Հավելված N 2
ՀՀ կառավարության 2025 թվականի
հուլիսի 24-ի N 1026-Ն որոշման

«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

1. 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:

2. ՀԱՍԿԱՑՈՒԹՅՈՒՆՆԵՐԸ ԵՎ ՍԱՀՄԱՆՈՒՄՆԵՐԸ

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

1) հավաստագրման կենտրոն՝ Հայաստանի Հանրապետության օրենսդրությամբ սահմանված կարգով հավաստագրման կենտրոնի հավատարմագիր ստացած իրավաբանական անձ.

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 կամ վերջինիս հավելում հանդիսացող՝ բաժանորդի տվյալների նույնականացման ներկառուցված թվային մոդուլի (այսուհետ՝ ներկառուցված թվային մոդուլ (eSIM) 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) խելացի սարքերի վրա հիմնված էլեկտրոնային թվային ստորագրություն՝ հավատարմագրված հավաստագրման կենտրոնի թողարկած անհատական հավաստագրերը հեռավար սարքավորումների անվտանգության մոդուլում ստուգելու (HSM-ում) հնարավորությամբ օժտված էլեկտրոնային թվային ստորագրություն: Սարքավորումների անվտանգության մոդուլում պաշտպանվում և կառավարվում են օգտատիրոջ թվային բանալիները, կատարվում են գաղտնագրման և գաղտնազերծման գործառույթներ թվային ստորագրությունների կիրառման համար: Խելացի

սարքերի վրա հիմնված էլեկտրոնային թվային ստորագրության ընդունման հնարավորությունն առցանց տեղեկատվական համակարգերում նշված է ձևում պատկերված և հավաստագրման կենտրոնին պատկանող «Խելացի սարքի վրա հիմնված էլեկտրոնային թվային ստորագրություն» ապրանքային նշանով.

5) բջջային էլեկտրոնային թվային ստորագրության օպերատոր՝ հավաստագրման կենտրոնի պաշտոնական կայքում 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 սույն հավելվածի 4-րդ և 5-րդ գլուխներով սահմանված տեխնիկական պահանջներին.

6) «Ես եմ» ազգային նույնականացման հարթակ՝ ապահովում է միջազգայնորեն ընդունված «Օփըն ԻԱյԴի Քընեքթ» (OpenID Connect) նույնականացման արձանագրության վրա կառուցված Հայաստանի Հանրապետության քաղաքացու նույնականացման քարտի, բջջային հեռախոսի և խելացի սարքերի վրա հիմնված Հայաստանի Հանրապետությունում թվային խիստ նույնականացման տեխնոլոգիական լուծումների հասանելիությունը.

7) 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.

8) 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.

9) խելացի սարք՝ սարք, որը կարող է միանալ ցանցին, գործարկել ծրագրային ապահովում և օգտագործվել տվյալների մշակման, փոխանցման կամ հաղորդակցության նպատակով (սմարթֆոն, պլանշետ և այլն):

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

4. Սկսած 2024 թվականի հունվարի 1-ից առցանց հանրային ծառայությունների մատուցման համակարգերում մուտքն իրականացվում է բացառապես «Ես եմ» ազգային նույնականացման հարթակի միջոցով:

5. Հայաստանի Հանրապետության պետական մարմինների տեղեկատվական համակարգերում միաժամանակ պետք է ինտեգրված լինեն նույնականացման քարտի կիրառմամբ էլեկտրոնային թվային ստորագրությամբ, բջջային էլեկտրոնային թվային ստորագրությամբ և խելացի սարքերի վրա հիմնված 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 իր առցանց տեղեկատվական համակարգում նույնականացման քարտի էլեկտրոնային թվային ստորագրությամբ կամ խելացի սարքերի վրա հիմնված էլեկտրոնային թվային ստորագրությամբ ծրագրային ինտեգրում կատարելու համար դիմում է համապատասխան ծառայությունը մատուցող 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: Պետական մարմինն իր տեղեկատվական համակարգում «Ես եմ» ազգային նույնականացման հարթակն ինտեգրելու համար համապատասխան դիմումը ներկայացնում է «Հայաստանի տեղեկատվական համակարգերի գործակալություն» հիմնադրամ:

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

4. ՊԵՏԱԿԱՆ ԵՎ ՏԵՂԱԿԱՆ ԻՆՔՆԱԿԱՌԱՎԱՐՄԱՆ ՄԱՐՄԻՆՆԵՐԻ ՏԵՂԵԿԱՏՎԱԿԱՆ ՀԱՄԱԿԱՐԳԵՐՈՒՄ ՆՈՒՅՆԱԿԱՆԱՑՄԱՆ ՔԱՐՏԻ ԿԻՐԱՌՄԱՄԲ ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅՈՒՆ ԿԱՄ ԲՋՋԱՅԻՆ ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅԱՆ ԿԻՐԱՌՄԱՄԲ ԾԱՌԱՅՈՒԹՅՈՒՆՆԵՐԻ ՄԱՏՈՒՑՄԱՆ ՏԵԽՆԻԿԱԿԱՆ ԸՆԴՀԱՆՈՒՐ ՊԱՀԱՆՋՆԵՐԸ

8. Էլեկտրոնային ծառայություն ստացող ֆիզիկական անձը (այսուհետ՝ օգտատեր) 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 «Նույնականացման քարտի կիրառմամբ էլեկտրոնային թվային ստորագրություն» կամ «Բջջային էլեկտրոնային թվային ստորագրություն» կամ «Խելացի սարքերի վրա հիմնված էլեկտրոնային թվային ստորագրություն» ապրանքային նշանների 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. Բջջային էլեկտրոնային թվային ստորագրության օպերատորների ծրագրա-սարքավորումային համալիրները պետք է գտնվեն Հայաստանի Հանրապետության տարածքում:

11. Հավաստագրման կենտրոնն իր պաշտոնական ինտերնետային կայքում 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:

12. Բջջային էլեկտրոնային թվային ստորագրության ծառայություններից օգտվելու համար Հայաստանի Հանրապետության նույնականացման քարտ ունեցող ցանկացած անձ նախ պետք է ձեռք բերի նոր սերնդի շարժական բջջային կապի հեռախոսաքարտ (USIM) կամ ներկառուցված թվային մոդուլ (eSIM) կամ հնարավորություն ունենա դիմելու իր բջջային կապի օպերատորին՝ շարժական բջջային կապի հեռախոսաքարտը (SIM) նորով փոխարինելու համար: Հեռախոսաքարտի ստացումը կամ փոխարինումը կամ ներկառուցված թվային մոդուլի (eSIM) ձեռքբերումը 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:

13. Պետական կառավարման և տեղական ինքնակառավարման մարմինների կողմից մատուցվող ծառայությունները կամ գործողությունները բջջային էլեկտրոնային թվային ստորագրության կիրառմամբ ձեռք բերելու համար Հայաստանի Հանրապետությունում կացության կարգավիճակ և այդ կարգավիճակը հաստատող վավեր փաստաթուղթ (ժամանակավոր կացության քարտ, մշտական կացության քարտ, հատուկ անձնագիր) կամ բնակության օրինականությունը հավաստող տեղեկանք

ունեցող օտարերկրացին (այսուհետ՝ օտարերկրացի օգտատեր) նշված փաստաթղթով և անձնագրով օտարերկրացիների հաշվառման համակարգում նույնականացման վերաբերյալ համապատասխան նշում կատարելու նպատակով անձամբ ներկայանում է Հայաստանի Հանրապետության ներքին գործերի նախարարության միգրացիայի և քաղաքացիության ծառայություն՝ օտարերկրացիների հաշվառման համակարգում նույնականացման վերաբերյալ համապատասխան նշում կատարելու համար: Նշված գործընթացն իրականացվելուց հետո օտարերկրացի օգտատերը կարող է ձեռք բերել նոր սերնդի շարժական բջջային կապի հեռախոսաքարտ (USIM) կամ դիմել իր բջջային կապի օպերատորին՝ շարժական բջջային կապի հեռախոսաքարտը (SIM) նորով փոխարինելու համար: Հեռախոսաքարտի ստացումը կամ փոխարինումը կատարվում է 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:

14. Փոխարինված կամ նոր ձեռք բերված շարժական բջջային կապի հեռախոսաքարտը կամ ներկառուցված թվային մոդուլը (eSIM) պետք է ներառի հանրային բանալիների ենթակառուցվածքի ծրագրային մոդուլ, որը համատեղելի է սույն հավելվածի 18-րդ կետում նշված բիզնես գործընթացներն ապահովելու համար:

15. Բջջային էլեկտրոնային թվային ստորագրության ծառայության հետ համատեղելի շարժական բջջային կապի հեռախոսաքարտը կամ ներկառուցված թվային մոդուլը (eSIM) ստանալուց հետո օգտատերը պետք է հնարավորություն ունենա առցանց ակտիվացնելու իր բջջային էլեկտրոնային թվային ստորագրությունը բջջային էլեկտրոնային թվային ստորագրության օպերատորի պաշտոնական կայքում՝ օգտագործելով թվային խիստ նույնականացման որևէ միջոց: Եթե բջջային էլեկտրոնային թվային ստորագրության օպերատորի լուծումը նախատեսում է նաև ծառայության ոչ առցանց ակտիվացում, ապա օգտատերը կարող է ակտիվացնել ծառայությունը շարժական բջջային կապի համապատասխան օպերատորի գրասենյակում՝ ներկայացնելով անձնագիրը կամ նույնականացման քարտը, իսկ Հայաստանի Հանրապետությունում կացության կարգավիճակ ունենալու դեպքում՝ անձնագիրը և

կացության կարգավիճակը հաստատող փաստաթուղթը (ժամանակավոր կացության քարտը, մշտական կացության քարտը, հատուկ անձնագիրը) կամ Հայաստանի Հանրապետությունում բնակության օրինականությունը հավաստող տեղեկանքը:

16. Բջջային էլեկտրոնային թվային ստորագրության օպերատորի կողմից օգտագործվող տեխնիկական լուծումը պետք է համապատասխանի ԻԹիԷսԱյ ԹիԷս (ETSI TS) 102 204, ԻԹիԷսԱյ ԹիԱր (ETSI TR) 102 203, ԻԹիԷսԱյ ԹիԱր (ETSI TR) 102 206 ստանդարտներով սահմանված չափանիշներին և իր կողմից տրամադրվող 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 անձնական նույնականացման PIN 1 կամ PIN 2 կոդով՝

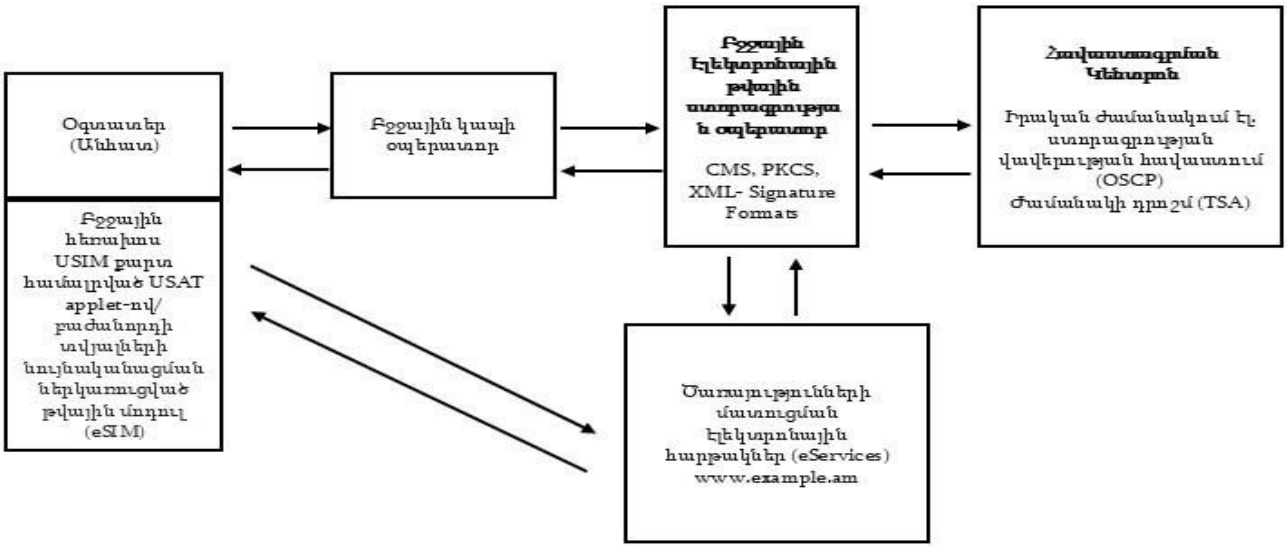
1) PIN 1 տեսակի կոդ՝ անհատի խիստ նույնականացում իրականացնելու համար.

2) PIN 2 տեսակի կոդ՝ էլեկտրոնային թվային ստորագրության համար:

17. Բջջային էլեկտրոնային թվային ստորագրության օպերատորը պետք է ապահովի PIN 1 կամ PIN 2 տեսակի կոդերն ապաբլոկավորելու համար նախատեսված օգտատերի սպասարկման հստակ գործընթաց՝ անվտանգ հեռավար եղանակով, հետևելով բջջային ԱյԴի Մենյուի (ID Menu) հրահանգներին կամ այցելելով բջջային կապի իրեն սպասարկող օպերատորի գրասենյակ:

18. 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՝ համաձայն սույն կետում 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 կապի օպերատորի կողմից թողարկված բջջային կապի այն հեռախոսահամարը, որի հետ կատարված է բջջային էլեկտրոնային թվային ստորագրության օպերատորի ամբողջական տեխնոլոգիական ինտեգրում.

2) սպասարկվող բջջային հեռախոսահամարը օգտատիրոջ 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 (API) ուղարկելու համապատասխան ֆորմատով հաղորդագրություն: Տեղեկատվական համակարգը, որն ինտեգրված է բջջային

էլեկտրոնային թվային ստորագրության օպերատորի կենտրոնական համակարգին, անմիջապես ավտոմատ կերպով պետք է իրականացնի ստացված համապատասխան ստորագրվող էլեկտրոնային փաստաթղթի հեշ ֆունկցիայի հաշվարկ՝ հեշ արժեքը որոշելու նպատակով, որն ուղարկվում է բջջային էլեկտրոնային թվային ստորագրության օպերատորի կենտրոնական համակարգին ինտեգրված ծրագրային ապահովման (API) միջոցով.

3) տվյալ ստորագրության հավաստագրի համար նախապես սահմանված հեշ («HASH») արժեքի համընկնման 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 օգտատիրոջ համար՝ կիրառելով լրացուցիչ ծառայությունների կարճ հաղորդագրության (USSD - Unstructured Supplementary Service Data կամ Encripted SMS - Encrypted Short Message Service՝ USIM քարտի կամ ներկառուցված թվային մոդուլի (eSIM) առկայության պարագայում) համակարգերի միջոցով տվյալներ հաղորդելու տեխնոլոգիան.

4) նախապես սահմանված համապատասխանաբար անձնական նույնականացման կոդ PIN 1-ի կամ անհատական նույնականացման կոդ PIN 2-ի ճշտությամբ մուտքագրելու դեպքում շարժական բջջային կապի հեռախոսաքարտի կամ ներկառուցված թվային մոդուլի (eSIM) 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 կամ Encripted SMS - Encrypted Short Message Service, USIM քարտի կամ ներկառուցված թվային մոդուլի (eSIM) առկայության պարագայում) տեխնոլոգիական հենքով բջջային կարճ հաղորդագրություն է ուղարկում բջջային օպերատորի համակարգին՝ տվյալները բջջային էլեկտրոնային թվային ստորագրության օպերատորի կենտրոնական համակարգին փոխանցելու համար.

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

6) 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).

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

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

9) տվյալների փոխանցումը պետք է կատարվի «ԹիԷլԷս» (TLS) անվտանգ պրոտոկոլի միջոցով առնվազն «ԹիԷլԷս 1.2» (TLS 1.2) կամ բարձր տարբերակով և «ԱրԷսԷյ» (RSA) ստանդարտի գաղտնագրմամբ և հավաստագրմամբ՝ կիրառելով «RSA» կրիպտոգրաֆիկ բանալիների 2048 բիտ կամ բարձր տարբերակ:

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

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

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

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

4) ETSI EN 319 162-2V 0.0.4 (2013-11) - ASiC Baseline Profile.

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

6) Xades BES profile.

7) HASH ալգորիթմեր SHA1 մինչև SHA512.

8) RSA և ECDSA բանալիների ալգորիթմեր:

20. 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 պրոտոկոլները՝ «Layer 2» կամ «Layer 3» պարտադիր օժտված գաղտնագրման ալգորիթմերով առնվազն «3DES», «AES», «RC5», «Blowfish» կամ «IPSec, AES with 256 bit keys»:

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

1) Windows օպերացիոն ծրագրի միջավայրում՝

ա. Windows XP 32bit,

բ. Windows Vista 32bit և 64bit,

գ. Windows 7 SP1 32bit և 64bit,

դ. Windows 8 32bit և 64bit,

ե. Windows 8.1 32bi bit և 64bit,

զ. Windows 10 32bit և 64bit.

2) MacOS X օպերացիոն ծրագրի միջավայրում՝

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

3) Linux օպերացիոն ծրագրի միջավայրում՝

ա. Ubunutu 12.04LTS, 13.10, 14.04LTS, 14.10:

5. ՊԵՏԱԿԱՆ ԵՎ ՏԵՂԱԿԱՆ ԻՆՔՆԱԿԱՌԱՎԱՐՄԱՆ ՄԱՐՄԻՆՆԵՐԻ ՏԵՂԵԿԱՏՎԱԿԱՆ ՀԱՄԱԿԱՐԳԵՐՈՒՄ ԽԵԼԱՑԻ ՍԱՐՔԻ ՀԻՄԱՆ ՎՐԱ ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅԱՆ ԿԻՐԱՌՄԱՄԲ ԾԱՌԱՅՈՒԹՅՈՒՆՆԵՐԻ ՄԱՏՈՒՑՄԱՆ ՏԵԽՆԻԿԱԿԱՆ ԸՆԴՀԱՆՈՒՐ ՊԱՀԱՆՋՆԵՐԸ

22. Խելացի սարքի հիման վրա էլեկտրոնային թվային ստորագրության ծառայություններից օգտվելու համար օգտատերը հավաստագրման կենտրոնի պաշտոնական կայքից կամ ԱյՕԷս (iOS) կամ Անդրոիդ (Android) հարթակներից ներբեռնում է հավաստագրման կենտրոնի պաշտոնական հավելվածը:

23. Հավաստագրման կենտրոնի պաշտոնական հավելվածը ներբեռնելուց հետո օգտատիրոջը պետք է այցելի հավաստագրման կենտրոնի պաշտոնական կայքում հրապարակված հասցեներում գտնվող որևէ կետ՝ անձը հաստատող փաստաթղթի հետ նույնականացում անցնելու համար: Սույն կետում նշված նույնականացման պատշաճ իրականացման պատասխանատվությունը կրում է հավաստագրման կենտրոնը:

24. Խելացի սարքի հիման վրա էլեկտրոնային թվային ստորագրության ծրագրային տիրույթը պետք է պաշտպանված լինի առնվազն հետևյալ տեսակի անձնական նույնականացման կոդերով (PIN 1 և PIN 2) և էլեկտրոնային ծառայություն ստացող անձի նոր գրանցմամբ՝

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

2) PIN 2 տեսակի կոդ՝ էլեկտրոնային թվային ստորագրության համար.

3) էլեկտրոնային ծառայություն ստացող անձի նոր գրանցում համապատասխանաբար PIN 1 կամ PIN 2 տեսակի կոդերն ապաբլոկավորելու համար:

25. Խելացի սարքի հիման վրա էլեկտրոնային թվային ստորագրության՝

1) կիրառվող տեխնոլոգիական լուծումը պետք է նախագծված լինի այնպես, որ անձը, ում պատկանում է էլեկտրոնային նույնականացման միջոցը, կարող է հուսալիորեն պաշտպանել այն երրորդ անձանց կողմից օգտագործումից.

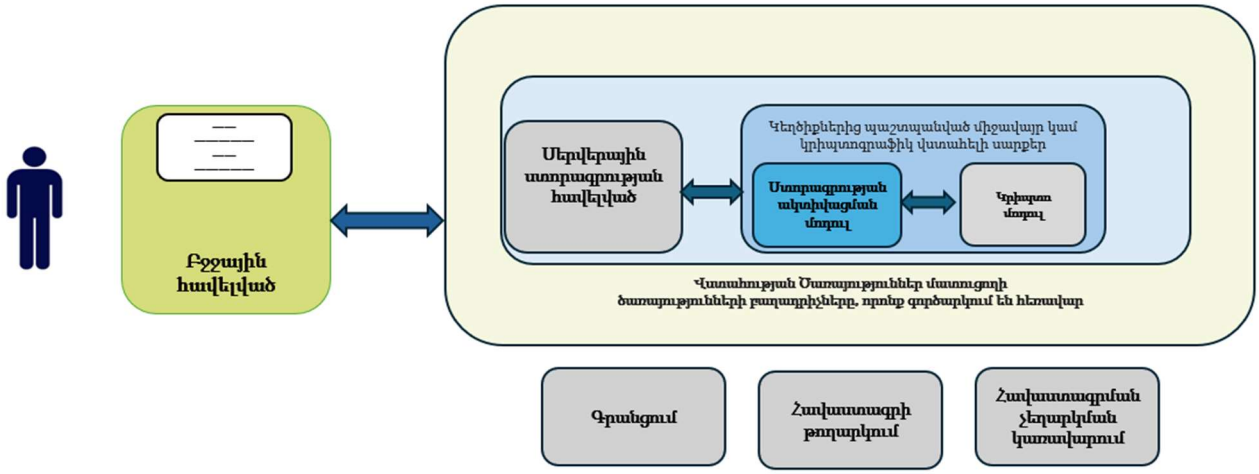
2) կիրառվող տեխնոլոգիական լուծումը պետք է մշակված լինի այնպես, որ էլեկտրոնային նույնականացման միջոցը ենթադրաբար պետք է օգտագործվի

բացառապես այն անձի վերահսկողության կամ տիրապետության ներքո, ում պատկանում է.

3) կիրառվող տեխնոլոգիական լուծումը էլեկտրոնային նույնականացման միջոցը պետք է պաշտպանի կրկնօրինակումից և կեղծումից, ինչպես նաև բարձր ներուժ ունեցող հարձակումներից.

4) մասնավոր բանալին (private key) կամ բանալու մասը պետք է լինի օգտատիրոջ տիրապետման և հսկողության ներքո:

26. Նվազագույն տեխնիկական պահանջները բավարարելու նպատակով հավաստագրման կենտրոնի ներդրած խելացի սարքի հիման վրա էլեկտրոնային թվային ստորագրության ծրագրային համակարգը պետք է ապահովի ստորև ներկայացված ավտոմատացված գործողությունների տրամաբանական հերթականություն՝



:

27. Հավաստագրման կենտրոնի կողմից ներդրված խելացի սարքի հիման վրա գործող էլեկտրոնային թվային ստորագրության ծրագրասարքավորումային համալիրները գտնվում են Հայաստանի Հանրապետության տարածքում:

28. Խելացի սարքերի հիման վրա փաստաթղթերի ստորագրման ներդրված համակարգը պետք է ապահովի առնվազն հետևյալ ստանդարտների կիրառումը՝

1) ETSI TS 119 431-1.

2) ETSI TS 119 431-2 V1.1.1 (2018-12).

3) ETSI TS 119 432.

4) ETSI TS 119 312.

5) ETSI TS 419 241-1.

6) ETSI TS 419 241-2:

29. Սույն հավելվածի 28-րդ կետում նշված ստանդարտներին համապատասխանությունը գնահատում է Հայաստանի Հանրապետության կառավարության լիազորած մարմինը (այսուհետ՝ լիազոր մարմին)՝ հավաստագրման կենտրոնի՝ օրենքով և դրա հիման վրա ընդունված իրավական ակտերով սահմանված կարգով հավատարմագրման փուլում:

30. Սույն հավելվածի 28-րդ կետում նշված ստանդարտներին համապատասխանության նկատմամբ վերահսկողություն իրականացնում է լիազոր մարմինը՝ օրենքով սահմանված կարգով: Հավաստագրման կենտրոնը երկու տարին մեկ անգամ իրականացնում է սույն որոշմամբ նշված ստանդարտներին և փաստաթղթերին համապատասխանության անկախ գնահատում և գնահատումից հետո 10 աշխատանքային օրվա ընթացքում արդյունքները ներկայացնում է լիազոր մարմին:

31. Լիազոր մարմինն իրավունք ունի իր միջոցների հաշվին իրականացնել սույն հավելվածի 28-րդ կետում նշված ստանդարտներին համապատասխանության գնահատում, եթե ունի հիմնավորված կասկածներ համապատասխանության վերաբերյալ: Այդ դեպքում լիազոր մարմինը հիմնավորում է իր դիրքորոշումը գրավոր:

32. Սույն հավելվածի 29-րդ, 30-րդ և 31-րդ կետերում նշված գործընթացներին լիազոր մարմինը կարող է ներգրավել համապատասխան մասնագիտական կարողություններ ունեցող իրավաբանական կամ ֆիզիկական անձանց:

Ձև

«ՆՈՒՅՆԱԿԱՆԱՑՄԱՆ ՔԱՐՏԻ ԿԻՐԱՌՄԱՄԲ ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅՈՒՆ»
ապրանքային նշանի պատկեր

«ԲՋՋԱՅԻՆ ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅՈՒՆ»
ապրանքային նշանի պատկեր

«ԽԵԼԱՑԻ ՍԱՐՔԵՐԻ ՎՐԱ ՀԻՄՆՎԱԾ ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅՈՒՆ»
ապրանքային նշանի պատկեր

»:

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ
ՎԱՐՉԱՊԵՏԻ ԱՇԽԱՏԱԿԱԶՄԻ
ՂԵԿԱՎԱՐԻ ՏԵՂԱԿԱԼ Ա. ԽԱՉԱՏՐՅԱՆ

26.07.2025
ՀԱՎԱՍՏՎԱԾ Է
ԷԼԵԿՏՐՈՆԱՅԻՆ
ՍՏՈՐԱԳՐՈՒԹՅԱՄԲ