



# INFORMATION SHEETS



**For further information**

Email: [info@superstructuregroup.com](mailto:info@superstructuregroup.com)

Website: [www.superstructuregroup.com](http://www.superstructuregroup.com)

**Head Office**

Superstructure Group Limited  
Ash House, Fairfield Avenue  
Staines, Middlesex TW18 4AB  
United Kingdom  
Ph +44 870 803 2579  
Fax +44 1784 224 245

**Regional Office**

Superstructure Group (AP) Limited  
Level 1, 19 Tory Street  
P O Box 19127, Courtenay Place  
Wellington, New Zealand  
Ph +64 4 385 0001  
Fax +64 4 381 3934

# THE HEART OF THE MATTER...



At the core of SiD are three key categories of information:

- Information from all forms of *source documentation* such as statements, job sheets, diary notes, or even bank statements, is entered in “information reports”.
- Any particular *entity or item of interest*, such as a person, a car, a location or a weapon, is called an “object”, and each object has its own “object profile”, which is built up over time.
- The *associations* between any two (or more) objects, for example, “A” is the child of “B”, are called “relationships” or “links”.

## Efficient Data Entry

SiD’s straightforward user interface is easy to learn, with comprehensive, window-level help. Information may be typed in directly, or imported from word processing applications. Documents and images can also be scanned in and Excel spreadsheets may be imported. Extensive use of lookup tables throughout SiD makes it easy to correctly enter values such as place names etc, thus improving the quality of data input, and later the ease of searching for these values. There are several options for loading object profiles; a full profile version, and a rapid load

version where text such as a person’s name may be highlighted from the body of a source document and quickly added to a new object profile. This method is used where minimal information is available on an object.

## Duplicate Checking & Profile Combing

When new objects are loaded, a weighted algorithm automatically checks the likelihood of any possible duplicate records, based on identified attributes such as name, date of birth, passport number etc. Where two profiles containing information about the same person are found, these can be automatically merged into the selected master profile.

## Comprehensive Searching

Getting information out of SiD is as easy as getting it in, with search facilities that are both advanced and easy to use. Full text and contents searching capabilities are provided.

Simplicity of searching is a popular aspect of SiD, as is the ability to search on people’s names irrespective of name order. For example, a search for TAN LIM CHIN will also return the profile for CHIN TAN LIM.

# ARRESTING FEATURES



## Infinite Adaptability

What sets SiD apart from other advanced relational databases – from any field of endeavour – is its infinite adaptability. This means that if, for example, partway through an investigation the need for a new DNA profile category becomes apparent; the investigator can add this as an item of information available to all object profiles, there and then. This flexibility applies to adding new types of relationships, new types of objects and information reports – in fact to most of the system.

## Arrest, Disclosure and Prosecution

SiD electronically creates relationships between objects in the database. As soon as one looks at an object profile, any relationships with other objects are immediately apparent. Similarly, the information report(s) referring to that object are shown, as are cross-references between information reports.

## Project Library

The Project Library module can be used to create files (called “projects”) of cross-references to object profiles and information reports that already exist within SiD. For example, an analyst or file manager working on an operation might create a project for

the phase of the operation concerned with vehicle movements. Within this project, called “Vehicle Movements”, there might be sub-groups for “Driver”, “Vehicles”, “Green Commer Van”.

Together these features make the paperwork required for arrest, disclosure and prosecution fast and easy.

Being electronic, SiD eliminates the need for many copies of documentation. Only the evidential copy is required, while the electronic data is on hand for all other uses.

## Precise Security Control

Comprehensive security facilities in SiD allow the same database to be used for all investigations, whether they are general, undercover or internal, with no danger of compromising security restrictions applied to the most sensitive of information. This is achieved in several ways, including the use of user roles that give users permission to perform some functions on the system but not others, and the use of data access privileges which allow access to particular data only to users with corresponding access rights.

# INTELLIGENCE SUPPORT



SiD takes the hard work out of intelligence analysis, with an integrated set of analysis tools and two-way interfaces to powerful visualisation programs including i2®, ArcView and MapInfo.

## Integrated Analysis Tools

SiD delivers all the productivity gains to be expected of a modern, information storage and retrieval system – rapid data entry, extensive search facilities, comprehensive documentation management – but also offers an integrated set of specialist analysis tools that are essential for intelligence-led law enforcement. These include the Telephone Analyser module that is used to analyse telephone call records supplied by telephone service providers.

### Telephone Analyser

Telephone analyser allows importing of files in Excel, delimited, or fixed-length text format files as well as allowing manual input. This data can then be automatically transferred into the main SiD database, where each telephone number is created as a unique object, and each call is recorded as a time-dependent relationship between each telephone number.

### Seamless i2® interface

At this stage the user can select a phone number or numbers for inclusion in an i2® link analysis. This reveals all relationships between the selected telephone numbers and other objects such as people, or locations, that already exist within SiD.

In addition, users can use the i2® Analyst Notebook to add new information such as additional relationships between existing objects, and have i2® diagrams stored against profiles. Combined with SiD's powerful search tools, which may be used to select data for inclusion, the i2® interface enables rapid visual display of large amounts of complex relationship data.

### Point-and-click relationship build

SiD includes its own graphic relationship build facility. SiD ensures all relationships are referenced to the source document (information report) that gives evidence of the association. Relationships can be time-dependent and can have attributes associated with them; for example, person X was a shareholder of company Y from August 1990 to July 1992 with 2000 shares at \$40,000 total value. Pre-defined relationship types have their own

**relationship rules** that ensure only naturally occurring relationships can be entered.

## Integrated, Secure System

SiD makes data gained from operation-by-operation investigation activities available as a national intelligence database – while protecting all

# INVESTIGATION SUPPORT



SiD uniquely integrates the intelligence analysis capability with a full case management facility. Full task assignment and tracking capability, gives the officer in charge complete status reporting.

## Investigation Management

This database provides all the efficiencies to be expected of a modern, nation-wide information storage and retrieval system – rapid data entry, extensive search facilities, comprehensive documentation management – but also offers advanced tools for investigation management. These include the Directives module, which manages operational tasks.

### Case Management — Task Management (Directives)

Directives assigns officers to various tasks within the enquiry and gives full status tracking of outstanding, and follow-on tasks. At any point in time the commanding officer can quickly compare progress on various lines of enquiry – and direct the re-sourcing of the investigation accordingly. It also keeps an audit trail of the documents relating to that investigation, including for example, the source document for each directive and the document that results in the closure of each directive. Directives includes start up checklists for standard investigation procedures for different types of crimes; for example, “Obtain any video surveillance coverage in the area. Check taxi records...” These checklists can be revised whenever necessary.

## Who is investigating whom?

A useful feature is the ability to set interest flags against object profiles, which tell the user who else has accessed that profile since they last logged on. These flags can be apparent to all users – or just to the users who set them. Set interest flags may be used to enhance team working between officers, or for covert analysis of who has been accessing specific information.

## Area Canvass

Area Canvass is another unique management tool offered by SiD. It provides comprehensive facilities for the design and management of door-to-door surveys of people who may have information relating to an enquiry. Preparing surveys and assigning streets and street numbers to officers is a breeze with a tailor-made questionnaire facility. The display of the area canvass progress and results can be readily manipulated on-screen. There are many sorting criteria to choose from; for example, an area canvass may be viewed according to street number, status, and people associated with each number; or it may be viewed according to all the people interviewed so far, sorted by response. Area Canvass can import location data from geographic information systems, such as ArcView and MapInfo, and export data to these systems so that

# ENTITY RECOGNITION



Entity Recognition is the process of turning information into structured data that can be processed and analyzed, combined with other data sources and presented as views of the information that may not be immediately obvious. This process is often described as extracting **Actionable Intelligence**.

## Why Entity Recognition makes a difference

Entity Recognition leverages advanced intelligence extraction techniques used in information collection, analysis and dissemination processes. This delivers significant time efficiency and productivity gains across collection, analysis and dissemination flows by identifying with higher degrees of accuracy entities associated with potential events or threats. Consequently, risks surrounding these events and threats are reduced.

Entity Recognition differs from search in that it provides a framework for identifying complex relationships between sets of words (text and numerical data) including the specification of contexts in which matches should be either disregarded, or specifically targeted and then given more or less significance. Every targeted sentence is assigned an optional numeric weight, which can be used to discriminate between sentences and whole documents to limit the yield of documents or sentences. This further improves usability by allowing the user to influence the ranking of hits in the result set.

## How is Entity Recognition implemented?

Fundamental to Entity Recognition is the ability to broadly define topic areas of interest and to deploy capability for identifying and extracting entities from large and continuous volumes of content. This mandates the need for a flexible but dynamic topics framework to deliver highly accurate results. The topics framework provides for the ability to describe the attributes of entities for entity extraction, and define the relationships between the entities to interpret the facts.

Entities are weighted based on value assumptions assigned to entities in a topic in order to rank the results. This we describe as Intelligence Value Estimation (IVE) and it is the dynamic and flexible attribution of value weightings to topics of interest. This enables a granular focus to be applied to specific areas of interest within content. Intelligence values can be used to automatically raise the visibility of content based on dynamically changing requirements and filter out lower priority content. IVE's are assigned based on recognition of entities in content and are fully accountable.

# ENTITY RECOGNITION (cont)



In describing the attributes of entities, the circumstances in which entities are of interest are specified. This includes Pre-requisites, a combination of one or more entities that must be present to make another set of entities of interest; and Disqualifiers, a combination of one or more entities that if present make all other entities of no value.

## Topics

Topics are reusable, structured specifications of entities and relationships between entities. Topics specify selection and ranking of sets of terms in sequence with sensitivity to proximity and frequency.

Topics consist of:

- One or more Categories that define the entities, i.e. a named list of terms in sequence with optional weight and precision, e.g. regular search expressions, search terms, lists, patterns or combinations thereof; and
- One or more Equations that define the relationships between the Categories that are of interest.

When applied to documents, Topics identify and rank matching content based on its Intelligence

SiD Content Analysis  
Powered by:

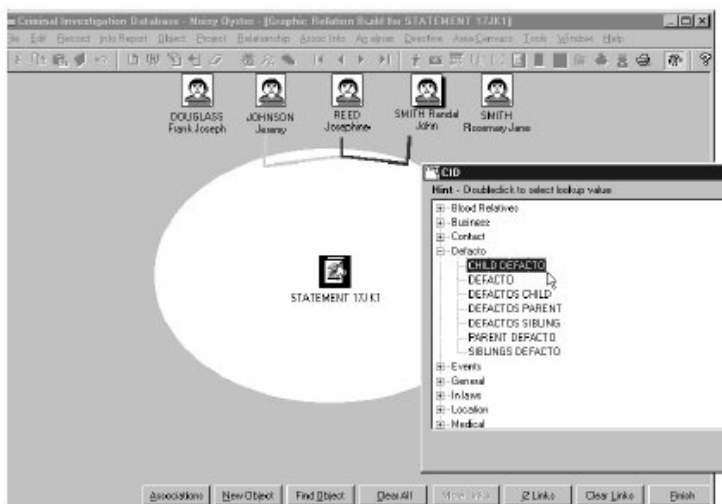


# ASSOCIATIONS AND LINK ANALYSIS

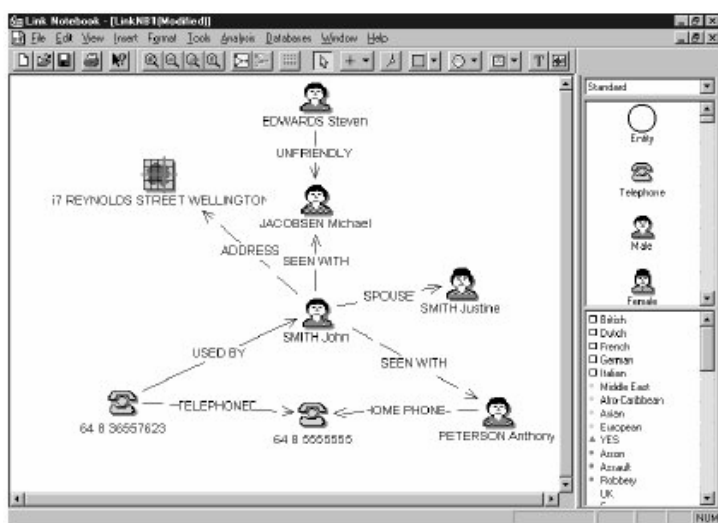


SiD has point and click building of associations and a direct, seamless link to the i2<sup>®</sup> Analyst's Notebook product for generation of link diagrams and event flowcharting.

The detailed features of the Associations facility are:



- Point and click relationship build
- Audit cross-referencing to source documents (allowing multiple documents to indicate strength of relationship)
- Time based-relationships (for example, "Person A resides at this address between these dates")
- Relationship rule protection (for example, a vessel cannot be the father of a company)
- Multiple relationship add (e.g. all people involved in a single event)
- Find relationship between two entities (is A linked to B in any way)



The detailed features of the Link Analysis interface are:

- Level-by-level expansion of link diagrams
- Date, relationship type and object type analysis filters
- i2<sup>®</sup> diagrams stored for relevant profiles

# OBJECT PROFILES



Object profiles provide detailed attribute descriptions for all objects of interest to the investigation (persons, organisations, vehicles, items, phone numbers, addresses etc). The profiles are dynamically expandable with an unlimited amount of detail possible to record.

The detailed features of this facility are:

- Linking of any content in any MS Windows® application to any object. This feature allows linking Spreadsheet, Photos, Maps, Video clips to extend the recorded information.
- Linking of any web URL address to extend information in SiD to information held anywhere on the web
- Full search on the contents of all profiles
- Attribute-based searching (for example, Asian Males two metres tall)
- Order-independent searching for Asian names (for example, Ho Han Kwuk versus Kwuk o Han)
- Details for financial transaction data
- Full data security and post-operation downgrade option
- Linking of i2® diagrams to specific profiles
- “Cut and paste” building of profiles from IR’s
- Profile combining (alias resolution)
- Secure and broadcast alert flagging
- Unlimited text detail can be recorded for each profile
- Electronic file breakdown into user-defined project categories (for example, Disclosure/Evidential/Crime scene/Suspects etc)

- Full audit trail of any changes made (who, when, why)
- Cross reference back to any IR’s referencing this subject
- Unlimited expansion of profile detail (operation specific)
- Multiple entries for items (for example, recording of multiple passports)

A screenshot of the SiD software interface showing an object profile for 'FEED Josephine Rose (12/06/1972)'. The window title is 'FEED Josephine Rose (12/06/1972)'. The main area is divided into two panes. The left pane contains a list of expandable categories: Area Convoys (2), Associations (8), Audit History, Directives (0), i2 Diagram (0), Operational Security, Photos (0), Profile Text (0), Projects (0), Related Reports (2), and Spreadsheets (0). The right pane displays the attributes for the selected object, including: Family Name (FEED), First Name (JOSEPHINE), Middle Names (ROSE), Title (MS), Gender (FEMALE), Date of Birth (12/06/1972), Age (28), Called Name (JD), Ethnicity (EUROPEAN), Address (Home) (10 GRASS STREET ORIENTAL BAY WELLINGTON), Address (Business) (TELECOM HOUSE, MANNERS ST, WELLINGTON), Phone (Business) (04 801 2588), Phone (Home) (04 401 7995), Role in Operation (AREA CANNASS), and Occupation (CHEF). At the bottom of the window, there are several buttons: Expand Attributes, Look up Attributes, Archive Log, Other Ops, View IR Program, Add to Project, Print, and Finish.

**This object profile window has jumps to associated information on the left, and a customisable, expandable set of attributes on the right.**

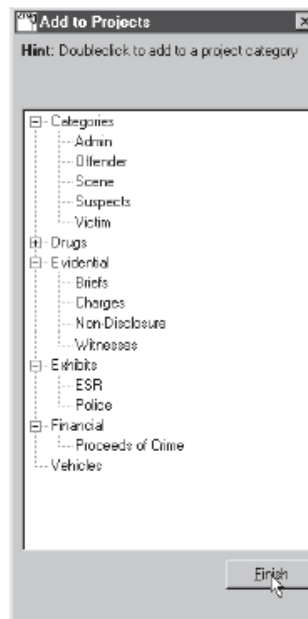
# DOCUMENT MANAGEMENT



All source documents entered into SiD are called information reports or IR's. There are numerous user-defined types of IR; for example, Statement, Job Sheet, Notebook Entry.

The detailed features of this facility are:

- Word processor interface (MSWord®) to allow import of previously typed documents
- Internal text editor to provide fully formatted amendment to text
- Spell check
- Linking of any content in any MS Windows® application to any object. This feature allows linking Spreadsheet, Photos, Maps, Video clips to extend the recorded information.
- Linking of any web URL address to extend information in SiD to information held anywhere on the web
- Full text search on the contents of all documents
- Thesaurus search for list of linked words (for example, LSD, acid, trips, blotters, mellow, tabs)
- Full audit trail of any changes made (who, when, why)
- Linking of multiple objects (people, vehicles etc) referred to in information reports to the respective information report
- Linking of related/superseded IRs
- All associations entered into SiD are referenced to the information report they are based on
- Searchable details for data from electronic or surveillance logs
- Searchable details for financial transaction data
- Full data security and post-operation downgrade option
- Electronic file breakdown into user-defined project categories (for example, Disclosure/ Evidential/ Crime scene/ Suspects etc)
- Full Admiralty source and information reliability rating



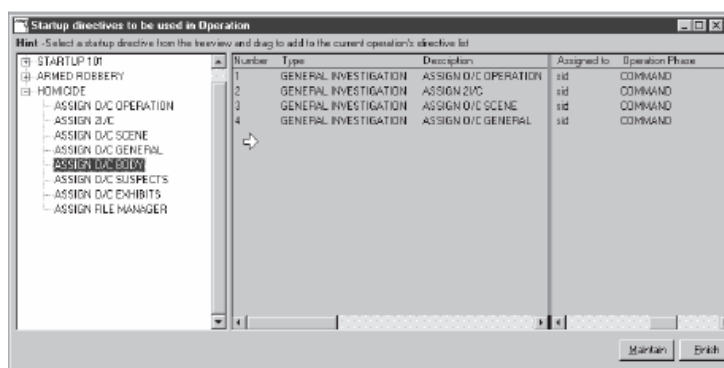
**This pop-up window allows rapid addition of information reports and object profiles to project library categories.**

# CASE MANAGEMENT

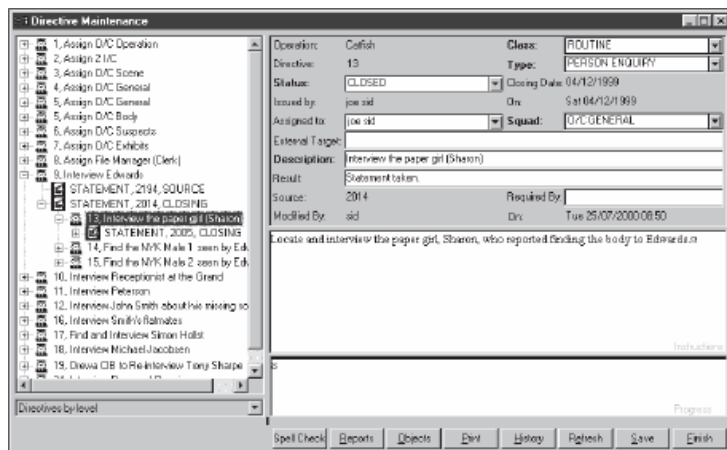


The Investigation Directives mechanism of SiD allows the operation commanders to manage task assignment and the various lines of enquiry.

The detailed features of this facility are:



- Start-up checklist for standard investigation procedures (for example, “Obtain any video surveillance coverage in the area.”)



- Assignments can be made by squad, external agency or by individual officer
- Descriptive and coded definition of the action to be taken
- Full status tracking (for example, “unassigned/active/closed/unresolved”)
- Priority allocation (for example, “urgent/priority/routine”)
- Date-required follow-up reporting
- Full generic task status reporting (for example, all outstanding actions for officer A)
- Linking of relevant IR’s to the line of investigation concerned
- Linking of relevant profiles to the line of investigation concerned

# TELEPHONE ANALYSIS/ ELECTRONIC SURVEILLANCE



SiD provides mechanisms for importing, storing and extending information captured by various means of electronic surveillance.

The detailed features of this facility are as follows:

- User-defined import data formats for data
- from various telecommunications agencies
- Excel® or delimited file support
- Direct link to SiD relationship build facilities
- Transcribers' log recording
- Audio log recording
- Generic output selection capability
- Output options to Excel®, i2® or multiple report formats
- Full reversal of import loads

**Maintain Analyser Log**

Operation Number: 1  
 Log Number: 2  
 Log Description: Phone tap re suspected drug dealer  
 Document Reference: 17JK42  
 Tape Reference From: TAPE 11-22  
 Tape Reference To: TAPE 11-456

Call Direction: No Repeating values  
 ISTD Code: [ ] Lookup  
 STD Code: [ ] Lookup  
 Number: [ ]  
 ISTD Default: 64 LSTD Default: [ ]

Call Date / Time	From Istd	From Lstd	Called From	To Istd	To Lstd	Number Called	Call Duration	Document Ref	Tape Ref	System Call ID
17/09/1994 18:15:00	64	3	1234567	64	3	9876543	00:00:58	29595	0C001	21
17/09/1994 18:18:00	64	3	9876543	64	3	1234567	00:01:02	29595	K1001	22
17/09/1994 18:21:00	64	3	1234567	64	3	9876543	00:01:05	29595	0C001	23
17/09/1994 18:25:00	64	3	9876543	64	3	1234567	00:02:56	29595	6E001	24
17/09/1994 18:55:00	64	3	9876543	64	3	1234567	00:05:12	29595	6E001	25
19/09/1994 11:45:00	64	3	1234567	64	3	9876543	00:03:55	29595	0C002	26
19/09/1994 12:07:00	64	3	9876543	64	3	1234567	00:10:16	29595	6E002	27

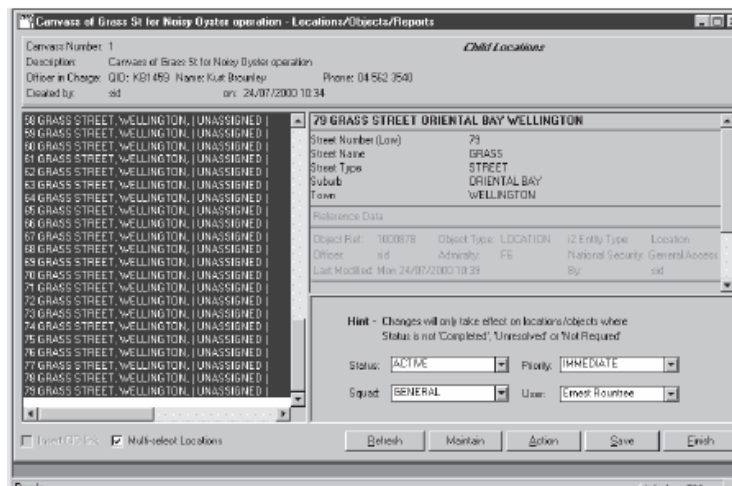
The Maintain Analyser Log window enables rapid, manual data entry.

# AREA CANVASS

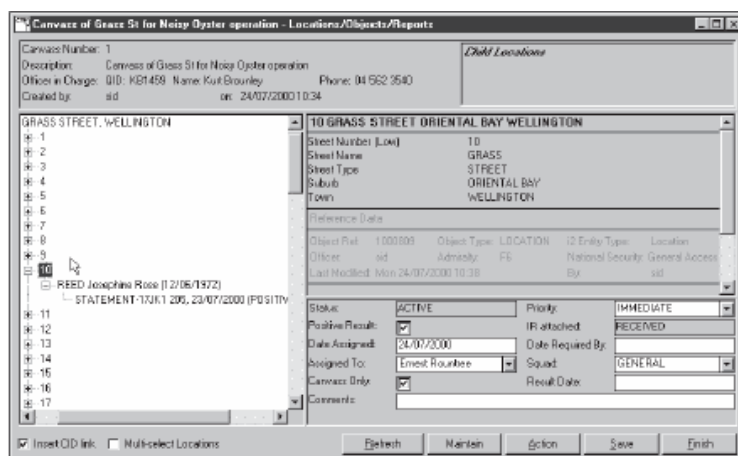


SiD provides mechanisms for managing an area canvass and reporting the status of a canvass via an integrated GIS tool.

The detailed features of this facility are:



The multi-assign feature saves time when assigning many locations to a single officer.



The Locations/Objects/Reports window allows rapid linking of objects and information reports to locations.

- User-defined import data formats for data from various GIS export formats
- Excel® or delimited file support
- Generation of street numbers for unmapped areas
- Full status tracking (for example, “unassigned/active/closed/unresolved”)
- Priority allocation (for example, “urgent/priority/routine”)
- Link to locations already recorded in SiD
- Linking of relevant IRs to the location concerned
- Linking of relevant profiles to the location concerned
- Generic output selection capability
- Output options to Excel®, i2®, GIS or multiple report formats
- Template definitions for capture of details (for example, “persons, vehicles, addresses”)
- Questionnaire definition, including facility for embedded photos
- Address checklist for assigned officers/squads

# SECURITY



Elaborate security provisions allow organisation-wide access to the database – while maintaining all levels of data protection and functional security. Exclusions are based on individual user privileges *and* assignment to particular operations, allowing precise control of access to data.

## Encryption

SiD has been implemented with a full public/private encryption mechanism for certification to beyond military standards, using third-party software.

## Functional Security

Functional security is delivered by a pre-defined set of user roles that give selections of functionality rights appropriate to the personnel roles in typical operations. Each role is aligned with the actual tasks performed by personnel in typical operations. They ensure personnel are granted appropriate access to functions. For example, typists should not be able to delete information reports, and officers in command should not be able to delete directives. Users need passwords to log on, and can have one user role only for each operation they are assigned to. These roles are organisation-wide, however if one person performs tasks from more than one role in an operation, a new user role can be created to allow for this. SiD maintains a history of role changes within operations.

## National and Operational Data Security

There are two kinds of data security: national and operational. National security is a hierarchical classification that is usually aligned to Government security classifications. When users enter information reports and objects in the database, they select the appropriate security level. Unless users have national security rights corresponding to, or higher than the security level of the object or information report, they cannot access data on it. This means searches do not return objects or information reports and relationships are not visible unless the user is authorised to access both objects or information reports.

### Manageable views of data

Operational security provides manageable “views” of data in the system, by presenting only information from the operation that the user is currently logged onto. These “views” may be expanded if relevant information might be available from other operations. A new operation is defined for each investigation, and where security requirements dictate, sub-operations may be defined within an operation (for example, for a covert operation running in parallel to the main operation).

# SECURITY (cont)



## Covert operations invisible to other users

A covert, internal operation may be run in parallel with an external investigation into the same incident. Personnel in the covert operation can use all data from the external investigation, but only the officers working on the internal operation will be aware that it exists. Similarly, officers working on undercover operations can safely enter data, and prevent their identities being revealed to personnel who are not part of the operation.

## Control the types of data from an operation other users can see

Operational security enables those setting up new operations to control what types of information users can access, depending on whether or not they are assigned to that operation. It is *additional* to national security: irrespective of the operational security level, users must have a national security level corresponding to, or higher than that entered for the information report or object, or they will not have access to it.

There are three kinds of operational security:

- **High**, means all information reports and objects entered for that operation are available only to users assigned to the operation.
- **Medium**, means all information reports entered for that operation are available only to users assigned to the operation. Objects are available to users with corresponding or higher national security levels, irrespective of whether they are assigned to the operation.
- **Low**, means information reports and objects entered for that operation are available irrespective of whether users are assigned to the operation.

The medium operational security setting has the advantage of preventing users who are not part of the operation from seeing the information reports which are particular to that operation, while allowing them to see object profiles, which may well be of interest to other investigations.

## Universal operational security upgrade/downgrade facility

If the operational security requirements change, all data from that operation can be universally upgraded or downgraded. For example, on completion of an operation, it may be useful to downgrade all data to allow general access. Similarly, additional security requirements may become apparent during an operation, and it can be upgraded to medium or high operational security at any time.

Information reports all have a security downgrade override option that, when selected, excludes them from any security downgrade.

## Audit Trails Kept Throughout

SiD keeps comprehensive audit histories of all changes made to data, as well as enforcing a business rule that ensures changes to evidential data are linked back to an existing source document (information report).

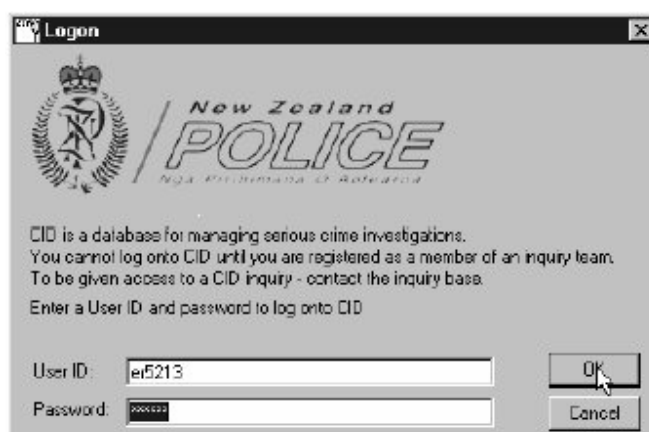
# SYSTEM SECURITY



SiD provides multiple levels of protection via data security and functional security access restrictions. SiD has proven capability for implementation with a full public/private key encryption mechanism (such as Smartcrypt) for certification to Top Secret level.

The detailed features of this facility are as follows:

- Individual user password protection – directly linked to database usernames
- User-defined levels of functional access with read/write/delete restrictions on any function
- Operation-by-operation data protection for IRs
- Operation-by-operation data protection for profiles
- User access only to assigned operations
- Unauthorised data is invisible to users
- National security override
- Database login protection
- Database security schema—secure



# TECHNICAL



SiD is a client server application. The system is scalable from a stand alone operation through to wide area network. Current implementations include multiple sites with nation-wide WAN operation.

- PowerBuilder/VB client (50MB Executable components)
- Thin Client Template data entry
- Oracle or MS SQL Server database support
- Recommended client - Standard Pentium 500 MHz (128MB RAM)  
Database client software required (Oracle only)
- Recommended for Stand alone:  
Pentium 800MHz (512MB RAM)  
Disk requirements, highly variable but indicatively, 200MB per operation  
Windows 9x, NT, 2000 and XP clients  
Interfaces:  
Importing and exporting – Office 95, 97 and 2000 – WORD and Excel  
Exporting i2 (version 6) - displaying link charts representing inter-object relationships  
Installation – Administrator privileges required

## FUTURE DIRECTION

- SiD is currently undergoing a face-lift and will soon be released as an n-tier .NET application.
- The Client Template data entry will be the first phased implementation under the new .NET platform.
- Among the many enhancements being incorporated in future version is the exposure of some of SiDs functionality as web services. This will allow easier connectivity with other applications.
- Another new feature is Multi-language support allowing SiD to be deployed in countries that do not speak English (or would prefer to use another language). This will also support complete customization of labels on the user interface to meet local business needs.