den enhet som lagrar valrösterna (information om väljarens val i det specifika valet).

I den här designen bortses generalla tekniker för att skydda systemet mot nätverksintrång och andra nätverksattacker, såsom brandväggar, IDS (Intrusion Detection System) eller IPS (Intrusion Prevention System) då detta ej är av intresse för designen. Verksamhetsåtgärder, såsom hur systemet introduceras till användare samt hur lång varje fas i valprocessen är (den fullständiga processen varmed väljarnas vilja registreras och offentliggörs) bortses av samma orsak liksom beslut nära implementeringen.

1.2 Krav på allmänna val

Det första kravet som ett röstningssystem måste uppfylla är att alla individer i ett samhälle får möjlighet att delta för att korrekt kunna registrera folkets vilja. Därefter att individer får möjlighet att rösta (att lägga sin valröst i ett val) på vad de vill inom de avgränsningar som existerar för valet. Röstningssystemet ska även motverka påverkan på individen som får denne att inte rösta efter egen vilja [2]. Eftersom lika mycket hänsyn ska tas till varje individs vilja så får det endast existera en valröst för varje individ i röstningssystemet. Beräkningen utav dessa valröster, d.v.s. röstningssystemets resultat, ska motsvara väljarnas vilja. Slutligen måste alla individer kunna granska röstningssystemet för att försäkra sig om att det uppfyller alla krav. Från detta kan man utröna följande krav på allmänna val[3]:

Alla ska ha rösträtt
Alla individer av myndig ålder i ett samhälle ska ha en realistisk möjlighet att delta i röstningssystemet.

Väljarfrihet
Alla väljare ska ha möjligheten att rösta på vad de behagar inom de avgränsningar som existerar för valet. Avgränsningar såsom att ett parti/person måste anmäla sig innan man kan rösta på denna/denne [4].

Valhemligheten får ej avslöjas
Det ska ej gå att utröna kopplingen mellan väljaren och väljarens valröst eftersom denna information kan användas för att påverka väljaren (t.ex. med trakasserier) utifrån den lagda valrösten samt för röstförsäljning (när en individ mot direkt betalning överlåter makten över innehållet i sin valröst till någon annan).

Väljaren har endast en röst
Alla väljare ska endast ha tillgång till en valröst per val. Alla valröster ska vara jämbördiga.

Resultatet ska vara korrekt
Beräkningen utav valröster ska genomföras på ett sätt som garanterar att varje valröst räknas en gång och summeras ihop jämbördigt för att resultatet ska motsvara väljarnas vilja.

Väljarna ska kunna granska röstningssystemet
För ett specifikt röstningssystem ska alla väljare kunna kontrollera att samtliga väljare och valröster i systemet hanteras på ett sätt som uppfyller kraven för ett röstningssystem [5]. Detta för att både öka väljarnas förtroende för systemet samt för att öka säkerheten i systemet genom att försöka upptäcka brister.

1.3 Krav och traditionella röstningssystem

Valprocessen i det traditionella röstningssystemet (röstningssystem där valrösten lagras på en fysisk sedel och räknas för hand) delas upp i fyra olika faser, förberedelsefasen, röstningsfasen, röstberäkningsfasen och avslutningsfasen. Förberedelsefasen är tidsperioden i valprocessen före röstningsfasen. Röstningsfasen är tidsperioden i valprocessen då väljaren kan lägga sin röst. Röstberäkningsfasen är tidsperioden i valprocessen då valrösterna räknas. Avslutningsfasen är tidsperioden i valprocessen efter röstberäkningsfasen [6].

I ett traditionellt röstningssystem uppfylls kravet om att alla ska ha en realistisk möjlighet att delta genom att främst fördela vallokalerna (som väljaren måste besöka för att rösta) inom rimliga avstånd till människor över hela landet.

I ett traditionellt röstningssystem kan ofta alla väljare ställa upp för att bli kandidater i valet. I Sverige tillåts väljare att t.o.m. skriva in helt egna partier och personer på en blank valsedel, därmed får väljaren i praktiken rösta på vad som helst [4].

Valhemligheten bevaras genom att väljaren endast tillåts att rösta i en viss vallokal. I vallokalen tvingas väljaren att både skapa sin valröst och sedan dölja valrösten genom att lägga det i ett neutralt kuvert i ett utrymme skyddat från övervakning.

Då väljaren endast tillåts att rösta i en specifik vallokal och funktionärer i vallokalen noterar vilka väljare som har lagt sin valröst i valurnan/valurnorna kan funktionärer kontrollera att varje väljare inte lägger ner mer än en valröst i valurnan/valurnorna.

Eftersom valurnorna är slutna och övervakas kan ingen person ta bort, lägga till eller ändra de valröster som redan finns i valurnorna förrän de ska beräknas. Resultatet beräknas sedan ofta ett antal gånger under olika tillfällen för att säkerställa att de beräknats korrekt [7-8].

Genom att tillåta väljare att agera som funktionärer samt medverka och övervaka själva röstberäkningsprocessen kan väljaren enkelt granska systemet på lokal nivå. En enskild väljare kan dock inte granska hela röstningssystemet själv p.g.a. att det är omöjligt att granska alla vallokaler och röstberäkningar samtidigt.

1.4 Traditionella röstningssystem och I-röstningssystem

I-röstningssystem skiljer sig från traditionella röstningssystem i flera avseenden. I det traditionella röstningssystemet kan röstningsmiljön, d.v.s. den miljö väljaren befinner sig i när denne röstar, säkras för att skydda valhemligheten. Detta blir tyvärr betydligt svårare i ett I-röstningssystem eftersom väljaren kan rösta hemifrån, vilket också leder till att det blir betydligt bekvämare att rösta.

I I-röstningssystem har man möjligheten att implementera betydligt mer kraftfulla åtgärder för att försäkra sig om att resultatet från röstningssystemet är korrekt.

En annan stor skillnad mellan I-röstningssystem och traditionella röstningssystem är att I-röstningssystem är mer komplexa [9]. Detta gör det både svårare för väljarna att använda systemet samt granska det. Komplexiteten i I-röstningssystem leder även till att väljare har olika förutsättningar för, och därmed möjligheter, att använda samt granska systemet.

I-röstningssystem är ofta väldigt centraliserade till skillnad från traditionella system vilket underlättar den nationella granskningen men samtidigt även underlättar manipulation av systemet i stor skala.

2 Krav

2.1 Analys av krav på ett I-röstningssystem

I grunden finns det tre viktiga övergripande krav som ett röstningssystem måste uppfylla för att vara användbart, nämligen att det har väljarnas förtroende, att det är användarvänligt för väljarna samt att det ger ett korrekt utfall [6].

- Saknas väljarnas förtroende för systemet kommer väljarna inte ha någon vilja att använda systemet.
- Saknas användarvänlighet för väljarna kommer väljarna inte att ha förmågan att använda systemet.
- Saknas ett korrekt utfall uppfylls inte systemets mening, nämligen att fastställa folkets vilja.

Tyvärr kolliderar dessa krav ofta. Maximal korrekthet åstadkoms endast på bekostnad utav förtroende eller användarvänlighet, o.s.v. Utmaningen blir att försöka finna den optimala kompromissen mellan dessa tre krav så att en maximal andel av väljarna får sina viljor registrerade.

Förtroende bygger framförallt på systemets enkelhet, transparens (förmågan till insyn av systemet) och förmåga att bevisa korrekthet. Man har större förtroende för ett system som är enkelt och som man i stor utsträckning förstår. Ett där man lätt kan kontrollera att systemet fungerar som det är meningen samt ett som ger starka bevis för att systemet ger ett korrekt utfall.

Användarvänlighet bygger framförallt på användargränssnittets enkelhet. Det i sin tur leder till begränsningar på komplexiteten av systemet.

Korrekthet bygger framförallt på kontroller och komplexa operationer och metoder för att säkerställa resultatet. Operationer som t.ex. bevarar valhemligheten, kontrollerar att bara en röst (abstrakt representation utav en persons vilja) per väljare räknas samt att väljaren själv tillåts granska resultat.

Då man konstruerade de allra första röstningssystemen var tekniken väldigt begränsad och förtroendet väldigt lågt därför ökade man förtroendet genom att maximera transparensen. På grund av detta valde man ofta att alla röstberättigade samlades på en viss plats, en viss tid. Rösta gjordes genom att räcka upp handen och resultatet utröntes med hjälp av ögat. Dessa system var väldigt transparenta. Det var lätt att klart och tydligt se vad alla röstade på och det var lätt att själv verifiera (att utföra en mängd definierade handlingar som syftar till att säkerställa något) resultatet. De hade dock två stora problem. Det första var att det fungerade endast på en mindre mängd människor. I det antika Aten löste man detta med att begränsa antalet röstberättigade människor, vilket däremot kraftigt går emot de demokratiska principerna [10]. Det andra problemet var att den totala transparensen resulterade i att det blev lätt för väljarna att sälja sina röster, vilket också gjordes. I det antika Atens röstningssystem blev försäljningen av röster så stor att röstning sågs som något i praktiken väldigt odemokratiskt [11].

Dagens röstningssystem konstruerades med hänsyn till dessa erfarenheter. För att möjliggöra demokrati i en grupp med en större mängd människor har man konstruerat en fysisk röstsymbol som man beräknar på lokal nivå och vars resultat sedan även beräknas i allt större områden tills alla röster är beräknade.

För att motverka försäljningen av röster konstruerades något som i Sverige kallas valhemligheten. Det är en princip som säger att en röst bör vara hemlig för alla andra än ägaren av rösten. I praktiken åstadkoms detta genom att ingen ska kunna utröna vad en annan individ har röstat på samt att man inte ska kunna bevisa för någon annan vad man har röstat på. Valhemligheten försvårar försäljningen av röster då köparen ej kan försäkra sig om att han verkligen fått det han betalade för. Båda dessa åtgärder har gjort röstning betydligt mer komplext, mindre transparent och i vissa avseenden även minskat användarvänligheten (mer komplicerat att lägga sin röst). Trots detta har förtroendet för systemet i och med att bevisen för korrekthet har stärkts och korrektheten av valresultatet har ökat tack vare bevarandet av valhemligheten.

I ett framtida I-röstningssystem kommer möjligheterna att öka användarvänligheten och korrektheten samt stärka bevisen för korrekthet att bli än större. Tyvärr kommer även komplexiteten att öka och transparensen att minska ännu mer. Därför bör det vara av yttersta vikt att fokusera på förtroende för I-röstningssystem eftersom det är I-röstningssystemets svaga punkt. Detta bör åstadkommas genom att minimera komplexiteten, maximera transparensen samt förstärka bevisen för korrekthet.

2.2 Krav på ett I-röstningssystem

2.2.1 Alla har rösträtt

I-röstningssystemet måste sträva efter att ge alla användare lika möjligheter att använda systemet. För att uppnå detta måste I-röstningssystemet ha ett väljargränssnitt som är begriplig och lätt att använda av alla. I-röstningssystemet får inte heller försvåra för väljarna att registrera sig inför ett val. Uppfylls dessa krav så har en väljare lika möjligheter att använda systemet oberoende om väljaren har ett funktionshinder eller begränsade datorkunskaper.

I-röstningssystemet ska innehålla åtgärder för att bibehålla systemets integritet (att systemet ej är obehörigt eller oavsiktligt förändrat) samt skydda tillgängligheten av systemets tjänster under röstningsfasen. Systemet bör ha åtgärder som motverkar bl.a. systemhaveri, funktionsfel och systemavbrott. I händelse av att några av dessa problem inträffar ska väljaren ges möjlighet att rösta vid ett senare tillfälle.

I-röstningssystemets ska se till att transporten av valrösten över Internet går så fort som möjligt. Valröster som inkommit från Internet ska endast accepteras av systemet under röstningsfasen med viss marginal för att ta hänsyn till eventuella förseningar av valrösten under transporten över Internet [12].

2.2.2 Väljarfrihet

I-röstningssystemet ska ge väljarna möjligheten att kunna rösta på det alternativ denne önskar även om det skulle innebära att väljaren väljer att rösta blankt [13]. Det bör inte vara orealistiskt omständigt för väljaren att rösta på ett sällsynt parti.

Efter att röstningen är klar ska I-röstningssystemet skicka tillbaka en bekräftelse till väljarna med information om statusen på dennes valröst. I-röstningssystemet ska tydligt ange till väljaren om röstningen har varit framgångsrik, om det har stött på något problem samt om hela röstningsförfarandet har fullbordats. Väljaren ska kunna ändra sin valröst när som helst under röstningsfasen och få en bekräftelse på att dennes röst har ändrats. Väljaren ska kunna avbryta röstprocessen utan att dennes valröst registreras och väljaren ska även få en bekräftelse av att valrösten inte lagrats.

2.2.3 Valhemligheten får ej avslöjas

I-röstningssystemet ska skydda mot avslöjande utav känslig information om väljaren och dennes röst under valprocessen samt granskning utav systemet. Systemet ska därför verka för att valrösten och

valrösterna som räknas är och förblir anonyma under valprocessen samt motverka möjligheten att rekonstruera en länk mellan varje enskild väljare och dennes valröst. Valröst och väljarinformation ska förseglas så länge data förvaras på ett sådant sätt att de kan kopplas till varandra. Särskilt viktigt är att autentiseringsinformationen ska separeras från väljarens valröst vid ett fördefinierat steg i valprocessen [6]. Åtgärder ska även vidtas för att säkerställa att den information som behövs vid röstberäkningen inte kan användas för att identifiera väljaren och dennes valröst. Flera tänkbara åtgärder bör användas för att minska risken för bedrägeri eller obehörigt agerande som kan påverka I-röstningssystemet under valprocessen.

Om det skulle finnas någon information som kan koppla väljaren med dennes röst ska informationen endast vara tillgänglig för behöriga.

I-röstningssystemet ska göra det omöjligt för väljaren att konstruera ett kvitto som kan bevisa vem denne har röstat på. Detta är ett måste för att minska möjligheten att köpa valröster. Därför bör en väljare bemyndigas att kunna rösta om så många gånger som denne vill och vid varje ny valröst ska den gamla valrösten ersättas av den nya. Detta förhindrar även familjeröstning, d.v.s. där en väljares val påverkas av en dominant familjemedlem vid röstningstillfället [14]. Efter att väljaren har röstat klart är det extremt viktigt att I-röstningssystemet raderar alla uppgifter i samband med väljarens röstprocess från användargränssnittet.

Vid undantag, störningar och krascher ska inte I-röstningssystemet avslöja koppling från den sista väljaren till dennes röst.

2.2.4 Väljaren har endast en röst

Vid riksval ska I-röstningssystemet kunna identifiera väljaren och hindra väljaren från att sätta in mer än en valröst i I-röstningssystemet.

I-röstningssystemet ska även garantera att vid systemhaveri ska ingen väljare förlora sin valröst eller på något vis få möjligheten att lägga två valröster.

2.2.5 Resultatet ska vara korrekt

I-röstningssystemet ska bara lagra de valröster som kommer från autentiserade väljare. All annan tillgång till I-röstningssystemet för väljaren ska nekas. I-röstningssystemet ska inte påverka väljarnas beslut samt förhindra annan påverkan på väljaren under valprocessen.

Kommunikation mellan enheter i I-röstningssystemet kräver verifiering utav enhetens autenticitet (att det är den korrekta enheten man kommunicerar med) [12]. Om autenticitet ej kan styrkas ska kommunikationen avbrytas. I-röstningssystemet ska inte påverkas utav andra system som tillhör väljaren.

När det gäller verifikation av valresultatet måste I-röstningssystemet kunna verifiera att antalet människor som har röstat stämmer överens med antalet valröster som finns i systemet. Även andra funktioner i I-röstningssystem som kan påverka korrektheten av resultaten ska kunna kontrolleras.

I-röstningssystemet ska möjliggöra en omgjord röstningsfas och röstberäkningsfas om nödvändigt. För att verifiera korrektheten av valrösterna ska I-röstningssystemet tillhandahålla funktionalitet som möjliggör en omgjord röstberäkningsfas samt uppladdning av alla valröster till andra beräkningsmoduler. Detta gör verifikation utav röstberäkningen med flera olika implementationer möjligt för att garantera korrektheten under röstberäkningsfasen.

Vid systemfel ska I-röstningssystemet ge återkoppling till alla parter i form av ett felmeddelande där det står vad för typ av händelse som har skett, t.ex. om det är ett systemhaveri eller någon typ av funktionsstörning.

2.2.6 Väljarna ska kunna granska I-röstningssystemet

Informationen om hur I-röstningssystemet fungerar i allmänhet samt information om samtliga komponenter ska göras tillgänglig för allmänheten [6,8]. Men informationen om data rörande själva valet i I-röstningssystemet ska bara lämnas ut till valmyndigheten.

Valmyndigheten ska utse parterna som har tillgång till den centrala infrastrukturen samt datan i systemet för granskning. Det ska finnas tydliga bestämmelser och regler för sådana utnämningar.

3 Bakgrund

3.1 Röstning i Sverige idag

3.1.1 Förberedelsefas

I förberedelsefasen bestäms individens rösträtt av Skatteverkets folkbokföringsregister. I Sverige har alla medborgare över 18 års ålder med bostadsort rösträtt [8]. Alla som har rösträtt kommer automatiskt att hamna i en röstlängd (en lista med väljare i ett visst valdistrikt) och få ett röstkort hemskickat.

3.1.2 Röstningsfasen

I dagens Sverige kan den som får rösta, rösta på 4 olika sätt [15].

- Rösta i ens vallokal på valdagen
- Förtidsrösta i vissa vallokaler
- Rösta från utlandet
- Rösta med ombud

Röstning i ens vallokal på valdagen

På valdagen får man endast rösta i den vallokal som står på röstkortet. I vallokalen tar väljaren valkuvert samt valsedlar, går bakom en valskärm, skriver/kryssar på valsedeln och lägger dem i kuverten. Endast en valsedel ska läggas i varje kuvert och därefter ger väljaren kuvertet till en funktionär samt legitimerar sig. Funktionären kontrollerar att väljaren inte har röstat förut, sedan lägger funktionären ner kuvertet i en valurna och prickar av väljaren i röstlängden. En röst på valdagen har företräde gentemot alla andra röster du lagt. År 2010 röstade hela 60 % på valdagen i Sverige [15].

Förtidsrösta i vissa vallokaler

Förtidsröstning fungerar på ett snarlikt sätt som röstning på valdagen. Skillnaden är att man kan rösta så tidigt som 18 dagar innan själva valdagen, att man kan rösta i vilken vallokal som helst samt att man måste ha med sig röstkortet. Funktionären lägger nu endast valkuverten tillsammans med röstkortet i ytterligare ett kuvert innan det läggs i en uppsamlingslåda. Efter att vallokalerna stängs på valdagen så öppnas uppsamlingslådan i väljarens valdistrikt och väljaren prickas av i röstlängden.

Rösta från utlandet

Röstning från utlandet är mer eller mindre en förtidsröst. Väljaren måste själv införskaffa valsedlar samt valkuvert och två vittnen måste intyga att rösten blivit lagd på ett korrekt sätt. Rösten läggs därefter i ett brev och postas.

Rösta med ombud

Man kan även både förtidsrösta och rösta på valdagen via ombud. Vid röstning med ombud införskaffas valkuvert och valsedlar av ombudet. Väljaren röstar då med dessa och ger tillbaka dem till ombudet. Därefter intygar budet, ett vittne och väljaren att allt gått rätt till. Slutligen tar budet valrösten och lämnar in det på en vallokal på valdagen eller en vallokal för förtidsröstning. För att få rösta med ombud måste väljaren vara väldigt sjuk, funktionshindrad, gammal eller vara intagen på ett/en häkte/kriminalvårdsanstalt [16].

3.1.3 Röstberäkningsfasen

Röstberäkningen börjar direkt i vallokal efter att den stängts på valdagen för att få fram ett preliminärt resultat. Därefter skickas alla valrösterna från vallokalerna till länsstyrelsen. Alla röster som inte har hunnit komma in till vallokalerna på valdagen beräknas hos valnämnderna. De granskar även röster som har blivit underkända från valdagen. Därefter skickas även alla dessa röster till länsstyrelsen. Länsstyrelsen utför sedan den sista och giltiga beräkningen utav rösterna. Under samtliga beräkningar får vem som helst närvara och granska processen. Man uppskattar att mellan 30 000 till 40 000 människor varje val år får ersättning för att hjälpa till med valet [17].

3.1.4 Avslutningsfas

När väl resultatet är framställt så lagras alla valröster hos länsstyrelsen under mandatperioden [8].

3.2 I-röstning i Estland

I Estland påbörjades det projekt som skulle resultera i ett I-röstningssystem redan 2003. I-röstningssystemet från det projektet användes första gången 2005 i ett lokalval. Sedan har det även använts i parlamentsvalet 2007, Europaparlamentsvalet 2009, lokalvalet 2009 samt parlamentsvalet 2011 utan några allvarliga komplikationer [18]. Parlamentsvalet 2007 i Estland är världens första riksval utfört med ett I-röstningssystem [19] och 2011 röstade 24,3 % av alla röstande via I-röstningssystemet [18].

Systemet är uppbyggt av i stort sett 3 huvudkomponenter, en webbserver (som tar emot röster från Internet), en röstlagringskomponent samt en rösträknare och använder i huvudsak asymmetrisk kryptering (för mer information om asymmetrisk kryptering se 4.1.3 Analys av krypterings metoder) [20]. Systemet använder sig även utav ett statligt utfärdat ID-kort för autentisering, med autentisering menas bevisandet av att en enhet (i detta fall väljare) är den som den utger sig att vara [21].

Systemet används som ett komplement till det traditionella röstningssystemet, d.v.s. man kan fortfarande rösta som vanligt på valdagen, för att försäkra sig om att alla kan delta i valet. Valhemligheten skyddas genom uppdatering utav röster (att man kan ersätta sin gamla röst med en ny röst en eller fler gånger), att kopplingen mellan valrösten och väljaren endast existerar då valrösten är krypterad samt att hanteringen utav nyckeln till dekrypteringen är aktsam. Med denna nyckel kan man nämligen dekryptera alla valröster i systemet. Endast en valröst per väljare tillåts i systemet genom att undersöka kopplingen mellan väljaren och en krypterad valröst. Korrektheten utav resultatet försäkras med diverse loggfiler och koder som kontrollerar integriteten hos den digitala datan. Väljaren tillåts endast granska systemet via sin valmyndighet [22].

4 Analys av designval

4.1 Beslutsunderlag

För att avgöra vilka processer som ska användas för att utföra kritiska funktioner i I-röstningssystemet listas lämpliga alternativ upp, en konsekvensanalys görs och utifrån den avgörs vilken process som är att föredra. Tyvärr är empiriska studier för att styrka dessa designval sällan möjliga att genomföra men har använts i den mån det är möjligt.

4.1.1 Analys av övergripande systemdesign

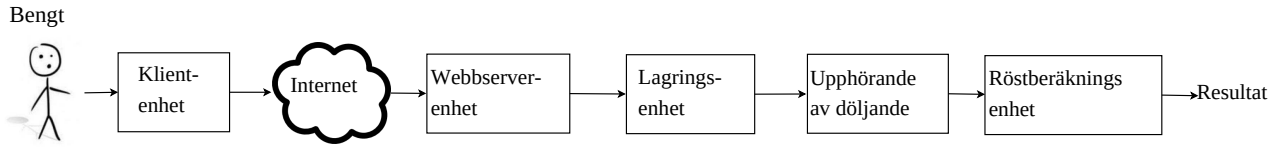
För att kunna skicka valrösterna i ett I-röstningssystem måste först en klientenhet existera som skickar valrösten över Internet till resten av systemet samt sköter kommunikationen mellan resten av systemet och väljaren.

För att ta emot valrösterna i ett I-röstningssystem måste en webbserverenhet existera. Denna bör endast ta emot valröster och annan nödvändig information och skicka den vidare till resten av systemet. Webbserverenheten bör dessutom vidarebefordra eventuella meddelanden från systemet till väljaren.

För att kunna räkna valröster kan man inte summera ihop valrösterna direkt utan man måste lagra dem. Först efter att själva röstningsfasen är över kan man räkna ihop dem. Koppling måste finnas mellan den lagrade rösten och väljaren i systemet vilket givetvis utgör ett stort problem då denna koppling potentiellt kan användas för att avslöja valhemligheten. Tyvärr finns det ingen väg runt detta. Denna koppling är däremot ett mindre problem för valhemligheten än de problem som ett I-röstningssystem utan uppdatering av valröster skulle medföra. För att försäkra sig om att denna koppling inte används obehörigt så bör den endast finnas i en isolerad enhet, en lagringsenhet, med endast denna funktion. I denna enhet bör även valrösterna lagras i slumpmässig ordning så att man inte från ordningen kan identifiera väljares valröster.

För att försvåra själva användandet av kopplingen mellan väljare och valröst (utifall den hamnar i fel händer) så bör man försöka att med en reversibel metod dölja röstdata (eftersom den måste visas igen vid räkning senare) och med en potentiellt irreversibel metod dölja identifikationen. För att kunna använda kopplingen måste man därmed lösa båda dessa data döljande metoderna. Funktionen för att upphäva döljandet bör endast finnas i en separat enhet med endast denna funktion.

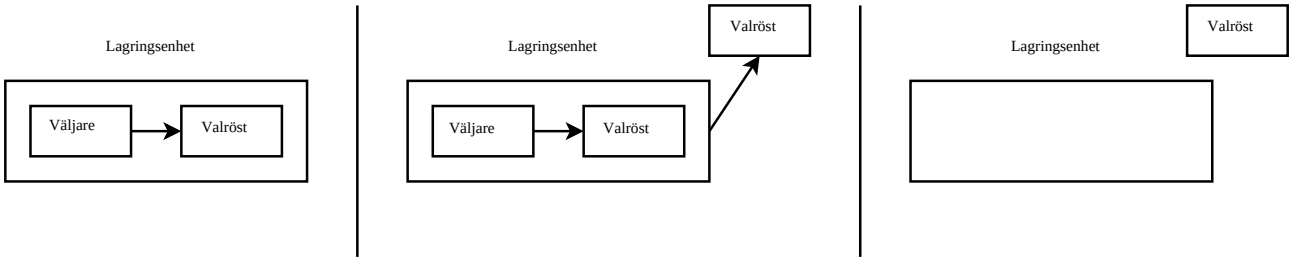
Slutligen måste det även finnas en enhet som räknar ihop utfallet från rösterna. För en övergripande modell utav systemet se figur 1 på sidan 8.



Figur 1: Abstrakt modell över röstningsprocessen i systemet.

En övergripande design med minimal information

Vill man minimera risken för att valhemligheten avslöjas och har ett mindre behov av att väljare ska kunna verifiera sin röst bör man, liksom i Estland, förstöra kopplingen mellan väljare och valröst så fort som möjligt. Ett lämpligt sätt att förstöra den på vore att exportera datan med valröster separat från identifikation- och autentiseringsdata samt därefter rensa all data i lagringsenheten (se figur 2 på sidan 9).



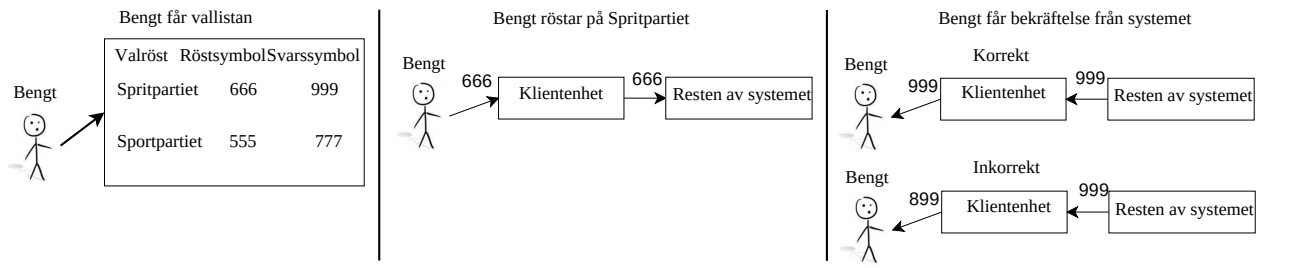
Figur 2: Modell av förstörandet utav koppling mellan väljare och valröst i lagringsenheten.

En övergripande design med maximal information

Skulle man vilja ge väljaren möjlighet att själv verifiera att ens egen valröst registrerats och räknats korrekt måste man tolerera att hotet mot valhemligheten ökar. En lista kan t.ex. publiceras med samtliga valröster som beräknats där varje valröst offentliggörs tillsammans med någon unik information som ägaren av rösten känner till. Väljaren som har röstat kan då söka igenom listan, hitta sin egen röst med hjälp av denna information och sedan verifiera att valrösten är korrekt. Detta kräver dock att en koppling mellan valrösten och väljaren publiceras samt måste existera under hela valprocessen. Denna koppling måste även konstrueras innan någon röst är lagd då systemet annars har möjligheten att ge olika väljare som har lagt samma valröst samma unika verifieringsinformation, d.v.s. koppla olika väljare till samma publicerade valröst. Verifieringsinformationen kan förslagsvis vara en så unik siffra att sannolikheten att gissa denna siffra för någon valröst är låg. Siffran måste också förmedlas på ett sätt som gör det omöjligt för väljaren att bevisa för någon annan att detta är väljarens korrekta siffra. I praktiken spelar det ingen större roll om man kan bevisa att den unika siffran är väljarens eftersom köparen kan betala först efter att valrösten verifierats. Även om säljaren har möjligheten att ge köparen en felaktig siffra och dessutom har tur nog att en korrekt valröst med denna siffra i resultatet existerar, är sannolikheten för detta så låg att det fortfarande är lönsamt för köparen.

En övergripande design med verifiering utav klientenhetens funktion

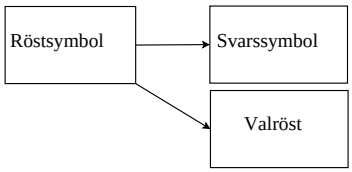
Klientenheten är den enda komponenten i systemet som väljaren måste ansvara för själv eftersom den verkar på väljarens dator. Därför skulle man vilja försäkra sig om att valrösten registrerats korrekt utan att behöva förlita sig på klientenheten. Detta skulle man kunna göra genom att skapa en slumpmässig samling symboler (förslagsvis siffror) som symboliserar en viss valröst samt där varje potentiell valröst har två unika symboler. Den grundläggande idén är att väljaren ska få en lista med alla möjliga valröster som väljaren skulle kunna välja och där varje valröst har en röstsymbol och en svarssymbol. Röstsymbolen kan väljaren skicka till resten av systemet via klientenheten och väljaren får sedan tillbaka en svarssymbol som denna kan verifiera med sin lista (se figur 3 på sidan 9). Givet att väljaren har förtroende för resten av systemet kan väljaren då vara säker på att klientenheten har hanterat dennes valröst korrekt.



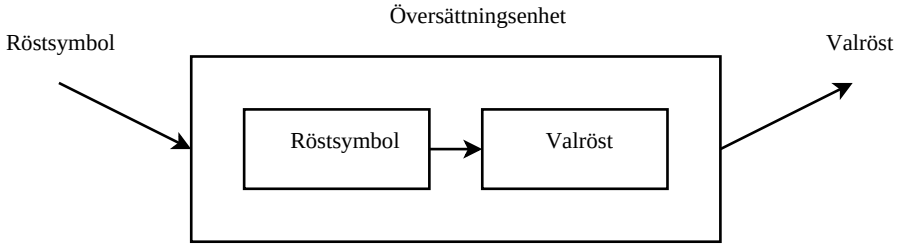
Figur 3: Modell utav väljarens röstande samt valröst verifiering.

Detta kräver dock en hel del av designen. Först måste man skapa en samling av unika röst- och svarssymbolspar för varje väljares potentiella valröst och förmedla dessa till väljaren under förberedel-

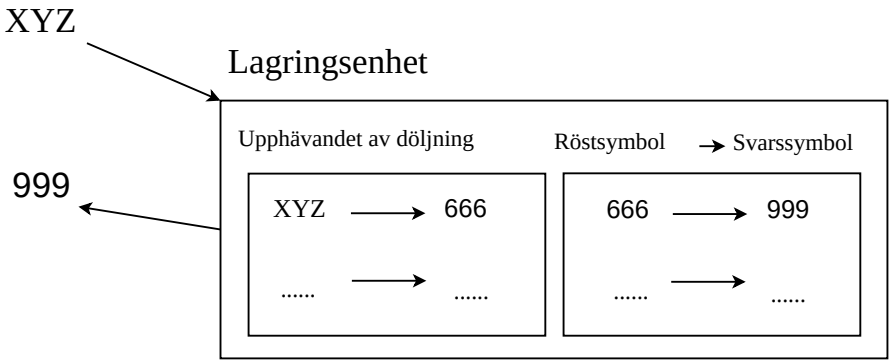
sefasen. Denna information måste sedan förstöras på ett säkert sätt eftersom den innehåller väldigt mycket känslig information. Därefter måste man i systemet ha en koppling mellan röst- och svarssymbolspar för att man ska få tillbaka rätt svarssymbol. Sedan måste även en koppling mellan röstsymbol och valröst existera för att man ska kunna få fram den korrekta valrösten (se figur 4 på sidan 10). Denna koppling bör användas i en separat enhet, en översättningsenhet, för att översätta röstsymbolen till en valröst (se figur 5 på sidan 10). Röstsymbolen måste döljas vid transport över Internet. Döljandet måste sedan upphävas vid ankomst till lagringsenheten för att denna ska kunna skicka en korrekt svarssymbol tillbaka samt verifiera väljaren (se figur 6 på sidan 10). Detta gör att upphävande av döljandet måste ske under röstningen vilket ökar risken för att döljandet avslöjas. För att öka säkerheten kan en till oberoende döljning införas som döljer själva valrösten i kopplingen mellan röstsymbol och valröst. Detta gör att en till enhet behövs för att upphäva detta döljande innan valrösterna kan beräknas. För ett exempel på systemets röstningsprocess se figur 7 på sidan 10.



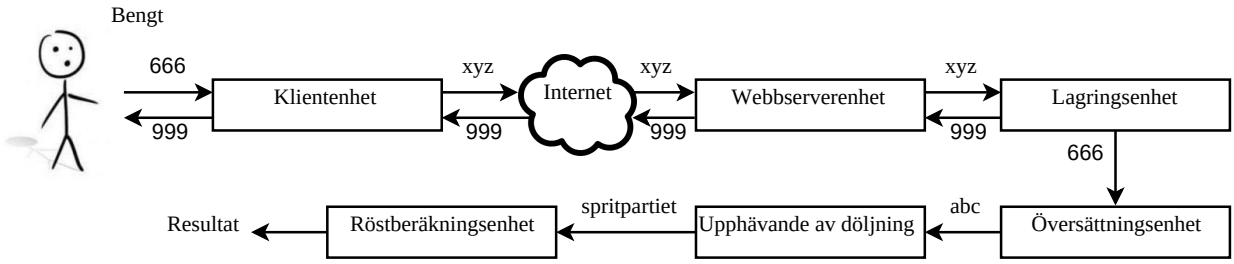
Figur 4: Modell utav kopplingen mellan röstsymbol, svarssymbol samt valröst.



Figur 5: Modell utav översättningsenheten.



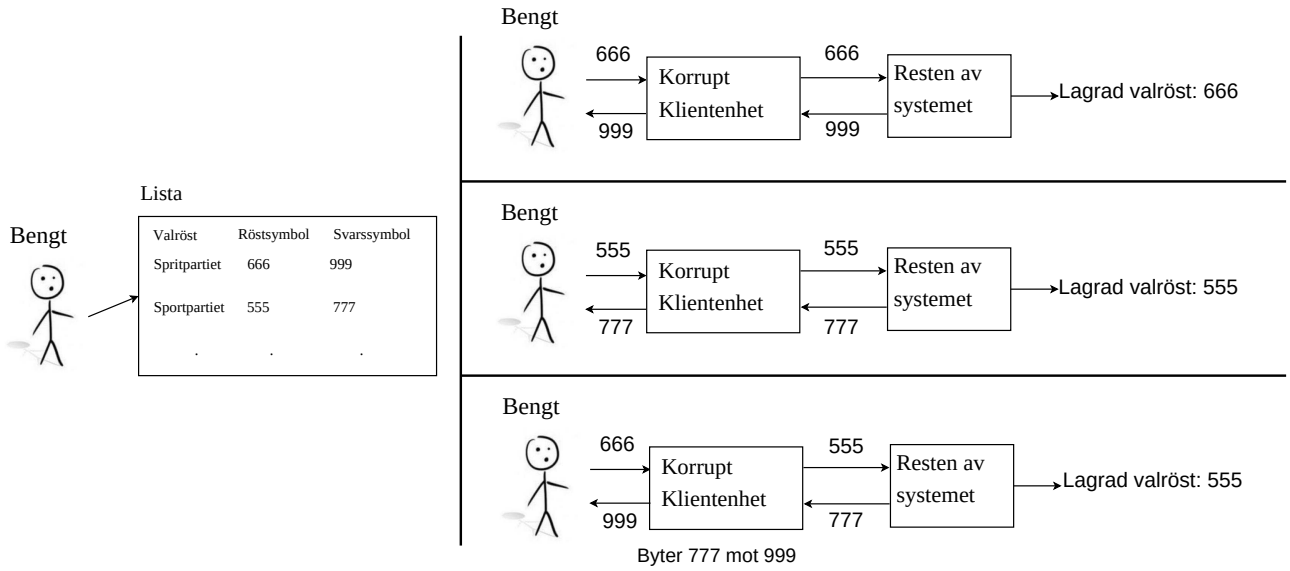
Figur 6: Modell utav lagringsenhetens process för att returnera korrekt svarssymbol.



Figur 7: Ett exempel på en röstningsprocess i systemet.

Ett problem med denna lösning är att man måste specificera alla möjliga valröster innan röstningsfasen påbörjas vilket även begränsar antalet möjliga valalternativ. Ytterligare ett problem är att systemet

blir komplext och att det skapas mycket känslig information som måste hållas åtskilt från varandra eller förstöras. Klientenheten kan också fortfarande lura en väljare om denne försöker rösta med samma valröst mer än en gång eftersom klientenheten kan spara röstkoderna samt svarskoderna och dessa två ej ändras. Ett exempel är om en väljare röstar på A, sen B och till sist ångrar sig och röstar på A igen så kan klientenheten sista gången skicka röstkoden för B, istället för A, och visa A:s svarskod till väljaren som då tror att denne röstat med valröst A, se figur 8 på sidan 11.



Figur 8: Beskrivning av en attack på systemet genom klientenheten.

En övergripande design bestående av en kombination utav flera designer

Olika människor har olika önskemål på ett röstningssystem, somliga föredrar att valhemligheten skyddas medan andra att korrektheten säkras. För att tillmötesgå båda dessa önskemål skulle man kunna kombinera olika designer till en enda design. I händelse av att ett av dessa system skulle få ett systemhaveri kan en väljare i värsta fall använda något av de andra delsystemen för att rösta.

Däremot skulle det i många fall bli den svagaste designen som utgör miniminivån av säkerhet mot ett visst hot för den gemensamma designen. Den designen som sämst skyddar mot röstförsäljning skulle t.ex. kunna användas för röstförsäljning vilket skulle göra de andra designernas skydd mot röstförsäljning helt redundanta. Det skulle även uppkomma flera integrationsproblem mellan dessa designer, t.ex. måste man försäkra sig om att en väljare bara får en röst registrerad i samtliga delsystem. Dessutom behöver man bara lyckas manipulera ett av delsystemen för att manipulera hela valresultatet.

4.1.2 Analys av transportmetoder

Transporten till systemet sker via Internet. Eftersom Internet är ett öppet nätverk där diverse routrar har möjlighet att läsa av eller t.o.m. ändra informationen som skickas så måste man försäkra sig om att informationen både behåller sin integritet och sekretess (förhindrande av obehörigt avslöjande av information).

Idag finns det mer eller mindre bara en vedertagen metod för att uppnå detta och det är kryptering. Därför bör den röstande personens dator först identifiera och autentisera sig. Därefter bör meddelandet skickas i krypterad form till systemet som på något sätt bör kunna verifiera att meddelandet kommer från den personen som tidigare identifierade och autentiserade sig.

Om man skulle välja kryptering för döljandet utav information vid transportering så kan döljandet av ett meddelande alltid i teorin upphävas genom att helt enkelt testa alla möjliga potentiella nycklar

(med hjälp av nyckeln kan man sedan dekryptera meddelandet). Att man skulle lyckas dekryptera ett krypterat meddelande under röstningsprocessen är inte troligt med en tillräckligt svårgissad nyckel. Men att man kan göra det ett antal år senare och avslöja vad någon röstade på är däremot relativt troligt [23].

Detta problem förvärras utav att metoder som gör en nyckel svårare att gissa även försvårar användandet utav nyckeln (tiden för att kryptera/dekryptera ökar) vilket i sin tur leder till att nyckeln helst ska vara svårgissad men inte alltför svårgissad. Dessutom ökar kapaciteten för antalet gissningar en dator klarar av att utföra per tidsenhet kraftigt med tiden. Detta leder till att en nyckel som idag skulle kräva ca 20 år för en dator att hitta, fyra år senare endast kanske behöver fem år (enligt Moores lag [24]).

I ett I-röstningssystem är kraven på prestanda hos krypteringssystemet inte höga vilket gör att man har råd att använda mer svårgissade nycklar. Men faktumet att det blir en tidsfråga innan valhemligheten avslöjas med ett kryptosystem kvarstår. Har man däremot i åtanke att syftet med valhemligheten främst är att motverka röstförsäljning och att skydda väljaren mot påverkan såsom trakasserier inser man ganska snart att det är ett mindre problem. Få är beredda att köpa en valröst om man kan konfirmera att man fick valrösten först 20 år senare och få är intresserade av att trakassera någon för ett val som gjordes för 20 år sedan.

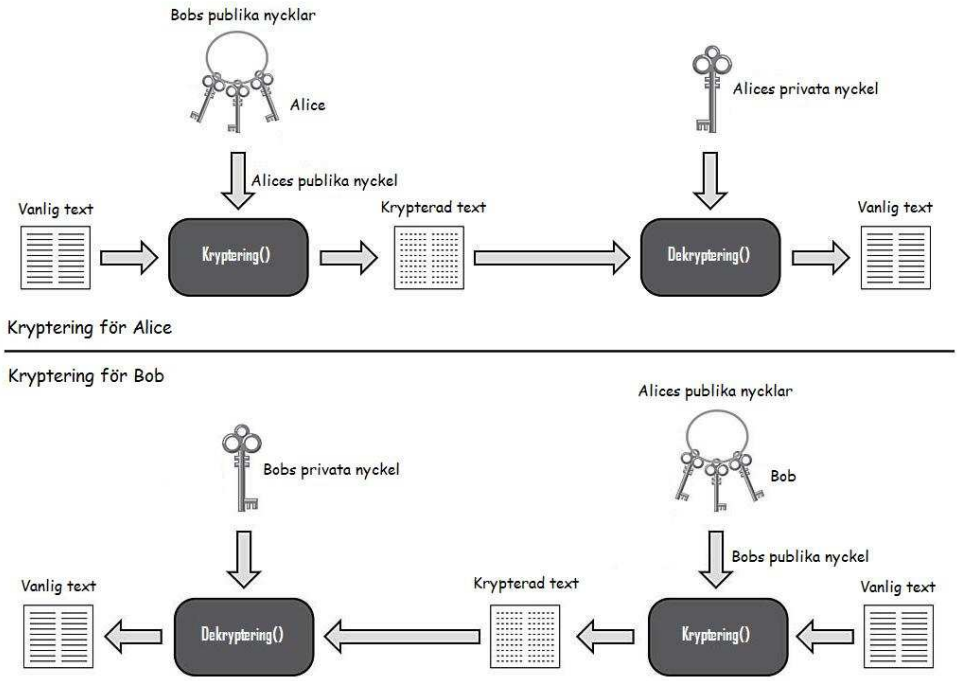
När det gäller att transportera data mellan eventuella enheter inom systemet kan man antingen använda någon form av nätverk eller ett externt lagringsmedium (som en DVD-skiva eller USB-minne) som fysiskt fraktas mellan enheterna. Nätverk är snabba och smidiga medan en fysisk transport utav externa lagringsmedium är betydligt mer omständigt men också säkrare. Omständigheten är däremot ett lågt pris att betala och därför bör fysisk transport av externa lagringsmedium i så stor utsträckning som möjligt användas.

4.1.3 Analys av krypteringsmetoder

Det finns två kategorier utav kryptering, asymmetrisk och symmetrisk kryptering. Symmetrisk kryptering är en teknik som innebär att man använder samma nyckel för att både kryptera som att dekryptera ett meddelande. Asymmetrisk kryptering är en teknik som innebär att man använder två olika nycklar, en öppen för andra att kryptera med och en egen privat för att kunna dekryptera med (se figur 9 på sidan 13). Fördelarna med symmetrisk kryptering är att den är relativt snabb och tekniken är på en hög abstraktionsnivå enkel att förstå. Nackdelen är att den förutsätter en annan säker kanal för förmedling av nyckeln. Fördelarna med asymmetrisk kryptering är att den endast kräver en osäker kanal för förmedling utav nyckeln. Nackdelen är att den inte är lika snabb som symmetrisk kryptering samt svårare att förstå [25]. Då skapandet av en annan säker kanal för förmedlingen av nyckel framförallt vore alltför komplicerat så är asymmetrisk kryptering att föredra.

Ett av de mest ansedda asymmetriska kryptosystemen bör användas eftersom de är gediget undersökta, använda och testade. De mest välansedda asymmetriska krypteringarna är ElGamal, RSA OAEP, Pailliers kryptosystem, ECC och Cramer-Shoups kryptosystem [26].

Både ElGamal och Pailliers kryptosystem har en väldigt intressant "formbarhets" egenskap, såsom att det är lätt att givet en krypterad text går att generera en annan giltig krypterad text. Dessa två kryptosystem har även en speciell typ av formbarhets egenskap som kallas homomorfi. Det innebär att en operation på en krypterad text är ekvivalent med en operation på den dekrypterade texten [27]. Pailliers kryptosystem är dessutom additivt homomorfisk vid multiplikation (om man multiplicerar en krypterad trea med en fyra och sedan dekrypterar svaret så får man en sjua) [28]. Detta skulle kunna användas för att enkelt summera ihop hela resultatet utan att dekryptera valrösterna. Tyvärr skulle det medföra vissa konkreta problem, t.ex. skulle man vara tvungen att säkerställa att valrösterna är korrekta innan man multiplicerar/adderar dem. Detta för att undvika att en väljare skickar in en -1 valröst eller en +2 valröst till systemet som sedan aningslöst adderar/multiplicerar valrösten till resultatet. Att kontrollera rösterna skulle införa flera komplexa moment och i sig självt införa



Figur 9: Beskrivning utav asymmetrisk kryptering.

extra säkerhetsrisker [28]. Hela systemet skulle dessutom ytterligare kraftigt kompliceras för att ge en förhållandevis liten teoretisk extra säkerhet. Ett sådant system skulle också omöjliggöra någon form av verifiering för röstaren eller uppdatering av röster. Därför bör man inte utnyttja de homomorfiska egenskaperna som vissa av dessa kryptosystem besitter. Av dessa fem kryptosystem så är RSA OAEP den mest beprövade och mest formellt undersökta algoritmen samt en av dem som ej har någon formbarhets egenskap [29] och därför bör man använda den.

Ska man välja RSA OAEP så bör nyckeln vara tillräckligt lång (längre betyder svårare att gissa) för att motverka försök att genom gissningar hitta den, men kort nog för att kunna dekryptera alla röster inom rimlig tid under röstberäkningsfasen. Denna nyckellängd kommer p.g.a. den snabba utvecklingen av datorprocesskraften att behöva ökas med tiden. Idag skulle det ta en dator med en Intel Core 2 1.83 GHz processor ca 12 timmar (6.08ms/dekryptering [30]) att dekryptera de ca 7 miljoner potentiella (antalet röstberättigade människor i Sverige [31]) valrösterna om de är krypterade med en nyckel på 2048-bitar.

4.1.4 Analys av identifierings- och autentiseringsmetoder

Då en väljare endast får ha en valröst som räknas måste man kunna skilja en väljare från alla de andra väljarna, d.v.s. identifiera väljarna. Eftersom detta är ett ganska vanligt problem finns det redan vedertagna metoder för identifiering av människor. I Sverige har vi dessutom ett väldigt gediget system, nämligen personnummersystemet, för detta ändamål. Eftersom användandet av personnummer dessutom är en väldigt beprövad och allmänt betrodd metod i Sverige så finns det liten vinning i att konstruera ett helt nytt system.

För autentisering kan i huvudsak tre olika metoder användas, eller en kombination utav dessa. Nämligen autentisering baserad på:

- Inneboende egenskaper (något man är)
- Kunskap (något man vet)

- Ägandeskap (något man har) [32]

Med Inneboende egenskaper menas t.ex. regnbågshinnan, näthinnan, fingeravtryck, ansiktet eller rösten. För att undersöka dessa egenskaper används t.ex. en speciell kamera för att fotografera egenskapen och sedan jämför den tagna bilden med en tidigare tagen bild. Dessa kan därför förhållandevis lätt manipuleras genom att helt enkelt ta, eller konstruera, en egen bild av t.ex. en regnbågshinna och sedan presentera den för autentiseringsmetoden istället för ett riktigt öga [33].

För att minska detta problem har man blivit tvungen att ta så högupplösta bilder att de blir svåra att manipulera, vilket i sin tur leder till att systemet blir dyrare då varje väljare måste ha en autentiseringsdosa med en sådan kamera. Detta blir ett ännu större problem när åtanke tas till att man endast kan samla in autentiseringsdata (det man jämför med vid autentisering) var femte eller tionde år (eftersom detta måste göras i en säker miljö och inte för ofta). Autentiseringsutrustning måste då vara tillräckligt kraftig för att inte kunna manipuleras av annan utrustning tio eller fem år senare. Då fototekniken, och i viss mån ljudtekniken, är tekniker som idag utvecklas med väldigt snabbt så blir autentisering med hjälp av teknisk analys utav inneboende egenskaper mer eller mindre praktiskt omöjligt (antingen blir det för osäkert eller för dyrt). Utöver kostnaden har även flera av dessa tekniker alldeles för hög chans att både inte känna igen korrekta egenskaper samt att känna igen inkorrekta egenskaper.

Som kunskap använder man någon form av information, såsom ett lösenord/passkod/lösenfras/etc., som sedan hålls hemligt av systemet och väljaren. Detta är en förhållandevis billig samt bekväm metod men också den som generellt ger minst säkerhet. För att maximera säkerheten kan man överväga att använda sig utav systemgenererade passkoder (de är svårare att gissa för en dator) men om väljaren då väljer att skriva ner koden eftersom den är svår att komma ihåg så minskar säkerheten istället.

Med ägandeskap menas ofta någon form av fysiskt ting, ofta en typ av kort. Det finns i huvudsak fyra olika sorters korttekniker som kan kombineras:

- RFID kort [34]
- Magnetremsekort [35]
- Dumt smart-card [35]
- Smart-card [35]

RFID (Radio Frequency Identification) kort är ett kort som går att läsa av på avstånd. Det gör att användandet av kortet blir betydligt lättare eftersom kortet inte behöver sättas in i någon läsare utan endast måste hållas i närheten utav läsaren. Detta gör i sin tur dock att säkerheten blir betydligt mindre eftersom det går att läsa av kortet av andra läsare utan att väljaren skulle märka det. Det gör dessutom både läsaren och kortet dyrare [34]. Eftersom de marginella vinsterna i användarvänlighet inte uppväger kostnads och säkerhetsrisk ökningarna bör man inte använda tekniken för detta ändamål.

Ett magnetremsekort är ett kort med en remsa som har magnetisk information. Denna remsa är väldigt lätt att skapa samt att läsa och detta gör läsaren och korten billiga. Detta ökar däremot också möjligheten för andra att läsa och återskapa en väljares kort [35].

Ett dumt smart-card har ett litet minne på kortet med elektronisk information som är svårare att skapa och att läsa än ett magnetremsekort. Det är också svårare att bygga ett eget minne och konfigurera den för att imitera ett annat dumt smart-card [35].

Ett smart-card är ett kort med minne samt en processor. Det gör att kortet kan använda sig av ett challenge-response protokoll, d.v.s. ett protokoll där man kan autentisera sig utan att den information som behövs för att kopiera kortet någonsin lämnar kortet. Detta gör att smart-card:et är betydligt säkrare än de andra korten. De är dessutom inte så dyra och de kan även användas vid kryptering och digital signering [35].

4.1.5 Analys av säkerhetskopieringsmetoder

Efter allvarliga systemhaveri, katastrofer eller attentat vill man kunna återuppta valprocessen. För att det ska vara möjligt måste man se till att systemets data är intakt trots denna typ av händelse. Detta görs ofta genom att skapa säkerhetskopior på den nödvändiga datan i systemet som man sedan lagrar på en annan plats. Problemet med säkerhetskopior är att man ökar mängden känslig information genom att duplicera den samt gör det svårare att skydda den genom att lagra informationen på olika platser.

4.1.6 Analys av verifieringsmetoder

Det finns flera möjliga metoder för att verifiera framförallt att insamlingen samt räkningen utav röster har gått rätt till. En möjlighet är att registrera egenskaper hos data som bör stämma överens både innan och efter att delar av systemet har processat datan, som t.ex. att antalet inkomna valröster bör stämma överens med antalet beräknade valröster i resultatet.

Systemet kan även själv generera unik kontrolldata från och för viktig information. Därefter kan systemet återigen generera kontrolldata och jämföra den nya kontrolldatan med den gamla och stämmer de överens har informationen inte modifierats. Detta bör göras vid alla transporter av data mellan enheter för att kontrollera att data ej modifierats på vägen.

Man kan även generera loggar där man lagrar alla förändringar utav data för att säkerställa att processeringen av datan gått korrekt till. Detta bör göras i lagringsenheten för att uppdateringen av röster ska gå rätt till. Även information om ogiltig data som upptäckts vid processen bör lagras för att lättare undersöka fel.

En konfirmation/notifiering bör skickas till väljaren när denne har röstat som upplyser väljaren om att valrösten tagits emot korrekt/inkorrekt om så skett.

4.1.7 Analys av granskningsmetoder

Samtlig utrustning bör kontrolleras både före och efter användandet. Kontroller bör ske utav en tredje part, eller flera oberoende parter som alla måste korrumperas för att förvanska kontrollen. Valmyndigheten bör utse dessa parter och väljarna måste lita på att valmyndigheten gör detta på ett korrekt sätt.

Varje ändring i systemet bör lagras med information om vad som gjordes, när och av vem. Vid processering av data bör ej felaktig data förekomma men om det sker så bör dessa data lagras i loggar där själva datan, information om var datan kom ifrån samt information om när datan upptäcktes lagras.

I-röstningssystemet och framförallt valprocessens olika delresultat bör granskas under hela valprocessen.

4.1.8 Analys av metoder för att öka tillgängligheten

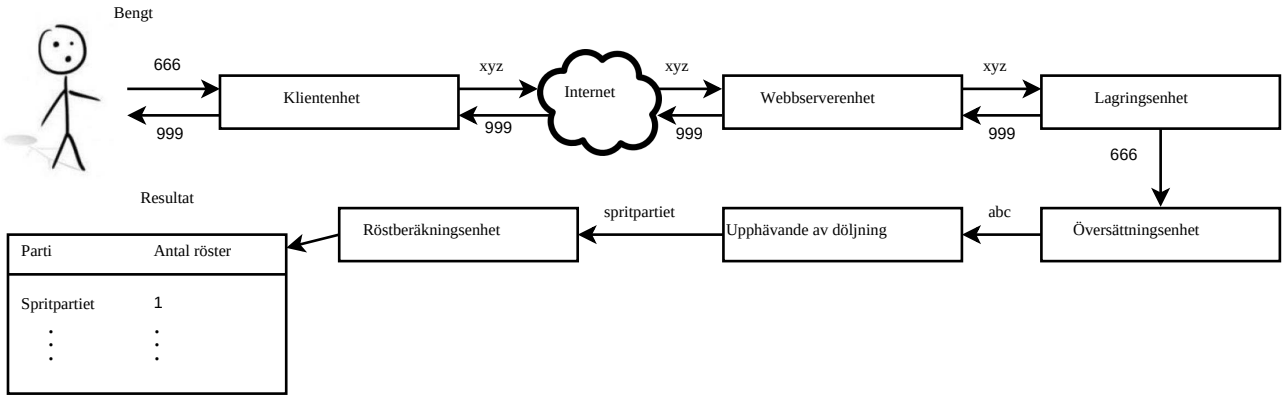
Genom att tillhandahålla ett röstningssystem som väljaren bekvämt kan använda hemifrån över Internet kommer förmodligen valdeltagandet att öka. Valdeltagandet kommer dessutom förmodligen att öka allra mest i den yngre målgruppen (18 till 29 år) som idag är den målgrupp med lägst valdeltagandet med hänsyn till ålder [36].

Men eftersom många människor fortfarande inte har Internet hemma så måste man erbjuda alternativa metoder för att rösta i systemet. Då systemet kräver en dator, en Internetuppkoppling, en klientenhet och möjligtvis en smart-card-läsare utöver det som är personligt (eventuellt smart-card:et, PIN-koden samt koderna för valrösterna) vore det bäst att under röstningsfasen upprätta valstationer där dessa

opersonliga saker tillhandahålls i en miljö säker från påverkan. Dessa valstationer kan även användas av väljare som utsätts för attacker mot klientenheten som förhindrar röstning eller helt enkelt väljare som inte litar på sin egen dator, Internetuppkoppling, klientenhet eller smart-card-läsare. Viss användarvänlighet går förlorad om man använder valstationer men alternativet är att man inte kan delta överhuvudtaget. De allra flesta kommer förmodligen inte att utnyttja dessa valstationer. I Estland har andelen väljare som röstar över Internet ökad exponentiellt fastän traditionella vallokaler erbjudits och redan idag röstar som sagt 24,3 % av alla röstande väljare i Estland över Internet [18].

5 Design

Systemet består av en sändande klientenhet (en mjukvara), en mottagande webbserverenhet (en server med tillhörande mjukvara), en lagringsenhet (en dator med tillhörande mjukvara), en översättningsenhet (en dator), en dekrypteringsenhet (ett minne tillsammans med hårdvara konstruerad för dekryptering) och en röstberäkningsenhet (en dator med tillhörande mjukvara). Se figur 10 på sidan 16 för en beskrivning av systemprocessen. För att använda systemet behöver man också kunna identifiera samt autentisera sig (se 5.2 Identifiering och Autentisering).



Figur 10: En beskrivning av systemprocessen.

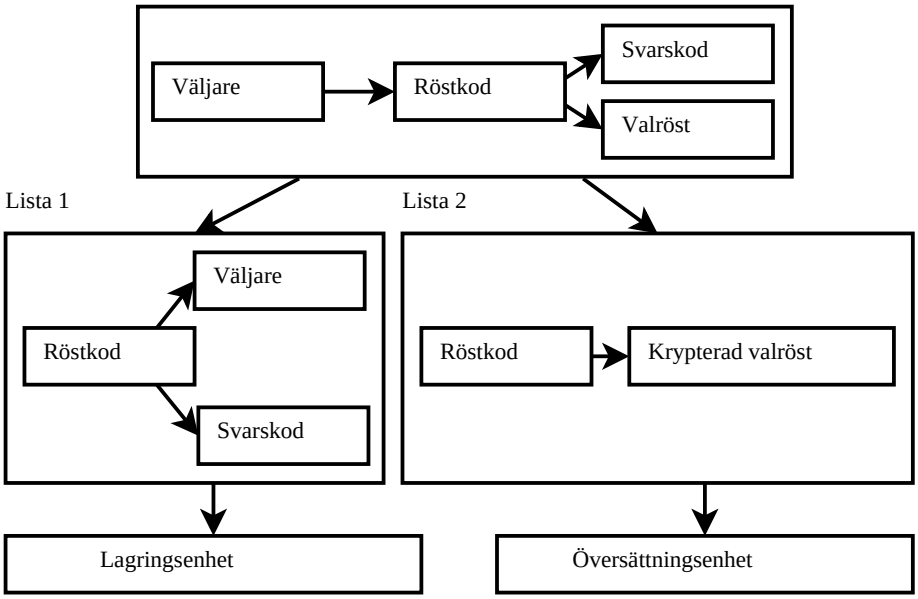
5.1 Valprocessen

5.1.1 Förberedelsefas

Inför varje val skapas två RSA OAEP nyckelpar med längd 2048 bitar, ett internt nyckelpar som bara kommer att användas inom systemet och ett externt som kommer att användas över Internet. Den externa publika nyckeln kan göras offentlig med ett passande certifikat (någons försäkran av att nyckeln är giltig) från systemet och läggs in i klientenheten. Den externa privata nyckeln läggs in i lagringsenheten och den interna privata nyckeln förvaras på en säker plats. De vanligaste valrösterna (t.ex. en valröst för socialdemokraterna med Bengt Eriksson personkryssad) skapas för varje väljare och för varje väljare och valröst skapas två koder, en röstkod och en svarskod. Vill väljaren använda en sällsynt valröst kan denne anmäla detta i förväg och denna valröst kommer då genereras för denna väljare. Varje valröst har alltså en väljare den tillhör samt en unik röstkod och en unik svarskod (se vallista i figur 3 på sidan 9). Brev som innehåller en specifik väljares koder samt vad dessa koder betyder (vilken kod som är röst- samt svarskod och vilken valröst de hänvisar till) skapas och skickas till den specifika väljaren via det traditionella postsystemet.

Efter att breven har skapats så krypteras valrösterna med den interna publika nyckeln. Därefter delas informationen upp i två listor, en som innehåller alla röstkoder, deras motsvarande svarskod och deras motsvarande väljare samt en lista som innehåller alla röstkoder och deras motsvarande krypterade valröst. Listan med alla röstkoder, deras svarskod och deras väljare införs i lagringsenheten och listan

med röstkoder samt deras motsvarande krypterade valröst lagras i översättningsenheten (se figur 11 på sidan 17). All annan information om röstkoderna, svarskoderna och valrösterna förstörs tillsammans med alla kopplingar mellan denna information och identifieringen utav en väljare.

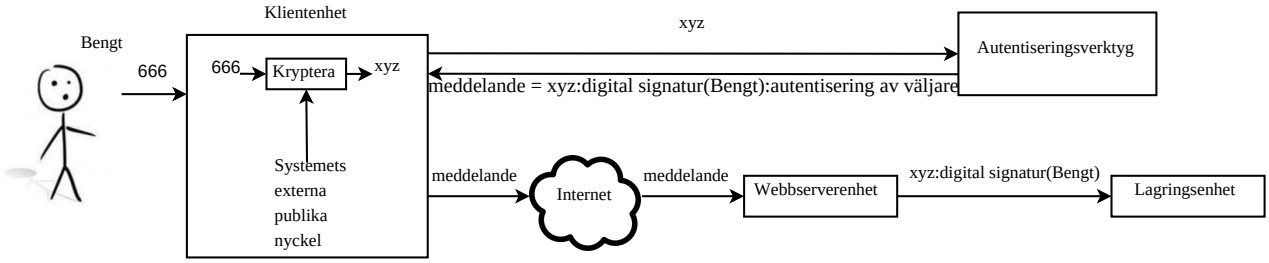


Figur 11: Modell utav uppdelandet av ursprungs-informationen och införandet av dessa in i passande enhet.

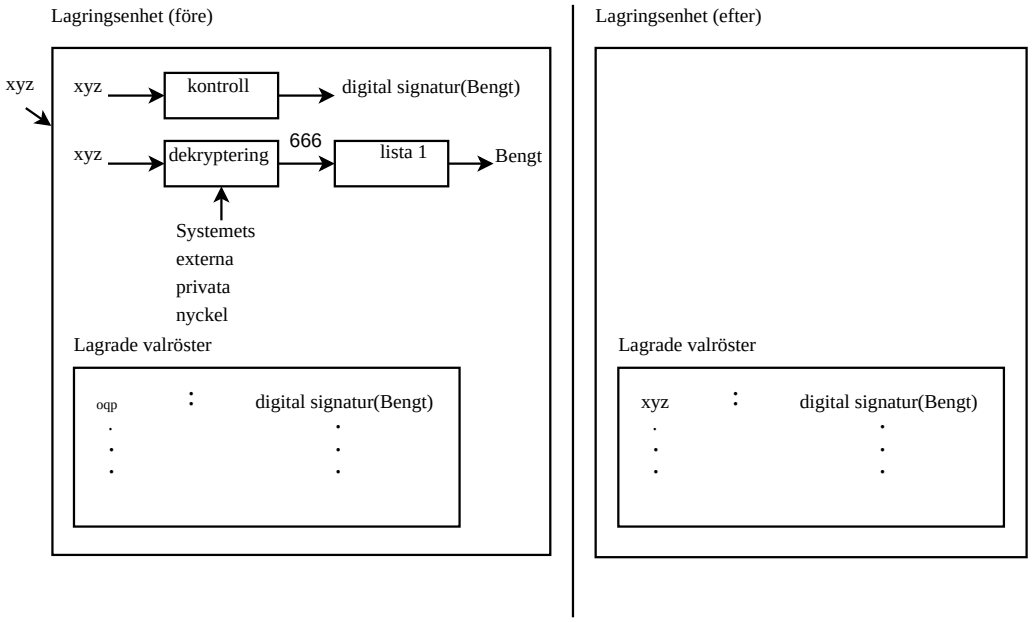
En hemsida som använder SSL (ett vedertaget protokoll för kryptering över Internet mellan två enheter) konstrueras också som användarna kan ladda ner klientenheten ifrån. Väljaren behöver även införskaffa nödvändiga verktygen för autentisering (se 5.2 Identifiering och Autentisering). Lagringsenheten måste få tillgång till en lista med personnummer för väljare samt deras publika nyckel för att verifiera deras digitala signatur (se 5.2 Identifiering och Autentisering).

5.1.2 Röstningsfas

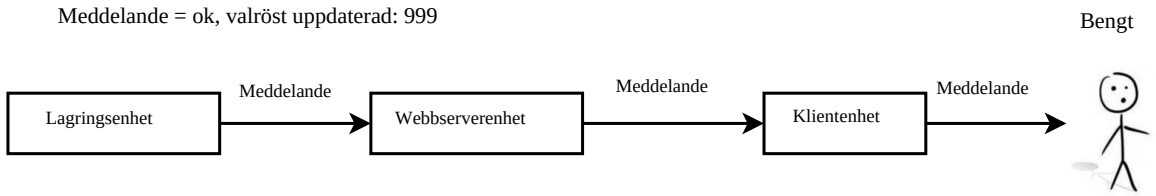
När en väljare ska rösta använder denne klientenheten för att etablera en SSL-uppkoppling till webbserverenheten. All kommunikation mellan klientenheten och webbserverenheten kommer gå via denna uppkoppling. Därefter skriver väljaren in röstkoden i klientenheten. Klientenheten i sin tur krypterar röstkoden med systemets externa publika nyckel samt använder autentiseringsverktygen för att autentisera väljaren och digitalt signera meddelandet (se 5.2 Identifiering och Autentisering) innan den skickar detta till webbserverenheten. Webbserverenheten autentiserar väljaren och skickar sedan den digitala signaturen och den krypterade röstkoden till lagringsenheten. För ett illustrativt exempel se figur 12 på sidan 18. Lagringsenheten kontrollerar att signaturen stämmer, d.v.s. att det är det givna meddelandet som signerats. Därefter dekrypteras röstkoden med systemet externa privata nyckel och sedan verifierar lagringsenheten att röstkoden tillhör den väljare valrösten kommer ifrån (med Lista 1, se figur 11 på sidan 17). Lagringsenheten undersöker sedan om väljaren har röstat tidigare genom att titta på de krypterade röstkoder och signaturer som redan är lagrade. Existerar en krypterad röstkod för den aktuella väljaren tas den bort. Därefter lagras den nyligen inkomna röstkoden i krypterad form tillsammans med sin signatur på en slumpmässig plats i lagringsenheten. För ett mer belysande exempel se figur 13 på sidan 18. Slutligen skickar lagringsenheten ett svarsmeddelande tillbaka till webbserverenheten som innehåller information om hur det har gått, om en valröst ersatts eller ej samt eventuellt svarskoden. Webbserverenheten skickar i sin tur det meddelandet vidare till klientenheten och väljaren via SSL uppkopplingen. För ett mer åskådliggörande exempel se figur 14 på sidan 18.



Figur 12: Exempel på en valröst processering från väljare till lagringsenhet under röstningsfasen.



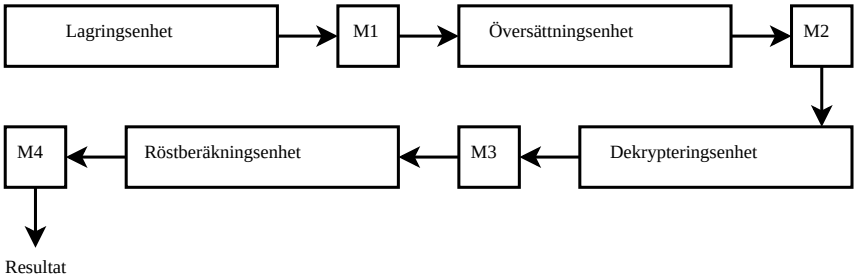
Figur 13: Exempel på valröst processering i lagringsenheten under röstningsfasen.



Figur 14: Exempel på transport utav verifierings meddelanden i systemet.

5.1.3 Röstberäkningsfas

När väl röstningsfasen är avklarad kontrolleras alla signaturer än en gång mot de krypterade röstkoderna samt listan med legitima väljare. Därefter dekrypteras röstkoderna i lagringsenheten och exporteras till ett externt lagringsmedium (M1). M1 läggs därefter in i översättningsenheten som i sin tur översätter röstkoderna till krypterade valröster och exporterar de krypterade valrösterna till ett annat externt lagringsmedium (M2). M2 läggs i sin tur in i dekrypteringsenheten tillsammans med systemets privata interna nyckel. Dekrypteringsenheten börjar därefter dekryptera valrösterna och exporterar de slutgiltiga rösterna till röstberäkningsenheten via ytterligare ett externt lagringsmedium (M3). Röstberäkningsenheten utvinner slutligen resultatet från rösterna och exporterar det till ett sista externt lagringsmedium (M4). För en övergripande modell utav datatransport i röstberäkningsfasen se figur 15 på sidan 19. Informationen som finns i de externa lagringsmedierna (M3 & M4) som förs in och ut ur röstberäkningsenheten offentliggörs även på hemsidan för valet.



Figur 15: Modell utav transport av data mellan enheter i systemet under röstberäkningsfasen.

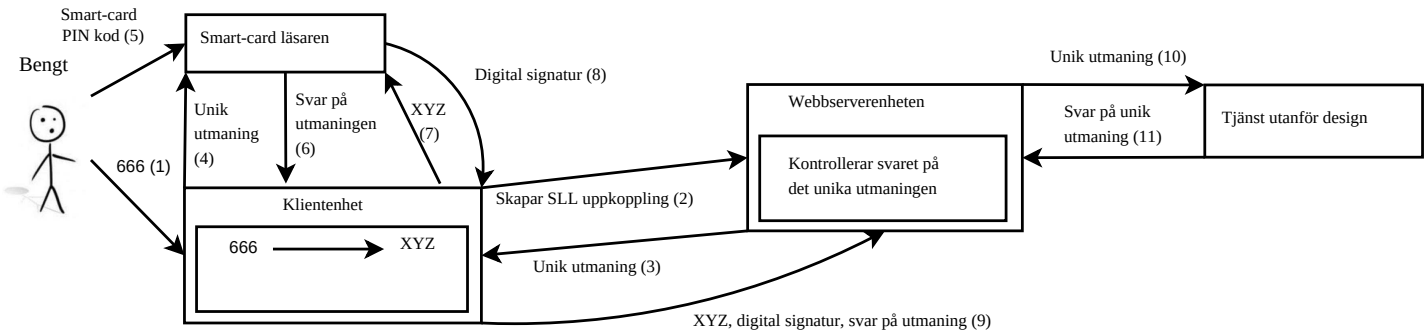
5.1.4 Avslutningsfas

De ej krypterade rösterna lagras i valmyndighetens databas under mandatperioden. Därefter påbörjas den granskning som sker efter själva valprocessen (se 5.5 Granskning). Slutligen förstörs systemets nycklar genom att alla minnen där den finns rensas och alla dataminnen i själva systemet (webbserverenheten, lagringsenheten, dekrypteringsenheten och loggar) rensas. Alla externa lagringsmedium förstörs helt och hållet.

5.2 Identifiering och Autentisering

För identifiering ska väljarnas personnummer användas och för autentisering ska en personlig systemgenererad PIN-kod, ett smart-card samt en smart-card-läsare användas. PIN-koden, kortet och läsaren ska skickas till den röstberättigade personen som tre stycken skilda rekommenderade försändelser (man måste gå ner till posten/banken och identifiera sig för att få hämta ut det).

När det väl är dags att rösta kopplar man upp klientenheten mot webbserverenheten och sätter in smart-card:et i smart-card-läsaren. Webbserverenheten kommer därefter skicka en för tillfället unik och slumpmässigt vald utmaning till smart-card:et via klientenheten och smart-card-läsaren. Därefter krypterar klientenheten röstkoden med systemets externa publika nyckel. Efter detta tar smart-card:et emot PIN-koden från väljaren via smart-card-läsaren samt den krypterade röstkoden från väljaren via klientenheten. Med hjälp av dessa processar smart-card:et PIN-koden samt utmaningen till ett svar på utmaningen samt PIN-koden och den krypterade röstkoden till en digital signatur utav den krypterade röstkoden. En digital signatur skapas genom att först hasha ett meddelande (en hash är en kontrollsumma som är unik för i detta fall meddelandet som den genererades utav och det är dessutom omöjligt att från denna kontrollsumma återskapa meddelandet) och sedan kryptera hashen med ens privata nyckel. Gör man en ny hash av meddelandet samt dekrypterar den digitala signaturen och dessa är identiska så vet man att meddelandet kommer från ägaren av nyckeln samt att meddelandet ej har ändrats. Klientenheten lägger sedan ihop den krypterade röstkoden, dess digitala signatur och svaret på utmaningen från webbserverenheten till ett meddelande och skickar det till webbserverenheten. Svaret på utmaningen jämförs sedan i webbserverenheten med ett korrekt svar som tillhandahålls utav en tjänst utanför systemet. Om de båda svaren överensstämmer är väljaren autentiserad. För ett mer förklarande exempel se figur 16 på sidan 20.



Figur 16: Exempel på identifierings- och autentiserings process i systemet.
1. Väljaren skriver in röstkoden i klientenheten.
2. Klientenheten skapar en SSL uppkoppling till Webbserverenheten.
3. Webbserverenheten skickar den unika utmaningen till Klientenheten.
4. Klientenheten skickar den unika utmaningen till smart-card-läsaren.
5. Väljaren skriver in PIN-kod i smart-card-läsaren.
6. Smart-card-läsaren skickar tillbaka svaret på utmaningen till Klientenheten.
7. Klientenheten skickar den krypterade röstkoden till smart-card-läsaren.
8. Smart-card-läsaren skickar en digital signatur till Klientenheten.
9. Klientenheten skickar valrösten till webbserverenheten.
10. Webbserverenheten skickar en unik utmaning till en tjänst utanför designen.
11. Webbserverenheten hämtar svaret på den unika utmaningen.

5.3 Säkerhetskopiering

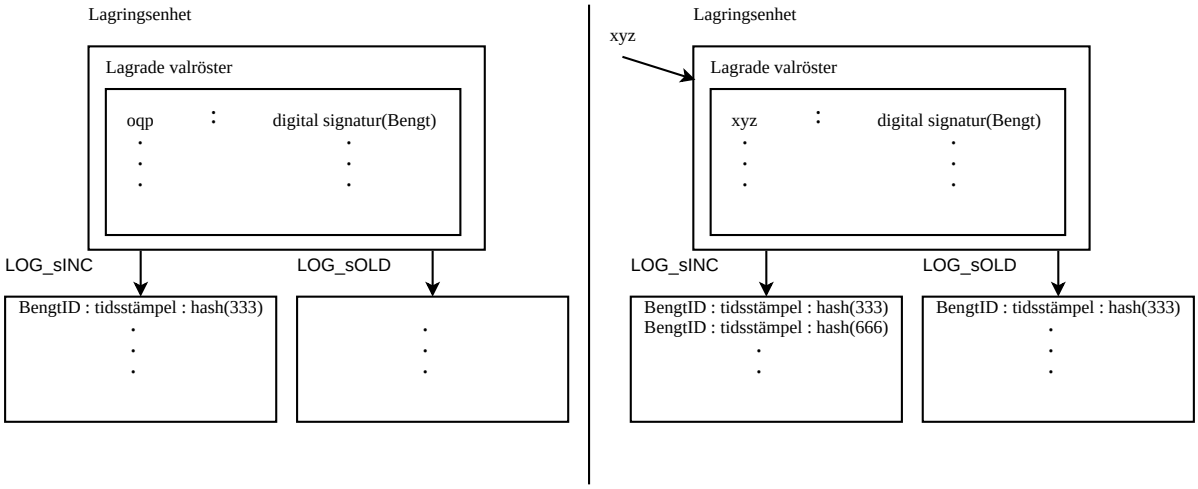
Det existerar även en databas på en säker avsides plats som innehåller följande data:

- De krypterade röstkoderna och deras digitala signaturer i lagringsenheten
- Listan med kopplingen mellan röstkod, väljare samt svarskod i lagringsenheten
- Listan med kopplingen mellan röstkod samt krypterad valröst i översättningsenheten
- Systemets externa publika och privata nyckel
- Systemets interna publika och privata nyckel

All data utöver de krypterade röstkoderna och deras digitala signaturer transporteras till databasen fysiskt i förberedelsefasen. De krypterade röstkoderna och deras digitala signaturer måste däremot skickas till databasen löpande under röstningsfasen, men denna information skickas redan över Internet så vanlig SSL kryptering kan användas.

5.4 Verifiering

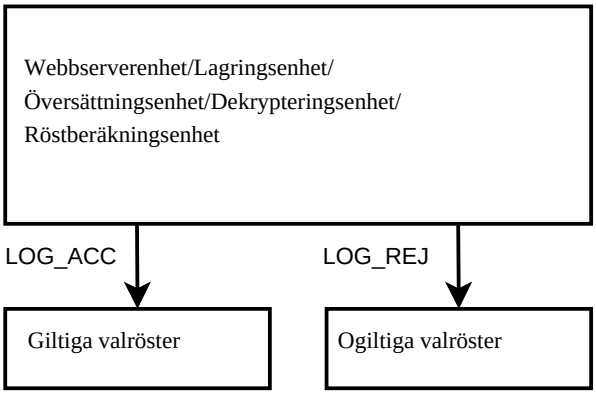
I lagringsenheten skapas en logg (LOG_sINC) som lagrar varje röst som kommer in i lagringsenhetens grundformat, nämligen väljarens ID-nummer, en tidstämpel för när den mottogs samt en hash utav röstkoden. Dessutom skapas även en logg (LOG_sOLD) för varje valröst som tas bort när väljaren uppdaterar sin valröst, alla dessa valröster lagras i samma format. För ett mer upplysande exempel se figur 17 på sidan 21. När röstningsfasen väl är avslutad summeras antalet valröster i lagringsenheten och kontrolleras med summan av valröster i den första loggen subtraherat med summan av valröster i den andra loggen. Man kontrollerar även att alla valröster i LOG_sOLD återfinns i LOG_sINC samt att alla valröster i LOG_sOLD uppdaterats med en annan, senare, valröst i LOG_sINC.



Figur 17: Modell utav förfarande i LOG_sINC och LOG_sOLD vid uppdatering av röst.

I lagringsenheten, översättningsenheten, dekrypteringsenheten och röstberäkningsenheten beräknar man antalet valröster som ankommer till enheten samt antalet valröster som exporteras när man är klar. Dessa summor kontrolleras mot varandra efter att enheten är klar.

I webbserverenheten, lagringsenheten, översättningsenheten, dekrypteringsenheten och röstberäkningsenheten skapas även varsitt logg-par där den ena loggen (LOG_ACC) innehåller valröster som klassificerats som giltiga av enheten och den andra (LOG_REJ) innehåller valröster som klassificerats som ogiltiga av enheten. En valröst läggs in i endera loggen när valrösten processas. När varje enhet är klar med sitt processande kontrolleras antalet valröster i de båda loggarna med det totala antalet inkomna och exporterade röster i varje enhet. För en mer övergripande modell se figur 18 på sidan 21.



Figur 18: Modell utav loggar för giltiga och ogiltiga valröster i relevanta enheter.

Samtliga loggar har en tidstämpel i varje post för när den specifika valrösten processades utav enheten. I webbserverenheten lagras dessutom väljarens ID-nummer, utmaningen som skickades till väljaren samt hela meddelandet som kom in, d.v.s. den krypterade röstkoden, den digitala signaturen samt svaret på utmaningen. I lagringsenheten lagras varje post i dess loggar i lagringsenhetens grundformat. I översättningsenheten lagras utöver tidstämpeln även röstkoden i varje post. I dekrypteringsenheten lagras utöver tidstämpeln även den krypterade valrösten i varje post. I röstberäkningsenheten lagras utöver tidstämpeln även den dekrypterade valrösten i varje post.

Varje gång data exporteras från lagringsenheten, översättningsenheten, dekrypteringsenheten eller röstberäkningsenheten genereras kontrolldata för all data som sedan följer med i exporten. Varje gång data importeras från tidigare nämnda enheter genereras återigen kontrolldata för all data och jämförs med den kontrolldatan som åtföljde datan.

5.5 Granskning

Innan varje val ska I-röstningssystemet kontrolleras och verifieras. Valmyndigheten bestämmer sedan om väljaren själv ska kunna granska I-röstningssystemet, endast specifika delar av systemet eller om granskningen sker via ombud. Det viktiga är att hela systemet kontrolleras regelbundet, även då det inte är något valår. Om det skulle ske någon ändring i systemet, t.ex. att man skulle lägga till en ny komponent i systemet, ska systemet granskas igen.

Varje ändring i systemet eller dess konfigurationer kräver identifiering, autentisering och loggning. Alla röster som klassificeras av systemet som ogiltiga, eller händelser då rösternas integritet inte kan verifieras, räknas som systemfel och ska utredas. Alla utredningar ska utföras av oberoende parter utsedda av valmyndigheten. Systemet bör regelbundet utsättas för granskning utav parter utsedda utav valmyndigheten som undersöker alla komponenter i systemet. Vid systemhaveri ska nödvändig information om händelsen för granskning lagras, såsom tidpunkt, händelseförlopp, systemtillstånd etc.

Kritisk tekniska åtgärder eller undersökningar ska utföras av lag om minst tre personer och att sammansättningen av dessa tre personer ska ändras regelbundet. All granskande verksamhet kräver fysiskt närvaro vid systemet.

Under valprocessen ska det ske konstant granskning för verifiering av att systemet fungerar korrekt. I-röstningssystemet ska ha funktionalitet att spela in, övervaka och kontrollera granskningsdata och även kunna skydda integriteten och autenticiteten hos granskningsregistret som skapas. Det är viktigt att I-röstningssystemet ska få tillgång till en tillförlitligt tidskälla som ger en exakt tidsstämpel åt alla aktiviteter som sker i systemet och alla valröster som kommer in i systemet.

5.6 Alternativa röstningsmetoder

Valstationer där en säker miljö med säkra datorer, Internetuppkopplingar, klientenheter samt smartcard-läsare ska finnas utspridda över Sverige.

6 Diskussion

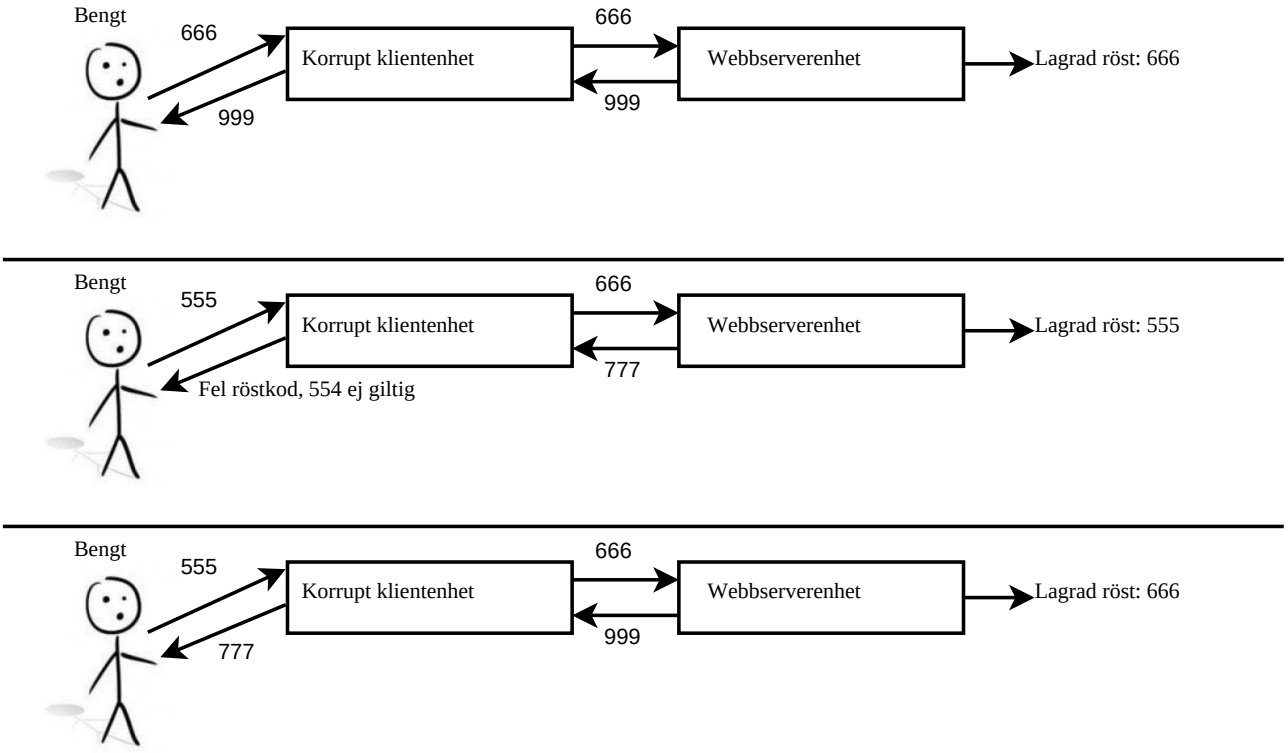
Valet av övergripande design leder till att systemet blir mer komplext vilket i sin tur ökar risken för misstag samt att systemet blir svårförstått och därmed minskar även förtroendet för systemet. Mycket känslig data genereras i systemet fastän det är något man vill undvika då det är svårt att helt förstöra data. Bland annat skapas en koppling mellan potentiella valröster och väljare i början av processen vilken kan användas varhelst i processen för att knyta en väljare till en valröst. Misslyckas förstörandet av dessa data skapas därför ett allvarligt hot mot valhemligheten.

Ett mer subtilt problem med designen är att den även leder till att man måste förgenerera alla möjliga röstalternativ innan röstningsfasen påbörjas. Detta faktum tillsammans med möjligheten att framförallt skriva in ett helt eget parti och/eller namn att personrösta på, resulterar i ett ganska stort problem. Att förgenerera koder och valröster för varenda möjlig bokstavskombination utifall någon skulle vilja rösta på det vore omöjligt. I praktiken lindras problemet utav att man inte får personrösta fritt i partier som skickar ut egna kandidatlistor (man får bara kryssa, inte skriva egna namn, på en valröst om det finns fördefinierade alternativ). En kandidatlista är en lista från ett visst parti med namn på personer, från just det partiet, som man kan personkryssa på. För partier som inte har skickat ut egna kandidatlistor blir det problem. För att lösa detta kan man tvinga de som vill använda ett mer sällsynt röstalternativ att anmäla detta tillsammans med kanske två till sex andra alternativ som denne sedan får koder till i sitt brev när det väl är dags att rösta. Implementationen av detta system får valmyndigheten stå för.

Kravet på att man måste förgenerera alla röstalternativ medför dock även en fördel. Nämligen att de tvetydigheter som uppstår när man får skriva vad som helst och detta sedan måste klassificeras elimi-

neras. Om det finns ett parti som heter “sportpartiet” och ett som heter “spritpartiet” och någon skickar in “sprtpartiet ” vad ska man då göra? Förgenererade valröster leder till att man kan vara säker på att ens röst inte förklarats ogiltig för att man t.ex. inte kunnat tyda handstilen eller stavningen.

Ett annat subtilt problem är som sagt att röst- och svarskoden inte ändras och att dessa kan läsas utav klientenheten vilket leder till att klientenheten kan lura användaren. Väljaren kan dock vara säker på att svarskoden är korrekt första gången du använder dess röstkod då enda sättet för klientenheten att veta svarskoden är genom att skicka valrösten (givet att resten av systemet är säkert). Vill väljaren uppdatera rösten tillbaka till något väljaren tidigare röstat på (och du ska skicka en röstkod du tidigare skickat) kan väljaren aldrig lita på svarskoden. Notera att väljaren inte behöver se svarskoden för att klientenheten ska kunna lura väljaren. En klientenhet skulle t.ex. kunna spara den första valrösten du skickar, när väljaren sedan försöker uppdatera sin valröst skickar klientenheten valrösten, registrerar svarskoden men säger till väljaren att denne matat in fel röstkod (och visar en felaktig röstkod med någon liten ändring från den korrekta). Väljaren försöker då skicka samma röstkod igen men klientenheten skickar istället den allra första röstkoden väljaren skickade och visar väljaren svarskoden för den andra röstkoden. Väljaren tror då att valrösten ändrats utan att den har ändrats (se figur 19 på sidan 23). I händelsen att klientenheten agerar underligt (t.ex. säger att väljaren skickat en röstkod denne inte skickat eller att fel svarskod erhållits) så bör alltså väljaren behandla klientenheten som en skadlig programvara och gå och rösta i en valstation.



Figur 19: Beskrivning av ytterligare en attack på systemet genom klientenheten.

Den stora fördelen med designen är däremot att varje väljare själv kan verifiera att korrekt valröst lagrats samt att man inte behöver lita på klientenheten för att göra detta. Då klientenheten med största sannolikhet är den mest utsatta enheten i hela systemet är det en väldigt stor vinst att inte behöva lita på den för systemets säkerhet. Genom att öka säkerheten, och därmed korrektheten, ökas även förtroendet till en grad som överstiger den förlust man får i förtroendet utav komplexiteten. För de allra flesta kommer även användarvänligheten att endast marginellt försämras jämfört med andra I-röstningssystem. Detta eftersom väldigt få, per definition, röstar på obskyra partier eller personer och därmed är tvungna att anmäla valröster i förväg.

I designen tillades även en extra nivå av kryptering i systemet (kryptering av valrösterna) då krypteringen av det data som transporteras över Internet måste dekrypteras när den väl kommer fram till

lagringsenheten. Eftersom den nyckeln därmed används hela tiden och finns i en redan känslig enhet är det nödvändigt att lägga till ytterligare en kryptering. Kostnadsökning i främst komplexitet men också tid vid röstberäkningsfasen (vid dekrypteringen) är värt priset. Därmed räcker det inte att t.ex. bryta krypteringen för transporten över Internet och utvinna röstkoden samt att få tillgång till datan i översättningsenheten för att avslöja valhemligheten.

I rapportens design används RSA OAEP kryptering framförallt då det är den mest beprövade asymmetriska krypteringsalgoritmen samt att den ej har någon "formbarhets " egenskap. RSA OAEP används med 2048 bitars nycklar då det är en bra kompromiss mellan tiden det tar att dekryptera vid främst räkning samt tiden det tar att bryta krypteringen.

I designen använder man två olika metoder för autentisering i kombination för att autentisera en väljare, ett smart-card och en systemgenererad PIN-kod. Att använda en kombination utav metoder för autentisering leder till ett säkrare system då deras svagheter ofta kompletterar varandra. Teknikerna för att använda inneboende egenskaper är däremot alldeles för dyr samt osäker för att användas.

Faktumet att PIN-koden är systemgenererade kan som sagt leda till att säkerheten minskas om väljaren väljer att skriva ner den då den kan vara svår att lägga på minnet. Men i praktiken leder detta till att avvägningen mellan säkerhet och användarvänlighet förflyttas till väljaren. Vill väljaren ha hög säkerhet i systemet kan denne memorera passkoden och förstöra alla fysiska spår utav den. Vill väljaren å andra sidan ha det mer användarvänligt kan denne sätta upp en post-it lapp på dataskärmen.

Smart-card:et möjliggör framförallt att kritiska operationer vid ett challenge-response protokoll sker utanför klientenheten (i smart-card:et istället), vilket gör att man inte behöver lita på klientenheten för detta. Dessutom är kostnadsskillnaden mellan smart-card:et och de billigare alternativen marginell och skillnaden för hur väljaren använder korten i det närmaste obefintlig. RFID tekniken anses även alltför osäker jämfört med den lilla ökning utav användarvänligheten den ger.

I designen beskrivs ej implementationen av PIN-koden och smart-card:et men man kan dock påpeka att användandet av BankID inte rekommenderas. BankID är det smart-card och PIN-kod system som används utav de flesta svenska banker vid autentisering över Internet. Skulle man använda BankID skulle bankerna, som ej drivs av allmänhetens intresse, få för stort inflytande över säkerheten i systemet. Att implementera ett enda ID-kort och PIN-kod system som sköts utav staten och som kan användas för statliga och privata tjänster över Internet, som t.ex. i Estland, vore att föredra.

7 Slutsats

Att skapa ett I-röstningssystem är en betydligt större utmaning än vad man kan tro och det kommer alltid att finnas inneboende problem hos ett I-röstningssystem. Trots att det har skrivits en ofantlig mängd rapporter samt artiklar om ämnet och flera länder har infört samt försökt införa I-röstningssystem så lyser den perfekta lösningen med sin frånvaro.

Det kanske största övergripande problemet med hela röstningssystemsfältet är hur viktigt människors beteenden och uppfattning av systemet är för röstningssystemet, såsom trakasserier, röstförsäljning, förtroende och användarvänlighet. Detta medför stora svårigheter med att använda empiriska studier för att ta designbeslut samt utvärdera designen.

Ett av de största problemen för I-röstningssystem är just förtroendet för systemet. I-röstningssystem är mer eller mindre per definition komplexa och svårförståeliga jämfört med traditionella röstningssystem och därmed svåra att lita på. Genom att tillhandahålla kontroll utav den lagda valrösten till väljaren samt en hel del interna kontroller så försöker designen förstärka förtroendet för systemet hos väljarna.

Ett annat stort problem som alltid förekommer med I-röstningssystem är kravet på att väljaren har tillgången till både dator och Internet. Detta leder till att de som inte har tillgång till dator eller Internet måste uppsöka någon form av valstation för att kunna lägga sin valröst. Många fördelar

med ett I-röstningssystem förloras om man använder valstationerna men även mycket bibehålls, som verifiering av ens lagda röst och gedigen kontrollerad röstberäkning.

Möjligheten att rösta hemifrån, som återfinns i nästan alla I-röstningssystem, medför stora problem med att säkra miljön vari väljaren röstar från påverkan (t.ex. familjeröstning) och avslöjande utav valhemligheten (t.ex. röstförsäljning). En funktion för uppdatering av röst lindrar problemet en hel del men löser det inte. Familjeröstning eller röstning i sista stunden är fortfarande möjliga vägar för att otillbörligt påverka en väljares valröst. Möjligheten att rösta hemifrån leder även till att väljaren får förlita sig till någon form av mjukvara som exekveras på deras dator. Detta är ett stort problem eftersom människors datorer, samt mjukvaran på dem, är lätta att manipulera och därmed lura väljaren.

Det sista stora problemet med I-röstningssystem är att röstinsamling och röstberäkning utförs väldigt centraliserat. Det medför att få komponenter behöver manipuleras för att åstadkomma väldigt stor påverkan utav resultatet. Eftersom resultatet av ett I-röstningssystem har en så hög betydelse kommer även viljan att påverka det otillbörligt vara väldigt hög. Centralisering leder även till att antalet systemkritiska komponenter minskar vilket i sin tur leder till att man kan fokusera ens säkerhetsåtgärder på dessa och därmed göra dessa säkerhetsåtgärder mer robusta.

Den största fördelen med I-röstningssystem är förmodligen användarvänligheten. Genom att sänka trösklarna för att rösta kommer valdeltagandet att öka vilket leder till mer korrekta resultat, d.v.s. att resultatet speglar folkets vilja bättre. I-röstningssystem kommer förmodligen även som sagt att öka valdeltagandet i målgruppen som idag har det lägsta valdeltagandet med hänsyn till ålder.

En annan stor fördel med I-röstningssystem är att korrektheten i röstberäkning är nästintill exakt. Dessutom kan I-röstningssystem med olika åtgärder nästan eliminera antalet felaktigt lagda eller hanterade röster, vilket idag är en väldigt stor orsak till att röster inte räknas och att resultat blir mindre korrekt.

Den kanske hitintills största drivkraften bakom införandet utav I-röstningssystem är förmodligen den monetära kostnaden. Det går att göra I-röstningssystem betydligt billigare än traditionella röstningssystem. De besparade pengarna kan sedan användas på andra ändamål. Historiskt har dock vissa länder (Tyskland, Nederländerna och Finland) valt att spara in även på säkerheten i nya röstningssystem till den grad att de blivit obrukbara och därefter har de blivit tvungna att avveckla dem efter ett par år. Att försöka spara in alltför mycket på I-röstningssystem kan därför bli väldigt kostsamt.

I-röstningssystem åtgärdar många av de största problemen med dagens röstningssystem. Däremot införs det problem som i väldigt liten skala återfinns i dagens system. Dessa problem har man därför inte sett effekterna av på dagens samhälle vilket gör det väldigt svårt att förutse konsekvenserna av dessa samt utvärdera dem. Skulle t.ex. en marginellt osäkrare röstningsmiljö få en röstförsäljningsbransch att explodera i, eller få ingen påverkan överhuvudtaget på, dagens samhälle?

Många funktioner som vore otänkbara i det traditionella systemet möjliggörs i I-röstningssystem, såsom verifiering utav väljarens egen valröst, röstning hemifrån för alla väljare, uppdateringar av valröst och även mer visionära saker som val initierade utav väljare själva. Trots problemen med I-röstningssystem tror vi därför att det finns stor potential för att de med tiden kan optimeras till dagens förhållanden, behov och möjligheter.

Givet allt detta så har denna rapports design fokuserat på att ge väljaren möjligheten att verifiera sin valröst, minska beroendet utav klientenheten, öka användarvänligheten och korrektheten samt bevara valhemligheten. Vi tror att dessa prioriteringar ger en passande I-röstningssystemsdesign för riksval i Sverige.

8 Referenser

[1] Coleman Kevin.
Internet Voting, CRS Report for Congress [hemsida på Internet].
c2003 [citerad 2012 Mars 16].
Tillgänglig på:
http://www.infousa.ru/information/rs20639.pdf

[2] Iannucci Lisa.
Holding Fair Elections [hemsida på Internet].
c2011 [citerad 2012 mar 13].
Tillgänglig på:
http://cooperator.com/articles/2329/1/Holding-Fair-Elections/Page1.html

[3] Valmyndigheten.
Vallagen (SFS 2005:837) [hemsida på Internet].
Inget datum [senast uppdaterad 2011 jun 30; citerad 2012 mar 26].
Tillgänglig på:
http://www.val.se/det_svenska_valsystemet/lagar/vallagen/

[4] Valmyndigheten.
Registrera partibeteckning [hemsida på Internet].
Inget datum [senast uppdaterad 2012 apr 02; citerad 2012 mar 28].
Tillgänglig på:
http://www.val.se/det_svenska_valsystemet/partier/registrera_partibeteckning/index.html

[5] Braun Nadja, Helena Maria, Lemon Alves, et.al. *Auditing of e-voting systems* [hemsida på Internet].
Inget datum [citerad 2012 mar 27].
Tillgänglig på:
http://aceproject.org/ace-en/focus/e-voting/e-voting-auditing

[6] Committee of Ministers of the Council of Europe.
LEGAL, OPERATIONAL ANDTECHNICAL STANDARDS FOR E-VOTING [hemsida på Internet].
2004 nov 30 [citerad 04 apr 2012].
Tillgänglig på:
http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/Key_Documents/Rec%282004%2911_Eng_Evoting_and_Expl_Memo_en.pdf

[7] Oikeusministeriö.
Counting of the Election Results [hemsida på Internet].
Inget datum [citerad 2012 mar 20].
Tillgänglig på:
http://www.vaalit.fi/21959.htm

[8] Valmyndigheten.
Allmänt om val [hemsida på Internet].
Inget datum [senast uppdaterad 2012 mar 26; citerad 2012 mar 28].
Tillgänglig på:
http://www.val.se/det_svenska_valsystemet/allmant_om_val/index.html

[9] Wildstrom Steve.
Internet Voting Is Years Away, And Maybe Always Will Be [hemsida på Internet].
2012 apr [citerad 2012 apr 10].
Tillgänglig på:
http://techpinions.com/internet-voting-is-years-away-and-maybe-always-will-be/6343

[10] Demont Paul.
Allotment and Democracy in Ancient Greece [hemsida på Internet].
2010 dec 13 [citerad 2012 apr 11].
Tillgänglig på:
http://www.booksandideas.net/IMG/pdf/20101213_demont_EN.pdf

[11] Wikipedia.
Athenian democracy [hemsida på Internet].
Inget datum [senast uppdaterad 2012 mar 24, citerad 2012 apr 11].
Tillgänglig på:
http://en.wikipedia.org/wiki/Athenian_democracy

[12] Volkamer Melanie.
Evaluation of Electronic, VotingRequirements and Evaluation Procedures to Support Responsible Election Authorities: Chapter 6 Requirements for Remote Electronic Voting [hemsida på Internet].
c2009 [citerad 2012 mar 28].
Tillgänglig på:
http://www.springerlink.com/content/978-3-642-01661-5/contents/

[13] Wikipedia.
Protest vote [hemsida på Internet].
Inget datum [senast uppdaterad 2012 mar 20; citerad 2012 mar 24].
Tillgänglig på:
http://en.wikipedia.org/wiki/Protest_vote

[14] Dundas Carl, Sen Debashis, Spinelli Antonia, et al.
Family and proxy voting in Macedonia [hemsida på Internet].
c2007 [senast uppdaterad c2009; citerad 2012 mar 27].
Tillgänglig på:
http://aceproject.org/electoral-advice/archive/questions/replies/77098994

[15] Valmyndigheten.
Röstning [hemsida på Internet].
Inget datum [senast uppdaterad 2011 aug 09; citerad 2012 mar 26].
Tillgänglig på:
http://www.val.se/det_svenska_valsystemet/rostning/index.html

[16] Valmyndigheten.
Budrösta [hemsida på Internet].
Inget datum [senast uppdaterad 2011 mar 24; citerad 2012 mar 26].
Tillgänglig på:
http://www.val.se/det_svenska_valsystemet/rostning/budrosta/index.html

[17] Valmyndigheten.
Jobba med val [hemsida på Internet].
Inget datum [senast uppdaterad 2008 nov 24; citerad 2012 mar 26].
Tillgänglig på:
http://www.val.se/det_svenska_valsystemet/jobba_med_val/index.html

[18] Vabariigi Valimiskomisjon.
Statistics about Internet Voting in Estonia [hemsida på Internet].
Inget datum [citerad 2012 apr 11].
Tillgänglig på:
http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics

[19] British Broadcasting Corporation News.
Estonia claims new e-voting first [hemsida på Internet].
Inget datum [senast uppdaterad 2007 mar 1, citerad 2012 apr 11].

Tillgänglig på:
http://news.bbc.co.uk/2/hi/europe/6407269.stm

[20] Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens.
eID Interoperability for PEGS: Update of Country Profiles study Estonian country profile [hemsida på Internet].
2009 Jul [citerad 2012 apr 11].
Tillgänglig på:
http://ec.europa.eu/idabc/servlets/Doc7398.pdf?id=32304

[21] Vabariigi Valimiskomisjon.
E-Voting System General Overview [hemsida på Internet].
c2005 [senast uppdaterad 2010, citerad 2012 apr 11].
Tillgänglig på:
http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf

[22] Vabariigi Valimiskomisjon.
E-voting concept security: analysis and measures [hemsida på Internet].
2010 Dec 27 [citerad 2012 apr 11].
Tillgänglig på:
http://www.vvk.ee/public/dok/E-voting_concept_security_analysis_and_measures_2010.pdf

[23] Paar Christof, Pelzl Jan.
Understanding Cryptography: A Textbook for Students and Practitioners [bok men hämtad från hemsida på Internet].
2010 jul 8 [citerad 2012 jul 8].
Relevant sektion tillgänglig på:
http://wiki.crypto.rub.de/Buch/download/Understanding-Cryptography-Chapter1.pdf

[24] Kanellos Michael.
Moore's Law to roll on for another decade [hemsida på Internet].
2003 feb 10 [citerad 2012 apr 11].
Tillgänglig på:
http://news.cnet.com/2100-1001-984051.html

[25] Crolla Koen.
Symmetric and Asymmetric Encryption [hemsida på Internet].
2007 dec 2 [citerad 2012 apr 11].
Tillgänglig på:
http://cairnarvon.rotahall.org/2007/12/02/symmetric-and-asymmetric-encryption/

[26] Wikipedia.
Public-key cryptography [hemsida på Internet].
Inget datum [senast uppdaterad 2012 apr 10, citerad 2012 apr 11].
Tillgänglig på:
http://en.wikipedia.org/wiki/Public_key

[27] Armknecht Frederik, Katzenbeisser Stefan, Peter Andreas.
Group Homomorphic Encryption: Characterizations, Impossibility Results, and Applications [hemsida på Internet].
2010 Sep 29 [senast uppdaterad 2012 jan 6, citerad 2012 apr 11].
Tillgänglig på:
http://eprint.iacr.org/2010/501.pdf

[28] Rivest Ron.
Lecture Notes 15 : Voting, Homomorphic Encryption [hemsida på internet].
2002 okt 29 [citerad 2012 apr 11].

Tillgänglig på:
http://web.mit.edu/6.857/OldStuff/Fall02/handouts/L15-voting.pdf

[29] Fujisaki Eiichiro, Okamoto Tatsuaki, Pointcheval David, et al.
RSA-OAEP is Secure under the RSA Assumption [hemsida på Internet].
2000 nov 27 [senast uppdaterad 2001 maj 29, citerad 2012 apr 11].
Tillgänglig på:
http://eprint.iacr.org/2000/061.pdf

[30] Dai Wei.
Crypto++ 5.6.0 Benchmarks [hemsida på Internet].
Inget datum [senast uppdaterad 2009 mar 31, citerad 2012 apr 11].
Tillgänglig på:
http://www.cryptopp.com/benchmarks.html

[31] Statistiska centralbyrån.
Antalet förstagångsväljare fortsätter att öka [hemsida på Internet].
2010 jan 19 [citerad 2012 mar 30].
Tillgänglig på:
http://www.scb.se/Pages/PressRelease____285869.aspx

[32] The Federal Financial Institutions Examination Council.
Authentication in an Internet Banking Environment [hemsida på Internet].
2001 aug 8 [citerad 2012 apr 11].
Tillgänglig på:
http://www.ffiec.gov/pdf/authentication_guidance.pdf

[33] Harowitz Sherry.
Faking Fingerprints and Eying Solutions [hemsida på Internet].
2007 Mar [citerad 2012 apr 11].
Tillgänglig på:
http://www.securitymanagement.com/article/faking-fingerprints-and-eying-solutions

[34] Alphacard.
Proximity Cards & RFID Cards [hemsida på Internet].
Inget datum [citerad 2012 Apr 11].
Tillgänglig på:
http://www.alphacard.com/id-cards/rfid-cards.shtml

[35] High Tech Aid.
Introduction to Magnetic Stripe & Other Card Technologies [hemsida på Internet].
Inget datum [citerad 2012 apr 11].
Tillgänglig på:
http://www.hightechaid.com/tech/card/intro_ms.htm

[36] Statistiska centralbyrån.
Allmänna val, valdeltagandeundersökningen: Ett mer jämlikt valdeltagande [hemsida på Internet].
2011 apr 14 [citerad 2012 apr 14].
Tillgänglig på:
http://www.scb.se/Pages/PressRelease____311613.aspx