EU-ACT
EU Action Against Drugs and Organised Crime

FIIAPP
COOPERACIÓN ESPAÑOLA

Technical and functional requirements- Electronic System of Analysis and Coordination of Information at the Ministry of Interior Affairs of the Kyrgyz Republic.

1 Index

1 Description of the project

M.A.K.S. will be a web-based software application in which all information about police investigations will be stored and it will facilitate the coordination between all units and police stations in the country. Also, the software will allow the analytical monitoring of the generated information, being a tool to held and support operative groups and their investigations.

2 Aims to be covered by M.A.K.S.

The main goal of this software must be the recording and coordination of all investigations in Kyrgyzstan, being a referential point of their data with different levels of security in regard to the access to the information set on them.

The Electronic System of Analysis and Information Coordination must cover the following current needs:

1. Allowing better analysis of available information and discover crossed information among related investigations.
2. Getting a centralized database, capable of being accessed from any Police Stations or Units independently of its geographical settlement.
3. Reducing the time spent on communications and administrative procedures.
4. Reducing paper work, human error, repetitions of work and redundancies, and making easier the collection of data.
5. Impose the same methodology for collection, recording and handling of information to all members of the MoI, avoiding gaps, mistrust and conflicts
6. Methodology of M.A.K.S. coordination has being world-widely tested and used, so on that way they will be avoided errors previously made by another countries, learning from their experience.
7. Creation of a standard mechanism to facilitate the exchange of information.
8. Make possible that two units will work on the same investigation, they will conduct independently from each other the investigation or they can work together.
9. Automatic system for finding coincidences in the investigations. Processing all possible conflicts and cooperation between groups.
10. Registration, control and coordination of the investigations and suspects.
11. Getting better capabilities of reporting for decision making.
12. Adoption of effective policy and operational measure in compliance with international human rights and rule of law.
    + Ensure the confidentiality and protection of personal data stored.
    + Control over accesses to the database.
    + Avoid malicious changes/modifications in the database.
13. Elimination of minor or local databases, partial, amateur made tools, or departmental solutions with unification of those current systems.
14. Produce statistical information and external reports.
15. Facilitate predictive analysis

3 Scope of work. Technical features.

1. Accomplishment of TUNDUK standards to fit into the Republican tendencies of software development systems for public administrations.
2. Fulfilment of Normative and Standard procedures from European Union about information management.
3. Protections of data. The communications will be done in an encrypted way.
4. Control over accesses to the databases or changes/modifications made. Auditing capabilities.
5. Generation of statistical information and external reports.
6. Software and exposed services must run on Windows Server 2012 to Windows Server 2019 over IIS
7. Database must be done in SQL Server with standard queries cross-compatible with versions from SQL Server 2012 to SQL Server 2019.
8. Developing language for back-end must be with preference, Microsoft C# .NET and/or PHP.
9. MAKS should be created like a web app.
10. Handling interface must be done accomplishing the standards of HTML 5 with CSS 3
11. Libraries of 3rd parts must be avoided. Server functions must be done only with the capabilities of the programming language chosen, and presentation functions on the interface must be done also, and only, with the standard functions of HTML 5, CSS 3 and standards of natural JavaScript, without the help of any other framework to avoid problems of further maintenance of the technology used or unexpected deprecations changes or incompatibilities coming from external collaborative collectives.
12. Main functions of current software “Portrait” must be assumed into the new MAKS and current data there must be migrated in all possible cases into the new system letting the current “Portrait” and the even older “Taistous” software just for consultative purposes. See appendix I about “Portrait” for extended details.
13. Multilanguage Frontend (Interface in English, Russian and Kyrgyz)
14. Data Encryption Features and compliance with International standards of security, control and management of sensible and personal information. Minimum encryption capability would be 3-DES or stronger.
15. Interface and functionalities must be accessed through light components (Web browser) using secured web services to access to the main app site server.
16. App and databases must be capable to be in different servers if the case, to allow future growth of the system.
17. No “business logic” procedures or algorithms must be kept into the database. All logic must relay in the software to be developed, keeping the database clean and free of code, just as a repository of relational information.
18. The MAKS system must be self-sufficient for its expected functions, but it must be also ready to export information to exchange it with other systems or to elaborate reports of Intelligence. A way to export information to IBM i2 must be provided.

4 Scope of Work: Software components.

The system to cover the mentioned aims, must contain the following software components.

For more extended detail, see Appendix 2 about MAKS.

4.1 Administration

Only accessible by OAD headquarters. With the following functions:

1. Creation of new units.
2. Management (create, edit, activate, disactivate) of users with management of levels of security and permissions.
3. Auditory with codified certification. Auditing capabilities.
4. Limits of coincidences to generate coordination
5. Encrypted passwords

4.2 Repository of Information

Divided in 2 big databases, modules or repositories of information:

4.2.1 Investigation

Module containing all data of the investigations, past or present.

Functions to handle it must contain information to handle

1. The data of the investigation itself.
2. History of investigations.
3. Organized crime.
4. Investigation management.
5. Documents and related files
6. Collaborations
7. People and all personal data capable of being kept as for entities module.
8. Any other data as detailed in appendix 2.
9. Operational data of police interest.
10. Hierarchical storage of information divided in Main level, Central level, Local level and District level.

4.2.2 Identities

Module to keep information about entities (individuals, groups or juridical structures such as companies) involved in an investigation or arrested.

Must contain the following functions:

1. Search engine by individual fields or combined group of them being capable to keep some parameter or group of parameters as a filter. It should also export reports with the results of a search. Search scope must be only in within the scope of the user.
2. Add or modify information manually.
3. Add or modify information automatically through a template.

4. Linking or putting entities in relation among them. Creation of relationships.
5. To be kept all data of people as it is described in details for MAKS (appendix 2) and as described in details of PORTRAIT (appendix 1) for their assimilation by the migration of data.

4.3 Coordination

Module with 3 main functionalities.

4.3.1 Create and manage all possible coordinations produced.

1. Coordinations must be different according to the profile of the user and his level of access and scope of work.
2. All crosses, positive matches, and all process of coordination and resolution of conflicts must be also kept.

4.3.2 Allow the user to find information out of his unit or structure.

This function will show the power of having all information in one system. Then the crossovers are produced.

With the coordination module, searches should happen in all possible scope of matches and all levels, to provide the good coincidences, finding of unexpected links and to provide the good information in coordination and documents of it for each level of access or scope of the different users.

4.3.3 Search Engine of Coordination

It should allow searches in the whole database system. Here search engine can be manual or automatic when making the coordination of investigations.

The system must distinguish between “crosses” and “connections”.

4.4 Module of face recognition

Portrait contains a module of dace recognition which is not providing any accuracy in the matching. In order to fully absorb all functions of Portrait, MAKS must have also a module of facial recognition, but with much better matching than the current one.

As requirements for this module:

1. Facial parameters must not be set manually as it happens now. Images should be processed automatically upon insertion of them into the system, to attach to them the geometrical structure that will be used for recognition.
2. Main recognizant algorithm must contain a workable level of artificial intelligence.
3. Trigonometrical parameters between key face point and angular relations must be developed.

4. Not only key points as now but also angles of the faces must be taken in mind to avoid bad matching. Lighting or distance of the faces must not affect negatively in the face recognition. Descriptions and special features of each person should be taken in mind too for purposes of searching matches in the pairs photo-individual and helping or feeding the artificial intelligence behind.
5. For extended details about the current way of working of the system of Face Recognition of Portrait, appendix 1 must be checked.

5 Scope of Work: Methodology

1. To achieve the success of development in time-manner, the developing company should apply RAD methodology.
2. Architecture of development must be server-light client oriented, with clear separation Model-View-Controller where it could be applied.
3. Project methodology must include detailed work plan, chronology, reports, and partial deliveries, same as periodical control meetings with all the counterparts.
4. Plans of testing must be included for each software delivery and validated by the responsible staff of the MoI or the correspondent police or intelligence units.

6 Scope of Work: Migrations

Current data stored on Portrait and Taisontos existing tools must be migrated into the new system. Normalization of data to fit in the current system will be assumed by the developer/implementer firm.

The elected company must carry the absorption/migration of current data under the following parameters:

For Portrait

- Current database size is about 800 Gb.
- Expected volume of tables: About 100 service objects, about 30-50 tables, about 7 million registries.
- Current technology of database: Oracle 11.

For Taitous

- Current database size about 2,78 Gb information.
- Around 30 table objects in the database.
- Current technology of database SQL Server.

This might imply the intervention of a database specialist and such task can last from 1 to 2 months, and it might be prepared coordinately with the new database to be developed for MAKS.

Whatever electable offer must assume and perform these migrations.

7 Scope of Work: Training of staff

The developer must provide detailed manuals of use of the system in digital format.

The MoI will select the staff to be trained in the use of the system, and the provider must organize and give an adequate training with practical workshops. Training materials and manuals will be given to the participants in the workshop.

Staff subject of being trained is potentially 70 officers.

8 Scope of Work: Deployment

The system must be deployed for the beneficiary after being developed.

1. The system will be considered as deployed when all tests will be satisfactory, all possible data to be migrated will be already into the system, and units can start working with it satisfactory.
2. Deployment cannot be considered as finished if training of staff is not done. Workshops for those training must be conducted by the developing company, and also documentation for the final users must be ready and delivered in digital form.
3. Both, deployment period and the project itself will be considered finished when, after the previously mentioned subjects, a document with the strategy for implementation for all country will be delivered, containing the aims, deadlines, activities, risks and anti-risk measures, and recommendations.

9 Assumptions

1. MoI as beneficiary of this project and interested part, will provide to the developer company with current reports and forms, and access to existing data, database structure or current tools. Same, they should provide collaboration if requested, for solving doubts or giving information and explanations that can be useful for tuning or developing the required features, or to model the processes, functions or the algorithmic properly and accordingly with the needs.
2. MoI will provide the needed server for the software and will allow remote access to it for the developing agency during project developing time or for maintenance tasks. Requirements of hardware for this purpose are 256 Gb RAM, and 20 Tb of storage in hard disks, with minimum 2 processors, 2 cores, speed higher than 2 GHz, server technology, with Windows Server minimum version 2012. MoI will host and maintain this machine.

10 Generalities

1. The FIIAPP mission in Kyrgyzstan will coordinate the project being free for making any supervision or checking of works when it will be considered.
2. The consultant or selected company must propose incremental steps dividing the project into phases.
3. On every phase, it will be a delivery or report to be checked by the coordination office of FIIAPP in cooperation with the beneficiary of the project, the MoI.
4. The matching of project features will be checked by a specialist from FIIAPPP for their approval.
5. Approvals of the counterparts will be required for closing a phase.
6. Next phases of the project cannot start if the previous phase is not closed.

7. Final system on work, after development and deployment, must accomplish the aims for this project settled in point 2.

11 Deliverables

- Inception report (2 weeks after starting).
- Monthly report about the jobs done and the accomplishment of working plan (each month from the starting of the project).
- Document of technical requirements + Functional Analysis (1.5 months from the start of the project).
- Technical analysis (3 months from the starting).
- Installable files of the software (maximum 8 months from the starting). Manual of operation of the software developed must be included in this delivery.
- Report of training + report of data migration + strategy for country implementation + final report (maximum 11 months from the starting).

12 Appendix 1: About “Portrait”.

Nowadays there are 2 applications in the MoI with their corresponding databases, known as “Portrait” and “Taistous” being this last one older than the other and now just used for consulting historical data.

Portrait is mostly a database of people arrested or involved in some investigation. It is manually fed by the Operative Analysis Department with information coming monthly from the investigation groups instead of being fed directly from them. This is slow, inefficient and it is not ensuring that all information will appear properly or in a timely manner.

Jointly with many relevant data about the people involved in investigations or those arrested, it has the feature of having a very basic module of face recognition, which has been also proved as very inefficient and rarely matching correctly.

12.1 Details of software “Portrait” for integrations and migrations.

This software is used for keeping information about identities and making face recognition. It was provided from a similar need in Russia through OSCE program, because it is needed for their project called “Safety City”.

But they didn’t used it like it was given. It was adapted (somehow tailored) to their local needs and circumstances. The “tailor” who adapted it, was a Russian man. He was in the charge of adapting it to the needs of MVD.

Portrait is working under Oracle 11 and contains 2 databases.

It just allows to fast identify people by their photo.

Regions have the full access to the software, so it is accessible by all ODB and GOM (City Department of Police) departments.

Jointly with the photo, there are general data of the person, such as where he was born, where he lives, physical and personal details, mobile phone, family data, citizen ID, citizen driving licenses… The set of data which can be kept is really very detailed and complete.

As Portrait is keeping the information about the detained or arrested people, the input of the information is happening after the crime is done. It is only updated every 3 months, so this delay is a problem for the analytical or investigation purposes. Crime move quicker than administration.

Nowadays the system Portrait it has about 6.7 million registries distributed among 30 tables in the database, which has in total about 100 service objects.

Currently it means a size in database about 800 Gb.

One good key point is that they have access to the source code, so they can reprogram it if needed or create new screens and fields.

It is a desktop-based software. The screens of the system are accessible by tabs. Now let´s focus in the detail of the information contained on this system with the detail of every of the tabs:

Tab Face

- Entity, office or department which introduced the information
- Person who introduced the information
- Date of input
- Several photos. Not limited in number of photos.
- Number of social security (PIN or INN)
- Place of birth
- Country
- Oblast
- Rayon
- Village
- Education
- Place of education
- Specialization
- Name
- Family name (Surname)
- Middle name
- Birthday
- Sex (gender)
- Nationality (limited to 3 nationalities)
- Group of blood.
- Nickname / alias / last date of it (they only have one field for this)
- Citizenship (People can have more than one citizenship)
- Family status (civil status)

Tab Credentials

- Category of crime or reason to be there. (Relation of the person with the case or type of offense)
- Case: Article of code in the legislation codex. (They have all the different legislation codex in a list. Administrative, labor, and criminal codes).
- Notes
- Date of registration
- Short description of the crime/offense
- Region who put
- Person who put
- Place (After he goes jailed)
- Time of arresting
- Time of release from prison
- Date of coming into prison
- If he was previously convicted and article´s number (Several cases can be)
- OBD (Which region police department they entered the information)
- Department into the police station.

Now they are adding the previous crime history of a person because in IT department they introduce it from tribunals but only for statistical purposes, not for operative ones.

Tab List (list of people)

It appears a list of people as the result of a search given. They face really slow searches. Meaning 5 or 10 minutes and upper. The results delay a lot to appear.

Tab Face Recognition (Albon Gabi)

It sets or modify recognition points in the photos. It also handles the several photos the system allows.

Recognition happens if a set of points in a lineal array are adjusted to the real photo. Having in mind that the array (about 9 points in a lineal connection to be dragged manually when the photo appears) is not keeping angular information between related physical features of the photo and that the photos themselves are quite different in size and format, and that no trigonometrical features or analysis nor 3D matrix points are applied, it is not any real facial recognition algorithm and it is really useless to identify a person.

In a test we made for recognition of a suspect from a given photo, the system gave about 300 different people with absolutely different physical appearance than from the testing photo given. And no one of them was the suspect, indeed.

So, the final conclusion is that such a method is fully useless for purposes of face recognition. It is not even filtering by race or prominent face signs which are already kept in the database. It seems the image research do not consult other database fields before giving the results.

Tab Document

Here several documents can be recorded.

- Condition of being documented
- Type of document
- Series of document
- Date it was issued
- Giving entity
- Notes
- Date of expiration

Tab Address

- Type of address (Registered, rented, area where he sets if homeless, living, visiting)
- Country, Region, Province, District, Village, street, house, corpus (example: 180/1 means house 180 corpus 1), apartment, notes.

Tab Photo

In this tab screen they are uploading the photos. They should put also the points for the face recognition. Photos uploaded are kept in the database into a blob field.

The procedure of setting up the points must be done manually. It is an array of points without geometry of referential points, and no angular measures.

Photos are not given with a background reference of dimensions or a ruler behind, and they are made from different distances, so it is not even possible to measure distance between key face points, making the recognition features as a useless matter.

Special Signs Tab

Here they are recorded possible signs of recognition of the person. For example, if the person has a tattoo, photo of the tattoo and description.

- Type (on related list external signs on the skin, scars, warts
- Place in the body
- Description

Tab description of the aspect of the person

- Ethnics
- Race (European, mongoloid, negroid)
- Shape of body
- Face shape
- Eyes size
- Nose size
- Ears shape
- Hair color
- Height types
- Eyebrows
- Color of eyes
- Mouth shape
- Teeth (No teeth, prothesis, dark, yellow…)
- Notes

Amazingly, the system contains all information required as for making a robot portrait of the suspect, but such useful feature is not implemented in Portrait.

Relatives tab

Once chosen a person, you can see the same list of tabs but for the other person. It appears like in a second line down the main collection of tabs. (Nested into the tab of the previously selected person) Then on each of the secondary tabs, same information than in the main person, is visible.

There is only this second level. No other relation is possible.

This information is making appear a new system of databases which may be redundant or not.

Tab of ways of connection

This is mostly for telephones.

- Way of connection (Meaning what is the connection or linkage between the telephone and the person)
- Type of connection (Home Phone-Land line, Satellite, Work…)
- Number
- IMEI
- Notes

Tab Files

This tab is for files related with the case.

It can be there whatever files or attachments.

From a total list, the detail of one is:

- File opening
- Date of file
- Comments / Description

Tab Organization / Work Place

- Relationship (Director, Worker, Shareholder, wife of president…)
- Full name of organization (Not linked with the list of organization in the Ministry of Justice)
- Short name of organization
- INN of company
- Date of registration
- Place of registration
- Main activities (open field)
- Actual activities
- Additional Info

On this tab is possible to add several organizations

Tab for Type of Crime Group

- Who is this person in the gang?
- Name of group (Typologies)
- Territory of crime activity (Environment or crime lines)
- Additional info

Tab transport / vehicles

- Relation with the vehicle
- Brand (Typologies)
- Model
- Color
- Year of manufacturing
- Number of plates
- Date of registration
- Additional info

Tab weapons

- Way of relation with the weapon (Typologies)
- Classification (Gas, traumatic, smooth, hunting, sniffle)
- Type (Automatic, pistol, rifle…)
- Model
- Serial Number
- Caliber (Typologies)
- Country of producer

- Year of manufacturing
- Permission docs
- Department giving permission
- Date of permission
- Notes
- Photos of weapon
- Date of photo
- For knifes or other weapons they do not have records

Tab Events

- Relation with the event (Convicted, accused, wanted, victim, partner in crime, witness)
- Crime solved or not
- Date of event (starting / ending dates and time)
- Rayon of happening
- Number of case (KUP – Digital Book Case) Journal
- Date of registration of the case
- Number of criminal cases
- Date of opening of the criminal case
- Article of law (duplicated, as it already was set in previous tabs)
- Article of administrative offense (also duplicated)
- Chapter, section, paragraph (They do not have this in the previous one)

Tab Fabula (For some events)

- Description of facts
- Object of the crime making
- Way of making the crime (method)
- Level of damage of the victim
- Who solved the case?
- Injured? (It has not so much sense this one.)
- Date of solving

Notes about the facial recognition capabilities of “portrait”.

When a photo is uploaded, first you put the points. Additionally, you tell the age and sex.

This is giving back a list of photos to compare.

But the function of comparation works badly. Results are not accurate.

For this purpose, the data come divided into anthropometrics, complex graphic and contour.

12.2 Evaluation of duplicities/lacks Portrait-MAKS

According to the information collected about portrait and the data fields what must be in MAKS, this is the those are the common and different points of information in between.

To be noticed that MAKS is making distinction between people under investigation and people already arrested, being the personal data kept on both approximately the same.

To be noticed also that Portrait contains a lot of fields with very good detail on each one of the subjects.

Obviously in a development of MAKS and a migration of data contained in Portrait, a very detailed interface – migration plan – and field detail should happen, but that is the subject for an analysis by the side of the future developers of the solution.

All structures of data must be created in detail and joint in a logical way. Until the moment, and with the information retrieved about portrait and about MAKS, none of them is giving the good matching on the reality and organization of information as it should be for such a coordination and information system… so improvements must be done in both systems when both will be converted into a new tool, and this fact should be taken in mind in time of development and for sure, first of it, that should appear in the Terms of Reference.

PORTRAIT	MAKS
Tab Face (Photos)	Person table fields
Tab Credentials	Person table fields
Tab List (list of people)	Person table fields – partners in crime
Tab Face Recognition (Albon Gabi)	NO
Tab Document	Person table fields – documents Companies table fields – documents
Tab Address	Person table fields – addresses Companies table fields – addresses
Tab Photo	Person table fields
Special Signs Tab	Person table fields – marks
Tab description of the aspect of the person	Person table fields – appearance description
Relatives tab	
Tab of ways of connection	Person table fields – telephones Person table fields – emails
Tab Files	Person table fields – documents Companies table fields – documents
Tab Organization / Work Place	Person table fields companies
Tab for Type of Crime Group	
Tab transport / vehicles	Person table fields – vehicles Companies table fields - vehicles

Tab weapons	Person table fields – weapons
Tab Events	Person table fields – crimes committed
Tab Fabula (For some events)	Person table fields – crimes committed
NO	Accounts in social networks
NO	Bank accounts
NO	Operational data
NO	Conclusions

13 Appendix 2: Functional details about “MAKS”.

Here are detailed all functional requirements that the development of MAKS must cover for the functionalities expected by the tool itself.

The technical requirements for MASKS were set accordingly to report from the Spanish Police Specialist Mr. Diego Terroba after checking on the field the needs of coordination and analysis in the Ministry of Internal Affairs of the Kyrgyz Republic, and they are set on the following points.

13.1 General aspects

This new tool should be designed to allow OAD department continue with his current tasks and allow them to coordinate all investigation groups in de country.

The application must be able not only to store all information got by investigation groups but also to find coincidences and process all possible cases of conflicts and cooperation between groups.

In order to ease the task of maintenance and administration by IT department, MAKS should be web application implemented preferable in C#.net.

The members of investigation groups won’t have access to MAKS, only members of OAD and his group will have access.

The communication between investigation groups and OAD will be using standard templates that must be designed in order to allow the automatic record and coordination of information.

13.2 Modules:

In order to fulfil all functionalities required and to be OAD department self-sufficient MAKS should have at least the followings modules:

- Administration
- Repository of Information
- Coordination

13.2.1 Administration

This module should only be accessible by OAD headquarter.

This module allows special users to make following actions:

- Create new units: indicating name, level and unit’s father.
- Create / Modify / Inactivate and Activate users: indicating personal data, unit/units which he belongs, security level, area/s of work, and permission in each unit (search, add, modify, coordinate…), which could be different for each unit.

For example: a user could have access to all areas of work to one unit including secret investigations but he could only have access to search *investigation of one area of work in other unit and without access to secret investigations.*

- Extract auditory: Allow user to extract pieces personalized of auditory.

For example: extracting activity of a user from one day to another.

-Which users have accessed to some investigation?
-Which users have modified or added information to a specific investigation…?
-Which user realize a specific coordination.
-Which user modify / activate… a specific user.

- Validate audit records: every record should have a hash code which will can be validated. This process should certify that audit has not been illegally modified.
- Modify the maximum number of coincidences allows to generate coordination for each entity searched. (These limits will be detailed ahead in point “13.2.3.1 Manual search engine of coordination”).
- The most sensible information like password should be maintain encrypted, only during creation or modification of a user the password should be established but never visible.
- Every action done using this module should generate auditions as any other module in MAKS.

Audits should include at least the following information:

- User
- Date and time
- Action
- User / unit modified
- Search done
- Hash code

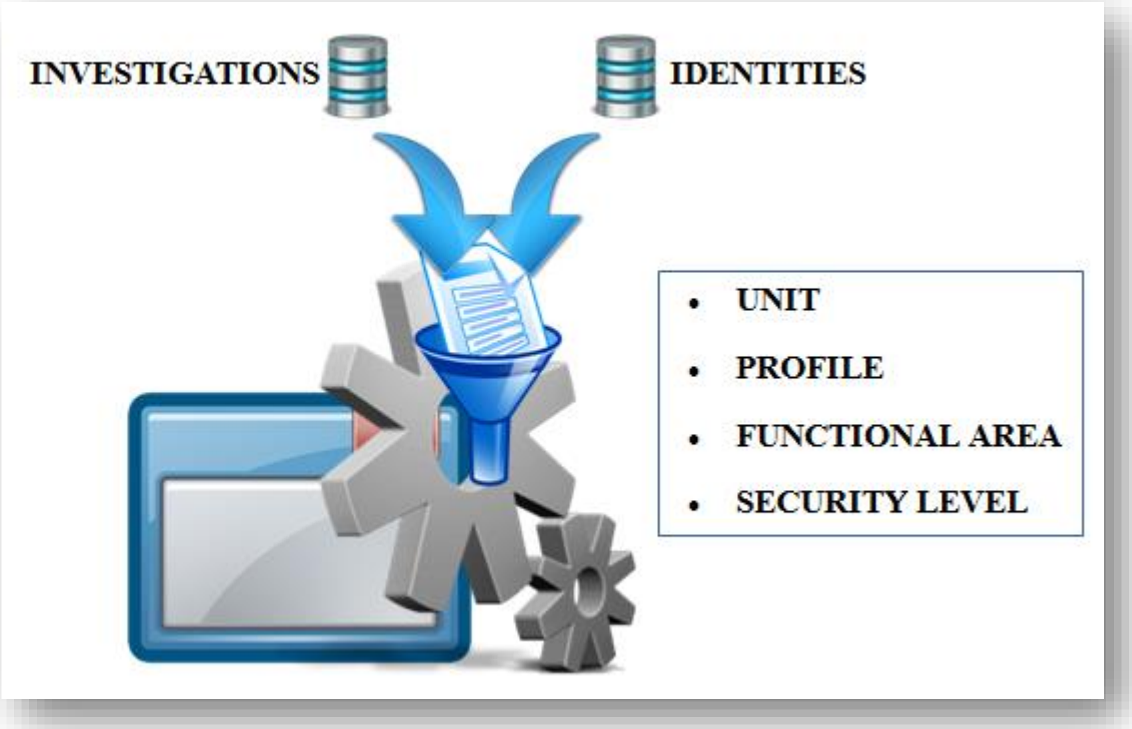
13.2.2 Repository of information

This is the main module of MAKS, it should be accessible by most user of MAKS.

The data stored will be detailed ahead but MAKS should have at least two different databases, INVESTIGATION and IDENTITIES.

The content of INVESTIGATION database should be filter according to user profile, while IDENTITIES database is open to all OAD departments.

This module should be personalized according to unit/units which user belongs, his security level, his area/s of work, his permissions...



All actions done in this module should generate audits which should include at least the following information:

- User
- Date and time
- Action
- Data added / modify / searched
- NI of investigation visualized.
- Hash code

13.2.2.1 Search engine

If a user has permission to make searches, the system should show a search engine which allows user to search any kind of information, individually or combining different fields and conjunction.

> *For example: search all suspects and all investigation with suspects which first name is Alexander OR Alexei AND with a tattoo in his left arm AND who is involved in any crimes different from terrorism…*
>
> *User will be able to search any kind of information stored: investigations, people, telephones, vehicles…*

MAKS should be prepared to allow user to make searches using asterisks “*” and wildcards “?”.

The system should offer the possibility to save the parameters of search in external file for later use. The file generated could be used to ease repetitive searches or statistics elaborations…

This module should be prepared to answer with a list of candidates of the kind of entity selected by user and if the entity selected is suspects, tattoos or any other entity with images stored, MAKS should be prepare also to answer with text and a list of possible images.

Example of possible outputs of suspects:

ID. Investigation	ID. Suspect	Field1	Field2	Field…
1	1	xxx	xxx	xxx
2	2	xxx	xxx	xxx
3	3	xxx	xxx	xxx
4	4	xxx	xxx	xxx
5	5	xxx	xxx	xxx
6	6	xxx	xxx	xxx

Example of possible outputs of tattoos:

ID. Investigation	ID. Suspect	ID. Tatoo	Field1	Field…
1	1	1	xxx	xxx
2	2	2	xxx	xxx
3	3	3	xxx	xxx
4	4	4	xxx	xxx
5	5	5	xxx	xxx
6	6	6	xxx	xxx

The result will show a preview of most important fields of the entity selected, but the system must also allow to personalize the response allowing user to indicate the fields that he wants to see for each entity

The system also should offer the possibility to extract the results to external files as excel files or doc files. This is useful to generate reports or to work with other applications like Microsoft Excel or IBM Analyst Notebook (I2).

All searches done in this module over INVESTIGATIONS won't generate coordination and the information listed can only belongs to the unit to which the user belongs or to some hierarchically inferior unit.

All searches done in this module over IDENTITIES won't generate coordination and the information listed will belong to the whole database, without limits because IDENTITIES is a database of free access for every Operative Analysis Group.

13.2.2.2 Add / modify information manually

Once the user has found an interesting result using the search engine, he will be able to enter on it and move freely through all entities which belong to that Investigation/Identity, analyzing all information available.

This movement through entities must be eased by system maintaining a navigation tree indicating where the user is actually.

If user is working over INVESTIGATIONS, he will be able to jump to other investigation which will be linked by entity "COLLABORATIONS".

This jump will allow users to analyze also the information in that Investigation but the jump will be only authorized if both Investigations are linked by similar record in "COLLABORATION" and the resolution of that collaboration is "Work Together".

Despite a user can access to Investigation of other units he will only be able to add or modify information to those which belong to the unit where user belongs.

If a user access to an investigation through the jump previously detailed, he will only be able to add or modify information in it if that Investigation also belong to his unit.

If user is working over IDENTITIES, he will be able to access directly to any record of database, and he will be able to jump from one identity to another through links established by "PARTNERS IN CRIME".

This jump will allow user to analyze also the information in that identity. In this database the jump will be authorized always, even the other identity has not a similar entry in "PARTNERS IN CRIME".

Despite every unit can create identities, every user with permission of modify identities can modify any information independently if the identify belongs to his unit or other.

The system must be prepared to easy the treatment of information with automatization for repetitive tasks.

> *For example: if a user wants to introduce a new "PARTNER IN CRIME" in an Identity or Suspect in a Investigation, the system must offer the possibility to find this person in the database in order to no to introduce all data manually.*
>
> *Once a user saves a new "PARTNER IN CRIME" in a Suspect, the system must create a similar record to the other person reciprocally, in order to avoid loss of time for the user.*

13.2.2.3 Add / modify information automatically

Once an Investigation group has sent a template to introduce new information in the system, and the members of OAD department has validate it (NI "number of the investigation", Id. Suspects, what are new data and which one not…) and all coordinations have been resolved. The system must offer the possibility to accept that template and save all information automatically.

This procedure must not delete or modify any existing data, but It must create new necessary entities and fill gaps in existing records.

If an investigation group notifies a mistaken in any data, all changes of existing data should be done manually.

Like in previous point "add / modify information manually" the system must be prepared to automatize tasks of treatment, to avoid repetitive tasks and losses of time.

> *Example: Once a template includes a new "PARTNER IN CRIME" for a Suspect, the system must create a similar record to the other person reciprocally.*

13.2.3 Coordination module

This module must be oriented to manage all possible coordinations, coincidences and conflicts generated by investigations groups and their work.

It has two main functionalities:

1. Create and provide users a tool to manage all possible coordinations produced.
2. To allow user to find information out of his unit or structure.

To achieve both purposes the system must count with two search engine and a module to manage coordinations:

There are two main differences between then search engine in MAKS's module of repository of information and the search engines in MAKS's module of coordination:

1. In repository of information the system search for coincidences in user's unit database and in those databases which belongs to hierarchically inferior units while in coordination the system search in the whole databases.
2. Searches done in repository of information do not generate coordinations while coordination provoke matches, crosses and coincidences.
3. In repository of information the system search for coincidences in specific fields and entities indicated by user while in coordination the system search in a wider way in order to find all coincidences.

This module has also to generate audits which should include at least the following information:

- User
- Date and time
- Action
- Data coordinated
- NI of Investigation matched, crossed …
- Coordination generated
- Modification done in coordinations
- Hash code

13.2.3.1 Manual search engine

The first engine must allow users to coordinate information manually of a simple entity, indicating the reason of coordination.

For example: search a plate number because an Investigation group has demanded information about a possible car involved in a crime…

The system must search in all databases not only INVESTIGATIONS but also IDENTITIES.

This search engine must simplify the work for users, so if a user search for a passport number, the system must search in all entities which stored information about passport (suspects, partners in crime, intervened effects, things stolen…).

These big categories must be 9 at least:

1. PEOPLE: Name, middle name and surname, with the possibility of narrowing the search by entering the date of birth.
2. NICKNAME: a familiar name given to a person instead of or as well as the real name.
3. VEHICLES: Plate numbers, Type, brand, model...
4. ADDRESSES: Addresses, Virtual addresses and IP addresses.
5. BANKS
6. COMPANIES
7. PHONES
8. OBJECTS: Documents, weapons or effects

Not all information coincident with the search will be shown, those information that user is allowed to see (because it is in his unit or belong to a free and passive Investigation of any unit or belong to IDENTITIES database) will be shown, and give the user the opportunity to enter in each entity to see all information available.

Once the coincidence and data available is analyzed, it could be discarded by user or it could produce a “Connection” or a “Cross” (see “Standard Operative Procedure for Coordination of Investigations manual” for further information).

But all information that are in the system that coincide with the search done, but user is not allow to see it (because it belongs to other unit or it belong to an Area that user can access or if it is secret and the user has not access to it) it will generate a coordination and it will be called a “match”.

MAKS should avoid repetitive coordinations, if two users coordinate the same data and provoke the same coincidences between two or more investigations the system must avoid to create twice the same coordination because it will provoke losses of time.

All Connections, Crosses and Matches produced will be shown in module of coordination but it won't be seen necessarily by user who done the search, it will be seen by user which be in charge to resolve that coordination according to "Standard Operative Procedure for Coordination of Investigations manual".

Obviously not all searches done in this module will generate coordination, because a user could search for all suspects called "Dimitry" and it could generate thousands of coordination and cause a system crash.

The maximum number of coincidences allows to generate coordination must be defined initially but it could be change from Administration Module.

The maximum number of coincidences must depend on the entity and fields searched; it must not be the same limit if a user search for a passport number that for a surname.

13.2.3.2 Automatic search engine

The second engine must allow users to coordinate information automatically. Like in first engine the user must indicating the reason of coordination but he won't introduce the data, we will introduce the template sent by Investigation group.

The system must be capable of search all coincidences, and divided it between visible data and matches.

As well as manual search engine, the user must divide the visible results between discard, cross and connections.

13.2.3.3 Module to manage coordinations

The module will be use to manage all coordinations produced on MAKS, obviously the coordinations shows to every user will depend on user's profile and unit.

This module will show all coordination produced, not only those which are pending to resolve but also those which has been resolved.

For each coordination, user will see:

i. Which data were coordinated?
ii. Data that provoke the match.
iii. The reason of coordination.
iv. User who done the coordination.
v. Date of the coordination.
vi. Relevant data related.
vii. Decision made by every investigation group involved.
viii. Comments
ix. Final decision.

Once a final decision is made the system will make all necessary changes according to "Standard Operative Procedure for Coordination of Investigations manual".

There will also be a search engine of coordination in order to look for certain coordinations resolved or in process, and a functionality to produce statistics.

For example: number of coordination produced by a unit, number of coordination produced by an area of work, number of coordination between two areas, number of coordination resolved by a user…

13.3 Stored information in MAKS

MAKS will have at least three different databases one for INVESTIGATIONS, one for IDENTITIES and one for COORDINATIONS.

INVESTIGATION database will contain all data related with investigation past or present.

IDENTITIES will contain all information about people that was involved in an investigation and was arrested.

COORDINATIONS will contain all information about matches, coincidences and crosses.

All information from "Portrait" and "Taistous" should be migrated to IDENTITIES, creating if it is necessary new fields not indicated in this report in order not to lose information.

- For Portrait, size is about 800 Gb. Expected volume of tables: About 100 service objects, about 30-50 tables, about 7 million registries. Oracle 11.
- For Taitous, about 2,78 Gb information and around 30 tables in the database. SQL Server.

This might imply the intervention of a database specialist and such task can last from 1 to 2 months, and it might be prepared coordinately with the new database to be developed for MAKS.

In order to ease IT's tasks of maintenance databases should be implemented preferably in SQL Server.

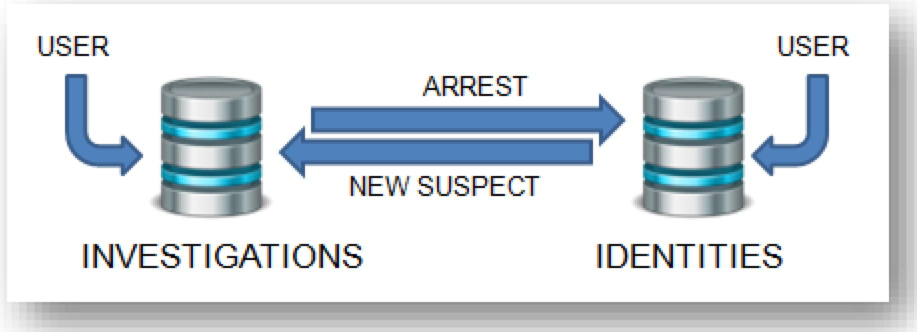
The main differences between INVESTIGATIONS and ENTITIES are two:

- The information contained in the first one is mostly speculative or incomplete. The investigation groups provide information as soon as they get them using templates specifically designed to this purpose.

- In the second one the information are trustworthy because once a person is arrested, you know certainly his name, passport, photo, fingerprint… all information are complete and reliable.

Information is introduced in both databases by user or by automatic procedures but also both databases exchange information as it is detailed below.

MAKS stores information in first place in INVESTIGATION database, once a person is arrested MAKS move automatically all information related with this person to IDENTITIES creating a new record or if the person had been arrested before including all new data in the existing record.



But the information also goes from IDENTITIES to INVESTIGATION, if an investigation group, started to investigate a person who is already in IDENTITIES, the system should offer the option to export all or selected parts of the information available about this person to the current investigation.

13.3.1 Investigation database:

This database should contain at least the following information, entities and fields.

Every entity should store automatically date of creation and date of last modification:

- Investigation: (Main entity, the rest of them are subordinated to this one)
    - NI: Number of Investigation (example: BI00001/19).
    - Starting Date
    - Date of Conclusion
    - Name
    - Name of special operation
    - Type (A,B or C)
    - Reason (Investigation, Information, Investigation in collaboration or Joint Investigation)
    - Situation (Active, Passive, Passive/RJ, Ended)
    - Grade of confidentiality (Free, Secret, Reserved)
    - “n” Areas of work
    - Territorial scope
    - Location
    - “n” crimes committed
    - “n” investigations related
    - Comments.
- History
    - Date of change
    - Previous starting Date
    - Previous date of Conclusion
    - Previous name
    - Previous name of special operation
    - Previous type (A,B or C)
    - Previous reason (Investigation, Information, Investigation in collaboration or Joint Investigation)
    - Previous situation (Active, Passive, Passive/RJ, Ended)

  - Previous grade of confidentiality (Free, Secret, Reserved)
  - Previous “n” Areas of work
  - Previous territorial scope
  - Previous location
  - Previous comments.

- Organized Crime:
  - Apply or not
  - ID
  - “7” Criteria
  - Comments
  - Documents

- Investigation manager:
  - Date
  - Starting Date
  - Situation
  - Participation
  - Name of the investigation group
  - Telephone
  - Email
  - Country
  - Province
  - City
- Documents:
  - Date
  - Type
  - Registration
  - Origin
  - Evaluation
  - Use or purpose
  - Destination
  - Data
  - Document (pdf, doc, text, photo..)
  - Comments / Remarks

- Collaboration:
  - Date
  - Date of Resolution
  - Final date of the collaboration
  - Unit
  - NI: Investigation related
  - Type of collaboration
  - Comments / Remarks
- Person:
  - Name
  - Middle name

- Surname
- Sex
- Birthdates
- Place of birth
- Country of birth
- Nationality
- Father’s name
- Mother’s name
- Profession
- “n” documents
    - Type
    - Number
    - Expiration date
- Grade of participation (victim, witness, author…)
- “n” nicknames
- “n” photos
- Description
- Appearance description
    - Height
    - Weight
    - Age
    - Race
    - Hair color
    - Hear length
    - Skin color
- “n” marks - tattoos
    - Description
    - Place
    - Photo
- “n” Partners in crime
    - Name
    - Middle name
    - Surname
    - “n” documents
        - Type
        - Number
        - Expiration date
- “n” crimes committed
    - Article inflicted
    - Description
    - Modus Operandy
    - Place

- “n” phones
    - Number
    - IMEI
    - IMSI

    - Date
  - “n” emails
    - Name
    - Date
    - IP
  - “n” accounts in social networks
    - Name
    - Network
    - IP
    - Adress
  - “n” addresses
    - Vial
    - Street
    - Number
    - Floor
    - Door
    - City
    - Country
    - Name
    - Coordinates
  - “n” Weapons
    - Type
    - Caliber
    - Serial number
    - Date
    - Description
  - “n” Bank accounts
    - Type
    - Number
    - Bank
    - Quantity
    - Date
  - “n“ Companies
    - Name
    - Address
    - Type
    - Relationship with
  - “n” Posts
    - Company
    - Level
    - Date
  - “10” Finger Prints Form
  - “n” Finger Prints images
    - Date
    - Location
    - Image
    - Description

    - Starting Date
    - “n” Properties
        - Vial
        - Street
        - Number
        - Floor
        - Door
        - City
        - Country
        - Name
        - Date
    - “n” Vehicles
        - Type (car, motorbike, plane, boat…)
        - Brand
        - Model
        - Color
        - Plate
        - VIN
        - Date
    - Comments
    - “n” Documents.
        - Date
        - Location
        - Description
        - Document
        - Format
- Companies:
    - Name
    - Identification
    - Country
    - Date
    - “n” Activity
        - Sector
        - Subsector
        - Description
    - “n” Telephones
        - Brand
        - Model
        - IMEI
        - IMSI
        - Telephone number
        - Company
    - “n” Address
        - Vial
        - Street
        - Number
        - Floor

    - Door
    - City
    - Country
    - Name
    - Coordinates
  - “n” Properties
    - Vial
    - Street
    - Number
    - Floor
    - Door
    - City
    - Country
    - Name
    - Date
  - “n” Bank accounts
    - Type
    - Number
    - Bank
    - Quantity
  - “n” vehicles
    - Type
    - Brand
    - Model
    - Color
    - Plate
    - VIN
    - Date
  - “n” employees
    - Name
    - Middle name
    - Surname
    - “n” documents
      - Type
      - Number
      - Expiration date
  - “n” Documents
    - Date
    - Location
    - Description
    - Document
    - Format
  - Comments
- Operational data
  - “n” address under surveillance
    - Vial
    - Street

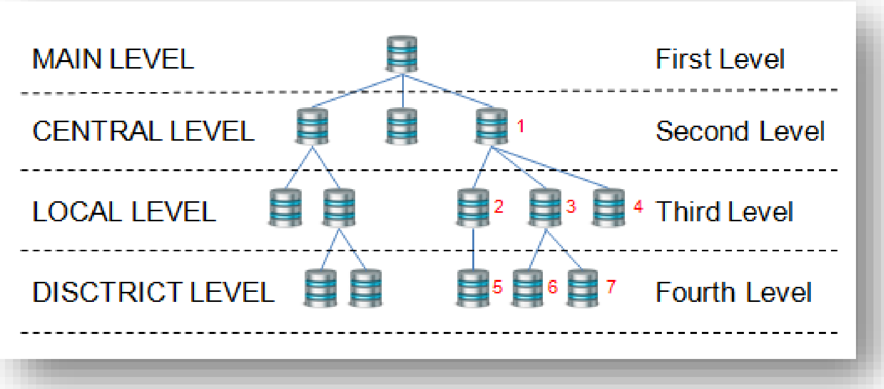
        - Number
        - Floor
        - Door
        - City
        - Country
        - Name
        - Coordinates
    - “n” taped phones
        - Brand
        - Model
        - IMEI
        - IMSI
        - Telephone number
        - Company
        - Starting date
        - Ending date
    - “n” geolocalized car/ship
        - Type
        - Brand
        - Model
        - Color
        - Plate
        - VIN
        - Date
        - Starting date
        - Ending date
    - “n” photos
        - Date
        - Location
        - Description
        - Document
        - Format
    - “n” weapons/tools used
        - Type
        - Caliber
        - Serial number
        - Date
        - Description
    - “n” multimedia files
        - Date
        - Location
        - Description
        - Document
        - Format
    - Comments
- Conclusions:
    - Date

- “n” actions
- “n” people arrested
- Results
- “n” effects recovery/intercepted
- “n” intervened drugs
- Money
- Comments.

There is not obligation about how the data will be storage but it must be a hierarchical structure of Operative Analysis Groups with 4 different levels at least.

- MAIN LEVEL (first level): Users who belong to this first level must see hypothetically all information in database, depending of user’s permissions and other parameters.
- CENTRAL LEVEL (second level): Users who belong to groups of this level must see his own information and all information of units of third and fourth level of their own structure, depending of user’s permissions and other parameters.
- LOCAL LEVEL (third level): Users who belong to groups of this level must see his own information and all information of units of fourth level of his structure, depending of user’s permissions and other parameters.

- DISCTRICT LEVEL (fourth level): Users who belong to groups of this level only will see information of his group, depending of user’s permissions and other parameters.



Despite of the above schema, MAKS will require only 3 levels as local and district would be assumed in the same level. Just in case, and for future purposes, the establishment of a 4th level must be ready to be implemented with none or minor changes.

Initially there won’t be any group of fourth level, but the system must be prepared to allow administrator not only to create new groups of fourth level but also groups of any level dynamically and assign users to those units, without any cost and without external intervention.

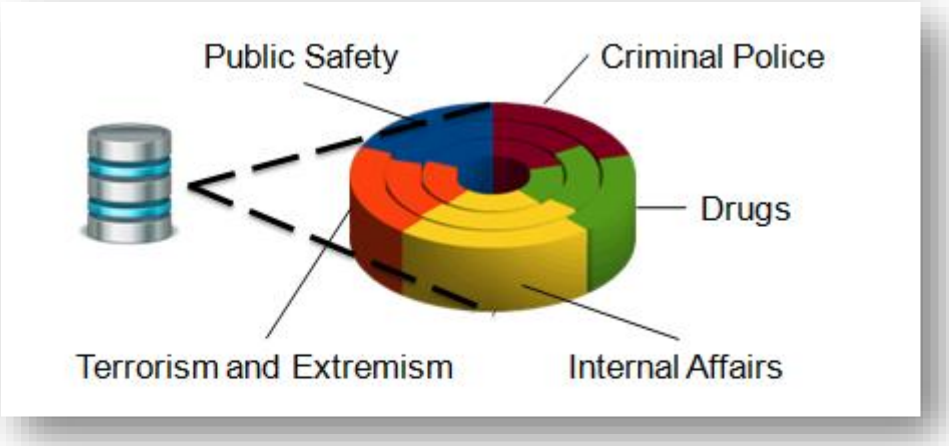
It is important to mention that, once an investigation is finished and the main research group allows it, all information in it will be released (it becomes free and passive). It means that all operative analysis group will be able to see, thorough coordination, so under these circumstances any group will be able to see information of any other operative analysis group independently of the structure and his position in it.

The investigation will be also divided by areas:

- Drugs
- Public Safety
- Criminal Police
- Terrorism and Extremism
- Internal Affairs

Only users with access to a specific area will be able to see the investigations under that area.

This division allows allow to create groups even users specialized in a concrete areas and others multidisciplinary which will be able to work with different research groups.



Like previously if an investigation in released, every operative analysis group will be able to see it and work with it, independently if user has this area of work in his profile or not.

The investigation will be in 1 of 3 security levels: Free, Secret or Reserved.

Only users of highest level will be able to see all investigations.

The investigation will be also in different states Active, Passive or Ended.

1.1.1 Identities database:

This database should contain at least the following information entities and fields, every entity should store automatically date of creation and date of last modification:

- Person:
  - Name
  - Middle name
  - Surname
  - Sex
  - Birthdates
  - Place of birth
  - Country of birth
  - Nationality

- Father’s name
- Mother’s name
- Profession
- “n” documents
    - Type
    - Number
    - Expiration date
- “n” nicknames
- “n” photos
- Description
- Appearance description
    - Height
    - Weight
    - Age
    - Race
    - Hair color
    - Hear length
    - Skin color
- “n” marks - tattoos
    - Description
    - Place
    - Photo
- “n” Partners in crime
    - Name
    - Middle name
    - Surname
    - “n” documents
        - Type
        - Number
        - Expiration date
- “n” crimes committed
    - Article inflicted
    - Description
    - Modus Operandi
    - Place
    - Date
- “n” phones
    - Number
    - IMEI
    - IMSI
    - Date
- “n” emails
    - Name
    - Date
    - IP
- “n” accounts in social networks
    - Name

    - Network
    - IP
    - Address
- “n” addresses
    - Vial
    - Street
    - Number
    - Floor
    - Door
    - City
    - Country
    - Name
    - Coordinates
- “n” Weapons
    - Type
    - Caliber
    - Serial number
    - Date
    - Description
- “n” Bank accounts
    - Type
    - Number
    - Bank
    - Quantity
    - Date
- “n“ Companies
    - Name
    - Address
    - Type
    - Relationship with
- “n” Posts
    - Company
    - Level
    - Date
- “10” Finger Prints Form
- “n” Finger Prints images
    - Date
    - Location
    - Image
    - Description
- Starting Date
- “n” Properties
    - Vial
    - Street
    - Number
    - Floor
    - Door

        - City
        - Country
        - Name
        - Date
    - “n” Vehicles
        - Type
        - Brand
        - Model
        - Color
        - Plate
        - VIN
        - Date
    - Comments
    - “n” Documents.
        - Date
        - Location
        - Description
        - Document
        - Format
    - “n” Investigation Involved
        - NI
        - Date
        - Grade of participation

13.3.2 Coordination database

This database will store all information about crosses, positives, matches and all process follow to resolve a conflict between two investigation group.

Only users with permission to coordinate will have access to this database.

The structure of this database is not defined, but the functionality as been detailed above.

13.4 Audits

All action in MAKS should be recorded for after audition, including actions in Administration, Repository and Coordination Modules.

No user should be out of these records and no user should have capacity to modify or delete them.

In order to avoid falsified records every audit should be validated using hash code or similar, which should be created using all available data (user, action, date…).

Administration module should count with a search engine to find audition records and a functionality to validate them.

The algorithm which evaluates the hash code should be maintained in secret.

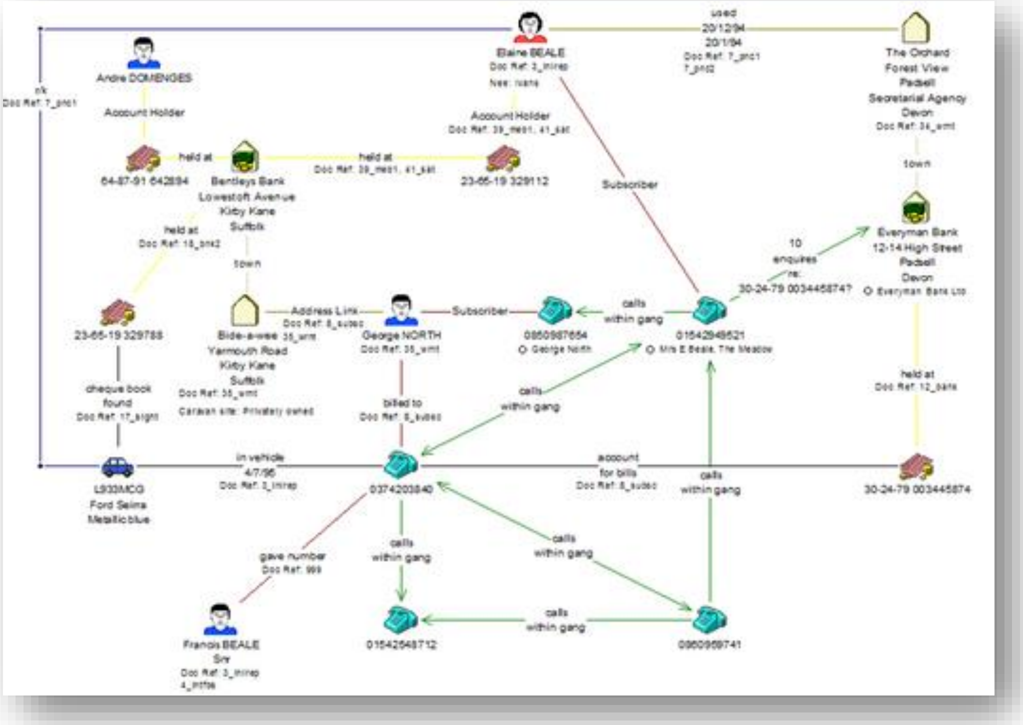
13.5 Connection with other systems

MAKS should be self-sufficient to store information and to manage coordinations although it should be prepared to interact with other systems in order to elaborate reports and intelligence.

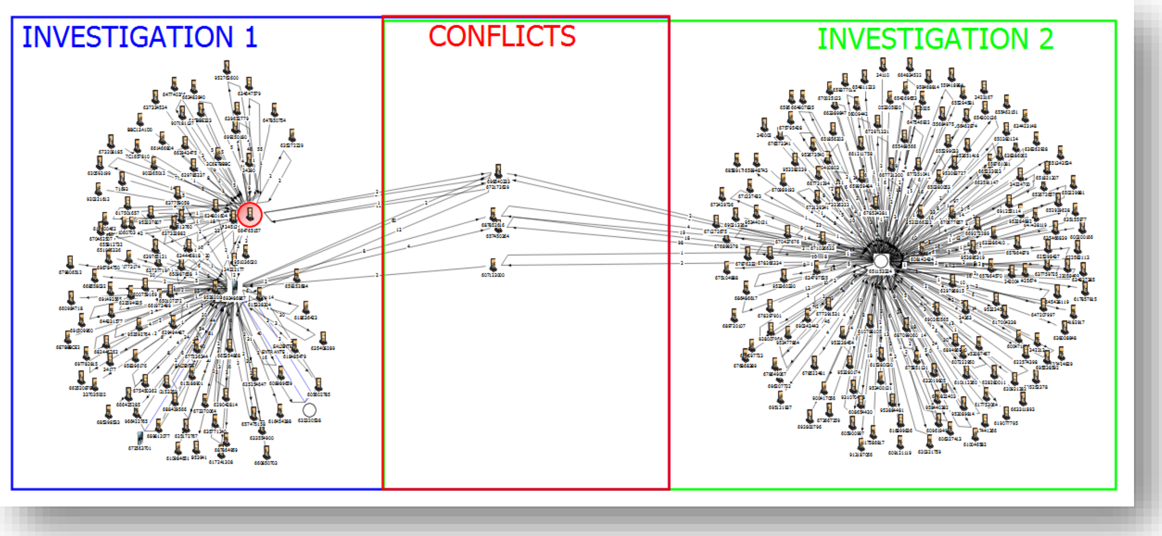
Every form, entity and investigation should be prepared to be exported to external document, to word document and excel document at least.

In addition, MAKS should provide a connection with IBM i2 Analyst Notebook, it could be by excel documents or IBM i2 iBase.

It will be use to elaborate intelligence reports and to give investigations group a new point of view about their investigations.



This connection can be also used to resolve coordination because it will give OAD groups a fast view about connections between investigations and their possible conflicts.



If “Portrait”, AOD’s application is maintained as application for face recognition it is necessary to implement a connection between “Portrait” and MAKS in order not to record all information twice.

Finally, all communication with MAKS should be encrypted by VPN or similar, in order to avoid leaks of information and vulnerabilities.