ÅDA
Offentliga Ålands IT-bolag

Slutrapport

Projekt: IMPLEMENTATION AV I-RÖSTNING

Version: 1.0

Dokument: Slutrapport

Version: 20191202

Författare: Styrgruppen för projektet

Innehåll

1 Basfakta

1.1 Projektet

Projektets mål var att implementera röstning via internet i lagtingsvalet 2019.

I januari 2019 anlitas Åda Ab för projektledning samt delar av projektarbetet för att rösta via internet. En styrgrupp tillsattes bestående av Casper Wrede (valadministratör, Ålands landskapsregering), Ronny Lundström (förvaltningsansvarig IT, Ålands landskapsregering) och Katarina Donning (vd, Åda Ab).

1.2 Bakgrund

Arbetet med att införa röstning via internet i lagtingsvalet på Åland 2019 startades redan november 2016. En sakkunnigkommitté för röstning via internet samt en politisk referensgrupp tillsattes i november 2016. I januari 2018 ombildades denna till en internetröstningskommission.
I april 2018 anlitades Åda för upphandlingen av en service för röstning via internet. En styrgrupp tillsätts.
Vid lagtingsvalet den 3:e söndagen i oktober 2019 (20.10.2019) skulle förtidsröstning för personer som är röstberättigade men skrivna utanför Åland ges möjlighet att rösta över Internet. För detta ändamål har Åda i samarbete med Ålands landskapsregering (LR) (valmyndigheten) upphandlat ett Internet röstningssystem (i-röstning) av Scytl secure electronic voting S.A i Barcelona, Spanien (Scytl).
7.1.2019 skrevs avtal med vinnande leverantör om att ombesörja internet röstningssystem som EaaS (Election as a Service).

1.3 Sammanfattning

1.3.1 Projektets omfattning

Implementation av ett i-röstning system för att LR (valmyndigheten) skulle kunna genomföra röstning över internet. Systemet implementerades som en EaaS tjänst (Election as a Service) för detta ändamål av vinnande anbudsgivare Scytl.

Ålands landskapsregering köpte in projektledarresurs samt visst projektgruppsarbete (de aktiviteter som kunde utföras av projektledaren samt testledning) från Åda Ab. Valets genomförande ingick inte i projektet.

Projektets huvudsakliga syfte var att säkerställa att i-röstningsystemet är tillgängligt för röstning i enlighet med den åländska vallagen.

2 Måluppfyllelse

2.1 Resultat, leveransobjekt enligt projektplan antagen av styrgruppen 16.5.2019

Lev. nr.	Beskrivning	Mottagare	Godkännande	Datum
1	Valplattform för internetröstning	Styrgruppen	Styrgruppen	Kunde aldrig godkännas fullt ut.
2	Testrapport från användartester	Styrgruppen	Styrgruppen	Levererades 17/5 2019
3	Auditering och säkerhetstester rapport	Styrgruppen	Styrgruppen	Levererades 7/6 2019
4	Slutrapport	Styrgruppen	Styrgruppen	Levererades 3/12 2019

2.2 Tid

Tidsplanen var redan från början av projektet snäv, men genomförbar. Det medgavs inte några förseningar eller förändringar som påverkade leveranstiderna inom projektet.

I juni då produktionsmiljön inte levererades enligt överenskommen tidplan blev tidsnöden i projektet uppenbar. Befolkningsregistercentralen (BRC) hade sommarstängt under juli månad och inga uppdateringar kunde således göras under semesterperioden. Pilottesterna flyttades från juni till augusti då det var svårt att få tag på testare under den tidpunkten. I augusti då pilottesterna sedan kunde genomföras förväntade sig Beställaren en fungerande produkt, men det visade sig att leverantören hade fortsatta problem med att implementera integrationen mot e-identifieringslösningen hos BRC. Gränssnittet i sig bygger på beprövade metoder och tydliga instruktioner och integrationer har gjorts av många organisationer tidigare, varför projektet inte förväntade sig att detta skulle vara ett stort problem.

Styrgruppen beslöt också genomföra penetrationstester baserat på den rapport gällande säkerhetsdokumentation som levererades i juni 2019. Vid penetrationstesterna uppdagades allvarliga säkerhetsbrister, som behövde åtgärdas innan produktion, vilket försköt tidsplanen ytterligare.

Ovanstående problem ledde till förseningar och projektet kunde sedermera inte godkänna resultatet. Styrgruppen rekommenderade att och beslut togs att inte gå i produktion med internetvalet.

2.3 Kostnad

Åda	Enligt offert €	Utfall €
Offererat från Åda för projektledning	22 450,00	27 668,75

Scytl	Enligt offert €	Utfall €
Rat 1 betalning vid kontraktssignering	4 000,00	4 000,00
Leverans del 1	12 000,00	12 000,00
Leverans del 2	8 000,00	8 000,00
Leverans del 3	8 000,00	0,00
Leverans del 4	8 000,00	0,00
Support under förtidsröstning	5 000,00	0,00
CR #1 Penetrationstest	13 350,00	13 350,00
CR #2 Pilottest 2	3 600,00	3 600,00
CR #3 Electoral operations and onsite support	13 380	13 380
CR #4 Pilot test no 4	6 600	-
TOTALT	**81 930**	**54 330**

Deductive labs	Enligt offert €	Utfall €
Genomgång med Scytl samt dokumentanalys	4 650,00	3 610,00
Upphandling och koordinering av penetrationstest	Ca. 2 100	7 102,40
TOTALT	**Ca 6 750**	**10 712,40**

Nixu	Enligt offert €	Utfall €
Penetrationstest	29 190,00	Delbetalning 1 3 521,27
Penetrationstest	Enligt ovan	Delbetalning 2 19 373,00
Penetrationstest	Enligt ovan	Delbetalning 3 4 262,59
Publik rapport	Ca. 2 780	Ej levererad ännu
TOTALT	**31 970**	**27 156,86**

Verifieringsapp	Enligt offert €	Utfall €
Google registrerings- samt utvecklingskonto	-	22,58
Apple registrering- samt utvecklingskonto	-	79,84
TOTALT		**102,42**

Omkostnader av test	Enligt offert €	Utfall €
Hyra av Klinten	-	96,00
Matdivisionen	-	123,60
TOTALT		**219,60**

Totala utgifter för projektet

Leverantör	Enligt offert	Utfall
Åda	22 450	27 668,75
Scytl	81 930	54 330
Deductive labs	6 750	10 712,40
Nixu	31 970	27 156,86
Verifierings app		102,42
Omkostnader tester		219,60
TOTALT	**143 100**	**120 190,03**

2.3.1 Sammanfattning kostnader

Enligt ovanstående sammanställning av kostnaderna framgår att projektets totala kostnader är lägre än den beslutade budgeten. Fyra betalningar är reklamerade hos Leverantören pga att leveransen inte kunnat accepteras då projektleveranserna var behäftade med fel och produktionssättningen avbröts innan systemet kunde användas för sitt ändamål.
Det pågår diskussioner med leverantören om de reklamerade betalningarna, dessa hanteras utanför projektet.

3 Projektförlopp

Projektet startade under januari månad 2019. Testmiljön sattes upp av leverantören och levererades till styrgruppen inom utsatt tid.

Användarbarhetstester av gränssnittet utfördes i testmiljön under perioden 9 – 24.5 2019 och resultatet levererades till styrgruppen 28.5.2019. En sammanställning över de brister som upptäckts under testperioden levererades vidare till leverantören med uppdrag att uppdatera användargränssnittet. Dessa godkändes sedan av beställaren (CW).

Vid leverans av produktionsmiljön den 12.7.2019 hade leverantören svårigheter med att bygga integrationen mot e-identifikation. Detta då BRC hade produktionsstopp under juli månad. Leveransen av produktionsmiljön försenades delvis p g a svårigheter med denna integration mot e-identifieringsgränssnittet.

Den säkerhetsauditering som utfördes under maj-juni (genomgång av leverantörens system- och tekniska dokumentation) gällande i-röstningssystemet levererades 7.6.2019. Genomgången visade på vissa brister, vilket föranledde att styrgruppen för projektet ansåg att ett penetrationstest av systemet skulle utföras. Projektledaren fick i uppdrag att inhämta offert från företag som genomför penetrationstester. Offerterna behandlades på styrgruppsmöte 19.7.2019 och beslut om vinnande offert togs. Det bestämdes samtidigt att det företag som bistått i systemdokumentations genomgången skulle få i uppgift att koordinera penetrationstesterna, i o m att de besatt den tekniska expertis inom säkerhetsfrågor som krävdes.

Styrgruppen levererande sin rekommendation till landskapsregeringen gällande genomförande av i-röstning den 11.6.2019. Styrgruppen

konstaterar då att vissa punkter har lyfts i genomgången av dokumentationen, men att de tillsammans med information om hur systemet används på övriga håll inte pekar på att det skulle föreligga några överhängande risker med att fortsätta genomförandet av projektet och med mål att tillhandahålla e-röstning i höstens lagtingsval.

Planeringen av penetrationstesterna påbörjades i början av augusti där både leverantören av i-röstningssystemet och det företag som skulle genomföra penetrationstesterna, jämte den som skötte koordinering av detta deltog. Från början uppstod problem med access till leverantörens system och svårigheter med att få tillgång till efterfrågad dokumentation. Detta försenades ytterligare och viss dokumentation levererades aldrig till leverantören av penetrationstesterna.

Under augusti utfördes en första pilottest för att kontrollera att e-identifieringens integration var korrekt. Pilottesten skulle enligt tidplan utförts i juni, men bokades om p g a svårigheter med att få tillräckligt antal testpersoner. Under pilottesten upptäcktes stora säkerhetsbrister i integrationen mot e-identifieringen.

En ny pilottest bokades således till 13.9 2019. Denna sköts sedan, på leverantörens begäran, upp till 19-20.9 2019. Då pilottesten påbörjades fanns ännu allvarliga säkerhetsbrister i integrationen mot e-identifieringen. Pilottesten kunde därför inte slutföras. Under de påföljande veckorna arbetade leverantören med att få integrationen att fungera. Dessa testades sedan och godkändes per mejl den 3.10 2019. Dock kunde aldrig en fullständig pilottest utföras eftersom tidsplanen inte tillät det innan e-röstningen skulle påbörjas.

Under denna tid arbetades det även med penetrationstesterna. Dock hade leverantören svårt att tillhandahålla material för att kunna utföra penetrationstesterna till slut.

Datainspektionen på Åland beslöt i juni att påbörja ett tillsynsärende i juni 2019. Tillsynsrapporten levererades 19.9.2019. Rapporten visade på brister i personuppgiftsbiträdesavtalet mellan Åda och Ålands landskapsregering. Det ansågs vara för allmängiltigt för att omfatta specifika tjänster. Avtalet arbetades om och reglerades innan planerad produktionssättning av tjänsten. Även brister i leverantörens rutiner inom personuppgiftsområdet uppmärksammades i rapporten.

Då rapporten för de delar av penetrationstesterna som kunde utföras levererades till styrgruppen 7.10.2019 visade det sig att det fanns tre medium risker. Vid genomgång av dessa med säkerhetskunniga från Nixu som utfört testerna och säkerhetsansvarig på Åda konstaterades att mediumrisker inte bör förekomma i ett i-röstningssystem och att dessa fel bör åtgärdas omedelbart. Rekommendationen omfattades av styrgruppen. Bristerna påtalades till leverantören 7.10.2019. Leverantören åtgärdade bristerna samma dag och styrgruppen beslutade att beställa en sista test från Nixu. Testen kunde utföras först på eftermiddagen 8.10.2019. Bristerna visade sig då vara åtgärdade och de tre mediumriskerna eliminerade.

Samtidigt som penetrationstestrapporten färdigställdes av Nixu så gick säkerhetsansvarig på Åda under perioden 2 - 8.10.2019 genom denna och TechLaws rapport som Datainspektionen beställt och analyserade utfallet av rapporterna. Baserat på analysen av TechLaws rapport, utfallet av

penetrationstesterna och svar på frågor som ställts till leverantören med anledning av detta, så var rekommendationen att inte gå vidare med att starta internetröstningen. Det bör även tilläggas att styrgruppen i ett sent (7.10.2019) skede fick muntlig information om att Scytl använder sig av en molntjänst via Amazon Web Services (AWS) för AntiDDoS övervakning via Amazons WAF-tjänst. Denna information hade inte meddelats beställaren och utredning pågår för tillfället för att konstatera om detta var en tredjepartstjänst som borde ha meddelats beställaren i enlighet med personuppgiftsbiträdesavtalet.

Den 8.10.2019 på eftermiddagen beslöt styrgruppen att rekommendera till centralnämnden för lagtingsval att inte gå vidare med internetröstning i lagtingsvalet då flera öppna frågor kring informationssäkerheten och tjänsten fanns. De öppna frågorna var:

- Penetrationstesterna hade inte genomförts i sin helhet. Fullständigt material hade inte erhållits från leverantören varför en del av penetrationstesterna inte kunnat genomföras fullt ut.
- Pilottesterna var inte genomförda i sin helhet. Den var en del av projektleveransen och då produktionsmiljön var behäftad med fel ännu i ett sent skede av projektet så var tiden för knapp för att hinna genomföra en fullständig pilottest. Pilottesterna kunde ha slutförts efter att internetröstningen påbörjats, men innan den avslutats. Dock är syftet med en pilottest att trygga leveransen för beställaren genom att denne verifierar att tjänsten levererats i enlighet med ställda krav och att betalning kan utgå enligt överenskommen betalningsplan.
- Konsekvensbedömningen var inte genomförd i sin helhet innan internetröstningen skulle påbörjas. Om känsliga persondata hanteras i ett system ska det enligt dataskyddsförordningen och lagstiftningen genomföras en konsekvensbedömning. Detta var även något som påtalades av Datainspektionen vid den granskning som genomfördes. Penetrationstesternas genomförande var en av konsekvensbedömningens aktiviteter, som inte kunde slutföras.

4 Erfarenheter och rekommendationer

1.1 Erfarenheter

Implementeringen av internetröstningen slutfördes inte till sin helhet eftersom styrgruppen för projektet den 8.10.2019 tog beslut om att rekommendera för centralnämnden för lagtingsval att inte genomföra internetröstning i lagtingsvalet p g a de brister som fanns i levererad tjänst.

Vallagen som antogs i juni 2019 möjliggör internetröstning även i framtida lagtingsval. Erfarenheterna är av den anledningen desto viktigare att lyfta för att, inför kommande lagtingsval, ta lärdom av de erfarenheter implementationen av internetröstning inför lagtingsvalet 2019 förde med sig:

Snäv tidsplan:
Projektets tidsplan tillät inte några förseningar. Upphandlingen av tjänsten kunde påbörjas i ett sent skede då nya vallagens färdigställande drog ut på

tiden. Vallagen var en viktig faktor i upphandlingen och under kravställningen.

Tidplanen var i fas t o m juni. I augusti uppdagades fel i leverantörens lösning för integrationen mot BRC och e-identifieringen. Dessa fel påverkade tidplanen menligt.

Pilottesterna (genrep av förfarandet) gick inte som planerat p g a fel i leveransen:
Att genomföra ordentliga pilottester var en framgångsfaktor i projektet.

Pilottestomgång 1 flyttades fram från juni till augusti 2019 p g a att systemet inte var levererat och att det var svårt att genomföra pilottesterna under midsommarveckan i juni. Den pilottest som sedan gjordes i augusti kunde inte genomföras i sin helhet då systemet var behäftat med fel. En ytterligare pilottestomgång i mindre skala schemalades i september. Syftet med denna var att köra ett fullskaligt internetval, med både förberedelser, röstning och efterarbete. Pilottest omgång 2 kunde inte heller avslutas p g a att samma fel uppdagades, dvs problem med integration mot e-identifieringen.

1.2 Rekommendation

Påbörja projektet i tid inför en eventuell internetröstning i lagtingsvalet 2023:
Det behöver finnas ordentligt med tid för att genomföra pilottester, penetrationstester, konsekvensanalyser samt genomgång av säkerhetsdokumentationen. Ett IT-projekt för alltid med sig uppgifter att hantera på vägen och då behöver det finnas ordentligt med ledtid för att hantera dessa uppgifter.

Rekommenderbart är kontrakt med en leverantör finns minst 1 år före tjänsten ska tas i bruk.

Tidsplan med tydliga beslutspunkter:
Med tanke på den dignitet ett avbrytande av projektet fick så borde projektet ha haft en tydlig tidsplan där det framgått tydligt vem som informerar och när vissa beslut bör tas och hur eventuella konsekvenser av dessa kan hanteras. Projektets styrgrupp diskuterade inte konsekvenserna av olika beslut och rekommendationer i den omfattning som borde ha gjorts med tanke på att projektet i sig var banbrytande. Planen kunde också ha tydliggjort när och till vem vissa beslut och rekommendationer borde ha kommunicerats.

Överlämning till förvaltning kräver tillräcklig tid:
Att gå från implementation av en tjänst i ett projekt till förvaltning av den samma i verksamheten är en aktivitet i sig. Det rådde oklarheter hos leverantören om vilka som var mottagarorganisation av systemet.

För implementationen av internetröstningssystemet blev tiden mellan implementation och övergång i förvaltning för kort i o m att tidplanen sprack redan i början av sommaren. Nu genomfördes inte implementationen fullt ut, men inför framtiden så bör det även finnas tillräcklig tid för överlämning till dem som ska förvalta systemet.

5 Referenser

Ref.	Dokumentnamn, beteckning och namn	Utgåva, datum
1	Upphandlingsmaterial	
2	Anbudssvar upphandling	
3	Tilldelningsbeslut	1.0, 03122018
4	Styrgruppsprotokoll	
5	Projektplan	1.0, 16052019
6	Tids- och aktivitetsplan	12072019
7	Utlåtande informationssäkerhet eval Scytl (Deductive labs)	1, 07062019
8	Resultat och beslut av den beslutade Dataskyddstillsynen gällande personuppgiftsbehandling i Lagtingsvalet, särskilt fokus I-valet Dnr T1-2019.	1, 19092019
9	Rapport gällande informationssäkerhet (TechLaw)	Kan begäras ut från DI
10	Publik rapport Penetrationstest (Nixu)	1, 27112019 (inväntar godkännande)
11	Konsekvensbedömning	2.0, 06092019

Svar på förvaltningschefens tilläggsfrågor angående röstning via internet vid lagtingsvalet 2019

- utgående från slutrapport avgiven av styrgruppen för implementering av i-röstning

Vd Katarina Donning, förvaltningsansvarig IT Ronny Lundström, valadministratör Casper Wrede, vilka utgjorde styrgrupp för implementering av i-röstning i lagtingsvalet 2019.

December 2019

Fråga 1: Vart tog internetröstningskommissionen vägen och vilken var dess roll?

Internetröstningskommissionen hade en rådgivande roll och var inte ett beslutande organ. Kommissionen hördes inför landskapsregeringens ställningstagande till tiderna för i-röstningen i juni 2019. Fastställande av tiderna innebar samtidigt att optionen att inte anordna i-röstning inte utnyttjades. Kommissionens medlemmar inviterades att delta i förberedelserna för den riskbedömning som förbereddes under tiden före valet, men som aldrig kunde avslutas.

Fråga 2: Vilka referenser fanns vid tiden för kontraktstecknandet över Scytls förmåga att leverera?

Scytl är ett av de ledande företagen inom digitalisering av alla funktioner i anslutning till val, inklusive i-röstning. Vid upphandlingen ställdes som ska-krav att leverantören skulle ha tillhandahållit ett system för i-röstning vid ett bindande nationellt val. Scytl´s system har använts i bindande val i exempelvis Frankrike, Schweiz och New South Wales, den största delstaten i Australien.

Fråga 3: Enligt rapporten var tidplanen redan från början och att det inte fanns utrymme för förseningar. I juni då leverans inte skedde enligt plan blev tidsnöden uppenbar. Vilka var mot den här bakgrunden de motiv som gjorde att man ändå valde att gå vidare?

Förseningen av produktionsmiljön som inträffade i juni var inte särskilt oroväckande då det fanns möjlighet att ta igen den förlorade tiden under sommaren. Vi hade också från vår sida problem med att få ihop en tillräckligt stor grupp testdeltagare för den pilottest som var planerad till slutet av juni. Det skedde också ett byte av projektledare i juni. Pilottestet flyttades till mitten av augusti och det fanns därför inga skäl att forcera färdigställandet av produktionsmiljön.
Ingen av parterna kunde förutse de problem som neddragningen av beredskapen under semesterperioden hos Befolkningsregistercentralen skulle förorsaka.

Fråga 4: Det förelåg enligt rapporten säkerhetsbrister och svårigheter den 13.9 och 19-20.9, övervägde man allvarligt att avbryta i det skedet?

Då bristerna som uppdagades handlade om i-röstningssystemets integrering med systemet för identifiering av väljarna via Suomi.fi-portalen, vilket enligt sakkunniga är en tämligen okomplicerad operation och det därför fanns grundad anledning att tro att problemen skulle kunna lösas, ansågs det mest ändamålsenligt att invänta resultaten från den pågående stresstestningen.