ՀԱՎԱՍՏԱԳՐՄԱՆ ԳՈՐԾՈՒՆԵՈՒԹՅԱՆ ԿԱՆՈՆԱԿԱՐԳ

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅՈՒՆՈՒՄ ՀԱՎԱՍՏԱԳՐՄԱՆ ԿԵՆՏՐՈՆԻ ՀԻՄՆԱԴՐՄԱՆ

ՆԱԽԱԳԾԻ ՀԱՄԱՐ

Տարբերակ 1.2

Հունիսի 19, 2012

Պայմանագիր	Ստորագրված՝ Մայիս 11, 2012թ.
Գնորդ	Էլեկտրոնային կառավարման ենթակառուցվածքների ներդրման գրասենյան ՓԲԸ (ԷԿԵՆԳ ՓԲԸ)
Մատակարար	Լեհական Անվտանգության Տպագրություն

Փաստաթղթի մանրամասները

Էլ. փաստաթղթի անվանումը: ՀԿՀԳԿ Հավաստագրման Գործունեության Կանոնակարգ 1v2.docx

Էջերի քանակը: 50

Հաստատված է՝

Այս փաստաթուղթը պետք է հաստատված լինի Գնորդի Նախագծի Ղեկավարի կողմից.

Անուն	Ստորագրություն	Թողարկման ամսաթիվ	Տարբերակ
Արթուր Ղուլյան		25-05-2012	1.1
Արթուր Ղուլյան		22-06-2012	1.2

Տարբերակների հերթականությունը

Տարբերակ	Ամսաթիվ	Հեղինակ	Մեկնաբանություններ
0.1	2011-09-20	Արթուր Միեկինա	Փաստաթղթի աշխատանքային տարբերակ
1.0	2011-11-11	Ֆրանցիզեկ Վոլովսկի	Ստուգում և ուղղումներ Փաստաթղթի առաջին տարբերակ
1.1	2012-03-20	Արթուր Միեկինա Ֆրանցիզեկ Վոլովսկի	Սահմանված Պարամետրերի փոփոխում
1.2	2012-06-19	Արթուր Միեկինա	OCSP պրոտոկոլ

Բովանդակություն

1. Ներածություն

1.1. Ընդհանուր Նկարագրություն

Սույն փաստաթուղթը նկարագրում է Հավաստագրման Կանոնակարգը, որն ըստ Հավաստագրման Քաղաքականության (ՀՔ) պահանջների, կիրառվում է Էլ. Նույնականացման քարտերի Հավաստագրման Կենտրոնի (ՀԿ) կողմից: Հավաստագրման Գործունության Կանոնակարգը (ՀԳԿ) պետք է ընթերցվի Հավաստագրման Քաղականության հետ միասին:

Փաստաթղթի կառուցվածքը հիմնված է RFC 3647 "Ինտերնետ X.509 Հանրային Բանալիների Ենթակառուցվածքի Հավաստագրման Քաղաքականությունը և Հավաստագրման Գործունեությունը" փաստաթղթի վրա: Փաստաթղթի միատիպ կառուցվածքը ապահովելու նպատակով՝ Հավաստագրման Քաղաքականության որոշ գլուխներ ամբողջությամբ պահպանվել են նույնիսկ այն մասերում, որտեղ Հավաստագրման Գործունեության Կանոնակարգը չի պարզաբանում այն գործնական ձևերի մասին, որոնք ճշգրիտ նկարագրված են Հավաստագրման Քաղականության մեջ:

Հավաստագրման Գործունեության Կանոնակարգը նկարագրում է այն գործողությունները, որոնք կենտրոնը կիրառում է հավաստագրեր թողարկելու ժամանակ:

ՀՔ և ՀԳԿ –ն արծարծում են նույն թեմաները՝ այն է վստահելի կողմերի նպատակները և շահերը, որոնց հանրային բանալու հավաստագիրը պետք է լինի հավաստի: ՀՔ և ՀԳԿ-ի միջև հիմնական տարբերությունը դրույթների շեշտադրումն է: ՀՔ-ը սահմանում է ստանդարտներ և պահանջներ, որոնք բխում են ՀԲԵ –ի կողմից: Հավաստագրման Քաղաքականության նպատակն է սահմանել մասնակիցների գործողությունները: Ի տարբերություն վերջինիս, ՀԳԿ-ը սահմանում է, թե ինչպես ՀԿ-ը և համապատասխան ոլորտի այլ մասնակիցներ ներդնում են ընթացակարգեր և վերահսկում դրանք՝ համաձայն ՀՔ պահանջների: Այլ կերպ՝ ՀԳԿ-ի նպատակն է բացահայտել մասնակիցների գործառույթները և դրանց վերահսկումը:

ՀՔ և ՀԳԿ-ի միջև առկա լրացուցիչ տարբերությունը վերաբերում է յուրաքանչյուր դրույթի մանրամասներին: Չնայած ՀԳԿ-երը տարբերվում են միմյանցից ըստ իրենց մանրամասների, ընդհանուր առմամբ ՀԳԿ-ն ավելի մանրամասն է, քան Հավաստագրման Քաղաքականությունը: ՀԳԿ-ը մանրամասն նկարագրում է ընթացակարգերը և դրանց վերահսկումը ՝ բավարարելու ՀՔ ընդհանուր պահանջները:

Ներկայումս Հայաստանի Հանրապետությունում Էլ.-նկն. քարտերի Հավաստագրման Ծառայության Մատակարար (ՀԾՄ) հանդիսանում է Էլեկտրոնային կառավարման ենթակառուցվածքների ներդրման գրասենյակ՝ ԷԿԵՆԳ ՓԲԸ-ն:

ԷԿԵՆԳ ՓԲԸ–ն ստանձնում է Հավաստագրման Ծառայությունների Մատակարարի դերը՝ համաձայն 2001 թ-ի հուլիսի 9-ի Օրենքի (այսուհետ՝ "Թվային ստորագրությունների օրենք") և Եվրոպական 1999/93 Որոշման:

Էլ. Նույնականացման քարտերի ՀԿ - Հավաստագրման Կենտրոնի անվանումն է, որը թողարկում է նույնականացման և ստորագրության հավաստագրեր Էլ. Նույնականացման

Քարտերի համար: Այս ծառայությունները մատուցվում են համաձայն Հայաստանի Հանրապետության 2005թ. Հունվարի 15-ի '' Էլեկտրոնային Փաստաթղթի և Էլեկտրոնային Ստորագրության'' մասին օրենքի:

ԷԿԵՆԳ ՓԲԸ-ն՝ ի դեմս Հայաստանի Հանրապետության, ստանձնում է Հավաստագրման Կենտրոնի և Հավաստագրման Ծառայության Մատակարարի (ՀԾՄ) պարտականությունը և պատասխանատու է Գրանցվողների հավաստագրերի համար, որոնք թողարկվում են Էլ.-Նկն. քարտերի ՀԿ-ում: Հայաստանի Հանրապետությունը պատասխանատու է Էլ. նույնականացման քարտերի ՀԿ-ի և կենտրոնի կողմից թողարկված հավաստագրերի համար:

1.2. Փաստաթղթի Անվանումը և Նույնականացում

Հավաստագրման Գործունեության Կանոնակարգի սույն փաստաթուղթն ունի հատուկ անուն՝ ***Հավաստագրման Կենտրոնի Հավաստագրման Գործունեության Կանոնակարգ (ՀԿՀԳԿ)***: Փաստաթղթի էլեկտրոնային տարբերակը գտնվում է պահոցում. տես հղում՝ http://www.ekeng.am/?page_id=74:

Հավաստագրման Գործունեության Կանոնակարգի կողմնորոշիչը ներառված չէ թողարկված հավաստագրերի մեջ: Հավաստագրման ընթացակարգերի կողմնորոշիչները, պատկանելով հավաստագրման ընթացակարգերի ժողովածուին, ներառված են սույն Հավաստագրման Գործունեության Կանոնակարգի մեջ:

1.3. ՀԲԵ Մասնակիցներ

Սույն գլուխը նկարագրում է Հավաստագրման Կենտրոնները, Գրանցվող անձանց, Գրանցման Մարմիններին և Էլ.- նկն. քարտերի ՀԿ-ի վստահելի կողմերին:

Հավաստագրման Գործունեության Կանոնակարգը կարգավորում է Էլ.- Նկն. Քարտերի ՀԿ-ի սուբյեկների միջև առկա գլխավոր հարաբերությունները:

Կանոնակարգի դրույթները վերաբերում են հատկապես հետևյալ մարմիններին՝

- Հավաստագրման Կենտրոններ
- Գրանցման մարմիններ,
- Գրանցվողներ
- Վստահելի կողմեր:

1.3.1. Հավաստագրման Կենտրոն

Հավաստագրման Կենտրոնը (Էլ.-Նկն. ՀԿ) թողարկում է թվային հավաստագրեր, որոնք կիրառվում են Էլեկտրոնային Նույնականացման Քարտերի մեջ: Էլ.-նկն. ՀԿ-ն ապահովում է բոլոր ծառայությունների հասանելիությունը՝ ներառյալ հավաստագրերի թողարկումը, անվավերությունը և կարգավիճակի ստուգումը, քանի-որ դրանք կարող են հասանելի կամ պահանջված լինել հատուկ ծրագրերում:

Էլ.-Նկն. ՀԿ-ը գործում և վերահսկվում է Էլեկտրոնային Փաստաթղթի և Էլեկտրոնային Ստորագրության մասին՝ ՀՀ օրենքի 15 կետով:
ՀԿ ծառայություններ մատուցելու համար՝ ներառյալ հավաստագրի թողարկումը, կասեցումը, անվավերությունը, թարմացումը, կարգավիճակի ստուգումը, Էլ.-Նկն. Քարտերի ՀԿ-ը կիրառում և տրամադրում է ապահով սարքավորումներ՝ Հայաստանի Հանրապետությունում աղետային իրավիճակներում վերականգնողական աշխատանքներ իրականացնելու համար:

Էլ.-Նկն. ՀԿ-ի պատասխանատվությունն ընդգրկում է հավաստագրի կենսացիկլի կառավարումը՝

- Թողարկում
- Կասեցում/ապակասեցում
- Անվավերություն
- Կարգավիճակի ստուգում
- Դիրեկտորիայի ծառայություն:

Էլ.-Նկն ՀԿ-ը թողարկում և հրապարակում է Անվավեր Հավաստագրերի Ցուցակը (ԱՀՑ) հետևյալ հղումով՝ http://www.ekeng.am/?page_id=74/ca.crl

1.3.2. Գրանցման Մարմիններ

Գրանցման Մարմինը (ԳՄ) հավաստում է, որ տվյալ հանրային բանալին պատկանում է տվյալ սուբյեկտին (օրինակ՝ անձ):
ԳՄ- ը պատասխանատու է հետևյալի համար՝

- Գրանցվողների անձի հաստատում
- Վավերացման ենթակա տվյալների գրանցում
- Հատուկ գրանցվող անձի հավաստագիրը թողարկելու թույլտվություն
- Գրանցվող անձի Հավաստագրի պահպանում ճիշտ նույնականացման քարտում
- Գրանցվող անձի ճիշտ քարտի ձեռքբերում և ապահով ակտիվացում
- Հավաստագրի կասեցում և անվավերություն. մարմին, որը կասեցնում և/կամ անվավեր է համարում հավաստագիրը՝ համաձայն թվային ստորագրությունների օրենքի:

1.3.3. Գրանցվողներ

Էլ.-Նկն ՀԿ-ի Գրանցվող անձիք այն քաղաքացիներն են, ովքեր ունեն ակտիվացված հավաստագրերով էլ. նույնականացման քարտեր: Գրանցվողները նույնականացվում են երկու ճանապարհով՝ հավաստագրերով և հավաստագրում ներառված բանալիներով՝ փակ և դրան կապակցված հանրային բանալիով:
Էլ. նույնականացման քարտի ձեռքբերման գործընթացի սկզբում, Գրանցվող անձը իրավունք ունի նշել արդյոք ցանկանում է կիրառել իր հավաստագիրը, թե ոչ: Էլ. նույնականացման քարտը տրամադրվում է Գրանցվող անձանց հավաստագիրը քարտի մեջ ներառված: Այն հավաստագրերը, որոնք գրանցվող անձիք չեն ցանկանում կիրառել, ժամանակավորապես կկասեցվեն:
Նույնականացման և էլեկտրոնային ստորագրության հավաստագիրը միշտ կկասեցվի այն Գրանցվողների համար, ովքեր դեռ չեն բոլորել 16 տարեկանը:

1.3.4. Վստահելի կողմեր

Վստահելի կողմերը այն իրավաբանական կամ ֆիզիկական անձիք են, որոնց հավաստագիրը և/կամ էլեկտրոնային ստորագրությունը ստուգվում է հանրային բանալու միջոցով՝ ներառված գրանցվողի հավաստագրում: Թվային հավաստագրի վավերականությունը ստուգելու համար, վստահելի կողմերը պետք է մշտապես ստուգեն հավաստագրի վավերականության ժամկետը և ժամկետի հաղորդագրությունը՝ տրամադրված ՀԿ-ի կողմից (ԱՀՑ–ի) միջոցով:

1.4 Հավաստագրի Կիրառումը

Հավաստագրի կիրառումը սահմանում է թույլատրված հավաստագրի կիրառման ոլորտները և հավաստագրի տեսակը (օրինակ՝ էլեկտրոնային ստորագրության հավաստագիր, գաղտնիության կամ հավաստագրման ընթացակարգի կողմնորոշիչներ):

Հավաստագրի անվանումը	Կիրառում
Էլ. ստորագրություն	ՄԻԱՅՆ Թվային ստորագրություն (տվյալների անժխտելիություն)
Էլ. նույնականացում	Թվային ստորագրություն և բանալու կողավորում
Ենթակառուցվածքի հավաստագրեր	Ենթակառուցվածքի հավաստագրերը հատկապես կիրառվում են: a. պրոտոկոլները համաձայնեցնելու կամ բանալու գաղտնի տվյալները բաշխելու համար b. Պահոցի կամ տվյալների փոխանցման ժամանակ, հիմնական օգտվողների, գրանցվողների, դեպքերի և հավաստագրերի ամբողջությունը և գաղտնիությունը ապահովելու համար c. ստուգելու սարքավորումների հասանելիությունը, վերահսկելու ստորագրող անձի ծրագիրը

1.5. Հավաստագրման Գործունեության Կանոնակարգի Կառավարում

Սույն կանոնակարգը կազմվել է Էլ. -Նկն. քարտերի Հավաստագրման Կենտրոնի համար: Հավաստագրման Գործունեության Կանոնակարգը տեղադրված է կայքում, տես՝հղում. http://www.ekeng.am/?page_id=74

ԷԿԵՆԳ ՓԲԸ-ն պարտավոր է հիմնադրել ՀԲԵ Կառավարման Մարմին, որը հանձնարարված է՝

- կազմել նոր՝ հավաստագրման ծառայությունների տրամադրմանն առնչվող փաստաթղթեր
- փոփոխել հավաստագրման ծառայությունների տրամադրման փաստաթղթերը
- վերանայել հավաստագրման ծառայությունների տրամադրման փաստաթղթերը (առնվազն 12 ամիսը մեկ հաճախականությամբ)
- կարծիք հայտնել հավաստագրման ծառայությունների տրամադրմանն առնչվող առաջարկությունների վերաբերյալ, որոնք առաջ են գալիս Հայաստանի Հանրապետության, Գրանցվողների, վստահելի կողմերի կամ արտաքին փորձագետների կողմից
- պահպանել հավաստագրման փաստաթղթերը
- տեղեկացնել գրանցվողներին և Վստահելի Կողմերին՝ թարմացնելու փաստաթղթերը:

ՀԲԵ Ղեկավար Մարմնի կազմը հաստատվում է ԷԿԵՆԳ ՓԲԸ-ի կողմից:

1.5.1 Կոնտակտային Տվյալներ

Սույն Հավաստագրման Գործունեության Կանոնակարգին առնչվող բոլոր հարցերի դեպքում դիմել հետևյալ կոնտակտային տվյալներով՝

Էլեկտրոնային կառավարման ենթակառուցվածքների Ներդրման գրասենյակ ՓԲԸ

Հասցե: Հանրապետության Հրապարակ, Կառավարական տուն 1, Երևան 0010, ՀՀ

Հեռ՝ *+ 374 10 512 882*; **Էլ-փոստ:** cssupport@ekeng.am

1.6. Օգտագործվող Տերմիններ և Հապավումներ

Այն հիմնական բառերը, ինչպիսիք են՝ *ԱՆՀՐԱԺԵՇՏ Է՝՝ԱՆՀՐԱԺԵՇՏ ՉԷ՝՝ՊԱՀԱՆՋՎՈՒՄ Է,՝՝ ՊԵՏՔ Է՝՝ՊԵՏՔ ՉԷ,՝՝ ԽՈՐՀՈՒՐԴ Է ՏՐՎՈՒՄ՝՝ ՀՆԱՐԱՎՈՐ Է ՝՝ և ՝՝ԱՅԼԸՆՏՐԱՆՔԱՅԻՆ Է ՝՝* մեկնաբանվելու են այնպես, ինչպես նկարագրված է [RFC2119] – ում:

Սույն փաստաթղթում այս հասկացությունները կկիրառվեն հետևյալ իմաստներով.

Տերմին	Նկարագրություն
էլ.-նկն. քարտերի ՀԿ	էլ. Նույնականացման քարտերի Հավաստագրման Կենտրոն: ՀԿ, որը թողարկում է Գրանցվողների հավաստագրերը:
Էլ.-նկն. քարտեր	Էլ-նկն. քարտերի ողջ համակարգը՝ ներառյալ կազմը, ենթակառուցվածքը, ընթացակարգերը, կոնտակտային տվյալները և նկն. քարտին առնչվող այլ

	անհրաժեշտ միջոցներ:
Հավաստագրման Ծառայության Մատակարար	Յուրաքանչյուր ֆիզիկական կամ իրավաբանական անձ, որը տրամադրում կամ տնօրինում է Հավաստագրեր կամ մատուցում է թվային ստորագրություններին առնչվող այլ ծառայություններ: Այս ՀԳԿ –ի համատեքստում, Հավաստագրման Ծառայության Մատարակար հանդիսանում է ԷԿԵՆԳ ՓԲԸ-ն:
Հավաստագրման քաղաքականություն	Կարգերի և կանոնների ամբողջություն, որը սահմանում է հավաստագրի կիրառումը օգտվողների հատուկ խմբի և/կամ անվտանգության ընդհանուր պահանջներով դասի համար:
Հավաստագրման Գործունեության Կանոնակարգ	Հավաստագրման քաղաքականության բովանդակությամբ փաստաթուղթ, որը նկարագրում է հավաստագրման գործընթացի բաց բանալիների գործառույթները, գործընթացի մասնակիցներին (Հավաստագրման Կենտրոններ, Գրանցող Մարմիններ, Գրանցվողներ և Հավատարմատար կողմեր) և որպես արդյունք՝ հավաստագրերի կիրառման ոլորտները:
Գրանցվող անձ	Հավաստագրի սեփականատեր, այն է. Օգտվող՝ ուղղակիորեն կապված հավաստագրում ներառված բաց բանալուն՝ հիմք ընդունելով հավաստագրի համապատասխան դաշտերի պարունակությունը:
Գրանցված անձի հավաստագրերը	Օգտվողի համար թողարկված հավաստագրեր՝ նախատեսված երկու կիրառման համար: • Թվային ստորագրության հավաստագիր (ստեղծելու էլեկտրոնային ստորագրություն) • Էլեկտրոնային նույնականացման հավաստագիր (նախատեսված էլեկտրոնային գործարքների նույնականացման համար)

Ենթակառուցվածքի հավաստագրեր	Հավաստագրեր, որոնք կիրառվում են ապահովելու անձի ծագման անժխտելիությունը, հավաստիությունը և գաղտնիությունը տվյալների փոխանակման ընթացքում, որը իրագործվում է էլ.-նկն. քարտերի համակարգի ստորաբաժանումների միջև:
ԷԿԵՆԳ ՓԲԸ (ՀԾՄ)	Էլեկտրոնային Կառավարման Ենթակառուցվածքների Ներդրման Գրասենյակ՝ ԷԿԵՆԳ ՓԲԸ
Կողմնորոշիչ	Տեղեկատվական միավորին ստորադասված թվային եզակի ցուցիչ, որը սահմանում է տվյալ նշանակությունը:
Հանրային Բանալիների Ենթակառուցվածք ՀԲԵ	Տեխնիկական, գործառնական և կազմակերպչական հարցերի ամբողջություն, որոնք հնարավորություն են տալիս մատուցել տվյալների գաղտնիությունն ապահովվող տարբեր ծառայություններ՝ բաց բանալու կրիպտոգրաֆիայի և հավաստագրերի կիրառմամբ:
Էլեկտրոնային նույնականացման քարտ (էլ.-նկն. քարտ)	Քարտ, որը տալիս է գրանցված անձանց նույնականացման, տվյալների իսկության և փոխանցումների ժամանակ թվային ստորագրության հնարավորություն:
Անվավեր Հավաստագրերի ցուցակ (ԱՀՑ)	Անվավեր հավաստագրերի ցուցակ և անվավեր հավաստագրման կենտրոնի հավաստագրերի ցուցակ
Ինքնաստորագրվող հավաստագիր	Հավաստագրման Կենտրոնի Հավաստագիր, որը պարունակում է կողմնորոշիչ՝ տարբերակելու Հավաստագրման Կենտրոնը և մանրամասներ, որոնք վերաբերում են հավաստագիրը թողարկող անձին և հավաստագրի սեփականատիրոջը: Ինքնաստորագրված հավաստագիրը պարունակում է Հավաստագրման Կենտրոնի բաց բանալի՝ նախատեսված ստուգելու հավաստագիրը:
Պահոց	Տվյալների բազա և/կամ ֆայլերի քարտացուցակ, որը պահում է իր մեջ թվային հավաստագրեր և առցանց այլ տեղեկատվություն:

Տարածաշրջանային Գրանցման Մարմին (ՏԳՄ)	Տարածաշրջանային Գրանցման Մարմին: Կենտրոն, որտեղ գրանցվողը կարող է հայտ ներկայացնել Էլ.-նկն. Քարտի համար, որը կառավարվում է ազգային ոստիկանության կողմից:
RSA ալգորիթմ	Ծածկագրման ալգորիթմ, որի տեխնիկական նշանակությունը հստակ սահմանված է որպես b6 օբյեկտի ցուցիչը {joint-iso-ccitt(2) ds(5) modul(1) algorithm (8) Encryption Algorithm(1) 1}.
Բանալիների գեներացման գործընթաց	Գործընթաց, որում զույգ բանալին գեներացվում է կրիպտոգրաֆիկ մոդուլի կիրառման միջոցով և որտեղ էլ գտնվում է բանալին:
Հավաստագրման վստահելի ուղի	Բազմաթիվ հավաստագրերի շղթա՝ անհրաժեշտ նույնականացնելու բաց բանալի պարունակող հավաստագրի վաղեմությունը:
ՓԱԿՀ	Փաստաթղթերի Անվտանգ Կառավարման Համակարգ: Այն իրականացնում է կենտրոնական կենսաչափական փաստաթղթերի կառավարման համակարգի գործառույթները:
ՓԱԱՀ	Փաստաթղթերի Անվտանգ Անհատականացման Համակարգ: Համակարգը պատասխանատու է փաստաթղթերի անհատականացման և քարտերի կառավարման համար:
ԱՀՑ	Անվավեր Հավաստագրերի Ցուցակ
HSM(Սարքավորումների անվտանգության մոդուլ, Հոսթի Անվտանգության մոդուլ)	Նախատեսված է կրիպտոգրաֆիկ բանալիների պահոցի և կրիպտոգրաֆիկ գործառույթների համար:

2.Հրապարակման և Պահոցի Պատասխանատվություն

Էլ. նույնականացման քարտերի ՀԿ–ը հրապարակում է թողարկված թվային հավաստագրերի մասին տեղեկատվությունը առցանց Պահոցում. տես հղում՝ http://www.ekeng.am/?page_id=74

Էլ.–նկն. քարտերի Հավաստագրման Կենտրոնը պահում է փաստաթղթերի առցանց Պահոց, որտեղ հրապարակվում է կենտրոնի գործունեության, գործընթացների և որոշ ընթացակարգերի մասին, ներառյալ ՀԳԿ-ը, որը հասանելի է http://www.ekeng.am/?page_id=74 հղումով: ՀԿ-ը իրավունք է վերապահում հպարակել և հասանելի դարձնել իր ընթացակարգերի մասին տեղեկությունը բոլոր անհրաժեշտ միջոցներով:
ՀԲԵ –ի մասնակիցները տեղեկացված են, որ ՀԿ-ը կարող է հրապարակել տեղեկատվություն, որն ուղղակի կամ անուղղակիորեն հասանելի է Հավաստագրման Կենտրոնի հանրային Պահոցի թղթապանակներում և նպատակ է հետապնդում տեղեկատվություն տրամադրել հավաստագրի կարգավիճակի մասին: ՀԿ-ը հրապարակում է թվային հավաստագրերի կարգավիճակների տեղեկատվությունը հաճախակի պարբերականությամբ, ինչպես նշված է սույն ՀԳԿ-ում:
ՀԿ-ը տեղադրել և պահում է բոլոր թողարկված հավաստագրերի Պահոցը: Այն նմանապես տեղեկացնում է թողարկված հավաստագրի կարգավիճակի մասին:
ՀԿ-ը պարբերաբար հրապարակում է ԱՀՑ-ը հետևյալ հղումով՝ http://www.ekeng.am/?page_id=74/ca.crl. ՀԿ-ի OCSP սերվերը հասանելի է հետևյալ հղումով՝ http://.eid.....: Այն տրամադրում է տեղեկություն հավաստագրի կարգավիճակի մասին, որը թողարկվել է ՀԿ–ի վստահելի կողմի դիմումով՝ համաձայն IETF RFC 2560 պահանջի: ԱՀՑ-ում գտնվող յուրաքանչյուր հավաստագրի կարգավիճակ պետք է համապատասխանի այն տեղեկատվությանը, որը տրամադրել է OCSP սերվերը:
ՀԿ-ը պահպանում է ԱՀՑ-ի բաշխման և պահոցի հասցեն այնքան ժամանակ, քանի դեռ բոլոր հավաստագրերի ժամկետները չեն սպառվել: Փաստաթղթերի հաստատված տարբերակները, որոնք հրապարակվում են Պահոցում, բեռնվում են 24 ժամվա ընթացքում: Էլ.-նկն. քարտերի ՀԿ-ի կողմից հրապարակված ամբողջ տեղեկությունը հասանելի է հանրությանը հետևյալ հղումով՝ http://www.ekeng.am/?page_id=74

Էլ.-նկն. քարտերի ՀԿ սպասարկման ստորաբաժանումը ներդրել է պաշտպանական մեխանիզմներ՝ որոնք թույլ չեն տալիս պահոցում հրապարակված տեղեկությունը անթույլատրելի ձևով ավելացնել, ջնջել կամ փոփոխել: Պահոցի տեղեկության ամբողջության խախտումը բացահայտելու դեպքում, Էլ.-նկն. քարտերի ՀԿ-ը ձեռնարկում է համապատասխան միջոցներ՝ վերականգնելու տեղեկատվական ամբողջականությունը, կիրառելու օրինական տույժեր չարաշահումների դեպքում, տեղեկացնելու տուժող կողմերին և փոխհատուցելու դրանց կորուստները:

3. Նույնականացում և Անձի Հաստատում

3.1 Անվանում

ՀԿ-ը թողարկում է հավաստագրեր այն տվյալների հիման վրա, որը տրամադրվել է Գրանցվողին ԳՄ-ի կողմից: Գրանցվողները ստեղծում են իրենց համար տարբերակիչ անուն: Տարբերակիչ անունը պայմանանշանների հաջորդականություն է, որը նույնականացնում է գրանցվողին:
Հավաստագրման Կենտրոնը սահմանում է ընդունված նշանների հաջորդականությունը և դրանց կարևորությունը: Գրանցվողի անունը պետք է պարունակի ազգային տառատեսակներ, եթե դրանք ներառվել են իր տվյալներում:
Գրանցված անձի հավաստագրի մասին տեղեկությունը ենթակա է ճշգրիտ ստուգման: Հավաստագրման Կենտրոնը վերահսկում է այն նույնականացման քարտերի և այլ փաստաթղթերի միջոցով, որը լիազորում է գրանցվողին գործել ի դեմս ընկերության (եթե դա այդ դեպքն է): Հավաստագրման ծառայություններին հավաստագրի հայտ կարող են ներկայացնել միայն գրանցվող անձիք և ընկերության լիազորված ներկայացուցիչները:

Գրանցված անձի հավաստագրի տվյալները պետք է պարունակեն ոչ դատարկ՝ տարբերակիչ անուն: Այն պետք է պարունակի հետևյալ աղյուսակում նշված որոշ կամ բոլոր պայմանանշանները՝

Պայմանանշանի անվանում	Հապավում	Նկարագրություն
Ընդհանուր անուն	cn	Գրանցված անձի անունը: Այն որպես կանոն կազմված է անունից և ազգանունից : Սերվերի կամ ցանցային սարքավորումների հավաստագրերի համար, պայմանանշանը կարող է պարունակել սարքի DNS անունը կամ ընկերության կողմից այլ՝ տարբերակիչ անվանում:
Անուն (անուններ)	givenName	Գրանցվողների անուն կամ անուններ
Ազգանուն	sn	Գրանցված անձանց ազգանունները
Օգտվողի հիմնական անուն	upn	Եզակի անվանում, որը տարբերակում է գրանցված անձին համակարգերում (օրինակ՝ համակարգչի օգտվողի անունը)
Սերիայի համար	serialnumber	Եզակի համար, որը տարբերակում է գրանցված անձին: Նմանատիպ ցուցիչ էլ. – նկն. քարտերի ՀԿ –ի դեպքում համարվում է սոցիալական համարը:
Կազմակերպություն	o	Կազմակերպության անվանումը

Կազմակերպության ստորաբաժանում	ou	Կազմակերպության ստորաբաժանումը ընկերության ներսում
Երկրի Անվանումը	c	Ծագման երկրի անվանումը (միակ թույլատրելի արժեքը՝ AM).
Էլ-փոստ	emailAddress	Գրանցված անձանց կամ Սերվերի էլ-փոստ
Հավաստագրի նկարագրությունը	Description	Հավաստագրման անվանում

Աղյուսակ 1. Տարբերակիչ անվան թույլատրելի պայմանանշանները

Այս պայմանանշանները կարող են հանդիպել Գրանցվողի անվան մեջ միայն մեկ անգամ: Թույլատրելի են Գրանցվողների տարբերակիչ անվան միայն հետևյալ համադրությունները.

1. Գրանցվող անձը անհատ է, որի հավաստագիրը կարող է ներառել հետևալ տեղեկատվությունը

- Ընդհանուր անուն (ներ)
- Անուն (ներ)
- Ազգանուն
- Սերիայի համար
- Երկրի անվանում
- Էլ-փոստի հասցե
- Հավաստագրի նկարագրություն

2. Սերվերի կամ այլ համակարգչային սարքավորման դեպքում, հավաստագրի մեջ հնարավոր է ներմուծել հետևյալ տեղեկատվությունը:

- Ընդհանուր անուն
- Կազմակերպություն
- Կազմակերպության ստորաբաժանում
- Երկրի անվանում
- Էլ-փոստի հասցե
- Հավաստագրի նկարագրություն

Գրանցվող անձի, սերվերի կամ այլ համակարգչային սարքավորման սահմանումները կարող են իրենց մեջ պարունակել առնվազն պայմանշաններից հետևյալը

- Ընդհանուր անունը (cn);
- Երկրի անվանում ("c").

3.2 Անձի Նախնական Հաստատում

Գրանցվող անձի նույնականացումը, որը դիմում է ներկայացնում էլ.-Նկն. քարտ ստանալու համար, կատարվում է էլ.-նկն քարտի տրամադրման կանոնակարգերին և գործընթացներին համապատասխան:

Գրանցվող անձի նույնականացումը կատարվում է միմիայն ՏԳՄ անհատապես ներկայանալու միջոցով: Գրանցվող անձը պետք է ներկայացնի իր նույնականացման քարտը և լրացված հայտը՝ հավաստագիրը թողարկելու նպատակով: Հայտը պետք է ստորագրված լինի գրանցվողի կողմից:
Ստուգումը ավարտելուց հետո, ստորագրվում է հավաստագրման ծառայությունների մատուցման պայմանագիր:
ԳՄ-ը սահմանում է հստակ գործընթացներ, որոնք կիրառվում են ՏԳՄ-ի կողմից:
Սերվերի կամ այլ սարքավորումների հավաստագրերի Էլեկտրոնային թողարկման դեպքում պետք է կատարվի ընկերության լիազոր անձի հաստատում: Գրանցվող անձի կամ ընկերության լիազոր անձի հաստատումը պետք է կատարվի հետևյալ փաստաթղթերից որևէ մեկը ներկայացնելուց հետո

- Նույնականացման քարտ
- Անձնագիր

3.3 Նույնականացում Վերաթողարկվող Հավաստագրի Դեպքում

Եթե գրանցվող անձի հավաստագիրը սպառվել է և կատարվել է հավաստագրի վերաթողարկում, ապա նա պետք է ենթարկվի 3.2 բաժնում նկարագրված գործընթացին: Եթե Գրանցվողի հավաստագրերն անվավեր են ճանաչվել, ապա նա պետք է ենթարկվի 3.2 կետում նկարագրված ընթացակարգին:

3.4 Նույնականացում և Հաստատում Անվավեր կամ Կասեցված Հայտերի Դեպքում

Հավաստագրի կարգավիճակի կառավարման ընթացակարգերը առանձնահատուկ կարևոր ասպեկտներ են, որոնք էապես ազդում են Հավաստագրման Կենտրոնի հանդեպ վստահության և վերջինիս կողմից տրամադրվող ծառայության վրա:

Հավաստագրի անվավերության, կասեցման կամ ապակասեցման հայտը պետք է կատարվի՝

- անհատապես (ՏԳՄ-ի միջոցով),
- ԷԿԵՆԳ ՓԲԸ-ին հասցեագրված էլ-փոստի միջոցով
- Տվյալ նպատակին ծառայող ԳՄ-ի սպասարկման կենտրոնների միջոցով:

Հավաստագրի վավերականության ժամկետի կառավարման մանրամասն ընթացակարգը կնկարագրվի 4 –րդ Գլխում:

4. Հավաստագրի Կենսացիկլ և Գործառութային Պահանջներ

Հավաստագրման Ծառայության Մատակարարի (ՀԾՄ) բոլոր մարմինները՝ ներառյալ Տարածքային Գրանցման Մարմինները (ՏԳՄ), Գրանցվողները, վստահելի կողմերը և/կամ այլ մասնակիցները կրում են պարտավորություն՝ ուղղակի կամ անուղղակի ձևով տեղեկացնելու Գրանցման Մարմնին (ԳՄ) հավաստագրում տեղի ունեցած բոլոր փոփոխությունների կամ որևէ այլ փաստի մասին, որն ազդում է հավաստագրի վավերականության վրա: ԳՄ-ը ձեռնարկում է համապատասխան միջոցներ՝ իրադրությունը շտկելու նպատակով (օրինակ՝դիմել ՀԿ-ին առկա հավաստագրերը անվավեր ճանաչելու և ճշգրիտ տվյալներով նոր հավաստագրեր գեներացնելու համար):
ՀԿ-ը թողարկում, դադարեցնում կամ ժամանակավոր կասեցնում է հավաստագրերը բացառապես ԳՄ-ի և ՀԾՄ-ի կողմից, եթե տվյալ դեպքերը ԳՄ-ի կողմից նախապես հստակ սահմանվել են:

4.1 Հավաստագրի Հայտագրման Կարգը

Հավաստագրի համար հայտ ներկայացնելու գործընթացը նկարագրում է Գրանցվողների քայլերը: Այս գործընթացի ժամանակ, Գրանցվող անձը պարտավոր է

- Կարդալ և ընդունել ՀՔ կամ ՀԳ Կանոնակարգը,
- Ընտրել թվային հավաստագրի տեսակը (նկարագրված 1.4 կետում),
- Լրացնել հայտ՝ հավաստագիրը թողարկելու նպատակով,
- Պատրաստել փաստաթուղթ անձի ստուգման համար (մաս 3.2-ում նշված են ընդունելի փաստաթղթերի ցանկը):
- Ներկայանալ ՏԳՄ՝ ընթացակարգը ավարտելու նպատակով:

4.2 Հավաստագրի Հայտագրման Գործընթացը

ԷԿԵՆԳ ՓԲԸ նույնականացնում և հաստատում է պահանջվող բոլոր տվյալները: Նախքան հավաստագրի թողարկումը, Գրանցման Մարմինը պետք է հաստատի Գրանցվող անձի իսկությունը: Անձի իսկությունը պարզվում է ՏԳՄ-ի լիազոր անձնակազմի կողմից: ՏԳՄ անձնակազմը իրավունք ունի մերժել Գրանցվողի հավաստագրի դիմում-հայտը, եթե տրամադրված փաստաթղթում հայտնաբերվել են հակասություններ կամ հնարավոր չէ միանշանակ հաստատել Գրանցվողի անձը: Եթե դիմում-հայտը հաստատվել է, ՏԳՄ-ն փոխանցում է գրանցված տվյալները ԳՄ-ին: ԳՄ-ը իր հերթին հաստատում կամ մերժում է հայտը:

4.3 Հավաստագրի Թողարկում

Յուրաքանչյուր հավաստագիր կարող է թողարկվել CVCA (country verify CA) աշխատանքային խմբից նվազագույնը 2 անդամի ներկայությամբ: Հավաստագրի հայտի հաստատումից հետո, ԳՄ-ը ուղարկում է հավաստագրի թողարկման դիմումը ՀԿ: ՀԿ-ը չի ստուգում տվյալների ամբողջականությունը, միասնությունը և եզակիությունը, որը ներկայացվել է ԳՄ-ի կողմից, բայց լիարժեք վստահում է ԳՄ-ի տրամադրված տվյալների ճշտությանը: ՀԿ-ը ստուգում է միայն, որ ԳՄ-ի կողմից տրամադրված հավաստագրի սերիան լինի եզակի և դեռևս չօգտագործված այլ Գրանցվողի Հավաստագրում, որի դեպքում լրացուցիչ կտեղեկացվեր ԳՄ-ի կողմից:

ԳՄ-ի կողմից ստացված բոլոր դիմումները հավանություն են ստանում, եթե

- Պահպանում են վավերականության ժամկետները
- Օգտագործում են անվտանգ հաղորդակցման ուղիներ
- Բոլոր համապատասխան ստուգումները կատարվել են համաձայն սահմանված ՀԿ ընթացակարգի:

ՀԿ-ը նույնականացնում է ԳՄ –ի կողմից ներկայացրած անձին՝ տրամադրված տվյալների հիման վրա:
ՀԿ-ը հավաստիանում է, որ թողարկված հավաստագիրը պարունակում է բոլոր անհրաժեշտ տվյալները, որը ներկայացվել է ԳՄ-ին և հատկապես սերիայի համարը՝ կցված հավաստագրին ԳՄ-ի կողմից:
Հավաստագրի թողարկումից հետո, ՀԿ-ը հրապարակում է թողարկված հավաստագրերը Պահոցում:
Հավաստագիրը թողարկելուց հետո, ՀԿ-ը կասեցնում է հավաստագիրը: Այնուհետև հավաստագիրը փոխանցվում է ԳՄ-ին: ԳՄ-ը ՓԱԿՀ-ի միջոցով բեռնում է Գրանցվողների հավաստագրերը էլ.-նկն. քարտերի մեջ, իսկ ՓԱԱՀ-ը անվտանգ ձևով տրամադրում է էլ. –նկն. քարտը հավաստագրի հետ միասին ՏԳՄ-ին, իսկ PIN կոդերը Գրանցվողին՝ փոստի միջոցով:
Ենթակառուցվածքների հավաստագրերը թողարկվում են համաձայն ԷԿԵՆԳ ՓԲԸ ներքին ընթացակարգի:

4.4 Հավաստագրի Ընդունում

Էլեկտրոնային Նույնականացման քարտը գործարկման փուլից հետո գտնվում է ոչ ակտիվ վիճակում: ՏԳՄ-ը ակտիվացնում է քարտը Գրանցվողի ներկայությամբ՝ թարմացնելով կարգավիճակը ԳՄ-ի տվյալների բազայում: Գրանցվողը և ԳՄ-ը պահանջում են քարտի ակտիվացման տվյալները, որն անվտանգ ձևով տրամադրվում է ԱՓԿՀ-ի կողմից: Քարտը կարող է ակտիվանալ միայն գրանցվողի կողմից PIN կոդերը կիրառելու դեպքում:
Անձը կարող է ստանալ նույնականացման քարտ՝ ըստ իր հայեցողության: (Դիմում Էլեկտրոնային Նույնականացման քարտի համար՝ սկսած 16 տարեկանից): Հավաստագրի ակտիվացման գործընթացը պահանջում է, որպեսզի Գրանցվող անձը ստուգի հավաստագրի պարունակությունը:

Գրանցվողի հավաստագրի հաստատման ընթացակարգը պետք է կատարվի անմիջապես Գրանցվողի կողմից՝ իր դիմումի համաձայն: Հավաստագրի պարունակությանն առնչվող յուրաքանչյուր հակասության դեպքում, Գրանցվողը ստիպված է դիմել ՏԳՄ-ին: Տվյալ դեպքում թողարկված հավաստագիրը պետք է անվավեր համարվի, իսկ Գրանցվող անձը ստանա նոր հավաստագիր: Եթե թողարկված հավաստագրերի վերաբերյալ սխալների հաշվետվությունը բացակայում է, ապա նշանակում է հավաստագիրն ընդունվել է:

Հավաստագրի ընդունումը կարող է մերժվել, օրինակ Գրանցվողի ոչ ճշգրիտ տվյալների կամ Գրանցվողը դեռ չի հասել օրենսդրական տարիքի՝ հավաստագիր ձեռք բերելու համար: ՏԳՄ-ները փոխանցում են թողարկված հավաստագրերի վերաբերյալ առարկությունները ԳՄ-ին, որպեսզի ՀԿ-ը անվավեր համարի տվյալ հավաստագրերը:

4.5 Զույգ Բանալիների և Հավաստագրի Կիրառում

Բանալիներին և հավաստագրերին առնչվող պատասխանատվությունը նկարագրվում է հետևյալ կետերում՝

4.5.1 Գրանցվողի Պարտականությունները

Համաձան սույն ՀԳԿ-ի, Գրանցվողի պարտականություններն են՝

- Պաշտպանել հավաստագիրը կեղծիքներից
- Օգտագործել հավաստագրերը միայն օրինական կամ թույլատրելի դեպքերում՝ համաձայն ՀԳԿ-ի:
- Օգտագործել հավաստագիրը պատեհ հանգամանքներում:
- Խուսափել փակ բանալիները կեղծելու. կորստի, տվյալները հայտնաբերելու, փոփոխելու կամ անթույլատրելի կիրառման դեպքերից:

4.5.2 Վստահելի Կողմերի Պարտականությունները

Վստահելի կողմը պետք է՝

- Վավերացնի հավաստագիրը՝ օգտագործելով ԱՀՑ, OCSP պրոտոկոլ՝ համաձայն հավաստագրի վավերացման ընթացակարգի;
- Ընդունել տվյալ հավաստագիրը միայն այն դեպքում, եթե այն չի կասեցվել կամ ճանաչվել անվավեր:
- Վստահել հավաստագիրը ողջամիտ հանգամանքներում:

4.6 Նոր Հավաստագիր

Գրանցվողի հավաստագիրը կարող է նորացվել միայն հետևյալ դեպքերում՝

- Նոր Էլեկտրոնային նույնականացման քարտի ձեռքբերում,
- Հավաստագրի վերաթողարկում՝ այն անվավեր համարելուց հետո:

Ընթացակարգը նույնն է, ինչ եղել է առաջին հայտի ժամանակ:

4.7 Հավաստագրի Վերաթողարկում

Գրանցվողի հավաստագիրը անվավեր ճանաչելուց հետո, այն չի կարող կրկին ակտիվացվել և հետևաբար, պետք փոխարինվի նոր հավաստագրով: Գրանցվողի հայտի հիման վրա, ՏԳՄ-ը գեներացնում է Էլեկտրոնային Նույնականացման քարտի նոր բանալիների զույգ և փոխարինում անվավեր հավաստագիրը նորով:

4.8 Հավաստագրի Փոփոխումը

Չի կիրառվում:

4.9 Հավաստագրի Անվավերություն և Կասեցում

Մինչև գրանցվողի մերժման կամ ընդունման հայտը, Գրանցվողի հավաստագիրը մնում է ժամանակավոր կասեցված Էլեկտրոնային Նույնականացման քարտում: Գրանցվողի հավաստագրի նախնական ակտիվացումը պետք է կատարվի իր թողարկումից մեկ ամսվա ընթացքում: ԳՄ-ը կամ ՏԳՄ-երը անմիջապես գործում են այս պահանջները բավարարելու նպատակով: Գրանցվողը պետք է դիմի ՏԳՄ կամ ԳՄ-ի սպասարկման բաժին՝ հավաստագիրն անվավեր ճանաչելու կամ կասեցնելու համար: ՏԳՄ-ի աշխատանքային ժամերը սահմանափակ են, մինչդեռ ԳՄ-ի սպասարկման բաժինը գործում է շաբաթական օր, 24 ժամ:
ՏԳՄ-ը կամ ԳՄ-ի սպասարկման բաժինը ԳՄ-ի միջոցով պահանջում է կասեցնել Գրանցվողի հավաստագրերը, եթե՝

- Գրանցվողի կողմից ստացվել է հաղորդագրություն, որ կասկած է առաջացել հավաստագիրը կորցնելու, գողանալու, տվյալների փոփոխման և բացահայտման, փակ կամ զույգ բանալիների կեղծման վերաբերյալ:
- Համաձայն սույն ՀԳԿ-ի, ՏԳՄ-ի գործունեությունը հետաձգվում կամ կանխվում է բնական աղետների, համակարգչային կամ տեղեկատվական ձախողման և այլ դեպքերում, որը դուրս է մարդկային վերահսկումից և հետևաբար անձի տվյալները գողանալու կամ վնասվելու սպառնալիքի տակ է:

- Ստացվել է Գրանցվողի կողմից հաղորդագրություն՝ հավաստագիրը կորցնելու, գողանալու, տվյալների բացահայտման, փոփոխման, և փակ կամ զույգ բանալիների կեղծման վերաբերյալ:
- Փոփոխվել է Գրանցվողի Հավաստագրի տվյալները:

ՀԿ-ը կասեցնում կամ անվավեր է համարում գրանցվողների հավաստագրերը՝ համաձայն ԳՄ կամ ՀԾՄ-ի դիմումի: ԳՄ-ը, մեկ շաբաթ հետո անվավեր է ճանաչում կասեցված հավաստագրերի զույգ բանալիները, եթե Գրանցվողի կողմից չի ստանում հաղորդագրություն ապակասեցնելու հավաստագիրը:
Առանձնահատուկ հանգամանքներում (օրինակ՝ աղետ, ՀԿ բանալիների կեղծում, անվտագության խափանում …) ՀԾՄ–ը կարող է պահանջել կասեցնել և/կամ անվավեր ճանաչել հավաստագրերը:
ԳՄ-ը հետևում է, որպեսի Գրանցվողը նախազգուշացվի նման կասեցման/դադարի մասին:
Վստահելի կողմերը, նախքան հավաստագրին վստահելը, պետք է օգտագործեն այն առցանց միջոցները, որոնք հրապարակվում են ՀԿ Պահոցում՝ հավաստագրերի կարգավիճակը ստուգելու համար: ՀԿ-ը թարմացնում է ԱՀՑ-ը և OSCP-ին: ԱՀՑ-ները հաճախակի թարմացվում են՝ նվազագույնը երեք ժամը մեկ պարբերականությամբ:
ՀԿ-ը թույլ է տալիս մուտք գործել OCSP-ի պահոց և կայք, որտեղ տեղադրվում են հավաստագրերի կարգավիճակները:

4.9.1 Կասեցման և Անվավերության Ժամկետներ

Կասեցումը կարող է տևել առավելագույնը յոթ օրացուցային օր՝ ստեղծելու կասեցման պատճառ հանդիսացող նախադրյալները: Նմանատիպ բացասական պայմաններում Գրանցվող անձը կարող է պահանջել կրկին ակտիվացնել (ապակասեցնել) Հավաստագիրը՝ հիմնվելով հետևյալ պայմանների վրա՝

- Գրանցվող անձը առանց որևէ կասկածի պարզել է, որ իր մտավախությունը, որ տեղի է ունեցել փակ բանալու կամ զույգ բանալիների կորուստ, գողություն, փոփոխություն, անթույլատրելի բացահայտում կամ այլ տիպի սպառնալիք, սխալմունք է:
- Չկան այլ պատճառներ՝ կասկածելու գրանցվող անձի հավաստագրերի փակ բանալու գաղտնիության կամ ապահովության վերաբերյալ:
- Պահանջել ապակասեցնել Գրանցվողի Հավաստագրերը, որի դեպքում Գրանցվողը անձամբ պետք է ներկայանա ՏԳՄ:

ՏԳՄ-ը անմիջապես պահանջում է Գրանցվողի Հավաստագրերի ապակասեցում ԳՄ-ի միջոցով միայն այն բանից հետո, երբ՝

- Ստանում է հաղորդագրություն Գրանցվող անձից, որ տեղի է ունեցել սխալմունք Գրանցվողի Հավաստագրերի փակ կամ զույգ բանալիների կորստի, գողության, փոփոխման կամ անթույլատրելի բացահայտման վերաբերյալ:
- Հերքվել է կասկածը այն մասին, որ այլ անձի տվյալները կարող են գողացված լինել կամ գտնվել սպառնալիքի տակ և որ ԳՄ-ի պարտականությունը երկարաձգվել կամ խոչընդոտվել է բնական աղետի, տեղեկատվական կամ համակարգչային խափանման կամ այլ պատճառով, որը դուրս է անհատի վերահսկողությունից:
- ԳՄ-ի պահանջի համաձայն, ՀԿ–ը կարող է կասեցնել կամ անվավեր համարել Գրանցվողի հավաստագրերը:

ՀԿ-ը, 1 շաբաթ հետո, ավտոմատ կերպով անվավեր է ճանաչում կասեցված հավաստագիրը, եթե մինչ այդ չի ստանում ապակասեցման հաղորդագրություն ԳՄ-ի կողմից: ՀԿ-ը զգուշացնում է ԳՄ-ին բոլոր կասեցված հավաստագրերի վերաբերյալ:

ՀԿ-ը Պահոցում հրապարակում է տեղեկատվություն կասեցված կամ անվավեր ճանաչված հավաստագրերի մասին:

4.10 Առցանց անվավեր ճանաչում/կարգավիճակի ստուգում

ԷԿԵՆԳ ընկերությունը տրամադրում է հավաստագրի կարգավիճակի ստուգման ծառայություն իրական ժամանակում՝ համաձայն OCSP RFC 2560-ի: Օգտագործելով OCSP պրոտոկոլ, հնարավոր է ձեռք բերել ավելի հաճախակի և թարմացված տեղեկություն (ի տարբերություն ԱՀՑ-ի) հավաստագրի կարգավիճակի մասին:
OCSP–ին տրամադրում է հետևյալ տեղեկատվությունը հավաստագրի կարգավիճակի մասին՝

լավ – նշանակում է դրական պատասխան հայցին, որը պետք է մեկնաբանվի որպես հավաստագրի վավերականության հաստատում
անվավեր – նշանակում է հավաստագիրը անվավեր է ճանաչվել
անհայտ – նշանակում է հավաստագիրը չի թողարկվել հավաստագրման որևէ մասնաճյուղ կենտրոնի կողմից:

Հավաստագրի կարգավիճակը հասանելի է իրական ժամանակում:

4.11 Հավաստագրի Կարգավիճակի Ծառայություն

ՀԿ հավաստագրի կարգավիճակի ստուգման ծառայությունները՝ ներառյալ ԱՀՑ-ը (CRL) և OSCP-ին հասանելի են հետևյալ հղումով ՝ http://www.ekeng.am/?page_id=74/ca.crl

ԱՀՑ-ները ստորագրվում են ՀԿ-ի կողմից: ԱՀՑ-ը թողարկվում է 24 ժամը մեկ՝նախապես համաձայնեցված ժամին: ՀԿ-ը բոլոր նախկին 12 ամիսների ԱՀՑ-ը հրապարակում է Պահոցում:

4.12 Գրանցման ավարտ

Չի կիրառվում

4.13 Բանալու պահպանում երրորդ անձի կողմից կամ վերականգնում

Բանալու պահումը երրորդ անձի կողմից կամ բանալու վերականգնումը թույլատրված չէ:

5 Սարքավորումներ, Կառավարում և Օպերացիոն Վերահսկում

Այս բաժինը նկարագրում է անվտանգության (ոչ տեխնիկական) վերահսկումը, որը կիրառվում է էլ.-Նկն.քարտի ՀԿ-ի կամ այլ ՀԲԵ գործընկերների կողմից՝ կատարելու բանալիների գեներացման, անձի հաստատման, հավաստագրի թողարկման, հավաստագրի անվավերության, աուդիտի կամ արխիվացման գործառույթները:

5.1 Վերահսկում

Վերահսկման նպատակը անվտանգության պայմանների (ոչ տեխնիկական) վերահսկումն է՝ կանխելու անթույլատրելի մուտքը, վնասի և միջամտության առկայությունը այն տարածքներում, որտեղ տեղակայված են տեղեկատվական սարքավորումները և թողարկվում, վավերացվում և կիրառվում են հավաստագրերը:

Էլ.-նկն. ՀԿ-ը ապահովում է, որպեսզի ծառայության մատուցումը կատարվի ապահով միջավայրում, որն ենթադրում է ՝

a) Տարածք և կառուցվածք: Էլ.-նկն. ՀԿ-ը գործում է ֆիզիկապես անվտանգ տարածքում՝պայմանավորված սենյակների բաժանվածությամբ անվտանգ գոտում և համապատասխան պատերի կառուցվածքով: ՀԿ–ի գործողությունները կատարվում են անվտանգ գոտում բարձր անվտանգության սենյակներում, ֆիզիկապես պաշտպանված կառույցում, որը բացահայտում և կանխում է անթույլատրելի մուտքը:

b) Ֆիզիկական մուտք: Էլ.–նկն. քարտի ՀԿ-ը վերահսկվում և ենթարկվում է աուդիտի: Միայն լիազորված անձիք ֆիզիկապես մուտքի իրավունք ունեն ՀԿ: Էլ.-նկն. ՀԿ–ի անձնակազմի ստուգումը կատարվում է պարբերական ձևով: Էլ. նույնականացման քարտի ՀԿ-ի համակարգի ապահովումը պատշաճ ձևով կազմակերպելու համար, պահանջվում է ապահովել հետևյալ պաշտպանիչ միջոցները՝

- Համապատասխան դռներ և կողպեքներ;
- Մուտքի վերահսկողություն;
- Շարժման սենսորային համակարգ;
- ՓՀՄՑ համակարգեր (Փակ հեռուստատեսային մալուխային ցանցեր);
- Կահավորված աշխատասենյակներ,
- Պատուհաններ՝ համապատասխան կառուցվածքով
- Ապահով համակարգ՝ անխափան էլեկտրականությամբ և օդափոխիչով,
- Կողոպտիչ տագնապի ազդանշանային համակարգ
- Հրդեհի բացահայտման և հակահրդեհային համակարգ

a) **Կրիչների Պահեստ** – Ողջ տեղեկատվական բազան, որը ներառում է ծրագրեր, տվյալներ, աուդիտի, արխիվի կամ պահուստային միջոցներ, որոնք պահվում են կողպված պահարանում կամ աշխատասենյակում՝ պաշտպանված պատահական վնասներից: Մուտքը դեպի պահեստ սահմանափակվում է լիազոր անձանց աշխատանքային խմբով:

b) **Թափոնի կառավարում** – Գաղտնի փաստաթղթերը և նյութերը, թափվելուց առաջ, պետք է մասնատվեն:

Կրիչները, որոնք հավաքում կամ փոխանցում են գաղտնի տվյալներ, նախքան թափոնի վերածվելը, արտացոլում են անընթեռնելի տվյալներ (ապահով ջնջված կամ ֆիզիկապես

ոչնչացված): Կրիպտոգրաֆիկ սարքավորումները և ծածկագրված մատերիալը, ինչպես նաև ապարատային սարքավորումների պահոցը ֆիզիկապես ոչնչացվում են նախքան թափոնի վերածվելը:

5.2 Ընթացակարգերի Վերահսկողություն

Անվտանգության, հատկապես պարտականությունների բաշխման ընթացակարգերը՝ հիմք ընդունելով կրկնակի ստուգման սկզբմունքը, կիրառվում են օրինակ Էլ.-նկն. քարտերի փոփոխվող ՀԿ-ի դեպքում, որը գեներացնում է հավաստագրեր ՀԿ-ի ենթակառուցվածքների համար կամ անվավեր է ճանաչում հավաստագրերը:
Էլ.-Նկն. ՀԿ-ը ապահովում է, որպեսզի մուտքը ՀԲԵ-ի սարքավորումների համակարգ լինի սահմանափակ, իսկ լիազորված մարդկանց խմբի մուտքը սահմանափակվի՝ առնվազն անհատական օպերատորական մուտքային տվյալներով:

Օպերատորների հիմնական գործողությունները, որոնք առնչվում են հավաստագրման ընթակարգերին և տվյալների անվտանգությանը, պահանջում են կրկնակի վերահսկողություն: Դրան կարելի է հասնել՝ կատարելով գաղտնիության բաժանում, որն անհրաժեշտ է հատուկ գործողություն կատարելու՝ երկու կամ բազմակի նույնականացման նպատակով: Գաղտնաբառերի տրամադրումը պետք է վերահսկվի ձևակերպված գործընթացների միջոցով:
Հավաստագրման Գործունեությունը և Գրանցման Մարմինները ենթակա են աուդիտի և վերահսկվում են աուդիտորների և անվտանգության աշխատակիցների կողմից: Համակարգի գլխավոր դեպքերը օժանդակ ձևով պահպանվում են համապատասխան օպերացիոն համակարգերի աուդիտային մեխանիզմների կողմից՝ համակարգի անվտանգությունը ապահովելու նպատակով:

Անվտանգության պահանջները հատկապես վերաբերում են հետևյալին՝

a) Պաշտպանիչ միջոցներ (օրինակ՝միջցանցային էկրաններ՝ firewall) են կիրառվում CV (երկրի վերահսկում) ներքին ցանցերի վեբ տիրույթներում (domain)՝ երրորդ կողմի ներխուժումը արտաքին տիրույթներից կանխելու համար: Օգտվողի տերմինալից մինչև համակարգչային ծառայությունները վերահսկվում են ցանցի միջոցով: Հասանելի օգտվողների համար կկիրառվեն մեխանիզմներ (օրինակ՝ HTTP, FTP), որոնք սահմանափակում են ծառայությունների քանակը՝ համաձայն AR-CA ընթացակարգերի:
b) Թվային տվյալները պաշտպանված են անթույլատրելի մուտքի կամ տվյալների փոփոխման դեմ: Համակարգի օգտվողները մուտք ունեն միայն դեպի թույլատրված ծառայություններ, համակարգի ծրագրերի կիրառումը կլինի սահմանափակ և խիստ վերահսկելի, իսկ մուտքը դեպի Էլ.-նկն քարտերի ՀԿ կարգելափակվի աշխատանքի ավարտից հետո՝չթույլատրված մարդկանց մուտքը կանխելու նպատակով (օրինակ screensaver գաղտնաբառով):
c) Անապահով ցանցում գաղտնի տվյալները պաշտպանված են տվյալների փոխանցման դեպքում (օրինակ ՝ ծածկագրման կամ այն մեխանիզմների միջոցով, որոնք ապահովում են տվյալների ամբողջականությունը):
d) Էլ.-նկն. ՀԿ-ը բոլոր օգտվողներին արդյունավետ ձևով տրամադրում է մուտքային տվյալներ՝ (ներառյալ օպերատորներ, վարչական աշխատողներ և օգտվողներ, որոնք ունեն ուղղակի մուտք դեպի համակարգ) համակարգի անվտանգութունն ապահովելու նպատակով՝ ներառյալ կառավարումը, աուդիտը, մուտքային տվյալների ջնջում կամ ճշգրիտ

(ժամանակին) փոփոխում: Մուտքը դեպի տեղեկատվական համակարգ և գործառույթներ սահմանափակվում է միայն լիազորված անձնակազմով:

- **Էլ.-նկն. քարտերի ՀԿ-ի Մենեջեր** – պաշտոն, որը ներառում է պարտականություններ էլ.-նկն. քարտերի ՀԿ-ի գործառույթների վերաբերյալ: Նա պատասխանատու է էլ. Նկն. քարտերի ՀԿ-ի գործունեության համար, ծառայությունների մատուցման և զարգացման, ներդրումների, օպերատիվ պատրաստվածության և շարունակական գործունեության համար: Նա ունի սահմանափակ մուտք դեպի էլ. նկն. քարտերի ՀԿ: Մուտք չունի դեպի օպերացիոն տվյալների բազա և AR-CA կրիպտոգրաֆիկ բանալիներ:

- **Անվտանգության աշխատակից** – անձ, որը պատասխանատու է անվտանգության բոլոր հարցերի համար: Նրա պարտականությունները ներառում են էլ.-նկն. քարտերի ՀԿ-ի անվտանգությունը և պատահարների դեպքում արագ արձագանքումը: Նա վերահսկում է էլ.-նկն քարտերի ՀԿ-ի անվտանգությունը և անձնակազմը: Նա մուտք ունի դեպի ՀԿ օպերատիվ գործունեության ռեգիստրներ (համակարգի տեղեկությունների արձանագրման՝ log ֆայլեր) և սահմանափակ մուտք դեպի ՀԿ-ի ենթակառուցվածք: Նա պատասխանատու է անվտանգության ընթացակարգերի իրագործման համար: Նա համատեղ աշխատում և ստեղծում է ՀԿ-ի փաստաթղթերը: Նա պատրաստում է անվտանգության պլանը՝ ՀԿ-ի անխափան աշխատանքը ապահովելու նպատակով:
- **Աուդիտի աշխատակից** – վերլուծում է ռեգիստրներում գրանցված դեպքերի տվյալները, որը տեղի է ունենում տեղեկատվական համակարգերում հավաստագրման ծառայություն մատուցելիս:
- **Ցանցային ադմինիստրատոր**, **տվյալների բազայի ադմինիստրատոր, համակարգի ադմինիստրատոր** – պատասխանատու է օպերացիոն շահագործման, էլ.-նկն քարտերի ՀԿ-ի տեխնիկական արդյունավետության և պատրաստակամության համար: Նրանք ունեն տարաբաշխված մուտք դեպի էլ.-նկն. քարտերի ՀԿ: Նրանք բաշխում են պարտականությունները թիմի անդամների միջև: Ծածկագրված գործողությունները պետք է կատարվեն առնվազն երկու՝ առանձին հմտությունների տեր մարդկանց կողմից: Նրանք չունեն մուտք դեպի ՀԿ կրիպտոգրաֆիկ բանալիների բազա: Նրանք ենթարկվում են ՀԿ-ի ղեկավար մարմնին:

էլ.-նկն. քարտերի ողջ համակարգը պարունակում է բավարար SS միջոցներ՝ առանձնացնելու դերերը, որոնք ներառում են ադմինիստրատորների միջև անվտանգության կանոնների բաշխման և շահագործման գործառույթները: Համակարգի ծրագրերի կիրառումը վերահսկվում է ամենայն ճշգրտությամբ: Մուտքը սահմանափակված է այնպես, որ հասանելի է լոկ օգտվողներին:

e) Էլ.-նկն. քարտերի անձնակազմը հաջորդականորեն նույնականացվում է ներքևում նշված ձևով. վերահսկվում է էլ.-նկն. քարտերի ՀԿ-ի ՀԲԵ-ի ծրագրերի չարաշահումը, որն առնչվում է էլ. -նկն քարտերի մուտքային տվյալներին կամ հավաստագրի կառավարմանը:

f) ՀԿ-ի անձնակազմի գործունեությունը կանոնակարգված է. օրինակ պահելով դեպքերի գրանցամատյան, ինչպես նախանշված էր 5.4 ենթագլխում: ՀԿ – օպերատորների անվտանգությանն առնչվող գլխավոր որոշումները կայացվում են ամբողջությամբ այն անձի կողմից, որը կատարում է տվյալ գործողությունը:

Գլխավոր որոշումները են՝

- Էլ.- նկն. քարտերի ՀԿ ՀԲԵ-ի համակարգի փոփոխությունը,
- Հավաստագրերի գեներացում
- Հավաստագրերի չեղյալ/անվավեր համարումը
- Համակարգի փաստաթղթերի փոփոխումը և ստեղծումը:

Էկ.- նկն. քարտերի ՀԿ պետք է ավտոմատ (էլեկտրոնային) գեներացնի համապատասխան դեպքերի գրանցամատյան: Բոլոր դեպքերի գրանցումները՝ ստեղծված էլ. Նկն քարտերի ՀԿ-ի մոդուլի կողմից, պետք է պարունակեն հետևյալ տարրերը՝

- Գրացման ժամը և ամսաթիվը
- Եզակի դեպքի ցուցիչ
- Դեպքի տեսակը
- Տեղեկատվություն, որը նշում է դեպքի վայրը (օրինակ՝ տերմինալ, պորտ, տարածք և այլն)

Այլ՝ մնացյալ ենթահամակարգերի դեպքում, դեպքերի գրանցումները պետք է պարունակեն առնվազն հետևյալ տարրերը՝

- Գրանցման ամսաթիվը և ժամը
- Դեպքի ամսաթիվը, որը պարունակում է տեղեկություն և թույլ է տալիս միանշանակ նույնականացնել դեպքի ծագումը, բնույթը և պարամետրերը:

Ընթացիկ և արխիվացման գրանցամատյանները պետք է օգտագործվեն այն ձևով, որ զերծ մնան անթույլատրելի փոփոխումից կամ վնասվելուց:
Էլ.-նկն. քարտերի ՀԿ-ը պետք է պարբերաբար գրանցի առանձին ենթահամակարգերի պատահարները գրանցամատյանում:
Էլ.-նկն քարտերի ՀԿ-ը պահում է դեպքերի գրանցամատյանը արտաքին ապահով տեղում՝ նախապես համաձայնեցված ժամանակահատվածի համար:
Ընթացիկ և լրացված դեպքերի գրանցամատյանը կարող է ստուգվել միայն թույլատրված անձանց կողմից՝ անվտանգության նկատառումներից ելնելով:

5.3 Անձնակազմի վերահսկողություն

Ողջ էլ.–նկն. քարտերի ՀԿ ՀԲԵ-ի համակարգերը օգտագործվում են որակավորված և փորձառու անձնակազմի կողմից: Նրանք առանձնապես համապատասխանում են հետևյալ պահանջներին:

a) Էլ. նկն. քարտերի ՀԿ –ն ունի բավարար աշխատակիցներ, որոնք ունեն մասնագետի գիտելիքներ, փորձ և որակավորում և պահաջվում են հատուկ ծառայությունների և հետևյալ պաշտոնների համար.

- Էլ.- նկն քարտերի ՀԿ-ի ղեկավար
- Անվտանգության Աշխատակից
- Աուդիտի Աշխատակից
- Ցանցային ադմինիստրատոր
- Տվյալների բազայի ադմինիստրատոր

- Համակարգի օպերատոր

b) Անձնակազմը անցնում է անվտանգության թեստեր, որը համապատասխանում է տվյալ դերին:
c) Այն անձիք, ովքեր խախտում են ՀԿ –ի ընթացակարգերը կամ գործընթացները, ենթարկվում են կարգապահական տույժերի:
d) Ըստ պարտականությունների, անվտանգության և պատասխանատու դերերը նշվում են համակարգի անվտանգության ընթացակարգում: Վստահված դերերը, որով պայմանավորված է համակարգի անվտանգությունը, ճշգրտորեն նշվում են 5.2 գլխում:
e) Ողջ անձնակազմը (ժամանակավոր և մշտական) ունի պարտականություններ, որոնք սահմանվում են՝ հաշվի առնելով պարտականությունների բաշխումը և որոշ լիազորությունները, ինչպես նշված է 5.2 գլխում:
f) ՀԿ-ի լիազոր անձնակազմը զերզ է մնում շահերի բախումից, որը կարող է վնաս հասցնել համակարգին:
g) Այն անձը, որը մուտք ունի դեպի ՀԿ փակ բանալիների բազա, ղեկավարի կողմից պաշտոնապես ստանձնում է է լիազոր անձի դեր:
h) ՀԿ-ը չի նշանակում որևէ անձի որպես ղեկավար կամ լիազոր անձ, եթե նա նախկինում մեղադրվել է հանցանքի համար կամ այլ պատիժ է կրել և որի բնութագիրը չի համապատասխանում տվյալ պաշտոնին: Տվյալ անձը չի կարող պաշտոնը ստանձնել, եթե չի անցկացվել համապատասխան ստուգում:

5.4 Աուդիտի Գրանցման Տվյալների Ընթացակարգեր

Էլ.-նկն քարտերի ՀԿ-ը, օգտվում է նույնիսկ գրանցման ընթացակարգերից՝ վերլուծություններ կատարելու և ՀԿ-ի համակարգի ճիշտ ու սխալ կիրառման վերաբերյալ եզրակացություններ կատարելու նպատակով:
Համակարգի կարևոր դեպքերը պետք է գեներացնեն տվյալներ: Դրանք առնվազն ներառում են հետևյալը՝

- Հավաստագրի կիրառում, դիմում, թողարկում, թարմացում, վերաթողարկում կամ անվավերություն
- Մուտքի փորձեր դեպի գաղտնի համակարգեր (օրինակ՝ HSM):
- Գործողություններ՝ կատարված աշխատանքային խմբի անդամների կողմից:
- Ֆիզիկապես մուտքի/ելքի ապահովում
- Բոլոր դեպքերի գրանցումները
- Պատահարի ամսաթիվ և ժամ
- Պատահարի ցուցիչ
- Անձի նույնականացում, որը դեպքի պատճառ է հանդիսացել
- Դեպքի նկարագրությունը

Էլ.-նկն. քարտերի ՀԿ-ը ապահովում է, որպեսզի հավաստագրի զգալի տվյալները գրանցվեն համապատասխան ժամանակահատվածում և առնվազն համապատասխանի 8-րդ գլխում նկարագրված աուդիտի և այլ պահանջներին:
Էլ.-նկն. քարտերի ՀԿ-ը ապահովում է ընթացիկ և լրացված տվյալների գաղտնիությունը և ամբողջությունը, որն առնչվում է հավաստագրերին և որոնք լրացվում են ամբողջական և գաղտնի ձևով: Էլ.-նկն.քարտերի ՀԿ-ը ապահովում է նաև, որպեսզի դեպքերի գրանցամատյաններում գրանցվեն նաև բանալիների և հավաստագրի կառավարման դեպքերը՝ սկսած հավաստագրի գրանցման գործընթացից մինչև հավաստագրի անվավերությունը, և դեպքերի վերաբերյալ տրամադրվող ճիշտ ժամանակը, ներառյալ այն դեպքերի, որոնք առնչվում են հավաստագրի և բանալիների կենսացիկլին:
Դեպքերի գրանցամատյանում ընդգրկված հատուկ տվյալները և պատահարները զետեղվում են փաստաթղթերում՝ Գործառնական և Անվտանգության Ընթացակարգերի համաձայն: Կարևոր է, որ դեպքերը գրանցվեն գրանցամատյանում այն ձևով, որպեսզի հեշտությամբ չջնջվեն կամ ոչնչացվեն պահանջվող արխիվացման ժամանակահատվածում (բացառությամբ՝ երկարաժամկետ պահպանման դեպքում): Մանրամասները նկարագրվել են Գործառնական և Անվտանգության Ընթացակարգերում:

5.5 Տվյալների Արխիվացում

ԷԿԵՆԳԸ պատասխանատու է աուդիտի ողջ տվյալների արխիվացման՝ ՀԿ-ի գործունեությանը վերաբերող էլեկտրոնային և թղթային գրանցումների համար:

Արխիվացված տվյալները պետք է պաշտպանված լինեն հետևյալի դեմ՝

- Փոփոխման և ոչնչացման
- Տվյալների բազա անթույլատրելի մուտքի
- Տեղեկատվական տվյալների պահոցի, որը պարբերաբար ենթարկվում է միգրացիաների
- Տվյալների հին ֆորմատի դեմ՝ բաց և ընդհանուր ստանդարտները ընդունելու միջոցով:

Էլ.-նկն. քարտերի ՀԿ-ը ներդրել է իր ՀԲԵ համակարգում արխիվացման ճիշտ ընթացակարգեր, որոնք տրամադրում են գաղտնի և ամբողջական տվյալներ:

5.6 Բանալու Փոխանցում

ՀԿ-ը ապահովում է, որպեսզի բանալիները գեներացվեն վերահսկելի պայմաններում և 5.2 ենթագլխում նկարագրված անվտանգության և համակարգի կառավարման ընթացակարգերին համաձայն: Էլ.-նկն. քարտերի ՀԿ-ը ստեղծում է ինքնաստորագրված հավաստագիր և էջանիշի հավաստագիր: Ընթացակարգը, որը համապատասխանում է սույն Հավաստագրման Կանոնակարգին առանձնացնում է բանալիների փոխանցման երկու հնարավորություն.

1. Էլ.-նկն. ՀԿ-ի ինքնաստորագրված հավաստագիրը թողարկվում և բաշխվում է համաձայն 2-րդ գլխի:
2. Էլ.նկն. քարտերի ՀԿ-ը հրապարակում է ՀԿ-ի նոր հանրային բանալի՝ էջանիշի հավաստագրով:

Էջանիշի հավաստագիրը ապահովում է գործընթացների շարունակական բնույթը՝ առանց հեռակա՝ ՀԿ-ի ինքնաստորագրված հավաստագիրը վստահելու անհրաժեշտության:

AR-CA բանալու փոխանակումը պարտադիր է, եթե ՀԿ-ի հավաստագիրը կորցնում է իր վավերականությունը կամ ՀԿ-ի փակ բանալին հասանելի չէ: Նման դեպքեր պատահում են հավաստագրի ժամկետի սպառման կամ փակ բանալու մուտքի անհասանելիության դեպքում (օրինակ՝ ապարատային սարքավորման խափանման դեպքում, որը պահում է հանրային բանալին):
Այնուամենայնիվ, նոր ինքնաստորագրված հավաստագրի հեռահար թողարկումը բավականին անհարմար է: Այն պետք է գեներացվի և լինի հասանելի, իսկ Վստահելի կողմերը վստահեն ինքնաստորագրված հավաստագրին:
Հետևաբար, եթե ՀԿ-ի հավաստագիրը դուրս է գործածությունից ոչ կարևոր պատճառներով (օրինակ՝ ապարատային սարքավորման խափանում, որը պահում է հանրային բանալի), այն կարող է փոխարինվել էջանիշի հավաստագրով:

5.7 Տվյալների Չարաշահում և Աղետային Իրավիճակ

Էլ.-նկն. քարտերի ՀԿ-ը ձեռնարկում է միջոցներ՝անխափան ծառայություն ապահովելու նպատակով. օրինակ՝

a) Միջոցներ, որը նվազեցնում է միջամտությունների ազդեցությունը՝ համակարգի անխափան աշխատանքը երաշխավորելու նպատակով: Նախատեսվում է կիրառել բարձր ինժիներական ցանցային ենթակառուցվածք, որը հասանելի է նշված տարածքում՝ սարքերի պարամետրերը ստուգելու և ֆիլտրող սարքավորումները նախօրոք գործարկելու միջոցով, որն ապահովում է անխափան էլեկտրոէներգիայի սնուցում կանխատեսված աշխատանքային ժամանակահատվածի համար՝ առանց օգտվելու էլեկտրոէներգիայի հանրային ցանցից:
b) Միջոցներ, որը նվազեցնում է նմանատիպ աղետների՝ օրինակ հրդեհ կամ հեղեղի ազդեցությունը համապատասխան պաշտպանիչ համակարգերի կիրառման դեպքում:

c) Միջոցներ, որոնք համաձայն տվյալ աշխատանքային համակարգի, հնարավորիս ապահովում են գլխավոր անձնակազմի հասանելիությունը, որն էլ իր հերթին ապահովում է ՀԿ-ի շարունակական գործունությունը: 5.3 գլխում նկարագրված հիմնական պաշտոնատարները պետք է ունենան իրենց փոխարինողները՝ պահպանելով դերերի անվտանգ բաշխման սկզբմունքը:

5.7.1 Տվյալների Չարաշահման և Պատահարների Ընթացակարգերը

Էլ. նկն.քարտերի ՀԿ-ը աղետի դեպքում, ներառյալ անձի փակ բանալու չարաշահումը, ապահովում է վերականգնել այն, որքան հնարավոր է շուտ՝ պահպանելով ներքևում նշված դեպքերը՝

1. Էլ.-Նկն. քարտերի ՀԿ-ը սահմանում և պահպանում է “Բիզնես շարունակական պլանը” աղետի դեպքում՝ արագ հակազդելու նպատակով (տես՝ ենթագլուխ 5.7.3):
2. ՀԿ –ի համակարգի տվյալները, որոնք անհրաժեշտ են կենտրոնի նորացման համար, տպվում և պահվում են համապատասխան անվտանգ տեղերում. այնպես, որ հնարավոր լինի ձախողման/աղետի դեպքում թարմացնել տվյալները: Տվյալ դեպքում կիրառվում են կողմնակի պահուստային միջոցներ:
3. Հաշվի առնելով աղետի հաճախականությունը և դրան առնչվող գործընթացների պլանավորումը, “Բիզնես շարունակական Պլանը” դիտում է փակ բանալու անվտանգության խախտումը որպես լուրջ խախտում:

5.7.2 Համակարգչային Միջոցներ, Ծրագրեր և/կամ Չարաշահված Տվյալներ

Համակարգչային վնասված միջոցների, ծրագրի և/կամ տվյալների վերաբերյալ ողջ տեղեկատվությունը փոխանցվում է անվտանգության աշխատակցին, որը համաձայն մշակված ընթացակարգի տալիս է հանձնարարականներ:
Այս ընթացակարգերը մշակված են՝ վերլուծելու հարձակման ուժգնությունը և հետազոտելու պատահարը, նվազեցնելու և դրա արդյունքները ապագայում իսպառ վերացնելու նպատակով: Ըստ անհրաժեշտության, էլ.-նկն. քարտերի ՀԿ-ի փակ բանալու չարաշահման կամ այլ վնասի դեպքում, համապատասխան քայլեր պետք է ձեռնարկվեն համաձայն Աղետի Վերականգման Պլանի՝ ընդհուպ մինչև վնասված տվյալների/սարքավորման, նմանատիպ սարքավորումների և /կամ արխիվացված/փոխարինող տվյալների վերականգնումը:

5.7.3 Անձի Փակ Բանալու Չարաշահման Ընթացակարգեր

Էլ.-նկն. քարտերի ՀԿ-ը “Բիզնես շարունակական Պլան” փաստաթղթում մանրամասն նկարագրում է էլ.-նկն. քարտերի ծառայության տրամադրումը ձախողման դեպքում, որի արդյունքում կենտրոնի հնարավորությունները արգելակվում են:

Էլ.-նկն. քարտերի ՀԿ-ի շտապ դեպքերը պայմանավորված են բնական աղետներով կամ կրիպտոգրաֆիկ սխալներով. օրինակ՝
1. Երկրաշարժ, ջրհեղեղ, մի- քանի օրվա էլեկտրոէներգիայի խափանում,
2. Կիրառվող ալգորիթմների խախտում (խնդիրներ EC կամ SHA-1)

Էլ. -նկն. քարտերի ՀԿ-ի փակ բանալու խափանում:

5.7.4 Բիզնես Հնարներ Աղետից Հետո

ՀԿ-ը ունի Աղետների Վերականգման Պլան՝ վտանգները կանխելու կամ սահմանափակելու համար՝

- ՀԿ-ի համակարգի վնասվածություն:
- Ծրագրի անսարքություն;
- Ցանցային ծառայությունների զգալի կորուստ:
- Ցանցի մասնակի վնասվածություն:

Բոլոր գրանցվողները և վստահելի կողմերը տեղեկացվում են, որքան հնարավոր է շուտ և տվյալ իրավիճակում ամենահարմար տարբերակով, յուրաքանչյուր էական անսարքության կամ վնասի մասին, որը վերաբերում է տեղեկատվական համակարգին կամ ցանցային միջավայրին: Աղետի վերականգման պլանը ներառում է ընթացակարգեր, որոնք կիրառվում են համակարգի յուրաքանչյուր պատահարի դեպքում (չարաշահում, վնասի բացահայտում և այլն):

5.8 Էլ.-նկն. Քարտերի ՀԿ-ի Փակումը

Էլ.-նկն քարտերի ՀԿ-ը պետք է ներդնի ընթացակարգեր և միջոցներ՝ սահմանափակելու կենտրոնի փակման հնարավորությունը: Այն նվազում է.

- Հաջորդող ՀԿ-ի հավաստագրերի թողարկման ընթացակարգերով,
- Փոխանցել հավաստագրման ծառայությունը արտաքին հավաստագրման կենտրոնին: Փակման կապակցությամբ, ՀԿ-ը պարտավոր է տեղեկացնել Գրանցվողներին և Վստահելի Կողմերին: Գրանցվողները տեղեկացվում են էլ-փոստի, իսկ Վստահելի Կողմերը կայքում հրապարակված հաղորդագրության միջոցով: Տեղեկությունը պետք է տրամադրվի առնվազն մեկ ամիս առաջ: Բոլոր գրանցվողների վավեր հավաստագրերի և ՀԿ-ի հավաստագրերի չեղյալ հայտարարումը եզրափակվում է գործունեության ավարտով:

6 Տեխնիկական Անվտանգության Վերահսկում

6.1 Զույգ Բանալիների Գեներացում և Տեղադրում

ՀԿ-ը պահում է իր փակ բանալիները համաձայն սույն ՀԳԿ պահանջների: ՀԿ-ը օգտագործում է փակ բանալիները միայն հավաստագրեր, ԱՀՑ ստորագրելու համար՝ զույգ բանալիներից որևէ մեկը օգտագործելու միջոցով:

6.1.1 Զույգ Բանալիների Գեներացում

Փակ բանալին գեներացվում է այս անվտանգ սարքում (օրինակ՝ HSM, կրիպտոգրաֆիկ բանալի): ՀԿ-ի փակ բանալիների գեներացումը հաստատվում է զույգ բանալիների սկզբմունքով: Մարդիկ գեներացման գործընթացի ժամանակ իրենց անձի իսկությունը հաստատում են ՀԿ-ի համակարգում գաղտնաբառի միջոցով – անվտանգ կրիպտոգրաֆիկ քարտով:
ՀԿ փակ բանալու գեներացումը կատարվում է առանձին անվտանգ սենյակում՝ վստահված անձնակազմի կողմից՝ նվազագույնը կրկնակի վերահսկողության ներքո: Պատասխանատու մարդկանց թիվը այս գործընթացի դեպքում պետք է սահմանափակվի նվազագույնով, իսկ գործընթացը պետք է կատարվի համաձայն ՀԿ կանոնների:

6.1.2 Փակ Բանալու Տրամադրումը Գրանցվողին

Էլ.- նկն. քարտերի ՀԿ-ը տրամադրում է փակ բանալին Գրանցվողին:
Էկետրոնային Նույնականացման Քարտի ձեռքբերման գործընթացի սկզբում Գրանցվողները իրավունք ունեն նշելու, որ ցանկանում են օգտագործել իրենց Հավաստագրերը: Էլեկտրոնային Նույնականացման քարտը պետք է տրամադրվի Գրանցվողին Հավաստագիրը բեռնված և ժամանակավորապես կասեցված վիճակում: Գրանցվողները կարող են ակտիվացնել հավաստագրերը ՏԳՄ-ում՝ օգտագործելով փոստային ծառայությամբ ուղարկված PIN կոդը:
Ենթակառուցվածքի հավաստագրերը փակ բանալիներով տրամադրվում են ՀԿ-ի անձնակազմին՝ համաձայն ԷԿԵՆԳ ՓԲԸ ներքին ընթացակարգի:

6.1.3 Հանրային Բանալու Տրամադրումը Հավաստագրման Կենտրոնին

Գրանցման Մարմինը տրամադրում է Գրանցվողների հանրային բանալիները Հավաստագրման Կենտրոնին: Դրանք ուղարկվում են էլեկտրոնային եղանակով, Հավաստագրման Կենտրոնի ծրագրային մեխանիզմների միջոցով: Այս մեխանիզմները

ապահովում են ուղարկվող հանրային բանալիների ամբողջականությունը և անժխտելիությունը:

6.1.4 ՀԿ Հանրային Բանալու Տրամադրումը Վստահելի Կողմերին:

ՀԿ-ի հանրային բանալին, որը թողակում է Գրանցվողների հավաստագրերը, բաշխվում է ITU-T X.509 v.3 ստանդարտի հավաստագրերի ձևով: Մինչդեռ էլ.-նկն. Քարտերի հավաստագրերն ունեն ինքնահավաստագրերի ձև, ՀԿ-ը բաշխում է իր հավաստագրերը երկու տարբեր մեթոդների միջոցով՝

- Տեղադրելով ԷԿԵՆԳ հանրային Պահոցում, հղում՝ http://www.ekeng.am/?page_id=74
- Վստահելի ծրագրերի հետ միասին (օրինակ՝ վեբ բրաուզերներ, էլ-փոստ ծրագրեր), որը թույլ է տալիս օգտվել Է ԷԿԵՆԳ-ի ծառայություններից:

6.1.5 Բանալու Չափը և Ծածկագրման Ալգորիթմներ

Սույն ՀԳԿ– ը և համապատասխան ՀՔ սահմանում են՝

- Զույգ բանալիները պետք է գեներացվեն՝ օգտագործելով RSA ծածկագրման ալգորիթմ:
- Հավաստագրման Կենտրոնի զույգ բանալիների երկարությունը կազմում է 4096 բիթ:
- Գրանցվողի զույգ բանալիների երկարությունըն կազմում է 2048 բիթ:
- Ենթակառուցվածքի հավաստագրի երկարությունը (օր. Համակարգի ադմինիստրատորներ) կազմում է 2048 բիթ:

6.1.6 Բանալու Կիրառման Նպատակները

Բանալու դաշտերի յուրաքանչյուր բիթ պետք է համապատասխանի հետևյալ կանոններին (յուրաքանչյուր բիթ ունի համապատասխան նշանակություն)

a) **ԹվայինՀավաստագիր(digitalSignature)** – հավաստագիր՝ նախատեսված էլեկտրոնային ստորագրության ստուգման համար, որն ունի այլ նպատակներ, քան այն, որոնք նշված են b), f) and g) կետերում:
b) **Անժխտելիություն (nonRepudiation)**– հավաստագիր՝ նախատեսված մատուցելու տվյալների անժխտելիության ծառայություն հատուկ անհատներին: Այն ունի այլ նպատակներ, քան այն, ինչ նշված է f) and g) կետերում: Անժխտելիության բիթը կարելի ուղարկել հանրային բանալու հավաստագրով, որը ստուգում է էլեկտրոնային ստորագրությունները և չպետք է համատեղվի այլ՝ հատկապես c) և e) կետերում նկարագրված նպատակների հետ և առնչվի գաղտնի տվյալների տրամադրմանը:
c) **Բանալուկոդավորում (keyEncipherment)**– նախատեսված է սիմետրիկ ալգորիթմային բանալիները կոդավորելու համար՝ ապահովելով տվյալների գաղտնիությունը:
d) **ՏվյալներիԾածկագրում(dataEncipherment)** – նախատեսված գրանցվողների տվյալները կոդավորելու համար և չի համապատասխանում c) և e) կետերին:
e) **ԲանալուՀամաձայնեցում (keyAgreement)** – նախատեսված բանալու համաձայնեցման պրոտոկոլների համար

f) **ԲանալիՀավաստՍտորագրման** (**keyCertSign)** – հանրային բանալի, որը կիրառվում է էլեկտրոնային ստորագրությունների ստուգման համար այն հավաստագրերում, որոնք թողարկվում եմ հավաստագրման ծառայությունների կողմից:

g) **ԱՀՑստորագրում** (**cRLSign) –** հանրային բանալի՝ ստուգելու անվավեր կամ կասեցված հավաստագրերի ցուցակների էլեկտրոնային ստորագրությունները, որոնք թողարկվել են հավաստագրման ծառայությունների կողմից:

h) **Միայնկողավորում (encipherOnly) –** կարող է կիրառվել միայն **ԲանալուՀամաձայնեցում** բիթի հետ՝ տվյալների ծածկագրման նպատակը ԲանալուՀամաձայանեցման պրոտոկոլի մեջ նշելու համար:

i) **Միայնապակոդավորում(decipherOnly)** - կարող է կիրառվել միայն ԲանալուՀամաձայնեցում բիթի հետ՝ բանալու համաձայնեցման պրոտոկոլի մեջ բանալու ապակոդավորման նպատակը նշելու համար:

6.1.7 Թարմացված բանալու Կիրառություն

Ի լրումն ստանդարտ բանալու, այս դաշտը սահմանում է կիրառման մեկ կամ մի քանի ոլորտներ: Սահմանված են բանալու կիրառման հետևյալ հնարավոր նպատակները՝

a) սերվերԱuth(serverAuth)– TLS WWW սերվերի նույնականացում: Բանալու բիթը համատեղելի է թվայինՍտորագրություն, բանալուԿոդավորում և բանալուՀամաձայնեցում բիթերի հետ:

b) **հաճախորդի անձի ստուգում(client authetication**) - Բանալի, որը համատեղելի է թվայինՍտորագրություն և/կամ բանալուՀամաձայանեցում բիթերի հետ:

c) կոդիՍտորագրում(codeSigning)– ստորագրում է ներբեռնելի կոդը: Բանալու արժեքը կարող է համատեղելի լինել թվայինՍտորագրություն բիթի հետ:

d) էլ-փոստիԱպահովում(emailProttection) – Բանալի, որը համատեղելի է թվայինՍտորագրութուն, անժխտելիություն և/կամ բանալուԿոդավորում կամ ԲանալուՀամաձայնեցում բիթերի հետ:

e) **Ժամադրոշմ (timeStamping) –** միացնում է որևէ օբյեկտի հեշը (hash) ժամին: Բանալու կիրառման արժեք, որը համատեղելի է թվայինՍտորագրություն և/կամ անժխտելիություն (non-Repudation) բիթերի հետ:

f) **OCSP ստորագրում (OCSPSigning)–** բանալու կիրառման բիթ, որը համատեղելի է թվայինՍտորագրություն և կամ անժխտելիություն բիթերի հետ:

6.2 Փակ Բանալու Պահպանումը և Կրիպտոգրաֆիկ Մոդուլների Տեխնիկական Անվտանգությունը

ՀԿ-ը ապահով գեներացնում և պահում է փակ բանալին (ները)՝ օգտագործելով անվտանգ համակարգ և ձեռնարկում անհրաժեշտ միջոցներ՝ կանխելու անթույլատրելի կիրառումը և դրանց ոչնչացումը: Այս գործընթացը կատարվում է Հայաստանի Հանրապետության ներկայացուցիչների վերահսկման ներքո ՝ ապահովելու կառավարության վստահությունը ՀԿ-ի Բանալու Գեներացման ընթացակարգի ճիշտ և անվտանգ կատարման հանդեպ: ՀԿ-ը ներդնում և կազմում է բանալիների գեներացման ընթացակարգերի փաստաթուղթը՝ համաձայն այս ՀԳԿ-ի: ՀԿ-ը ընդունում է եվրոպական, միջազգային և հանրային ստանդարտները վստահելի համակարգերում: Առնվազն երեք վստահելի աշխատակիցներ

մասնակցում են ՀԿ-ի փակ բանալու (բանալիների) գեներացման և տեղադրման գործընթացին:

6.2.1 Կրիպտոգրաֆիկ Մոդուլի Ստանդարտներ և Վերահսկում

Էլ.-նկն. քարտերի ՀԿ-ի փակ բանալու գեներացումը կատարվում է ապահով կրիպտոգրաֆիկ սարքի միջոցով՝ պահպանելով համապատասխան պահանջները՝ ներառյալ FIPS ստանդարտների 140-1 մակարդակ 3-ը:
ՀԿ փակ բանալու գեներացումը պահանջում է ՀԿ-ի անձնակազմի ավելի քան մեկ լիազոր անձի ներկայություն, որը կծառայի համապատասխան պաշտոնում, ինչպես նաև առնվազն կառավարության և ՀԾՄ-ի մեկ ներկայացուցիչ: ՀԿ ղեկավար մարմնի ավելի քան մեկ անդամի դեպքում միայն թույլատրվում է բանալու գեներացումը:

6.2.2 Փակ Բանալու (n out of m) Բազմակի Ստուգում

Հավաստագրման Կենտրոնի փակ բանալին գեներացվում է անվտանգ սարքի միջոցով (օրինակ է HSM, կրիպտոգրաֆիկ բանալի) և բաժանվում “5-ից 3-ը” սկզբմունքով: Սա նշանակում է, որ 5 գաղտնի շարքից 3-ը թույլ կտան ՀԿ-ի փակ բանալուն վերականգնվել: Գրանցվողների փակ բանալիները բաժանելի չեն՝ գաղտնիությունը ապահովելու համար:

Բաժանելի գաղտնիքները պահվում են կրիպտոգրաֆիկ քարտերի վրա՝ պաշտպանված PIN կոդով և փոխանցվում սեփականատերերին վավերացված ձևով:
Առնվազն ՀԿ-ի երեք անդամ պետք է միաժամանակ ակտիվացնեն ՀԿ փակ բանալին:

6.2.3 Փակ Բանալու Պահումը Երրորդ Անձի Կողմից

Սույն Հավաստագրման Գործունեության Կանոնակարգը չի թույլատրում բանալու պահումը երրորդ անձի կողմից:

6.2.4 Պահուստային Փակ Բանալի

ՀԿ-ի պահուստային մեխանիզմները գործում են փակ բանալու բաժանման միջոցով, որը պետք է բաժանվի ավելի մեծ թվի քան այն, որը պահանջվում է բանալին վերականգնելու համար:

6.2.5 Փակ Բանալու Արխիվացում

Փակ բանալու արխիվացումը նախատեսված չէ սույն Հավաստագրման Գործունեության Կանոնակարգի կողմից:

6.2.6 Փակ Բանալու Փոխանցումը Կրիպտոգրաֆիկ բանալուց կամ բանալու մեջ

Փակ բանալու մուտքը կրիպտոգրաֆիկ մոդուլի մեջ նախատեսված չէ Սույն Հավաստագրման Գործունեության Կանոնակարգի կողմից:

6.2.7 Փակ բանալու Ակտիվացման Մեթոդ

ՀԿ-ի փակ բանալու ակտիվացումը պահանջում է երկու մարդկանց համագործակցության անհրաժեշտություն, որոնք ունեն քարտերի PIN կոդերը և բանալիները, 3/5 հատուկ բաժանման սկզբմունքով:
Գրանցվողի բանալիները ակտիվացնելու համար պետք է իմանալ ID քարտի PIN կոդը:

6.2.8 Փակ Բանալու Ոչնչացման Մեթոդ

Իր կենսացիկլի վերջում, ՀԿ-ի փակ բանալին ոչնչացվում է ՀՀ Պետական Մարմնի ներկայացուցչի ներկայությամբ, որպեսզի փակ բանալիները երևէ չվերականգնվեն և կրկին կիրառվեն: ՀԿ բանալիները ոչնչացվում են իրենց սկզբնական և պահուստային տեղեկատվական միջոցները ոչնչացնելու միջոցով, ջնջելով և մասնատելով դրանց մասերը և ջնջելով, անջատելով և վերջնակապանես վերացնելով ցանկացած ապարատային մոդուլ, որտեղ պահվում են բանալիները:
Բանալիների ոչնչացման ընթացակարգի մասին կազմվում է փաստաթուղթ և դրան վերաբերող յուրաքանչյուր գրանցում արխիվացվում է:
Գրանցվող անձը պատասխանատու է իր բանալիների ոչնչացման համար:

6.3 Բանալու Կառավարման Այլ Ասպեկտներ

6.3.1 Հանրային Բանալու Արխիվացում

ՀԿ-ը անվտանգ ձևով պահպանում և արխիվացնում է իր փակ բանալու ակտիվացման տվյալները և գործառույթները:
Գրանցվող անձը պարտավոր է պահել PIN կոդը, որը թույլ է տալիս փակ բանալու միջոցով մուտք գործել ՀԿ, որը թողարկում է հավաստագրեր, արխիվացնում Գրանցվողի Հանրային բանալիները:

6.3.2 Հավաստագրի Գործառութային Ժամանակահատված

Կիրառման ժամանակահատվածը պայմանավորված է հավաստագրով:
2-րդ աղյուսակը ներկայացնում է հավաստագրի կիրառման առավելագույն և նվազագույն կիրառումը:

Հավաստագրի Տեսակ	**Վավերականության Ժամանակահատված**
Ազգային ՀԿ	25 տարի
Գլխավոր ՀԿ	14 տարի
Էլ-ստորագրություն	10 տարի
Էլ. Նույնականացում	10 տարի
Ենթակառուցվածքի հավաստագրեր	5 տարի

Աղյուսակ 2: Հավաստագրի կիրառման ժամանակահատվածներ

6.4 Ակտիվացման Տվյալներ

ՀԿ-ը ապահով պահում և արխիվացնում է ակտիվացման տվյալները իրենց փակ բանալիների և գործառույթների հետ:
Գրանցվող անձը պարտավոր է պահպանել PIN կոդը՝ փակ բանալու մուտքային տվյալը:

6.5 Համակարգչի Անվտանգության Վերահսկում

ՀԿ ներդնում է համակարգչային անվտանգության վերահսկման որոշ մեխանիզմներ:

6.6 Տեխնիկական Վերահսկման Կենսացիկլ

Էլ.-նկն. քարտերի ՀԿ-ը, փոփոխությունների դեպքում, պաշտպանված է անվտանգ սարքավորումներով:
Էլ.- նկն. քարտերի ՀԿ-ի յուրաքանչյուր նախագծի մշակման և տեխնիկական առաջադրանքի մշակման փուլում, կատարվում է անվտանգության պահանջների վերլուծություն SS համակարգերի անվտանգությունն ապահովելու նպատակով, որն իր ազդեցությունն ունի անվտանգ համակարգերի և ծրագրերի վրա:
Էլ.-նկն. քարտերի ՀԿ-ի բոլոր ծրագրերի համար գործում են ընթացակարգեր՝ կառավարելու ծրագրային փոփոխությունները և ծրագրային հրատապ իրավիճակները:

6.7 Ցանցի Անվտանգության Վերահսկողություն

ՀԿ-ը պահում է անվտանգության համակարգերի բարձրակարգ ցանց՝ ներառյալ միջցանցային էկրանները (firewalls): Ցանցային ներխուժումը վերահսկվում և բացահայտվում է. հատկապես՝

ՀԿ-ի և ԳՄ –ի միջև ողջ հաղորդագրությունը, որը վերաբերում է Գրանցվողի Հավաստագրի Կենսացիկլի յուրաքանչյուր փուլին, պաշտպանված է ՀԲԵ ծածկագրման և ստորագրման մեթոդներով՝ գաղտնիությունը և անձի իսկությունը փոխադարձ հաստատելու նպատակով: Այն ներառում է հաղորդակցություն՝ հավաստագրի հայտերի, թողարկման, կասեցման, ապակասեցման և անվավերության վերաբերյալ:

ՀԿ-ի կայքը ապահովում է ծածկագրված կապ՝Անվտանգ Պորտի Շերտ (SSL) պրոտոկոլի և հակավիրուսային ապահովման միջոցով:

ՀԿ-ի ցանցը պաշտպանված է միջցանցային էկրաններով (firewall) –ով և ծրագրային ներխուժումները հայտնաբերող համակարգերով:

Արգելված է մուտքը դեպի ՀԿ-ի գաղտնի՝ ներառյալ ՀԿ-ի տվյալների բազան դրսից՝ ՀԿ-ի օպերատորի անձնական ցանցի միջոցով: Տվյալների տրամադրման կամ հայցի ինտերնետ սեսսիաները կոդավորվում են:

6.8 Ժամադրոշմ

Չի կիրառվում:

7 Հավաստագրի և ԱՀՑ-ի բնութագիր

Այս բաժինը բնութագրում է ԱՀՑ-ը, հավաստագրի և OCSP ֆորմատները:

7.1 Հավաստագրի Բնութագիրը

Հավաստագրերը կամ ԱՀՑ-ների բնութագրերը համատեղելի են ITU-T ստանդարտի X.509 v3 (RFC 3280) ֆորմատների հետ:

Էկետրոնային հավաստագիրը կառուցվածքային տվյալների դաշտերից բաղկացած հաջորդականություն է, որը պարունակում է Գրանցվողի տվյալները՝ հավաստագրին կցված հանրային բանալի և այլ տվյալներ, որն անհրաժեշտ է թվային հավաստագրի արդյունավետ կիրառման համար:

Հավաստագիրը պարունակում է հետևյալ հիմնական դաշտերը՝

Դաշտի անվանում	Արժեք	Դաշտի նկարագրություն
Տարբերակ	2	Հավաստագրի ֆորմատի երրորդ տարբերակ (X.509 v.3)
Սերիայի համարը	Թվային արժեք	Հավաստագրի սերիայի համարը, եզակի համար ՀԿ տիրույթում (domain)
Ստորագրության ալգորիթմ	Sha256withRSA	Ալգորիթմի ցուցիչ, որը կիրառվում է հավաստագրեր թողարկող կենտրոնի կողմից
Թողարկող	Տարբերակիչանուն (DN)	Հավաստագրման կենտրոնի տարբերակիչ անուն (DN)
Հետո (Not before)	ՀԿԺ (UTC)	Վավերականության ժամկետ՝ հավաստագրի վավերականության ժամկետի սկիզբը
Առաջ (Not after)	ՀԿԺ(UTC)	Վավերականության ժամկետ՝ հավաստագրի վավերականության ժամկետի ավարտը
Սուբյեկտ	Տարբերակիչ անուն (DN)	Գրանցվողի և հավաստագրի տարբերակիչ անունը
Հանրային բանալու տեղեկություն	RSA հանրային բանալի	Հանրային բանալու արժեք՝ բանալուն առնչվող ալգորիթմի կողմնորոշիչով
Հավաստագրի տիպ/ձևաչափ (extension)	Տիպերի խումբը	Հավաստագրի տիպը տալիս է լրացուցիչ տեղեկատվություն հավաստագրի կիրառման վերաբերյալ: Հավաստագրի տիպերի թույլատրելի խումբը տրված է Գլուխ 7.1.1-ում:
Ստորագրություն	Թվային ստորագրություն	Թվային ստորագրություն՝ գեներացված ՀԿ-ի կողմից գրանցվողի հավաստագրում.

Վերը նշված բոլոր դաշտերը գտնվում են Գրանցվողների հավաստագրերում՝թողարկված էլ.-նկն. Քարտերի ՀԿ-ի կողմից:

7.1.1 Հավաստագրի Տիպեր

Հավաստագրի տիպերը իրենց մեջ կրում են լրացուցիչ տեղեկություն, ինչպես օրինակ՝ հանրային բանալու կիրառումը հավաստագրում կամ Գրանցվող անձի նույնականացնումը: Ներքևում նշված են բոլոր ընդունելի տիպերը, որոնք կարող է ներառվել Գրանցվողի Հավաստագրերում՝ թողարկված համաձայն ՀԳԿ և ՀՔ պահանջների:

Անվանում	Արժեք	Նկարագրություն	Կարգավիճակ
Բանալու կիրառում (keyUsage)	Բիթերի համադրություն	Նշում է զույգ բանալիների կիրառման սահմանը: Թույլատրելի համադրությունները նկարագրված են Գլուխ 6.1.6.	Կրիտիկական
Թարմացված բանալու կիրառում (ExtendedKeyUsage)	Բիթերի համադրություն	Թույլատրելի համադրությունները նկարագրված են գլուխ 6.1.7-ում:	Ոչ կրիտիկական
Բանալու Կողմնորոշիչ (SubjecKeyIdentifier)	Տվյալների կառուցվածք	Բանալիների կողմնորոշչի տիպը թույլ է տալիս նույնականացնել հավաստագրեր, որոնք պարունակում են հատուկ հանրային բանալի	Ոչ կրիտիկական
Հավաստագման կենտրոնի բանալու կողմնորոշիչ (Authority Key Identifier)	Տվյալների կառուցվածք	Նույնականացնում է հանրային բանալին, որը համապատասխանում է փակ բանալուն և կիրառվում է ԱՀՑ-ը ստորագրելու համար	Ոչ կրիտիկական
Սուբյեկտի այլընտրանքային անուն (SubjectAlternativeName)	Էլ փոստ - RFC 822	Հավաստագրին կապված սուբյեկտի լրացուցիչ նույնականացում	Ոչ կրիտիկական
ԱՀՑ-ի բաշխման կետեր (CRLDistribution points)	հղում	Անվավեր Հավաստագրերի ցուցակի բաշխման կետեր	Ոչ կրիտիկական
Կենտրոնի տեղեկատվության հասանելիություն (Authority Info Access)	հղում	OCSP:http://…….	Ոչ կրիտիկական
Հիմնական Սահմանափակումները (BasicConstraints)	Բիթերի համադրություն	Սահմանում է ՀԿ-ի հավաստագրի սուբյեկտին և հավաստագրման ուղու առավելագույն երկարությունը	Կրիտիկական

Հավաստագրի տիպը կարևոր է հավաստագրի վերծանման և դրա հետ կապված հանրային բանալու համար: Հավաստագրի տիպը կարելի է բնորոշել որպես՝

- Կրիտիկական – հավաստագրի տիպի տվյալները պետք է անվերապահորեն գործարկվեն և համապատասխան վերծանվեն վստահելի կողմին (օրինակ՝ համապատասխան ծրագրի միջոցով)։ Եթե նշված տվյալները ճիշտ չեն կարող վերծանվել, վստահելի կողմը ստիպված է մերժել այն տեղեկատվությունը, որը կիրառել է հավաստագիր էլեկտրոնային եղանակով:

- Ոչ կրիտիկական – տվյալներ, որը պահվում է պիտակված ոչ կրիտիկական տիպերում և կարող է այլընտրաքային ձևով գործարկվել վստահելի անձի կողմից։ Եթե վստահելի կողմը ընդունակ չէ ստուգել տվյալները, ապա կարող է առանց վարանելու հրաժարվել գործողությունից, առանց վախենալու, որ վստահված հավաստագիրը վնասված է:

7.1.2 Էլ. Ստորագրության Հավաստագիրը

Դաշտ	**Նկարագրություն/Արժեք**	**Կարգավիճակի դաշտը**
Կենտրոնի բանալու կողմնորոշիչ (AuthorityKeyIdentifier)	Նույնականացնում է հանրային բանալին, որը կիրառվում է ստուգելու թողարկված հավաստագիրը	Ոչ կրիտիկական
ԲանալուԿիրառում (keyUsage)	Գրանցվողի բանալու կիրառությունը Թույլատրելի արժեքներ • անժխտելիություն	Կրիտիկական
Հավաստագրի Ընթացակարգեր (certificatePolicies)	Հավաստագրման ընթացակարգի սահմանում	Ոչ կրիտիկական
Ընթացակարգի Կողմնորոշիչ (policyIdentifier)	OID {....} (ՀՔ սահմանում, որի համաձայն թողարկվում է հավաստագիրը)	Ոչ կրիտիկական
Սուբյեկտի այլընտրանքային անուն (subjectAltName)	Հնարավոր արժեքների այլընտրանքային տիպ rfc822Name (էլ-փոստի հասցե)	Ոչ կրիտիկական

Հիմնական Սահմանափակումները (BasicConstraints)	Դատարկ հաջորդականություն (սահմանելու արդյոք գրանցվողը օգտվող է թե մարմին, որը թողարկում է հավաստագրեր)	Կրիտիկական
ԱՀՑ-ի բաշխման կետեր (CRLDistribution points)	Դաշտը սահմանում է սերվերի հասցեն, որտեղից կարող եք ներբեռնել ԱՀՑ-ն (CRL) :	Ոչ կրիտիկական
Կենտրոնի տեղեկատվության հասանելիություն (Authority Info Access)	OCSP:http://……	Ոչ կրիտիկական

7.1.3 Հավաստագիր Էլ. Նույնականացման Համար

Դաշտ	Նկարագրություն/Արժեք	Կարգավիճակի դաշտը
Հավաստագրման Բանալու Կողմնորոշիչ (AuthorityKeyIdentifier)	Նույնականացնում է հանրային բանալին, որը կիրառվում է ստուգելու թողարկված հավաստագիրը	Ոչ կրիտիկական
ԲանալուԿիրառում (keyUsage)	Սահմանում է Գրանցվողի բանալու կիրառությունը Թվային Ստորագրություն Բանալու Ծածկագրում Տվյալների Ծախկագրում	Կրիտիկական
Հավաստագրի Ընթացակարգեր (certificatePolicies)	Հավաստագրման ընթացակարգի սահմանում	Ոչ կրիտիկական
Ընթացակարգի Կողմնորոշիչ (policyIdentifier)	OID {....} (ՀՔ սահմանում, որի համաձայն թողարկվում է հավաստագիրը)	Ոչ կրիտիկական
Սուբյեկտի այլընտրանքային անուն (subjectAltName)	Հնարավոր արժեքների այլընտրանքային տիպ rfc822Name (էլ-փոստի հասցե)	Ոչ կրիտիկական
Հիմնական Սահմանափակումները (BasicConstraints)	Դատարկ հաջորդականություն (սահմանելու արդյոք գրանցվողը օգտվող է թե մարմին, որը թողարկում է հավաստագիր)	Կրիտիկական
ԱՀՑ-ի բաշխման կետեր (CRLDistribution points)	Դաշտը սահմանում է սերվերի հասցեն, որտեղից կարող եք ներբեռնել ԱՀՑ-ն (CRL) :	Ոչ կրիտիկական

7.1.4 Ենթակառուցվածքի Հավաստագիր

Ենթակառուցվածքի հավաստագրերը չեն կարող կիրառվել՝ ստուգելու վստահված էլեկտրոնային ստորագրություններ: Ենթակառուցվածքի հավաստագրերի տիպը հիմնված է էլ. նույնականացման հավաստագրերի տիպի վրա: Դրանց կիրառությունը հատկապես նույնատիպ է ծածկագրման ալգորիթմների և դրանց պարամետրերի տեսանկյունից, ինչպես սահմանված է Գլուխ 6-ում: Նրանք ունեն նաև նույն հեշերի ֆունկցիաները:
Տարբերությունները հետևյալն են՝

a) ընդունված ստանդարտների և տիպերի պակասը
b) ԲանալուԿիրառում(KeyUsage) արժեքում հնարավոր է կիրառել բիթերի համադրություններ՝ սահմանելու հավաստագրի կիրառման հետևալ ձևերը:

- *“ԹվայինՍտորագրություն”* – ապահովում է տվյալների փոխանցման կամ արխիվացման դեպքում, հավաստագրի ամբողջականությունը, հիմնական օգտվողներին և դեպքերի լոգ ֆայլերը՝ ստուգելու սարքավորումների հասանելիությունը
- “ԲանալուԿոդավորում” և “ԲանալուՀամաձայնեցում” – համաձայնեցնել պրոտոկոլները և բանալու բաշխումը ՝ տվյալների գաղտնիությունը ապահովելու նպատակով: Ենթակաուցածքների հավաստագրերին կցվող Կրիպտոգրաֆիկ բանալիները պահվում են կրիպտոգրաֆիկ բաղկացուցիչներում:

7.2 ԱՀՑ (CRL) Բնութագիր

ԱՀՑ-ը (CRL) տվյալներից բաղկացած դաշտերի հաջորդականություն է, որը պարունակում է տեղեկատվություն անվավեր կամ կասեցված հավաստագրերի, ինչպես նաև պարունակում է տեղեկություն Հավաստագրման Կենտրոնի պատասխանատուի կողմից տվյալ ցուցակի գեներացման վերաբերյալ: Յուրաքանչյուր ԱՀՑ պարտադիր ներառում է տեղեկություն իր վավերականության ժամանակահատվածի մասին:

ԱՀՑ-ը պարունակում է հետևյալ դաշտերը

Դաշտ անվանում	Արժեք	Նկարագրություն
Տարբերակ	1	X.509 տարբերակիչ համարանիշ
Սերիայի համար	Թվային արժեք	Հավաստագրի սերիայի համարը, եզակի համարանիշ հավաստագրման կենտրոնի տիրույթում
Ստորագրության ալգորիթմ	Sha256withRSA	Ալգորիթմի ցուցիչ, որը կիրառվում է հավաստագրեր թողարկող կենտրոնի կողմից
Թողարկող	Տարբերակիչ անուն (DN)	Հավաստագրման կենտրոնի տարբերակիչ անուն (DN)

Այսթարմացումը	ՀԿԺ (UTC)	ԱՀՑ վավերականության ժամկետի սկիզբը
Հաջորդթարմացումը	ՀԿԺ (UTC	ԱՀՑ վավերականության ժամկետի ավարտը
ԱնվավերՀավաստագրեր	Անվավեր կամ ժամանակավոր կասեցված հավաստագրերի ցուցակ	Տեղեկությունը բաղկացած է 4 ենթադաշտերից: • userCertificate –անվավեր հավաստագրի սերիայի համարը, • revocationDate –անվավեր հավաստագրի ամսաթիվը, • crlEntryExtensions –մուտք դեպի ԱՀՑ (պարունակում է լրացուցիչ տեղեկություն անվավեր հավաստագրերի մասին – այլընտրանքային), CRLReason (պարունակում է հավաստագրի անվավերության պատճառը – այլընտրանքային)
Օգտվողի Հավաստագիր	Թվային արժեք	Անվավեր կամ կասեցված հավաստագրի սերիայի համար
Անվավերության ամսաթիվը	ՀԿԺ (Czas wg UTC)	անվավերության կամ կասեցման ամսաթիվը և ժամը.
ԱՀՑ-ի Պատճառ	Թվային արժեք	Հավաստագրի կասեցման կամ անվավերության պատճառը: Ընդունելի դաշտի արժեք՝ նշված 7.2.2 դաշտում
Հավաստագրի տիպ	Տիպերի խումբ	Սահմանում է լրացուցիչ տեղեկություն հավաստագրի կիրառման մասին
	Թվային Ստորագրություն	Թվային Ստորագրություն՝ գեներացված ՀԿ-ի կողմից ԱՀՑ-ի համար

Ներքևում նշված են հավաստագրերի բոլոր ընդունված տիպերը (extensions), որոնք կարող են ներառվել ԱՀՑ-ում:

Տիպ	Արժեք	Դաշտի նկարագրություն	Դաշտի կարգավիճակը
Հավաստագրման Բանալու Կողմնորոշիչ	Տվյալների կառուցվածք	Նշում է ՀԿ հավաստագրում, որը պարունակում է հանրային բանալու որոնման հնարավորություն (օրինակ – ծրագրի կողմից)	Ոչ կարևոր

Հիմք ընդունելով ITU-T X.509 v3 (RFC 2459) հավաստագիրը, ԱՀՑ-ում կարելի է ընտրել հավաստագրի վավերականության փոփոխման պատճառներից մեկը:

Պատճառի կոդը	Կոդի արժեքը	Նկարագրություն
unspecified	0	Նշված չէ
keyCompromise	1	Բանալու բացահայտում կամ կեղծում
cAcompromise	2	ՀԿ բանալու կորզում
affiliationChanged	3	Գրանցվողների տվյալների փոփոխություն
superseded	4	Հավաստագրի թարմացում
cessationofOperation	5	Հավաստագրի կիրառման դադար

certificateHold	6	Հավաստագրի կասեցում

Հավաստագրի (ապա) կասեցման տեղեկատվությունը չի հրապարակվում ԱՀՑ-ում: (Ապա) Կասեցումը հանդիսանում է տվյալ հավաստագրի անվավերության պատճառը ԱՀՑ-ից:

7.3 OCSP Պրոտոկոլի Բնութագիրը

OCSP հետևում է IETF PKIX RFC2560 OCSP v1 ստանդարտներին:

Հավաստագրի կարգավիճակի ստուգումը կատարվում է ԷԿԵՆԳ –ի կողմից՝ ի դեմս հավաստագրման կենտրոնի: OCSP սերվերը, որը թողարկում է տեղեկություն հավաստագրի կարգավիճակի մասին, ունի հատուկ զույգ բանալիներ՝ ստեղծված միայն այդ նպատակի համար:

Հավաստագրերի կարգավիճակի ստուգման սերվերի հավաստագիրը պարունակում է extKeyUsage արժեքը՝ նկարագրված RFC 5280 փաստաթղթում: Այս տիպը պետք է սահմանվի որպես կրիտիկական և նշանակում է, որ հավաստագրման կենտրոնը, որը թողարկում է հավաստագիր OCSP սերվերի համար, հավաստում է իր ստորագրությամբ թողարկելու հավաստագրի կարգավիճակի մշակված կառուցվածք (այս կենտրոնի գրանցվողների հավաստագրեր):
Էլ. Ստորագրության հավաստագրերը պետք է նաև պարունակեն ոչ կրիտիկական ձևեր: AuthorityInfoAccess արժեքը սահմանում է ծառայությունից օգտվելու հնարավորությունը՝ հաստատելու հավաստագրի վավերականությունը առցանց տարբերակով: (OCSP)

Դաշտ	**Նկարագրություն /Արժեք**	**Կարգավիճակի դաշտ**
AuthorityKeyIdentifier	Սահմանում է Հանրային բանալին, որը կիրառվում է՝ թողարկված հավաստագիրը ստուգելու համար	Ոչ կրիտիկական
keyUsage	Գրանցվողի բանալու կիրառությունը Թույլատրելի արժեքներ: • Թվային Ստորագրություն	Ոչ կրիտիկական
extendedKeyUsage	OCSP ստորագրում	Ոչ կրիտիկական
ocspNoCheck	Զրո	Ոչ կրիտիկական

8 Համաձայնեցման Աուդիտ և Այլ Գնահատումներ

ՀԾՄ (Հավաստագրման ծառայության մատակարարը) անցնում է աուդիտ՝ ապահովելու ՀԳԿ-ի պահանջները, ստանդարտները, ընթացակարգերը և ծառայության մակարդակը: ՀԾՄ-ի գործունեությունը և ընթացակարգերը ենթարկվում են աուդիտի, որը չի հրապարակվում որոշակի հանգամանքներում՝ ինչպես օրինակ գաղտնիություն, առևտրային գաղտնիք և այլն: Նմանատիպ աուդիտները կարող են անցկացվել ուղղակի կամ գործակալի միջոցով՝

- Հավաստագրման Ծառայության Մատակարարի Վերահսկիչ մարմնի կողմից:
- Հայաստանի կառավարության կողմից կամ ՀՀ Կառավարության կողմից նշանակված երրորդ անձի կողմից:

ՀԾՄ-ը գնահատում է այս աուդիտների արդյունքները՝ հետագայում դրանք կիրառելու նպատակով: Աուդիտներ անցկացնելու համար, նշանակվում է անկախ աուդիտոր, որը չի առնչվում ՀԿ-ի հետ ուղղակի կամ անուղղակի ձևով կամ որևէ այլ ՀԿ-ի հետ՝ շահերի բախումից խուսափելու նպատակով:
Աուդիտը անդրադառնում է հետևյալ հարցերին՝

- ՀԾՄ-ի գործառնական ընթացակարգերի և սկզբմունքների համաձայնեցումը ՀԳԿ ընթացակարգերի և ծառայության մակարդակների պահանջներին:
- Ենթակառուցվածքի կառավարում, որը ներդրվում է ՀԾՄ ծառայությունների կողմից:
- Ֆիզիկական ենթակառուցվածքների Կառավարում
- ՀԳԿ- ի կետերի պահպանումը
- ՀՀ օրենքների պահպանումը
- Ծառայության մակարդակի հաստատումը
- Աուդիտի, գրանցումների, համապատասխան փաստաթղթերի զննում
- Յուրաքանչյուր ձախողման պատճառի բացահայտում՝ վերը նշված պայմանները պահպանելու նպատակով

Եթե բացահայտվել են խախտումներ, ՀԾՄ-ը տրամադրում է աուդիտորին հաշվետվություն՝ ձեռնարկելու միջոցներ իրավիճակը շտկելու և համաձայնության գալու նպատակով: Անբավարար առաջարկված միջոցների դեպքում, երկրորդ աուդիտ կարող է կազմակերպվել՝ պահանջները ապահովելու նպատակով:

9 Այլ Կետեր և Օրինական Դրույթներ

9.1 Ծառայության Վճար

Ողջ անհրաժեշտ տեղեկատվությունը ներկայացված է ԷԿԵՆԳ կայքում:

9.2 Ֆինանսական Պատասխանատվություն

Չի կիրառվում

9.3 Բիզնես Տեղեկատվության Գաղտնիություն

ՀԾՄ-ը պահպանում է անձնական տվյալների և գաղտնիության կանոնները, ինչպես այն նկարագրված է սույն ՀԳԿ-ում: Գաղտնի տվյալները ներառում են՝

- Բացի հավաստագրի մեջ ներառված տվյալներից, այլ՝ անհատական տվյալներ քաղաքացիների մասին
- Հավաստագրի կասեցման կամ անվավերության ճշգրիտ պատճառը:
- Աուդիտի հետևանքները:
- Հաշվետվության նպատակով կատարված գրանցումներ, ինչպես օրինակ ԳՄ-ի կողմից հայցերի գրանցումները
- ՀԿ ծառայությունների նամակագրությունը
- ՀԿ-ի Փակ բանալի (բանալիներ).

Հետևյալը չի հանդիսանում որպես գաղտնի տեղեկություն՝

- Հավաստագրեր և դրանց պարունակությունը;
- Հավաստագրի կարգավիճակը.

ՀԾՄ-ը չի թողարկում և չի պահանջվում թողարկել գաղտնի տեղեկատվություն, որը չի հաստատվել և արդարացվել հետևյալ հայցերից որևէ մեկով՝

- Այն մարմնի կողմից, որի դեպքում ՀԿ-ն ունի պարտավորությունը պահպանելու տվյալ կողմի տվյալների գաղտնիությունը: ՀԿ-ն ունի նման պարտավորություն ԳՄ-ի հանդեպ և պատասխանում է անմիջապես նման հայցերին:
- Դատարանի կարգադրություն:

Հայաստանի Կառավարության հետ ՀԾՄ պայմանագրի շրջանակներում, ՀԾՄ-ը կարող է վարչական ծախսեր կատարել՝ նման բացահայտումներ անցկացնելու նպատակով: Այն կողմերը, որոնք պահանջում և ստանում են գաղտնի տեղեկություն, տնօրինում են այդ տվյալները այն պայմանով, որ պետք է օգտագործեն դրանք ըստ տվյալ նպատակի, պաշտպանեն տվյալները կեղծելուց, խուսափեն դրանք կիրառելուց կամ երրորդ անձանց այն տրամադրելուց: Նաև տվյալ անձիք պարտավորվում են դիտարկել անձի անհատական տվալների գաղտնիությունը օրենքի շրջանակներում:

9.4 Անձնական Տվյալների Գաղտնիություն

Բոլոր անհրաժեշտ տվյալները պետք է պաշտպանված լինեն՝ համաձայն Հայաստանի Հանրապետության օրենքի:

ՀԾՄ –ը, հավաստագրի կամ Գրանցվողի անձնական տվյալներից բացի, չի պահում այլ տվյալներ, քան այն, որոնք տրամադրվել են Գրանցվողին կամ թույլատրված են ՀՀ կողմից: ՀԾՄ-ը չի կարող կիրառել անձի տվյալները այլ նպատակների համար, եթե չունի հստակ համաձայնություն տվյալ անձի կամ օրենքի կողմից:

9.5 Մտավոր Սեփականության Իրավունք

Հայաստանի Հանրապետությունն ունի և իրեն է վերապահում մտավոր սեփականության իրավունքները, որն առնչվում է տվյալների բազային, վեբ կայքերին, ՀԿ թվային հավաստագրերին և այլ հրապարակումներին, որը բխում է ՀԿ-ից՝ ներառյալ սույն ՀԳԿ: Այս ՀԾՄ-ն ունի և իրեն է վերապահում մտավոր սեփականության՝ ենթակառուցվածքների, տվյալների բազայի, վեբ կայքերի որոշ կամ բոլոր իրավունքները:

9.6 Երաշխիք

Բոլոր կողմերը՝ ներառյալ ՀԿ-ը, ԳՄ-ը, ՏԳՄ-ները և Գրանցվողները երաշխավորում են իրենց փակ բանալիների ամբողջականությունը:
Գրանցվողի պարտականություններ:

Չնայած սույն ՀԳԿ-ում նշվածի, Գրանցվողի պարտականությունները ներառում են ներքևում նշվածը՝

- Խուսափել կեղծելուց հավաստագիրը :
- Կիրառել հավաստագրերը միայն օրինական կամ թույլատրլի նպատակների համար՝ համաձայն ՀԳԿ-ի:
- Հայտ ներկայացնել նոր Էլեկտրոնային Նույնականացման Քարտի համար (հետևաբար Գրանցվողի Հավաստագրեր) ՝ հավաստագրում տվյալների փոփոխություն դեպքում:
- Օգտագործել հավաստագիրը՝ ըստ պատեհ հանգամանքների
- Կանխարգելել փակ բանալու կորզումը, կորուստը, տվյալների բացահայտումը, փոփոխումը կամ ոչ թույլատրելի կիրառությունը :
- Դիմել հավաստագրի կասեցման համար՝ հավաստագրի տվյալների ամբողջությունը կասկածելու դեպքում : Այս դեպքերը ներառում են ցուցմունքներ՝ կորստի, գողության, տվյալների փոփոխության, չթույլատրված տվյալների բացահայտման կամ Գրանցվողի հավաստագրերի փակ կամ զույգ բանալիների կեղծման վերաբերյալ:
- Դիմել հավաստագրի կասեցման համար՝ հավաստագրի տվյալների ամբողջությունը կասկածելու դեպքում : Այս դեպքերն են՝ կորուստ, գողություն, տվյալների փոփոխություն, չթույլատրված տվյալների բացահայտում կամ Քաղաքացու հավաստագրերի փակ կամ զույգ բանալիների վնաս կամ տվյալների (օրինակ ՝ PIN կոդ) ակտիվացման ժամանակ փակ բանալու կորզում:
- Օգտագործել զույգ բանալիները՝ էլեկտրոնային ստորագրության համար և Գրանցվողի դեպքում նշված սահմանափակումները հաշվի առնելով:
- Պահել Փակ բանալին խնամքով՝ վերջինիս անցանկալի կիրառումից խուսափելու նպատակով :

- Տվյալների կեղծման դեպքում, պարտավորվել անմիջապես դադարեցնել փակ բանալու կիրառությունը.

Վստահելի Կողմերի Պարտավորությունները:

Վստահելի կողմը, որն ընդունում է ՀԿ-ի հավաստագիրը պետք է՝

- Բավականաչափ տեղեկացված լինի ՀԲԵ-ի թվային հավաստագրերի մասին:
- Ստանա հաղորդագրություն և ընդունի ՀԳԿ-ի և վստահելի կողմերի պայմանները:
- Վավերացնի հավաստագիրը՝ օգտագործելով ԱՀՑ կամ OCSP հավաստագրման ուղու վավերացման ընթացակարգը
- Վստահի հավաստագիրը իր վավերականության ժամանակահատվածում, եթե այն չի կասեցվել կամ ճանաչվել անվավեր:
- Վստահել հավաստագիրը՝ ըստ պատեհ հանգամանքների:

ՀԾՄ-ի (ԷԿԵՆԳ ՓԲԸ) պարտականությունները

ՀԾՄ պարտավոր է կատարել հետևյալը:

- Գործել համաձայն սույն ՀԳԿ-ի և դրա փոփոխությունների, ինչպես հրապարակված է ասյտեղ՝ հղում. http://www.ekeng.am/?page_id=74
- Տրամադրել ենթակառուցվածքի և հավաստագրման ծառայություններ. ներառյալ ՀԿ Պահոցի հիմնադրումը և գործունեությունը, ինչպես նաև կայքը հանրային հավաստագրման ծառայությունների գործունեության համար:
- Տրամադրել Հավաստագրման մեխանիզմներ, ներառյալ բանալու գեներացման մեխանիզմը, բանալու անվտանգությունը և տվյալների գաղտնիությունը բաժանելու ընթացակարգերը, որը վերաբերում է իր ենթակառուցվածքին :
- Թողակել էլեկտրոնային հավաստագրեր՝ համաձայն սույն ՀԳԿ-ի և ստանձնել այստեղ նշված պարտավորությունները:
- Տեղեկացնել Գրանցման Մարմնին, եթե ՀԿ-ը ընդունակ չէ վավերացնել հայտը համաձայն սույն ՀԳԿ-ի:
- ԳՄ-ի վավերացված հայտի դեպքում՝ անմիջապես գործել՝ թողարկելու հավաստագիրը համաձայն սույն ՀԳԿ-ի:
- ԳՄ-ի կողմից հավաստագիրը անվավեր ճանաչելու հայտի դեպքում՝ անմիջապես ջնջել հավաստագիրը համաձայն սույն ՀԳԿ-ի:
- ԳՄ-ի կողմից հավաստագիրը կասեցնելու հայտի դեպքում՝ անմիջապես կասեցնել հավաստագիրը համաձայն սույն ՀԳԿ-ի:
- ԳՄ-ի կողմից հավաստագիրը ապակասեցնուլու հայցի դեպքում՝ անմիջապես ապակասեցնել հավաստագիրը համաձայն սույն ՀԳԿ-ի:
- Հրապարակել հավաստագրերը համաձայն սույն ՀԳԿ-ի:
- Հրապարակել ԱՀՑ-ները և OCSP պատասխանները համաձայն սույն ՀԳԿ-ի:
- Գործել համաձայն Հունվարի 15-ի ՀՀ օրենքի “Էլեկտրոնային Փաստաթղթի և Էլեկտրոնային Ստորագրության” վերաբերյալ, , 2005թ-ի 1999/93 Էլեկտրոնային ստորագրությունների վերաբերյալ Եվրոպական Կարգադրության դրույթների:
- ՀԾՄ-ը պատասխանատվություն է կրում Գրանցվողների և Վստահելի Կողմերի հանդեպ հետևյալ ակտերի կամ բացթողումների դեպքում՝

Թողարկել թվային հավաստագրեր, որոնք չեն ցուցակագրում ԳՄ – ի կողմից տրամադրվող տվյալները:

- o Եթե ՀԿ-ի փակ բանալին կեղծվել է;
- o Կասեցված հավաստագիրը 7 օր հետո անվավեր ճանաչելու գործողությունը ձախողվել է:
- o Կասեցված կամ անվավեր հավաստագիրը ԱՀՑ-ում ընդգրկելու գործողությունը ձախողվել է:
- Գաղտնի կամ անձնական տվյալների անթույլատրելի բացահայտում:

Գրանցման Մարմնի պարտավորություններ

ԳՄ-ի գործունեությունը ՀԿ-ի ոլորտում ներառում է հետևյալը՝

- Տրամադրել ճշգրիտ տեղեկություն ՀԿ-ի հետ հաղորդակցման ընթացքում:
- Ապահովել, որպեսզի ՀԿ-ին տրամադրված հանրային բանալին համապատասխանի կիրառվող փակ բանալուն:
- Ստեղծել հավաստագրի հայտեր համաձայն սույն ՀԳԿ-ի:
- Կատարել ողջ ստուգումը և վավերացման գործողությունները՝ համաձայն ՀԿ և ՀԳԿ ընթացակարգերի:
- Իրականացնել ՀԿ-ի ընթացակարգերի և ՀԳԿ-ով նախատեսված բոլոր գործողությունների վերահսկողությունը:
- Տրամադրել ՀԿ-ին հայտատուի ստորագրված հայտը:
- Ստանալ, ստուգել և փոխանցել ՀԿ-ին հավաստագրերի անվավերության, կասեցման և ապակասեցման բոլոր հայտերը՝ համաձայն ՀԿ և ՀԳԿ ընթացակարգերի:
- Ստուգել հավաստագրի թարմացման ժամանակ քաղաքացու կողմից տրամադրված տվյալների ճշտությունը և վավերությունը :

ԳՄ-ը, և ոչ թե ՀԿ-ը, պատասխանատու է յուրաքանչյուր վնասի համար, որը տեղի է ունեցել հավաստագրում ոչ ճշտված տվյալներ մուտքագրելու արդյունքում:

9.7 Երաշխիքային Պարտավորության Հրաժարում

ՀԾՄ-ի երաշխիքները հիմնված են ընդհանուր՝ սույն Հավաստագրման Գործունեության Կանոնակարգի կանոնների վրա և գործում են համաձայն ՀՀ օրենսդրական ակտերի:

9.8 Պատասխանատվության Սահմանափակում

Չի կիրառվում:

9.9 Վնասների Փոխհատուցում

Չի կիրառվում:

9.10 Ժամկետ և Ավարտ

Այս կանոնակարգը մնում է ուժի մեջ մինչև իր անվավեր ճանաչվելը և ՀԿ-ի կողմից դրա վերաբերյալ իր Պահոցում պաշտոնական հրապարակումը, տես հղում. http://www.ekeng.am/?page_id=74

Բոլոր փոփոխությունները համապատասխան ձևով կսահմանվեն փաստաթղթային տարբերակում:

9.11 Անհատական Ծանուցումներ և Կապ

ՀԳԿ-ի մասին ծանուցումները կարող են հասցեագրվել ԷԿԵՆԳ ընկերություն՝ հետևյալ հասցեով.
Էկետրոնային Կառավարման Ենթակառուցվածքների Ներդրման Գրասենյակ ՓԲԸ
Հասցե: հանրապետության Հրապարակ, Կառավարական Տուն 1, 0010 Երևան, ՀՀ
Հեռ: *+ 374 10 512 882*; **Էլ-փոստ: cs**support@ekeng.am