Iulian Boldea, Cornel Sigmirean (Editors)
MULTICULTURAL REPRESENTATIONS. Literature and Discourse as Forms of Dialogue
Arhipelag XXI Press, Tîrgu Mureș, 2016
ISBN: 978-606-8624-16-7
Section: Social Sciences, Psychology, Sociology and Education Sciences

ABOUT SCHENGHEN AREA – AN EXPLORATORY STUDY

Bogdan Țigănoaia

Assist. Prof., PhD, Politehnica University of Bucharest

Abstract: This paper is an exploratory study about Schenghen area. Aspects such as the Schengen Information System - SIS, SIS architecture, data categories in SIS, data security in SIS, the National Computer System for Alerts - NCSA, SIRENE and public key infrastructure - PKI, electronic signature, digital certificate, timestamp, are presented. The paper ends with some final issues.

Keywords: SIS, Schenghen, SIRENE, PKI

1. Introducere – despre zona Schenghen

Punctul de plecare în scrierea prezentului articol îl reprezintă studierea mai multor surse bibliografice în domeniul Schenghen cum ar fi Strategia naţională de aderare la spaţiul Schengen – H.G. nr. 1314/2007, Convenţia de Aplicare a Acordului Schengen – CAAS, Planul de Acţiune Schengen – PAS [7], Broşura M.A.I. - Sistemul Informatic Schengen, precum și referința bibliografică [1].

La începutul anilor ’80, a demarat, la nivel european, o discuție în legatură cu importanța termenului **libertate de mișcare.** După discuţii îndelungate, Franţa, Luxemburg, Germania, Belgia şi Olanda au hotărât să creeze un spaţiu fără frontiere interne. Acordul între aceste state a fost semnat la 14 iunie 1985 în localitatea Schengen din Luxemburg. A urmat semnarea Convenţiei de Aplicare a Acordului Schengen (CAAS [6]), în data de 19 iunie 1990. A intrat în vigoare în 1995, eliminând controalele la frontierele interne ale statelor semnatare, creând o singură frontieră externă, unde controalele se desfăşoară conform unui set de reguli clare. Au fost stabilite reguli comune în materie de vize, migraţie, azil, precum şi măsuri referitoare la cooperarea poliţienească, judiciară sau vamală [2]. Principalele măsuri avute în vedere, în funcţie de fiecare domeniu al cooperării Schengen, sunt: controlul frontierelor, politica de vize, migraţia, azilul, cooperarea poliţieneasca, cooperarea judiciară, lupta impotriva drogurilor, arme de foc şi muniţii, Sistemul Informatic Schengen (SIS), protecţia datelor cu caracter personal [5]. Urmatoarele măsuri [2]:

• eliminarea controalelor la frontierele interne şi stabilirea unui set de reguli pentru trecerea frontierelor externe;
• separarea fluxurilor de pasageri în porturi şi aeroporturi;
• armonizarea regulilor referitoare la condiţiile de acordare a vizelor;

• stabilirea unor reguli pentru solicitanţii de azil;
• introducerea unor reguli referitoare la supravegherea şi urmărirea transfrontalieră pentru forţele de poliţie din statele Schengen;
• întărirea cooperării judiciare prin intermediul unui sistem rapid de extrădare şi implementare a deciziilor judecătoreşti;
• crearea Sistemului Informatic Schengen.
împreună cu Acordul Schengen, Convenţia de Aplicare a Acordului Schengen, deciziile şi declaraţiile adoptate de către Comitetul Executiv Schengen, precum şi protocoalele, acordurile de aderare şi legislaţia relevantă constituie ***acquis-ul Schengen.*** Initial, acquis-ul Schengen nu a facut parte din cadrul legislativ comunitar. Acest lucru s-a schimbat însa odată cu *semnarea Tratatului de la Amsterdam, în data de 2 octombrie 1997, intrat în vigoare la data de 1 mai 1999*. Un Protocol atașat Tratatului de la Amsterdam încorporează acquis-ul Schengen în cadrul legislativ și instituțional al Uniunii Europene.Începând cu acest moment, *acquis-ul Schengen face parte din legislația comunitară* [3].

Intrarea Bulgariei și României în spațiul european Schengen, spaţiu al justiţiei, libertăţii şi securităţii, în luna martie 2011, a fost oprită de opoziția unor state membre, precum Germania, Finlanda și Austria. În vara anului 2011 a intervenit modificarea treptată în raport cu intrarea României și Bulgariei a pozițiilor Germaniei, Austriei și Finlandei în sens favorabil. În iunie 2011 Parlamentul UE s-a pronunțat pentru intrarea României și Bulgariei în Spațiul Schengen, dar Consiliul Ministerial UE nu a acceptat opinia acestuia, cu motivația unor nemulțumiri exprimate de guvernele Olandei și Finlandei față de pretinse lacune în domeniul măsurilor anticorupție și combaterii crimelor organizate ce ar exista în Bulgaria și România [4]. In toamna anului 2011, Olanda s-a opus aderării celor două state la spațiul Schenghen, nuanțându-și reținerile dinainte. Există păreri la București, că opoziția oficială a Olandei față de intrarea Bulgariei și României ar veni de la confruntări politice interne existente în această țară membră a UE, și nu reliefează fondat realitatea politică din sud-estul Europei. Este evident că, dat fiind poziția geografică și mărimea teritorială a Olandei, această țară vest-europeană nu ar fi direct afectată de traficul de persoane din și spre Bulgaria și România, dacă politicienii olandezi (guvernul) ar fi și ei de acord cu intrarea celor două țări UE în Spațiul Schengen. România și Bulgaria sunt nemulțumite și intrigate de aceste poziții politice, ele argumentând că argumentele contra citate nu fac parte din criteriile de acceptare (condiții) în zona europeană Schengen, aplicate concret la intrarea altor state ale Uniunii Europene [4].

2. Sistemul Informatic Schenghen – SIS

A. Arhitectura SIS

Sistemul Informatic Schengen (SIS), reprezintă o bază de date electronică de interes poliţienesc care permite autorităţilor cu competente in domeniu să coopereze în vederea menţinerii securitatii pe teritoriul national al statelor din spatiul Schenghen. Informațiile sunt comunicate prin acest sistem, SIS.

Sistemul Informatic Schengen este alcătuit dintr-un sistem central C.SIS, care se află la Strasbourg, împreună cu părţile naţionale N.SIS aflate în fiecare stat membru Schengen. C.SIS şi părţile naţionale N.SIS comunică în vederea asigurării integrităţii datelor, prin schimburi online de informaţii. Semnalările incluse în C.SIS sunt acele alerte care vizează persoane sau obiecte şi care sunt de interes pentru toate statele membre Schengen. Schimbul suplimentar de informaţii se realizează prin intermediul birourilor SIRENE naţionale [1].

Arhitectura SIS este formată din [2]:

a) un sistem central („SIS II central") compus din:

- ✓ funcţie de suport tehnic (CS-SIS) care conţine o bază de date - baza de date SIS II
- ✓ interfaţă naţională uniformă (NI-SIS)

b) un sistem naţional (N.SIS II) în fiecare dintre statele membre, care constă în sistemele naţionale de date care comunică cu SIS II central. Un sistem N.SIS II poate conţine un fişier de date (o copie naţională) care să fie constituită din o copie completă sau parţială a bazei de date SIS II

c) infrastructură de comunicaţii între CS-SIS şi NI-SIS care asigură o reţea virtuală criptată consacrată datelor din SIS II şi schimbului de date între birourile SIRENE, în conformitate cu art. 7 alin. (2) din Decizia 533/2007

d) Austria asigură gestionarea unei baze de date de rezervă, aflata la Sankt Johann, în Pongau, care poate începe să funcţioneze în cazul defectării unităţii centrale de la Strasbourg

Arhitectura SIS II va permite [2]:

- ✓ interogarea directă în sistemul central – acest lucru oferă statelor membre posibilitatea de a renunţa la copia nţională
- ✓ statele membre pot păstra o copie a bazei de date centrale la nivel naţional, totală sau parţială

În figura 1, se poate observa arhitectura şi modul de funcţionare a SIS [1]

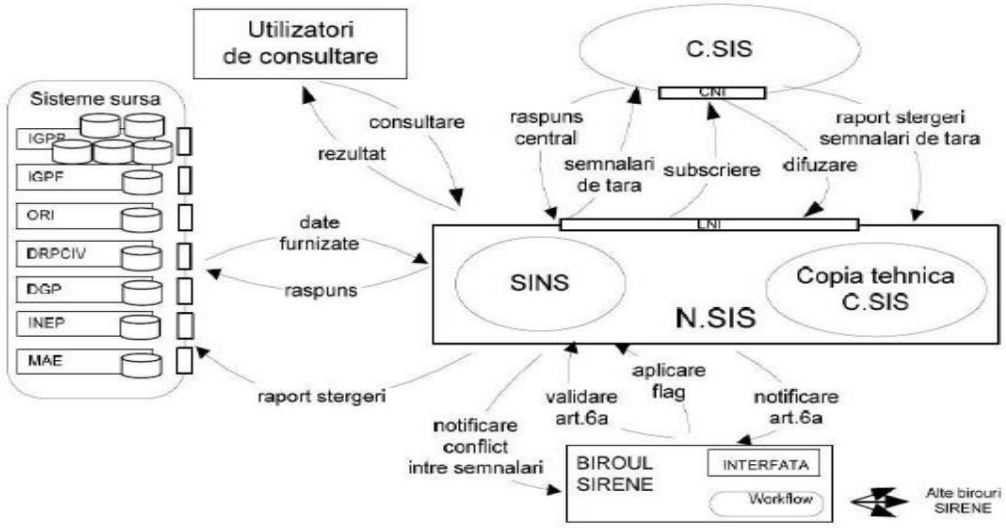

Figura 1: SIS

În urma vizitelor de evaluare, rapoartele pozitive ale experților internaționali confirmă că România îndeplinește toate cerințele din punct de vedere tehnic, decizia de aderare a țării noastre fiind una politică.

B. Categorii de date in SIS

Categoriile de date ce pot fi adăugate în SIS se referă atât la persoane cât şi la semnalări legate de obiecte. ***Exemple de semnalari legate de persoane:***

a) Persoane care fac obiectul unor proceduri de extrădare sau de predare în baza unui mandat european de arestare (art. 95 CAAS)
b) Persoane străine împotriva cărora s-a dispus măsura nepermiterii intrării şi străinii împotriva cărora a fost dispusă măsura expulzării, returnării sau împotriva cărora a fost dispusă o măsură de îndepărtare de pe teritoriul României (art. 96 CAAS)
c) Persoane dispărute sau care, în interesul propriei protecţii sau pentru prevenirea ameninţărilor, trebuie plasate în mod provizoriu într-un loc sigur la cererea autorităţii competente sau a autorităţii judiciare competente (art. 97 CAAS)
d) Persoane citate pentru a se prezenta în faţa autorităţilor judiciare în cadrul unei proceduri penale care antrenează răspunderea cu privire la fapte pentru care au fost urmărite sau persoanele cărora trebuie să li se comunice o hotărâre penală (art. 98 CAAS)
e) Persoane care fac obiectul supravegherii discrete sau controlului specific (art. 99 CAAS)

Exemple de semnalări referitoare la obiecte:

a) Ambarcaţiuni, aeronave

b) Echipamente industriale, motoare exterioare, containere
c) Vehiculele cu motor, cu o capacitate cilindrică mai mare de 50 cm^3 , care au fost furate, tăinuite sau pierdute (art. 100 lit. a CAAS)
d) Documentele furate, tăinuite sau pierdute care privesc vehicule (art. 100 lit. f CAAS)
e) Plăcile cu numere de înmatriculare furate, tăinuite sau pierdute (art. 100 lit. f CAAS)
f) Remorcile şi rulotele cu o greutate netă mai mare de 750 kg, care au fost furate, tăinuite sau pierdute (art. 100 lit. b CAAS)
g) Armele letale furate, tăinuite sau pierdute (art. 100 lit. c CAAS)
h) Date privind înscrisuri oficiale necompletate, care au fost furate, tăinuite sau pierdute (art. 100 lit. d CAAS)
i) documentele de identitate eliberate (paşapoarte, cărţi de identitate, permise de conducere) care au fost furate, însuşite ilegal sau pierdute (art. 100 lit. e CAAS)
j) Bancnotele sau titlurile de valoare furate, tăinuite sau pierdute (art. 100 lit. g CAAS)

Accesul la date conţinute în SIS este rezervat în exclusivitate autorităţilor competente:

C. Securitatea datelor in SIS

Legat de nivelul de securitate, statele membre sunt obligate să asigure un nivel cel puţin egal cu cel precizat în Convenţia Consiliului Europei privind protecţia persoanelor împotriva procesării automate a datelor personale din 29 ianuarie 1981 şi în Recomandarea nr. R (87) 15 a Comitetului Miniştrilor Consiliului Europei, din 17 septembrie 1987 [2]. Datele personale din SIS se pot menţine atâta timp cât sunt necesare dar nu mai mult de 3 ani de la data introducerii lor. Persoanele pot solicita accesul la datele personale conţinute în SIS, conform art. 109 din CAAS. Acest drept se exercită în conformitate cu legislaţia naţională a statului faţă de care se invocă accesul la date personale [1].

a. Infrastructura cu chei publice

Pe lângă dezvoltarea infrastructurii tehnice şi de comunicaţii pentru accesul autorităţilor competente la bazele de date (art. 101 din Convenţia Schengen), un alt obiectiv asumat de România este şi extinderea infrastructurii cu chei publice - PKI la nivelul sistemelor informatice sectoriale din cadrul MAI [1]. Infrastructura de chei publice [8] (PKI) este un ansamblu de echipamente, programe, oameni, proceduri şi politici care utilizează semnătura digitală pentru a facilita o asociere verificabilă între componenta publică a unei chei asimetrice (cheia publică) şi entitatea căreia îi apartine (persoană, organizaţie). Funcţiile de bază ale unui sistem PKI sunt: ***certificarea*** – certificatul digital conține cheia publică a deținătorului și informații de identificare, ***validarea*** – certificatelor digitale online sau offline, în orice moment și ***revocarea*** – invalidarea certificatelor digitale.

i. Semnătura electronică

Semnătura electronică reprezintă date în formă electronică, care sunt atașate sau logic asociate cu alte date în formă electronică și care servesc ca metodă de identificare [art. 4 pct. 3 din Legea 455/2001]. Semnătura electronică asigura autentificarea, integritatea și nonrepudierea datelor semnate. Mai multe informații despre semnătura electronică găsiți în [1].

ii. Certificatul digital

Un ***certificat de cheie publică (certificat digital)*** e o structură de date folosită pentru a se putea asocia, în mod sigur, o cheie publică cu nişte atribute de utilizator. Atributele pot fi, de exemplu, informaţii de autentificare (nume, adresă) sau informaţii de autorizare (de acces la o sursă). Certificatul face legătura între o cheie publică şi un nume [9].

iii. Marca temporală– colecție de date în formă electronică, atașată în mod unic

unui document electronic; ea certifică faptul că anumite date în formă electronică au fost prezentate la un moment de timp determinat furnizorului de servicii de marcare temporală (Legea 451 din 2004)

De ce este necesară marca temporală? Non–repudierea semnăturii electronice pe termen lung

Scenariu:

19.09.2016

- Bogdan semnează electronic un document prin care se obligă să facă o plată către George în data de 01.10.2016
- Andrei verifică semnătura electronică a lui Bogdan de pe document si verificarea este in regula.

23.09.2016

- Bogdan merge la Autoritatea de Certificare si revocă certificatul motivând că a pierdut token-ul criptografic
- Autoritatea de certificare revocă certificatul si publică lista de certificate revocate în care apare data revocării 23.09.2016 pentru certificate

01.10.2016

- Bogdan nu face plata
- Andrei îi prezintă documentul semnat electronic de Bogdan
- Bogdan neagă faptul că a semnat el documentul, deoarece el a pierdut token-ul si certificatul său a fost revocat
- Andrei îi arată lista de certificate revocate din care rezultă că revocarea a avut loc după semnarea documentului de către Bogdan, dată la care certificatul era valid
- Bogdan sustine contrariul

Concluzie: inexistenta unui moment de timp, garantat de un furnizor de marcare temporală, asociat cu semnătura electronică face greoaie, chiar imposibilă validarea unei semnături electronice ulterior.

D. SIRENE

Biroul Sirene are ca principal rol specific responsabilitatea furnizării de informaţii în timp real utilizatorului final, cu posibilitatea completării informaţiei cu date suplimentare, în cel mai scurt timp [2]. Biroul SIRENE funcţionează în regim 24/7 şi reprezintă interfaţa umană a Sistemului Informatic Schengen, reprezentând totodată un punct important de legătură cu celelalte state membre. Biroul SIRENE a fost înfiinţat în România în august 2004 şi a fost inaugurat în 16 septembrie 2010, făcând parte din cadrul Centrului de Cooperare Poliţienească Internaţională al Inspectoratului General al Poliţiei Române [1].

E. Sistemul Informatic Naţional De Semnalări – SINS

SINS va gestiona semnalările emise de statul român, iar împreună cu copia naţională a CS.SIS, va forma sistemul N.SIS pentru România. SINS va conţine toate semnalările naţionale (de tip Schengen sau non-Schengen) emise de autorităţile române competente şi pot fi de interes Schengen (cele care vor alimenta CS.SIS II) şi de interes non-Schengen (cele de interes doar pe teritoriul naţional). Acest sistem va fi pus la dispoziţia tuturor instituţiilor în vederea consultării şi/sau actualizării în funcţie de competenţele legale, în conformitate cu prevederile CAAS [2].

3. Aspecte finale

În contextul viitoarei aderări a Romaniei la spaţiul de liberă circulaţie, lucrarea este un studiu exploratoriu despre zona Schenghen, fiind abordate subiecte precum SIS, SINS, protecția datelor în SIS, SIRENE, infrastructura cu chei publice - PKI.

BIBLIOGRAPHY

[1] Adrian Iacob, Bogdan Tiganoaia, *Sistemul informatic Schengen şi infrastructura cu chei publice la nivelul M.A.I. În contextul aderării României la spaţiul Schengen,* Simpozionul Ştiinţific „Aderarea României la Spaţiul Schengen - de la deziderat la realitate”, Academia de Politie “Al. Ioan Cuza” Bucuresti, 2011.
[2] Broşura M.A.I.- Sistemul Informatic Schengen, https://www.politiadefrontiera.ro/files/docu/1460139101184-sis.pdf
[3] http://www.schengen.mai.gov.ro/
[4] https://ro.wikipedia.org/wiki/Spa%C8%9Biul_Schengen
[5] H.G. nr.1314/2007 privind Strategia naţională de aderare la spaţiul Schengen
[6] Convenţia de Aplicare a Acordului Schengen - CAAS
[7] Planul de Acţiune Schengen - PAS 2009
[8] Politica şi arhitectura securităţii datelor in Internet, Gabriel Neagu, 2009
[9] Prof. univ.dr. Constantin Popescu - Departamentul de Matematica si Informatica, http://webhost.uoradea.ro/cpopescu/curs-si.html