

Rapporter om bedömning av överensstämmelse av kvalificerade betrodda tjänster enligt eIDAS

Transport- och kommunikationsverkets anvisning

215/2019 O

215/2019 O
9.10.2019

Innehåll

1	Inledning	2
1.1	Syftet med anvisningen	2
1.2	Anvisningens ikraftträdande	2
1.3	Författningar, definitioner och förkortningar:	3
2	Inlämnande av rapporter om överensstämmelsebedömning	4
3	Förteckning över betrodda tjänsteleverantörer (trusted list)	6
4	Innehållet i rapporter om överensstämmelsebedömningar	6
4.1	Basuppgifter om organ för bedömning av överensstämmelse.....	6
4.2	Basuppgifter om den betrodd tjänst som ska bedömas	6
4.3	Basuppgifter om processen för bedömning av överensstämmelse.....	7
4.4	Påvisande av överensstämmelse med krav.....	8
4.4.1	Specialkrav som gäller tjänsteleverantörer.....	8
4.4.2	Särskilda krav på kvalificerade betrodda tjänster.....	9
4.5	Rapportering av avvikelser.....	9

215/2019 O
9.10.2019

1 Inledning

1.1 Syftet med anvisningen

Anvisningen gäller kvalificerade betrodda tjänster enligt eIDAS-förordningen.

Anvisningen är avsedd för de ackrediterade organ för bedömning av överensstämmelse som granskar att en kvalificerad tillhandahållare av betrodda tjänster och en kvalificerad betrodd tjänst är i överensstämmelse med kraven. Anvisningen specificerar minimiinnehållet och strukturen i de rapporter som bedömningen resulterar i.

En särskild anvisning har utfärdats om de anmälningar som ska lämnas till Transport- och kommunikationsverket (214/2016 O).

Med stöd av 42 § i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009, autentiseringslag) är Transport- och kommunikationsverkets uppgift att ha tillsyn över efterlevnaden av den lagen och EU:s eIDAS-förordning. Denna anvisning har utfärdats med stöd av denna allmänna fullmakt enligt 42 § i nämnda lag.

1.2 Anvisningens ikraftträdande

Anvisningen 215/2019 O träder i kraft den 9 oktober 2019.

Anvisningen gäller tills vidare och den kompletteras och ändras vid behov. I så fall förblir anvisningens nummer 215 oförändrat, medan datumet ändras och året också vid behov. De nya versionerna av anvisningen anges i tabellen nedan.

Gällande anvisning publiceras på Transport- och kommunikationsverkets webbplats på <https://www.kyberturvallisuuskeskus.fi/sv/elektronisk-identifiering> och <https://www.traficom.fi/sv/foreskrifter>

Version	Datum	Beskrivning/ändring	Författare
215/2019 O Rapporter om bedömning av överensstämmelse av kvalificerade betrodda tjänster	9.10.2019	Den andra utfärdade versionen - Avsnittet om inspektionsberättelser om bedömning av identifieringstjänster har flyttats till anvisning 211/2019 O - Anvisningens text har bearbetats tekniskt på grund av myndighetens namnändring	Transport- och kommunikationsverket, Cybersäkerhetscentret

215/2019 O
9.10.2019

		och rubriker har modifierats.	
215/2016 O Be- rättelser om be- dömning av identifierings- tjänster och be- trodda tjänster	2.11.2016	Den första utfärdade versionen	Kommunikationsver- ket, Cybersäkerhets- centret

1.3 Författningar, definitioner och förkortningar:

eIDAS: Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

Autentiseringslag: lag om stark autentisering och betrodda elektroniska tjänster (617/2009 jämte ändringar)

Kvalificerad tillhandahållare av betrodda tjänster (QTSP, qualified trusted service provider):

eIDAS artikel 3 Definitioner

20) kvalificerad tillhandahållare av betrodda tjänster: en tillhandahållare av betrodda tjänster som tillhandahåller en eller flera kvalificerade betrodda tjänster och som beviljats status som kvalificerad av tillsynsorganet.

Kvalificerad betrodd tjänst (QTS, qualified trusted service):

eIDAS artikel 3 Definitioner

16) betrodd tjänst: en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av

a) skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplatser eller elektroniska tidsstämplatser, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller

b) skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller

c) bevarande av elektroniska underskrifter, stämplatser eller certifikat med anknytning till dessa tjänster

17) kvalificerad betrodd tjänst: en betrodd tjänst som uppfyller tillämpliga krav i denna förordning,

Organ för bedömning av överensstämmelse (CAB, conformity assessment body):

215/2019 O
9.10.2019

eIDAS artikel 3 Definitioner

18) organ för bedömning av överensstämmelse: ett organ enligt definitionen i artikel 2.13 i förordning (EG) nr 765/2008 som i enlighet med den förordningen är ackrediterat för överensstämmelsebedömning av en kvalificerad tillhandahållare av en betrodd tjänst och den kvalificerade betrodda tjänst som denne tillhandahåller.

Rapport om överensstämmelsebedömning (CAR, conformity assessment report):

Se artikel 20 i eIDAS: Tillsyn över kvalificerade tillhandahållare av betrodda tjänster

1. Kvalificerade tillhandahållare av betrodda tjänster ska [...] granskas av ett organ för bedömning av överensstämmelse. Syftet med denna granskning ska vara att bekräfta att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning. De kvalificerade tillhandahållarna av betrodda tjänster ska lämna in den resulterande rapporten om överensstämmelsebedömning till tillsynsorganet [...].

[...]

Se artikel 21 i eIDAS: Igångsättande av en kvalificerad betrodd tjänst

1. När tillhandahållare av betrodda tjänster som inte har status som kvalificerade har för avsikt att börja tillhandahålla kvalificerade betrodda tjänster, ska de anmäla sin avsikt till tillsynsorganet och samtidigt lämna in en rapport om överensstämmelsebedömning som utfärdats av ett organ för bedömning av överensstämmelse.

[...]

2 Inlämnande av rapporter om överensstämmelsebedömning

Rapporten om överensstämmelsebedömning ska lämnas in till Transport- och kommunikationsverket:

1. innan verksamheten inleds, när tillhandahållare av betrodda tjänster som inte har status som kvalificerade, har för avsikt att börja tillhandahålla kvalificerade betrodda tjänster, och
2. minst varje 24 månader efter det att tillhandahållaren av betrodda tjänster vid inledande av verksamheten lämnat in rapporten om överensstämmelse till Transport- och kommunikationsverket.

BESTÄMMELSER

Artikel 20 i eIDAS: Tillsyn över kvalificerade tillhandahållare av betrodda tjänster

215/2019 O
9.10.2019

1. Kvalificerade tillhandahållare av betrodda tjänster ska minst en gång vartannat år och på egen bekostnad granskas av ett organ för bedömning av överensstämmelse. Syftet med denna granskning ska vara att bekräfta att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning. De kvalificerade tillhandahållarna av betrodda tjänster ska lämna in den resulterande rapporten om överensstämmelsebedömning till tillsynsorganet inom en period av tre arbetsdagar efter mottagande av denna.

2. Tillsynsorganet får, utan att det påverkar tillämpningen av punkt 1, när som helst granska eller begära att ett organ för bedömning av överensstämmelse gör en överensstämmelsebedömning av de kvalificerade tillhandahållarna av betrodda tjänster på dessa tillhandahållare av betrodda tjänsters egen bekostnad för att bekräfta att dessa och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning. Vid misstänkta överträdelser av reglerna om skydd för personuppgifter ska tillsynsorganet informera dataskyddsmyndigheterna om sina granskningsresultat.

[...]

Artikel 21 i eIDAS: Igångsättande av en kvalificerad betrodd tjänst

1. När tillhandahållare av betrodda tjänster som inte har status som kvalificerade har för avsikt att börja tillhandahålla kvalificerade betrodda tjänster, ska de anmäla sin avsikt till tillsynsorganet och samtidigt lämna in en rapport om överensstämmelsebedömning som utfärdats av ett organ för bedömning av överensstämmelse.

2. Tillsynsorganet ska kontrollera huruvida tillhandahållaren av betrodda tjänster och de betrodda tjänster som denne tillhandahåller uppfyller kraven i denna förordning, och i synnerhet kraven för kvalificerade tillhandahållare av betrodda tjänster och för de kvalificerade betrodda tjänster som de tillhandahåller.

Om tillsynsorganet kommer fram till att tillhandahållaren av betrodda tjänster och de betrodda tjänster som denne tillhandahåller uppfyller de krav som avses i första stycket, ska det bevilja status som kvalificerad tillhandahållare av betrodda tjänster och de betrodda tjänster som denne tillhandahåller samt informera det organ som avses i artikel 22.3 för att de förteckningar över betrodda tjänsteleverantörer som avses i artikel 22.1 ska kunna uppdateras, senast tre månader efter anmälan i enlighet med punkt 1 i denna artikel.

Om kontrollen inte har slutförts inom tre månader från anmälan, ska tillsynsorganet informera tillhandahållaren av betrodda tjänster om detta och ange orsakerna till förseningen samt när kontrollen beräknas vara slutförd.

3. Kvalificerade tillhandahållare av betrodda tjänster får börja tillhandahålla den kvalificerade betrodda tjänsten efter det att status som kvalificerad har angetts i de förteckningar över betrodda tjänsteleverantörer som avses i artikel 22.1.

[...]

32 § i lagen om stark autentisering och betrodda elektroniska tjänster

Ett organ för bedömning av överensstämmelse ska inspektera en kvalificerad tillhandahållare av betrodda tjänster och överensstämmelsen hos en kvalificerad betrodd tjänst med iakttagande av bestämmelserna i EU:s förordning om elektronisk identifiering.

215/2019 O
9.10.2019

Bestämmelser om Transport- och kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelse finns i 42 §. Som bedömningsgrund kan Transport- och kommunikationsverket fastställa bestämmelser eller riktlinjer som antagits av Europeiska unionen eller något annat internationellt organ, publicerade och generellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt.

3 Förteckning över betrodda tjänsteleverantörer (trusted list)

Om de anmälda tjänsterna uppfyller kraven för kvalificerade tillhandahållare av betrodda tjänster och kvalificerade betrodda tjänster, beviljar Transport- och kommunikationsverket status som kvalificerad till tillhandahållare av betrodda tjänster och de betrodda tjänster som denne tillhandahåller samt för in tjänsterna i förteckningar över betrodda tjänsteleverantörer.

Finlands förteckning över betrodda tjänsteleverantörer finns på webben på <https://dp.trustedlist.fi/fi-tl.pdf>

Artikel 22 i eIDAS: Förteckningar över betrodda tjänsteleverantörer

1. Varje medlemsstat ska upprätta, underhålla och offentliggöra förteckningar med uppgifter om kvalificerade tillhandahållare av betrodda tjänster som den ansvarar för, tillsammans med uppgifter om de kvalificerade betrodda tjänster som dessa tillhandahåller.

4 Innehållet i rapporter om överensstämmelsebedömningar

Rapporter om bedömning av överensstämmelse av kvalificerade betrodda tjänster ska innehålla minst följande basuppgifter.

4.1 Basuppgifter om organ för bedömning av överensstämmelse

1. Företagets eller organisationens namn och unika registreringsnummer;
2. Om företaget eller organisationen har etablerat sig i någon annan stat i EES-området än i Finland, det register där den utländska organisationen eller det utländska företaget har förts in;
3. Postadress och kontaktpersoner; e-postadresser med tanke på förfrågningar från Transport- och kommunikationsverket.

4.2 Basuppgifter om den betrodd tjänst som ska bedömas

4. Namn på den kvalificerade betrodda tjänst som är föremål för bedömning eller namn på den tjänst för vilken status som kvalificerad ansöks om samt typer av tjänst i

215/2019 O
9.10.2019

enlighet med punkt 4 i avsnitt 4.1.1 i anmälningsanvisningen 214/2016 O, det vill säga:

- a. kvalificerat certifikat för elektronisk underskrift (artikel 28 i eIDAS)
- b. kvalificerad valideringstjänst för kvalificerad elektronisk underskrift (artikel 33 i eIDAS)
- c. kvalificerad tjänst för bevarande av kvalificerad elektronisk underskrift (artikel 34 i eIDAS)
- d. kvalificerat certifikat för elektronisk stämpel (artikel 38 i eIDAS)
- e. kvalificerad valideringstjänst för kvalificerad elektronisk stämpel (artikel 40 i eIDAS)
- f. kvalificerad tjänst för bevarande av kvalificerad elektronisk stämpel (artikel 40 i eIDAS)
- g. kvalificerad elektronisk tidsstämpling (artikel 42 i eIDAS)
- h. kvalificerad elektronisk tjänst för rekommenderade leveranser (artikel 44 i eIDAS)
- i. kvalificerat certifikat för autentisering av webbplatser (artikel 45 i eIDAS).

4.3 Basuppgifter om processen för bedömning av överensstämmelse

- 5. Beskrivning av vilken del av de betrodda tjänsterna bedömningen omfattar;
- 6. Utredning om vilka metoder som har använts vid bedömningen av olika delområden;
- 7. Uppgifter om den dokumentation som har använts vid bedömningen av överensstämmelsen;
- 8. Tidpunkt för bedömning och bedömningens längd enligt personarbetstiden (som dagsverken eller timmar).

Rapporten om överensbestämmelsebedömning ska innehålla en beskrivning av vilken/vilka kvalificerade betrodda tjänster bedömningen omfattar och om bedömningen omfattar hela eller en del av tjänsten. Tillhandahållaren av en kvalificerad betrodd tjänst kan beställa bedömningen i delar även hos två eller flera organ för bedömning av överensstämmelse. Det är viktigt att

215/2019 O
9.10.2019

det av rapporten på ett entydigt sätt framgår om bedömningsorganets rapport omfattar endast en del av kraven eller alla krav i 4.4.

Av rapporten om bedömning av överensstämmelse ska framgå vilka metoder som har använts vid bedömningen av överensstämmelsen med kraven. Enbart en förteckning över standarder kan inte anses vara tillräcklig, utan rapporten om överensstämmelsebedömning ska innehålla en beskrivning av vilken metod som har använts vid bedömningen av varje sådant delområde som avses i avsnitt 4.4.

Rapporten om överensstämmelsebedömningen ska innehålla en förteckning över tjänsteleverantörens dokument som har utvärderats. Allt material som gäller bedömningen behöver inte bifogas den rapport som lämnas till Transport- och kommunikationsverket. Vid behov kan Transport- och kommunikationsverket be leverantören lämna en mer detaljerad dokumentation. Transport- och kommunikationsverkets rätt till information bygger på 43 § i lagen om stark autentisering och betrodda elektroniska tjänster. Enligt paragrafen har Transport- och kommunikationsverket trots sekretessbestämmelserna rätt att få den information som behövs för skötseln av uppgifterna av dem vars rättigheter och skyldigheter den aktuella lagen gäller och av dem som handlar för dessas räkning.

4.4 Påvisande av överensstämmelse med krav

Syftet med bedömningen av överensstämmelsen hos en betrodd tjänst är att visa att kvalificerade betrodda tjänster som anmälts till Transport- och kommunikationsverket uppfyller kraven i eIDAS-förordningen.

Av rapporten om bedömning av överensstämmelse ska framgå på vilket sätt uppfyllandet av följande krav har bedömts och på vilken grund man bedömer om den betrodda tjänsten uppfyller följande krav:

4.4.1 Specialkrav som gäller tjänsteleverantörer

9. Krav på behandling och skydd av uppgifter (artikel 5 i eIDAS);
10. Krav på skadeståndsansvar och bevisbörda (artikel 13.1 och 13.2 i eIDAS och 41 § i autentiseringslagen);
11. Tillgänglighet för personer med funktionshinder (artikel 15 i eIDAS);

215/2019 O
9.10.2019

12.Säkerhetskrav på tillhandahållare av betrodda tjänster (artikel 19.1 i eIDAS); och

13.Krav på kvalificerade tillhandahållare av betrodda tjänster (artikel 24.2 i eIDAS, med undantag för 2 k).

4.4.2 Särskilda krav på kvalificerade betrodda tjänster

14.Allmänna kriterier för bedömning av betrodda tjänster enligt 20–21 § i föreskrift 72;

15.Krav på kvalificerade certifikat (artikel 24.1 a-d, 24.2 k, 24.3 och 24.4 i eIDAS);

16.Krav på kvalificerade certifikat för elektroniska underskrifter (artikel 28.1 i eIDAS)

17. Krav på kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter (artikel 32 och 33 i eIDAS);

18.Krav på kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter (artikel 34 i eIDAS);

19. Krav på kvalificerade certifikat för elektroniska stämplatser (artikel 38 i eIDAS);

20.Krav på kvalificerad valideringstjänst för kvalificerade elektroniska stämplatser (artikel 40, 32 och 33 i eIDAS);

21.Krav på kvalificerad tjänst för bevarande av kvalificerade elektroniska stämplatser (artikel 40 och 34 i eIDAS);

22.Krav på kvalificerade elektroniska tidsstämplatser (artikel 42 i eIDAS);

23.Krav på kvalificerade elektroniska tjänster för rekommenderade leveranser (artikel 44 i eIDAS); och

24.Krav på kvalificerade certifikat för autentisering av webbplatser (artikel 45 i eIDAS);

4.5 Rapportering av avvikelser

Vid bedömning av överensstämmelse hittas vanligen avvikelser som korrigeras under bedömningen eller kort därefter. Avvikelser som har upptäckts i normala situationer har korrigerats innan rapporten om överensbestämmelsebedömning har lämnats till Transport- och kommunikationsverket.

Om några avvikelser lämnas kvar ska de på ett entydigt sätt framgå av rapporten om överensstämmelsebedömning. I så fall

215/2019 O
9.10.2019

ska rapporten innehålla uppgift om vilka mindre avvikelser eller andra slags avvikelser har lämnats kvar i systemet och enligt vilket tidsschema och på vilket sätt avvikelserna kommer att korrigeras. Transport- och kommunikationsverket kommer inte att ta fram någon allvarlighetsskala för avvikelser, utan leverantören av betrodda tjänster och bedömningsorganet får i bedömnings- och anmälningsfasen bestämma om hur allvarliga avvikelserna är. Transport- och kommunikationsverket gör en slutlig bedömning av om vilka avvikelser som godkänns. Vid behov kräver Transport- och kommunikationsverket korrigerande upptäckta avvikelser.