Հավելված N 1
ՀՀ կառավարության 2017 թվականի
մայիսի 25-ի N 572 - Ն որոշման

Կ Ա Ր Գ

ՊԵՏԱԿԱՆ ՄԱՐՄԻՆՆԵՐՈՒՄ ԷԼԵԿՏՐՈՆԱՅԻՆ ՓԱՍՏԱԹՂԹԵՐԻ ԵՎ ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅՈՒՆՆԵՐԻ ԿԻՐԱՌՄԱՆ

I. ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

1. Սույն կարգով կարգավորվում են պետական մարմիններում էլեկտրոնային փաստաթղթերի և էլեկտրոնային թվային ստորագրությունների կիրառման առանձնահատկությունների հետ կապված հարաբերությունները:

2. Հայաստանի Հանրապետության պետական մարմինները պարտավոր են օրենքով նախատեսված ծառայություններն էլեկտրոնային համակարգերի միջոցով մատուցելու դեպքում էլեկտրոնային հարթակներում կամ ինտերնետային կայքերում ապահովել առցանց եղանակով անհատի խիստ նույնականացման ծրագրային գործիքների կիրառմամբ տեղեկատվական համակարգեր մուտք գործելու, նման համակարգերում էլեկտրոնային փաստաթղթեր (այդ թվում՝ դիմումներ, հարցումներ և հայտեր) ներկայացնելու, ինչպես նաև նման էլեկտրոնային փաստաթղթերն էլեկտրոնային թվային ստորագրությամբ հավաստելու տեխնիկական հնարավորություն:

3. Պետական մարմինների կողմից և պատվիրակված լիազորությունների շրջանակներում այլ անձանց կողմից տեղեկատվական համակարգերում էլեկտրոնային փաստաթղթեր կազմելու նպատակով անձնական տվյալների շրջանառությունը կատարվում է Հայաստանի Հանրապետության կառավարության 2017 թվականի փետրվարի 16-ի N 192-Ն որոշմամբ սահմանված կարգով:

4. Պետական մարմինների տեղեկատվական համակարգերում անհատի խիստ նույնականացման գործիքների շարքին է դասվում հավաստագրման կենտրոնի կողմից Հայաստանի Հանրապետության նույնականացման քարտում զետեղված անհատական հավաստագրի վավերությունը հավաստագրման կենտրոնի կողմից սահմանված ծրագրային եղանակներից որևէ մեկով ստուգելու տեխնիկական հնարավորությունը:

II. ՊԵՏԱԿԱՆ ՄԱՐՄԻՆՆԵՐՈՒՄ ԷԼԵԿՏՐՈՆԱՅԻՆ ՓԱՍՏԱԹՂԹԵՐՈՒՄ ԳԱՂՏՆԻՔ ՊԱՐՈՒՆԱԿՈՂ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆԸ

5. Պետական մարմիններն իրենք են ապահովում իրենց տնօրինած տեղեկատվական համակարգերում պահպանվող էլեկտրոնային փաստաթղթերի պաշտպանվածությունը՝ իրականացնելով տեղեկատվական համակարգերի ենթակառուցվածքների սպասարկման և շահագործման համար անհրաժեշտ ծրագրային և ապարատային պաշտպանության միջոցներ:

6. Պետական մարմինների կողմից «Պետական և ծառայողական գաղտնիքի մասին» Հայաստանի Հանրապետության օրենքով կարգավորվող պետական և ծառայողական գաղտնիքի շարքը դասվող գաղտնագրված տեղեկություններ պարունակող կամ կազմող էլեկտրոնային փաստաթղթեր պահպանող և մշակող տեղեկատվական համակարգերի կիրառումը համաձայնեցվում է Հայաստանի Հանրապետության կառավարությանն առընթեր ազգային անվտանգության ծառայության հետ: Այդ տեղեկատվական համակարգերի համակցումն էլեկտրոնային հաղորդակցության ցանցերին, որոնք հնարավորություն են տալիս Հայաստանի Հանրապետության պետական սահմաններից դուրս տեղեկատվություն հաղորդելու, և «Ինտերնետ» միջազգային համակարգչային ցանցին, իրականացվում է միայն Հայաստանի Հանրապետության կառավարությանն առընթեր ազգային անվտանգության ծառայության կողմից կիրառման թույլտվություն ստացած և հատուկ այդ նպատակների համար նախատեսված տեղեկատվության պաշտպանության, այդ թվում՝ նաև էլեկտրոնային եղանակով կրիպտոգրաֆիկական փոխակերպման միջոցների օգտագործմամբ:

7. Հայաստանի Հանրապետության կառավարությանն առընթեր ազգային անվտանգության ծառայությունն է շահագործում «Ինտերնետ» միջազգային համակարգչային ցանցի (այսուհետ՝ «Ինտերնետ» ցանց) հատուկ հանգույց, որը նախատեսված է պետական մարմինների «Ինտերնետ» ցանցում տեղակայված և (կամ) ներկայացված հանրամատչելի տեղեկատվության պաշտպանությունն ու «Ինտերնետ» ցանցին պետական մարմինների տեղեկատվական համակարգերի անվտանգ համակցումն ապահովելու համար: Հատուկ հանգույցի սարքավորումները տեղակայվում են Հայաստանի Հանրապետության կառավարությանն առընթեր ազգային անվտանգության ծառայության, Հայաստանի Հանրապետության պետական կառավարման այլ մարմինների, պետական ոչ առևտրային կազմակերպությունների շինություններում, ինչպես նաև այն օպերատորների տեխնոլոգիական տարածքներում, որոնց ենթակառուցվածքներն օգտագործվում են հանգույցի կազմակերպման համար:

8. «Պետական և ծառայողական գաղտնիքի մասին» Հայաստանի Հանրապետության օրենքով կարգավորվող պետական և ծառայողական գաղտնիքի շարքը դասվող տեղեկություններ պարունակող կամ կազմող էլեկտրոնային փաստաթղթերի նկատմամբ պետական մարմինների կողմից կիրառվող էլեկտրոնային թվային ստորագրությունների ստեղծման և ստուգման ապարատային և ծրագրային միջոցներն ընտրվում և այդ էլեկտրոնային թվային ստորագրությունների հետ կապված ծառայությունները մատուցվում են Հայաստանի Հանրապետության կառավարությանն առընթեր ազգային անվտանգության ծառայության կողմից սահմանված կարգով:

9. Բացառությամբ սույն կարգի 8-րդ կետում նշված դեպքերի՝ պետական մարմիններն իրենց տեղեկատվական համակարգերով էլեկտրոնային ծառայություններ մատուցելիս կիրառում են անձի խիստ նույնականացման գործիքներ՝ օգտագործելով Հայաստանի Հանրապետության նույնականացման քարտերում զետեղված էլեկտրոնային թվային ստորագրությու-

ներ թողարկող և սպասարկող հավաստագրման կենտրոնի հավաստագրերը և դրանց իսկությունը որոշելու համար վերջինիս կողմից սահմանված ծրագրային միջոցները:

III. ՊԵՏԱԿԱՆ ՄԱՐՄԻՆՆԵՐՈՒՄ ԷԼԵԿՏՐՈՆԱՅԻՆ ՓԱՍՏԱԹՂԹԵՐԻ ԵՎ ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅԱՆ ԿԻՐԱՌՈՒՄԸ

10. Պետական մարմիններում «Ինտերնետ» ցանցի միջոցով տեղեկատվական համակարգերում ստացվող էլեկտրոնային փաստաթղթերը համարվում են պատշաճ ստորագրված, եթե տվյալ փաստաթղթին այն ստորագրող անձի կողմից կցված է Հայաստանի Հանրապետության հավաստագրման կենտրոնի «Էլեկտրոնային կառավարման ենթակառուցվածքների ներդրման գրասենյակ» փակ բաժնետիրական ընկերության կողմից ժամանակի դրոշմով թողարկված վավեր հավաստագիրը: Նման փաստաթղթերը հավասարեցվում են թղթային կրիչի վրա ստորագրված փաստաթղթի հետ:

11. Պետական մարմիններում շրջանառվող փաստաթղթերը կարող են ստորագրվել անմիջապես տեղեկատվական համակարգի ծրագրային միջավայրում, եթե տվյալ համակարգն ինտեգրված է էլեկտրոնային թվային ստորագրության էլեկտրոնային ժամանակի և վավերության դրոշմակնիք կիրառելու հնարավորությամբ կամ տեղեկատվական համակարգի միջավայրից դուրս այլ ծրագրային միջավայրում, որի դեպքում էլեկտրոնային թվային ստորագրությամբ ստորագրված ֆայլը ներբեռնվում է տեղեկատվական համակարգ:

12. Էլեկտրոնային փաստաթղթում այն ստորագրող անձի զուտ ձեռագիր ստորագրության տեսանելի արտապատկերի բացակայությունը չի կարող հիմք հանդիսանալ տվյալ էլեկտրոնային փաստաթուղթն էլեկտրոնային թվային ստորագրության վավերությունը վիճարկելու համար, եթե տվյալ էլեկտրոնային փաստաթղթին կցված է այն ստորագրող անձի վավերապայմաններով հավաստագրման կենտրոնի կողմից հավաստված հավաստագիրը: Էլեկտրոնային թվային հավաստագրի իսկությունն ստուգելու կարգը սահմանվում է հավաստագրման կենտրոնի կողմից:

13. Նույն փաստաթուղթը կարող է ունենալ տարբեր անձանց պատկանող մեկից ավելի էլեկտրոնային թվային ստորագրություններ, որոնց վավերապայմանները կարող են տարբերվել մեկը մյուսից:

IV. ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐ ՊԱՐՈՒՆԱԿՈՂ ԷԼԵԿՏՐՈՆԱՅԻՆ ՓԱՍՏԱԹՂԹԻ ՓՈԽԱՆՑՈՒՄԸ

14. Պետական մարմիններում պաշտոնատար անձանց կողմից Հայաստանի Հանրապետության օրենսդրությամբ սահմանված գործառույթներն իրականացնելու նպատակով այլ պետական մարմնի կամ տեղական ինքնակառավարման մարմնի տվյալների բազային անձնական տվյալներ պարունակող տեղեկատվության հարցումներ կատարելիս պետք է կիրառվի տվյալ հարցումը կատարող անհատի խիստ նույնականացման ծրագրային գործիք:

15. «Անձնական տվյալների պաշտպանության մասին» Հայաստանի Հանրապետության օրենքով սահմանված օրինականության կամ համաչափության սկզբունքների հնարավոր խախտման դեպք հայտնաբերելու կամ դրա վտանգի առաջացման մասին պետական մարմինը հնարավորինս սեղմ ժամկետում ծանուցում է անձնական տվյալների պաշտպանություն իրականացնող լիազոր մարմնին:

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ
ԿԱՌԱՎԱՐՈՒԹՅԱՆ ԱՇԽԱՏԱԿԱԶՄԻ
ՂԵԿԱՎԱՐ-ՆԱԽԱՐԱՐԻ ԱՌԱՋԻՆ
ՏԵՂԱԿԱԼ Վ. ՍՏԵՓԱՆՅԱՆ

Հավելված N 2
ՀՀ կառավարության 2017 թվականի
մայիսի 25-ի N 572 - Ն որոշման

ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅԱՆ ԿԻՐԱՌՄԱՄԲ ՊԵՏԱԿԱՆ ԵՎ ՏԵՂԱԿԱՆ ԻՆՔՆԱԿԱՌԱՎԱՐՄԱՆ ՄԱՐՄԻՆՆԵՐԻ ԿՈՂՄԻՑ ՄԱՏՈՒՑՎՈՂ ԾԱՌԱՅՈՒԹՅՈՒՆՆԵՐԸ ԿԱՄ ԳՈՐԾՈՂՈՒԹՅՈՒՆՆԵՐՆ ԷԼԵԿՏՐՈՆԱՅԻՆ ՁԵՎՈՎ ՁԵՌՔ ԲԵՐԵԼԻՍ ՎԵՐՋԻՆՆԵՐԻՍ ԿՈՂՄԻՑ ՍՏԵՂԾՎԱԾ ԵՎ ՇԱՀԱԳՈՐԾՎՈՂ ԷԼԵԿՏՐՈՆԱՅԻՆ ՀԱՄԱԿԱՐԳԵՐԻ ՏԵԽՆԻԿԱԿԱՆ ԸՆԴՀԱՆՈՒՐ ՊԱՀԱՆՋՆԵՐԸ

I. ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

1. Սույն տեխնիկական ընդհանուր պահանջները կիրառվում են էլեկտրոնային թվային ստորագրության կիրառմամբ պետական և տեղական ինքնակառավարման մարմինների կողմից մատուցվող ծառայությունները կամ գործողություններն էլեկտրոնային ձևով ձեռք բերելիս վերջիններիս կողմից ստեղծված և շահագործվող էլեկտրոնային համակարգերի նկատմամբ, ինչպես նաև այդ համակարգերի միջոցով տեղեկատվության փոխանակման կամ նման համակարգերին ինտեգրման հայտ ներկայացրած այլ անձանց կողմից շահագործվող կամ ստեղծված էլեկտրոնային համակարգերի նկատմամբ:

2. Ստորև սահմանված տեխնիկական ընդհանուր պահանջները ենթակա են կիրառման նոր ստեղծվող տեղեկատվական համակարգերում, ինչպես նաև արդեն իսկ գործող տեղեկատվական համակարգերում:

II. ՀԱՍԿԱՑՈՒԹՅՈՒՆՆԵՐԸ ԵՎ ՍԱՀՄԱՆՈՒՄՆԵՐԸ

3. Սույն տեխնիկական ընդհանուր պահանջները մեկնաբանելիս այսուհետ կիրառվում են հետևյալ հասկացությունները՝

1) հավաստագրման կենտրոն՝ «Էլեկտրոնային կառավարման ենթակառուցվածքների ներդրման գրասենյակ» փակ բաժնետիրական ընկերություն.

2) նույնականացման քարտի կիրառմամբ էլեկտրոնային թվային ստորագրություն՝ Հայաստանի Հանրապետության կողմից անհատներին տրամադրված նույնականացման քարտում զետեղված և հավաստագրման կենտրոնի կողմից թողարկված անհատական հավաստագիրը դրա հետ զուգորդված հանրային հավաստագրի հետ համադրելու հնարավորությամբ օժտված էլեկտրոնային թվային ստորագրության տեսակ, որի ընդունման հնարավորությունն առցանց տեղեկատվական համակարգերում նշված է ձևում պատկերված և հավաստագրման կենտրոնին պատկանող «Նույնականացման քարտի կիրառմամբ էլեկտրոնային թվային ստորագրություն» ապրանքային նշանով.

3) բջջային էլեկտրոնային թվային ստորագրություն՝ Հայաստանի Հանրապետությունում գործող շարժական բջջային կապի ծառայություններ մատուցող օպերատորի կողմից տրամադրված նյութական կրիչի (շարժական բջջային կապի հեռախոսաքարտի) էլեկտրոնային պահոցի վրա անհատական հավաստագիրն ստուգելու համար բջջային ստորագրության օպերատորի մշակած ծրագրային գործիքով հավաստիանալու հնարավորությամբ օժտված էլեկտրոնային թվային ստորագրության տեսակ, որի ընդունման հնարավորությունն առցանց տեղեկատվական համակարգերում նշված է ձևում պատկերված և հավաստագրման կենտրոնին պատկանող «Բջջային էլեկտրոնային թվային ստորագրություն» ապրանքային նշանով.

4) բջջային էլեկտրոնային թվային ստորագրության օպերատոր՝ հավաստագրման կենտրոնի պաշտոնական կայքում (www.ekeng.am) գրանցված և բջջային էլեկտրոնային թվային ստորագրության կիրառման համար հավաստագրերի վավերականությունն ստուգելու հետ կապված տվյալների մշակում և հաշվառում իրականացնող իրավաբանական անձինք, որոնց ներդրած ծրագրային լուծումները համապատասխանում են հավաստագրման

կենտրոնի կողմից սահմանված անհատի խիստ նույնականացում իրականացնելու համար ստորև սահմանված տեխնիկական պահանջներին.

5) պետական մարմինների կողմից մատուցվող էլեկտրոնային ծառայություններ՝ Հայաստանի Հանրապետության պետական մարմինների կողմից կամ օրենքով նախատեսված այլ ծառայություններ մատուցելու «Ինտերնետ» ցանցի առցանց համակարգերում (էլեկտրոնային հարթակներում, փաստաթղթաշրջանառության ծրագրային միջավայրում և ինտերնետային կայքերում) հաղորդակցվելու, էլեկտրոնային փաստաթղթեր լրացնելու, ներբեռնելու կամ ուղարկելու, նման փաստաթղթերն ստորագրելու ծրագրային հնարավորություն նախատեսող գործընթացներ.

6) անհատի խիստ նույնականացում՝ հավաստագրման կենտրոնի կողմից հանրային բանալիների ենթակառուցվածքի (PKI) ծրագրային և ապարատային գործիքների կիրառմամբ տվյալ անձի համար նախկինում անհատապես թողարկված հավաստագիրը տվյալ անձի ինքնության հետ հստակ նույնականացնելու ավտոմատացված գործընթաց:

III. ՊԵՏԱԿԱՆ ԵՎ ՏԵՂԱԿԱՆ ԻՆՔՆԱԿԱՌԱՎԱՐՄԱՆ ՄԱՐՄԻՆՆԵՐԻ ԿՈՂՄԻՑ ԷԼԵԿՏՐՈՆԱՅԻՆ ԾԱՌԱՅՈՒԹՅՈՒՆՆԵՐ ՄԱՏՈՒՑԵԼՈՒ ՆՊԱՏԱԿՈՎ ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅԱՆ ԾՐԱԳՐԱՅԻՆ ԻՆՏԵԳՐՄԱՆ ԵՎ ՀԱՄԱՊԱՏԱՍԽԱՆ ԾՐԱԳՐԱՅԻՆ ԳՈՐԾԻՔՆԵՐԻ ՆԵՐԴՐՄԱՆ ԿԱՐԳԸ

4. Պետական և տեղական ինքնակառավարման մարմինների կողմից ստեղծված և շահագործվող էլեկտրոնային համակարգերը պետք է տեխնիկական հնարավորություն ունենան էլեկտրոնային ծառայություններ կամ գործողություններ մատուցել նույնականացման քարտի կիրառմամբ կամ բջջային էլեկտրոնային թվային ստորագրությամբ:

5. Հայաստանի Հանրապետության պետական մարմինների տեղեկատվական համակարգերում միաժամանակ պետք է ինտեգրված լինեն նույնականացման քարտի կիրառմամբ էլեկտրոնային թվային ստորագրությամբ և բջջային էլեկտրոնային թվային ստորագրությամբ

էլեկտրոնային ծառայություններ հայցելու և ստանալու տեխնիկական հնարավորություն և հասանելիություն: Ծրագրային ինտեգրման աշխատանքները կատարվում են առցանց տեղեկատվական համակարգը կառավարող պետական մարմնի կամ վերջինիս կողմից պատվիրակված լիազորությունների շրջանակներում գործող կառավարչի միջոցներով:

6. Պետական մարմինն առցանց համակարգում նույնականացման քարտի էլեկտրոնային թվային ստորագրությամբ ծրագրային ինտեգրում կատարելու համար պետք է դիմի հավաստագրման կենտրոնին, իսկ նույնականացման քարտի կիրառմամբ հավելյալ արժեքով ծառայությունների կամ բջջային էլեկտրոնային թվային ստորագրությամբ ծրագրային ինտեգրում կատարելու համար բջջային էլեկտրոնային թվային ստորագրության օպերատորին՝ ծրագրային ինտեգրման տեխնիկական պայմաններն ստանալու համար:

7. Ծրագրային ինտեգրման տեխնիկական պայմանների համաձայն ինտեգրման աշխատանքները կատարելուց հետո առցանց համակարգի կառավարիչը դիմում է ներկայացնում հավաստագրման կենտրոնին կամ բջջային էլեկտրոնային թվային ստորագրության օպերատորին՝ ինտեգրված համակարգի աշխատունակության թեստային փորձարկումներ իրականացնելու և վերջիններիս հետ ծառայությունների մատուցման և անհատի խիստ նույնականացման համակարգի սպասարկման պայմանագրեր կնքելու համար:

IV. ՊԵՏԱԿԱՆ ԵՎ ՏԵՂԱԿԱՆ ԻՆՔՆԱԿԱՌԱՎԱՐՄԱՆ ՄԱՐՄԻՆՆԵՐԻ ՏԵՂԵԿԱՏՎԱԿԱՆ ՀԱՄԱԿԱՐԳԵՐՈՒՄ ԲՋՋԱՅԻՆ ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅԱՆ ԿԻՐԱՌՄԱՄԲ ԾԱՌԱՅՈՒԹՅՈՒՆՆԵՐԻ ՄԱՏՈՒՑՄԱՆ ՏԵԽՆԻԿԱԿԱՆ ԸՆԴՀԱՆՈՒՐ ՊԱՀԱՆՋՆԵՐԸ

8. Էլեկտրոնային ծառայություն ստացող ֆիզիկական անձը (այսուհետ՝ հաճախորդ) պետական և տեղական ինքնակառավարման մարմնի տեղեկատվական համակարգում խիստ նույնականացման գործընթաց կամ էլեկտրոնային փաստաթուղթ ստորագրելու հնարավորություն պետք է ունենա «Ինտերնետ» ցանցում գործող տվյալ տեղեկատվական համակարգի

տեսանելի մասում «Բջջային էլեկտրոնային թվային ստորագրություն» ապրանքային նշանի առկայության դեպքում:

9. Բջջային էլեկտրոնային թվային ստորագրության օպերատոր կարող է հանդիսանալ Հայաստանի Հանրապետությունում գրանցված և հավաստագրման կենտրոնի տեխնիկական պահանջները բավարարող ցանկացած իրավաբանական անձ, որի կողմից առաջարկվող տեխնոլոգիական լուծումը բավարարում է սույն պահանջներով սահմանված նվազագույն տեխնիկական պահանջները:

10. Հավաստագրման կենտրոնն իր ինտերնետային կայքում (www.ekeng.am) հրապարակում է Հայաստանի Հանրապետությունում բջջային էլեկտրոնային թվային ստորագրության օպերատորների, ինչպես նաև վերջիններիս հետ ամբողջական ծրագրային ինտեգրում իրականացրած բջջային հեռախոսակապի օպերատորների ցանկը, որոնց կողմից սպասարկվող հեռախոսահամարների համար առկա է բջջային էլեկտրոնային թվային ստորագրության ծառայության ակտիվացման հնարավորությունը:

11. Բջջային էլեկտրոնային թվային ստորագրության ծառայություններից օգտվելու համար Հայաստանի Հանրապետության նույնականացման քարտ ունեցող ցանկացած օգտատեր (անհատ) նախ պետք է ձեռք բերի նոր սերնդի շարժական բջջային կապի հեռախոսաքարտ (USIM) կամ հնարավորություն ունենա դիմելու իր բջջային կապի օպերատորին՝ շարժական բջջային կապի հեռախոսաքարտը (SIM) նորով փոխարինելու համար: Հեռախոսաքարտի ստացումը կամ փոխարինումը պետք է կատարվի այն բջջային կապի օպերատորների գրասենյակներում, որոնց հետ տվյալ բջջային էլեկտրոնային թվային ստորագրության օպերատորն ունի կնքված պայմանագիր և որոնց մասին տվյալներն առկա են հավաստագրման կենտրոնի պաշտոնական կայքում (www.ekeng.am):

12. Փոխարինված կամ նոր ձեռք բերված շարժական բջջային կապի հեռախոսաքարտը պետք է ներառի հանրային բանալիների ենթակառուցվածքի ծրագրային մոդուլ, որը համատեղելի է ստորև նշված բիզնես գործընթացներն ապահովելու համար:

13. Բջջային էլեկտրոնային թվային ստորագրության ծառայության հետ համատեղելի շարժական բջջային կապի հեռախոսաքարտն ստանալուց հետո հաճախորդը պետք է հնարավորություն ունենա ակտիվացնելու իր բջջային էլեկտրոնային թվային ստորագրությունը բջջային էլեկտրոնային թվային ստորագրության օպերատորի պաշտոնական կայքում՝ օգտագործելով իր վավեր նույնականացման քարտը:

14. Բջջային էլեկտրոնային թվային ստորագրության օպերատորի կողմից ծառայությունների մատուցման դեպքում ի լրումն բջջային օպերատորի կողմից սահմանված բջջային քարտի պաշտպանության համար սահմանված անձնական նույնականացման համարների վերջնական օգտատիրոջ բջջային քարտում տեղադրված բջջային ստորագրության ծրագրային տիրույթը նույնպես պետք է պաշտպանված լինի առնվազն հետևյալ տեսակի անձնական նույնականացման կոդերով (PIN1 կամ PIN2) և անձնական ապաբլոկավորման կոդով (PUK)՝

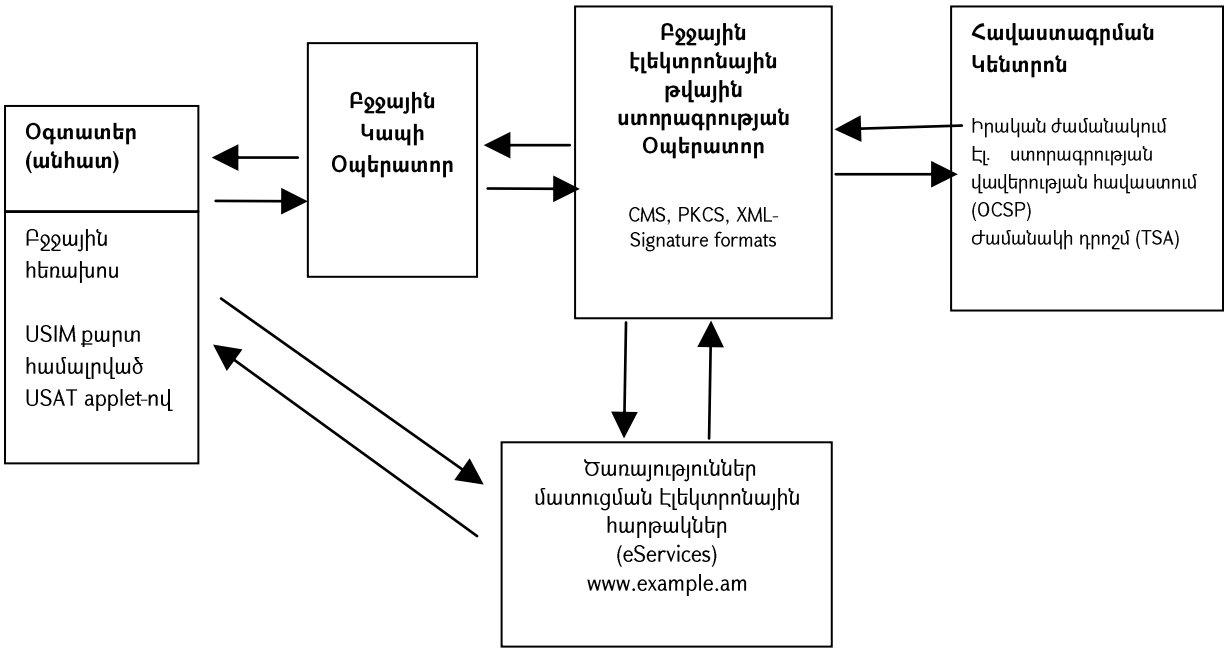
1) PIN1 տեսակի կոդ՝ անհատի խիստ նույնականացում իրականացնելու համար.

2) PIN2 տեսակի կոդ՝ էլեկտրոնային թվային ստորագրության համար.

3) PUK տեսակի կոդ՝ համապատասխանաբար PIN1 կամ PIN2 տեսակի կոդերն ապաբլոկավորելու համար:

15. Նվազագույն տեխնիկական պահանջները բավարարելու նպատակով բջջային էլեկտրոնային թվային ստորագրության օպերատորի ներդրած բջջային էլեկտրոնային թվային ստորագրության ծրագրային համակարգը պետք է ապահովի հետևյալ ավտոմատացված գործողությունների տրամաբանական հերթականություն՝ ըստ ստորև ներկայացված բիզնես գործընթացների սխեմայի և նկարագրության.

Բիզնես գործընթացների սխեմա



1) «Ինտերնետ» ցանցում որոշակի կայքով տեղեկատվական համակարգ մուտք գործելու համար օգտատերը (անհատը) պետք է հնարավորություն ունենա մուտքագրելու Հայաստանի Հանրապետությունում գործող այն բջջային էլեկտրոնային թվային ստորագրության օպերատորի կողմից թողարկված բջջային կապի հեռախոսահամարը, որի հետ կատարված է ամբողջական ծրագրային ինտեգրում.

2) սպասարկվող բջջային հեռախոսահամարը հաճախորդի կողմից տվյալ տեղեկատվական համակարգում մուտքագրվելուց հետո տեղեկատվական համակարգը պետք է հնարավորություն ունենա բջջային էլեկտրոնային թվային ստորագրության օպերատորի հետ հաստատված փակ կամ կոդավորված կապի և ինտեգրված ծրագրային ապահովման միջոցով ուղարկելու համապատասխան ֆորմատով հաղորդագրություն բջջային էլեկտրոնային թվային ստորագրության օպերատորի կենտրոնական համակարգին, որն անմիջապես ավտոմատ կերպով պետք է իրականացնի ստացված հաղորդագրության հեշ ֆունկցիայի հաշվարկ՝ հեշ արժեքը որոշելու նպատակով.

3) տվյալ ստորագրության հավաստագրի համար նախապես սահմանված հեշ («HASH») արժեքի համընկման դեպքում բջջային էլեկտրոնային թվային ստորագրության օպերատորի կենտրոնական համակարգը ծրագրային հրահանգ՝ քառանիշ կոդ է ձևավորում և այն բջջային հեռախոսակապի օպերատորին, որն սպասարկում է տվյալ բջջային հեռախոսահամարը, և միաժամանակ ծրագրային հրահանգ՝ նույն քառանիշ կոդն է ձևավորում էլեկտրոնային ծառայությունը մատուցող տեղեկատվական համակարգում ծառայությունը հայցող հաճախորդի համար՝ կիրառելով լրացուցիչ ծառայությունների կարճ հաղորդագրության (USSD - Unstructured Supplementary Service Data) համակարգի միջոցով տվյալներ հաղորդելու տեխնոլոգիան.

4) բջջային հեռախոսային օպերատորն ստացված քառանիշ կոդը լրացուցիչ ծառայությունների կարճ հաղորդագրության (USSD - Unstructured Supplementary Service Data) համակարգի միջոցով բջջային կարճ հաղորդագրություն է ուղարկում հաճախորդի բջջային հեռախոսահամարին՝ միաժամանակ հաճախորդին առաջարկելով հաստատել իսկությունը և մուտքագրել համապատասխանաբար քառանիշ անհատական նույնականացման կոդը (PIN 1) կամ հնգանիշ անհատական նույնականացման կոդը (PIN 2).

5) հաճախորդը պետք է հնարավորություն ունենա առավելագույնս 45 վայրկյանի ընթացքում ստուգելու և համեմատելու տեղեկատվական համակարգում արտացոլված քառանիշ բջջային կարճ հաղորդագրությամբ ստացված քառանիշ կամ հնգանիշ կոդի հետ և դրանք համընկնելու դեպքում մուտքագրել քառանիշ անհատական նույնականացման կոդը (PIN 1)՝ խիստ նույնականացում իրականացնելու համար կամ և հնգանիշ անհատական նույնականացման կոդը (PIN 2)՝ գործարք կատարելու կամ էլեկտրոնային փաստաթուղթն էլեկտրոնային թվային ստորագրությամբ վավերացնելու համար.

6) նախապես սահմանված համապատասխանաբար քառանիշ անհատական նույնակա-նացման կոդը (PIN 1) կամ հնգանիշ անհատական նույնականացման կոդը (PIN 2) ճշտությամբ մուտքագրելու դեպքում շարժական բջջային կապի հեռախոսաքարտի վրա զետեղված հանրային

բանալիների ենթակառուցվածքի ծրագրային մոդուլն իրականացնում է անհատի ստորագրության գաղտնագրված ծրագրային հեշ հաշվարկ և նույն բջջային օպերատորի կարճ հաղորդագրության (USSD - Unstructured Supplementary Service Data) տեխնոլոգիական հենքով բջջային կարճ հաղորդագրություն է ուղարկում բջջային օպերատորի համակարգին՝ տվյալները բջջային էլեկտրոնային թվային ստորագրության օպերատորի կենտրոնական համակարգին փոխանցելու համար.

7) բջջային էլեկտրոնային թվային ստորագրության օպերատորի կենտրոնական համակարգը ծրագրային հարցում է կատարում հավաստագրման կենտրոն՝ հավաստագրի հանրային բանալին ստանալու և հաճախորդի անհատական հավաստագրի կարգավիճակն ստուգելու նպատակով.

8) հավաստագրման կենտրոնն իրականացնում է ստացված անհատական հավաստագրի ստուգում և տվյալ պահին այն վավեր և գործող լինելու դեպքում ծրագրային պատասխան է ուղարկում բջջային էլեկտրոնային թվային ստորագրության օպերատորին՝ միաժամանակ հաղորդագրությանը կցելով ժամանակի դրոշմ (TSA) և իրական ժամանակում ստորագրության վավերության հավաստում (OCSP).

9) վավեր ստորագրության դեպքում բջջային էլեկտրոնային թվային ստորագրության օպերատորը համապատասխան ծրագրային հրահանգ է ուղարկում էլեկտրոնային ծառայություն մատուցող տեղեկատվական համակարգին՝ հաճախորդին խիստ նույնականացումը հաջողությամբ իրականացնելու վերաբերյալ.

10) տեղեկատվական համակարգն անհատի խիստ նույնականացումը հաջողված իրականացնելու դեպքում հաճախորդին հնարավորություն է ընձեռում ստանալու մատուցվող էլեկտրոնային ծառայությունը: Հակառակ դեպքում ծառայության մատուցումը տեղեկատվական համակարգի կողմից մերժվում է.

11) տվյալների փոխանցումը պետք է կատարվի «RSA» ստանդարտի գաղտնագրմամբ և հավաստագրմամբ՝ կիրառելով «RSA» կրիպտոգրաֆիկ բանալիների 1024 to 2048 բիտ կամ բարձր տարբերակ:

16. Բջջային էլեկտրոնային թվային ստորագրության օպերատորի էլեկտրոնային եղանակով փաստաթղթերի ստորագրման ներդրված համակարգը պետք է ապահովի հետևյալ ստանդարտների կիրառումը՝

ETSI EN 319 132-1 V0.0.4 (2013-11) – XML Advanced Electronic Signatures (XAdES),

ETSI EN 319 132-2 V0.0.4 (2013-11) – XAdES Baseline Profile,

ETSI EN 319 162-1V0.0.3 (2013-11) – Associated Signature Containers ,

(ASiC); ETSI EN 319 162-2V 0.0.4 (2013-11) – ASiC Baseline Profile,

ETSI TS 102 176-1 V2.1.1 (2011-07) – Algorithms and Parameters for Secure Electronic Signatures,

Xades BES profil,

HASH ալգորիթմեր SHA1 միջև SHA512,

RSA և ECDSA բանալիների ալգորիթմեր:

17. Բջջային էլեկտրոնային թվային ստորագրության օպերատորը տվյալների փոխանակումը բջջային կապի օպերատորի և հավաստագրման կենտրոնի հետ պետք է իրականացնի փակ կամ կոդավորված կապուղիներով՝ ապահովելով էլեկտրոնային տվյալների փոխանցման անվտանգության համար հանրորեն ճանաչված միջազգային չափանիշները՝ կապուղիները պետք է առանձնացված լինեն «Ինտերնետ» ցանցից և պաշտպանված լինեն արտաքին միջավայրի հարձակումներից: Տվյալների փոխանակման համար ձևավորված կապուղիները պետք է ունենան հետևյալ պրոտոկոլներ՝ «Layer 2» կամ «Layer 3» պարտադիր օժտված գաղտնագրման ալգորիթմներով առնվազն «3DES», «AES», «RC5», «Blowfish» կամ «IPSec, AES with 256 bit keys».

18. Բջջային էլեկտրոնային թվային ստորագրության օպերատորի ծրագրային լուծումը պետք է համատեղելի լինի վերջնական օգտագործողի համար առնվազն հետևյալ օպերացիոն միջավայրերում կիրառելու տեսանկյունից՝

Windows օպերացիոն ծրագրի միջավայրում.

Windows XP 32bit,

Windows Vista 32bit և 64bit,

Windows 7 SP1 32bit և 64bit,

Windows 8 32bit և 64bit

Windows 8.1 32bi bit և 64bit,

Windows 10 32bit և 64bit,

MacOS X օպերացիոն ծրագրի միջավայրում .

Mac OS X 10.8, 10.9, 10.10 (Intel),

Linux օպերացիոն ծրագրի միջավայրում .

Ubunutu 12.04LTS, 13.10, 14.04LTS, 14.10:

19. Բջջային էլեկտրոնային թվային ստորագրության օպերատորի ծրագրային լուծումը պետք է համատեղելի լինի վերջնական օգտագործողի համար առնվազն հետևյալ օպերացիոն միջավայրերում աշխատող ցանցային դիտարկիչներում (web browser) կիրառելու տեսանկյունից՝

Windows օպերացիոն համակարգում՝ «Internet Explorer», «Mozilla Firefox» և «Google Chrome»,

Mac OSX պերացիոն համակարգում՝ «Mozilla Firefox», «Safari» և «Google Chrome»,

Linux օպերացիոն համակարգում՝ «Mozilla Firefox», «Google Chrome»:

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ
ԿԱՌԱՎԱՐՈՒԹՅԱՆ ԱՇԽԱՏԱԿԱԶՄԻ
ՂԵԿԱՎԱՐ-ՆԱԽԱՐԱՐԻ ԱՌԱՋԻՆ
ՏԵՂԱԿԱԼ Վ. ՍՏԵՓԱՆՅԱՆ

Ձև

«ՆՈՒՅՆԱԿԱՆԱՑՄԱՆ ՔԱՐՏԻ ԿԻՐԱՌՄԱՄԲ
ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅՈՒՆ»
ապրանքային նշանի պատկեր

«ԲՋՋԱՅԻՆ ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅՈՒՆ»
ապրանքային նշանի պատկեր