Elektron Hökumət Sertifikat Xidmətləri Mərkəzinin Sertifikatın tətbiqi qaydaları

19 avqust 2010

Versiya 1.0

Mündəricat

1 Giriş 4

1.1 İstifadəçilər və tətbiq sahəsi 4

1.2 Sənədin adı və identifikasiyası 5

1.3 Sertifikat siyasətinin identifikasiyası 5

1.4 Tərəflər 5

1.5 Sertifikatların istifadəsi 7

1.6 Fəaliyyət siyasəti 8

1.7 Anlayışlar və qısaltmalar 8

2 Yayımlanma və saxlama məsuliyyəti 17

2.1 Direktoriya və sertifikatın yoxlanılması xidmətləri 17

2.2 İnformasiyanın yayımlanması 19

2.3 Yayımlanma vaxtı və mütəmadiliyi 19

2.4 Direktoriyaya daxilolmaya nəzarət 20

3 İmza sahibinin identifikasiya və autentifikasiyası (İ&A) 20

3.1 Adlandırma 20

3.2 İlkin identiklik yoxlaması 230

3.3 Yeni açar sorğusu zamanı identifikasiya və autentifikasiya 24

3.4 Ləğvetmə sorğusu zamanı identifikasiya və autentifikasiya 24

3.5 Sertifikatın statusunun dəyişdirilməsi barədə sorğu 24

4 Sertifikatlarla bağlı fəaliyyət tələbləri 26

4.1 Sertifikat Ərizəsi 26

4.2 Sertifikat Ərizəsinin emalı 26
4.3 Sertifikatın verilməsi 30
4.4 Sertifikatın təqdim edilməsi 401
4.5 Açar cütü və Sertifikatdan istifadə 412
4.6 Sertifikatın dəyişdirilməsi 433
4.7 Sertifikatın yenilənməsi 433
4.8 Sertifikatın modifikasiyası 433
4.9 Sertifikatın qüvvəsinin dayandırılması və ləğvi 433
4.10 Sertifikat statusu xidmətləri 41
4.11 Sertifikatın etibarlılığının yoxlanması 42
4.12 Sertifikata xidmətin başa çatması 456
4.13 Açarın saxlamaq üçün başqasına verilməsi 456
5 Vasitələrə, idarəetməyə və fəaliyyətə nəzarət 456
5.1 Fiziki təhlükəsizlik nəzarəti 44
5.2 Prosedurların idarə olunması 45
5.3 Kadrların idarə olunması 47
5.4 Audit-loqların aparılma proseduru 48
5.5 Sertifikat Xidmətləri ilə bağlı qeydlərin arxivləşdirilməsi 51
5.6 EH-SXM-in açarının dəyişdirilməsi 52
5.7 Konfidensiallığın pozulması və qəza hallarında bərpa 53
5.8 EH-SXM-in fəaliyyətinə xitam verilməsi 54
6 Texniki təhlükəsizlik nəzarəti 55
6.1 Açar cütünün yaradılması və ilkin quraşdırılması 55

6.2 Gizli açarın mühafizəsi 56
6.3 Açar cütünün idarə olunmasının digər məqamları 59
6.4 Aktivləşdirmə məlumatı 59
6.5 Vaxt göstəricisi 60
7 Sertifikat və CRL profilləri 60
7.1 Sertifikat profilləri 61
7.2 CRL profilləri 64
8 Uyğunluq auditi və digər yoxlamalar 65
9 Digər işlər və hüquqi məsələlər 66
9.1 Ödənişlər 66
9.2 Maliyyə məsuliyyəti 66
9.3 Fəaliyyətlə bağlı məlumatların konfidensiallığı 66
9.4 Fərdi məlumatların konfidensiallığı 68
9.5 Əqli mülkiyyət hüquqları 69
9.6 Təmsilçilik və zəmanətlər 70
9.7 Məsuliyyət və məsuliyyətdən azad olma 70
9.8 Təzminat 70
9.9 Qüvvədə olma və qüvvədən düşmə 71
9.10 İştirakçılara fərdi bildirişlər və onlarla əlaqə 71
9.11 Dəyişikliklər 71
9.12 Mübahisələrin həlli proseduru 71
10 İstinadlar 72

Giriş

Elektron Hökumət Sertifikat Xidmətləri Mərkəzi (EH-SXM) “Elektron imza və elektron sənəd haqqında” Azərbaycan Respublikasının Qanununa müvafiq olaraq elektron imza üçün Sertifikat verən və imzaların istifadəsi üzrə xidmətləri göstərən hüquqi şəxsdir.

“Sertifikatın tətbiqi qaydaları” (bundan sonra - Qaydalar) adlandırılmış bu sənəd RFC 3647 və ETSI TS 101 456 sənədlərinin və Azərbaycan Respublikasının qanunvericiliyinin tələblərinə müvafiq olaraq EH-SXM tərəfindən hazırlanmışdır və sertifikat xidmətlərinin göstərilməsi ilə bağlı olan inzibati, texniki və hüquqi məsələləri (fəaliyyəti) tənzimləyir.

EH-SXM gücləndirilmiş elektron imza yaradılması üçün yararlı olan imza yaratma və yoxlama məlumatları əsasında Təkmil Sertifikatların verilməsini və onların idarə olunmasını təmin edir. Bu məqsədlə aşağıdakı mexanizmlər təmin edilir:

- **Autentifikasiya** – İmza sahibini dəqiq identikləşdirmək;
- **Verilənlərin tamlığı** – əlaqəli olduğu məlumat bildirişinin bütövlüyünü, dəyişməzliyini, təhrif olunmadığını və saxtalaşdırılmadığını müəyyən etmək;
- **İmtina edilməzlik** – İmza sahibinin nəzarəti altında olan elektron imza vasitələri ilə yaradılma.

EH-SXM-in sertifikat xidmətləri üzrə fəaliyyəti ISO/IEC 27001 Information Security Management System və ISO 9001 Quality Management System uyğun olaraq hazırlanmış daxili təlimatlar əsasında həyata keçirilir.

1.1 İstifadəçilər və tətbiq sahəsi

Bu Qaydalar EH-SXM-in fəaliyyəti, həmçinin aşağıdakı açar və Sertifikatların fəaliyyət dövrünün idarə edilməsi ilə bağlı məsələləri əhatə edir:

- Verilmiş Sertifikatlar reyestrini və CRL-i (Ləğv edilmiş Sertifikatlar siyahısını) imzalamaq üçün EH-SXM-in Sertifikatı;
- EH-SXM-in etibarlı OCSP-responderinin (Sertifikatların onlayn yoxlanılması protokolunun) Sertifikatı;
- Təhlükəsiz imza yaratma üçün İmza sahibinin təkmil Sertifikatı; və
- Təhlükəsiz autentifikasiya üçün İmza sahibinin qeyri-təkmil Sertifikatı.

Bu Qaydaların istifadəçiləri EH-SXM-in verdiyi Sertifikatlarla əlaqəli olan bütün tərəflərdir. Bu Qaydalar EH-SXM-in tərəfindən verilən infrastruktur Sertifikatlarına şamil edilmir və onlarla bağlı məsələlər daxili sənədlərlə tənzimlənir.

1.2 Sənədin adı və identifikasiyası

Bu Qaydalar EH-SXM-ə aiddir və cari versiyası, həmçinin digər əlaqəli sənədlər http://www.e-imza.az/ ünvanında yerləşir.

Adı:	EH-SXM-in Sertifikatın tətbiqi qaydaları
Versiyası:	Versiya 1.0
Tarixi:	19 avqust 2010
Etibarlılığı:	Sənədin cari versiyası növbəti buraxılışa qədər qüvvədədir.
OID:	1.3.6.1.4.1. 32843.7.1

Bu Qaydalar EH-SXM tərəfindən 19 avqust 2010 tarixində təsdiqlənmişdir. Sənədin adı, təsdiqlənmə tarixi, versiyası sənədin üz qabığında əks edilir.

1.3 Sertifikat siyasətinin identifikasiyası

Bu Qaydalar EH-SXM-in Sertifikat siyasətinin (OID 1.3.6.1.4.1.32843.9.1) tələblərinə uyğun olaraq Sertifikatların verilməsi, idarə edilməsi, qüvvəsinin dayandırılması və ləğv edilməsi ilə bağlı prosesləri əks etdirir.

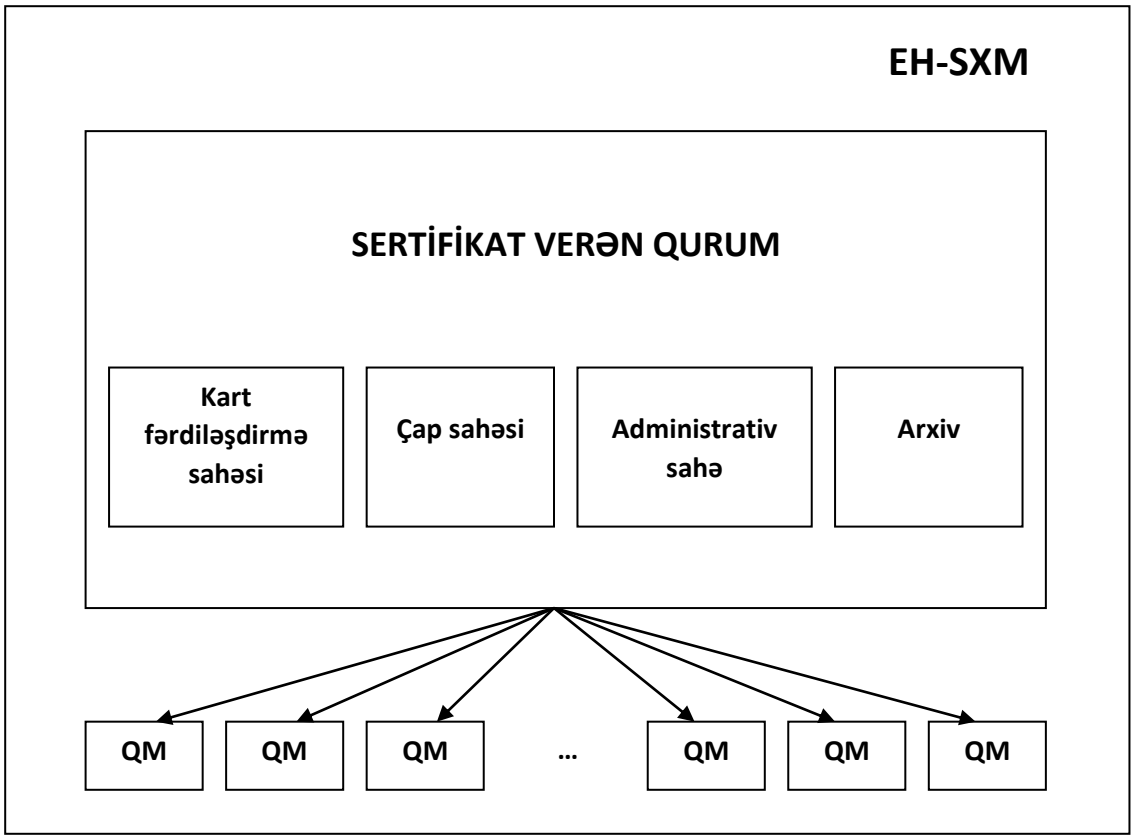
EH-SXM-in Sertifikat siyasətini http://www.e-imza.az ünvanında əldə edilə bilər.

1.4 Tərəflər

Tərəflər olaraq bu Qaydalarda hüquq və öhdəlikləri təsvir olunan EH-SXM-in qurumları, Sertifikat xidmətlərinin istehlakçıları və istifadəçiləri hesab edilir.

1.4.1 EH-SXM-in strukturu (iyerarxiyası)

EH-SXM-in tərkibinə Sertifikat verən qurum və Qeydiyyat Mərkəz(lər)i daxildir. EH-SXM Sertifikatın verilməsini öz Sertifikat siyasəti çərçivəsində həyata keçirir. Diaqramda EH-SXM-in iyerarxik quruluşu göstərilir:



1.4.1.1 Sertifikat verən qurum

Sertifikat verən qurum Sertifikat xidmətlərinin göstərilməsi ilə bağlı olaraq Sertifikatların hazırlanması və verilməsinə məsuldur.

1.4.1.2 Qeydiyyat Mərkəzi

Qeydiyyat Mərkəzi Sertifikat almaq üçün EH-SXM-ə olan müraciətlərə baxılması, sertifikatların qüvvəsinin dayandırılması, bərpası və ləğvi ilə bağlı İmza sahibinə xidmətlər göstərir. Mərkəz İmza sahibi barədə yazılar yaradır, onun identikləşdirməsini və məlumatların yoxlanılmasını, Sertifikat sorğusunun yaradılmasını və EH-SXM-ə göndərilməsini həyata keçirir.

1.4.1.3 İmza sahibi

İmza sahibi EH-SXM-ə müraciət etmiş, identifikasiya və autentifikasiya olunmuş, Sertifikat almış fiziki şəxsdir.

1.4.1.4 Üçüncü tərəf

EH-SXM tərəfindən verilmiş Sertifikata müvafiq Gizli açarla yaradılmış elektron imza ilə imzalanmış sənədi almış və aidiyyəti Sertifikatı yoxlamış şəxsdir.

1.4.1.5 Digər tərəflər

EH-SXM-in hər hansı Sertifikat xidmətlərinin yerinə yetirilməsi həvalə edilmiş qurum sayılır. Hal-hazırda bütün xidmətlər tam olaraq EH-SXM tərəfindən həyata keçirildiyi üçün digər tərəf mövcud deyildir.

EH-SXM müqavilə əsasında digər tərəflərə xidmətlərin həyata keçirilməsini həvalə edə bilər və bu zaman digər tərəf bu Qaydaların tələblərinə riayət etməli, xidmətləri dəqiq və tam yerinə yetirməli, konfidensiallıq və fərdi məlumatların qorunmasını təmin etməlidir.

1.5 Sertifikatların istifadəsi

1.5.1 Düzgün istifadə halları

EH-SXM-in Sertifikatları təyinatına və istifadə sahələrinə müvafiq olaraq tətbiq edilməlidir. EH-SXM-in təkmil Sertifikatları əl imzası tələb olunan hallarda gücləndirilmiş elektron imza yaratmaq məqsədilə istifadə edilir. Elektron Hökumət, elektron ticarət və digər bu kimi sahələrdə sənəd və formaları, işgüzar müqavilə və sazişlər kimi rəsmi sənədləri, elektron məktubları, İnternet vasitəsilə həyata keçirilən əməliyyatları (tranzaksiyaları) imzalamaq, şəbəkə mühitində autentifikasiya vasitələri ilə şəxsin kimliyini təsdiq etmək Sertifikatların düzgün istifadə halları sayılır.

İnfrastruktur Sertifikatları avadanlıqların (serverlərin) etibarlı işinin təmin edilməsi məqsədilə avadanlığın tanınmasını həyata keçirmək və etibarlı istifadə kanalının yaradılması üçün istifadə edilir.

1.5.1.1 Qadağan olunmuş istifadə halları

EH-SXM-in təkmil Sertifikatlarının Azərbaycan Respublikasının qanunvericiliyinə uyğun olaraq təkmil Sertifikatlardan və onlara əsaslanan gücləndirilmiş elektron imzalardan istifadənin məhdudlaşdırıldığı hallarda tətbiqi qadağandır.

1.6 Fəaliyyət siyasəti

EH-SXM Sertifikat xidmətlərini təmin edən mərkəz olaraq bu Qaydaların Sertifikat siyasətinə müvafiq müəyyənləşdirilməsinə və həyata keçirilməsinə məsuldur.

1.6.1 Qaydaların işlənilməsinə məsul mərkəz

Bu Qaydaların müəyyənləşdirilməsi, əlavə və dəyişikliklərin edilməsi üzrə bütün hüquq və öhdəliklər EH-SXM-ə aiddir.

1.6.2 Əlaqə məlumatları

Bu Qaydalarla bağlı əlaqə üçün aşağıdakı imkanlar mövcuddur:

Rəsmi adı: Elektron Hökumət Sertifikat Xidmətləri Mərkəzi

Poçt ünvanı: AZ1000, Ü.Hacıbəyov küçəsi 36,

Tel: 598-33-40; 493-94-38

Faks: 565-14-52

Zəng Mərkəzi: 157

E-poçt ünvanı: info@e-imza.az

Veb: www.e-imza.az

1.7 Anlayışlar və qısaltmalar

1.7.1 Anlayışlar

Açıq açar	bax. Elektron imzanı yoxlama məlumatları
Açıq açar infrastrukturu	Autentifikasiyanı, şifrlənməni, tamlığı və inkar (imtina) edilməzliyi dəstəkləyə bilən Açıq açarların idarə olunmasını təmin edən infrastruktur
Açıq açar Sertifikatı (PKC)	bax**.** Sertifikat
Akkreditə edilmiş SXM	təkmil Sertifikat vermək hüququ müvafiq icra hakimiyyəti orqanı tərəfindən şəhadətnamə ilə təsdiqlənmiş Sertifikat xidmətləri mərkəzi
Baza CRL	dCRL-in generasiyasında əsas kimi istifadə olunan CRL
SXM-in Sertifikatı	bir SXM tərəfindən digər SXM-ə verilən Sertifikat
CRL paylanma nöqtəsi	CRL-lər üçün direktoriya girişi və ya

	digər paylanma mənbəyi; CRL paylanma nöqtəsi ilə paylanmış CRL SXM tərəfindən verilən tam Sertifikatlar çoxluğunun yalnız bir altçoxluğuna dair ləğvetmə qeydlərini və ya bir neçə SXM tərəfindən verilən ləğvetmə qeydlərini təşkil edə bilər
Delta CRL (dCRL)	istinad olunan baza CRL-in verilməsindən sonra ləğvetmə statusları dəyişən Sertifikatlar üçün qeydlər əks olunan natamam ləğvetmə siyahısı
Elektron imza	digər verilənlərə əlavə edilən və ya onlarla məntiqi əlaqəli olan, İmza sahibini identikləşdirməyə imkan verən verilənlər
Elektron İmza sahibi	öz adından və ya qanunvericilikdə nəzərdə tutulmuş qaydada ona səlahiyyət vermiş şəxs adından çıxış edən fiziki şəxs
Elektron imza vasitələri	elektron imza yaradılması və yoxlanılması, eləcə də imza yaratma və yoxlama məlumatları yaratmaq üçün istifadə edilən proqram və texniki vasitələr
Elektron imza yaratma məlumatları	elektron imza yaratmaq üçün istifadə edilən və ancaq İmza sahibinə bəlli olan kod və ya

	kriptoqrafik açardan ibarət təkrarolunmaz verilənlər;
Elektron imzanı yoxlama məlumatları	elektron imzanın həqiqiliyini yoxlamaq üçün istifadə edilən kod və ya kriptoqrafik açardan ibarət olan və elektron imza yaratma məlumatlarına uyğun təkrarolunmaz verilənlər;
Elektron imzanın həqiqiliyi	elektron imzanı yoxlama məlumatları vasitəsilə yoxlanılan elektron imzanın sahibinə məxsus olmasının, imzanın əlaqəli olduğu məlumat bildirişinin bütövlüyünün, dəyişdirilmədiyinin və təhrif edilmədiyinin təsdiqi
Elektron sənəd	informasiya sistemində istifadə üçün elektron formada təqdim edilən və elektron imza ilə təsdiq olunmuş sənəd
Etibar	ümumi halda qeyd etmək olar ki, bir şəxs digər şəxsə onun dəqiq gözlədiyi kimi hərəkət edəcəyini ehtimal edərək etibar edir. Bu etibar yalnız konkret funksiyalara tətbiq oluna bilər. Bu strukturda “etibarın” əsas rolu autentifikasiya edən şəxs və mərkəz arasında əlaqəni təsvir etməkdən ibarətdir; şəxs əmin olmalıdır ki, o, mərkəzin yalnız

	qüvvədə olan və etibarlı Sertifikatlar verdiyinə etibar edə bilər
Etibar dayağı	Açıq açara əlavə olaraq aşağıdakı məlumat toplusudur: alqoritm identifikatoru, Açıq açar parametrləri (tətbiqə yararlıdırsa), Gizli açar sahibinin Məxsusi adı və etibarlılıq müddəti. Etibar dayağı özüimzalanmış Sertifikatlar formasında təmin edilə bilər. Etibar dayağı Sertifikat istifadə edən sistem tərəfindən etibarlı sayılır və Sertifikat yollarında Sertifikatları yoxlamaq üçün istifadə olunur
Etibar edən tərəf	**Qərarlar qəbul edərkən Sertifikatda olan məlumatlara etibar edən istifadəçi və ya agent**
Gizli açar	bax. Elektron imza yaratma məlumatları
Gücləndirilmiş autentifikasiya	**Kriptoqrafik metodların köməyi ilə aparılan autentifikasiya**
Gücləndirilmiş elektron imza	İmza sahibinin nəzarəti altında olan elektron imza vasitələri ilə yaradılan və yalnız İmza sahibinə məxsus olmaqla onu identikləşdirən, əlaqəli olduğu məlumat bildirişinin bütövlüyünü, dəyişməzliyini, təhrif olunmadığını və saxtalaşdırılmadığını müəyyən etməyə imkan verən

	elektron imza
Heş funksiya	Qiymətləri böyük (mümkün qədər çox böyük) oblastdan daha kiçik oblasta çevirən (riyazi) funksiya. “Yaxşı” heş funksiya o funksiyadır ki, oblastdakı (böyük) qiymətlər çoxluğuna funksiyanın tətbiqinin nəticələri diapazon üzrə müntəzəm paylanmış (və yəqin ki təsadüfi olaraq) olsun
İmza sahibi	bax Elektron İmza sahibi
İmza sahibi barəsində məlumatlar	**Sertifikat alarkən İmza sahibinin bildirdiyi və sistemin işi zamanı onun barəsində toplanılan məlumatlar**
İmza vasitələri	bax Elektron imza vasitələri
Ləğv edilmiş Sertifikatlar siyahısı (CRL)	Sertifikat verən tərəfindən artıq etibarlı sayılmayan Sertifikatlar toplusundan ibarət imzalanmış siyahı. Ümumi CRL terminindən əlavə, CRL-in xüsusi tətbiq sahələrini əhatə edən bəzi konkret növləri müəyyən edilmişdir
Məlumat bildirişi	məlumatın verilənlər daşıyıcısında yazılmış forması
Məlumatın konfidensiallığı	Bu xidmət məlumatın icazəsiz açılmadan qorunması üçün istifadə edilə bilər. Məlumatın

	konfidensiallığı xidməti autentifikasiya strukturu vasitəsilə dəstəklənir. O, məlumatın ələ keçirilməsinə qarşı mühafizə kimi istifadə oluna bilər
Özüimzalanmış Sertifikat	Sertifikatı imzalamaq üçün SXM tərəfindən istifadə olunan Gizli açarın Sertifikatda təsdiqlənən Açıq açara uyğun gələn özüverilmiş Sertifikatların xüsusi halı. SXM Açıq açarı və ya əməliyyatları barədə digər məlumatları elan etmək üçün özüimzalanmış Sertifikatdan istifadə edə bilər
Sertifikat	İmza sahibini identikləşdirmək üçün nəzərdə tutulan və elektron imzanı yoxlama məlumatlarının İmza sahibinə məxsus olması barədə Sertifikat xidmətləri mərkəzinin verdiyi kağız və ya elektron sənəd
Sertifikat Xidmətləri Mərkəzi (SXM)	elektron imza üçün Sertifikat verən və imzaların istifadəsi üzrə bu qanunla müəyyən edilmiş digər xidmətləri göstərən hüquqi şəxs və ya hüquqi şəxs yaratmadan sahibkarlıq fəaliyyəti ilə məşğul olan fiziki şəxs
Sertifikat istifadəçisi	**digər şəxsin atributlarını və/və ya Açıq açarını dəqiq bilmək istəyən**

	şəxs
Sertifikat siyasəti	Sertifikatın ümumi təhlükəsizlik tələbləri olan konkret cəmiyyətə və/və ya sinfə tətbiq edilməsinin mümkünlüyünü göstərən müəyyən edilmiş qaydalar toplusu. Məsələn, verilmiş qiymət həddi daxilində əmtəə ticarəti üçün elektron məlumat mübadilə əqdinin təsdiqlənməsinə sertifikat növünün tətbiq olunmasını əks edən ayrıca Sertifikat siyasəti
Sertifikat yolu	Direktoriyanın məlumat ağacında başlanğıc obyektin Açıq açarı ilə sonuncu obyektin Açıq açarını əldə etmək üçün istifadə olunan obyektlərin Açıq açar Sertifikatlarının nizamlanmış ardıcıllığı
Sertifikatın etibarlılığının yoxlanması	Sertifikat yolunun qurulması və hazırlanması daxil olmaqla Sertifikatın və həmin Sertifikat yolunda olan bütün Sertifikatların hazırkı vaxtda etibarlı olmasının (yəni vaxtı bitməyib və ya ləğv edilməyib) təsdiq edilməsi prosesi
Sertifikatın seriya nömrəsi	SXM-in daxilində unikal olan və həmin mərkəzin verdiyi Sertifikatla birmənalı əlaqəli olan tam ədəd

Sertifikatın tətbiqi qaydaları	Sertifikat Xidmətləri Mərkəzinin Sertifikatları verərkən istifadə etdiyi tətbiq qaydaları
Sertifikatlaşdırılmış elektron imza vasitələri	**müəyyən olunmuş tələblərə uyğunluğu Sertifikatlaşdırma qaydaları əsasında təsdiq edilmiş elektron imza vasitələri**
Təhlükəsizlik siyasəti	təhlükəsizlik xidmətləri və vasitələrinin istifadəsini və təmin edilməsini idarə edən, təhlükəsizlik mərkəzi tərəfindən müəyyən edilmiş qaydalar toplusu
Təkmil Sertifikat	akkreditə edilmiş SXM tərəfindən gücləndirilmiş elektron imzanı yoxlama məlumatları barəsində verilən Sertifikat
Vaxt göstəricisi	müəyyən vaxt anında məlumat bildirişinin ona təqdim edilməsi barədə akkreditə edilmiş mərkəzin elektron qeydi

1.7.2 Qısaltmalar

Bu Qaydalarda aşağıdakı qısaltmalar tətbiq olunur:

CA	Certification Authority	Sertifikat Xidmətləri Mərkəzi (SXM)
CRL	Certificate Revocation	Ləğv edilmiş Sertifikatlar

	List	siyahısı
CN	Common Name	Ümumi ad
CP	Certificate Policy	Sertifikat siyasəti
CPS	Certification Practice Statement	Sertifikatın tətbiqi qaydaları
CSP	Certification Service Provider	Sertifikat xidməti provayderi (bax SXM)
dCRL	Delta Certificate Revocation List	Delta CRL
DIB	Directory Information Base	Direktoriyanın informasiya bazası
DIT	Directory Information Tree	Direktoriyanın məlumat ağacı
DN	Distinguished Name	Məxsusi adlar
DSEDL	Digital Signature and Electronic Documents Law	Elektron imza və elektron sənəd haqqında Azərbaycan Respublikasının Qanunu
I&A	Identification and Authentication	İdentifikasiya və Autentifikasiya
ID	Identification	İdentifikasiya
ISO	International Organisation for	Beynəlxalq Standartlaşdırma

	Standardisation	Təşkilatı
EGOV CSP ICA	Issuing CA of e-Government Certification Center	Elektron Hökumət Sertifikat Xidmətləri Mərkəzi (EH-SXM)
OCSP	Online Certificate Status Protocol	Sertifikatların onlayn yoxlanılması protokolu
O	Organisation	Təşkilat
OID	Object Identifier	Obyekt identifikatoru
OU	Organisational Unit	Təşkilati qurum, şöbə
PKC	Public-Key Certificate	Açıq açar Sertifikatı
PKCS	Public-Key Cryptography Standards	Açıq açar kriptoqrafiya standartı
PKI	Public-Key Infrastructure	Açıq açar infrastrukturu
QC	Qualified Certificate	Təkmil Sertifikat
RA	Registration Authority	Qeydiyyat Mərkəzi
RFC	Request for Comments	Şərh üçün sorğu
RSA	A specific public key algorithm	Xüsusi Açıq açar alqoritmi
SSCD	Secure Signature	Təhlükəsiz imza yaratma

Creation Device	qurğusu

2 Yayımlanma və saxlama məsuliyyəti

2.1 Direktoriya və sertifikatın yoxlanılması xidmətləri

2.1.1 Direktoriya xidmətləri

EH-SXM Direktoriya xidmətləri LDAP və HTTP vasitəsilə aşağıdakılara onlayn giriş təmin edilən xidmətlərdir:

- EH-SXM tərəfindən verilmiş yayımlanan Sertifikatlar, Ali Mərkəzin və tabelikdə olan SXM-lərinin Sertifikatları;
- Ali Mərkəzin, həmçinin onun tabeliyində olan mərkəzlərin CRL-ləri (EH-SXM daxil olmaqla).

EH-SXM tərəfindən imza sahiblərinə verilən Sertifikatlar yalnız LDAP vasitəsilə yayımlanır (bu Sertifikatlar HTTP ilə yayımlanmır) və bu Sertifikatlara giriş məhduddur.

Sertifikatların yayımlanması yalnız İmza sahibinin razılığı olduqda mümkündür.

2.1.1.1 Sertifikatların saxlanma müddəti

Sertifikatlar EH-SXM-in Direktoriya xidmətləri tərəfindən Sertifikatların müddəti başa çatdıqdan sonra 15 il ərzində saxlanılacaqdır. Bu imzanın sahibinin kimliyini müəyyən etməyə imkan verəcəkdir. Bütün sənədlər və məlumatlar kağız və elektron formada EH-SXM-in mərkəzləşdirilmiş arxivində Azərbaycan Respublikasının müvafiq qanunvericiliyinin tələblərinə uyğun olaraq saxlanacaqdır.

2.1.1.2 CRL-in saxlanma müddəti

EH-SXM-in verdiyi CRL-lər Direktoriya xidmətləri tərəfindən CRL-in müddəti başa çatdıqdan sonrakı 15 il ərzində saxlanılacaq. Buna görə də istənilən vaxt Sertifikatın etibarlılığını yoxlamaq mümkün olacaq.

2.1.2 Sertifikatın etibarlılığının yoxlanması xidmətləri

EH-SXM tərəfindən verilən Sertifikatların etibarlılığının yoxlanması OCSP-responder vasitəsilə təmin edilir. Bütün Sertifikatlar OCSP-responder tərəfindən istənilən vaxt yoxlanıla bilər. Sertifikatların etibarlılığının yoxlanması xidmətlərindən istifadə fasiləsiz olaraq 24 saat 7 gün (24x7) ərzində mümkün olacaq.

Sertifikatın statusu “aktiv”dən “ləğv edilmiş”ə dəyişdirildikdə müvafiq olaraq Sertifikat rəsmi ləğv edilmiş və ya qüvvəsi dayandırılmış hesab olunur. Bu Sertifikatın qüvvəsinin dayandırılması və ya ləğv edilməsi sorğusundan sonra baş verir. Sertifikatın cari vəziyyəti OCSP-responder vasitəsilə yoxlanıla bilər. EH-SXM sorğu aldıqdan sonra 24 saat ərzində OCSP-responder vasitəsilə yoxlamaqla Sertifikatın statusunun aktuallaşdırılmasına zəmanət verir. Müvafiq delta CRL sorğu alındıqdan sonra ən geci 3 saat ərzində yayımlanacaq.

Şübhə yarandıqda Üçüncü tərəf Sertifikatın statusu barədə ən düzgün informasiyanı EH-SXM-in etibarlı OCSP-responderi vasitəsilə əldə etməlidir.

2.1.2.1 Yoxlanılma xidmətlərinin növləri

Sertifikatların OCSP-dən yoxlanılması CRL vasitəsilə yoxlanılmadan daha əlverişlidir, çünki OCSP Sertifikatın ləğvi (dayandırılması) barədə vaxta müvafiq daha dəqiq məlumat verə bilər.

Ləğv və ya dayandırma haqqında sorğunun və hesabatın qəbulu ilə Sertifikatın statusu haqqında Üçüncü tərəfə açıq olan məlumata edilən

dəyişiklik arasında maksimum gecikmə Sertifikatın etibarlılığının yoxlanılması metodundan asılıdır:

- EH-SXM-in etibarlı OCSP-responderindən istifadə edərək Sertifikatın etibarlılığı 24 saat müddətində yoxlanılmalıdır.
- Delta CRL-dən istifadə edərək Sertifikatın etibarlılığı 3 saat müddətində yoxlanılmalıdır.

2.1.2.2 Ali SXM-in Sertifikatının ilkin yoxlanışı

Ali SXM-in Sertifikatı özüimzalanan Sertifikat olduğu üçün bu EH-SXM tərəfindən verilən bütün Sertifikatlar üçün etibar dayağıdır. Buna görə də prosedura başlamazdan əvvəl Ali SXM-in heşi yoxlanılmalıdır. Ali SXM Sertifikatının heşi EH-SXM-in saytında əks olunur.

2.1.2.3 Sertifikatın etibarlılığının yoxlanılması haqqında məlumatın təsviri

Sertifikatın etibarlılığının yoxlanılması haqqında məlumatın təsviri aşağıdakı bölmələrdə verilmişdir:

CRL (CRL səbəb kodlarının təsviri): bölmə 4.9.5

OCSP (OCSP-responderin təsviri): bölmə 4.10.2

2.2 İnformasiyanın yayımlanması

Ərizəçilər, imza sahibləri və Üçüncü tərəflər Ərizə, Sertifikatların verilməsi, həmçinin EH-SXM barədə məlumat almaq üçün fasiləsiz olaraq 24 saat 7gün (24x7) fəaliyyətdə olan http://www.e-imza.az saytından istifadə edə bilərlər.

EH-SXM saytda aşağıdakı sənədlərin cari versiyasını yerləşdirəcəkdir:

- Sertifikat xidmətlərinin gцstərilməsi haqqənda təlimat;

- Ənformasiya sistemi, avadanləq və prosedur təhlıkəsizliyinin təsviri;
- EH-SXM-in Sertifikat siyasəti;
- EH-SXM-in Sertifikatın tətbiqi qaydaları;
- Vaxt göstəricilərinin qeyd edilmə siyasəti və Vaxt göstəricilərinin qeyd edilmə qaydası

Bundan əlavə EH-SXM-in saytından aşağıdakı məlumatlar da əldə edilə bilər:

- Sertifikatdan istifadə və smart kartların verilməsi;
- Sertifikat xidmətlərinin göstərilməsi haqqında Müqavilə ɛablonu;
- Sertifikat üçün Ərizə forması(ları);
- EH-SXM barədə məlumat: adı, ünvanı və əlaqə koordinatları;
- Qeydiyyat Mərkəzlərinin siyahısı;
- Ali SXM-in Sertifikatı və onun SHA1 heş funksiyasından istifadə edərək yaradılmış heşi;
- EH-SXM-in Sertifikatı və onun etibarlı xidmətləri (TSA və OCSP-responderin Sertifikatları daxil olmaqla).

2.3 Yayımlanma vaxtı və mütəmadiliyi

Saytda məlumatların yayımlanması üçün vaxt və mütəmadilik ilə bağlı aşağıdakı tələblərə riayət edilməlidir:

Sertifikatlar	Yaradıldıqdan və Ərizəçi tərəfindən qəbul edildikdən dərhal sonra yayımlanacaq
EH-SXM-in CRL-i	Delta CRL (3 saatdan bir), baza CRL (5 gündən bir)
Siyasət, Təlimat	Siyasət və Təlimatlar təsdiq olunduqdan sonra saytda yerləşdiriləcək

2.4 Direktoriyaya daxilolmaya nəzarət

EH-SXM Direktoriya xidmətləri tərəfindən dərc edilən məlumatlar daxilolma növünə görə açıq informasiyadır. EH-SXM səlahiyyəti olmayan şəxslər tərəfindən əlavə etmə, silmə və ya saxlanılan qeydlərin dəyişdirilməsinin qarşısını almaq üçün məqsədəmüvafiq məntiqi və fiziki təhlükəsizlik tədbirləri tətbiq edir.

Sertifikatların mötəbərliyi informasiya bazasında dəyişiklik etmək hüquqlarının və sistemə girişin məhdudlaşdırılması ilə təmin olunur. Bundan başqa EH-SXM Direktoriya xidmətlərinin daxili tamlıq mexanizmi var. EH-SXM tez-tez məlumat fayllarının tamlığını yoxlayır ki, bununla da informasiya bazasının aşağı səviyyəli korlanmasını belə aşkar etmək mümkün olur.

3 İmza sahibinin identifikasiya və autentifikasiyası (İ&A)

3.1 Adlandırma

3.1.1 Ad növləri

EH-SXM tərəfindən verilən bütün Sertifikatların “İssuer” sahəsi X.509 standartındakı Məxsusi adlara malikdir. Aşağıdakı atributlardan istifadə olunur:

Ölkə Adı (C)	AZ
Təşkilat Adı (O)	CSP
Təşkilat bölməsinin Adı (OU)	Certification Services
Ümumi Ad (CN)	AZ e-Government Authority (ICA)

EH-SXM tərəfindən verilən bütün Sertifikatların “Subject” sahəsi X.509 standartındakı Məxsusi adlara malikdir. Aşağıdakı atributlardan istifadə olunur:

Ölkə adı (C)	<İmza sahibinin ölkəsi (ISO 3166 kodu)>
Təşkilat adı (O)	<İmza sahibinin təşkilatı>
Təşkilat bölməsinin adı (OU)	<İmza sahibinin təşkilatının bölməsi>
Ümumi ad (CN)	<Adı> <Soyadı> <Ata adı> və ya <PN: təxəllüs> yalnız təkmil Sertifikatda istifadə olunur
Soyad (SN)	<Soyadı (identifikasiya sənədində yazıldığı kimi)> Təxəllüs olduqda istifadə olunmur
Ad (G)	<Adı (identifikasiya sənədində yazıldığı kimi)> Təxəllüs olduqda istifadə olunmur
Seriya nömrəsi	<unikal ID nömrə (Şəxsi kod)>

İnterfeysdəki “Şəxsi kod” şəxsiyyət vəsiqəsində istifadə olunan koddur.

Gücləndirilmiş imza Sertifikatında “Subject Alternative Name” genişlənməsində İmza sahibinin istəyi ilə Sertifikat Ərizəsinə baxılma prosesində müəyyənləşdirilmiş elektron poçt ünvanı da (Type RFC822 Name) göstərilir.

“Soyad”, “Ad”, “Seriya nömrəsi”, “Ümumi ad”, “Təşkilat adı” və “Təşkilat bölməsinin adı”nın hər biri üçün sətrin maksimal uzunluğu 64 işarədir.

“Ümumi ad”, “Ad”, “Soyad”, “Təşkilat adı”, “Təşkilat bölməsinin adı” və “Titul” atributları UTF-8 kod cədvəlinə uyğun olaraq yazılır. Bu atributlarda UTF-8 kod cədvəlinə uyğun xüsusi işarələr də ola bilər.

Təkmil Sertifikatlar üçün İmza sahibi təxəllüs seçə bilər (3.1.3-ə bax).

3.1.2 Adların mənalı olması zərurəti

Sertifikatdakı “Subject” və “İssuer” sahələrindəki adlar mənalı olmalıdır ki, bu adlar və onların aid olduğu qurumlar arasında mövcud əlaqə EH-SXM-ə aşkar olsun.

3.1.3 İmza sahibinin təxəllüsü

İmza sahibi Sertifikat Ərizəsinə baxılma prosesində özünə təxəllüs seçə bilər. Əgər İmza sahibi təkmil Sertifikatda ad yerinə təxəllüsdən istifadə etmək istəyirsə, bunun təxəllüs olduğu göstərilir (İmza sahibinin əsl şəxsi adından fərqləndirmək üçün “PN:” prefiksi əlavə olunur). Sertifikat kimliyin müəyyənləşdirildiyini, lakin onun aşkar bildirilmədiyini göstərir.

Təxəllüsdən istifadə edilərsə, seçilmiş təxəllüs “Subject” sahəsinin “commonName” (CN) atributunda yerləşdirilir. Bu halda ad və soyad istifadə olunmur.

İmza sahibinin autentifikasiya Sertifikatında təxəllüsdən istifadəyə icazə verilmir.

Bütün hallarda İmza sahibi adını və əlaqə məlumatlarını EH-SXM-ə bildirməlidir. EH-SXM şəxsin adını İmza sahibinin icazə verdiyi tərəfə və ya müvafiq hökumət orqanının yazılı sorğusuna əsasən açıqlaya bilər.

Təxəllüsə görə İmza sahibi özü məsuliyyət daşıyır. EH-SXM təxəllüsün mənasının və yazılışının yoxlanmasını həyata keçirmir. EH-SXM qanuna zidd

təxəllüsün istifadəsi və ya bununla bağlı hər hansı digər səbəbdən Sertifikat Ərizəsinə baxılmasından imtina edə bilər.

3.1.4 Müxtəlif ad formalarının şərhi qaydaları

Sertifikatlarda qeyd olunan adlar X500 standartına uyğun olmalıdır.

3.1.5 Adların unikallığı

Hər bir elektron Sertifikat Məxsusi ad atributlarının unikal dəstinə malikdir. Bu atributlarda şəxsin adı, təşkilatın adı, təşkilatın bölməsi və unikal identifikator cəmləşir. Unikal identifikator ya şəxsiyyət vəsiqəsində istifadə olunan kod və ya EH-SXM tərəfindən verilən (təxəllüs istifadə olunan hər Sertifikat üçün) unikal koddur.

Unikal olmayan hər hansı elektron Sertifikat sorğusu EH-SXM tərəfindən imtina edilir. EH-SXM tərəfindən Ərizəçinin adının unikal olmaması səbəbindən imtina edilmiş Ərizələr haqqında texniki baxımdan mümkün qədər tez bildiriş verilir.

İmza sahibi eyni “Subject” sahəsinə malik iki və ya daha çox Sertifikata sahib ola bilər.

3.1.6 Ticarət nişanlarının tanınması, autentifikasiyası və rolu

3.1.6.1 Açıq və Gizli açarlar

Açıq və Gizli açarların bütün əqli mülkiyyət hüquqları EH-SXM-ə məxsusdur.

3.1.6.2 Sertifikat

Ərizəçinin Sertifikat Ərizəsində digər şəxslərin əqli mülkiyyət hüquqlarını pozan adlardan istifadə etməsi qadağandır. Bununla belə EH-SXM Ərizəçinin Sertifikat Ərizəsində göstərdiyi ada əqli mülkiyyət hüquqlarının olmasını yoxlamır. EH-SXM hər hansı domen adı, əmtəə nişanı və ya xidmət markasına sahibliklə bağlı mübahisələrdə qərar vermir, vasitəçilik etmir və ya onların həllində iştirak etmir.

EH-SXM bu Qaydalarda və müvafiq Sertifikat siyasətində müəyyən edilmiş prosedur və siyasətə uyğun olaraq hər hansı Sertifikatın qüvvəsini istənilən vaxt dayandıra və ya ləğv edə bilər.

3.2 İlkin identiklik yoxlaması

EH-SXM və ya onun Qeydiyyat Mərkəzi Ərizəçinin düzgün identifikasiya və autentifikasiyasını, həmçinin onun Sertifikat sorğusunun tam, dəqiq və lazımi qaydada tərtibinin təsdiqlənməsini təmin edir.

EH-SXM Ərizəçini identikləşdirmək üçün bütün müvafiq məlumatları, münasib olarsa, onun yoxlanması üçün istifadə olunan sənədlərdəki hər hansı istinad nömrələri və etibarlıq müddəti ilə bağlı məhdudiyyətlər də daxil olmaqla Ərizəçinin istənilən məxsusi məlumatlarını qeydə alır.

3.2.1 Fərdin autentifikasiyası

Fərdin autentifikasiyası Ərizəçinin və ya səlahiyyətli nümayəndənin şəxsən (fiziki olaraq) Qeydiyyat Mərkəzində iştirakı ilə təmin edilir. Ərizəçi özünün kimliyini müvafiq orqan tərəfindən verilmiº və qüvvədə olan ºəxsiyyət vəsiqəsi ilə təsdiq etməlidir.

3.2.2 Təşkilatın autentifikasiyası

Ərizəçi hüquqi şəxslə və ya digər təşkilati qurumla əlaqədə identifikasiya olunan şəxs olduqda, autentifikasiya aşağıdakılara əsasən aparılır:

- Ərizəçinin tam adı (adı və soyadı);
- Şəxsiyyət vəsiqəsində istifadə olunan kod və ya eyni adlı digər şəxslərdən mümkün qədər çox fərqləndirmək üçün istifadə olunan başqa atributlar;
- Əlaqəli olduğu hüquqi şəxsin və digər qurumun adı və hüquqi statusu;
- Əlaqəli hüquqi şəxsin və ya digər qurumun dövlət qeydiyyatı barədə məlumat;

- Ərizəçinin hüquqi şəxs və ya digər qurumla bağlılığını təsdiq edən sənəd.

Ərizəçi hər dəfə Sertifikata müəyyən bir təşkilat haqqında məlumatın daxil edilməsini tələb etdikdə, həmin təşkilatdan bununla bağlı yazılı əsas təqdim etməlidir. Bütün hallarda məlumatı təsdiqləyən hüquqi sənədlər ayrıca təqdim olunmalıdır.

3.2.3 Səlahiyyətin yoxlanılması

Əgər Sertifikatda İmza sahibi vəzifəli şəxs kimi qeyd edilirsə, şəxsin iş yeri və onun təşkilatın adından çıxış etmək səlahiyyəti təsdiq olunmalıdır və bu barədə Ərizəçi EH-SXM-ə müvafiq sənəd təqdim etməlidir.

3.2.4 Məlumatın yoxlanılması

Ərizəçi tərəfindən təqdim olunmuş məlumatlar İAMAS-la yoxlanılacaq. Yoxlamanın nəticələri və İlkin identiklik yoxlaması prosedurunun düzgünlüyü rola müvafiq olaraq EH-SXM-in yüksək səlahiyyətli əməkdaşı tərəfindən yoxlanılır.

3.2.4.1 Yoxlanılmayan Məlumatlar

Ərizəçinin e-poçt ünvanı İlkin identiklik yoxlaması zamanı yoxlanılmır (“yoxlanılmayan Ərizəçi məlumatı” adlandırılır).

3.2.5 Gizli açar sahibini müəyyənləşdirmək metodu

EH-SXM-ə təhlükəsiz olaraq göndərilməsi üçün Sertifikat sorğusu PKCS#10-yə uyğun olmalıdır. PKCS#10 Sertifikat sorğusundakı imzanın yoxlanılması müvafiq Gizli açarın əldə edilməsi üçün yetərli əsas verir.

3.3 Yeni açar sorğusu zamanı identifikasiya və autentifikasiya

Açarın yenilənməsi qüvvədə olma vaxtı başa çatmış Sertifikata əsasən İmza sahibi tərəfindən yeni açar əldə edilməsi üçün EH-SXM tərəfindən tətbiq olunan və Ərizəçinin yeni Sertifikatla təmin olunması metodudur.

3.4 Ləğvetmə sorğusu zamanı identifikasiya və autentifikasiya

EH-SXM ləğvetmə sorğusunun etibarlı üsullarla qəbulunu təmin edir. Bu İmza sahibinin yazılı müraciəti vasitəsilə onun sorğusu və identikliyinin təsdiqi əsasında həyata keçirilir.

3.5 Sertifikatın statusunun dəyişdirilməsi barədə sorğu

EH-SXM müvafiq qaydada Sertifikatın qüvvəsinin dayandırılması, bərpa edilməsi və Sertifikatın ləğv edilməsi xidmətlərini həyata keçirir.

Sertifikat qüvvəsinin dayandırılması onun müvəqqəti olaraq etibarsız sayılmasına səbəb olur. Bu Sertifikatın statusu yenidən bərpa oluna (aktivləşdirilə) bilər.

Sertifikat ləğv edildikdə isə onun qüvvədə olmasına xitam verilir və bərpası mümkün deyil.

Sertifikatın statusunun dəyişdirilməsi üçün müvafiq sorğu ilə müraciət olunmalıdır.

3.5.1 İmza sahibi Sertifikatlarının qüvvəsinin dayandırılması sorğusu

İmza sahibi Sertifikatın qüvvəsinin dayandırılması sorğusunu aşağıdakı üsullarla təqdim edə bilər:

- EH-SXM-in Zəng Mərkəzinə zəng edərək. EH-SXM-in Zəng Mərkəzi fasiləsiz olaraq 24 saat/7gün (24x7) fəaliyyət göstərir. Zəng Mərkəzinin əlaqə məlumatlarını bənd 1.6.2-də və ya http://www.e-imza.az ünvanında əldə etmək olar.
- EH-SXM-in Qeydiyyat Mərkəzinə yazılı müraciətlə. Sorğu barədə Ərizəni təqdim etmək üçün İmza sahibi Qeydiyyat Mərkəzinə müraciət etməlidir. EH-SXM-in Qeydiyyat Mərkəzlərinin əlaqə məlumatlarını http://www.e-imza.az ünvanında əldə etmək olar.

- Qanunvericiliklə müəyyənləşdirilmiş səlahiyyətli şəxs (orqan) tərəfindən sorğu verməklə.

Zəng Mərkəzinə telefonla müraciət zamanı İmza sahibinin identikləşdirilməsi üçün müvafiq parolun bildirilməsi tələb olunur. Bu parol Sertifikat Ərizəsi yaradılarkən İmza sahibi tərəfindən müəyyənləşdirilir.

Yazılı müraciət zamanı Qeydiyyat Mərkəzində İmza sahibinin identikləşdirməsi şəxsiyyət vəsiqəsinə əsasən aparılır və onun adı, soyadı, atasının adı, şəxsi kod, müraciətin səbəbi müəyyənləşdirilir.

3.5.2 İmza sahibi Sertifikatını ləğv etmək barədə sorğu

Qanunvericiliklə müəyyən edilmiş şəxslər (bax 4.9.1) EH-SXM-in Qeydiyyat Mərkəzinə Sertifikatın ləğvi barədə yazılı sorğu ilə müraciət edə bilərlər. EH-SXM-in Qeydiyyat Mərkəzlərinin əlaqə məlumatları http://www.e-imza.az ünvanında əldə edilə bilər.

Yazılı müraciət zamanı Qeydiyyat Mərkəzində İmza sahibinin identikləşdirməsi şəxsiyyət vəsiqəsinə əsasən aparılır və onun adı, soyadı, atasının adı, şəxsi kod, müraciətin səbəbi müəyyənləşdirilir.

3.5.3 İmza Sahibi Sertifikatının qüvvəsinin bərpa edilməsi haqqında sorğu

Qanunvericiliklə müəyyən edilmiş şəxslər (bax 4.9.1) EH-SXM-in Qeydiyyat Mərkəzinə Sertifikatın qüvvəsinin bərpa edilməsi barədə yazılı sorğu ilə müraciət edə bilərlər. EH-SXM-in Qeydiyyat Mərkəzlərinin əlaqə məlumatları http://www.e-imza.az ünvanında əldə edilə bilər.

Yazılı müraciət zamanı Qeydiyyat Mərkəzində İmza sahibinin identikləşdirməsi şəxsiyyət vəsiqəsinə əsasən aparılır və onun adı, soyadı, atasının adı, şəxsi kod, müraciətin səbəbi müəyyənləşdirilir.

3.5.4 EH-SXM-in Sertifikatının ləğvi barədə sorğu

EH-SXM-in Sertifikatı dayandırıla bilməz. Lazım gəldikdə bu sertifikat onun etibarlılıq müddəti başa çatmamış da ləğv edilə bilər. Etibarlı SXM Sertifikatlarının ləğvi barədə sorğu yazılı formada kağız üzərində təqdim edilməlidir.

Bütün ləğvetmə sorğuları etibarlı olmalıdır. Ali Sertifikat Mərkəzinin Təhlükəsizlik səlahiyyətlisi EH-SXM Sertifikatının ləğvi barədə sorğunun tam, düzgün və lazımi qaydada avtorizasiya edildiyini təsdiq etməlidir. Belə etibarlılıq yoxlaması sorğuların, onları verə bilən şəxsin səlahiyyəti barədə məlumatlar daxil olmaqla bu Qaydaların prosedurları (bax 3.5.2) ilə uyğun gəlib-gəlmədiyini müəyyən edir.

EH-SXM-in Sertifikatının ləğvi EH-SXM-in rəisi və Ali SXM-in Təhlükəsizlik səlahiyyətlisi ilə əlaqə yaradıldıqdan sonra həyata keçiriləcək.

4 Sertifikatlarla bağlı fəaliyyət tələbləri

Bu bölmədə Sertifikatın fəaliyyət dövründə EH-SXM, Ərizəçi, İmza sahibi, Üçüncü və digər tərəflərin həyata keçirdiyi fəaliyyətin əsasları açıqlanır.

4.1 Sertifikat Ərizəsi

4.1.1 Sertifikat Ərizəsini kimlər təqdim edə bilər?

Öz adından və ya qanunvericilikdə nəzərdə tutulmuş qaydada ona səlahiyyət vermiş hüquqi şəxs adından çıxış edən fiziki şəxslər Sertifikat verilməsi üçün Ərizə ilə EH-SXM-ə müraciət edə bilərlər.

4.2 Sertifikat Ərizəsinin emalı

Sertifikat Ərizəsinin emalı prosesi ərizələrin təqdim edilməsini, ərizəçinin identifikasiya və autentifikasiyasını, müraciətlər barədə qərarın qəbul edilməsini əhatə edir.

4.2.1 Sertifikat Ərizəsinin təqdim edilməsi

Ərizəçi Sertifikatın verilməsi üçün EH-SXM-in Qeydiyyat Mərkəzinə gələrək yazılı müraciət etməli və Ərizədə müvafiq məlumatlar doldurulmalıdır.

Ərizəçinin Sertifikatın verilməsi üçün müraciət Ərizəsində olan bütün məlumatlar EH-SXM-in İnformasiya sistemində Azərbaycan Respublikasının müvafiq qanunvericiliyinə əsasən saxlanılacaq, mühafizə ediləcək və arxivləşdiriləcəkdir.

Ərizəçinin müraciətinə əsasən Sertifikatın verilməsi üçün tələb olunan məlumatlar aşağıdakılardır:

Məlumat	Mənbə	Məqsəd
Soyadı, adı, atasının adı	İdentifikasiya sənədi	Sertifikat (təxəllüs istifadə olunmayıbsa)
Smart kartdakı ad	Ərizə forması	Smart kart
Təxəllüs	Ərizə forması	Sertifikat
Doğum tarixi və yeri	Şəxsiyyət vəsiqəsi	Ərizə, onun ləğvi və dayandırılması üçün identifikasiya və autentifikasiya
Poçt ünvanı və əlaqə məlumatları	Ərizə forması	İmza sahibi ilə əlaqələrin idarə olunması
Şəxsi kod	Şəxsiyyət vəsiqəsi	Sertifikat
Şəxsiyyəti təsdiq edən sənədinin verilmə tarixi	Şəxsiyyət vəsiqəsi	Şəxsiyyəti təsdiq edən sənədinin yoxlanması

Şəxsiyyəti təsdiq edən sənədin etibarlılıq müddəti	Şəxsiyyət vəsiqəsi	Şəxsiyyəti təsdiq edən sənədin yoxlanması
Şəxsiyyəti təsdiq edən sənədi vermiş ölkə	Şəxsiyyət vəsiqəsi	Şəxsiyyəti təsdiq edən sənədin yoxlanması
Sertifikatın əlavə atributları	Ərizə forması	Sertifikat
Sertifikatın dərc edilməsinə razılıq (bəli/xeyr)	Ərizə forması	Verilmiş Sertifikatların reyestri
Təşkilatın adı	Ərizə forması	Sertifikat
Təşkilatın bölməsi	Ərizə forması	Sertifikat
Təşkilatın qeydiyyat nömrəsi	Ərizə forması	İmza sahibi ilə əlaqələrin idarə olunması (EH-SXM-in informasiya bazasında konfidensial saxlanılır)
Təşkilatın əlaqə məlumatları	Ərizə forması	İmza sahibi ilə əlaqələrin idarə olunması (EH-SXM-in informasiya bazasında konfidensial saxlanılır)
Təşkilat haqqında məlumatın Sertifikata daxil edilməsinə razılıq (bəli/xeyr)	Ərizə forması	İmza sahibi ilə əlaqələrin idarə olunması (EH-SXM-in informasiya bazasında konfidensial saxlanılır)
E-poçt ünvanının Sertifikata daxil edilməsinə razılıq	Ərizə forması	İmza sahibi ilə Əlaqələrin idarə olunması (EH-SXM-in informasiya bazasında

(bəli/xeyr)		konfidensial saxlanılır)
Məlumatların (bildirişlərin) alınması üsulu (poçt və ya e-poçt)	Ərizə forması	İmza sahibi ilə əlaqələrin idarə olunması (EH-SXM-in informasiya bazasında konfidensial saxlanılır)
Gizli sual	Ərizə forması	Dayandırma sorğusunun telefonla verilməsi zamanı identikləşdirmə
Gizli sualın cavabı (parol)	Ərizə forması	Dayandırma sorğusunun telefonla verilməsi zamanı identikləşdirmə
Smart kartın alınacağı Qeydiyyat Mərkəzi	Ərizə forması	İmza sahibi ilə əlaqələrin idarə olunması (EH-SXM-in informasiya bazasında konfidensial saxlanılır)

Qeydiyyat Mərkəzinə müraciət zamanı bənd 3.2-də təsvir olunmuş ilkin identiklik yoxlaması proseduru həyata keçirilir:

- Fərdin autentifikasiyası (bax. 3.2.1);
- Təşkilatın autentifikasiyası (bax. 3.2.2.);
- Səlahiyyətin yoxlanılması (bax. 3.2.3).

Qeydiyyat məlumatları doldurulduqdan və ilkin identiklik yoxlamasından sonra müvafiq formalı Ərizə çap edilir, Ərizəçi və Qeydiyyat operatoru tərəfindən imzalanır. Ərizənin imzalanması ilə Ərizəçi həmçinin Sertifikatın verilmiş Sertifikatlar reyestrində yayımlanması üzrə mövqeyini müəyyənləşdirmiş olur.

Ərizə hüquqi və ya fiziki şəxsin nümayəndəsi tərəfindən verildiyi təqdirdə nümayəndənin Ərizəçi adından müraciət etmək səlahiyyəti notarial qaydada təsdiq olunmuş etibarnamə ilə müəyyən olunur.

Qeydiyyat operatoru Sertifikatın istifadəsi, Gizli açar və smart kartların bu Qaydalarda müəyyən olunmuş istifadə qaydaları, lazımi təhlükəsizlik tədbirləri barədə Ərizəçini məlumatlandırır.

Bu mərhələdən sonra İnformasiya sistemi vasitəsilə Ərizə barədə məlumatlar Qeydiyyat səlahiyyətlisinə göndərilir.

4.2.2 Sertifikat Ərizəsinin təsdiqi və ya ondan imtina edilməsi

Qeydiyyat səlahiyyətlisi Ərizəçi barədə identikləşdirmə məlumatlarını yoxlamaq üçün informasiya bazasındakı və İAMAS-dakı məlumatlardan istifadə edir və aşağıdakıları əsas götürərək Ərizəni təsdiq və ya ondan imtina edir:

- Sertifikat Ərizəsində şəxs haqqında düzgün, lazımi və tam məlumat verilməsini;
- Ərizənin bu Qaydalara uyğun olaraq icra edildiyini.

Sertifikat Ərizəsindən aşağıdakı hallarda imtina edilə bilər:

- İdentifikasiya sənədi etibarlı olmadıqda;
- Ərizəçi bu Qaydaların 3.1.3 və 4.1.1 bəndlərində nəzərdə tutulmuş şərtlərə uyğun gəlmədikdə;
- Bu Qaydaların 3.2 bəndində nəzərə tutulmuş ilkin identiklik yoxlaması üçün tələb olunan məlumatların identifikasiyası və autentifikasiyası tamamlanmadıqda;
- İAMAS-da heç bir məlumat olmadıqda və ya məlumatların Ərizədə göstərilmiş məlumatlara uyğun gəlmədikdə;
- Ərizə forması Ərizəçi və ya Qeydiyyat operatoru tərəfindən imzalanmadıqda.

Ərizə yoxlanılıb təsdiq edildikdən sonra Qeydiyyat səlahiyyətlisi autentifikasiya Sertifikatı ilə özünü EH-SXM-in informasiya sistemində identifikasiya edir və smart kart istehsalı haqqında sorğu göndərir. Göndəriş təhlükəsiz VPN kanalı vasitəsilə həyata keçirilir.

4.2.3 Sertifikat Ərizəsinin emal müddəti

Sertifikat ərizəsinin emalı 2 iş günü ərzində həyata keçirilir.

Sertifikat Ərizəsi imtina və ya ləğv edilənə qədər aktiv qalır.

4.3 Sertifikatın verilməsi

4.3.1 Sertifikatın verilməsi zamanı EH-SXM-in fəaliyyəti

Ərizə təsdiq edildikdən sonra (bənd 4.2.2) Qeydiyyat səlahiyyətlisi smart kartın hazırlanması, Açıq və Gizli açarların yaradılması sorğusunu formalaşdırır. Smart kart sorğusu alındıqdan sonra EH-SXM-də Sertifikatın verilməsi prosesi təhlükəsiz olaraq aşağıdakı kimi həyata keçirilir:

- Seçilmiş smart kartlar üçün PİN və PUK kodlar yaradılır;
- Təhlükəsiz imza yaratma qurğusu (SSCD) ilə smart kartdakı imza Sertifikatı üçün açar cütü yaradılır;
- Lazımi sayda Sertifikat sorğuları yaradır və autentifikasiya olunmuş və şifrlənmiş əlaqə kanalları ilə Sertifikat verən quruma göndərilir. Bu məqsədlə Açıq açar SSCD-də oxunur və PKCS#10 Sertifikat sorğusu PKCS#7 formatında imzalanmış məlumat paketinə daxil edilir;
- EH-SXM-in Sertifikat verən qurumu Sertifikat sorğusunun etibarlılığını aşağıdakı yollarla təsdiq edir:
  - Sertifikat sorğusunun imzasını yoxlamaqla;
  - Sertifikat sorğusu haqqında məlumatın strukturunu, məzmununu və tamlığını yoxlamaqla;
  - Sertifikat sorğusuna uyğun smart kart sorğusunun mövcudluğunu yoxlamaqla;

– Sertifikat sorğusundakı məlumatları təsdiq edilmiş Ərizələrlə müqayisə edərək;

- Yoxlama müsbət nəticələndikdə EH-SXM-in Sertifikat verən qurumu Ərizəçinin identifikasiya məlumatlarını Gizli açarla əlaqələndirən və elektron imza ilə imzalanmış Sertifikat yaradır;
- Tərkibində Sertifikatlar barədə informasiya olan nəticə ismarışı (mesajı) yaradır, autentifikasiya olunmuş və şifrlənmiş əlaqə kanalı ilə cavab ismarıcı (mesajı) göndərir;
- Sertifikatlar smart karta yazılır və smart kartların fiziki fərdiləşməsi həyata keçirilir;
- PİN məktubu hazırlanır;
- Müqavilə tərtib edilib çap olunur;
- Təkmil imza Sertifikatı kağız üzərində çap edilir.

4.3.2 Sertifikatların verilməsi bildirişi

Sertifikatlar yaradıldıqdan sonra EH-SXM Ərizəçiyə hazırlanmış PİN məktubunu və smart kartın alınmasına dəvət barədə Bildiriş göndərir. Bildirişdə smart kartın alınmasının son müddəti, alınma məntəqəsinin ünvanı göstərilir. Müqavilə, Sertifikatın kağız üzərindəki forması və Sertifikatlar yazılmış smart kart sorğu edən Qeydiyyat Mərkəzinə göndərilir. Qeydiyyat Mərkəzi onları aldıqda bu haqqında Təhvil-təslim jurnalında müvafiq qeydlər edir və təhlükəsiz qaydada saxlanılmasını təmin edir.

4.4 Sertifikatın təqdim edilməsi

Sertifikat təqdim edildikdən sonra Ərizəçi onu aldığını, eyni zamanda Sertifikatdakı məlumatların düzgün olmasını EH-SXM Qeydiyyat Mərkəzinə bildirməlidir. Bu bildiriş alınmayana qədər EH-SXM Sertifikatı aktivləşdirmir.

4.4.1 Sertifikatın təqdim edilmə proseduru

Ərizəçi Sertifikatı almaq üçün şəxsən (və ya onun Sertifikat Ərizəsində göstərdiyi şəxs) Qeydiyyat Mərkəzinə gəlməli və özünün identifikasiya sənədini təqdim etməlidir. Qeydiyyat Mərkəzində Ərizəçinin şəxsiyyəti müəyyənləşdirildikdən sonra Ərizəçi Sertifikatın və imza vasitələrinin istifadə qaydaları, EH-SXM-in hüquqi statusu və akkreditə vəziyyəti barədə məlumatlandırılır. Bundan sonra hazırlanmış Müqavilə, kağız daşıyıcıda və elektron formada smart kartda olan Sertifikat Ərizəçiyə təqdim edilir. 2 (iki) nüsxədə tərtib edilmiş Müqavilə və kağız daşıyıcıdakı Sertifikat Ərizəçi tərəfindən imzalanaraq bir nüsxəsi EH-SXM-ə qaytarılır. Ərizəçi smart kartda yazılmış açarların və kağız daşıyıcıdakı Sertifikatın alınması, həmçinin Mərkəz tərəfindən məlumatlandırılmanın aparılması barədə müvafiq jurnallarda imza edir.

Sertifikat EH-SXM tərəfindən aktivləşdirilir və Ərizəçiyə aid bütün sənədlər arxivləşdirilir.

4.4.2 Sertifikatın EH-SXM tərəfindən yayımlanması

Verilmiş Sertifikatlar EH-SXM-in Direktoriya xidmətlərində aktivləşdirilərək yayımlanır. Sertifikatlarının yayımlanması Ərizəçinin razılığı əsasında həyata keçirilir.

4.5 Açar cütü və Sertifikatdan istifadə

4.5.1 İmza sahibinin Gizli açarı və Sertifikatdan istifadəsi

Sertifikat siyasətinə [2] əsasən hazırlanmış EH-SXM-in təkmil Sertifikatları yalnız təhlükəsiz imzaların yaradılması üçün istifadə oluna bilər. Azərbaycan Respublikasının mövcud qanunvericiliyinə, bu Qaydalara və Sertifikat siyasətinə, imzalanmış Müqaviləyə uyğun olaraq, İmza sahibi malik olduğu Gizli açardan istifadə edərkən aşağıdakıları təmin etməlidir:

- Sertifikatdan onda göstərilmiş istifadə sahələrinə, Gizli açar və imza yaratma vasitələrindən təyinatına müvafiq istifadə edilməlidir;
- İmza sahibinin Müqavilə ilə razılaşması və Sertifikatın məzmununu qəbul etməsindən sonra Gizli açardan istifadəsinə icazə verilir.
- İmza sahibi Gizli açar daşıyıcısını şəxsən təhlükəsiz saxlamalı, Gizli açardan başqasının istifadəsinə yol verməməli və Sertifikatın qüvvədə olma müddəti başa çatdıqda, dayandırıldıqda və ya ləğv edildikdə ondan istifadə etməməlidir;
- Gizli açar daşıyıcısından istifadə üçün giriş kodları (PİN, PUK) gizli saxlanılmalıdır;
- Müqavilə tələblərinə uyğun olaraq, Gizli açarın konfidensiallığının pozulması, onun sui-istifadəsi bəlli olduqda və ya buna şübhə yarandıqda 3 (üç) saat ərzində bu haqda EH-SXM-ə məlumat verməlidir.

4.5.2 Üçüncü tərəfin Açıq açar və Sertifikatdan istifadəsi

Üçüncü tərəf etibar etməsi üçün özü aşağıdakıları qiymətləndirməlidir:

- Sertifikatın bu Qaydalarla məhdudlaşdırılmayan istifadə sahələrinə müvafiq tətbiq olunmasının müəyyənləşdirilməsi. Bu müəyyənləşdirmənin nəticəsinə görə EH-SXM məsuliyyət daşımır;
- Sertifikatın və Sertifikat yolundakı bütün SXM-lərin Sertifikatlarının statusu. Əgər bu Sertifikatlardan hər hansı biri ləğv edilmişdirsə, Üçüncü tərəf İmza sahibinin Sertifikatına və ya Sertifikat yolundakı ləğv olunmuş Sertifikata etibar etməməlidir.

4.6 Sertifikatın dəyişdirilməsi

Sertifikatın dəyişdirilməsi Açıq açarı və ya Sertifikatdakı məlumatları saxlamaqla İmza sahibinə yeni Sertifikatın verilməsidir.

EH-SXM Sertifikat dəyişdirilməsi xidmətini göstərmir.

4.7 Sertifikatın yenilənməsi

Sertifikatın yenilənməsi yeni açar cütünün yaradılması və yeni Açıq açarı təsdiq edən yeni Sertifikatın verilməsidir.

Sertifikatın qüvvədən düşməsinə 30 gün qalmış İmza sahibi EH-SXM tərəfindən məktubla və ya e-poçtla məlumatlandırılır. Sertifikat qüvvədən düşdükdə İmza sahibi bu Qaydaların 4.1-ci bəndinə müvafiq olaraq yeni Sertifikatın alınması üçün müraciət edə bilər.

4.8 Sertifikatın modifikasiyası

EH-SXM mövcud Sertifikata heç bir dəyişiklik etmir, çünki Sertifikata ediləcək dəyişikliklər onun etibardan düşməsinə və Sertifikatın yoxlanılması zamanı mənfi nəticəyə səbəb olur. Sertifikat məlumatlarından hər hansı biri dəyişdikdə EH-SXM dəyişdirilmiş məlumatları özündə əks etdirən yeni Sertifikat verir. Məsələn, İmza sahibinin soyadı dəyişdikdə onu əks etdirən yeni Sertifikat verilməlidir.

Sertifikatdakı məlumatlar dəyişdikdə İmza sahibi mövcud Sertifikatın ləğvi və yeni Sertifikatın alınması üçün müraciət etməlidir.

4.9 Sertifikatın qüvvəsinin dayandırılması və ləğvi

Dayandırma və ləğv sorğuları bu Qaydalardakı prosedur və tələblərə uyğun olmalıdır.

İmza sahibi Sertifikatının qüvvəsinin dayandırılması proseduru 3.5.1-ci, Sertifikatı ləğvetmə proseduru isə 3.5.2-ci bənddə təsvir olunmuşdur.

4.9.1 Kimlər dayandırma və ya ləğvetmə sorğusu verə bilər

Aşağıdakılar bu Qaydaların tələblərinə uyğun olaraq Sertifikatın qüvvəsinin dayandırılması və ya ləğvi barədə müraciət edə bilər:

- İmza sahibi;
- Qanunvericiliklə müəyyənləşmiş səlahiyyətli şəxs (orqan);
- EH-SXM (Bu Qaydaların 4.9.2.1 və 4.9.3.1-ci bəndlərində müəyyən olunmuş hallarda).

Bu prosedurlar EH-SXM-in Dayandırma və ya Ləğvetmə səlahiyyətliləri tərəfindən qanunvericiliyin və bu Qaydaların tələblərinə müvafiq şəkildə həyata keçirilir.

4.9.2 Dayandırma

4.9.2.1 Dayandırma halları

EH-SXM aşağıdakı hallarda dərhal Sertifikatın qüvvəsini dayandırır:

- Müvafiq sorğu alındıqda;
- Məhkəmə qərarı olduqda.

EH-SXM tərəfindən verilmiş Sertifikatın qüvvəsinin dayandırılma sorğusu təsdiq olunduqdan sonra dərhal icra olunur.

4.9.2.2 Dayandırma sorğusu proseduru

Qeydiyyat Mərkəzinə yazılı və Zəng Mərkəzinə telefonla müraciət əsasında Sertifikatın qüvvəsinin dayandırılma sorğusu aşağıdakı kimi icra edilir:

Qeydiyyat Mərkəzində:

- Sorğu verən şəxs Dayandırma operatoruna dayandırma barədə müraciət edir;
- Dayandırma operatoru sorğunu düzgün qaydada hazırlayır;

- Bu Qaydaların 3.5.1-ci bəndinə uyğun olaraq həmin şəxsin identikləşdirilməsi həyata keçirilir;
- Dayandırma operatoru özünü (autentifikasiya Sertifikatından istifadə edərək) EH-SXM-in informasiya sistemində autentifikasiya edir;
- Dayandırma operatoru sorğunun emalını başladır;
- Dayandırma səlahiyyətlisi özünü (autentifikasiya Sertifikatından istifadə edərək) EH-SXM-in informasiya sistemində autentifikasiya edərək dayandırma sorğusunu təsdiq və icra edir;
- EH-SXM adi və ya elektron poçt vasitəsilə İmza sahibinə Sertifikatın qüvvəsinin dayandırılması barədə bildiriş göndərir.

Zəng Mərkəzində (157 nömrəli telefona zəng olduqda):

- Sorğu verən şəxs Sertifikatın qüvvəsinin dayandırılması barədə müraciət edir;
- Bu Qaydaların 3.5.1-ci bəndinə uyğun olaraq həmin şəxsin identikləşdirilməsi həyata keçirilir;
- Operator gizli sualı verir;
- Sorğu edən şəxs gizli sualı cavablandırır;
- Cavab düzgün olduqda operator Sertifikatın qüvvəsinin dayandırılması sorğusunu hazırlayıb onun emalını başladır;
- Zəng Mərkəzinin səlahiyyətlisi və ya Dayandırma səlahiyyətlisi sorğunun icrasını təmin edir.

4.9.2.3 Sertifikatın qüvvəsinin dayandırılma sorğusunun yerinə yetirilmə müddəti

Sertifikatın qüvvəsinin dayandırılma sorğusunun qəbulu ilə Sertifikatın statusu haqqında Üçüncü tərəfə açıq olan məlumatlara dəyişiklik edilməsi müddəti Sertifikatın etibarlılığının yoxlanması metodundan asılı olaraq ən geci aşağıdakı kimidir:

- EH-SXM-in etibarlı OCSP-responderi – 3 saat;
- Baza CRL ilə yoxlanma – 5 gün.

Üçüncü tərəf Sertifikatın statusu barədə ən aktual məlumatı EH-SXM-in etibarlı OCSP-responderindən əldə bilər.

4.9.2.4 Dayandırma müddətinə məhdudiyyətlər

Sertifikatın verilməsi üçün əsas olan məlumatların düzgünlüyünə və ya İmza sahibinin Gizli açarının təhlükəsizliyinə EH-SXM-in əsaslı şübhələri olduqda Sertifikat 48 saatdan artıq müddətə dayandırıla bilməz, digər hallarda isə müddət məhdudiyyəti yoxdur.

4.9.2.5 Bərpa

Qüvvəsi dayandırılmış Sertifikatlarla aşağıdakı əməliyyatlar aparıla bilər:

- Qüvvəsi dayandırılmış Sertifikat barədə CRL-dəki qeydlər Sertifikatın qüvvədə olma müddəti başa çatanadək dəyişilməz qalır (OCSP-responder Sertifikatın qüvvədə olması barədə sorğunu mənfi cavablandırır);
- Qüvvəsi dayandırılmış Sertifikat üçün CRL-dəki qeydlər həmin Sertifikatın ləğvetmə məlumatları ilə əvəz olunur və yenilənmiş CRL dərc olunur (OCSP-responder Sertifikatın qüvvədə olması barədə sorğunu mənfi cavablandırır);
- Qüvvəsi dayandırılmış Sertifikat bərpa olunur, onun barəsindəki qeydlər CRL-dən silinir və yeni CRL dərc olunur (OCSP-responder Sertifikatın qüvvədə olması barədə sorğunu müsbət cavablandırır);

Bərpa sorğusu sorğu verən şəxs tərəfindən yazılı müraciət əsasında həyata keçirilir.

4.9.2.6 Bərpa sorğusunun yerinə yetirilmə müddəti

Sertifikat bərpa edildikdən sonra 3 saat ərzində delta CRL-də yerləşdirilməlidir.

4.9.3 Ləğvetmə

4.9.3.1 Ləğv edilmə halları

Bu Qaydaların 4.9.1-ci bəndində göstərilmiş şəxslər tərəfindən verilən düzgün Sertifikatı ləğvetmə sorğusu EH-SXM tərəfindən qəbul edildikdən sonra dərhal həyata keçirilir. Dərhal dedikdə əməliyyatların ardıcıllığına müvafiq olaraq tələb olunan, lakin 1 saatdan gec olmayaraq vaxt nəzərdə tutulur. Sertifikatı ləğvetmə sorğusu aşağıdakı hallarda verilir:

- İmza sahibinin müraciəti əsasında;
- Qanunvericiliyə əsasən səlahiyyətli şəxsin (orqanın) qərarı və ya müraciəti əsasında;
- Sertifikatın verilməsi üçün təqdim olunan sənəd və məlumatların saxta, səhv və ya qüvvədən düşmüş olması bəlli olduqda;
- İmza sahibinin Gizli açar üzərində nəzarəti itirildikdə (smart kart itdikdə, konfidensiallıq pozulduqda);
- EH-SXM və İmza sahibi arasındakı Müqavilə şərtlərinə riayət olunmadıqda və ya Müqaviləyə xitam verildikdə;
- Gizli açarın yaradılması üçün tətbiq olunan alqoritm, parametr və vasitələrin imzaların təhlükəsiz istifadəsini təmin edə bilməyəcəyi barədə əsaslı şübhə yarandıqda;
- Qanunvericiliklə müəyyən edilmiş digər hallarda.

4.9.3.2 Sertifikatı ləğvetmə sorğusu proseduru

Sertifikatı ləğvetmə sorğusu verən şəxs EH-SXM-ə müraciət etməlidir. EH-SXM-də Sertifikatı ləğvetmə sorğusu ilə bağlı aşağıdakılar yerinə yetirilir:

- Sorğu verən şəxs Ləğvetmə operatoruna ləğvetmə barədə müraciət edir;
- Ləğvetmə operatoru ləğvetmə sorğusunun düzgün qaydada hazırlanmasını təmin edir;
- Bu Qaydaların 3.5.2-ci bəndinə uyğun olaraq həmin şəxsin identikləşdirilməsi həyata keçirilir;
- Ləğvetmə operatoru özünü EH-SXM-in İnformasiya sistemində autentifikasiya edir (Autentifikasiya Sertifikatından istifadə edərək);
- Ləğvetmə operatoru sorğunun emalını başladır;
- Ləğvetmə səlahiyyətlisi özünü EH-SXM-in informasiya sistemində autentifikasiya edərək (autentifikasiya Sertifikatından istifadə edərək) ləğvetmə sorğusunu təsdiq və icra edir;
- EH-SXM adi və ya elektron poçt vasitəsilə İmza sahibinə Sertifikatın ləğv edilməsi barədə bildiriş göndərir.

4.9.3.3 EH-SXM tərəfindən Sertifikatı ləğvetmə sorğusunun yerinə yetirilmə müddəti

Sertifikatın ləğvetmə sorğusunun qəbulu ilə Sertifikatın statusu haqqında Üçüncü tərəfə açıq olan məlumatlara dəyişiklik edilməsi müddəti Sertifikatın etibarlılığının yoxlanması metodundan asılı olaraq ən geci aşağıdakı kimidir:

- EH-SXM-in etibarlı OCSP-responderi – 3 saat;
- Baza CRL ilə yoxlanma – 5 gün.

Üçüncü tərəf Sertifikatın statusu barədə ən aktual məlumatı EH-SXM-in etibarlı OCSP-responderindən əldə bilər.

4.9.4 Üçüncü tərəf üçün ləğvetmənin yoxlanması tələbi

Üçüncü tərəf əmin olmaq istədiyi Sertifikatın statusunu yoxlaya bilər. Sertifikatın statusunun yoxlanılması üçün Üçüncü tərəf EH-SXM-in Direktoriya xidmətləri vasitəsi ilə baza CRL-dən istifadə edə bilər. Nəzərə almaq lazımdır ki, qüvvəsi dayandırılmış və ya ləğv edilmiş Sertifikatın statusu barədə məlumatlar CRL-də 5 gün ərzində dərc olunur.

Üçüncü tərəf Sertifikatın statusunun yoxlanılması üçün OCSP-responderdən istifadə edərsə, EH-SXM-in daxili Sertifikat bazasından Sertifikat statusuna dair ən aktual məlumatı əldə edə bilər. Sertifikat statusunda aparılmış dəyişikliklər barədə qeydlər EH-SXM-in daxili Sertifikat bazasında dərhal yerinə yetirildiyi üçün Üçüncü tərəfin yoxlama üçün EH-SXM-in etibarlı OCSP-responderindən istifadəsi məsləhət görülür.

4.9.5 CRL səbəb kodları

Sertifikat ləğv olunduqda EH-SXM bunun səbəbini göstərir. Bu məqsədlə RFC 3280-də [8] müəyyənləşdirilmiş aşağıdakı səbəblər istifadə edilmişdir:

CRL səbəb kodu	İzahı
Unspecified	Sertifikat səbəb kodu olmadan və ya müəyyən olunmamış səbəblə ləğv olunub.
keyCompromise	İmza sahibinin Sertifikatla bağlı Gizli açarınının konfidensiallığı pozulub. Bu o deməkdir ki, ya smart kart, ya da parol avtorizasiya olunmamış şəxsin sərəncamındadır. Bu, smart kartın itməsi halını da əhatə edir.
cACompromise	SXM-in Gizli açarının saxlandığı kriptoqrafik modulun (HSM) konfidensiallığı pozulub və o, avtorizasiya olunmamış şəxsin

	sərəncamındadır.
affiliationChanged	Bu səbəb kodu hər iki halda istifadə olunacaq: İmza sahibinin Sertifikatındakı hər hansı əhəmiyyətli məlumat dəyişsə; İmza sahibi Sertifikatın Məxsusi ad atributunda göstərilmiş təşkilatla əlaqəsini kəssə.
Superseded	İmza sahibinin Sertifikatı bərpa edilib. (səbəb yuxarıda göstərilən səbəblərdən fərqli olduqda). EH-SXM Sertifikat dəyişdirilməsi xidmətini göstərmədiyi üçün tətbiq edilmir.
cessationOfOperation	İmza sahibinin EH-SXM-lə əlaqəsi hər hansı səbəbdən kəsilib.
certificateHold	Sertifikatın qüvvəsi dayandırılıb. EH-SXM dayanma zamanı Sertifikata zamin durmayacaq.
removeFromCRL	Əgər Sertifikatın qüvvəsi ‘certificateHold’ səbəb kodu ilə dayandırılsa, Sertifikatı (‘reactivate’) bərpa etmək mümkündür. Bərpa prosesi zamanı Sertifikat hələ də CRL-də qalacaq, amma ‘removeFromCRL’ səbəb kodu ilə göstəriləcək. Qeyd: bu, ‘certificateHold’ səbəbinə xasdır və ancaq delta CRL-lər tərəfindən istifadə olunur.

4.9.6 CRL-in dərc mütəmadiliyi

Yaradılıb və imzalanıb	Növ	Məzmun	Qüvvədə olma müddəti (dərc vaxtı da daxildir)	Dərc vaxtı
Ali SXM	Baza	Ali SXM tərəfindən ləğv edilmiş Sertifikatlar	3 ay (və ləğv edildikdən sonra)	1 həftə
Ali SXM-in Siyasət Sertifikat Mərkəzi	Baza	Ali SXM-in Siyasət Sertifikat Mərkəzi tərəfindən ləğv edilmiş Sertifikatlar	3 ay (və ləğv edildikdən sonra)	1 həftə
EH-SXM	Baza	EH-SXM tərəfindən ləğv edilmiş Sertifikatlar	5 gün	2 gün
	Delta	EH-SXM tərəfindən ləğv edilmiş Sertifikatlar	3 saat	

Qüvvədə olma müddəti və növbəti təzələnmə vaxtı arasındakı müddət CRL-in qüvvədə olmasını göstərir. Texniki səbəblərdən (CRL-in yaradılması vaxt tələb edir) növbəti CRL göstərilən müddətdən əvvəl (dərc vaxtı ərzində) dərc oluna bilər, lakin gec dərc olunmamalıdır.

CRL-də olan Sertifikat qüvvədən düşdükdə, o, növbəti dərc olunan CRL-dən silinəcək və Sertifikatlar bu Qaydaların 2.1.1.1 bəndində müəyyən olunmuş müddətə arxivləşdiriləcəkdir.

4.9.7 CRL üçün maksimal ləngimə

CRL yaradıldıqdan sonra münasib vaxt ərzində Direktoriyaya göndərilir. Bu adətən yaradıldıqdan sonra avtomatik olaraq baş verir.

4.9.8 Sertifikatın statusunun onlayn yoxlanılması imkanı

EH-SXM-in Sertifikat yoxlama xidmətləri OCSP-responder vasitəsilə EH-SXM tərəfindən verilmiş Sertifikatların statusunun onlayn yoxlanılmasını təmin edir.

4.9.9 Ləğvetmənin onlayn yoxlanılması tələbləri

OCSP cavabları EH-SXM-in daxili Sertifikat məlumat bazasındakı Sertifikat statusuna əsaslanır və Sertifikatın statusu dəyişdirildikdən dərhal sonra yerinə yetirilir. EH-SXM Üçüncü tərəflərə cari statusu EH-SXM-in etibarlı OCSP- responderindən istifadə edərək yoxlamağı tövsiyə edir.

Digər bir mexanizm isə EH-SXM Direktoriya xidmətləri ilə yüklənə bilən CRL vasitəsilə Sertifikat statusunun oflayn yoxlanılmasıdır.

4.9.10 Ləğvetmənin yoxlanılmasının digər formaları

Tətbiq edilmir.

4.9.11 Açarın konfidensiallığının pozulması ilə bağlı xüsusi tələblər

Generasiya üçün istifadə olunan alqoritm, parametr və qurğuların, Gizli açardan istifadənin təhlükəsizliyinə şübhə yarandıqda EH-SXM-in Təhlükəsizlik səlahiyyətlisi təhqiqata başlayır. EH-SXM-in Gizli açarının konfidensiallığı pozulduqda onun Sertifikatı dərhal ləğv edilməlidir. Bu halda EH-SXM xidmət göstərdiyi İmza sahiblərini, əlaqədə olduğu SXM-ləri və Üçüncü tərəfi məlumatlandırır və onlara verilmiş Sertifikatların dəyişdirilməsini ödənişsiz təmin edir.

4.10 Sertifikat statusu xidmətləri

EH-SXM-in Sertifikat yoxlama xidməti OCSP-responder vasitəsilə Ali SXM və EH-SXM tərəfindən verilmiş Sertifikatlar üzrə RFC 2560-ya [6] uyğun olaraq Sertifikatların statusunun onlayn yoxlanılmasını təmin edilir.

OCSP-responderə **http://ehm.e-imza.az/ocsp/ocsp.responder** İnternet ünvanında müraciət mümkündür.

4.10.1 Əməliyyat xüsusiyyətləri

Sertifikatın statusunu yoxlamaq üçün OCSP-responderə müraciətə məhdudiyyət yoxdur və autentifikasiya tələb olunmur.

Statusu yoxlamaq üçün EH-SXM-in etibarlı OCSP-responderi aşağıdakı əməliyyatları yerinə yetirir:

- RFC-də müəyyən olunmuş aşağıdakıları nəzərə alaraq Sertifikatın statusu barədə sorğunun düzgünlüyünü yoxlayır:
  - Sorğunun tələblərə müvafiq hazırlanması;
  - Responderin sorğu edilən xidməti təmin etmək üçün konfiqurasiya olunması;
  - Sorğuda responderə lazım olan məlumatın olması;
- Bu yoxlama müvəffəqiyyətsiz olarsa, nəticə barədə cavab hazırlanır və geri göndərilir;
- Yoxlama müvəffəqiyyətli olduqda, OCSP-responder Sertifikatın statusu barədə Sertifikat informasiya bazasına sorğu verir;
- Cavab mesajı hazırlanır və bu, qeyd olunan etibarlı cavablandırma Sertifikatı (EH-SXM OCSP Sertifikatı) ilə əlaqəli olan Gizli açardan istifadə edilərək imzalanır;
- Cavabı sorğu verənə göndərir;

- Sertifikatın statusu haqqında sorğunun tamamlanmasını audit-loqda əməliyyatın statusu ilə birlikdə qeyd edir;

OCSP SHA1 heş alqoritmi və nonce genişlənməsi əsasında etibarlı cavablandırma Sertifikatından istifadə edərək cavabları imzalayır. Etibarlı cavablandırma Sertifikatı qüvvədən düşdükdə və ya ləğv olunduqda, OCSP-responder işini dayandırır. EH-SXM-in etibarlı OCSP-responderi Sertifikatın statusu haqqında məlumatı heç vaxt qüvvədən düşmüş Sertifikatla imzalamır.

Qeyd edək ki, səhvlər haqqında mesajlar imzalanmır.

4.10.2 Cavablar

OCSP-responder Sertifikatın statusu haqqında sorğuları cavablandırdıqda aşağıdakı variantlardan istifadə edir:

OCSP cavabı	İzahı
Aktiv	Sorğunun müsbət nəticəsi halında verilən cavabdır. Bu cavab Sertifikatın qüvvəsinin dayandırılmadığını və ya ləğv olunmadığını göstərir, lakin cavabın yaradıldığı vaxt Sertifikatın qüvvədə olma intervalından kənar da ola bilər.
Ləğv olunub	Sertifikatın ləğv olunduğunu (dayandırıldığını) göstərir.
Naməlum	Sertifikat informasiya bazasında tapılmayıb! Status sorğusu EH-SXM tərəfindən verilməyən və ya bu Qaydaların 2.1.1.1-ci bəndinə uyğun olaraq silinmiş Sertifikat barəsində verilmişdir.

4.11 Sertifikatın etibarlılığının yoxlanması

EH-SXM-in verdiyi Sertifikatların etibarlılığını aşağıdakı üsullarla yoxlamaq olar:

- İnternetə çıxış imkanı varsa, Sertifikatın etibarlılığını OCSP-responderdən istifadə edərək Sertifikat statusu xidmətləri ilə yoxlamaq mümkündür. OCSP ilə Sertifikatın statusunu EH-SXM-in http://www.e-imza.az İnternet ünvanında yoxlamaq olar.
- OCSP-responderdən istifadə etmək imkanı yoxdursa, CRL–dən istifadə etmək olar. Sertifikatda CRL-in dərcini tapmaq üçün yol göstərilmişdir (7-ci bölmə). Əgər Sertifikat CRL-dədirsə, deməli dərc zamanı Sertifikat etibarlı deyil.

OCSP-responderdən istifadə etmək imkanı və qüvvədə olan CRL yoxdursa, onda Sertifikatın etibarlılığı yoxlanıla bilməz.

EH-SXM-in xüsusi hallar üçün məsləhətləri:

Situasiya	Təklif olunan yoxlama metodu
Yaxın zamanda ləğv olunmuş Sertifikat	CRL-in məlumatı gecikə bilər, ona görə də yoxlama üçün OCSP-responder metodu məsləhət görülür.
Yaxın zamanda qüvvəsi dayandırılmış Sertifikat	CRL-in məlumatı gecikə bilər, ona görə də yoxlama üçün OCSP-responder metodu məsləhət görülür.
Yaxın zamanda bərpa edilmiş Sertifikat	CRL-in məlumatı gecikə bilər, ona görə də yoxlama üçün OCSP-responder metodu məsləhət görülür. Yaddaşda saxlanılan CRL tarixçəsindən dayandırma müddətində etibarlılığı yoxlamaq üçün istifadə

	etmək olar.
Vaxtı başa çatmış Sertifikat	Məsləhət görülən yoxlama metodu yaddaşda saxlanılan CRL tarixçəsindən istifadədir.

4.12 Sertifikata xidmətin başa çatması

İmza sahibi EH-SXM-in sertifikat xidmətlərindən istifadəni aşağıdakı hallarda bitirə bilər:

- Yeni Sertifikat almayaraq, verilmiş Sertifikatın qüvvəsinin başa çatmasını gözləmək;
- Yeni Sertifikat almayaraq, verilmiş Sertifikatın qüvvədə olması müddəti bitməmiş onu ləğv etdirmək.

4.13 Açarın saxlamaq üçün başqasına verilməsi

İmza sahibi EH-SXM tərəfindən verilmiş smart kartı, onda olan Gizli açarı və Gizli açar daşıyıcısından istifadə üçün giriş kodlarını başqasına verməməlidir.

5 Vasitələrə, idarəetməyə və fəaliyyətə nəzarət

EH-SXM bu Qaydalarla müəyyənləşdirilən və İnformasiya təhlükəsizliyi AZS 324-2008 (ISO/IEC 27002:2005) [5] Beynəlxalq Standartına əsaslanan təhlükəsizlik tələblərinə riayət edir. Bu siyasətə uyğun EH-SXM-in müstəqil audit tələbləri 8-ci bölmədə təsvir olunmuşdur. EH-SXM-in Təhlükəsizlik təlimatındakı [] həssas təhlükəsizlik məlumatları yalnız EH-SXM ilə razılaşma nəticəsində əldə edilə bilər. Bu tələblərin xülasəsi aşağıda verilmişdir:

5.1 Fiziki təhlükəsizlik nəzarəti

EH-SXM modifikasiyadan mühafizə olunmuş etibarlı sistem və məhsullardan istifadə edir və onlar vasitəsilə həyata keçirilən proseslərdə

texniki və kriptoqrafik təhlükəsizlik təmin edilir. EH-SXM bu Qaydaların təhlükəsizlik tələblərini dəstəkləyən Fiziki təhlükəsizlik qaydalarını [14] həyata keçirir. Fiziki təhlükəsizlik qaydaları və proseduru həssas təhlükəsizlik məlumatlarına malikdir və yalnız EH-SXM ilə razılaşma nəticəsində əldə edilə bilər. Bu tələblər aşağıda qısaca təsvir olunub.

5.1.1 EH-SXM-in yerləşdiyi yer

EH-SXM fiziki olaraq mühafizə olunan mühitdə yerləşməli, informasiya sistemlərindən, onlardakı məlumatlardan açıq və ya gizli yolla icazəsiz istifadənin, ələ keçirilmənin, müdaxilənin aşkara çıxarılması və qarşısının alınması üçün təhlükəsizlik tədbirləri görülməlidir.

5.1.2 Fiziki giriş

EH-SXM-ə və onun informasiya sistemlərinə fiziki giriş daimi nəzarət altındadır.

5.1.3 Enerji və hava təchizatı

Dayanıqlı və davamlı fəaliyyəti təmin etmək üçün EH-SXM elektrik enerjisi ilə fasiləsiz qidalandırma vasitələri və havanın istilik və rütubətinin tənzimlənməsi üçün avadanlıqlarla təchiz edilmişdir.

5.1.4 Su sızması

EH-SXM su sızması nəticəsində fəaliyyətinə dəyə biləcək təsirləri minimuma endirmək üçün müvafiq tədbirləri həyata keçirmişdir.

5.1.5 Yanğının qarşısının alınması və mühafizə

EH-SXM yanğının qarşısını almaq və onu söndürmək üçün müvafiq tədbirləri görmüşdür.

5.1.6 İnformasiya daşıyıcıları

İnformasiya mənbələri və daşıyıcıları kimi istifadə edilən istehsal proqram təminatı, verilənlər (məlumatlar), audit-loqlar və onların ehtiyat nüsxələri, sənəd arxivləri EH-SXM-də təsadüfi zədələnmə (məsələn, su, yanğın, elektromaqnit təsirindən) və icazəsiz fiziki müdaxilədən mühafizə edilir.

5.1.7 Tullantıların məhv edilməsi

EH-SXM-də tullanılması nəzərdə tutulan kağız və elektron informasiya daşıyıcıları, həmçinin qurğular onlarda olan məlumatların həssaslıq səviyyəsinə uyğun və onların bərpa olunmasını istisna edən üsullarla məhv edilir.

5.1.8 Kənar ehtiyat nüsxə

EH-SXM-in kritik sistem məlumatlarının, audit-loqların və digər həssas məlumatların müntəzəm olaraq ehtiyat nüsxələri yaradılır, təhlükəsiz saxlanılması və müvafiq hallarda istifadəsi təmin edilir.

5.2 Prosedurların idarə olunması

5.2.1 Məsul rollar

EH-SXM-in bütün fəaliyyəti EH-SXM-in Təşkilati təsvirində əks olunmuş [13] rollarla bağlıdır. Məsul rollara aşağıdakıları yerinə yetirən rollar aiddir:

- **Təhlükəsizlik səlahiyyətlisi:** təhlükəsizlik tədbirlərinin həyata keçirilməsinə ümumi cavadehlik daşıyır. Həmçinin EH-SXM-in özünün istifadə etdiyi Sertifikatların generasiyası, ləğvi və qüvvəsinin dayandırılmasını təsdiq edir.
- **Sistem səlahiyyətlisi:** EH-SXM-in informasiya sisteminin gündəlik işinə cavabdehdir. Sistemin ehtiyat nüsxəsinin yaradılmasını və bərpasını yerinə yetirmək səlahiyyəti vardır.
- **Sistem administratorları:** Qeydiyyat, Sertifikatın yaradılması, qurğu təchizatı və ləğvetmə üçün EH-SXM-in mötəbər sistemlərinin ilkin quraşdırılması, konfiqurasiyası və saxlanması üçün avtorizasiya olunub.
- **Sistem operatoru:** EH-SXM informasiya bazasının, əməliyyat sisteminin ehtiyat nüsxələrinə və bərpasına avtorizasiya olunub;
- **Sistem auditorları:** EH-SXM-in mötəbər sistemlərinin arxivlərinə və audit-loquna baxmağa avtorizasiya olunub.

Burada qeyd olunan Məsul rolları tutanlar EH-SXM-in Məsul şəxsləri kateqoriyasına aiddir və təşkilatda informasiya təhlükəsizliyi siyasətinin tətbiq edilməsi və həyata keçirməsinə cavabdehdirlər.

5.2.2 Tapşırıqlar üzrə tələb olunan şəxslərin sayı

EH-SXM işləri yerinə yetirilmək üçün vəzifə bölgüsü və həssas tapşırıqların müxtəlif Məsul şəxslər tərəfindən icrasını təmin etmək məqsədilə ciddi nəzarət prosedurları tətbiq edir.

Aşağıdakı qurğulara və onların yerləşdiyi yerə ən azı iki Məsul şəxsin birgə girişi tələb olunur:

- HSM-lər, sistem kartları və fərdiləşdirilməmiş smart kartlara məntiqi və ya fiziki giriş,
- Məlumat arxivlərinə fiziki giriş;

- EH-SXM-in mərkəzi, həssas və kritik sistemlərinə, onların ehtiyat nüsxələrinə məntiqi giriş.

5.2.3 Hər rol üçün identifikasiya və autentifikasiya

Şəxslərin mühafizə olunan yerlərə, kritik sistemlərə girişi smart kart vasitəsilə həyata keçirilir. Smart kartlar təhlükəsizlik sisteminə əvvəlcədən tanıdılır, istifadə zamanı ilkin olaraq şəxsin autentifikasiyası həyata keçirilir və müsbət olan halda əməliyyata icazə verilir.

5.2.4 Vəzifə bölgüsü tələb olunan rollar

Vəzifələrə uyğun rolların bölgüsü aşağıdakılara əsaslanır:

- aparıcı rollara əməliyyat məsələləri və ya təşkilati işlər tapşırıla bilməz;
- qərarverici və məsləhətçi rollara (xüsusən daxili və xarici audit) əməliyyat məsələləri və ya təşkilati işlər tapşırıla bilməz;
- inzibati rollara əməliyyat məsələləri tapşırıla bilməz.

Həssas məsuliyyətlərin bölgüsü zamanı aşağıdakılar qadağandır:

- EH-SXM-in yerləşdiyi yerə giriş hüququ verən şəxslər inzibati vəzifə tuta bilməzlər;
- İstehsal sistemi və şəbəkənin inzibatçılığı müxtəlif şəxslər vasitəsilə həyata keçirilir;
- Sertifikat Ərizəçilərini identifikasiya və autentifikasiya edən şəxslər onlara Sertifikat verə bilməz;

5.3 Kadrların idarə olunması

Məsul şəxs olmağa namizədlərin identifikasiyası onların şəxsən iştirakı ilə şəxsiyyət vəsiqəsi əsasında aparılır. Vəzifəyə uyğunluq bu Qaydaların 5.3.1-ci bəndində təsvir olunmuş yoxlamanın nəticəsində müəyyənləşdirilir. Namizəd Məsul şəxs təyin edildikdən sonra vəzifələrinin icrasına başlamadan

ona qurğularla işləmək və onların yerləşdiyi yerə daxil olmaq üçün səlahiyyətləri müəyyənləşdirilməlidir.

5.3.1 Kadrlara aid tələblər

EH-SXM fəaliyyətinin təmini üçün bilikli, təcrübəli və səriştəli, həmçinin öhdəliklərini yerinə yetirmək bacarığına malik işçi heyətə malik olmalıdır. Vəzifəyə namizədlər bilik, təcrübə və səriştəsini təsdiq edən müvafiq sənədləri təqdim etməlidir. Namizədlər ən azı təhlükəsizlik texnologiyası, kriptoqrafiya, elektron imzanın idarə edilmə infrastrukturu, təhlükəsizliyin qiymətləndirilməsi üzrə texniki normalar, informasiya sistemləri üzrə təcrübəyə malik olmalıdır. Namizədin vəzifəyə uyğun olub-olmamasını müəyyənləşdirmək üçün qabaqcadan yoxlama aparılır.

5.3.2 Kadrların yoxlanması proseduru

Namizədin vəzifəyə uyğunluğu onun müvafiq qanunvericilik, etik davranış qaydaları, fəaliyyət tələbləri, üzərinə götürdüyü öhdəliklərə əsasən müəyyənləşdirilir.

Məsul rollarda xidmət edən əməkdaşların fəaliyyətinin bu Qaydaların tələblərinə uyğunluğu EH-SXM tərəfindən vaxtaşırı yoxlanılacaqdır.

5.3.3 Təlim tələbləri

EH-SXM-in işçi heyətinə vəzifələrinin icrasına başlamadan əvvəl aşağıdakı sahələrdə təlim keçirilməlidir:

- Fəaliyyət və təhlükəsizlik prinsipləri;
- İnformasiya sisteminin proqram təminatından istifadə qaydaları;
- Vəzifə təlimatları;
- Qəza hallarında işin bərpası və davamlığı proseduru.

5.3.4 Hazırlıq üzrə təkrar təlimlər

Bu Qaydaların 5.3.3-cü bəndinə uyğun təlimlər mütəmadi olaraq, lakin ildə bir dəfədən az olmayaraq keçirilə bilər.

5.3.5 İşlərin yerdəyişməsi tezliyi və ardıcıllığı

Tətbiq edilmir.

5.3.6 İcazəsiz hərəkətlərə görə cəzalar

EH-SXM işçi heyətinin intizam təlimatını (EH-SXM-in Təhlükəsizlik siyasətinin tərkib hissəsi kimi) hazırlayır, həyata keçirir və icrasına nəzarət edir. İntizam pozuntusu üzrə tədbirlərə (işdən çıxarma da daxil olmaqla) icazəsiz hərəkətlərin ciddiliyi və baş vermə tezliyinə uyğun olan müxtəlif cəzalar aiddir.

5.3.7 Podratçılar üzrə tələblər

EH-SXM zərurət yarandıqda aşağıdakı şərtləri nəzərə almaqla Məsul şəxslər kimi müstəqil podratçı və ya məsləhətçilər cəlb edə bilər:

- Məsul şəxs rollarını yerinə yetirəcək işçinin olmaması;
- Podratçı və ya məsləhətçiyə öz işçisi kimi tam etibar etməsi.

Başqa hallarda, müstəqil podratçı və məsləhətçilərin EH-SXM-in mühafizə olunan vasitələrinə daxil olması Məsul şəxslər tərəfindən müşayiət və ya nəzarət olunmalıdır.

5.3.8 İşçi heyətə verilən sənədlər

EH-SXM işçi heyətə (Məsul şəxslər də daxil olmaqla) vəzifələrini bacarıqla və lazımi səviyyədə yerinə yetirmək üçün tələb olunan zəruri təlimlər keçməli və onları müvafiq sənədlərlə təmin etməlidir.

5.4 Audit-loqların aparılma proseduru

Jurnala daxil edilən bütün qeydlər aşağıdakı elementlərə malik olmalıdır:

- Qeydin tarixi və zamanı;
- Qeydin seriya və sıra nömrəsi (avtomatik jurnal qeydləri üçün);
- Qeydin növü;
- Qeydin mənbəyi (məs: terminal, port, məkanı, istehlakçı və s.);
- Qeyd aparanın identifikatoru.

5.4.1 Qeydə alınan hadisələrin növləri

5.4.1.1 Qeydiyyat məlumatı

Aşağıdakılar da daxil olmaqla bütün qeydiyyat məlumatları (bu Qaydaların 4.2.1-ci bəndində təsvir olunub) qeydə alınır:

- Qeydiyyat üçün Ərizəçinin təqdim etdiyi sənədlərin növü;
- Unikal identifikasiya məlumatı;
- İmzalanmış Müqavilə də daxil olmaqla Ərizənin və identifikasiya sənədlərinin nüsxələrinin ehtiyat saxlama yeri;
- İmzan sahibinin Ərizəsindəki hər hansı spesifik seçimlər (məsələn, Sertifikatın yayımlanmasına razılıq);
- Ərizəni qəbul edən qurumun identifikasiyası;
- Qəbul edən SXM və ya təqdim edən Qeydiyyat Mərkəzinin adı.

5.4.1.2 Sertifikatın yaradılması

- EH-SXM açarlarının fəaliyyət dövrü ilə bağlı bütün hadisələrin audit-loqlarını aparır;
- EH-SXM verdiyi Sertifikatların fəaliyyət dövrü ilə bağlı bütün hadisələrin audit-loqlarını aparır.

5.4.1.3 SSCD-nin idarə olunması

- EH-SXM yaradılan açarların fəaliyyət dövrü ilə bağlı bütün hadisələrin audit-loqlarını aparır;
- EH-SXM SSCD-lərin (smart kartlar və HSM-lərə aid) fəaliyyət dövrü ilə bağlı bütün hadisələrin, o cümlədən onların hazırlanması, paylanılması və məhv edilməsinin audit-loqlarını aparır.

5.4.1.4 Ləğvetmənin idarə olunması

- EH-SXM dayandırma, bərpa və ləğvetmə ilə bağlı bütün hadisələrin audit-loqlarını aparır.

5.4.2 Audit-loqların aparılma mütəmadiliyi

Audit-loqlar EH-SXM-in müvafiq Məsul şəxsi tərəfindən həftədə ən azı bir dəfə yoxlanılır və bütün mühüm hadisələr audit-loqun icmalında şərh olunur. Bu yoxlama loqa müdaxilə edilmədiyinə əmin olmaq, bütün loq qeydlərini nəzərdən keçirmək, hər hansı xəbərdarlıq və ya pozuntuları daha ətraflı araşdırmaq üçün aparılır. Yoxlamadan sonrakı bütün addımlar sənədləşdirilir.

5.4.3 Audit-loqun saxlanma müddəti

Audit-loq ən azı iki ay saxlanılır və sonra bu Qaydaların 5.5.2-ci bəndinə müvafiq qaydada arxivləşdirilir.

5.4.4 Audit-loqun mühafizəsi

Audit-loq faylları icazəsiz daxil olma, modifikasiya, məhv edilmə və müdaxilədən qoruma mexanizminə malik elektron audit-loq sistemi ilə mühafizə olunur. Elektron audit-loq sistemi Vaxt göstəricisinin qoyulmasını da əhatə edir. Kağız audit məlumatları da icazəsiz daxil olma, modifikasiya, məhv edilmədən mühafizə edilməlidir.

5.4.5 Audit-loqun ehtiyat nüsxəsinin yaradılma proseduru

Audit-loqun artan (incremental) ehtiyat nüsxəsi hər gün və tam (ful) nüsxəsi isə hər həftə yaradılır.

5.4.6 Audit sistemi

Audit məlumatları avtomatik olaraq proqram, şəbəkə və əməliyyat sistemi səviyyələrində yaranır və qeyd edilir. Yaradılmış qeyri-elektron audit məlumatları isə EH-SXM-in Məsul şəxsi tərəfindən qeydə alınır.

5.4.7 Hadisə barədə bildiriş

Audit sistemi tərəfindən qeydə alınmış hadisələr barədə səbəbkar şəxsə, təşkilata və ya s. Bildiriş göndərilmir.

Müntəzəm olaraq çatışmazlıqların qiymətləndirilməsi jurnalda qeyd edilmiş hadisələrin təhlükəsizliyinin müəyyənləşdirilməsini və lazımi tədbirlərin görülməsini təmin edir.

5.4.8 Çatışmazlığın qiymətləndirilməsi

Hadisələrin audit-loqlarından sistemin çatışmazlıqlarının monitorinqi üçün istifadə edilir. Aşkar edilən çatışmazlıqlar təhlükəsizlik baxımından yoxlanılır, qiymətləndirilir və aradan qaldırılır. Bu real vaxt rejimində avtomatik aparılan loq məlumatları əsasında gündəlik, aylıq və illik olaraq yerinə yetirilir.

5.5 Sertifikat Xidmətləri ilə bağlı qeydlərin arxivləşdirilməsi

5.5.1 Arxivləşdirilmiş qeydlərin növü

EH-SXM-in Sertifikat xidmətləri ilə bağlı qeydləri arxivləşdirilir və bu Qaydaların 5.5.2-ci bəndində göstərilən müddətdə saxlanılır.

5.5.2 Arxivin saxlanma müddəti

EH-SXM-in Sertifikat xidmətləri ilə bağlı qeydlər on beş (15) il müddətinə saxlanılır. Bu müddət xüsusi sənəd və məlumatlar üçün artırıla bilər.

5.5.3 Arxivin qorunması

Arxivlər daxilolmaya nəzarət sistemləri ilə mühafizə olunan ayrıca yerdə yerləşdirilir. Heç kim arxiv məlumatını dəyişə və ya məhv edə bilməz, onlara müraciətə ciddi məhdudiyyət tətbiq edilir.

Arxiv məlumatlarının məlumat daşıyıcıları və onların emal proqramları işlək vəziyyətdə saxlanmalıdır ki, bu Qaydaların 5.5.2-ci bəndində müəyyən olunmuş müddət ərzində saxlanılan arxiv məlumatlarından istifadə edilə bilinsin.

5.5.4 Arxivlərin ehtiyat nüsxəsinin yaradılma proseduru

Arxivin oflayn ehtiyat nüsxəsinin yaradılması proseduru ilkin arxivlər itirildikdə və ya məhv olduqda qısa müddət ərzində onu tam bərpa etmək üçün istifadə edilə biləcək ehtiyat nüsxənin yaradılmasından ibarətdir.

5.5.5 Vaxt göstəricisi ilə bağlı tələblər

Verilənlər bazasına daxil edilən yazılar dəqiq tarix və zaman məlumatına malik olmalıdır. Bu Vaxt göstəricisi şifrlənməməlidir.

5.5.6 Arxiv sistemi

EH-SXM daxili Arxiv sistemindən istifadə edir.

5.5.7 Arxivdən məlumatların əldə edilməsi və yoxlanılması

Yalnız səlahiyyətli Məsul şəxslər arxivə giriş əldə edə bilərlər. Arxivdən əldə edilmiş sənəd və məlumatlar geri qaytarılarkən onların tamlığı yoxlanılır.

5.6 EH-SXM-in açarının dəyişdirilməsi

EH-SXM-in açarının dəyişdirilməsi avtomatik olaraq aparılmır, açarların vaxtı əlaqəli olduqları Sertifikatın qüvvədə olma vaxtı bitdikdə qurtarır. EH-SXM Sertifikatının qüvvədə olma vaxtı bitməzdən üç (3) il qabaq açarın dəyişdirilməsi üçün müraciət edir. İmza sahiblərinin Sertifikat yolundakı digər SXM-lərin Sertifikatlarının qüvvədə olma müddətləri aşağıdakı cədvəldə göstərilib.

SXM	Etibarlılıq müddəti	Əməliyyat müddəti (son buraxılış tarixi)
Ali SXM	18 il	9 il
Ali SXM-in Siyasət Sertifikat Mərkəzi	12 il	6 il
EH-SXM	6 il	3 il

EH-SXM-in cari açarı ilə Sertifikatların verilməsi son buraxılış tarixində dayandırılır, bu zamanadək isə yeni açar əldə edilməlidir. Yeni açarlar Ali SXM-in Siyasət Sertifikat Mərkəzi tərəfindən (Ali SXM-in Siyasət Sertifikat Mərkəzinin Açar yenilənməsi tələblərinə uyğun olaraq) verilir. EH-SXM-in yeni Açıq açarının Sertifikatı Direktoriya xidmətləri tərəfindən yayımlanır. Son buraxılış tarixindən sonra daxil olmuş Sertifikat sorğuları EH-SXM-in yeni Gizli açarı ilə imzalanır.

EH-SXM-in açarının dəyişdirilməsi ilə İmza sahibləri və Üçüncü tərəf üçün Sertifikat yolunun qırılması minimallaşdırılır. Bununla bağlı olaraq, EH-SXM cari Gizli Açarla imzalanmış CRL-lərin dərcini cari açarın qüvvədə olma müddəti bitənədək davam etdirir. Beləliklə, son buraxılış tarixindən sonra biri cari açar, digəri isə yeni açarla imzalanmış iki CRL mövcud olur.

5.7 Konfidensiallığın pozulması və qəza hallarında bərpa

5.7.1 Hadisələrin və konfidensiallığın pozulmasının idarə olunma proseduru

EH-SXM ayrıca yerdə saxlanılan aşağıdakı məlumatların ehtiyat nüsxələrindən konfidensiallığın pozulması və qəza hallarında istifadə edəcəkdir: Sertifikat Ərizələrinin məlumatları, audit məlumatları və bütün

verilmiş Sertifikatların verilənlər bazası. EH-SXM-də Gizli açarların ehtiyat nüsxələri yaradılmır və bu Qaydaların 6.2.4-cü bəndində buna ətraflı baxılır.

İnformasiya təhlükəsizliyi hadisələri və EH-SXM-in Gizli açarlarının konfidensiallığının pozulması hallarının idarə olunması proseduru EH-SXM-in Qəza hallarında Bərpa planında göstərilir. Bu planda hadisələrə uyğun olaraq onların idarə olunması proseduru və məsuliyyət əks etdirilir. Bu planın əsas məqsədi Sertifikat xidmətlərinin dərhal bərpa olunması və təhlükəsizliyin davamlı olaraq təmin edilməsidir. Görüləcək işlərin əsasları aşağıdakı bəndlərdə təsvir olunur.

5.7.2 Korlanmış hesablama resurslarının bərpası

Resursların, proqram təminatının və verilənlərin güman edilən və ya faktiki konfidensiallığının pozulması hallarında müvafiq bərpa proseduru (bu Qaydaların 5.7.4-cü bəndinə müvafiq olaraq) həyata keçirilir.

5.7.3 SXM-in konfidensiallığı pozulmuş Gizli açarı ilə bağlı prosedurlar

EH-SXM-in Gizli açarının konfidensialllığı pozulduqda və ya buna şübhə yarandıqda EH-SXM aşağıdakıları təmin edir:

- İmza sahiblərini, əlaqədə olduğu SXM-ləri və Üçüncü tərəfi məlumatlandırır;
- Konfidensiallığı pozulmuş Gizli açardan istifadə edilməsinin qarşısını almaq üçün Sertifikatların verilməsi və CRL-in yayımlanması üzrə göstərilən xidmətləri dayandırır;

EH-SXM-in işçi heyəti tərəfindən istifadə edilən Gizli açarlardan hər hansının konfidensiallığı pozulduqda və ya buna şübhə yarandıqda bu barədə dərhal müvafiq Məsul şəxs məlumatlandırılmalı və Sertifikatının ləğvetmə sorğusu verilməlidir.

İmza sahibinə məxsus Gizli açarın konfidensiallığı pozulduqda və ya buna şübhə yarandıqda bu barədə dərhal EH-SXM və Üçüncü tərəf məlumatlandırılmalı və Sertifikatın ləğvetmə sorğusu verilməlidir.

5.7.4 Qəzadan sonra işin davamlığı imkanları

İnformasiya sistemlərinin qaynar ilkin quraşdırılmasının həyata keçirilməsi ilə EH-SXM-in Sertifikat xidmətləri göstərməsi imkanı yüksək səviyyədə təmin olunur.

Hesablama resursları, proqram təminatı və məlumatları itirildikdə və ya korlandıqda EH-SXM Qəza hallarında Bərpa planına müvafiq tədbirlər görür. Bu planda EH-SXM-in bu Qaydalara uyğun xidmətlər göstərməsi üçün digər coğrafi ərazidə yerləşən əməliyyat vasitələri də nəzərdə tutula bilər.

Sertifikatın qüvvəsinin dayandırılması və ya ləğvi, Sertifikatın etibarlılığının yoxlanması və CRL-lərin dərci kimi əsas xidmətlər ən geci 4 saat ərzində bərpa edilməlidir. Tam funksionallıq 72 saat ərzində təmin olunacaqdır. Planda bu vasitələrin hazırlığının tam və ya vaxtaşırı sınaqdan keçirilməsi imkanı nəzərdə tutulmalıdır. Planda müvafiq sənədlərə istinad edilir və o, səlahiyyətli şəxslər tərəfindən təftiş edilə bilər.

5.8 EH-SXM-in fəaliyyətinə xitam verilməsi

EH-SXM-in fəaliyyətinə xitam vermək zəruriyyəti yarandıqda, qüvvədə olan Sertifikatlara malik İmza sahiblərinə, əlaqəli SXM-lərə və müvafiq icra hakimiyyəti orqanına bu barədə xəbər verilir və onlara göstərilən xidmətlərdə fasilənin minimuma endirilməsi üçün xüsusi Xitam planı hazırlanır. Bu planda əsasən aşağıdakılar nəzərdə tutulur:

- İmza sahiblərinə, əlaqəli SXM-lərə və müvafiq icra hakimiyyəti orqanına bildiriş göndərilməsi;
- EH-SXM-in Sertifikatının ləğvi;

- Verilmiş Sertifikatlar, onlarla və Sertifikat sorğuları ilə bağlı məlumatların, onların arxivlərinin başqa SXM-ə və ya müvafiq icra hakimiyyəti orqanına təhvil verməsi;
- İmza sahiblərinə dəstək xidmətlərinin davam etdirilməsi;
- CRL-lərin dərci kimi ləğvetmə xidmətlərinin və ya statusun onlayn yoxlanılması xidmətlərinin davam etdirilməsi;
- Fərdi məlumatların konfidensiallığının mühafizə olunması.

6 Texniki təhlükəsizlik nəzarəti

6.1 Açar cütünün yaradılması və ilkin quraşdırılması

6.1.1 Açar cütünün yaradılması

EH-SXM-də açar cütü səlahiyyətli və səriştəli Məsul şəxslər tərəfindən təhlükəsiz informasiya sistemi və proseslərdən istifadə edərək, konfidensiallıq və şifrlənmə səviyyəsi təmin olunaraq yaradılır.

EH-SXM-in Gizli açarları açar generasiyası və yadda saxlanılması üçün nəzərdə tutulan FIPS 140-2 Level 3 ilə Sertifikatlaşdırılmış HSM-də generasiya olunacaq və saxlanılacaq.

EH-SXM-də Ərizəçilər üçün yaradılan açar cütü EAL4+, SSCD-nin 3-cü növ təhlükəsizlik tələblərinə cavab verən smart kartlara yazılır.

6.1.2 Gizli açarın İmza sahibinə çatdırılması

Açar cütü yazılmış Smart kart sahibinə çatdırılmaq üçün saxtalaşdırmanın qarşısını alan formada qablaşdırılaraq poçt vasitəsilə EH-SXM-dən müvafiq Qeydiyyat Mərkəzinə göndərilir. EH-SXM-də bu prosesin qeydiyyatı aparılır və audit-loqlarda müvafiq qeydlər edilir. Smart kart Qeydiyyat Mərkəzində Kart təqdimatı səlahiyyətlisi tərəfindən İmza sahibinə

şəxsən təqdim edilir. Gizli açarı tətbiq etmək üçün İmza sahibinə əvvəlcə poçtla göndərilmiş PİN koddan istifadə edilməlidir.

6.1.3 İmza sahibinin Açıq açarının Sertifikat verən quruma çatdırılması

Açıq açarlar Kart fərdiləşdirmə sahəsində yaradılır və smart karta yazılır. Açıq açar Sertifikatlaşdırma üçün SSL seansı vasitəsilə PKCS#10 Sertifikat sorğusu kimi təhlükəsiz qaydada SSCD-dən EH-SXM-ə göndərilir. PKCS#10 Sertifikat sorğusundakı imzanın həqiqiliyinin müəyyənləşdirilməsi müvafiq Gizli açarın kimə məxsus olmasını təsdiq edir. Açıq açarın EH-SXM-ə çatdırılması zamanı onun dəyişdirilməməsi, Ərizəçinin Açıq açarla əlaqəli Gizli açarı əldə etməsi təmin edilir.

6.1.4 Açıq açarın Üçüncü tərəfə çatdırılması

EH-SXM bütün Açıq açarları Direktoriya xidməti vasitəsilə yayımlayır. Bundan əlavə Ali SXM-in özüimzalanmış Sertifikatının heş qiyməti ilkin yoxlama üçün bu Qaydaların 2.1.2.2.-ci bəndində göstərildiyi kimi yayımlanır.

Gizli açar İmza sahibinə smart kartda çatdırılır. Açar yaradılması zamanı EH-SXM-in İnformasiya sistemi İmza sahibinin Sertifikatının mərkəzin Açıq açarından istifadə edilərək təsdiq olunma imkanını yoxlayır. İmza sahibinin razılığı ilə onun Sertifikatı yüklənmək üçün Sertifikat bazasında yerləşdirilə bilər.

6.1.5 Açarların ölçüsü

Açar	Ölçü
EH-SXM-in Gizli açarı	2048 bit

İmza sahibinin Gizli açarı	2048 bit
İmza sahibinin autentifikasiya Açarı	2048 bit

RSA 1024Bit/2048 Bit (PKCS#1) kriptoqrafik alqoritmindən istifadə olunmuşdur.

6.1.6 Açıq açarın parametrinin yaradılması və keyfiyyətin yoxlanılması

Tətbiq edilmir.

6.1.7 Açarın istifadə məqsədləri

İmza sahibinin Gizli açarı bu Qaydaların 4.5.1-ci bəndinə uyğun olaraq istifadə edilə bilər.

EH-SXM-in Gizli açarı yalnız İmza sahiblərinə verilən Sertifikatların, etibarlı OCSP-responderin X.509 v3-ə uyğun olaraq istifadə sahəsində göstərilmiş təyinatla CRL-in imzalanması üçün istifadə edilə bilər (bax 7.1).

6.2 Gizli açarın mühafizəsi

6.2.1 Kriptoqrafik modul üçün standartlar

EH-SXM tərəfindən istifadə olunan HSM FIPS 140-2, 3-cü səviyyə göstəricilərinə cavab verir. İmza sahiblərinin Açar cütünün daşıyıcısı və SSCD kimi istifadə olunan smart kartlar EAL4+ və Ümumi Meyarlarla (ISO/IEC 15408) qiymətləndirilən təhlükəsizlik tələblərinə uyğundur. EH-SXM bu uyğunluq yoxlamasının nəticələrini tələb edə bilər.

6.2.2 Gizli açara bir neçə şəxsin nəzarəti

EH-SXM həssas kriptoqrafik əməliyyatları yerinə yetirmək üçün bir neçə Məsul şəxsin iştirakını tələb edən texniki və prosedur mexanizmlərini tətbiq edir. Bu şəxslərdən heç biri təklikdə hər hansı Gizli açardan istifadə etmək üçün lazım olan giriş kodlarına tam sahib deyil. EH-SXM-in Gizli açarına giriş əldə etmək üçün 5 şəxsdən 3-nün iştirakı lazımdır.

6.2.3 Gizli açarı saxlamaq üçün başqasına verilməsi

İmza sahibinin və ya EH-SXM-in Gizli açarı saxlamaq üçün başqasına verilə bilməz.

6.2.4 Gizli açarın ehtiyat nüsxəsi

Avadanlıqlardakı texniki nasazlıqlar, enerji təchizatının qəza kəsilməsi nəticəsində açarın itirilməsi hallarının qarşısının alınması üçün EH-SXM-in Gizli açarının ehtiyat nüsxəsi yaradılır və təhlükəsizlik şəraitində saxlanılır. Gizli açarın ehtiyat nüsxəsinin yaradılması EH-SXM-in açarının yaradılması mərhələsində həyata keçirilir. EH-SXM-in Gizli açarlarının ehtiyat nüsxələrinin konfidensiallığı qorunmalı və onların tamlığı, autentikliyi saxlanılmalıdır.

Gizli açarlar təkrar açar yaratma kart dəstindən istifadə edilərək yaradılır. Açarın yaradılması fiziki baxımdan təhlükəsiz yerdə iki Məsul şəxsin nəzarəti altında aparılır və prosedur sənədləşdirilir.

İmza sahibinin Gizli açarı smart kartda yaradılır və saxlanılır. O, smart kartdan çıxarılmır və ehtiyat nüsxəsi yaradılmır.

6.2.5 Gizli açarın arxivləşdirilməsi

EH-SXM-in Gizli açarının arxivləşdirilməsi aparılmır və onun qüvvədə olma müddəti bitdikdə bu Qaydalara uyğun olaraq təhlükəsizlik təmin edilməklə məhv edilir.

6.2.6 Gizli açarın kriptoqrafik modula ötürülməsi

EH-SXM-in açar cütü istifadə olunacağı HSM-də yaradılır.

İmza sahibinin imza və autentifikasiya Sertifikatları 3-cü növ SSCD olan smart kartda yaradılır və heç bir kriptoqrafik modullardan və ya modullara ötürülmür.

6.2.7 Gizli açarın kriptoqrafik modulda saxlanması

EH-SXM-in Gizli açarı HSM-də şifrlənmiş formada saxlanılır.

İmza sahibinin imza və autentifikasiya Sertifikatları smart kartda saxlanılır və smart kartdan çıxarılmır.

6.2.8 Gizli açarı aktivləşdirmə metodu

EH-SXM-in Gizli açarını yalnız HSM-də FİPS-in tələblərinə uyğun rejimdə işləyən, əvvəlcədən müəyyənləşmiş Operator smart kartının nömrəsini təqdim etməklə aktivləşdirmək olar. EH-SXM-in Gizli açarının aktivləşdirilməsi giriş və PİN-in yoxlanmasını və ya xüsusi təhlükəsizlik parametrlərinə uyğun giriş frazasını tələb edir.

Smart kartdakı Gizli açardan istifadə PİN-in daxil edilməsini tələb edir:

- Ümumilikdə, təkmil Sertifikatlar üçün Gizli açar PİN vasitəsilə qorunur. Bir imzanın generasiyası məqsədilə PİN-in daxil edilməsi təkmil imza üçün Gizli açarı aktivləşdirir (imzanın hər generasiyası üçün hər dəfə PİN-in daxil edilməsi lazımdır).

- Autentifikasiya üçün Gizli açar PİN vasitəsilə qorunur. PİN sessiya üçün Gizli açarı aktivləşdirir (smart kartın elektrik təchizatı qurtarana və ya tətbiqi proqram dayanana qədər).

6.2.9 Gizli açarı deaktivləşdirmə metodu

Bu Qaydaların 6.2.10-cu bəndinə baxın.

6.2.10 Gizli açarın məhv edilmə metodu

Sertifikatının qüvvədə olma vaxtı başa çatdıqda və ya Sertifikat ləğv olunduqda EH-SXM-in Gizli açarı məhv edilir. Gizli açarlar onların itməsi, oğurlanması, modifikasiyasını, səlahiyyətsiz açıqlanması və ya istifadəsinin qarşısını alan yolla məhv edilir.

Smart kartdakı Gizli açarların məhv edilməsi bilavasitə həmin smart kartın fiziki dağıdılması yolu ilə həyata keçirilir. İmza sahibləri malik olduqları smart kartları təhlükəsiz məhv edilmə üçün EH-SXM-ə qaytara bilərlər.

6.2.11 Kriptoqrafik modulun səviyyəsi

Bu Qaydaların 6.2.1-ci bəndinə baxın.

6.3 Açar cütünün idarə olunmasının digər məqamları

6.3.1 Açıq açarın arxivləşdirilməsi

Bütün verilmiş Sertifikatlar saxlanılmalıdır və bu EH-SXM-in ehtiyat nüsxəsinin yaradılma proseduru, o cümlədən arxivləşdirmə vasitəsilə təmin edilir. Sertifikatın arxivdə saxlanma müddəti on beş (15) ildir.

6.3.2 Sertifikatın və Açar cütünün istifadə müddətləri

Sertifikatdan qüvvədə olma vaxtı bitənədək və ya ləğv edilənədək istifadə etmək olar. Açar cütünün istifadəsi əlaqəli olduğu Sertifikatın istifadə müddəti ilə məhdudlanır, lakin Açıq açarla həmin müddətdən sonra da imza yoxlanılması aparıla bilər. Sertifikatların maksimum istifadə müddəti aşağıdakı cədvəldə göstərilib:

Sertifikat	Etibarlılıq Müddəti
Ali SXM-in Sertifikatı (özüimzalanmış)	18 ilə qədər
Ali SXM-in Siyasət Sertifikat Mərkəzinin Sertifikatı	12 ilə qədər
EH-SXM Sertifikatı	6 ilə qədər
İmza sahibinin imza Sertifikatı	3 ilə qədər
İmza sahibinin autentifikasiya Sertifikatı	3 ilə qədər
OCSP-responderin Sertifikatı	3 ilə qədər

Tətbiq edilən kriptoqrafik alqoritm və parametrlərin uyğunluğuna EH-SXM tərəfindən daim nəzarət edilir. Əgər Sertifikatın qüvvədə olma müddətində alqoritm və ya açar uzunluğunun təhlükəsizlik baxımında qənaətbəxş olmaması müəyyənləşdirilərsə, Sertifikatın ləğvi və yeni Sertifikatın əldə edilməsi həyata keçirilir.

6.4 Aktivləşdirmə məlumatı

6.4.1 Aktivləşdirmə məlumatının yaradılması və ilkin quraşdırılması

Gizli açar daşıyıcısına (smart karta) giriş kodu kimi PİN istifadə olunur. Giriş kodları və smart kart İmza sahibinə ayrı-ayrılıqda və təhlükəsizlik təmin

edilən üsullarla çatdırılır. Giriş kodları adi poçt vasitəsilə, smart kartlar isə Qeydiyyat Mərkəzində təqdim edilir.

6.4.2 Aktivləşdirmə məlumatının mühafizəsi

İmza sahibi Gizli açarın aktivləşdirmə məlumatlarını mühafizə etməli, onların itməsi, oğurlanması, modifikasiyası, digər şəxslərə bəlli olması və ya səlahiyyətsiz istifadəsinin qarşısını almalıdır.

Təhlükəsizlik baxımından aktivləşdirmə məlumatlarının hər hansı bir yerə yazılmadan yadda saxlanılaraq istifadəsi məqsədəuyğundur. Əgər yazıb istifadə edilərsə, bu məlumatlar kriptoqrafik modulla əlaqəli olan məlumat kimi mühafizə olunmalıdır.

6.4.3 Aktivləşdirmə məlumatları ilə bağlı digər məqamlar

6.4.3.1 Aktivləşdirmə məlumatlarının ötürülməsi

Gizli açarların aktivləşdirmə məlumatları ötürülərkən onların itməsi, oğurlanması, modifikasiyası, digər şəxslərə bəlli olması və ya səlahiyyətsiz istifadəsinin qarşısının alınmasını təmin edən üsullar tətbiq edilməlidir.

6.4.3.2 Aktivləşdirmə məlumatlarının məhv edilməsi

EH-SXM Gizli açarların aktivləşdirmə məlumatlarının məhvi üçün onların itməsi, oğurlanması, modifikasiyası, digər şəxslərə bəlli olması və ya səlahiyyətsiz istifadəsinin qarşısının alınmasını təmin edən üsullar tətbiq edilməlidir.

6.5 Vaxt göstəricisi

EH-SXM vaxt göstəricilərinin qeyd edilməsini təmin edən TSA-ya malikdir. TSA TS 101 861 v1.2.1-lə müəyyənləşdirilən profildən və TSP protokolundan istifadə edir. Ətraflı məlumat üçün EH-SXM-in Vaxt göstəricilərinin qeyd edilmə siyasəti [15] və Vaxt göstəricilərinin qeyd edilmə qaydasına [16] baxın.

EH-SXM TSA-ya https://ehm.e-imza.az/tsa/tsa.responder İnternet ünvanında müraciət oluna bilər.

7 Sertifikat və CRL profilləri

EH-SXM tərəfindən verilən bütün elektron Sertifikatlar RFC 3280-də [7] müəyyən olunmuş elektron Sertifikat və CRL profillərinə uyğun olmalıdır.

7.1 Sertifikat profilləri

7.1.1 EH-SXM-in Sertifikat profilləri

	EH-SXM	**Vaxt göstəricisi serveri**	**OCSP-responder**
Təsviri	Hüquqi və fiziki şəxslərə Sertifikat verən EH-SXM-in Sertifikatı	Vaxt göstəricilərinin imzalanması üçün istifadə edilən Vaxt göstəricisi mərkəzinə verilən Sertifikat	EH-SXM tərəfindən verilmiş Sertifikatların statusu ilə bağlı onlayn sorğulara verilən cavabları imzalamaq üçün istifadə olunan Sertifikat
Əsas Sertifikat sahələri			
X.509 versiyası	3		
Seriya nömrəsi	Unikal tam ədəd (hər Sertifikat üçün unikaldır) Məsələn: 6c e0 47 a2 a6 9f e5 34 00 00 00 00 00 04		
İmza alqoritmi	sha1WithRSAEncryption		
Sertifikat verən qurum	CN = AZ Policy Authority (PCA) OU = Certification Services O = CSP C = AZ	CN = AZ Policy Authority (PCA) OU = Certification Services O = CSP C = AZ	CN = AZ e-Government Authority (ICA) OU = Certification Services O = CSP C = AZ

Etibarlılıq müddəti	6 il	6 il	3 il
Subyekt	CN = AZ e-Government Authority (ICA) OU = Certification Services O = CSP C = AZ	CN = AZ Time Stamping Authority OU = Certification Services O = CSP C = AZ	CN = AZ e-Government Authority (OCSP) OU = Certification Services O = CSP C = AZ
Subyektin Açıq açarı haqqında məlumatlar	Algorithm = RSA Açar qiyməti = Açıq açardan ibarət bit sətri Açarın uzunluğu = 2048 bit	Algorithm = RSA Açar qiyməti = Açıq açardan ibarət bit sətri Açarın uzunluğu = 2048 bit	Algorithm = RSA Açar qiyməti = Açıq açardan ibarət bit sətri Açarın uzunluğu = 2048 bit
Genişlənmələr			
Açarın istifadəsi	Certificate Sign, CRL Sign (critical)	Digital Signature, Non-Repudiation	Digital Signature, Non-repudiation
Əsas məhdudiyyətlər	Subyektin tipi = SXM (CA) Yol uzunluğu məhdudiyyəti = yoxdur		
Subyektin açarının identifikatoru	Subyektin Açıq açarının heşi		
SXM-in versiyası	SXM-in açarlarının versiyası (Sertifikatlar). Versiyanın nömrəsi hər yenilənmədə artır. Məsələn: V0.0		
Sertifikat siyasətləri	[1]Sertifikat siyasəti: Siyasət İdentifikatoru = 1.3.6.1.4.1.32843.1.1 [1,1] Siyasət spesifikatorları: Siyasət spesifikatorunun İD-si: CPS Spesifikator: http://asxm.e-imza.az/repository	[1]Sertifikat siyasəti: Siyasət İdentifikatoru = 1.3.6.1.4.1.32843.1.1 [1,1] Siyasət spesifikatorları: Siyasət spesifikatorunun İD-si: CPS Spesifikator: http://asxm.e-imza.az/repository	[1]Sertifikat siyasəti: Siyasət İdentifikatoru = 1.3.6.1.4.1.32843.1.3 [1,1] Siyasət spesifikatorları: Siyasət spesifikatorunun İD-si: CPS Spesifikator: http://ehm.e-imza.az/repository
Mərkəz açarı identifikatoru	Sertifikat verən qurumun Açıq açarının heşi	Sertifikat verən qurumun Açıq açarının heşi	Sertifikat verən qurumun Açıq açarının heşi
CRL paylanma nöqtələri	[1]CRL paylanma **n**öqtəsi Paylanma nöqtəsinin adı: Tam adı: URL= http://asxm.e-imza.az/cdp/AZ%20Policy%20Authority%20(PCA).crl URL= ldap://asxm.e-imza.az/cn=AZ%20Policy%20Authority%20(PCA),OU=Certification%20Services,O=CSP,C=AZ?certificaterevocationlist?bas	[1]CRL paylanma **n**öqtəsi Paylanma **n**öqtəsinin adı: Tam adı: URL= http://asxm.e-imza.az/cdp/AZ%20Policy%20Authority%20(PCA).crl URL= ldap://asxm.e-imza.az/cn=AZ%20Policy%20Authority%20(PCA),OU=Certification%20Services,O=CSP,C=AZ?certificaterevocationlist?bas	[1]CRL paylanma nöqtəsi Paylanma **n**öqtəsinin adı: Tam adı: URL= http://ehm.e-imza.az/cdp/AZ%20e-Government%20Authority%20(ICA).crl URL= ldap://ehm.e-imza.az/cn=AZ%20e-Government%20Authority%20(ICA),OU=Certification%20Services,O=C

	e?objectclass=certificationauthority	e?objectclass=certificationauthority	SP,C=AZ?certificaterevocationlist?base?objectclass=certificationauthority
Mərkəz haqqında məlumata müraciət	[1] Mərkəz haqqında məlumata müraciət Müraciət metodu = Sertifikat verən qurum (1.3.6.1.5.5.7.48.2) Alternativ adı: URL= http://asxm.e-imza.az/aia/AZ%20Policy%20Authority%20(PCA).crt [2] Mərkəz haqqında məlumata müraciət Müraciət metodu = Sertifikat verən qurumun Sertifikatı (1.3.6.1.5.5.7.48.2) Alternativ adı: URL= ldap://asxm.e-imza.az/CN=AZ%20Policy%20Authority%20(PCA),OU=Certification%20Services,O=CSP,C=AZ?cacertificate?base?objectclass=certificationauthority	[1] Mərkəz haqqında məlumata müraciət Müraciət metodu = Sertifikat verən qurum (1.3.6.1.5.5.7.48.2) Alternativ adı: URL= http://asxm.e-imza.az/aia/AZ%20Policy%20Authority%20(PCA).crt [2] Mərkəz haqqında məlumata müraciət Müraciət metodu = Sertifikat verən Mərkəzin Sertifikatı (1.3.6.1.5.5.7.48.2) Alternativ adı: URL= ldap://asxm.e-imza.az/CN=AZ%20Policy%20Authority%20(PCA),OU=Certification%20Services,O=CSP,C=AZ?cacertificate?base?objectclass=certificationauthority	[1] Mərkəz haqqında məlumata müraciət Müraciət metodu = Sertifikat verən qurum (1.3.6.1.5.5.7.48.2) Alternativ adı: URL= http://ehm.e-imza.az/aia/AZ%20e-Government%20Authority%20(ICA).crt [2] Mərkəz haqqında məlumata müraciət Müraciət metodu = Sertifikatların Onlayn yoxlanılması Protokolu (OCSP) (1.3.6.1.5.5.7.48.1) Alternativ adı: URL=http://ehm.e-imza.az/ocsp/ocsp.responder [3] Mərkəz haqqında məlumata müraciət Müraciət metodu = Sertifikat verən Mərkəzin Sertifikatı (1.3.6.1.5.5.7.48.2) Alternativ adı: URL= ldap://ehm.e-imza.az/cn=AZ%20e-Government%20Authority%20(ICA),OU=Certification%20Services,O=CSP,C=AZ?cacertificate?base?objectclass=certificationauthority
Genişləndirilmiş Açar istifadəsi		Vaxt göstəricisi (1.3.6.1.5.5.7.3.8)	OID = 1.3.6.1.5.5.7.3.9 (id-kp-OCSPSigning)

7.1.2 EH-SXM tərəfindən verilən İmza sahibi Sertifikatlarının profili

	Gücləndirilmiş Elektron imza	**Autentifikasiya**
Təsviri	Azərbaycan vətəndaşlarına verilmiş təkmil Sertifikat.	Azərbaycan vətəndaşlarına verilmiş autentifikasiya Sertifikatı.
Əsas Sertifikat sahələri		
X.509 versiyası	3	
Seriya nömrəsi	Unikal tam ədəd (EH-SXM tərəfindən verilən hər Sertifikat üçün unikaldır) Məsələn: 34:74:cc:10:d4:2a:fa:d2:00:00:00:00:00:03	
İmza alqoritmi	sha1WithRSAEncryption	

Sertifikat verən qurum	CN = AZ e-Government Authority (ICA) OU = Certification Services O = CSP C = AZ	
Etibarlılıq müddəti	3 il	3 il
Subyekt	CN = <adı> <soyadı> <ata adı + [“oğlu” | “qızı”]>	CN = <adı> <soyadı> < ata adı + [“oğlu” | “qızı”]>
	GN = <adı>	GN = <adı>
	SN = <soyadı>	SN = <soyadı>
	Seriya nömrəsi = <IAMAS şəxsi kod>	Seriya nömrəsi = <IAMAS şəxsi kod>
	C = AZ	C = AZ
	və ya	
	CN = PN: <təxəllüs>	
	Seriya nömrəsi= <IAMAS şəxsi kod>	
	C = AZ	
Subyektin Açıq açarı haqqında məlumat	Alqoritm = RSA Açar qiyməti = Açıq açardan ibarət bit sətri Açarın uzunluğu= 2048 bit	Alqoritm = RSA Açar qiyməti = Açıq açardan ibarət bit sətri Açarın uzunluğu= 2048 bit
Genişlənmələr		
Açarın İstifadəsi	Digital Signature, Non-Repudiation	Digital Signature
Subyektin açarının identifikatoru	İmza Sahibinin Açıq açarının heşi	
Sertifikat siyasəti	[1]Sertifikat siyasəti: Siyasət İdentifikatoru = 1.3.6.1.4.1.32843.1.3 [1,1] Siyasət spesifikatorları: Siyasət spesifikatorunun İD-si: CPS Spesifikator: http://ehm.e-imza.az/repository	
Mərkəz Açarı İdentifikatoru	Sertifikatı verən qurumun Açıq açarının heşi	

CRL Paylanma Nöqtələri	[1]CRL paylanma nöqtəsi Paylanma nöqtəsinin adı: Tam adı: URL= http://ehm.e-imza.az/cdp/AZ%20e-Government%20Authority%20(ICA).crl URL= ldap://ehm.e-imza.az/cn=AZ%20e-Government%20Authority%20(ICA),OU=Certification%20Services,O=CSP,C=AZ?certificaterevocationlist?base?objectclass=certificationauthority	
Mərkəz haqqında məlumata müraciət	[1] Mərkəz haqqında məlumata müraciət Müraciət metodu = Sertifikat verən qurum (1.3.6.1.5.5.7.48.2) Alternativ adı: URL= http://ehm.e-imza.az/aia/AZ%20e-Government%20Authority%20(ICA).crt [2] Mərkəz haqqında məlumata müraciət Müraciət metodu = Sertifikatların onlayn yoxlanılması protokolu (OCSP) (1.3.6.1.5.5.7.48.1) Alternativ adı: URL=http://ehm.e-imza.az/ocsp/ocsp.responder [3] Mərkəz haqqında məlumata müraciət Müraciət metodu = Sertifikat verən Mərkəzin Sertifikatı (1.3.6.1.5.5.7.48.2) Alternativ adı: URL= ldap://ehm.e-imza.az/cn=AZ%20e-Government%20Authority%20(ICA),OU=Certification%20Services,O=CSP,C=AZ?cacertificate?base?objectclass=certificationauthority	
Genişləndirilmiş açar istifadəsi	Document Signing (1.3.6.1.4.1.311.10.3.12) Secure Email (1.3.6.1.5.5.7.3.4)	Client Authentication (1.3.6.1.5.5.7.3.2)
Subyektin alternativ adı	İmza sahibinin alternativ adı bölməsinin RFC822 ad sahəsində şəxsin electron poçtu əlavə oluna bilər	
Sertifikat şablonu üzrə məlumatlar	Sertifikatı vermək üçün istifadə olunan şablonun identifikatoru və versiya nömrəsi	
Təkmil Sertifikat tələbləri	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-QcSSCD (0.4.0.1862.1.3)	
Proqram Siyasətləri	[1]Proqram Sertifikat siyasəti: Siyasət İdentifikatoru= Document Signing [2] Proqram Sertifikat siyasəti: Siyasət İdentifikatoru = Secure Email	[1]Proqram Sertifikat siyasəti: Siyasət İdentifikatoru= Client Authentication

7.2 CRL profilləri

7.2.1 EH-SXM-in CRL profili

CRL Standartı	Atribut	Məzmun
Versiya		V2
Sertifikat verən qurum		CN = AZ e-Government Authority (ICA) OU = Certification Services O = CSP C = AZ
Qüvvədə olma tarixi		Verilmə tarixi və vaxtı
Növbəti yeniləmə		Növbəti yeniləmənin tarix və vaxtı
İmza alqoritmi		sha1RSA
Ləğv edilmiş Sertifikatlar		
Seriya nömrəsi		Ləğv edilmiş və ya qüvvəsi dayandırılmış Sertifikatların seriya nömrələri
Ləğvetmə tarixi		Sertifikatın ləğvi və ya qüvvəsinin dayandırılmasının tarixi və vaxtı
CRL səbəb kodu		Sertifikatın ləğvi və qüvvəsinin dayandırılması üçün səbəb
CRL genişlənməsi		
Mərkəz açarı identifikatoru	**Açar identifikatoru**	EH-SXM-in Açıq açarının heşi
SXM versiyası		V0.0
CRL nömrəsi		EH-SXM tərəfindən avtomatik olaraq verilir
Növbəti CRL-in dərci		Dərc tarixi + 5 gün
Ən yeni CRL	**Paylanma nöqtəsinin adı**	URL = http://ehm.e-imza.az/cdp/AZ%20e-Government%20Authority%20(ICA)+.crl URL = ldap://ehm.e-imza.az/cn=AZ%20e-Government%20Authority%20(ICA),OU=Certification%20Services,O=CSP,C=AZ?deltarevocationlist?base?objectclass=certificationauthority

7.2.2 EH-SXM-in delta CRL-i

CRL Standartı	Atribut	Məzmun
Versiya		V2
Sertifikat verən qurum		CN = AZ e-Government Authority (ICA) OU = Certification Services O = CSP C = AZ
Qüvvədə olma tarixi		Verilmə tarixi və vaxtı

Növbəti yeniləmə		Növbəti yeniləmənin tarix və vaxtı
İmza alqoritmi		sha1RSA
Ləğv edilmiş Sertifikatlar		
Seriya nömrəsi		Ləğv edilmiş və ya qüvvəsi dayandırılmış Sertifikatların seriya nömrələri
Ləğvetmə tarixi		Sertifikatın ləğvi və ya qüvvəsinin dayandırılmasının tarixi və vaxtı
CRL səbəb kodu		Sertifikatın ləğvi və qüvvəsinin dayandırılması üçün səbəb
CRL genişlənməsi		
Mərkəz Açarı identifikatoru	**Açar identifikatoru**	EH-SXM-in Açıq açarının heşi
SXM versiyası		V0.0
CRL nömrəsi		EH-SXM tərəfindən avtomatik olaraq verilir
Növbəti CRL-in dərci		Dərc tarixi + 3 saat
Delta CRL indikatoru	**Baza CRL nömrəsi**	Bu, delta CRL-in generasiyasında əsas kimi istifadə olunan CRL-i identifikasiya edir.

8 Uyğunluq auditi və digər yoxlamalar

EH-SXM-in Sertifikat xidmətləri göstərməsi üçün İnformasiya sisteminin təhlükəsizliyinin auditi keçirilməlidir. Audit qanunvericiliyə və bu Qaydalara uyğun olaraq EH-SXM-in fəaliyyətə başladığı müddət nəzərə alınmaqla, hər il keçirilir.

Audit zamanı aşağıdakı sənədlər nəzərdən keçirilir:

- Fiziki təhlükəsizlik;
- Texnoloji qiymətləndirmə;
- EH-SXM-in idarəçiliyi (o cümlədən, fiziki və ətraf mühitin təhlükəsizliyi, açar əməliyyatlarının və Sertifikatın fəaliyyət dövrünün idarə olunması)
- İşçi heyətin seçilməsi;
- Müvafiq Sertifikat siyasəti və Sertifikatın tətbiqi qaydaları;
- Müqavilələr;
- Məlumatın mühafizəsi və konfidensiallığın qorunması;
- Qəza hallarında Bərpa planı.

Audit zamanı aşkara çıxarılmış mühüm uyğunsuzluq və ya çatışmazlıqların aradan qaldırılması üçün EH-SXM tərəfindən tədbirlər

müəyyənləşdirilir. Bu tədbirlərin icra olunmasına EH-SXM-in rəhbərliyi cavabdehdir.

Audit barədə məlumat **http://www.e-imza.az/repository** İnternet ünvanında yerləşdirilə bilər.

9 Digər işlər və hüquqi məsələlər

9.1 Ödənişlər

9.1.1 Sertifikatın idarə olunması haqqı

EH-SXM Sertifikatın verilməsi və yenilənməsini ödəniş əsasında həyata keçirir və onların qiymət cədvəli **http://www.e-imza.az** İnternet ünvanında yerləşir.

9.1.2 Sertifikatın etibarlılığının yoxlanılması haqqı

EH-SXM Sertifikatın etibarlılığının yoxlanılmasını ödənişsiz həyata keçirir.

9.1.3 Ödənişi qaytarma siyasəti

EH-SXM ödənişi qaytarma siyasətini yarada bilər. Əgər bu siyasət imza sahiblərinə tətbiq edilərsə, onda ən yeni versiya təmin olunmalıdır və bu, **http://www.e-imza.az** veb-saytında dərc oluna bilər.

9.2 Maliyyə məsuliyyəti

EH-SXM-in İmza sahibləri qarşısında məsuliyyəti və belə məsuliyyətin yuxarı həddi imzalanmış Müqaviləyə əsasən müəyyənləşdirilir. Bu halda Müqavilədə bu Qaydalara istinad edilir.

EH-SXM İmza sahibləri, Üçüncü tərəf və digər qurumlar qarşısında yalnız qəbul olunmuş Sertifikat siyasətində müəyyən edilmiş çərçivədə məsuliyyət daşıyır.

EH-SXM-in Üçüncü tərəf və digər qurumlar qarşısında maddi məsuliyyətinin yuxarı həddinə dair tələblər qanunvericiliklə tənzimlənir.

9.3 Fəaliyyətlə bağlı məlumatların konfidensiallığı

9.3.1 Konfidensial saxlanılan məlumat növləri

9.3.1.1 Fəaliyyət və quruluş sənədləri

Fəaliyyəti və quruluşu, həmçinin Sertifikatının etibarlılığının yoxlanması ilə bağlı detallar barədə məlumatlar əks olunan həssas daxili sənədləri, məsləhət və audit məqsədləri üçün istifadə istisna olmaqla, EH-SXM konfidensial saxlayır.

9.3.1.2 Audit məlumatları

EH-SXM fəaliyyəti və Sertifikatın etibarlılığının yoxlanılması ilə bağlı bütün audit məlumatları konfidensial saxlayır. EH-SXM öz qərarına və ya qanunvericiliyin tələblərinə müvafiq olaraq saytında audit barədə qısa icmal dərc edə bilər.

Qanunvericiliyin və müvafiq prosedur tələblərinə əsasən order və digər hüquqi tələblər barədə müraciət olduqda, audit məlumatlar haqqında tam şəkildə bu Qaydaların 9.3.4 və 9.3.5-ci bəndlərinə uyğun çıxarış verilə bilər.

9.3.1.3 Fərdi məlumatların konfidensiallığı

EH-SXM tərəfindən toplanan, işlənilən və ya istifadə edilən fərdi məlumatların konfidensiallığı “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanununa və bu Qaydaların 9.4-cü bəndinə müvafiq olaraq təmin olunur.

9.3.2 Konfidensial sayılmayan məlumat növləri

9.3.2.1 Sertifikat və onun statusu haqqında məlumatlar

EH-SXM tərəfindən kütləvi istifadə üçün verilmiş bütün Sertifikatlar yayımlana bilər. EH-SXM-in verdiyi Sertifikatların statusu haqqında məlumatlar bu Qaydalar, etibarlı SXM-lərin Sertifikatın tətbiqi qaydaları, Sertifikat siyasətləri və digər müvafiq razılaşmalar (məsələn, etibarlı tərəf razılaşması) əsasında Sertifikatın etibarlılığının yoxlanması xidmətlərinə müraciət imkanı olan hər kəs üçün açıqdır.

9.3.2.2 EH-SXM-in sənədləri

EH-SXM-in aşağıdakı sənədləri konfidensial sayılmır və ictimaiyyətə açıqlanır:

- Təsdiq olunmuş Sertifikat siyasəti və Sertifikatın tətbiqi qaydaları;
- Dərc olunmaq üçün məqbul sayılan digər sənədlər.

9.3.3 Sertifikatın ləğvi məlumatlarının açıqlanması

EH-SXM-in Sertifikatı ləğv edildikdə onun səbəbi açıqlana bilər. Sertifikatın ləğvi və ya Sertifikatın etibarlılığının yoxlanılması haqqında məlumatlar OCSP-responder və CRL-dən istifadə edərək açıqlanır. EH-SXM-in yoxlama xidmətləri barəsində sorğu verilmiş Sertifikatın etibarlı olub-olmadığını, ləğv edildiyini və ya qüvvəsinin dayandırıldığını, ya da statusu barədə məlumatın olmamasını müəyyənləşdirməyə imkan verir. Digər hər hansı məlumat açıqlanmır.

9.3.4 Hüquq-mühafizə orqanına çıxarışın verilməsi

Aşağıdakı hallar istisna olmaqla EH-SXM saxladığı heç bir sənəd və ya qeydi hüquq-mühafizə orqanlarına və ya əməkdaşlarına verə bilməz:

- müvafiq qaydada sorğu verildikdə;
- digər hüquqi prosedurlara əməl edildikdə.

9.3.5 Mülki iş üzrə sübut və ya araşdırma məqsədilə çıxarışın verilməsi

Aşağıdakı hallar istisna olmaqla, konfidensial sənəd və ya qeyd heç kimə verilmir:

- Düzgün (məsələn, bütün hüquqi prosedurlara müvafiq) doldurulmuş sorğu verildikdə;
- Sorğu verən şəxs səlahiyyətli və dəqiq identikləşdirilən olarsa.

EH-SXM mülki iş üzrə sübut və ya araşdırma məqsədilə sorğu edilən məlumatları müvafiq qanunvericilik tələblərinə uyğun prosedurlara riayət edərək təqdim etməlidir. Bunun üçün qanunvericiliyə müvafiq olan və təsdiq edilmiş daxili prosedurlar işlənilə bilər.

9.4 Fərdi məlumatların konfidensiallığı

EH-SXM tərəfindən toplanan, işlənilən və ya istifadə edilən fərdi məlumatların konfidensiallığı “Fərdi məlumatlar haqqında” və “Elektron İmza və elektron sənəd haqqında” Azərbaycan Respublikasının Qanunlarına müvafiq olaraq mühafizə olunur. Fərdi məlumatlar yalnız qanunvericilikdə nəzərdə tutulmuş hallarda Üçüncü tərəfə verilə bilər.

9.4.1 Konfidensial saxlanılan məlumatlar

EH-SXM fərdi məlumatların toplanması, işlənilməsi və istifadəsini tərəfindən "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanununa və bu Qaydaların tələblərinə müvafiq olaraq həyata keçirir.

Məlumatın aid olduğu şəxs və ya qurum tərəfindən açıqlanmasına birbaşa razılıq verilənə qədər qeydiyyat məlumatları konfidensial məlumat sayılır.

EH-SXM fəaliyyətinə xitam verdikdə, İmza sahiblərinin razılığı ilə onların Sertifikatları və bu Sertifikatlarla bağlı məlumatları akkreditə edilmiş başqa SXM-ə və ya səlahiyyətli orqana təhvil verməlidir. Təhvil verilməmiş Sertifikatlar ləğv edilir və saxlanılmaq üçün səlahiyyətli orqana verilir. Bütün hallarda belə məlumatlar saxlanılır və aidiyyəti İmza sahiblərinə Sertifikat xidmətlərinin göstərilməsi üçün istifadəsi təmin edilir.

9.4.2 Konfidensial sayılmayan məlumatlar

Qanunvericiliyə, EH-SXM-lə bağlanmış Müqaviləyə uyğun olaraq İmza sahibinin razılığı ilə Sertifikat və onun statusu barədə məlumatlar istifadə məqsədilə açıqlana bilər. Sertifikat siyasəti və bu Qaydalarda başqa hallar müəyyən edilməmişdirsə, İmza sahibi Sertifikatı əldə edərkən Sertifikatdakı məlumatı və Sertifikat xidmətlərinin göstərilməsi ilə bağlı digər məlumatları yayımlamaq üçün EH-SXM-ə icazə verir.

9.4.3 Konfidensial məlumatların mühafizəsinə görə məsuliyyət

EH-SXM-in bütün işçi heyəti və qurumları fərdi məlumatları mühafizə etməli, onların konfidensiallığının pozulması və ya Üçüncü tərəfə bəlli olmasının qarşısını almaq üçün qanunvericiliyin tələblərinə riayət etməlidir.

9.4.4 Konfidensial məlumatlardan istifadə barədə xəbərdarlıq və razılıq

Bu Qaydalarda başqa hallar nəzərdə tutulmamışdırsa, konfidensial məlumat aid olduğu şəxsin razılığı olmadan istifadə edilə bilməz.

9.4.5 Məhkəmə və inzibati proseslə bağlı açıqlama

EH-SXM aşağıdakı hallarda konfidensial məlumatları açıqlaya bilər:

- məhkəməyə çağırış və axtarış orderi ilə əlaqədar;
- mülki və ya inzibati işlə bağlı olaraq məhkəmə, inzibati və digər hüquqi proses zamanı məhkəməyə çağırış, yazılı izahat və sənədlərin hazırlanması kimi sorğularla əlaqədar.

9.4.6 Məlumatların açıqlanmasının digər şərtləri

Tətbiq edilmir.

9.5 Əqli mülkiyyət hüquqları

EH-SXM-in fəaliyyətinin təşkili ilə bağlı olan bütün sənədlərin, o cümlədən Sertifikatların, CRL-lərin, Sertifikat statusu mesajlarının, Sertifikat Direktoriyasının, həmçinin Müqavilələrin müəlliflik hüquqları da daxil olmaqla bütün əqli mülkiyyət hüquqları EH-SXM-ə məxsusdur.

9.6 Təmsilçilik və zəmanətlər

Tətbiq edilmir.

9.7 Məsuliyyət və məsuliyyətdən azad olma

EH-SXM bu Qaydaların əsasında Sertifikat xidmətləri göstərəcəkdir. Aşağıdakılar da daxil olmaqla, bu Qaydalarda əks olunan öhdəliklərdən başqa bütün digər öhdəliklər istisna edilir:

- Sertifikata daxil olan lakin EH-SXM tərəfindən verilməyən və ya yoxlanılmayan məlumatın düzgünlüyü və ya tamlığı;
- Bu Qaydalarda nəzərdə tutulmayan;
- EH-SXM-in idarəçiliyindən kənar məsələlər.

EH-SXM xəbərdarlıq edib-etməməsindən və ya onları qabaqcadan görmək imkanından asılı olmayaraq, aşağıdakılardan irəli gələn hər hansı zərərə görə cavabdeh deyil:

- İmza sahibi və Üçüncü tərəf arasındakı əməliyyatlar;
- bu Qaydalarla müəyyənləşdirilməmiş istifadə sahələri üzrə və ya məqsədlərlə kriptoqrafik açarlara, elektron imzalara və ya Sertifikat xidmətlərinə etibar edilməsi və onlardan istifadə;
- Üçüncü tərəf məhsulları və ya xidmətləri (proqram və texniki təminat da daxil olmaqla);
- hər hansı dolayı və ya birbaşa zərər.

EH-SXM dəymiş zərərə görə bu Qaydaların 9.2-ci bəndində nəzərdə tutulmuş məbləğ həddində məsuliyyət daşıyır.

9.8 Təzminat

EH-SXM-in fəaliyyəti nəticəsində İmza sahibinə vurulmuş maddi zərərin ödənilməsi İmza sahibi ilə mərkəz arasındakı Müqaviləyə əsasən müəyyənləşdirilir. Bu məqsədlə sığortalama imkanları da nəzərdə tutula bilər.

EH-SXM-in İmza sahibləri qarşısındakı məsuliyyətinin yuxarı həddi İmza sahiblərinin hamısı üçün eynidir.

9.9 Qüvvədə olma və qüvvədən düşmə

9.9.1 Qüvvədə olma

Bu Qaydalar EH-SXM-in Direktoriyasında dərc edildikdən sonra qüvvəyə minir. Bu Qaydalara edilən əlavə və dəyişikliklər də həmin qaydada qüvvəyə minir.

9.9.2 Qüvvədən düşmə

Bu Qaydalar onlara edilmiş əlavə və dəyişikliklərlə birgə növbəti versiyanın buraxılışına qədər qüvvədədir.

9.10 İştirakçılara fərdi bildirişlər və onlarla əlaqə

Tətbiq edilmir.

9.11 Dəyişikliklər

9.11.1 Bu Qaydaların dəyişdirilməsi proseduru

Bu Qaydaların aparılması və təsdiqi üçün daxili prosedurlar müəyyən edilir. Bunun nəticəsində Qaydaların cari fəaliyyətə tam uyğunluğu təmin edilir.

9.11.2 Məlumatlandırma mexanizmi və müddət

Bu Qaydaların cari versiyası EH-SXM-in saytında yerləşdirilir.

9.11.3 OİD-də dəyişikliklər

Bu Qaydalara edilən dəyişikliklər zamanı cari versiya ilə ciddi fərqlər yaranarsa, yeni OİD təyin edilir. Yeni OİD-in təyin edilməsi qərarı bu Qaydalara dəyişikliklər edilmə prosesinin tərkib hissəsidir.

9.12 Mübahisələrin həlli proseduru

9.12.1 Sertifikatın tətbiqi qaydalarının iyerarxiyası

Bu Qaydalarla digər siyasətlər, planlar, razılaşmalar, müqavilələr və ya prosedurlar arasında ziddiyyət yaransa, bu Qaydaların müddəaları əsas götürülür.

9.12.2 Mübahisələrin həlli prosesi

Bu Qaydaların həyata keçirilməsi ilə bağlı Tərəflər arasında mübahisə yaranarsa, məhkəməyə müraciət etməzdən əvvəl danışıqlar yolu ilə yaranmış vəziyyətin həllinə səy göstərilməlidir.

Əgər Tərəflər danışıqlar yolu ilə həllə nail ola bilmirlərsə, onda qanunvericiliyə müvafiq olaraq məhkəməyə müraciət edilə bilər [11] .

Tərəflərin mübahisəni bu Qaydalara uyğun olaraq həll etmək üçün atdıqları addımlara baxmayaraq, bu Qaydaların ehtimal olunan və ya real ciddi pozuntuları halında və ya EH-SXM-in fəaliyyətinin təhlükəsizliyinə bütövlükdə və ya qismən təsir edən mübahisə ilə bağlı EH-SXM məhkəmə qərarı ilə qadağa olunma hüququndan istifadə edə bilər.

9.12.3 Qanunvericilik

Bu Qaydalar Azərbaycan Respublikasının qanunvericiliyinə əsasən tənzimlənir və təfsir edilir.

9.12.4 Qarışıq müddəalar

Tətbiq edilmir.

9.12.5 Digər müddəalar

Tətbiq edilmir.

10 İstinadlar

[1] Elektron imza və elektron sənəd haqqında Azərbaycan Respublikasının Qanunu, Bakı şəhəri, 9 mart 2004-cü il.

[2] Elektron Hökumət Sertifikat Xidmətləri Mərkəzinin Sertifikat siyasəti

[3] Certification Practice Statement of Root Certification Authority of Root Certification Centre (CPS RCA)

[4] Certification Practice Statement of Policy Certification Authority of Root Certification Centre (CPS PCA)

[5] AZS 324-2008 (ISO/IEC 27002:2005) İnformasiya texnologiyası – Təhlükəsizlik metodları – İnformasiya təhlükəsizliyinin idarə edilməsi üzrə əməli qaydalar (Information technology – Security techniques – Code of practice for information security management).- SMPDK.- Bakı, 2008

[6] RFC 2560 X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol, June 1999

[7] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003

[8] RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002

[9] ETSI TS 101456 V1.3.1 (2005-05) Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified Certificates

[10] AICPA/CICA WEBTRUSTSM/TM Program For Certification Authorities Version 1.0

[11] Law on Courts

[12] Delivery and support of Certification Services, internal ICC CSP documentation

[13] ICC CSP Organisation Description, internal ICC CSP documentation

[14] Physical Security Regulations and Procedures, internal ICC CSP documentation

[15] Time Stamp Policy of ICC EGOV CSP (TP)

[16] Time Stamping Authority Practice Statement of ICC EGOV CSP (TPS)

[17] Infrastructure certificate Practice Statement of ICC CSP