Internettvalgstyrets Representanter
Internetpilot 2013

Endelig verifikasjonsrapport fra beskyttelse av krypteringsnøkler, trykking av valgkort, bevisførsel og øvrig beskyttelse av hemmeligheter

Kåre Vollan, Promis AS og Quality AS
4. november 2013
Versjon 1-1

1. Innledning

Kommunal- og regionaldepartementet (KRD) utnevnte Internettvalgstyret (IVS) i juli 2013 for å overvåke forsøkene med internett-stemmegivning ved stortingsvalget i 2013. IVS valgte Promis AS som sin representant for å verifisere prosessene på deres vegne. Promis satte videre ansvaret til Quality AS med deres representant Kåre Vollan som teamleder. Frem til 6. august var Anne Kristine Næss fra Promis AS nestleder i teamet. En verifikasjonsplan med metodebeskrivelser ble utarbeidet før prosessene startet. Dessuten ble verifikasjon av bevisføring under opptellingsprosessene satt bort til Computas AS som utarbeidet programmer med matematisk verifikasjon.

Denne rapporten gjengir de gjennomførte aktiviteter og resultatene av disse. Den inneholder dessuten forslag til forbedringer for eventuelle senere internettvalg, selv om dette ikke var en uttrykt del av mandatet.

Det bør bemerkes at vår verifikasjon var begrenset til det å beskytte hemmeligheter og bevisførsel av definerte skritt slik dette er definert nedenfor, og omfattet ikke andre kvalitetsaspekter eller andre skritt i prosessen.

2. Prosessene

IVS og deres sekretariat som består av E-Valg 2013 gruppen i KRD, spesifiserte i tilbudsinvitasjonen at IVS skulle sikre at hemmeligholdet av valget ikke skulle brytes. Det innebar at en viss informasjon måtte holdes hemmelig til enhver tid. De tre områdene som ble identifisert som IVS-representantens områder er angitt FOR 2013-06-19 nr. 669: Forskrift om forsøk med internettstemmegivning under forhåndsstemmegivningen og elektronisk avkryssing i manntallet på valgtinget ved stortingsvalget i 2013 i utvalgte kommuner, §10, 1, a, b og e. Områdene var:

> «(1) Internettvalgstyret skal:
>
> a) sørge for at informasjon om hva returkodene betyr, destrueres etter trykking, jf. § 7 (4)
>
> b) sørge for at kryptografiske nøkler behandles forsvarlig, jf. § 8 (3)
>
> […]
>
> e) sørge for verifisering av systemet fra uavhengig tredjepart, jf. § 29.»

§ 7 omhandler Valgkort og returkoder og sier i avsnitt 4:

> «(4) Etter trykking skal internettvalgstyret sørge for at informasjon i i-valgsystemet om hvilken returkode som tilhører hvilken valgliste, slettes på en betryggende måte. For å

ivareta denne oppgaven kan internettvalgstyret leie inn en it-revisor som kontrollerer at trykking av returkoder på valgkortene er utført i samsvar med regelverket. It-revisor skal rapportere til internettvalgstyret.»

§ 8 om Forberedelse til internettvalg sier i avsnitt (3):

«(3) Internettvalgstyret skal sørge for at kryptografiske nøkler, som skal ivareta stemmens hemmelighold, genereres og oppbevares på en betryggende måte. De skal også sørge for at de kryptografiske nøklene samt all kryptert informasjon destrueres på betryggende måte etter valget. Internettvalgstyret kan leie inn it-revisor som på deres vegne kontrollerer at prosessen gjennomføres på en forsvarlig måte. It-revisor skal rapportere til internettvalgstyret.»

§ 29 refererer til verifisering av matematiske bevis under opptellingsprosessen:

«(1) I-valgsystemet skal generere matematiske beviser for at stemmelagring og opptelling gjøres korrekt. Bevisene skal gjøres tilgjengelig for tredjeparter for verifisering.

(2) Internettvalgstyret skal sørge for at de matematiske bevisene for korrekthet og integritet som genereres av opptellingsprosessen blir kontrollert og verifisert av uavhengig tredjepart.

(3) Internettvalgstyret tar stilling til søknader fra partier eller grupper som stiller liste ved valget som på selvstendig grunnlag ønsker å gjennomføre nevnte verifisering. Den som har gjennomført slik verifisering skal dokumentere og oversende resultatet til internettvalgstyret.»

Vi har som IVS-representanter ivaretatt rollen som It-revisor i de to første oppgavene og som uavhengig tredjepart under det siste punktet.

Særlig to egenskaper karakteriserer den norske E-valgløsningen: i) muligheten for velgeren til å stemme så mange ganger hun vil på internett og på papir på valgdagen, og ii) Utsendelse av returkoder som gir velgeren en mulighet for å sjekke at stemmen er korrekt registrert i systemet. Det første punktet gjør at de digitale stemmene må være koblet til stemmegiveren frem til opptelling. Under tellingen må denne koblingen brytes slik at det er umulig å spore stemmen tilbake til personen som har avgitt den, og punkt ii) gir en teoretisk mulighet for å avsløre hva en velger har stemt dersom man 1) har tilgang til de trykte returkodene, altså velgerens valgkort og 2) overvåker SMS-ene som sendes ut etter stemmegivning. Særlig punkt ii) gjør løsningen ganske komplisert.

Den teoretiske muligheten for at hemmeligholdet kunne bli brutt, gjorde det spesielt viktig for IVS å ha tillit til at de kryptografiske nøklene nødvendige for å avdekke hemmelighetene, ble tatt vare på en sikker måte, og at trykkeprosessen ikke ville gjøre informasjon som kombinerte velger og returkoder tilgjengelig for uvedkommende. Stemmen ville ikke kunne endres selv om hemmelighetene kommer på avveie; det er kun hemmeligholdet som eventuelt vil settes i fare. I tillegg ville returkodene kunne bli manipulert slik at de ikke ville kunne benyttes til å verifisere stemmene eller andre deler av prosessene kunne ødelegges.

Det må understrekes at uautorisert bruk av hemmelighetene normalt ville være høyst teoretisk siden de krevde usannsynlige konspirasjoner og mye teknisk kunnskap. Den feilen som

oppsto i krypteringen og som omtales nedenfor, falt utenfor dette skjemaet og ble derfor håndtert særskilt.

Lekkasjer kunne komme av:

i) Uplanlagt deling av informasjon hvor slik informasjon kommer i urette hender;
ii) Bevisste angrep utenfra med sikte på å få eller ødelegge informasjon;
iii) Bevisste angrep innenfra med tanke på å misbruke eller ødelegge informasjon.

Det siste punktet er sannsynligvis det minst sannsynlige, men det er også det som er vanskeligst å beskytte seg mot. Det var ikke mulig å sikre seg mot dette hundre prosent, men rimelige tiltak ble tatt for å sikre at prosessene ble kontrollerbare og vel strukturerte slik at kun svært avanserte og intrikate forsøk ville forbli uavslørt.

3. Sikring av de kryptografiske nøkler

Den kryptografiske nøkkelen som var nødvendig for å få tilgang til returkodene, var sammensatt av to deler:

K(IVS) = K (RCG) + K(VCS),

der RCG står for «Return Code Generator», VCS for «Vote Collector Server» og IVS for Internettvalgstyret. VCS og RCG nøklene må være tilstede i systemet under valget, og IVS-nøkkelen benyttes ved dekryptering av stemmene på valgnatten. Kunnskapen om hvordan man beregner K(IVS) er distribuert ved en såkalt «Shamir secret sharing-algoritme» til smartkort som ble gitt til hver av de ni IVS-medlemmene. Seks av de ni kunne åpne den nødvendige informasjonen ved opptellingen.

K(VCS) og K(RCG) ble generert henholdsvis 1.1 og 12. juli på to ulike og såkalte air-gapped servere (kalt VCS-representant og RCG-representant). (Se dokumentet fra Scytl «KRD eValg2011 platform, Update for 2013 Parliamentary elections, Election Configuration», versjon 1.0 avsnitt 8.1 and 8.2 (eller «eValg2011 platform Bootstrap Process» versjon 2 avsnittene 3.17 og 3.18).) Prosessen for generering av returkoder var slik:

Først ble et kryptert filsystem (LUKS Linux Unified Key Setup) installert på to par minnepinner, med passord generert og passet på av oss (IVS-representantene). Ett par (en hovedpinne og en reserve) ble brukt på VCS-representantserverne og ett par på RCG-representanten. LUKS-krypteringen av minnepinnene ble utført på en PC merket KMS (Key Management system).

Så ble returkodene generert i to skritt i server-rommet i R5s åttende etasje. Rommet inneholdt et serverstativ med ti servere, der fire maskiner er VCS-representanter, fem er RCG-representanter og én reserveserver. Det samme serverstativet ble benyttet i forbindelse med tellingen, men da med andre disker.

Det første skrittet ble utført 11. juli hvor de partielle returkodene ble generert for velgere i hver av de deltagende kommunene og med de tilhørende partiene. Først ble VCS-hemmelighetene generert (K(VCS)) og kopiert til det ene LUKS-krypterte minnepinneparet. En av disse minnepinnene ble brukt til å distribuere innholdet til VCS-representantserverne og anvendt når de partielle returkodene på VCS-representantene ble generert for hver kommune, mens den andre var holdt i reserve. Sistnevnte hemmelighet var beskyttet av et

passord som ble satt av oss. Etter dette skulle master-passordet ikke benyttes. De fire serverne ble styrt fra en PC merket CLEANSING. Den krypterte VCS-hovedminnepinnen ble bare anvendt på den PCen.

På slutten av første dag ble de partielle returkodene kopiert, først til en disk (merket bb366c70) ved en USB inngang og deretter til RCG-representantene ved hjelp av en PC merket MIXING. Hovedminnepinnen for RCG-representanten ble bare anvendt på den PCen.

For fremtiden kan det vurderes om de to PCene (CLEANSING og MIXING) burde være under IVS-representantens kontroll.

To personer fra IVS-representanten fulgte prosessen. Disse to, med én ekstra reserveperson, visste hvordan passordene for minnebrikkene var sammensatt. Prosessen var godt organisert, og vi hadde ingen kommentarer til hvordan den ble gjennomført. Noen småproblemer (i forbindelse med installering av LUKS-krypterte filsystem på minnepinnene) ved bruk av PCen merket KMS, ble løst under full kontroll.

12. juli ble de fulle returkodene produsert på RCG-representantene. Tilsvarende som for VCS, ble først RCG-hemmelighetene generert. I denne prosessen ble en av hemmelighetene kryptert med et passord som vi satte, og den andre (K(RCG)) ble kopiert til det andre LUKS-krypterte minnepinneparet. Førstnevnte hemmelighet ble kopiert til alle RCG-representant-serverne og ble brukt i forbindelse med generering av de fullstendige returkodene. Så ble returkodene generert kommunevis ved bruk av det samme passordet.

Opprinnelig var planen at diskene på VCS og RCG representantene skulle bli slettet ved overskriving når trykking av returkortene var utført, men noen filer ble overskrevet allerede 12. juli, se nedenfor.

Ved slutten av prosessen ble de fire minnebrikkene som var beskyttet med passord bare vi kjente, og som inneholdt hemmelighetene (K(VCS og K (RCG)) nedlåst. De som var merket 22619fc9 og 99e456f4 ble låst ned i en safe i R5, og reservepinnene merket 2d970590 og 3f8af8cb ble låst ned i serverrommet i R6. Vi overvar ikke selve innlåsingen, men vi hadde kontroll med passordene som skulle til for å få tilgang til data på pinnene. Pinnene skulle anvendes en gang i perioden 6. til 9. i forbindelse med endelig konfigurering av valget. Da ville returkodene samt K(VCS) og K(RCG) bli overført til de faktiske serverne i bruk under valget. VCS-serverne stod i datarommet i R6 under kontroll av KRD og RCG ved Direktoratet for samfunnssikkerhet i Tønsberg. Den opprinnelige planen var å kryptere VCS-hemmelighetene med en nøkkel generert og oppbevart i en såkalt Hardware Security Module (HSM).. Disse ble imidlertid erstattet av noen noe svakere krypteringsløsning produsert av Scytl. Det samme var tilfelle for RCG-serverne. For å få tilgang til alle disse serverne, måtte man ha passord som ble lagret på krypterte minnepinner som hvert av de tre medlemmene av KRDs kjerneteam hadde ansvaret for.

To personer fra IVS-representanten var til stede 12. juli opp til dette punkt. Én fortsatte observasjonen til alt var ferdig (Vollan). Etter å ha forlatt bygningen, ble han kalt tilbake av KRD fordi man hadde funnet en teoretisk mulighet for at returkoder kunne bli laget på nytt fra de samme data som fremdeles fantes på diskene. Da han var tilbake i KRD ble ulike muligheter diskutert, og Scytl ble konsultert. Resultatet var at de viktige kildefilene ble slettet og overskrevet fra diskene, etter at filer ved navn som inneholdt “ballotIDS” og “final-votingcards” var blitt sikkerhetskopiert over på en kryptert disk merket 56baa247. Disken

kunne bare åpnes ved passord generert og tatt vare på av oss. Filene ble slettet også fra den portable disken merket bb366c70, og disken merket 56baa247 ble låst ned i en safe.

Det er meget beklagelig at et «hull» i prosessen for generering av returkoder ble avdekket og at dette ikke var blitt avslørt tidligere. Når det er sagt må det understrekes at det på grunn av datamengdene er svært usannsynlig at data kunne kompromitteres i løpet av den timen vi var ute av huset, og den løsningen som ble funnet, var god og prosessen med å tette «hullet» var helt åpen og kontrollerbar.

En plan for destruksjon av data ble fremlagt etter dette. Der fremgår det at de gjenværende data på VCS og RCG representantene og på den portable disken som inneholder sensitive data, ville bli slettet først etter at valget var over for å sikre en mulighet for å gjenskape data. Siden vi hadde passordene nødvendige for å få tilgang til disse data, hadde vi ingen innvendinger mot denne planen.

11. august overvar vi etableringen av en testvelger. Testvelgeren er en ”fiktiv” stemme som sendes gjennom e-valgsystemet før valget har startet, uten at den blir lagret på stemmeserverne. Denne benyttes til å verifisere at sertifikatene og krypteringsnøklene er generert på korrekt måte, uten at noen teststemme blir lagret i databasen. Ved en feil hadde en tidligere testvelger fått VCS og RCG-bidrag fra ulike kommuner, og denne kunne dermed ikke brukes. Vi åpnet de nødvendige filer med det passordet vi tidligere hadde etablert, og vi så at testene ved bruk av testvelgeren var vellykkede.

4. Sikring av returkodene under og like etter trykking av returkort

4.1 Den planlagte prosessen

Oppgaven ble beskrevet i mandatet som å forsikre at returkodene ble slettet etter trykking. Vi tolket dette, i forståelse med IVS, til å omfatte det å sikre at alt som kunne avsløre sammenhengen mellom velger og returkoder ble holdt hemmelig i løpet av selve trykkeprosessen også.

I løpet av trykkeprosessen var returkodene i ukryptert form tilgjengelig, og prosessen var derfor følsom. Informasjonen var imidlertid ikke synlig i trykkeriet. Informasjonen var lagret på en fulldiskkryptert PC som bare vi hadde passordet til. PCen inneholdt to filer per kommune som begge var nødvendige for trykkingen: én med velgerens navn og én med returkodene. Disse var kryptert med trykkeriets offentlige nøkkel og kunne åpnes med en privat nøkkel som trykkeriet hadde. PCen dekrypterte informasjonen og sammenføyet navn og returkode i klartekst slik at kortene kunne trykkes. Ingen informasjon ble lagret på printerens interne disker. Prosessen var automatisert og foregikk uten menneskelig innblanding.

Valgkortene skulle trykkes på en maskin fra firmaet Canon. Kortene skulle trykkes på begge sider og så bli sendt i et lukket system til en enhet som skulle folde og lime kortene. Etter foldingen ville kortene på de synlige sidene inneholde åpen informasjon om velgerens navn, adresse, osv. mens innsiden ville inneholde returkodene. Hver for seg var innside og utside ikke sensitive, men sammen utgjorde de følsom informasjon som måtte beskyttes. Så lenge prosessen virket som planlagt, ville de to sidene ikke kunne leses samtidig av dem involvert i prosessen.

De kritiske områdene var:

i) PCen inneholdt følsom informasjon som den mottok på minnepinner. PCen ble hold innelåst i en safe som KRD hadde koden til. Vi var de eneste som kunne starte PCen med passord.

i) Den fysiske koblingen mellom PCen og trykkemaskinen gikk via en kontroller merket «Version V2 ++ HE». Vi sjekket at denne var intakt til enhver tid.

ii) Ved foldeheten kunne man få et glimt av returkortet før det ble foldet, riktignok i en brøkdel av et sekund. Vi måtte passe på at det ikke ble satt opp opptaksutstyr som kunne overvåke dette.

iii) Det at trykkemaskinen var satt opp slik at det ikke ble skrevet data til de interne diskene, måtte sjekkes mot spesifikasjonene, «Statement of Volatility». Vi mottok dessuten en protokoll fra Canon-representanten som bekreftet dette. Dette gjorde at vi ikke anbefalte at de interne diskene ble fysisk destruert etter trykkingen.

iv) Hvis papir satte seg fast eller ved andre trykkeproblemer, måtte ufoldede kort tas ut, og trykking måtte gjentas. Alternativt kunne enkeltkort måtte trykkes på nytt. I denne prosessen ville begge sider av kortet kunne besiktiges. Vi var til stede for å bevitne at slike kort ble håndtert på en måte at bare én side var synlig for operatøren når de ble foldet og limt i en separat prosess eller destruert i makuleringsmaskinen.

v) Ved feil i trykkeprosessen var altså ofte kort åpne. Dette ble brukt som en mulighet til å gjøre stikkprøver av at partiene med returkodene var i overensstemmelse med partilisten for kommunen. Selv om dette var utenfor vårt mandat, utførte vi slike stikkprøver ved at operatøren holdt opp et kort med navn og adresse synlig for seg og returkodene synlige for oss.

vi) Etter at trykkingen var ferdig, ble disken på PCen slettet og overskrevet i vårt nærvær, samt at minnepinnen med trykkedata ble makulert.

Trykkerimaskinen skulle ha en kapasitet på nær hundre kort per minutt.

IVS-representanten engasjerte et antall studenter som var til stede til enhver tid under trykkeprosessen, så lenge PCen var åpen. To sjekklister ble utarbeidet – en for åpningen første dag og en for den daglige verifiseringen, se vedlegg. Studentene fikk opplæring i prosessen og i bruk av sjekklistene. Funnene nedenfor er basert på de utfylte sjekklistene og observasjoner forøvrig.

4.2 Funnene

På første dag i trykkeriet dukket det opp en rekke problemer. Først ble en del enkeltkort forkastet før de ble limt sammen, senere ble hele bunker kjørt feil, og ved slutten av dagen var et ikke mulig å trykke noe feilfritt. Bare 8.000 kort ble trykket, mot en kapasitet på 20 til 40.000, og en hel del av disse ble ikke foldet og limt. Det ble diskutert en rekke forslag til forbedring av prosessen, og en egen separat folde- og limemaskin ble bestilt.

På sluttet av dagen var det altså bunker med åpne kort. Disse representerte en risiko. En rutine ble innført der slike kort ble lagt i klart merkede esker med den gule innsiden ned slik at operatørene bare kunne se adressesiden. Den første dagen ble disse eskene låst inn i et lagerrom med kodelås. Rommet ble bare anvendt av dette prosjektet, og det ble bevoktet av vektere fra et sikkerhetsfirma. Vi bevitnet både lukking av rommet og åpning neste dag. I resten av trykkeprosessen ble dette ikke nødvendig da det var kommet inn separate foldemaskiner, og man gjorde det til at poeng ikke å lagre åpne kort over natten.

Ved åpningen annen dag, overvar vi ikke at PCen ble tatt ut av safen på grunn av en misforståelse. Dette tok imidlertid bare noen minutter og kan ikke karakteriseres som en reell risiko, ettersom disken var kryptert med passord satt av oss.

Om morgenen den andre trykkedagen ble reservedeler til foldeenheten fløyet inn, og den opprinnelige konfigurasjonen virket etter det bedre. En separat foldemaskin ble brukt på de kortene som ble trykket, men ikke foldet i hovedmaskinen. Den separate foldemaskinen måtte ha innsiden synlig under bruk, men operatørene kunne fremdeles ikke se to sider av samme kort.

På dag tre kom det inn en foldemaskin til, og denne hadde meget høy kapasitet.

På dag fire ble klartekstfilene med trykkeinformasjonen flyttet fra en minnebrikke hvor de ble lagt etter å ha blitt generert, til disken på PCen siden den var passordbeskyttet. Minnepinnen hadde ligget i safen hver natt, noe vi hadde bevitnet. Risikoen for misbruk var svært lav, men prosessen skulle klart ha vært at filene bare ble lagt på PCens interndisk fra starten av.

På dag åtte (31. juli) gikk man tom for papir, og trykkingen var ikke gjenopptatt 5. august da vi ferdigstilte vår foreløpige rapport til IVS. Da gjenstod det ca. 70.000 kort som ikke var trykket. Trykkingen ble gjenopptatt og ferdigstilt 6. august.

Stikkprøvene som ble gjort av innholdet i de to sidene (se 4.1 v)) hadde alle riktige partier for den kommunen det gjaldt.

Det ble ikke observert brudd på sikkerhetsreglene utover det som er beskrevet over. PCen og minnebrikken som ble brukt under trykkingen, ble tatt ut av safen under vårt nærvær 11. august, disken ble slettet og overskredet, og minnebrikken fysisk ødelagt i en miksemaskin.

5. Produksjon av smartkort til de ni IVS-medlemmene

6. august hadde IVS møte, og to smartkort ble generert for hvert av de ni medlemmene. Kunnskapen for utregning av dekrypteringsnøkkelen, som brukes for å åpne de elektroniske stemmene, ble lagret på tilsammen atten smartkort. Ni av disse inneholdt informasjon fra VCS og ni fra RCG. Hvert av IVS-medlemmene hadde ett kort med kunnskap fra VCS og ett fra RCG. Informasjonen var lagret på en slik måte at for å gjennomføre dekrypteringen, måtte minst seks av IVS-medlemmene komme sammen med sine smartkort

Vår representant fulgte denne prosessen og skrev inn passordene vi hadde generert og passet på, for å åpne de to minnepinnene som inneholdt VCS-hemmelighetene og de to som inneholdt RCG-hemmelighetene. Derved ble de ni settene av to smartkort generert. Etter dette ble minnepinnene tatt ut (unmounted) av maskinen, og disse kunne ikke bli brukt igjen uten de passordene bare vi hadde.

I dette møtet ble dessuten vår foreløpige rapport fremlagt.

6. Verifikasjon av matematiske bevis under opptelling

Samsvar av krypterte stemmer og kvitteringer mellom RCG, VCS og GitHub

Det ble utviklet en egen komponent for å utføre en kryssjekk mellom de krypterte stemmene og kvitteringene fra RCG på den ene siden, og de krypterte stemmene og kvitteringene fra VCS på den andre siden. I tillegg kunne kvitteringene fra både RCG og VCS også

kryssjekkes mot kvitteringene lastet ned fra GitHub - det eksterne bullentin board (oppslagstavle).

Dette beviset sikrer at KRD ikke kan la være å registrere stemmer som velgerne har fått kvittering på, eller endre dem. Det sikrer også at KRD ikke kan legge til stemmer uten at en velger får beskjed om det, siden RCG da ville sendt ut en returkode til vedkommende.
På grunn av krypteringsproblemene (se nedenfor) ble det besluttet å holde RCG avslått, og dermed ble kvitteringene og de krypterte stemmene fra VCS ikke sammenlignet med RCG. Siden de krypterte stemmene på VCS også inneholdt en signatur fra RCG, ville det fremdeles vært umulig for KRD å legge til ekstra stemmer uten at RCG eller verifikasjonsteamet hadde fått vite om dem, for da ville den krypterte stemmen ikke vært signert eller signert riktig av RCG.
Verifikasjonsteamet mener at det var tilstrekkelig at settet med kvitteringer fra VCS kunne kryssjekkes mot settet med krypterte stemmer fra VCS, og at settet med kvitteringer fra VCS kunne kryssjekkes med kvitteringene som ble publisert på GitHub. Ingen avvik ble funnet.

Klargjøring (cleansing)
Opprinnelig plan var å føre bevis over at ingen nye stemmer ble lagt til av KRD under klargjøringsprosessen. På grunn av at ca. 29.000 stemmer hadde fått samme ElGamal-hemmelighet under krypteringen var det vanskelig å lage et vanntett bevis for dette på så kort varsel. Det ble derfor besluttet å kjøre en parallell klargjøringsprosess basert på samme maskinvare, software-stack og kildekode som KRD brukte under valgnatten.

Kildekodegjennomgangen var basert på en kopi av kildekoden lastet ned en stund før krypteringsproblemet ble oppdaget, i tillegg til de publiserte forskjellene mellom nedlastet versjon og versjonen brukt under valgnatten. Det ble ikke oppdaget funksjonalitet i kildekoden som skulle tilsi at integriteten av valget ble brutt under klargjøringsprosessen. Kildekoden ble kompilert uavhengig av KRDs produksjonskode, men med hjelp av en av deres sommerstudenter som hadde gjort dette før. Kompileringen var ikke triviell på grunn av en del avhengigheter til noen biblioteker.

Maskinvaren som ble anvendt under bevisførselen, var en reserveserver for klargjøring som KRD hadde stående tilgjengelig. Disken ble slettet, og all programvare ble installert fra bunnen av. Software-komponenter ble innhentet fra KRD, men noen kontrollsummer ble produsert for etterkontroll:

- Operativsystemet Centos 5.9 ble installert fra en original kopi med riktig kontrollsum.
- Java (JDK 1.6) ble installert fra en kopi med riktig kontrollsum.
- Database PostgreSQL 9.2.4 ble installert fra en original kopi, men uten at det var en kontrollsum tilgjengelig.

For andre, mindre pakker ble kontrollsummene ikke kontrollert. Selve kjøringen av klargjøringsprosessen ble utført ved hjelp av samme script som KRD brukte for sin klargjøringsprosess.

Under foreløpig telling viste resultatene et avvik på fem stemmer, men dette avviket kunne forklares gjennom en bug-fix som hadde blitt utført fra versjon 3.2.5 (som verifikasjonsteamet hadde kompilert) til versjon 3.2.8 (som er siste versjon og brukt av KRD). Endelig opptelling ble kjørt på samme måte som foreløpig opptelling, men i seks runder:

1. Hammerfest og Radøy: ingen avvik

2. Bremanger, Mandal, Larvik, Re, Tynset og Vefsn: 2 avvik
3. Ålesund: 1 avvik
4. Bodø: ingen avvik
5. Fredrikstad: 2 avvik
6. Sandnes: ingen avvik

Avvikene som ble avdekket under endelig opptelling, var de samme fem som ble funnet under den foreløpige tellingen.

Mixing (Verificatum)
Det ble utviklet en egen komponent (av Léo Perrin) for å utføre denne delen av verifikasjonen. Programmet sjekker det kryptografiske beviset for at mixingprosessen byttet rekkefølgen på stemmene i valgurnen på riktig måte, og at stemmene ble re-kryptert på riktig måte.
På samme måte som for klargjøring ble mixingen kjørt i 6 runder:

1. Hammerfest og Radøy
2. Bremanger, Mandal, Larvik, Re, Tynset og Vefsn
3. Ålesund
4. Bodø
5. Fredrikstad
6. Sandnes

Ingen avvik ble funnet.

Mixing (Scytl)
Det ble utviklet en egen komponent for å utføre denne delen av verifikasjonen. Programmet sjekker det kryptografiske beviset for at mixingprosessen rekrypterte stemmene på riktig måte, og at ingen stemmer ble fjernet, lagt til eller endret under prosessen. Under valgnatten besluttet KRD og verifikasjonsteamet i samråd at det ikke skulle kjøres en parallell mixingprosess basert på Scytls egen protokoll, og derfor var det heller ikke behov for å kjøre dette beviset.

Dekryptering
Det ble utviklet en egen komponent for å utføre denne delen av verifikasjonen. Komponenten sjekket, for hver eneste dekrypterte stemme, et bevis basert på en Schnorr-signatur, og dette beviset beviste at den krypterte stemmen ble dekryptert med IVS' hemmelige nøkkel. Siden det var et lite avvik i strukturen på krypterte stemmer avhengig av om Verificatum ble brukt som mixing eller Scytls egen mixingprotokoll, måtte denne komponenten kunne håndtere begge tilfeller.

Også kryptering ble kjørt i 6 runder:

1. Hammerfest og Radøy
2. Bremanger, Mandal, Larvik, Re, Tynset og Vefsn
3. Ålesund
4. Bodø
5. Fredrikstad
6. Sandnes

Ingen avvik ble funnet.

7. Håndtering av data etter at krypteringsfeilen ble oppdaget

Under arbeid med bevisene, oppdaget vi en betydelig feil i krypteringen. Etter at feilen ble oppdaget 3. september og korrigert 4. september, ble behovet for strengere sikkerhet rundt de databasene som teoretisk kunne avsløre hva velgere hadde stemt, større.

I IVS-møtet 10. september ble det bestemt at IVS-representantene skulle delta i den fysiske beskyttelsen av alle følsomme data. Samme dag ble noen disker fra VCS-serverne tatt ut fra serverrommet i R5 og R6 og lagt i et låsbart skap som bare vi hadde nøkkel til, og dette skapet ble lagt i KRDs safe for strengt hemmelig materiale, som bare få betrodde kan åpne.

RCG-serverne i Tønsberg med backup i Ås var satt i låsbare skap som bare kunne åpnes med to nøkler samtidig. 12. September ble vi gitt det ene nøkkelsettet til disse.

VCS-serverne sto i det mest beskyttede serverrommet i R6, og det ble ansett som tilstrekkelig beskyttet.

Den 17. september 2013, etter at den første klagefristen på syv dager etter valgdagen var utløpt, ble disker som inneholdt tilstrekkelige data til å gjøre en ny opptelling tatt vare på, og resten av diskene ble overskrevet. Fra VCS-serverne i R6 ble åtte disker med data tatt vare på, og resten av diskene med data ble overskrevet. De åtte diskene ble lagt i boksen vi hadde nøkler til og som var oppbevart i safen for følsomt material i R5.

Ved RCG-serverne hos DSB i Tønsberg ble fire disker med data tatt ut, og resten av dem med sensitive avstemningsdata ble overskrevet. Overskrevet ble også diskene ved reserveløsningen i Ås. De fire diskene fra Tønsberg ble lagt i den låste boksen i safen i R5.

22. oktober ble den låste boksen hentet ut fra safen i R5, åpnet av oss, og en instans av VCS-databasen og en av RCG-databasen, til sammen seks disker, ble slettet og overskrevet i vårt nærvær. I tillegg ble fjorten disker som inneholdt operativsystemer slettet. Derved var all den informasjon som kunne kompromittere hemmeligholdet av valget slettet.

8. Stikkprøvebasert overvåkning av prosessene

VCS- og RCG-serverne var hver for seg tilgjengelige for to personer. Én fra kjerneteamet og én fra hver av de to servergruppene kunne teoretisk danne en konspirasjon for å åpne hemmelighetene, men da med store vanskeligheter. Det ble generert logger over hvem som var inne på maskinene og når, og fra 11. august hadde vi tilgang til disse loggene fra våre egne arbeidsplasser.

Kvitteringene på GitHub

Som en del av protokollen ble det for hver stemme som ble registrert lagt ut en kvittering på et ekstern «bulletin board». Til dette formålet ble det brukt et repository i GitHub, noe som gjorde det lett å laste ned filen med kvitteringene og verifisere dem. Det ble laget et lite script som automatisk lastet ned hele repositoryet og verifiserte innholdet i det. Denne verifiseringen besto av følgende deler:

- Kontroll av at signaturen var i samsvar med et sertifikat KRD hadde publisert på websidene sine
- Sjekk av kvitteringene ved forrige nedlasting for å verifisere at ingen kvitteringer ble fjernet underveis.

Scriptet ble installert på en datamaskin og satt opp til å bli kjørt én gang i timen. Det ble ikke funnet noen avvik i løpet av valgperioden. Den nedlastede filen ble også brukt i det matematiske beviset som verifiserte samsvar mellom krypterte stemmer og kvitteringer mellom RCG, VCS og GitHub.

Serveraktivitet (Splunk)
KRD tilgjengeliggjorde noen loggfiler fra RCG og VCS gjennom logganalyseverktøyet Splunk. På den måten var det mulig å overvåke hva som skjedde på serversiden og oppdage eventuelle avvik. Verifikasjonsteamet brukte verktøyet til å sjekke fra tid til annen om det hadde skjedd noe unormalt på noen av serverne eller om noen hadde tilgang til databasene, men fant i løpet av valgperioden ingen avvik. Verifikasjonsteamet sjekket også at RCG ble slått av ikke lenge etter slutten av valgperioden, og forble slått av inntil destrueringen av dataene på serveren.

Håndtering av minnepinner
Verifikasjonsteamet var til stede under åpningen av pakken med minnepinner som ble brukt under valgnatten til å flytte data mellom datamaskinene. Som en test ble det hentet ut én minnepinne, for å verifisere at det ikke var noen generelle produksjonsfeil på dem. Resten av minnepinnene ble lagt i et lite pengeskrin som verifikasjonsteamet fikk nøkkelen til, mens KRD bevarte pengeskrinet i et låst skap. I løpet av valgnatten ble det hentet ut minnepinner ved behov, og disse minnepinnene ble fulgt opp helt til deres destruksjon i en blender.

Destruering av data på våre datamaskiner
Som en del av verifikasjonsarbeidet ble det flyttet over noen filer med sensitiv innhold til verifikasjonsteamets datamaskiner. Dataene på disse datamaskiners harddisker ble slettet ved hjelp av kommandoen «shred» før verifikasjonsteam fikk datamaskinene tilbake. Representanter fra KRD og verifikasjonsteamet overvar at dette ble gjort.

Passordkontroll på KRDs servere
Verifikasjonsteamet satt et eget passord for harddisk og root-bruker på severne som ble brukt for klargjøring og mixing, slik at KRD ikke hadde tilgang til dataene på disse serverne uten at verifikasjonsteamet var tilstede. Verifikasjonsteamet påså at disse serverne ble slått av før de forlot lokalene.

9. Konklusjoner

Beskrevne prosesser
De to hovedprosessene (generering av hemmeligheter og trykking) som er dekket av denne rapporten, ble alle utført på en ryddig og oversiktlig måte, og staben var meget profesjonell og bevisst at hemmelighetene måtte ivaretas på en god måte. De to tilfellene vi observerte som teoretisk kunne ha kompromittert prosessen, den under generering av RCG-koder hvor kildefiler ble ligget ubevoktet en time, og den med trykkefiler på minnebrikker i stedet for på harddisk, ble håndtert øyeblikkelig etter at de ble oppdaget. *For fremtiden bør de kritiske prosessene ved etablering og sletting av hemmeligheter beskrives i detalj og verifiseres av kompetent personale slik at slik hull ikke oppstår under veis.*

Større opptellingsteam for e-stemmer
De samme personene utførte forskjellige oppgaver i løpet av valgnatten, deriblant nedlasting av manntallet, klargjøring, mixing, dekryptering og opplasting av telleresultatene. Dette førte til mye fokusskifte for dem som måtte utføre alle disse oppgavene, ofte under et tidspress

fordi kommunene forventet et resultat så snart som mulig etter at de hadde ferdigstilt manntallet sitt. Verifikasjonsteamet mener det hadde vært en fordel om hver person hadde kun noen få oppgaver. Det ville føre til at det blir lettere å kjøre de forskjellige prosessene i parallell.

Fastsatte tidspunkter for opptelling av e-stemmer
Hvis man skal kjøre e-valg i større skala enn for opptil ca. 15 kommuner, kan det være en fordel å avtale faste tidspunkter for når opptelling av e-stemmer skal settes i gang. Dette kan f.eks. skje hver hele time, eller eventuelt hver halve time hvis det er kapasitet for det. Dette vil lette tidspresset på KRD, samtidig som det vil være mye mer forutsigbar for kommunene når de vil få tilbake telleresultater for e-stemmer.

Morgenteam
Det bør vurderes om det skal settes opp et «morgenteam», som kan kjøre opptelling for de siste kommunene tidlig på tirsdag morgen. Verifikasjonsteamet bør på tilsvarende måte ha et morgenteam for å kunne følge opp KRD på tirsdag morgen.

KRD som superbruker for kommunene
Det bør vurderes om ikke KRD sentralt kunne registrere at manntallet er registrert ferdig i kommunene. Da vil man unngå problemer der kommunene glemmer å registrere manntallet ferdig.

Vedlegg

The IVS Representative

E-Valg 2013

Quality AS

Printing House Checklist Opening and Closing

Name: **Date:**

Time started: **Time ended:**

The serial number of the first voting card observed (approximately):

The serial number of the last voting card observed (approximately):

Check item	Comment (OK or a comment)
First Day	
The PC is loaded with data from a USB stick.	
We generate a password	
Check the protocol used and the documentation on the use (non-use) of the disks	
Was the test run of the dummy printing file correct?	
Last Day	
After having completed the printing the PC disk will be overwritten totally.	

The IVS Representative

E-Valg 2013

Quality AS

Printing House Checklist Every Day

Name: **Date:**

Time started: **Time ended:**

The serial number of the first voting card observed (approximately):

The serial number of the last voting card observed (approximately):

Check item	Comment (OK or a comment)
The PC was taken out of the safe by KRD staff	
The PC was opened by us with a password	
Only this one PC is connected to the printer	
The yellow cable connects to the computer marked Version V2 ++ HE, with only six other connections	
Has there been any equipment close to the folding unit which could be used for photographs, video recording or similar?	
Where there any paper jams or other irregularities in the process?	
If irregularities, did they maculate (shred) all cards involved?	

In case of paper jam, did they either (1) start from the next serial number after the last correct one; or (2) replace discarded cards individually?	
Before maculating cards which have to be discarded some should be checked at a random basis for general correctness on the inside. A representative for the printer should hold the card with only the address side visible to him or her and the verifier is to check the inside. Please note the serial number of the checked cards, and the result (OK or a comment). If mistakes, please report to KRD.	
Where any unauthorised persons present in the corner dedicated for the Return card printing?	
Did the Post collect the printed cards around 10 am?	
Was the PC locked up in the safe at the end of the day?	
Were the printed cards locked in the room with the safe at the end of the day?	
Other comments	