Elektron hökumət portalı modeli və onun təhlükəsizlik məsələləri

Cəmşid Naxçıvanski

AMEA İnformasiya Texnologiyaları İnstitutu

cemshid@rabita.az

***Xülasə*— Məqalədə elektron hökumət portalının konseptual modeli üzərindən onun komponentləri, struktur mexanizmləri və təhlükəsizlik məsələləri təsvir edilmişdir. Təhlükəsiz informasiya mübadiləsi, informasiyanın tamlığı ilə bağlı sistemdə nəzərdə tutulan yanaşmalar, alqoritmlər və protokollar barədə məlumat verilmişdir.**

***Açar sözlər*— elektron hökumət modeli; təhlükəsizlik, portal;**

I. GİRİŞ

Nəzərdə tutulan Elektron Hökumət Portalı (EHP) sistemi ümumilikdə nisbətən müstəqil iki hissədən ibarətdir - Baza sistemi və Mərkəzi portal. Baza sistemi veb servislər [1] əsasında paylaşılmış və təhlükəsiz iş mühitini formalaşdıran, Mərkəzi portal isə fərdi istifadəçilərə xidmət göstərən hissədir. Bu iki hissədən daha mürəkkəbi baza sistemidir, çünki o daha çox paylaşılmış komponentlərdən ibarətdir.

Baza sistemi EHP sisteminə qoşulmuş təşkilatlar arasındakı veb-servislərin vasitəçisi rolunu oynayır. Bu təşkilatların hər birində istifadəçilər və veb-servislər üçün şlüz rolunu yerinə yetirən təhlükəsizlik serveri quraşdırılır. Şlüz aşağıdakıları təmin edir:

- əldə olunmuş məlumatın inandırıcılığını, tanınmasını və bütövlüyünü;
- digər təşkilatlara ötürülən məlumatların məxfiliyini;
- təşkilat səviyyəsində idarəni.

Sübutedici qüvvəsinin təmin olunması məqsədilə Şlüz rəqəmsal imzanın mexanizmini, loqların müdafiəsini və vaxt ştampını tətbiq edir.

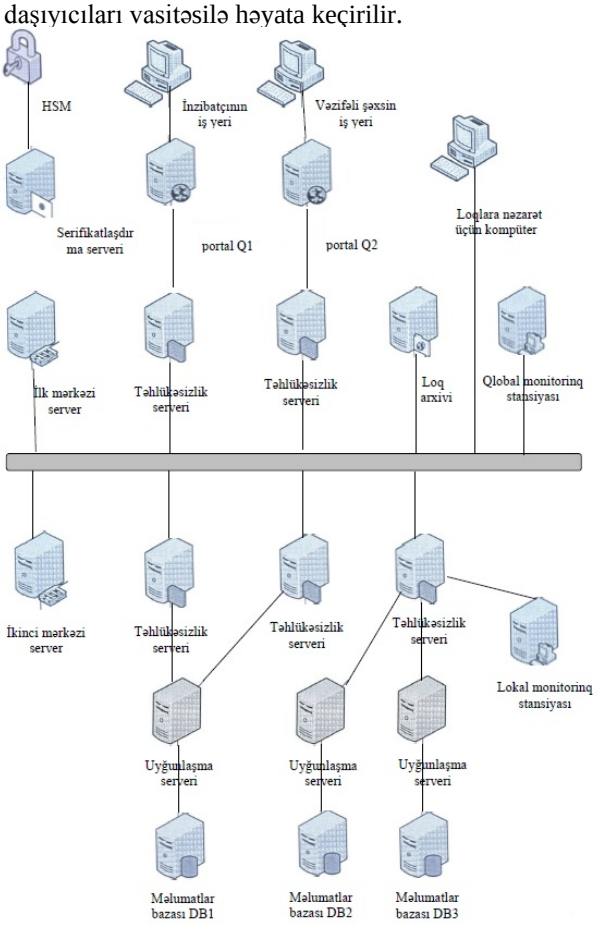
Mərkəzi portalın vətəndaşlar, sahibkarlar və müxtəlif təşkilatdaxili istifadəçilər üçün nəzərdə tutulmuş formaları vardır. Bütün bu portallar Baza sistemi üzərindən təhlukəsiz məlumat mübadiləsi edirlər.

II. KOMPONENTLƏR

Sistemin strukturuna nəzər yetirdikdə onun müxtəlif komponentlərdən ibarət olduğu görünür (Şəkil 1.). İrəlidə hər bir komponent barədə məlumat verilmiş və onun təhlükəsizliklə bağlı rolu izah edilmişdir. Sistemin işini anlamaq üçün nəzərə almaq lazımdır ki, təşkilatlar arasındakı bütün xidməti məlumatlar təhlükəsizlik serverləri arasında mübadilə olunur və ümümi təhlükəsizliyi təmin etmək üçün bütün komponentlər əlaqəli şəkildə çalışır.

A. Sertifikatlaşdırma Mərkəzi (Serveri)

Sertifikatlaşdırma mərkəzi, sistemi istifadə edən bütün təşkilatlara sertifikatların verilməsi xidmətini həyata keçirir. Təhlükəsizlik baxımından sertifikatlaşdırma mərkəzinin serveri offlayn(hər hansı bir şəbəkəyə qoşulmamış) rejimdə işlədiyindən digər serverlər ilə məlumat mübadiləsi xüsusi məlumat daşıyıcıları vasitəsilə həyata keçirilir.



Şəkil 1. EHP-nin ümumi strukturu

Sertifikatlaşdırma xidmətləri sistemin bütün iş zamanı ərzində verilmiş bütün sertifikatının qeydiyyatını aparır, onların etibarlılığını yoxlayır. Sertifikat bazası mübahisələrin həlli və imzalanmış hər hansı konkret məlumatlar üçün məsuliyyətli təşkilatı aydınlaşdırmaq üçün istifadə edilə bilir.

Sertifikatlaşdırma mərkəzi offlayn rejimdə işlədiyindən, bütün məlumatlar xarici daşıyıcıları (disket, CD/DVD, USB)

vasitəsilə aparılır. Təşkilat haqqında məlumatlar hər bir dəyişiklikdən sonra eksport edilir və mərkəzi serverin kataloq xidmətinin köməyi ilə paylanılır. Lazımi səviyyədə təhlükəsizliyə nail olmaq məqsədilə, sertifikat açarlarının mühafizəsi üçün HSM kriptoqrafik modullarından istifadə oluna bilər [2].

B. Mərkəzi server

Mərkəzi serverin əsas vəzifəsi - təhlükəsizlik serverləri üçün kataloq xidmətləri və vaxt möhürü təmin etməkdir.

Kataloq xidmətləri sistem ilə bağlı təşkilatlar, onların təhlükəsizlik serverləri (məsələn, IP-ünvanları, etibarlı sertifikatlar) və digər mərkəzi nəzarət məlumatları (məsələn, təşkilatların mümkün qrupları) haqqında informasiya verir. Ötürülən məlumatın sübutedici dəyərini təmin etmək üçün təhlükəsizlik serverlərində digər qorunma mexanizmləri ilə birlikdə vaxt möhürü servisi də tətbiq oluna bilər [3].

C. Təhlükəsizlik serveri

Təhlükəsizlik serveri təşkilatlar arasında veb-servislərin vasitəçisi rolunu görür. Bir server digər təhlükəsizlik serverlərinə (yəni, təşkilatlara) veb-servislər təklif edə, eləcə də onların təklif etdiyi veb-servisləri istifadə edə bilər [4]. Bundan başqa, təhlükəsizlik serverləri ona təşkilatların təklif etdiyi servislər barədə məlumat verən daxili meta servislərlə təchiz olunub və sistem kataloqundan əldə edilə bilir. Təhlükəsizlik serverləri həmçinin Sertifikatlaşdırma mərkəzinin verdiyi sertifikatlarla qarşı tərəf arasında təhlükəsiz kanalın (HTTPS [5]) yaradılması və uyğun mübadilə məlumatlarının rəqəmsal imzalanması işini də həyata keçirir.

D. Adaptasiya (Uyğunlaşma) serveri

Adaptasiya serverinin əsas rolu Təhlükəsizlik serverindən gələn sorğuları yerli sistemin başa düşəcəyi formaya çevirməklə yerli məlumatlar bazası ilə EHP sistemi arasında inteqrasiyanı(adaptasiyanı) təmin etməkdir. EHP sisteminə qoşulan hər bir təşkilat özündə müəyyən verilənlər bazası formalaşdırır. Bu verilənlər bazası müxtəlif verilənlər bazası idarəetmə sistemləri (MsSQL, Oracle, MySql və s) üzərində qurula bilər. Adaptasiya serverinin köməyi ilə təhlükəsizlik serverindən gələn sorğu burada emal olunaraq, uyğun verilənlər bazasının anlayacağı formaya gətirilir və sorğuya uyğun cavab əldə olunur. Daha sonra əldə olunan cavab yenidən emal olunaraq təhlükəsizlik serverinə, oradan da sorğunun ilk göndərildiyi təhlükəsizlik serverinə ötürülür.

E. Monitorinq stansiyası

EHP sisteminin vəziyyətinə nəzarət etmək üçün monitorinq sisteminin qurulması nəzərdə tutulur. Monitorinq stansiyaları monitorinq sisteminin bir hissəsidir və EHP sistemində serverlərin mövcud vəziyyəti barədə operativ məlumat toplayır.

Monitorinq stansiyası yerli və ya mərkəzi stansiya rolunu yerinə yetirə bilər.

- Yerli monitorinq stansiyasını təhlükəsizlik serverinin sistem inzibatçısı quraşdırır. Bununla tabeliyində olan təhlükəsizlik serverlərindəki məlumatları izləyə bilir.
- Mərkəzi monitorinq stansiyasını mərkəzin sistemin inzibatçı quraşdırır. O, bütün təhlükəsizlik serverləri və mərkəzi serverlər barədə məlumat ala bilir. Beləliklə, mərkəzi monitorinq stansiyası vasitəsilə bütün təhlükəsizlik serverləri və sistemin istifadəsi ilə bağlı statistikanı əldə etmək mümkün olur.

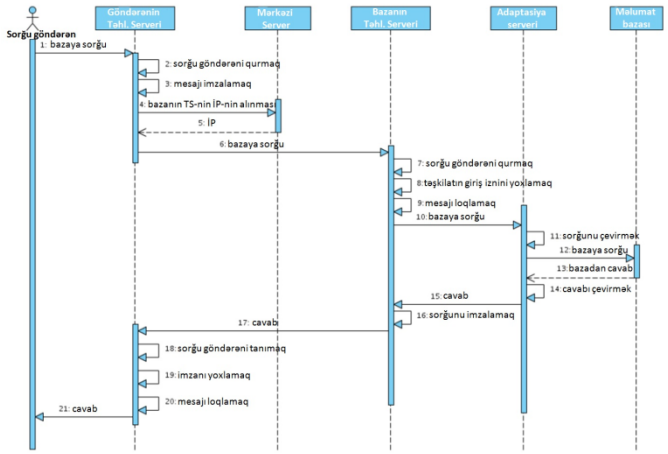
Təhlükəsizlik serverləri və mərkəzi serverlər monitorinq stansiyalarına üç növ məlumat verir:

- Vəziyyət haqqında məlumatlar - serverlər vaxtaşırı olaraq onların vəziyyətini təsvir edən parametrlər (prosessor yükü, boş yaddaşın həcmi və s.) barədə əhəmiyyətli məlumatlar göndərirlər;
- Zədələnmələr barədə məlumatlar - əgər sorğuların verilməsi zamanı nasazlıq baş veribsə müvafiq məlumatlar monitorinq stansiyasına göndərilir;
- Sorğu haqqında məlumat - təhlükəsizlik serverləri hər sorğuya (sorğu göndərən müəssisə, fərdi identifikasiya kodu, məlumat və sorğu adı) uyğun monitorinq stansiyasına məlumat göndərir.

Serverlər və monitorinq stansiyaları arasında ötürülən monitorinq məlumatları uyğun simmetrik şifrələmə alqoritmindən istifadə edilərək şifrələnir. Şifrələmə açarları DNS vasitəsilə paylanır.

Məlumat bazasına müraciət və onun fəaliyyət prosesini aşağıdakı diaqramdakı kimi təsvir edə bilərik (Şəkil 2.):

1) Sorğu nümayəndəsi (portal) yerli təhlükəsizlik serverinə sorğu göndərir;
2) Təhlükəsizlik serveri sorğu göndərəni tanıyır, məlumatı imzalayır, mərkəzi serverdən sorğu göndəriləcək təhlükəsizlik serverinin İP adresini əldə edir və məlumatları qorunmuş şəkildə göndərir;
3) Məlumat bazasının təhlükəsizlik serveri sorğu göndərəni müəyyən edir, sorğu göndərən tərəfin məlumat əldə etmək hüququ olub-olmadığını yoxlayır, loq məlumatlarını yazır və sorğunu adaptasiya serverinə göndərir;
4) Adaptasiya serveri sorğunu yerli sistemin başa düşəcəyi formaya uyğunlaşdırıb məlumat bazasına sorğu verir;
5) Məlumat bazası serveri sorğuya cavab verir;
6) Adaptasiya serveri məlumat bazasından gələn sorğunu təhlükəsizlik serverinin anlayacağı formaya çevirir və onu təhlükəsizlik serverinə göndərir;
7) Məlumat bazasının təhlükəsizlik serveri sorğuya uyğun cavabı imzalayır və onu sorğu göndərən tərəfin təhlükəsizlik serverinə təhlükəsiz şəkildə göndərir;



Şəkil 2. Sorğuların fəaliyyət gedişi.

8) Müəssisənin təhlükəsizlik serveri imzanı yoxlayır, sorğuya cavabı loqda yadda saxlayır və sorğunu sorğu nümayəndəsinə ötürür.

III. STRUKTUR MEXANİZMLƏRİ

Təhlükəsizlik məsələləri ilə bağlı olaraq sistemdə bəzi texniki mexanizmlər tətbiq olunur.

A. Heş-funksiyanın tətbiqi

Təhlükəsizliyin daha kritik olduğu hissələrdə SHA-512 heş funksiyası, faylların eksport və import hallarının tamlığını yoxlamaq üçün MD5 heş funksiyasından istifadə oluna bilər [6]. Heş funksiya həmçinin DNS-də dərc olunmuş hesablama açarlarını yazdırmaq üçün də istifadə olunur.

B. NTP (şəbəkə zamanı protokolu)

EHP sistemində server saatları sinxronizasiya olunmalıdır. Bu DNS servisinin düzgün funksionallığı, sistemə təhlükəsiz qeydiyyat üçün mühüm amildir. Zamanın sinxronlaşdırılması üçün NTP protokolundan istifadə edə bilərik [7].

Burada əsas mərkəzi serverin saatının sinxronlaşdırılması uyğun ümümi icazəli qaynaq vasitəsilə edilə bilər. İkinci mərkəzi server öz saatını birinci mərkəzi serverin saatına görə təhlükəsizlik serveri və monitorinq stansiyası isə öz saatlarını mərkəzi serverlərin saatlarına görə sinxronlaşdıra bilərlər.

C. Sorğuların təsdiq dəyərinin yoxlanılması

EHP sistemi vasitəsilə göndərilən sorğulara uyğun cavab formalaşan zaman bəzi mühüm işlər yerinə yetirilməlidir. İlk olaraq, sorğusuna cavab alan tərəf sübut edə bilməlidir ki, həqiqətən də sorğuya gələn cavab onun sorğuladığı məlumat bazasından gəlib. Həmçinin məlumat bazası da avtorizasiya olunmuş və olunmamış sorğuları fərqləndirə bilməlidir.

Avtorizasiya olunmuş sorğuları təsdiq etmək üçün aşağıdakı komponentlərdən istifadə edə bilərik:

- **Təhlükəsizlik serverinin sorğularının loqu** − cari təhlükəsizlik serveri üzərindən keçən bütün sorğu və cavabların loqunu özündə saxlayır. Sorğular məlumat bazası tərəfdə saxlanılır, cavablar isə təşkilat tərəfdə. Loqa yazılan yeni məlumat heş funksiyası ilə bir əvvəlki loqa bağlanılır. Bununla loqlar üzərində aparılacaq hər hansı saxta-laşdırmanın qarşısı alınır, belə ki, saxtalaşdırılmış loqlarda yazıların qırılmaz zənciri formalaşmır.
- **Mərkəzi serverin loqu** − bütün təhlükəsizlik serverlərinin aralıq loqlarını özündə saxlayır. Bununla biz təhlükəsiz serverinin administrato-runun yadda saxlanılmış loqlar üzərindəki saxtalaşdırmasının qarşısını alırıq.
- **Sertifikatlaşdırma mərkəzinin məlumat bazası** − bütün sertifikatları özündə saxlayır və sistemə paylaşdırır. Bu imzalanmış sorğunun kimə aid olduğunu aydınlaşdımağa icazə verir.
- **Xüsusiyyətlər** − sorğu və cavabları izah etmək üçün istifadə olunurlar. Sorğunun identifikasiyası zamanı onun təşkilat tərəfində generasiya olunub saxlanılmış unikal nömrəsi (ID) yoxlanılır.

Sorğuların təsdiqi təhlükəsizlik serveri və mərkəzi server tərəfində üç hissədən ibarətdir. Sorğuların həqiqiliyini təsdiq etmək üçün onlar mərkəzi server və təhlükəsizlik serveri arasında göndərilir. Həqiqiliyin və bütövlüyün olması son dərəcə vacibdir, çünki bunlar birbaşa yoxlamanın nəticəsinə təsir göstərir.

Sorğu həqiqliyinin yoxlanılması bir neçə mərhələdən keçir.

- İlk mərhələ təhlükəsizlik serverində baş verir: loqlar arxivindən verilən identifikatora görə sorğu tapılır, onun ID-si, heşi və sertifikatın heşi mətn faylına eksport olunur. Fayl mərkəzi serverə ötürülür.
- Sonrakı mərhələ mərkəzi serverdə baş verir: mətn faylı sorğu ilə birlikdə təhlükəsizlik serverindən yüklənir, daha sonra heş loqları bazasından və sertifikatlar bazasından uyğun heş və sertifikat axtarılır. Tapılan informasiyaya uyğun fayl geri təhlükəsizlik serverinə göndərilir.
- Son mərhələdə yenidən təhlükəsizlik serveri keçirilir: mərkəzi serverin cavabı yüklənir, loq sorğusu deşifrələnir (əgər gizli loq sorğusu varsa) və yoxlanılır, daha sonra sorğunun həqiqiliyi haqqında son cavab əldə olunur.

Sorğu aşağıdakı şərtlər yerinə yetirildikdə həqiqi sayılır:

- Mərkəzi serverin cavabı yoxlanılan əlaqəli cavaba və heşə aiddirsə;
- Yoxlanılan əlaqəli cavabın heşi mərkəzi serverin loq arxivində tapılıbsa və onun buradakı qeydiyyat tarixi təhlükəsizlik serverindəki qeydiyyat tarixi ilə bir dəqiqə dəqiqliyi ilə (bir dəqiqədən çox fərq etməyərək) üst-üstə düşürsə;
- Mərkəzi serverin sertifikat arxivində müvafiq sertifikat tapılıb və sorğu göndərilən anda etibarlıdırsa, həmçinin təhkükəsizlik serverində əlaqəli sorğu heşinin yaradılması tarixi də göndərilən anda etibarlıdırsa. Sorğu zamanı həqiqiliyi sübut etmədə nəzərə almaq lazımdır ki, yoxlanılan

sorğunun sertifikatı onun heşinin mərkəzi serverə ötürülməsindən əvvəl ləğv oluna bilər;

- Rəqəmsal imza həqiqilik mesajıdır. Əgər sorğu loqu sifrələnib və deşifrələnmə zamanı xəta baş veribsə və ya deşifrələnmə qəbul edilməyibsə, o zaman yoxlanılma prosesi mümkün olmayacaqdır.

D. Kataloq xidməti

Kataloq xidmətinin DNSSEC əlavəsi istifadə edilərək DNS sistemi üzərində qurulması mümkündür [8]. Belə həll DNS sisteminin bütün müsbət xüsusiyyətlərini (miqyaslılıq, davamlılıq, təhlükəsiz rəqəmsal imzalardan istifadə) istifadə etməyə imkan verəcəkdir. Etibarlılığı təmin etmək üçün bir əsas mərkəzi server və bir neçə əlavə mərkəzi server quraşdırmaq olar. Əlavə serverlər fiziki olaraq başqa yerlərdə də ola bilərlər. Əsas serverdəki bütün əməliyyatların əlavə serverlərdə təkrarlanması avtomatik olaraq standart DNS-protokolu vasitəsilə yerinə yetirilə bilər.

E. Açarların Dəyişdirilməsi

Açarların dəyişdirilməsi prosedurları zamanı sistemin fasiləsiz işini təmin etmək üçün EHP mühüm açar dəyişdirmə protokolundan istifadə edə bilər. Bu prosedur bir neçə addımda əldə olunur.

1) Tərəflərdən biri yeni açar generasiya edir, amma köhnə açar ilə işləməkdə davam edir.

2) Yeni açar dərc olunur. Bütün digər tərəflər həm köhnə, həm də yeni açarı istifadə etməyə başlayır.

3) İstinad edilən tərəf artıq yeni açar istifadə etməyə başlayır. Digər tərəflər artıq bu açarı tanıdığından sistemin işi fasiləsiz davam edir.

4) İstinad edilən tərəf köhnə açarı silir.

5) Əvvəlki açar ləğv edilir və digər tərəflər köhnə açarın istifadəsini dayandırırlar.

ƏDƏBIYYAT

[1] W3C: “Web Services Glossary”. 2004-02-11.

[2] Network Working Group: “HTTP Over TLS”. The Internet Engineering Task Force. May 2000

[3] IETF RFC 3161,official specification

[4] F. Hirsch, J. Kemp, J. Ilkka, “Mobile Web Services: Architecture and Implementation.” John Wiley & Sons. 2007.

[5] NIST: “Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths". January 2011.

[6] http://en.wikipedia.org/wiki/SHA-2

[7] D. L. Mills, “Computer Network Time Synchronization: The Network Time Protocol.” Taylor & Francis. pp. 12, 2010.

[8] "RFC 4033: DNS Security Introduction and Requirements". The Internet Society. March 2005. p. 12.