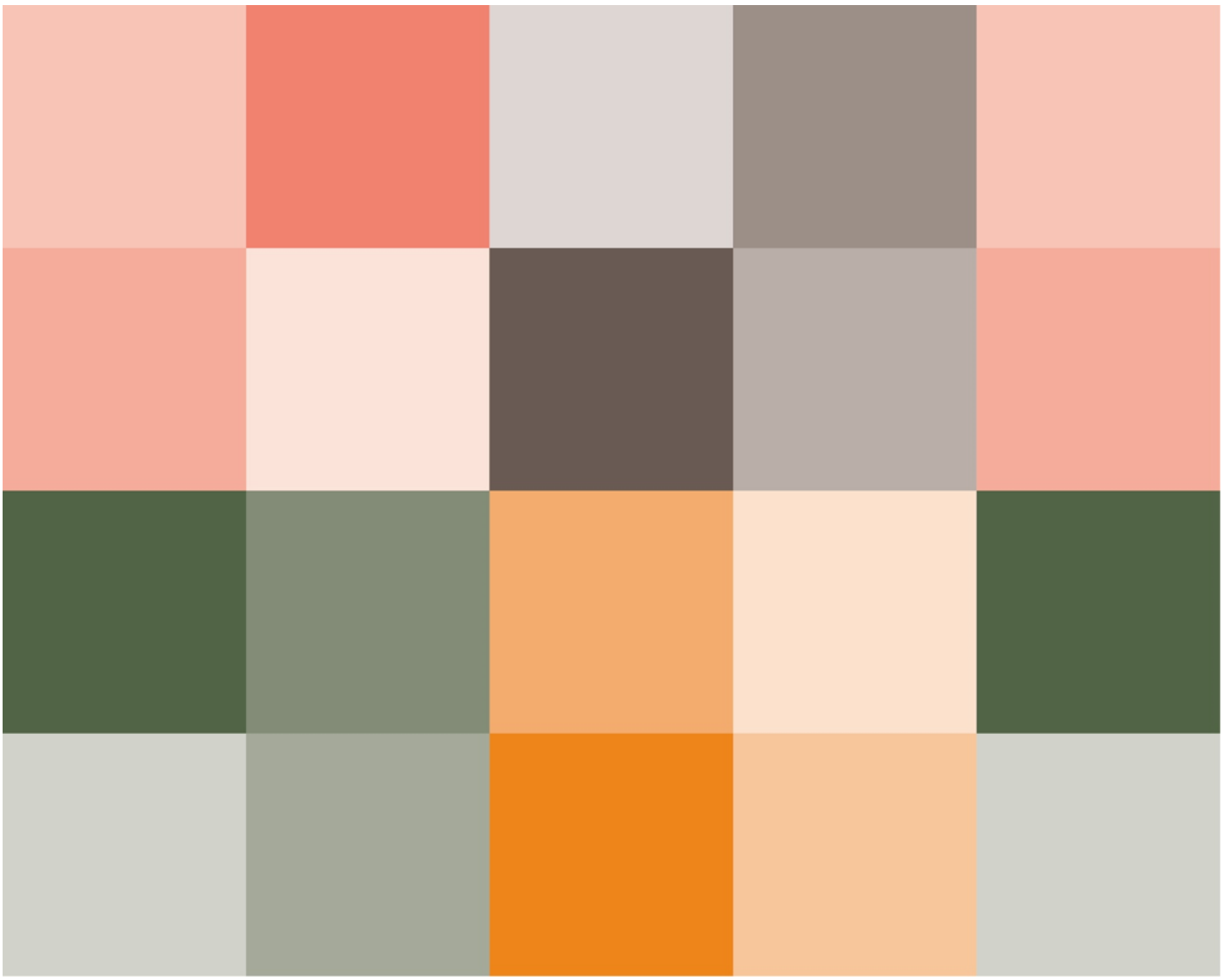


Bilaga 1 – Teknisk fördjupning

En beskrivning av lösningen för det tekniska systemet för bevisutbyte

Datum: 2024-12-11

Diarienummer: 2024–2183

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Innehållsförteckning

1 Inledning

I denna bilaga beskrivs detaljerna i det tekniska systemet för bevisutbyte mer ingående än i huvudrapporten. För ytterligare fördjupning om de olika komponenterna, arkitektoniska beskrivningar och mer information om behöriga myndigheters anslutning hänvisas till Diggs webbplats[1] och Github[2]. Se huvudrapporten för förslag om ansvarsfördelning för de olika delarna.

Avsnitt 2 beskriver de svenska och de EU-gemensamma komponenterna som det tekniska systemet består av. Avsnitt 3 beskriver de krav som finns på loggning.

Begrepp och förkortningar är desamma som i huvudrapporten.

2 Komponenter i det tekniska systemet

I detta avsnitt beskrivs de komponenter som ingår i det tekniska systemet. Det tekniska systemet ska bestå av de delar som listas i art. 2 i genomförandeförordningen och förtydligas i de tekniska designdokumenten[3] som revideras löpande av kommissionen och medlemsstaterna i undergruppen OOTS Specifications. Varje medlemsstat har tagit fram nationella lösningsarkitekturer och har gjort olika vägval, så även Sverige. EU-kommissionens beskrivningar av nationella komponenter i det tekniska systemet överensstämmer därmed inte helt med den svenska nationella arkitekturen, då vi har anpassat vår lösning utifrån våra nationella förhållanden och förutsättningar.

2.1 EU-gemensamma komponenter

För att det ska vara möjligt att koppla ihop behöriga myndigheter i EU:s medlemsstater består den EU-gemensamma arkitekturen av befintliga EU-byggblock som återanvänts för att maximera interoperabilitet och kostnadseffektivitet. eIDAS och eDelivery är två exempel på befintliga EU-byggblock som används och som är en förutsättning för att medlemsstaterna ska uppfylla art. 2 e och f genomförandeförordningen.

I den EU-gemensamma arkitekturen ingår utöver EU-byggblocken de EU-gemensamma tjänsterna (art. 2 g genomförandeförordningen) som består av en bevismäklare, en datatjänstekatalog och ett semantiskt register. Tjänsterna används för att slå upp vilka bevis som finns och var de kan hittas. Informationen behövs för att kunna skapa korrekta bevisförfrågningar. Det framgår av art. 4.2 ibid. att de bevislämnande parternas datatjänster (här kallade bevistjänster) ska registreras. Det pågår en diskussion mellan EU-kommissionen och medlemsstaterna om även information om de bevisbegärande parternas förfaranden och vilka bevis som begärs i dem ska registreras.

---

[1] https://www.digg.se/sdg

[2] https://github.com/diggsweden/sdg-intermediation-se och https://github.com/diggsweden/sdg-intermediation-eu

[3] https://ec.europa.eu/digital-building-blocks/sites/display/OOTS/Technical+Design+Documents

2.2 Nationella komponenter

Sveriges lösningsstrategi för det tekniska systemet bygger på att Digg ansvarar för ett antal förvaltningsgemensamma komponenter som svenska behöriga myndigheter kan ansluta till. De komponenter som ingår i den nationella lösningen för anslutning till det tekniska systemet listas här nedan och beskrivs i kommande avsnitt.

- Åtkomstpunkt för eDelivery (OOTS-nod)
- Auktorisationstjänst och svensk eIDAS-nod
- Förhandsgranskningstjänst
- Uppslag och bevishämtning

Utöver de förvaltningsgemensamma komponenterna är de bevisbegärande och de bevislämnande parternas komponenter också delar av Sveriges lösning.

De förvaltningsgemensamma komponenterna är i skrivande stund färdigutvecklade eller nästan färdigutvecklade. Komponenterna har testats med andra medlemsstater och är redo för testning med svenska behöriga myndigheter.

2.2.1 Åtkomstpunkt för eDelivery (OOTS-nod)

Sveriges och de andra medlemsstaternas lösningar binds samman av åtkomstpunkter för eDelivery (art. 2 f genomförandeförordningen). Inom det tekniska systemet kallas åtkomstpunkterna för OOTS-noder. Det är via dessa noder som alla bevisförfrågningar och bevisutbyten sker. Enligt genomförandeförordningens definition är en åtkomstpunkt en kommunikationskomponent som ingår i den elektroniska leveranstjänsten eDelivery (art 1.4 genomförandeförordningen). eDelivery baseras på tekniska specifikationer och standarder som har utvecklats inom ramen för Fonden för ett sammanlänkat Europa och vidareutvecklats inom ramen för programmet för ett digitalt Europa.

OOTS-noden kan också beskrivas som en standardiserad säker kommunikationstjänst som främst används i olika tjänster som initierats av EU men som även kan användas i nationella system. Tekniken används till exempel i upphandlingsnätverket PEPPOL och den svenska kommunikationstjänsten Säker Digital Kommunikation. Den svenska OOTS-noden hanterar både in- och utgående trafik, till och från de andra medlemsstaternas OOTS-noder.

Medlemsstaterna får enligt art. 3.3 genomförandeförordningen välja antalet åtkomstpunkter för eDelivery. Sveriges val att bara ha en åtkomstpunkt baseras främst på att det anses vara mest kostnadseffektivt att ha en förvaltningsgemensam lösning.

2.2.2 Auktorisationstjänst och svensk eIDAS-nod

En användare behöver identifiera sig vid två tillfällen, beroende på vald lösning i de aktuella medlemsstaterna. En första gång i förfarandeportalen när ett förfarande inleds, eventuellt en andra gång för att ge information som behövs för att söka fram och hämta beviset, och en sista gång, om den bevislämnande parten så kräver, inför förhandsgranskning av beviset i den andra medlemsstaten.

När en användare av en svensk förfarandeportal ska hämta bevis från en annan medlemsstat krävs enbart en identifiering i Sverige, den i förfarandeportalen. Den svenska lösningen för att söka fram beviset (se avsnitt 2.2.5) kräver inte en extra identifiering. Dock kommer användaren behöva återidentifiera sig i den andra medlemsstaten.

Vid förhandsgranskning (se avsnitt 2.2.3) får den bevislämnande parten kräva att användaren återidentifierar sig för identitets- och bevismatchning (art. 16 genomförandeförordningen). Denna process utförs i den svenska lösningen av komponenten Auktorisationstjänst.

Innan användaren tillåts förhandsgranska sitt bevis får användaren ange vilken e-legitimation denne har i en legitimeringstjänst varpå en identifieringsprocess utförs med den valda leverantören. Identitetsleverantören kan vara svensk, om användaren har en svensk e-legitimation. Det kan också vara en utländsk identitetsleverantör, legitimering sker då via den svenska eIDAS-noden (art. 2 e genomförandeförordningen) i legitimeringstjänsten Sweden Connect (se Figur 1). Efter en lyckad identifiering skickar identitetsleverantören ett identitetsintyg till Auktorisationstjänsten. Om identitetsintyget kan matchas med uppgifterna i bevisbegäran begär Förhandsgranskningstjänsten ett åtkomstintyg från Auktorisationstjänsten som skickas med till den bevislämnande parten. Detta möjliggör i sin tur att den bevislämnande parten kan returnera det aktuella beviset till Förhandsgranskningstjänsten.

Auktorisationstjänsten är tekniskt sett en fristående komponent men den är nära knuten till Förhandsgranskningstjänsten och Anvisningstjänsten och är därmed en av de förvaltningsgemensamma komponenterna.

Sweden Connect är en standardiserad infrastruktur för e-legitimeringstjänster som Digg tillhandahåller (3 § 1 p. myndighetens instruktion) för att undvika att offentliga aktörer ska behöva anpassa sig till flera grundläggande tekniska gränssnitt. Sweden Connect består av ett tekniskt ramverk, metadata och kontaktinformation om alla anslutna aktörer. Digg är även Sveriges kontaktpunkt (Single Point of Contact) inom eIDAS och företräder Sverige i eIDAS samarbetsnätverk. Både offentliga och privata aktörer kan ansluta sina e-tjänster till Sweden Connect. Genom infrastrukturen får e-tjänster tillgång till inloggning med både svenska och utländska e-legitimationer. De utländska e-legitimationer som ingår är de som anmälts av andra eIDAS-anslutna länder. Digg är även ansluten som aktör och kan därmed, för egen och andras räkning, genomföra gränsöverskridande e-legitimering.

2.2.3 Förhandsgranskningstjänst

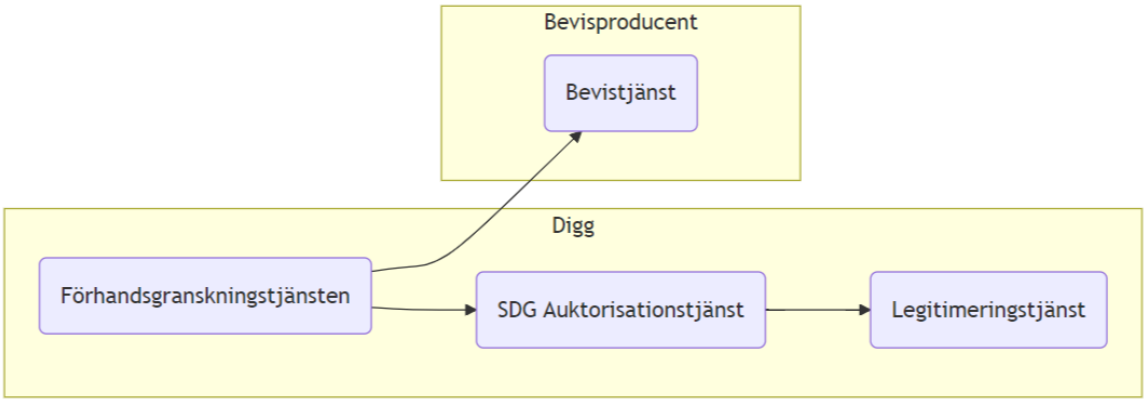
Förhandsgranskningstjänsten är en förvaltningsgemensam tjänst som innehåller det utrymme för förhandsgranskning som avses i art. 1.14 och 2 c genomförandeförordningen. Tjänsten används då en användare vill hämta bevis från Sverige. Användaren ges möjlighet att förhandsgranska beviset som ska hämtas från en svensk bevislämnande part och skickas till en förfarandeportal i en annan medlemsstat. Förhandsgranskningen är central för tilliten till det tekniska systemet och för användarens rätt att avgöra om beviset ska föras över till det andra landet eller inte.

När den utländska förfarandeportalen har lokaliserat att beviset finns i Sverige skickas en bevisförfrågan från förfarandeportalen till Förhandsgranskningstjänsten via ländernas OOTS-

noder. Förhandsgranskningstjänsten skickar tillbaka en länk som förfarandeportalen presenterar för användaren. Användaren omdirigeras via länken till den svenska Förhandsgranskningstjänsten. Tjänsten kontrollerar bevisbegäran och omdirigerar användaren för återautentisering i Auktorisationstjänsten. Användaren behöver återidentifiera sig i Förhandsgranskningstjänsten eftersom det behöver säkerställas att det är samma person. Beviset hämtas från den bevislämnande parten via dess bevistjänst, och användaren får möjlighet att förhandsgranska beviset. Användaren behöver göra ett aktivt val om beviset ska delas eller inte efter att ha haft möjlighet att förhandsgranska det. Om användaren väljer att dela beviset skickar Förhandsgranskningstjänsten beviset till förfarandeportalen via OOTS-noderna och användaren blir omdirigerad tillbaka till förfarandeportalen.

Två databaser för kort- respektive långtidslagring av transaktionsdata finns kopplade till Förhandsgranskningstjänsten. När användaren förhandsgranskar ett bevis sker en tillfällig lagring av beviset tills användaren aktivt har valt att dela det. Beviset raderas när användaren väljer att dela eller inte dela beviset, alternativt inte gör något val och sessionstiden går ut. I databasen för långtidslagring sparas strukturerad data om bevisutbytet enligt kraven i genomförandeförordningen och de tekniska designdokumenten.

Om förfarandet behöver hämta flera bevis sker flera olika hämtningar, trots att bevisen kommer från samma bevislämnande part. Det beror på att specifikationerna för bevisförfrågan och bevissvar bara gäller för ett bevis och att det i respektive förfrågan inte framgår om det kommer ytterligare bevisförfrågningar. Medlemsstaternas förhandsgranskningsfunktioner kan därmed inte vänta på om det kommer eventuella ytterligare förfrågningar vilket gör att varje hämtning behöver hanteras separat.



Figur 1 - Förhandsgranskningstjänsten tar emot bevisbegäran från OOTS-noden (ej i bild) och omdirigerar användaren till Auktorisationstjänsten som i sin tur omdirigerar hen till legitimeringstjänsten Sweden Connect om hen har en utländsk e-legitimation. Efter godkänd återidentifiering hämtas beviset från den bevislämnande partens bevistjänst och förhandsgranskas av användaren i Förhandsgranskningstjänsten.

2.2.4 Bevislämnande parter

De bevislämnande parterna (art. 2 a genomförandeförordningen), eller i förekommande fall förmedlingsplattformarna, behöver göra sina bevistjänster tillgängliga för Förhandsgranskningstjänsten (se Figur 1). En bevistjänst är detsamma som den datatjänst som avses

i art. 1.12 genomförandeförordningen. Digg har valt att använda begreppet bevistjänst i detta avseende eftersom ordet datatjänst har flera betydelser i genomförandeförordningen.

En bevistjänst görs tillgänglig genom att den bevislämnande parten implementerar ett API som definieras av Digg[4]. När ett bevis efterfrågas anropar Förhandsgranskningstjänsten detta API hos den bevislämnande parten som returnerar beviset till Förhandsgranskningstjänsten.

2.2.5 Uppslag och bevishämtning

De bevisbegärande parternas förfarandeportaler ansluts till tjänsten Uppslag och bevishämtning via API[5]. Tjänsten tillhandahåller funktionalitet för att göra bevisförfrågningar och hämta bevis från andra medlemsstater. Uppslag och bevishämtning är inte en obligatorisk del av det tekniska systemets struktur (jfr de komponenter som anges i art. 2 genomförandeförordningen) men är en kostnadseffektiv förvaltningsgemensam lösning för Sverige då inte varje bevisbegärande part själv behöver skapa funktionen.

Användaren omdirigeras från förfarandeportalen till tjänsten Uppslag och bevishämtning för att där göra de nödvändiga val som krävs för att det ska vara möjligt att söka fram beviset i den andra medlemsstaten. Dessa val gör användaren i en webbaserad delkomponent kallad Bevisväljare. Informationen från användaren används för att lokalisera beviset genom de EU-gemensamma tjänsterna, och sedan skickar Uppslag och bevishämtning den kompletta bevisförfrågan till det andra landet. Det andra landet returnerar en länk till sitt utrymme för förhandsgranskning till Uppslag och bevishämtning som omdirigerar användaren till det andra landets förhandsgranskning. Där kan användaren se sitt bevis och kontrollera att det är korrekt, och därefter välja att dela det med det svenska förfarandet.

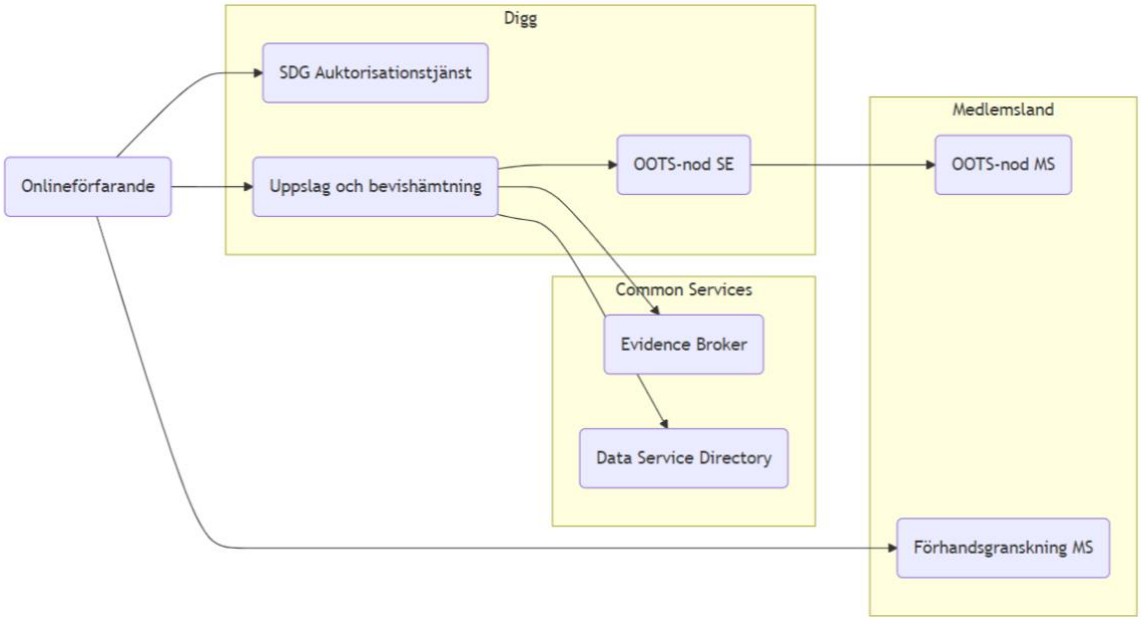
Efter att användaren har förhandsgranskat och valt att dela beviset omdirigeras denne tillbaka till förfarandeportalen varpå beviset hämtas via ett API-anrop mot Uppslag och bevishämtning.

Uppslag och bevishämtning kan bara hämta ett bevis i taget. Om flera bevis ska hämtas i samma förfarande sker flera separata hämtningar, trots att bevisen kommer från samma bevislämnande part, vilket beror på hur specifikationerna för bevisförfrågan ser ut, se avsnitt 2.2.3. Om användaren vill använda samma bevis i ett annat förfarande vid ett annat tillfälle behöver en ny begäran göras via det andra förfarandet.

---

[4] API:et heter Intermediation-SE, för mer information se https://github.com/diggsweden/sdg-intermediation-se

[5] API:et heter Intermediation-EU, för mer information se https://github.com/diggsweden/sdg-intermediation-eu



Figur 2 - En användare av en svensk förfarandeportal (i bilden onlineförfarande) identifierar sig en legitimeringstjänst och omdirigeras därefter till Uppslag och bevishämtning. Där gör användaren de val som krävs för att beviset ska hittas i de EU-gemensamma tjänsterna (i bilden Common Services). Bevisbegäran skickas till det andra landet från Uppslag och bevishämtning via OOTS-noderna och användaren omdirigeras till det andra landets förhandsgranskning. När användaren har godkänt bevisutbytet omdirigeras användaren tillbaka till förfarandeportalen och beviset skickas till Uppslag och bevishämtning från det andra landet. Förfarandeportalen kan därefter hämta beviset från Uppslag och bevishämtning. Den bevisbegärande parten behöver vara auktoriserad för att anropa API:et, därför finns även Diggs Auktorisationstjänst med i bilden.

2.2.6 Bevisbegärande parter

En bevisbegärande part har en förfarandeportal som är en webbsida eller en mobilapplikation där en användare kan få tillgång till och utföra ett sådant onlineförfarande som avses i art. 14.1 SDG-förordningen (art. 1.19 genomförandeförordningen), exempelvis en e-tjänst för ansökan. Portalen är alltså en del av den process som förfarandet utgör.

Förfarandeportalen behöver vara ansluten till en eIDAS-nod för att möjliggöra för en användare med utländsk e-legitimation att identifiera sig. Användaren omdirigeras efter identifiering till Uppslag och bevishämtning (se avsnitt 2.2.5). Efter bevisutbytet är klart blir användaren omdirigerad tillbaka till förfarandeportalen. Om användaren har valt att dela beviset i den utländska förhandsgranskningen kan förfarandeportalen hämta beviset från Uppslag och bevishämtning som har hämtat det från den andra medlemsstaten. Beviset finns sedan i förfarandeportalen och användaren ser det som en bifogad fil.

2.3 Anslutning mellan komponenter

I den svenska nationella arkitekturen för det tekniska systemet finns alltså både förvaltningsgemensamma och myndighetsspecifika komponenter. De bevislämnande parterna gör sina bevistjänster tillgängliga för Förhandsgranskningstjänsten (Figur 1) som i sin tur är ansluten till den svenska eIDAS-noden via Auktorisationstjänsten och den svenska OOTS-noden. De bevisbegärande parterna (Figur 2) etablerar förfarandeportaler som ansluter till tjänsten Uppslag

och bevishämtning för val av bevis varpå bevisbegäran skickas till den andra medlemsstaten via OOTS-noden. Förfarandeportalerna ska även vara anslutna till eIDAS-noden.

3 Loggning i det tekniska systemet

För att stödja driften av det tekniska systemet måste händelser relaterade till användningen av systemet loggas (art. 17 genomförandeförordningen). I art 28.6 ibid. finns krav på lämpliga och proportionerliga säkerhetsåtgärder för loggar.

Kravet på loggning gäller även de bevislämnande och de bevisbegärande parterna samt, i tillämpliga fall, förmedlingsplattformar. Loggning ska därför ske i olika delar av systemet; bevisbegärande parters förfarandeportaler, bevislämnande parters bevistjänster och de förvaltningsgemensamma komponenterna.

Digg kommer bara att utföra loggning i de förvaltningsgemensamma komponenter som Digg ansvarar för. Detta kommer att ske med tre olika loggar som implementeras på olika sätt.

- Applikationslogg som lagras i tre månader i en central loggserver och som inte innehåller personuppgifter.
- Säkerhetslogg som lagras i tre månader som innehåller personuppgifter och vad användaren har gjort för val.
- Transaktionsuppgifter om bevisutbyte enligt krav i genomförandeförordningen och de tekniska designdokumenten. Personuppgifter förekommer och uppgifterna sparas som strukturerat data i databas i minst 12 månader.