KTH Computer Science
and Communication

Riksdagsval via Internet

Ett system för säkra val via Internet i Sverige

Jonas af Sandeberg
Pilotgatan 4
12832 Skarpnäck
070-7989373
jonasp9@kth.se

Handledare: Henrik Eriksson

Kursnr: DD143X
Examensarbete inom datalogi vid CSC
Kungliga Tekniska Högskolan

Sammanfattning

I denna uppsats designas ett system för val via Internet i Sverige. För att göra detta undersöks först hur dagens system för val i Sverige ser ut. Därefter undersöks vilka tekniker som kan användas för att bygga ett sådant system. Slutligen undersöks system som redan använts för val via Internet i andra länder. Utifrån resultatet i undersökningarna designas sedan ett system för val via Internet i Sverige. Designen tar hänsyn till alla säkerhetskrav för demokratiska val. Uppsatsen visar på att det är möjligt att designa ett system för val via Internet i Sverige samt att införandet av ett sådant system bör öka valdeltagandet.

Abstract

Net Voting

In this essay a system for voting via the Internet in Sweden is designed. To do this the current swedish election system is examined. Research is also done on what technologies can be used to build such a system. Lastly systems already used for Internet voting in other countries are examined. Based on the result of the research a system for voting via the Internet in Sweden is designed. The system is designed to follow all safety regulations demanded by a democtratic election. The essay shows that it is possible to design a system for voting via the Internet in Sweden and also that such a system likely would increase the turnout in elections.

Innehåll

Figurer

Kapitel 1

Inledning

En grundprincip för demokrati är att alla ges möjlighet att rösta. Demokrati bygger på att folket via röstning visar sin vilja. FN anser det vara en medborgerlig och politisk rättighet att varje medborgare ska ha rätt och möjlighet att rösta vid val [3].

Att delta i ett riksdagsval eller en folkomröstning ska därför vara så enkelt som möjligt. Ingen ska avstå från att delta på grund av att det är för krångligt att rösta, oavsett var man befinner sig i världen under valet. Om rösterna kan läggas via Internet skulle det underlätta röstningen för många och även räkningen av rösterna. Ett system för att genomföra val på Internet skulle kunna förbättra möjligheterna för en väl fungerande demokrati.

1.1 Problem

1.1.1 Uppsatsens sammanhang

Detta är en kandidatuppsats som skrivits i kursen *Examensarbete inom datalogi, grundnivå* med kurskod DD143X. Kursen ges av CSC på Kungliga Tekniska Högskolan och ingår i utbildningen *Civilingenjör Datateknik*.

1.1.2 Uppsatsens mål

Målet med uppsatsen är att designa ett system för val via Internet i Sverige. För att göra detta undersöks först existerande tekniker som kan användas för att bygga systemet. Därefter undersöks redan använda system för detta ändamål.

1.1.3 Begränsning

Valsystemet ska designas så att det är säkert och utnyttjar existerande tekniker. Fokus ligger främst på den tekniska delen av systemet. Denna uppsats går inte in på djupet inom varje område utan designen är på en rätt hög abstraktionsnivå och ingen implementation görs.

1.2 Ordlista

Autenticitet: Autenticitet betyder äkthet. Med ett autentiskt e-postmeddelande menas att det är garanterat att det kommer från den påstådda avsändaren, det är alltså inte förfalskat [4].

DoS-attack: En DoS(Denial of Service)-attack är en attack som syftar till att göra ett datasystem otillgängliga för dess användare [5]. Oftast görs detta genom att skicka massvis med data till systemet för att det ska bli överbelastat och inte ha resurser kvar att ta hand om något annat.

Hemlig nyckel: Den nyckel i asymmetrisk kryptering som hålls hemlig, ingen annan än ägaren ska ha tillgång till den [6].

Integritet: Med integritet (eller dataintegritet) menas att data är densamma som ursprungliga data [7]. Till exempel om en fil överförts från en dator till en annan och förändras på något sätt på vägen så är dess integritet skadad.

Intrusion detection and prevention system (IDPS): Kallas ibland också för "Intrusion prevention system" (IPS). Dessa system övervakar nätverk eller datasystem för att hitta otillåtna aktiviteter och därefter försöka stoppa dessa [8]. Dessutom sparas information om allt som upptäcks.

Kanton: En kanton är en delstat i Schweiz.

"Man-in-the-middle attack": En "man-in-the-middle attack" är en attack som går ut på att en angripare fångar upp trafiken mellan två parter [9]. De båda parterna luras att tro att de pratar enskilt med varandra medan all trafik egentligen går genom angriparen som kan läsa trafiken eller modifiera den efter tycke.

Nyckel: Används vid kryptering som parameter till krypteringsalgoritmen för att bestämma hur utdata ska se ut [6]. Nyckeln behövs för att kryptering ska vara användbart. För att kunna dekryptera något krävs tillgång till rätt nyckel.

Rösträtt: För att en väljare ska få rösta i ett val krävs att denne har rösträtt [10].

Trojan: En trojan är programvara som ger ut sig för att vara användbar (kan också vara det på riktigt) men som utför hemliga funktioner som kan vara skadliga [11].

Valsedel: Ett papper motsvarande en röst på ett visst alternativ i ett val [10].

Virus: Ett virus är programvara som verkar genom att modifiera annan

programvara på datorn och får den programvaran att köra sin egen kod. Kan på detta sätt utföra skadliga eller icke-skadliga funktioner [12].

Öppen nyckel: Den nyckel i asymmetrisk kryptering som inte hålls hemlig utan delas ut till andra [6].

Del I

Bakgrund

Kapitel 2

Valen i Sverige idag

I Sverige har vi val vart fjärde år [10]. Den andra söndagen i september är det dessa år val till riksdagen, kommun- samt landstingsfullmäktige.

Sverige är medlem i Europeiska unionen. Därför är det vart femte år även val till Europaparlamentet, som för alla medlemsländer i Europeiska unionen. Detta val är i juni, i Sverige är det alltid på en söndag.

Förutom dessa återkommande val kan riksdagen besluta om extra val. Dessa måste då ske inom tre månader från när beslutet togs. Därför skiljer sig några av reglerna åt jämfört med vanliga val, till exempel hur lång perioden för förtidsröstning är. I princip är det dock samma regler som gäller.

2.1 Hur röstningen går till

Valen i Sverige sker idag genom att väljarna på valdagen går till en vallokal [10]. Vilken vallokal den enskilde väljaren ska gå till bestäms utifrån bostadsort. Väl där får väljaren ta en valsedel för varje val denne deltar i och lägga valsedlarna i separata kuvert. Innan kuverten läggs i valurnorna måste väljaren legitimera sig med en giltig id-handling.

Även innan valdagen går det att rösta. Detta kan göras i speciella röstningslokaler från och med 18 dagar innan valdagen. Röstningslokaler kan till exempel vara bibliotek eller kommunhus. En väljare som röstar i förväg i en röstningslokal måste ha med sig sitt röstkort. Har en väljare inte möjlighet att ta sig till varken en röstnings- eller vallokal kan denne rösta med bud. Då får någon annan ta väljarens röst antingen till en val- eller röstningslokal, för detta gäller speciella regler. En väljare som inte är i Sverige under valperioden kan rösta på vissa utlandsmyndigheter. Då börjar röstningen 24 dagar innan valdagen och kan ibland vara öppen endast en kort tid då rösterna måste hinna till Sverige i tid för valet. Från utlandet går det även att brevrösta. Rösten måste då skickas tidigast 45 dagar före valet och senast på valdagen. Det går inte att brevrösta från Sverige.

Om en väljare röstat i förväg men ändrat sig kan denne rösta på nytt på valdagen. Den tidigare rösten ogiltigförklaras och den nya rösten räknas istället.

2.2 Rösträtt

Alla som har rätt att rösta i Sverige vid ett visst val får hem ett röstkort i brevlådan. För att ha rösträtt i val till Riksdagen krävs medborgarskap i Sverige, att väljaren uppnått 18 års ålder senast på valdagen samt att väljaren är eller har varit folkbokförd i Sverige [10].

De som uppfyller kraven för rösträtt till riksdagen uppfyller även kraven för rösträtt i val till Europaparlamentet. Medborgare från andra medlemsstater i Europeiska unionen får också rösta i detta val om de är folkbokförda i Sverige senast 30 dagar före valdagen samt att de anmält sig. Det är endast tillåtet att rösta i ett land i valet till Europaparlamentet. Lägger en väljare sin röst i Sverige får denne alltså inte rösta i något av de andra medlemsländerna.

respektive landstinget samt att väljaren är minst 18 år. Förutom det krävs svenskt medborgarskap För val till landstings- och kommunfullmäktige krävs att väljaren är folkbokförd inom kommunen eller medborgarskap i något annat land som tillhör Europeiska unionen. I det senare fallet krävs att väljaren senast 30 dagar innan valet var folkbokförd i Sverige. Även Norska och Isländska medborgare har rösträtt under samma förutsättningar som medborgare i Europeiska unionen. En utländsk medborgare från något annat än de nämnda länderna måste ha varit folkbokförd i Sverige i tre år i följd före valdagen för att erhålla rösträtt.

2.3 Rösträkning

När röstperioden är slut räknas rösterna i varje valdistrikt, tillsammans med de förtidsröster som hunnit komma in till det distriktet, för hand [10]. Därefter rapporterar varje distrikt resultatet via telefon till Valmyndigheten. På detta sätt fås redan samma kväll ett preliminärt resultat av valet. Dock återstår vissa röster att räknas i form av förtidsröster och brevröster som inte hunnit fram till vallokalerna. Det exakta resultatet är alltså inte färdigt förrän flera dagar senare. Landstingsvalet som räknas sist brukar vara klart först ca 10 dagar efter valdagen.

2.4 Säkerhetskrav

Det finns många säkerhetsaspekter att tänka på i ett val. För att ett val ska gå att genomföra måste följande punkter vara uppfyllda [13].

- Det måste gå att styrka identiteten hos väljaren.
- Det måste gå att bekräfta att väljaren har rösträtt i just det här valet.
- Ingen väljare får utnyttja sin röst mer än en gång. Flera röster kan läggas men endast en får räknas.
- Det får inte gå att manipulera en lagd röst.

- Det måste gå att garantera anonymitet, ingen får kunna se vad en annan väljare röstat.
- Det måste gå att säkerställa att räkningen av rösterna är korrekt.
- Systemet måste vara tillförlitligt.

2.5 Säkerhetslösningar i dagens system

I dagens system har hänsyn tagits till de säkerhetsaspekter som togs upp tidigare i kapitel 2.4. En väljare måste styrka sin identitet med en giltig id-handling och finnas med i röstlängden, listan över väljare i det distriktet, för att få rösta. När väljaren lägger sin röst prickas denne av i listan och får därefter inte lägga någon ny röst. Lagda röster ligger i lådor som ingen utom de som ska räkna rösterna kan komma in i. Anonymitet garanteras genom att valsedeln läggs i ett slutet kuvert innan det läggs ned i valurnan. Den som tar emot rösten kontrollerar också att rösten är korrekt genom att se så det är rätt färg på valsedel som ligger i kuvertet. Kuverten är försedda med ett litet "fönster" som gör det möjligt att se att det ligger en valsedel i kuvertet samt vilken färg det är på valsedeln, men inget mer.

Kapitel 3

Tekniker som kan användas

Här undersöks vilka tekniker som kan användas för att införa ett system för val via Internet i Sverige som uppfyller kraven i kapitel 2.4.

3.1 BankID

I Sverige är idag BankID det vanligaste sättet att verifiera en persons identitet på Internet [14]. För slutanvändare fungerar BankID genom att ett säkerhetsprogram laddas ned och installeras [15]. Därefter beställs ett BankID från en bank. Exakt hur detta går till varierar från bank till bank. För att få beställa BankID krävs en giltig legitimation, innehas inte något sätt att legitimera sig på via Internet kan banken avkräva ett besök på ett kontor för legitimering. Efter lyckad legitimering laddas en personlig fil ned som är ens e-legitimation. När filen laddas ned väljs en personlig kod. Denna kod krävs sedan för legitimering. När koden valts importeras filen av säkerhetsprogrammet och legitimering via Internet är nu möjlig.

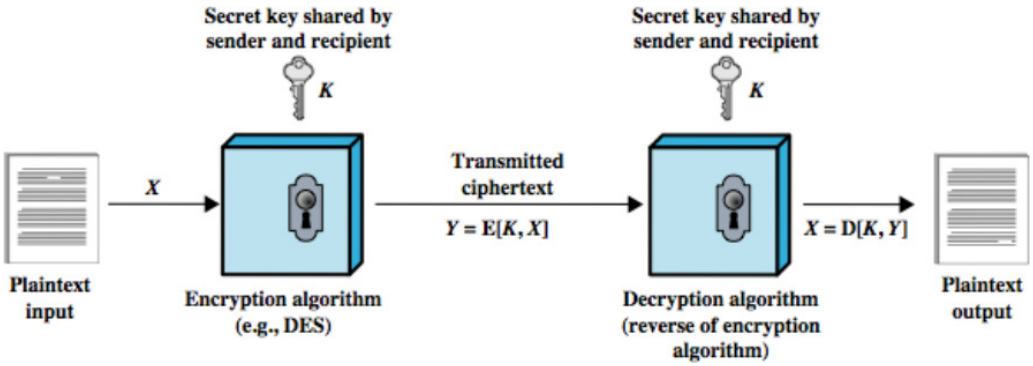
Sedan oktober 2011 finns även mobilt BankID till vissa tjänster [16]. Det fungerar på ett liknande sätt men då är säkerhetsprogrammet och certifikatet på en smart mobiltelefon istället. Fördelen säkerhetsmässigt blir att det krävs fysisk tillgång till den smarta mobiltelefonen för att kunna legitimera sig, det räcker inte med att få tag på en fil. Installationen sker på ett liknande sätt som med BankID på fil.

3.2 Kryptering

För att hemlighålla digitalt material och skydda det så att inte obehöriga kan ta del av det kan kryptering användas. Kryptering skyddar ditt material från obehöriga genom att använda en algoritm som kastar om datan i ditt material så att det inte blir läsligt [6]. Vill du kunna läsa materialet måste du göra krypteringsalgoritmer baklänges, detta kallas dekryptering. Kryptering kan göras på flera olika sätt. Två varianter är symmetrisk- och asymmetrisk kryptering.

3.2.1 Symmetrisk kryptering

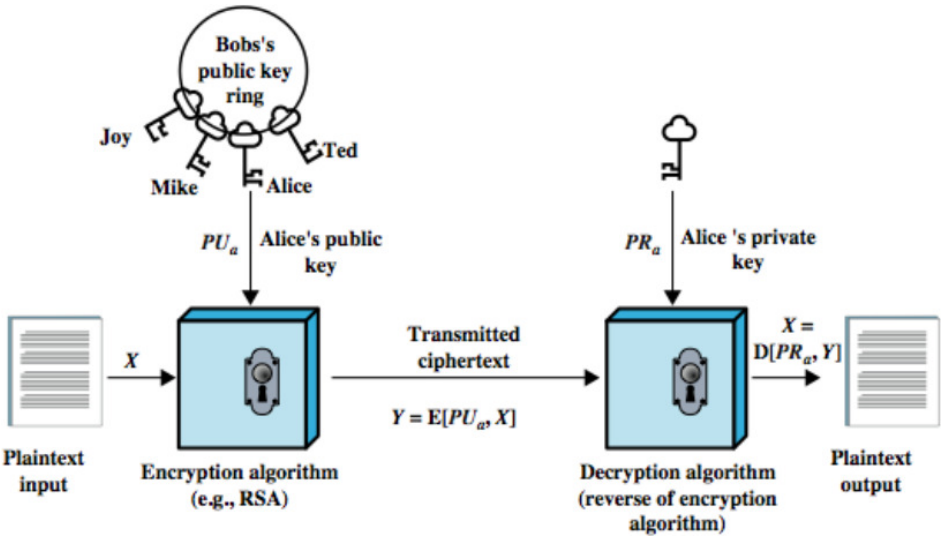
I symmetrisk kryptering används samma nyckel vid kryptering och dekryptering [6]. Både avsändaren och mottagaren måste därmed ha tillgång till samma nyckel för att kunna använda sig av denna typ av kryptering. Att på ett säkert sätt komma fram till en gemensam nyckel utan att någon obehörig får tillgång till nyckeln kan vara ett problem. Detta problem är löst i asymmetrisk kryptering som beskrivs härnäst. En fördel symmetrisk kryptering har över asymmetrisk kryptering är att den kräver mindre beräkningskapacitet.



Figur 3.1. Symmetrisk kryptering [1]

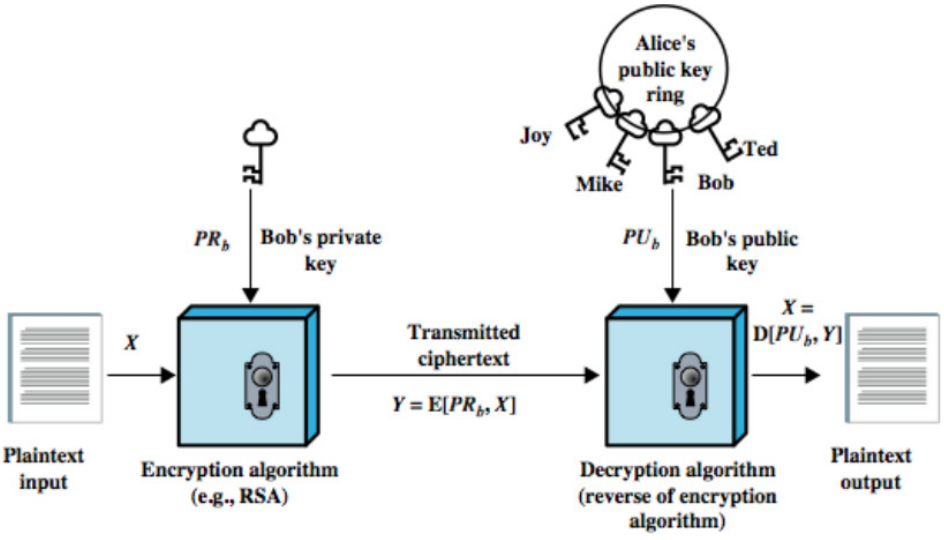
3.2.2 Asymmetrisk kryptering

Skillnaden i asymmetrisk kryptering är att två olika nycklar används [6]. Ena nyckeln hålls hemlig medan den andra är öppen. Asymmetrisk kryptering kan därför användas på flera sätt. Om du krypterar ett meddelande med din kompis Alices öppna nyckel, som i Figur 3.2, blir hon den enda som kan läsa meddelandet. Alice är ju den enda med tillgång till sin hemliga nyckel och alltså den enda som kan dekryptera meddelandet. Denna typ av asymmetriska kryptering används vid signering av certifikat.



Figur 3.2. Asymmetrisk kryptering [1]

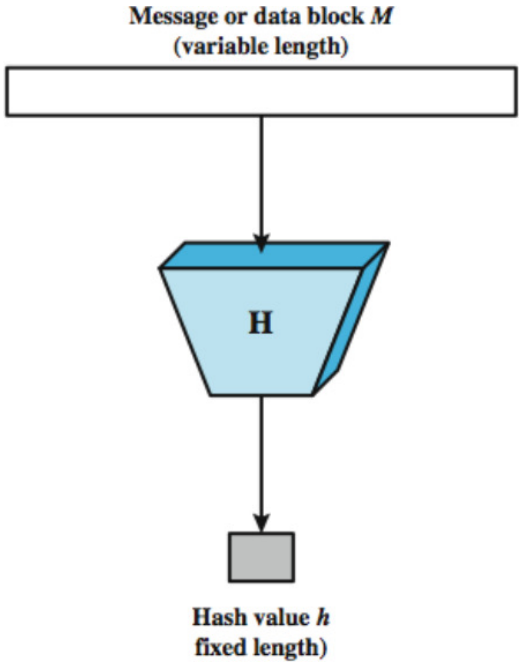
Ett annat sätt asymmetrisk kryptering kan användas på är genom att kryptera ett meddelande med sin hemliga nyckel som i Figur 3.3 [6]. Därefter kan andra dekryptera meddelandet med din öppna nyckel. Därmed kan de vara säkra på att det verkligen var du som skrev meddelandet eftersom endast du har tillgång till din hemliga nyckel. På detta sätt kan asymmetrisk kryptering användas för verifiering av meddelandets autenticitet.



Figur 3.3. Verifiering av ett meddelandes autenticitet med hjälp av asymmetrisk kryptering [1]

3.3 Hashfunktioner

Som Figur 3.4 visar tar en hashfunktion indata av variabel längd och producerar ett hashvärde av en specifik längd [4]. Ofta fylls meddelandet ut till en längd ursprungliga meddelandet. Detta försvårar att någon hittar ett annat meddelande som ger samma som är jämt delbar med ett bestämt värde (exempelvis 1024). Utfyllnaden innehåller då längden på det hashvärde. För att en hashfunktion ska vara bra krävs att det är i princip beräkningsmässigt otänkbart att utifrån ett hashvärde beräkna det ursprungliga meddelandet samt att hitta två meddelanden som ger samma hashvärde.

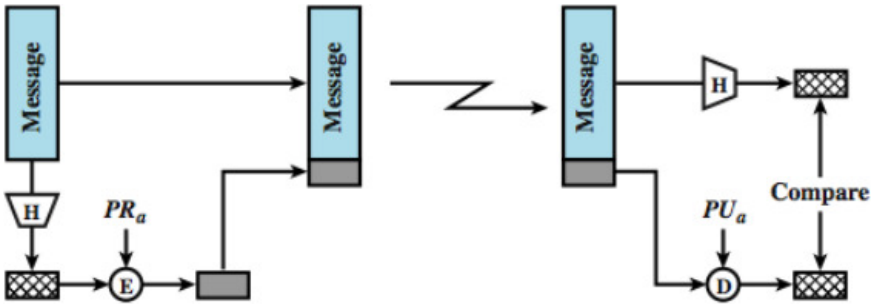


Figur 3.4. En hashfunktion [1]

3.4 Elektronisk signatur

För att skydda integriteten av ett meddelande och garantera att det inte har modifierats på vägen till mottagaren kan en elektronisk signatur användas [17]. Detta kan göras på flera sätt. Det sätt som används i uppsatsens design använder sig av en hashfunktion och asymmetrisk kryptering. Som det går att se i Figur 3.5 körs meddelandet först i en hashfunktion (H). Det erhållna hashvärdet krypteras sedan med användarens hemliga nyckel (PR_a) och läggs till på slutet av meddelandet. Det krypterade hashvärdet kallas för en elektronisk signatur (grå rutan). När mottagaren tagit emot meddelandet plockas signaturen bort. Med hjälp av avsändarens öppna nyckel (PU_a) dekrypteras hashvärdet. Mottagaren

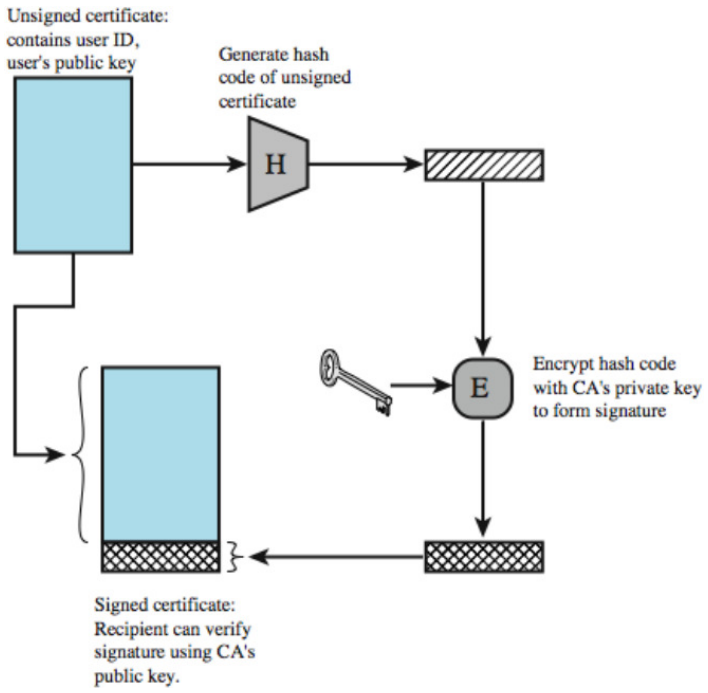
skickar meddelandet genom samma hashfunktion som avsändaren och jämför sitt hashvärde med det mottagna. Om de är lika är integriteten hos meddelandet fastställd.



Figur 3.5. Elektronisk signatur för säkerställning av ett meddelandes integritet [1]

3.5 Certifikat

Som Figur 3.6 visar kan ett certifikat delas in i två delar. Första delen (den blå rutan i Figuren) innehåller information om vem certifikatet är utgivet till, dennes öppna nyckel, hur länge certifikatet gäller och vem som utfärdat det etc. [17]. Den andra delen är en elektronisk signatur. Hashvärdet i signaturen beräknas utifrån all information i certifikatets första del och krypteras sedan med utgivarens hemliga nyckel. På detta sätt kan certifikatet valideras genom att ett eget hashvärde beräknas och jämförs med hashvärdet i signaturen. Är de lika har det säkerställts att ingenting i certifikatet har ändrats och därmed påvisat certifikatets autenticitet.



Figur 3.6. Signering av certifikat [1]

3.6 Kryptering med öppen nyckel

För att certifikat ska kunna användas till legitimering på ett säkert sätt krävs att det går att lita på autenticiteten hos certifikaten. PKI (eng. Public key infrastructure) är en infrastruktur som löser detta problem [18]. Principen är att det högst upp i kedjan finns en, eller flera, certifikatutgivare (eng. Certificate Authority, förkortas CA). Utgivaren är den som ger ut och signerar certifikat. Ett certifikat som är signerat av en utgivare betraktas som autentiskt eftersom ingen annan än utgivaren har tillgång till utgivarens hemliga nyckel.

3.7 Krypterad trafik

SSL (Secure Sockets Layer) och den nyare TLS (Transport Layer Security) är protokoll för säker överföring av data [19]. TLS är lite nyare men fungerar på liknande sätt som SSL. SSL använder sig av ett protokoll som beskrivs mer i detalj nedan. Det fungerar genom att två parter via en sekvens meddelanden bestämmer en krypteringsalgoritm, en algoritm för generering av hashvärden samt en symmetrisk nyckel för dessa algoritmer. På detta sätt kan sedan en krypterad överföring användas mellan parterna. Datan som överförs kan inte avlyssnas av någon som inte har tillgång till den symmetriska nyckeln. En elektronisk signatur garanterar att ingen har ändrat på den överförda datan.

3.7.1 Handslagsprotokollet

När en anslutning ska öppnas görs detta enligt “Handlagsprotokollet” (min översättning, eng. Handshake protocol) [19]. Protokollet bestämmer vilka algoritmer som ska användas för kryptering och signering samt sköter utbytet av den gemensamma nyckeln. Exakt hur det ser ut varierar dock, bland annat på om båda parter har certifikat samt klientens webbläsare etc. Detta exempel är en något förenklad beskrivning av hur det skulle kunna se ut om endast servern har ett certifikat.

Klienten skickar först ett meddelande med information om vilka krypteringsalgoritmer etc. som den har stöd för [20]. Meddelandet innehåller även ett slumpat tal som kommer användas för att generera den delade nyckeln. Servern svarar med information om vilka tekniker som stöds, eventuellt ett sessions ID, samt ett slumpat tal. Därefter skickar servern ett certifikat till klienten. Klienten genererar en nyckel med de båda slumpade talen. Nyckeln krypteras med serverns öppna nyckel och skickas till servern. Endast om servern har tillgång till den hemliga nyckeln tillhörande det certifikat som servern skickade kan processen gå vidare. På detta sätt vet klienten att servern verkligen är densamma som certifikatet säger. Nu har båda parter tillgång till nyckeln och den kan användas för att kryptera den data som skickas.

Kapitel 4

Tidigare använda system

I detta kapitel beskrivs ett par tidigare system som använts för val via Internet, hur de systemen utformats samt resultaten de gav.

4.1 Schweiz

I Schweiz tilläts år 2008 den del av befolkningen som var utomlands under valperioden att rösta via Internet [21]. Året efter blev Genève den andra kantonen i Schweiz att tillåta Internetröstning [22]. I detta kapitel beskrivs hur det Schweiziska systemet är uppbyggt.

4.1.1 Design

Alla som har rösträtt får hem ett röstkort som krävs för att rösta via Internet. Dessa röstkort innehåller ett unikt slumpat röstkortsnummer. Förutom detta finns även en PIN-kod samt en kontrollkod för extra verifiering av servern. Innan röstkorten skickas ut körs alla röstkortsnummer genom hashfunktionen och hashvärdena sparas i systemet. Röstkortsnummret skickas aldrig under röstningen utan istället skickas hashvärdet för röstkortsnummret. Detta gör det väldigt svårt att gissa röstkortsnummret innan röstningsprocessen slutförts.

När en väljare kopplar upp sig mot servern verifieras denna med ett certifikat och en anslutning via SSL öppnas. Klienten skickar också ett certifikat som kontrolleras av servern, detta för att försvåra "man-in-the-middle-attacker" [23]. Hashvärdet av röstkortsnummret används för identifiering av väljaren. Därefter används röstkortsnummret som en delad nyckel av servern och klienten.

Alla meddelanden som skickas till servern krypteras med den delade nyckeln. Därefter skapas ett hashvärde som krypteras med klientens hemliga nyckel. På detta sätt både krypteras och signeras alla meddelanden. Detta försäkrar meddelandets autenticitet och integritet, alltså att meddelandet verkligen kommer från den riktiga klienten och att det inte har blivit ändrat på vägen till servern. En Java-applet används för att utföra hashfunktionen och krypteringen.

När väljaren skickat in sin röst till servern får väljaren tillbaka en bekräftelse på att rösten kommit fram. I bekräftelsen finns även en kontrollkod som väljaren jämför med kontrollkoden på röstkortet. Denna kontrollkod har endast den riktiga server tillgång till och på så sätt kan väljaren vara säker på att denne inte röstat via en falsk server.

Lagring av röster

Innan valet förseglas den digitala valurnan med kryptering och öppnas inte förrän efter valets slut [23]. Det är flera parter involverade i att skapa och förvara de olika nycklarna som krävs för att låsa och öppna valurnan. På detta sätt blir det väldigt svårt att öppna valurnan för någon obehörig.

När en röst har lagts krypteras den tillsammans med platsen för röstningen och lagras i den digitala valurnan [23]. I listan över väljare markeras att väljaren har röstat. Det lagras ingenting som kan koppla en röst till en väljare. För varje röst som lagras stegas en räknare upp ett steg. Mätaren är krypterad med symmetrisk kryptering av applikationen. Räknaren används för att kunna verifiera att alla röster har räknats när räkningen utförts.

För att kunna räkna rösterna och få fram valresultatet krävs samarbete av de personer som ansvarar över lagringen av nycklarna [23]. Totalt sett är minst 11 personer delaktiga i skapandet och lagringen av nycklarna. Detta ökar säkerheten eftersom det blir mycket svårare att få tag i alla nycklar som krävs för att öppna valurnan.

4.2 Estland

Röstning via Internet testades första gången i valet år 2005 och har nu hunnit användas i fem val [24].

4.2.1 Design

Kort beskrivet fungerar deras system ungefär som deras brevröstning [25]. För brevröstningen används två kuvert. I det första kuvertet lägger väljaren sin röst och försluter det sedan. Detta kuvert innehåller ingen information om väljaren. Därefter lägger väljaren det slutna kuvertet i ett annat kuvert som innehåller all nödvändig information om väljaren. Kuverten skickas till valmyndigheten där uppgifterna om väljaren kontrolleras och det yttre kuvertet öppnas. Därefter läggs det inre kuvertet i valurnan. På detta sätt hålls väljarens röst anonym. I det digitala systemet består det inre kuvertet i huvudsak av en krypterad röst medan det yttre består av en digital signatur.

I Estland är det tillåtet att rösta flera gånger via Internet. Det är endast den senaste rösten som räknas. Röstar väljaren med någon annan metod än via Internet så räknas den andra rösten. Har väljaren förtidsröstat, oavsett sätt, kan denne ändå rösta på valdagen i en vallokal och då räknas endast rösten från vallokalen.

För att identifiera väljaren används ID-kort och en dosa. Estländska ID-kort har ett chip som kan läsas av dosor (liknande de som bland annat Nordea har i Sverige). Eftersom en stor del av befolkningen har denna sorts ID-kort och dosa så är röstningssystemet väldigt lättillgängligt. Även ett mobilt ID samt ett digitalt ID går att använda till legitimering [24].

4.3 Resultat av tidigare använda system

4.3.1 Schweiz

I Genève finns det ingen statistik som kan visa på effekten av införandet av Internetröstning [26]. Detta på grund av en lag som endast tillåter att 20% av befolkningen i en kanton tillåts använda Internetröstning. Eftersom endast en liten del av befolkningen ges möjlighet att rösta via Internet är det svårt att dra några slutsatser om huruvida deltagandet påverkats.

4.3.2 Estland

Statistiken i Figur 4.1 tyder på att valdeltagandet i Estland har ökat sedan valet då röstning via Internet infördes. I lokala valet år 2005 var valdeltagandet 47,4%, år 2009 hade det stigit till 60,6%. Även i parlamentvalen har deltagandet stigit något, från 61,9% år 2007 till 63,5% år 2011.

Ännu tydligare är att andelen som utnyttjat möjligheten att rösta via Internet ökat för varje val som hållits sedan systemet infördes. I valet 2005 var det 1,9% av de deltagande väljarna som röstade jämfört med 24,3% år 2011.

Om det är införandet av Internetröstning som fått det totala valdeltagandet att öka går inte att säga med säkerhet endast utifrån denna statistik. Att användandet av systemet ökat tyder dock på att befolkningens tilltro till systemet ökar och att många tycker det finns fördelar med att rösta via Internet. Om inga fördelar finns skulle väljarna hålla sig till att rösta med de tidigare systemen. Resonemanget att valdeltagandet ökar när tillgängligheten ökar ser alltså ut att få stöd av denna statistik. Med Internetröstning kan väljarna rösta vilken tid de vill och varifrån de vill vilket bör anses som förbättrad tillgänglighet jämfört med tidigare system.

	Local elections 2005	Parliamentary elections 2007	European Parliament elections 2009	Local elections 2009	Parliamentary elections 2011
Eligible voters	1 059 292	897 243	909 628	1 094 317	913 346
Participating voters(voters turned out)	502 504	555 463	399 181	662 813	580 264
Voter turnout	47,4%	61,9%	43,9%	60,6%	63,5%
I-voters	9 317	30 275	58 669	104 413	140 846
I-votes counted	**9 287**	**30 243**	**58 614**	**104 313**	**140 764**
I-votes cancelled (replaced with paper ballot)	30	32	55	100	82
Multiple I-votes(replaced with I-vote)	364	789	910	2 373	4 384
I-voters among eligible voters	0,9%	3,4%	6,5%	9,5%	15,4%
I-voters among participating voters	**1,9%**	**5,5%**	**14,7%**	**15,8%**	**24,3%**
I-votes among advance votes	7,2%	17,6%	45,4%	44%	56,4%
I-votes cast abroad among I-votes	n.a.	2% * 51 states	3% * 66 states	2,8% ** 82 states	3,9%* 105 states
I-voting periood	3 days	3 days	7 days	7 days	7 days
I-voters using mobile-ID	n.a.	n.a.	n.a.	n.a.	2 690
I-voters using mobile-ID among I-voters	n.a.	n.a.	n.a.	n.a.	1,9%

** permanently and temporarily abroad*

*** temporarily abroad*

Figur 4.1. Statistik över Internetröstning i Estland [2]

Del II

Resultat

Kapitel 5

Design

I detta kapitel beskrivs ett förslag på hur val via Internet skulle kunna utföras i Sverige.

5.1 Förberedelser

Innan valperioden börjar måste vissa förberedelser göras av Valmyndigheten.

- Nycklar för kryptering av röster måste genereras och ansvaret över dem bör delas upp på flera personer så att ingen ensam person kan dekryptera rösterna. Förslagsvis kan nycklarna delas upp till personer både inom valmyndigheten och någon ytterligare institution, exempelvis polisen.
- Röstkortsnummer och kontrollkoder ska genereras och tryckas på respektive röstkort tillsammans med all annan information som sedan tidigare ska finnas på röstkorten. Kontrollkoden lagras i klartext i databasen över väljare medan röstkortsnummret körs genom en hashfunktion och lagras som ett hashvärde.
- Systemet måste sättas upp i ett skyddat nätverk. Skydd som bör användas är till exempel en välkonfigurerad brandvägg samt ett system som upptäcker och skyddar mot intrång och attacker, ett så kallat "Intrusion detection and prevention system". Dessa system tas inte upp i denna uppsats.

För väljarnas del krävs endast en förberedelse: att väljaren har ett BankID på den dator som ska användas för röstningen.

5.2 Själva röstningen

Samma valperiod bör gälla för Internetröstning som för annan förtidsröstning. Valprocessen börjar med att väljaren kopplar upp sig mot servern i sin webbläsare. En kontroll görs att BankID är installerat på väljarens dator, annars kan väljaren inte gå vidare. Väljaren loggar in med BankID och identifierar sig själv.

Anslutningen är krypterad via TLS. Information om vilka val väljaren kan göra skickas från servern. Väljaren fyller i valsedeln samt fyller i sitt unika röstkortsnummer. När väljaren är klar och väljer att skicka in sin röst kontrolleras att valsedeln är korrekt ifylld. Om allt är korrekt skickas röstkortsnummret in i hashfunktionen. Rösten krypteras med symmetrisk kryptering där hashvärdet används som nyckel.

Innan rösten skickas iväg signeras den genom att beräkna ett hashvärde och sedan kryptera hashvärdet med väljarens hemliga nyckel via BankID. När den krypterade och signerade rösten tagits emot av servern kontrolleras först signaturen för att säkerställa röstens integritet. Om signaturen är korrekt letas hashvärdet och kontrollkoden för väljaren upp i databasen. Hashvärdet används för att dekryptera rösten.

En krypterad bekräftelse skickas tillbaka till väljaren, återigen används hashvärdet som nyckel. Bekräftelsen innehåller de alternativ väljaren röstat på samt kontrollkoden. Väljaren jämför kontrollkoden med den som finns på röstkortet för att försäkra sig om att rösten skickats till den riktiga servern.

Därefter markeras i databasen över väljare att väljaren röstat samt vilken tid röstningen skedde. Rösten krypteras med serverns öppna nyckel och lagras tillsammans med den digitala signaturen. Räknaren som håller koll på hur många röster som lagts räknas upp ett steg.

Om en röst kommer in med en signatur tillhörande en väljare som redan har röstat går det till som vanligt med några undantag. Istället för att markera att väljaren röstat markeras i listan vilket nummer på rösten det är (andra, tredje etc.) och en ny tidsstämpel läggs till. Alla tidpunkter lagras, även för de ersatta rösterna. Rösten adderas inte till de övriga i databasen med röster utan ersätter den tidigare rösten med matchande signatur.

Alla viktiga händelser som sker sparas i loggar för att kunna upptäcka om något går fel och annars för att i efterhand kunna bevisa att allt gått rätt till.

5.3 Efter valperioden

När valperioden för Internetröstningen är över stängs systemet så att inga fler röster kan läggas.

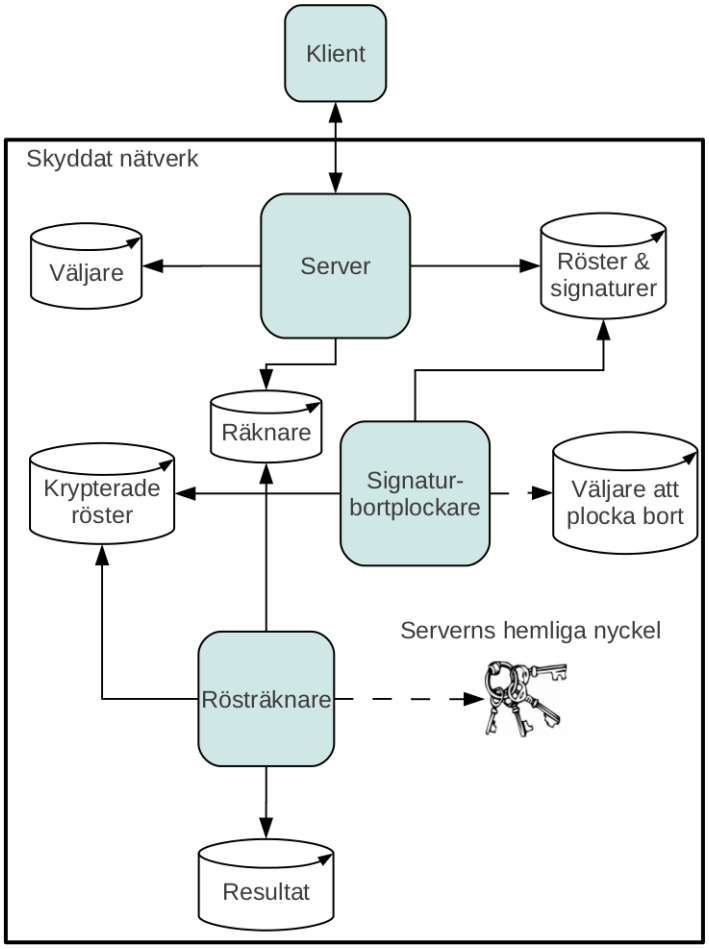
Efter att vallokalerna har stängt sammanställs listorna över vilka som röstat på valdagen och förtidsröstat på annat sätt än via Internet. Den sammanställda listan jämförs sedan med listan över väljare som röstat via Internet, de som röstat på fler sätt än via Internet får sin Internetröst bortplockad. Endast en röst sparas i denna prioritetsordning: röst på valdagen, förtidsröst i röstningslokal, brevröst, röst via Internet.

När alla röster plockats bort tas alla signaturer bort. Därefter samlas alla som ansvarar för delar av serverns hemliga nyckel. Tillsammans låser de upp rösterna. Därefter räknas rösterna och summan av de räknade rösterna jämförs med räknaren för att verifiera att ingen röst missats.

5.4 Modell

I Figur 5.1 visas en modell över hur systemet ser ut. De blå boxarna är processer och de vita cylindrarna är databaser. Pilarna visar vilka processer som har tillgång till vilka databaser.

De streckade linjerna visar de delar som kommer in i systemet efter valperiodens slut. Serverns hemliga nyckel är uppdelad och lagras separat från systemet. Listan över vilka röster som ska plockas bort sammanställs efter valet utifrån väljarlistan i detta system samt listorna över väljare som röstat på andra sätt.



Figur 5.1. Modell av systemet

Kapitel 6

Diskussion

I detta kapitel diskuteras de val som gjorts i designen samt vilka hot som finns mot systemet. Allt i uppsatsen är baserat på teoretiska undersökningar. Ingen implementation och därmed ej heller några tester av systemet är gjorda. Därför kan ingen garanti lämnas för att de tekniker som används är tillräckligt säkra. Sådana tester måste göras innan systemet kan tas i bruk.

6.1 Identifiering

För identifiering av väljarna används både BankID och hemskickade röstkort.

6.1.1 BankID

I Sverige finns inte samma standard på ID-kort som i Estland. De flesta ID-kort saknar chip som kan läsas av en dosa för användning som e-legitimation, endast Swedbank erbjuder idag sina kunder ID-kort som även kan användas som e-legitimation [27]. Alltså passar det inte att använda den lösning för identifiering som Estland använder om inte Sverige byter standard för ID-kort. Att använda sig av certifikat som i Genève är lättare. BankID används redan i stor utsträckning i Sverige och tekniken bygger på just certifikat. Att använda fysiska ID-kort med dosa bör vara något säkrare då det kräver tillgång både till det fysiska kortet och den tillhörande PIN-koden. För att stjäla någons identitet med BankID krävs visserligen tillgång till filen där certifikatet lagras samt den tillhörande PIN-koden. Att stjäla ett fysiskt ID-kort obemärkt är mycket svårare än att stjäla en fil, bland annat eftersom det går att göra en kopia på filen och lämna kvar originalet. På detta sätt vet du inte om att någon stulit din identitet och kan därför inte göra något åt det.

Att BankID redan används i stor utsträckning bör öka tilltron till systemet. Om allmänheten inte litade på BankID borde det inte användas i så stor utsträckning eftersom det finns andra lösningar att tillgå. Några exempel är

Nordeas dosor som används med deras konto- och kreditkort [28]. Även Telia har en variant av e-legitimation på kort [29].

Utöver BankID skulle även de andra varianterna av e-legitimation som används i Sverige idag kunna användas i detta system. Om fler varianter används så ökar tillgängligheten av systemet då alla kanske inte har tillgång till BankID, dock har inte denna uppsats undersökt fler varianter och därför är endast BankID med i designen.

6.1.2 Röstkort

För att förstärka säkerheten på identifieringen används, utöver certifikat, fysiska röstkort med unika röstkortsnummer. Dessa skickas ut till alla med rösträtt. På detta sätt ökas säkerheten genom användning av röstkortsnummret som ett fysiskt igenkänningstecken.

Inför valen i Sverige skickas redan röstkort ut till alla med rösträtt. Att ändra dessa kort så att de innehåller ett unikt nummer som kan användas för identifiering är inte svårt. Eftersom det redan skickas ut röstkort skulle detta inte innebära någon större ökning av utgiften för själva utskicken. Skickas röstkorten som rekommenderade brev, vilket innebär att mottagaren måste ha med giltig id-handling och hämta ut röstkortet hos ett av Postens utlämningsställen skulle det bli svårare att stjäla röstkorten. Dock skulle detta förmodligen medföra ökade avgifter och framför allt mer arbete då alla med rösträtt kommer behöva besöka ett av Postens utlämningsställen. Eftersom röstkortet i sig inte räcker till identifiering är denna extra säkerhet förmodligen inte nödvändig och utesluts därför i denna design.

6.2 Anonymitet, integritet och autenticitet

För att säkerställa att rösten är anonym, autentisk samt att dess integritet är skyddad krävs åtgärder i två steg. Dels i samband med att väljaren röstar och dels i lagringen av rösten.

6.2.1 Under röstningen

Innan rösten skickas krypteras den med symmetrisk kryptering. Detta gör att ingen som inte har nyckeln som delas av väljaren och servern inte kan se innehållet i rösten. Anslutningen sker över TLS för att förhindra avlyssning, rösten är alltså dubbelt krypterad när den skickas. Den dubbla krypteringen skyddar mot “man-in-the-middle-attacker” som TLS annars kan utsättas för [23]. Utöver detta måste väljaren signera rösten. Signaturen fungerar som garanti för röstens integritet och autenticitet.

6.2.2 Lagring

För att garantera anonymitet och autenticitet bör information om väljaren aldrig lagras tillsammans med väljarens röst. På detta sätt kan ingen som får tillgång till systemet koppla en röst till en väljare och därmed garanteras anonymitet och autenticitet vid lagringen. Om det ska gå att rösta flera gånger måste det dock lagras någonting som identifierar rösten för att den ska kunna tas bort när den nya rösten läggs. En röst på valdagen ersätter i dagens svenska system en eventuell förtidsröst. Om detta ska bibehållas krävs också någon form av koppling mellan väljare och röst. En kompromiss för detta skulle kunna vara att denna koppling sparas endast under valperioden men tas bort direkt efter valet. På detta sätt är det alltså endast möjligt att koppla ihop röst med väljare under valperioden.

Kopplingen lagras genom att låta den digitala signaturen med information om väljaren finnas kvar tillsammans med rösten. Rösten krypteras med serverns öppna nyckel och dekrypteras först efter att signaturerna plockats bort. Alltså kommer ingen kunna se vad någon röstat även om signaturen lagras tillsammans med rösten. Eftersom samma nyckel används vid krypteringen av alla röster kan det vara så att röster på samma alternativ (parti, kandidat etc.) ser likadana ut efter kryptering. För att undvika detta läggs en rad med slumpmässiga siffror till på slutet av varje röst innan kryptering. Dessa tas bort när rösten dekrypteras och läses aldrig. Dess enda syfte är att göra varje röst unik för att förhindra igenkänning av krypterade röster.

Eftersom endast servern har tillgång till sin öppna nyckel kan ingen utom systemet kryptera en röst och lagra den. Detta försvårar ytterligare för angripare som försöker lagra förfalskade röster.

6.3 Rösträkning

Först efter att röster från väljare som röstat på annat sätt än via Internet plockats bort och även alla signaturer på de återstående rösterna plockats bort kan rösträkningen börja. Internetrösterna räknas av systemet medan räkningen av röster lagda på annat sätt räknas på samma sätt som tidigare. Räknaren som används av systemet under valet garanterar att alla röster har räknats.

Eftersom ingen räkning görs förrän efter valperiodens slut garanteras att ingen kan ta reda på ställningen i valet under valets gång.

6.4 Tillförlitlighet

Om alla viktiga händelser loggas ordentligt så möjliggörs att i efterhand kunna kontrollera att ingenting gått fel och därmed bevisa systemets tillförlitlighet. Om till exempel en logg skapas när en röst kommer in i systemet samt en när rösten har lagrats kan det garanteras att alla röster som kommit till systemet verkligen

finns lagrade. Sätts ett system upp som sköter den här övervakningen automatiskt upptäckts direkt när någonting går fel och nödvändiga åtgärder kan vidtas.

6.5 Hot mot systemet

Det finns flera typer av hot mot ett system för val via Internet.

6.5.1 Hot mot valresultatet

Virus, trojaner och liknande kan finnas på väljarnas datorer. Denna typ av skadlig programvara skulle kunna hota resultatet av valet genom att modifiera väljarnas röster. Även anonymiteten hos väljarna kan hotas om någon med hjälp av den skadliga programvaran kan se vad du röstar på. I systemet finns flera skydd mot denna typ av attacker. Krypteringen med röstkortsnummrets hashvärde som delad nyckel är ett sådant skydd, den krypterade överföringen genom TLS ett annat. Utöver skydden i systemet får varje enskild väljare ta ansvar för att hålla sin dator fri från skadlig programvara.

I det tidigare svenska systemet fanns en svårighet i att köpa röster. Det var omöjligt för den som köpte rösten att veta vad säljaren verkligen röstade på. Med Internetröstning kan den som köper en röst sitta med vid röstningen och se på bekräftelsen vad säljaren faktiskt röstade på. Dock motverkas detta av att säljaren kan rösta på nytt och ersätta rösten senare.

6.5.2 Hot mot väljarna

Att med hot eller våld tvinga någon att rösta på ett specifikt alternativ blir också lättare med Internetröstning av samma anledning som försäljningen av röster. När valet kan ske var som helst finns inte längre det skydd som en vallokal ger vid röstningen. Det skydd som finns mot detta hot är återigen att väljaren kan ersätta sin röst med en ny. Alltså kan de som med hot eller våld tvingar någon att rösta ändå inte vara säker på att väljaren verkligen röstar som gärningsmannen vill.

6.5.3 Hot mot tillgängligheten

Attacker som syftar till att minska tillgängligheten av systemet motverkar systemets syfte, att öka tillgängligheten för väljarna. Dessa hot kan till exempel vara DoS-attacker eller utslagning av elnät. Hur systemet på bästa sätt skyddas mot dessa typer av attacker undersöks inte i denna uppsats.

6.6 Slutsats

Utifrån designen i uppsatsen är det möjligt att skapa ett system för val via Internet i Sverige. Med hjälp av BankID och ett röstkort med ett unikt nummer kan väljarna på ett säkert sätt legitimera sig. Både symmetrisk och asymmetrisk kryptering används på olika sätt för att skydda rösternas anonymitet, autenticitet och integritet. Dock måste systemets säkerhet och tillförlitlighet testas ordentligt innan det kan tas i bruk.

Införandet av ett system för val via Internet i Sverige skulle troligtvis ha en positiv effekt på valdeltagandet och därmed även på demokratin. Fortsatt forskning i området är därför högst önskvärd för att kunna förbättra demokratin med hjälp av ett säkert system för val via Internet i Sverige.

Del III

Referenser

Litteraturförteckning

[1] Computer Security DD2395: Cryptography [Föreläsningsanteckningar]. Stockholm: Sonja Buchegger; [citerad 2012 apr 5]. Tillgänglig på: http://www.csc.kth.se/utbildning/kth/kurser/DD2395/dasakh11/Slides/dasakh11Lecture02crypto20.pdf.

[2] Statistics about Internet Voting in Estonia [hemsida]. Tallinn: Vabariigi Valimiskomisjon; [citerad 2012 apr 2]. Tillgänglig på: http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics/.

[3] Internationell konvention om medborgerliga och politiska rättigheter [hemsida]. Stockholm: Regeringen; [citerad 2012 apr 3]. Tillgänglig på: http://www.manskligarattigheter.gov.se/dynamaster/file_archive/060505/fa60247e4d4729d44afe2354639cc316/Konventionen%20om%20medb%20och%20pol%20r%e4ttigheter.pdf.

[4] Stallings W, Brown L. Computer Security: Principles and Practice. 1:a uppl. New Jersey: Pearson; 2008. s. 49–56.

[5] Stallings W, Brown L. Computer Security: Principles and Practice. 1:a uppl. New Jersey: Pearson; 2008. s. 249–272.

[6] Stallings W, Brown L. Computer Security: Principles and Practice. 1:a uppl. New Jersey: Pearson; 2008. s. 42–61.

[7] Dataintegritet [hemsida]. Stockholm: Talentum Media AB; [citerad 2012 apr 12]. Tillgänglig på: http://www.nyteknik.se/uppslagsverk/dataintegritet.

[8] Stallings W, Brown L. Computer Security: Principles and Practice. 1:a uppl. New Jersey: Pearson; 2008. s. 291–294.

[9] Stallings W, Brown L. Computer Security: Principles and Practice. 1:a uppl. New Jersey: Pearson; 2008. s. 644–645.

[10] Val i Sverige [hemsida]. Stockholm: Valmyndigheten; 2011 [citerad 2012 feb 21]. Tillgänglig på: http://www.val.se/pdf/Val%20i%20Sverige_reviderad%202011.pdf.

[11] Stallings W, Brown L. Computer Security: Principles and Practice. 1:a uppl. New Jersey: Pearson; 2008. s. 216–219.

[12] Stallings W, Brown L. Computer Security: Principles and Practice. 1:a uppl. New Jersey: Pearson; 2008. s. 216–230.

[13] Teknik och administration i valförfarandet [Rapport]. Stockholm: Justitedepartementet; [citerad 2012 mar 5]. [s. 81-85]. Tillgänglig på: http://www.regeringen.se/content/1/c4/06/11/56f2c3e3.pdf.

[14] BankID är den lösning som används av flest [hemsida]. Stockholm: Finansiell ID-Teknik BID AB; [citerad 2012 feb 20]. Tillgänglig på: http://www.bankid.com/Documents/wwwbankidcom/Diagram%20nr%201.pdf.

[15] Frågor & Svar [hemsida]. Stockholm: Finansiell ID-Teknik BID AB; [citerad 2012 feb 20]. Tillgänglig på: http://support.bankid.com/sv/supportbankidcom/FragorSvar/.

[16] Swedbank och Skandia först av bankerna med Mobilt BankID [hemsida]. Stockholm: Finansiell ID-Teknik BID AB; [citerad 2012 feb 20]. Tillgänglig på: http://www.bankid.com/sv/Aktuellt/Swedbank-och-Skandia-forst-av-bankerna-med-Mobilt-BankID/.

[17] Stallings W, Brown L. Computer Security: Principles and Practice. 1:a uppl. New Jersey: Pearson; 2008. s. 61–64.

[18] Stallings W, Brown L. Computer Security: Principles and Practice. 1:a uppl. New Jersey: Pearson; 2008. s. 680–683.

[19] Stallings W, Brown L. Computer Security: Principles and Practice. 1:a uppl. New Jersey: Pearson; 2008. s. 652–656.

[20] SSL/TLS in Detail [hemsida]. USA: Microsoft; [citerad 2012 apr 5]. Tillgänglig på: http://technet.microsoft.com/en-us/library/cc785811(v=ws.10).aspx.

[21] Online voting: challenges and outcomes [hemsida]. Geneve: Republique et canton de Geneve; [citerad 2012 mar 6]. Tillgänglig på: http://www.ge.ch/evoting/english/presentation_projet.asp.

[22] Welcome to the state of Geneva web site [hemsida]. Geneve: Republique et canton de Geneve; [citerad 2012 mar 6]. Tillgänglig på: http://www.ge.ch/evoting/english/welcome.asp.

[23] Uncovering the veil on Geneva's internet voting solution [hemsida]. Geneve: Republique et canton de Geneve; [citerad 2012 mar 12]. Tillgänglig på: http://www.ge.ch/evoting/english/doc/Flash_IT_vote_electronique_SIDP_final_english.pdf.

[24] Internet Voting in Estonia [hemsida]. Tallinn: Vabariigi Valimiskomisjon; [citerad 2012 mar 6]. Tillgänglig på: http://www.vvk.ee/voting-methods-in-estonia/engindex.

[25] E-Voting System: General Overview [hemsida]. Tallinn: Vabariigi Valimiskomisjon; [citerad 2012 mar 12]. Tillgänglig på: http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf.

[26] What impact does internet voting have on turnout? [hemsida]. Geneve: Republique et canton de Geneve; [citerad 2012 apr 3]. Tillgänglig på: http://www.ge.ch/evoting/english/faq-internet-voting.asp.

[27] ID-kort [hemsida]. Stockholm: Swedbank AB; [citerad 2012 apr 6]. Tillgänglig på: http://www.swedbank.se/privat/kort-och-betalningar/id-kort-och-bankid/id-kort/index.htm.

[28] E-legitimation [hemsida]. Stockholm: Nordea; [citerad 2012 apr 6]. Tillgänglig på: http://www.nordea.se/Privat/Internet%2boch%2btelefon/e-legitimation/207904.html.

[29] Telia e-legitimation [hemsida]. Stockholm: Telia; [citerad 2012 apr 6]. Tillgänglig på: http://www.telia.se/privat/katalog/VisaProdukt.do?channelId=-76442&tabId=0&OID=1537014385&type=PRODUCT.