KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2015/1502

av den 8 september 2015

om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av 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 ([1]), särskilt artikel 8.3, och

av följande skäl:

(1) Enligt artikel 8 i förordning (EU) nr 910/2014 behöver ett system för elektronisk identifiering som anmälts i enlighet med artikel 9.1 specificera tillitsnivåerna låg, väsentlig och/eller hög för medel för elektronisk identifiering som har utfärdats inom det systemet.

(2) Det är väsentligt att fastställa tekniska minimispecifikationer, standarder och förfaranden så att en gemensam förståelse kan uppnås av tillitsnivåernas detaljuppgifter och att interoperabilitet säkras vid kartläggningen av de nationella tillitsnivåerna för anmälda system för elektronisk identifiering i förhållande till tillitsnivåerna enligt artikel 8, såsom föreskrivs genom artikel 12.4 b i förordning (EU) nr 910/2014.

(3) Den internationella standarden ISO/IEC 29115 har beaktats för specifikationerna och förfarandena i denna genomförandeakt såsom varande den främsta internationella standard som är tillgänglig i fråga om tillitsnivåer för medel för elektronisk identifiering. Innehållet i förordning (EU) nr 910/2014 skiljer sig dock från internationell standard, i synnerhet i fråga om krav på styrkande och kontroll av identitet, liksom vad gäller det sätt på vilket hänsyn tas till skillnaderna mellan medlemsstaternas identitetsbestämmelser och befintliga verktyg i EU för samma syfte. Även om bilagan bygger på denna internationella standard bör den därför inte hänvisa till något specifikt innehåll i ISO/IEC 29115.

(4) Denna förordning har utarbetats på ett resultatbaserat sätt såsom varande mest lämpliga metod, vilket också avspeglas i de definitioner som använts för att specificera termer och begrepp. De tar hänsyn till syftet med förordning (EU) nr 910/2014 i fråga om tillitsnivåerna för medel för elektronisk identifiering. Största möjliga hänsyn bör därför tas till det storskaliga pilotprojektet Stork, inklusive de specifikationer som utarbetats av detta projekt, samt definitioner och begrepp i ISO/IEC 29115 när specifikationer och förfaranden i denna genomförandeakt ska fastställas.

(5) Tillförlitliga källor kan ta många former, exempelvis registreringskontor, handlingar eller organ, beroende på det sammanhang där en aspekt av identitetsbevis behöver verifieras. De tillförlitliga källorna kan skilja sig åt i olika medlemsstater, också om sammanhangen liknar varandra.

(6) Krav på styrkande och kontroll av identitet bör beakta olika system och praxis och samtidigt säkerställa en tillräckligt hög tillitsnivå för att skapa nödvändigt förtroende. Ett godtagande av förfaranden som använts tidigare för andra syften än att utfärda medel för elektronisk identifiering bör därför villkoras med att bekräftelse erhålls om att dessa förfaranden uppfyller kraven för motsvarande tillitsnivå.

([1]) EUT L 257, 28.8.2014, s. 73.

(7) Vissa autentiseringsfaktorer, som exempelvis delade hemligheter, fysiska anordningar och fysiska attribut, används vanligtvis. Användningen av ett stort antal autentiseringsfaktorer, särskilt från olika faktorkategorier, bör dock uppmuntras för att höja säkerheten i autentiseringsprocessen.

(8) Denna förordning bör inte påverka juridiska personers representationsrättigheter. Bilagan bör dock innehålla föreskrifter om krav på bindningen mellan fysiska och juridiska personers medel för elektronisk identifiering.

(9) Betydelsen av informationssäkerhet och system för tjänstehantering bör uppmärksammas, vilket även gäller betydelsen av att använda erkända metoder och tillämpa principerna i standarder som exempelvis ISO/IEC 27000- och ISO/IEC 20000-serierna.

(10) Bästa praxis i fråga om tillitsnivåer i medlemsstaterna bör också beaktas.

(11) It-säkerhetscertifiering som baseras på internationella standarder är ett viktigt verktyg för verifiering av hur väl en produkts säkerhet motsvarar kraven i denna genomförandeakt.

(12) Den kommitté som avses i artikel 48 i förordning (EU) nr 910/2014 har inte avgivit något yttrande inom den tidsfrist som beslutades av dess ordförande.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

1. Tillitsnivåerna låg, väsentlig och hög för medel för elektronisk identifiering utfärdade inom ett anmält system för elektronisk identifiering ska fastställas med hänvisning till specifikationerna och förfarandena i bilagan.

2. Specifikationerna och förfarandena i bilagan ska användas för att specificera tillitsnivå för medel för elektronisk identifiering som utfärdats inom ett system för elektronisk identifiering genom att tillförlitlighet och kvalitet fastställs för följande beståndsdelar:

a) Inskrivning, i enlighet med vad som fastställs i avsnitt 2.1 i bilagan till denna förordning i kraft av artikel 8.3 a i förordning (EU) nr 910/2014.

b) Hantering av medel för elektronisk identifiering, i enlighet med avsnitt 2.2 i bilagan till denna förordning i kraft av artikel 8.3 b och f i förordning (EU) nr 910/2014.

c) Autentisering i enlighet med avsnitt 2.3 i bilagan till denna förordning i kraft av artikel 8.3 c i förordning (EU) nr 910/2014.

d) Hantering och organisering, i enlighet med avsnitt 2.4 i bilagan till denna förordning i kraft av artikel 8.3 d och e i förordning (EU) nr 910/2014.

3. När medel för elektronisk identifiering, som utfärdats inom ett anmält system för elektronisk identifiering, uppfyller ett krav för en högre tillitsnivå ska det antas uppfylla likvärdiga krav på en lägre tillitsnivå.

4. Såvida inte något annat anges i relevant del av bilagan ska alla beståndsdelar i bilagan angående en viss tillitsnivå, gällande medel för elektronisk identifiering som utfärdats inom ett anmält system för elektroniskt identifiering, uppfyllas för att motsvara den hävdade tillitsnivån.

Artikel 2

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 8 september 2015.

På kommissionens vägnar
Jean-Claude JUNCKER
Ordförande

BILAGA

Tekniska specifikationer och förfaranden för tillitsnivåerna låg, väsentlig och hög avseende de medel för elektronisk identifiering som utfärdats inom ramen för ett anmält system för elektronisk identifiering

1. Tillämpliga definitioner

I denna bilaga gäller följande definitioner:

1. *tillförlitlig källa*: en källa oavsett form som är tillförlitlig när det gäller att tillhandahålla korrekta uppgifter, information och/eller bevis som kan användas för att styrka en identitet.

2. *Autentiseringsfaktor*: en faktor som bekräftas vara bunden till en person och som tillhör någon av följande kategorier:

   a) *innehavsbaserad autentiseringsfaktor*: en autentiseringsfaktor som personen måste kunna visa att den innehar.

   b) *kunskapsbaserad autentiseringsfaktor*: en autentiseringsfaktor som personen måste kunna visa att den har kunskap om.

   c) *egenskapsbaserad autentiseringsfaktor*: en autentiseringsfaktor som utgår från en kroppslig egenskap hos en fysisk person, som denne måste kunna visa att den har.

3. *dynamisk autentisering*: en elektronisk process som använder kryptering eller andra metoder för att på begäran skapa ett elektroniskt bevis för att en person har kontroll över eller är i besittning av identifieringsinformationen, och som ändras vid varje autentisering mellan personen och det system som kontrollerar personens identitet.

4. *ledningssystem för informationssäkerhet*: en uppsättning processer och förfaranden avsedda att hantera godtagbara risknivåer förknippade med informationssäkerhet.

2. Tekniska specifikationer och förfaranden

De tekniska specifikationer och förfaranden som beskrivs i denna bilaga ska användas för att fastställa hur de krav och kriterier som avses i artikel 8 i förordning (EU) nr 910/2014 ska tillämpas för medel för elektronisk identifiering som utfärdats inom ramen för ett system för elektronisk identifiering.

2.1 *Inskrivning*

2.1.1 Ansökan och registrering

Tillitsnivå	Erforderliga beståndsdelar
Låg	1. Säkerställa att den sökande är medveten om villkoren förenade med användningen av medlet för elektronisk identifiering. 2. Säkerställa att den sökande är medveten om rekommenderade säkerhetsåtgärder kopplade till medlet för elektronisk identifiering. 3. Samla in de relevanta identitetsuppgifter som krävs för styrkande och kontroll av identitet.
Väsentlig	Samma som nivån låg.
Hög	Samma som nivån låg.

2.1.2 Styrkande och kontroll av identitet (fysisk person)

Tillitsnivå	Erforderliga beståndsdelar
Låg	1. Personen kan antas inneha bevis som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs och som avser den påstådda identiteten. 2. Beviset kan antas vara äkta eller existera enligt en tillförlitlig källa, och beviset förefaller vara giltigt. 3. Enligt en officiell källa existerar den påstådda identiteten, och det kan antas att den person som åberopar denna identitet är en och samma person.
Väsentlig	Nivå låg, samt ett av de alternativ som anges i punkterna 1–4 måste vara uppfyllt: 1. Kontroll har skett av att personen innehar ett bevis som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs och som avser den påstådda identiteten, och beviset kontrolleras för att fastställa att det är äkta, eller enligt en tillförlitlig källa existerar det och avser en verklig person, och åtgärder har vidtagits för att minimera risken att personens identitet inte är den påstådda identiteten, varvid det tas hänsyn till exempelvis risken för att beviset har förlorats, stulits, upphävts, återkallats eller löpt ut, eller 2. en identitetshandling uppvisas under ett registreringsförfarande i den medlemsstat där handlingen utfärdades, och handlingen tycks avse den person som uppvisar den, och åtgärder har vidtagits för att minimera risken att personens identitet inte är den påstådda identiteten, varvid det tas hänsyn till exempelvis risken för att handlingen har förlorats, stulits, upphävts, återkallats eller löpt ut, eller 3. om förfaranden som tidigare använts av ett offentligt eller privat företag i samma medlemsstat för andra ändamål än utfärdandet av medel för elektronisk identifiering ger en tillit som är likvärdig de förfaranden som anges i avsnitt 2.1.2 för tillitsnivån väsentlig, behöver den enhet som ansvarar för registreringen inte upprepa de tidigare förfarandena, förutsatt att en sådan likvärdig tillit bekräftas av ett sådant organ för bedömning av överensstämmelse som anges i artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 ([1]) eller av ett likvärdigt organ, eller 4. om medel för elektronisk identifiering utfärdas på grundval av ett giltigt anmält medel för elektronisk identifiering med tillitsnivån väsentlig eller hög, och riskerna för ändring i personidentifieringsuppgifterna beaktas, krävs det inte att förfarandena för styrkande och kontroll av identitet upprepas. Om medlet för elektronisk identifiering som utgör utgångspunkt inte har anmälts, ska tillitsnivån väsentlig eller hög bekräftas av det organ för bedömning av överensstämmelse som avses i artikel 2.13 i förordning (EG) nr 765/2008 eller av ett likvärdigt organ.

Tillitsnivå	Erforderliga beståndsdelar
Hög	Kraven i punkt 1 eller 2 ska uppfyllas: 1. Nivå väsentlig, samt ett av de alternativ som anges i leden a–c måste vara uppfyllt: a) När en person har kontrollerats och befunnits inneha fotografiskt eller biometriskt identifieringsbevis som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs, och den bevisningen avser den påstådda identiteten, kontrolleras beviset för att fastställa om det är giltigt enligt en tillförlitlig källa. och Sökanden har identifierats som den påstådda identiteten genom jämförelse av en eller flera fysiska egenskaper hos personen med en tillförlitlig källa, eller b) Om förfaranden som tidigare använts av ett offentligt eller privat företag i samma medlemsstat för andra ändamål än utfärdandet av medel för elektronisk identifiering ger en tillit som är likvärdig med de förfaranden som anges i avsnitt 2.1.2 för tillitsnivån hög, behöver den enhet som ansvarar för registreringen inte upprepa de tidigare förfarandena, förutsatt att en sådan likvärdig tillit bekräftas av ett sådant organ för bedömning av överensstämmelse som anges i artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 eller av ett likvärdigt organ, och åtgärder vidtas för att styrka att resultaten från tidigare förfaranden fortfarande är giltiga, eller c) Om medel för elektronisk identifiering utfärdas på grundval av ett giltigt anmält medel för elektronisk identifiering med tillitsnivån hög, och riskerna för ändring i personidentifieringsuppgifterna beaktas, krävs det inte att förfarandena för styrkande och kontroll av identitet upprepas. Om medlet för elektronisk identifiering som utgör utgångspunkt inte har anmälts, ska tillitsnivån hög bekräftas av det organ för bedömning av överensstämmelse som avses i artikel 2.13 i förordning (EG) nr 765/2008 eller av ett likvärdigt organ, och åtgärder vidtas för att styrka att resultaten av detta tidigare förfarande för utfärdande av ett anmält medel för elektronisk identifiering fortfarande är giltiga, ELLER 2. om den sökande inte lägger fram något erkänt fotografiskt eller biometriskt identifieringsbevis, ska samma förfaranden som används på nationell nivå i medlemsstaten av den enhet som ansvarar för registreringen för att erhålla sådant erkänt fotografiskt eller biometriskt identifieringsbevis tillämpas.

([1]) Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

2.1.3 Styrkande och kontroll av identitet (juridisk person)

Tillitsnivå	Erforderliga beståndsdelar
Låg	1. Den juridiska personens påstådda identitet styrks på grundval av bevis som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs.

Tillitsnivå	Erforderliga beståndsdelar
	2. Beviset förefaller vara giltigt och kan antas vara äkta, eller existera enligt en tillförlitlig källa, om införandet av en juridisk person i den tillförlitliga källan är frivilligt och regleras genom en överenskommelse mellan den juridiska personen och den tillförlitliga källan. 3. Den juridiska personen är enligt en tillförlitlig källa inte i en ställning som skulle hindra den från att handla som den juridiska personen.
Väsentlig	Nivå låg, samt ett av alternativen i punkterna 1–3 måste vara uppfyllt: 1. Den juridiska personens påstådda identitet styrks på grundval av bevis som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs, inklusive den juridiska personens namn, juridiska form, och (om så är tillämpligt) registeringsnummer, och beviset kontrolleras för att avgöra om det är äkta, eller existerar enligt en tillförlitlig källa, om införandet av den juridiska personen i den tillförlitliga källan krävs för att den juridiska personen ska få bedriva verksamhet inom sin sektor, och åtgärder har vidtagits för att minimera risken att den juridiska personens identitet inte är den påstådda identiteten, varvid det tas hänsyn till exempelvis risken för att handlingar har förlorats, stulits, upphävts, återkallats eller löpt ut, eller 2. Om förfaranden som tidigare använts av ett offentligt eller privat företag i samma medlemsstat för andra ändamål än utfärdande av medel för elektronisk identifiering ger en tillit som är likvärdig med de förfaranden som anges i avsnitt 2.1.3 för tillitsnivån väsentlig, behöver den enhet som ansvarar för registreringen inte upprepa de tidigare förfarandena, förutsatt att en sådan likvärdig tillit bekräftas av ett sådant organ för bedömning av överensstämmelse som anges i artikel 2.13 i förordning (EG) nr 765/2008 eller av ett likvärdigt organ, eller 3. Om medel för elektronisk identifiering utfärdas på grundval av ett giltigt anmält medel för elektronisk identifiering med tillitsnivån väsentlig eller hög, krävs det inte att förfarandena för styrkande och kontroll av identitet upprepas. Om medlet för elektronisk identifiering som utgör utgångspunkt inte har anmälts, ska tillitsnivån väsentlig eller hög bekräftas av det organ för bedömning av överensstämmelse som avses i artikel 2.13 i förordning (EG) nr 765/2008 eller av ett likvärdigt organ.
Hög	Nivå låg, samt ett av de alternativ som anges i punkterna 1–3 måste vara uppfyllt: 1. Den juridiska personens påstådda identitet styrks på grundval av bevis som erkänns i den medlemsstat där ansökan om medlet för elektronisk identitet görs, och innefattar den juridiska personens namn, juridiska form, och åtminstone en unik identifierare som avser den juridiska personen och som används i nationella sammanhang, och beviset kontrolleras för att fastställa att det är äkta enligt en tillförlitlig källa, eller

Tillitsnivå	Erforderliga beståndsdelar
	2. om de förfaranden som tidigare använts av ett offentligt eller privat företag i samma medlemsstat för andra ändamål än utfärdande av medel för elektronisk identifiering ger en tillit som är likvärdig de förfaranden som anges i avsnitt 2.1.3 för tillitsnivån hög, behöver den enhet som ansvarar för registreringen inte upprepa de tidigare förfarandena, förutsatt att en sådan likvärdig tillit bekräftas av ett sådant organ för bedömning av överensstämmelse som anges i artikel 2.13 i förordning (EG) nr 765/2008 eller av ett likvärdigt organ, och åtgärder vidtas för att styrka att resultaten från dessa tidigare förfaranden fortfarande är giltiga, eller 3. om medel för elektronisk identifiering utfärdas på grundval av ett giltigt anmält medel för elektronisk identifiering med tillitsnivån hög, krävs det inte att förfarandena för styrkande och kontroll av identitet upprepas. Om medlet för elektronisk identifiering som utgångspunkt inte har anmälts, ska tillitsnivån hög bekräftas av det organ för bedömning av överensstämmelse som avses i artikel 2.13 i förordning (EG) nr 765/2008 eller av ett likvärdigt organ, och åtgärder vidtas för att styrka att resultaten av detta tidigare förfarande för utfärdande av ett anmält medel för elektronisk identifiering fortfarande är giltiga.

2.1.4 Bindning mellan fysiska och juridiska personers medel för elektronisk identifiering

För en bindning mellan en fysisk persons medel för elektronisk identifiering och en juridisk persons medel för elektronisk identifiering (nedan kallad *bindning*) gäller följande villkor:

1. En bindning ska vara möjlig att upphäva och/eller återkalla. En bindnings livscykel (t.ex. aktivering, upphävande, förnyelse, återkallelse) ska förvaltas enligt nationellt erkända förfaranden.

2. Den fysiska person vars medel för elektronisk identifiering är bundet till den juridiska personens medel för elektronisk identifiering får delegera nyttjandet av bindningen till en annan fysisk person på grundval av nationellt erkända förfaranden. Emellertid förblir den delegerande fysiska personen ansvarig.

3. Bindningen ska göras på följande sätt:

Tillitsnivå	Erforderliga beståndsdelar
Låg	1. Styrkandet av den fysiska persons identitet som handlar på den juridiska personens vägnar har enligt kontroll utförts på nivån låg eller högre. 2. Bindningen har upprättats på grundval av nationellt erkända förfaranden. 3. Den fysiska personen är enligt en tillförlitlig källa inte i en ställning som skulle hindra den från att handla på den juridiska personens vägnar.
Väsentlig	Nivå låg punkt 3, samt 1. styrkandet av den fysiska persons identitet som handlar på den juridiska personens vägnar har enligt kontroll utförts på nivån väsentlig eller hög,

Tillitsnivå	Erforderliga beståndsdelar
	2. bindningen har upprättats på grundval av nationellt erkända förfaranden, vilket resulterat i att bindningen registrerats i en tillförlitlig källa, 3. bindningen har kontrollerats på grundval av uppgifter från en tillförlitlig källa.
Hög	Nivå låg punkt 3 och nivå väsentlig punkt 2, samt 1. styrkandet av den fysiska persons identitet som handlar på den juridiska personens vägnar har enligt kontroll utförts på nivån hög, 2. bindningen har kontrollerats på grundval av en unik identifierare som avser den juridiska personen och som används i nationella sammanhang och på grundval av uppgifter från en tillförlitlig källa som är unik för den fysiska personen.

2.2 *Hantering av medel för elektronisk identifiering*

2.2.1 Medel för elektronisk identifiering: egenskaper och utformning

Tillitsnivå	Erforderliga beståndsdelar
Låg	1. Medlet för elektronisk identifiering använder minst en autentiseringsfaktor. 2. Medlet för elektronisk identifiering är utformat så att utfärdaren vidtar rimliga åtgärder för att kontrollera att det endast används under ägarens kontroll eller innehav.
Väsentlig	1. Medlet för elektronisk identifiering använder minst två autentiseringsfaktorer från olika kategorier. 2. Medlet för elektronisk identifiering är utformat så att det kan antas att det endast används under ägarens kontroll eller innehav.
Hög	Nivå väsentlig, samt 1. medlet för elektronisk identifiering skyddar mot kopiering och manipulering samt mot angripare med hög angreppskapacitet, 2. medlet för elektronisk identifiering är utformat så att ägaren på tillförlitligt sätt kan skyddas mot användning av andra.

2.2.2 Utfärdande, leverans och aktivering

Tillitsnivå	Erforderliga beståndsdelar
Låg	Efter utfärdandet levereras medlet för elektronisk identifiering via en mekanism genom vilken medlet kan antas nå endast den avsedda personen.
Väsentlig	Efter utfärdandet levereras medlet för elektronisk identifiering via en mekanism genom vilken det kan antas att medlet levereras endast till ägaren.
Hög	Aktiveringsprocessen kontrollerar att medlet för elektronisk identifiering endast levererades till ägaren.

2.2.3 Upphävande, återkallelse och återaktivering

Tillitsnivå	Erforderliga beståndsdelar
Låg	1. Det är möjligt att avbryta och/eller återkalla ett medel för elektronisk identifiering i god tid och på ett verksamt sätt. 2. Åtgärder ska föreligga för att förhindra att upphävande, återkallelse och/eller reaktivering sker på otillåtet sätt. 3. Återaktivering ska ske endast om samma krav angående tilliten som fastställts före upphävandet eller återkallelsen fortsätter att uppfyllas.
Väsentlig	Samma som nivån låg.
Hög	Samma som nivån låg.

2.2.4 Förnyelse och ersättning

Tillitsnivå	Erforderliga beståndsdelar
Låg	Med beaktande av riskerna för ändring i personidentifieringsuppgifterna måste förnyelse eller ersättning uppfylla samma tillitskrav som det ursprungliga styrkandet och kontrollen av identiteten eller grundas på ett giltigt medel för elektronisk identifiering med samma eller högre tillitsnivå.
Väsentlig	Samma som nivån låg.
Hög	Nivå låg, samt om förnyelse eller ersättning grundas på ett giltigt medel för elektronisk identifiering, kontrolleras identitetsuppgifterna mot en tillförlitlig källa.

2.3 *Autentisering*

Detta avsnitt handlar om hot vid användning av autentiseringsmekanismen och förtecknar de krav som gäller för varje tillitsnivå. I detta avsnitt ska kontroller antas stå i proportion till riskerna på en viss nivå.

2.3.1 Autentiseringsmekanism

Av följande tabell framgår kraven per tillitsnivå för den autentiseringsmekanism där den fysiska eller juridiska personen använder medlet för elektronisk identifiering för att bekräfta sin identitet för en förlitande part.

Tillitsnivå	Erforderliga beståndsdelar
Låg	1. Innan personidentifieringsuppgifter lämnas ut sker en tillförlitlig kontroll av medlet för elektronisk identifiering och dess giltighet. 2. Om personidentifieringsuppgifter lagras som en del av autentiseringsmekanismen är dessa uppgifter säkrade för att skydda mot förlust och från att den äventyras, inklusive offlineanalys. 3. Autentiseringsmekanismen genomför säkerhetskontroller för att verifiera medlet för elektronisk identifiering, varför det är högst osannolikt att exempelvis gissningar, tjuvlyssning, omspelning eller manipulation av kommunikation som görs av en angripare med förhöjd/grundläggande angreppspotential kan underminera autentiseringsmekanismerna.

Tillitsnivå	Erforderliga beståndsdelar
Väsentlig	Nivå låg, samt 1. innan personidentifieringsuppgifter lämnas ut sker en tillförlitlig kontroll av medlet för elektronisk identifiering och dess giltighet med hjälp av en dynamisk autentisering, 2. autentiseringsmekanismen genomför säkerhetskontroller för att verifiera medlet för elektronisk identifiering, varför det är högst osannolikt att exempelvis gissningar, tjuvlyssning, omspelning eller manipulation av kommunikation som görs av en angripare med måttlig angreppspotential kan underminera autentiseringsmekanismerna.
Hög	Nivå väsentlig, samt autentiseringsmekanismen genomför säkerhetskontroller för att verifiera medlet för elektronisk identifiering, varför det är högst osannolikt att exempelvis gissningar, tjuvlyssning, omspelning eller manipulation av kommunikation som görs av en angripare med stor angreppspotential kan underminera autentiseringsmekanismerna.

2.4 *Hantering och organisation*

Alla deltagare som tillhandahåller en tjänst för elektronisk identifiering i ett gränsöverskridande sammanhang (nedan kallad en *tillhandahållare av tjänster*) ska i dokumenterad form ha praxis, policyer och strategier för ledning av informationssäkerhet vad avser risker samt andra erkända kontroller som ger styrningsorganen för system för elektronisk identifiering i respektive medlemsstat garantier att effektiva förfaranden föreligger. Alla krav/beståndsdelar i hela avsnitt 2.4 ska antas stå i proportion till riskerna på en viss nivå.

2.4.1 Allmänna bestämmelser

Tillitsnivå	Erforderliga beståndsdelar
Låg	1. Tillhandahållare av tjänster som levererar en operativ tjänst som omfattas av denna förordning är en offentlig myndighet eller rättslig enhet som erkänns som sådan i en medlemsstats nationella lagstiftning, med etablerad organisation och till fullo operativ i alla delar som är relevanta för tillhandahållandet av tjänsterna. 2. Tillhandahållarna av tjänster uppfyller alla rättsliga krav som åligger dem i samband med drift och leverans av tjänsten, däribland de typer av information som kan komma att eftersökas, hur en identitet styrks, vilken information som får lagras och hur länge. 3. Tillhandahållarna av tjänster kan visa att de har förmåga att ta på sig skadeståndsskyldighet samt att de har tillräckliga ekonomiska resurser för att fortsätta driften och tillhandahålla tjänsterna. 4. Tillhandahållarna av tjänster är ansvariga för fullgörandet av eventuella åtaganden som lagts ut på entreprenad till en annan enhet, och att systemets policy efterlevs, på samma sätt som om de själva hade utfört arbetsuppgifterna. 5. System för elektronisk identifiering som inte inrättats enligt nationell rätt ska ha en fullt användbar plan för verksamhetens upphörande. En sådan plan ska innefatta en metodisk nedläggning av driften eller fortsättning genom en annan tillhandahållare av tjänster, sättet på vilket behöriga myndigheter och slutanvändare informeras samt ingående uppgifter om hur register ska skyddas, bevaras och destrueras i enlighet med systemets policy.
Väsentlig	Samma som nivån låg.
Hög	Samma som nivån låg.

2.4.2 Offentliggjorda meddelanden och användaruppgifter

Tillitsnivå	Erforderliga beståndsdelar
Låg	1. En offentliggjord tjänstedefinition ska finnas som innefattar alla tillämpliga villkor och avgifter, däribland eventuella begränsningar av användningen. Tjänstedefinitionen ska innefatta en policy för integritetsskydd. 2. Lämpliga policyer och förfaranden ska införas för att tjänsteanvändarna ska informeras i tid och på ett tillförlitligt sätt om eventuella ändringar av tjänstedefinitionen och om alla tillämpliga villkor och policyn för integritetsskydd för den specificerade tjänsten. 3. Lämpliga policyer och förfaranden ska införas så att alla förfrågningar om upplysningar kan besvaras till fullo och på korrekt sätt.
Väsentlig	Samma som nivån låg.
Hög	Samma som nivån låg.

2.4.3 Ledning avseende informationssäkerhet

Tillitsnivå	Erforderliga beståndsdelar
Låg	Det finns ett effektivt ledningssystem för informationssäkerhet för hantering och kontroll av informationssäkerhetsrisker.
Väsentlig	Nivå låg, samt ledningssystemet för informationssäkerhet följer utprovade standarder eller principer för hantering och kontroll av informationssäkerhetsrisker.
Hög	Samma som nivån väsentlig.

2.4.4 Registerföring

Tillitsnivå	Erforderliga beståndsdelar
Låg	1. Registrera och lagra relevant information med hjälp av ett effektivt registerhanteringssystem, med beaktande av tillämplig lagstiftning och god praxis i fråga om skydd och lagring av personuppgifter. 2. Lagra – i den mån det är tillåtet enligt nationell lag eller andra nationella administrativa bestämmelser – och skydda register så länge som de behövs för granskning och undersökning av säkerhetsöverträdelser och för lagring, varefter registren ska förstöras på ett säkert sätt.
Väsentlig	Samma som nivån låg.
Hög	Samma som nivån låg.

2.4.5 Anläggningar och personal

Av följande tabell framgår kraven i fråga om anläggningar och personal och underleverantörer, om tillämpligt, som åtar sig uppgifter som omfattas av denna förordning. Uppfyllandet av vart och ett av kraven ska stå i proportion till den risknivå som är knuten till den tillitsnivå som tillhandahålls.

Tillitsnivå	Erforderliga beståndsdelar
Låg	1. Förfaranden ska finnas som ser till att personal och underleverantörer är tillräckligt utbildade, kvalificerade och erfarna i de färdigheter som krävs för att sköta sina roller. 2. Tillräcklig personal och underleverantörer ska finnas för att korrekt driva och bemanna tjänsten i enlighet med policyer och förfaranden som gäller för den. 3. Anläggningar som används för att tillhandahålla tjänsten ska kontinuerligt övervakas och skyddas mot skador orsakade av miljöhändelser, obehörig åtkomst och andra faktorer som kan inverka på tjänstens säkerhet. 4. Anläggningar som används för att tillhandahålla tjänsten ska säkerställa att tillträde till utrymmen där personliga, kryptografiska eller andra känsliga uppgifter finns eller behandlas, är begränsat till auktoriserad personal eller underleverantörer.
Väsentlig	Samma som nivån låg.
Hög	Samma som nivån låg.

2.4.6 Tekniska kontroller

Tillitsnivå	Erforderliga beståndsdelar
Låg	1. Proportionella tekniska kontroller ska finnas för att hantera riskerna för tjänsternas säkerhet, och för att skydda de behandlade uppgifternas sekretess, integritet och tillgänglighet. 2. Elektroniska kommunikationskanaler som används för att utbyta personuppgifter eller känslig information skyddas mot avlyssning, manipulation och omspelning. 3. Tillgång till känsligt kryptografiskt material, om sådant används för utfärdande av medel för elektronisk identifiering och autentisering, ska strikt begränsas till de befattningar och applikationer som kräver tillgång. Det ska säkerställas att sådant material aldrig ständigt lagras i klartext. 4. Förfaranden finns för att se till att säkerheten upprätthålls över tiden och att förmåga finns att agera om risknivån förändras eller vid incidenter och säkerhetsöverträdelser. 5. Alla medel som innehåller personuppgifter eller kryptografiska eller andra känsliga uppgifter ska lagras, transporteras och bortskaffas på ett säkert sätt.
Väsentlig	Samma som nivån låg, samt känsligt kryptografiskt material, om sådant används för utfärdande av medel för elektronisk identifiering och autentisering, ska skyddas från manipulation
Hög	Samma som nivån väsentlig.

2.4.7 Efterlevnad och revision

Tillitsnivå	Erforderliga beståndsdelar
Låg	Regelbundna interna revisioner, som är utformade så att de omfattar alla delar som är relevanta för tillhandahållandet av tjänster, för att garantera efterlevnaden av relevant policy.

Tillitsnivå	Erforderliga beståndsdelar
Väsentlig	Förekomst av regelbundna oberoende interna eller externa revisioner, som är utformade så att de omfattar alla delar som är relevanta för tillhandahållandet av tjänster, för att garantera efterlevnaden av relevant policy.
Hög	1. Förekomst av regelbundna oberoende externa revisioner, som är utformade så att de omfattar alla delar som är relevanta för tillhandahållandet av tjänster, för att garantera efterlevnaden av relevant policy. 2. Om systemet förvaltas direkt av en statlig myndighet sker revision i enlighet med nationell lagstiftning.