ՀԱՍՏԱՏՎԱԾ Է

Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի   
2018 թվականի հուլիսի 9-ի   
թիվ 110 որոշմամբ

**ՀԻՄՆԱԴՐՈՒՅԹ**

Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնի մասին

I. Ընդհանուր դրույթներ

1. Սույն հիմնադրույթով սահմանվում է Եվրասիական տնտեսական հանձնաժողովի (այսուհետ՝ Հանձնաժողով) հավաստագրման կենտրոնի նշանակությունը, հիմնական խնդիրները եւ գործառույթները, ինչպես նաեւ դրա իրավունքները, պարտականությունները, պատասխանատվությունը եւ գործունեության դադարեցման կարգը։

2. Հանձնաժողովի հավաստագրման կենտրոնի հիմնական նշանակությունն է Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների էլեկտրոնային թվային ստորագրության ստուգման բանալիների սերտիֆիկատների ստեղծումը՝ վերջիններիս կողմից էլեկտրոնային փաստաթղթերի (այդ թվում՝ Հանձնաժողովի տեղային հաշվողական ցանցի սահմաններում կապի էլեկտրոնային ուղիներով փոխանցվող սահմանափակ տարածման փաստաթղթերի) ստորագրման հնարավորությունն ապահովելու համար։

3. Սույն հիմնադրույթում օգտագործվող հասկացությունները ունեն հետեւյալ նշանակությունը.

**գաղտնագրային ստանդարտ**՝ գաղտնագրային բանալու օգտագործմամբ տեղեկատվության վերափոխման (գաղտնագրային վերափոխում), այդ թվում՝ էլեկտրոնային թվային ստորագրության ձեւավորման եւ ստուգման կանոններ եւ ալգորիթմներ սահմանող տեխնիկական մասնագրերի ամբողջություն.

**ԷԹՍ ստուգման բանալու սերտիֆիկատ**՝ հավաստագրման կենտրոնի կողմից հրատարակված՝ ԷԹՍ բանալու օգտագործմամբ հավաստագրման կենտրոնի էլեկտրոնային թվային ստորագրությամբ ստորագրված եւ էլեկտրոնային փոխգործակցության կոնկրետ սուբյեկտին սերտիֆիկատում նշված՝ ԷԹՍ ստուգման բանալու պատկանելիությունը հաստատող տեղեկատվություն եւ համապատասխան գաղտնագրային ստանդարտներով եւ վստահության անդրսահմանային տարածության ստեղծմանը, զարգացմանը եւ աշխատանքին ներկայացվող պահանջներով նախատեսված այլ տեղեկատվություն պարունակող էլեկտրոնային փաստաթուղթ.

**հավաստագրման կենտրոն**՝ ԷԹՍ ստուգման բանալիների սերտիֆիկատների հրատարակման, տարածման, պահման եւ այդ սերտիֆիկատների վավերականության ստուգման մասով ծառայությունների տրամադրումը Հանձնաժողովի ակտերին, Եվրասիական տնտեսական միության անդամ պետության օրենսդրությանը համապատասխան ապահովող լիազորված մարմնին կամ կազմակերպությանը.

**Հանձնաժողովի հավաստագրման կենտրոն**՝ Հանձնաժողովի կոլեգիայի անդամներին, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցներին ԷԹՍ ստուգման բանալիների սերտիֆիկատներով ապահովելու համար նախատեսված հավաստագրման կենտրոն.

**էլեկտրոնային թվային ստորագրություն**՝ էլեկտրոնային տեսքով տեղեկատվություն, որը միացված է էլեկտրոնային տեսքով այլ տեղեկատվության կամ այլ կերպ կապված է այդպիսի տեղեկատվության հետ, ծառայում է այդ տեղեկատվության ամբողջականության եւ իսկության հսկողության համար, ապահովում է հեղինակությունից հրաժարվելու անհնարինությունը, մշակվում է փակ (անձնական) բանալու (ԷԹՍ բանալու) օգտագործմամբ տվյալ տեղեկատվության նկատմամբ գաղտնագրային վերափոխման կիրառման միջոցով եւ ստուգվում է բաց բանալու (ԷԹՍ ստուգման բանալու) օգտագործմամբ։

Սույն հիմնադրույթում օգտագործվող մյուս հասկացությունները կիրառվում են Տեղեկատվական-հաղորդակցական տեխնոլոգիաների եւ Եվրասիական տնտեսական միության շրջանակներում տեղեկատվական փոխգործակցության մասին արձանագրությամբ (Եվրասիական տնտեսական միության մասին 2014 թվականի մայիսի 29-ի պայմանագրի 3-րդ հավելված) սահմանված իմաստներով եւ Հանձնաժողովի խորհրդի կողմից հաստատվող՝ Վստահության անդրսահմանային տարածության ստեղծմանը, զարգացմանը եւ աշխատանքին ներկայացվող պահանջներում։

4. Էլեկտրոնային փաստաթղթերի ձեւակերպմանը ներկայացվող պահանջները սահմանվում են Հանձնաժողովի խորհրդի կողմից հաստատվող՝ Վստահության անդրսահմանային տարածության ստեղծմանը, զարգացմանը եւ աշխատանքին ներկայացվող պահանջներում եւ Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2015 թվականի սեպտեմբերի 28-ի թիվ 12 որոշմամբ հաստատված՝ Եվրասիական տնտեսական հանձնաժողովի անդամ պետությունների պետական իշխանության մարմինների՝ միմյանց միջեւ եւ Եվրասիական տնտեսական հանձնաժողովի հետ անդրսահմանային փոխգործակցության ժամանակ էլեկտրոնային փաստաթղթերի փոխանակման մասին հիմնադրույթում։

5. Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների էլեկտրոնային թվային ստորագրությունը (այսուհետ՝ ԷԹՍ) ճանաչվում է վավեր հետեւյալ պայմանների միաժամանակյա պահպանման դեպքում՝

ա) ԷԹՍ ստուգման բանալու սերտիֆիկատը ստեղծվել եւ տրվել է Հանձնաժողովի հավաստագրման կենտրոնի կողմից.

բ) ԷԹՍ-ով ստորագրած տվյալների ամբողջականությունը չի խախտվել.

գ) ԷԹՍ-ն մշակվել է փակ (անձնական) բանալու օգտագործմամբ, որի բաց բանալու համապատասխան սերտիֆիկատը (ԷԹՍ ստուգման բանալու սերտիֆիկատ) նշված է այդ ԷԹՍ-ի կազմում.

դ) ԷԹՍ ստուգման բանալու սերտիֆիկատը վավեր է էլեկտրոնային փաստաթղթի ստորագրման պահի դրությամբ.

ե) Հանձնաժողովի հավաստագրման կենտրոնի սերտիֆիկատը վավեր է էլեկտրոնային փաստաթղթի ստորագրման պահի դրությամբ։

II. Հանձնաժողովի հավաստագրման կենտրոնի   
խնդիրները եւ գործառույթները

6. Հանձնաժողովի հավաստագրման կենտրոնի հիմնական խնդիրներն են.

ա) ԷԹՍ ստուգման բաց բանալու՝ փակ (անձնական) բանալուն համապատասխանության հաստատումը, ինչպես նաեւ Հանձնաժողովի կոլեգիայի անդամի, Հանձնաժողովի պաշտոնատար անձի կամ աշխատակցի ԷԹՍ ստուգման բանալու սերտիֆիկատի իսկության հաստատումը.

բ) էլեկտրոնային փաստաթղթերի միջազգային (անդրսահմանային) փոխանակման ժամանակ Հանձնաժողովի կոլեգիայի, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների ԷԹՍ ստուգման բանալիների սերտիֆիկատների նկատմամբ վստահության երաշխիքների ապահովումը.

գ) Հանձնաժողովի կոլեգիայի, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների ԷԹՍ ստուգման բանալիների սերտիֆիկատների հրատարակումը, տարածումը, պահումը եւ այդ սերտիֆիկատների վավերականության ստուգումը.

դ) Հանձնաժողովի կոլեգիայի, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների ԷԹՍ ստուգման բանալիների սերտիֆիկատներում նշված տեղեկությունների հավաստիության հաստատումը։

7. Հանձնաժողովի հավաստագրման կենտրոնի կողմից Միության իրավունքին համապատասխան իրականացվում են հետեւյալ գործառույթները՝

ա) Հանձնաժողովի կողմից հաստատվող պահանջներին համապատասխանող՝ ԷԹՍ ստուգման բանալիների սերտիֆիկատների ստեղծումը եւ տրամադրումը Հանձնաժողովի կոլեգիայի անդամներին, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցներին.

բ) ԷԹՍ ստուգման բանալիների սերտիֆիկատներ տրամադրելիս Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների՝ անձի ստուգման ապահովումը.

գ) տեղեկատվության ընդհանուր հասանելիության ռեժիմում «Ինտերնետ» տեղեկատվական-հեռահաղորդակցական ցանցում Հանձնաժողովի հավաստագրման կենտրոնի ծառայություններից օգտվելու պայմանների մասին տեղեկատվության, ներառյալ՝ դրանց օգտագործման մասով սահմանափակումների մասին տեղեկատվության հրապարակումը.

դ) էլեկտրոնային փոխգործակցության բոլոր սուբյեկտներին Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների ԷԹՍ ստուգման բանալիների բոլոր տրված սերտիֆիկատների կարգավիճակի (արդիականության) մասին տեղեկատվության ժամանակին տրամադրումը։ Այդպիսի տեղեկատվությունը պետք է հասանելի լինի ցանկացած ժամանակ, այդ թվում նաեւ Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների ԷԹՍ ստուգման բանալու սերտիֆիկատի գործողությունը դադարեցնելուց հետո եւ տրամադրվի ավտոմատացված եղանակով.

ե) Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների ԷԹՍ ստուգման բանալիների սերտիֆիկատների ռեեստրում եւ Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների ԷԹՍ ստուգման բանալիների հետ կանչված սերտիֆիկատների ցանկում տեղեկատվություն մուտքագրելը։ Հանձնաժողովի կոլեգիայի անդամի, Հանձնաժողովի պաշտոնատար անձի եւ աշխատակցի ԷԹՍ ստուգման բանալու սերտիֆիկատը համարվում է հետ կանչված այդպիսի սերտիֆիկատի համապատասխան կարգավիճակի (արդիականության) մասին տեղեկատվություն պարունակող եւ էլեկտրոնային փոխգործակցության սուբյեկտներին ցանկացած ժամանակ հասանելի հետ կանչված սերտիֆիկատների ցանկի հրապարակման պահից.

զ) Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների (այդ թվում՝ Հանձնաժողովի կոլեգիայի անդամներին, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցներին ԷԹՍ ստուգման բանալիների սերտիֆիկատներով ապահովելու գործունեությունը դադարեցնելուց հետո) ԷԹՍ ստուգման բանալիների սերտիֆիկատների կարգավիճակների (արդիականության) տրման, ստացման եւ փոփոխման մասին տեղեկատվության փաստաթղթավորումը եւ պահպանումը՝ թողարկված ԷԹՍ ստուգման բանալիների սերտիֆիկատների կիրառման հետ կապված կոնֆլիկտային իրավիճակները վերլուծելիս ապացույցների ներկայացման համար։ Նշված տեղեկատվության պահումը կարող է իրականացվել էլեկտրոնային տեսքով.

է) Հանձնաժողովի հավաստագրման կենտրոնի կողմից ստեղծված եւ պահվող գաղտնագրային բանալիների գաղտնիության, ամբողջականության ապահովումը.

ը) Եվրասիական տնտեսական միության անդամ պետությունների լիազորված մարմիններին, Հանձնաժողովի կոլեգիայի անդամներին, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցներին ԷԹՍ ստուգման բանալիների սերտիֆիկատներով ապահովելու գործունեությունը դադարեցնելու մտադրության կամ գործունեության դադարեցման այլ դեպքերի մասին տեղեկացնելը։

8. Հանձնաժողովի հավաստագրման կենտրոնի ստեղծման, զարգացման եւ աշխատանքի մասով աշխատանքների կազմակերպումն իրականացնում է Հանձնաժողովի կառուցվածքային ստորաբաժանումը, որի ղեկավարման ոլորտին են դասվել տվյալ հարցերը։ Հանձնաժողովի հավաստագրման կենտրոնի աշխատանքն իրականացվում է կանոնակարգին համապատասխան՝ համաձայն հավելվածի։

III. Հանձնաժողովի հավաստագրման կենտրոնի իրավունքները, պարտականությունը եւ պատասխանատվությունը

9. Իր գործառույթները կատարելու համար Հանձնաժողովի հավաստագրման կենտրոնն իրավասու է՝

ա) անցկացնել ԷԹՍ ստուգման բանալիների սերտիֆիկատներ ստանալու նպատակով Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների կողմից ներկայացվող տեղեկությունների ստուգում.

բ) մերժել Հանձնաժողովի կոլեգիայի անդամներին, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցներին ԷԹՍ ստուգման բանալիների սերտիֆիկատների ստացման մեջ վերջիններիս կողմից ԷԹՍ ստուգման բանալիների սերտիֆիկատների ստացման համար ոչ հավաստի տեղեկություններ կամ ոչ լրիվ ծավալով տեղեկություններ ներկայացնելու դեպքում.

գ) կասեցնել կամ չեղարկել ԷԹՍ ստուգման բանալիների թողարկված սերտիֆիկատների գործողությունն այնպիսի տեղեկություններ հրապարակելու դեպքում, որոնք էական կերպով կարող են անդրադառնալ ԷԹՍ ստուգման բանալիների սերտիֆիկատների հետագա օգտագործման, դրանց իրավաբանական ուժը կորցնելու, ԷԹՍ համապատասխան միջոցները կորցնելու, այն փաստաթղթերի գործողության դադարեցման հնարավորության վրա, որոնց հիման վրա ձեւակերպվել են ԷԹՍ ստուգման բանալիների սերտիֆիկատները, եւ Միության մարմինների ակտերով սահմանված այլ դեպքերում.

դ) կազմակերպել, ապահովել եւ վերահսկել Հանձնաժողովի հավաստագրման կենտրոնի միջոցները շահագործելիս Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների կողմից տեղեկատվական անվտանգության պահանջների կատարումը.

ե) մասնակցել Հանձնաժողովի հավաստագրման կենտրոնի հարցերը կանոնակարգող փաստաթղթերի մշակմանը եւ համաձայնեցմանը.

զ) սահմանել Հանձնաժողովի հավաստագրման կենտրոնի ԷԹՍ ստուգման բանալու արմատային սերտիֆիկատի եւ Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների ԷԹՍ ստուգման բանալիների սերտիֆիկատների գործողության ժամկետը։

10. Իր գործառույթները կատարելիս Հանձնաժողովի հավաստագրման կենտրոնը պարտավոր է՝

ա) ապահովել Հանձնաժողովի հավաստագրման կենտրոնում Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների գրանցման կարգը եւ ժամկետները՝ վերջիններիս կողմից ներկայացված փաստաթղթերի հիման վրա՝ դրանցում նշված տեղեկությունների պարտադիր ստուգմամբ.

բ) գրավոր ձեւով տեղեկացնել Հանձնաժողովի կոլեգիայի անդամներին, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցներին ԷԹՍ եւ ԷԹՍ միջոցների օգտագործման պայմանների եւ կարգի մասին, ԷԹՍ-ի օգտագործման հետ կապված ռիսկերի մասին եւ ԷԹՍ-ի անվտանգության եւ դրա ստուգման ապահովման համար անհրաժեշտ միջոցների մասին.

գ) Հանձնաժողովի կոլեգիայի անդամներին, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցներին ծանոթացնել Հանձնաժողովի հավաստագրման կենտրոնի աշխատակարգի հետ.

դ) արդիականացնել Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների ԷԹՍ ստուգման բանալիների սերտիֆիկատների ռեեստրում առկա տեղեկատվությունը եւ ապահովել դրա պաշտպանությունը ոչ իրավաչափ մուտքից, ոչնչացումից, ձեւափոխումից, արգելափակումից եւ այլ ոչ իրավաչափ գործողություններից.

ե) ներկայացնել ցանկացած անձի վերջինիս դիմումի համաձայն Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների ԷԹՍ ստուգման բանալիների սերտիֆիկատների ռեեստրում առկա տեղեկատվություն, այդ թվում՝ Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների ԷԹՍ ստուգման բանալիների սերտիֆիկատների չեղարկման մասին տեղեկատվություն.

զ) ապահովել Հանձնաժողովի հավաստագրման կենտրոնի կողմից ստեղծված ԷԹՍ բանալիների գաղտնիությունը.

է) ապահովել ԷԹՍ ստուգման բանալիների սերտիֆիկատների կարգավիճակի թողարկման, ստուգման, գործողության կասեցման, վերականգնման եւ չեղարկման, ԷԹՍ ստուգման բանալիների չեղարկված բանալիների մասին տեղեկատվության հրապարակման տեխնիկական ընթացակարգերի լրիվ ծավալով կատարումը.

ը) մասնակցել որպես երրորդ կողմ Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների ԷԹՍ ստուգման բանալիների սերտիֆիկատների կիրառման հետ կապված կոնֆլիկտային իրավիճակները լուծելիս.

թ) ապահովել առնվազն 15 տարվա ընթացքում Հանձնաժողովի հավաստագրման կենտրոնի կողմից ստեղծված ԷԹՍ ստուգման բանալիների սերտիֆիկատների, թղթային կրիչներով այն փաստաթղթերի պահումը, որոնց հիման վրա թողարկվել են ԷԹՍ ստուգման բանալիների սերտիֆիկատները, եւ Հանձնաժողովի հավաստագրման կենտրոնի այլ փաստաթղթերի պահումը՝ Հանձնաժողովում սահմանված՝ պահոցային պահման լրացած ժամկետով փաստաթղթերի ոչնչացման կարգի պահպանմամբ.

ժ) պահպանել առնվազն 15 տարվա ընթացքում Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների անձը հաստատող հիմնական փաստաթղթերի վավերապայմանները.

ժա) չեղարկել Հանձնաժողովի հավաստագրման կենտրոնի ԷԹՍ ստուգման բանալու սերտիֆիկատը տվյալ սերտիֆիկատին համապատասխանող ԷԹՍ բանալու կոմպրոմետացիայի դեպքում։

11. Հանձնաժողովի հավաստագրման կենտրոնը, Միության մարմինների ակտերին համապատասխան, պատասխանատվություն է կրում երրորդ անձանց վնաս պատճառելու դեպքում.

ա) սույն հիմնադրույթով, ինչպես նաեւ ԷԹՍ կիրառման կարգավորման ոլորտում Միության մարմինների ակտերով նախատեսված պարտականությունների չկատարման կամ ոչ պատշաճ կատարման արդյունքում.

բ) ԷԹՍ միջոցները եւ Հանձնաժողովի հավաստագրման կենտրոնի միջոցները օգտագործելիս աշխատանքների եւ տեղեկատվության անվտանգության հսկողության ոչ պատշաճ կազմակերպման արդյունքում.

գ) Հանձնաժողովի հավաստագրման կենտրոնի միջոցներից օգտվելու կանոնների չպահպանման արդյունքում։

V. Հանձնաժողովի հավաստագրման կենտրոնի   
գործունեության դադարեցումը

12. Հանձնաժողովի հավաստագրման կենտրոնի գործունեությունը դադարում է Հանձնաժողովի կոլեգիայի որոշմամբ Հանձնաժողովի հավաստագրման կենտրոնի գործառույթներն այլ հավաստագրման կենտրոնի փոխանցելու կամ Հանձնաժողովի հավաստագրման կենտրոնի տեղեկատվական համակարգերի լիկվիդացման հետ կապված։

13. Հանձնաժողովի հավաստագրման կենտրոնը վերջինիս գործունեության դադարեցման մասին որոշում ընդունելու դեպքում տեղեկացնում է դրա մասին Հանձնաժողովի կոլեգիայի անդամներին, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցներին գործունեությունը դադարեցնելուց 1 ամիս առաջ։

14. Հանձնաժողովի հավաստագրման կենտրոնի գործառույթներն այլ հավաստագրման կենտրոնի փոխանցելու դեպքում փոխանցվում է Հանձնաժողովի հավաստագրման կենտրոնի գործունեության դադարեցման օրվա դրությամբ թողարկված Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների ԷԹՍ ստուգման բանալիների սերտիֆիկատների ռեեստրը։

15. Հանձնաժողովի հավաստագրման կենտրոնի տեղեկատվական համակարգերի լիկվիդացման դեպքում Հանձնաժողովի կոլեգիայի անդամներին, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցներին ԷԹՍ ստուգման բանալիների սերտիֆիկատների ռեեստրը եւ Հանձնաժողովի հավաստագրման կենտրոնի այլ էլեկտրոնային եւ թղթային փաստաթղթեր փոխանցվում են պահոցային պահման՝ Հանձնաժողովում սահմանված կարգով։

ՀԱՎԵԼՎԱԾ

Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնի մասին հիմնադրույթի

**ԿԱՆՈՆԱԿԱՐԳ**

Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնի

1. Ներածություն

1.1 Ընդհանուր դրույթներ

Սույն փաստաթղթով սահմանվում են՝

ա) Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնի (այսուհետ՝ Հանձնաժողովի ՀԿ) կողմից թողարկված՝ ԷԹՍ ստուգման բանալիների սերտիֆիկատների (այսուհետ՝ սերտիֆիկատներ) կիրառման կանոնները, ներառյալ՝ սերտիֆիկատներ տիրապետողների պարտականությունները.

բ) Հանձնաժողովի ՀԿ-ի ծառայությունների աշխատակարգը.

գ) տվյալների ընդունված ձեւաչափերը եւ փոխգործակցության արձանագրությունները.

դ) Հանձնաժողովի ՀԿ-ի անվտանգ աշխատանքի համար անհրաժեշտ հիմնական կազմակերպատեխնիկական միջոցառումները։

Տվյալ փաստաթուղթը կազմված է RFC 3647 «Internet Х.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework» առաջարկությանը համապատասխան։ Փաստաթղթի կառուցվածքը, բաժինների եւ ենթաբաժինների համարակալումը համապատասխանում են RFC 3647 առաջարկությանը. որոշ ենթաբաժիններ բաղկացած են միայն «Պայմաններ չկան» արտահայտությունից, ինչը նշանակում է, որ Հանձնաժողովի ՀԿ-ի համար չեն մտցվում պայմաններ տվյալ ենթաբաժնի համար։

1.2. Կանոնակարգի վավերապայմանները

Փաստաթղթի լրիվ անվանումը՝ Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնի կանոնակարգ։

Փաստաթղթի կրճատ անվանումը՝ Հանձնաժողովի ՀԿ-ի կանոնակարգ։

Փաստաթղթի օբյեկտային նույնականացուցիչը՝ 1.2.643.3.294.1.1

Ընթացիկ տարբերակը՝ 1.0

Հրատարակման ամսաթիվը՝

1.3. Բաց բանալիների ենթակառուցվածքի մասնակիցները

Հանձնաժողովի ՀԿ-ի բաց բանալիների ենթակառուցվածքն իր մեջ ներառում է՝ Հանձնաժողովի ՀԿ-ն, սերտիֆիկատներ տիրապետողներին եւ սերտիֆիկատներից օգտվողներին։

Հավաստագրման կենտրոնի կազմում մտնում են՝

Սերտիֆիկացման կենտրոնը (այսուհետ՝ ՍԿ).

Գրանցման կենտրոնը (այսուհետ՝ ԳԿ).

Հրապարակման ծառայությունը (այսուհետ՝ ՀԾ).

Տեղեկացման ծառայությունը (այսուհետ՝ ՏԾ).

WEB-ծառայությունները՝

ա) հետ կանչված սերտիֆիկատների ցանկերի տարածման կետերը (այսուհետ՝ CDP).

բ) իրական ժամանակի ռեժիմում սերտիֆիկատների կարգավիճակների ստուգման ծառայությունը (այսուհետ՝ OCSP-ծառայություն).

գ) ժամանակի դրոշմավորման ծառայությունը (այսուհետ՝ TSP-ծառայություն)։

1.3.1. Սերտիֆիկացման կենտրոն

ՍԿ-ն նախատեսված է սերտիֆիկատների, չեղարկված (հետ կանչված) սերտիֆիկատների ցանկերի (ՀՍՑ) թողարկման, սերտիֆիկատների եւ ՀՍՑ-ի էտալոնային շտեմարանի պահման համար։

ՍԿ-ն փոխգործակցում է միայն ԳԿ-ի հետ տեղային ցանցի առանձին հատվածի մասով SOK ձեւաչափի ֆայլերի փոխանակման համար ViPNet Client կազմից ViPNet MFTP պաշտպանված ցանցային միացման օգտագործմամբ։

ՍԿ-ի վրա գտնվում է բոլոր պատրաստված սերտիֆիկատների շտեմարանը։

ՍԿ-ի գործառույթներին են դասվում հետեւյալ հիմնական գործառույթները՝

սերտիֆիկատների թողարկում.

ԷԹՍ ստուգման բանալիների եզակիության ստուգում.

սերտիֆիկատների ռեեստրի վարում.

ՀՍՑ հրատարակում.

թողարկված սերտիֆիկատների չեղարկում, գործողության կասեցում եւ վերականգնում։

1.3.2. Գրանցման կենտրոն

ԳԿ-ն նախատեսված է սերտիֆիկատներ տիրապետողների գրանցման տվյալների, սերտիֆիկատների հարցումների եւ սերտիֆիկատների պահման համար։

ԳԿ-ն փոխգործակցում է ՍԿ-ի հետ տեղային ցանցի առանձին հատվածի մասով SOK ձեւաչափի ֆայլերի փոխանցման տեսքով պաշտպանված ցանցային արձանագրության օգտագործմամբ։ ԳԿ-ն համակարգում սերտիֆիկատներ տիրապետողների մուտքի (գրանցման) միակ կետն է։ Միայն ԳԿ-ում գրանցված Հանձնաժողովի ՀԿ-ի օգտվողները կարող են ստանալ Հանձնաժողովի ՀԿ-ի սերտիֆիկատ։

ԳԿ-ի գործառույթներին են դասվում հետեւյալ գործառույթները՝ սերտիֆիկատներ տիրապետողների ռեեստրի վարումը.

Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների համար ԷԹՍ բանալիների եւ ԷԹՍ ստուգման բանալիների ստեղծումը.

ՍԿ-ում սերտիֆիկատների հրատարակման, չեղարկման, գործողության կասեցման եւ վերականգնման հարցումների ստեղծումը։

1.3.3. Հրապարակման ծառայություն

ՀԾ-ն նախատեսված է Հանձնաժողովի ՀԿ-ի ռեպոզիտարիայում Հանձնաժողովի ՀԿ-ի տեղեկատվության հրապարակման համար։

ՀԾ-ն փոխգործակցում է ՍԿ-ի հետ տեղային ցանկի առանձին հատվածի մասով՝ պաշտպանված ցանցային արձանագրության օգտագործմամբ։

ՀԾ-ի գործառույթներին դասվում են հետեւյալ գործառույթները՝

սերտիֆիկատների հրապարակում.

Հանձնաժողովի ՀԿ-ի լիազորված անձի սերտիֆիկատների հրապարակում.

ՀՍՑ-ի հրապարակում։

1.3.4. Տեղեկացման ծառայություն

ՏԾ-ն նախատեսված է Հանձնաժողովի ՀԿ-ի ադմինիստրատորներին եւ սերտիֆիկատներ տիրապետողներին տեղեկացնելու համար։

ՏԾ-ն փոխգործակցում է ՍԿ-ի տվյալների շտեմարանի հետ։ ՏԾ-ն ՍԿ-ի տվյալների շտեմարանի հարցման ժամանակ ստացված սերտիֆիկատների մասին տեղեկատվության հիման վրա ձեւավորում է էլեկտրոնային փոստով ուղարկելու (փոստային SMTP-սերվերի օգնությամբ) համար համապատասխան հաղորդումներ։ Փոստային հաղորդումները պահպանվում են ՍԿ-ի կոշտ սկավառակի վրա համապատասխան թղթապանակում եւ փոխանցվում են SMTP-սերվերով համակարգիչ՝ հանովի կրիչների օգնությամբ։

Տեղեկացման ծառայությունն ընձեռում է հետեւյալ հնարավորությունները՝

Հանձնաժողովի ՀԿ-ի ադմինիստրատորներին սերտիֆիկատների հետ կապված իրադարձությունների մասին ծանուցումների ուղարկում.

ա) սերտիֆիկատների գործողության ժամկետը լրանալու մասին.

բ) սերտիֆիկատի մասով հարցումների կարգավիճակի փոփոխության մասին.

գ) սերտիֆիկատների թողարկման, գործողության կասեցման, գործողության վերականգնման, հետկանչման մասով չմշակված հարցումների տրված քանակը գերազանցելու մասին.

սերտիֆիկատներ տիրապետողներին վերջիններիս սերտիֆիկատների գործողության ժամկետը լրանալու մասին ծանուցումներ ուղարկելը.

Հանձնաժողովի ՀԿ-ում թողարկված սերտիֆիկատների մասին հաշվետվությունների ձեւավորում։

1.3.5. WEB-պորտալ

WEB-պորտալը նախատեսված է ընդհանուր օգտագործման ցանցի օգնությամբ ՀԿ-ի ռեպոզիտարիային մուտք ապահովելու համար (ՀԿ-ի ռեպոզիտարիաների մասին մանրամասն տես 2-րդ բաժին):

Internet ընդհանուր օգտագործման ցանցում WEB-պորտալի URL-հասցեներ՝

<http://ca.eecommission.org>,

<https://ca.eecommission.org>

Կազմակերպատեխնիկական համալիր միջոցներով ապահովվում են WEB-պորտալի մատչելիության պահանջվող ցուցանիշները։

1.3.6. Իրական ժամանակի ռեժիմում սերտիֆիկատների կարգավիճակների ստուգման ծառայություն

OCSP-ծառայությունը նախատեսված է OCSP (Online Certificate Status Protocol) արձանագրության հիման վրա սերտիֆիկատների կարգավիճակի որոշման գործառույթների կատարման համար։

OCSP-ծառայությունն ապահովում է ԲԲԵ-ի կառուցման մասով միջազգային առաջարկությունների օգտագործումը՝ հաշվի առնելով ԳՕՍՏ 28147-89, ԳՕՍՏ Ռ 34.11-2012, ԳՕՍՏ Ռ 34.10-2012 կիրառումը.

RFC 2560 - "Internet Х.509 Public Key Infrastructure. Online Certificate Status Protocol - OCSP".

RFC 5280 - "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile"։

OCSP-ծառայության աշխատակարգը շարադրված է սույն կանոնակարգի թիվ 1 հավելվածում։

1.3.7. Ժամանակի դրոշմավորման ծառայություն

TSP-ծառայությունն ունի ժամանակի ճշգրիտ եւ հուսալի աղբյուր ու կատարում է ժամանակի դրոշմների ստեղծման գործառույթներ։ Ժամանակի դրոշմն ԷԹՍ-ով ստորագրված փաստաթուղթ է, որով TSP-ծառայությունը հավաստում է, որ ժամանակի տվյալ պահին իրեն տրամադրվել է այլ փաստաթղթից հեշ-ֆունկցիայի արժեք։ Ընդ որում, հեշ-ֆունկցիայի արժեքը նույնպես նշվում է ժամանակի դրոշմում։

TSP-ծառայությունն ապահովում է ԲԲԵ կառուցման մասով միջազգային առաջարկությունների օգտագործումը՝ հաշվի առնելով ԳՕՍՏ 28147-89, ԳՕՍՏ Ռ 34.11-2012, ԳՕՍՏ Ռ 34.10-2012 կիրառումը.

RFC 3161 - "Internet Х.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)"։

TSP-ծառայության աշխատակարգը շարադրված է սույն կանոնակարգի 1-ին հավելվածում։

1.3.8. Սերտիֆիկատ տիրապետողը

Սերտիֆիկատներ տիրապետողներն են՝

Հանձնաժողովի կոլեգիայի անդամները, Հանձնաժողովի պաշտոնատար անձինք եւ աշխատակիցները, որոնց սույն կանոնակարգով սահմանված կարգով տրվել է սերտիֆիկատ, եւ որոնք տիրապետում են տրված սերտիֆիկատի կազմում ներառված՝ ԷԹՍ ստուգման բանալուն համապատասխանող ԷԹՍ բանալին.

Հանձնաժողովի տեխնոլոգիական ծառայությունների աշխատանքն ապահովելու համար նախատեսված ԷԹՍ ստուգման բանալիների սերտիֆիկատների պահման եւ օգտագործման համար պատասխանատու նշանակված Հանձնաժողովի պաշտոնատար անձինք կամ աշխատակիցները։

1.3.9. Սերտիֆիկատից օգտվողը

Սերտիֆիկատից օգտվողը սույն կանոնակարգի համաձայն թողարկված սերտիֆիկատներ ընդունող եւ Հանձնաժողովի ՀԿ-ի լիազորված անձի սերտիֆիկատներին վստահելով գործող անձն է։

1.4. Սերտիֆիկատների օգտագործում

1.4.1. Թույլատրելի օգտագործում

Հանձնաժողովի ՀԿ-ն թողարկում է սերտիֆիկատների հետեւյալ տիպերը՝

Հանձնաժողովի ՀԿ-ի սերտիֆիկացման կենտրոնի ԷԹՍ ստուգման բանալիների սերտիֆիկատները.

OCSP-ծառայության ԷԹՍ ստուգման բանալիների սերտիֆիկատները.

TSP-ծառայության ԷԹՍ ստուգման բանալիների սերտիֆիկատները.

սերվերների աուտենտիֆիկացման սերտիֆիկատները.

Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների սերտիֆիկատները, որոնց Հանձնաժողովի ՀԿ-ի կանոնակարգով սահմանված կարգով տրվել է սերտիֆիկատ, եւ որոնք տիրապետում են տրված սերտիֆիկատի կազմում ներառված ԷԹՍ ստուգման բանալուն համապատասխանող ԷԹՍ բանալին.

Հանձնաժողովի երրորդ կողմին վստահված սերտիֆիկատները։

Սերտիֆիկատները կարող են օգտագործվել միայն այն սերտիֆիկատների կիրառման քաղաքականություններին համապատասխան, որոնց նույնականացուցիչները նշված են սերտիֆիկատներում։ Ընդ որում, սերտիֆիկատներում թույլատրվում է նշել սերտիֆիկատների կիրառման միայն այն քաղաքականությունների նույնականացուցիչները, որոնք համապատասխանում են սույն կանոնակարգին։

Սույն կանոնակարգին համապատասխանող սերտիֆիկատների կիրառման քաղաքականությունների օբյեկտային նույնականացուցիչները բերված են թիվ 2 հավելվածում։

1.4.2. Արգելված օգտագործում

Արգելվում է օգտագործել սերտիֆիկատ այն սերտիֆիկատների քաղաքականություններից եւ ոչ մեկում չնշված նպատակներով, որոնց նույնականացուցիչները նշված են սերտիֆիկատում։

1.5. Կանոնակարգով կառավարում

1.5.1. Հանձնաժողովի ՀԿ-ի վավերապայմանները

Հանձնաժողովի ՀԿ-ի հասցեն՝

119121, ք. Մոսկվա, Սմոլենսկի բուլվար, շենք 3/5, շինություն 1

Հեռախոսահամարը՝ +7 (495) 669-24-00

Ֆաքսը՝ 8 (495) 669-24-15

e-mail՝ info@eecommission.org

1.5.2. Կոնտակտային անձ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.5.3. Սույն կանոնակարգի համապատասխանությունը սերտիֆիկատների կիրառման քաղաքականություններին որոշող անձ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.5.4. Հանձնաժողովի ՀԿ-ի կանոնակարգի եւ սերտիֆիկատների կիրառման քաղաքականությունների հաստատման ընթացակարգ

Հանձնաժողովի ՀԿ-ի կանոնակարգի հաստատումն իրականացվում է Հանձնաժողովի ՀԿ-ի մասին դրույթի հաստատման հետ միաժամանակ։

Սերտիֆիկատների կիրառման քաղաքականությունների հաստատումն իրականացվում է Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի նախագահի հրամանով՝ Եվրասիական տնտեսական հանձնաժողովի Տեղեկատվական տեխնոլոգիաների դեպարտամենտի եւ Գործերի կառավարման դեպարտամենտի հետ համաձայնեցմամբ։

Շտկումները եւ (կամ) լրացումները հրապարակվում են Հանձնաժողովի ՀԿ-ի ռեպոզիտարիայում շտկումներ եւ (կամ) լրացումներ պարունակող փաստաթղթերի կամ փաստաթղթի շտկված եւ (կամ) լրացված նոր տարբերակների տեսքով։

1.6. Սահմանումներ եւ տառային հապավումներ

1.6.1. Սահմանումներ

Աուտենտիֆիկացումը տրամադրված տվյալների ու հատկանիշների եւ նախկինում ֆիքսված եզակի տվյալների ու հատկանիշների համեմատության միջոցով օգտվողի իսկության ստուգման ընթացակարգն է։

Սերտիֆիկատ տիրապետողը Հանձնաժողովի կոլեգիայի անդամն է, Հանձնաժողովի պաշտոնատար անձը կամ աշխատակիցը, որին սույն կանոնակարգով սահմանված կարգով տրված է տրված սերտիֆիկատի կազմում ներառված` ԷԹՍ ստուգման բանալուն համապատասխանող ԷԹՍ բանալին տիրապետողի սերտիֆիկատ։

Ակտիվացման տվյալները բանալու կրիչի կառավարման համար պահանջվող բանալիներից տարբերվող փակ տվյալներն են։

ԷԹՍ բանալին էլեկտրոնային թվային ստորագրության ստեղծման համար նախատեսված սիմվոլների եզակի հաջորդականությունն է։

Հայտատուն սերտիֆիկատի թողարկման հայտ ներկայացրած սուբյեկտն է։

Նույնականացումը սուբյեկտի՝ տարբերակիչ հատկանիշներին միանշանակ համապատասխանությունը սահմանող գործընթացն է։

Տեղեկատվությունն անձանց, առարկաների, փաստերի, իրադարձությունների եւ գործընթացների մասին տեղեկությունն է՝ անկախ դրանց ներկայացման ձեւից։

Բաց բանալիների ենթակառուցվածքը կամ (ԲԲԵ)-ն ճարտարապետությունը, կազմակերպումը, եղանակները եւ ընթացակարգերն են, որոնցով ապահովվում է սերտիֆիկատների վրա հիմնված գաղտնագրային համակարգի կառավարումը եւ կիրառումը։

Քաղաքականության որակավորիչը սերտիֆիկատների կիրառման քաղաքականությունից կախված տեղեկատվությունն է, որը կարող է ուղեկցել սերտիֆիկատների կիրառման քաղաքականության նույնականացուցիչը Х.509 սերտիֆիկատում։

Բանալու զույգը ԷԹՍ բանալին եւ դրան համապատասխանող ԷԹՍ ստուգման բանալին է։

Էլեկտրոնային թվային ստորագրության բանալու կոմպրոմետացիան ԷԹՍ բանալու հրապարակման հանգեցված՝ ֆիզիկական անձի գործողությունների արդյունքն է։

Հանձնաժողովի ՀԿ-ի ԳԿ-ի օպերատորը Հանձնաժողովի հավաստագրման կենտրոնի աշխատակից համարվող, սերտիֆիկատների թողարկման, գործողության կասեցման, գործողության վերականգնման, հետկանչման հայտերի քննարկմամբ եւ մշակմամբ զբաղվող ֆիզիկական անձն է։

Էլեկտրոնային թվային ստորագրության ստուգման բանալին էլեկտրոնային թվային ստորագրության բանալու հետ միանշանակ կապված եւ էլեկտրոնային թվային ստորագրության իսկության ստուգման համար նախատեսված սիմվոլների եզակի հաջորդականությունն է։

Սերտիֆիկատների կիրառման քաղաքականությունը (Certificate Policy) անվտանգության տրված պահանջներով հավելվածների որոշակի միությամբ եւ (կամ) դասով սերտիֆիկատի օգտագործումը որոշող կանոնների հավաքակազմն է։

Սերտիֆիկատից օգտվողը սույն կանոնակարգի համաձայն թողարկված սերտիֆիկատներ ընդունող եւ Հանձնաժողովի ՀԿ-ի լիազորված անձի սերտիֆիկատներին վստահելով գործող անձն է։

Սերտիֆիկացման ուղին (շղթան) սերտիֆիկատների կանոնակարգված հաջորդականությունն է, որը կարող է մշակվել սկզբնական օբյեկտի ԷԹՍ ստուգման բանալու հետ միասին վերջնական օբյեկտի ԷԹՍ-ի ստուգման բանալին ճանաչելու համար։

Հավաստագրման կենտրոնի կանոնակարգը (Certification Practice Statement) փաստաթուղթ է, որը պարունակում է ընթացակարգերի եւ գործողությունների նկարագրություն, որոնք ՀԿ-ն օգտագործում է սերտիֆիկատների թողարկման, կառավարման, հետկանչման եւ վերականգնման ժամանակ։

ԷԹՍ ստուգման բանալու սերտիֆիկատը (սերտիֆիկատ) հավաստագրման կենտրոնի կողմից տրված եւ սերտիֆիկատ տիրապետողին էլեկտրոնային թվային ստորագրության ստուգման բանալու պատկանելիությունը հաստատող էլեկտրոնային փաստաթուղթ կամ թղթային կրիչով փաստաթուղթն է։

Հանձնաժողովի ՀԿ-ի օգտվողի հետ համաձայնագիրը (Համաձայնագիր) Հանձնաժողովի ՀԿ-ի եւ ՀԿ-ի օգտվողի միջեւ համաձայնագիրն է, որով սահմանվում են սերտիֆիկատների օգտագործմանը վերաբերող՝ կողմերի իրավունքները եւ պարտականությունները, եւ որն արտահայտված է սերտիֆիկատի պատրաստման հայտի ստորագրման միջոցով սույն կանոնակարգին ՀԿ-ի օգտվողի միանալու մեջ։

Չեղարկված (հետկանչված) սերտիֆիկատների ցանկը կամ ՀՍՑ-ն Հանձնաժողովի ՀԿ-ի լիազորված անձի ԷԹՍ-ով ստորագրված էլեկտրոնային փաստաթուղթն է, որը պարունակում է սերտիֆիկատների սերիական համարների ցանկ, որոնք որոշակի ժամանակահատվածում հետ են կանչվել, կամ որոնց գործողությունը կասեցվել է։ Սերտիֆիկատները, որոնց համարներն առկա են ՀՍՑ-ի ֆայլի ցանկում, համարվում են Հանձնաժողովի ՀԿ-ի շրջանառությունից հետ կանչված։

Էլեկտրոնային թվային ստորագրության միջոցները (ԷԹՍ միջոցներ) ծածկագրային (գաղտնագրային) միջոցներն են, որոնք օգտագործվում են հետեւյալ գործառույթներից առնվազն մեկի իրագործման համար՝ ԷԹՍ ստեղծում, ԷԹՍ ստուգում, ԷԹՍ բանալու եւ ԷԹՍ ստուգման բանալու ստեղծում։

Հավաստագրման կենտրոնի լիազորված անձը Հանձնաժողովի ՀԿ-ի լիազորված անձն է, որն օժտված է սերտիֆիկատները եւ ՀՍՑ-ն իր էլեկտրոնային թվային ստորագրությամբ վավերացնելու լիազորություններով։

Էլեկտրոնային փաստաթուղթն էլեկտրոնային թվային ստորագրությամբ (էլեկտրոնային ստորագրությամբ) վավերացված եւ էլեկտրոնային տեսքով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի պահանջներին բավարարող՝ էլեկտրոնային տեսքով փաստաթուղթն է։

Էլեկտրոնային թվային ստորագրությունը (էլեկտրոնային ստորագրություն)՝ ԷԹՍ-ն, էլեկտրոնային տեսքով տեղեկատվությունն է, որը միացված է էլեկտրոնային տեսքով այլ տեղեկատվության կամ այլ կերպ կապված է այդպիսի տեղեկատվության հետ, ծառայում է այդ տեղեկատվության ամբողջականության եւ իսկության հսկողության համար, ապահովում է հեղինակությունից հրաժարվելու անհնարինությունը, մշակվում է տվյալ տեղեկատվության նկատմամբ գաղտնագրական վերափոխման կիրառման միջոցով՝ փակ (անձնական) բանալու (ԷԹՍ բանալու) օգտագործմամբ, եւ ստուգվում է բաց բանալու (ԷԹՍ ստուգման բանալու) օգտագործմամբ։

Սերտիֆիկատի թողարկման, գործողության կասեցման, գործողության վերականգնման կամ հետկանչման հարցումը ԳԿ-ի օպերատորի կողմից ձեւավորված եւ ԳԿ օպերատորի ԷԹՍ-ով վավերացված ֆայլն է։ ԳԿ-ի օպերատորի ԷԹՍ-ով ստորագրված հարցումները մշակվում են Հանձնաժողովի ՀԿ-ի լիազորված անձի կողմից։

PKCS#10 (RFC 2986)՝ սերտիֆիկատի թողարկման հարցման ձեւաչափը եւ շարահյուսությունը որոշող ստանդարտ։

1.6.2. Տառային հապավումներ

CDP CRL Distribution Point (ՀՍՑ տարածման կետ).

CRL Certificate Revocation List (Չեղարկված (հետկանչված) սերտիֆիկատների ցանկ). PKCS Public-Key Cryptography Standard.

PKI Public Key Infrastructure (Էլեկտրոնային ստորագրության ստուգման բանալու ենթակառուցվածք).

RFC Request For Comments.

DN Distinguished Name (Տարբերակիչ անուն).

ԲԲԵ՝ Բաց բանալիների ենթակառուցվածք.

ԾԱ՝ Ծրագրային ապահովում.

ՀՍՑ՝ Չեղարկված (հետկանչված) սերտիֆիկատների ցանկ.

ՏԳՊՄ՝ Տեղեկատվության գաղտնագրային պաշտպանության միջոցներ.

ՀԿ՝ Հավաստագրման կենտրոն.

ԳԿ՝ Գրանցման կենտրոն.

ԷԹՍ՝ Էլեկտրոնային թվային ստորագրություն (էլեկտրոնային ստորագրություն)։

2. Հրապարակում եւ ռեպոզիտարիայում տեղեկատվության արդիականության համար պատասխանատվություն

2.1. Ռեպոզիտարիում

Հանձնաժողովի ՀԿ-ն պահում է արդիական վիճակում ռեպոզիտարիումը։ Որպես ռեպոզիտարիում օգտագործվում է WEB-պորտալում առանձնացված դիրեկտորիան։

2.2. Տեղեկատվության հրապարակում

Հրապարակման ենթակա է՝

Հանձնաժողովի ՀԿ-ի լիազորված անձի սերտիֆիկատները.

ՀՍՑ-ն.

սերտիֆիկատների կիրառման քաղաքականությունները.

սույն կանոնակարգը.

սերտիֆիկատի թողարկման, գործողության կասեցման, գործողության վերականգնման, հետկանչման հայտերի ձեւանմուշները՝ սույն կանոնակարգի 3-րդ հավելվածի համաձայն.

ուղեկցող տեղեկատվությունը, ծանուցումները, թարմացումները եւ ուղղումները։

2.3. Հրատարակումների ժամը եւ հաճախականությունը

Տեղեկատվության հրատարակումն իրականացվում է դրա հասանելի դառնալուն պես եւ արդիական վիճակում այն պահելու համար անհրաժեշտ հաճախականությամբ։

2.4. Մուտք ռեպոզիտարիային

Ամբողջ հրապարակվող տեղեկատվությունը հանրամատչելի է Հանձնաժողովի ՀԿ-ի օգտվողների համար։ Ռեպոզիտարիայի ադմինիստրատորն օգտագործում է տարբեր մեխանիզմներ՝ հրապարակված տեղեկատվության չթույլատրված փոփոխության, լրացման եւ (կամ) հեռացման կանխարգելման համար։

3. Նույնականացում եւ աուտենտիֆիկացում

3.1. Անվանակոչումը

3.1.1. Անունների տիպերը

Որպես անուն սերտիֆիկատում օգտագործվում է տարբերակիչ անուն՝ համաձայն Х.500 ստանդարտի։

3.1.2. Անունների մեկնաբանությանը ներկայացվող պահանջներ

Սերտիֆիկատներում առկա անունները միանշանակ նույնականացնում են սուբյեկներին։

3.1.3. Անանուն կամ կեղծանուններով հայտատուներ

Սերտիֆիկատների թողարկումը անանուն հայտատուների համար անթույլատրելի է:

Կեղծանունների օգտագործումը թույլատրվում է։

3.1.4. Տարբեր ձեւերի անունների մեկնաբանման կանոնները

Պայմաններ չկան։

3.1.5. Անունների եզակիությունը

Հնարավոր է միեւնույն տարբերակիչ անունով մի քանի սերտիֆիկատների գոյությունը։ Ընդ որում, Հանձնաժողովի ՀԿ-ն երաշխավորում է թողարկվող սերտիֆիկատների եզակիությունը։

3.1.6. Ապրանքանիշերի ճանաչումը, աուտենտիֆիկացումը եւ դերը

Անունները, որոնց տիրապերող չէ Հայտատուն, չեն կարող օգտագործվել սերտիֆիկատում։ Հանձնաժողովի ՀԿ-ն կարող է չստուգել դոմենային անունների, ապրանքանիշերի եւ (կամ) մտավոր սեփականության այլ օբյեկտների տիրապետման մասով հայտատուի իրավունքները, սակայն դրանց տիրապետման իրավունքի շուրջ որեւէ վեճի առաջացման դեպքում պետք է կասեցնի սերտիֆիկատի գործողությունը մինչ լուծման ավարտը եւ վեճի արդյունքներին համապատասխան՝ դրա ավարտից հետո որոշի սերտիֆիկատի կարգավիճակը։

3.2. Իսկության սկզբնական հաստատումը

3.2.1. ԷԹՍ բանալու տիրապետման ապացույցի մեթոդը

Եթե բանալու զույգը ստեղծվում է Հանձնաժողովի հավաստագրման կենտրոնի կողմից, ապա ապացույց չի պահանջվում։

Եթե բանալու զույգը ստեղծվում է հայտատուի կողմից ինքնուրույն, ապա ԷԹՍ բանալու տիրապետման ապացույցի մեթոդ է համարվում ԷԹՍ բանալու տիրապետման գաղտնագրային ցուցադրումը։ ԷԹՍ բանալու տիրապետման ցուցադրումն իրականացվում է Հանձնաժողովի ՀԿ-ի կողմից տրամադրվող տվյալների որոշակի հավաքակազմի՝ հայտատուի կողմից ստորագրման միջոցով՝ ԷԹՍ սեփական բանալու օգտագործմամբ եւ Հանձնաժողովի ՀԿ-ում ստորագրված տվյալների փոխանցման միջոցով, որտեղ իրականացվում է ԷԹՍ ստուգում՝ ԷԹՍ ստուգման բանալու օգտագործմամբ։ ԷԹՍ ստուգման ճիշտ ավարտված ընթացակարգն ԷԹՍ բանալու տիրապետման ապացույցն է։ ԷԹՍ ստուգման ոչ ճիշտ ավարտված ընթացակարգը հանգեցնում է սերտիֆիկատի գործողության ավարտին եւ հետկանչմանը։

3.2.2. Կազմակերպման նույնականացման տեղեկատվության ստուգումը

Պայմաններ չկան։

3.2.3. Անձնական նույնականացման տեղեկատվության ստուգումը

Օգտվողի անձնական նույնականացման տեղեկատվությունն ստուգվում է անձը հաստատող փաստաթղթերի եւ կադրային տեղեկատվության հիման վրա։

3.2.4. Չստուգվող տեղեկատվություն

Չի թույլատրվում սերտիֆիկատում չստուգվող կամ չստուգված տեղեկատվության նշումը։

3.2.5. Լիազորությունների ստուգում

Հայտատուի լիազորությունների ստուգումն իրականացվում է սերտիֆիկատների կիրառման այն քաղաքականությամբ նախատեսված կարգով, որին համապատասխան սերտիֆիկատը թողարկվում է։

3.2.6. Փոխգործակցության չափանիշներ

Պայմաններ չկան։

3.3. **Աուտենտիֆիկացում եւ նույնականացում՝ բանալիների թարմացման համար**

3.3.1. Աուտենտիֆիկացում եւ նույնականացում՝ բանալիների պլանային փոխարինման համար

Աուտենտիֆիկացումը եւ նույնականացումն իրականացվում են ըստ գործող սերտիֆիկատի, անձը հաստատող փաստաթղթի կամ երկգործոնային աուտենտիֆիկացման համակարգերի օգտագործմամբ։

3.4. Աուտենտիֆիկացում եւ նույնականացում՝ հետկանչումից հետո բանալիների թարմացման համար

Աուտենտիֆիկացումը եւ նույնականացումն իրականացվում են ըստ անձը հաստատող փաստաթղթի կամ երկգործոնային աուտենտիֆիկացման համակարգերի օգտագործմամբ։

3.4.1. Աուտենտիֆիկացում եւ նույնականացում՝ հետկանչման հարցման համար

Աուտենտիֆիկացումն ու նույնականացումն իրականացվում են ըստ անձը հաստատող փաստաթղթի, գործող սերտիֆիկատի, կապի ցանկացած միջոցներով փոխանցված մեկանգամյա գաղտնաբառի, հետկանչման՝ փաստաթղթերով հաստատված հարցման կամ երկգործոնային աուտենտիֆիկացման համակարգերի օգտագործմամբ։

4. Սերտիֆիկատի կյանքի ցիկլի ֆունկցիոնալ պահանջները

Սույն բաժնում նկարագրվում են Հանձնաժողովի ՀԿ-ի ծառայությունների ներկայացման պայմանները եւ կարգը։

Հանձնաժողովի ՀԿ-ն տրամադրում է հետեւյալ տեսակի ծառայությունները՝

Հանձնաժողովի ՀԿ-ի ռեեստրում հայտատուի մասին գրանցման տեղեկատվության ներմուծում.

բանալու զույգի ձեւավորում` հայտատուի հարցմամբ բանալու կրիչի վրա դրա հետագա գրառմամբ.

հայտատուի համար էլեկտրոնային ձեւով սերտիֆիկատի պատրաստում՝ սերտիֆիկատ տիրապետողի համար թղթային կրիչով սերտիֆիկատի պատճենի պատրաստում.

Հանձնաժողովի ՀԿ-ի կողմից պատրաստված սերտիֆիկատների ռեեստրի վարում.

սերտիֆիկատներից օգտվողների հարցումներով թողարկված սերտիֆիկատների ռեեստրից էլեկտրոնային ձեւով սերտիֆիկատների տրամադրում.

սերտիֆիկատներ տիրապետողների դիմումների համաձայն սերտիֆիկատների չեղարկում (հետկանչում).

սերտիֆիկատներ տիրապետողների դիմումների համաձայն սերտիֆիկատների գործողության կասեցում եւ վերականգնում.

սերտիֆիկատներից օգտվողներին չեղարկված (հետկանչված) սերտիֆիկատների եւ գործողության կասեցված ժամկետով սերտիֆիկատների մասին տեղեկությունների տրամադրում.

ըստ սերտիֆիկատից օգտվողի դիմումի էլեկտրոնային ձեւով ներկայացված փաստաթղթերում ԷԹՍ իսկության հաստատում.

Հանձնաժողովի ՀԿ-ի լիազորված անձի ԷԹՍ իսկության հաստատում սերտիֆիկատից օգտվողի դիմումի համաձայն վերջիններիս կողմից պատրաստված սերտիֆիկատներում.

ԷԹՍ միջոցների տարածում։

ԷԹՍ վավերականության եւ ժամանակի դրոշմների մասով աշխատանքների անցկացման կարգը ներկայացված է սույն կանոնակարգի թիվ 4 հավելվածում։

4.1. **Սերտիֆիկատի թողարկման հայտ**

4.1.1. Սերտիֆիկատի թողարկման հայտ

Սերտիֆիկատի թողարկման հայտ կարող է ներկայացնել Հանձնաժողովի կոլեգիայի անդամը, Հանձնաժողովի պաշտոնատար անձը կամ աշխատակիցը։

4.1.2. Գրանցման գործընթացը եւ պահանջները

Գրանցման գործընթացն իրականացվում է սերտիֆիկատների կիրառման այն քաղաքականությամբ նախատեսված կարգով, որին համապատասխան սերտիֆիկատը թողարկվում է։

4.1.3. Հայտատուի կողմից դրա գրանցման ընթացակարգի անցկացման համար ներկայացված փաստաթղթերի ցանկ

Փաստաթղթերի ցանկը որոշվում է սերտիֆիկատների կիրառման այն քաղաքականությամբ, որին համապատասխան սերտիֆիկատը թողարկվում է։

4.2. Սերտիֆիկատի թողարկման հայտի մշակում

4.2.1. Հայտատուի նույնականացում եւ աուտենտիֆիկացում Աուտենտիֆիկացումն ու նույնականացումն իրականացվում են սույն կանոնակարգի 3.2 բաժնի պահանջներին համապատասխան։

4.2.2. Սերտիֆիկատի թողարկման հայտի ընդունում կամ մերժում

Հանձնաժողովի ՀԿ-ն կարող է մերժել սերտիֆիկատի թողարկման հայտը հետեւյալ դեպքերում՝

հայտը փոխանցվել է սույն կանոնակարգի պահանջներին, սերտիֆիկատների կիրառման քաղաքականությունների պահանջներին չհամապատասխանող եղանակով կամ չհամապատասխանող ձեւաչափով.

հայտում նշված տվյալները չեն համապատասխանում իրականությանը.

հայտում նշված տվյալները հաստատված չեն համապատասխան փաստաթղթերով.

հայտատուն չի անցել աուտենտիֆիկացման եւ նույնականացման ընթացակարգ.

սերտիֆիկատի թողարկումը կարող է որեւէ վնաս պատճառել Հանձնաժողովի ՀԿ-ին։

Սերտիֆիկատի թողարկման հայտն ընդունվում է, եթե բացակայում են դրա մերժման համար վերը թվարկված պատճառները։

4.2.3. Սերտիֆիկատի թողարկման հայտի մշակման ժամկետը

ԳԿ-ի օպերատորը պետք է սկսի սերտիֆիկատի թողարկման հայտի մշակումն այն ստանալու պահից։ Հայտի մշակման ժամանակի սահմանափակումը կարող է սահմանված լինել սերտիֆիկատների կիրառման այն քաղաքականության մեջ, որին համապատասխան սերտիֆիկատը թողարկվում է։ Հայտը համարվում է գործող մինչ դրա ընդունման կամ մերժման պահը։

Սերտիֆիկատի թողարկման հայտի փոխանցման ժամանակ է համարվում Հայտատուի կողմից ԳԿ-ի օպերատորին այն անձամբ հանձնելու ժամանակը։

Սերտիֆիկատի թողարկման հայտի մշակման ավարտի ժամանակ է համարվում սերտիֆիկատի թողարկման հայտի ստեղծման կամ հայտի ընդունումը մերժելու ժամանակը։

Եթե ԳԿ-ի օպերատորը մերժել է սերտիֆիկատի թողարկման հայտի ընդունումը, ապա հայտատուն պետք է տեղեկացվի մերժման եւ դրա պատճառների մասին։

4.3. Սերտիֆիկատի թողարկում

4.3.1. Սերտիֆիկատի թողարկման ժամանակ նախատեսված գործողությունները

Հանձնաժողովի ՀԿ-ն թողարկում է սերտիֆիկատ՝ ըստ ԳԿ-ի օպերատորի ԷԹՍ-ով վավերացված հարցման։ Սերտիֆիկատը թողարկվում է հայտում նշված տվյալների հիման վրա սերտիֆիկատների կիրառման այն քաղաքականությամբ նախատեսված կարգով, որին համապատասխան սերտիֆիկատը թողարկվում է։

Սերտիֆիկատը թողարկվում է Հանձնաժողովի ՀԿ-ի լիազորված անձի ԷԹՍ-ով վավերացված էլեկտրոնային փաստաթղթի ձեւով եւ ԳԿ-ի օպերատորի ձեռագիր ստորագրությամբ վավերացված թղթային կրիչով փաստաթղթի ձեւով։

4.3.2. Սերտիֆիկատի թողարկման մասին հայտատուին տեղեկացնելը

Հանձնաժողովի ՀԿ-ն տեղեկացնում է հայտատուին սերտիֆիկատի թողարկման մասին սերտիֆիկատի թողարկման հայտում նշված հասցեին email –հաղորդում ուղարկելու միջոցով։

4.4. Սերտիֆիկատի ճանաչումը

4.4.1. Սերտիֆիկատի ճանաչման գործողությունները

Սերտիֆիկատի ճանաչում է համարվում հայտատուի հետեւյալ գործողությունները՝

սերտիֆիկատի օգտագործումը.

թղթային ձեւով սերտիֆիկատի ձեռագրային ստորագրությամբ վավերացումը։

Դրանից բացի, եթե Հանձնաժողովի ՀԿ-ն 1 աշխատանքային օրվա ընթացքում չի ստանում սերտիֆիկատի մերժման մասին հայտատուից ծանուցում, ապա սերտիֆիկատը համարվում է ճանաչված։

4.4.2. Սերտիֆիկատի հրապարակումը հավաստագրման կենտրոնի կողմից

Հանձնաժողովի ՀԿ-ն հրապարակում է թողարկված սերտիֆիկատները ռեպոզիտարիայում։

4.4.3. Հանձնաժողովի ՀԿ-ին սերտիֆիկատի թողարկման մասին երրորդ կողմին ծանուցելը

Պայմաններ չկան։

4.5. Սերտիֆիկատի եւ բանալու զույգի օգտագործումը

4.5.1.Սերտիֆիկատի եւ բանալու զույգի օգտագործումը սերտիֆիկատ տիրապետողի կողմից

Սերտիֆիկատ տիրապետողը կարող է օգտագործել իր սեփական սերտիֆիկատը դրա ճանաչումից հետո եւ սերտիֆիկատի կիրառման քաղաքականությունների, սույն կանոնակարգի եւ այլ ուղեցույց փաստաթղթերի պահանջներին համապատասխան։ Սերտիֆիկատ տիրապետողը պետք է պաշտպանի ԷԹՍ բանալին կոմպրոմետացիայից:

Թույլատվում է միայն գործող սերտիֆիկատի օգտագործումը սերտիֆիկատների կիրառման այն քաղաքականությունների պահանջներին համապատասխան, որոնց նույնականացուցիչները նշված են սերտիֆիկատում։

4.5.2.Սերտիֆիկատի եւ ԷԹՍ ստուգման բանալու օգտագործումը սերտիֆիկատից օգտվողի կողմից

Մինչ սերտիֆիկատ օգտագործելը սերտիֆիկատից օգտվողը պարտավոր է՝

ծանոթանալ սերտիֆիկատների կիրառման քաղաքականության եւ սույն կանոնակարգի հետ, որոնց համապատասխան սերտիֆիկատը թողարկվել է.

ստուգել օգտագործվող սերտիֆիկատի եւ սերտիֆիկացման ուղու մեջ մտնող՝ Հանձնաժողովի ՀԿ-ի լիազորված անձի սերտիֆիկատի կարգավիճակը։

Սերտիֆիկատից օգտվողը կարող է օգտագործել միայն գործող սերտիֆիկատ սերտիֆիկատների կիրառման այն քաղաքականության պահանջներին համապատասխան, որի նույնականացուցիչը նշված է սերտիֆիկատում։

4.6. Սերտիֆիկատի թարմացումը

Սերտիֆիկատի թարմացումը նոր սերտիֆիկատի թողարկում է՝ առանց ԷԹՍ ստուգման բանալու կամ սերտիֆիկատում այլ տեղեկատվության փոփոխության։

4.6.1. Սերտիֆիկատի թարմացման հանգամանքները

Հանձնաժողովի ՀԿ-ն չի իրականացնում սերտիֆիկատների թարմացում։

4.6.2. Ո՞վ կարող է սերտիֆիկատի թարմացման հարցում կատարել

Պայմաններ չկան։

4.6.3. Սերտիֆիկատների թարմացման հարցումների մշակում

Պայմաններ չկան։

4.6.4. Նոր սերտիֆիկատի թողարկման մասին տեղեկացում հայտատուին

Պայմաններ չկան։

4.6.5. Թարմացված սերտիֆիկատի ճանաչման մասով գործողություններ

Պայմաններ չկան։

4.6.6. Թարմացված սերտիֆիկատի հրապարակում

Պայմաններ չկան։

4.6.7. Սերտիֆիկատի թարմացման մասին երրորդ կողմին ծանուցելը

Պայմաններ չկան։

4.7. Բանալիների թարմացումը

Տվյալ բաժնում նկարագրվում է նոր սերտիֆիկատի թողարկումը բանալու զույգի թարմացման դեպքում։

4.7.1. Բանալու զույգի թարմացման հանգամանքները

Բանալու զույգի թարմացումը հնարավոր է ԷԹՍ բանալու կոմպրոմետացման դեպքում, ինչպես նաեւ սերտիֆիկատի գործողության ժամկետը լրանալու դեպքում։ Բանալու զույգերի գեներացումն իրականացվում է սույն կանոնակարգի 6.2 ենթաբաժնին համապատասխան։

4.7.2. Ո՞վ կարող է բանալու զույգի թարմացման դեպքում սերտիֆիկատի թողարկման հայտ ներկայացնել

Բանալու զույգի թարմացման դեպքում սերտիֆիկատի թողարկման հայտը կարող է ներկայացնել սերտիֆիկատ տիրապետողը։

4.7.3. Բանալու զույգի թարմացման դեպքում սերտիֆիկատի թողարկման հայտի մշակումը

Բանալու զույգի թարմացման դեպքում սերտիֆիկատի թողարկման հաստատումն իրականացվում է 4.2 ենթաբաժնին համապատասխան, իսկ սերտիֆիկատի թողարկումը՝ սույն կանոնակարգի 4.3 կետին համապատասխան։

4.7.4. Նոր սերտիֆիկատի թողարկման մասին սերտիֆիկատ տիրապետողին տեղեկացնելը

Տեղեկացումը կատարվում է սույն կանոնակարգի 4.3.2 կետին համապատասխան։

4.7.5. Բանալու զույգի թարմացման դեպքում նոր սերտիֆիկատի ճանաչման մասով գործողությունները

Ճանաչումն իրականացվում է սույն կանոնակարգի 4.4.1 կետին համապատասխան։

4.7.6. Բանալու զույգի թարմացման դեպքում նոր սերտիֆիկատի հրապարակումը

Հրապարակումն իրականացվում է սույն կանոնակարգի 4.4.2 կետին համապատասխան։

4.7.7. Բանալու զույգի թարմացման դեպքում նոր սերտիֆիկատի թողարկման մասին երրորդ կողմին ծանուցելը

Պայմաններ չկան։

4.8. Սերտիֆիկատի փոփոխությունը

Սերտիֆիկատի փոփոխությունը նոր սերտիֆիկատի թողարկումն է գոյություն ունեցող սերտիֆիկատում ներառված տեղեկատվության փոփոխության անհրաժեշտության դեպքում։ Ընդ որում, հին սերտիֆիկատը հետ է կանչվում։

4.8.1. Սերտիֆիկատի փոփոխության հանգամանքները

Սերտիֆիկատի փոփոխությունը կատարվում է այն դեպքում, երբ սերտիֆիկատում առկա տեղեկատվությունը դառնում է ոչ արդիական, եւ այն սերտիֆիկատ մտցնելիս սխալ է թույլ տրվել։

4.8.2. Ո՞վ կարող է սերտիֆիկատի փոփոխության հայտ ներկայացնել

Սերտիֆիկատի փոփոխության հայտ կարող է ներկայացնել սերտիֆիկատ տիրապետողը։

4.8.3. Սերտիֆիկատի փոփոխության հայտի մշակում

Սերտիֆիկատի փոփոխության հայտի հաստատումն իրականացվում է սույն կանոնակարգի 4.2 ենթաբաժնին, իսկ սերտիֆիկատի թողարկումը՝ 4.3.1 բաժնին համապատասխան։

4.8.4. Նոր սերտիֆիկատի թողարկման մասին սերտիֆիկատ տիրապետողին տեղեկացնելը

Տեղեկացումը կատարվում է սույն կանոնակարգի 4.3.2 կետին համապատասխան։

4.8.5. Փոփոխված սերտիֆիկատի ճանաչման մասով գործողությունները

Ճանաչումն իրականացվում է սույն կանոնակարգի 4.4.1 կետին համապատասխան։

4.8.6. Հանձնաժողովի ՀԿ-ի փոփոխված սերտիֆիկատի հրապարակումը

Հրապարակումն իրականացվում է 4.4.2 կետին համապատասխան։

4.8.7. Հանձնաժողովի ՀԿ-ի փոփոխված սերտիֆիկատի թողարկման մասին երրորդ կողմին ծանուցելը

Պայմաններ չկան։

4.9. Սերտիֆիկատի հետկանչումը, գործողության կասեցումը եւ գործողության վերականգնումը

Սերտիֆիկատի գործողության ժամկետը լրանալուն պես սերտիֆիկատը ավտոմատ կերպով համարվում է չեղարկված։ Սերտիֆիկատը համարվում է հետկանչված, կասեցված կամ վերականգնված այդ սերտիֆիկատի կարգավիճակի փոփոխության մասին տեղեկատվություն պարունակող ՀՍՑ-ն հանձնաժողովի ՀԿ-ի ռեպոզիտարիայում հրապարակելու պահից։

4.9.1. Սերտիֆիկատի հետկանչման հանգամանքները

Սերտիֆիկատը կարող է հետ կանչվել հետեւյալ հանգամանքներում՝

սերտիֆիկատում նշված ԷԹՍ ստուգման բանալուն համապատասխանող ԷԹՍ բանալու կոմպրոմետացիայի դեպքում.

սերտիֆիկատ տիրապետողի կողմից սույն կանոնակարգի պահանջները չպահպանելու դեպքում.

Հանձնաժողովի ՀԿ-ի գործունեության դադարեցման դեպքում.

սերտիֆիկատի հետագա օգտագործումը կարող է վնաս պատճառել Հանձնաժողովի ՀԿ-ին.

ըստ սերտիֆիկատ տիրապետողի հարցման.

սերտիֆիկատների կիրառման այն քաղաքականությամբ նախատեսված այլ հանգամանքներում, որին համապատասխան սերտիֆիկատը թողարկվել է։

4.9.2. Սերտիֆիկատի հետկանչման հայտ

Սերտիֆիկատի հետկանչման հայտը կարող է ներկայացվել՝

սերտիֆիկատ տիրապետողի կողմից.

Հանձնաժողովի ՀԿ-ի աշխատակցի կողմից, եթե այն տիրապետում է սերտիֆիկատի հետկանչում պահանջող հավաստի տեղեկատվություն.

սերտիֆիկատների կիրառման այն քաղաքականությամբ նախատեսված այլ անձի կողմից, որին համապատասխան սերտիֆիկատը թողարկվել է։

4.9.3. Սերտիֆիկատի հետկանչման հայտի ուսումնասիրման ընթացակարգը

Սերտիֆիկատի հետկանչման հայտը կարող է ներկայացվել թղթային կամ էլեկտրոնային ձեւով կամ կապի ցանկացած միջոցի օգտագործմամբ, սակայն ցանկացած դեպքում սույն կանոնակարգի 3.4 ենթաբաժնի համաձայն աուտենտիֆիկացմամբ։

Սերտիֆիկատի հետկանչման հայտը պետք է պարունակի հետեւյալ տեղեկատվությունը՝

սերտիֆիկատի սերիական համարը կամ սերտիֆիկատը միանշանակ նույնականացնել թույլ տվող այլ տեղեկատվություն.

սերտիֆիկատի հետկանչման պատճառը.

անհրաժեշտ մեկնաբանությունները։

Սերտիֆիկատի հետկանչման հայտն ստանալուց հետո ԳԿ-ի օպերատորը կատարում է հայտի վերիֆիկացում, եւ եթե այն բարեհաջող է անցել, ապա ձեւավորում է սերտիֆիկատի հետկանչման հարցում եւ ստորագրում է այն իր ԷԹՍ-ով։

Հանձնաժողովի ՀԿ-ի լիազորված անձը ԳԿ-ի օպերատորի ԷԹՍ-ով ստորագրած սերտիֆիկատի հետկանչման հարցման հիման վրա հետ է կանչում սերտիֆիկատը։ Սերտիֆիկատի հետկանչումից հետո Հանձնաժողովի ՀԿ-ն մեկ ժամվա ընթացքում հրապարակում է հետկանչված սերտիֆիկատի մասին տեղեկատվություն պարունակող թարմացված ՀՍՑ-ն։

4.9.4. Սերտիֆիկատի հետկանչման հայտի փոխանցման ժամկետը

Սերտիֆիկատի հետկանչման հայտը պետք է հնարավորինս շտապ փոխանցվի ԳԿ-ի օպերատորին։

4.9.5. Սերտիֆիկատի հետկանչման հայտի մշակման ժամկետը

Սերտիֆիկատի հետկանչի հայտն ուսումնասիրվում է այն ներկայացնելու պահից աշխատանքային օրվա չորս ժամվա ընթացքում։ Հայտի ներկայացման ժամանակ է համարվում՝

էլեկտրոնային փոստով փոխանցման դեպքում՝ ԳԿ-ի օպերատորի հասցեին հաղորդումն ուղարկելու ժամանակը.

անձամբ հանձնելու դեպքում կամ այլ եղանակներով փոխանցմամբ՝ ԳԿ-ի օպերատորի կողմից հայտի ստացման ժամանակը։

4.9.6. Սերտիֆիկատներից օգտվողներին սերտիֆիկատի կարգավիճակի ստուգման մասով ներկայացվող պահանջները

Սերտիֆիկատից օգտվողը պարտավոր է ստուգել սերտիֆիկատի կարգավիճակը յուրաքանչյուր օգտագործումից առաջ՝ օգտագործելով Հանձնաժողովի ՀԿ-ի կողմից հրապարակվող ՀՍՑ-ն կամ Հանձնաժողովի ՀԿ-ի OCSP-ծառայության կողմից տրամադրվող՝ իրական ժամանակի ռեժիմում սերտիֆիկատի կարգավիճակի ստուգման ծառայությունը։

4.9.7. Հետկանչված սերտիֆիկատների ցանկի թողարկման հաճախականությունը

Հանձնաժողովի ՀԿ-ն հրապարակում է արդիական ՀՍՑ-ներ աշխատանքային օրերին 24 ժամը մեկ հաճախականությամբ։ Այն դեպքում, երբ ՀՍՑ-ի հրապարակման օրվան հաջորդում են ոչ աշխատանքային կամ տոնական օրեր, ապա ՀՍՑ-ի գործողության ժամկետը երկարացվում է մինչեւ մոտակա աշխատանքային օրը։ Սերտիֆիկատի հետկանչման դեպքում ՀՍՑ-ի հրապարակումն իրականացվում է 4.9.3 ենթակետում շարադրված ընթացակարգին համապատասխան։

Եթե ՀՍՑ-ում ներառված սերտիֆիկատի գործողության ժամկետը լրանում է, ապա այն կարող է հեռացվել այնտեղից գործողության ժամկետի ավարտից հետո։

4.9.8. Հետկանչված սերտիֆիկատների ցանկի հրապարակման ուշացման առավելագույն ժամանակը

ՀՍՑ-ի հրապարակման ուշացման առավելագույն ժամանակը կազմում է 6 ժամ։

4.9.9. OCSP-ծառայության մատչելիությունը

Հանձնաժողովի ՀԿ-ի OCSP-ծառայությունը մատչելի է հետեւյալ URL-հասցեով՝

<https://ca-ocsp.eecommission.org:8877>

Կազմակերպատեխնիկական համալիր միջոցներով ապահովվում են OCSP-ծառայության մատչելիության պահանջվող ցուցանիշները։

4.9.10. OCSP-ծառայությանը ներկայացվող պահանջները

OCSP-ծառայությունն ապահովում է ԲԲԵ-ի կառուցման մասով միջազգային առաջարկությունների օգտագործումը՝ հաշվի առնելով ԳՕՍՏ 28147-89, ԳՕՍՏ Ռ 34.11-2012, ԳՕՍՏ Ռ 34.10-2012 կիրառումը.

RFC 2560 - "Internet Х.509 Public Key Infrastructure. Online Certificate Status Protocol - OCSP".

RFC 5280 - "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile"։

4.9.11. Սերտիֆիկատի հետկանչման մասին տեղեկացման այլ մատչելի ձեւեր

Նախատեսված չեն։

4.9.12. Բանալիների կոմպրոմետացիային վերաբերող հատուկ պահանջները

Հանձնաժողովի ՀԿ-ի, OCSP-ծառայության կամ TSP-ծառայության լիազորված անձի ԷԹՍ բանալու կոմպրոմետացիայի դեպքում ԲԲԵ մասնակիցները տեղեկացվում են համապատասխան email- հաղորդումներ ուղարկելու միջոցով։

4.9.13. Սերտիֆիկատի գործողության կասեցման հանգամանքները

Սերտիֆիկատի գործողությունը պետք է կասեցվի հետեւյալ հանգամանքներում՝

ըստ սերտիֆիկատ տիրապետողի հարցումի.

տվյալ պահին սերտիֆիկատի իսկության մասին որոշման ընդունում թույլ չտվող որեւէ ուսումնասիրման առաջացում.

սերտիֆիկատների կիրառման այն քաղաքականությամբ նախատեսված այլ հանգամանքներում, որին համապատասխան սերտիֆիկատը թողարկվել է։

4.9.14. Սերտֆիկատի գործողության կասեցման հայտը

Սերտիֆիկատի գործողության կասեցման հայտը կարող է ներկայացվել՝

սերտիֆիկատ տիրապետողի կողմից.

Հանձնաժողովի ՀԿ-ի աշխատակցի կողմից, եթե վերջինս տիրապետում է սերտիֆիկատի գործողության կասեցում պահանջող հավաստի տեղեկատվություն.

սերտիֆիկատների կիրառման այն քաղաքականությամբ նախատեսված այլ անձի կողմից, որին համապատասխան սերտիֆիկատը թողարկվել է։

4.9.15. Սերտիֆիկատի գործողության կասեցման հայտի ուսումնասիրման ընթացակարգը

Սերտիֆիկատի գործողության կասեցման հայտը կարող է ներկայացվել թղթային կամ էլեկտրոնային ձեւով կամ կապի ցանկացած միջոցի օգտագործմամբ, սակայն ցանկացած դեպքում սույն կանոնակարգի 3.4 ենթաբաժնի համաձայն աուտենտիֆիկացմամբ։

Սերտիֆիկատի գործողության կասեցման հայտը պետք է պարունակի հետեւյալ տեղեկատվությունը՝

սերտիֆիկատի սերիական համարը կամ սերտիֆիկատը միանշանակ նույնականացնել թույլ տվող այլ տեղեկատվություն.

կասեցման պատճառը.

անհրաժեշտ մեկնաբանությունները։

Սերտիֆիկատի գործողության կասեցման հայտն ստանալուց հետո ԳԿ-ի օպերատորն անցկացնում է հայտի վերիֆիկացում, եւ եթե այն բարեհաջող է անցնում, ապա կատարում է սերտիֆիկատի գործողության կասեցման հարցման ձեւավորում եւ ստորագրում է այն իր ԷԹՍ-ով։ Հանձնաժողովի ՀԿ-ի լիազորված անձը ԳԿ-ի օպերատորի ԷԹՍ-ով ստորագրված սերտիֆիկատի գործողության կասեցման հարցման հիման վրա կասեցնում է սերտիֆիկատի գործողությունը։ Սերտիֆիկատի գործողությունը կասեցնելուց հետո այն տիրապետողը ծանուցվում է դրա մասին, իսկ Հանձնաժողովի ՀԿ-ն հրապարակում է սերտիֆիկատի գործողության կասեցման մասին տեղեկատվություն պարունակող ՀՍՑ-ն։

Սերտիֆիկատի գործողության կասեցման հայտն ուսումնասիրվում է այն ներկայացնելու պահից 1 աշխատանքային օրվա ընթացքում։ Հայտի ներկայացման ժամանակ է համարվում՝

էլեկտրոնային փոստով փոխանցման դեպքում՝ ՀԿ-ի փոստային սերվերին հաղորդման փոխանցման ժամանակը.

անձամբ հանձնելու դեպքում կամ այլ եղանակներով փոխանցմամբ՝ ստացման ժամանակը։

4.9.16. Սերտիֆիկատի գործողության կասեցման ժամկետի սահմանափակումը

Չի սահմանվում։

4.9.17. Սերտիֆիկատի գործողության վերականգնման հանգամանքները

Սերտիֆիկատի գործողությունը կարող է վերականգնվել՝

ըստ սերտիֆիկատ տիրապետողի հայտի.

Հանձնաժողովի ՀԿ-ի որոշմամբ։

4.9.18. Սերտիֆիկատի գործողության վերականգնման հայտը

Սերտիֆիկատի գործողության վերականգնման հայտը կարող է ներկայացվել՝

սերտիֆիկատ տիրապետողի կողմից.

Հանձնաժողովի ՀԿ-ի աշխատակցի կողմից, եթե այն տիրապետում է սերտիֆիկատի գործողության վերականգնում պահանջող հավաստի տեղեկատվությամբ, կամ սերտիֆիկատի գործողության հետագա կասեցման կամ հետկանչման համար պատճառների բացակայության մասին տեղեկատվությամբ։

4.9.19. Սերտիֆիկատի գործողության վերականգնման հայտի ուսումնասիրման ընթացակարգը

Սերտիֆիկատի գործողության վերականգնման հայտը կարող է ներկայացվել թղթային կամ էլեկտրոնային ձեւով կամ էլ կապի ցանկացած միջոցների օգտագործմամբ, սակայն ցանկացած դեպքում սույն կանոնակարգի 3.4 ենթաբաժնի համաձայն աուտենտիֆիկացմամբ։

Ցանկացած դեպքում սերտիֆիկատի գործողության վերականգնման հայտը պետք է պարունակի սերտիֆիկատի սերիական համարը կամ սերտիֆիկատը միանշանակ նույնականացնել թույլ տվող այլ տեղեկատվություն։

Սերտիֆիկատի գործողության վերականգնման հայտն ստանալուց հետո ԳԿ-ի օպերատորը կատարում է հարցման վերիֆիկացում, եւ եթե այն անցնում է բարեհաջող, ապա ձեւովորում է սերտիֆիկատի գործողության վերականգնման հարցում եւ ստորագրում այն իր ԷԹՍ-ով։ Հանձնաժողովի ՀԿ-ի լիազորված անձը ԳԿ-ի օպերատորի ԷԹՍ-ով ստորագրված սերտիֆիկատի գործողության վերականգնման հարցման հիման վրա կատարում է սերտիֆիկատի գործողության վերականգնում։ Սերտիֆիկատի գործողության վերականգնումից հետո այն տիրապետողը ծանուցվում է, իսկ սերտիֆիկատի գործողության կասեցման մասին տեղեկատվություն չպարունակող ՀՍՑ-ն հրապարակվում է։

Սերտիֆիկատի գործողության վերականգնման հայտն ուսումնասիրվում է այն ներկայացնելու պահից 1 աշխատանքային օրվա ընթացքում։ Սերտիֆիկատի գործողության վերականգնման հայտի ներկայացման ժամանակ է համարվում՝

էլեկտրոնային փոստով փոխանցման դեպքում՝ ԳԿ-ի օպերատորի հասցեին հաղորդման ուղարկելու ժամանակը.

անձամբ հանձնելու դեպքում կամ այլ եղանակներով փոխանցմամբ՝ ԳԿ-ի օպերատորի կողմից հայտի ստացման ժամանակը։

4.10. Սերտիֆիկատների կարգավիճակի ստուգման մասով Հանձնաժողովի ՀԿ-ի ծառայությունները

4.10.1. Շահագործման բնութագրերը

Սերտիֆիկատների կարգավիճակը ստուգելու համար Հանձնաժողովի ՀԿ-ն տրամադրում է մուտք ՀՍՑ-ին ՀԿ-ի ռեպոզիտարիայում, ինչպես նաեւ տրամադրում է մուտք OCSP- ծառայությանը։

4.10.2. Ծառայությունների մատչելիությունը

Կազմակերպատեխնիկական համալիր միջոցներով ապահովվում է ՀՍՑ եւ OCSP-ծառայության մատչելիությունը 24x7 ռեժիմով։

ՀՍՑ-ները հրապարակվում են հետեւյալ URL-հասցեներով՝

<http://ca.eecommission.org/share/CAcrlXX.crl>,

<https://ca.eecommission.org/share/CAcrlXX.crl>,

որտեղ XX-ը ՍԿ-ի սերտիֆիկատի տարբերակն է։

4.10.3. Լրացուցիչ հնարավորություններ

Նախատեսված չեն։

4.11. Ծառայություններից օգտվելը դադարեցնելը

Սերտիֆիկատ տիրապետողը կարող է հրաժարվել Հանձնաժողովի ՀԿ-ի ծառայություններից հետեւյալ կերպ՝

հրաժարվելով սերտիֆիկատի թարմացումից դրա գործողության ժամկետը լրանալուն պես.

ներկայացնելով իր սերտիֆիկատի հետկանչման հայտ մինչ գործողության ժամկետի լրանալը՝ առանց նորը տրամադրելու։

4.12. Դեպոնացում եւ բանալիների վերադարձ

Հանձնաժողովի ՀԿ-ն չի իրականացնում դեպոնացում եւ բանալիների վերադարձ։

4.12.1.Դեպոնացման եւ բանալիների վերադարձի մեթոդները եւ քաղաքականությունը

Նախատեսված չէ։

4.12.2. Սեսիոն բանալու ինկապսուլյացիայի եւ վերականգնման մեթոդները եւ քաղաքականությունը

Նախատեսված չէ։

5. Անվտանգության ապահովման կազմակերպական, շահագործման եւ ֆիզիկական միջոցները

Սույն բաժնում նկարագրվում են Հանձնաժողովի ՀԿ-ի տեղեկատվական ռեսուրսների պաշտպանության միջոցները, պաշտպանության միջոցների շահագործման կարգը, ինչպես նաեւ Հանձնաժողովի ՀԿ-ի սպասարկող անձնակազմի գործողությունների կարգը։

5.1. Անվտանգության ապահովման ֆիզիկական միջոցները

Անվտանգության ապահովման ֆիզիկական միջոցները սահմանվում են ոչ բնակելի տարածքների վարձակալության պայմանագրով, որով նախատեսվում է այն շենք մուտք գործելիս պահակակետի առկայությունը, որտեղ գտնվում են վարձակալվող տարածքները։

5.1.1. Հանձնաժողովի ՀԿ-ի բաղադրիչների տեղակայումը եւ դրանց մուտքի կազմակերպումը

Հանձնաժողովի ՀԿ-ի բոլոր բաղադրիչները գտնվում են չթույլատրված մուտքի, գաղտնի տեղեկատվության օգտագործման կամ բացահայտման կանխման եւ որոշման համար սարքավորված՝ սահմանափակ մուտքով մասնագիտացված տարածքներում։

5.1.2. Ֆիզիկական մուտքը

Ֆիզիկական մուտքը Հանձնաժողովի ՀԿ-ի բաղադրիչներին պաշտպանված է առնվազն մուտքի երկու մակարդակներով։ Մուտքի յուրաքանչյուր մակարդակում իրականացվում է մուտքի թույլտվության ստուգում։

Մուտքի հսկողությունը Հանձնաժողովի ՀԿ-ի ծրագրային բաղադրիչներին իրականացվում է երկգործոնային աուտենտիֆիկացման օգտագործմամբ, ներառյալ՝ բանալի-տեղեկատվության ապարատային կրիչների օգտագործումը։

5.1.3. Էլեկտրասնուցումը

Հանձնաժողովի ՀԿ-ի ապարատային ապահովումն ապահովված է դրանց հաստիքային աշխատանքն ապահովող անխափան էլեկտրասնուցման աղբյուրներով։

5.1.4. Լավորակումը եւ խոնավությունը

Տարածքներում լավորակմանը եւ խոնավությանը ներկայացվող պահանջները համապատասխանում են ապարատային ապահովման շահագործման տեխնիկական պայմաններին։

5.1.5. Հրդեհային անվտանգությունը

Հրդեհային անվտանգության միջոցները համապատասխանում են Հանձնաժողովի կացության երկրի հրդեհային անվտանգության մասով ուղեցույց փաստաթղթերի պահանջներին։

5.1.6. Տեղեկատվության կրիչների պահումը

Պահոցային պահմանը ենթակա ամբողջ տեղեկատվությունը պահվում է հատուկ սարքավորված արխիվապահոցում, որին մուտք կարող է գործել անձանց սահմանափակ շրջանակ։

5.1.7. Տեղեկատվության ոչնչացումը

Կարեւոր տեղեկատվություն պարունակող տեղեկատվության բոլոր կրիչները պահման ժամկետի ավարտից հետո ենթակա են ոչնչացման տեղեկատվության կրիչների ֆիզիկական ոչնչացման միջոցով։

ԷԹՍ բանալիները ոչնչացվում են համապատասխան ՏՊԳՄ-ի շահագործման փաստաթղթերում նշված կարգին համապատասխան։

5.1.8. Արտաքին պահոցային պահումը

Նախատեսված չէ։

5.2. Անվտանգության ապահովման գործընթացային միջոցները

5.2.1. Վստահված դերերը

Վստահված դերերը ներկայացված են առնվազն հետեւյալ դերերով՝

ԳԿ-ի օպերատոր.

համակարգային ադմինիստրատոր.

ՀԿ-ի ադմինիստրատոր.

աուդիտի ադմինիստրատոր։

5.2.2. Գործողությունների կատարման համար պահանջվող աշխատակիցների թիվը

Բոլոր աշխատանքները, բացառությամբ Հանձնաժողովի ՀԿ-ի լիազորված անձի բանալիների (ՍԿ-ի, OCSP-ծառայության, TSP-ծառայության բանալիներ) գեներացման, կարող են կատարվել անհատական կարգով եւ չեն պահանջում կոլեգիալություն, եթե այլ բան սահմանված չէ սերտիֆիկատների կիրառման այն քաղաքականությամբ, որին համապատասխան սերտիֆիկատը թողարկվում է։

ՍԿ-ի, OCSP-ծառայության, TSP-ծառայության բանալիների գեներացման համար անհրաժեշտ է Հանձնաժողովի ՀԿ-ի առնվազն երկու աշխատակից։

5.2.3. Նույնականացումը եւ աուտենտիֆիկացումը յուրաքանչյուր դերի համար

Հանձնաժողովի ՀԿ-ի աշխատակցի սկզբնական աուտենտիֆիկացումը եւ նույնականացումն իրականացվում են աշխատանքի ընդունելիս անձը հաստատող ընդունված փաստաթղթերի օգտագործմամբ։ Հանձնաժողովի ՀԿ-ի ծրագրային-ապարատային ապահովմանը մուտքն իրականացվում է ստացված դերին համապատասխան։ Հանձնաժողովի ՀԿ-ի աշխատակցի հետագա աուտենտիֆիկացումը եւ նույնականացումը կատարվում են աուտենտիֆիկացման եւ նույնականացման ծրագրային-ապարատային միջոցների օգտագործմամբ։

5.2.4. Պարտականությունների բաժանում պահանջող դերերը

Աուդիտի ադմինիստրատորի դերը դերերից եւ ոչ մեկի հետ չի կարող միավորվել։

5.3. Անձնակազմի կառավարումը

5.3.1. Որակավորմանը, փորձին եւ գաղտնի նյութերին տրվող մուտքին ներկայացվող պահանջները

Վստահված դերեր կատարող անձնակազմին ներկայացվում են առնվազն հետեւյալ պահանջները՝

լոյալություն.

անվտանգության քաղաքականությունների ըմբռնում եւ պահպանում.

իր պարտավորությունների կատարման համար անհրաժեշտ պատրաստում։

5.3.2. Ընդհանուր պահանջներին համապատասխանության մասով ստուգման ընթացակարգերը

Հանձնաժողովի ՀԿ-ի աշխատակցին վստահված դեր նշանակելիս վերջինս անցնում է ստուգման ընթացակարգ՝ սույն կանոնակարգի 5.3.1 բաժնի պահանջներին համապատասխան։

5.3.3. Մասնագիտական պատրաստմանը ներկայացվող պահանջները

Հանձնաժողովի ՀԿ-ի աշխատակիցների պատրաստման ծրագիրը ներառում է հետեւյալը՝

PKI հայեցակարգը՝ ծառայողական պարտականությունների կատարման համար անհրաժեշտ ծավալներով.

պաշտոնեական պարտականությունները.

Հանձնաժողովի ՀԿ-ի անվտանգության եւ գործունեության քաղաքականությունները եւ ընթացակարգերը.

Հանձնաժողովի ՀԿ-ի ծավալուն ապարատային եւ ծրագրային ապահովման օգտագործումը եւ շահագործումը։

5.3.4. Վերապատրաստմանը ներկայացվող պահանջները եւ դրա հաճախականությունը

Հանձնաժողովի ՀԿ-ի անձնակազմի վերապատրաստումն իրականացվում է Հանձնաժողովի ՀԿ-ի աշխատակիցների կողմից իրենց որակավորման պահպանման եւ կատարելագործման ու գործառութային պարտականությունների բարեհաջող կատարման համար անհրաժեշտ ծավալներով եւ հաճախականությամբ։

5.3.5. Կադրային տեղափոխությունների հաճախականությունը եւ հաջորդականությունը

Պայմաններ չկան։

5.3.6. Անիրավազոր գործողությունների համար սանկցիաները

Հանձնաժողովի ՀԿ-ի անձնակազմի ցանկացած անիրավազոր գործողություն հանգեցնում է սանկցիաների՝ Հանձնաժողովի ՀԿ-ի կացության երկրի գործող օրենսդրությանը համապատասխան։

Սերտիֆիկատ տիրապետողի ցանկացած անիրավազոր գործողություն կարող է պատժվել Հանձնաժողովի ՀԿ-ի հետ համաձայնագրի անհապաղ լուծմամբ, այդ թվում՝ սերտիֆիկատի հետկանչմամբ, ինչպես նաեւ հետապնդվել Հանձնաժողովի ՀԿ-ի կացության երկրի օրենսդրությանը համապատասխան։

5.3.7. Պահանջներ՝ անկախ կապալառուների համար

Վստահված դերեր կատարող, սակայն Հանձնաժողովի ՀԿ-ի աշխատակից չհամարվող բոլոր անձանց նկատմամբ ներկայացվում են նույն պահանջները, ինչ Հանձնաժողովի ՀԿ-ի աշխատակիցների նկատմամբ։

5.3.8. Անձնակազմը փաստաթղթերով ապահովելը

Հանձնաժողովի ՀԿ-ն ապահովում է իր անձնակազմն անհրաժեշտ փաստաթղթերով՝ վերջիններիս պաշտոնեական պարտականությունների բարեհաջող կատարման համար։

5.4. Իրադարձությունների գրանցման ընթացակարգերը

5.4.1. Գրանցվող իրադարձությունների տիպերը

Գրանցման ենթակա են իրադարձությունների հետեւյալ տիպերը՝

Հանձնաժողովի ՀԿ-ի բանալիների կենսական ցիկլի իրադարձությունները, ներառյալ՝ գեներացումը, պահեստային պատճենումը, վերականգնումը, արխիվացումը եւ ոչնչացումը.

սերտիֆիկատների կենսական ցիկլի իրադարձությունները, ներառյալ՝

սերտիֆիկատների թողարկման, գործողության կասեցման, գործողության վերականգնման, հետկանչման հայտերը ներկայացնելը, բանալիների թարմացման հայտերը ներկայացնելը, հայտերի տվյալների մշակման արդյունքները.

սերտիֆիկատների եւ ՀՍՑ-ների թողարկումը.

անվտանգության վրա ազդող իրադարձությունները.

որեւէ գործողություն կատարելու բոլոր անհաջող փորձերը.

որեւէ կերպ Հանձնաժողովի ՀԿ-ի բաղադրիչներին մուտքի փորձերը.

Հանձնաժողովի ՀԿ-ի անձնակազմի կողմից իրականացվող գործողությունները.

Հանձնաժողովի ՀԿ-ի ծրագրային-ապարատային ապահովման վթարները եւ այլ անկանոնություններ.

Հանձնաժողովի ՀԿ-ի անձնակազմի՝ Հանձնաժողովի ՀԿ-ի բաղադրիչներին մուտքի պրոֆիլների փոփոխությունը.

միջցանցային էկրանների գործունեությունը։

Իրադարձության գրանցման մասին գրառումը պետք է պարունակի հետեւյալ տեղեկատվությունը՝

իրադարձության ամսաթիվը եւ ժամը.

գրառման հեղինակը.

իրադարձության տիպը։

5.4.2. Իրադարձությունների գրանցման մատյանների մշակման հաճախականությունը

Իրադարձությունների գրանցման մատյանների ֆայլերն ստուգվում եւ արխիվացվում են աուդիտի ադմինիստրատորի կողմից շաբաթն առնվազն երկու անգամ։ Իրադարձությունների գրանցման մատյանները նույնպես ստուգվում են կասկածելի կամ արտասովոր ակտիվության դեպքերում, ինչպես նաեւ կրիտիկական իրավիճակների առաջացման դեպքում։ Իրադարձությունների գրանցման մատյանների մշակումը պետք է ներառի իրադարձությունների ստուգում եւ վերիֆիկացում առ այն, որ գրառումները մատյաններում չեն փոփոխվել կամ կեղծվել։

5.4.3. Իրադարձությունների գրանցման մատյանների պահման ժամկետը

Իրադարձությունների գրանցման մատյանների պահման նվազագույն ժամկետը կազմում է 15 տարի։

5.4.4. Իրադարձությունների գրանցման մատյանների պաշտպանությունը

Իրադարձությունների գրանցման մատյաններին մուտք կարող են գործել՝

համակարգային ադմինիստրատորը,

ՀԿ-ի ադմինիստրատորը,

աուդիտի ադմինիստրատորը։

Իրադարձությունների գրանցման մատյանները պաշտպանվում են չթույլատրված մուտքից, ձեւափոխությունից, փոփոխությունից կամ հեռացումից իրադարձությունների գրանցման համակարգով։

5.4.5. Իրադարձությունների գրանցման մատյանների պահեստային պատճենման ընթացակարգերը

Իրադարձությունների գրանցման մատյանների պահեստային պատճենումն իրականացվում է պահեստային պատճենման ընդհանուր ընթացակարգերին համապատասխան։

5.4.6. Իրադարձությունների գրանցման համակարգը

Ավտոմատ կերպով գրանցվող իրադարձությունների մասին տվյալները գրառվում են հավելվածներով եւ օպերացիոն համակարգերով։ Ձեռքով գրանցվող իրադարձությունների մասին տվյալները գրառվում են Հանձնաժողովի ՀԿ-ի անձնակազմի կողմից։

5.4.7. Իրադարձության պատճառ հանդիսացած սուբյեկտի տեղեկացումը

Չի կատարվում։

5.4.8. Խոցելիության գնահատումը

Համակարգերի խոցելիության գնահատումը կատարվում է իրադարձությունների գրանցման մատյանների մշակման անցկացման ընթացքում։

5.5. Պահոցային գրառումներ

5.5.1. Արխիվացվող տեղեկատվության կազմը

Պարտադիր պահոցային պահմանը ենթակա է՝

սերտիֆիկատների թողարկման, հետկանչման, գործողության կասեցման եւ գործողության վերականգնման հայտերը, ուղեկցող տեղեկատվությունը.

ԷԹՍ բանալիների պատրաստման հայտերը.

թողարկված սերտիֆիկատները.

իրադարձությունների գրանցման մատյանները.

թողարկված ՀՍՑ-ների ռեեստրը.

Հանձնաժողովի ՀԿ-ի փաստաթղթերը.

Հանձնաժողովի ՀԿ-ի ներքին եւ արտաքին նամակագրությունը։

5.5.2. Պահոցային տեղեկատվության պահման ժամկետը

5.5.1 ենթակետում նշված տեղեկատվությունը պահվում է Հանձնաժողովի ՀԿ-ի գործունեության ժամկետի ամբողջ ընթացքում, սակայն 15 տարուց ոչ պակաս։ Հանձնաժողովի ՀԿ-ի գործունեության դադարեցման դեպքում մինչ տեղեկատվության պահման ժամկետները լրանալը նշված տեղեկատվությունը փոխանցվում է պահման փաստաթղթերի պահոցային պահում իրականացնող Հանձնաժողովի ենթաբաժին։

Պահման ժամկետն ավարտվելուց հետո տեղեկատվությունը ոչնչացվում է տեղեկատվության կրիչների ֆիզիկական ոչնչացման միջոցով։ Պահոցային փաստաթղթերի՝ ոչնչացման համար առանձնացումը եւ ոչնչացումն իրականացվում են Հանձնաժողովի ՀԿ-ի աշխատակիցներից ձեւավորվող եւ Հանձնաժողովի ՀԿ-ի ղեկավարի կարգադրությամբ նշանակվող մշտապես գործող հանձնաժողովի կողմից։

5.5.3. Պահոցի պաշտպանությունը

Պահոցային փաստաթղթերը եւ տեղեկատվությունն օտարելի կրիչների վրա պահվում են հատուկ սարքավորված տարածքում՝ Հանձնաժողովի ակտերով սահմանվող պահոցային փաստաթղթերի պահման ռեժիմն ապահովող արխիվապահոցում։ Պահոցային տեղեկատվության՝ ձեւափոխությունից, հեռացումից եւ հրապարակումից պաշտպանությունն իրականացվում է մուտքի սահմանափակման մեթոդներով եւ միջոցներով։

5.5.4. Պահոցի պահեստային պատճենման ընթացակարգը

Պայմաններ չկան։

5.5.5. Պահոցային գրառումների ժամանակի դրոշմին ներկայացվող պահանջները

Նախատեսված չէ։

5.5.6. Պահոցային պահման համակարգը

Կիրառվում է Հանձնաժողովի պահոցային պահման ներքին համակարգը։

5.5.7. Պահոցային տեղեկատվության ստացման եւ վերիֆիկացման ընթացակարգը

Մուտքը պահոցին թույլատրվում է միայն վստահված դեր ունեցող Հանձնաժողովի ՀԿ-ի աշխատակիցներին։ Այլ սուբյեկտների համար մուտքը թույլատրվում է միայն Հանձնաժողովի ՀԿ-ի ղեկավարի որոշմամբ։ Տեղեկատվություն ստանալիս կատարվում է դրա ամբողջականության հսկողություն։

5.6. Բանալիների փոխարինումը

Հանձնաժողովի ՀԿ-ն Հանձնաժողովի ՀԿ-ի բաղադրիչների բանալու զույգի պլանային թարմացման դեպքում պետք է իրականացնի տվյալ ընթացակարգն առանց համակարգի աշխատունակության խախտման եւ սերտիֆիկատներից օգտվողների եւ սերտիֆիկատներ տիրապետողների համար թափանցիկ։

5.7. Վերականգնումը կոմպրոմետացիայի եւ վթարի դեպքում

5.7.1. Գործողությունները կոմպրոմետացիայի եւ վթարի դեպքում

ԲԲԵ-ի բոլոր մասնակիցները պետք է տեղեկացվեն Հանձնաժողովի ՀԿ-ի բաղադրիչների (ՍԿ, OCSP-ծառայություն, TSP-ծառայություն) էլեկտրոնային ստորագրության բանալիների կոմպրոմետացիայի դեպքում կամ Հանձնաժողովի ՀԿ-ի հաստիքային աշխատանքի վրա ազդող պատահարների դեպքում։

Կոմպրոմետացիայի դեպքում Հանձնաժողովի ՀԿ-ն ամենասեղմ ժամկետներում անցնում է աշխատանքի՝ նոր բանալու զույգերի օգտագործմամբ։

Հանձնաժողովի ՀԿ-ի որեւէ բաղադրիչների՝ ինչ-ինչ պատճառներով շարքից դուրս գալու դեպքում իրականացվում է դրանց վերականգնումը պահեստային պատճեններից։ Պարտադիր պահեստային պատճենմանը ենթակա է հետեւյալ տեղեկատվությունը՝

հայտերը եւ ուղեկցող տեղեկատվությունը,

թողարկված սերտիֆիկատների ռեեստրը,

իրադարձությունների գրանցման մատյանները։

Հանձնաժողովի ՀԿ-ի բանալիների պահեստային պատճենումն իրականացվում է սույն կանոնակարգի 6.3.4 կետի համաձայն։

5.7.2. Համակարգչային ռեսուրսների, ծրագրային ապահովման եւ (կամ) տվյալների վնասվելը

Համակարգչային ռեսուրսների, ծրագրային ապահովման եւ (կամ) տվյալների վնասվելու (վնասվելու կասկածի) դեպքում Հանձնաժողովի ՀԿ-ն վերականգնում է աշխատունակությունը՝ օգտագործելով պահեստային պատճեններ։

Բոլոր սուբյեկտները, որոնց վրա անդրադառնում է տեղի ունեցած վթարը կամ խափանումը, անհապաղ տեղեկացվում են։ Վերականգնման ավարտից հետո բոլոր սուբյեկտները, ում շահերի վրա ազդել է վթարը կամ խափանումը, տեղեկացվում են վերականգնման մասին։

5.7.3. Վերականգնման ընթացակարգը Հանձնաժողովի ՀԿ-ի լիազորված անձի էլեկտրոնային ստորագրության բանալու կոմպրոմետացիայի դեպքում

Հանձնաժողովի ՀԿ-ի լիազորված անձի էլեկտրոնային ստորագրության բանալու կոմպրոմետացիայի դեպքում իրականացվում է վերջինիս սերտիֆիկատի հետկանչում, ինչպես նաեւ ԲԲԵ բոլոր սուբյեկտների տեղեկացում կոմպրոմետացիայի մասին մատչելի մեթոդներով։

Բանալիների կոմպրոմետացիայի դեպքում սերտիֆիկատներ տիրապետողները պարտավոր են անհապաղ տեղեկացնել Հանձնաժողովի ՀԿ-ին կոմպրոմետացիայի փաստի մասին։ Հանձնաժողովի ՀԿ-ն իրականացնում է նման սերտիֆիկատների հետկանչումը՝ սույն կանոնակարգի 4.9.3 բաժնում նշված կարգին համապատասխան։

5.7.4. Աղետներից հետո աշխատանքի անընդհատության հնարավորությունը

Աղետներից հետո աշխատանքի անընդհատությունն ապահովվում է Հանձնաժողովի ՀԿ-ի բաղադրիչների աշխատունակության վերականգնման կանոնակարգում նշված միջոցներով։

5.8. Հանձնաժողովի ՀԿ-ի գործունեության դադարեցումը

Հանձնաժողովի ՀԿ-ի գործունեությունը դադարում է Հանձնաժողովի հավաստագրման կենտրոնի մասին դրույթով նախատեսված կարգին համապատասխան։ Դրանից բացի, Հանձնաժողովի ՀԿ-ն տեղեկացնում է բոլոր սերտիֆիկատներ տիրապետողներին եւ սերտիֆիկատներից օգտվողներին իր գործունեության դադարեցման մասին։

6. Անվտանգության ապահովման տեխնիկական միջոցները

6.1. ԷԹՍ միջոցներին ներկայացվող պահանջները

Սերտիֆիկատներ տիրապետողները պետք է օգտագործեն Հանձնաժողովի խորհրդի կողմից հաստատվող անդրսահմանային տարածության ստեղծմանը, զարգացմանը եւ աշխատանքին ներկայացվող պահանջներում շարադրված ԷԹՍ միջոցներին ներկայացվող պահանջներին համապատասխանող ԷԹՍ միջոցները։ Մինչ նշված միջոցները օգտագործելը դրանց համապատասխանությունը սահմանված պահանջներին պետք է հաստատվի Հանձնաժողովի կացության երկրի լիազորված մարմինների կողմից՝ վերջինիս օրենսդրությամբ սահմանված կարգով։

6.2. Բանալու զույգի գեներացումը եւ ինստալյացիան

6.2.1. Բանալու զույգերի գեներացումը

Հանձնաժողովի կոլեգիայի անդամի, Հանձնաժողովի պաշտոնատար անձի կամ աշխատակցի անունով սերտիֆիկատների թողարկման դեպքում բանալու զույգերի գեներացումն իրականացվում է ԳԿ-ի օպերատորի ԱԱՎ-ում ՏԳՊՄ ViPNet CSP 4.2-ի կիրառմամբ (կատարման տարբերակ 3)։ Բանալու զույգերը գրառվում են բանալու կրիչների վրա, որոնց նկատմամբ պահանջները բերված են սույն կանոնակարգի 6.3.1 բաժնում։

Ավտոմատացված համակարգերի համար սերտիֆիկատների թողարկման դեպքում բանալու զույգերի գեներացումն իրականացվում է սերտիֆիկատների կիրառման այն քաղաքականությամբ նախատեսված կարգով, որին համապատասխան տվյալ սերտիֆիկատները թողարկվում են։

6.2.2. ԷԹՍ բանալու փոխանցումը սերտիֆիկատ տիրապետողին

ԳԿ-ի օպերատորի ԱԱՎ-ում բանալու զույգի գեներացման դեպքում ԷԹՍ բանալու փոխանցումն իրականացվում է սերտիֆիկատ տիրապետողին բանալու կրիչի փոխանցման միջոցով։ Բանալու կրիչը փոխանցվում է ԷԹՍ բանալու գաղտնիությունը երաշխավորող եղանակով։

6.2.3. Հանձնաժողովի ՀԿ-ում ԷԹՍ ստուգման բանալու փոխանցումը

Պահանջներ չեն ներկայացվում։

6.2.4. Հանձնաժողովի ՀԿ-ի լիազորված անձի ԷԹՍ ստուգման բանալու փոխանցումը

Հանձնաժողովի ՀԿ-ի լիազորված անձի ԷԹՍ ստուգման բանալին առկա է ՍԿ-ի սերտիֆիկատում։ ՍԿ-ի սերտիֆիկատը հրապարակված է ռեպոզիտարիայում հետեւյալ URL-հասցեներով՝

<http://ca.eecommissioii.org/share/CAcertXX.cer>,

<https://ca.eecommission.org/share/CAcertXX.cer>,

որտեղ XX-ը ԳԿ-ի սերտիֆիկատի տարբերակն է։

6.2.5. Բանալիների չափսերը

ԷԹՍ-ի ձեւավորման եւ ստուգման համար օգտագործվող բանալիների երկարությունը՝

ԷԹՍ բանալի՝ 256 բիթ,

ԷԹՍ ստուգման բանալի՝ 512 բիթ (ԳՕՍՏ Ռ 34.10-2012),

Ծածկագրման համար օգտագործվող բանալիների երկարությունը՝

Ծածկագրման համար սեսիոն բանալի ըստ ԳՕՍՏ 28147-89՝ 256 բիթ,

ԷԹՍ բանալի՝ 256 բիթ,

ԷԹՍ ստուգման բանալի՝ 512 բիթ (ԳՈՍՏ Ռ 34.10-2012-ի հիման վրա)։

6.2.6. ԷԹՍ ստուգման եւ որակի ստուգման բանալու պարամետրերի գեներացում

Չի կիրառվում։

6.2.7. Բանալիների օգտագործման նպատակները

Սույն կանոնակարգի 7.1.2 կետին համապատասխան։

6.3. ԷԹՍ բանալու պաշտպանությունը եւ գաղտնագրային մոդուլների տեխնիկական հսկողությունը

6.3.1. Գաղտնագրային մոդուլների ստանդարտները եւ հսկողությունը

ԷԹՍ բանալիների ձեւավորումը կատարվում է կրիչների հետեւյալ տիպերի վրա՝

ViPNet CSP 4.2-ով օժանդակվող կրիչների տիպեր (ֆորմուլյար FRKE.00106-03 30 01 FO).

ViPNet HSM ծրագրային-ապարատային համալիր գաղտնագրային մոդուլ (ֆորմուլյար FRKE.00127-01 30 01 FO)։

Բանալիների պահման համար օտարելի կրիչի օգտագործմամբ համակարգչի վրա ԷԹՍ բանալիների պատճենների ստեղծումն անթույլատրելի է։

6.3.2. ԷԹՍ բանալու հսկողությունը մի քանի անձանց կողմից

ԷԹՍ բանալու հսկողությունը մի քանի անձանց կողմից թույլատրելի է միայն ViPNet HSM ծրագրային-ապարատային համալիր գաղտնագրային մոդուլում ԷԹՍ բանալու պահման դեպքում։

6.3.3. ԷԹՍ բանալու դեպոնացումը

ԷԹՍ բանալու դեպոնացումն անթույլատրելի է։

6.3.4. ԷԹՍ բանալու պահեստային պատճենը

Հանձնաժողովի ՀԿ-ի բաղադրիչների ԷԹՍ բանալիների պահեստային պատճենումը եւ պահեստային պատճենների պահումն իրականացվում է բանալիավորի կրիչի մակարդակից ոչ պակաս պաշտպանվածության մակարդակ ապահովող մեթոդների եւ միջոցների օգտագործմամբ։

6.3.5. ԷԹՍ բանալու արխիվացումը

Հանձնաժողովի ՀԿ-ն չի իրականացնում ԷԹՍ բանալիների պահոցային պահում։

6.3.6. Գաղտնագրային մոդուլից եւ գաղտնագրային մոդուլ ԷԹՍ բանալու տեղափոխումը

Սերտիֆիկատների, OCSP-ծառայության անդորրագրերի ստորագրման համար օգտագործվող՝ ՀԿ-ի լիազորված անձի ԷԹՍ բանալիների գեներացումը տեղի է ունենում անմիջապես ViPNet HSM ծրագրային-ապարատային համալիր գաղտնագրային մոդուլում (կատարման տարբերակ 1)։ Սերտիֆիկատների ստորագրման համար օգտագործվող՝ ՀԿ-ի լիազորված անձի ԷԹՍ բանալու տեղափոխումը գաղտնագրային մոդուլից իրականացվում է բանալու պահեստային պատճենման ընթացքում գաղտնագրային մոդուլի մասով շահագործման փաստաթղթերով նախատեսված կարգով։ Լիազորված անձի ԷԹՍ բանալիների տեղափոխման գործընթացը պետք է վերահսկվի Հանձնաժողովի ՀԿ-ի առնվազն երկու աշխատակիցների կողմից։

Հանձնաժողովի ՀԿ-ի լիազորված անձի ԷԹՍ բանալու պահեստային պատճենի միանձնյա պահում չի թույլատրվում։ Հանձնաժողովի ՀԿ-ի ԷԹՍ բանալու պահեստային բանալու պահումն իրականացվում է բանալին (գաղտնիքը) երկուսը երեքից սխեմայով բաժանման եղանակով։ Հանձնաժողովի ՀԿ-ի ԷԹՍ պահեստային բանալու (գաղտնիքի) առանձին մասերի պահման համար պատասխանատուներն են՝

համակարգային ադմինիստրատորը,

ՀԿ-ի ադմինիստրատորը,

աուդիտի ադմինիստրատորը։

6.3.7. ԷԹՍ բանալիների պահումը գաղտնագրային մոդուլում

Սերտիֆիկատների եւ OCSP-ծառայության անդորրագրերի ստորագրման համար օգտագործվող՝ Հանձնաժողովի ՀԿ-ի լիազորված անձի ԷԹՍ բանալիները պահվում են գաղտնագրային մոդուլում ծածկագրված տեսքով։

6.3.8. ԷԹՍ բանալու ակտիվացման մեթոդը

ԷԹՍ բանալու ակտիվացումն իրականացվում է միայն այն տիրապետողի կողմից։

ԷԹՍ բանալու ակտիվացման համար պետք է օգտագործվեն սույն կանոնակարգի 6.5 ենթաբաժնի պահանջները բավարարող ակտիվացման տվյալները։ ԷԹՍ բանալու ակտիվացումը պետք է կատարվի սահմանափակ ժամանակահատվածով։

6.3.9. ԷԹՍ բանալու ապաակտիվացման մեթոդը

ԷԹՍ բանալու ապաակտիվացումը կատարվում է կա՛մ ավտոմատ կերպով, կա՛մ բանալու կրիչի անջատման միջոցով։

6.3.10. ԷԹՍ բանալու ոչնչացման մեթոդը

Գործողության կամ պահոցային պահման (եթե դա իրականացվում է) ժամկետն ավարտվելուց հետո ԷԹՍ-ն ոչնչացվում է դրա վերականգնման անհնարինությունը երաշխավորող մեթոդներով։

6.3.11. Գաղտնագրային մոդուլների գնահատումը

Տե՛ս բաժին 6.2.1

6.4. Բանալու զույգերի կառավարման այլ ասպեկտներ

6.4.1. ԷԹՍ ստուգման բանալու արխիվացումը

ԷԹՍ ստուգման բանալին արխիվացվում է սերտիֆիկատի կազմում սույն կանոնակարգի 5.5 ենթաբաժնին համապատասխան։

6.4.2. Սերտիֆիկատի գործողության եւ բանալու զույգի օգտագործման ժամկետները

ԷԹՍ բանալիների գործողության ժամկետը կազմում է՝

Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների՝ 1 տարուց ոչ ավելի,

ՍԿ-ի՝ 3 տարուց ոչ ավելի (դրանցից 15 ամիսը՝ սերտիֆիկատների ստորագրման համար, մնացած ժամանակը՝ միայն ՀՍՑ-ի ստորագրման համար),

OCSP-ծառայության՝ 6 ամսից ոչ ավելի,

TSP-ծառայության՝ 3 ամսից ոչ ավելի։

Սերտիֆիկատների գործողության ժամկետը կազմում է՝

Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների՝ 15 տարուց ոչ ավելի,

ՍԿ-ի՝ 16 տարուց ոչ ավելի,

OCSP-ծառայության՝ 15 տարուց ոչ ավելի,

TSP-ծառայության՝ 15 տարուց ոչ ավելի։

6.5. Ակտիվացման տվյալները

6.5.1. Ակտիվացման տվյալների գեներացումը եւ ինստալյացիան

Ակտիվացման տվյալներն օգտագործվում են բանալու կրիչների պաշտպանության համար։ Ակտիվացման տվյալներն ստեղծվում են բանալու զույգի գեներացումից առաջ։ Հանձնաժողովի ՀԿ-ն կարող է չիրականացնել ակտիվացման տվյալների ստեղծում հայտատուների համար։

Որպես ակտիվացման տվյալներ կարող են օգտագործվել՝

ծածկագիր, PIN,

կենսաչափական տեղեկատվություն,

խիստ երկգործոնային աուտենտիֆիկացման համակարգեր։

Սերտիֆիկատների կիրառման բոլոր քաղաքականությունների համար ծածկագիրը (PIN) պետք է բավարարի հետեւյալ նվազագույն պահանջները՝

հայտնի լինի միայն սերտիֆիկատ տիրապետողին,

երկարությունը՝ առնվազն 8 նիշ,

այբուբենի հզորությունը՝ առնվազն 10 նիշ,

չպետք է պարունակի բառեր, բառակապակցություններ, անուններ եւ այլն։

Սերտիֆիկատների կիրառման քաղաքականություններում կարող են սահմանվել լրացուցիչ պահանջներ ակտիվացման տվյալների նկատմամբ։

6.5.2. Ակտիվացման տվյալների պաշտպանությունը

Ակտիվացման տվյալները պետք է պաշտպանված լինեն կորստից, փչանալուց, չթույլատրված օգտագործումից կամ բացահայտումից։

6.5.3. Ակտիվացման տվյալներին վերաբերող այլ ասպեկտներ

Ակտիվացման տվյալների փոխանցումը կամ ոչնչացումը պետք է իրականացվի կորստի, գողության, հրապարակման, փչացման, ձեւափոխության կամ չթույլատրված օգտագործման անհնարինությունն ապահովող մեթոդներով։

6.6. Հաշվողական տեխնիկայի անվտանգության կառավարման միջոցները

6.6.1. Հաշվողական տեխնիկայի անվտանգության մասով հատուկ տեխնիկական պահանջները

Օգտագործվող հաշվողական տեխնիկան ապահովում է Հանձնաժողովի ՀԿ-ի տվյալների եւ ԷԹՍ բանալիների պահպանվածությունը եւ պաշտպանությունը ոչնչացումից, փչացումից, ձեւափոխությունից, հրապարակումից կամ չթույլատրված օգտագործումից։

6.6.2. Հաշվողական տեխնիկայի անվտանգության գնահատումը

Հանձնաժողովի ՀԿ-ի ավտոմատացված համակարգն ատեստավորված է չհաստատված մուտքից տեղեկատվության պաշտպանվածության պահանջներին համապատասխանության մասով։

6.7. Կյանքի ցիկլի կառավարման տեխնիկական միջոցները

6.7.1. Համակարգի մշակման կառավարման միջոցները

Պայմաններ չկան։

6.7.2. Անվտանգության կազմակերպման կառավարման միջոցները

Հանձնաժողովի ՀԿ-ն օգտագործում է օգտագործվող համակարգերի անվտանգ կոնֆիգուրացիայի եւ ամբողջականության ստուգման մեխանիզմներ։

6.7.3. Կյանքի ցիկլի անվտանգության կառավարման միջոցները

Պայմաններ չկան։

6.8. Ցանցային անվտանգության կառավարման միջոցները

Հանձնաժողովի ՀԿ-ն օգտագործում է տեղեկատվությանը չթույլատրված մուտքը կանխող եւ հարձակումներից պաշտպանող ցանցային անվտանգության միջոցներ։

6.9. Ժամանակի նշաններ

Սերտիֆիկատները եւ ՀՍՑ-ն պարունակում են տեղեկատվություն ամսաթվի եւ ժամի մասին։ Հանձնաժողովի ՀԿ-ն միաժամանակեցնում է բոլոր ծրագրային եւ տեխնիկական միջոցները՝ ըստ ԳԼՕՆԱԱՀ-ի ճշգրիտ ժամի ազդանշանների։

7. Սերտիֆիկատների, ՀՍՑ, OCSP-պատասխանների եւ TSP- պատասխանների կառուցվածքը

7.1. Սերտիֆիկատի կառուցվածքը

Սերտիֆիկատների կառուցվածքը համապատասխանում է Հանձնաժողովի կողմից հաստատվող էլեկտրոնային թվային ստորագրության ստուգման բանալիների սերտիֆիկատներին ներկայացվող պահանջներին։

Բոլոր թողարկվող սերտիֆիկատները պարունակում են հետեւյալ բազային դաշտերը՝

Serial Number՝ Հանձնաժողովի ՀԿ-ի սերտիֆիկատների ռեեստրում սերտիֆիկատի եզակի սերիական (գրանցման) համարը,

Signature Algorithm՝ սերտիֆիկատի ստորագրման համար օգտագործվող ալգորիթմի օբյեկտային նույնականացուցիչը,

Issuer՝ Հանձնաժողովի ՀԿ-ի ՍԿ-ի տարբերակիչ անունը,

Valid From՝ սերտիֆիկատի գործողության սկզբի ամսաթիվը,

Valid То՝ սերտիֆիկատի գործողության ավարտի ամսաթիվը,

Subject՝ սերտիֆիկատ տիրապետողի կամ Հանձնաժողովի ավտոմատացված համակարգի նույնականացման տվյալները,

Subject Public Key՝ սերտիֆիկատ տիրապետողի կամ Հանձնաժողովի ավտոմատացված համակարգի ԷԹՍ ստուգման բանալին,

Version՝ Х.509 ձեւաչափի սերտիֆիկատի կառուցվածքի տարբերակը,

Signature՝ Հանձնաժողովի ՀԿ-ի լիազորված անձի ԷԹՍ-ն։

7.1.1. Տարբերակի համարը

Թողարկվող սերտիֆիկատների տարբերակը ցածր չէ 3-ից։

7.1.2. Սերտիֆիկատի ընդլայնումները

Թողարկվող սերտիֆիկատներում կարող են օգտագործվել միայն տվյալ բաժնում թվարկված ընդլայնումները։ Այն դեպքում, երբ թվարկված ընդլայնումների որեւէ դաշտի (դրոշի) արժեքը սահմանված չէ սույն կանոնակարգով, Հանձնաժողովի ՀԿ-ն իրավասու է որոշել թողարկվող սերտիֆիկատների համար տվյալ դաշտի արժեքը` Х.509 եւ RFC 5280 պահանջներին համապատասխան։

Authority Key Identifier

Տվյալ ընդլայնումը պարտադիր է բոլոր սերտիֆիկատների համար` բացառությամբ (Հանձնաժողովի ՀԿ-ի ՍԿ-ի սերտիֆիկատների) ինքնաստորագրվածների, եւ կրիտիկական չէ։ Այս ընդլայնումը պետք է պարտադիր կերպով պարունակի keyldentifier դաշտը, որում առկա է Հանձնաժողովի ՀԿ-ի ՍԿ-ի ԷԹՍ ստուգման բանալու նույնականացուցիչը։ Մնացած դաշտերը պարտադիր չեն։

Subject Key Identifier

Տվյալ ընդլայնումը պետք է առկա լինի բոլոր սերտիֆիկատներում, լինի ոչ կրիտիկական եւ պարունակի սերտիֆիկատ տիրապետողի կամ Հանձնաժողովի ավտոմատացված համակարգի ԷԹՍ ստուգման բանալու նույնականացուցիչը։

KeyUsage

Տվյալ ընդլայնումը պետք է առկա լինի բոլոր սերտիֆիկատներում եւ լինի կրիտիկական։

KeyUsage ընդլայնման դաշտերի արժեքը՝

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Բիթային դիմակի տեղաշարժը | Դաշտը | ՀԿ-ի լիազորված անձի սերտիֆիկատը | OCSP- ծառայության եւ TSP- ծառայության սերտիֆիկատները | Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների սերտիֆիկատները | Նկարագրությունը |
| 0 | digital Signature | 0 | 0/1 | 0/1 | ԷԹՍ |
| 1 | nonRepudiation | 0 | 0/1 | 0/1 | Հեղինակությունից չհրաժարվելը |
| 2 | keyEncipherment | 0 | 0/1 | 0/1 | Բանալիների ծածկագրում |
| 3 | dataEnciphennent | 0 | 0/1 | 0/1 | Տվյալների ծածկագրում |
| 4 | keyAgreement | 0 | 0/1 | 0/1 | Բանալիների համաձայնեցում |
| 5 | keyCertSign | 1 | 0 | 0 | Սերտիֆիկատների ԷԹՍ |
| 6 | CRLSign | 1 | 0 | 0 | ՀՍՑ-ի ԷԹՍ |
| 7 | encipherOnly | 0 | 0/1 | 0/1 | Ծածկագրում |
| 8 | decipherOnly | 0 | 0/1 | 0/1 | Վերծանում |

Certificate Policies

Տվյալ ընդլայնումը պետք է առկա լինի Հանձնաժողովի ՀԿ-ի կողմից թողարկված յուրաքանչյուր սերտիֆիկատում, պարունակի սերտիֆիկատների կիրառման այն քաղաքականության օբյեկտային նույնականացուցիչը, որին համապատասխան տվյալ սերտիֆիկատը տրվել է։ Սերտիֆիկատների կիրառման քաղաքականությունների նույնականացուցիչներն օգտագործվում են սույն կանոնակարգի 7.1.6 եւ 7.1.7 բաժիններին համապատասխան։ Ընդլայնումը կրիտիկական չէ։

Basic Constraints

Ընդլայնումը պետք է առկա լինի Հանձնաժողովի ՀԿ-ի ՍԿ-ի սերտիֆիկատում եւ կրիտիկական է։ сА դրոշի արժեքը սահմանված է 1 (true)։ Հանձնաժողովի ՀԿ-ի ՍԿ-ի սերտիֆիկատի ընդլայնումը նույնպես պարունակում է pathLenConstraint դաշտը, որի արժեքը սահմանված է 0 (զրո)։

Name Constraints

Օգտագործվում է սույն կանոնակարգի 3.1 բաժնին համապատասխան։

Policy Constraints

Օգտագործվում է սույն կանոնակարգի 7.1.7 բաժնին համապատասխան։

CRL Distribution Points

Տվյալ ընդլայնումը պետք է առկա լինի Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց, աշխատակիցների եւ Հանձնաժողովի ավտոմատացված համակարգերի բոլոր սերտիֆիկատներում, լինի ոչ կրիտիկական եւ պարունակի ՀՍՑ տարածման կետերի ցանկը։ ՀՍՑ տարածման կետերի ցանկը բերված է սույն կանոնակարգի 4.10.2 բաժնում։

Authority Information Access

Ընդլայնումը պետք է առկա լինի բոլոր սերտիֆիկատներում, լինի ոչ կրիտիկական եւ պարունակի Հանձնաժողովի ՀԿ-ի ՍԿ-ի սերտիֆիկատի հրապարակման կետի URL-հասցեն՝ սույն կանոնակարգի 6.2.4 բաժնին համապատասխան, եւ Հանձնաժողովի ՀԿ-ի OCSP-ծառայության URL-հասցեն՝ սույն կանոնակարգի 4.9.9 բաժնին համապատասխան։

Extended Key Usage

Տվյալ ընդլայնումն առկա է սերտիֆիկատներում եւ կրիտիկական չէ։

Ընդլայնումը պարունակում է սերտիֆիկատների կիրառման այն քաղաքականությամբ նախատեսված սերտիֆիկատների օգտագործման ոլորտների օբյեկտային նույնականացուցիչներ, որին համապատասխան սերտիֆիկատը թողարկվել է։

7.1.3. Գաղտնագրային ալգորիթմների օբյեկտային նույնականացուցիչները

ԲԲԵ բոլոր մասնակիցները պետք է իրենց աշխատանքում օգտագործեն RFC 3279, RFC 7091 համապատասխանող օբյեկտային նույնականացուցիչներով գաղտնագրային ալգորիթմներ։

7.1.4. Անունների ձեւերը

Սերտիֆիկատում Հանձնաժողովի ՀԿ-ի լիազորված անձի եւ սերտիֆիկատ տիրապետողի նույնականացման տվյալների դաշտերը պարունակում են Х.500 ձեւաչափի անվան ատրիբուտներ։

7.1.5. Անունների սահմանափակումները

ՀԿ-ի լիազորված անձի նույնականացման տվյալների դաշտի պարտադիր ատրիբուտներն են՝

Common Name՝ Հանձնաժողովի ՀԿ-ի ՍԿ-ի կեղծանուն,

Organization՝ Եվրասիական տնտեսական հանձնաժողով,

Organization Unit՝ Եվրասիական տնտեսական հանձնաժողովի ՀԿ,

Country՝ Հանձնաժողովի կացության երկրի տառային ծածկագիր (օրինակ՝ RU),

Email - ca-info@cccommission.org։

Սերտիֆիկատ տիրապետողի նույնականացման տվյալների դաշտի պարտադիր ատրիբուտները սահմանվում են սերտիֆիկատների կիրառման քաղաքականությամբ, որին համապատասխան սերտիֆիկատը թողարկվում է։

7.1.6. Սերտիֆիկատների կիրառման կիրառվող քաղաքականությունների օբյեկտային նույնականացուցիչները

Սերտիֆիկատների կիրառման քաղաքականությունների օբյեկտային նույնականացուցիչները թվարկված են սույն կանոնակարգի թիվ 2 հավելվածում։ ՀԿ-ի լիազորված անձի սերտիֆիկատում կարող է օգտագործվել սերտիֆիկատների կիրառման ցանկացած քաղաքականություն նշանակող OID 2.5.29.32.0։

7.1.7. Policy Constraints ընդլայնման օգտագործումը

Պայմաններ չկան։

7.1.8. Քաղաքականության որակավորիչների նշանակությունը եւ շարահյուսությունը

Պայմաններ չկան։

7.1.9. Certificate Policies կրիտիկական ընդլայնման նշանակության մշակումը

Պայմաններ չկան։

7.2. Հետ կանչված սերտիֆիկատների ցանկերի կառուցվածքը

ՀՍՑ-ի կառուցվածքը պետք է համապատասխանի RFC 5280 "Internet Х.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"-ին։

ՀՍՑ-ն պարունակում է հետեւյալ հիմնական դաշտերը՝

Version՝ Х.509 ձեւաչափի ՀՍՑ կառուցվածքի տարբերակը,

Signature Algorithm՝ ՀՍՑ-ի ստորագրման համար օգտագործվող ալգորիթմի օբյեկտային նույնականացուցիչը,

Signature՝ Հանձնաժողովի ՀԿ-ի լիազորված անձի ԷԹՍ։

Issuer – Հանձնաժողովի ՀԿ-ի ՍԿ-ի տարբերակիչ անունը,

This Update՝ ընթացիկ ՀՍՑ-ի թողարկման ամսաթիվը եւ ժամը,

Next Update՝ հաջորդ ՀՍՑ-ի պլանային թողարկման ամսաթիվը եւ ժամը,

Next Publication՝ ՀՍՑ-ի պլանային հրապարակման ամսաթիվը եւ ժամը,

Revoked Certificates՝ սերտիֆիկատի սերիական համարը եւ հետկանչման ամսաթիվը ներառող՝ չեղարկված (հետ կանչված) սերտիֆիկատների ցանկը։ Տվյալ դաշտը կարող է բացակայել, եթե հետ կանչված սերտիֆիկատներ չկան։

7.2.1. Տարբերակի համարը

2-րդ տարբերակի բոլոր թողարկվող ՀՍՑ-ները։

7.2.2. ՀՍՑ եւ ՀՍՑ տարրերի Authority Key Identifier ընդլայնումները

ՀԿ-ի լիազորված անձի բանալու նույնականացուցիչը, որով ստորագրվել է տվյալ ՀՍՑ-ն։

CRL Number

ՀՍՑ-ի հերթական համար պարունակող ոչ կրիտիկական առաջարկվող ընդլայնում։

Reason Code

Սերտիֆիկատի հետկանչման պատճառ պարունակող ՀՍՑ տարրի ոչ կրիտիկական առաջարկվող ընդլայնումը։

Invalidity Date չի կիրառվում։

7.3. OCSP-պատասխանի կառուցվածքը

OCSP-ծառայության բոլոր պատասխանները (OCSP-պատասխանները) պարունակում են հետեւյալ դաշտերը՝

Version՝ OCSP-պատասխանի կառուցվածքի տարբերակը,

Status՝ OCSP-պատասխանի կարգավիճակը,

Signature algorithm՝ OCSP-պատասխանի ստորագրման համար օգտագործվող ալգորիթմի օբյեկտային նույնականացուցիչը,

HasNonce՝ OCSP-պատասխանի նույնականացուցչի առկայության ցուցիչը,

id-pkix-ocsp-nonce՝ OCSP-պատասխանի նույնականացուցիչը,

ProducedAt՝ OCSP- ծառայության կողմից OCSP-պատասխանի ստորագրման ամսաթիվը եւ ժամը,

Extensions՝ չի կիրառվում,

Certificate of signer of OCSP response՝ OCSP–ծառայության սերտիֆիկատ տիրապետողի (Հանձնաժողովի ՀԿ-ի լիազորված անձի) նույնականացման տվյալները,

Verification of certificate of signer of OCSP response՝ OCSP-ծառայության սերտիֆիկատի ստուգման արդյունքը,

Verification of OCSP response՝ OCSP - ծառայության ԷԹՍ ստուգման արդյունքը։

Single responses՝ հարցման մեջ ստուգվող սերտիֆիկատների քանակը, որոնցից յուրաքանչյուրի համար՝

Hash algorithm՝ հեշավորման ալգորիթմի նույնականացուցիչը.

о Serial number՝ սերտիֆիկատի սերիական համարը,

Issuer key hash՝ ՀԿ-ի լիազորված անձի նույնականացման տվյալների հեշը,

Issuer name hash՝ ՀԿ-ի լիազորված անձի ԷԹՍ ստուգման բանալու հեշը,

Certificate status՝ սերտիֆիկատի կարգավիճակի ստուգման արդյունքը,

RevTime՝ սերտիֆիկատի հետկանչման ամսաթիվը եւ ժամը,

RevReason՝ սերտիֆիկատի հետկանչման պատճառը,

ThisUpdate՝ ամսաթիվը եւ ժամը, երբ իրականացվել է սերտիֆիկատի ստուգումը,

NextUpdate՝ ամսաթիվը եւ ժամը, որոնցից ոչ ուշ մատչելի է լինելու սերտիֆիկատի կարգավիճակի մասին տեղեկատվությունը (եթե ամսաթիվը եւ ժամը նշված չեն, ապա տեղեկատվությունը մշտապես մատչելի է),

Archive cutoff՝ չի կիրառվում,

Extensions՝ չի կիրառվում,

Verification of single response՝ OCSP-պատասխանի ստուգման արդյունքը,

Certificates from OCSP response՝ OCSP-ծառայության սերտիֆիկատը։

7.3.1. Տարբերակի համարը

OCSP-պատասխանի կառուցվածքի տարբերակը՝ 1։

7.3.2. OCSP-պատասխանի տիպը

Հանձնաժողովի ՀԿ-ի OCSP-ծառայությունը ձեւավորում է բազային տիպի OCSP-պատասխանները։

7.3.3. OCSP-ծառայության սերտիֆիկատը

OCSP-ծառայությունում OCSP-պատասխանների ստորագրման համար կիրառվում է սերտիֆիկատ, որի Extended Key Usage ընդլայնումը պարունակում է 1.3.6.1.5.5.7.3.9 նույնականացուցիչ (OCSP ստորագրումը)։

7.4. Ժամանակի դրոշմի կառուցվածքը

TSP-ծառայության բոլոր պատասխանները (ժամանակի դրոշմները) պարունակում են հետեւյալ դաշտերը՝

Policy ID՝ քաղաքականության նույնականացուցիչ, որին համապատասխան թողարկվել է ժամանակի դրոշմը,

Serial Number՝ ժամանակի դրոշմի սերիական համարը (նույնականացուցիչը),

Accuracy (microseconds)՝ TSP-ծառայության ժամերի ճշգրտությունը, մկվ,

Ordering՝ 0,

HasNonce՝ 1,

TSA՝ TSP-ծառայության նույնականացման տվյալները,

Stamp time՝ TSP- ծառայության կողմից ժամանակի դրոշմի ստորագրման ամսաթիվը եւ ժամը,

Hash algorithm՝ հեշավորման ալգորիթմի նույնականացուցիչը,

Hash size՝ հեշի չափսը, բայթ,

Hash՝ հեշի արժեքը,

Certificate of signer of time-stamp՝ TSP-ծառայության սերտիֆիկատ տիրապետողի (Հանձնաժողովի ՀԿ-ի լիազորված անձի) նույնականացման տվյալները,

Verification of time-stamp՝ ժամանակի դրոշմի ստուգման արդյունքը,

Verification of certificate of signer of time-stamp՝ TSP-ծառայության օպերատորի սերտիֆիկատի ստուգման արդյունքը,

Certificates from time-stamp (1)՝ Common Name = Հանձնաժողովի ՀԿ-ի ТSР-ծառայությունը, OU= Եվրասիական տնտեսական հանձնաժողովի ՀԿ-ն, О =Եվրասիական տնտեսական հանձնաժողովը, C=RU, Е= info@eecommission.org

7.4.1. Տարբերակի համարը

TSP-պատասխանի կառուցվածքի տարբերակը՝ 1։

7.4.2. TSP-ծառայության սերտիֆիկատը

TSP-ծառայությունում TSP-պատասխանների ստորագրման համար կիրառվում է սերտիֆիկատ, որի Extended Key Usage ընդլայնումը պարունակում է 1.3.6.1.5.5.7.3.8 նույնականացուցիչը (Ժամանակի նշման կարգավորում)։

8. Համապատասխանության աուդիտ եւ այլ գնահատումներ

8.1. Գնահատման հաճախականությունը եւ պայմանները

Հանձնաժողովի ՀԿ-ի ներքին եւ արտաքին աուդիտն անցկացվում է Հանձնաժողովի ՀԿ-ի ղեկավարության որոշմամբ։

8.2. Փորձագետի նույնականացումը եւ որակավորումը

Ներքին աուդիտն անցկացվում է Հանձնաժողովի ՀԿ-ի աուդիտի ադմինիստրատորի կողմից։

Արտաքին աուդիտն անցկացվում է հետեւյալ պահանջներին բավարարող անկախ կազմակերպության կողմից՝

ունի PKI տեխնոլոգիաների եւ տեղեկատվական անվտանգության հիման վրա տեղեկատվական համակարգերի շահագործման փորձ, ինչպես նաեւ անվտանգության աուդիտի անցկացման փորձ,

ունի բարձրագույն կրթություն ունեցող կամ «Տեղեկատվական անվտանգություն» մասնագիտությամբ վերապատրաստում անցած առնվազն երկու մասնագետ։

8.3. Փորձագետի վերաբերմունքը գնահատվողի նկատմամբ

Արտաքին աուդիտ անցկացնելու համար ներգրավվում է Հանձնաժողովի ՀԿ-ից կազմակերպչական կամ իրավաբանական առումով անկախ կազմակերպություն։

8.4. Աուդիտում ընդգրկված ոլորտները

Աուդիտի անցկացման ժամանակ ուսումնասիրվող հարցերի ոլորտը՝

Հանձնաժողովի ՀԿ-ի ֆիզիկական անվտանգությունը,

աուտենտիֆիկացումը եւ նույնականացումը,

Հանձնաժողովի ՀԿ-ի ծառայությունները,

ծրագրային ապահովման եւ ցանցին մուտքի անվտանգությունը,

Հանձնաժողովի ՀԿ-ի աշխատակիցների անձնական անվտանգության ապահովումը,

իրադարձությունների մատյանների եւ համակարգի մոնիթորինգի վարումը,

արխիվացման եւ պահեստային պատճենման ընթացակարգերը։

8.5. Թերությունների հայտնաբերման դեպքում ձեռնարկվող գործողությունները

Թերությունների հայտնաբերման դեպքում Հանձնաժողովի ՀԿ-ի ղեկավարությունը կազմակերպում է աշխատանքներ կարճ ժամկետներում դրանք վերացնելու ուղղությամբ։

8.6. Աուդիտի արդյունքների հաղորդումը

Անցկացված արտաքին աուդիտորական ստուգումների մասին հաշվետվություններն ուղղվում են Հանձնաժողովի ՀԿ-ի ղեկավարին։

9. Այլ կոմերցիոն եւ իրավաբանական հարցեր

9.1. Վճարումը

9.1.1. Սերտիֆիկատների թողարկման կամ թարմացման համար վճարումը

Հանձնաժողովի ՀԿ-ն իր ծառայությունները տրամադրում է անհատույց հիմունքներով։

9.1.2. Սերտիֆիկատների ռեեստրին մուտքի համար վճարումը

Սերտիֆիկատների ռեեստրին մուտքի համար վճարում նախատեսված չէ։

9.1.3. Սերտիֆիկատների հետկանչման կամ կարգավիճակի մասին տեղեկատվության ստացման ծառայություններին մուտքի համար վճարումը

Սերտիֆիկատների հետկանչման կամ կարգավիճակի մասին տեղեկատվության ստացման ծառայություններին մուտքի համար վճարում նախատեսված չէ։

9.1.4. Այլ ծառայությունների համար վճարումը

Հանձնաժողովի ՀԿ-ն իր ծառայությունները տրամադրում է անհատույց հիմունքներով։

9.1.5. Վճարումների վերադարձման պայմանները

Պայմաններ չկան։

9.2. Ֆինանսական պատասխանատվություն

9.2.1. Ապահովագրական ապահովում

Պայմաններ չկան։

9.2.2. Այլ ակտիվներ

Պայմաններ չկան։

9.2.3. Սերտիֆիկատներ տիրապետողների համար ապահովագրության կամ երաշխիքի գործողության ոլորտը

Պայմաններ չկան։

9.3. Տեղեկատվության գաղտնիությունը

9.3.1. Գաղտնի համարվող տեղեկատվությունը

Գաղտնի տեղեկատվություն է համարվում՝

ԷԹՍ բանալիները,

Հանձնաժողովի ՀԿ-ում առկա եւ սերտիֆիկատի կամ որպես ՀՍՑ-ի մաս անմիջական ուղարկման ոչ ենթակա սերտիֆիկատներ տիրապետողների անձնական եւ կորպորատիվ տեղեկատվությունը,

Հանձնաժողովի ՀԿ-ի իրադարձությունների գրանցման մատյաններում պահվող տեղեկատվությունը,

Հանձնաժողովի ՀԿ-ի գործունեության կատարված ստուգումների մասով հաշվետու նյութերը,

Հանձնաժողովի ՀԿ-ի ապարատային եւ ծրագրային ապահովման պաշտպանության եղանակների եւ կարգի, վարչարարության եւ չկանխատեսված իրավիճակների դեպքում գործողությունների եղանակների մասին տեղեկատվությունը,

«ծառայողական օգտագործման համար» կամ «գաղտնի» դրոշմով փաստաթղթերը։

9.3.2. Գաղտնի չհամարվող տեղեկատվությունը

Գաղտնի տեղեկատվություն չհամարվող տեղեկատվությունը բաց տեղեկատվություն է։ Բաց տեղեկատվությունը կարող է հրապրարակվել Հանձնաժողովի ՀԿ-ի որոշմամբ։ Հրապարակման վայրը, եղանակը եւ ժամը նույնպես որոշվում են Հանձնաժողովի ՀԿ-ի որոշմամբ։

Սերտիֆիկատներում եւ Հանձնաժողովի ՀԿ-ի կողմից թողարկվող ՀՍՑ-ում ներառվող տեղեկատվությունը գաղտնի չի համարվում։ Ենթադրվում է, որ հայտատուն գիտի, թե ինչ տեղեկատվություն է լինելու սերտիֆիկատում, եւ համաձայն է դրա հրապարակման հետ։

Հանձնաժողովի ՀԿ-ի կանոնակարգի տվյալներին համապատասխան հրապարակման ենթակա ամբողջ տեղեկատվությունը նույնպես չի համարվում գաղտնի։

9.3.3. Գաղտնի տեղեկատվության պաշտպանության մասով պարտավորությունները

Բոլոր մասնակիցները չպետք է մատչելի դարձնեն եւ ամեն կերպ պետք է խոչընդոտեն գաղտնի տեղեկատվությունը մատչելի դարձնելը որեւէ երրորդ անձանց՝ բացառությամբ Հանձնաժողովի կացության երկրի գործող օրենսդրությանը համապատասխան կամ դատական որոշման առկայության դեպքում այն մատչելի դարձնելը պահանջող դեպքերի։

9.4. Անձնական տվյալների պաշտպանություն

9.4.1. Անձնական տվյալների պաշտպանության ապահովումը

Հանձնաժողովի ՀԿ-ն իրականացնում է սերտիֆիկատներ տիրապետողների անձնական տվյալների պաշտպանություն՝ Հանձնաժողովի կացության երկրի օրենսդրությանը համապատասխան։

9.4.2. Որպես անձնական դիտարկվող տվյալները

Հանձնաժողովի կացության երկրի օրենսդրությանը համապատասխան որպես այդպիսին որոշված տվյալները՝ բացառությամբ այն տվյալների, որոնք պետք է հրապարակվեն ԷԹՍ ոլորտում Հանձնաժողովի կացության երկրի գործող օրենսդրությանը համապատասխան։

9.4.3. Որպես անձնական չդիտարկվող տվյալները

Անձնական չհամարվող բոլոր տվյալները։

9.4.4. Անձնական տվյալների պաշտպանության մասով պարտավորությունը

Հանձնաժողովի ՀԿ-ն պաշտպանում է սերտիֆիկատներ տիրապետողների անձնական տվյալները եւ ամեն կերպ խոչընդոտում է երրորդ անձանց դրանք մատչելի դարձնելը։

9.4.5. Անձնական տվյալների օգտագործման կանխումը եւ համաձայնությունը

Անձնական տվյալների ցանկացած օգտագործում հնարավոր է միայն դրանք տիրապետողի համաձայնությամբ։ Սերտիֆիկատի թողարկման հայտը համարվում է սերտիֆիկատում՝ հայտում նշված անձնական տվյալների օգտագործման համաձայնություն է։

9.4.6. Մատչելի դարձնելը՝ դատական կամ վարչական գործընթացին համապատասխան

Անձնական տվյալները մատչելի դարձնելն իրականացվում է Հանձնաժողովի կացության երկրի գործող օրենսդրությանը համապատասխան։

9.4.7. Տեղեկատվությունը մատչելի դարձնելու այլ պայմաններ

Պայմաններ չկան։

9.5. Մտավոր սեփականության նկատմամբ իրավունքները

Հանձնաժողովը բոլոր այն փաստաթղթերի, ծրագրային-տեխնիկական միջոցների եւ տեղեկատվական ռեսուրսների սեփականատերն է, որոնք ստեղծվել են Հանձնաժողովի միջոցների հաշվին, ձեռք են բերվել օրինական հիմունքներով, ստացվել են նվիրատվության կամ ժառանգության կարգով։

Հանձնաժողովի ՀԿ-ի աշխատակիցների կողմից իրենց ծառայողական պարտականությունների կատարման ժամանակ արտադրված, այդ թվում նաեւ մտավոր բնույթի ամբողջ արտադրանքը Հանձնաժողովի սեփականությունն է, եթե առանձին պայմանագրով այլ ռեժիմ չի նախատեսվում։

Հանձնաժողովը, Հանձնաժողովի կացության երկրի օրենսդրությանը համապատասխան, իր կողմից ստեղծված մտավոր սեփականության բոլոր օբյեկտների նկատմամբ բացառիկ իրավատեր է։

Բոլոր առեւտրային նշանները, լիցենզիաները, գրաֆիկական սիմվոլները եւ Հանձնաժողովի ՀԿ-ի կողմից մյուս օգտագործվողները տիրապետողների մտավոր սեփականությունն են։

9.6. Հայտերը եւ երաշխիքները

9.6.1. Հանձնաժողովի ՀԿ-ի հայտերը եւ երաշխիքները

Հանձնաժողովի ՀԿ-ն երաշխավորում է՝

որ իր գործունեությունը համապատասխանում է Հանձնաժողովի կացության երկրի օրենսդրությամբ եւ Հանձնաժողովի ակտերով սահմանված պահանջներին,

թողարկված սերտիֆիկատներում եւ ՀՍՑ-ում Հանձնաժողովի ՀԿ-ի աշխատակիցների մեղքով որեւէ աղավաղման կամ սխալի բացակայությունը,

սերտիֆիկատների այն քաղաքականությունների պահանջներին սերտիֆիկատի համապատասխանությունը, որին համապատասխան այն թողարկվել է,

ռեպոզիտարիայի եւ չեղարկման (հետկանչման) ծառայություններից օգտվելը՝ սույն կանոնակարգին համապատասխան։

9.6.2. ՍԿ-ի հայտերը եւ երաշխիքները

Տե՛ս սույն կանոնակարգի 9.6.1-րդ կետը։

9.6.3. Սերտիֆիկատ տիրապետողի հայտերը եւ երաշխիքները

Սերտիֆիկատ տիրապետողը երաշխավորում է, որ՝

սերտիֆիկատի թողարկման հայտում վերջինիս փոխանցած ամբողջ տեղեկատվությունը հավաստի է,

ԷԹՍ բանալին պահվում է գաղտնի, եւ չթույլատրված մուտքը դրան անհնարին է։

սերտիֆիկատն օգտագործվում է միայն ըստ նշանակության եւ սույն կանոնակարգի պահանջներին եւ սերտիֆիկատների կիրառման այն քաղաքականությանը համապատասխան, որին համապատասխան սերտիֆիկատը թողարկվել է,

անհապաղ կտեղեկացնի Հանձնաժողովի ՀԿ-ին ԷԹՍ բանալու կոմպրոմետացիայի դեպքում։

9.6.4. Սերտիֆիկատներից օգտվողի հայտերը եւ երաշխիքները

Օգտագործելով սերտիֆիկատները՝ սերտիֆիկատներից օգտվողը երաշխավորում է, որ՝

սերտիֆիկատի օգտագործումն իրականացվում է սերտիֆիկատում նշված նշանակությանը եւ սույն կանոնակարգի պահանջներին համապատասխան,

սերտիֆիկատի օգտագործումն իրականացվում է միայն ԷԹՍ սերտիֆիկատի եւ վավերականությունը ցույց տված դրա կարգավիճակի ստուգումն անցկացնելուց հետո եւ սերտիֆիկատների կիրառման այն քաղաքականությանը համապատասխան, որի նույնականացուցիչը նշված է սերտիֆիկատում։

9.6.5. Այլ մասնակիցների հայտերը եւ երաշխիքները

Պայմաններ չկան։

9.7. Հրաժարում երաշխիքներից

Պայմաններ չկան։

9.8. Պատասխանատվության սահմանափակում

Հանձնաժողովի ՀԿ-ն պատասխանատվություն չի կրում իրենից չկախված պատճառներով իր պարտականությունները չկատարելու համար։

Հանձնաժողովի ՀԿ-ն պատասխանատվություն չի կրում սերտիֆիկատներ տիրապետողների եւ սերտիֆիկատներից օգտվողների կողմից սույն կանոնակարգի եւ սերտիֆիկատների կիրառման քաղաքականությունների խախտման դեպքում։

9.9. Վնասի փոխհատուցումը

Պայմաններ չկան։

9.10. Կանոնակարգի գործողության ժամանակահատվածը եւ դադարեցումը

9.10.1. Գործողության ժամանակահատվածը

Սույն կանոնակարգը եւ դրա փոփոխությունները համարվում են գործող հրապարակման պահից մինչեւ դրա գործողության դադարեցման պահը։

9.10.2. Գործողության դադարեցումը

Սույն կանոնակարգը պարբերաբար շտկվում է եւ լրացվում՝ մնալով գործող մինչեւ նոր տարբերակի հրապարակումը, դրա գործողության դադարեցման մասին ծանուցումը կամ այդպիսի ծանուցման մեջ սերտիֆիկատների քաղաքականությունների գործողությունների դադարեցման ամսաթիվը։

9.10.3. Գործողության դադարեցման արդյունքը եւ երկարակյացությունը

Սույն կանոնակարգի գործողությունն ավարտելուց հետո դրա պահանջները շարունակում են գործել սույն կանոնակարգի գործողության ժամանակահատվածում թողարկված՝ Հանձնաժողովի ՀԿ-ի սերտիֆիկատներից օգտվող բոլոր մասնակիցների համար՝ այդ սերտիֆիկատների գործողության ամբողջ ժամկետի ընթացքում։

9.11. Անհատական ծանուցումները եւ կապը մասնակիցների միջեւ

ԲԲԵ մասնակիցները կարող են օգտվել միմյանց միջեւ կապի ցանկացած եղանակից, եթե որեւէ համաձայնագրով այլ բան սահմանված չէ։

9.12. Փոփոխությունները

9.12.1. Փոփոխության ընթացակարգը

Սույն կանոնակարգում փոփոխությունները կարող են կատարվել Հանձնաժողովի ՀԿ-ի ղեկավարի կողմից։ Փոփոխությունները կարող են ձեւակերպվել փոփոխված փաստաթղթի տեսքով կամ թարմացման տեսքով։ Փոփոխությունները եւ թարմացումները հրապարակվում են։

9.12.2. Տեղեկացման ժամկետը եւ մեխանիզմը

Հանձնաժողովի ՀԿ-ն իրեն իրավունք է վերապահում առանց տեղեկացման ոչ էական փոփոխություններ կատարել Հանձնաժողովի ՀԿ-ի կանոնակարգում եւ սերտիֆիկատների կիրառման քաղաքականություններում վրիպումների, սխալների, URL կամ կոնտակտային տեղեկատվության փոփոխության դեպքում։

Այն դեպքում, երբ Հանձնաժողովի ՀԿ-ի ղեկավարը համարում է, որ անհապաղ անհրաժեշտ է սերտիֆիկատների կիրառման քաղաքականությունների էական փոփոխություն ԲԲԵ կամ դրա ցանկացած մասի անվտանգության խախտման կանխման կամ դադարեցման համար, նա կարող է դա անել եւ հրապարակել, որից հետո տեղեկացնել մասնակիցներին։

Բացառությամբ վերը նկարագրված դեպքերի՝ Հանձնաժողովի ՀԿ կանոնակարգի եւ սերտիֆիկատների կիրառման քաղաքականությունների փոփոխությունները եւ թարմացումները հրապարակվում են Հանձնաժողովի ՀԿ-ի ռեպոզիտարիայում ոչ ուշ, քան տվյալ փոփոխությունները եւ լրացումները գործողության մեջ դնելուց 14 օր առաջ։

9.12.3. Հանգամանք, որի դեպքում OID -ն պետք է փոփոխվի

Եթե Հանձնաժողովի ՀԿ-ն որոշում է, որ անհրաժեշտ է OID փաստաթղթի փոխարինում, ապա նոր թարմացումը պետք է պարունակի նոր OID։

9.13. Վեճերի լուծման պայմանները

Վեճերի առաջացման դեպքում կողմերը ձեռնարկում են բոլոր անհրաժեշտ քայլերը վիճելի հարցերի՝ բանակցությունների միջոցով կարգավորման համար, որոնք կարող են առաջանալ սույն կանոնակարգի շրջանակներում։ Սերտիֆիկատների կիրառման քաղաքականությունների գործողության հետ կապված եւ բանակցությունների ընթացքում կողմերի միջեւ չկարգավորված վեճերը պետք է քննարկվեն վարչական կարգով։

9.14. Կիրառվող օրենսդրությունը

Սույն կանոնակարգի դրույթների օրինականության որոշման, պարզաբանման, մեկնաբանման եւ կատարման համար իրավունքի ցանկացած սուբյեկտ պետք է օգտվի Հանձնաժողովի կացության երկրի օրենսդրությունից եւ Միության մարմինների ակտերից։

9.15. Համապատասխանությունը կիրառվող օրենսդրությանը

Բոլոր մասնակիցները պետք է ղեկավարվեն Հանձնաժողովի կացության երկրի օրենսդրությամբ, ինչպես նաեւ Հանձնաժողովի կացության երկրի ծրագրային-ապարատային միջոցների եւ տեխնիկական տեղեկատվության ԷԹՍ, ծածկագրման եւ արտահանման/ներմուծման ոլորտում վերահսկվող կազմակերպությունների ուղեցույց փաստաթղթերով։

9.16. Տարատեսակ դրույթները

9.16.1. Համաձայնագրի լրիվությունը

Պայմաններ չկան։

9.16.2. Իրավունքների եւ պարտականությունների փոխանցումը

Պայմաններ չկան։

9.16.3. Բաժանելիությունը

Այն դեպքում, երբ դատարանի որոշմամբ տվյալ փաստաթղթի որեւէ դրույթ ճանաչվելու է իրավաբանական ուժ չունեցող, մնացած դրույթները, այնուամենայնիվ, շարունակում եմ գործել։

9.16.4. Իրավակիրառումը

Պայմաններ չկան։

9.16.5. Ֆորս մաժոր

Հանձնաժողովի ՀԿ-ի կանոնակարգի կողմերն ազատվում են պատասխանատվությունից՝ սույն կանոնակարգի համաձայն իրենց պարտականությունների լրիվ կամ մասնակի չկատարման համար, եթե այդ չկատարումը սույն կանոնակարգին համապատասխան պարտավորությունների առաջացումից հետո առաջացած ֆորսմաժորային հանգամանքների հետեւանք է։

Ֆորսմաժորային հանգամանքներ են ճանաչվում տվյալ պայմաններում արտակարգ (այսինքն՝ Հանձնաժողովի ՀԿ-ի կանոնակարգի կողմերի խելամիտ հսկողությունից դուրս գտնվող) եւ անկանխելի հանգամանքները, ներառյալ՝ ռազմական գործողությունները, զանգվածային անկարգությունները, տարերային աղետները, գործադուլները, ապարատածրագրային ապահովման աշխատանքի տեխնիկական խափանումները, հրդեհները, պայթյունները եւ այլ տեխնածին աղետներ, Հանձնաժողովի կացության երկրի պետական եւ տեղական մարմինների գործողությունները (անգործությունը), որոնք հանգեցրել են Հանձնաժողովի ՀԿ-ի կանոնակարգի կողմի (կողմերի) կողմից սույն կանոնակարգի համաձայն իրենց պարտավորությունների կատարման անհնարինությանը։

Ֆորսմաժորային հանգամանքների առաջացման դեպքում Հանձնաժողովի ՀԿ-ի կանոնակարգի կողմերի կողմից սույն կանոնակարգի համաձայն իրենց պարտավորությունների կատարման ժամկետը տեղափոխվում է այն ժամանակին համաչափ, որի ընթացքում գործում են այդ հանգամանքները։

Հանձնաժողովի ՀԿ-ի կանոնակարգի կողմը, որի համար ստեղծվել է սույն կանոնակարգի համաձայն իր պարտավորությունների կատարման անհնարինությունը, պետք է անհապաղ գրավոր տեղեկացնի Հանձնաժողովի ՀԿ-ի կանոնակարգի մյուս կողմին ֆորսմաժորային հանգամանքների վրա հասնելու, գործողության ենթադրվող ժամկետի եւ դադարելու մասին, ինչպես նաեւ ներկայացնի նշված հանգամանքների առկայության ապացույցները։

Անհաղթահարելի ուժի հանգամանքների վրա հասնելու մասին չտեղեկացնելը կամ ոչ ժամանակին տեղեկացնելը հանգեցնում է այդ հանգամանքները վկայակոչելու իրավունքի կորստին։

Այն դեպքում, երբ Հանձնաժողովի ՀԿ-ի կանոնակարգի կողմերի կողմից սույն կանոնակարգի համաձայն որեւէ պարտավորության լրիվ կամ մասնակի կատարման անհնարինությունը պայմանավորված է ֆորսմաժորային հանգամանքների ազդեցությամբ եւ գոյություն ունի մեկ ամսից ավելի, ապա Հանձնաժողովի ՀԿ-ի կանոնակարգի կողմերից յուրաքանչյուրն իրավասու է միակողմանի հրաժարվել այդ պարտավորության հետագա կատարումից։

9.17. Այլ դրույթներ

Պայմաններ չկան։

\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ՀԱՎԵԼՎԱԾ ԹԻՎ 1

Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնի կանոնակարգի

Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնի   
OCSP-ծառայության եւ TSP-ծառայության աշխատակարգը

1. Հանձնաժողովի ՀԿ-ն OCSP-ծառայության միջոցով սերտիֆիկատների կարգավիճակի մասին արդիական տեղեկատվության տրամադրման մասով ծառայություններ է մատուցում։ Հանձնաժողովի ՀԿ-ի օգտվողների հարցումների հարցերով OCSP-ծառայությունը ձեւավորում եւ այդ օգտվողներին է տրամադրում OCSP-պատասխանները, որոնք պարունակում են ԷԹՍ բանալու հարցվող սերտիֆիկատի կարգավիճակի մասին տեղեկատվություն։ OCSP-պատասխանները ներկայացվում են Հանձնաժողովի ՀԿ-ի լիազորված անձի ստորագրության բանալու սերտիֆիկատի օգտագործմամբ ստորագրված էլեկտրոնային փաստաթղթի ձեւով։ OCSP-պատասխանը ճանաչվում է գործող հետեւյալ պայմանների միաժամանակյա կատարման դեպքում՝

հաստատված է OCSP-պատասխանում OCSP-ծառայության ԷԹՍ իսկությունը,

Հանձնաժողովի ՀԿ-ի լիազորված անձի սերտիֆիկատը OCSP-պատասխանի ԷԹՍ իսկության հաստատման պահի դրությամբ գործում է,

Հանձնաժողովի ՀԿ-ի լիազորված անձի ԷԹՍ բանալին OCSP-պատասխանի ձեւավորման պահի դրությամբ գործում է,

Հանձնաժողովի ՀԿ-ի լիազորված անձի սերտիֆիկատը Extended Key Usage ընդլայնման մեջ (օգտագործման ոլորտը՝ OCSP-ծառայության ԷԹՍ պատասխանը) պարունակում է OID 1.3.6.1.5.5.7.3.9-ը։

Հավաստագրման կենտրոնի կարգավիճակների ծառայության հաղորդման հասցեն է՝ https://ca-ocsp.eecommission.org:8877։ Նշված հասցեն ներառվում է Հանձնաժողովի ՀԿ-ի կողմից թողարկվող սերտիֆիկատների Authority Information Access (AIA) ընդլայնման մեջ։

2. Հավաստագրման կենտրոնը TSP-ծառայության միջոցով ժամանակի դրոշմների տրամադրման մասով ծառայություններ է մատուցում։ Էլեկտրոնային փաստաթղթին վերաբերող ժամանակի դրոշմը ճանաչվում է գործող հետեւյալ պայմանների միաժամանակյա կատարման դեպքում՝

հաստատված է ժամանակի դրոշմում Հանձնաժողովի ՀԿ-ի լիազորված անձի ԷԹՍ իսկությունը,

Հանձնաժողովի ՀԿ-ի լիազորված անձի սերտիֆիկատը ժամանակի դրոշմի ԷԹՍ իսկության հաստատման պահի դրությամբ գործում է,

Հանձնաժողովի ՀԿ-ի լիազորված անձի ԷԹՍ բանալին ժամանակի դրոշմի ձեւավորման պահի դրությամբ գործում է,

Հանձնաժողովի ՀԿ-ի լիազորված անձի սերտիֆիկատը Extended Key Usage ընդլայնման մեջ (օգտագործման ոլորտը՝ Ժամանակի դրոշմի կարգավորումը) պարունակում է OID=l.3.6.1.5.5.7.3.8-ը,

TSP-ծառայության հաղորդման հասցեն է՝

<https://ca-tsp.eecommission.org:8777>։

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ՀԱՎԵԼՎԱԾ ԹԻՎ 2

Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնի կանոնակարգի

Սերտիֆիկատների կիրառման օբյեկտային նույնականացուցիչները

|  |  |  |
| --- | --- | --- |
| Օբյեկտային նույնականացուցիչը | Սերտիֆիկատների կիրառման քաղաքականության կարճ անվանումը | Սերտիֆիկատների կիրառման քաղաքականության լրիվ անվանումը |
| 1.2.643.3.294.1.2.1 | Սերտիֆիկատների կիրառման բազային քաղաքականությունը | Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոն։ Հանձնաժողովի կոլեգիայի անդամների, Հանձնաժողովի պաշտոնատար անձանց եւ աշխատակիցների էլեկտրոնային թվային ստորագրության ստուգման բանալիների սերտիֆիկատների կիրառման քաղաքականությունը |
| 1.2.643.3.294.1.2.2 | OCSP-ծառայության սերտիֆիկատների կիրառման քաղաքականությունը | Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոն։ Հանձնաժողովի OCSP- ծառայության էլեկտրոնային թվային ստորագրության ստուգման բանալիների սերտիֆիկատների կիրառման քաղաքականությունը |
| 1.2.643.3.294.1.2.3 | TSP- ծառայության սերտիֆիկատների կիրառման քաղաքականությունը | Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոն։ Հանձնաժողովի ՀԿ-ի TSP-ծառայության էլեկտրոնային թվային ստորագրության ստուգման բանալիների սերտիֆիկատների կիրառման քաղաքականությունը |
| 1.2.643.3.294.1.2.4 | SSL սերտիֆիկատների կիրառման քաղաքականությունը | Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոն։ Սերվերների աուտենտիֆիկացման սերտիֆիկատների կիրառման քաղաքականությունը |
| 1.2.643.3.294.1.2.5 | ՎԵԿ-ի սերտիֆիկատների կիրառման քաղաքականությունը | Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոն։ Հանձնաժողովի վստահված երրորդ կողմի սերտիֆիկատների կիրառման քաղաքականությունը |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ՀԱՎԵԼՎԱԾ ԹԻՎ 3

Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնի կանոնակարգի

Հայտերի ձեւանմուշները

Սերտիֆիկատի թողարկման հայտ

Ես՝\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(պաշտոն, Ա.Ա.Հ.)

խնրում եմ թողարկել ԷԹՍ ստուգման բանալու սերտիֆիկատը

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-ում օգտագործման ոլորտով,

(նշել Հանձնաժողովի Ինտեգրացիոն հատվածի ենթահամակարգի անվանումը)

սերտիֆիկատի թողարկման համար հաղորդում են հետեւյալ տվյալները.

|  |  |
| --- | --- |
| Անուն, ազգանուն, հայրանուն |  |
| Ստորաբաժանում |  |
| Պաշտոն |  |
| Էլեկտրոնային փոստի հասցե (e-mail) |  |
| Բանալի արտահայտություն |  |

Սերտիֆիկատ տիրապետող \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ստորագրություն) (ազգանուն, անվան սկզբնատառեր)

Հաստատում եմ, որ նշված բանալի արտահայտությունն արտակարգ կապի համար ծածկագիր է ԷԹՍ բանալու կոմպրոմետացիայի դեպքում, եւ պարտավորվում եմ ապահովել տվյալ ծածկագրի գաղտնիության պահպանումը։

Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնի կանոնակարգի հետ ծանոթացել եմ։ Իմ անվամբ թողարկվող սերտիֆիկատին համապատասխանող ԷԹՍ բանալու կոմպրոմետացիայի փաստի բացահայտման դեպքում պարտավորվում եմ անհապաղ տեղեկացնել այդ իրադարձության մասին Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնին։

Սույնով ես՝

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ,

(սերտիֆիկատ տիրապետողի ազգանուն, անուն, հայրանուն)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(անձնագրի սերիա եւ համար, ում կողմից եւ երբ է տրվել)

համաձայնում են Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնի կողմից իմ անձնական տվյալների մշակման հետ եւ ընդունում եմ, որ ԷԹՍ ստուգման բանալիների սերտիֆիկատներ մտցվող անձնական տվյալները, որոնց տիրապետողը ես եմ, վերաբերում են հանրամատչելի անձնական տվյալներին։

Սերտիֆիկատ տիրապետող \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ստորագրություն) (ազգանուն, անվան սկզբնատառեր)

Ստորաբաժանման ղեկավար \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ստորագրություն) (ազգանուն, անվան սկզբնատառեր)

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ թ.

Սերտիֆիկատի չեղարկման (հետկանչման) հայտ

Ես՝ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(պաշտոն, Ա.Ա.Հ.)

կապված

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(սերտիֆիկատի հետկանչման պատճառը)

խնդրում եմ չեղարկել (հետ կանչել) հետեւյալ տվյալները պարունակող ԷԹՍ ստուգման բանալու իմ սերտիֆիկատը.

|  |  |
| --- | --- |
| Սերտիֆիկատի սերիական համար |  |
| Ազգանուն, անուն, հայրանուն |  |
| Ստորաբաժանում |  |
| Պաշտոն |  |
| Էլեկտրոնային փոստի հասցե (e-mail) |  |

Սերտիֆիկատ տիրապետող \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ստորագրություն) (ազգանուն, անվան սկզբնատառեր)

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ թ.

Սերտիֆիկատի գործողությունը կասեցնելու հայտ

Ես՝ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(պաշտոն, Ա.Ա.Հ.)

խնդրում եմ կասեցնել հետեւյալ տվյալները պարունակող ԷԹՍ ստուգման բանալու իմ սերտիֆիկատի գործողությունը.

|  |  |
| --- | --- |
| Սերտիֆիկատի սերիական համար |  |
| Ազգանուն, անուն, հայրանուն |  |
| Ստորաբաժանում |  |
| Պաշտոն |  |
| Էլեկտրոնային փոստի հասցե (e-mail) |  |

Սերտիֆիկատի գործողության կասեցման ժամկետ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ օր։

(օրերի քանակ)

Սերտիֆիկատ տիրապետող \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ստորագրություն) (ազգանուն, անվան սկզբնատառեր)

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ թ.

Սերտիֆիկատի գործողության վերականգնման հայտ

Ես՝ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(պաշտոն, Ա.Ա.Հ.)

խնդրում են վերականգնել հետեւյալ տվյալները պարունակող ԷԹՍ ստուգման բանալու իմ սերտիֆիկատի գործողությունը.

|  |  |
| --- | --- |
| Սերտիֆիկատի սերիական համար |  |
| Ազգանուն, անուն, հայրանուն |  |
| Ստորաբաժանում |  |
| Պաշտոն |  |
| Էլեկտրոնային փոստի հասցե (e-mail) |  |

Սերտիֆիկատ տիրապետող \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ստորագրություն) (ազգանուն, անվան սկզբնատառեր)

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ թ.

Էլեկտրոնային թվային ստորագրության բանալու ստեղծման հայտ

Ես՝ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(պաշտոն, Ա.Ա.Հ.)

խնդրում են ստեղծել էլեկտրոնային թվային ստորագրության բանալի։

Բանալու կրիչի տվյալները՝ էլեկտրոնային թվային ստորագրության ստեղծվող բանալու պահման համար.

|  |  |
| --- | --- |
| Բանալու կրիչի տիպը |  |
| Բանալու կրիչի սերիական համարը |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ստորագրություն) (ազգանուն, անվան սկզբնատառեր)

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ թ.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ՀԱՎԵԼՎԱԾ ԹԻՎ 4

Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնի կանոնակարգի

ԷԹՍ եւ ժամանակի դրոշմների վավերականությունը հաստատելու մասով աշխատանքների անցկացման կարգը

1. Հանձնաժողովի ՀԿ-ն սերտիֆիկատից օգտվողի հայտի համաձայն իրականացնում է էլեկտրոնային փաստաթղթի ԷԹՍ իսկության հաստատման, ժամանակի դրոշմի վավերականության կամ ժամանակի դրոշմի՝ էլելկտրոնային փաստաթղթին համապատասխանության հաստատման աշխատանքներ (այսուհետ՝ Հատուկ աշխատանքներ)։

2. Էլեկտրոնային փաստաթղթի ԷԹՍ իսկության մասին որոշումն ընդունում է Հանձնաժողովի ՀԿ-ն։

3. ԷԹՍ իսկության հաստատման հայտի էլեկտրոնային փաստաթղթում նշվում են՝

հայտի ներկայացման ամսաթիվը եւ ժամը,

սերտիֆիկատ տիրապետողի նույնականացման տվյալները, որի ԷԹՍ իսկությունն անհրաժեշտ է հաստատել էլեկտրոնային փաստաթղթում,

ԷԹՍ-ով էլեկտրոնային փաստաթուղթ պարունակող ֆայլի անվանումը, որի իսկությունն անհրաժեշտ է ստուգել,

Էլեկտրոնային փաստաթղթի ԷԹՍ-ի ձեւավորման ամսաթիվը եւ ժամը,

ամսաթիվ եւ ժամ, որոնց վրա հասնելուն պես պահանջվում է սահմանել ԷԹՍ-ի իսկությունը։

4. Էլեկտրոնային փաստաթղթում ԷԹՍ իսկության հաստատման հայտի պարտադիր հավելված է CD/DVD-ROM տեղեկատվության օտարելի կրիչը, որը պարունակում է՝

սերտիֆիկատ, որի օգտագործման հետ մեկտեղ անհրաժեշտ է իրականացնել էլեկտրոնային փաստաթղթում ԷԹՍ-ի իսկության հաստատում,

էլեկտրոնային փաստաթուղթ՝ տվյալներ եւ այդ տվյալների ԷԹՍ արժեք պարունակող մեկ ֆայլի կամ երկու ֆայլի տեսքով, որոնցից մեկը պարունակում է տվյալներ, իսկ մյուսը՝ այդ տվյալների ԷԹՍ արժեք։

5. Ժամանակի դրոշմի վավերականության եւ ժամանակի դրոշմի՝ էլեկտրոնային փաստաթղթին համապատասխանության հաստատման հայտում նշվում են՝

հայտի ներկայացման ամսաթիվը եւ ժամը,

ժամանակի դրոշմ պարունակող CMS ստանդարտի ֆայլի անվանումը, որի վավերականությունն անհրաժեշտ է հաստատել,

ելակետային տվյալներ պարունակող ֆայլի անվանումը, որոնց համար ձեւավորվել է ժամանակի դրոշմ,

ամսաթիվ եւ ժամ, որոնց վրա հասնելուն պես պահանջվում է հաստատել ժամանակի դրոշմի վավերականությունը։

6. Ժամանակի դրոշմի վավերականության եւ ժամանակի դրոշմի՝ էլեկտրոնային փաստաթղթին համապատասխանության հաստատման հայտի պարտադիր հավելված է CD/DVD-ROM տեղեկատվության օտարելի կրիչը, որը պարունակում է՝

ժամանակի դրոշմ պարունակող ֆայլ, որի վավերականությունն անհրաժեշտ է հաստատել,

ելակետային տվյալներ պարունակող ֆայլ, որոնց համար ձեւավորվել է ժամանակի դրոշմ։

7. Հատուկ աշխատաքներն իրականացնում է Հանձնաժողովի ՀԿ-ի աշխատակիցների կազմից ձեւավորված հանձնաժողովը։ Հատուկ աշխատանքների անցկացման արդյունքը Հանձնաժողովի ՀԿ-ի եզրակացությունն է։ Եզրակացությունը պարունակում է՝

ստուգում իրականացնող հանձնաժողովի կազմը,

ստուգման անցկացման համար հիմքը,

էլեկտրոնային փաստաթղթի ԷԹՍ ստուգման արդյունքը կամ ժամանակի դրոշմի եւ ելակետային տվյալներին դրա համապատասխանության ստուգման արդյունքը,

ստուգման անցկացման համար հանձնաժողովին ներկայացված տվյալները, կատարված ստուգման մասով հաշվետվությունը։

8. Կատարված ստուգման մասով հաշվետվությունը պարունակում է՝

ստուգման անցկացման ժամը եւ վայրը,

ստուգման բովանդակությունը եւ արդյունքները,

ստուգման արդյունքների հիմնավորումը։

9. Կատարված ստուգման մասով Հանձնաժողովի ՀԿ-ի եզրակացությունը կազմվում է կամայական ձեւով երկու օրինակից, ստորագրվում է հանձնաժողովի բոլոր անդամների կողմից։ Կատարված ստուգման մասով եզրակացության մեկ օրինակը տրամադրվում է հայտատուին։

10. Մեկ ԷԹՍ-ի կամ ժամանակի մեկ դրոշմի եւ կատարված ստուգման վերաբերյալ եզրակացությունն օգտվողին տրամադրելու մասով հատուկ աշխատանքների անցկացման ժամկետը կազմում է Հանձնաժողովի ՀԿ-ում հայտը ստանալու պահից տասը աշխատանքային օր։

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_