Dato: 7. september 2021

Opsummering fra efterfølgende dialogmøder

Domstolsstyrelsen forbereder udbuddet af kontrakt vedrørende drift og vedligeholdelse af Domstolsstyrelsens it-infrastruktur.

Domstolsstyrelsen har etableret et projekt (driftsudbudsprojektet) til håndtering af udbuddet. Projektet blev startet i december 2020, og følger statens IT projektmodels faser. Som en del af analysefasen blev der i marts 2021 afholdt indledende dialogmøder med potentielle leverandører med henblik på en generel afdækning af markedet ift. nye teknologier, ydelser mv.

Efterfølgende afholdt Domsstolsstyrelsen et informationsmøde for potentielle leverandører.

I juni 2021 afholdt Domstolsstyrelsen efterfølgende dialogmøder med potentielle leverandører med henblik på en mere konkretiseret dialog med relevante virksomheder om de i udbudssystemet oplyste, udvalgte temaer.

Nærværende notat indeholder en opsummering af de indkomne svar på de udvalgte temaer.

For at sikre en ligebehandling, blev der anvendt samme dagsorden til alle de efterfølgende dialogmøder.

De udvalgte temaer og spørgsmål dertil var som følger:

1. DevOps – implementering af processer, værktøjer og roller (både skriftligt og på mødet)
Baggrund Kunden har en række applikationsleverandører og ønsker at foretage automatiseret deployment via. release pipelines.
Spørgsmål 1.1. Hvilke roller er relevante at supplere den eksisterende organisation med for at opnå en effektiv understøttelse af det beskrevne DevOps set up? 1.2. Hvilke yderligere eller nye værktøjer hos driftsleverandøren, udviklingsleverandøren eller kunden er relevante at stille krav til for at sikre optimal understøttelse af det eksisterende DevOps set up? 1.3. Hvordan sikres der en optimal DevOps governance og samarbejde i multi-leverandør set up? 1.4. Hvordan sikres der en optimal DevOps governance i kombination med ITIL? 1.5. Hvordan sikres der optimal implementering af DevSecOps? 1.6. Hvordan sikres optimal 1) continuous deployment and release eller 2) continuous deployment og continuous release on demand, herunder i et multi-leverandør set up?

2. Sikkerhed (primært skriftligt)
Baggrund Den kommende kontrakt vil omfatte en række krav til informationssikkerhed.
Spørgsmål: 2.1 Leverandøren skal i relation til Kontraktens opfyldelse som udgangspunkt benytte fler-faktor autentifikation ifm. adgangen til Systemet. Hvad er jeres erfaringer med den form for autentifikation? 2.2 Hvordan vil I stille jer i forhold til et krav om at datacentre skal være certificeret som eller leve op til minimum Tier 3, jf. Uptime Institute.

2.3 Sikkerhedstesten, som udføres af Kunden, omfatter bl.a. sårbarhedsscanning.
Er der prisforskel på tilkøb af sårbarhedsscanning som option henholdsvis som en fast del af kontrakten?
Hvordan vil I anbefale, vi tilrettelægger ønsket om sårbarhedsscanningsservice i udbuddet.

2.4 Hvordan håndterer I diagnostics og hvordan sikrer I, at I har overblik over og dokumentation for fremsendelse af diagnostics og lignende data fra infrastrukturen til tredjeparter, herunder i tredjelande?
I skal være opmærksomme på, at vores generelle sikkerhedskrav om dataminimering, risikovurdering, tredjelandsoverførsler mv. tilsvarende finder anvendelse på diagnostics og lignende data fra infrastrukturen. Har I bemærkninger hertil?

2.5 I forbindelse med redundans, bedes det oplyst, om det er muligt at overholde et afstandskrav på mindst 25 km. mellem hvert af 3 driftscentre? Spørgsmål 2.5 er et eftersendt spørgsmål med svarfrist til 25. juni 2021, kl. 16:00

3. Vederlag og SLA (primært skriftligt, punkt 3.2, 3.3 og 3.4 dog både skriftligt og på mødet)

Spørgsmål:

3.1 Hvad er jeres erfaringer med effektivisering af driftsydelsen? Hvordan påvirker en sådan effektivisering prisen?
Vil I acceptere årlig effektiviseringsprocent, hvor prisen for drift falder med den anførte procent?
Hvilken procent vil være realistisk i forhold til markedsudviklingen?

3.2 Under hvilke forudsætninger vil I acceptere fordeling af vederlaget for transitionsfasen som en del af driftsvederlaget i kontraktens bindingsperiode?

3.3 Hvilken betydning har bindingsperioden i kontrakten for prisen?

3.4 Under hvilke forudsætninger vil forpligtige jer på SLA og bodsbetaling, hvis ikke deploy til infrastrukturen formelt godkendes af driftsleverandøren?

3.5 Vil et valg af et eller flere applikationsmonitoreringsværktøjer (f.eks. AppDynamics fra DSS' side samt krav om at driftsleverandøren overvåger disse være en prisdriver?

3.6 Hvis DSS ønsker mulighed for selv at have adgang til og mulighed for at lave ændringer direkte på infrastruktur, herunder servere og i DB, vil det have konsekvenser i forhold til overholdelse af SLA og pris?

3.7 Hvilken rapportering understøtter erfaringsmæssigt på bedste vis kundens indsigt i kvaliteten af ydelserne?
Hvilke værktøjer anvender I for at sikre størst mulig indsigt på en overskuelig måde?

4. Transition Ind (primært skriftligt)

Baggrund

Det er vigtigt for Domstolsstyrelsen, at transitionen sker korrekt og rettidigt. I den første dialogrunde modtog vi input om, at transitionen kan gennemføres på fra mellem 4-6 måneder og 12 måneder.

Spørgsmål

4.1 Er det realistisk at gennemføre en transition på 4-6 måneder?
Hvad mener I er realistisk?

4.2 Hvilken dokumentation har I som tilbudsgivere brug for fra udviklings- og vedligeholdelsesleverandører for at gennemføre transitionen korrekt og rettidigt?

4.3 Hvilken dokumentation har I som Leverandør brug for fra udviklings- og vedligeholdelsesleverandører for at kunne prissætte ydelserne?

4.4 Hvilke nøglepersoner fra kundens og leverandørens side har I erfaringer med er væsentlige at deltage i transitionen.

5. Transformation (både skriftligt og på mødet)

Baggrund

Domstolsstyrelsen har overvejelser om transformationsydelser.

Spørgsmål

5.1 Hvad kræver det erfaringsmæssigt at overgå fra drift, der er on premise til IaaS, herunder serverless computing – containers?

5.2 Segmentering af netværk.

- Hvad skal der til for at opfylde et sådant krav
- Hvilken forskel vil det gøre, hvis det foretages som en transformationsydelse under transitionen?
- Hvilke risici vil det indebære?
- Vil det have betydning for længden af transitionen?

Opsummering af punkt 1: DevOps – implementering af processer, værktøjer og roller
Nedenfor er givet en opsummering på spørgsmålene under dette punkt.

1.1.Hvilke roller er relevante at supplere den eksisterende organisation med for at opnå en effektiv understøttelse af det beskrevne DevOps set up?
Det generelle svar var, at de nødvendige roller skal aftales konkret mellem kunden, driftsleverandøren og kundens applikationsleverandører.

Der er enighed om at følgende roller er essentielle på kundesiden (eller for nogle roller indsourcet fra applikationsleverandør).:

- Product Owner
- Scrum Master
- Sikkerhedsansvarlig og/eller DevSecOps engineer
- Release manager
- DevOps engineer
- Automation architect (hvis der skal arbejdes med continuous deployment)

1.2. Hvilke yderligere eller nye værktøjer hos driftsleverandøren, udviklingsleverandøren eller kunden er relevante at stille krav til for at sikre optimal understøttelse af det eksisterende DevOps set up?
Det generelle svar var, at DevOps handler mest om mindset og kultur. Det er vigtigt, at kunden tager ejerskab på processerne og det valgte tekniske setup. Alle applikationsleverandører skal bruge samme tekniske setup med driftsleverandøren of de samme processer.

Der blev nævnt en del konkrete værktøjer til de enkelte delprocesser i et agilt leverance setup.

Generelt var der enighed om, at infrastructure as a code er fremtiden, men også en del forbehold i forhold til omlægningen af legacy systemer.

1.3.Hvordan sikres der en optimal DevOps governance og samarbejde i multi-leverandør set up?
Multileverandør setup strider generelt mod idéerne bag DevOps. Der er vigtigt at kunden tager ejerskab på alle værktøjer og alle processer. Kunden skal tage skal tage ansvar for at formidle samarbejdet mellem drifts- og applikationsleverandørerne.

Større fokus på kvalitetssikring af kode og færdig software.

1.4 Hvordan sikres der en optimal DevOps governance i kombination med ITIL?
Der er ingen modsætninger med DevOps og ITIL. ITIL 4 er tilpasset en mere agil verden.

1.5.Hvordan sikres der optimal implementering af DevSecOps?
Der anbefales en shift left strategi, hvor sikkerhed adresseres i alle led af processerne og så tidligt som muligt. Der skal anvendes de rette værktøjer til scanning af kode og sårbarhedsscanninger.

1.6 Hvordan sikres optimal? 1) continuous deployment and release eller 2) continuous deployment og continuous release on demand, herunder i et multi-leverandør set up?
Arbejdet med at definere og opsætte kontroller i forhold til continuos deplyment er stort. Det skal derfor overvejes hvor det giver værdi. Mange har continuos deployment til testmiljøer - meget få har det til produktionsmiljøer.

Opsummering af punkt 2: Sikkerhed
Nedenfor er givet en opsummering på spørgsmålene under dette punkt.

2.1 Leverandøren skal i relation til Kontraktens opfyldelse som udgangspunkt benytte fler-faktor autentifikation ifm. adgangen til Systemet. Hvad er jeres erfaringer med den form for autentifikation?
MFA er standard hos alle leverandører. De fleste kan understøtte en bred palette af MFA-løsninger i markedet.

2.2 Hvordan vil I stille jer i forhold til et krav om at datacentre skal være certificeret som eller leve op til minimum Tier 3, jf. Uptime Institute.
Krav om Tier 3 certificerede driftscentre vil være en udfordring for de fleste leverandører. Flere vil have behov for at benytte underleverandører eller udenlandske enheder for at leve op til dette krav.

2.3 Sikkerhedstesten, som udføres af Kunden, omfatter bl.a. sårbarhedsscanning. Er der prisforskel på tilkøb af sårbarhedsscanning som option henholdsvis som en fast del af kontrakten? Hvordan vil I anbefale, vi tilrettelægger ønsket om sårbarhedsscanningsservice i udbuddet?
Den generelle anbefaling var, at sårbarhedscanninger skal udføres og bør være en del af den faste kontrakt.

2.4 Hvordan håndterer I diagnostics og hvordan sikrer I, at I har overblik over og dokumentation for fremsendelse af diagnostics og lignende data fra infrastrukturen til tredjeparter, herunder i tredjelande?
Leverandørerne vil generelt sikre, at data kun kan tilgås af personale, der er sikkerhedsgodkendt af kunden. Data vil ikke blive overført til 3. lande. Flere leverandører vil kunne tilbyde kun at benytte dansk personale.
Anbefalingen er, at kunden er meget tydelig i sine krav på dette område f.eks. til SIEM og logning.

2.5 I forbindelse med redundans, bedes det oplyst, om det er muligt at overholde et afstandskrav på mindst 25 km. mellem hvert af 3 driftscentre? Spørgsmål 2.5 er et eftersendt spørgsmål med svarfrist til 25. juni 2021, kl. 16:00
Leverandørerne opfatter generelt dette som en forældet måde at anskue verdenen på. Kravet vil få flere af byderne til at afstå fra at byde, og resten vil skulle bruge datacentre i andre EU lande for at leve op til kravet.

Flere leverandører nævner, at de ikke ønsker så lang afstand mellem deres datacentre pga. latency.

Opsummering af punkt 3: Vederlag og SLA
Nedenfor er givet en opsummering på spørgsmålene under dette punkt.

3.1 Hvad er jeres erfaringer med effektivisering af driftsydelsen? Hvordan påvirker en sådan effektivisering prisen? Hvilken procent vil være realistisk i forhold til markedsudviklingen? Vil I acceptere årlig effektiviseringsprocent, hvor prisen for drift falder med den anførte procent?
Den generelle anbefaling var enten at bruge et indeks (F.eks. Zangenbergs) eller at fastsætte en fast sats, som den løbende driftsbetaling reduceres med pr. år. Der var meget forskellige bud på hvor stor en årlig reduktion der burde kunne opnås (2-8 %).

Et par af leverandørerne nævner at effektiviseringen bliver størst, hvis kunden giver leverandøren fuld design autoritet i forhold til drifts setup'et (dvs. ingen krav om egen eller dedikeret hardware og ingen krav til specifikke navngivne løsninger).

3.2 Under hvilke forudsætninger vil I acceptere fordeling af vederlaget for transitionsfasen som en del af driftsvederlaget i kontraktens bindingsperiode?
De fleste leverandører vil acceptere, at transitionsomkostningerne opkræves som en del af den løbende driftsbetaling. Der vil dog være en omkostning på dette, da leverandører foretrækker en aftale der er neutral i forhold til deres kapitalbinding.

3.3 Hvilken betydning har bindingsperioden i kontrakten for prisen?
Gennemsnittet af anbefalingerne fra leverandørerne var en bindingsperiode på 4-6 år, med optioner på forlængelse. Flere leverandører begrundede ønsket om en bindingsperiode med afskrivninger på indkøbt hardware.

Hvis kunden ikke ønsker en bindingsperiode på 4-6 år, bør kontrakten indeholde udtrædelsesbestemmelser, der kompenserer leverandørerne for de udgifter de ikke kan få dækket på anden måde i den resterende kontraktperiode.

Flere leverandører nævner også, at der vil være forskel i forhold til om, der kræves dedikeret hardware eller ikke. Kræves der dedikeret hardware bør det følges op med en bindingsperiode på 4-6 år. Generelt går markedet mod længere kontrakter og ofte med lange bindingsperioder.

3.4 Under hvilke forudsætninger vil I forpligtige jer på SLA og bodsbetaling, hvis ikke deploy til infrastrukturen formelt godkendes af driftsleverandøren?
Deploy til servere og andre changes skal overholde de aftalte change og releaseprocedurer. Det udelukker ikke at deploy til miljøer kan automatiseres i et DevOps setup, idet kvalitetssikringen er indbygget i processen.

Hvis kunden ønsker at kunne deployere kode uden om de aftalte change og releaseprocedurer, så vil leverandørerne ikke bindes af bod i forhold til de fejl dette vil kunne medføre. Det vil være kunden der skal løfte byrden med at dokumentere at de ikke var årsag til en evt. fejl.

Det kan blive svært at opretholde bod som et styringsredskab, hvis kunden ikke vil bindes af aftaler om change og releaseprocedurer.

3.5 Vil et valg af et eller flere applikationsmonitorerings-værktøjer (f.eks. AppDynamics fra DSS' side samt krav om at driftsleverandøren overvåger disse være en prisdriver?
Alle leverandørerne vil kunne drive og overvåge applikationerne i det værktøj kunden måtte ønske. Der er dog en klar anbefaling til at anvende det/de værktøjer leverandøren i forvejen anvender.

3.6 Hvis DSS ønsker mulighed for selv at have adgang til og mulighed for at lave ændringer direkte på infrastruktur, herunder servere og i DB, vil det have konsekvenser i forhold til overholdelse af SLA og pris?
Generelt var leverandører lidt uforstående overfor dette behov, men mener at det kan løses. De fleste leverandører vil gerne give admin rettigheder til databaser og lignende adgange, men vil ikke give adgange til core services, da disse ofte er delte med andre kunder.

Leverandører vil sikre sig mod at en handling udført af en af kundens medarbejdere kan udløse en bodsbetaling fra leverandøren. Det kan derfor være en udfordring at opretholde bod som et styringsredskab. Behovet skal være nøjagtigt specificeret i udbuddet. Der vil formentligt være en merpris for dette, men det afhænger af hvilke adgange og rettigheder kunden vil have.

3.7 Hvilken rapportering understøtter erfaringsmæssigt på bedste vis kundens indsigt i kvaliteten af ydelserne? Hvilke værktøjer anvender I for at sikre størst mulig indsigt på en overskuelig måde?
Alle leverandørerne lægger vægt på, at overvågning og rapportering i størst muligt omfang standardiseres og automatiseres og følger de processer leverandøren i forvejen bruger.

Skal der benyttes kundespecifikke værktøjer, vil der være en ekstra pris for dette.

Leverandørerne mener sig generelt set i stand til at levere overvågning og rapportering på de KPI'er kunden måtte stille krav om.

Opsummering af punkt 4: Transition Ind
Nedenfor er givet en opsummering på spørgsmålene under dette punkt.

4.1 Er det realistisk at gennemføre en transition på 4-6 måneder? Hvad mener I er realistisk?
Der blev fremhævet en del parametre, som alle har betydning for hvor lang en transitionsperiode vil være:

- Kvalitet af dokumentationen
- Kundens mulighed for at stille med tilstrækkelige og rette ressourcer
- Den afgivende leverandørs vilje til at spille positivt med og kundens evner til at styre samarbejdet
- Teknisk kompleksitet i det nuværende drifts setup
- Skal der udføres transformation i forbindelse med transition?
- Faktorer hos kundens andre leverandører (f.eks. leverandøren af fiberforbindelser)

Generelt anbefales at opdele transitionen i et antal bølger. Jo mere tid der er til transition - desto flere bølger kan der opdeles i. Jo flere bølger - desto lavere forretningsmæssig risiko for kunden.

De fleste bud for længden af transition lå på 2-3 måneder afklaringsfase og 6-9 måneder til at gennemføre transitionen. Meget afhænger af hastigheden i vidensoverdragelsen til den nye leverandør.

4.2 Hvilken dokumentation har I som tilbudsgivere brug for fra udviklings- og vedligeholdelsesleverandører for at gennemføre transitionen korrekt og rettidigt?
Leverandøren skal have adgang til alt materiale der har betydning for at kunne vurdere omfanget og størrelsen på opgaven. Det kan f.eks. være:

- CMDB-oplysninger (se skriftlige besvarelser)
- Nuværende lokationer og netværk til disse
- Oplysninger om netværksudstyr der skal driftes, vedligeholdelsesaftaler, udløb af serviceaftaler og specifikke teknologiske forhold
- Oplysninger om kundens system og applikationslandskab - flows og sammenhænge. Både lister og tegninger. Oplysninger om indbyrdes afhængigheder
- Generel teknisk indsigt i kundens og nuværende leverandørs infrastruktur
- Hvilke applikationer ligger på hvilke servere. Hvilke services og shared services samt databaser på andre servere kan applikationen tilgå
- Krav om dedikeret hardware
- Krav om brug af navngivne løsninger
- Krav om drift af hardware ejet af kunden
- Krav til leverandørens datacentre
- Særlige lovgivningsmæssige eller sikkerhedsmæssige krav
- Driftsvejledninger og instrukser
- Oplysninger om certifikater og adgange

- Hvilken adgang og rettigheder skal kundens eller kundens 3.parts leverandører have?
- Driftsplan/schedule fra nuværende leverandør
- Tegninger om kundens datanetværk
- Offentlige ip-adresser og portering af disse
- Kan ny leverandør få adgang til nuværende hypervisor?
- Kundens forventninger til nedetid og servicevinduer (fordelt på systemer og applikationer)
- Nuværende regler for patchning af servere (inkl. hvornår, rækkefølge og hvilke ændringer der kan forekomme)
- Hvad skal overvåges (ikke udtømmende)?
    - Applikationer
    - Netværk og komponenter
    - Servere og middelware
    - Ønsker til yderligere overvågning i fremtiden
    - Nuværende overvågningsteknologi
- Nuværende backuppolitik + ønsker til ændringer
- Oplysninger om licenser, forbrug og ejerskab
- *Processer og forretningsgange der overdrages til leverandøren
- Liste med kontaktpersoner og leverandører
- Eksisterende 3. parts kontrakter og aftaler med leverandører der skal videreføres under ny drifts-leverandør
- Arkitektoniske designdokumenter for drifts setup
- Adgang til kildekoden for systemer

4.3 Hvilken dokumentation har I som tilbudsgivere brug for fra udviklings- og vedligeholdelsesleverandører for at kunne prissætte ydelserne?
Det er vigtigt at systemer/applikationer og det nuværende driftsmæssige setup er veldokumenteret. Jo mere specifik og nøjagtig dokumentation kunden kan levere, desto bedre tilbud vil kunden kunne forvente at modtage, og jo færre mulige tvister vil der opstå under transitionen.

Spørgsmål/svar perioder og forhandling kan være med til udrydde tvivlsspørgsmål undervejs i udbuddet.

4.4 Hvilke nøglepersoner fra kundens og leverandørens side har I erfaringer med er væsentlige at deltage i transitionen. Vigtigste anbefaling er, at kunden på alle niveauer tager ansvar for gennemførelsen af transitionen. Det må ikke være op til den afgivende og den modtagende leverandør at aftale og gennemføre transitionen.

Følgende kompetencer skal bruges både hos kunde, afgivende leverandør og modtagende leverandør:
- Transitionsleder/projektleder
- Arkitekt
- Friftsleder
- Subject matter experts
- Testmanager + testere

Særligt hos kunden:
- Product Owners, der er beslutningskompetente

Opsummering af punkt 5: Transformation
Nedenfor er givet en opsummering på spørgsmålene under dette punkt.

5.1 Hvad kræver det erfaringsmæssigt at overgå fra drift, der er on premise til IaaS, herunder serverless computing – containers?
Den klare anbefaling er ikke at gennemføre dette i forbindelse med transitionen, men efterfølgende når transitionen er godkendt og driftsprøven gennemført.

De fleste leverandører anbefaler at gennemføre en omlægning af driften fra on premise drift til serverless computing i 2 trin.

1. Omlægning fra On premise til IAAS (forbrugsafregnet drift)
2. Omlægning og refactorering af systemet til drift i et serverless computing setup.

Det er vigtigt at systemet er veldokumenteret, at kunden tager ejerskab på omlægningen og kan stille ressourcer (product owner) der kan tegne forretningen, at der er opmærksomhed på systemets restlevetid - det er nemt at investere for meget i denne omlægning

5.2 Segmentering af netværk. Hvad skal der til for at opfylde et sådant krav. Hvilken forskel vil det gøre, hvis det foretages som en transformations-ydelse under transitionen? Hvilke risici vil det indebære? Vil det have betydning for længden af transitionen?

Anbefalingen til kunden er ikke at gennemføre transformation samtidigt med transition. Det forøger transitionsprojektets tekniske og kommercielle risici for meget.

Både generel segmentering og mikrosegmentering af netværket anbefales - men først efter transitionen.