

05-04-2026

EaR introduction



Elections and Referendums

Indhold

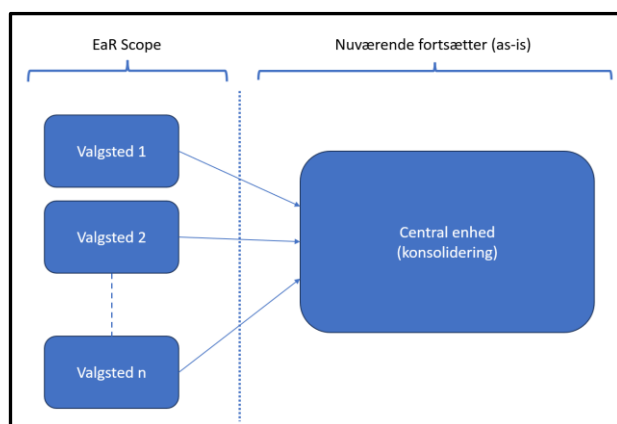
2. Introduktion	2
3. Systemoverblik	3
4. Forberedelses af valg	5
5. Afvikling af valg	6
5.1 Klargøring	6
5.3 Stemmeafgivning	8
5.4 Statusovervågning og sproguafhængighed	11
5.4 Afslutning og optælling	12
6. Mere om sikkerhed	14
7. Afsluttende bemærkninger	14

2. Introduktion

Nærværende dokumentets formål er at give en introduktion til EaR (Elections and Referendums) systemet. Systemets eneste formål er at effektiviserer optælling af stemmer på valgsteder efter valghandlingen er afsluttet. Denne effektivisering adresserer optællingshastighed, korrekthed i optælling samt rapportering af valgstedernes resultater til en central enhed der herefter foretager konsolideret optælling og evt. mandatfordeling for flere valgsteder.

EaR systemet kan samtidigt håndtere flere valg og valgtyper, som valg til folketing, kommuner, regioner, folkeafstemninger (indførelse af Euro, afskaffelse af retsforbeholdet) samt lokale afstemninger (f.eks. 'stop for Lynettholm byggeriet '). De ønskede valg kan konfigureres så de gennemføres i et for borgeren sammenhængende forløb.

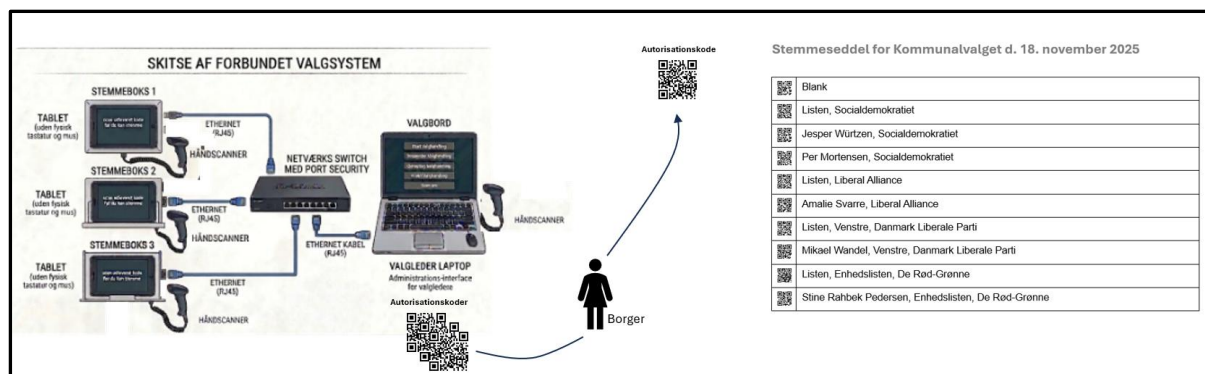
Som skitseret nedenfor omhandler EaR udelukkende valghandling på valgstederne med struktureret indrapportering af resultat fra hvert enkelt valgsted, hvor et typisk valgstedes resultat kan være optalt og klar til rapportering på mindre end et minut.



Dette dokument henvender sig primært til valgmyndigheder herunder bl.a. beslutningstagere, valgstyrere, valg tilforordnede samt IT-personel i stat, kommuner og regioner.

3. Systemoverblik

Fra et brugerperspektiv ser systemet således ud:



I skitsen ovenfor vises til venstre EaR's overordnede topologi, hvor systemet består af et valgbord hvorfra valghandlingen kontrolleres samt et antal stemmebokse, i eksemplet ovenfor er der tre stemmebokse. Såvel stemmebokse som valgbordet er alle udstyret med en håndscanner.

Det er et helt centralt sikkerhedselement at stemmebokse og valgbordet alle har deaktiveret al trådløs kommunikation (WIFI, Bluetooth, NFC). Stemmeboksene er derfor koblet til valgbordet via en traditionel netværks switch. Det anbefales at benytte en netværks switch der understøtter 'Port Security'.

Port Security er en mekanisme hvor man kan låse en given port på switchen til en bestemt computer og hvor ikke benyttede porte vil være deaktiveret.

Kombinationen af Port Security og deaktiveret trådløs kommunikation vanskeliggør i stor udstrækning cyberattacks og andre angreb fra eksterne netværk.

EaR systemet er baseret på at borgerne scanner QR-koder, interaktionen med systemets stemmebokse er udelukkende baseret på en håndscanner og en trykfølsom skærm, hvor der hverken er mus eller tastatur tilsluttet.

Inden hver valghandling er der en ekstern forberedelsesproces hvor valgstederne får tilsendt et antal QR autorisationskoder samt stemmesedler der er relevante for valgstedet (valgkredsen). Stemmesedlen viser lister og kandidater der kan stemmes på, men adskiller sig fra traditionelle stemmesedler ved at feltet til afkrydsning er afløst af en QR-kode udfor hver kandidat som borgeren skal scanne for at stemme på den pågældende kandidat.

QR autorisationskoderne udleveres til hver borger mens der ophænges en stemmeseddel i hver stemmeboks. Hvert valgsted modtager derfor et antal QR autorisationskoder der passer af antallet af valgstedets stemmeberettigede borgere. På samme måde modtager hvert valgsted det antal stemmesedler der passer til antallet af valgstedets digitale stemmebokse.

Nærværende notat forsøger at beskrive EaR systemets opbygning og virkemåde. Som det fremgår af beskrivelsen er EaR systemet afhængig af at få leveret QR autorisationskoder, Stemmesedler og er endvidere afhængig af forsvarlig håndtering af krypteringsnøgler og Excel password.

Hovedprogrammet **EaR.exe** benytter nedenstående syv støtteprogrammer. Disse syv programmer beskrives ikke yderligere i nærværende notat.

EarInitiator.exe, er 'master' programmet, der installeres på Valg Master PC'en. Det er dette program der genererer krypteringsnøglen og initierer de sikre USB nøgler der distribueres til valgstederne.

keyMgr.exe, der håndterer sikker distribution af krypteringsnøgler og Excel password. Programmet skal afvikles fra FIPS-140 Level-3 certificeret USB dongle

setupEaR.exe, er et program der håndterer installations og konfigurations procedure for valgbord og stemmebokse.

QRGenerator.exe, der danner og krypterer det ønskede antal QR autorisationskoder til et valgsted.

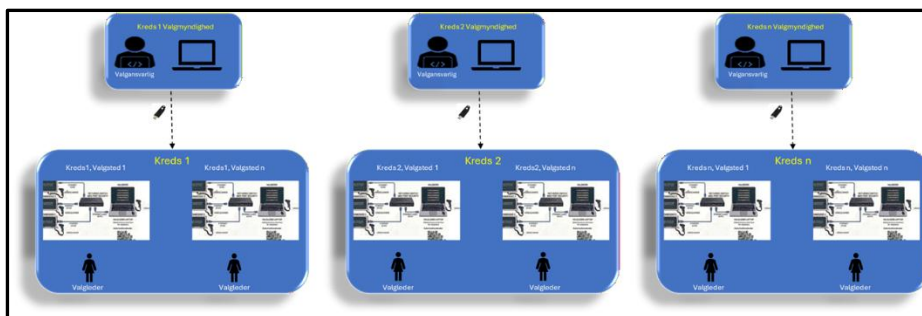
CandidateBuilder.exe, er et støtteprogram danner stemmesedler til valgstederne.

zint.exe, er et freeware program som er en del af Zint Barcode Studio der benyttes til programstyret dannelse af QR-koder.

dhcpsrv.exe, et freeware standardprogram (<https://www.dhcpserver.de/>) der installeres på valgbordet. Dette program er et standalone DHCP (Dynamic Host Configuration Protocol) program der sikrer at stemmebokse på et valgsted automatisk kan tildeles netværkskonfiguration uden valgstedet behøver at være forbundet til et åbent netværk. dhcpsrv.exe anbefales fordi det er simpelt og gratis, der findes andre muligheder.

4. Forberedelses af valg

Inden et valg skal de forskellige partier og kandidater registreres i systemet. Hver valgkreds har ansvar for kredsens setup. Man kan forestille sig et setup som skitseret nedenfor.



Den valgansvarlige har ansvar for at generere det nødvendige antal QR autorisationskoder til hvert valgsted med tilhørende positivliste.

Den ansvarlige for hver valgkreds har ansvar for at koordinere de enkelte partier leverer em kandidatliste med opstillingsrækkefølge eller sideordnet/alfabetisk, samt eventuelt et portrætfoto af kandidaterne.

Ved hjælp af støtteprogrammet Candidate Builder (CB.exe) registreres partier og kandidater i EaR-systemet. Den valgansvarlige kan vælge at delegerer CB.exe og dermed registreringen til de enkelte partier, der efter registrering returneres de registrerede kandidater med positivliste til den valgansvarlige, der lægger disse data ind i sin version af EaR.exe.

Den valgansvarlige skal herefter med programmet keyMgr.exe danne krypteringsnøgle samt opsætte konfigurationsparametre der er generelle for hvert valgsted.

keyMgr.exe kan kun afvikles fra en removable disk, hvor det anbefales at benytte en sikker USB-nøgle, f.eks. https://www.kingston.com/datasheets/IKD500S_us.pdf

På USB-nøglen findes nødvendige programmer og data. Herefter er man klar til at konfigurere de enkelte valgsteder.

Når hvert valgsted er teknisk/hardwaremæssigt klargjort vil personel fra den valgansvarliges kontor med den sikre USB-nøgle besøge valgstederne og med USB-nøglen initiere valgbord samt det antal stemmebokse der findes på det enkelte valgsted. Dette gøres ganske enkelt ved at isætte USB-nøglen og starte programmet setupEar.exe først for valgbordet, herefter for hver stemmeboks og herefter igen for valgbordet.

Dette installere EaR.exe på valgbord og stemmebokse, kopierer diverse filer med parametre og sprog samt installerer den dannede krypteringsnøgle, krypteret under TPM-chippen på henholdsvis valgbordet og stemmeboksene.

Proceduren sikrer at valgbord og stemmebokse kun kan kommunikere med hinanden.

5. Afvikling af valg

5.1 Klargøring

Valgbordet og stemmebokse klargøres med installation af program og konfigurationsfiler der matcher den aktuelle valghandling. Konfigurationsfilerne omfatter bl.a. positivlister for QR autorisationskoder og for de kandidater der kan stemmes på. Når en borger scanner en QR-kode tjekkes den scannede kode mod disse lister.

Det anbefales at stemmeboksene konfigureres til wake-on-lan, hvilket betyder at alle stemmebokse kan stå som slukkede og automatisk starte op, når de modtager en kommando fra valgbordet, hver stemmeboks bør være konfigureret til automatisk at starte EaR programmet ved opstart.

Ved opstart vil hver stemmeboks stå med en passiv skærm der viser teksten 'valghandlingen er ikke startet':



5.2 Identifikation og Adgang

Borgeren henvender sig på helt sædvanlig vis ved valgbordet og afleverer sit valgekort, hvorefter borgeren får udleveret en QR autorisationskode og får anvist en af de digitale stemmebokse. Her skal borgeren som det første scanne den udleverede QR autorisationskode, hvilket også vil fremgå af teksten på stemmeboksens skærm. Såfremt borgeren fejlagtigt starter med at scanne en kandidat vil EaR systemet opdage dette og guide borgeren til først at scanne den udleverede QR autorisationskode.

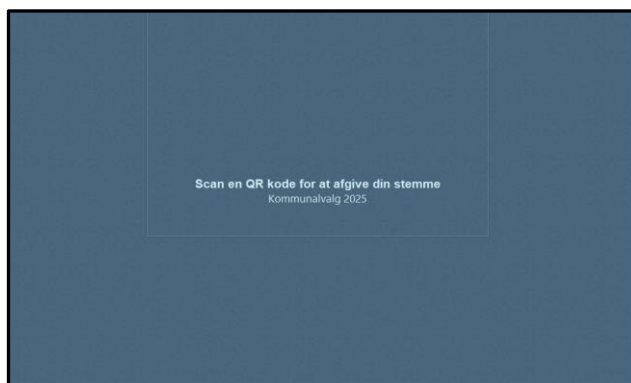
Fra valgbordet kan der sendes en start kommando til alle stemmebokse hvorefter hver stemmeboks viser teksten 'scan udleveret kode før du kan stemme':



Hermed er valghandlingen aktiv, og borgerne kan stemme.

5.3 Stemmeafgivning

Når den udleverede QR autorisationskode er scannet bliver borgeren præsenteret for denne skærm:



Herefter skal borgeren scanne QR-koden på stemmesedlen udfor det ønskede valg:

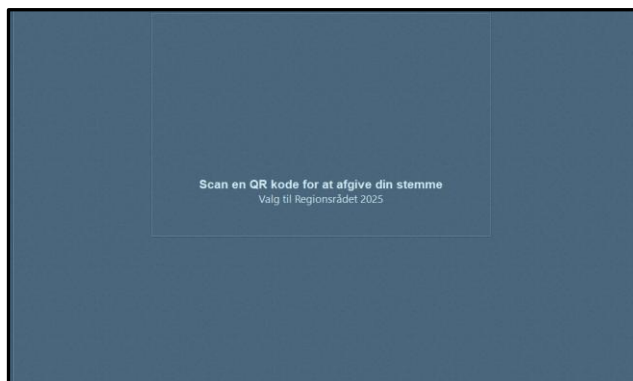


Hvis borgeren ønsker at afgive listestemme på Socialdemokratiet og scanner QR-koden udfor linjen med teksten: 'Listen, Socialdemokratiet' vises nu denne skærm som borgeren ska bekræfte:

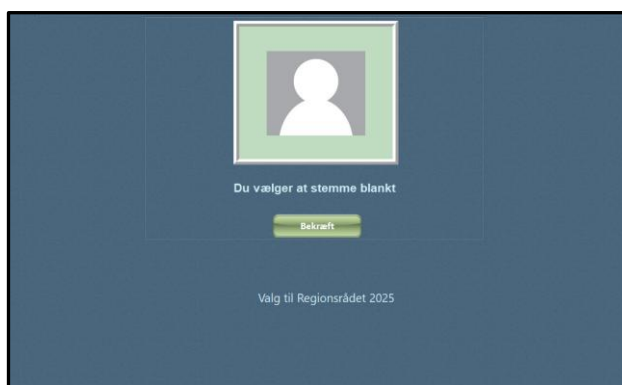


Såfremt borgeren på dette tidspunkt måtte ombestemme sig kan borgeren ganske enkelt blot scanne en QR-kode udfor den kandidat der ønskes i stedet – da vil et portrætfoto af kandidaten vises med navn og parti, dette valg kan borgeren da bekræfte ved med sin finger at trykke på den grønne 'Bekræft' knap.

Såfremt valghandlingen er konfigureret til at håndtere flere valg, som f.eks. valg til regionsrådet vil EaR systemet automatisk gå videre til denne valghandling og præsentere borgeren for denne skærm:



Til Regionsrådsvalget scanner borgeren QR-koden udfor 'Blank' og præsenteres for denne skærm:



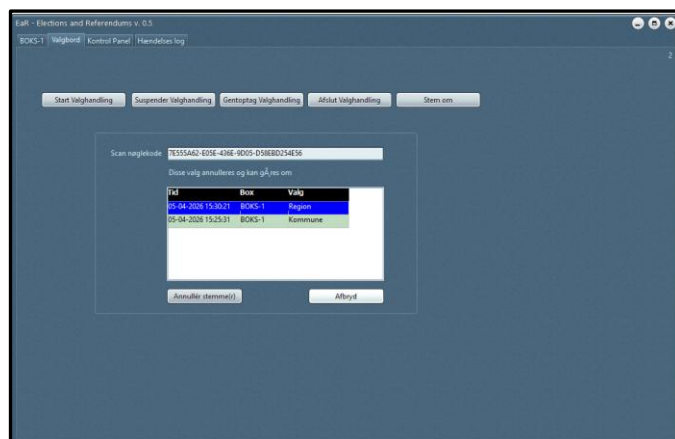
Når borgeren bekræfter sin blanke stemme præsenteres denne skærm:



Den pågældende borger har nu gennemført sit valg og kan forlade stemmeboksen. Efter få sekunder vender stemmeboksen tilbage til sin oprindelige tilstand hvor den viser teksten: 'scan udleveret kode før du kan stemme' og dermed er klar til næste borger

Der kan forekomme situationer hvor en borger fortryder sin afgivne stemme, i en sådan situation skal borgen henvende sig til valgbordet med sin udleverede QR autorisationskode. Den valgtilforordnede kan via en 'Stem Om' funktion scanne borgerens QR autorisationskode som da vil vise for hvilke valg borgeren har stemt men

ikke vise hvad der er stemt. Den valgtilforordnede kan da annullere stemmerne for QR autorisationskoden:

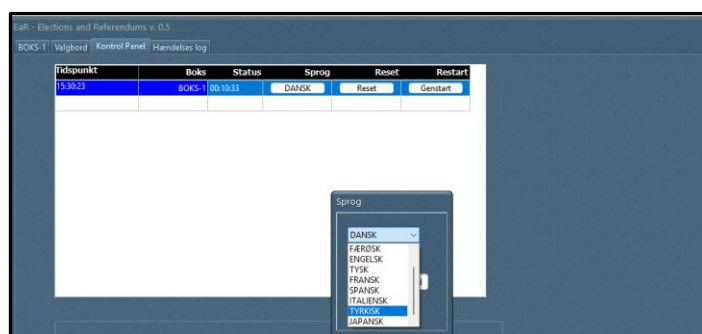


Hermed annulleres de ovenfor viste stemmer og borgeren kan gå tilbage i stemmeboksen og bruge den udleverede QR autorisationskode igen.

5.4 Statusovervågning og sproguafhængighed

En valgtilforordnet skal inden en ny borger lukkes ind i stemmeboksen tjekke status for den pågældende stemmeboks. Hvis den forrige borger har forladt stemmeboksen uden at have afgivet en eller flere stemmer skal den valgtilforordnede scanne sin QR-Reset kode som 'nulstiller' den pågældende stemmeboks. Herefter vil stemmeboksen igen vise teksten: 'scan udleveret kode før du kan stemme' og er dermed klar til næste borger.

Såfremt en borger der har anden etnisk baggrund ikke kan læse og forstå dansk, så kan man fra valgbordet ændre sproget i en given stemmeboks. F.eks. til tyrkisk:



I dette tilfælde vil borgeren i stemmeboksen da møde dette skærm billede:



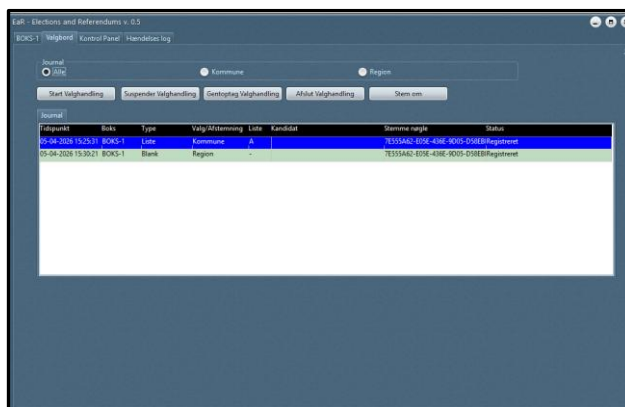
Efter gennemført valghandling vil sproget gå tilbage til at være standardsproget, i dette tilfælde dansk. Såfremt det ønskes er det muligt at fastholde tyrkisk som værende det gældende sprog for den pågældende stemmeboks.

Fra valgbordet er det ligeledes muligt at lukke ned for en stemmeboks.

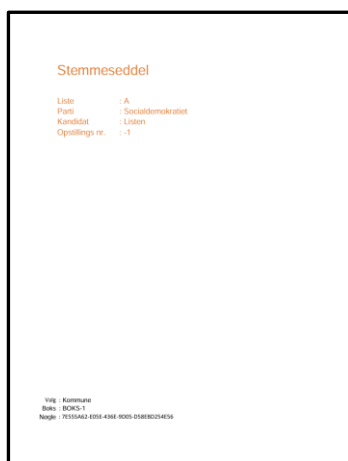
Det skal nævnes at valgbordet i udgangspunktet har sprogfiler til dansk og engelsk, det vil ikke være besværligt at konstruere sprogfiler til et hvilket som helst sprog, og dermed er EaR fuldt sprog agnostisk.

5.4 Afslutning og optælling

Fra valgbordet kan valglederen afslutte valghandlingen og får da vist en oversigt over de afgivne stemmer, hvor man umiddelbart kan få vist optælling fra de to valg 'Kommune' og 'Region':



Derudover er EaR indrettet til at dokumentere valgresultatet, dels ved en folder på skrivebordet der viser stemmesedler og skærmpoint dokumentation for hver enkelt afgivet stemme:



Bemærk at i bunden på såvel stemmeseddel som dokumenterende skærmpoint er der indsat at valg stempel der viser tidspunkt, stemmeboks og QR-autorisationskoden. Konstruktionen af dette stempel kan konfigureres, så hvis man føler angivelsen af tid og stemmeboks kan krænke borgerens anonymitet, så kan man i konfigurationsfilen blot angive at det kun er QR autorisationskoden der skal medtages.

I de situationer hvor en borger har stemt om dokumenteres de annullerede stemmer:

Stemmeseddel

Liste : A
Parti : Socialdemokratiet
Kandidat : Listen
Opstillings nr. : -1

Annuleret

Valg : Kommune
Boks : BOKS-1
Nogle : 7E555A62-E05E-436E-9D05-D58EBD254E56

EaR danner endvidere en Excel fil som er en journal over afgivne stemmer samt Excel filer for hvert valg der både indeholder optælling af liste- og personlige stemmer for det pågældende valgsted. Nedenfor vises eksempel på Excel rapport.

[illegible]

Stemmesedler, skærmpoint dokumentation, Excel filer samt en teknisk datafil der gør det muligt at rekonstruere hele valgproceduren på en anden PC, f.eks. hos en central valgmyndighed pakkes sammen i en krypteret zip filer der er password beskyttet og som ikke kan modificeres uden angivelse af det på gældende password.

6. Mere om sikkerhed

Tidligere i dette notat blev netværkssikkerheden beskrevet som 'air-gapped' uden forbindelsesmuligheder til eksterne systemer, dette er en del af den overordnede topologi.

Foruden netværkssikkerheden er al data krypteret, dette gælder for alle QR-koder, den tekniske datafil samt zip-filen med det komplette valgstedtsresultat. Ved valghandlingens afslutning dannes der på valgbordets skrivebord en folder med stemmesedler og skærmpoint dokumentation samt Excel filer – disse skal være tilgængelige for de valgtilforordnede og er derfor ikke krypteret.

QR-koder for stemmesedler har indlejret et distrikt-id, der kan opfattes som et valgkredsnummer, dette gør det muligt at frasortere QR-koder for stemmesedler fra andre kredse der via mobilt foto og SMS måtte være sendt til den stemmeafgivende borger fra en borger i en anden valgkreds.

De krypterede data er afhængig af tilgang til en krypteringsnøgle og den krypterede zip-fil er afhængig af tilgang til et password. Både krypteringsnøgle og password er centralt dannede og helt udenfor valgstedets kontrol. Tilgange beskyttes ved at man med et dedikeret key-management program fra en usb nøgle installerer krypteringsnøgle og password under valgbords computerens TPM-chip (Trusted Platform Module), der er en specialiseret chip på computerens bundkort, der er udviklet til at forbedre sikkerheden ved sikkert at gemme kryptografiske nøgler og passwords.

Den nuværende implementering der benytter en symmetrisk krypteringsalgoritme, bør det vurderes om denne kan udskiftes med asymmetrisk algoritme baseret på elliptiske kurver. Dette er ikke kritisk og kan være en vanskelig implementering, men brug af kryptering baseret på elliptiske kurver vil forbedre sikkerheden.

Alle hændelser logges i en hændelseslog der dokumenteres som en del af Excel filerne.

7. Afsluttende bemærkninger

Det skal understreges at den her beskrevne digitale valgprocedure uden gnidninger kan sameksistere med den eksisterende valgprocedure, hvor et begrænset antal stemmebokse kan være digitale mens alle øvrige stemmebokse er traditionelle.

Valget af håndscanner og QR-koder skyldes dels ønsket om at undgå intens bruger interaktion med stemmebokse, der uden scanner konceptet ville kræve navigering og indtastning, og dermed kræve stemmeboksene udstyret med mus og tastatur, hvilket giver ildesindede borgere bedre mulighed for at hacke systemet. Det vurderes endvidere at scanning af QR-koder for de fleste borgere er en velkendt øvelse, der f.eks. kendes fra MitID.

Det skal nævnes at hovedprogrammet er polymorf, hvor EaR.exe via specifikke konfigurations opsætninger både afvikles som valgbordet og som klientprogram i alle stemmebokse.

EaR.exe kan endvidere konfigureres til både at optræde som valgbord og stemmeboks. Dette kan være nyttigt hvis man ønsker at opsætte en isoleret trænings- og/eller demonstrations PC hvor borgere få vist hvordan det samlede system virker og selv øve sig inden borgeren beslutter sig for om der skal stemmes digitalt eller på traditionel vis.

Systemet har forsøgt at implementere mekanismer der griber fejlbetjening fra borgere og valgtilforordnede, med instruktion om den rette handling. Systemet har endvidere forsøgt at gardere sig bedst muligt mod diverse eksterne angreb. Disse systemer håndterer systemet automatisk med behørig logning af disse hændelser.

Der findes dog en situation der kræver valgtilforordnedes opmærksomhed. Denne situation opstår hvis en borger går ind i en stemmeboks og scanner den udleverede QR autorisationskode, for derefter at forlade stemmeboksen uden at afgive sin stemme. I denne situation står stemmeboksen åben så den næste borger vil have mulighed for direkte at afgive sin stemme og derefter scanne sin udleverede QR autorisationskode og stemme igen – denne borger kan altså stemme to gange.

Såfremt en valgtilforordnet opdager en borger har forladt stemmeboksen uden at stemme kan man fra valgbordet nulstille den pågældende stemmeboks, således den beder om at få scannet den udleverede kode.

