ASSEMBLY VOTING X

Det digitale valglokale

Fuldt dokumenteret End-to-End verificerbart valgsystem.

Assembly Voting

ET VALGRESULTAT HÆVET OVER ENHVER TVIVL

I et demokrati er det stemmerne der tæller og vælgerne der bestemmer.

Uanset om det er folketingsvalg, overenskomstafstemninger, eller et valg i den lille forening, så forventer alle et fair valg og et valgresultat hævet over enhver tvivl.

Tillid til valg bygger på overholdelse af de grundlæggende demokratiske principper om bl.a. transparens, anonymitet, delt ansvar og mulighed for kontrol af alle dele i valghandlingen. Det gælder i valglokalet og det gælder selvfølgelig også i digitale valg.

Med Assembly Voting X får du et digitalt valglokale efter samme demokratiske principper og med samme høje sikkerhed som man kender det fra det fysiske valglokale.

Assembly Voting X er det sikre digitale valglokale til alle typer af valg.

Med Assembly Voting X får du

Et End-to-End verificerbart valgsystem

Alle dele af valghandlingen før, under og efter stemmeafgivelsen kan kontrolleres og efterprøves af uafhængige parter.

Et sikkert og fuldt dokumenteret valgsystem

Dokumenteret sikkert og matematisk bevist valgsystem, med brug af kryptografiske algoritmer, der sikrer fuld anonymitet og integritet i stemmeprocessen.

Et brugervenligt valgsystem

Et komplet valgsystem der let kan sættes op til gældende valgregler, og som samtidig er nemt at betjene for vælgere, valgtilforordnede og administratorer.

Et økonomisk tilgængeligt valgsystem

Hidtil har denne type valgteknologi været økonomisk og praktisk utilgængelig for de fleste valg. Med Assembly Voting X, er den samme høje sikkerhed som ved parlamentsvalg, tilgængelig for alle typer og størrelser af valg.

Assembly Voting ApS, Ringager 4C, 1. th., 2605 Brøndby, Danmark
Tel: 26169638 @: salg@aion.dk cvr: 25600665

EN KOMPLET VALGLØSNING

Assembly Voting X leveres som en komplet valgløsning, hvor alle aktiviteter og processer fra start til slut er medtænkt og indeholdt. Med erfaringer fra mere end 6.000 gennemførte lov- og vedtægtsbestemte valg, har vi optimeret de tekniske såvel som administrative løsninger, så vi hurtigt og dokumenteret sikkert vil kunne levere en End-to-End verificerbar valgløsning til langt de fleste behov.

Assembly Voting X kan suppleres med en række andre systemer, der på forskellig vis kan bidrage til at gennemføre en dokumenteret sikker og brugervenlig demokratisk valgproces. Vi leverer bl.a. kandidatregistreringssystemer, supportsystemer og valglistesystemer. Alle systemer leveres som full-service eller self-service SaaS (Software as a Service), med mulighed for lokal hosting.

Assembly Votings systemer og datahåndteringsprocesser er dokumenteret ud fra ISAE3000 standarden, der sikrer at alle processer er transparente og i fuld overensstemmelse med GDPR.

Konfigurationsmuligheder

Typer af valg

- Kandidatvalg
- Kandidat- og listevalg
- Folkeafstemninger
- Overenskomstvalg
- Multiple stemmesedler

Stemmemedie

- PC og computer
- Tablet
- Smartphone
- Postale brevstemmer (hybrid valg)

Stemmeadgang

- Digitale signaturer, fx NemID
- Valgkoder
- Valgkoder og BrugerID

Stemmeprincipper

- Påkrævet antal stemmer
- Maximum antal stemmer
- Vægtede stemmer
- Skrive-stemme (digitale brevstemmer)
- Overskrivning af stemme
- Rangering af stemmer

Assembly Voting ApS, Ringager 4C, 1. th., 2605 Brøndby, Danmark
Tel: 26169638 @: salg@aion.dk cvr: 25600665

OM ASSEMBLY VOTING

Assembly Voting var den første udbyder af elektroniske valg i Danmark (2001), og er i dag markedets mest benyttede leverandør af digitale valgløsninger i Skandinavien.

Assembly Voting er baseret på idéen om at styrke den demokratiske deltagelse i samfunds- og foreningsliv, gennem sammentænkning af grundlæggende demokratiske processer og principper med nye, dokumenterede sikre og brugervenlige teknologier.

Assembly Voting leverer fuldt dokumenterede valgløsninger til bl.a. ministerier, kommuner, faglige organisationer, virksomheder og foreninger.

Primære systemer

Assembly Voting X
Det digitale valglokale - Dokumenteret sikkert online valgsystem.

Assembly Conference Voting
System til live-afstemninger uafhængigt af fysisk tilstedeværelse.

Assembly Votes
Fleksibel og komplet valgløsning til lov- og vedtægtsbestemte valg.

Assembly Candidacy
Registrering, validering og præsentation af kandidater.

Fakta

- Første digitale lov- og vedtægtsbestemte valg i DK (2001)
- +6.000 gennemførte valghandlinger
- +35 Mio. vælgere
- +35.000 kandidatvalideringer
- Full service, Partner- og selvbetjeningsløsninger
- ISAE3000 Certificeret

Kontakt vores salgsafdeling for at høre mere om hvordan vi kan gennemføre jeres næste valg

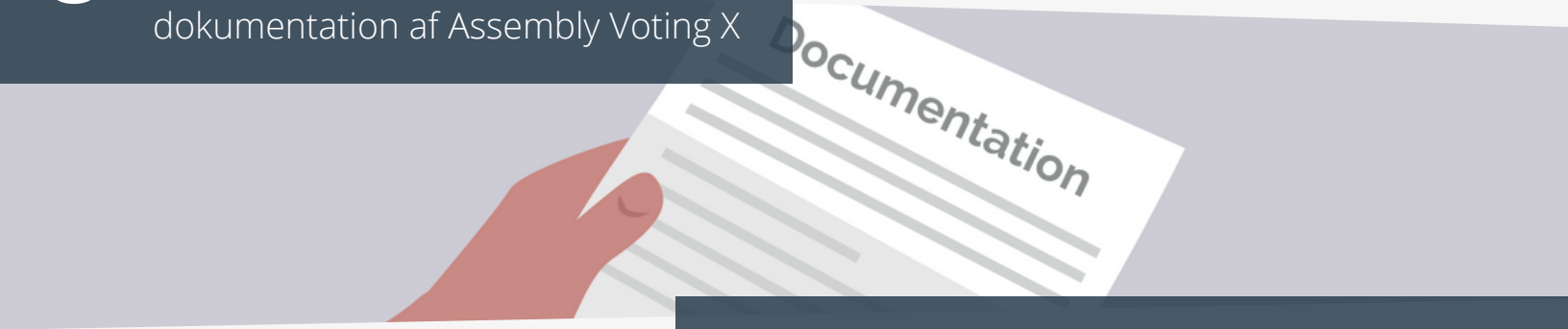
+45 26 16 96 38

salg@aion.dk

ASSEMBLY VOTING X
OVERSIGT

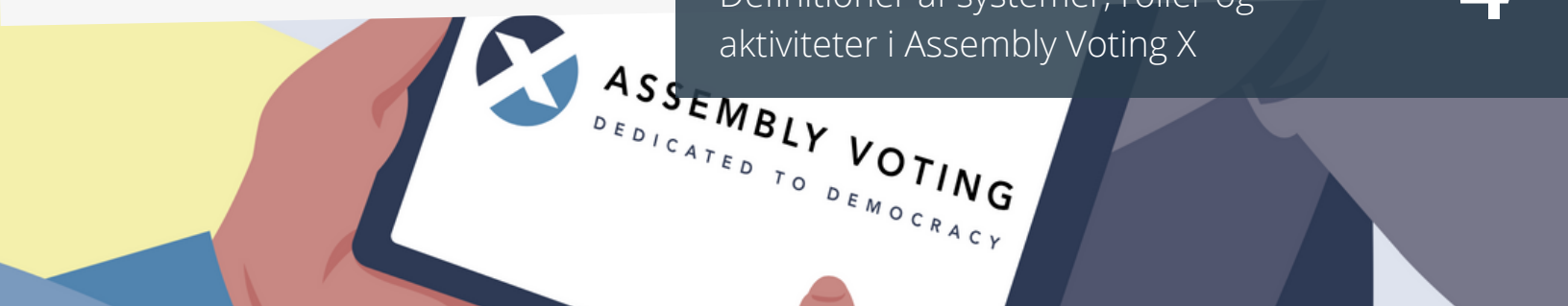
I **Det digitale valglokale**
Opbygning af det digitale valglokale

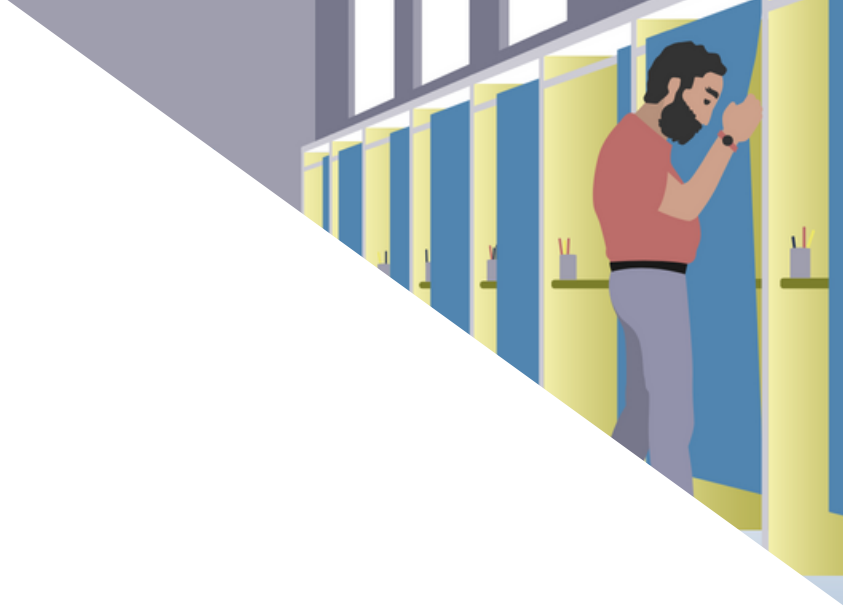
Valgprocessen 2
Introduktion til praktisk gennemførelse af valg med Assembly Voting X



3 **Teknologier og dokumentation**
Anvendte teknologier i - og dokumentation af Assembly Voting X

Ordbog 4
Definitioner af systemer, roller og aktiviteter i Assembly Voting X





I. DET DIGITALE VALGLOKALE

Assembly Voting X er bygget op omkring de samme grundlæggende demokratiske principper, som vi kender fra valglokalet, når vi for eksempel stemmer ved et Folketingsvalg. Det betyder, at alle dele af valgprocessen, fra start til slut, kan kontrolleres af valgtilforordnede og uvildige eksterne parter.

I det digitale valglokale er stemmeboksen, papirstemmen og valgurnen erstattet med avancerede og matematisk beviste krypteringsteknologier. Derved sikrer Assembly Voting X vælgernes stemmehemmelighed og anonymitet, ligesom systemet fører bevis for, at det kun er gyldige stemmer der indgår i valgresultatet.

Som i det fysiske valglokale er tilliden til valghandlingen i Assembly Voting X sikret gennem systemdesign, delt ansvar og verifikationsmuligheder i hele valgprocessen. Ikke gennem ukontrollerbar tillid til en systemleverandør og enkeltpersoner.

Succeskriteriet er et valgresultat hævet over enhver tvivl - hverken mere eller mindre!

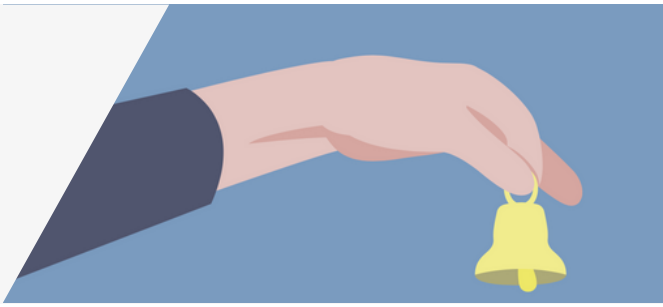
Det digitale valglokale - Assembly Voting X

Før-valg aktiviteter - Opsætning og forberedelse af valghandling

Fuldt transparent og dokumenteret proces med opsætning og datahåndtering i valgsystemet. Valgsystemet indeholder ingen valgkoder eller andre personfølsomme data, der vil kunne anvendes til uretmæssig stemmeafgivelse. Opsætningen dokumenteres og "låses" efter godkendelse i valgåbningsceremonien.

Valgåbning - Valgåbningsceremoni

Digitale valgtilforordnede kontrollerer, at valgopsætningen er i overensstemmelse med gældende regler og lovgivning. En Valgkontrol Applikation sikrer, at den "digitale valgurne" forsegles, så der ikke er adgang til resultater under valghandlingen. Først når valgåbningsceremonien er gennemført, kan valget åbnes.



Stemmeret - Personlige valgkort

Vælgeren får adgang til at stemme via en tilsendt kodekombination fra 2 uafhængige distributører. Der er mulighed for at benytte digital signatur, fx NemID. En krypteringsalgoritme gør det muligt at fremsende en kodekombination til den enkelte vælger, der kun er kendt af den enkelte vælger, og samtidig gemme en signatur til valgsystemet uden at "afsløre" kodekombinationen til valgsystemet eller sytemleverandøren.

Stemmehemmelighed - Stemmeafgivelse bag forhænget

Vælgerens stemme krypteres på egen lokale enhed i browseren, og fremsender efterfølgende et kryptogram med VælgerID og stemme til valgsystemet. Er vælgeren i tvivl om den afgivne stemme er korrekt krypteret, kan en Stemmekontrol app, der kan hentes fra App Store og Google Play, anvendes. Valgsystemet gør det muligt at overskrive sin stemme, hvis man skulle være udsat for stemmepres. Endvidere er det muligt at sætte valgsystemet op, så der kan afgives stemmer fra et "kontrolleret miljø" på udvalgte lokaliteter, hvor adgangen til stemmeafgivelsen foregår under opsyn. På den måde sikres fuld stemmehemmelighed under stemmeafgivelsen..

Brugervenlighed - Overskuelig og let tilgængelig stemmeseddel

Den elektroniske stemmeseddel gør det let at overskue de valgbare alternativer, og selve stemmeafgivelsen er designet så det ikke efterlader tvivl om hvem eller hvad, der er stemt på. I modsætning til papirstemmesedlen er den digitale stemmeseddel let tilgængelig for svagtseende og dyslektikere.

Assembly Voting ApS, Ringager 4C, 1. th., 2605 Brøndby, Danmark
Tel: 26169638 @: salg@aion.dk cvr: 25600665

Anonymitet - Digital kuvert med krypteret stemme inden i

Den afgivne stemme afsendes, modtages og opbevares i krypteret form. Princippet er det samme som med en fysisk brevstemme, der indeholder en "yderkuvert" med vælgerID og en "inderkuvert" med den afgivne stemme. Krypteringsteknologien sikrer, at det kun er validerede stemmekryptogrammer, der indgår i resultatoptællingen.

Stemmeintegritet - Kontrol med valgurnen

I det fysiske valglokale kan alle holde øje med valgurnen gennem valghandlingen. På tilsvarende vis kan man i det digitale valglokale holde øje med den digitale valgurne. En offentlig tilgængelig digital valgtavle baseret på blockchain-inspireret teknologi fungerer som valgurne, og her kan vælgerne, de valgtilforordnede og andre uvildige parter kontrollere de indkomne stemmekryptogrammer og øvrige aktiviteter i valgsystemet.

Valglukningsceremoni - Anonymisering af stemmer og opgørelse af valgresultat

Når et godkendt antal digitale valgtilforordnede er logget på Valgkontrol Applikationen, adskilles vælgerID og stemme irreversibelt fra hinanden via en digital Mixer proces. Denne proces foregår via flere uafhængige processer med bevis på, at der ikke er fjernet, tillagt eller modificeret stemmer undervejs i processen. Først nå anonymiseringen er gennemført kan dekrypteringen af stemmerne gennemføres.

Dokumentation - Fuld transparens før, under og efter valghandlingen

Der skal være fuld dokumentation omkring en valghandling. Det skal kunne efterprøves, om der er pågået aktiviteter, der kan så tvivl om valgresultatet. Assembly Voting X er et fuldt ud dokumenteret og matematisk bevist valgsystem. Alle systemaktiviteter dokumenteres og kan kontrolleres af vælgere, valgtilforordnede og eksterne parter. Systemet bygger på open-source teknologier og der stilles kontrolprotokoller til rådighed for ekstern kontrol med valgprocessen.

Hvad er et End-to-End verificerbart valgsystem?

En digital valgløsning, hvor alle dele af valgprocessen kan kontrolleres og efterprøves af valgtilforordnede og uvildige parter, som man kender fra det fysiske valglokale. Udgangspunktet er "tillid gennem design", hvor bl.a. vælgeranonymitet og resultatintegritet sikres gennem et fuldt ud dokumenterede og matematisk bevist valgsystem.

Hvad er et blackbox valgsystem?

En valgløsning, hvor det ikke er muligt for valgtilforordnede eller uvildige parter at kontrollere alle dele af valgprocessen. Udgangspunktet er "ukontrollerbar tillid" til at systemleverandører og valgansvarlige ikke laver fejl eller manipulation med enkelte dele af valgprocessen.

Assembly Voting ApS, Ringager 4C, 1. th., 2605 Brøndby, Danmark
Tel: 26169638 @: salg@aion.dk cvr: 25600665

2. VALGPROCESSEN

Assembly Voting X leveres som en full service løsning med en komplet drejebog til alle faser af valghandlingen. Selvom der anvendes avanceret teknologi, er det afgørende for valgets legitimitet, at systemerne er let tilgængelige og brugervenlige for valgets forskellige aktører; valgsystemadministratorer, valgadministratorer, valgtilforordnede, vælgere og evt. eksterne revisorer.

Med erfaring fra mere end 6.000 lov- og vedtægtsbestemte valg har vi designet løsningen, så alle aktører let og sikkert kan betjene de forskellige funktioner i løsningen. Det reducerer risikoen for fejl og bidrager til at skabe større tillid til valghandlingens gennemførelse.

Det er altid godt at være i god tid når det gælder forberedelse af en valghandling, men vores standardiserede processer og systemer er optimeret, så vi selv med kort varsel kan forberede og gennemføre dokumenterede sikre valghandlinger.

En komplet valgløsning - Assembly Voting X

Assembly Voting tilpasser aktiviteterne til de enkelte projekter i en samlet drejebog for hele valghandlingen. Præsenteret på de næste sider er en oversigt over de aktiviteter, der typisk er indeholdt i en Assembly Voting X valghandling.

Alle systemer og datahåndteringsprocesser er fuldt dokumenteret og revisionerede efter ISAE3000 standarden.

Før-valg aktiviteter

Hovedaktivitet	Delaktiviteter	Verifikation
Kravspecifikation	Krav til valgopsætningen specificeres med udgangspunkt i gældende lovgivning og valgregler. Herunder brug af log ind / digital signatur, digitale valgtilforordnede, m.m.	• Kravspecifikation dokumenteres og godkendes af valgkunde
Systemopsætning	Valgsystemet og de supplerende systemer sættes op i overensstemmelse med kravspecifikation.	• Validering af systemadmin • Log af alle system-aktiviteter
Valgmaterialer	Udarbejdelse af valgkort og supplerende valginformationer til vælgere og valgtilforordnede.	• Valgmaterialer godkendes af valgkunde • Valgmaterialer godkendes af Assembly Voting
Data	Der udarbejdes en DBA forud for upload af vælgerdata og data på valgtilforordnede via sikker upload-funktion (Assembly Files)	• Gensidig godkendelse af DBA • Log af aktiviteter i Upload-funktion
Test	Gennemførelse af test af valgopsætning, data, valgmaterialer, m.m.	• Godkendelse af kunde og/eller ekstern revision
Valgkode generering	Generering af en eller flere valgkoder af en eller flere distributører, ved hjælp af script. Tilhørende public code sendes tilbage til systemadministrator.	• Test ved hjælp af en testbruger med delte valgkoder
Upload af stemmeberettigede	Upload af stemmeberettigede til backend med tilhørende public key.	• Godkendelse af antal stemmeberettigede af kunde og/eller ekstern revision
Valgåbnings-ceremoni	Kontrol af valgopsætning, deling af krypteringsnøgler mellem valgtilforordnede og kontrol af "tom digital valgurne". Låsning af opsætning.	• Godkendelse via Valgkontrol App og digital valgtavle af valgtilforordnede

Fortsættes på næste side

Under-valg aktiviteter

Hovedaktivitet	Delaktiviteter	Verifikation
Udsendelse af valgkort	Valgkoder udsendes i valgkort fra uafhængige distributører til vælgerne.	• Bounce rapport og åbningsrate rapport.
Stemmeret	Vælgerne valideres, via indtastning af den tilsendte kodekombination og/eller NemID.	• Godkendelse via signatur fra kode-kombination
Kontrol af digital brevstemme	Vælgerne kan kontrollere, at deres stemme er korrekt krypteret i browseren ved at benytte Stemmekontrol APPen	• Godkendelse via Stemme-kontrol App af vælgere
Kontrol af registreret stemme	Vælgerne kan kontrollere, at deres stemme er korrekt registreret i den "digitale valgurne" ved at uploade stemmekvittering i valgtavlen	• Godkendelse via upload af stemme-kvittering af vælgere

Efter-valg aktiviteter

Hovedaktivitet	Delaktiviteter	Verifikation
Valgluknings-ceremoni	De valgtilforordnede logger på Valgkontrol Applikationen, hvorefter mixing-processen (anonymisering af stemmer), dekryptering og resultatopgørelsen igangsættes.	• Godkendelse via Valgkontrol App af valgtilforordnede
Valgresultat	De valgtilforordnede godkender valgresultatet, forud for offentliggørelse.	• Godkendelse via Valgkontrol App af valgtilforordnede
Dokumentation af valghandling	Fuld dokumentation af alle aktiviteter på offentligt tilgængelig valgtavle. Kontrolprotokoller til rådighed for (ekstern) revision af valghandling	• Godkendelse via kontrolprotokoller af digital valgtavle
System-dokumentation	Fuld dokumentation af valgsystemet er tilgængeligt: Teknisk design, matematiske beviser, open-source teknologier og server-setup	• Godkendelse via ekstern revision

3. TEKNOLOGIER & DOKUMENTATION

Assembly Voting X bygger på matematisk beviste algoritmer og teknologier. De anvendte teknologier er tilgængelige for revision via open source-software. Derved sikres det, at alle dele i valgsystemet er fuldt dokumenteret og tilgængeligt for forskere, uafhængige revisorer og øvrige interessenter.

Teknologiske nøglekomponenter i Assembly Voting X

Alle anvendte teknologier er velbeskrevet og dokumenteret videnskabeligt, for at sikre fuld dokumentation og transparens i valgsystemet.

- Discrete logarithm zero-knowledge proof
- Furukawa mixing proof
- SHA256 hash function
- Elliptic curve cryptography – secp256k1 curve
- Threshold cryptography based on ElGamal cryptosystem
- Schnorr digital signatures

Integritet

Integritet og kontrolmuligheder i alle dele af valgprocessen er en grundsten i en demokratisk valghandling. Assembly Voting X sikrer fuld integritet gennem individuelle og universelle verifikationsmuligheder til bl.a. stemmeberettigede, valgtilforordnede, uafhængige revisorer, observatører, m.fl.

Stemme afgivet i valgsystem som ønsket

Individuel verifikation: Systemet indeholder en mekanisme (ballot opener APP) der kan bevise at den digitale stemme er korrekt registreret i det kryptogram der indeholder stemmen.

Stemme registreret i valgsystem som afgivet

Individuel verifikation:en valgtavle bygget på blockchain inspireret teknologi logger, uden undtagelse, alle valgaktiviteter i systemet. Den stemmeberettigede kan via upload af stemmekvittering i valgtavlen kontrollere at stemmen er korrekt registreret og dermed ikke er blevet redigeret eller fjernet under forløbet i valgprocessen.

Stemme optalt som registreret

Universel verifikation: Stemmeoptællings-processen genererer bevis der dokumenterer korrektheden ved de opgjorte valgresultater. Dette betyder at valgets resultater svarer til indholdet af alle de krypterede stemmer der modtages under valgprocessen på valgtavlen.

System-sikkerhed

Valgystemet er bygget til at sikre anonymitet og stemmehemmelighed "by design". End-to-End kryptering i valgprocessen og mixing-processer ved resultatopgørelsen, sikrer vælgernes fulde anonymitet og stemmehemmelighed gennem hele valgprocessen.

Digital signatur

En indbygget "log ind procedure" baseret på digital signatur indeholder en verifikations-mekanisme der sikrer, at alle afgivne stemmer stammer fra stemmeberettigede. Yderligere bidrager den digital signatur til at sikre, at der ikke kan manipuleres med afgivne stemmer under valgprocessen.

End-to-End kryptering

En krypteringsprotokol sikrer, at det under ingen omstændigheder er muligt, at aflæse dele af resultatet, før valghandlingen er afsluttet, og de valgtilforordnede igangsætter valgafslutningsprocessen med dekryptering af stemmerne.

Mix-net

Gennem Mixing-protokollen brydes enhver forbindelse mellem vælgerens identitet og den afgivne stemme, og sikrer derved fuld anonymitet. Mixing-processen afholdes af flere uafhængige parter, og skal være korrekt færdiggjort før end det er muligt at påbegynde dekrypteringsprocessen af de registrerede stemmer.

Dokumentation

Valgsystemets komponenter bygger på matematisk beviste algoritmer og teknologier, der er tilgængelig for uvildig revision. Dokumentationen og brugen af open-source software er en central del af den universelle verifikation af valgsystemet.

Matematisk bevis

Alle de anvendte teknologier og systemopbygning er matematisk bevist og gennemgået af forskere.

Teknisk design

Detaljeret dokument over det tekniske design af Assembly Voting X løsningen.

Open-source software

Den anvendte open-source software der benyttes i Assembly Voting X er tilgængelig for revision på GitHub

ISAE3000

ISAE3000 er anvendt til revision af alle systemer og datahåndterings-processer i Assembly Voting

Assembly Voting ApS, Ringager 4C, 1. th., 2605 Brøndby, Danmark
Tel: 26169638 @: salg@aion.dk cvr: 25600665

4. ORDBOG

I det digitale valglokale er der en række aktiviteter og funktioner, der hver især bidrager til at sikre en korrekt afviklet valghandling. Nogle kendes fra det fysiske valglokale, mens andre er tilføjet for at sikre samme kontrolmuligheder og sikkerhed i det digitale valglokale.

Digital valgtilforordnet

Skal godkende valgopsætning og forsegle den digitale valgurne forud for valgets åbning.

Digital valgadministrator

Navngiven ansvarlig administrator for opsætning af valgsystem i overensstemmelse med valgregler.

Individuel verifikation

Funktioner i valgsystemet, der gør den enkelte vælger i stand til at kontrollere, at valgsystemet håndterer stemmeafgivelsen korrekt.

Mixing-proces

Teknologi til adskillelse af vælgerID og stemme forud for opgørelse af valgresultatet.

Stemmekontrol APP

En APP der kan hentes på App Store eller Google Play til vælgerkontrol af indhold af den stemme der krypteres i valgsystemet.

Stemmekvittering

Kvittering der modtages efter endt stemmeregistrering. Kvitteringen kan uploades på valgtavlen for at kontrollere at stemmen er korrekt registreret.

Universel verifikation

Funktioner og dokumentation der kan anvendes til generel kontrol med valgsystemet og valghandlingen. Fx kontrol af registreringer på valgtavlen.

Valgtavle

På en offentlig valgtavle registreres alle aktiviteter under valghandlingen. Valgtavlen anvendes til både individuel og universel verifikation af en korrekt afviklet valghandling.

Valgkontrol Applikation

De digitale valgtilforordnede anvender Valgkontrol Applikationen til at gennemføre valgåbnings- og valglukningsceremonien med.

Valgåbningsceremoni

Inden valget åbnes skal de digitale valgtilforordnede gennemføre valgåbningsceremonien, hvor de godkender valgopsætningen og deler dekrypteringsnøgler med hinanden så ingen har adgang til stemmer undervejs.

Valglukningsceremoni

Før valgresultatet gøres op skal de digitale valgtilforordnede logge på Valgkontrol Applikationen. Efterfølgende starter mixing-processen, dekryptering af stemmerne og resultat generering.