Հավելված
ՀՀ կառավարության 2025 թվականի
հուլիսի 24-ի N 1015 - Ն որոշման

Կ Ա Ր Գ

ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅԱՆ ՀԱՎԱՍՏԱԳՐՄԱՆ ԿԵՆՏՐՈՆՆԵՐԻ ՀԱՎԱՏԱՐՄԱԳՐՄԱՆ

1. ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

1. Սույն կարգով սահմանվում է էլեկտրոնային թվային ստորագրության հավաստագրման կենտրոնների (այսուհետ՝ հավաստագրման կենտրոն) հավատարմագրման կարգը:

2. Հավատարմագրումն իրականացնում է Հայաստանի Հանրապետության կառավարության լիազորած մարմինը (այսուհետ՝ լիազոր մարմին):

3. Էլեկտրոնային թվային ստորագրության հավաստագրման կենտրոնների հավատարմագրման համար դրանց կողմից տրամադրվող էլեկտրոնային թվային ստորագրության հավաստագրերը և էլեկտրոնային թվային ստորագրությունների հետ կապված այլ մատուցվող ծառայությունները պետք է համապատասխանեն սույն կարգով սահմանված պահանջներին և չափանիշներին:

2. ՀԱՎԱՍՏԱԳՐՄԱՆ ԿԵՆՏՐՈՆՆԵՐԻ ՀԱՎԱՏԱՐՄԱԳՐՄԱՆ ԸՆԹԱՑԱԿԱՐԳԸ

4. Հավաստագրման կենտրոնի հավատարմագրման համար հիմք են ծառայում հավաստագրման կենտրոնի կողմից տրամադրվող էլեկտրոնային թվային ստորագրության հավաստագրերի, այդ հավաստագրերին համապատասխանող էլեկտրոնային թվային ստորագրությունների ստեղծման ապարատային կամ ծրագրային միջոցների ու իր կողմից մատուցվող էլեկտրոնային թվային ստո-

րագրությունների հետ կապված այլ ծառայությունների՝ Հայաստանի Հանրապետության կառավարության հաստատած չափանիշներին համապատասխանության սերտիֆիկատները՝ տրված Հայաստանի Հանրապետության օրենսդրությամբ սահմանված կարգով լիազոր մարմնի կողմից միակողմանիորեն կամ երկկողմանիորեն ճանաչված տեղական կամ միջազգային սերտիֆիկացնող մարմինների կողմից:

5. Հավաստագրման կենտրոնը կարող է հավատարմագրվել՝

1) լիազոր մարմնի կողմից ճանաչման կարգով, եթե ներկայացվել է «eIDAS» կանոնակարգով սահմանված ստանդարտների հիման վրա առնվազն երկու ԵՄ երկրում համանման համակարգի ներդրում ապահովված ընկերության կողմից տրված հավաստում (proof of concept, POC) կամ նման ներդրումն ապահովված ընկերության հետ փայամասնակցությամբ գործունեություն ծավալելու փաստը հիմնավորող փաստաթղթեր.

2) հավաստագրման կենտրոնի կողմից լիազոր մարմնին դիմելու միջոցով, եթե դիմումին կից ներկայացվում են սույն կարգի 4-րդ կետում նշված հիմքերը:

6. Լիազոր մարմինն անհրաժեշտ հիմքերի առկայության դեպքում հավատարմագրում է հավաստագրման կենտրոնը և կատարում համապատասխան գրառում հավատարմագրված հավաստագրման կենտրոնների մատյանում (ռեգիստրում), ինչի մասին եռօրյա ժամկետում գրավոր տեղեկացնում է հավաստագրման կենտրոնին՝ լիազոր մարմնի պաշտոնական էլեկտրոնային հասցեով հաղորդագրություն ուղարկելով դիմող հավաստագրման կենտրոնին:

7. Սույն կարգի 5-րդ կետով սահմանված հավատարմագրումը մերժվում է, եթե լիազոր մարմնի հիմնավորված դիրքորոշման համաձայն չի ապահովվում հավաստագրման կենտրոնի գործունեության անընդհատությունը, անվտանգությունը, կամ դիմողը չի համապատասխանում սույն կարգի 16-րդ կետի պայմաններին, կամ դիմողի ներկայացրած փաստաթղթերը ակնհայտ կեղծ են կամ խեղաթյուրված, կամ ներկայացված փաստաթղթերը չեն համապատասխանում օրենքի և դրա հիման վրա ընդունված ենթաօրենսդրական ակտերի պահանջներին: Եթե դիմողի ներկայացրած փաստաթղթերը թերի են կամ ոչ ամբողջական,

ապա լիազոր մարմինը եռօրյա ժամկետում գրավոր տեղեկացնում է դիմողին՝ թերությունները վերացնելու կամ ամբողջականությունն ապահովելու համար՝ համապատասխան հիմնավորմամբ:

8. Հավատարմագրված հավաստագրման կենտրոնների կամ այլ շահագրգիռ անձանց կողմից համապատասխան դիմումի առկայության դեպքում լիազոր մարմինը տրամադրում է հավաստագրման կենտրոնի հավատարմագրման մասին տեղեկանք:

3. ՀԱՎԱՏԱՐՄԱԳՐՈՒՄՆ ՈՒԺԸ ԿՈՐՑՐԱԾ ՃԱՆԱՉԵԼԸ

9. Լիազոր մարմինը կարող է հավաստագրման կենտրոնին դատական կարգով զրկել հավատարմագրումից, եթե վերահսկման ընթացքում լիազոր մարմնի կողմից բացահայտվել են հավաստագրման կենտրոնի տրամադրած էլեկտրոնային թվային ստորագրությունների հավաստագրերի, դրանց համապատասխանող էլեկտրոնային թվային ստորագրությունների ստեղծման ապարատային կամ ծրագրային միջոցների ու էլեկտրոնային թվային ստորագրությունների հետ կապված՝ մատուցվող այլ ծառայությունների անհամապատասխանություններ Հայաստանի Հանրապետության օրենսդրությանը կամ սերտիֆիկատներում նշված չափանիշներին:

4. ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅԱՆ ՀԱՎԱՍՏԱԳՐԻ ՁԵՎԱՉԱՓԸ ԵՎ ԱԼԳՈՐԻԹՄԸ

10. Հավատարմագրվող հավաստագրման կենտրոնների կողմից տրամադրվող էլեկտրոնային թվային ստորագրության հավաստագրերը պետք է համապատասխանեն հետևյալ ալգորիթմների ստանդարտներից որևէ մեկին՝

1) առնվազն 1024 բիտ երկարությամբ բանալի ունեցող, դիսկրետ լոգարիթմների վրա հիմնված ալգորիթմներ.

2) առնվազն 512 բիտ երկարությամբ բանալի ունեցող, էլիպտիկ կորերի վրա հիմնված ալգորիթմներ.

3) 2025 թվականի հունվարի 1-ից հետո հավատարմագրման համար դիմելու դեպքում՝ առնվազն 4096 բիտ երկարությամբ բանալի ունեցող, դիսկրետ լոգարիթմների վրա հիմնված ալգորիթմներ կամ առնվազն 256 բիտ երկարությամբ բանալի ունեցող, էլիպտիկ կորերի վրա հիմնված ալգորիթմներ:

11. Հավատարմագրվող հավաստագրման կենտրոնների կողմից տրամադրվող էլեկտրոնային թվային ստորագրության հավաստագրի ձևաչափը պետք է համապատասխանի Հեռահաղորդակցության միջազգային կազմակերպության կողմից մշակված հանրային (բաց) կրիպտոգրաֆիկ բանալիների (ստուգման տվյալների) տարածման և նույնականացման չափանիշներին: Պետական և տեղական ինքնակառավարման մարմիններում շրջանառվող փաստաթղթերը ստորագրելու արդյունքում հավաստագրման կենտրոնի տեղեկատվական համակարգերում ստորագրված փաստաթղթերը չպետք է պահպանվեն:

5. ԾԱՌԱՅՈՒԹՅՈՒՆՆԵՐԻՆ, ՀԱՄԱԿԱՐԳԵՐԻՆ ԵՎ ԱՊԱՐԱՏԱԾՐԱԳՐԱՅԻՆ ՄԻՋՈՑՆԵՐԻՆ ՆԵՐԿԱՅԱՑՎՈՂ ՊԱՀԱՆՋՆԵՐԸ

12. Հավատարմագրվող հավաստագրման կենտրոնների կողմից էլեկտրոնային թվային ստորագրության հավաստագրերի տնօրինման համակարգերը, այդ հավաստագրերին համապատասխանող էլեկտրոնային թվային ստորագրությունների ստեղծման ապարատածրագրային միջոցներն ու ծառայությունների մատուցման գործընթացները պետք է համապատասխանեն Ստանդարտացման միջազգային կազմակերպության կողմից ընդունված տեղեկատվության անվտանգության կառավարման և տեղեկատվական համակարգերի անվտանգության հետևյալ սկզբունքներին՝ անհատական տվյալների գաղտնիության և այլ տեղեկատվության պատշաճ ֆիզիկական ու էլեկտրոնային պաշտպանվածության ապահովում, անվտանգության ռիսկերի արդյունավետ կառավարում, կիբեռանվտանգության բավարար մակարդակի ապահովում, անվտանգության կանոնների, այդ թվում՝ կիբեռանվտանգության, ապահովումը երաշխավորող համապա-

տասխան անձնակազմի և ապարատածրագրային միջոցների առկայություն, տեղեկատվության անվտանգության կանոնների ապահովվածության վերաբերյալ հաճախորդների և այլ շահագրգիռ անձանց իրազեկվածության ապահովում (օրինակ՝ ԻՍՕ 27001):

13. Հավատարմագրվող հավաստագրման կենտրոնները կարող են մատուցել հետևյալ ծառայությունները՝

1) նույնականացման քարտի կիրառմամբ էլեկտրոնային թվային ստորագրության թողարկում և տրամադրում.

2) բջջային էլեկտրոնային թվային ստորագրության թողարկում և տրամադրում.

3) հեռավար էլեկտրոնային թվային ստորագրության (Remote Signature Creation) թողարկում և տրամադրում:

14. Հավաստագրման կենտրոնը 13-րդ կետում նշված ծառայությունները մատուցելիս պարտավոր է ստորագրության ստեղծման համակարգին (հավաստագրի առցանց ստուգման արձանագրության (OCSP) միջոցով) տրամադրել յուրաքանչյուր էլեկտրոնային թվային ստորագրության ստեղծման և ստուգման տվյալները կամ հավաստագրերը:

15. Հավաստագրման կենտրոնները չեն կարող մատուցել էլեկտրոնային թվային ստորագրության հետ չկապված այլ ծառայություններ կամ կատարել այլ աշխատանքներ:

16. Հավատարմագրվող հավաստագրման կենտրոնները պետք է որպես իրավաբանական անձ գրանցված լինեն պետական միասնական գրանցամատյանում և բավարարեն հետևյալ պայմաններին՝

1) ապահովեն իրենց ծառայությունների սակագների գնագոյացման հիմնավորված քաղաքականություն, առնվազն հրապարակեն իրենց կողմից մատուցվող ծառայություններից յուրաքանչյուրի պայմանագրերի օրինակելի ձևերը, գները, մատուցման ընթացակարգը.

2) լիազոր մարմնին տեղեկացնեն մատուցվող ծառայություններում տեխնոլոգիական փոփոխությունների մասին այդպիսի փոփոխություն կատարելուց

առնվազն տասն աշխատանքային օր առաջ, ինչպես նաև ծանուցեն գործունեությունը դադարեցնելու մտադրության մասին գործունեությունը դադարեցնելուց առնվազն երկու ամիս առաջ.

3) անձնական տվյալների պաշտպանության ապահովման նպատակով համապատասխանեն «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի և դրա հիման վրա ընդունված ենթաօրենսդրական ակտերի պահանջներին, որը հավաստվելու է անձնական տվյալների պաշտպանության ոլորտում լիազորված մարմնի կողմից իրավաբանական անձի անձնական տվյալներ մշակող էլեկտրոնային համակարգերը բավարար պաշտպանության մակարդակ ունեցող ճանաչվելու միջոցով.

4) համապատասխանեն «Էլեկտրոնային փաստաթղթի և էլեկտրոնային թվային ստորագրության մասին» ՀՀ օրենքով և դրա հիման վրա ընդունված ենթաօրենսդրական ակտերով սահմանված պահանջներին և ապահովեն այդ իրավական ակտերով սահմանված պարտականությունների կատարումը.

5) ապահովեն, որ իրենց կողմից օգտագործվող ծրագրասարքավորումային համալիրները գտնվեն Հայաստանի Հանրապետության տարածքում, և դրանք չեն կարող ուղղակի կամ անուղղակիորեն, բաժնային մասնակցությամբ ամբողջությամբ կամ մասնակիորեն պատկանել օտարերկրյա պետությանը կամ օտարերկրյա պետական մասնակցությամբ ընկերություններին (կոնսորցիումներին).

6) էլեկտրոնային թվային ստորագրությունների ստեղծման համար օգտագործեն համապատասխանության անկախ գնահատում անցած սարքեր և սարքավորումներ.

7) հնարավոր վնասների համար ապահովագրեն իրենց ռիսկը՝ 2 մլրդ դրամի չափով կամ ներկայացնեն բավարար ֆինանսական միջոցներ՝ նույն չափով դրամական կամ երաշխիքի տեսքով, որն անձեռնմխելի է և պահպանվում է գործունեության ամբողջ ընթացքում.

8) ամրագրեն իրենց կապիտալի չափը կանոնադրությամբ, որը չի կարող պակաս լինել 1 մլրդ դրամից.

9) ապահովեն էլեկտրոնային ստորագրությունների վկայագրերի համապատասխանությունը ԻԹիԷսԱյ ԹիԷս (ETSI TS) 319 412-1 ստանդարտով սահմանված վկայագրի պրոֆիլի պահանջներին:

17. Հավաստագրման կենտրոնները մշակում, կիրառում, ըստ անհրաժեշտության թարմացնում են ստորև նշված փաստաթղթերը՝ ապահովելով ստորագրության ստեղծման կիրառական ծառայության բաղադրիչի (SCASC) համապատասխան փաստաթղթավորում առնվազն հետևյալ ուղղություններով՝

1) գործելակարգի հայտարարություն (statement) ստորագրության ստեղծման ծառայության կիրառական բաղադրիչի համար.

2) թվային ստորագրության ստեղծման ընթացակարգեր, այդ թվում՝ էլեկտրոնային թվային ստորագրության հավաստագիրը տրամադրելուց առաջ անձը հաստատող փաստաթղթերի հիման վրա անձի նույնականացման ընթացակարգը: Ընթացակարգերում կարևոր է հստակեցնել այն չափանիշները, որոնք որպես գործընթացների ներքին կանոններ որդեգրել է հավաստագրման կենտրոնը, և որոնց հիման վրա ստեղծվում են թվային ստորագրությունները.

3) ստորագրության կիրառելիության կանոններ, որոնք կարող են ներառել ստորագրության ստեղծման ծրագրի (SCA) կողմից կիրառվելիք ստորագրության ստեղծման սահմանափակումները, ինչպես նաև այլ չափանիշներ, որոնք նկարագրում են ստորագրության կիրառելիությունը որոշակի գործարար պահանջների համար.

4) ստորագրության ստեղծման քաղաքականություն, որը ներկայացնում է ստորագրության ստեղծման պայմանների, պահանջների և սահմանափակումների ամբողջությունը, որը մշակվում է ստորագրության ստեղծման ծրագրի կողմից.

5) անձնական տվյալների մշակման գործընթացների պայմաններն ու պահանջները, որոնք բացահայտում են անձնական տվյալների անվտանգ մշակման և գաղտնիության ապահովման ընթացակարգը, անձնական տվյալները պաշտպանելու միջոցառումները:

6) ստորագրության ստեղծման ծառայության գործարկման և կիրառական կառավարման փաստաթուղթ, որն առնվազն պետք է ներկայացնի հետևյալ տեղեկատվությունը՝ հաշվի առնելով միջազգային լավագույն փորձը.

ա. կազմակերպության ներքին կառավարման համակարգի նկարագրություն,

բ. մարդկային ռեսուրսների կառավարման նկարագրություն և ընտրության նվազագույն չափանիշներ: Անձնակազմի և պայմանագրային հարաբերությունների հիման վրա աշխատանքներ կատարող և ծառայություններ մատուցող անձանց ընտրության չափանիշները պետք է հիմնված լինեն առնվազն հետևյալ սկզբունքների վրա՝ անհրաժեշտ փորձ, որակավորում, հուսալիություն, համապատասխան գիտելիք անվտանգության և անձնական տվյալների պաշտպանության կանոնների վերաբերյալ,

գ. ակտիվների կառավարում,

դ. մուտքերի վերահսկում,

ե. կրիպտոգրաֆիական վերահսկողություն,

զ. ֆիզիկական անվտանգություն,

է. գործառնական անվտանգություն,

ը. ցանցային անվտանգություն,

թ. միջադեպերի կառավարում,

ժ. ապացույցների փաստագրում և պահպանում, այդ թվում, բայց չսահմանափակվելով՝ գործողությունների գրանցամատյանները պետք է պարունակեն յուրաքանչյուր գործողության ժամանակային նշում, պետք է փաստագրվի ցանկացած թվային ստորագրության ստեղծման և բաժանորդի նույնականացման գործողություն: Մշակման հաճախականությունը, պահպանման ժամկետը, պաշտպանության միջոցները, տվյալների պահուստավորման ընթացակարգերը, փաստագրման համակարգի արխիվացման գործընթացները, ինչպես նաև միջոցառումների գրանցամատյանների խոցելիության գնահատումը պետք է նկարագրվեն SCASC-ի գործելակարգի հայտարարության մեջ: Բացի այդ՝ գործողությունների գրանցամատյանները պետք է պարունակեն գործողության տեսակը, դրա հաջող ընթացքի կամ խզման կամ այլ խափանման մասին տեղեկությունը,

ինչպես նաև տվյալ գործողության սկզբնաղբյուրի (անձի կամ բաղադրիչի) նույնականացուցիչը,

ժա. ստորագրվող տվյալների պահպանումը բացառող մեթոդի նկարագրություն,

ժբ. ծառայությունների մատուցման գործընթացներում օգտագործվող համակարգերի, սարքերի, սարքավորումների և ապրանքների որակը, տեխնիկական անվտանգությունը ու հուսալիությունն ապահովող չափանիշները, հատկանիշները և նկարագրությունը, նշում սերտիֆիկացման առկայության կամ դրա բացակայության մասին: Սերտիֆիկացում անցած լինելու դեպքում հիմնավորող փաստաթղթերը կցվում են լիազոր մարմին ներկայացվող հայտին,

ժգ. հավաստագրման կենտրոնի գործունեության կամ ծառայությունների մատուցման դադարեցման արդիական ծրագիր: Նշված ծրագիրը ենթակա է վերանայման և թարմացման առնվազն երկու տարին մեկ անգամ,

ժդ. մատուցվող ծառայությունների սխեմաների նկարագրությունը,

ժե. հավաստագրման կենտրոնի գործունեության անընդհատության տնտեսական ծրագիրը, որը պետք է կազմված լինի առաջիկա երեք տարվա համար և պարունակի ներքին կազմակերպական կառուցվածքը, եկամուտների և ծախսերի հաշվարկը, հեռանկարային զարգացման միտումները, ներդրումների կանխատեսվող նկարագրությունը, միջոցների ներգրավման հիմնական գործիքները, մրցակցությանը դիմակայելու մեթոդները, կառավարման սկզբունքները և հնարավոր ռիսկերի գնահատումը:

18. Թվարկված բոլոր փաստաթղթերը հայտի հետ միաժամանակ ներկայացվում են լիազոր մարմին, ուսումնասիրվում և գնահատվում են համապատասխանության գնահատման ընթացքում: Լիազոր մարմինն ուսումնասիրում է հավաստագրման կենտրոնի և նրա կողմից մատուցվող ծառայությունների համապատասխանությունը օրենսդրական ակտերին և սույն կարգի 17-րդ կետով նշված փաստաթղթերին:

19. «Էլեկտրոնային փաստաթղթի և էլեկտրոնային թվային ստորագրության մասին» ՀՀ օրենքի 15-րդ հոդվածով նախատեսված վերահսկողություն

ապահովելու նպատակով էլեկտրոնային թվային ստորագրության հավաստագրման կենտրոնները պարտավոր են անցնել սույն կարգի պահանջներին համապատասխանության անկախ աուդիտ առնվազն երկու տարին մեկ անգամ, որն առնվազն ներառում է ծառայությունների որակի, գործընթացների, տեխնոլոգիական լուծումների և տեխնիկական ենթակառուցվածքի անվտանգության, ինչպես նաև գործընթացների իրավական համապատասխանության և բիզնես կենսունակության, այդ թվում՝ ֆինանսական, գնահատականները: Աուդիտի արդյունքները ստանալուց հետո երեք աշխատանքային օրվա ընթացքում այն պետք է ներկայացվի լիազոր մարմին:

20. Հավաստագրման կենտրոնի կողմից ներկայացված աուդիտի բացահայտումների շտկման հարցում հավաստիանալու նպատակով կամ եթե աուդիտի արդյունքները գնահատել է ոչ արժանահավատ կամ առկա է հիմնավոր կասկած, որ էլեկտրոնային թվային ստորագրության հավաստագիրը կարող է կեղծվել կամ դրա օգտագործումը կարող է վնաս պատճառել ստորագրող անձին կամ երրորդ անձի, ապա լիազոր մարմինը կարող է՝

1) իր միջոցներով ցանկացած պահի անցկացնել միջանկյալ աուդիտ.

2) հավաստագրման կենտրոնից պահանջել հավաստագրման կենտրոնի միջոցների հաշվին անցնել սույն հավելվածի 4-րդ կետով նախատեսված համապատասխանության գնահատման գործընթաց և լիազոր մարմին ներկայացնել համապատասխանության սերտիֆիկատները կամ դրանց վերահաստատումը:

21. Իրեն հայտնի դարձած անձնական տվյալների պաշտպանության կանոնների խախտման դեպքում լիազոր մարմինը պարտավոր է այդ մասին 5 աշխատանքային օրվա ընթացքում տեղեկացնել տվյալների պաշտպանության օրենքով նախատեսված մարմիններին:

22. Սույն կարգի 19-րդ կետում նշված անկախ աուդիտն իրականացնող իրավաբանական անձը պետք է ունենա համապատասխան որակավորում և հավատարմագրում էլեկտրոնային թվային ստորագրության հավաստագրման կենտրոնների աուդիտ իրականացնելու համար՝ տրված Եվրոպական միության անդամ երկրներից մեկում:

23. Լիազոր մարմինը միջանկյալ աուդիտ իրականացնելու գործընթացին կարող է ներգրավել համապատասխան մասնագիտական կարողություններ ունեցող կառույցների կամ փորձագետների:

24. Հավաստագրման կենտրոնները սույն կարգի 13-րդ կետի 1-ին, 2-րդ և 3-րդ ենթակետերով նախատեսված ծառայություններից յուրաքանչյուրի համար հավատարմագրում պետք է ստանան առանձին:

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ
ՎԱՐՉԱՊԵՏԻ ԱՇԽԱՏԱԿԱԶՄԻ
ՂԵԿԱՎԱՐԻ ՏԵՂԱԿԱԼ Ա. ԽԱՉԱՏՐՅԱՆ