

# АРХИТЕКТУРА НА СИСТЕМАТА ЗА ИНФОРМАЦИОННА СИГУРНОСТ В ПРОЕКТА INDECT

Николай Т. Стоянов

## *INDECT – INFORMATION SECURITY SYSTEM ARCHITECTURE*

*Nikolai T Stoianov*

**Abstract:** *This paper presents one idea for creating information security system.. This system is part from European project “Intelligent information system supporting observation, searching and detection for security of citizens in urban environment – INDECT”. The architecture of the system are explained.*

**Keywords:** *information security, computer security, cryptography, cryptographic software, online data protection.*

## ЕВРОПЕЙСКИ ПРОЕКТ INDECT – ЦЕЛИ И ЗАДАЧИ

Сигурността на гражданите е от първостепенно значение. Постоянното увеличаване на тяхната сигурност и защита трябва да е една от стратегическите цели на всяко правителство и неговите агенции и служби като полиция, пожарна, местна администрация и др. [2, 6].

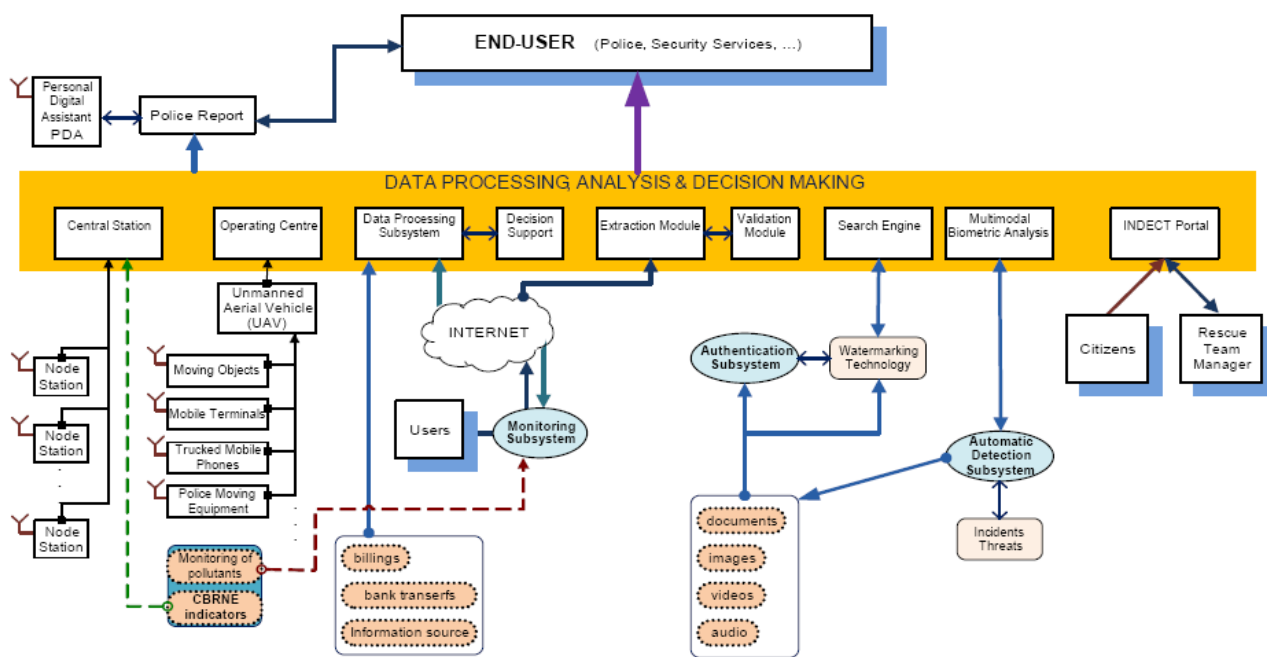
Основните цели на европейския проект “Intelligent information system supporting observation, searching and detection for security of citizens in urban environment – INDECT” са [3, 4, 5]:

- Разработване на платформа за регистриране и обмен на оперативна информация, съхранение на мултимедийно съдържание, интелигентно търсене, автоматично разкриване на заплахи и разпознаване на необичайни поведения или насилие.
- Разработване на нов тип „машина за търсене”, която комбинира директно търсене на изображения и видео информация базирайки се на т.нар. „водни занаци”;
- Разработване на набор от техники, чрез които да може да се наблюдава Интернет пространството, да се анализира активността на потребителите на Интернет и да се открива извършването на криминални действия и/или заплахи.

Очакваните резултати които трябва да се постигнат с внедряването на проекта INDECT са [3, 4, 5]:

- Реализация на опитна установка в различни европейски градове и демонстрация на работата на прототип състоящ се от 15 възела;
- Имплементация на разпределена компютърна система имаща възможност за съхранение и обмен на информация и поддържаща интелигентно търсене;
- Конструирание на фамилия от прототипи на мобилни устройства използвани за следене на подвижни обекти;
- Конструирание на машина за търсене, която да поддържа бързо откриване на хора и документи базирано на т.нар. „воден знак“;
- Проектиране на агенти за автоматично наблюдение на публични ресурси (web сайтове, форуми, UseNet групи, файлови сървери, p2p мрежи, индивидуални компютри и др.).

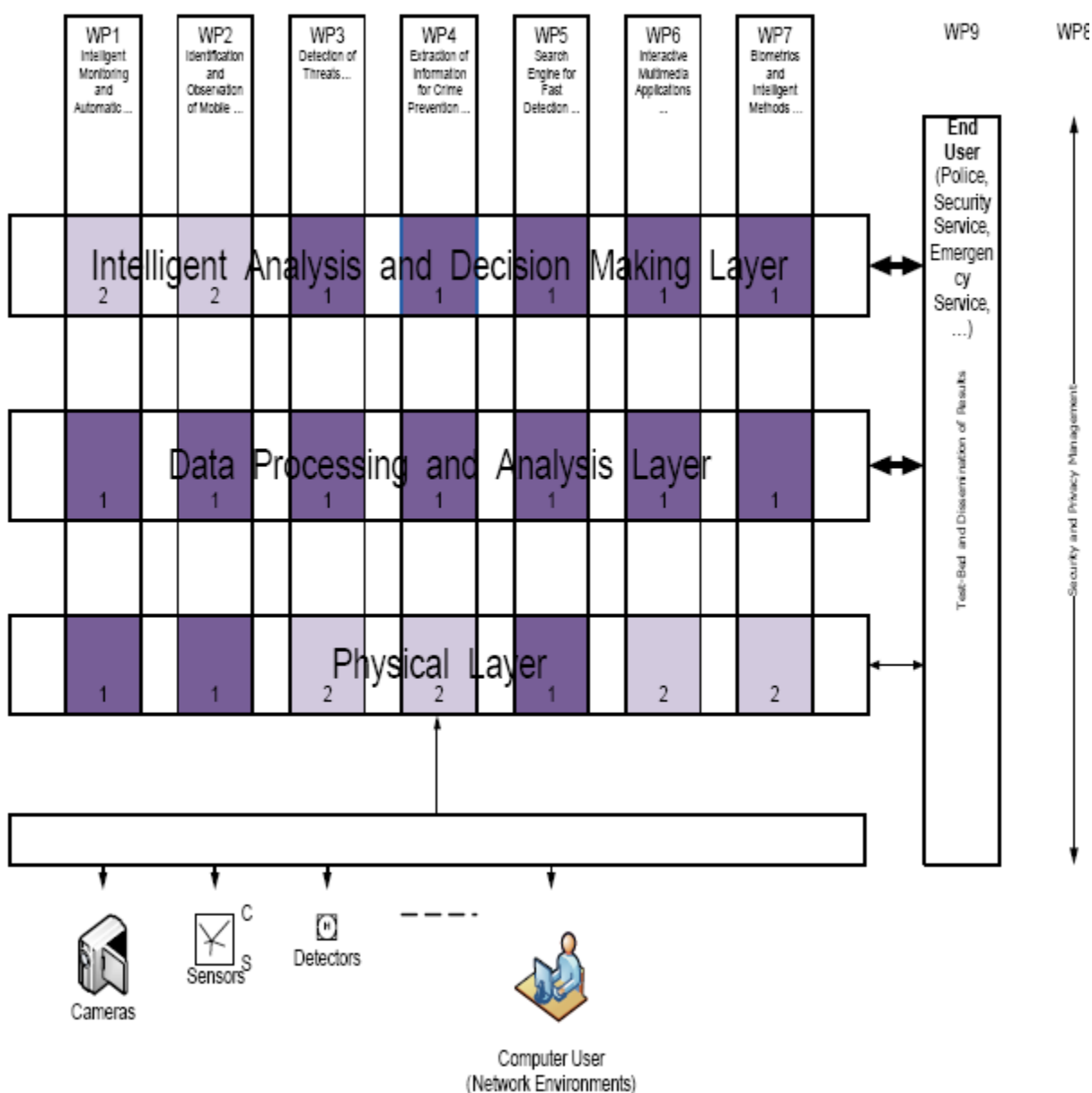
На фигура 1 е показана базовата диаграма на проекта INDECT и връзките между отделните негови елементи.



Фиг. 1. Базова диаграма на INDECT [3]

Сигурността става все по-важен елемент за всички правителства и организации. Защитата на енергийните източници и преносните системи, комуникационната инфраструктура, конферентните центрове, летища и на градове с голямо движение на хора е от първоатепенно значение. На практика всяко претъпкано място е опасно и риска трябва да бъде контролиран и управляван колкото е възможно по-добре [1]. Чрез контрола на достъпа до обществени места се очакваше да се минимизират заплахите от опасни актове на насилие. Един от най-ефективните начини за намаляване на риска е чрез

прилагане на методи и механизми за активно наблюдение. Това от своя страна налага наличието на интелигентни системи за търсене и разпознаване, изграждане на информационна инфраструктура в градовете и наличие на активни и пасивни сензори, датчици и устройства за наблюдение. Всички изброени методи, техники и механизми се очаква да бъдат интегрирани в проекта INDECT. На фигура 2 е показана архитектурата на процесите между различните направления за осигуряване на сигурността и защитата на хората. Задача 8 (WP8) има за цел да защити информацията в така създаваната и работеща сложна система за откриване, наблюдение и контрол.



Фиг. 2. Архитектура на процесите в проекта INDECT [3]

За постигане на основните цели в проекта, той се разделя на следните основни елемента (фиг. 2) [3]:

- Дефиниране и демонстрация на архитектура за мултимедиино наблюдение.
- Идентификация на изискванията и предложение за решение за аудио- и видеооборудване, което да може да бъде експлоатирано както в статични (сгради), така и в мобилни (автомобили, влакове и др.) платформи.
- Изучаване на опита и изграждане на мултисензорна система за наблюдение.
- Разработване и изграждане на комплексна многомодулна система за биометрични процедури с цел проверка и/или разпознаване на хора.
- Разработване на методи и процедури за автоматизирано създаване на релации между информация получавана от различни по тип и вид източници и създаването на метаданни за тази информация.

## **АРХИТЕКТУРА НА СИСТЕМАТА ЗА ИНФОРМАЦИОННА СИГУРНОСТ**

Системата за информационна сигурност на проекта INDECT трябва да има следните възможности:

- Еднозначна идентификация и автентификация;
  - Методи за криптографска защита на информацията;
  - Съхранение на данните в един или няколко масива (RAID)
  - Централизирано управление на потребителите;
  - Централизирано управление на политиката за сигурност в системата;
  - Мониторинг и контрол на извършените действия;
  - Разделение на потребителите по функционални групи;
  - Невъзможност за отказ от авторство
- и др.

За постигане на тези изисквания е нецелесъобразно да се изгради единна система за информационна сигурност за всички потребители (администратори, полицейски служители и др.) Имайки предвид, че системите, изградени по проекта, са както стационарни, така и мобилни, от друга страна, достъпът до информация е възможно да бъде както web базиран, така и със специални приложения. Авторът счита, че една разпределена система за сигурност на информацията би била по гъвкава, оперативна и лесна за администриране.

Подобна система функционално може да се декомпозира на следните елементи:

- център за генериране и разпределение на криптографски ключове и параметри;
- криптографски приложения;
- криптографски комуникационни устройства;
- център за управление на криптографски устройства;
- подсистема идентификация и автентификация на потребители, услуги и устройства;
- подсистема за изграждане и управление на инфраструктура с публичен ключ (PKI);
- подсистема за наблюдение и управление на информационната сигурност;
- подсистема за възстановяване след бедствия и аварии;
- подсистема за връзка с други подобни системи (шлюзове или gateways).

От друга страна, системата може да се раздели по признака къде се експлоатира:

- Мобилни потребители (автомобили на полицейски служители);
- Стационарни потребители (служители в полицейски управления);
- Администратори на системите в проекта INDECT;
- Други (външни за полицейските управления) потребители.

Независимо от начина на декомпозиция на системата за сигурност на информацията тя трябва да се разглежда като единно цяло. Нийната цялостност трябва да не противоречи както на основните изисквания на другите системи в проекта, така и на необходимостта от единен начин на работа на всички потребители на проекта INDECT.

## **ЗАКЛЮЧЕНИЕ**

Необходимостта от наблюдение на градските пространства е безспорна. С навлизането на информационните технологии във всички сфери на обществения живот ни откриват нови хоризонти за откриване, реагиране и борба с противообществените прояви. С изграждането на протоипите по проекта INDECT Европейският съюз ще постави недвусмислено въпроса за нулева толерантност към такъв тип действия в градовете от ЕС. Информационната сигурност и защитата на информацията обменяна от всички детектори, камери, оператори и бази данни в системата на проекта INDECT е от

първостепенно значение. Гарантирането на тайната (конфиденциалността), цялостността (интегритета), наличността, идентификацията и автентификацията и невъзможността за отказ от авторство са основните въпроси която всяка предложена и реализирана архитектура на система за информационна сигурност третира.

## ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1. Стоянов Н., А. Генчев, Р. Илиев, Някой аспекти при анализа на риска в информационни системи за сигурност и отбрана, Международна научна конференция, Шуменски университет, Шумен, 2008.
2. Целков В., Н. Стоянов, Защитени криптографски приложения в компютърните системи и мрежи, София, Нова Звезда, 2009, ISBN: 978-954-8933-20-9.
3. Description of Work (DoW) of the INDECT project, SEVENTH FRAMEWORK PROGRAMME THEME 10 Security.
4. [http://cordis.europa.eu/fetch?CALLER=FP7\\_PROJ\\_EN](http://cordis.europa.eu/fetch?CALLER=FP7_PROJ_EN).
5. <http://www.indect-project.eu/>.
6. Stoianov N., One new look about information security aspects, Годишник на Института за перспективни изследвания за отбрана, ВА “Г. С. Раковски”, София, 2008.