UOT 004.056 DOI: 10.25045/jpit.v12.i1.03

İmamverdiyev Y.N.[1], Abbasov H.H.[2]
[1]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[2]NRYTN Milli Sertifikat Xidmətləri Mərkəzi, Bakı, Azərbaycan
[1]yadigar@iit.science.az, [2]hebib@rabita.az

MİLLİ E-İMZA İNFRASTRUKTURUNUN AKTUAL ELMİ-TƏDQİQAT PROBLEMLƏRİ

Daxil olmuşdur: 27.11.2020 Düzəliş olunmuşdur: 04.12.2020 Qəbul olunmuşdur: 17.12.2020

Təqdim olunan araşdırma işində elektron imza (e-imza) ilə bağlı milli e-imza infrastrukturunun mövcud texniki və məntiqi imkanlarını araşdırmaqla, sistemə düşən yükün optimal idarə edilməsi və problemlərin araşdırılması müəyyən edilib. E-imza vətəndaşların elektron mühitdə identikləşdirilməsi üçün şəxsiyyət vəsiqəsi rolunu təmin etdiyi üçün e-dövlət ekosistemində formalaşdırılan informativ və interaktiv elektron xidmətlərə əlçatanlığın təmin edilməsi və bu xidmətlərdən təhlükəsiz istifadə edilməsi e-imza vasitəsi ilə həyata keçirilir. Məqalədə milli e-imza infrastrukturunun yeni texnoloji çağırışlar, mobillik imkanlarının artırılması, məhdud resusrlu qurğularda yüksək məhsuldarlığın təmin edilməsi, e-xidmətlərdən geniş istifadə üçün yüksək təhlükəsizlik tələbləri baxımından təkmilləşdirilməsi problemləri analiz edilir və aktual elmi-praktiki məsələlər müəyyən edilir. Müəyyən edilən problemlərin həlli istiqamətində beynəlxalq təcrübə araşdırılmaqla milli infrastrukturun komponentlərinin təhlükəsizliyinin və inam zəncirnin qiymətləndirilməsi istiqamətində mərkəzlərinin işinin modelləşdirilməsi üçün elmi-tədqiqat istiqamətləri analiz edilmişdir. Məqalədə milli e-imza infrastrukturunun özünün təhlükəsizlik problemlərinin müəyyən edilməsi ilə mərkəzlərin xidmət sahələrində təhlükəszilik komponenti kimi səmərəsi müəyyən edilir.

Açar sözlər: *e-imza, açıq açar infrastrukturu, milli e-imza infrastrukturu, etimad, Əşyaların İnterneti, sertifikat.*

Giriş

Adətən, e-imza alqoritmləri açıq açarlı kriptoqrafiyaya əsaslanırlar və e-imzanın praktikada reallaşdırılması üçün xüsusi infrastrukturun – Açıq Açarlar İnfrastrukturunun (AAİ) (*ing. Public Key Infrastructure, PKI*) qurulması tələb edilir [1]. Əksər ölkələrdə e-imza infrastrukturunun formalaşdırılmasına keçən əsrin sonlarında başlanmışdı. Ölkəmizdə də milli e-imza infrastrukturunun qurulması işlərinə 2004-cü ilin mayında "Elektron imza və elektron sənəd haqqında" Azərbaycan Respublikası Qanununun qəbul edilməsi ilə təkan verilmişdi. Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyi bu qanundan irəli gələn məsələləri müvafiq mərkəzi icra hakimiyyəti orqanları ilə birlikdə planlaşdıraraq Milli Sertifikat Xidmətləri Mərkəzi qurmuşdur. Bu mərkəz Kök Sertifikat Mərkəzi və onun tabeliyində iyerarxik bağlılığı olan Siyasət Mərkəzi, Hakimiyyət Orqanları Mərkəzi və Elektron Hökumət Mərkəzindən ibarətdir. Hər bir mərkəz zəruri aparat və proqram təminatı ilə təmin edilmişdir və özünün müstəqil sertifikat siyasətini formalaşdırır.

E-imza sertifikatlarının bütün vətəndaşlara verilməsi üçün Milli Sertifikat Xidmətləri Mərkəzi tərəfindən yeni nəsil şəxsiyyət vəsiqələrinə (e-İD layihəsi) vəsiqə sahibinin gücləndirilmiş və təkmil elektron imza sertifikatları, imza yaratma və yoxlama məlumatları daxil edilir. Bu layihənin tam icrasından sonra e-hökumət konsepsiyasının daha da inkişafı üçün mobil e-hökumətin qurulması və nəticə etibari ilə dövlət, özəl və yerli özünüidarəetmə orqanlarının xidmətlərinin elektronlaşması bütünlükdə e-dövlətin əsasını təmin edəcək.

Elektron xidmətlərin, o cümlərdən e-dövlət xidmətlərinin geniş istifadəsi ilə elektron qarşılıqlı əlaqələrin qurulması zamanı tərəflərin təhlükəsiz və hüquqi autentifikasiyası vasitəsi kimi e-imzanın istifadəsi də genişlənir. Bundan əlavə, istifadəçilərin, həmçinin e-xidmətlərin mobilliyini təmin etmək üçün e-imzanın mobil və bulud platformalarında reallaşdırılması məsələsi meydana çıxır.

Əşyaların İnternetinin həyatın müxtəlif sahələrinə (o cümlədən, e-tibbə) tətbiqi ilə təkcə insanların deyil, onların adından "çıxış edən" əşyaların da autentifikasiyası üçün e-imzadan istifadə edilir. Hazırda bir çox ölkənin eİD sistemləri e-imza infrastrukturuna əsaslanaraq fəaliyyət göstərir [2].

Beləliklə, yuxarıda sadalanan proseslər ölkənin e-imza infrastrukturunun təkmilləşdirilməsini, miqyaslanmasını, yeni texnoloji platformalara keçidini, müxtəlif ölkələrin e-imza infrastrukturları arasında etimad münasibətlərinin təmin edilməsi üçün müvafiq mexanizimlərin reallaşdırılmasını zəruri edir. Bu problemlər həm təşkilati və hüquqi tənzimləmə tədbirlərinin görülməsini, həm də yeni texnoloji həllərin işlənməsini və tətbiqini tələb edir. Bu baxımdan milli e-imza infrastrukturunun təkmilləşdirilməsi üçün vacib elmi-tədqiqat problemlərinin müəyyən edilməsi aktual elmi-praktiki məsələdir. Təqdim olunan tədqiqat işi bu sahədə aktual elmi-tədqiqatların əsas istiqamətlərinin müəyyən edilməsinə və onların həlli vəziyyətinin analizinə həsr olunur.

Açıq açarlar infrastrukturunun əsas elementləri

AAİ termini açıq açarlı kriptoqrafik texnologiyaların istifadəsi üçün zəruri olan proqram-aparat vasitələri və təşkilati-texniki tədbirlər kompleksini əhatə edir. AAİ aşağıdakı komponentləri əhatə edir [3]:

Sertifikat Xidmətləri Mərkəzi (SXM) – AAİ-nin əsas idarəetmə komponentidir, tabeçiliyində olan SXM-lər və və son istifadəçilər üçün elektron sertifikatların verilməsi üçün nəzərdə tutulub. Hazırlanmış bütün sertifikatların reyestrindən başqa, SXM sistemin reqlamenti ilə müəyyən edilən müntəzəmliklə geri çağırılmış sertifikatların siyahısını (*ing. Certificate Revocation List, CRL*) formalaşdırır.

Qeydiyyat Mərkəzi (QM) – AAİ-nın məcburi olmayan komponentidir. QM-in əsas vəzifəsi – istifadəçilərin qeydiyyatı və onların SXM ilə qarşılıqlı əlaqəsinin təminidir. QM rəqəmsal sertifikatın tərkibinə daxil edilən bütün məlumatları toplayır, yoxlayır və sertifikat hazırlanması üçün SXM-ə təqdim edir.

Son istifadəçi – sertifikatın sahibi olan və AAİ-dən istifadə edən istifadəçi, tətbiqi proqram və ya sistem.

Sertifikatlar bazası – cari sertifikatlar və geri çağırılmış sertifikatlar AAİ-nun müvafiq verilənlər bazasında saxlanır. Bu açıq verilənlər bazasıdır, verilmiş və geri çağırılmış sertifikatlar haqqında informasiya bazadan sorğu əsasında göndərilir. Belə sorğular üçün real vaxt rejimində onlayn sertifikatların statusu protokolunun (*ing. Online Certificate Status Protocol, OCSP*) yoxlanılmasından istifadə etmək olar. Sertifikatlar bazası öz verilənlərini ya sadə kataloqlu giriş protokolunda (*ing. Lightweight Directory Access Protocol, LDAP*), ya da X.500 əsasında yaradılmış kataloqda nəşr edir.

AAİ qurulmasının bir neçə müxtəlif arxitektura modeli fərqləndirilir:

- iyerarxik: infrastrukturda ən yüksək SXM qeydiyyat mərkəzlərinin işini idarə edir; onlar da öz növbəsində son istifadəçilərlə qarşılıqlı əlaqəni təmin edirlər;
- şəbəkə: müstəqil SXM-lər bir-birini qarşılıqlı sertifikasiya edərək şəbəkədə birləşirlər;
- qarışıq: əvvəlki iki modelin əlamətlərini birləşdirir.

İyerarxiya prinsipi ilə qurulmuş AAİ-də bütün SXM-lər iyerarxik tabeçilik prinsipinə görə birləşirlər. Kök (mərkəzi) SXM özü üçün və tabe SXM-lər üçün sertifikatlar buraxır. Tabe SXM-lər isə öz növbəsində iyerarxiyanın sonrakı səviyyəsindəki SXM-lər üçün və ya öz istifadəçiləri üçün sertifikatlar buraxırlar.

Şəbəkə arxitekturasında bütün SXM-lər bərabər və ya eyniranqlı olurlar, yəni iyerarxiyanın eyni səviyyələrində yerləşirlər. Şəbəkə modeli ilk dəfə 1991-ci ildə F.Zimmerman tərəfindən ümumi istifadə üçün yaradılmış daha yaxşı məxfilik (*ing. Pretty Good Privacy, PGP*) kriptoqrafik paketində reallaşdırılıb.

Milli e-imza infrastrukturunun fiziki və məntiqi modeli

Milli e-imza infrastrukturu hibrid model əsasında formalaşdırılır, özündə həm iyerarxik, həm də şəbəkə modelinin elementlərini ehtiva edir.

Milli e-imza infrastrukturunun fiziki modeli. Milli e-imza infrastrukturuna daxil olan komponentlər fiziki olaraq üç qrupda cəmləşir:

- AAİ-yə daxil olan əsas komponentlər (proqram təminatı və serverlər);
- Mərkəzlərin açarlarının saxlanması və vahid vaxt mənbəyi üzrə aparat təhlükəsizliyi modulları (*ing. Hardware Security Module, HSM*), vaxt ştamplama orqanı (*ing. Time Stamping Authority, TSA*), əsas vaxt mənbəyi saatı (ing.*Time Source Master Clock, TSMC*);
- Şəbəkə avadanlıqları.

Bu fiziki model əsasında dayanıqlılıq ehtiyat elementlər ilə təmin edilir.

Milli e-imza infrastrukturunun məntiqi modeli. Milli e-imza infrastrukturunun fiziki modeli əsasında məntiqi modeli qurulur. Məntiqi modelə Milli Sertifikat Xidmətləri mərkəzinə məntiqi bağlı olan "Hakimiyyət Orqanları" və "Elektron Hökumət" sertifikat xidmətləri mərkəzlərinin əsas obyeklər toplusu, təqdim edilən məhsulun tipi, müraciət əsasında formalaşan ərizə, müvafiq imza daşıyıcısı, şəxsi identifikasiya kodunun (*ing. Personal Identification Number, PIN*) zərfləri üçün məlumatların hazırlanması, fərdiləşmə modulu, xəbərdarlıq sistemi, vaxt möhürü obyektləri, subyekt üzrə məlumatların idarə edilməsi və son istifadəçi sertifikatının verilməsi mexanizmi, arxivləşdirmə və audit obyektləri daxildir.

Milli e-imza infrastrukturu quruculuğu sahəsində bəzi ölkələrin təcrübəsi

Dünya ölkələrində e-imza qanunları 1990-cı illərdən qəbul edilməyə və onun həyata keçirilməsi üçün e-imza infrastrukturlarının qurulmasına başlanmışdır. Bu bölmədə milli e-imza infrastrukturu quruculuğu sahəsində bəzi ölkələrin təcrübəsi analiz edilir.

Son illərdə fiziki şəxslərə, müəssisələrə və dövlət təşkilatlarına e-xidmətlər göstərmək üçün Avropa İttifaqının bir sıra təşəbbüsləri və çərçivə sənədləri hazırlanmışdır. Bu səylərin əksəriyyəti çoxsaylı milli və transmilli tranzaksiyalar üçün rəqəmsal sertifikatların istifadəsini nəzərdə tutur. Milli PKI konsepsiyası [4]-də sistemli yanaşma vasitəsilə təqdim edilir, əsas dəstək faktorları müqayisə edilir, geniş yayılmış istifadə halları müzakirə edilir və Avropa miqyasında açıq problemlər araşdırılır.

Avropada milli eID sistemlər arasındakı fərqləri izah etmək üçün [2]-də səmərəli bir yanaşma müəyyən olunur. Aparıcı aktorlarla geniş ekspert müsahibələrinə əsaslanaraq, Avstriya, Belçika, Almaniya və İspaniyada milli e-şəxsiyyət vəsiqələrinin tətbiqi proseslərinin ilk müqayisəsi aparılmış və bu dörd haldan alınan ümumiləşdirmələrin etibarlılığını yoxlamaq üçün Danimarka, Finlandiya, Estoniya və İsveçdən ibarət dörd ölkənin hesabatı ilə tamamlanmışdır. Genişləndirilmiş müqayisələr Avropada eID sistemləri arasındakı müxtəlif texniki və təşkilati xüsusiyyətləri, məsələn, Danimarkada tamamilə proqram təminatına əsaslanan həllər və ya İsveçdə tam eIDM autsorsinqi kimi fərqləri göstərir.

Danimarka başqa ölkələrlə müqayisədə e-hökumətlə işə erkən başlamışdı və yüksək "e-hazırlıq" səviyyəsinə malik idi, lakin 20 il ərzində ölkədə ümummilli e-imza infrastrukturu qurulmamışdı. eID-nin Danimarkada texnoloji, təşkilati və hüquqi aspektlərinin analizi və bir sıra Avropa ölkələri ilə müqayisəsi bu paradoksu izah etməyə kömək etmişdir [5]. Tədqiqatçıların gəldiyi qənaətə görə, Danimarkada xüsusi yanaşmanın formalaşmasının üç əsas səbəbi konfidensiallıq, hökumətlərarası koordinasiyanın zəifliyi, dövlət və özəl sektorlar arasında əməkdaşlığın olmaması ilə əlaqədardır.

Elektron idarəetmədə son inkişaf rəqəmsal imza imkanlarından istifadə etməyi nəzərdə tutur, lakin istifadəçi təcrübəsinin azlığı, texnologiyalar və bununla əlaqəli prosedur problemlərinin olması e- imza imkanlarından istifadədə müəyyən çətinliklər yaradır. Hindistanda e-hökumətin tranzaksiyaları mərhələsində e-autentifikasiya və təhlükəsizliyi təmin etmək üçün başlanılmış

buludəsaslı rəqəmsal imza təşəbbüsü [6]-da müzakirə olunur. Məqalədə hazırda prototip mərhələsində olan e-imza xidməti proqram təminatı da təsvir edilir, təklif olunan həll e-hökumət və digər tətbiqlər üçün veb, mobil və buludəsaslı rəqəmsal imzalar üçün kompleks yanaşmanı nəzərə alır.

Koreya dünyada e-hökumətin inkişafını göstərən reytinq sıralamasında ilk yerlərdə olsa da, veb əlçatanlığı üzrə nisbətən aşağı nəticələr göstərirdi. Bunun səbəbləri [7]-də araşdırılır və rəqəmsal sertifikat üçün proqram təminatının yaradılması zamanı de-fakto texnologiya standartlarının (Microsoft ActiveX) seçimində buraxılmış səhvlər olduğu göstərilir. Hökümət, sertifikat mərkəzləri və sertifikat istehlakçıları Microsoft standartlarının istifadəsinin təsirlərini nəzərə almamışdı. Onun nəticələrinə Microsoft məhsullarının təxminən 99% bazar payı ilə inanılmaz inhisarı, Microsoft standartlarından xroniki asılılıq və zəif veb əlyetərlik problemləri daxildir. Məqalə Koreya e-hökumətinin diqqətlə qiymətləndirilməsinə çağırış edir.

İnkişaf etməkdə olan ölkələrdə milli e-imza infrastrukturunun qurulması və tətbiqi zamanı qarşıya çıxan çətinliklər və problemlər [8]-də analiz edilir. Bundan əlavə, məqalə Pakistan və bəzi Asiya ölkələri, əsasən Tayvan, Yaponiya və Sinqapurda AAİ-nin reallaşdırılması ilə bağlı texniki məsələlər, problemlər və öyrənilmiş dərsləri də işıqlandırır.

Avropa ölkələri geniş miqyasda mobil eID və e-imza həllərini tətbiq edirlər. Mövcud həllər müxtəlif texniki və təşkilati cəhətlərdən fərqlənirlər, bu, Avropa mobil eID və e-imza həlləri ekosistemini qeyri-bircins edir. Bu, belə həllərin hazırlanmasına və tətbiqinə cavabdeh olanların müvafiq tendensiyaları müəyyənləşdirmələrini, ən yaxşı təcrübələrə riayət etmələrini və düzgün qərar verələrini çətinləşdirir. Bu məsələlərin həllini asanlaşdırmaq üçün [9] hazırda Avropada mövcud olan mobil eID və e-imza həllərini araşdırır və qiymətləndirir, konkret tövsiyələr formalaşdırır.

Dünyada artan mobillik e-hökumət və eID həllərinə tələbləri artırır. Yalnız yerli vətəndaşlara e-hökumət xidmətləri göstərilməsi artıq qəbul edilə bilməz. E-hökumət və xüsusi halda, eID, qarşılıqlı uyarlığa yönəlməlidir. Avropa İttifaqı daxilində eID sistemlərinin qarşılıqlı uyarlığı xüsusilə açıq bir məsələdir. Üzv ölkələrdə mövcud eID sistemləri qarşılıqlı uyarlıq baxımından inkişaf etdirilməyib. [10]-də Avstriyanın eID yanaşması və xarici şəxslərin e-hökumət strukturuna necə qoşulduğu izah olunur.

E-imza infrastrukturunun təkmilləşdirilməsi üzrə aktual elmi-tədqiqat problemləri

Dünya ölkələrində, o cümlədən ölkəmizdə milli e-imza infrastrukturunun yaradılmasında və istifadəsində böyük praktiki təcrübə toplanmışdır [2, 3]. Hazırda bu infrastrukturların qabaqcıl elmi tədqiqatlar və texnologiyalar əsasında fasiləsiz təkmilləşdirilməsi işləri aparılır. Toplanmış praktiki təcrübədən və mövzu üzrə müvafiq elmi ədəbiyyatın analizindən çıxış edərək milli e-imza infrastrukturunun təkmilləşdirilməsi üzrə aktual elmi-tədqiqat problemlərini aşağıdakı şəkildə qruplaşdırmaq olar.

1. *Yeni texnologiyalar (mobil, bulud, Əşyaların İnterneti, NFC, blokçeyn və s.) konteksində yeni e-imza metodlarının işlənməsi.*

Mobil imza üçün müxtəlif metod və alqoritmlərin işlənməsi aktualdır, o cümlədən [11, 12]:

- Mobil qurğular üçün "yüngülçəkili" (*ing. lightweight*) kriptoqrafik alqoritmlərin işlənməsi [13, 14];
- Mobil qurğunun autentifikasiyası protokollarının işlənməsi (coğrafi koordinatlar və zaman məlumatları istifadə edilməklə) [15].

E-imza vasitələrinin yuxarıda qeyd olunan texnologiyalar üzrə reallaşdırılması sürətin artırılmasını və istifadə rahatlığını təmin etməyə imkan verir. Son nəsil ağıllı telefonlar mini kompüter funkisyalarını yerinə yetirir. Lakin buna baxmayaraq, mobil qurğular hələ də məhdud resursludur və uyğun kriptoqrafik alqoritmlərin nisbətən "yüngülçəkili" olması zəruridir [16]. Bu baxımdan seçilmiş müəyyən mobil qurğu üzrə optimal uzunluqlu asimmetrik açarların yaradılması məqsəduyğundur.

Mobil imza xidməti üçün təklif edilmiş həllərin iki çatışmayan tərəfi mövcuddur. Bir tərəfdən, bəzi həllər xidmətlərin bütün mobil şəbəkə operatorları tərəfindən dəstəklənməsini tələb edir, digərləri effektiv kommunikasiyalara əsaslanmırlar. [17]-də qeyd olunan problemləri həll edən SIPmsign adlı yeni mobil imza xidməti təqdim edilir. O, sessiya icraetmə protokoluna (*ing. Session Initiation Protocol, SİP*) əsaslanır və məlumat mübadiləsini daha etibarlı və səmərəli şəkildə təmin edir.

[18]-də Əşyaların İnterneti (*ing. Internet of Things, IoT*) üçün yüksək təhlükəsizliyə malik buludəsaslı rəqəmsal imza (SignOn) təqdim olunur. Əşyaların İnterneti sahəsindəki buludəsaslı imzanı ən yaxşı şəkildə reallaşdırmaq üçün məlumat mənbəyini autentifikasiya etmək üçün ECDSA (Elliptik əyrilər ilə rəqəmsal imza alqoritmi), bütün məlumat dəyişikliklərini aşkar etmək üçün heş funksiya (SHA-512) və təhlükəsizliyi daha çox təmin etmək üçün inkişaf etmiş şifrələmə standartı (*ing. Advanced Encryption Standard, AES*) istifadə olunur.

Yaxın təmas əlaqəsi (*ing. Near Field Communication, NFC*) texnologiyası mobil telefon vasitəsi ilə mobil tətbiqlərin işlənməsi və xidmətlərin göstərilməsi sahəsində yeni texnologiyalardan biridir. Təhlükəsiz yaxın təmas əlaqəsi tranzaksiyalarını təmin etmək üçün istifadə edilə bilən texnologiyalardan biri bulud hesablamalarıdır. [19]-da yaxın təmas əlaqəsi mobil ödəmələr konsepsiyasına əsaslanan protokol – NFC bulud cüzdan modelinin genişləndirilmiş bir versiyası təqdim edilir.

Kriptovalyutalar ilə meydana çıxan perspektivli texnologiyalardan biri də blokzəncirdir (BlockChain). Blokzəncir əsasında müxtəlif AAİ həllərin təklif edilməsinə cəhdlər edilir. Məsələn, domenlərarası təhlükəsiz marşrutlama protokolları üçün blokçeynəsaslı AAİ-dən istifadə edilir [20].

2. *Bulud platformasında mobil imza üçün protokolların işlənməsi.*

E-imza infrasturkturunun təqdim etdiyi imza vasitələri və bu vasitələrə qoyulan tələblərə əsasən açarların idarə olunması və əlyetərliyin təmin edilməsi vacib amildir. Əlyetərlik üçün iki/üç-faktorlu təhlükəsizlik mexanizmlərinin tətbiqində bir cox tərəf iştirak edir: mobil operatorlar, sertifikat xidmətləri mərkəzi, aparat təhlükəsizliyi modulu və imzalama sistemləri. Mobil imza vasitəsi, təbii ki, istifadəçinin işlərini daha sürətli edir və onun platformalardan asılılığını minimuma endirir. Bu zaman şəbəkə üzərində məlumat mübadiləsi açarların və imza sahibinin məlumatları xidmət proqramları (Software as a service, SaaS) üzərindən idarə edilə bilər. Bu isə e-imza sahibinin identikləşdirilməsini, məlumatların tamlığını və inkaredilməzliyini bulud üzərindən təmin edəcək [3].

Bulud texnologiyalarının təkcə mobil telefonlarla deyil, digər kompüter sistemləri ilə də daha yüksək mobillik imkanı yaratmaq potensialı vardır. [21]-də bu potensialın daha tam istifadə edilməsi üçün həlli vacib olan normativ hüquqi və texnoloji xarakterli əsas problemlər analiz edilir, inkişaf etmiş ölkələrin bu sahədə təcrübəsi araşdırılır və bir sıra elmi-praktiki tövsiyələr verilir.

Buludəsaslı rəqəmsal imzaya rəqəmsal imzanın kriptoqrafik əməliyyatlarını yerinə yetirən təhlükəsizlik infrastrukturuna etibarlı, rahat, tələb əsasında şəbəkə girişi üçün bir model kimi baxmaq olar. [22] buludəsaslı rəqəmsal imza modelində imzalayan ilə imza buludu arasında məlumat mübadiləsi üçün protokol təklif edir.

İstifadəçilər bulud hesablamaları proseslərində bəzi təhlükəsizlik problemləri ilə qarşılaşırlar. [23]-də ElGamal elliptik əyri kriptosisteminin hesablamaları üçün yeni bulud serveri təklif edilir. Təklif olunan protokollar istifadəçilərə müvafiq bulud xidmətləri təqdim etməklə yanaşı, bəzi aktiv hücumların və passiv hücumların, məsələn, modifikasiya hücumu, təxmini hesablama hücumu və s. qarşısını ala bilər.

Serverəsaslı imza həlləri kriptoqrafik açarları etibarlı şəkildə saxlaya bilən və istifadəçilər adından e-imza yarada bilən təhlükəsiz mərkəzi server komponentinə əsaslanır. Serverəsaslı imza həlləri və onların əsasında dayanan təhlükəsizlik konsepsiyalarının smartfonlar kimi mobil son istifadəçi cihazlarında istifadə edilməsi üçün mobil cihazların xüsusi xarakteristikalarına uyğun yeni serverəsaslı imza həlli təklif edilir [24]. Təklif olunan həll konkret prototipin reallaşdırılması ilə qiymətləndirilir.

Mövcud qiymətləndirmə metodları (məsələn, ümumi meyarlara görə mühafizə profilləri) serverəsaslı imza həllərinin qiymətləndirilməsi üçün yalnız qismən tətbiq oluna bilər. Bu problemi aradan qaldırmaq üçün serverəsaslı imza həlləri üçün yeni qiymətləndirmə modeli təklif edilir [25]. Təklif olunan model serverəsaslı imza həlləri üçün abstrakt arxitektura modelinə əsaslanır və buna görə istənilən reallaşdırmaya tətbiq edilə bilər.

Mövcud serverəsaslı eID və e-imza həlləri konkret istifadə variantına və ya tətbiq ssenarisinə uyğunlaşdırılır. Bu, həmin həllərin ixtiyari tətbiq ssenarilərində yerləşdirilməsini çətinləşdirir. Bu problemi aradan qaldırmaq üçün çevik serverəsaslı eID və elektron imza təklif edilir [26], onu asanlıqla istənilən tətbiq ssenarilərində yerləşdirmək olar və bu zaman yetərli təhlükəsizlik və istifadə rahatlığı təmin edilir.

Mövcud serverəsaslı imza yoxlama sxemlərində server yoxlanacaq məlumat-imza cütü haqqında bəzi məlumatları öyrənə bilər. [27]-də serverin köməyi ilə yoxlanan imzalar üçün server və imzanı yoxlayan tərəfin sözləşməsi hücumu çərçivəsində konfidensiallığın iki tərifi verilir. Sonra mövcud imza sxemləri əsasında konfidensiallığı təmin edən serverəsaslı imza yoxlama üçün iki konkret sxem təklif edilir, onların hər ikisinin təhlükəsizliyi sübut edilir.

Qanuni bazanın uzun illər mövcud olmasına baxmayaraq, təkmil e-imzaların bazar payı hələ də aşağıdır. Təkmil e-imzanın inkişaf etməsi üçün yeni dizaynlara son dərəcə ehtiyac duyulur. Bulud hesablamaları e-imzaların xidmət kimi təqdim olunması üçün yeni və çox vəd verən bir fürsət təqdim edir. [28] buludəsaslı e-imza xidmətinin reallaşdırlmasındakı çağırışları əhatə edir və e-imzanı yerinə yetirən buludu (İmza Buludunu) təsvir edir.

3. *Milli Sertifikat Xidmətləri Mərkəzinin işinin modelləşdirilməsi.*

Formalaşan və genişlənən e-xidmətlər və onların e-imza tələbləri sertifikat xidmətləri mərkəzlərinin üzərinə düşən iş yükünün həcmini kəskin artırır. Hazırda ölkəmizdə milli e-imza infrastrukturunun istifadəçilərinin sayı yüz minlərlədir, yaxın gələcəkdə bu sayın milyonlarla olacağı proqnozlaşdırılır. Buna görə mövcud e-imza infrastrukturunun miqyaslanması, təkmilləşdirilməsi problemləri meydana çıxır. İnfrastrukturun təkmilləşdirilməsi işlərini effektiv layihələndirmək və idarə etmək üçün sertifikat xidmətləri mərkəzlərinin işini müxtəlif situasiyalar və kriteriyalar baxımından modelləşdirmək, o cümlədən kütləvi xidmət sistemi kimi modelləşdirmək zəruridir.

Praktikada SXM-lərin rəqəmsal sertifikatların və CRL-lərin buraxılması prosesini daha yaxşı idarə etməsi üçün istehlakçıların alış və ləğv zamanı davranışlarını anlaması çox vacibdir. Bu problemi həll etmək üçün, istifadəçilərin rasional qərarlarını nəzərə alaraq SXM-lərin qiymət və ləğv strategiyaları [29]-da analitik modelləşdirilir. Rəqəmsal sertifikatın qiyməti, istifadəçinin İT sisteminin gözlənilən itkiləri ilə müəyyən edilməlidir və sertifikatın ləğv sayının, sertifikatın həyat tsikli ərzində zamanla azalması gözlənilir. Bu nəticəni VeriSign-dan alınan empirik verilənlər dəstəkləyir.

Sertifikatəsaslı AAİ autentifikasiyasını modelləşdirmək üçün formal yanaşma təqdim edilir [30]. Yanaşma bir-birini qarşılıqlı tamamlayan iki modeldən istifadə edir. Birincisi, autentifikasiya prosesində istifadə olunan əsas AAİ komponentlərinin vəziyyətini, onlar arasındakı əlaqələri və bu komponentlər üzərində "back-end" əməliyyatları modelləşdirmək üçün istifadə ediləcəkdir. İkincisi, davranışı və xüsusilə "front-end" qarşılıqlı əlaqələri və kommunikasiyaları modelləşdirmək üçün istifadə ediləcəkdir.

Hazırda sertifikat ləğvi yoxlamaları ya CRL serverləri, yaxud OCSP serverləri vasitəsilə həyata keçirilir. Təəssüf ki, bu metodların mövcud olmasına baxmayaraq, qabaqcıl kiberhücumlar veb brauzerləri ləğv edilmiş sertifikatın hələ də qüvvədə olduğuna inanmağa vadar edə bilər. Tez-tez yenilənən, birdəfəlik sertifikatlar və vaxt möhürlü sertifikatlar bu cür kiberhücumların tezliyini və təsirini azalda bilsə də, SXM və OCSP serverlərini çox yükləyirlər, serverlər müntəzəm olaraq vaxt nişanı qoymalıdırlar və verilmiş hər bir sertifikat üçün bütün cavabları imzalamalıdırlar, nəticədə xərclər çox yüksək olur. Bu yükü azaltmaq və təsvir olunan kiberhücumlara bir həll təmin etmək üçün [31]-də sıxılmış sertifikat statusu protokolu (*ing. Compressed Certificate Status*

Protocol, CCSP) təklif edilir, onun ilkin reallaşdırılması və qiymətləndirilməsi təqdim edilir: imzalanmış kolleksiyalar adlanan konsepsiya əsasında sertifikatların vəziyyəti haqqında vaxtında məlumat vermək üçün yeni bir yanaşmadır.

Əvvəllər verilmiş sertifikatları ləğv etmək imkanı istənilən AAİ təhlükəsizliyi üçün kritik vacibdir. Ümumi SSL ekosistemi yaxşı öyrənilsə də, sertifikatın ləğvinin tezliyi və müştərilərin (brauzerlər kimi) sertifikatların ləğv edilib-edilmədiyini yoxladığı hallar hələ də yaxşı öyrənilməyib. [32] İnternet AAİ-də sertifikatların ləğvinə yaxından nəzər salır və nəticələr sertifikatların effektiv şəkildə ləğvi imkanının çox aşağı olduğunu göstərir.

Hazırda nəqliyyat səviyyəsinin təhülkəsizliyi (*ing. Transport-Layer Security, TLS*) veb və veb-əsaslı tətbiqlər üçün İnternet təhlükəsizliyinin əsas təməlidir. TLS autentifikasiya üçün X.509 AAİ-dən asılıdır. AAİ-nin vacib hissəsi, məsələn, açar nüfuzdan düşdükdən sonra sertifikatları sürətli ləğv etmək imkanıdır. Hazırda OCSP ləğv məlumatlarını tez bir zamanda yaymağın ən məşhur üsuludur. Lakin OCSP gecikməsi və gizliliklə əlaqəli narahatlıqlar onun istifadəsi ilə bağlı suallar doğurur. Böyük bir tədqiqat universitetinin İnternet əlaqəsindəki canlı trafikin passiv şəbəkə monitorinqindən istifadə edərək OCSP araşdırılır və aktiv skanlamalardan istifadə edərək nəticələri yoxlanır [33].

Gözlənilən bir çox IoT tətbiqində təhlükəsizlik çox vacibdir. Lakin IoT sistemlərində mövcud təhlükəsizlik metodlarının tətbiqi IoT cihazlarının özünəməxsus heterogenliyi və nəhəng sayda olması səbəbindən sadə deyil. AAİ təhlükəsizliyin kritik sütun blokudur, lakin AAİ-də tək bir imtina halı mərkəzləşdirilmiş təbiəti səbəbindən bütün IoT sistemlərinə təsir edə bilər. [34]-də IoT üçün IoT-PKI adlanan mərkəzləşdirilməmiş bir AAİ təklif edilir, burada SXM-lər əvəzinə bir blokçeyn şəbəkəsində paylanmış qovşaqlardan istifadə edilir və beləliklə, miqyaslanma təmin edilir. IoT-PKI cihaz istehsalçılarının açar sızdırmalarından qoruyur, çünki cihaz sahiblərinə öz IoT cihazlarının sertifikatlarını idarə etməyə imkan verir.

AAİ mürəkkəb bir sistem olaraq, sistemin bütün hissələrində tələblərin identifikasiyası və müəyyən edilməsi prosesində xüsusi diqqət tələb edir. Səmərəli şəkildə müəyyən edilmiş tələblər uğurlu AAİ yaradılması və tətbiqi üçün əsasdır. [35] AAİ tələblərinin yeni klassifikasiya sxemini təklif edir, sxem sistemin yaşam dövrünün bütün mərhələlərində tələblərin effektiv şəkildə müəyyənləşdirilməsini təmin edir.

Açıq açar istifadə edən sistem real zamanda sertifikatın həqiqiliyinin yoxlanılması üçün ixtisaslaşdırılmış yoxlama tərəfi ilə tranzaksiya yerinə yetirir. Tranzaksiyanın sonunda yoxlama tərəfi sertifikatın həqiqilik vəziyyəti barədə cavab qaytarır. [36]-da açıq açar sertifikatını yoxlama xidməti praktik baxımdan analiz edilir, etibar edən tərəflərə sertifikat yoxlama xidməti təqdim etmək üçün məlumat yoxlama və sertifikatlaşdırma serveri (*ing. Data Validation and Certification Server, DVCS*) protokollarından istifadə edən bir sistemin tətbiqi təsvir edilir.

4. *AAİ şəbəkəsində etimadın (inamın) qiymətləndirilməsi modelləri.*

E-imza infrastrukturunu müxtəlif topologiyalar üzrə qurmaq olar. Çox zaman e-dövlət üçün mərkəzləşdirilmiş modellər tətbiq edilir və hazırda qurulmuş milli e-imza infrastrukturu iyerarxik model üzrə fəaliyyət göstərir [37]. Bu isə öz növbəsində bütün fəaliyyətdə olan sertifikat xidmətləri mərkəzlərinin struktur zəncir üzrə kök mərkəzə tabe olmasını təmin edir. Bu fiziki model özündə bir çox üstünlükləri ehtiva edir.

Praktikada bir çox halda istifadəçilər arasında məlumat mübadiləsinin təmin edilməsi mərkəzləşdirilməmiş sistem üzərindən icra edilir və PGP həlləri formalaşdırılır. Bir çox onlayn satış sistemlərində, e-ticarətdə P2P sistemlərindən istifadə edilir. Əsas hədəf təhlükəsiz mübadilə, zaman və sürət baxımından yüksək məhsuldarlığın əldə edilməsidir. Mərkəzləşdirilməyən model üç qrup – Web-of-trust, statik və hibrid yanaşmalar üzrə etimad asılılığını saxlayır [38].

[39] AAİ-lərdə istifadə olunan etimad mexanizmlərinin dərindən analiz edilməsinə çalışır və əsas AAİ spesifikasiya sənədlərində etimadın tam olaraq nə demək olduğunu dəqiq müəyyənləşdirmədiyini və real praktikada qeyri-aşkar etimad fərziyyələrinin olduğunu göstərir.

Bu qeyri-aşkar etimad fərziyyələri müxtəlif tərəflərin, xüsusən güvənən tərəflərin sertifikatın və etimadın mənasını fərqli anlamalarına və etimaddan sui-istifadəyə səbəb ola bilər.

Klassik etimad modelləri domenlərarası qarşılıqlı əlaqəni dəstəkləmir və mövcud domenlərarası etimad modelləri tam paylanmış deyillər. [40] məlum sertifikatlı reputasiya (*ing. Certified Reputation CR*) modelini yaxşılaşdırır və mobil paylanmış mühit üçün Domenlərarası Asan Etimad (*ing. Lightweight Cross-domain Trust, LCT*) modeli təklif edir. Etimad sertifikatlarında etimad reytinqləri fərqli üstünlük çəkiləri ilə etimadın müxtəlif aspektlərini ehtiva edir, bu sertifikatlar qəyyumlar tərəfindən toplanır və təmin edilir.

Hazırda AAİ-də istifadə edilən etimad modeli ilə bağlı bir sıra təhlükəsizlik insidentləri baş vermişdir. Əsas tənqidlərdən biri, arxitekturanın SXM-lərin etibarlı olması barədə qeyri-aşkar fərziyyəsidir. [41] həmin fərziyyəni bir SXM-nin fərdi etibarlılığının obyektiv meyarlara əsaslanan diferensial qiymətləndirilməsi ilə kompensasiya etmək üçün vahid bir metrika təklif edir. Metrika mövcud siyasətlərdən, texniki təlimatlardan və tədqiqatlardan əldə edilmiş çoxsaylı texniki və qeyri-texniki faktorlardan istifadə edir. O, müstəqil submetrikalardan ibarətdir, bu, mövcud kriteriyaların sadə bir şəkildə genişləndirilməsinə imkan verir.

SSL/TLS, İnternet üzərindən etibarlı rabitə təmin etmək üçün de-fakto protokoldur. Autentifikasiya və təhlükəsiz açar mübadiləsi üçün veb-PKI modelinə əsaslanır. Son zamanlarda müşahidə edilən veb-PKI insidentlərinin sayı artmışdır. Bu insidentlər domen sahiblərinin razılığı olmadan SXM-lər tərəfindən verilən saxta sertifikat risklərini üzə çıxarmışdır. Bu problemi həll etmək üçün [42]-də serverlərin öz sertifikatlarına İnternet üzərindən baxmasını təmin edən, sertifikat əvəzləməsi hücumunu aşkarlaya bilən praktik bir mexanizm təklif edilir. Bu mexanizmin köməyi ilə sertifikat əvəzləməsi hücumunun mənbəyini də aşkar etmək olar.

AAİ təşkilində əsas funksiya – etibarlı üçüncü tərəf kimi etimad funksiyası və verilən rəqəmsal sertifikatlara nəzarətdir. Etimad səviyyəsi [43]-də Omar və Lindsayın təklif etdiyi etimadın 27 meyar səviyyəsi üzrə qiymətləndirilir.

Etimad konsepsiyası təhlükəsiz müştəri-server kommunikasiyası üçün autentifikasiya mexanizminin formalaşdırılmasında mərkəzi yer tutur. Son zamanlar müxtəlif etimad anlayışlarına əsaslanan fərqli etimad modelləri təklif edilmişdir. [44]-də etimadın mənası AAİ kontekstində sertifikatların autentifikasiyası üçün araşdırılır. Ayrıca, müxtəlif yayılmış etimad modellərində etimadın ifadə edilməsi analiz olunur.

5. *E-imza infrastrukturunun təhlükəsizliyinin təmin edilməsi metodları.*

E-imza infrastrukturu ayrı-ayrı əsas altsistemlərdən və bəzi əlavə avtonom komponentlərdən ibarətdir. Ümumi sistemdə təhlükəsizliyin təmin edilməsi bir neçə səviyyədə icra edilir. Buraya aparat təhlükəsizliyi, fiziki təhlükəsizlik və proqram təhlükəsizliyi daxildir.

Sertifikat xidmətləri mərkəzi üçüncü avtonom tərəflərlə müxtəlif münasibətlər qurur, buna görə zəruri təhlükəsizlik tələbləri hər zaman qorunmalıdır. Bu tələblərə istifadədə olan avdanlıqların və servislərin bir-biri ilə məlumat mübadiləsində açar mübadiləsinin təşkili və bu açarların qorunması da daxildir.

Hazırda e-imza informasiya təhlükəsizliyi sistemlərinə birbaşa və dolayısı ilə təhlükəli şəkildə artan bir sıra hücumların şahidi oluruq. Bu hücumların çox halda uğurlu olması onlara qarşı yeni innovativ strategiyaların formlaşdırılmasını və yeni metodların işlənməsini zəruri edir [45].

X.509 sertifikatları e-xidmətlər və tətbiqlərdə reallaşdırılan bir çox təhlükəsizlik mexanizminin əsasını təşkil edir. Lakin sertifikatların yoxlanması prosesində bir sıra boşluqlar vardır (məsələn, əlçatmayan və ya yenilənməmiş verilənlərin olması ehtimalı). Belə boşluqların gətirdiyi təhdidlər üçün [46]-da riskin kəmiyyət qiymətləndirilməsinə ehtimal yanaşması və qeyri-müəyyənlik olduqda, etimadın idarə edilməsi mexanizmi təklif edilir.

Hazırda TLS sertifikatlarının böyük əksəriyyəti bir neçə SXM tərəfindən verilir. Bu vacib SXM-lərin sertifikatlarının ləğv olunması xeyli dərəcədə problemlidir, çünki onların ləğv edilməsi külli miqdarda əlaqədar ziyana səbəb ola bilər. Bu problemi həll etmək üçün mövcud ləğv sistemini təkmilləşdirən PKI Safety Net (PKISN) adlandırılan yeni yanaşma təklif edilir [47],

burada sertifikatları saxlamaq və ləğv etmək üçün hər kəsə açıq olan jurnallardan istifadə edilir (sertifikatların şəffaflığı naminə).

Təhlükələr arasında təhlükəsiz sertifikatlarla əlaqəli gizli açarların oğurlanması və bunlardan zərərli proqramları imzalamaq və ya proqram təminatı yaratmayan və bu səbəbdən kod imzalama sertifikatları olmayan qanuni şirkətləri təqlid etmək üçün istifadə daxildir. Stuxnet və Flame kimi qabaqcıl təhdidlərdən məlum olan bu növ sui-istifadə daha geniş zərərli proqram mühitində sistematik qiymətləndirilməyib. Xüsusilə, kod imzalayan AAİ istismarının üsulları, effektivlik pəncərəsi və təhlükəsizlik təsirləri yaxşı başa düşülməyib. Kod imzalayan AAİ-də üç növ boşluğu müəyyən edən bir təhdid modeli təklif edilir [48]. Kod imzası tədbirlərinə xas olan çətinliklər qanunsuz ola biləcək kod imzalama sertifikatlarının toplanması zamanı prioritetlərin verilməsi metodları tətbiq edilməklə həll edilir.

AAİ-nin iyerarxik modelində mərkəzləşdirilmiş arxitektura səbəbindən vahid imtina nöqtəsi problemi var və bu gözlənilməz təhdidlərlə əlaqədardır. [49]-da Cecoin adlı paylanmış sertifikat sxemi təqdim edilir, o, məşhur Bitcoin-ə əsaslanır və onun geridönməzlik, saxtalaşdırılmazlıq və ictimai yoxlama imkanından istifadə edir. Cecoin-də sertifikatlara valyuta kimi baxmaq və blokçeyndə qeydə almaq olar ki, bu da vahid imtina nöqtəsi problemini aradan qaldırır.

[50]-də AAİ-əsaslı mobil ticarət arxitekturasına müxtəlif növ hücumlar layihələndirilir və modelləşdirilir. Əlavə olaraq, *m*-ticarətdə (mobil rabitə vasitələrinin imkanlarından istifadə edilərək alqı-satqı) bu hücumlar üçün bir boşluq da müzakirə edilir. Buna görə məhsuldarlığı analiz etmək üçün təklif olunan metodu virtual mühitdə reallaşdıran tətbiq hazırlanmış və sınaqdan keçirilmişdir.

AAİ onlayn əməliyyatların təhlükəsizliyini təmin etmək, xüsusilə də autentifikasiya üçün *m*-ticarət platforması rolunu oynayır. [51]-də AAİ-əsaslı sorğu-cavab autentifikasiya metodu və bununla əlaqəli hücumlar izah edilir. Sorğu-cavab yanaşması, vaxt gecikməsi üsulu ilə birləşdirilərək autentifikasiya prosesinin etibarlılığını artıracaq yeni bir autentifikasiya protokolu yaradılır.

[52] X.509 sertifikatları ilə əlaqəli riski xüsusi meyarlar və etmad xarakteristikalarından istifadə edərək qiymətləndirən bir strukturlaşdırılmış çərçivə təklif edir. Sertifikatla əlaqəli riski qiymətləndirmək üçün sertifikat riskini üç səviyyəyə: yüksək risk, orta risk və aşağı riskə ayıran klassifikasiya metodu istifadə edilir. İstifadəçi sertifikatını daxil edir və sistem bu sertifikatla əlaqəli riski hesablayır, yüksək və ya orta risk sertifikatıdırsa, hansı parametrə görə risk daşıdığını göstərir.

Malayziya dünyada 1998-ci ildə biometrik pasport (e-Passport) verən ilk ölkə olmuşdur. Son illərdə e-Passportların 1-ci və 2-ci nəsillərində bir sıra boşluqlar aşkarlanmışdır, bu boşluqlar ciddi təhlükəsizlik problemlərinə səbəb ola bilər. [53] göstərir ki, Malayziya e-Passportu üçün riskləri klonlaşdırma, vasitəçilik, saxtalaşdırma və serverlə əlaqəli məsələlərdir. Əlaqə qurmanın şifrə ilə təsdiqlənməsi (*ing. Password Authenticated Connection Establishment, PACE*) protokolunu tətbiq etmək və Beynəlxalq Mülki Aviasiya Təşkilatı (*ing. International Civil Aviation Organization, ICAO*) standartlarına riayət etmək tövsiyə olunur.

Nəticə

Milli e-imza infrastrukturu e-dövlət üçün çox vacib bir platforma kimi çıxış edir. E-imza həlləri e-xidmətlər üzrə əsas autentifikasiya üsuludur və bütün onlayn əməliyyatların hüquqi statusu təkmil e-imza vasitəsilə təmin edilir. Ümumilikdə, e-imza infrastukturu güclü identifikasiya, dinamik genişlənmə və mobillik təklif etməklə e-dövlətin informasiya təhlükəsizliyinin təmin edilməsində əsas sütun rolunu oynayır.

Bu funksionallığı etibarlı təmin etmək üçün getdikcə mürəkkəbləşən informasiya təhlükəsizliyi və yeni texnologiyalar mühitində e-imza infrastrukturunun e-dövlət sistemlərinə səmərəli inteqrasiyası üçün multiplatformanın qurulması, sistemə düşən yükün düzgün paylanması və təhlükəsiz məlumat mübadiləsini təmin etmək üçün yuxarıda göstərilən prioritet istiqamətlər üzrə yeni metod, alqoritm və protokolların işlənməsi aktualdır.

Ədəbiyyat

1. Albarqi A., Ethar A., Fatimah Al G., Somaya A., Kar J. Public key infrastructure: A survey // Journal of Information Security, 2015, vol.6, pp.31–37.
2. Kubicek H., Noack T. Different countries – different paths extended comparison of the introduction of eIDs in eight European countries // Identity in the Information Society, 2010, vol.3, no.1, pp.235–245.
3. Əliquliyev R.M., İmamverdiyev Y.N. Kriptoqrafiyanın əsasları. Bakı: İnformasiya Texnologiyaları, 2006, 698 s.
4. Patsos D., Ciechanowicz C., Piper F. The status of national PKIs – A European overview // Information Security Technical Report, 2010, vol.15, Issue 1, pp.13–20.
5. Hoff J.V., Hoff F.V. The Danish eID case: Twenty years of delay // Identity in the Information Society, 2010, vol.3, no.1, pp.155–174.
6. Jain V., Kumar R., Saquib Z. An approach towards digital signatures for e-Governance in India / Proceedings of the 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia (EGOSE), 2015, pp.82–88.
7. Park H.M. The web accessibility crisis of the Korea's electronic government: Fatal consequences of the digital signature law and public key certificate / 45th Hawaii International Conference on System Science (HICSS), 2012, pp.2319–2328.
8. Malik N.M., Khalil T., Khalid S., Malik F.M. PKI implementation issues: A comparative Study of Pakistan with some Asian Countries // International Journal on Computer Science and Engineering, 2009, vol.1(2), pp.105–110.
9. Zefferer T., Teufl P. Leveraging the adoption of mobile eID and e-Signature solutions in Europe / International Conference on Electronic Government and the Information Systems Perspective, 2015, pp.86–100.
10. Rössler T. Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government // Computer Law & Security Review, 2008, vol.24, no.5, pp.447–453.
11. Ansper A., Buldas A., Freudenthal M., Willemson J. High-performance qualified digital signatures for X-road / Nordic Conference on Secure IT Systems, 2013, pp.123–138.
12. Husni E. Digital signing using national identity as a mobile ID / International Seminar on Intelligent Technology and its Applications, 2016, pp.261–264.
13. Liu D.Y.W., Xue G.Z., Xie Y., Luo X.P., Au M.H. Performance of digital signature schemes on mobile devices // Mobile security and privacy. Advances, Challenges and future research directions, 2017, vol.12, pp.247–256.
14. Xuan Z., Du Z., & Chen R. Comparison research on digital signature algorithms in mobile web services / International Conference on Management and Service Science, 2009, pp.1–4.
15. Gina G.G., Raul A. F.E., Horacio T.R., Alejandro V.A., Gualberto A.T. A lightweight digital signature cryptographic protocol for authentication and integrity based on location // Journal of Applied Sciences, Engineering and Technology, 2016, vol.12(5), pp.550–555.
16. Ahamad S.S., Udgata S.K., & Nair M. A secure lightweight and scalable mobile payment framework / Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), 2013, pp.545–553.
17. Ruiz-Martínez A., Inmaculada Marín-López, C., Sánchez-Martínez D., & Castell Egea I. SIPmsign: a lightweight mobile signature service based on the Session Initiation Protocol // Software: Practice and Experience, 2014, vol.44(5), pp.511–535.
18. El-Rahman S.A., Aldawsari D., Aldosari M., Alrashed O., & Alsubaie G. A secure cloud based digital signature application for IoT // International Journal of E-Services and Mobile Applications (IJESMA), 2018, vol.10(3), pp.42–60.
19. Pourghomi P., Saeed M.Q. A secure cloud-based NFC mobile payment protocol // International Journal of Advanced Computer Science and Applications, 2014, vol.5, no.10, pp.24–31.

20. Gómez-Arevalillo A.R., Papadimitratos P. Blockchain-based Public Key Infrastructure for inter-domain secure routing / International Workshop on Open Problems in Network Security, 2017, pp.20–38.
21. İmamverdiyev Y. E-dövlət üçün bulud texnologiyaları əsasında mobil elektron imza / İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransının əsərləri, 2015, s.138–141.
22. Kinastowski W. Digital signature as a cloud-based Service / Cloud Computing: The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization, 2013, pp.68–72.
23. Lee N.Y., Chen Z.L. Cloud server aided computation for ElGamal elliptic curve cryptosystem / Computer Software and Applications Conference Workshops, 2013, pp.11–15.
24. Zefferer T. A server-based signature solution for mobile devices / Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia, 2014, pp.175–184.
25. Zefferer T., & Zwattendorfer B. An implementation-independent evaluation model for server-based signature solutions / International Conference on Web Information Systems and Technologies, 2014, pp.302–309.
26. Rath C., Roth S., Schallar M., Zefferer T. Design and application of a secure and flexible server-based mobile eID and e-signature solution // International Journal on Advances in Security, 2014, vol.7, no.3-4, pp.50–61.
27. Xu L., Li J., Tang S. & Baek J. Server-aided verification signature with privacy for mobile computing // Mobile Information Systems, Article ID 626415, 2015, pp.1–11.
28. Kinastowski W. Signing cloud: Towards qualified electronic signature service in cloud / IEEE 5th International Conference on Cloud Computing Technology and Science, 2013, vol. 2, pp.224–227.
29. Zhang J., Hu N., Raja M.K. Digital certificate management: Optimal pricing and CRL releasing strategies // Decision Support Systems, 2014, vol.58, pp.74–78.
30. Haidar A.H., Abdullah A.E. Formal modelling of PKI based authentication // Electronic Notes in Theoretical Computer Science, 2009, vol.235, pp.55–70.
31. Chariton A.A., Degkleri E., Papadopoulos P., Ilia P., Markatos E.P. CCSP: A compressed certificate status protocol / IEEE Conference on Computer Communications, 2017, pp.1–9.
32. Liu Y., Tome W., Zhang L., Choffnes D., Levin D., Maggs B., Wilson C. An end-to-end measurement of certificate revocation in the web's PKI / Proceedings of the 2015 Internet Measurement Conference, 2015, pp.183–196.
33. Zhu L., Amann J. & Heidemann J. Measuring the latency and pervasiveness of TLS certificate revocation / International Conference on Passive and Active Network Measurement, 2016, pp.16–29.
34. Won J., Singla A., Bertino E. & Bollella G. Decentralized public key infrastructure for Internet-of-Things / IEEE Military Communications Conference, 2018, pp.907–913.
35. Prodanović R. & Vulić I. Classification as an approach to public key infrastructure requirements analysis // IET Software, 2019, vol.13(6), pp.518–527.
36. Berbecaru D. & Lioy A. Towards simplifying PKI implementation: Client-server based validation of public key certificates. arXiv preprint arXiv:1910.06641, 2019.
37. İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyinə etimadın qiymətləndirilməsi modeli // İnformasiya texnologiyaları problemləri, 2015, №1, s.25–32.
38. Имамвердиев Я.Н., Гаджирагимова М.Ш. Архитектура инфраструктуры доверия электронным документам в среде электронного государства // Телекоммуникации, 2011, №11, с.18–26.
39. Huang J., Nicol D.M. An anatomy of trust in public key infrastructure // International Journal of Critical Infrastructures, 2017, vol.13(2-3), pp.238–258.

40. Liu Z., Ma J., Jiang Z. & Miao Y. LCT: A lightweight cross-domain trust model for the mobile distributed environment // KSII Transactions on Internet and Information Systems (TIIS), 2016, vol.10, no.2, pp.914–934.
41. Heinl M.P., Giehl A., Wiedermann N., Plaga S. & Kargl F. MERCAT: A metric for the evaluation and reconsideration of certificate authority trustworthiness / Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop, 2019, pp.1–15.
42. Yüce E., & Selçuk A.A. Server notaries: a complementary approach to the web PKI trust model // IET Information Security, vol.12(5), pp.455–461.
43. Ferdinand A.I. & Gaol F.L. Evaluation level of trust on implementing public key infrastructure in Procurement System Certificate Authority which is held by National Crypto Agency // Advanced Science Letters, 2018, vol.24(7), pp.5255–5258.
44. Rahoof P.P. & Nair L.R. Incorporating trust in public key infrastructure certificates // Advances in Computational Sciences and Technology, 2017, vol.10(5), pp.671–686.
45. Mantas G., Lymberopoulos D., Komninos N. PKI security in large-scale healthcare networks // Journal of Medical Systems, 2012, vol.36(3), pp.1107–1116.
46. Hinarejos M.F., Almenárez F., Arias-Cabarcos P., Ferrer-Gomila J.L., Marín A. RiskLaine: A probabilistic approach for assessing risk in certificate-based security // IEEE Transactions on Information Forensics and Security, 2018, vol.13(8), pp.1975–1988.
47. Szalachowski P., Chuat L. Perrig A. PKI safety net (PKISN): Addressing the too-big-to-be-revoked problem of the TLS ecosystem / IEEE European Symposium on Security and Privacy (EuroS&P), 2016, pp.407–422.
48. Kim D., Kwon B.J., Dumitraş T. Certified malware: Measuring breaches of trust in the Windows code-signing PKI / Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp.1435–1448.
49. Qin B., Huang J., Wang Q., Luo X., Liang B. & Shi W. Cecoin: A decentralized PKI mitigating MitM attacks // Future Generation Computer Systems, 2020, vol.107, pp.805–815.
50. Vishwakarma S., Samant P.K. & Sharma A. Attacks in a PKI-based architecture for m-commerce // IEEE International Conference on Computational Intelligence & Communication Technology, 2015, pp.52–56.
51. Samant P. K., Saini P. & Challa R.K. A combined request/response and time delay technique to detect attacks in a PKI-based architecture for m-commerce / Proc. of the 3rd IEEE International Advance Computing Conference (IACC), 2013, pp.1357–1361.
52. Hawanna V., Kulkarni V.Y., Rane R.A., Mestri P., Panchal S. Risk rating system of X.509 certificates // Procedia Computer Science, 2016, vol.89, pp.152–161.
53. Suhaimi A.I.H., Noordin N., & Yakub M.F. Assessment of Malaysian e-passport PKI based on ISO 27000 series international standards // Journal of Physics: Conference Series, 2020, vol.1551, no.1, p.012003.

УДК 004.056

Имамвердиев Ядигар Н.[1], Аббасов Г.Г.[2]
[1]Институт Информационных Технологий НАНА, Баку, Азербайджан
[2]МТСВТ Национальный Центр Сертификационных Услуг, Баку, Азербайджан
[1]yadigar@iit.science.az, [2]hebib@rabita.az

Национальная инфраструктура электронной подписи: актуальные проблемы научных исследований

Путем изучения существующих технических и логических возможностей национальной инфраструктуры электронной подписи, связанной с электронными подписями, было выявлено оптимальное управление нагрузкой на систему и исследование проблем. Поскольку электронная подпись выполняет роль удостоверения личности для идентификации граждан в электронной среде, обеспечивает доступ к информативным и интерактивным электронным услугам, созданным в решениях электронного правительства, и безопасное использование этих услуг осуществляется посредством электронной подписи. В статье анализируются проблемы совершенствования национальной инфраструктуры электронной подписи с точки зрения новых технологических вызовов, повышения мобильности, обеспечения высокой производительности в устройствах с ограниченными ресурсами, высоких требований безопасности для широкого использования электронных услуг и выявления актуальных научных и практических проблем. На основе изучения международного опыта решения выявленных проблем проанализированы направления исследований для моделирования работы центров в области оценки безопасности и доверительной цепи компонентов национальной инфраструктуры. В статье определяется эффективность национальной инфраструктуры электронной подписи как компонента безопасности в зонах обслуживания центров путем выявления собственных проблем безопасности.

Ключевые слова: *электронная подпись, инфраструктура открытых ключей, национальная инфраструктура электронной подписи, доверие, интернет вещей, сертификат.*

Yadigar N. Imamverdiyev[1], Hebib H. Abbasov[2]
[1]Institute of Information Technology of ANAS, Baku, Azerbaijan
[2]National Certification Services Center of MTCHT, Baku, Azerbaijan
[1]yadigar@iit.science.az, [2]hebib@rabita.az2

National e-signature infrastructure: current problems of scientific research

By examining the existing technical and logical capabilities of the national e-signature infrastructure related to electronic signatures (e-signatures), the optimal management of the load on the system and the investigation of problems are identified. As e-signature provides the role of identity card for the identification of citizens in the electronic environment, ensuring access to informative and interactive e-services generated in e-government solutions and safe use of these services is carried out through e-signature. The article analyzes the problems of improving the national e-signature infrastructure in terms of new technological challenges, increasing mobility, ensuring high productivity in devices with limited resources, high security requirements for widespread use of e-services and identifies current scientific and practical issues. The research areas for modeling the work of the centers in the field of security and confidence chain assessment of the components of the national infrastructure are analyzed by studying the international experience in solving the identified problems. The article identifies the effectiveness of the national e-signature infrastructure as a security component in the service areas of the centers by identifying its own security issues.

Keywords: *e-signature, public key infrastructure, national e-signature infrastructure, trust, Internet of Things, certificate*.