E-dövlət üçün bulud texnologiyaları əsasında mobil elektron imza

Yadigar İmamverdiyev

AMEA İnformasiya Texnologiyaları İnstitutu

yadigar@lan.ab.az

***Xülasə*— Elektron imza e-dövlətdə elektron şəxsiyyət vəsiqəsi rolunu oynayır, vətəndaşların elektron xidmətlərdən təhlükəsiz istifadəsini və mobilliyini təmin etmək üçün yeni nəsil fiziki şəxsiyyət vəsiqələrinə də elektron imzaları yaratmaq və yoxlamaq üçün zəruri məlumatların daxil edilməsi nəzərdə tutulur. Bulud texnologiyalarının təkcə mobil telefonlarla deyil, digər kompüter sistemləri ilə də daha yüksək mobillik imkanı yaratmaq potensialı vardır. Məqalədə bu potensialın daha geniş və tam istifadə edilməsi üçün həlli vacib normativ hüquqi və texnoloji xarakterli əsas problemlər analiz edilir, inkişaf etmiş ölkələrin bu sahədə təcrübəsi araşdırılır və bir sıra elmi-praktiki tövsiyələr verilir.**

Açar sözlər*— *elektron imza; mobil imza; bulud texnologiyası; etimad infrastrukturu; sertifikat xidməti mərkəzi.

I. GİRİŞ

"Elektron imza və elektron sənəd haqqında" Azərbaycan Respublikasının Qanunu [1] qəbul edildikdən sonra elektron imza infrastrukturunun yaradılması və əməli fəaliyyəti istiqamətində Rabitə və Yüksək Texnologiyalar Nazirliyi, digər mərkəzi icra orqanları və əlaqədar qurumlar tərəfindən bir sıra diqqətəlayiq layihələr həyata keçirilmişdir [1]. Milli Sertifikat Xidmətləri Mərkəzi (Kök Sertifikat Mərkəzi və onun tabeliyində Hakimiyyət Orqanları Mərkəzi, Elektron Hökumət Mərkəzi və mobil-İD Mərkəzi) yaradılmış, onun tam funksional fəaliyyəti üçün zəruri aparat-proqram infrastrukturu qurulmuşdur. Eyni zamanda, mövcud elektron xidmətlərin elektron imza ilə inteqrasiyası həyata keçirilir ki, bu da vətəndaşlara mümkün qədər çox xidmətdən yararlanmaq imkanı yaradır. Daha bir vacib tədbir yaxın vaxtlarda tətbiq edilməsi nəzərdə tutulan yeni nəsil şəxsiyyət vəsiqələrinə vəsiqə sahibinin gücləndirilmiş elektron imzası ilə əlaqədar sertifikatların, elektron imza yaratma və elektron imzanı yoxlama məlumatlarının daxil edilməsidir [2].

2011-ci ilin sentyabr ayından rəsmi olaraq fəaliyyətə başlayan Mərkəz rayon poçt şöbələrində yaradılmış Qeydiyyat mərkəzləri vasitəsilə adi vətəndaşlara, sahibkarlıq fəaliyyəti ilə məşğul olan hüquqi və fiziki şəxslərə, həmçinin dövlət qulluqçularına xidmət göstərir. Mərkəz tərəfindən 2015-ci ilin 1-ci rübü də daxil olmaqla, ötən dövr ərzində 32 mindən artıq "Elektron İmza" sertifikatı verilmişdir. Qeyd edək ki, elektron imza sertifikatı smart kartda saxlanılır və elektron imzanın istifadəsi üçün kompüterə qoşulan kart oxuyucusu və xüsusi proqram təminatı istifadə edilmir.

Elektron imzanın reallaşdırılmasının geniş yayılan digər üsulu mobil telefonlardan istifadə edilməsidir. Nəticəsi mobil imza (m-imza) adlanan bu yanaşmanın yuxarıda qeyd edilən yanaşmadan bir çox üstünlükləri vardır [3]. Smartr kart, kart oxuyucusu, kompüter tələb edilmir, hər hansı proqram təminatına da ehtiyac yoxdur. İnternetə çıxışı olan mobil telefonla istənilən yerdən və istənilən an sənədləri rahatlıqla imzalamaq mümkündür. Mobil telefonların elektron imza üçün istifadə edilməsində bəzi problemlərin olmasına baxmayaraq (məsələn, ekranın ölçüləri, kommunikasiya xərcləri, məhdud hesablama resursları və s.), rahat olması və təmin etdiyi mobillik onların potensialından istifadə etməyə imkan verir.

Azərbaycan mobil telefonların yayılma faizinə görə dünyada qabaqcıl mövqelərdədir, ölkəmiz mobil İnternetin yayılma faizi də kifayət qədər yüksəkdir. Bunların nəticəsi olaraq, mobil imzaların istifadəsi də genişlənir. Vergilər Nazirliyinin Asan İmza Sertifikat Xidmətləri Mərkəzi tərəfindən 2015-ci ilin 1-ci rübü də daxil olmaqla, ötən dövr ərzində verilmiş "Asan İmza" sertifikatlarının sayının 155 mindən çox olması da bunu sübut edir [4].

Mobil telefonlar elektron imzanın mobilliyini təmin etməyin yeganə üsulu deyil. Son dövrlər gələcəyin ən perspektivli strateji texnologiyalarından biri kimi dəyərləndirilən bulud texnologiyalarından istifadə etməklə informasiya texnologiyalarının, o cümlədən elektron imzanın mobilliyini daha geniş platformada təmin etmək olar [5,6].

Bulud texnologiyaları müəyyən resurslara (hesablama resurslarına, proqram təminatına və məlumatlara) məsafədən müraciət etmək üçün rahat interfeys təqdim edir, infrastrukturu mərkəzləşdirməyə və xərclərə xeyli qənaət etməyə imkan verir [6]. Dövlət elektron xidmətlərinin bulud texnologiyaları üzərindən göstərilməsi əhalinin elektron xidmətlərə olan çıxışını əhəmiyyətli dərəcədə asanlaşdırır. Bu üstünlüklərinə görə bulud texnologiyaları dövlət sektorunda geniş tətbiq edilə bilər və hazırda bir sıra dövlət təşkilatları öz informasiya sistemlərinin buludlarda yerləşdirilməsi üzərində işləyirlər [5].

Bu işin məqsədi elektron imzanın bulud texnologiyalarından istifadə etməklə reallaşdırılması sahəsində meydana çıxan texnoloji problemləri analiz etmək və onların həlli istiqamətində müəyyən yollar axtarmaqdır.

Məqalə aşağıdakı kimi strukturlaşdırılmışdır. İkinci bölmədə elektron imza haqqında qısa icmal verilir. Üçüncü bölmədə mobil telefonlarda elektron imzanın reallaşdırılmasına mövcud yanaşmalar analiz edilir. Dördüncü bölmədə mobil imzanın müxtəlif ölkələrdə tətbiqi təcrübəsi araşdırılır. Təklif olunan yanaşmanın mahiyyəti barədə məlumat isə beşinci bölmədə verilir.

II. ELEKTRON İMZA – QISA QEYDLƏR

Bulud texnologiyaları əsasında elektron imzanın reallaşdırılmasında əsas çətinliklərdən biri qanunvericiliklə bağlıdır. Məsələ ondadır ki, buludda yerləşən elektron imza vasitələri imzalayan şəxsin bilavasitə nəzarətində deyil və bu səbəbdən onu "Elektron imza və elektron sənəd haqqında" Qanunda göstərilən tərifə görə, gücləndirilmiş elektron imza adlandırmaq mümkün deyil.

Gücləndirilmiş imza Açıq Açar İnfrastrukturunun (Public Key Infrastructure, PKI) köməyi ilə reallaşdırılır və sertifikat xidmətləri mərkəzi (SXM) tərəfindən verilmiş açıq açar sertifikatlarına olan etimada əsaslanır [7]. Sertifikat elektron imzanı yoxlama məlumatlarının imza sahibinə məxsus olduğunu təsdiqləyir.

Lakin yalnız gücləndirilmiş imzadan istifadə etməklə elektron sənədlərin bütün həyat tsiklində həqiqiliyini təmin etmək mümkün olmur. Bu onunla əlaqədardır ki, e-sənədin "yaşama müddəti" imzalama zamanı istifadə edilən gizli açara uyğun açıq açar sertifikatının qüvvədə olma müddəti ilə müəyyən edilir. Bir çox səbəbdən bu müddət 2-3 illə məhdudlaşır və sertifikatın müddəti bitdikdə və ya sertifikat vaxtından əvvəl ləğv edildikdə gücləndirilmiş imza da həqiqiliyini itirir. Buna görə də, gücləndirilmiş imzanın yaradılması (yoxlanması) ilə yanaşı, kriptoqrafik açarların, etimad infrastrukturunun idarə edilməsi, real zamanda sertifikatların yoxlanması, vaxt möhürü və təhlükəsiz uzunmüddətli arxivləşdirmə xidmətləri tələb edilir. Bütün bu xidmətlər XAdES (XML üçün), CAdES (CMS üçün), PAdES (PDF üçün) gücləndirilmiş imza formatlarına və RFC3161 (vaxt möhürü), IETF LTANS (arxivləşdirmə), RFC2560 (OCSP təsdiq), RFC5055 (SCVP təsdiq) kimi aparıcı sənaye standartlarına əsaslanır [8].

Avropa Şurası və Parlamentinin elektron imza sahəsində məşhur "1999/93/EC Direktivləri" gücləndirilmiş elektron imza ilə yanaşı "təkmil elektron imza" anlayışını da daxil edir. Təkmil elektron imza təkmil sertifikatlara əsaslanan və *təhlükəsiz imza yaratma qurğuları*nda (Secure Signature Creation Device, SSCD) yaradılan gücləndirilmiş elektron imzadır. *Təkmil sertifikat* akkreditə edilmiş sertifikat xidmətləri mərkəzi tərəfindən gücləndirilmiş elektron imzanı yoxlama məlumatları barəsində verilən sertifikatdır [9].

1999/93/EC Direktivləri təhlükəsiz imza yaratma qurğularının Ümumi Meyarlar standartı üzrə CC EAL4+ səviyyəsinə uyğunluq sertifikatına malik olmalarını tələb edir. Ayrıca, SXM-lərdə informasiya təhlükəsizliyinin idarə edilməsi sistemi ISO 27001 standartına uyğun olmalıdır.

PKI sistemlərinin qurulması praktikası göstərir ki, SXM-lərin funksiyalar spektrinin sadəcə genişləndirilməsi gözlənilən effekti vermir [8]. Bu xidmətlərin bir-biri ilə qarşılıqlı əlaqədə olaraq etibarlı və təhlükəsiz vahid etimad infrastrukturu formalaşdırması istiqamətində zəruri qanunvericilik, təşkilati və texniki bazis yaradılmalıdır.

Hazırda «Etibarlı üçüncü tərəf» (Trusted Third Party, TTP) servisləri e-dövlət miqyasında etimad infrastrukturunun qurulması üçün əsas platformadır [8]. «Etibarlı üçüncü tərəfin» əsas rolu elektron qarşılıqlı əlaqə iştirakçılarına zəmanət təmin etməkdən ibarətdir ki, məlumatlar və tranzaksiyalar öz ünvanına tamlığı, həqiqiliyi və müəllifliyi təmin edilməklə, vaxtında və dəqiq çatdırılır və istənilən münaqişə baş verdikdə hadisələrin gedişatını bərpa etməyə imkan verən lazımi sübutların hazırlanması və təqdimatı üçün müvafiq metodlar mövcuddur [8].

Elektron imza sahəsində ölkələrin qanunvericiliyi 1990-cı illərin sonlarında formalaşmağa başlayırdı və elektron imza üzrə Avropa Komissiyasının məşhur 1999/93/EC Direktivi "məsafədən elektron imza"nı nəzərə almamışdı. «Etibarlı üçüncü tərəf» konsepsiyasını inkişaf etdirən Avropa Birliyinin 910/2014 Reqlamenti qarşılıqlı informasiya əlaqəsinin daha yüksək təhlükəsizlik səviyyəsini təmin etmək üçün daha etibarlı etimad elementləri daxil edir [10] (Qeyd edək ki, 1999/93/EC Direktivi 1 iyul 2016-cı ildən qüvvədən düşür).

910/2014 Reqlamenti ndə aşağıdakılar nəzərdə tutulur:

- Etimad edilən servislər təsdiqlənmiş etimad xidmətləri provayderləri tərəfindən (SXM) göstərilir.
- İdentifikasiyaya və autentifikasiyaya etimad səviyyələri müəyyən edilib.
- Təkmil imza açarlarının yaradılmasını və istifadəsini üçüncü tərəfə etibar etmək olar;
- Təkmil imza serveri akkreditasiya edilmiş xidmət provayderləri tərəfindən idarə edilməlidir;
- SSCD tələbi təkmil imza yaratma qurğusu tələbi ilə əvəzlənib (Qualified Signature Creation Device, QSCD). Təkmil imza yaratma qurğuları Avropa Komissiyası tərəfindən təsdiq edilən siyahıda olmalıdır;
- Veb-saytların autentifikasiyası üçün təkmil giriş sertifikatları vermək lazımdır, bu sertifikatda saytın sahibi identifikasiya edilir. Belə sertifikatları yalnız təsdiqlənmiş etimad xidmətləri provayderləri verə bilər.

CEN TS 419241 texniki spesifikasiyasında gücləndirilmiş və təkmil elektron imza serverlərinə dair konkret tələblər və tövsiyələr vardır [11].

III. MOBİL TELEFONLARDA E-İMZANIN REALLAŞDIRILMASI

Kriptoqrafik açar məlumatlarını təhlükəsiz saxlamaq və kriptoqrafik əməliyyatları yerinə yetirmək üçün müəyyən təhlükəsiz aparat elementi (bloku) tələb edilir. Bu təhlükəsiz aparat elementinin reallaşdırılmasından və yerləşdirilməsindən asılı olaraq mobil imza həllərini iki sinfə bölmək olar:

SIM-ə əsaslanan həllər. Mobil telefonun SIM (subscriber identity module) kartı kriptoqrafik açarları və sertifikatları təhlükəsiz saxlamaq və kriptoqrafik əməliyyatları yerinə yetirmək üçün istifadə edilir. Bir çox halda xüsusi SIM-kartlardan istifadə etmək lazım gəlir, çünki istifadədə olan SIM-kartlar e-imza yaratmaq kimi kriptoqrafik əməliyyatları

dəstəkləməyə bilər. SIM-də saxlanan kriptoqrafik açar verilənlərinə və kriptoqrafik funksiyalara giriş yalnız qanuni istifadəçiyə məlum olan məxfi PIN ilə qorunur.

Server-əsaslı həllər. Server əsaslı həllərdə mobil imza həlləri təhlükəsiz aparat elementini mərkəzləşdirilmiş qaydada reallaşdırır. Adətən, kriptoqrafik açarların saxlanması və kriptoqrafik əməliyyatların yerinə yetirilməsi üçün aparat təhlükəsizlik modulları (Hardware Security Module, HSM) istifadə edilir. Belə həll Orthacker və həmmüəllifləri tərəfindən təklif edilmişdi [12]. İstifadəçinin mobil telefonunda nə kriptoqrafik funksiyaların reallaşdırılması, nə də kriptoqrafik açarların saxlanması tələb edilir. Lakin mobil telefon serverdə saxlanılan kriptoqrafik açarlara giriş əldə etmək və kriptoqrafik əməliyyatları yerinə yetirmək üçün məcburi olan autentifikasiya prosesinin tərkib hissəsidir.

Server əsasında mobil imza funksiyası bankların e-bankinq üçün istifadə etdikləri həllə oxşardır. Giriş kodu (mobil telefon nömrəsi) və PIN ilə uğurlu girişdən sonra həmin telefona SMS ilə TAN kodu (Transaction authentication number) göndərilir. TAN kodu bir neçə dəqiqə ərzində qüvvədə olur və onu müvafiq tətbiqi proqrama daxil etdikdə gücləndirilmiş elektron imza yaradılır.

IV. MOBİL İMZANIN TƏTBİQİ TƏCRÜBƏSİ

Yuxarıda göstərilən hər iki yanaşma üçün konkret həllər işlənmişdir və geniş miqyasda tətbiq edilir. Məsələn, SIM-əsasında mobil imza Türkiyə [13], Estoniya və Norveçdə [14] istifadə olunur. Server-əsaslı mobil imza sistemi Avstriyada 2009-cu ildən fəaliyyət göstərir [15].

Türkiyədə m-imza xidmətləri GSM operatorları Turkcell (2007, fevral), Avea (2008, fevral) və Vodafone (2013, yanvar) üzərindən göstərilir. M-imza 128K SIM kartlara yüklənən xüsusi proqram təminatı ilə həyata keçirilir. Bu SIM kartlar verilənlərin təhlükəsizliyini təhdid edən hücumlara qarşı kartlarda qabaqcıl təhlükəsizlik mexanizmlərinin mövcudluğunu sübut edən EAL4+ (Evaluation Assurance Level) sertifikatına malikdirlər. SIM kart üzərindəki m-imza məlumatlarını kopyalamaq mümkün deyil.

Türkiyədə 2014-cü ilin sonuna 1 milyon 700 min e-imza və mobil sertifikatı imza verilmişdi. Aktiv olaraq istifadə edilən e-imza sayı 750 min, mobil imza sayısı isə 21 473 olmuşdu [13].

2006-cı ildə Moldova hökuməti elektron imza layihəsində imzanın leptoplarda xüsusi çip vasitəsilə istifadəsi variantını da seçmişdi. Lakin bu variant vətəndaşlar üçün baha idi (30 ABŞ dolları). Moldovada mobil rəqəmsal imzanın istifadəsi 2013-cü ilin iyulunadək pulsuz olmuşdur. Hazırda fərdlər üçün ayda 10 imza üçün qiyməti 0.8 ABŞ dolları, özəl sektor üçün isə ayda 1000 imza üçün 3.9 ABŞ dollarıdır [16].

Avstriyada imza serveri akkreditasiya edilmiş SXM tərəfindən idarə edilir. İkifaktorlu autentifikasiya: telefonun nömrəsi + parol, SMS ilə birdəfəlik parol istifadə edilir. Açarlar HSM-də saxlanır və PDF sənədlərin imzalanması dəstəklənir [15].

V. BULUD TEXNOLOGİYALARI ÜZƏRİNDƏ MOBİL İMZA

Bulud texnologiyaları ─ ümumi kompüter resursları toplusunu (məsələn, şəbəkə, serverlər, məlumat anbarları, proqramlar və servislər) sorğu əsasında şəbəkə vasitəsilə əldə etməyə imkan verən modeldir [5]. Bulud texnologiyalarında istifadəçilərə servislər üç fundamental model (SaaS, PaaS, IaaS) əsasında təqdim olunur.

Proqram təminatı servis kimi (ing., Software as a Service, SaaS) provayderin bulud infrastrukturunda icra olunan proqram təminatı servis kimi istifadəçiyə təqdim olunur. Google Docs, Microsoft Office Live misal kimi göstərilə bilər.

Platforma servis kimi (ing., Platform as a Service, PaaS) müxtəlif platformalar istifadəçiyə servis şəklində təqdim olunur. Google App Engine, Microsoft Azure, Salesforce Force.com misal göstərilə bilər.

İnfrastruktur servis kimi (ing., Infrastructure as a Service, IaaS) hesablama infrastrukturu istifadəçiyə servis kimi təqdim olunur. Hesablama infrastrukturuna hesablama resursları, yaddaş, şəbəkə və s. aiddir. Belə infrastruktura Amazon Simple Storage Service (S3), RackSpace Cloud Servers misal ola bilər.

Məlum olduğu kimi, informasiya təhlükəsizliyini təmin etmək üçün autsorsinq xidmətləri mövcuddur. Belə xidmətləri bulud üzərindən də göstərmək mümkündür, Security-as-a-Service (SecaaS) xidmətləri bazarı formalaşma mərhələsindədir.

Gartner-in analizinə görə, informasiya təhlükəsizliyi bazarında ən çox tələbat olan bulud xidmətləri üçlüyü yaxın gələcəkdə e-poçtun müdafiəsi, veb-təhlükəsizliyin təmin edilməsi, həmçinin identifikatorların və girişin idarə edilməsi (identity and access management, IAM) üzrə xidmətlərindən ibarət olacaq [17]. Lakin yaxın bir neçə il ərzində ən çox gəlir artımının şifrləmə və elektron açarlar, informasiya təhlükəsizliyi hadisələrinin idarə edilməsi, boşluqların analizi və tətbiqi veb-proqramlar üçün şəbəkə ekranları seqmentlərində olacağı təxmin edilir.

Hazırda Norveçdə təkmil sertifikatı buludda olan gücləndirilmiş elektron imza istifadə edilir. Açarlar HSM-də saxlanır. Artıq 3 milyondan artıq sertifikat verilmişdir ki, onların böyük əksəriyyəti buluddadır. Mobil tətbiqlərin təxminən 600 min istifadəçisi var. Pik istifadə gündə təxminən 1,3 milyon əməliyyat olur, onlardan 20-25%-i imzalama əməliyyatıdır. İmzalanan sənədlərin formatı mətn, XML, PDF-dir. Sistem səlahiyyətli orqanlar tərəfindən attestasiya olunub [18].

Bulud mobil imza xidmətlərinin təklif edilən interfeyslərə, autentifikasiya metodlarına, saxlanca və imza formatlarına görə qiymətləndirilməsi [19]-də aparılır. Qiymətləndirilən imza xidmətlərinə Adobe EchoSign, Amazons CloudHSM, Avstriya mobil imzası, Cryptomathic Signer, Dictao Cloudcard,

DocuSign və Time4Mind imza xidmətləri daxildir. Izenpe, ARX, SigningHub, Cryptolog və Cryptas kimi digər vendorların da oxşar xidmətlər təklif etdiyi qeyd edilir.

NƏTİCƏ

Mobil qurğularda bulud imzası rahat və səmərəli vasitədir. Avropa təcrübəsi gücləndirilmiş bulud imzasının istifadəsi imkanlarını təsdiqləyir. Bu sahədə həm qanunvericilik, həm praktiki tətbiq, həm də texniki tənzimləmə baxımından əhəmiyyətli təcrübə toplanmışdır.

Qeyd etmək lazımdır ki, mövcud həllərin əksəriyyəti spesifik qanunvericilik sisteminə və ya müəyyən eyniləşdirmə sisteminə görə yaradılıb (məsələn, konkret milli eID sisteminə). Bu həllərin digər ölkələrdə tətbiqi əhəmiyyətli uyğunlaşdırma işləri və əlavə xərclər tələb edir.

ƏDƏBİYYAT

[1] Elektron imza və elektron sənəd haqqında Azərbaycan Respublikasının Qanunu, 26 may 2004-cü il.

[2] “Azərbaycan Respublikasında yeni nəsil şəxsiyyət vəsiqəsinin tətbiqi ilə bağlı əlavə tədbirlər haqqında” Azərbaycan Respublikasının Prezidentinin Sərəncamı, №893, 28 noyabr 2014-cü il.

[3] Mobile signature. http://en.wikipedia.org/wiki/Mobile_signature

[4] http://e-imza.az/stats.php?lang=az

[5] R. M. Əliquliyev, F. C. Abdullayeva, “Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi,” İnformasiya texnologiyaları problemləri, №1(7), s. 3-14, 2013.

[6] R. Q. Ələkbərov, M. A. Həşimov, T. İ. Mustafayev, “Cloud Computing xidmətinin təhlükəsizlik məsələləri və onların həlli yolları,” İnformasiya texnologiyaları problemləri, №2, s. 33-39, 2014.

[7] R.M.Əliquliyev, Y.N.İmamverdiyev, Rəqəm imzası texnologiyası, Bakı Elm, 2003.

[8] Я.Н. Имамвердиев, М.Ш. Гаджирагимова, “Архитектура инфраструктуры доверия электронным документам в среде электронного государства,” Телекоммуникации, №11, с. 18-26, 2011.

[9] Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures, published in the Official Journal of the European Communities (OJ) L 13, 19.01.2000,

[10] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal of the European Union, 257, 28.8.2014, p. 73–114.

[11] European Committee for Standardization. CEN TS 419241 - Security Requirements for Trustworthy Systems Supporting Server Signing - draft, June 2013.

[12] C. Orthacker, M. Centner, and C. Kittl, “Qualified mobile server signature,” in Security and Privacy – Silver Linings in the Cloud, ser. IFIP Advances in Information and Communication Technology, K. Rannenberg, V. Varadharajan, and C. Weber, Eds., vol. 330. Springer Berlin Heidelberg, 2010, pp. 103–111.

[13] http://bilgicagi.com/btk-2014-e-imza-mobil-imza-raporu/

[14] C. Rath, S. Roth, M. Schallar, T. Zefferer, “A Secure and Flexible Server-Based Mobile eID and e-Signature Solution,” The Eighth International Conference on Digital Society (ICDS), 2014, pp. 7-12.

[15] P. Lipp, H. Leitold, “Austrian Mobile Phone Signature,” ETSI Workshop Signatures in the Cloud, 2013. http://docbox.etsi.org/Workshop/2013/201303_SIGNATURES_IN_CLOUD/2d-Austria-SigningInTheCloud.pdf

[16] Centrul de Guvernare Electronică: Authentication and Mobile EID for the Public Sector in Moldova. 2011.

[17] Gartner: “User Survey Analysis: Global Buying Preferences for Security as a Service in Midsize and Large Organizations.” 2012..

[18] R.Hagen, “Norwegian BankID.” ETSI Workshop Signatures in the Cloud, 2013. http://docbox.etsi.org/Workshop/2013/201303_SIGNATURES_IN_CLOUD/2c-BSK-Norwegian-BankID.pdf

[19] F. Reimair, “Cloud-based signature solutions: A survey,” Secure Information Technology Center – Austria. October 2014