Assembly Voting findes i to primære versioner AVV1 Og AVV2, der opererer med 2 forskellige sikkerhedsnoveauer. Begges systemer er skrevet i Java og benytter JSF, Myfaces og Webbase. Systemerne hostes ved TDC Hosting i 3402.2 certificeret miljø med fokus på systemdokumentation, driftsafvikling, fysisk sikkerhed og sikkerhedskopiering. Læs mere om Assembly Voting valgsystemer.

Assembly Voting Version 1 (AVV1)
Bruges primært til afholdelse af vedtægtsbestemte valg i faglige organisationer og foreninger. Datatrafikken krypteres i såvel transaktion som lagring. Systemopsætningen er redundat, hvilket eliminerer risiko for datatab.

En stemme registreres i databasen som en relation imellem stemmeberettiget stemmeprofil og et valgalternativ. Anonymitet sikres efter et organiserende anonymitetsprincip, hvor systemleverandør via valgsystemet, alene har adgang til anonymiserede stemmeprofiler (randomiserede numeriske eller alfanumeriske koder). Valgkunde eller 3. part forestår udsendelse af gyldige valgkoder via personificerede valgkort til stemmeberettigede vælgere. Der er således organiseret adskillelse mellem valgliste med stemmeberettigede og stemmeregistrering i valgsystem.

Valgsystemet kan kun tilgås af godkendte navngivne personer i beskyttet miljø. For at øge tilgængeligheden kan AVV1 understøtte SMS som afstemningsmedie udover internet. Generelt kan man sige, at SMS reducerer ”sikkerheden” for anonymitet i valghandlingen. Det er koblingen i gateways mellem et anvendt telefonnummer og stemmeoplysningerne, der tilføjer en risikovariabel i relation til brud på anonymitet i stemmeafgivelsen.

Alle stemmemedier er i dette set up integreret i samme base. Dvs. man kan kun stemme afgive et gyldigt antal stemmer uanset medie. Det grundlæggende problem ved sms er at sikre fuld anonymitet på SMSgatewayen. I samarbejdet med gateway leverandør til Assembly Voting, er der udviklet en frakobling af stemmedata fra mobilnummer, så snart stemmen modtages. Så den medarbejder der håndterer gatewayen ikke har adgang til koblingen mellem tekststreng og telefonnummer. Assembly Voting oplyser om de tilknyttede problemstillinger ved SMS og IVR i relation til valghandlinger overfor valgkunder. Det er valgkundernes suveræne beslutning jf. valgvedtægter og tilknyttet valgbestyrelse / revision der beslutter hvilke afstemningsmedier, der skal være tilgængelige i den givne valghandling. Assembly Voting

Assembly Voting Version 2 (AVV2)
Bruges primært til højrisikovalg, fx lovbestemte valg. AVV2 er bygget op omkring asymmetrisk kryptering. En krypteringsnøgle består af 2 nøglehalvdele ofte kaldet ”den offentlige nøgle” og ”den private nøgle”. Den offentlige nøgle anvendes til at kryptere en tekst og kun den tilhørende private nøgle kan anvendes til dekryptering. Det kan udtrykkes lidt populært således: Med den offentlige nøgle kan man gemme en stemme i en forseglet kuvert. Seglet kan kun brydes hvis man har den private nøgle.

Implementering af stemmekryptering
I AVV2 er valgsystemet udvidet med et program, der installeres på en PC som ikke har netadgang. Denne PC benævnes resultatPC. På resultatPC’en generes et nøglesæt og den offentlige nøgle overføres manuelt til valgserveren, den private nøgle bliver på resultatPC’en. Når en vælger logger ind på valgserveren for at stemme overføres hele opstillingslisten og den offentlige nøgle til vælgerens PC, stemme dialogen inkl. navigering imellem valglister sker lokalt, når vælgeren har afgivet og bekræftet sin stemme krypteres denne med en offentlige nøgle og kryptogrammet sendes til valgserveren. Man kan bruge analogien, at stemmen lægges i en kuvert og forsegles.

Den krypterede stemme gemmes i databasen, relationen i databasen imellem stemmen og kandidaten etableres ikke. Dvs. personale med fuld databaseadgang kan i dette system se, at en stemmeprofil har stemt, men ikke hvad der stemt på profilen. Så selv om man skulle have adgang til den fulde udsendingsbase, vil man stadig ikke kunne tilbageføre afgivne stemmer til enkeltpersoner.

Når valget er afsluttet dannes en liste, som indeholder alle kryptogrammer, listen omordnes automatisk således sekvensen af kryptogrammerne ikke kan relateres til en sekvens af vælgerne i databasen. Denne

liste overføres manuelt til resultatPCen. ResultatPCen dekrypterer kryptogrammerne med anvendelse af den private nøgle og danner en valgbog med resultatet. Valgbogen kan printes direkte eller bæres tilbage til valgserveren.

Option: Netadgang fra resultatPC
Man kan lette processen hvis man giver resultatPC'en netadgang, dataoverførelsen imellem resultatPC'en og valgserveren kan ske direkte fra resultatPC'en. Dette svækker ikke sikkerheden i løsningen væsentligt, men gør argumentationen for sikkerheden lidt svagere idet man skal argumentere for at resultatPC'en ikke kan blive inficeret med malware som kan eksponere den private nøgle for tredje part.