BEST® CIF

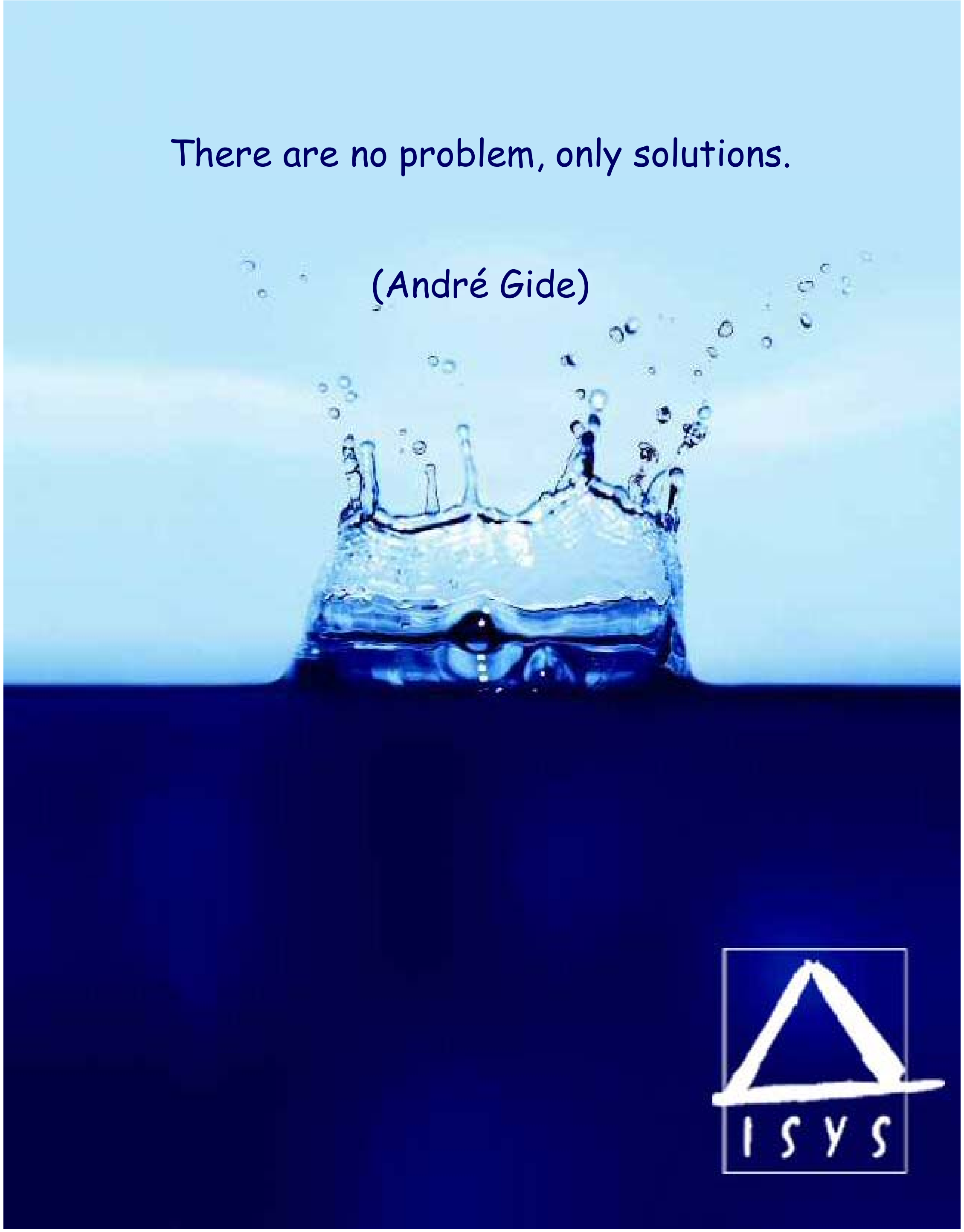
Central Information File

including the following modules:

BEST EDM
(Encrypted Data Management)

&

BEST DCS
(Document Confidentiality System)



There are no problem, only solutions.

(André Gide)

Agenda

BEST® EDM

Encrypted Data Management

Agenda

- Requirements/Objectives
- The Solution
- Selected Smart Cards
- System architecture
- Actors
- Overall security
- Certifications
- Final considerations

Requirements

- Management of confidential information contained in the Central Register File in a computerized way (instead of in paper format or on stand alone workstations), using a solid cryptography solution.
- Improve the overall security level of the current client confidential data management system.
- Allow a computerized check between client confidential information and World Check to automate the Anti Money Laundering and Compliance controls.

Objectives

- Confidentiality

  Hiding confidential data to who has not the permission for access them
- Data Integrity

  To prevent against who does not have the authority for data inputting, deletion, modification, …
- Authentication

  To verify the sender of every action onto confidential data
- Authorization

  To control the accesses, even at single function/object level
- Data Protection in regard to internal Information Technology Department

  To grant that the IT doesn’t have the clear access to ciphered data, even in case of physical theft of the disks
- To diminish the clear data exposure

  To only decipher the closely necessary data and for the minor possible time
- Communications

  To guarantee that all the information transit only through “sure” channels

The solution

- **BEST EDM** (hereinafter **EDM**) substitutes and improves the added physical security logics applied to the paper archives or to the stand alone workstation (usually placed in secured rooms) with an excellent improvement of the logical security level applied to clients confidential data. In other words, onto those clients confidential data are applied:
  - One more user authentication level by the use of smart cards (logon on card → PIN request)
  - A sophisticated data encryption logic onto the database
  - The information encryption onto the communication channels (between the client workstation and the server) during communications
- With **EDM** is possible to limit the number of the person that have the access to the confidential information, and it also possible to discriminate allowed data access and allowed application functionalities user by user
- The applied high-level data encryption does not make the application heavier for the hardware equipment in a perceivable way. For cipher/decipher data the waiting times are extremely shorts

The solution

- **EDM** contemplates the use of Java Smart Cards (meaning the Java Virtual Machine is entirely contained in the Smart Card) characterised by:
    - Smart Cart ID
    - PIN Code
    - PUK Code
    - User ID
    - Kind of Smart Card
    - User private key
- The Java Smart Cards are initially pre-configured for each institute to be sure that only internally configured smart card could be recognized by the application. Moreover all instances inside the Smart Cards are registered
- A Cardlet (program that allows to dialogue with smartcard, is required)

Selected Smart Cards

- Outlined Smart Card is Schlumberger Cyberflex Access Card
- Cyberflex™ Access cards (including the Cyberflex Access Developer 32K card) can operate with host-side programs written in a variety of programming languages, and can operate with programs designed to comply with the PKCS #11 specification or Microsoft's CryptoAPI architecture

- Cyberflex access cards support card programs, or card applets, written in compliance with Java Card 2.1.1 or higher specifications (Card applets are composed of Java byte codes and they contain all the objects needed by the program)

Selected Smart Cards

- Features of the Schlumberger Cyberflex Card:
  - Technical specifications:
    - Multi-application capable EEPROM: 32Kb
    - Global PIN capability & PIN sharing by application booklet
    - Interoperability
    - Secure Channel for communication with the card (mutual authentication of terminal application and cardlet, message digital signing and encryption using three 3DES keys: AUTH, MAC and KEK)
  - Standards compliance
    - ISO 7816
    - Java Card 2.1.1
    - Open Platform 2.0.1
    - 8-bit CPU micro controller
    - External Clock frequency: 1 to 7.5 MHz
    - Sleep mode
    - Temperature range from -25 to 75° C
    - EEPROM endurance: 700,000 cycles
    - Data retention: 10 years

System architecture

Applied Security standards:

- ISO 15408/CC Evaluation Criteria for IT Technology

  It is the first international information technology security evaluation criteria standard, defining Common Criteria (CC) used to evaluate security properties of information technology (IT) products and systems, such as operating systems, computer networks, distributed systems, applications and other hardware, firmware and software

- ISO 17799 Code of Practice for Information Security Management

  Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met. This is the subject of the standard

- FIPS 140-2 Security requirements for cryptographic modules

  This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system

System architecture

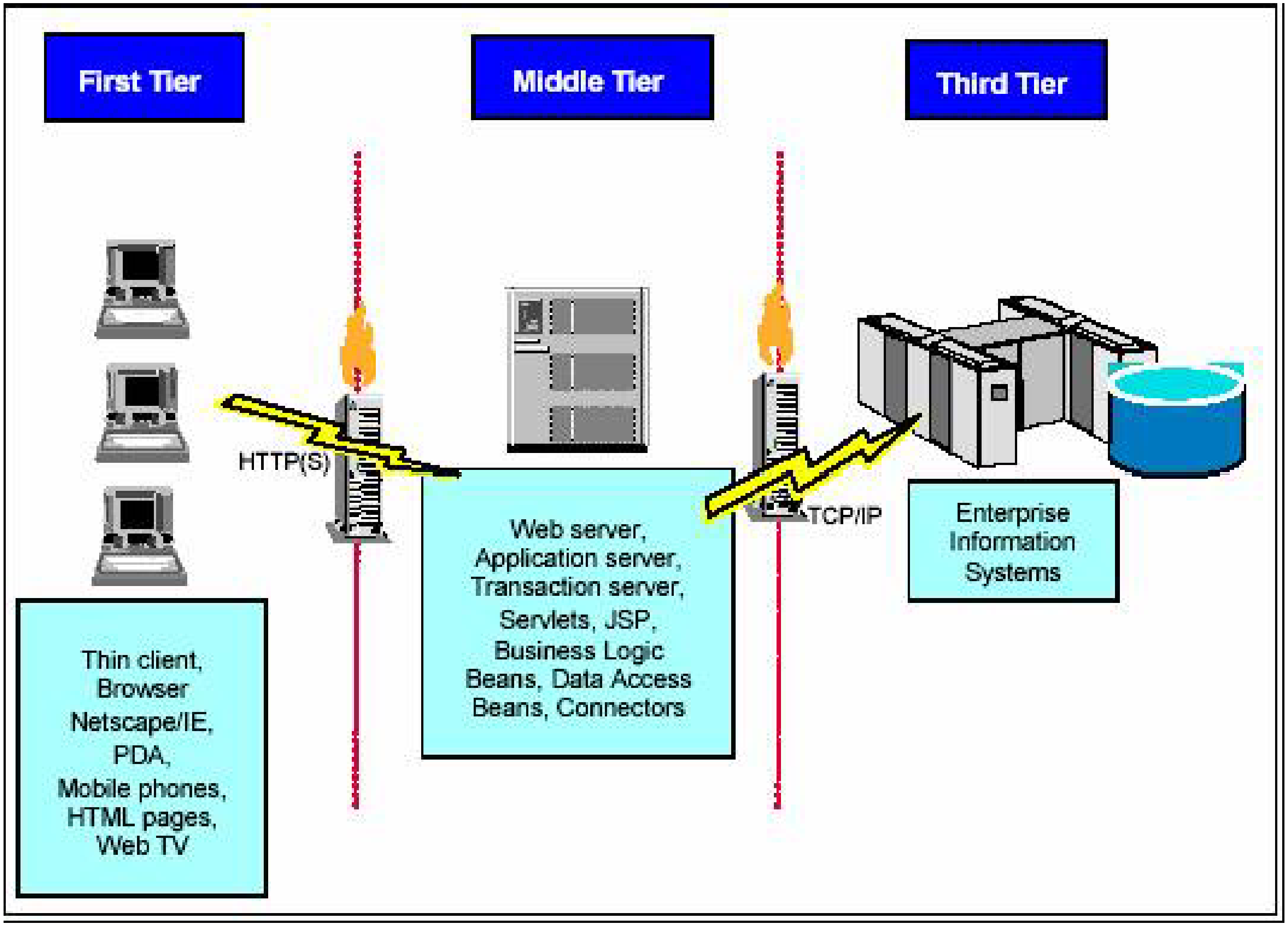
Applied encrypting schemas:

- Secret Key generation algorithm:
  - 3-DES 168 bits
  - Symmetric key
  - Key automatically generated
- Public and Private Keys generation algorithm:
  - RSA 1024 bits
  - Asymmetric keys (Public + Private)
  - Keys automatically generated
- Operative encryption/decryption logic:
  - Data are encrypted with the Secret Key (unique)
  - The Secret Key is encrypted with each user Public Key to obtain the Personalized Secret Key for each user.
  - The user Personalized Secret Key is decrypted with the user Private Key (contained into the user Smart Card) to obtain the Secret Key that allows the access to the data.
  - The Secret Key after first Cipher Manager generation is destroyed from the system.
  - Users Smart Cards do not contain the Secret Key.

System architecture

A common model for e-business solution development is based on an n-tier distributed environment where any number of tiers of application logic and business services is separated into components that communicate with each other across a network. In its most basic form, the model can be depicted as a “logical” three-tier computing model. This means that there is a logical, but not necessarily physical, separation of processes. This model is designed to support clients with high-function Web applications and servers for small and large enterprises. Following figure shows a high-level system model for running an e-business application.

System architecture



Actors

EDM contemplates following actors:

- Card manager (security)
- Cipher manager (security)
- Security officer (security)
- User

Note: To improve the security level is required that the three actors involved in the security lifecycle are different persons.

Actors

CARD MANAGER

- Functions
  - Does the smart cards set up for each user and generates the couple of keys (public and private). The private key is stored directly on the card while the public key is stored in the Public Key Database
  - Gives smart cards to users
  - Clears smart cards
- Who is?
  - An employee of security office or an IT user
  - Must be authorised to use the « Card Manager » program by the Security officer
  - Must have a « Card Manager » type smart card
  - Must not be authorised to use the « Cipher Manager » and to use the « User » applications

Actors

CIPHER MANAGER

- Functions
  - Manages the Personalized Secret Keys database, in other terms creates the Personalized Secret Key for each new user that needs it (no Card Manager).
  - Interact with the Security Officer for the Secret Key importing or re-keying activities

- Who is?
  - Should be a high-responsibility user
  - Must be authorized to use the « Cipher Manager » program by the Security officer
  - Must have a « Cipher » type Smart Card
  - Must not be authorised to use the « Card Manager » and the « User » applications

Actors

SECURITY OFFICER

- Functions
  - Assigns the operative authorisations
  - Controls the system logs
  - Interact with the Cipher Manager for the Secret Key importing or re-keying activities

- Who is?
  - The actual IT security responsible
  - Should have the right to define users role on the main server
  - Must have a « Security Officer » type Smart Card

Actors

USER

- Functions
  - Utilizes programs that use encrypted data
  - Can, accordingly to his rights, enquiry, modify, add confidential client data only for those clients for which he his entitled into Banking application and perform data migration and the comparison with World Check
- Who is?
  - A person of one of the subsequent departments:
    - Central File
    - Compliance
    - Internal Auditor
    - ???
  - Must be authorized to use the program by the Security officer
  - Must own a « User» type Smart Card
  - Should have the right to define users role on the main server
  - Must have a « Security Officer » type Smart Card
  - Must not be authorised to use the « Card Manager » and the « Cipher Manager» applications

Overall security

- All actors are ever bound to the subsequent login steps:
  - Smart Card logon (PIN request, 3 bad tries lock the Smart Card)
  - Server logon
  - Banking Application logon
- Moreover the application checks that the user that has done the logon onto the client workstation corresponds to the user stored into the Smart Card
- The separation of the duties in different actors contains the dangerousness of each single actor. A single actor does not have the right to do more than one stage of the security cycle (only 3 or 4 different actors acting together could represent a real danger)
- No ciphering/deciphering logic is present in client side programs; only authorized users having the smart card execute the cryptography programs on the Application server

Overall security

Security of keys

- Symmetric and asymmetric key generation is automated using IBM Crypto Lite in Java (module that module works in accordance with FIPS 140-2 specifications) . List of all keys is following:
  - Symmetric 3DES 168 bit key (guaranteed no weak key)
  - Asymmetric RSA 1024 bit key
  - PUK (from 6 to 12 bytes)

- Random key generation is effective for both symmetric and asymmetric encryption by usage of a qualified random key generation software module. IBM Crypto Lite module provides a good source of practically strong random data (a special algorithm patented in IBM).

Overall security

Security of communications

- Connection “Client / Application server”
  - End points in secure SSL communication are Web Application server and Web Browser on client side. Web browser instantiates Java applet inside HTML page for communication with Java Card applets. Java applet that is running inside Web Browser’s Java Virtual Machine is downloaded from Web Application server before execution, it is not resident in client operating environment. To be able to step outside the sandbox, it is signed and Web browser’s Java Virtual Machine automatically performs check on this
  - The communication is done exclusively by HTTPS protocol. The type of a SSL connection is a Version 2 “Server Only”
- Connection “Application server / Database server”
  - The communication is automatically, on iSeries server, ciphered with Secure Socket Level (SSL) JDBC

Overall security

- Connection "Client / Java Card"
  - To establish communication between Web Browser applet and Java Card applet, user must provide PIN information through Web Browser applet form. Only after provided PIN is successfully validated by Java Card applet, further user method calls could be accepted. If a card is removed from the reader, this state of a card is reset and subsequent communication with a card will require repeating of PIN validation process
  - During user login on a card, card serial number is read from the card and passed to the WebSphere application server to be verified against original card serial number recorded in a card personalization process. This is a security measure to prevent possible cloning of original Java Smart card
  - Another level of authentication of a Java Smart Card after successful login is obtained through matching private key extracted from Java Smart card with its public counterpart kept inside database, using IBM Crypto Lite software
  - Communication between terminal application and Java Card applet is protected using secure channel which includes encryption of sensitive data (e.g. PIN, PUK, private key, etc.) in both directions

Certifications

Third parties used products have the following certifications:

- Axalto Cyberflex smart card → FIPS 140-2 Level 3
- IBM CryptoLite in Java → FIPS 140-2 Level 1
- IBM WebSphere Application Server 6.1, enabled to use compliant FIPS 140-2 crypto modules
- IBM DB2 for i5/OS, enabled to use compliant FIPS 140-2 crypto modules

Where FIPS means Federal Information Processing Standard

EDM has fully passed various auditing controls in the banks where is in production.

Final considerations

- Dedicated Client PC

  When the smart card is removed or the application is ended the application stops and all temporary data are deleted
- Security Level

  It's necessary to individuate the necessary security degree to be satisfied by the application
- Disaster Recovery

  As in the normal Disaster Recovery strategy
- Back-ups

  Separate back-up for Data Database, Personalized Secret Key database, Public Key database (ciphered data).
- Smart cards
  - Have to be used in a controlled environment
  - Must be leaved to internal personal responsibilities
  - The network architecture can add security
  - Could be used also in an Extranet/Internet environment and/or for other purposes

Final considerations

- Overall security

  The security level is very advanced. However we know that if three or four different employers would act together against the company, and they cover all different actors in the security process, they could harm the system, even if they are every time tracked

- System quality
  - The whole system is very advanced and contemplates the use of IBM solutions, that do not need to be valued
  - This solution help to improve the internal security level, leaving all stored data (that are confidential for the bank) encrypted, and only an employee authorized for, with is own smart card, is own PIN, and is own key, after various authentication levels, could manage them

Agenda

BEST® DCS

Document Confidentiality System

Agenda

- Introduction
- The new solution
- Technology
- High-level workflows examples
- Installation

Introduction

The main scope of **BEST DCS** (hereinafter **DCS**) is to centralise and automate the document management process, with an integration with compliance and money laundering controls, extending the **EMD** (**E**ncrypted **D**ata **M**anagement) cryptography concept in order to have a front application of the central register module of **BEST**.

DCS is a server side web application entirely developed over new technologies. The application will use solid encryption algorithms developed by IBM (FIPS approved), the same already used by **EDM**, for that purpose.

DCS will allow also the management of document templates in order to automate (creating also bar codes on documents for automatic documents recognition and indexing) the whole process of relation opening making it fully STP.

DCS allows the bank to define the required workflow with a very simple parameterization activity.

The new solution

DCS allows:

- ✓ Simplified, centralized and STP account opening process (documents templates management, documents set management for kind of account to be opened, bar codes management for documents recognition, automated documents scanning (ADF scanners), automated documents indexing).
- ✓ Unique, centralized, Web application to manage client's data and documents both for ciphered and other clients.
- ✓ Indexed document storage and management of ciphered documents.
- ✓ High-level authorization and authentication mechanism based on smart card technology (the same used by **EDM**).
- ✓ Automated account opening in **BEST** and automatic client related data transfer in **BEST** (FCT061) and **EDM** (with documents reconciliation between different databases).
- ✓ Automated logging of all action performed by every user on **DCS** application.
- ✓ Simplified document modification/replacement process (thanks also to document versioning management).

The new solution

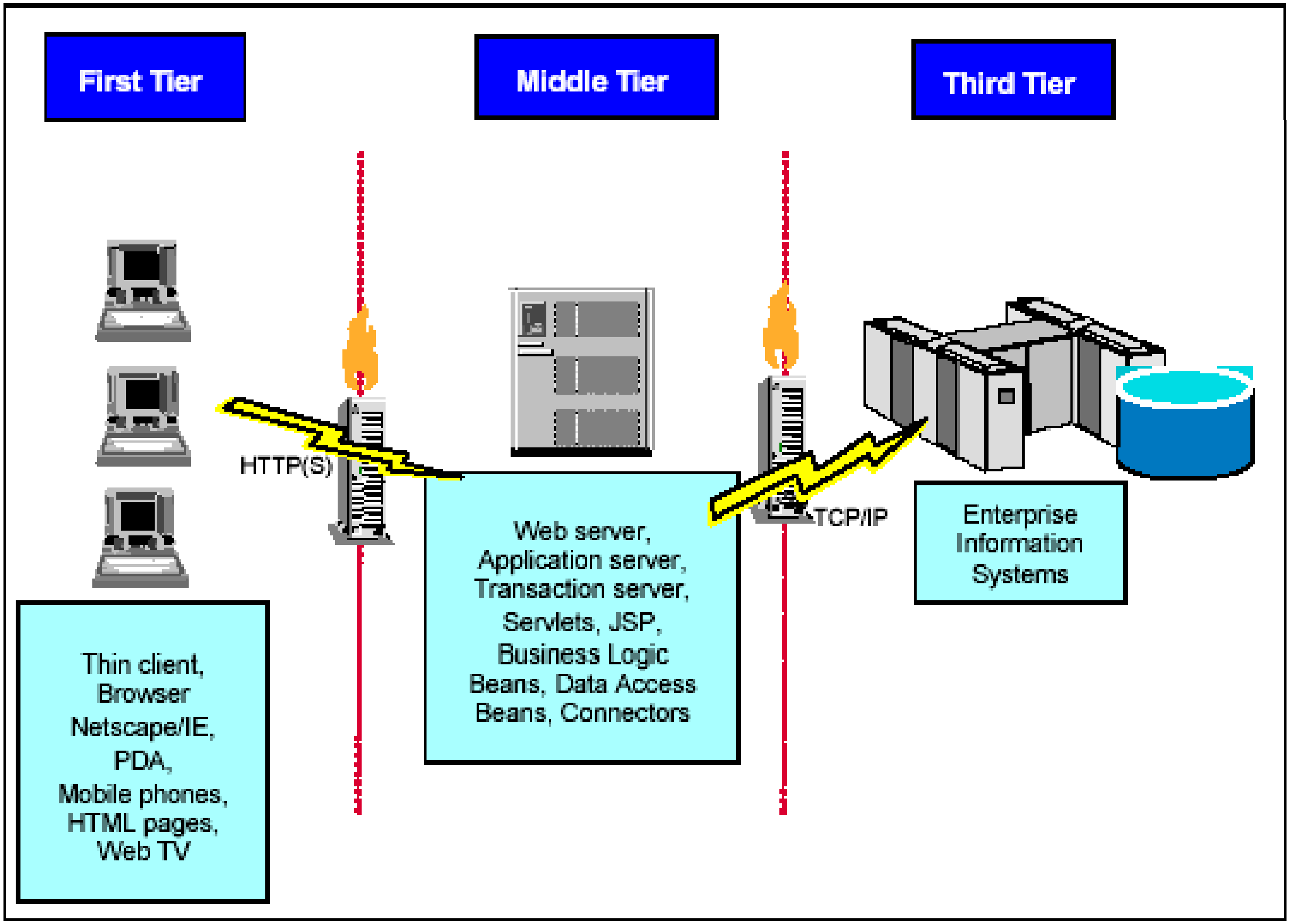
- ✓ Possibility to view the document directly from **DCS** application together with all client related data (i.e. signature control, compliance controls, ...), as well as from **BEST** only for authorized documents (no confidential documents).
- ✓ Different logical level of authorization for the various activities on client related data and documents.
- ✓ Assonance generation for the integration with World Check control (as in **EDM** and **BEST** **AML**), so on-line control as soon as name and surname are inserted.
- ✓ Automated signalling to Compliance in case of new account opening.
- ✓ Open workflow definition, inside the application will be present a workflow management system based on application parameters.
- ✓ Migration of actual documents in the new indexed and ciphered database.
- ✓ Possibility of an extension to a complete Customer Relationship Management application.
- ✓ Possibility to manage the account closing procedure, with closing documents management and check lists management.

Technology – Overall system design

Model for e-business solution

A common model for e-business solution development is based on an n-tier distributed environment where any number of tiers of application logic and business services is separated into components that communicate with each other across a network. In its most basic form, the model can be depicted as a “logical” three-tier computing model. This means that there is a logical, but not necessarily physical, separation of processes. This model is designed to support clients with high-function Web applications and servers for small and large enterprises. Following figure shows a high-level system model for running an e-business application.

Technology – Overall system design

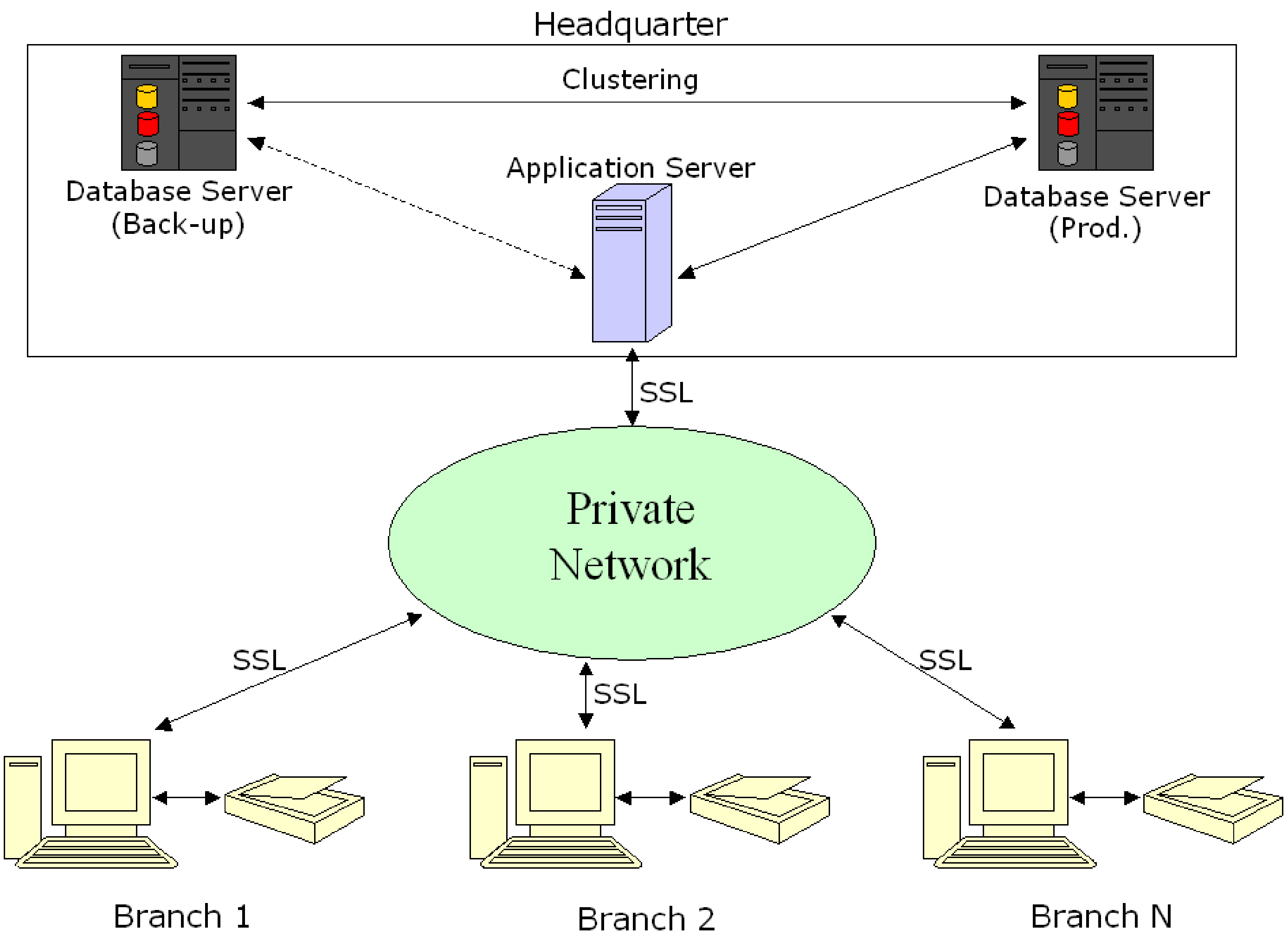


Thin client, Browser Netscape/IE, PDA, Mobile phones, HTML pages, Web TV

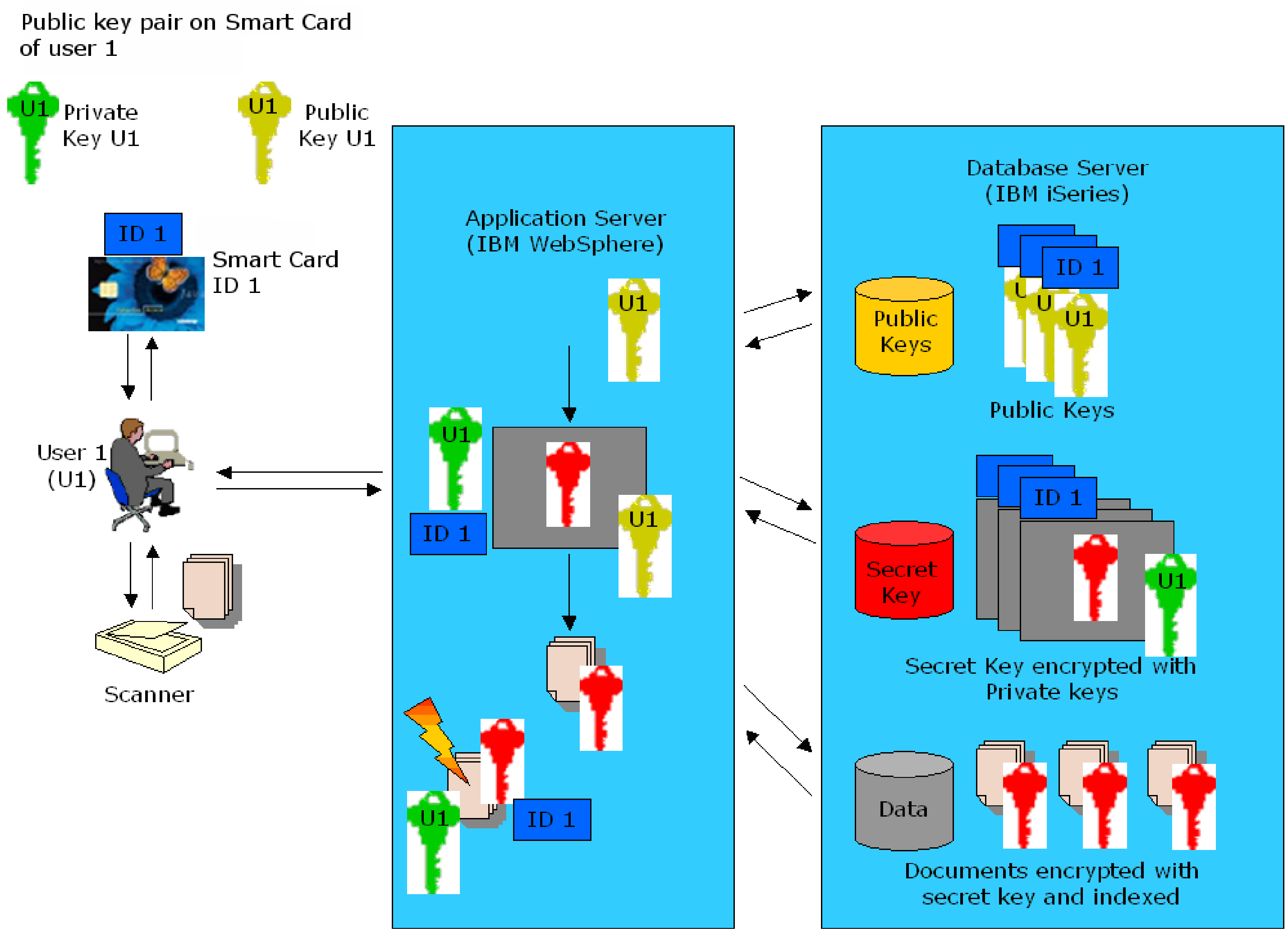
Web server, Application server, Transaction server, Servlets, JSP, Business Logic Beans, Data Access Beans, Connectors

Enterprise Information Systems

Technology – Overall system design



Technology – Security concept



Single login

DCS will consist in an extension of **EDM** module, in order to manage all account personal data, the document production (opening, complementary, new versions), the document retrieval, the document indexing, and so on…

As extension of **EDM**, the same login actually implemented for **EDM** are applied to **DCS** (so with automated check on **BEST** user and password and over authorities for branches and clients).

The authorized user after his authentication (smart card login, iSeries login, **BEST** login) will have at his disposal all actual implemented functionalities in **EDM** module, plus all new functionalities (**DCS** module) inside the same Web application.

Relation number reservation

First new functionality at user disposal is to ask the upcoming account number for an inputted client category and client subsidiary to reserve it in **BEST**.

Relation personal information management

The **BEST** **DCS** user will have the possibility to insert or modify all personal information behind an account (i.e. main holder information, holders information, ADEs information, powers of attorney information, plus all information that should be present on the documents like portfolio manager, assistant portfolio manager, evaluation currency, performance currency, and so on..).

The same after look logic actually available in **BEST** will be maintained, as well as all logics in force to attribute client fiscal status for IRS, all reasonability controls, and so on.

On-line World Check control

At any modification on relation personal information it is done an automated comparison with internal World Check (everyday updated accordingly to client subscription with World Check). In any case of possible matching the system will send to the user an alert message (as it is nowadays available inside **EDM** for numbered clients).

Documents template management

The documents templates will be managed within **DCS**. The user can modify existing documents templates or create new templates for new documents.

After having created a new template the system is able to automatically compile the required document with the available client data.

Set of mandatory documents management

The set of mandatory documents will be defined inside **DCS** application for each kind of account (numbered, named, company, and so on…).

In accordance to the kind of account to be opened the system is then able to automatically retrieve all mandatory documents to be compiled (automatically or manually in accordance with defined workflow) and printed out for the client.

Print of opening documents in blank

Inside **DCS** is possible to request the production of automatically compiled opening documents as well as blank opening documents (i.e. the portfolio manager has to go to the client to retrieve his data).

So it is possible to request for a pre-reserved account number to produce blank opening documents (only with the account number on them).

Print of automatically compiled opening documents

Inside **DCS** is possible to request the production of automatically compiled opening documents as well as blank opening documents (i.e. the portfolio manager has to go to the client to retrieve his data).

So it is possible to request, for an account number for which are available the necessaries personal data, the production of opening documents where are automatically reprised all available and necessary data. In case of lacking of required data the system sends an alert to the user.

Print of complementary documents

With the mandatory opening documents, there are other complementary documents. With or in addition to the request to print the mandatory documents the user can ask the system to prepare and print also other complementary documents.

If the request for complementary documents is made with the opening documents request, the system produces them in white if are required in white the opening documents or automatically compiled if are required automatically compiled the opening documents.

If the request for complementary document is made after the opening process, the required documents are automatically compiled with the available data. In case of lacking of required data the system sends an alert to the user.

Management of documents life-cycle

The system is able to automatically manage the status (pending, signed, expired, …) and the versioning of the documents.

Those information are automatically transferred to **BEST**.

Document retrieval via scanner/Document indexing

The system is able to retrieve signed document via scanner. Those document are produced with a bar code in order to be able to recognize (at their retrieval) and automatically index them into the document database.

When those document are retrieved via scanner they are transformed into pdf format to be encrypted and indexed archived.

All information about retrieved documents are automatically transferred into **BEST** to be used within the various application that check the availability of the documents (i.e. fiduciary orders, stock-exchange orders, ...).

Management of account status

The system is able to automatically manage the status of the account accordingly to the parameterized workflow.

As example the account could have the following status:

- Reserved (at number reservation);
- Pending DCS (as soon as information are inserted or white documents are printed, until opening document retrieval via scanner or information are completed).
- Pending 61 (until administrative information are not inserted).
- Pending compliance (until the ok for opening given by the compliance or by any other authority).
- Opened.

OK for opening management

The system is able to manage the “OK” for opening management.

Accordingly to the parameterized work-flow the system at one point will have to wait for an ok, to be given by the compliance or any other authority, that means that the account can be opened (all necessary documents are available, approval from compliance, …).

Workflow management

Within a workflow management system the authorized user can define the workflow to be implemented inside **DCS** application with a simple parameterization activity.

In other words is up to the bank to define the logical sequence of all available functionalities.

On-screen document retrieval

The stored documents could be retrieved (with all authorization controls on the client) by any authorized user inside **DCS** application.

Moreover some documents (accordingly to the system parameterization) could be also retrieved from **BEST** (i.e. signature forms).

Closing account management

In **DCS** is possible also to manage the following activities for the account closing process:

-Closing documents production

-Closing documents retrieval via scanner

-VISA function

-Check list of activities to be done (all single business closings) with possibility to have automated alerts via e-mail to the users

-Definitive account closing

Alerts and Printings

Accordingly to the parameterized workflow the system will automatically send alert to the user that has to continue the opening process (i.e. after the document retrieval the system sends an alert to the Compliance to inform it about new relation to be verified). These alerts are managed like flashing tests on the application (possibility to have automated e-mail sending), then the user can access a report table to see which accounts he has to handle.

Moreover the system previews all necessary printings:

-To view the handled accounts over a period and their status,

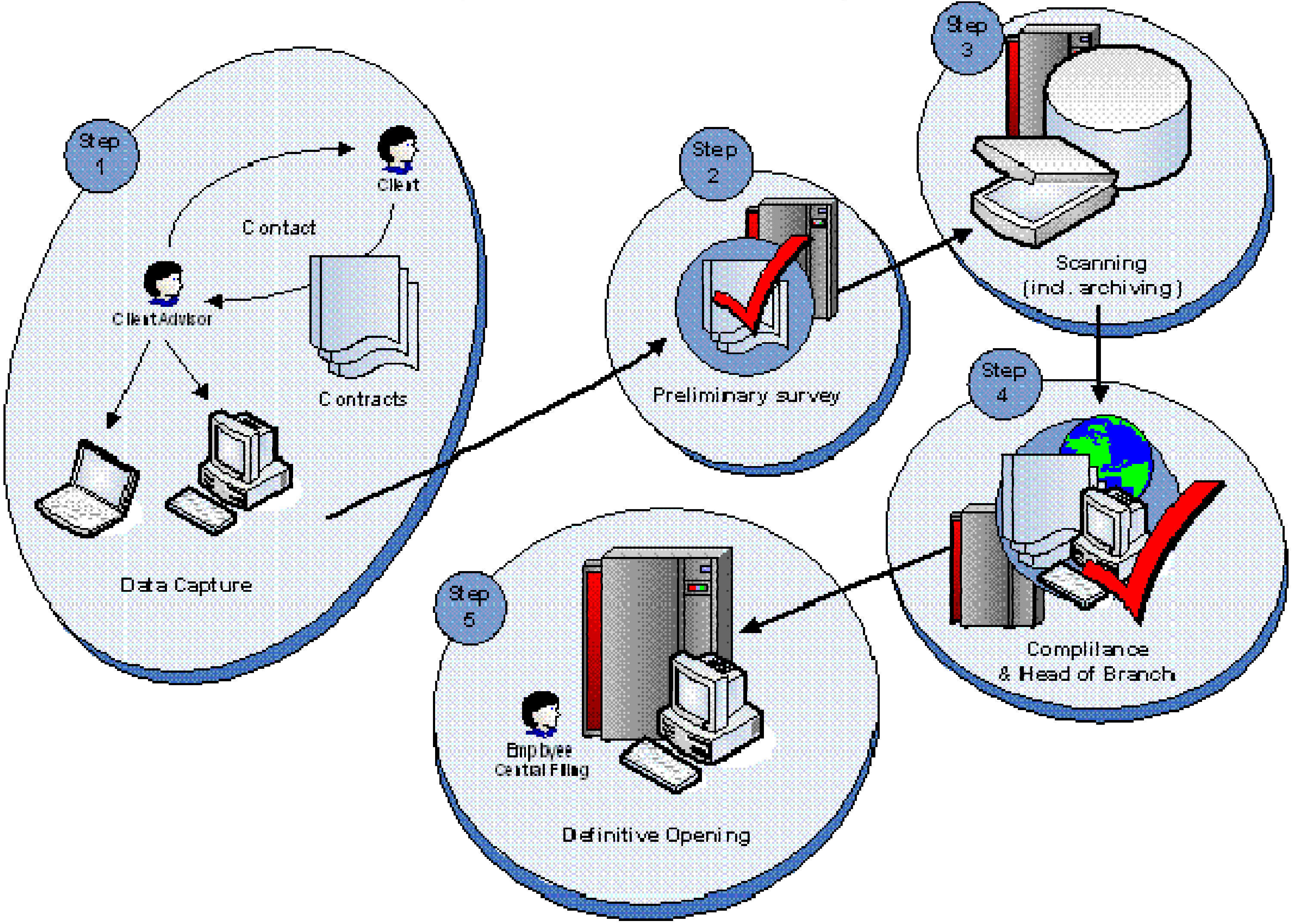
-To view the status of documents for an account or a group of accounts,

-To view all pending documents (printed and not signed),

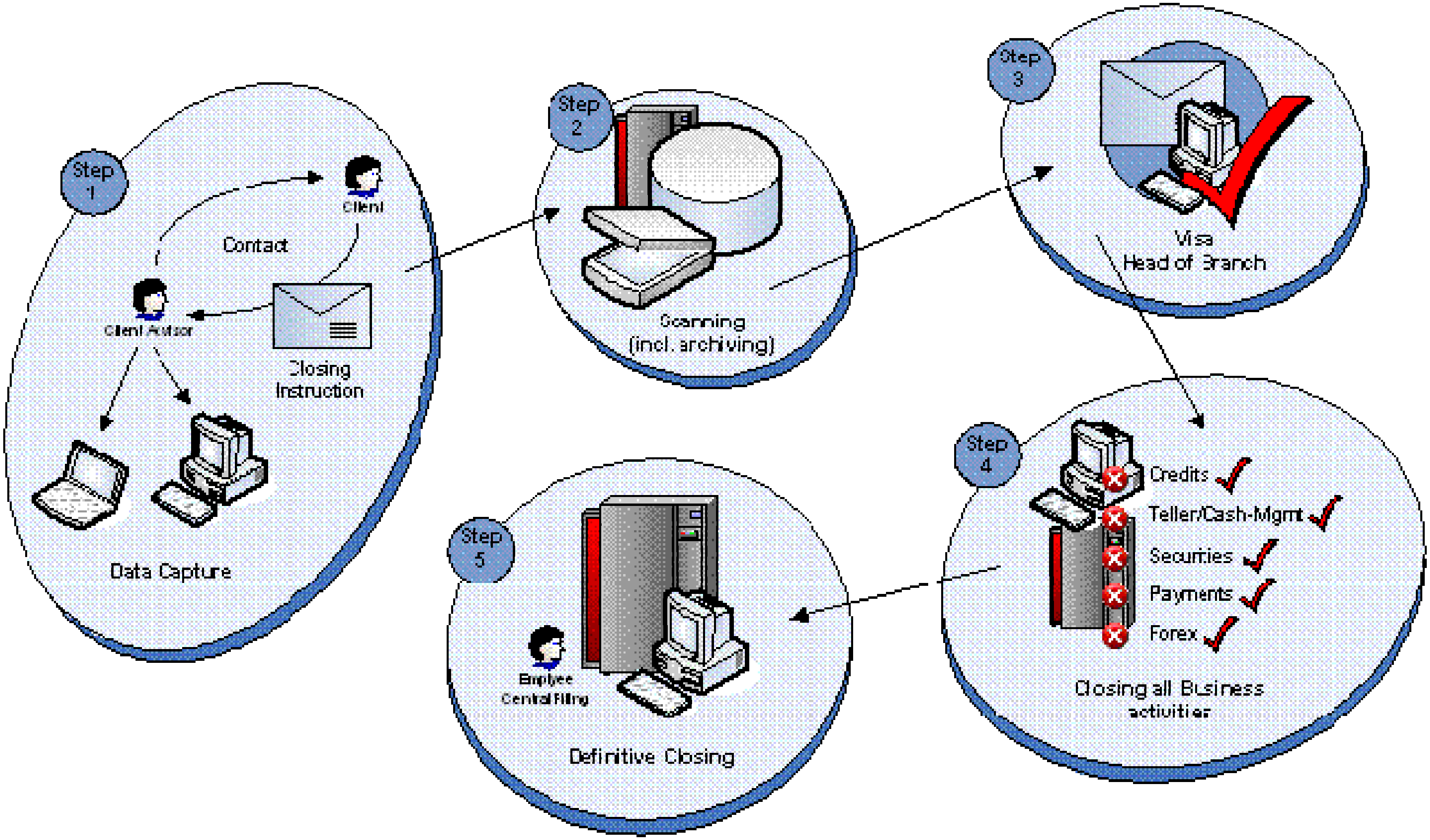
-To view all retrieved documents over a time period,

...

Hi-level workflows examples – Account opening

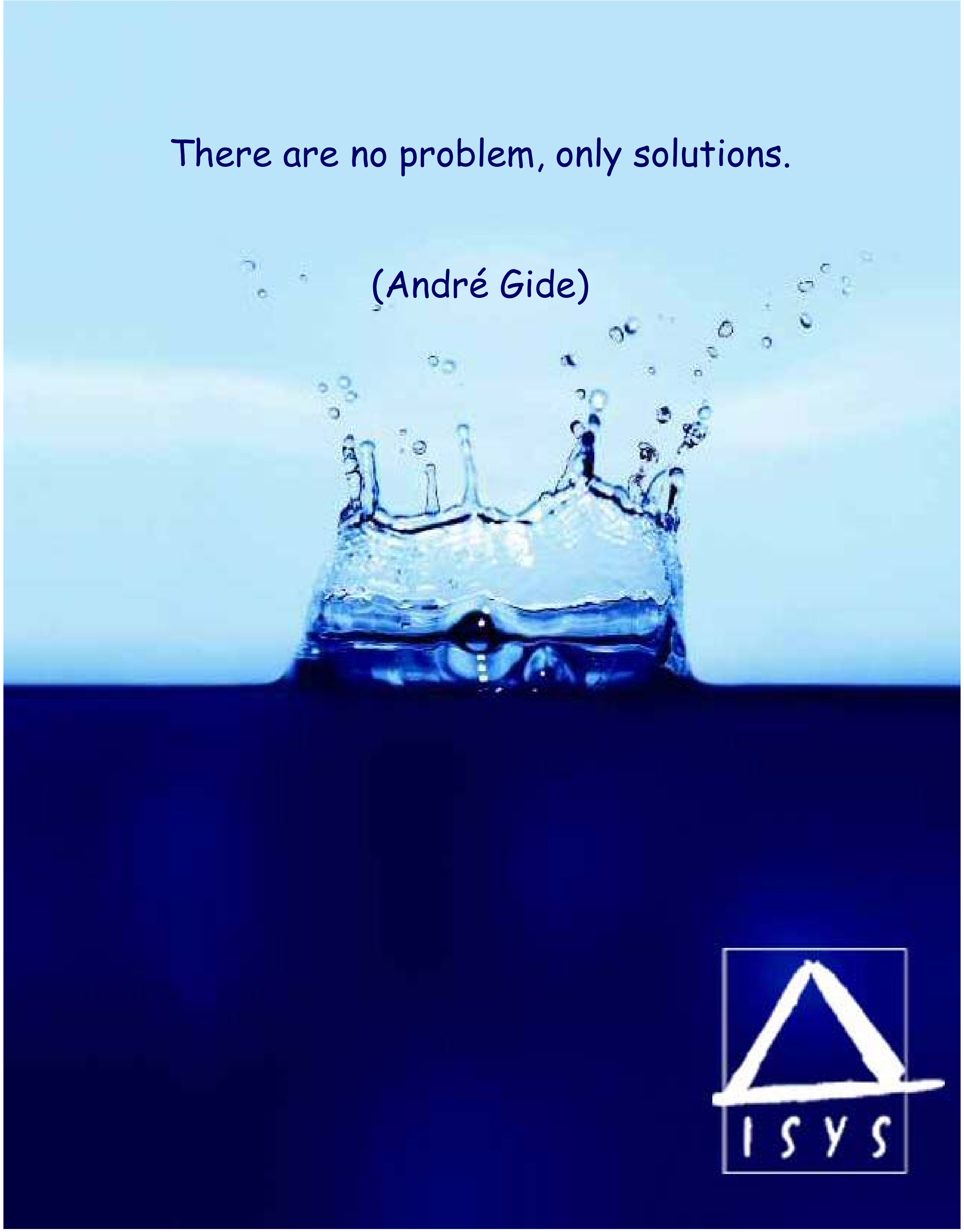


Hi-level workflows examples – Account closing



Thank you for your kind

Attention



There are no problem, only solutions.

(André Gide)