

Väljaandja:	Vabariigi Valitsus
Akti liik:	määrus
Teksti liik:	terviktekst
Redaktsiooni jõustumise kp:	22.01.2011
Redaktsiooni kehtivuse lõpp:	30.11.2014
Avaldamismärge:	RT I, 19.01.2011, 15

Infosüsteemide andmevahetuskiht

Vastu võetud 24.04.2008 nr 78
[RT I 2008, 18, 129](#)
 jõustumine 08.05.2008

Muudetud järgmiste aktidega

Vastuvõtmine	Avaldamine	Jõustumine
13.01.2011	RT I, 19.01.2011, 2	22.01.2011

Määrus kehtestatakse «[Avaliku teabe seaduse](#)» § 43⁹ lõike 1 punkti 5 alusel.

1. peatükk ÜLDSÄTTED

§ 1. Reguleerimisala

Määrusega kehtestatakse nõuded infosüsteemide andmevahetuskihile, selle kasutamisele ja haldamisele.

§ 2. Infosüsteemide andmevahetuskiht

Infosüsteemide andmevahetuskiht (edaspidi *X-tee*) on asutuste ja isikute vahelist turvalist ja tõestusväärtust tagavat internetipõhist andmevahetust ning riigi infosüsteemile turvalist juurdepääsu võimaldav tehniline infrastruktuur ja organisatsiooniline keskkond.

§ 3. X-tee osaline

- (1) X-tee osaline käesoleva määruse tähenduses on asutus või isik, kelle infosüsteem on X-teelega liidestatud.
- (2) Teenuse osutaja on X-tee osaline, kes osutab X-tee kaudu teenuseid.
- (3) Teenuse kasutaja on asutus või isik, kellel on õigus kasutada X-tee teenuseid. Teenuse kasutaja, kelle infosüsteem on X-teelega liidestatud, on ka X-tee osaline (edaspidi *X-tee osalisest teenuse kasutaja*).
- (4) Teenuse vahendaja on X-tee osaline, kelle infosüsteemi vahendusel kasutavad teenuse osutaja infosüsteemi teenuseid asutused ja isikud.

§ 4. X-tee kaudu osutatavad teenused

- (1) Teenus käesoleva määruse tähenduses on X-tee kaudu juurdepääsu saamine teenuse osutaja infosüsteemi ressurssidele.
- (2) Teenused võivad olla esitlusteenus ja talitlusteenus.
- (3) Esitlusteenus on teenuse kasutajale turvalise juurdepääsu võimaldamine teenuse osutaja infosüsteemi esitluskihile ilma konkreetsete andmetega seotud päringuid ja vastuseid eristamata. Esitluskiht on infosüsteemi kasutajaliides, milles liikudes tagatakse kasutajale vajalik teave.
- (4) Talitlusteenus on eeldefineeritud päring-vastus, mille teenuse kasutaja infosüsteem saadab teenuse osutaja infosüsteemile ja mille tulemusena antakse teenuse kasutaja infosüsteemile vastuseks kokkulepitud andmete koosseis.

(5) Talitlusteenus võib vastavalt kasutamise iseärasustele jaguneda järgmiselt:

- 1) baasteenus – teenuse kasutaja ja teenuse osutaja infosüsteemi vaheline ühekordne andmevahetus;
- 2) agregeeritud teenus – teenus kombineeritakse baasteenustest ja vajadusel X-tee välistest teenustest.

§ 5. X-tee toimimise põhimõtted

(1) *Läbipaistvus* – andmete X-tee läbimiseks ei muutu andmete omadused, nagu autentsus, usaldusväärsus, terviklus ja kasutatavus.

(2) *Käideldavus* – X-tee kesksete komponentide hulk on minimeeritud ja X-tee kasutava kahe infosüsteemi vahelise andmevahetuse toimimine on tagatud ka kesksete komponentide töö katkestuse puhul. X-tee infrastruktuur sisaldab vastuvahendeid nii ajutise katkestuse kui ka teenusetõkestamise ründe vastu.

(3) *Konfidentsiaalsus* – konfidentsiaalsus tagatakse andmete krüpteerimisega ja teenuse kasutamise kahetasemelise autoriseerimisega. X-tee kasutamine ei vähenda X-tee osalise infosüsteemi konfidentsiaalsuse taset.

(4) *Sõltumatus platvormist* – X-tee võimaldab mis tahes tarkvaraplatvormil oleval X-tee osalise infosüsteemil suhelda mis tahes tarkvaraplatvormil oleva teenuse osutaja infosüsteemiga. X-tee on realiseeritud tarkvaraplatvormidest sõltumatu rakenduslüüsina.

(5) *Multilateraalsus* – X-tee osalisel on võimalus taotleda juurdepääsu kõigile X-tee kaudu osutatavatele teenustele.

2. peatükk X-TEE ARHITEKTUUR

§ 6. X-tee arhitektuuriline koosseis

X-tee komponendid jagunevad järgmiselt:

- 1) turvaserverid;
- 2) kohalikud jälgimisjaamad;
- 3) X-tee kesksed komponendid;
- 4) lüüsid.

§ 7. X-tee turvaserver

(1) Turvaserver on füüsiliselt eraldiseisev ning X-tee osalise infosüsteemi liidestamiseks X-tee kasutatav arvuti koos sellele paigaldatud eritarkvaraga.

(2) Turvaserver täidab järgmisi ülesandeid:

- 1) krüpteerib ja dekrüpteerib sõnumeid;
- 2) koostab logisid;
- 3) kontrollib teenuse osutaja infosüsteemi puhul teenust kasutava X-tee osalise õigusi;
- 4) tõkestab volitamata X-tee osalise infosüsteemi juurdepääsu teenusele;
- 5) vahendab temaga seotud infosüsteemi sõnumeid teisele X-tee osalisele.

(3) Turvaserver kasutab andmete krüpteerimiseks ja dekrüpteerimiseks X-tee sertifitseerimiskeskuse poolt X-tee osalisele väljastatud sertifikaate.

(4) Turvaserveri käideldavuse, tervikluse ja konfidentsiaalsuse turvaosaklassid peavad olema vähemalt sama kõrged kui temaga seotud X-tee osalise infosüsteemil.

(5) Kui turvaserver teenindab mitut X-tee osalist, peab turvaserveri käideldavus olema vähemalt sama kõrge kui kõrgeima käideldavusega teenindataval infosüsteemil.

(6) Infosüsteemil võib olla mitu paralleelselt töötavat turvaserverit.

§ 8. Kohalik jälgimisjaam

(1) Kohalik jälgimisjaam on X-tee osalise halduses asuvate turvaserverite seisundit jälgiv ja X-tee osalise infosüsteemi kasutamisstatistikat koguv tarkvara.

(2) Kohalikul jälgimisjaamal puudub juurdepääs X-tee osalise turvaserverit läbivatele andmetele.

(3) X-tee osalisel ei ole kohaliku jälgimisjaama kasutamise kohustust.

§ 9. X-tee kesksed komponendid

(1) X-tee kesksed komponendid on:

- 1) keskserver;
- 2) sertifitseerimiskeskus;
- 3) auditeerimisserver;
- 4) keskne jälgimisjaam.

(2) X-tee kesksed komponendid tagavad X-tee käideldavuse läbi kolme kõiki infosüsteeme haarava teenuse:

- 1) serverite sertifitseerimise *offline*-teenus;
- 2) perioodiline ja mitteaegkriitiline ajatempliteenus;
- 3) liiasusega (dubleerimisega) ja lokaalse puhverdamisega kataloogiteenus.

(3) Keskserver väljastab X-tee osalise turvaserverile vajaliku teenuse osutaja turvaserveri aadressi ning vahendab kehtivusinfot X-tee osaliste turvaserverite sertifikaatide kohta. X-teel peab olema mitu paralleelselt erinevates võrkudes töötavat ja geograafiliselt hajutatud keskserverarvutit. Keskserveri turvaklass on K2T1S0 ning turvatase on M.

(4) Sertifitseerimiskeskus on X-tee haldaja organisatsiooniline üksus ja sertifitseerimismenetlust toetav infosüsteem X-tee osalise sertifitseerimiseks. Sertifitseerimisprotsessis kasutatakse riistvaralist turvamoodulit. Sertifitseerimiskeskuse turvaklass on K1T2S3 ning turvatase on H.

(5) Auditeerimisserver on tarkvara, mis võtab vastu ja arhiveerib X-tee osalise infosüsteemist perioodiliste intervallide järel saadetavad räsud. Auditeerimisserveri turvaklass on K2T2S2 ning turvatase on M.

(6) Keskne jälgimisjaam on turvaserverite seisundit jälgiv ja X-tee kasutusstatistikat koguv tarkvara. Kesknel jälgimisjaamal puudub juurdepääs X-tee läbivatele andmetele. Jälgimisjaama turvaklass on K2T1S1 ning turvatase on M.

§ 10. X-tee osalise infosüsteemi roll

(1) Infosüsteem võib olla samaaegselt nii teenuse osutaja, teenuse kasutaja kui ka teenuse vahendaja infosüsteemi rollis.

(2) Kui infosüsteem on nii teenuse osutaja kui ka X-tee osalisest teenuse kasutaja infosüsteemi rollis, siis peavad tal olema nende rollide jaoks erinevad sertifikaadid.

§ 11. Teenuse osutaja infosüsteemi X-teega seotud komponendid

(1) Teenuse osutaja infosüsteemi X-teega seotud komponendid on turvaserver, X-tee adapterserver ning vajadusel kohalik jälgimisjaam.

(2) Teenuse osutaja infosüsteemi X-teega seotud komponendid peavad asuma teenuse osutaja infosüsteemi sisevõrgus.

(3) Teenuse osutaja infosüsteemi X-teega seotud komponentide turvaklass peab olema vähemalt sama kõrge kui teenuse osutaja infosüsteemi turvaklass.

(4) Teenuse osutaja infosüsteemi adapterserver on tarkvara, mis teisendab ja vahendab turvaserverist saabunud päringu infosüsteemi tarkvaraplatvormile mõistetavale kujule, võtab vastu ning teisendab päringu vastuse X-tees nõutud kujule ning edastab selle oma turvaserverile saatmiseks päringu esitanud X-tee osalisele.

§ 12. X-tee osalisest teenuse kasutaja infosüsteemi X-teega seotud komponendid

(1) X-tee osalisest teenuse kasutaja infosüsteemi X-teega seotud komponendid on turvaserver, X-tee kasutajaliides ning vajadusel kohalik jälgimisjaam.

(2) X-tee osalisest teenuse kasutaja infosüsteemi X-tee komponentide turvaklass peab olema vähemalt sama kõrge kui kõige kõrgema turvaklassiga tarbitavatel teenuse kaudu edastatavatel andmetel.

(3) X-tee osalisest teenuse kasutaja infosüsteemi kasutajaliides tagab teenust kasutava füüsilise isiku kasutajaõiguste haldamise ning lubab volitatud füüsilisel isikul teenust kasutada.

(4) X-tee teenuseid võib kasutada mini-infosüsteem-portaali (edaspidi *MISP*) kaudu. *MISP* on standardne käesoleva paragrahvi nõuetele vastav infosüsteem.

§ 13. Teenuse vahendaja infosüsteemi X-teega seotud komponendid

(1) Teenuse vahendaja infosüsteemil on samad X-teega seotud komponendid mis teenuse kasutaja infosüsteemil.

(2) Teenuse vahendaja infosüsteemi turvaklass peab olema vähemalt sama kõrge kui tema kaudu vahendatava kõrgeima turvaklassiga teenuse turvaklass.

(3) Teenuse vahendaja infosüsteemis ei hallata teenust kasutava füüsilise isiku kasutajaõigusi.

§ 14. Lüüs

(1) Lüüs on tarkvara, mis võimaldab turvalist andmevahetust erinevate andmevahetuskeskkondade vahel. Lüüs vahendab oma turvaserveri kaudu päringuid koos teenuse kasutaja autentimist võimaldava infoga.

(2) Lüüsiga ühendatud andmevahetuskeskkondades toimub andmevahetus lüüsi haldaja vastutusel.

(3) Lüüsi turvatase peab olema sama kõrge kui liidestatavatest andmevahetuskeskkondadest kõrgeima turvatasemega andmevahetuskeskkonnal.

(4) Lüüse kasutatakse X-tee väliste andmevahetuskeskkondadega suhtlemiseks.

3. peatükk X-TEEGA LIITUMISE KÕRD JA X-TEE KASUTAMINE

§ 15. X-teega liitumise tingimused

(1) X-teega liitumise taotlemine toimub riigi infosüsteemi halduse infosüsteemi (edaspidi *RIHA*) kaudu.

(2) X-teega liitumisel sõlmib taotleja Riigi Infosüsteemi Arenduskeskusega liitumiskokkuleppe. Liitumiskokkuleppes fikseeritakse poolte õigused, kohustused ja vastutus.

(3) X-teega liitumisel on teenuse osutaja kohustatud:

- 1) tagama X-teega liitumise korral oma infosüsteemi turvalise ja häireteta töö;
- 2) tagama oma infosüsteemi järjepidevuse, haldamise ja arendamise, looma ja avama taotleja põhjendatud ettepanekul vajalikud teenused kahepoolselt kokkulepitud aja jooksul;
- 3) paigaldama turvaserveri, X-tee adapterserveri, vajadusel kohaliku jälgimisjaama ning kohandama oma infosüsteemi tööks X-tee keskkonnas;
- 4) liituma X-tee testkeskkonnaga ja pakkuma seal vastavaid testandmetega teenuseid;
- 5) arhiveerima teenuste päringulogisid;
- 6) töötama välja arhiveerimise protseduuri, kus on kirjas arhiveerimise sagedus ning arhiveeritava info loetelu;
- 7) määrama isikud, kes ja mis tingimustel saavad juurdepääsu arhiveeritud logidele;
- 8) hävitama pärast kasutamist kõrvaldamist turvaserveri privaatsvõtmete või päringulogide hoidmiseks kasutatud andmekandjad (näiteks kõvakettad ja CD-d);
- 9) määrama soovitud andmete X-tee kaudu edastamiseks teenuse osutaja infosüsteemile vajaliku turvataseme;
- 10) registreerima osutatavad teenused koos teenuse kirjeldusega ja teenuse osutamise põhimõtetega RIHA-s;
- 11) tagama pakutavate teenuste liitumiskokkuleppes kokkulepitud käideldavuse;
- 12) tõstma teenuse kasutaja põhjendatud ettepanekul teenuse käideldavuse taseme teenuse kasutajale vajalikule tasemele;
- 13) teavitama lõikes 2 nimetatud asutust ette plaanilistest katkestustest teenuse osutamisel;
- 14) hoidma teenuse kohta käivad andmed RIHA-s aktuaalsena;
- 15) teavitama RIHA kaudu teenuse muudatustest;
- 16) tagama vajadusel lüüsi kaudu infovahetuse teiste riikide infosüsteemidega;
- 17) teavitama viivitamatult lõikes 2 nimetatud asutust rikestest või häiretest X-tee töös;
- 18) täitma muid käesolevas määruses ja liitumiskokkuleppes sätestatud tingimusi.

(4) X-teega liitumisel on teenuse kasutaja ja teenuse vahendaja kohustatud:

- 1) tagama X-teega liidestatud infosüsteemi turvalise ja häireteta töö;
- 2) määrama isikud, kellel on õigus, või ameti- ja töökohad, millel töötades kaasneb õigus esitada päringuid X-tee kaudu;
- 3) määrama X-tee kaudu soovitud andmete kasutamiseks oma infosüsteemile vajaliku turvataseme;
- 4) paigaldama turvaserveri, X-tee kasutajaliidese, vajadusel kohaliku jälgimisjaama ning kohandama oma infosüsteemi tööks X-tee keskkonnas;
- 5) rakendama vajalikud turvameetmed, et saada õigus soovitud teenuse kasutamiseks;
- 6) X-tee kasutamisel ainult andmete lugemiseks rakendama turvameetmeid, mis on vähemalt sama kõrge turvaklassiga kui kõrgeima turvaklassiga teenusel, mida ta kasutab;
- 7) tagama, et tema poolt kasutatavad andmekaitse abinõud vastavad õigusaktides sätestatud ja teenuse osutajalt saadavatest andmetest tulenevatele tingimustele;
- 8) teavitama viivitamatult lõikes 2 nimetatud asutust rikestest või häiretest X-tee töös;
- 9) täitma muid käesolevas määruses ja liitumiskokkuleppes sätestatud tingimusi.

(5) X-teega liitumisel liidestatakse liituja infosüsteem X-teega.

(6) X-teega liitumisel määratakse liituja asutuse või isiku infosüsteemi X-teega toimimise eest vastutaja ja turvaserveri administraator.

(7) X-teelega liitumise järel tagatakse liitunud asutusele või isikule X-tee keskkonna kasutamine.

§ 16. X-teelega liitumisest keeldumine ja X-teelega liitumise kehtetuks tunnistamine

(1) Asutuse või isiku infosüsteemi ei liideta X-teelega, kui asutus või isik või tema infosüsteem ei vasta käesolevas määruses toodud nõuetele või X-tee toimimise põhimõtetele.

(2) X-tee osalise liitumise X-teelega võib kehtetuks tunnistada, kui

- 1) X-tee osaline on esitanud liitumisel valesid või eksitavaid andmeid;
- 2) X-tee osaline on rikkunud käesolevas määruses või liitumiskokkuleppes sätestatud tingimusi;
- 3) X-tee osaline kasutab X-tee teenuseid pahatahtlikult.

§ 17. X-tee kasutamine ja kasutamise eest tasu võtmine

(1) Füüsilisele isikule on tagatud ühetaoline juurdepääs portaali «eesti.ee» kaudu kõigile autoriseerimist mittedõudvatele teenustele.

(2) X-tee komponentide tarkvara ja MISP-i kasutamise eest tasu ei võeta.

(3) X-tee kaudu võib osutada tasulisi teenuseid.

(4) X-tee osalise infosüsteemi liidestamise, arendamise ja haldamise kulud katab X-tee osaline. Autentimisteenuse kulud katab X-tee osalisest teenuse kasutaja või teenuse vahendaja.

§ 18. Autentimine ja autoriseerimine

(1) X-tee osaline autentitakse talle X-tee sertifitseerimiskeskuse poolt väljastatud sertifikaadi põhjal.

(2) Füüsiline isik autentitakse Eesti või muu Euroopa Liidu liikmesriigi tunnustatud sertifikaadiga X-tee osalisest teenuse kasutaja või teenuse vahendaja infosüsteemis. Autentimiseks kasutatav sertifikaat peab vastama „Digitaalallkirja seaduses“ sertifikaatidele ja sertifikaadiga seotud teenustele esitatud nõuetele. [RT I, 19.01.2011, 2- jõust. 22.01.2011]

(3) Avaliku teabe kasutajat autentima ei pea.

(4) Kui baasteenuse algatajaks on infosüsteem, siis loetakse teenust kasutavaks füüsiliseks isikuks baasteenuse algataja infosüsteemi eest vastutav füüsiline isik.

(5) X-tee osalisest teenuse kasutaja autoriseeritakse teenuse osutaja infosüsteemis.

(6) Füüsiline isik autoriseeritakse X-tee osalisest teenuse kasutaja või teenuse vahendaja infosüsteemis, läbi mille ta teenust kasutab.

(7) Teenuse vahendaja infosüsteem saab autoriseerimisinfo teistest infosüsteemidest.

§ 19. Tehnilised ja andmeturbenõuded

(1) Infosüsteemile määratakse turvaklass ja turvaklassile vastavad turvameetmed võetakse kasutusele vastavalt «Avaliku teabe seaduse» § 43⁹ lõike 1 punkti 4 alusel kehtestatud määrusele.

(2) X-tee kasutamine on võimalik vaid eelnevalt X-tee sertifitseerimiskeskuse poolt väljastatud sertifikaadiga varustatud turvaserveri kaudu, kus andmevahetus krüpteeritakse ja allkirjastatakse turvaserveri sertifikaadiga ning varustatakse krüptograafiliselt aheldatud logiga, et tagada selle hilisem võltsimatus ja terviklus. Logisid tuleb säilitada vähemalt kolm aastat. X-tee osaline võib logide säilitamisele määrata pikema tähtaja.

(3) Esitlusteenuse puhul ei logita teenuse kasutaja tegevust teenuse osutaja infosüsteemi turvaserveris.

(4) Talitlusteenuse päringud logitakse teenuse osutaja infosüsteemi turvaserveris ja vastused päringu sooritanud X-tee osalise infosüsteemi turvaserveris.

(5) X-tee kasutamisega seonduvad probleemid ja turvaintsidendid fikseeritakse RIHA-s.

(6) X-tee osaline vastutab oma andmekogu pidamiseks kasutatava infosüsteemi turvalisuse eest vastavalt töödeldavate andmete turvaklassile.

(7) Julgeolekuasutuste poolt jälitustegevuse käigus «Julgeolekuasutuste seaduse» §-des 25 ja 26 sätestatud viisil kogutud teabega seotud päringute logid teenuse osutaja turvaserveris salvestatakse ja hoitakse turvaserveri

poolt krüpteeritud kujul. Logide lahtikrüpteerimine on võimalik ainult selleks spetsiaalselt sisustatud ruumis Riigikogu julgeolekuasutuste järelevalve erikomisjoni poolt.

§ 20. Juurdepääs andmetele

(1) Teenuse osutaja infosüsteemi haldaja teeb X-tee kaudu kättesaadavaks andmed, millele ei ole kehtestatud juurdepääsupiirangut.

(2) Juurdepääsuõigus konkreetsetele andmetele, teenusega seotud turvanõuded ning teenust iseloomustavad kvaliteedinõuded fikseeritakse iga konkreetse teenuse jaoks selle teenuse kirjelduses.

(3) X-teenusega liitunud asutus või isik vastutab tema turvaserveri kaudu teenuse kasutaja X-tee keskkonnale juurdepääsuõiguste andmise eest.

4. peatükk X-TEE HALDAMINE JA ARENDAMINE

§ 21. X-tee haldamine ja arendamine

(1) Majandus- ja Kommunikatsiooniministeerium koordineerib X-tee haldamist ja arendamist ning vastutab X-tee toimimise eest, sealhulgas:

- 1) vastutab X-tee järjepidevuse, haldamise ja arendamise eest;
- 2) teostab järelevalvet X-tee vastavuse üle kokkulepitud kvaliteedinäitajatele;
- 3) vaatab läbi ja kooskõlastab X-tee infrastruktuuri arendusprojektid;
- 4) lahendab X-tee kasutamise ja arendamisega seotud vaidlusi.

(2) Riigi Infosüsteemide Arenduskeskus täidab Majandus- ja Kommunikatsiooniministeeriumi juhiseid ja tagab X-tee haldamise ja arendamise, sealhulgas:

- 1) nõustab ja koolitab asutusi ja isikuid X-teenusega seotud küsimustes;
- 2) monitoorib X-tee kasutamist ja käsitleb turvaintsidente;
- 3) teostab X-tee aruandlust ja kasutusstatistikat;
- 4) valmistab ette ja viib läbi X-tee infrastruktuuri arendusprojektid;
- 5) toetab infosüsteemide uute teenuste avamisel ja osaleb infosüsteemide integratsiooniprojektides;
- 6) võimaldab vajadusel lüüsi kaudu infovahetust teiste riikide infosüsteemidega.

(3) X-tee komponentide tarkvara arendamise eest vastutavad järgmised institutsioonid:

- 1) X-tee arhitektuuri arendamise eest vastutab Majandus- ja Kommunikatsiooniministeerium;
- 2) X-tee kesksete komponentide arendamise eest vastutab Riigi Infosüsteemide Arenduskeskus;
- 3) portaali «eesti.ee» X-tee teenuste kasutajaliidese arendamise eest vastutab Riigi Infosüsteemide Arenduskeskus;
- 4) turvaserveri tarkvara arendamise eest vastutab Riigi Infosüsteemide Arenduskeskus;
- 5) teenust osutava infosüsteemi adapterserveri eest vastutab seda infosüsteemi haldav asutus või isik;
- 6) teenust kasutava infosüsteemi tarkvara arendamise eest vastutab seda infosüsteemi haldav asutus või isik;
- 7) MISIP-i tarkvara arendamise eest vastutab Riigi Infosüsteemide Arenduskeskus.

(4) X-tee tarkvara levitatakse vastavalt Euroopa Liidu tarkvara vaba kasutuse litsentsile EUPL (*the European Union Public Licence*).

5. peatükk RAKENDUSSÄTTED

§ 22. Määruse rakendamine

(1) Riigi Infosüsteemide Arenduskeskus loob täiendavad X-tee teenused autoriseerimisinfo edastamiseks teenuse vahendaja infosüsteemidesse X-tee osalisest teenuse kasutaja infosüsteemidest ja integreerib selle teenuse kasutamise võimaluse MISIP-i hiljemalt 1. septembriks 2008. a.

(2) Internetipankade autentimissüsteeme võib kasutada kuni „Isikut tõendavate dokumentide seaduse“ § 20¹ lõike 2 kohaselt Vabariigi Valitsuse määratud isikutele digitaalse isikutunnistuse väljaandmise alustamise ajani.
[RT I, 19.01.2011, 2- jõust. 22.01.2011]

(3) Kui andmekogu ei ole põhjendatult võimalik liidestada riigi infosüsteemi andmevahetuskihiga vastavalt «Avaliku teabe seaduse» § 58¹ lõikes 1 toodule 1. juuliks 2008. a, esitab vastutav töötaja Majandus- ja Kommunikatsiooniministeeriumile hiljemalt 1. juuniks 2008. a sellekohase taotluse ja liidestamise ajakava.

§ 23. Määruse jõustumine

Määruse § 13 lõige 3 jõustub 1. septembril 2008. a.