ÜGYFÉL-AZONOSÍTÁS ÉS -HITELESÍTÉS A MAGYAR E-KÖZIGAZGATÁSBAN

Sikolya Zsolt, zsolt.sikolya@ihm.gov.hu
Informatikai és Hírközlési Minisztérium

Bevezető

A közigazgatási hatósági szolgáltatások, de ennél szélesebb körre kitekintve a közszolgáltatások jelentős része – elsősorban az ún. tájékoztató szolgáltatások – nem igénylik a felhasználó azonosítását: azokat a felhasználók név nélkül, anonim módon vehetik igénybe. A hatósági eljárások túlnyomó résznek igénybevételéhez – és ez igaz a hatósági és egyéb közszolgáltatások egy részére is – az ügyfélnek valamilyen mértékben és hitelességgel azonosítania kell magát. Mindez igaz mind az ügyek hagyományos, tehát személyesen vagy papíron történő intézésére, mind pedig az elektronikus úton történő ügyintézésre is. A továbbiakban elsősorban a hatósági ügyintézés, azon belül is az elektronikus ügyintézés sajátosságaival fogunk foglalkozni, de alkalmanként az elektronikus út azonosítási módszereit összevetjük a hagyományos azonosítással is. A hatósági ügyek ügyfelei lehetnek természetes és jogi személyek, ill. jogi személyiséggel nem rendelkező szervezetek. Mivel ez utóbbi két ügyféltípus képviseletében is minden esetben természetes személy jár el, ezért a továbbiakban elsősorban a természetes személyek azonosításával foglalkozunk[1], és az ügyfél alatt természetes személyt, ill. képviselőt értünk.

Mivel már a címben is – és az előadás során gyakran – szerepel megkülönböztetve az azonosítás (identification) és a hitelesítés (authentication) fogalma, és mivel a különböző források nem egységesen értelmezik ezt a két fogalmat, elöljáróban megadjuk a két fogalomnak az előadás során használt értelmezését, melyet [1]-ből vettünk át:

Azonosítás: Arra vonatkozó információ megszerzésének folyamata, hogy kinek állítja magát a kérelmező.

Hitelesítés (személyé): Egy személy állított azonosságáról való bizonyosság megszerzése

A személy hitelességének (entity authentication) fogalmát meg kell különböztetni az adat (vagy dokumentum) hitelességének (data authentication) fogalmától, amelyet az adat sértetlenségének és eredetének bizonyosságaként értelmezünk [2].

Az e-közigazgatási eljárások új szabályozása

[1] Távlatilag nyilván lehetőség lesz majd arra is, hogy egyes hatósági ügyintézések során az ügyfél és a hatóság részéről automatizmusok kapcsolódjanak össze, és ilyenkor az automatizmusok azonosítása lesz a feladat, de az ilyen esetekben is a természetes személy ügyfél, vagy az ügyfél természetes személy képviselőjének felhatalmazására lesz szükség ahhoz, hogy a hatóság elfogadja az ügyfél automatizmusának eljárását.

A közigazgatási hatósági ügyintézés általános szabályait a 2005. november 1-jén hatályba lépett, a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.) állapítja meg [3]. Általánosságban a Ket. nem foglalkozik magának az ügyfél-azonosításnak és -hitelesítésnek a módjával, legfeljebb csak azt határozza meg, hogy az egyes eljárási cselekményeknél az ügyfél milyen adatait kell rögzíteni. A hagyományos ügyintézés esetében az ügyfél-azonosításnak és -hitelesítésnek már kialakult gyakorlata van, viszont az elektronikus ügyintézés teljesen új kihívást jelent a közigazgatás számára, ezért a Ket. részletesen szabályozza az elektronikus ügyfél-azonosítás és -hitelesítés lehetséges módozatait. További részleteket határoz meg a Ket. két végrehajtási rendelete ([4], [5]), amelyekre 193-as és 194-es kormányrendeletként fogunk a továbbiakban hivatkozni.

A hagyományos ügyintézés során az ügyfél kérelmét írásban (esetleg személyesen szóban) terjeszti elő. Az azonosítás/hitelesítés vonatkozásában két fő típussal találkozunk. Az egyik esetben elegendő, hogy az ügyfél a kérelemben azonosítja magát, és a kérelmet aláírja. Ilyenkor a hatóság „elhiszi" az állított azonosságot: nincs aláírásmintája, ezért le sem tudná ellenőrizni az aláírást. Ilyenkor az aláírásra csak azért van szükség, hogy egy esetleges későbbi jogvita esetén bizonyítható legyen a kérelem eredete és sértetlensége. A másik esetben személyes megjelenésre van szükség – legkésőbb az eljárás végső, érdemi fázisában – , és a kérelmezőnek személyazonosítására alkalmas hatósági igazolvánnyal (személyi igazolvány, útlevél, jogosítvány) kell igazolnia személyazonosságát. A Ket. nem rendelkezik arról – és általános útmutatást sem ad arra nézve –, hogy mely eljárásban milyen azonosítási/hitelesítési módszert kell használni. Az azonosítás/hitelesítés módjának előírása az ágazati jogszabályok hatásköre. Az első módszert alkalmazzák minden olyan esetben, amikor egy esetleges szándékos megtévesztés nagy valószínűséggel még az eljárás során vagy később amúgy is kiderül, és nem veszélyezteti az alapvető jogbiztonságot (pl. adóbevallás, adat igazolása stb.). A „szigorúbb" módszert szokták előírni pl. személyazonosítására alkalmas hatósági igazolvány átadásához – éppen az azonosító okmányokkal való visszaélés elkerülésére –, vagy különleges adatok közléséhez.

Az elektronikus ügyintézésnél egyelőre nem beszélhetünk ilyen kialakult gyakorlatról, és Magyarországon jelenleg még nem léteznek elektronikus hatósági igazolványok sem. Ezért a Ket. és a korábban említett végrehajtási rendeletei részletes előírásokat adnak az elektronikus ügyintézés során használható és használandó azonosítás/hitelesítés módjára vonatkozóan.

Az elektronikus aláírás használata

Az elektronikus hatósági ügyintézés során a kérelem benyújtásának elsődleges módja a fokozott biztonságú aláírással ellátott kérelemnek a központi rendszeren keresztül vagy közvetlenül a hatósághoz történő eljuttatása. Mint ismert, az elektronikus aláírás természetes használata a dokumentum hitelességének – sértetlenségének és eredetének – garantálása. A Ket. úgy rendelkezik, hogy amennyiben szükség van az ügyfél azonosítására – feltételezhetően itt az azonosság megerősítését, tehát a fenti terminológiánk szerint a hitelesítést kell alatta érteni –, úgy azt az elektronikus aláírás ellenőrzésével, valamint – mivel az e-aláírás általában önmagában nem alkalmas az aláíró azonosságának közvetlen ellenőrzésére – a hitelesítésszolgáltató által nyújtott viszontazonosítás útján kell elvégezni. A viszontazonosítás során – amint arról a 193-as kormányrendelet részletesebben is rendelkezik – lényegében az ügyfélnek a hatóság és a hitelesítésszolgáltató nyilvántartásában szereplő

természetes azonosítóit hasonlítja össze a hitelesítésszolgáltató.[2] Bár az ügyfél-hitelesítés alapjául (is) szolgáló elektronikus aláírásra vonatkozóan a jogszabályok nem követelik meg annak minősített voltát, de a regisztrációval szemben a minősített e-aláírással egyenértékű követelményeket támasztanak. A regisztrációnak személyesen kell történnie az ügyfél személyazonosságának személyazonosításra alkalmas (arcképes) okmány alapján történő ellenőrzésével, és az okmány adatainak a megfelelő közhiteles nyilvántartásban történő ellenőrzésével. Ezzel tehát a jogosulatlan azonosságszerzés szempontjából legdöntőbb mozzanattal, a regisztrációval szemben a legmagasabb biztonsági elvek érvényesülnek.

Az elektronikus aláírásnak személyhitelesítésre történő felhasználása meglehetősen szokatlan a nemzetközi gyakorlatban. Általában az az elterjedt nézet, hogy az (e-)aláírás és a(z elektronikus) személyhitelesítés azért nem keverendő össze, mivel más jogi fogalmak, teljesen más joghatások fűződnek hozzájuk [6]. Az aláírás egy jól kezelhető jogi fogalom, amellyel az aláíró vállal – letagadhatatlan módon – felelősséget az aláírt dokumentumban foglaltakért. Személyhitelesítés viszont egy folyamat, amelyre olyan esetekben kerül sor, amikor a hatóságnak kell felelősséget vállalnia azért, hogy ne jusson valaki illetéktelenül pl. hatósági igazolvány vagy érzékeny adat birtokába. Ha valaki átjut a személyhitelesítésen, joggal hajthat végre olyan cselekményeket, amelyekre ezzel jogosultságot szerzett. Bár mind az e-aláírásnak, mind az (erős) elektronikus személyhitelesítésnek leggyakrabban használt technikai megvalósítása a nyilvános kulcsú infrastruktúrán (PKI) alapul, a két különböző célra az esetek túlnyomó többségében különböző tanúsítványokat használnak. Az ismertetett jogi megfontolások miatt az elektronikusan aláírandó dokumentum tartalmát az aláírónak ismernie kell, hogy felelősséget vállalhasson érte, míg az elektronikus személyhitelesítésnél egy – a személy azonosságát ellenőrző hatóság által megküldött véletlenszerű – nem „visszajátszható” – adatot kell az ügyfélnek titkos kulcsával kódolnia ellenőrzés céljából (kérdés-válasz, challenge-response).

A 193-as kormányrendelet úgy igyekszik feloldani a fenti ellentmondást, hogy olyan esetekben is egy, az ügyfél által értelmezhető „belépési” kérelem aláírását írja elő, amikor az ügyfél valójában nem kérvényt kíván benyújtani a hatósághoz, hanem pl. párbeszédre épülő ügyintézés során „navigálni” szeretne a hatóság adatai között (pl. meg kívánja tekinteni, hogy hol tart az ügyének intézése). Természetesen ilyenkor biztosítani kell azt, hogy a kérelem tartalmazzon valamilyen nem ismétlődő adatot, hogy a kommunikáció ne legyen visszajátszható. Meg kell jegyezni, hogy szokatlan volta ellenére ez a megközelítés nem egyedülálló: az osztrák e-közigazgatási törvény által előírt „Bürgerkarte” koncepcióban sincs külön hitelesítő (autentikációs) tanúsítvány. A személy ágazati azonosítóinak származtatására használt egységes forrásazonosítót az e-aláírás nyilvános kulcsához kapcsolja egy, a forrásazonosítót kibocsátó hatóság aláírásával ellátott adatrekord, és a „beléptetéskor” szükséges ügyfél-hitelesítéshez a magyar megoldáshoz hasonlóan egy „nem visszajátszható” kérelmet iratnak alá az ügyféllel. A személyazonosság megállapításához a hatóság számára szükséges ágazati azonosító kódot az aláíró nyilvános kulcshoz hitelesen hozzákapcsolt forrásazonosítóból számítják ki egy egyirányú algoritmussal.

Amint az osztrák megoldás is egyedülálló a maga nemében, a magyar viszontazonosításra sincs példa más országokban. A nemzetközi együttműködésben külön problémát jelenthet, hogy a magyar megközelítés egy piaci szereplő, a hitelesítésszolgáltató számára ír elő kötelező jelleggel egy speciális szolgáltatást (természetesen csak a közigazgatási célú

[2] Mivel a hatóságok nyilvántartásainak nagy része nincs harmonizálva, és így meglehetősen pontatlan, ezért – bár az említett jogszabályok erről nem rendelkeznek – az IHM által a viszontazonosítás elvégzéséről kiadott ajánlás egy bizonyos jól meghatározott „toleranciát” ajánl alkalmazni az összehasonlításnál.

tanúsítványokat kibocsátóktól). Nem valószínű, hogy ilyen szolgáltatást külföldi hitelesítésszolgáltató vállalna.

Felhasználói név és jelszó használata

A Ket. rendelkezései szerint az elektronikus aláírással nem rendelkező ügyfelek számára csak a központi rendszer biztosítja az elektronikus ügyintézés lehetőségét. Ilyenkor egy ún. ügyfélkapun keresztül történik a belépés – lényegében egy felhasználói név és jelszó megadásával. Ezt megelőzően egy okmányirodában regisztrálnia kell az ügyfélnek, amely ugyanolyan szigorú személyazonosítással történik, mint amilyent az elektronikus aláírás regisztrációjánál már megismertünk. Az ügyfélkapun történő beléptetést követően a hatóság információs rendszere nem kapja meg az ügyfélről a központi rendszerben tárolt természetes személyazonosító adatokat, hanem – ha az ügyfél hiteles azonosítására van szükség, akkor – egy, az elektronikus aláírásnál megismerttel analóg viszontazonosítási folyamattal ellenőrizheti le az ügyfél vélt személyazonosságának valódiságát.

A hitelesítési módszerek összehasonlítása

A jelszavas ügyfél-hitelesítés lényegesen kevésbé biztonságos, mint a PKI alapú. Az előbbi egyetlen, viszonylag könnyen megszerezhető információ, a jelszó – feltételezetten kizárólagos – ismeretén alapul (egyfázisú, „single-factor” hitelesítés), míg az utóbbihoz a magánkulcs birtoklása és a magánkulcs aktivizálásához szükséges jelszó (ill. PIN-kód) ismerete szükséges (kétfázisú, two-factor hitelesítés) [7]. Az utóbbi esetben a jelszó nem is kerül ki nyilvános csatornára. Jelentős biztonsági hátránya ellenére a jelszavas ügyfél-hitelesítést egyszerűsége miatt számos országban használják közigazgatási szolgáltatások igénybevételéhez – igaz, hogy sok esetben egyszer használatos jelszót használnak, ami sokkal biztonságosabb a magyar megoldásnál. Ahogyan egyre több ország látja el polgárait elektronikus aláírással, ill. hitelesítésre szolgáló PKI-tanúsítvánnyal – főként személyazonossági vagy egészségügyi kártyára, esetleg bankkártyára, sőt SIM-kártyára telepítve –, egyre inkább felváltják a jelszavas rendszereket a PKI alapú hitelesítést alkalmazó rendszerek.

A Ket. – és végrehajtási rendeletei – egyenértékűként kezelik a két ügyfél-hitelesítési módszert, és nem teszik lehetővé, hogy ágazati jogszabály mérlegelje, hogy melyik használatát engedélyezi. Egyedül abban van választási lehetőség, hogy a hatóság alkalmazzon-e hitelesítést (viszontazonosítást), vagy esetleg csak fogadja el azt, amit az ügyfél magáról állít. Bizonyos esetekben azonban a 193-as kormányrendelet előírja a viszontazonosítás, tehát a „szigorú” ügyfél-hitelesítés használatát (pl. ha az ügyfél személyes adathoz, illetve adó-, bank-, biztosítási vagy értékpapírtitokhoz kíván hozzáférni).

A 193-as kormányrendelet bevezeti a kölcsönös és összefüggő adatcserét és kétirányú kapcsolatot alkalmazó ún. párbeszédre épülő, valamint a nem párbeszédre épülő ügyintézés fogalmát. Az előbbire tipikus példák a webes, az utóbbira pedig az elektronikus levelezésen alapuló rendszerek. Az elektronikus aláíráson alapuló ügyfél-hitelesítés mindkét típusú ügyintézésnél használható, míg a jelszavas belépést – és az ahhoz kapcsolódó viszontazonosítást – a jelenleg szabályozott formájában csak a párbeszédre épülő rendszerek tudják használni.

A magyar e-ügyintézés szabályozásában meg kell említeni még egy különlegességet, amely ugyan nem az ügyfél-hitelesítéshez, hanem a dokumentumhitelesítéshez kapcsolódik. A 193-as kormányrendelet szerint alapesetben a párbeszédre épülő ügyintézés – beleértve az ügyfélkapun történő, jelszavas belépést is – önmagában biztosítja a kapcsolat tartama alatt végzett egyes eljárási cselekményeknek az azonosított ügyfélhez rendelését. Az eljárási cselekményekbe bele kell érteni többek között valamely dokumentum beküldését is. Ez azt jelenti, hogy egy jelszavas belépéssel történő adóbevallás tartalmát érintő esetleges jogvita során az ügyfélnek kell bizonyítania azt, hogy az általa vélt bevallást küldte be, amely elektronikus aláírás nélkül meglehetősen reménytelen vállalkozás. Tehát egy kicsit sarkosan fogalmazva a magyar jogrendszer a jelszavas ügyfél-hitelesítéshez (is) a letagadhatatlanság vélelmét rendeli, míg – amint azt korábban láttuk – az elektronikus aláírást használja ügyfél-hitelesítésre (is), ami épp a fordítottja a nemzetközileg kialakult gyakorlatnak.

Nemzetközi kitekintés, európai tervek

Már a korábbiakban is többször vetettük össze a magyar e-közigazgatási ügyfél-azonosítást a külföldi példákkal. A nemzetközi gyakorlat elemzését folytatva megállapíthatjuk, hogy míg az e-közigazgatásban alkalmazott dokumentumhitelesítésnek – annak ellenére, hogy még a teljes mértékben átjárható megoldások hiányoznak – jól kialakult jogi és szabványosítási háttere van (gondolunk itt elsősorban az EU elektronikus aláírásra vonatkozó irányelvére [8] és a meglévő számos nemzetközi – ETSI, IETF stb. – szabványra), addig a személyhitelesítésnek nincs nemzetközi jogi háttere, a gyakorlata országonként – és sokszor az egyes országokon belül is – eltérő, nincsenek rá elterjedten használt szabványok. Alapvetően két fő típusra oszthatjuk a jelenleg használt megoldásokat: a központi és a szövetséges azonosságkezelésen (federated identity management) alapuló modellekre. Azon országok esetében, amelyek egységes személyazonosító kódot használnak, és központilag bocsátanak ki e-aláírásra, e-hitelesítésre alkalmas eszközt (pl. Belgium, Észtország), általában a személyhitelesítésre szolgáló tanúsítvány egy központi hitelesítésszolgáltató által aláírva (hitelesítve) tartalmazza az egységes személyazonosító kódot. A tanúsítványhoz tartozó magánkulcs használatával meg lehet győződni arról, hogy ténylegesen a tanúsítványban szereplő személyazonosító kód „tulajdonosa” folytat-e párbeszédet a hálózaton a hatósággal. De egyes, az egységes személyazonosító használatát tiltó országok (pl. Ausztria) is használnak központi modellt, amikor is egy központi hatóság állítja ki végső soron az elektronikus igazolványként szolgáló eszközt. Egyre inkább kezdenek elterjedni azonban az osztott, ill. szövetséges modellek. Ezeknek lényege az, hogy az ügyfelek megválaszthatják, hogy mely azonosságszolgáltatókat bízzák meg elektronikus azonosságuk igazolásával (hitelesítésével), az alkalmazásszolgáltatók pedig megállapodásokat kötnek az azonosság–szolgáltatókkal, hogy elfogadják hitelesítésüket, és így végül ún. bizalmi körök alakulnak ki, amelyeken belül „szövetséges” (egyezményes) alapon működik a személyhitelesítés. Adatvédelmi szempontból fontos, hogy ennél a modellnél az ügyfél akár esetenként is dönthet arról, hogy mely azonosságszolgáltatót választja, és hogy az milyen hitelesítési információt adhat át az alkalmazásszolgáltatónak. A skandináv országokban pl. a bankok mint azonosságszolgáltatók hitelesítését is elfogadják a közigazgatásban.

Míg a központi megoldásoknál az egységesség a modell jellegénél fogva biztosított, addig a szövetséges modellek különösen megkívánják szabványosítást. Jelenleg három ilyen szabványosítási kezdeményezés van erősen elterjedőben [9]: a Liberty Alliance, a Microsoft és az OASIS rendszere. A francia kormányzat a mintegy 170 céget, szervezetet tömörítő Liberty Alliance szabványait használja (tagja is a szervezetnek). Mivel a magyar e-

ügyintézési szabályozás bármely – megadott követelményeknek eleget tevő – hitelesítés-szolgáltató tanúsítványát elfogadja, ezért az elektronikus aláíráson alapuló hitelesítés a szövetséges modellekhez áll közel. Az ügyfélkapu viszont tipikus központi megoldás.

Végül szólnunk kell a páneurópai törekvésekről is, hisz ezek nagymértékben meg fogják határozni a magyar jogalkotás és megoldások alakulását. Az Európai Bizottság eEurope E-közigazgatási Alcsoportja 2005-ben kidolgozta az i2010 e-közigazgatási stratégiáját [10], melyet 2005. novemberben a manchesteri miniszteri e-közigazgatási konferencián tettek közzé. Ennek kivonata képezte az alapját a miniszteri konferencia közleményének is, mely felkérte a Bizottságot, hogy a stratégiát vegye figyelembe az i2010 e-közigazgatási cselekvési tervének elkészítése során. A cselekvési tervet 2006 áprilisára tervezik összeállítani. Ennek a tervnek a stratégia szerint négy fő iránya lesz, amelyből az egyik az e-azonosítással és hitelesítéssel, valamint az elektronikus dokumentumok hitelességével foglalkozik. A stratégia a legfontosabb tennivalók között megjelölte, hogy

- 2010-re legyen olyan megbízható e-azonosítás minden európai ügyfélre az adatvédelem figyelembevételével, melyet minden tagország saját felelősségében old meg, és elismer,
- ennek megalapozására készüljön el egy világos terminológia,
- legyen megoldva a meghatalmazás, közvetítés, szerepkezelés,
- legyenek egységes dokumentumformátumok,
- legyenek egységes kritériumok a hiteles dokumentumokra vonatkozóan,
- legyen megoldva a dokumentumok egységes azonosítása, hiteles archiválása.

Az első feladat végrehajtása során messzemenően figyelembe kell azt venni, hogy számos ország már jelentősen előrehaladt saját e-közigazgatási ügyfél-hitelesítési rendszerének megvalósítása terén. Ezek a megoldások jelenleg nem átjárhatóak, és mivel már hatalmas összegeket ruháztak be megvalósításukra, nem lehet szó arról, hogy a meglévő megoldásokat lecseréljék valamilyen páneurópai egységes megoldásra. További nehézséget jelent az egységesítés útjában az a tény, hogy az Európai Unió elsődleges jogát képező, az európai közösség létrehozásáról szóló szerződés [11] 18. cikke szerint az útiokmányokra, személyazonosító igazolványokra, a tartózkodási engedélyekre vagy bármely egyéb ilyen okmányra vonatkozó rendelkezések nem tartoznak közösségi hatáskörbe. Ez nyilván vonatkozik az elektronikus okmányokra is. Mindezek miatt a tervek szerint az egyes tagországok saját kompetenciájukban valósítják meg e-közigazgatási személyhitelesítési rendszerüket, de el kell ismerniük egymás hitelesítését. Az átjárhatóságot a szövetséges modell alkalmazásával, és a hozzá tartozó szabványosítással, ill. szabványok átvételével kell biztosítani. Fontos szempont, hogy többszintű legyen a modell, azaz tegye lehetővé a különböző biztonsági és hitelesítési igényekhez igazodóan a hitelesítés különböző szintjeinek használatát. Azt majd csak a későbbi vizsgálatok döntik el, hogy ehhez szükség van-e egy nemzetek fölötti uniós infrastruktúra felállítására, vagy az országok közötti kölcsönös elismerés lesz a járhatóbb út. Ugyancsak fontos biztosítani az uniós adatvédelmi irányelv maradéktalan érvényesülését. Az egyes országok igényein túl ki kell elégíteni a páneurópai közszolgáltatások hitelesítési igényeit is. Ezzel a kérdéssel elsősorban az Unió IDABC programja foglalkozik.

Irodalomjegyzék

[1] Architecture for a European interoperable eID system within a smart card infrastructure, CEN Workshop Agreement, CWA 15264-1, 2005, ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eAuth/cwa15264-01-2005-Apr.pdf

[2] Common Terminological Framework for Interoperable Electronic Identity Management, Consultation paper, MODINIS-IDM Project, 2005, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc

[3] A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény, http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400140.TV

[4] Az elektronikus ügyintézés részletes szabályairól szóló 193/2005. (IX. 22.) Korm. rendelet, http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0500193.KOR

[5] A közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó követelményekről szóló 194/2005. (IX. 22.) Korm. rendelet, http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0500194.KOR

[6] Myhr, T.: Regulating a European eID. A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID for the Porvoo e-ID Group, 2005, http://porvoo7.fjarmalaraduneyti.is/media/Porvoo7/Thomas_Myhr.doc

[7] Almási J.: Elektronikus aláírás és társai, Sans Serif, 2002

[8] Az Európai Parlament és a Tanács 1999/93/EK Irányelve (1999. december 13.) az elektronikus aláírásra vonatkozó közösségi keretfeltételekről, http://ccvista.taiex.be/Fulcrum/CCVista/hu/31999L0093-HU.doc

[9] Windley, P. J.: Digital Identity, O'Reilly, 2005

[10] Signposts towards eGovernment 2010, 2005, http://europa.eu.int/information_society/activities/egovernment_research/doc/minconf2005/signposts2005.pdf

[11] Szerződés az Európai Közösség létrehozásáról, http://www2.datanet.hu/im/Primleg/EUSz-EKSz_EAKSz_HU_04-05-01.htm#_Toc63341811