Általános célú biztonságos anonimitási architektúra

Tóth Gergely
tgm@mit.bme.hu

Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Konzulens: Hornák Zoltán
Témavezető: Dr. Vajda Ferenc

2003. június

A hálózati kommunikációval szemben újabban a bizalmasság mellett az anonimitás is megjelent a követelmények között. A hálózati biztonság területén már léteznek bevált algoritmusok, megbízható implementációk. Az anonimitás területén azonban a már létező módszerek ellenére még számos területen van szükség kutatásra. Emellett a két területen elért eredményeket kombinálni kell: egy általános célú biztonságos anonimitási architektúra kidolgozásával meg kell teremteni azt a keretrendszert, melynek alkalmazásával ezen szakterületek mély ismerete nélkül is garantálni lehet a megfelelő szintű kommunikációs biztonságot és anonimitást.

1 Háttér

Az elmúlt évtizedek során a számítástechnika, a hardver, a szoftver, valamint a kommunikáció terén tapasztalható rohamos fejlődés lehetővé tette az ügyviteli rendszerek egyre nagyobb fokú integrálását. Ez a tendencia az Internet térhódításával együtt az informatika elé újabb és újabb kihívásokat állít.

A kommunikációval szemben elsőként fellépő sávszélesség és megbízható adatátvitel problémákra már léteznek átfogó architekturális megoldások.

Napjainkban azonban újabb igények merülnek fel: a meglevő adottságok mellett most már a *bizalmas* kommunikációra is szükség van. A titkosítás, integritás-védelem, távoli azonosítás, letagadhatatlanság megoldására szintén léteznek már bevált megoldások [1] [2], azonban integrációjuk az anonimitási módszerekkel még nem teljes és nem szabványosított.

Ezen biztonsági megoldások fő jellemzője, hogy önálló hálózati rétegbe ágyazva jól definiált szolgáltatásokat nyújtanak, így egyrészt a felsőbb rétegek tervezőinek nem kell komoly kriptográfiai ismeretekkel rendelkeznie, másrészt a réteg módosításai nem érintik a felhasználót.

Legújabban a személyi és személyes adatok védelme került előtérbe. Ahogy egyre több és nagyobb adatbázist kapcsolnak össze és teszik ezeket kereshetővé, úgy lehet az egyes emberekről több és több információt összegyűjteni. Egyfajta ellenintézkedésként ezért van szükség az anonimitásra, azaz az alany személyazonosságának és személyi adatainak elrejtésére, hogy a nem megengedett on-line profil[*] összeállítását meg lehessen akadályozni.

Anonimitás elérése léteznek különböző technikák, azonban hiányzik ezek egységesítése és rendszerbe szervezése.

Az anonimitási megoldásokat alapvetően két nagy csoportba lehet osztani:

- *Anonim engedélyezési sémák*: lehetővé teszik, hogy egy szolgáltató az anonimitási hatóság segítségével megbizonyosodjon, egy számára anonim alany jogosult-e bizonyos szolgáltatások igénybevételére. Tipikus alkalmazási területek: anonim elektronikus fizetés (alany a vásárló, az anonimitási hatóság a bank, az engedélyezés pedig gyakorlatilag a fizetés) [3], anonim elektronikus szavazás (alany a szavazópolgár, anonimitási hatóság a szavazócédula kibocsátója, a szolgáltató pedig az elektronikus urna). Az anonim engedélyezési sémák hatékony működéséhez általában szükség van anonim átvitelre is (lásd a következő csoportot).
- *Anonim átviteli módszerek*: az alany és a szolgáltató közötti adatátvitel során mindkét fél számára transzparens módon biztosítják, hogy az alany anonim marad, személyazonosságát nem lehet visszakövetni [4] [5]. Tipikus alkalmazási terület az anonim elektronikus levelezés, vagy az anonim böngészés.

2 Célkitűzés

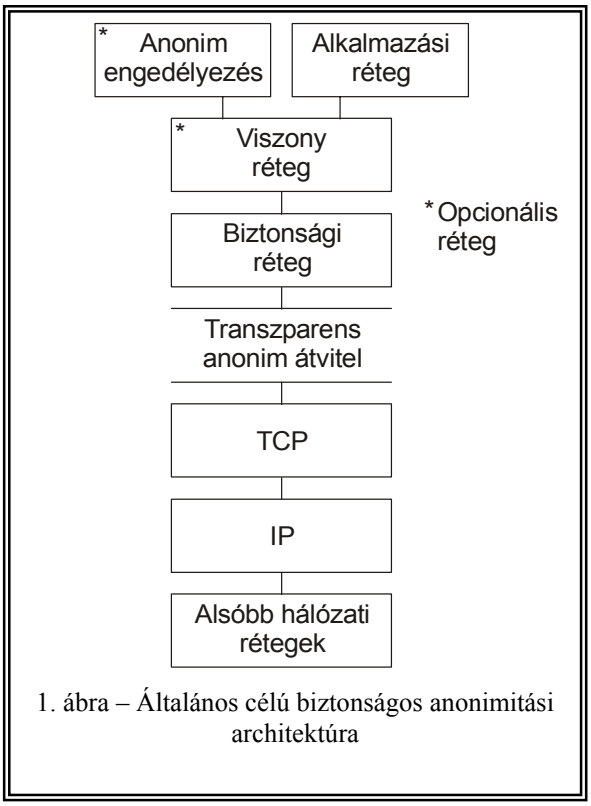
Egy olyan architektúrára van szükség, mely tartalmaz biztonsági funkciókat, garantálja az alany anonimitását és egységes keretet biztosít a különböző anonim engedélyezési sémák használatához, valamint azok összekapcsolásához az alkalmazási réteggel.

[*] Az on-line profil olyan személyes adatok gyűjteménye, melyet jogosulatlanul lehet összegyűjteni az alanyról a különböző elektronikus adatbázisokból és az Interneten történő kereséssel [16].

Ezen feltételek mellett fontos követelmény, hogy a jelenlegi alkalmazásokat a lehető legkisebb mértékben kelljen módosítani az új architektúrára való áttérésnél.

3 Architektúra

A célkitűzésnek megfelelő általános célú biztonságos anonimitási architektúra (lásd 1. ábra) a következő megfontolások alapján alakult ki:



1. ábra – Általános célú biztonságos anonimitási architektúra

- Továbbra is az Internet építőkövét a TCP/IP protokollcsaládot használjuk alappillérként.
- Közvetlenül a TCP réteg felett meg kell bontani a hagyományos TCP/IP kapcsolatot, mivel az alany és a szolgáltató között nem lehet közvetlen IP kapcsolat (IP cím ismeretében az alany esetleg visszakövethető). Erre szolgál a transzparens anonim átvitel, melynek feladata közbülső „átjátszó" állomások beiktatásával (melyek több alany üzeneteit keverik össze) az alany azonosításának megakadályozása a kommunikáció során (bővebben lásd 4. fejezet).

  Ez a funkcionalitás nem biztos, hogy megjelenik például az alanynál futó szoftverekben, mert olyan megoldás is elképzelhető, hogy az adatátvitelt megvalósító csatorna látja el ezt a feladatot.
- A biztonsági réteg a transzparens anonim átvitel felett helyezkedik el, mert itt már szükség van az alany és a szolgáltató közötti közvetlen végpont-végpont kapcsolatra (kriptográfiai műveletek elvégzésére).
- Legfelül helyezkedik el az alkalmazási réteg, mely számára biztosított az alany anonimitása (a transzparens anonim átvitel segítségével) és a kommunikáció bizalmassága (a biztonsági réteg segítségével).
- Az anonim engedélyezés az alkalmazási réteggel egy szinten helyezkedik el, mert tőle független funkciókat biztosít, ugyanakkor egyenrangú vele. Az anonim engedélyezési sémák keretrendszereként került kidolgozásra az AEP (*Anonymity Enhancing Protocol*) (lásd 6. fejezet, [6]).
- Mivel az anonim engedélyezés és az alkalmazási réteg a legtöbb forgatókönyv szerint egy közös viszonyt (*session*) alakít ki (pl. az anonim engedélyezés során megtörtént fizetés után az alkalmazási rétegben meg kell kezdeni a szolgáltatás igénybevételét), szükség van az őket összekötő viszony rétegre. Ez a réteg a biztonsági réteg felett és az anonim engedélyezés, valamint az alkalmazási réteg alatt helyezkedik el.

Az ismertetett architektúra két opcionális réteget tartalmaz: anonim engedélyezés szükségtelensége esetén (pl. mindenki számára hozzáférhető szolgáltatás) a viszonyrétegre sincs tovább szükség. Az is elképzelhető, hogy mind az anonim engedélyezést megvalósító protokollba, mind pedig az alkalmazási rétegbe beépítik a viszony kezelését, így a viszony réteg ismét feleslegessé válik.

4 Transzparens anonim átvitel, az anonimizált hálózat

A transzparens anonim átvitel feladata azon információk elrejtése a szolgáltató elől, mellyel az alanyt azonosítani lehetne (pl. személyazonosság, IP cím). Erre a feladatra számos algoritmus és technika létezik, melyeket alapvetően a következők szerint lehet csoportosítani:

- *viselkedés* szempontjából léteznek passzív (nem befolyásolja őket az üzenetek időbeli eloszlása) és aktív (adaptív) technikák;
- *késleltetés* szempontjából real-time (garantált maximális késleltetés [8]) és nem-determinisztikus (nem garantált, mikor kerül az üzenet kézbesítésre [7]) rendszereket különböztetünk meg;
- a *beiktatott közbülső csomópontok* száma alapján megkülönböztetünk proxy technikákat (1 „átjátszó" [5]), valamint elosztott rendszereket (több „átjátszó" [4]).

A következőkben bemutatásra kerülő PROB-csatorna (4.1 fejezet) alapvetően egy passzív, real-time, proxy rendszer, míg a MIX módszert (4.2 fejezet) az aktív, nem-determinisztikus, elosztott rendszer kategóriákba kell sorolni.

4.1 A PROB**-csatorna

A transzparens anonim átvitel megvalósításához egy elméleti hozzájárulás a PROB-csatorna modellje [9], amely például szolgálhat e terület megismeréséhez.

A csatorna *passzív*, viselkedését nem befolyásolja az üzenetek időbeli eloszlása; *real-time*, azaz beérkezett üzeneteket garantált maximális késleltetésen belül kézbesít; *megfigyelhető*, azaz kimeneteit le lehet hallgatni (bár az üzenetek titkosítása miatt ebből csak időzítési információ nyerhető) valamint *black-box*, így a belső implementációs sajátságok nem ismertek a lehetséges megfigyelők számára.

Célunk a csatorna paramétereinek ismeretében annak megállapítása, milyen valószínűséggel tudja egy passzív megfigyelő az üzenetek küldőjét meghatározni, azaz a csatorna által nyújtott anonimitást kompromittálni.

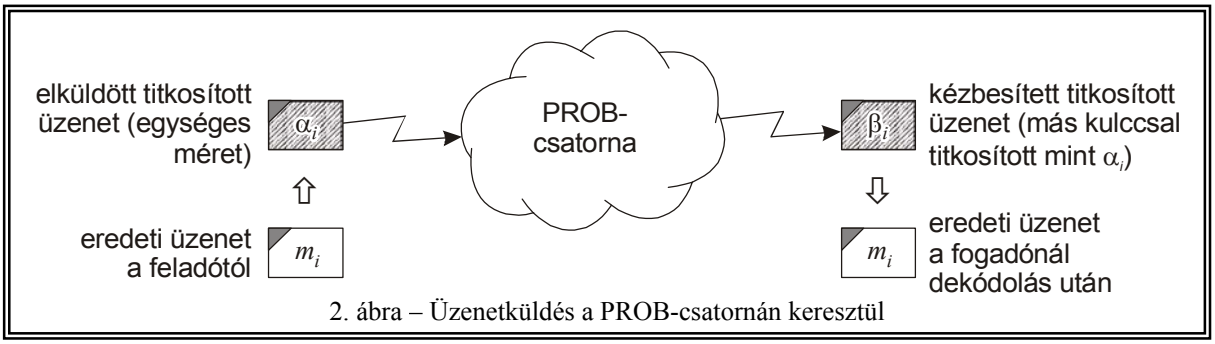
gára üzenet-független felső korlát adható (S a küldők halmaza):

$$\hat{P}_{\Psi} \approx \frac{\tau_{\max}}{|S| \cdot \tau_{\min}}$$

4.2 MIX módszer

Természetesen a PROB-csatorna csak passzív megfigyelők ellen hatásos, aktív támadók ellen más módszereket kell alkalmazni: ekkor a csatornának alkalmazkodnia kell a beérkező üzenetek eloszlásához. Erre kínál megoldást a MIX módszer [4].

Az eljárás lényege, hogy a két kommunikáló végpont közé közbülső csomópontokat, ún. MIX-eket iktat. Ezek után a küldő fél (akinek anonimitását biztosítani akarjuk) a küldendő üzenetet bekódolja: a MIX-eken történő áthaladás fordított sorrendjében titkosítja az eredeti üzenetet a megfelelő MIX nyilvános kulcsával



2. ábra – Üzenetküldés a PROB-csatornán keresztül

A modell szerint küldők üzeneteket küldenek a PROB-csatornán keresztül fogadóknak (lásd 2. ábra). Az üzeneteket (m_i-k) a küldők titkosítják (α_i-k), majd a csatornába küldik. A csatorna az üzeneteket átkódolja, majd bizonyos késleltetés után továbbítja azokat (β_i-k) a fogadóknak, akik dekódolás után megkapják az eredeti üzenetet.

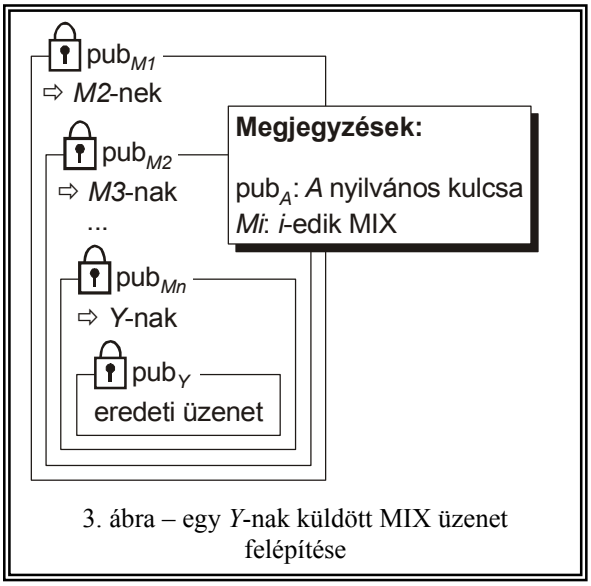
Fontos szerepet játszik a folyamatban a késleltetés, mely ebben a modellben egy meghatározott eloszlással rendelkező valószínűségi változó és két meghatározott határérték között mozog (minimális és maximális késleltetés).

Egy üzenet küldőjéhez való visszakövetésénél a megfigyelő (aki a teljes hálózati forgalmat képes lehallgatni) először azokat a küldőket határozza meg, akik a releváns időintervallumban (a késleltetés tulajdonságai alapján) üzenetet küldtek.

Az anonim átviteli rendszer feladata ezen *anonimitási halmaz* (a lehetséges küldők) elemszámának maximalizálása.

A modellben a kommunikációs szokások szabályozásával ($\tau_{\max}$ maximális és $\tau_{\min}$ minimális üzenetküldési periódus előírásával) valamint a késleltetés egyenletes eloszlásának bevezetésével a megfigyelő bizonyossá-

(lásd 3. ábra) és elhelyezi benne a következő MIX címét. Ezután egy MIX a bejövő üzenetet dekódolja, megkapja a következő állomás címét és a dekódolt üzenetet oda továbbítja.



3. ábra – egy *Y*-nak küldött MIX üzenet felépítése

A titkosítások miatt egy közbülső MIX semmit sem tud az eredeti küldőről, vagy a címzettről, ő két szomszédos MIX-et lát. A legelső MIX nem látja a címzettet, a legutolsó pedig a feladót nem. Így néhány MIX kompromittálódásával a rendszer által nyújtott anonimitás még nem kompromittálható.

** *passive, real-time, observable, black-box*

A MIX-ek aktív „átjátszók”, ugyanis egy bejövő üzenetet nem rögtön továbbítanak, hanem bizonyos számú üzenetet bevárnak, majd azok kimenő üzeneteit véletlenszerűen összekeverve továbbítják. Így adaptálódnak az üzenetküldések eloszlásához.

5 Biztonsági réteg

Miután a transzparens anonim átvitel kiépült az alany és a szolgáltató között, a biztonsági rétegek kapcsolata is felépül. Itt alapvetően a következő funkciókat kell ellátni, melyeket mind az anonim engedélyezés, mind az alkalmazási réteg igénybe vehet:

- *bizalmasság* biztosítása lehallgatás ellen (titkosítással),
- *integritás-védelem* biztosítása módosítás ellen (MAC – *message authentication code* – segítségével),
- *távoli azonosítás* megszemélyesítés ellen és letagadhatatlanság biztosítására (digitális aláírással),
- *időbélyegzés* visszajátszás ellen.

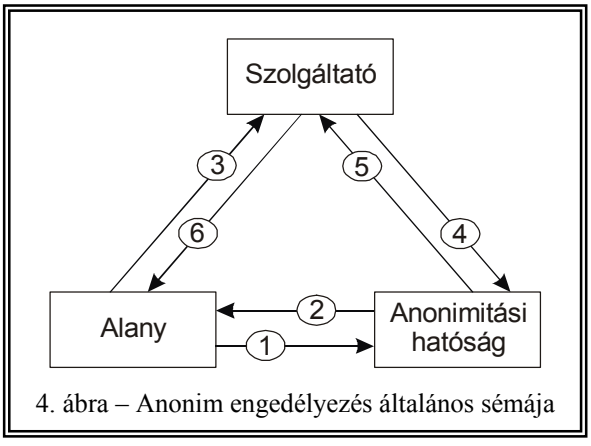
Ezen feladatok elvégzésére már léteznek bevált algoritmusok és implementációk (pl. AES [10], HMAC [11], DSS [12]).

6 Anonim engedélyezés

Az anonim engedélyezés során olyan módszerek kerülnek alkalmazásra, melyeket a PET-ek (*Privacy Enhancing Technologies*) [13] kategóriájába lehet besorolni.

6.1 Az anonim engedélyezés általános sémája

Ezek a technikák alapvetően a 4. ábrán bemutatott sémát követik:



4. ábra – Anonim engedélyezés általános sémája

- Az *előkészítő szakasz* során (itt az alany személyazonossága ismert) az alany az anonimitási hatósággal folytatott kommunikáció útján beszerzi a későbbiekben felhasznált anonimitási okmányokat (1) (2).
- A tényleges *anonim engedélyezés* során az alany a szolgáltató számára (és anonimitási szinttől függően az anonimitási hatóság számára is) anonim. Az engedélyezés során átadja az okmányokat a szolgáltatónak (3), aki azokat továbbítja az anonimitási hatóságnak (4). Amennyiben az okmányok megfelelőek és az alany jogosultságai a szolgáltatás teljesítését lehetővé teszik, úgy az anonimitási hatóság ezt jelzi a szolgáltatónak (5). Végül megtörténhet a szolgáltatás igénybevétele (6).

6.2 Anonimitási szintek

Az anonim engedélyezés során alkalmazható technikákat alapvetően két nagy csoportba lehet osztani:

- A *korlátozottan visszakövethető alany* szinten a rendszer két részrendszerre osztható [14]: az azonosított tartományban (*identity domain*) az alany személyazonossága ismert, míg az anonim tartományban (*pseudo domain*) az alany anonim. Az anonimitási hatóság feladata a két tartomány közötti átjárás felügyelete. A szolgáltatás igénybevétele az anonim tartományban történik, azonban bizonyos esetekben (pl. bűntény elkövetése esetén) az anonimitási hatóság utólag felfedheti a szolgáltató számára az addig anonim alany személyazonosságát.
- A *visszakövethetetlen alany* szinten a rendszer nem csak tértben, hanem időben is kettéválik: a két tartomány közötti átjárás egyirányúvá válik, csak az azonosított tartományból lehet az anonim tartományba átlépni, fordítva nem – így a szolgáltatás igénybevételétől már az anonimitási hatóság sem tudja az alany személyazonosságát megállapítani.

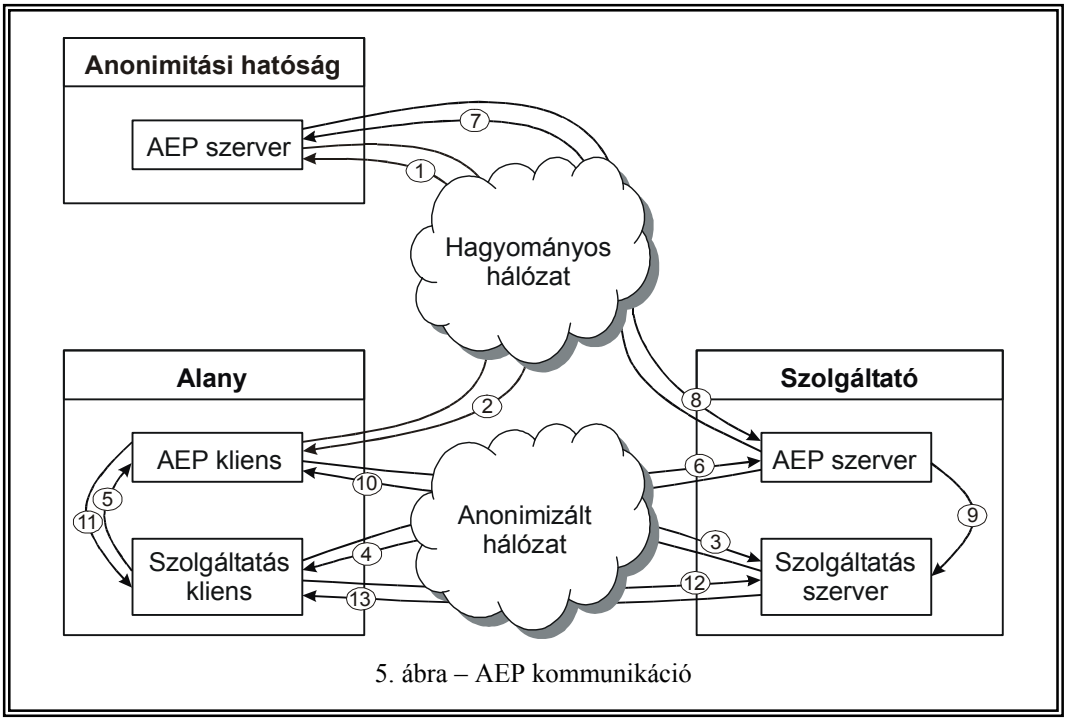
Az itt bemutatott anonimitási szinteket különböző módszerekkel lehet elérni: álnévvel biztosítható a korlátozottan visszakövethető alany szintje, míg a vak-aláírás módszerrel [3] a visszakövethetetlen alany szintje érhető el.

6.3 AEP – Anonymity Enhancing Protocol

AEP a 6.1 pontban ismertetett általános anonim engedélyezési sémát követve lehetőséget biztosít a 6.2 pontban bemutatott anonimitási szinteket megvalósító módszerek alkalmazására.

Legfontosabb tulajdonsága, hogy alapvetően egy keretrendszer, melyben tetszőleges anonim engedélyezési módszer megvalósítható, sőt ezek akár cserélhető *plug-in*ként is használhatóak a különböző igényeknek megfelelően.

A transzparens anonim átvitelre és a biztonsági réteg funkcióira építve AEP jelenleg egy XML-alapú kommunikáció során megvalósítja az anonim engedélyezési séma előkészítő és anonim engedélyező fázisait, valamint lehetőséget nyújt HTTP-re alapuló alkalmazások (tipikusan web-böngészés) számára a közös viszony kialakítására.



5. ábra – AEP kommunikáció

Az implementáció a következő lépéseket (lásd 5. ábra) tartalmazza:

- Az előkészítő szakasz során az alany beszerzi az anonimitási okmányokat az anonimitási hatóságtól (1) (2).
- Az anonim engedélyezés szakasza a szolgáltatás kérésével indul (3), ami után a szolgáltató felkéri az alanyt az engedélyezés megkezdésére (4). A szolgáltatás kliens (pl. böngésző) utasítja az AEP-klienst az engedélyezés megkezdésére (5). Az AEP-kliens átadja az anonimitási okmányokat a szolgáltatónak (6), aki azokat ellenőrizteti (7) (8). Amennyiben a jogosultságok megfelelőek, úgy megtörténhet a szolgáltatás (9). Erről a szolgáltató értesíti az alanyt (10), akinél az AEP-kliens elindítja (11) a szolgáltatás-kliensnél a szolgáltatás tényleges igénybevételét (12) (13).

A jelenlegi AEP implementáció platformfüggetlen JAVA alkalmazásként SQL alapú adattárolás mellett szabad szoftverként elérhető [15].

7 Összefoglalás

Az ismertetett általános célú biztonságos anonimitási architektúra egy olyan hálózati átviteli modell, mely ötvözi a kommunikációs biztonság területén elért eredményeket a különböző anonimitási módszerekkel. Az architektúra lehetőséget nyújt olyan alkalmazások megvalósításához, melyek a bevált kriptográfiai megoldásokra, valamint anonim átviteli és engedélyezési technikákra építve ezek funkcióit egységesen és megbízhatóan elérheti.

A továbbiakban az ismertetett architektúra elemezése mellett az anonim átvitel és engedélyezés módszereinek kutatása és a rendszerbe való integrálása látszik kívánatosnak.

Irodalomjegyzék

[1] A. O. Freier, P. Karlton, P. C. Kocher: *The SSL Protocol Version 3.0*, 1996.

[2] T. Dierks, C. Allen: *RFC 2246 – The TLS Protocol Version 1.0*, Certicom, 1999.

[3] D. Chaum: *Blind Unanticipated Signature Systems*, U.S.Patent 4 759 064, 1998.

[4] D. Chaum.: *Untraceable* Electronic *Mail, Return Addresses, and Digital Pseudonyms*, Communications of the ACM, volume 24, number 2, pp. 84-88, 1981.

[5] *Anonymizer.com – Online Privacy Services*, http://www.anonymizer.com

[6] G. Tóth: *Anonymity Enhancing Protocol*, diplomamunka, Siemens-díj 2002.

[7] *JAP – Anonymity & Privacy*, http://anon.inf.tu-dresden.de

[8] Reed, M., Syverson, P., Goldschlag, D.: *Anonymous Connections and Onion Routing*, IEEE Journal on Selected Areas in Communication Special Issue on Copyright and Privacy Protection, pp. 482-494, 1998.

[9] G. Tóth, Z. Hornák: *Megfigyelhető black-box csatorna forrásrejtő tulajdonsága*, Híradástechnika, 2003/5, pp. 41-44

[10] *FIPS 187 – Advanced Encryption Standard*, 2001.

[11] H. Krawczyk, M. Bellare, R. Canetti: *RFC 2104 – Keyed-Hashing for Message Authentication*, IBM, UCSD, 1997.

[12] *FIPS 186-2 – Digital Signature Standard*, 2000.

[13] I. Goldberg, D. Wagner, E. Brewer: *Privacy-enhancing technologies for the Internet*, University of California, Berkeley, 1997.

[14] R. Hes, J. Borking: *Privacy Enhancing Technologies – The Path to Anonymity*, Registratiekamer, 1998.

[15] *Team Monica Home* http://monica.sourceforge.net

[16] A. M. Froomkin: *Flood Conrol on the Information Ocean: Living with Anonymity, Digital Cash and Distributed Databases*, 1996.