InterPARES 2 Project
International Research on Permanent Authentic Records in Electronic Systems

Title: Case Study 20 Final Report: Revenue On-Line Service (ROS)

Status:	Final (public)
Version:	3.0
Submission Date:	June 2005
Release Date:	September 2007
Author:	The InterPARES 2 Project
Writer(s):	John McDonough, Ken Hannigan and Tom Quinlan National Archives of Ireland
Project Unit:	Focus 3
URL:	http://www.interpares.org/display_file.cfm?doc= ip2_cs20_final_report.pdf

Table of Contents

List of Figures

Version History

Version 1.0	16/01/04	Preliminary Report	John McDonough
Version 1.5	28/02/04	Incorporating revisions from discussion at IP2 Plenary Workshop	John McDonough
Version 2.0	09/08/04	Formatting and Domain Questions completed [?]	John McDonough
Version 2.2	10/08/04	Inclusion of screenshots	John McDonough
Version 2.3	18/08/04	Incorporating feedback	John McDonough
Version 2.4	02/06/05	Final edit	Ken Hannigan Tom Quinlan
Version 3.0	21/08/06	Final copy edit and revisions; addition of Section G	Randy Preston

Disclaimer

It should be noted by readers that ROS is in continual development and Revenue are rolling out newer versions of the application on a phased basis. This case study was taken in late 2003/early 2004 and so does not take account of later development of the system.

Acknowledgements

We wish to thank Sean Connolly and his staff at the Revenue Commissioners IT section for their assistance in conducting and reporting this case study. In particular we would like to thank Tony Egan for his time and input to ensuring that follow up queries were answered swiftly and effectively.

A. CASE STUDY OVERVIEW

This case study of the Revenue On-Line Service (ROS) was first proposed to the InterPARES 2 International Team in September 2003 at the Los Angeles Plenary Meeting. The case study was proposed and led by John McDonough of the National Archives of Ireland.

The case study is concerned with examining the functionality and record creating and access properties of ROS. ROS is a high profile e-government service offered to tax agents and customers by the Irish Revenue Commissioners. The service operates as a stand-alone or online application, linking to a web based portal that allows Authorised and Approved Persons[1] to access relevant tax information, complete and submit tax returns and, if necessary, make or arrange payments online.

Revenue has spent in excess of 23 million Euro over the past five years in developing its online services and hopes to have 50% of taxpayers using the system by 2006. The rationale for developing the online service is quite simple:

> ...people don't really want to see us and we don't really want to see them. The whole process should work without too much actual interaction. It should simply happen as a matter of course.[2]

More specifically, the overall goal of ROS is stated as follows:

> The Government is taking a leading role in encouraging electronic business and the development of the infrastructure for Internet trading. As part of this initiative we in Revenue are developing Internet services that are of direct benefit to the majority of taxpayers. We have identified return filing as such a service and have set ourselves the target of having 50% of tax returns filed over the Internet by the year 2005.
>
> ROS is being developed as part of Revenue's overall Customer Service strategy. In addition to the current filing and payment options available to customers we are now extending these options to include Internet filing. The purpose of the exercise is to make it as easy as possible for our customers to comply with their return filing and payment obligations. The existing paper based filing system will of course remain an option.[3].

Following creation and validation (sign and submit), records are passed to Revenue's corporate back-office systems for processing in the same format as those records generated from paper tax returns (Figure 1). These records are marked on the back-office databases as having originated from ROS so that outputs can be generated in digital format for delivery to the customer or tax

[1] An Authorised Person is defined in S917G of the *Taxes Consolidated Act 1997* as "an individual who receives a Digital Certificate applied for on their behalf by an Approved Person," while an Approved Person is defined as "an individual who applies for a Digital Certificate for [his or her] own use or on behalf of and Entity, and who applies for digital certificates for Authorised Persons." Henceforth, unless specified otherwise, both Authorised and Approved Persons are implied in this report through the use of the more generic designations of "user" and "customer."

[2] Sean Connolly, Head of ICT Unit, Revenue, quoted in *Sunday Business Post,* IT supplement, October 2003.

[3] See http://www.ros.ie/info/faq_aboutROS.html#Question2.

agent via ROS. The outputs involved are Notices of Assessment, Payment Receipts, etc., and these are placed in the customer's Inbox in the ROS secure site. A copy of any tax return e-filed is also stored in the customer's Inbox so that s/he will have a record of what s/he has filed.

It is important to note that information supplied to the back-end systems impacts directly on the media and manner of outputs—paper based returns generate a paper output; electronic returns generate an electronic output.

The areas of particular interest focused on the use of digital certificates within ROS and how these are managed. The claims that the system meets requirements for authenticity, accuracy, and integrity of data were also examined, particularly in the light of the *Irish E-Commerce Act 2000*, which received input during draft stages from The Revenue Commissioners.[4] ROS was consciously promoted as a means to reduce errors in tax returns as Revenue had found that nearly 20% of all returns were inaccurate or contained human error.[5] The strong emphasis placed by the Irish government on the importance of e-commerce products for the Irish and European economies was also a factor in the selection of ROS as it has been championed as a best practice in e-government product, receiving several national and international awards. Some of these awards include the Public Sector Times Award for best e-government Web site, an Irish Internet Association award for the Revenue Commissioners' contribution to e-government, the ICT Expo award for best example of Public Service e-commerce implementation in the Public Service and the Digital Media Award for Innovation in Business to Business.

In November 2001, ROS was awarded a European Union (EU) e-government label, a symbol of recognised excellence, and, at an EU Conference in Italy (July 2003) on e-government, ROS was again recognised as being one of the very best practices of its type in the category of "The role of e-government for European competitiveness."

Conclusions

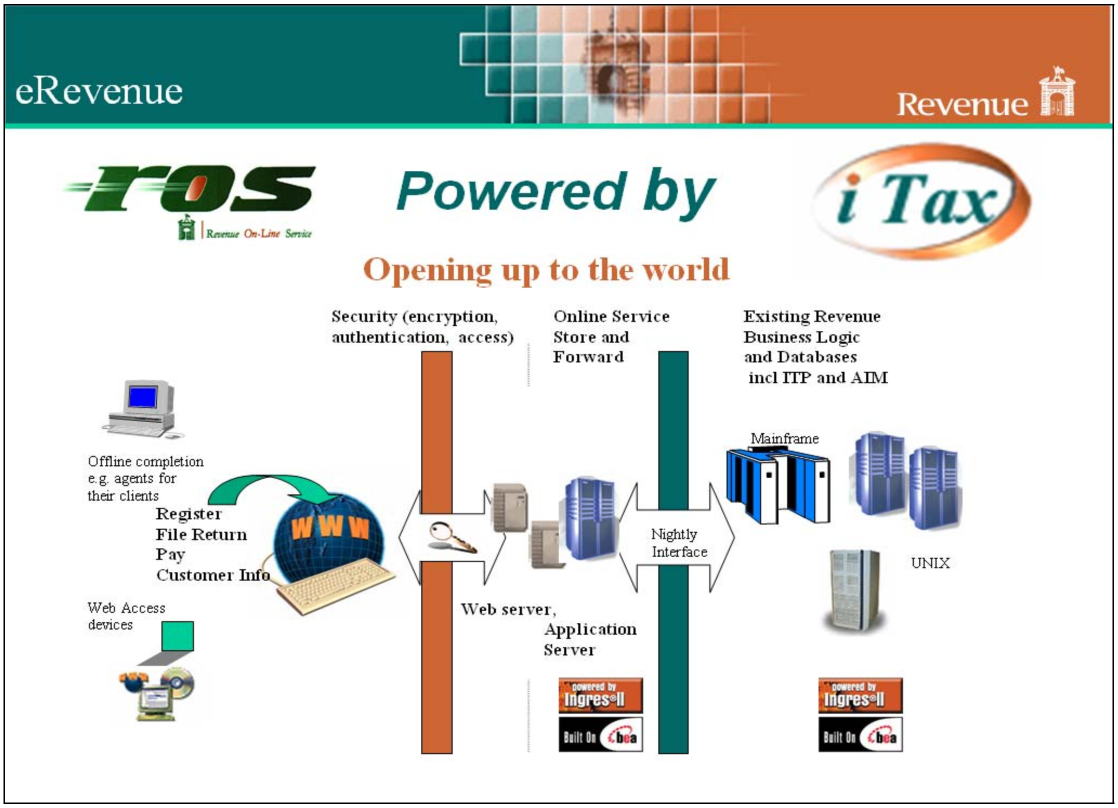
ROS is a dedicated system controlling both online creation of tax forms, and ingest of offline created tax forms. The system performs a set of validations to ensure that some of the data fields populated by users are accurate and can be checked using business logic.

The n-tiered system architecture separates some of the functionality of the record-making and recordkeeping systems using business rules to dictate the records contained in the subset stored within ROS.

ROS is very tightly integrated within the Revenue Public Key Infrastructure (PKI) environment and uses this to control access to the system. The use of PKI to confer 'non-repudiation' cannot be sustained, however. It remains to be seen what are the technical and legal implications of this, particularly in light of the *Irish E-commerce Act 2000*.

[4] Henceforth known as 'Revenue.'

[5] Baltimore Technologies (2003). "Securing Online Tax Services," *Customer Case Study*, Commissioned by the Irish Revenue Commission, p. 1. Available at: http://whitepapers.zdnet.co.uk/0,39025945,60111984p-39000550q,00.htm..



eRevenue

Revenue

ros Revenue On-Line Service

Powered by

i Tax

Opening up to the world

Security (encryption, authentication, access)
Online Service Store and Forward
Existing Revenue Business Logic and Databases incl ITP and AIM
Offline completion e.g. agents for their clients
Register
File Return
Pay
Customer Info
WWW
Web Access devices
Web server, Application Server
Nightly Interface
Mainframe
UNIX
powered by Ingres II
Built On bea
powered by Ingres II
Built On bea

Figure 1. ROS system architecture

There is no direct access to back-end systems. The creating agency has not communicated a long-term archiving policy for data stored in ROS/ITP[6] back-end systems.

ROS illustrates a growing number of e-government type systems that introduce additional levels of granularity in records creation, maintenance, access and preservation.

In short, ROS is a system that enables access. It offers a service within a tightly controlled environment. It allows for records creation and presentation. In this sense it is not a dynamic system, however, as evidential and authentic weight occurs only after the formal signing and sealing.

[6] Integrated Taxation Processing (ITP) is the central component of Revenue's overall Integrated Taxation Services framework. "It is a single, shared back-office system for the issuing of returns, the processing of returns and payments and the main collection activities for all the major taxes. It merges fully with the Common Registration System and the Active Intervention Management functions, providing a fully integrated computer support for Revenue's major business functions. ITP provides the platform for [Revenue's] Internet service through the Revenue Online Service (ROS) (Office of the Revenue Commissioners Ireland (2004). "Request for Tender (RFT): IT Solution to meet Customs Administration and Enforcement Requirements," p. 14. Available at: http://www.revenue.ie/aboutus/procurement/rft.doc).

B. Statement of Methodology

- Preparation of 50 questions based on 44 questions and 23 questions (September 2003)
- Submission of proposed question to Revenue for consideration (September 2003)
- Interviews (October 2003)
- Receipt of ROS offline application (November 2003)
- Use of available documentation and Web sites (January 2004)
- Compilation of secondary questions to meet shortfalls and gaps (April 2004)
- Round two communication and clarifications (May 2004)
- Draft Report submitted to Focus 3 for comments (September 2004)
- Final Report submitted (June 2005)
- Final Report revised (July-Aug 2006)

C. Description of Context

ROS is a digital capturing and publishing system used by Revenue to facilitate the electronic filing and payment of a range of tax returns in a secure online environment. It allows users, including both self-assessment taxpayers and agents, to securely log on, file tax returns, pay tax liabilities, and view details of their transactions with Revenue.

The key design features of the ROS application are listed below:

- The system is designed to allow Tax Agents or other registered agencies to make returns on behalf of their clients.
- Where it is beneficial to the customer, ROS forms have both online and offline versions available.
- All online submissions are instantly acknowledged.
- The ROS Access Control System allows a Tax Agent or a business to restrict staff access to ROS facilities as appropriate for their responsibilities. This facility is entirely in the control of the customer. This was designed and implemented in consultation with the main ROS users and large accountancy firms.
- The system provides a personalized secure Inbox for each customer. It allows Revenue to issue instant acknowledgements, receipts, notices of assessment, etc. to each ROS user. The ROS Inbox facility includes archive and search features. Generic e-mails are sent to alert customers that there is an item in their secure Inbox.
- Detailed help facilities, Frequently Asked Questions and demonstrations are available throughout the Web site.
- Where possible, forms are pre-populated with key information and tailored forms are presented based on data entered on the form.
- A rollover and an import facility are available in the offline application for some forms.
- Many forms are available in the Irish language as well as English and the site is screen reader compatible for users who are visually impaired.
- Batch filing facilities are available.
- A bulk filing facility is utilized for the uploading to ROS of employee cessation certificates (P45's) by an outside data processing contractor.
- The system is fully integrated with the Revenue business systems.

Provenancial

Revenue Commissioners Overview, Mission and Mandate[7]

General

The Office of the Revenue Commissioners was established by Government Order in 1923. The Order provided for a Board of Commissioners. The Board comprises a Chairman and two Commissioners all of whom carry the Civil Service rank of Secretary General. The Chairman of the Board is also the Accounting Officer for Revenue. The Mission Statement of Revenue is:

"To serve the community by fairly and efficiently collecting taxes and duties and implementing import and export controls."

Staff and Geographical Spread

There are in excess of 100 Revenue offices countrywide with a staff complement of over 7000 (approx.).

Core Business

The core business is the assessment and collection of taxes and duties. Revenue's mandate derives from obligations imposed by statute and by Government and as a result of Ireland's membership of the European Union. In broad terms the work includes:

- assessing, collecting and managing taxes and duties that account for over 93% of Exchequer Revenue;
- administering the Customs regime for the control of imports and exports and collection of duties and levies on behalf of the EU;
- working in co-operation with other State Agencies in the fight against drugs and in other cross Departmental initiatives;
- carrying out Agency work for other Departments;
- collecting PRSI [Pay Related Social Insurance] for the Department of Social, Community and Family Affairs; and
- providing policy advice on taxation issues.

Organisational Structure

Revenue's structure is designed around its customer base. Revenue Regions are responsible for customers within their geographical area, except for those large corporates and high wealth individuals dealt with by the Large Cases Division. There are also policy, legislation and interpretation functions.

[7] Taken from: http://www.revenue.ie/aboutus/rev_view.htm (Accessed 31 May 2004).

The main divisions and their roles within Revenue are as follows:

Division	**Role**
Strategic Planning Division	Supporting the Board in setting and reviewing corporate strategy and performance. Includes the Accountant General's Office.
Human Resources Division	Human resource management strategies, including training, manpower planning, PMDS, and employee assistance services.
Information, Communications Technology and e-Business Division	Information technology tools and services, telephony and logistics.
Operations Policy and Evaluation Division	Developing operational policy and supporting the operational areas in identifying and disseminating best practice.
Investigations and Prosecutions Division	Managing and co-ordinating all of Revenue's prosecution activity, particularly for serious cases of fraud and evasion.
Revenue Solicitor's Division	Provision of comprehensive legal support services, including the conduct of litigation and appeals and the prosecution of criminal offences.
Customs Division	Policy, legislation and international functions for Customs, including FEOGA (European Agricultural Guidance and Guarantee Fund) audit.
Direct Taxes Policy and Legislation Division	Policy and legislation functions for all of the direct taxes, including capital taxes.
Direct Taxes Interpretation and International Division	Interpretation and international functions for all direct taxes, including capital taxes.
Indirect Taxes Division	Policy, legislation, interpretation and international functions for all indirect taxes.
Collector General's Division	Collection and lodgement of the major taxes. It also operates pursuit mechanisms for those who fail to comply.

Juridical-Administrative

Revenue's Role and Responsibilities

The Irish Revenue is responsible for the collection and management of taxes and duties within the Irish Republic. Working to regulations imposed by Government, and as a result of Ireland's membership in the EU, Revenue also administers the Customs regime for the control of imports and exports and collection of duties and levies on behalf of the EU. During the lifetime of its current Corporate Plan, Revenue will collect gross revenues in excess of £60 billion.

The fundamental juridical context for the Revenue Commissioners dates back to 21 February 1923, when the Office of the Revenue Commissioners was established by Order 2/23. Order 2/23 established a single Board of Revenue Commissioners consisting of three Commissioners, one of whom is designated Chairman and Accounting Officer. The Order stipulates that the Board establish its chief office in Dublin.

The Order further stipulates that the Revenue Commissioners shall, in the exercise of their duty, be subject to the control of the Minister for Finance and shall obey all instructions issued to them in that behalf by the Minister. On 13 March 1923, the Minister for Finance further clarified the role of the Revenue Commissioners, as follows:

> While the Revenue Commissioners will be responsible directly to the Minister for Finance for the administration of Revenue Services, the Commissioners will act independently of Ministerial control in exercising the statutory powers vested in them in regard to the liability of the individual taxpayer.

The increase in the range, scope and powers of the Revenue Commissioners can be tracked through the various Finance and Tax Acts passed by the Irish Oireachtas (Parliament) over the last eighty years. Additionally, Ireland's membership in the EU since 1973 (then the European Economic Community) has required Ireland to adopt European-wide tax and excise legislation.

Of particular interest to this case study are the following acts:

- *Taxes Consolidation Act 1997,* allowing for the filing of tax returns electronically.

- *E-Commerce Act 2000*, articulating the policy in law regarding the creation, use and management of digital signatures and giving parity in weight to both paper and electronic documents and records.

Procedural

Revenue's Business Procedures for ROS

ROS is used to replace paper-based transactions, maintain existing levels of confidentiality and incorporate a level of security into an electronic transaction. Digital entities are created in the course of filing tax returns and paying taxes due to the Revenue Commissioners.

ROS is Revenue's interactive Internet facility providing business customers with a quick, secure and cost effective method to conduct their business electronically with Revenue. All correspondence between the ROS customers and ROS is encrypted using Public Key Infrastructure (PKI) technology,[8] and ROS customers are identified by their digital certificates. Also, all forms/tax returns are subject to validation and will not be accepted by the system until they pass this validation.

Procedural Controls for PKI

1. Certification Practice Statement[9]

The purpose of this document [PD0018] is to provide factual information describing the Certification practices employed by the Revenue Certificate Authority (CA) in relation to the following:

- Management of its PKI.
- Administration of the Revenue PKI under the Certificate Policy Statement (CP) as issued by the Revenue CA.
- Certificate lifecycle within its PKI.

These practices are detailed in the formal statement attached as Appendix 2 – Certification Practice Statement (CPS).

The Revenue CA is a self-signing Certification Authority. It should be noted that the Revenue CA and other Certification Authorities may issue multiple Certificate Policy Statements (CP) mapped to this CPS. In each case, the corresponding CP within this CPS will be nominated. For further details, see Appendix 2.

2. Certificate Policy Statement[10]

The purpose of this document [PD0039] is to inform those who may be issued with Certificates by the ROS CA of their rights and obligations. It also sets out the procedures the

[8] PKI technology involves the use of a 'key pair' consisting of a 'private key,' used by an approved person to create a digital signature, and a 'public key,' used by Revenue in an asymmetric cryptosystem to verify a digital signature that a private key creates.

[9] The following text is taken from: Office of the Revenue Commissioners Ireland (2000). "Revenue Public Key Infrastructure: Certification Practice Statement," p. 7.

[10] The following text is taken from: Office of the Revenue Commissioners Ireland (2000). "Revenue On-Line Service: Certificate Policy Statement," pp. 8-9.

ROS CA is to follow in discharging its obligations to those persons. The ROS CP has been produced in accordance with the general provisions of the Irish Government's policy and guidelines on the protection of information and information technology environments. The ROS CA is operated under the Revenue PKI in accordance with the Revenue CPS.

Documentary

Documents and records created by ROS

The originating framework for the records created using ROS is the legal obligation on companies and individuals to pay the taxes owed to the Irish state. Tax collection is the fundamental role of Revenue, and ROS enables Revenue to offer a speedy, secure and efficient means to submit data and payment details electronically. Given that Revenue has used ICT for several decades and maintains databases of electronic tax records, ROS facilitates the management of such records by having information keyed in by the creating agent rather than by having Revenue employees manually keying in data to back-end systems.

The entities identified in this case study are the digital certificates and associated signatures used by ROS and approved or authorized users, the various forms being made available electronically through ROS, and the payment details, such as the ROS Debit Instruction (RDI)

It is important to note that ROS is deliberately configured and presented so that the electronic forms mirror paper forms. Revenue further allows for their XML DTDs to be obtained for inclusion in third party software. This open approach is to ensure compatibility and maximize take-up of the electronic-based system.[11]

Technological

ROS IT Infrastructure

It should be noted that Revenue's ICT policy is twofold. Information Technology is used as a means to improve continuously the service to citizens, and as an efficient tool to counter tax evasion.[12]

The technological context is as follows:

- Security, including PKI environment
- Web site standards
- Internet protocols
- Data capturing and interfacing
- Back up and disaster recovery

[11] See Office of the Revenue Commissioners Ireland (2000). "Notes documentation for Income Tax Return for the Tax Year January 1st 2003 – December 31st 2003," Revenue Online Service. Available at: http://www.revenue.ie/pdf/f1103not.pdf.

[12] Sean Connolly, Head of ICT Division, Revenue. Course Notes for DCU lecture series on IT Systems and Public Sector.

The main application hosting and maintaining the digital environment is an Advantage Ingress 2.5 Relational Database. Core customer data is refreshed on a nightly basis from the corporate ITP back-office system.

The system uses open source, off-the-shelf applications where appropriate. However, the system required the development of a Java-based Off-Line Launcher, which is a proprietary ROS application required for submission of offline tax returns.

Minimum system requirements for users are given for MS Windows, Apple Macintosh and Unix/Linux systems. They are available at: http://www.ros.ie/PublisherServlet/requirements and http://www.ros.ie/PublisherServlet/info/faq_systemreq.

ROS Public Key Infrastructure

To ensure the integrity and security of all interaction with its customers, Revenue operates a PKI in association with LanCommunications/RSA Security that is in conformance with Recommendation x.509.[13]

System Architecture

All of the ROS system's components, including its security system, were built using open industry standards to: (1) minimize the footprint from the users' perspective (i.e., system is accessed via a standard Web browser), (2) increase the interoperability of its components, and (3) facilitate the re-use of Revenue's existing frameworks and systems.

The server side of the ROS system is built using Java, which allows it to run on any platform supporting Java, including UNIX and Windows NT, and increases the ability to easily accommodate individual architectural components. On the client side, for example, the return filing components, which by default operate in HTML, can easily be replaced with custom, third-party form software.[14]

The main system components, requirements and supported applications include:

- J2EE n-tier platform;
- BEA WebLogic and iPlanet Web servers;
- Advantage Ingress 2.5 relational database;
- Browser technology (HTML / XML) client interface;
- Both Internet Explorer version 4.1 or higher and Netscape Communicator version 4.x or higher are supported;
- Windows 95 or higher, Windows NT and Apple Macintosh operating systems;

[13] Recommendation x.509 is a specification for digital certificates published by the ITU-T (International Telecommunications Union - Telecommunication). It defines a standard certificate format for public key certificates and certification validation information and attributes required for the identification of a person or a computer system. See http://www.itu.int/rec/T-REC-X.509/en.

[14] Office of the Revenue Commissioners Ireland (2004). "Request for Tender (RFT): IT Solution to meet Customs Administration and Enforcement Requirements," p. 37. Available at: http://www.revenue.ie/aboutus/procurement/rft.doc.

- Adobe Acrobat Reader on the client side—required for reading documents issued by ROS in .pdf format;
- Application, Web, and database servers hosted on Sun Solaris;
- Security based on Baltimore Key Tools Pro (PKI);
- Additional security elements are 128 bit SSL encryption and Verisign Global certification.

D. Narrative Answers To The 23 Core Research Questions

1. What activities of the creator have you investigated?

a) Digital Certificate Creation and Delivery

There are three preliminary steps in the process of receiving Approved (in the case of an individual) or Authorized (in the case of a tax agent) User status in ROS:

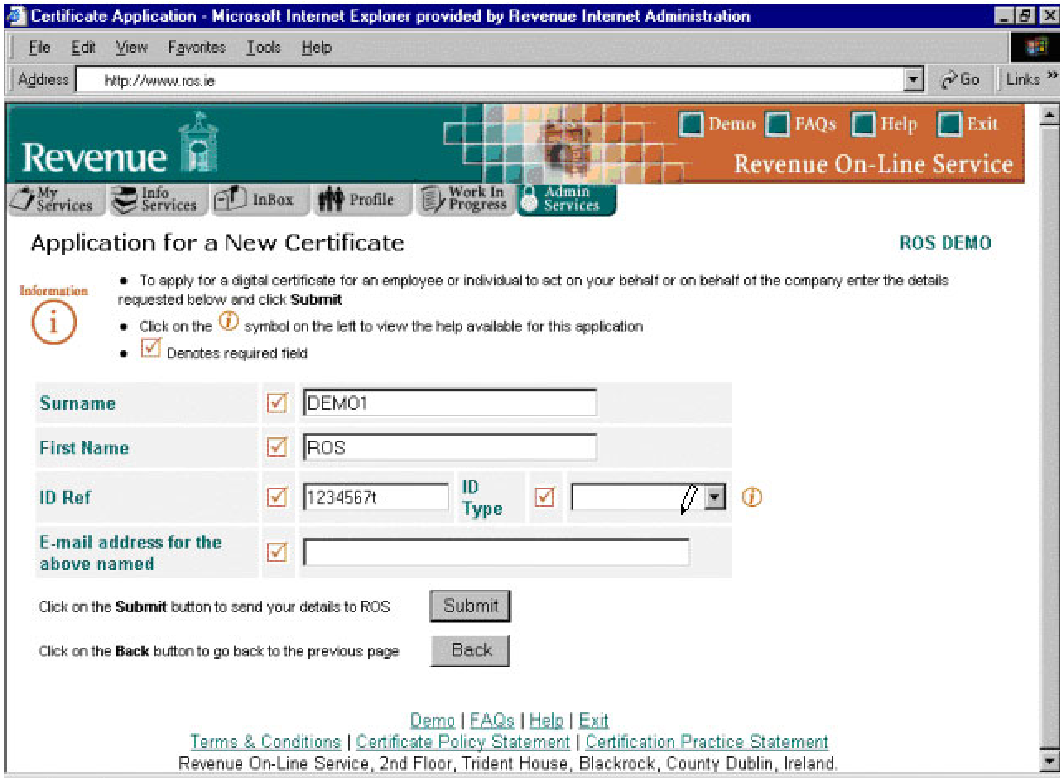
1. Obtain ROS Access Number (RAN) or Tax Agent Identification Number (TAIN) for a tax agent, and separate password;
2. Apply for digital certificate (Figure 2); and
3. Retrieve digital certificate.

ROS requires that a new user have a valid RAN or TAIN that is obtained directly from Revenue. Applications for this Identification number are made online but are posted to the individual by traditional mailing methods to maximise security. A separate password is also generated and posted separately. Revenue uses traditional mail to deliver to the customer address already on record to minimize risk of misrepresentation.

All users of the ROS application must be registered taxpayers and citizens of the Irish State and, as such, hold a PPS (Personal Public Security) number. When applying for the RAN or TAIN, some personal information such as name, address, PPS, phone number and e-mail address is requested. Following receipt of the RAN, the new user can then go online onto the ROS Web site and with the RAN and password obtain their digital certificate and download their private key.

b) User Management

The ROS system is designed for use by individuals and agents acting on behalf of individuals. All agents require an additional agent registration number from Revenue before they can be set up as Agents on ROS. User management is twofold: (1) the creation of an agent account with authorization from clients for the agent to act on their behalf in ROS, and (2) digital certificate and sub-certificate management. The latter option allows for the certificate administrator to create associate or sub certificates to the administrator certificate. Options exist for the new user to have “No Permissions,” “View,” “Prepare” or “File” rights for the various tax types granted to him/her (Figure 3). Revoking permissions is the opposite.


Certificate Application - Microsoft Internet Explorer provided by Revenue Internet Administration
File Edit View Favorites Tools Help
Address http://www.ros.ie
Go Links
Revenue
Demo FAQs Help Exit
Revenue On-Line Service
My Services
Info Services
InBox
Profile
Work In Progress
Admin Services
ROS DEMO
Information

Application for a New Certificate

- To apply for a digital certificate for an employee or individual to act on your behalf or on behalf of the company enter the details requested below and click **Submit**
- Click on the ⓘ symbol on the left to view the help available for this application
- ☑ Denotes required field

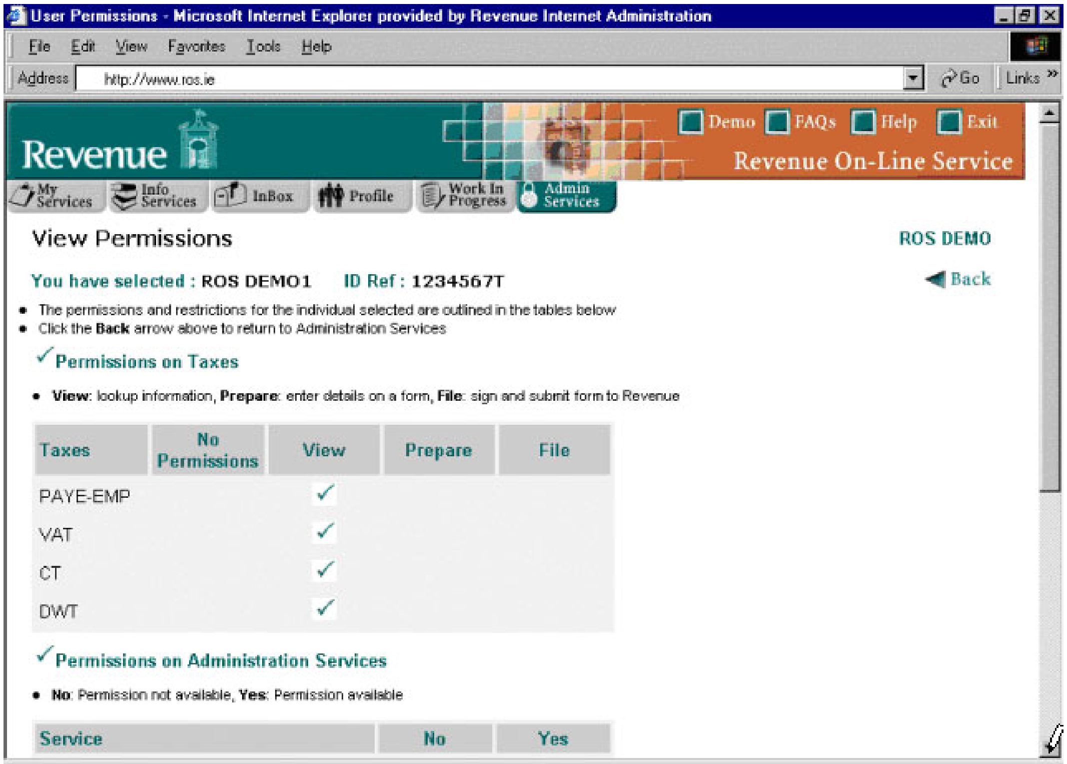
Surname	☑	DEMO1			
First Name	☑	ROS			
ID Ref	☑	1234567t	ID Type	☑	ⓘ
E-mail address for the above named	☑				

Click on the **Submit** button to send your details to ROS [Submit]

Click on the **Back** button to go back to the previous page [Back]

Demo | FAQs | Help | Exit
Terms & Conditions | Certificate Policy Statement | Certification Practice Statement
Revenue On-Line Service, 2nd Floor, Trident House, Blackrock, County Dublin, Ireland.

Figure 2. Application for new digital certificate


User Permissions - Microsoft Internet Explorer provided by Revenue Internet Administration
File Edit View Favorites Tools Help
Address http://www.ros.ie
Go Links
Revenue
Demo FAQs Help Exit
Revenue On-Line Service
My Services
Info Services
InBox
Profile
Work In Progress
Admin Services
ROS DEMO
Back

View Permissions

You have selected : ROS DEMO1 ID Ref : 1234567T

- The permissions and restrictions for the individual selected are outlined in the tables below
- Click the **Back** arrow above to return to Administration Services

✓Permissions on Taxes

- **View**: lookup information, **Prepare**: enter details on a form, **File**: sign and submit form to Revenue

Taxes	No Permissions	View	Prepare	File
PAYE-EMP		✓		
VAT		✓		
CT		✓		
DWT		✓		

✓Permissions on Administration Services

- **No**: Permission not available, **Yes**: Permission available

Service	No	Yes

Figure 3. Setting certificate permissions

c) Tax Form Creation

Currently, the ROS application allows for twenty-two tax forms to be populated.[15]

d) Records Transactions

The formal act of signing and submitting a tax form to Revenue via ROS is considered a transaction and evidence of a record. An additional component of the transaction occurs when a financial payment is authorized and made. Form submission and payment may be combined into a single transaction or conducted separately.

e) Records Transactions

The formal act of signing and submitting a tax form to Revenue via ROS is considered a transaction and evidence of a record. An additional component of the transaction occurs when a financial payment is authorized and made. Form submission and payment may be combined into a single transaction or conducted separately.

f) Records Interfacing and Viewing

The ROS application allows users and agents to view previously submitted returns and other records using the ROS Customer Information Service.

2. Which of these activities generate the digital entities that are the objects of your case study?

a) Digital Certificate Creation and Delivery

The activity involved in setting up a new approved user creates a digital certificate and private key. Revenue Certification Authority is the creating agency for digital certificates. A related area is user management, which oversees the creation and allocation of authorized users in accordance with the ROS Access Control System (ACS).

ROS offers six options to registered users (i.e., those who have completed the registration process and have received a valid digital certificate and access number), including:

1. File a tax return with payment;
2. File a tax return without payment;
3. Upload a tax return completed offline;
4. Make a payment;
5. Complete a Debit Instruction online; and
6. Download a Debit Instruction form for completion offline.

b) Tax Form Creation (including both on- and offline systems)

The main records creation activity within ROS is the filing of electronic tax forms.

[15] This is increasing as later phases of ROS are released.

c) Records Transactions

ROS enables approved or authorized users to submit formally a tax return electronically. The user or agent has the option of including or directing a financial payment in respect of any liability owed to Revenue. This can take one of three forms (See Question 4, below) and enable the user to pay all, some or none of his/her liability.

For purposes of clarity, the researcher considers the following three classes of objects to encompass the body of digital entities generated by the ROS application that are of primary interest in this case study:

1. Digital Certificates and Signatures;
2. Tax Forms (including their export from ROS—See Question 7, below); and
3. Debit Instruction Forms (including their export to financial systems—See Question 7, below).

3. For what purpose(s) are the digital entities you have examined created?

Digital Certificates and Signatures

Digital certificates are created to facilitate user identification and recognition, in addition to ensuring the integrity of any submitted data.

Tax Forms

Tax forms are created to facilitate tax filing and meeting legislative obligations.

Debit Instruction Forms

Debit instructions are created to discharge financial liabilities under tax legislation.

4. What form do these digital entities take? (e.g., e-mail, CAD, database)

All three entities take the form of structured data that is packaged according to requirements as either a delineated flat file or XML. The pages are presented in a compatible Web browser and are rendered using standardised style sheets.

Digital Certificates and Signatures

The digital certificate is a proprietary file with structured data and a unique hash key.

Tax Forms

The following forms are created within ROS:

- VAT: Bi-monthly VAT3 return and annual Return of Trading Details;
- Employers' Payroll Returns: Monthly P30 return, annual P35 return;
- Self-employed Income Tax Form 11 annual return;
- Corporation Tax CT1 annual returns including accounts menus;
- Dividend Withholding Tax returns;
- Investment Undertaking Tax returns;
- Vehicle Registration Tax: Vehicle Birth Certificates and Registration forms;
- Professional Services Withholding Tax returns: monthly F30 and annual F35;
- Special Savings Incentive Account returns: monthly and annual;
- Deposit Interest Retention Tax returns: monthly and annual Life Assurance Exit Tax returns;
- Environmental Levy Tax;
- Gift and Inheritance Tax Return: IT38; and
- Relevant Contracts Tax Return: C30.

Copies of all submitted forms are stored in the user's ROS Inbox.

Debit Instruction Forms

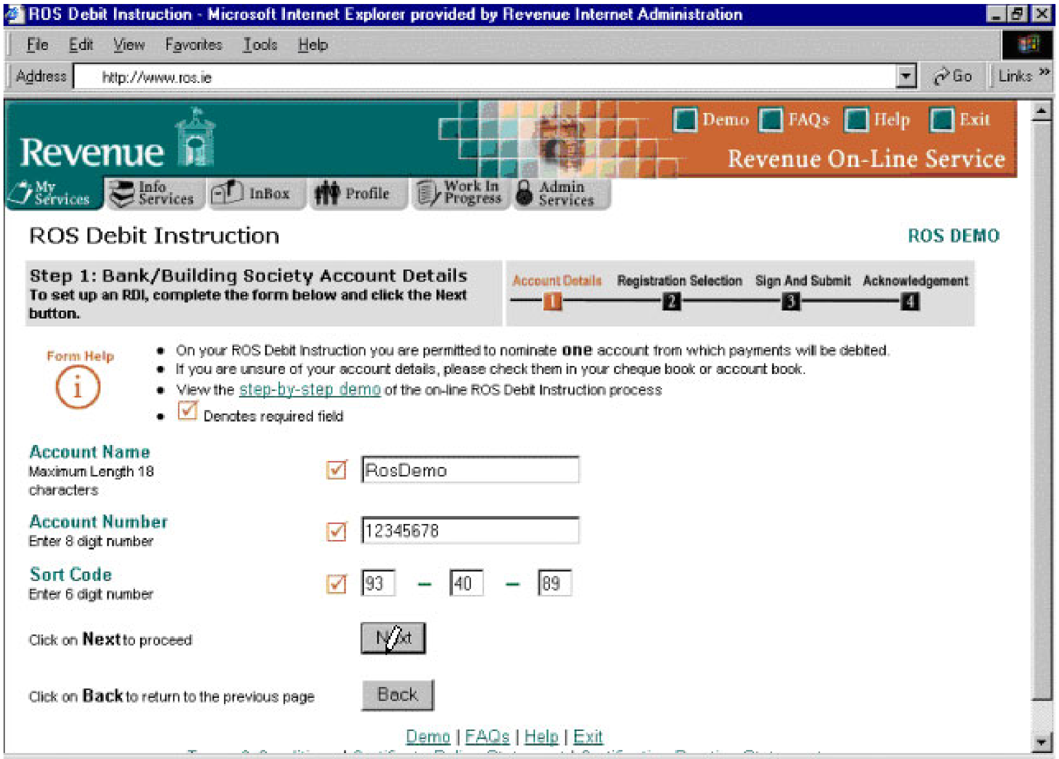
There are two distinct forms for debit instructions, including: (1) an ROS Debit Instruction (RDI) form, and (2) an electronic payment instruction form.

1. ROS Debit Instruction (RDI) Form

An RDI is required to be in place before a user can authorize payments for any of the taxes available in ROS via a debit instruction. The RDI form can be completed online by the taxpayer or his/her tax agent on the ROS site, digitally signed and digitally transmitted to Revenue (Figure 4). Upon successful submission of an RDI form, a copy of the RDI is immediately forwarded to the user's ROS Inbox.

2. Electronic Payment Instruction Form

The electronic payment instruction form involves a four-step process that allows a user to pay a tax liability (or make a Nil Declaration) against a selected tax type using one of several online payment methods. In step one of the process, the user selects the tax type and registration number, via drop-down boxes, against which the payment action is to be taken (Figure 5). In step two of the process, the user selects the payment method to be used via a radio button (Figure 6). This part of the form contains fields that are pre-filled with data appropriate the circumstances of the user's payment situation. For example, in cases where an RDI has been set up, the form will include the user's banking details, drawn from the user's RDI, and the amount of the user's relevant tax liability and payment due date, drawn from the registration link established by the user between the RDI and the tax type(s) to which the RDI is to be applied. In cases where an RDI has not


ROS Debit Instruction - Microsoft Internet Explorer provided by Revenue Internet Administration
File Edit View Favorites Tools Help
Address http://www.ros.ie
Go
Links
Revenue
Demo FAQs Help Exit
Revenue On-Line Service
My Services
Info Services
InBox
Profile
Work In Progress
Admin Services

ROS Debit Instruction

ROS DEMO

Step 1: Bank/Building Society Account Details
To set up an RDI, complete the form below and click the Next button.

Account Details — 1 · Registration Selection — 2 · Sign And Submit — 3 · Acknowledgement — 4

Form Help

- On your ROS Debit Instruction you are permitted to nominate **one** account from which payments will be debited.
- If you are unsure of your account details, please check them in your cheque book or account book.
- View the step-by-step demo of the on-line ROS Debit Instruction process
- ☑ Denotes required field

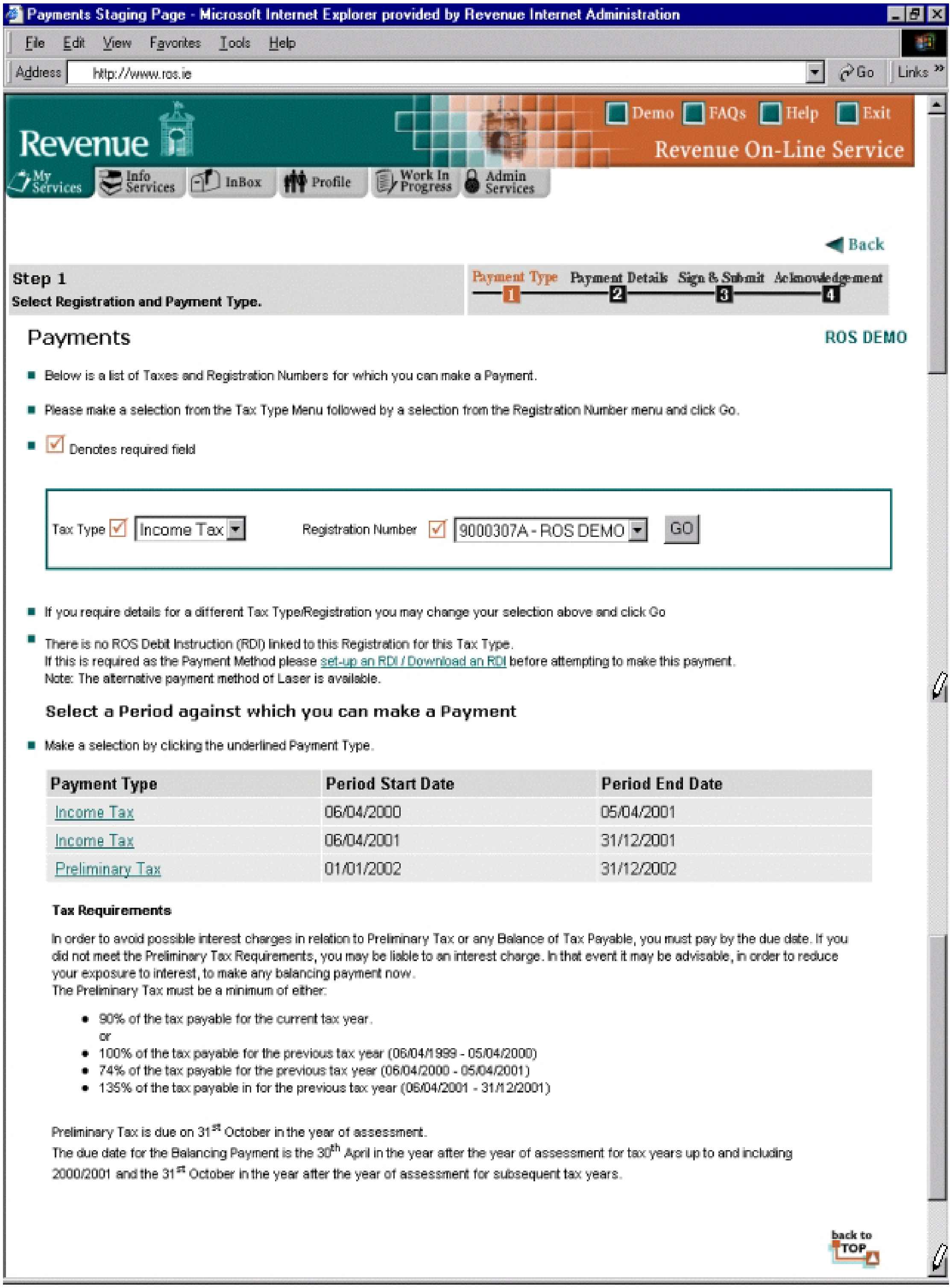
Account Name Maximum Length 18 characters	☑	RosDemo
Account Number Enter 8 digit number	☑	12345678
Sort Code Enter 6 digit number	☑	93 – 40 – 89
Click on **Next** to proceed		Next
Click on **Back** to return to the previous page		Back

Demo | FAQs | Help | Exit

Figure 4. ROS Debit Instruction Step 1 screen

been set up, RDI-specific fields will not appear on the form. Instead, the user will have the option of selecting, via a radio button, whether s/he wishes to make a Nil Declaration or pay a liability via Laser card.[16] In all cases where there is a tax liability, the total payment and payment date fields will be pre-filled to reflect that information based on the tax type selected by the user in part one of the online payment form. Both fields can be directly edited by the user, if required (e.g., to allow users to split the total amount due into a series of smaller payments). In step three of the process, the user selects the appropriate certificate from a drop-down list, enters his/her password, and then clicks the "Sign and Submit" button (Figure 7). If successful, this results in an "Acknowledgement" screen (step four) alerting the user that the payment instruction has been receive by ROS and providing a "Notice Number" that uniquely identifies that transaction (Figure 8). The Notice Number is to be used in any future correspondence relating to the payment.

[16] Laser (http://www.laser.ie) is the primary bank debit card system used in Ireland.



Step 1
Select Registration and Payment Type.

Payments

- Below is a list of Taxes and Registration Numbers for which you can make a Payment.
- Please make a selection from the Tax Type Menu followed by a selection from the Registration Number menu and click Go.
- ☑ Denotes required field

Tax Type ☑ Income Tax Registration Number ☑ 9000307A - ROS DEMO GO

- If you require details for a different Tax Type/Registration you may change your selection above and click Go
- There is no ROS Debit Instruction (RDI) linked to this Registration for this Tax Type.
  If this is required as the Payment Method please set-up an RDI / Download an RDI before attempting to make this payment.
  Note: The alternative payment method of Laser is available.

Select a Period against which you can make a Payment

- Make a selection by clicking the underlined Payment Type.

Payment Type	Period Start Date	Period End Date
Income Tax	06/04/2000	05/04/2001
Income Tax	06/04/2001	31/12/2001
Preliminary Tax	01/01/2002	31/12/2002

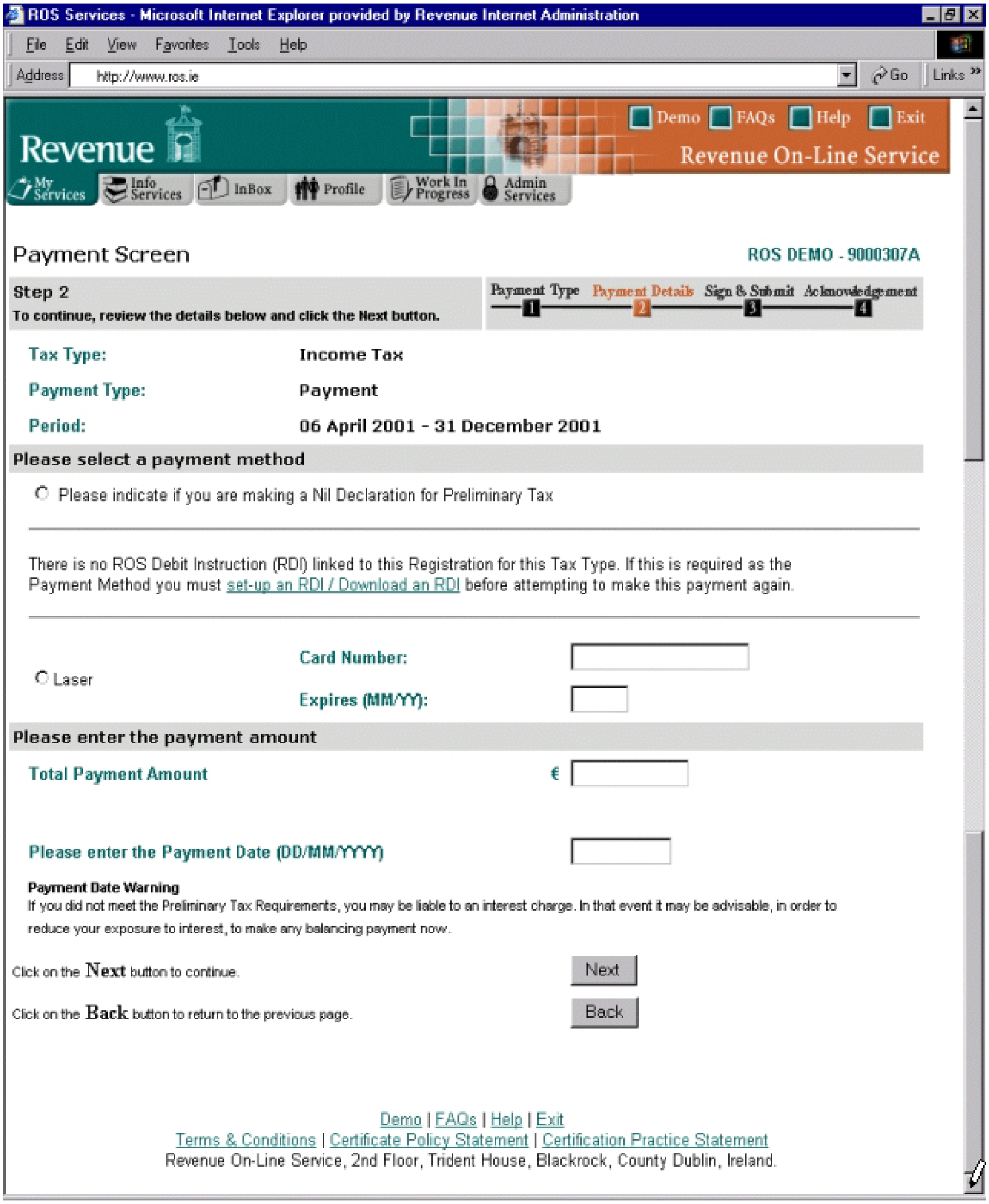
Tax Requirements

In order to avoid possible interest charges in relation to Preliminary Tax or any Balance of Tax Payable, you must pay by the due date. If you did not meet the Preliminary Tax Requirements, you may be liable to an interest charge. In that event it may be advisable, in order to reduce your exposure to interest, to make any balancing payment now.
The Preliminary Tax must be a minimum of either:

- 90% of the tax payable for the current tax year.
  or
- 100% of the tax payable for the previous tax year (06/04/1999 - 05/04/2000)
- 74% of the tax payable for the previous tax year (06/04/2000 - 05/04/2001)
- 135% of the tax payable in for the previous tax year (06/04/2001 - 31/12/2001)

Preliminary Tax is due on 31st October in the year of assessment.
The due date for the Balancing Payment is the 30th April in the year after the year of assessment for tax years up to and including 2000/2001 and the 31st October in the year after the year of assessment for subsequent tax years.

Figure 5. ROS Debit Instruction Step 1 screen



Payment Screen

ROS DEMO - 9000307A

Step 2

To continue, review the details below and click the Next button.

Tax Type:	Income Tax
Payment Type:	Payment
Period:	06 April 2001 - 31 December 2001

Please select a payment method

○ Please indicate if you are making a Nil Declaration for Preliminary Tax

There is no ROS Debit Instruction (RDI) linked to this Registration for this Tax Type. If this is required as the Payment Method you must set-up an RDI / Download an RDI before attempting to make this payment again.

○ Laser

Card Number:

Expires (MM/YY):

Please enter the payment amount

Total Payment Amount €

Please enter the Payment Date (DD/MM/YYYY)

Payment Date Warning

If you did not meet the Preliminary Tax Requirements, you may be liable to an interest charge. In that event it may be advisable, in order to reduce your exposure to interest, to make any balancing payment now.

Click on the Next button to continue.

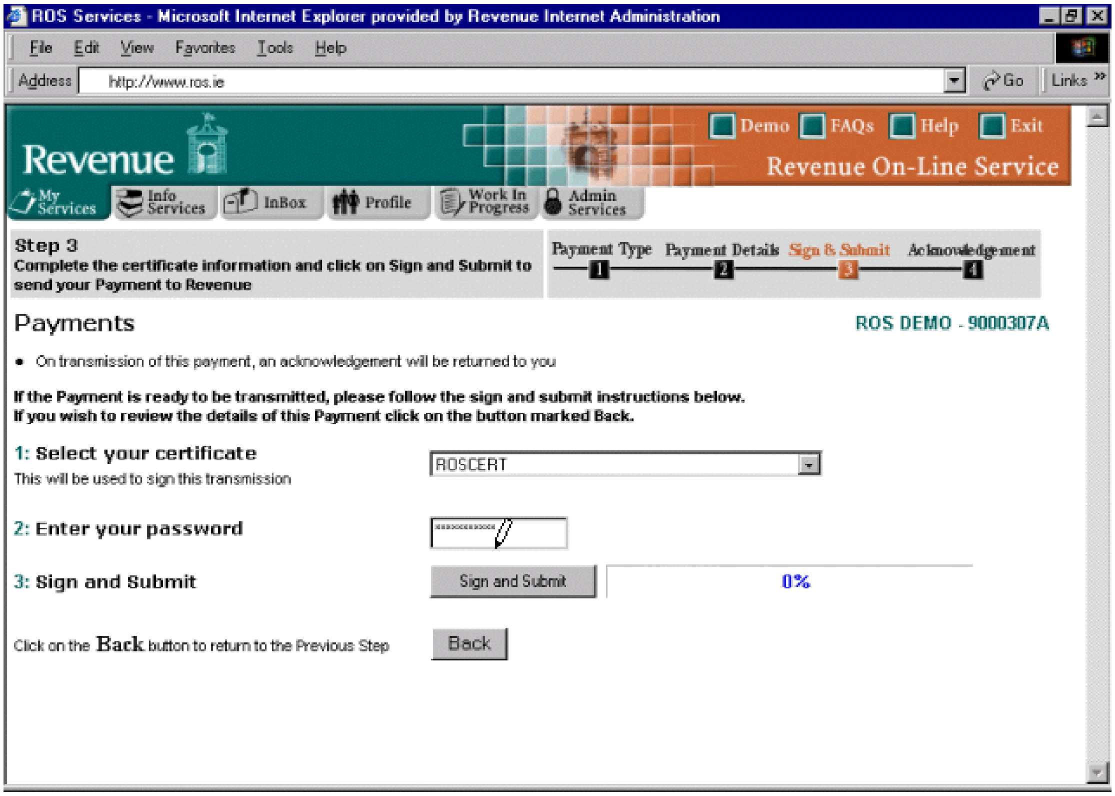
Click on the Back button to return to the previous page.

Demo | FAQs | Help | Exit

Terms & Conditions | Certificate Policy Statement | Certification Practice Statement

Revenue On-Line Service, 2nd Floor, Trident House, Blackrock, County Dublin, Ireland.

Figure 6. ROS Payment Instruction Form - Step 2 screen



Step 3
Complete the certificate information and click on Sign and Submit to send your Payment to Revenue

Payments

ROS DEMO - 9000307A

- On transmission of this payment, an acknowledgement will be returned to you

If the Payment is ready to be transmitted, please follow the sign and submit instructions below.
If you wish to review the details of this Payment click on the button marked Back.

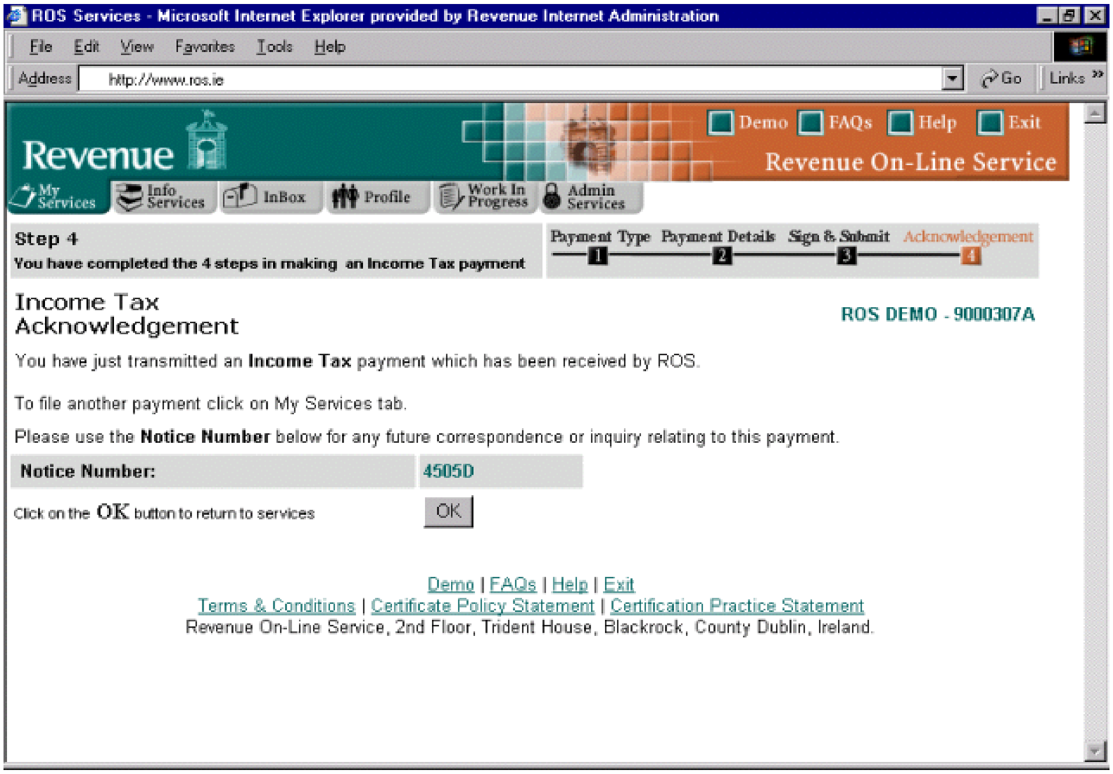
1: Select your certificate ROSCERT
This will be used to sign this transmission

2: Enter your password ************

3: Sign and Submit [Sign and Submit] 0%

Click on the **Back** button to return to the Previous Step [Back]

Figure 8. ROS Payment Instruction Form - Step 3 screen



Step 4
You have completed the 4 steps in making an Income Tax payment

Income Tax
Acknowledgement

ROS DEMO - 9000307A

You have just transmitted an **Income Tax** payment which has been received by ROS.

To file another payment click on My Services tab.

Please use the **Notice Number** below for any future correspondence or inquiry relating to this payment.

Notice Number:	4505D

Click on the **OK** button to return to services [OK]

Demo | FAQs | Help | Exit
Terms & Conditions | Certificate Policy Statement | Certification Practice Statement
Revenue On-Line Service, 2nd Floor, Trident House, Blackrock, County Dublin, Ireland.

Figure 7. ROS Payment Instruction Form - Step 4 screen

4a. What are the key formal elements, attributes, and behaviour (if any) of the digital entities?

This study identified a number of key formal elements (both intrinsic and extrinsic), attributes and behaviours common to the various digital entities generated within the three general classes of objects examined in this case study (i.e., Digital Certificates and Signatures, Tax Forms, and Debit Instruction Forms). The shared elements, attributes and behaviours identified include:

- the Revenue logo;
- forms font and style;
- a certification practice statement;
- a certificate policy statement;
- a privacy policy statement;
- a terms and conditions statement;
- copyright statements;
- contact details; and
- standardized Web page templates, including style sheets, used for rendering a consistent look and feel.

In addition, as is discussed below, the study identified a number of key formal elements, attributes and/or behaviours specific to the digital entities within each of the three general classes of objects.

Digital Certificates and Signatures

Elements and Attributes

The unique intrinsic elements and attributes that are considered integral to the validity and completeness of these documents include:[17]

Field	Value
Version	"2" (representing the international X.509 v3 standard)
Serial Number	An integer that acts as a unique identifier, generated by the ROS CA
Signature Algorithm	MD5,RSA, md5WithRSAEncryption algorithm (OID: 1.2.840.113529.1.1.5), as defined within PKCS#1
Issuer	C=IE, O=Irish Revenue Commissioners, OU=Revenue Online Service, CN=ROS CA
Validity (From)	The date the certificate is valid from. (*date of issue*)
Validity (To)	
Subject	Distinguished Name of Approved Person or Authorized Person *(John Citizen)* *for example, c=IE, o=XYZ Company, ou=RAN, cn=John Citizen*
Certificate Policies	Certificate Policy OID: 1.2.372.980003.1.1.1.1.0 CPS URL: www.revenue.ie Policy qualifier: Certificates issued under this CP are aimed at Approved Persons or Authorized Persons who may use them only to

[17] Office of the Revenue Commissioners Ireland (2000). "Revenue Online Service Certificate Policy Statement," pp. 18-19.

	communicate with the Office of the Revenue Commissioners.
Public Key	The public key in RSA form. RSA (2048 bits) The public key expressed in hexadecimal.
Key Usage	The ROS CA certificate is to be used for: Digital Signature, Non-repudiation
Thumbprint Algorithm	The MD5 hash of the ROS CA's public key.
	The MD5 hash of the ROS CA's public key. This value is used to identify the ROS CA as being known and trusted by the recipient.
Digital Signature	
ROS CA	Digital signature
Policy Qualifier	Certificates issued under this CP are given to Approved Persons or Authorized Persons who may use them only to communicate with the Office of the Revenue Commissioners.

Behaviour

The digital certificate is a required user validation and verification system component that, through its use in signing and encrypting user data prior to transfer, automatically interacts with the system in all ROS-enabled user transactions.

Tax Forms

Elements and Attributes

The only unique intrinsic elements and attributes that are considered integral to the validity and completeness of these documents are the structured data fields and their data, both of which are required to meet the legislative requirements in tax compliance.[18] The unique extrinsic elements and attributes that constitute the external appearance of these documents include:[19]

- the special layout of the data fields;
- hyperlinks to individual form data fields, form pages and contextualized help text;
- the digital signature, either of an applicant (as in the case of a person filing his/her own return), or of an agent (as in the case of an approved or authorized person filing a return, or group of returns, on behalf of another person or group of persons);[20] and
- a digital time-stamp (each completed and submitted form is viewable and retrievable based on its time/date stamp).

[18] Information on intrinsic elements, expressed as a Data Type Description (DTD), for individual forms is available to developers of ROS-compatible software at: http://www.ros.ie/PublisherServlet/downloads.

[19] The extrinsic elements and attributes of the online and offline ROS tax forms are designed, in part, to mirror existing paper based forms, while adding additional functionality in the form of pre-population and dynamically-generated content for certain fields.

[20] When filing a group of returns in batch, the digital signature of the agent (i.e., an approved or authorized person, as defined in Sections 917G and (17G(3)(b) of the *Taxes Consolidation Act 1997*— see http://www.irishstatutebook.ie/ZZA2Y1999S209.html) is not applied to each of the returns in the batch individually, but rather to the entire batch (Office of the Revenue Commissioners Ireland (2000). "Consultative Document on the Electronic Filing of Self-Assessed Tax Returns Form 11 and Form CT1," Revenue Online Service, p. 17. Available at: http://www.revenue.ie/pdf/consult7.pdf).

Behaviour

There is a degree of user and data input interaction, verification and validation undertaken by the application during population of the forms to help ensure the accuracy and reliability of the records that are generated. Some of this activity is generic in nature in that it occurs irrespective of the particular form in question or the user completing the form. For example, tax return forms are split into a number of sections displayed on separate pages. Certain sections need only be opened and completed if the user has entries to be made in those sections. Also, all forms contain automated error-checking functionality (referred to by ROS documentation as "validation") to help ensure that only valid entries can be made in the relevant data entry fields. A number of calculation features associated with the forms allow users to perform various computations, such as an indicative calculation of the tax due per return, or the calculation of a value to enter into a particular field (e.g., the amount of Benefit-in-Kind to enter).

More form- and/or user-specific functions are built into the ROS system, and displayed in interactive fashion on the forms. These interactive 'help' functions assist users in deciding which section(s) of a form are applicable in any given circumstance, as well as which input fields within a section are relevant and the types of entries to be made.

Two types of automated, real-time error checking or validation controls are built into the ROS software application. There are "rejection checks," which ensure that users correct data entry errors before they can proceed any further, and "warning checks," which alert users that the data entered are outside the normal limits expected. In fact, Revenue's ROS forms are designed on the principle that they "contain, at a minimum, the same validation rules which are applied in the Revenue assessing system through which returns are input by Revenue staff."[21]

Related to the issue of form validation and accuracy is the inclusion of a special 'Expression of Doubt' field in the 'Personal Detail' screen of the ROS Form 11 and on the 'Company Details' screen of the ROS Form CT1 tax forms. This field provides a check box that a user may select to indicate that they are unsure about the treatment of any item in his/her return. When selected, a user is then presented with a free flow text input field in which up to 1000[22] text characters can be entered to provide details about the point(s) at issue.

As noted above, many of the forms have a degree of interactivity that is 'tailored' to each individual user's requirements and history. This 'tailoring' is achieved in two ways. First, certain fields in the forms are automatically populated using data carried forward from returns previously filed by the user. For example, in the case of an individual's income tax return, if available, the form automatically includes personal contact and related details from the most recent return filed by the user. Second, certain fields are automatically populated using data generated from the results of intelligent questions asked in the body of the return. In the case of allowances and reliefs, for example, the form's pre-filled amounts are automatically adjusted to update them with any changes legislated for in the government's current budget that are relevant to the user's particular tax situation. These and other

[21] Ibid., p. 20.

[22] The actual number of characters varies between 500 and 1000, depending on the form in question.

automated form activities replicate "what happens in tax districts where staff processing paper returns have similar data carried forward on their return entry screens."[23]

In addition to completing forms online, users may elect to complete forms offline by first installing the ROS Off-Line application (available either via a file download or on a free CD provided by Revenue) on their personal computers. Once installed, the ROS Offline application enables users to download relevant forms from the ROS system, complete and digitally sign them offline, and then transmit the completed form data to ROS. According to ROS documentation, all "downloaded form[s] contain the same pre-filled information and the same validation and calculation functionality as [is] contained in the online form[s]."[24]

As a consequence of these context-specific form behaviours, individual forms will, in many cases, manifest themselves and behave somewhat differently for different users, or even for the same user depending on the user's answers to form questions, the data values entered, and any subsequent modifications initiated by the user to his/her original inputs. There may also be differences in layout and presentation related to whether a user is working with an online or offline form.

Debit Instruction Forms

Elements and Attributes
The unique intrinsic elements and attributes that are considered integral to the validity and completeness of these documents include the user's:

- bank account name (maximum 18 characters);
- 8-digit bank account number;
- 6-digit account sort code (a bank/building society identifier);
- bank's name (automatically populated base on sort code entered), and
- the explicit agreement between the user, his/her bank and Revenue authorizing payments to Revenue from the user's bank/building society account (the agreement also informs Revenue of the method and delivery of payment).

Behaviour
As with the tax forms discussed above, there are real-time error checking or validation controls built in to the Debit Instruction form (both on- and offline versions). These controls ensure that users correct data entry errors before they can save the form or move to another page in the form. On-screen prompts, built-in field length limitations, pop-up error messages and help text assist the user during data entry to ensure the information entered is accurate, complete and in the correct format. Upon successful completion of the form, the user is instructed to select his/her digital certificate, enter their password and click the 'Sign and Submit' button, at which point the completed form is digitally signed (using information from the digital certificate) and electronically submitted to Revenue. A successful RDI submission results in an instant acknowledgement in the user's ROS Inbox, while successful

[23] Office of the Revenue Commissioners Ireland (2000). "Consultative Document on the Electronic Filing of Self-Assessed Tax Returns Form 11 and Form CT1," Revenue Online Service, p. 24. Available at: http://www.revenue.ie/pdf/consult7.pdf.
[24] Ibid., pp. 15-16.

online payment of a user's tax liability via an RDI results in the generation of a receipt for the user that is also placed in the user's ROS Inbox.[25]

4b. What are the digital components of which they consist and their specifications?

As with the formal elements, attributes and behaviours discussed above, there are digital components common to the various digital entities generated within the three general classes of objects examined here. These shared components include:

- **Text**
  Text is provided in four formats, only two of which are applicable to typical ROS users, including: (1) rendered HTML (used for Web site navigation and form population), (2) Adobe Portable Document format (.pdf) (used for presenting forms for printing, for presenting the various site policy documents, and for downloadable files outlining Data Type Descriptions (DTD) of ROS forms for use by software companies in developing ROS-compatible products), (3) XML Schema format (.xsd) (used for downloadable files outlining Data Type Descriptions (DTD) of ROS forms for use by software companies in developing ROS-compatible products), and (4) Microsoft Word format (.doc) (used for downloadable files outlining Data Type Descriptions (DTD) of ROS forms for use by software companies in developing ROS-compatible products).
- **HTML Web page files** (created using the HTML 4.01 transitional specification)
- **XML style sheets** (conforming to level 1 of the WC3 Cascading Style Sheet mechanism)[26]
- **Image files**
  Image files, usually in graphics interface format (.gif) and perhaps occasionally in jpg format, are used for logos and also for images displayed in the online Flash file tutorials of ROS functionality available in the 'Demos' section of the Web site.

Digital Certificates and Signatures

The components of the digital certificate are a public key, a private key and descriptive data about the private key's owner.

Revenue operates a PKI with public keys, private keys and certificates. The primary goal of the Revenue PKI is to maintain the trust of those who have been issued with certificates. Revenue itself acts as the certifying authority and creates and signs its own certificate. It also signs the certificate created by the ROS CA, thus acting as the highest point of trust in the Revenue PKI. The practices and policies associated with the management of the Revenue PKI are further detailed in the following Revenue documents: "Certification Practice Statement"[27] and "Revenue On-Line Service: Certificate Policy Statement."[28]

[25] However, what happens in the case of unsuccessful payments and overpayments is not known. It is unclear, for example, whether an unsuccessful payment attempt also generates a receipt indicating that although payment was attempted, it was not successful. It is not known how, if at all, these various scenarios manifest themselves on a Debit Instruction Form (e.g., indication of a user's current payment status and/or payment history, including successful and unsuccessful payment attempts), or whether such information is recorded elsewhere in a separate log file. And, if the latter, whether there is an explicit link from the user's Debit Instruction Form to the log file (or its data).

[26] See W3C, *Cascading Style Sheets, level 1*, for CSS1 style sheet specifications. Available at http://www.w3.org/TR/REC-CSS1.

[27] Issued by the Office of the Revenue Commissioners, 28 Sept 2000. Available at: http://www.revenue.ie/pdf/pd0018.pdf.

An additional component maintained by Revenue is the SOAP 'security wrapper.'[29] The 'security wrapper' encompasses the entire transaction dataset received from the customer by ROS. This includes the transaction element, i.e., tax return and payment instruction, as well as the 'security packaging' element, i.e., digital signature, date/time-stamp, etc.[30]

Tax Forms

The components of the tax forms are HTML pages, and their underlying script, which display structured data fields originally stored as an XML DTD. The forms are presented online via a Web browser or offline via a bespoke stand-alone Java application. The store of data that is used to pre-populate (and re-populate) certain data entry and data selection fields in the tax forms is also a component and is sourced from back-end systems.

When presenting a form for printing, the form is rendered in pdf format, requiring Adobe Acrobat as a plug-in component.

Debit Instruction Forms

The components are an HTML page displaying structured data fields and data. The store of data that is used to pre-populate (and re-populate) certain data entry and data selection fields in the Debit Instruction forms is also a component and is sourced from back-end systems.

4c. What is the relationship between the intellectual aspects and the technical components?

Given that the ROS system operates within a highly complex, online and offline electronic environment, consideration of its technical components is critical for understanding and evaluating the system's intellectual aspects, which include the content, context and structure of the documents and records generated and/or maintained within the system. The relationship between the ROS system's intellection aspects and its technical components is a highly structured one that, to varying degrees, is both mandated and highly regulated by Revenue policies and legislated tax and customs requirements. In turn, the system's technical components help facilitate and enforce these requirements through the direct and indirect control of both the physical and intellectual interactivity and integrity of the ROS system. As such, the technical components play a critical role in ensuring the accuracy, reliability, and authenticity of the documents and records generated by the system. In this sense, it is clear that the intellectual aspects of content, context and structure rely heavily on the integrity of the technical components for their satisfactory manifestation and maintenance.

At the most basic level, it is the code underlying the various technical components that controls the activities and interactions between components and between users and their interactions with the components. For the most part, this control consists of numerous automated error-checking

[28] Issued by the Office of the Revenue Commissioners, 28 Sept 2000. Available at: http://www.revenue.ie/pdf/pd0039.pdf.

[29] SOAP (Simple Object Access Protocol) is an XML-based protocol that facilitates the exchange of information over HTTP between different applications running on different operating systems, with different technologies and programming languages. ROS uses SOAP version 1.1 for it web services. All forms submitted electronically to ROS must be digitally signed. The digital signature and credentials are included in the SOAP Header.

[30] Response from ROS staff to e-mail query received 14/05/04.

and validation functions designed to ensure the integrity of all component-component and component-user interactions. Given the generally highly sensitive nature of the information and transactions involved in the ROS system, there is an obvious need to ensure, through strict security, transaction, and software protocols and requirements, the accuracy, reliability and authenticity of the documents and records generated and/or maintained by the system. Consequently, there appears to be relatively little opportunity for the introduction (purposeful, accidental or otherwise) of either component- or user-initiated activities that will *significantly* impact the ability of the system to safeguard its key content, contextual and structural aspects.

Assessing these relationships within the context of the digital entities examined in this case study reveals that the ROS system's digital certificates impact primarily on context, while its tax forms impact on content and structure, and the debit instructions impact on both content and context.

Digital Certificates and Signatures – Context

In the course of retrieving and configuring the digital certificate, an application called KCrypto, which administers Revenue's asymmetric encipherment system, is installed on the user's computer. The digital certificate itself is also installed on the user's computer.

The Revenue PKI supports the creation and use of Public and Private Key Pairs and Certificates by Revenue and its customers. These Keys and Certificates are used to ensure the authenticity, integrity, confidentiality and non-repudiation of all transactions between Revenue and its customers. Application of the Revenue PKI involves four distinct, yet interrelated, transformation tasks, including signing and verifying signature schemes, and enciphering and deciphering transmissions. For each transmission, the signing and enciphering tasks are administered and controlled by a user's private key, while the verification and deciphering tasks are administered and controlled by Revenue's public key.[31]

Tax Forms – Content and Structure

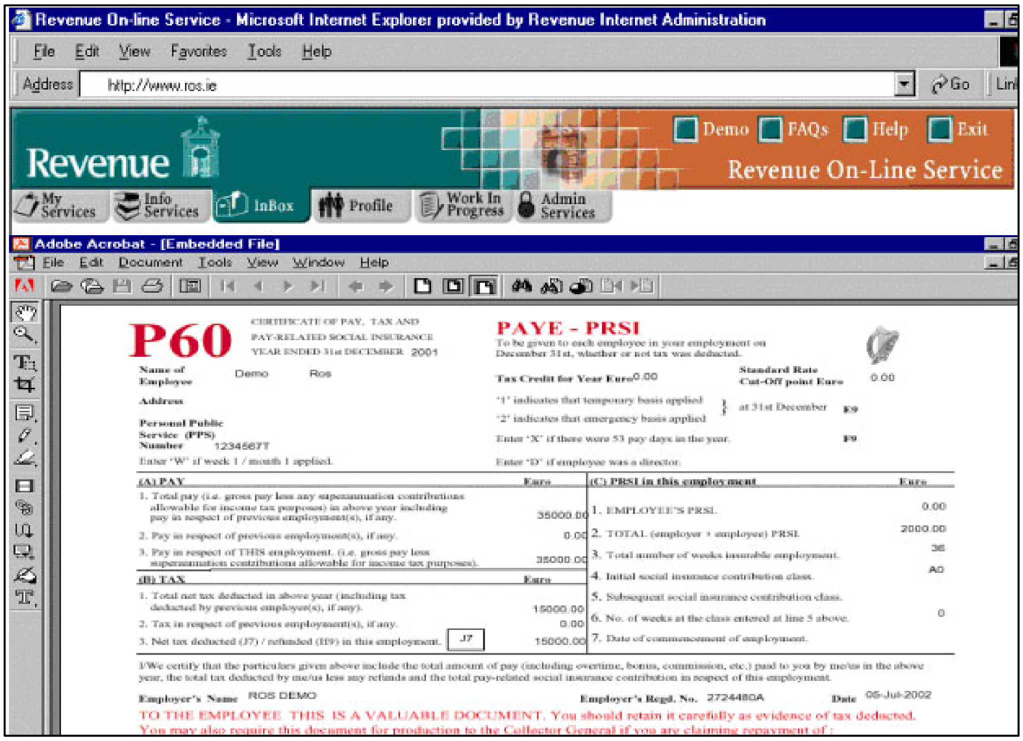
Revenue made a conscious decision to have the online and offline forms mirror the content and structure of paper-based forms. Where appropriate, pre-population and intuitive field displays minimize the need to input duplicate information or scroll through white space.

In addition to the interactive online and offline forms, some forms can be downloaded to the user's computer as a PDF file (Figure 9). These forms can then be printed and filled in manually. The content and structure of these forms mirrors the paper forms normally sent to the citizen by surface mail.

Debit Instructions – Content and Context

The RDI and Laser payment options are similar to online banking options. The RDI includes the digital signature as a means to authenticate the communication for payment(s) to be debited from the user's account(s).

[31] Office of the Revenue Commissioners Ireland (2000). "Revenue Public Key Infrastructure: Certification Practice Statement.".


Revenue On-line Service - Microsoft Internet Explorer provided by Revenue Internet Administration
File Edit View Favorites Tools Help
Address http://www.ros.ie
Go
Revenue
Demo FAQs Help Exit
Revenue On-Line Service
My Services
Info Services
InBox
Profile
Work In Progress
Admin Services
Adobe Acrobat - [Embedded File]
File Edit Document Tools View Window Help

P60 CERTIFICATE OF PAY, TAX AND PAY-RELATED SOCIAL INSURANCE YEAR ENDED 31st DECEMBER 2001

PAYE - PRSI
To be given to each employee in your employment on December 31st, whether or not tax was deducted.

Name of Employee Demo Ros

Address

Personal Public Service (PPS) Number 1234567T

Enter 'W' if week 1 / month 1 applied.

Tax Credit for Year Euro 0.00

Standard Rate Cut-Off point Euro 0.00

'1' indicates that temporary basis applied
'2' indicates that emergency basis applied } at 31st December F9

Enter 'X' if there were 53 pay days in the year. F9

Enter 'D' if employee was a director.

(A) PAY	Euro
1. Total pay (i.e. gross pay less any superannuation contributions allowable for income tax purposes) in above year including pay in respect of previous employment(s), if any.	35000.00
2. Pay in respect of previous employment(s), if any.	0.00
3. Pay in respect of THIS employment. (i.e. gross pay less superannuation contributions allowable for income tax purposes).	35000.00

(B) TAX		Euro
1. Total net tax deducted in above year (including tax deducted by previous employer(s), if any).		15000.00
2. Tax in respect of previous employment(s), if any.		0.00
3. Net tax deducted (J7) / refunded (H9) in this employment.	J7	15000.00

(C) PRSI in this employment	Euro
1. EMPLOYEE'S PRSI.	0.00
2. TOTAL (employer + employee) PRSI.	2000.00
3. Total number of weeks insurable employment.	36
4. Initial social insurance contribution class.	AO
5. Subsequent social insurance contribution class.	
6. No. of weeks at the class entered at line 5 above.	0
7. Date of commencement of employment.	

I/We certify that the particulars given above include the total amount of pay (including overtime, bonus, commission, etc.) paid to you by me/us in the above year, the total tax deducted by me/us less any refunds and the total pay-related social insurance contribution in respect of this employment.

Employer's Name ROS DEMO Employer's Regd. No. 2724480A Date 05-Jul-2002

TO THE EMPLOYEE THIS IS A VALUABLE DOCUMENT. You should retain it carefully as evidence of tax deducted.
You may also require this document for production to the Collector General if you are claiming repayment of :

Figure 9. Downloadable, non-interactive form in Adobe PDF format

4d. How are the digital entities identified (e.g., is there a [persistent] unique identifier)?

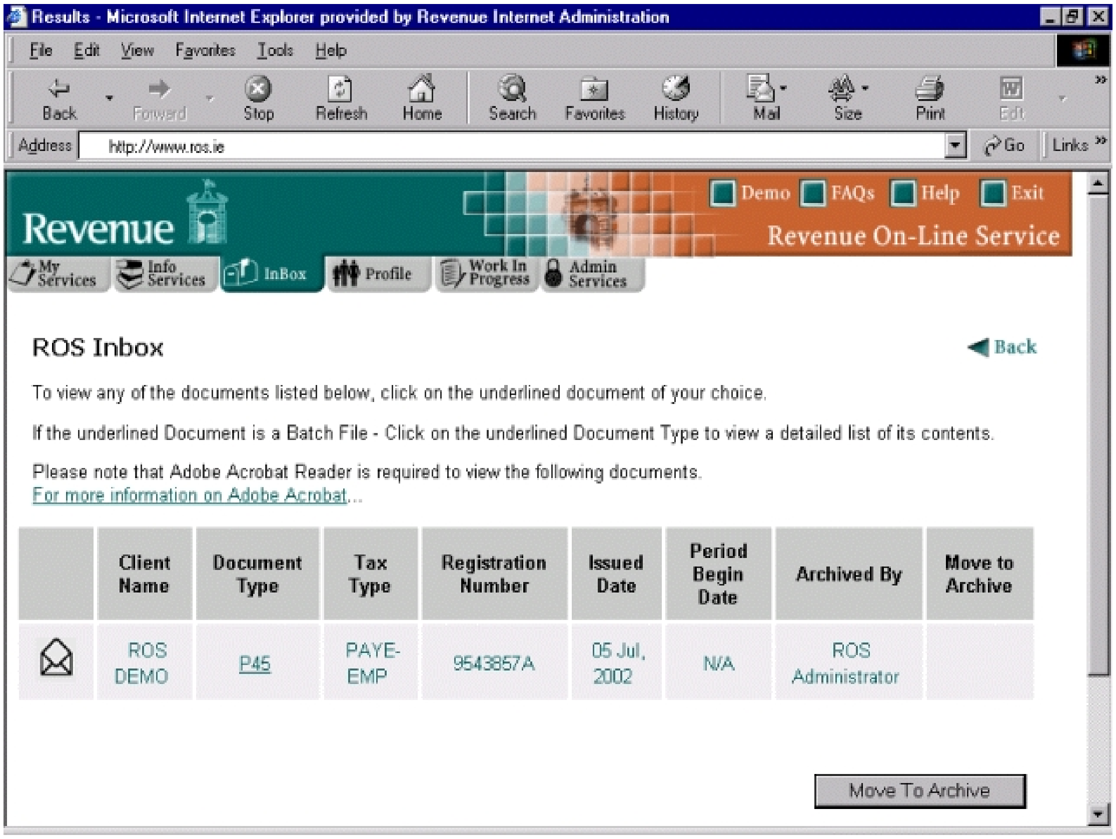
All user-accessible documents and document identifiers in ROS are presented in human readable, human friendly format. According to Revenue, there is no need for specialized codes and keys beyond those normally used by Revenue (e.g., knowledge that a P45 is a declaration of tax paid following cessation of employment). Note that this applies only to data presented via the ROS Customer Information Service. Back-end systems may view data differently. Also, as ROS rearranges data for transfer to ITP and other systems, there may be additional strings of structured data types being generated and exported.

As shown in Figure 10, individual records in an ROS customer's Inbox are uniquely identified using a combination of six elements: (1) client name, (2) document type, (3) tax type, (4) registration number, (5) issued date, and (6) period begin date (e.g., for digital certificates).

Digital Certificates and Signatures

All digital certificates issued to ROS customers include a serial number, which is an integer generated by the ROS CA that acts as a unique identifier.[32] As well, digital certificates are publicly available electronic documents and, as such, can be uniquely identified by the owner's name and personal details. Online access to a customer's digital certificate record(s)

[32] Office of the Revenue Commissioners Ireland (2000). "Revenue Public Key Infrastructure: Certification Practice Statement," p. 18.


Results - Microsoft Internet Explorer provided by Revenue Internet Administration
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Size Print Edit
Address http://www.ros.ie
Go Links
Revenue
Demo FAQs Help Exit
Revenue On-Line Service
My Services
Info Services
InBox
Profile
Work In Progress
Admin Services
Back
Move To Archive

ROS Inbox

To view any of the documents listed below, click on the underlined document of your choice.

If the underlined Document is a Batch File - Click on the underlined Document Type to view a detailed list of its contents.

Please note that Adobe Acrobat Reader is required to view the following documents.
For more information on Adobe Acrobat...

	Client Name	Document Type	Tax Type	Registration Number	Issued Date	Period Begin Date	Archived By	Move to Archive
✉	ROS DEMO	P45	PAYE-EMP	9543857A	05 Jul, 2002	N/A	ROS Administrator	

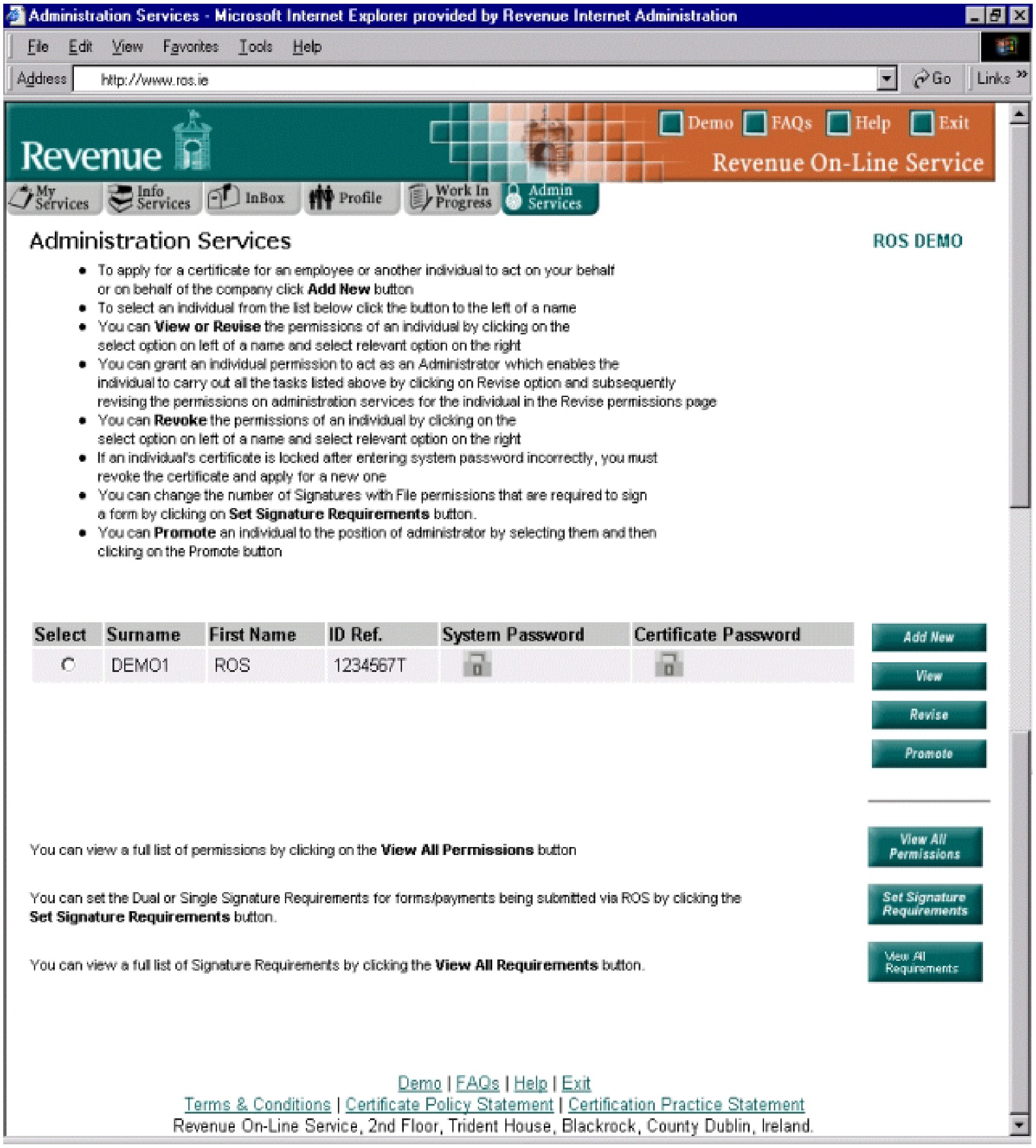
Figure 10. ROS Inbox showing identifiers used to uniquely identify user's records

is provided via the customer's ROS Administrative Services Web page (Figure 11). Self-assessment taxpayers may create up to 100 associated certificates, while agents may create an unlimited number of associated certificates. Individual certificates are uniquely identified using a combination of three elements: (1) surname (of certificate owner), (2) first name (of certificate owner), and (3) ID reference (see Figure 7).

Tax Forms

Online access to ROS system tax form records by ROS customers is provided via a customer's ROS Inbox. Individual tax form records in the customer's ROS Inbox are uniquely identified using a combination of five elements: (1) client name, (2) document type, (3) tax type, (4) registration number, and (5) issued date (see Figure 10).

Unique identification of tax forms submitted to ROS and/or received by ROS customers from Revenue is achieved through the use of a UID by back-end systems to identify each entry (record) in the database.



Administration Services

- To apply for a certificate for an employee or another individual to act on your behalf or on behalf of the company click **Add New** button
- To select an individual from the list below click the button to the left of a name
- You can **View or Revise** the permissions of an individual by clicking on the select option on left of a name and select relevant option on the right
- You can grant an individual permission to act as an Administrator which enables the individual to carry out all the tasks listed above by clicking on Revise option and subsequently revising the permissions on administration services for the individual in the Revise permissions page
- You can **Revoke** the permissions of an individual by clicking on the select option on left of a name and select relevant option on the right
- If an individual's certificate is locked after entering system password incorrectly, you must revoke the certificate and apply for a new one
- You can change the number of Signatures with File permissions that are required to sign a form by clicking on **Set Signature Requirements** button.
- You can **Promote** an individual to the position of administrator by selecting them and then clicking on the Promote button

Select	Surname	First Name	ID Ref.	System Password	Certificate Password
○	DEMO1	ROS	1234567T	🔒	🔒

You can view a full list of permissions by clicking on the **View All Permissions** button

You can set the Dual or Single Signature Requirements for forms/payments being submitted via ROS by clicking the **Set Signature Requirements** button.

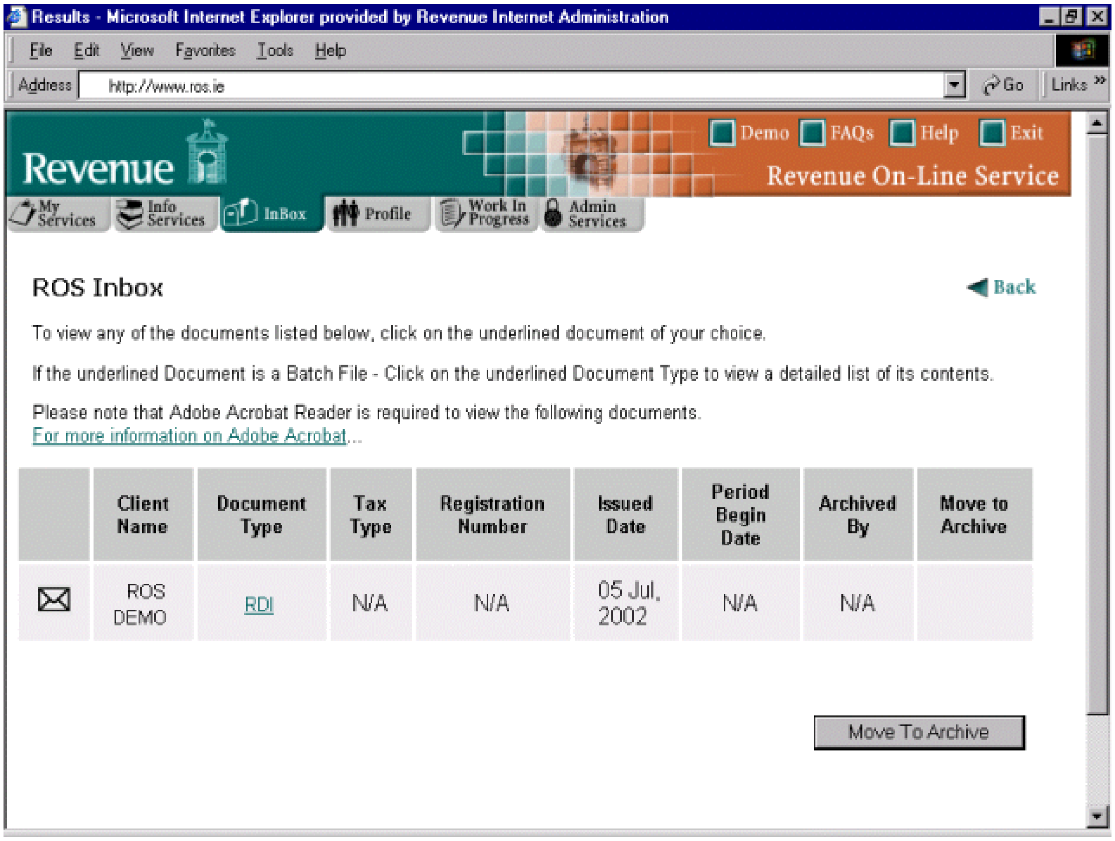
You can view a full list of Signature Requirements by clicking the **View All Requirements** button.

Demo | FAQs | Help | Exit
Terms & Conditions | Certificate Policy Statement | Certification Practice Statement
Revenue On-Line Service, 2nd Floor, Trident House, Blackrock, County Dublin, Ireland.

Figure 11. ROS Administration Services Web page showing identifiers used to uniquely identify user's associated certificates

Debit Instruction Forms

Online access to ROS Debit Instruction (RDI) records by ROS customers is provided via a customer's ROS Inbox. As shown in Figure 12, individual RDI records in the customer's Inbox appear to be identified using a combination of just two elements: (1) client name, and (2) issued date.


Results - Microsoft Internet Explorer provided by Revenue Internet Administration
File Edit View Favorites Tools Help
Address http://www.ros.ie
Go
Links
Revenue
Demo
FAQs
Help
Exit
Revenue On-Line Service
My Services
Info Services
InBox
Profile
Work In Progress
Admin Services
Back
Move To Archive

ROS Inbox

To view any of the documents listed below, click on the underlined document of your choice.

If the underlined Document is a Batch File - Click on the underlined Document Type to view a detailed list of its contents.

Please note that Adobe Acrobat Reader is required to view the following documents.
For more information on Adobe Acrobat...

	Client Name	Document Type	Tax Type	Registration Number	Issued Date	Period Begin Date	Archived By	Move to Archive
✉	ROS DEMO	RDI	N/A	N/A	05 Jul, 2002	N/A	N/A	

Figure 12. ROS Inbox Web page showing identifiers used to identify user's ROS Debit Instructions

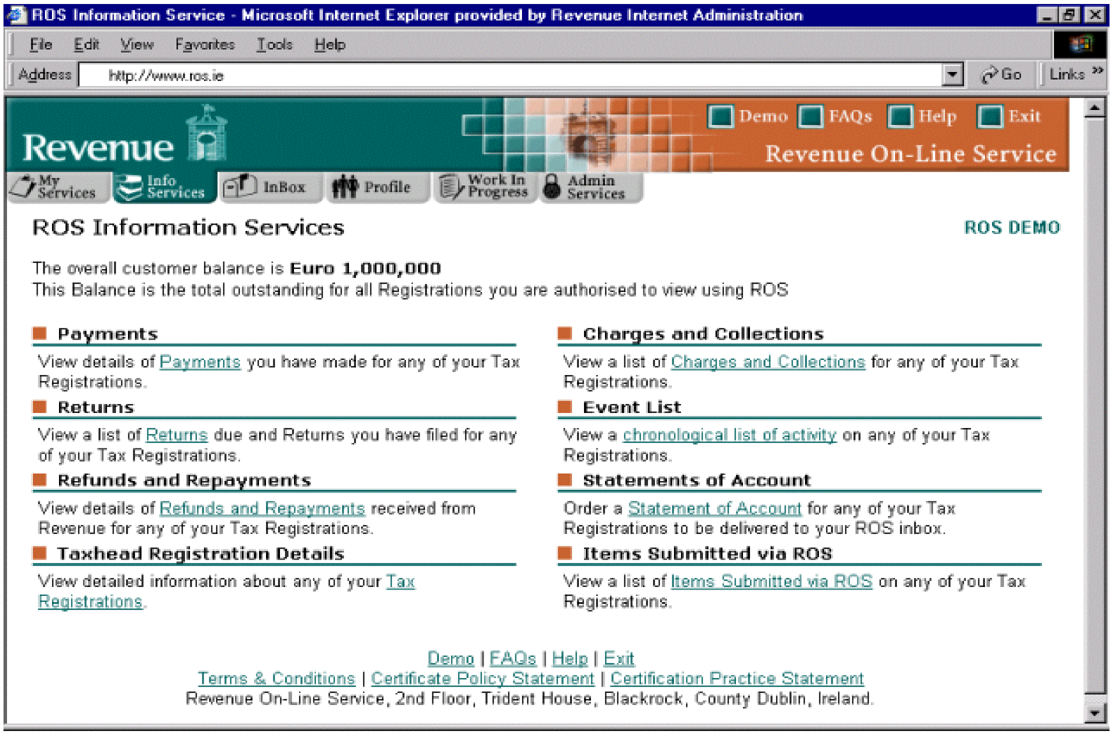
The unique identification of RDIs submitted to ROS is achieved through the use of a UID by back-end systems to identify each RDI entry (record) in the database.

A user's or agent's RAN or PPS identifies Debit Instructions.

4e. In the organization of the digital entities, what kind of aggregation levels exist, if any?

As shown in Figure 13, Revenue's ROS Information Services Web page provides structured access to a user's ROS-related records and activities organized into eight distinct categories. Users can generate structured, and, if desired, filtered listings of individual records within each category by entering specific search parameters into the search fields provided for each category (Figures 14 and 15). Such listings are automatically arranged in reverse chronological order (i.e., newest to oldest) by date (see Figure 15). It should be noted that these views are not generated using 'real-time' or 'live' data from the ITP database, but are instead generated using static data from the latest update to the database in ROS.[33] It should also be noted that there are differing

[33] The time delay is something similar to paying a VISA bill online, which results in an automatic account debit, but time-delayed VISA credit until back-end processing is completed


ROS Information Service - Microsoft Internet Explorer provided by Revenue Internet Administration
File Edit View Favorites Tools Help
Address http://www.ros.ie
Go Links
Revenue
Demo FAQs Help Exit
Revenue On-Line Service
My Services
Info Services
InBox
Profile
Work In Progress
Admin Services

ROS Information Services

ROS DEMO

The overall customer balance is **Euro 1,000,000**
This Balance is the total outstanding for all Registrations you are authorised to view using ROS

Payments
View details of Payments you have made for any of your Tax Registrations.

Returns
View a list of Returns due and Returns you have filed for any of your Tax Registrations.

Refunds and Repayments
View details of Refunds and Repayments received from Revenue for any of your Tax Registrations.

Taxhead Registration Details
View detailed information about any of your Tax Registrations.

Charges and Collections
View a list of Charges and Collections for any of your Tax Registrations.

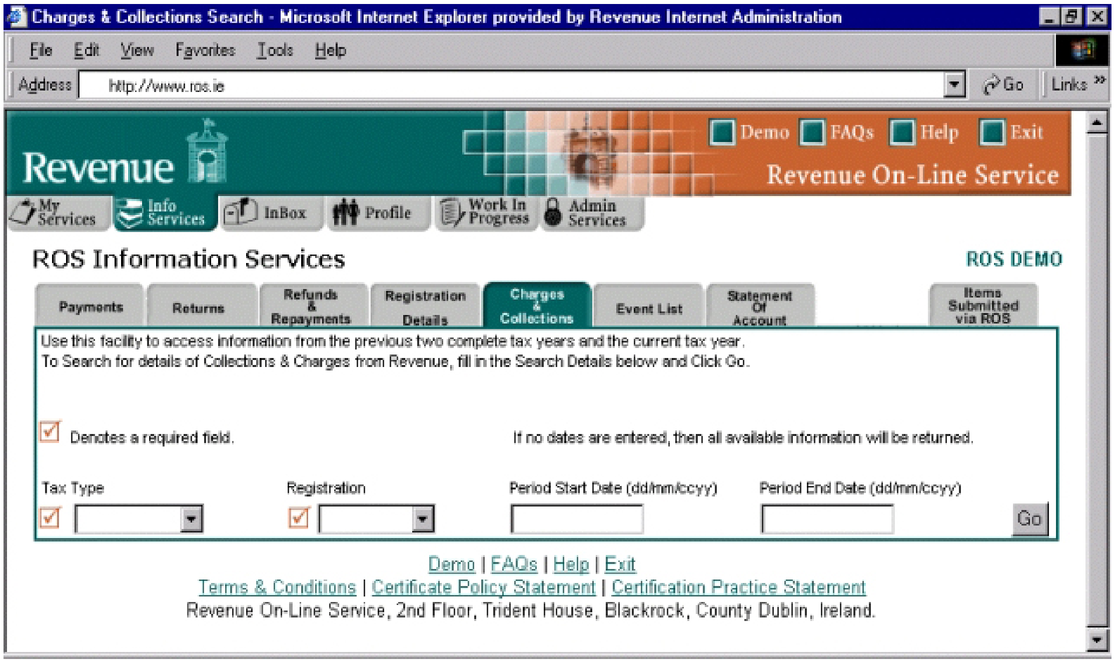
Event List
View a chronological list of activity on any of your Tax Registrations.

Statements of Account
Order a Statement of Account for any of your Tax Registrations to be delivered to your ROS inbox.

Items Submitted via ROS
View a list of Items Submitted via ROS on any of your Tax Registrations.

Demo | FAQs | Help | Exit
Terms & Conditions | Certificate Policy Statement | Certification Practice Statement
Revenue On-Line Service, 2nd Floor, Trident House, Blackrock, County Dublin, Ireland.

Figure 14. ROS Information Services Web page showing aggregation scheme used to provide users with structured access to their ROS-related records



ROS Information Services

ROS DEMO

Use this facility to access information from the previous two complete tax years and the current tax year.
To Search for details of Collections & Charges from Revenue, fill in the Search Details below and Click Go.

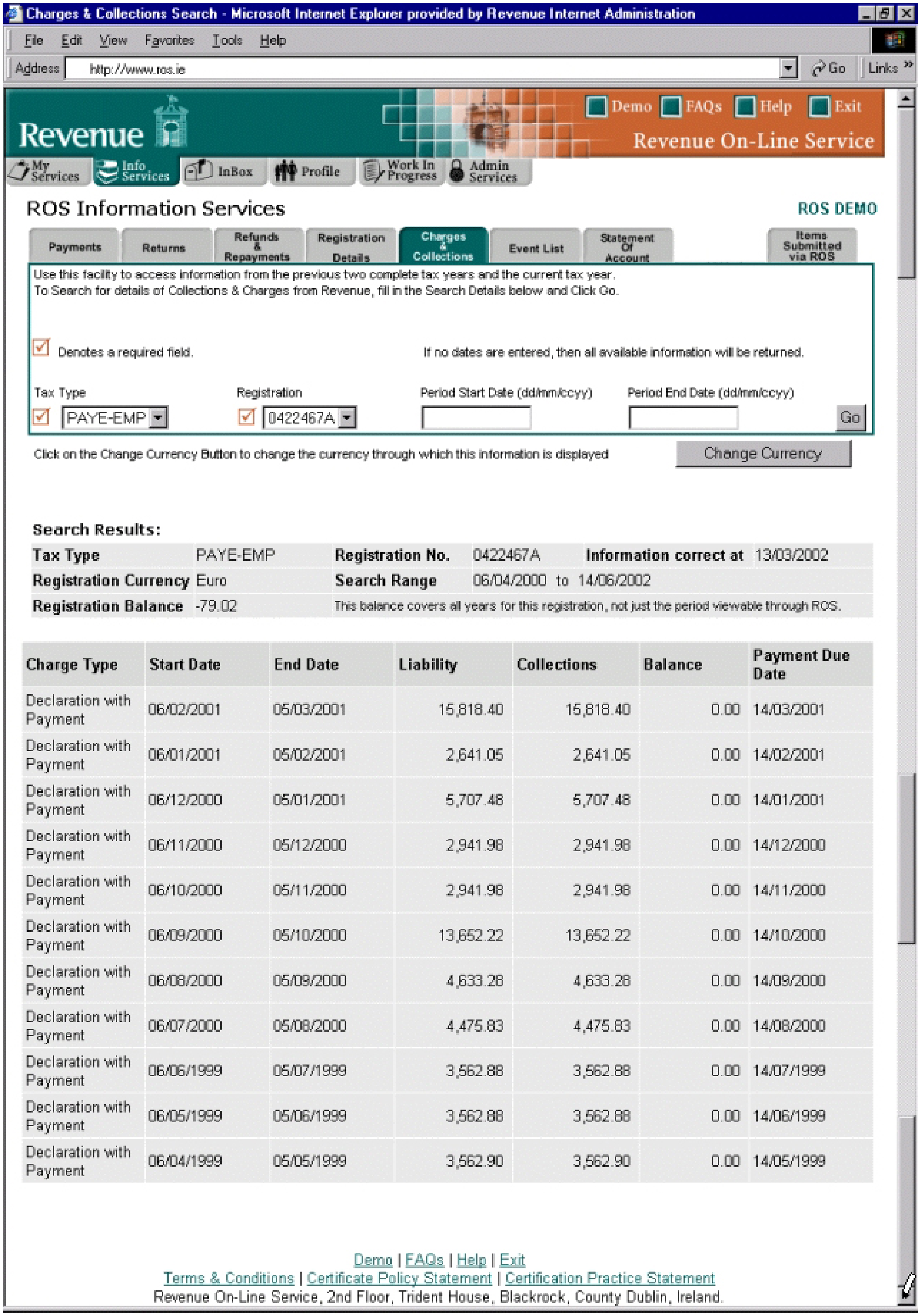
☑ Denotes a required field.

If no dates are entered, then all available information will be returned.

Tax Type ☑ | Registration ☑ | Period Start Date (dd/mm/ccyy) | Period End Date (dd/mm/ccyy)

Demo | FAQs | Help | Exit
Terms & Conditions | Certificate Policy Statement | Certification Practice Statement
Revenue On-Line Service, 2nd Floor, Trident House, Blackrock, County Dublin, Ireland.

Figure 13. ROS Charges & Collections Web page (within user's ROS Information Services Web page) showing search fields available to users for retrieving structured, filtered listings of their ROS records pertaining to past and/or current charges and collections for any of their Tax Registrations



ROS Information Services

ROS DEMO

Use this facility to access information from the previous two complete tax years and the current tax year.
To Search for details of Collections & Charges from Revenue, fill in the Search Details below and Click Go.

☑ Denotes a required field.

If no dates are entered, then all available information will be returned.

Tax Type	Registration	Period Start Date (dd/mm/ccyy)	Period End Date (dd/mm/ccyy)	
☑ PAYE-EMP	☑ 0422467A			Go

Click on the Change Currency Button to change the currency through which this information is displayed

Change Currency

Search Results:

Tax Type	PAYE-EMP	Registration No.	0422467A	Information correct at	13/03/2002
Registration Currency	Euro	Search Range	06/04/2000 to 14/06/2002		
Registration Balance	-79.02	This balance covers all years for this registration, not just the period viewable through ROS.			

Charge Type	Start Date	End Date	Liability	Collections	Balance	Payment Due Date
Declaration with Payment	06/02/2001	05/03/2001	15,818.40	15,818.40	0.00	14/03/2001
Declaration with Payment	06/01/2001	05/02/2001	2,641.05	2,641.05	0.00	14/02/2001
Declaration with Payment	06/12/2000	05/01/2001	5,707.48	5,707.48	0.00	14/01/2001
Declaration with Payment	06/11/2000	05/12/2000	2,941.98	2,941.98	0.00	14/12/2000
Declaration with Payment	06/10/2000	05/11/2000	2,941.98	2,941.98	0.00	14/11/2000
Declaration with Payment	06/09/2000	05/10/2000	13,652.22	13,652.22	0.00	14/10/2000
Declaration with Payment	06/08/2000	05/09/2000	4,633.28	4,633.28	0.00	14/09/2000
Declaration with Payment	06/07/2000	05/08/2000	4,475.83	4,475.83	0.00	14/08/2000
Declaration with Payment	06/06/1999	05/07/1999	3,562.88	3,562.88	0.00	14/07/1999
Declaration with Payment	06/05/1999	05/06/1999	3,562.88	3,562.88	0.00	14/06/1999
Declaration with Payment	06/04/1999	05/05/1999	3,562.90	3,562.90	0.00	14/05/1999

Demo | FAQs | Help | Exit
Terms & Conditions | Certificate Policy Statement | Certification Practice Statement
Revenue On-Line Service, 2nd Floor, Trident House, Blackrock, County Dublin, Ireland.

Figure 15. ROS Charges & Collections Web page (within user's ROS Information Services Web page) showing structured listing of search return results arranged in reverse chronological order by Payment Due Date

levels (or types) of aggregation related to different types of users; for example, between self-assessing users (RAN) and agents (TAIN), where an agent may act on behalf of several users.

Digital Certificates and Signatures

After applying for a digital certificate, a user must then retrieve his/her certificate. This retrieval process results in installation of the certificate directly onto the hard drive of the user's computer under an ROS sub-directory that is automatically created during the certificate retrieval process. If the certificate or the sub-directory is subsequently deleted (accidentally or otherwise), the user must reapply for a new certificate.

Tax Forms

There are three options available to users for accessing their completed and submitted tax forms online, including: (1) via the ROS Inbox search function (Figure 16), (2) via the 'Items Submitted via ROS' link on the ROS Information Services Web page (see Figure 13), and (3) via the 'Returns' link on the ROS Information Services Web page (see Figure 13). In each case, the tax forms are arranged and managed based on Tax Type and Issued Date. They are ordered and presented to the user within ROS within each Tax Type chronologically by Issued Date.

Debit Instruction Forms

Upon successful submission of an RDI, a copy of the submitted RDI is immediately forwarded to the user's ROS Inbox. It appears that a user may only have one RDI active at any one time. Presumably, however, users can retain copies of any previous RDIs via the 'Move to Archive' function available in their Inbox (see Figure 12). A copy of every past RDI, arranged chronologically by issued date, may also be accessible via the 'Items Submitted via ROS' area of a user's ROS Information Services Web page (see Figure 13).

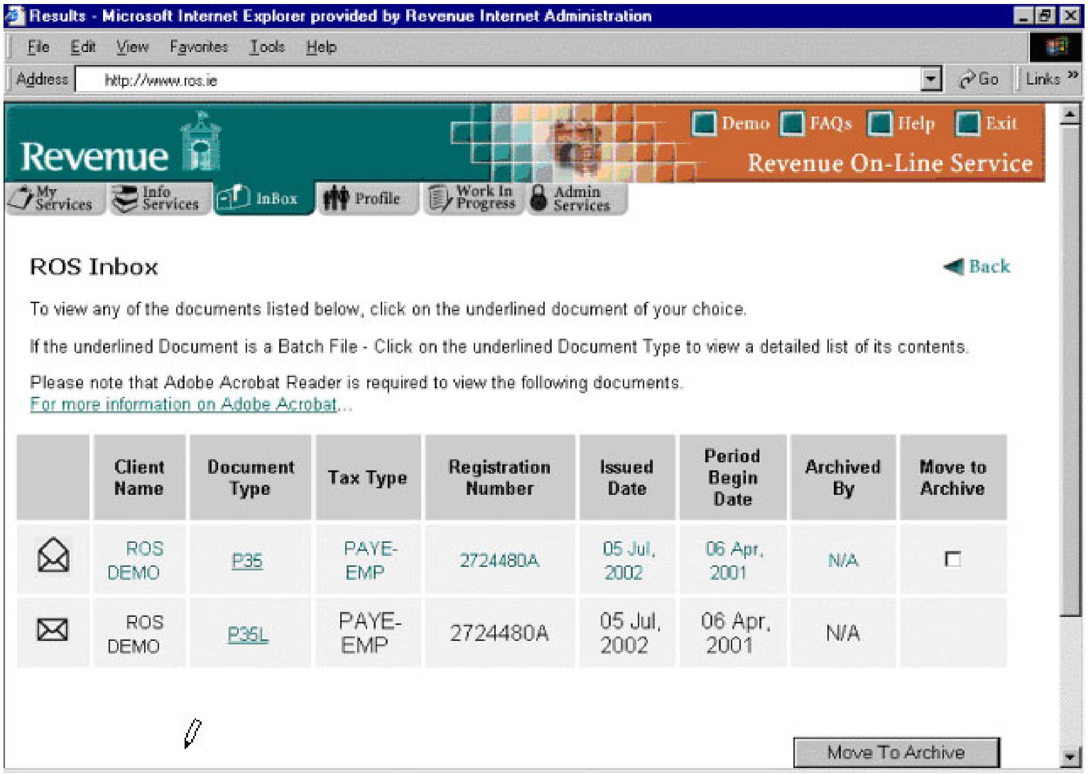
4f. What determines the way in which the digital entities are organized?

Digital Certificates and Signatures

As shown in Figure 17, the organisation of digital certificates within the ROS system is based on the direct linkage between a particular certificate and user/agent within the Revenue PKI framework, and the two year lifespan of the certificate.

Tax Forms

Tax records are structured by tax type and tax number on ITP's relational database. The customer's tax history (payments, refunds, returns, etc.) is accessible via the various links provided on the ROS Information Services Web page (see Figure 13). Each ROS user can access the same type of data as can a Revenue employee regarding his/her tax and transaction history. Access to this data is controlled by ROS security, and the customer's digital certificate. In most cases, the tax records are organised chronologically by date (e.g., Issued Date, Payment Due Date) according to tax type and/or document type for the client's convenience, making them easy to locate, retrieve and view (see Figures 13 and 15).



ROS Inbox

To view any of the documents listed below, click on the underlined document of your choice.

If the underlined Document is a Batch File - Click on the underlined Document Type to view a detailed list of its contents.

Please note that Adobe Acrobat Reader is required to view the following documents.
For more information on Adobe Acrobat...

	Client Name	Document Type	Tax Type	Registration Number	Issued Date	Period Begin Date	Archived By	Move to Archive
✉	ROS DEMO	P35	PAYE-EMP	2724480A	05 Jul, 2002	06 Apr, 2001	N/A	□
✉	ROS DEMO	P35L	PAYE-EMP	2724480A	05 Jul, 2002	06 Apr, 2001	N/A	

Figure 16. ROS Inbox showing completed and submitted tax forms arranged by Tax Type and Issued Date, as accessed via the Inbox search function

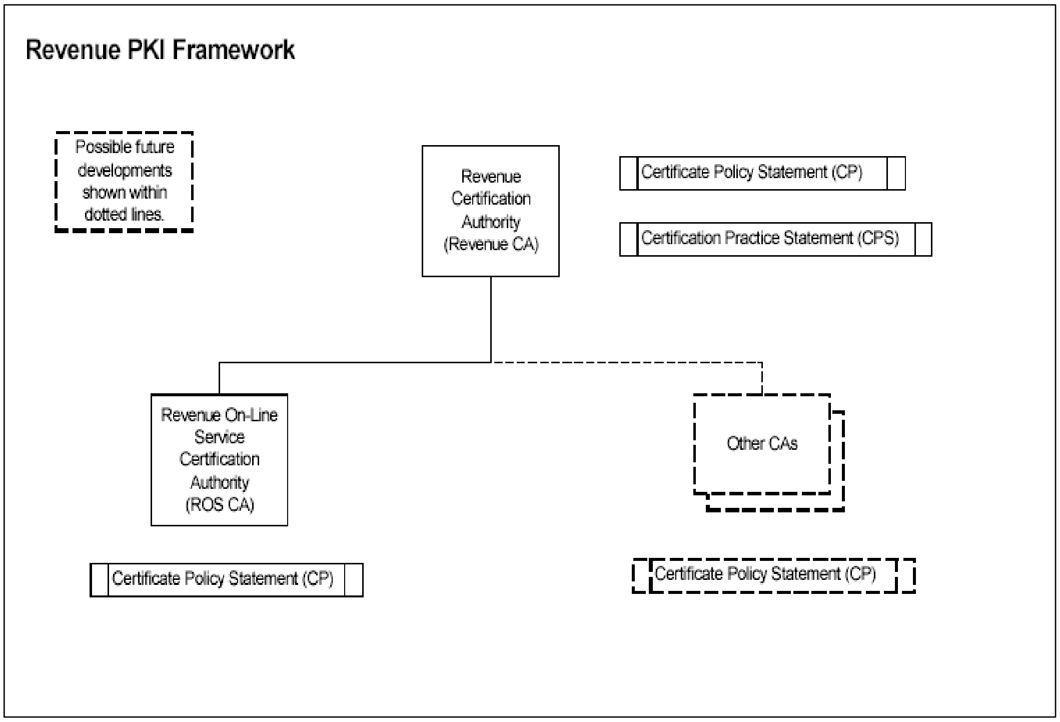

Revenue PKI Framework
Possible future developments shown within dotted lines.
Revenue Certification Authority (Revenue CA)
Certificate Policy Statement (CP)
Certification Practice Statement (CPS)
Revenue On-Line Service Certification Authority (ROS CA)
Certificate Policy Statement (CP)
Other CAs
Certificate Policy Statement (CP)

Figure 17. Revenue PKI framework

Debit Instruction Forms

Once created by a user, an RDI is exported from ROS to the back-end systems and to the financial institution designated in the RDI. Copies of the user's current RDI and all previous RDIs (if any) are stored within ROS as part of the user's tax history in ROS, organized chronologically by issued date, and can be viewed and/or printed at any by the user.

5. How are those digital entities created?

It is understood by the researcher that ROS is used as a mean to validate and transfer submitted tax forms to the main Revenue back-end system(s).

Digital Certificates and Signatures

The digital certificates are generated in line with Revenue's PKI technology. Revenue employs Baltimore Technologies as the sub-contractors for digital certificate creation using Baltimore's UniCERT product. As part of the process, a third party application called KCrypto is downloaded from the Revenue Web site or the free CD-ROM to the user's computer. This application enables the PKI technologies to create and store the digital certificate (including the private key) on the user's computer.

Note that following the sale by Baltimore Technologies of their securities business, Revenue issued an RFT with a December 2003 deadline for a new service provider to host, manage and support the PKI for ROS.[34] The new PKI service provider is LanCommunication / RSA Security.

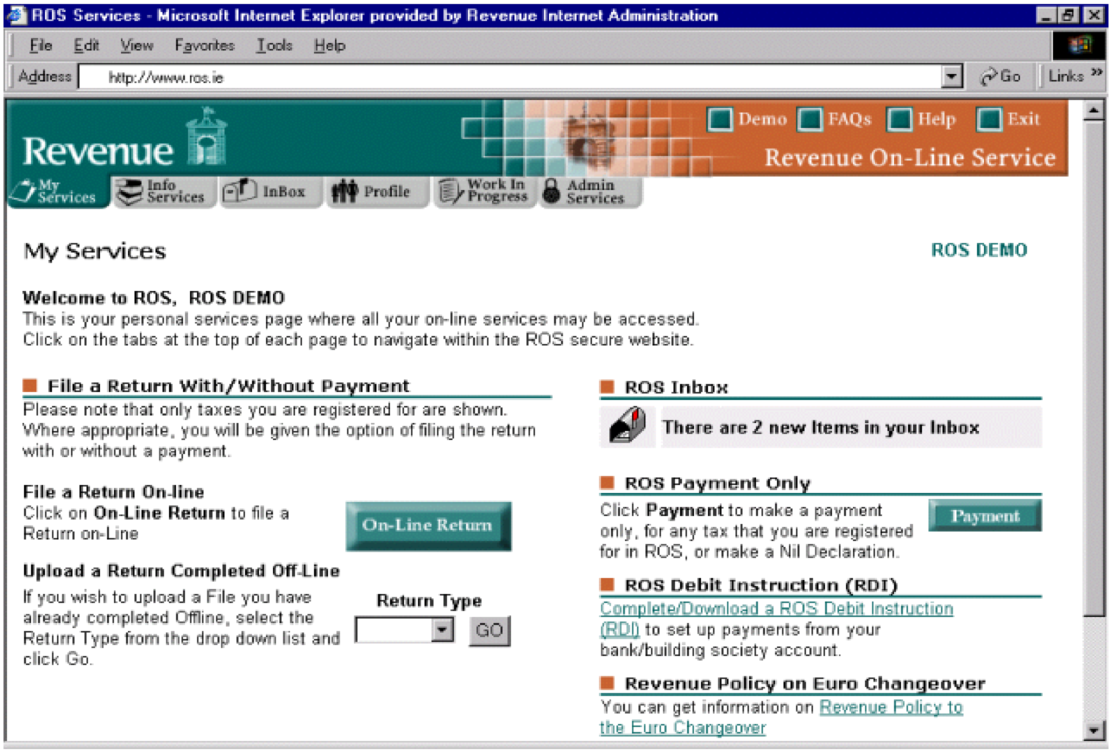
Tax Forms

The tax forms are created based on XML DTDs rendered by a bespoke proprietary Java-based application that is either downloaded to the user's computer or accessed via the ROS Web site.

When a user or agent logs into ROS, they view their recent tax history in their Inbox in a similar manner to an e-mail application (Figures 18 and 19). The presented data is a virtual copy of Revenue's back-end ITP system that is updated on a daily basis. The virtual copy allows ROS users to view their tax details and status in near real time (the database copy is time/date stamped to inform users about when the subset was last updated and how old it is—usually about 48 hours old). ROS updates the back-end systems at 2:30pm so that payment instructions can be sent to banking institutions on the same working day as the tax records are sent to the Revenue systems.

All tax returns, forms, and payment instructions are interfaced to the Revenue back-office systems for processing on a daily basis, and any outputs (e.g., payment receipts, notice of assessment, etc.) generated as a result are interfaced back to ROS for placing in the customer's secure ROS Inbox.

[34] See http://www.electricnews.net/news.html?code=9380529 (Accessed 9 Aug 2004).


ROS Services - Microsoft Internet Explorer provided by Revenue Internet Administration
File Edit View Favorites Tools Help
Address http://www.ros.ie
Go
Links
Revenue
Demo FAQs Help Exit
Revenue On-Line Service
My Services
Info Services
InBox
Profile
Work In Progress
Admin Services

My Services

ROS DEMO

Welcome to ROS, ROS DEMO
This is your personal services page where all your on-line services may be accessed.
Click on the tabs at the top of each page to navigate within the ROS secure website.

File a Return With/Without Payment
Please note that only taxes you are registered for are shown. Where appropriate, you will be given the option of filing the return with or without a payment.

File a Return On-line
Click on **On-Line Return** to file a Return on-Line

On-Line Return

Upload a Return Completed Off-Line
If you wish to upload a File you have already completed Offline, select the Return Type from the drop down list and click Go.

Return Type

GO

ROS Inbox
There are 2 new Items in your Inbox

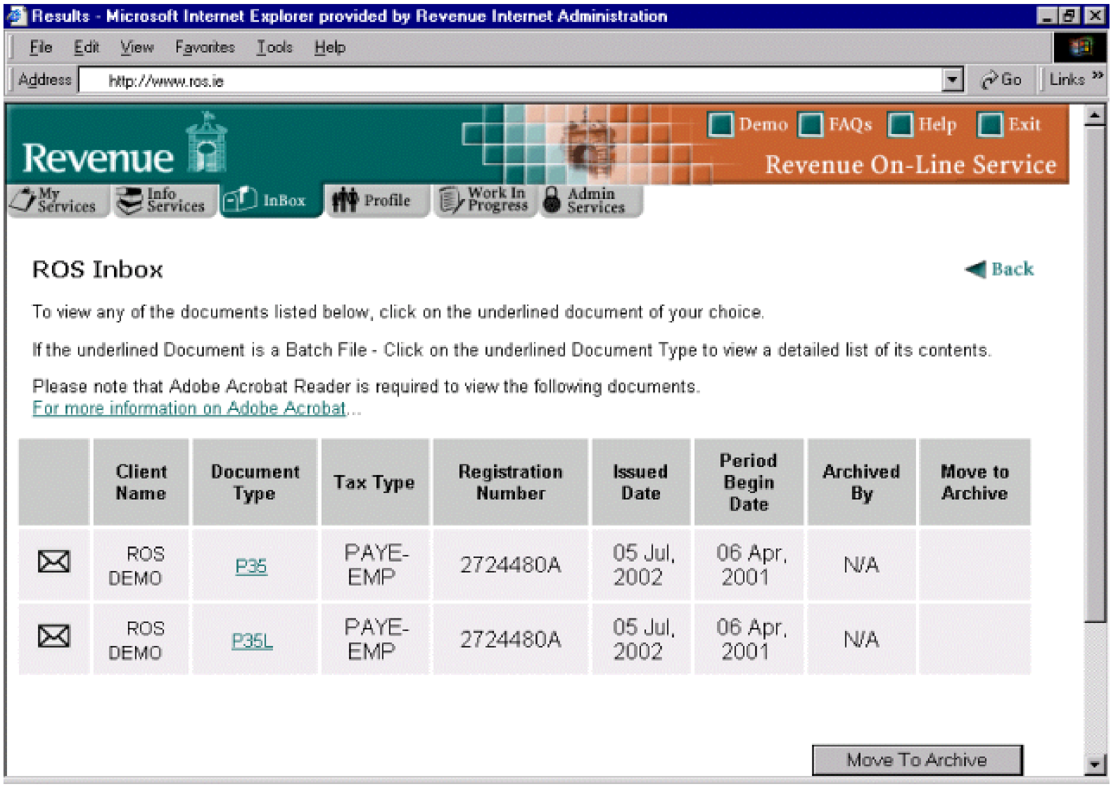
ROS Payment Only
Click **Payment** to make a payment only, for any tax that you are registered for in ROS, or make a Nil Declaration.

Payment

ROS Debit Instruction (RDI)
Complete/Download a ROS Debit Instruction (RDI) to set up payments from your bank/building society account.

Revenue Policy on Euro Changeover
You can get information on Revenue Policy to the Euro Changeover

Figure 18. ROS My Services Web page with indication of two new items in the user's ROS Inbox


Results - Microsoft Internet Explorer provided by Revenue Internet Administration
File Edit View Favorites Tools Help
Address http://www.ros.ie
Go
Links
Revenue
Demo FAQs Help Exit
Revenue On-Line Service
My Services
Info Services
InBox
Profile
Work In Progress
Admin Services
Back

ROS Inbox

To view any of the documents listed below, click on the underlined document of your choice.

If the underlined Document is a Batch File - Click on the underlined Document Type to view a detailed list of its contents.

Please note that Adobe Acrobat Reader is required to view the following documents.
For more information on Adobe Acrobat...

	Client Name	Document Type	Tax Type	Registration Number	Issued Date	Period Begin Date	Archived By	Move to Archive
✉	ROS DEMO	P35	PAYE-EMP	2724480A	05 Jul, 2002	06 Apr, 2001	N/A	
✉	ROS DEMO	P35L	PAYE-EMP	2724480A	05 Jul, 2002	06 Apr, 2001	N/A	

Move To Archive

Figure 19. New items are displayed in a user's ROS Inbox

Debit Instruction Forms

Debit Instructions and Laser Payments are exported from ROS at the same time as the ITP data. However, financial instructions are sent directly to banking systems based on a dedicated infrastructure linking them to Revenue. Payment authorizations are processed immediately to maximise interest generation for Revenue.

5a. What is the nature of the system(s) with which they are created? (e.g., functionality, software, hardware, peripherals etc.)

All of the ROS application's components, including its security system, were built using open industry standards, and to the degree possible, off-the-shelf applications, to: (1) minimize the footprint from the users' perspective (i.e., system is accessed via a standard Web browser), (2) increase the interoperability of its components, and (3) facilitate the re-use of Revenue's existing frameworks and systems.

The server side of ROS employs an Advantage Ingress 2.5 Relational Database from Computer Associates to store core customer data. Information in the ROS database is refreshed on a nightly basis from Revenue's ITP back-office system. The Web server system is built using Java, which increases the system's ability to easily accommodate individual and/or customized architectural components. On the client side, for example, the return filing components, which by default operate in HTML, can easily be replaced with custom, third-party form software.

In addition to the use of off-the-shelf applications (e.g., Adobe Reader), the ROS application also uses a proprietary, Java-based, Off-Line Launcher to facilitate submission of offline tax returns.

Users access the ROS Web site using their own hardware and software (browser and Adobe Reader). While the functionality of the user's platform can vary considerably, it must meet certain minimum system requirements to be able to interact properly with the various components of the ROS application. At a minimum, users must have one of the supported Java virtual machines installed and enabled on their computer (a digital certificate cannot be established without this).[35] ROS currently only supports Microsoft Windows and Apple Macintosh operating systems, although support for UNIX and LINUX platforms is anticipated "at a later stage." Users must also have a working e-mail account so that they can receive messages from ROS notifying them when returns are due and when documents have been placed in the user's ROS Inbox.

Digital Certificates and Signatures

The creation of Keys and Certificates is controlled and administered by the Revenue PKI (see Figure 17) using approved products from a PKI service provider that are designed to automate Key and Certificate management functions. Revenue's Registration Authority (RA) service domain, which operates under the Revenue PKI, is responsible for supplying user registration functions and for facilitating key generation requests. Within the ROS CA

[35] For details, see: http://www.ros.ie/PublisherServlet/requirements#java.

environment, the ROS application itself provides some of this RA functionality within the user's computer environment.[36]

Public and Private Keys used by the ROS CA are generated and stored in software evaluated to standards agreed to by Revenue (up to ITSEC E3 certification). As noted earlier, Revenue, in association with LanCommunications/RSA Security, operates its PKI in conformance with Recommendation x.509, a widely used specification for digital certificates published by the ITU-T. Consequently, the Revenue PKI supports and uses X.509 Version 3 Certificate extensions and does not support the use of Private extensions. The Revenue PKI certificate validation system examines the status assigned to an extension to determine how the certificate is treated. For example, if the system does not recognize an extension designated as critical, the certificate is rejected, while a non-critical extension that is not recognized by the system may be ignored.[37]

The Revenue PKI system supports and uses the following algorithm object identifiers (OIDs):[38]

Hashing/digest algorithms:

- Secure Hash Algorithm-1 (SHA-1)
- Message Digest 5 (MD5)

Padding algorithms:

- 1. ISO 9796
- 2. PKCS#1

Encryption algorithms:

- 1. Rivest Shamir Adleman
- 2. Data Encryption Standard

The use of multiple algorithms within the same hierarchy is also supported.

Creation of a certificate requires a Key Pair. A user's Private Key (minimum of 1024 bits) is generated on his/her own computer by a signed cryptographic software applet supplied by Revenue as part of the "Certificate Retrieval" option from the ROS application's main Web page. The cryptographic software applet is designed to ensure that the Private Key is destroyed in memory by overwriting it with zeros when the user exits the software.[39] The applet securely stores the generated key within the user's computer (a user's Private Key is never held within the Revenue PKI or by Revenue[40]), and subsequently generates a request

[36] Office of the Revenue Commissioners Ireland (2000). "Revenue Public Key Infrastructure: Certification Practice Statement," p. 18.
[37] Office of the Revenue Commissioners Ireland (2000). "Revenue Online Service Certificate Policy Statement," pp. 31, 39, 41.
[38] Ibid., pp. 41-42.
[39] The code contained in the applet is subject to independent review by a trusted third party appointed by the Revenue Policy Approval Authority (Office of the Revenue Commissioners Ireland (2000). "Revenue Public Key Infrastructure: Certification Practice Statement," p. 16).
[40] The Revenue PKI operates in full compliance with the confidentiality requirements defined within the *Electronic Commerce Act* (2000), Section 27 (Office of the Revenue Commissioners Ireland (2000). "Revenue Online Service Certificate Policy Statement," p. 39).

for a new certificate to the ROS CA. Private Key escrow is not supported by the Revenue PKI. Certificates are requested and distributed over the Internet, using a protected session (128 bit SSL). Certificates are also stored within the Revenue X.500 directory.[41]

When a user signs onto ROS, the Revenue PKI uses its own certificate to identify itself to the user's browser. In turn, the customer's own certificate is used to uniquely identify him/her to the ROS server.

Tax Forms

As is discussed in greater detail above in Question 4a (see: Tax Forms, especially the Behaviour section), the ROS system includes varying degrees of form- and/or user-specific functionality. It also accommodates both online and offline tax form creation options, both of which include automated real-time error checking or validation controls to help ensure the accuracy of the data entered and the overall reliability of the records created.

For online users, creation and submission of tax forms is accomplished via a series of interactive, Java-based form templates residing on the ROS server. Virtually identical forms are available to offline users via the ROS Off-Line application, which installs a proprietary application on the user's computer.[42] Once the ROS Offline Application is installed, the customer uses the application to download the necessary tax forms from the ROS Web site, and complete them within the user's own computer environment. Once completed, the user must then log onto the ROS Web site to sign and submit the tax form via the 'Upload a Return Completed Off-Line' option available on the 'My Services' page.

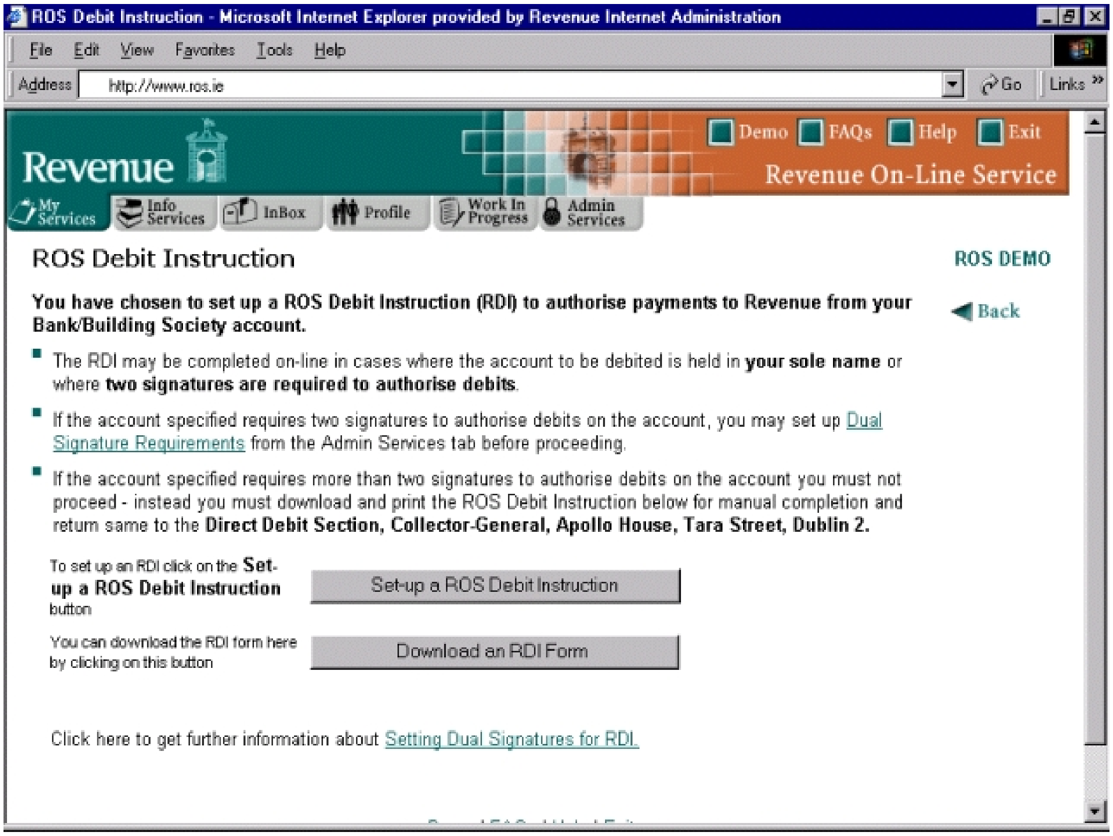
Digital copies of submitted tax forms are immediately sent by the ROS system to a user's ROS Inbox in PDF format. Customers may then use Adobe Reader to view these copies online, copy them to their local computer environment and/or print them out in hard copy.

Debit Instruction Forms

Similar to the tax forms creation functionality noted in the previous section, the ROS system accommodates both online and offline RDI form creation options (Figure 20). As is discussed in greater detail above in Question 4a (see: Debit Instruction Forms, especially the Behaviour section), the ROS system includes real-time error checking or validation controls for both the online and offline RDI form interfaces to help ensure the accuracy of the data entered and the overall reliability of the records created.

It is possible to use ROS for 'payment only' and create an RDI to make a payment without filing a tax return. As well, it is noted that there is a level of integration between ROS/ITP and banking back-end systems. It is presumed that an RDI authorizes the debiting of specified accounts in line with other electronic commerce applications.

[41] Ibid., pp. 31, 35, 38-40.
[42] ROS customers may also use certified third-party software to complete offline tax forms.


ROS Debit Instruction - Microsoft Internet Explorer provided by Revenue Internet Administration
File Edit View Favorites Tools Help
Address http://www.ros.ie
Go
Links
Revenue
Demo FAQs Help Exit
Revenue On-Line Service
My Services
Info Services
InBox
Profile
Work In Progress
Admin Services
ROS DEMO
Back

ROS Debit Instruction

You have chosen to set up a ROS Debit Instruction (RDI) to authorise payments to Revenue from your Bank/Building Society account.

- The RDI may be completed on-line in cases where the account to be debited is held in **your sole name** or where **two signatures are required to authorise debits**.
- If the account specified requires two signatures to authorise debits on the account, you may set up Dual Signature Requirements from the Admin Services tab before proceeding.
- If the account specified requires more than two signatures to authorise debits on the account you must not proceed - instead you must download and print the ROS Debit Instruction below for manual completion and return same to the **Direct Debit Section, Collector-General, Apollo House, Tara Street, Dublin 2.**

To set up an RDI click on the **Set-up a ROS Debit Instruction** button

Set-up a ROS Debit Instruction

You can download the RDI form here by clicking on this button

Download an RDI Form

Click here to get further information about Setting Dual Signatures for RDI.

Figure 20. ROS Debit Instruction interface used to set up an RDI online or download an RDI form to be completed offline

5b. Does the system manage the complete range of digital entities created in the identified activity or activities for the organization (or part of it) in which they operate?

Digital Certificates and Signatures

The ROS system manages all digital certificates as a subset of the Revenue CA.

Tax Forms

The ROS system manages information about all tax forms submitted electronically through the system, although the actual authentic copies of the digital entities actually reside on Revenue's ITP back-end database system. Also, ROS will only display information about prior transactions if they occurred through the ROS system. However, by using the ROS Customer Information Service, users can obtain a 'god's eye view' of their current standing with Revenue, including prior transactions. There is no ability, however, to 'drill down' into transactions that took place using paper or personal visits to the tax office.

Debit Instruction Forms

While a record of the RDI is retained in the ROS system and linked to the tax type(s) indicated by the user when establishing the RDI, the entity has been transferred to the financial institution for payment authorization. The payment of taxes via an RDI updates the ITP system by noting the payment and reducing the tax liability data.

6. From what precise process(es) or procedure(s), or part thereof, do the digital entities result?

Initial contact with ROS may occur via e-mail as the application posts an automatically-generated e-mail when there is a new message in the user's ROS Inbox. The message may inform the user that a payment is (over)due, a tax return is to be filled, or an update has been received.

Digital Certificates and Signatures

The creation of digital certificates is tightly controlled via a regimented series of online processes, facilitated by a series of Java-controlled forms, together with offline processes in the form of the delivery of system passwords to customers via letter mail. These certificate creation processes are described in more detail in Question 10 below.

Tax Forms

The ROS system accommodates three different options for completing tax forms: (1) online while signed on to the ROS system, (2) offline using the ROS Offline Application, and (3) offline using third-party software.

1. **Online.** To complete a return online, a user or agent logs onto the ROS Web site and enters his/her RAN to gain access to the secure section of the Web site. A tax form is then filled out online, during any number of individual sessions,[43] via a series of Java-controlled form screens, digitally signed and submitted. Although various real-time data validations are conducted throughout the process of completing a tax return, once a return is signed and submitted, the ROS system performs a final validation on the form and will reject any form that fails this validation. Upon successful submission, a copy of the return is immediately placed in the customer's secure ROS Inbox.

2. **Offline via ROS Offline Application**. To use this option, a user must first install the ROS Offline Application software on his/her computer. This free application is available via download from the ROS Web site, or by request on CD-ROM. Once installed, the user or agent launches the ROS Offline Application on his/her computer, downloads, installs and then completes the required tax form(s). This may be done over several sessions.

[43] The online option allows users to save, and later return to, partially completed returns prior to final completion and submission. Partially completed, saved online returns are stored in the ROS database (Office of the Revenue Commissioners Ireland (2000). "Consultative Document on the Electronic Filing of Self-Assessed Tax Returns Form 11 and Form CT1," Revenue Online Service, p. 7. Available at: http://www.revenue.ie/pdf/consult7.pdf).

3. **Offline via a Third-Party Application**. The particular processes involved in completing forms using this option may vary somewhat depending on the third-party application used.

Regardless of the offline option used, once a return is completed and ready to be submitted, the user must then log onto the ROS Web site to sign and submit the return via the 'Upload a Return Completed Off-Line' option available on the 'My Services' page. As shown in Figure 21, the ROS file upload function involves a four-step process, including: (1) identifying (adding) the files to be uploaded, (2) digitally signing the forms (by selecting the appropriate certificate), (3) validating the certificate's user via a password, and (4) transmitting the signed forms to the Revenue database.

The offline options are recommended for complex forms such as corporation tax forms and payments that may require the collation of large amounts of information. In these situations, the user or agent may not have all of the information to hand, so the partially completed offline return can be saved for finishing later. In the case of tax agents, this approach also allows them to batch file multiple returns simultaneously.

For both online and offline submissions, the user must click the 'sign and submit' button to complete the transaction. Revenue regards this as the conscious decision made to finalize the transaction from the user side and send the tax return for processing. Revenue sees the signing action as a 'ceremony,' which is central to the ROS system claim of non-repudiation as it inextricably links the submitted form to the person or agent involved.

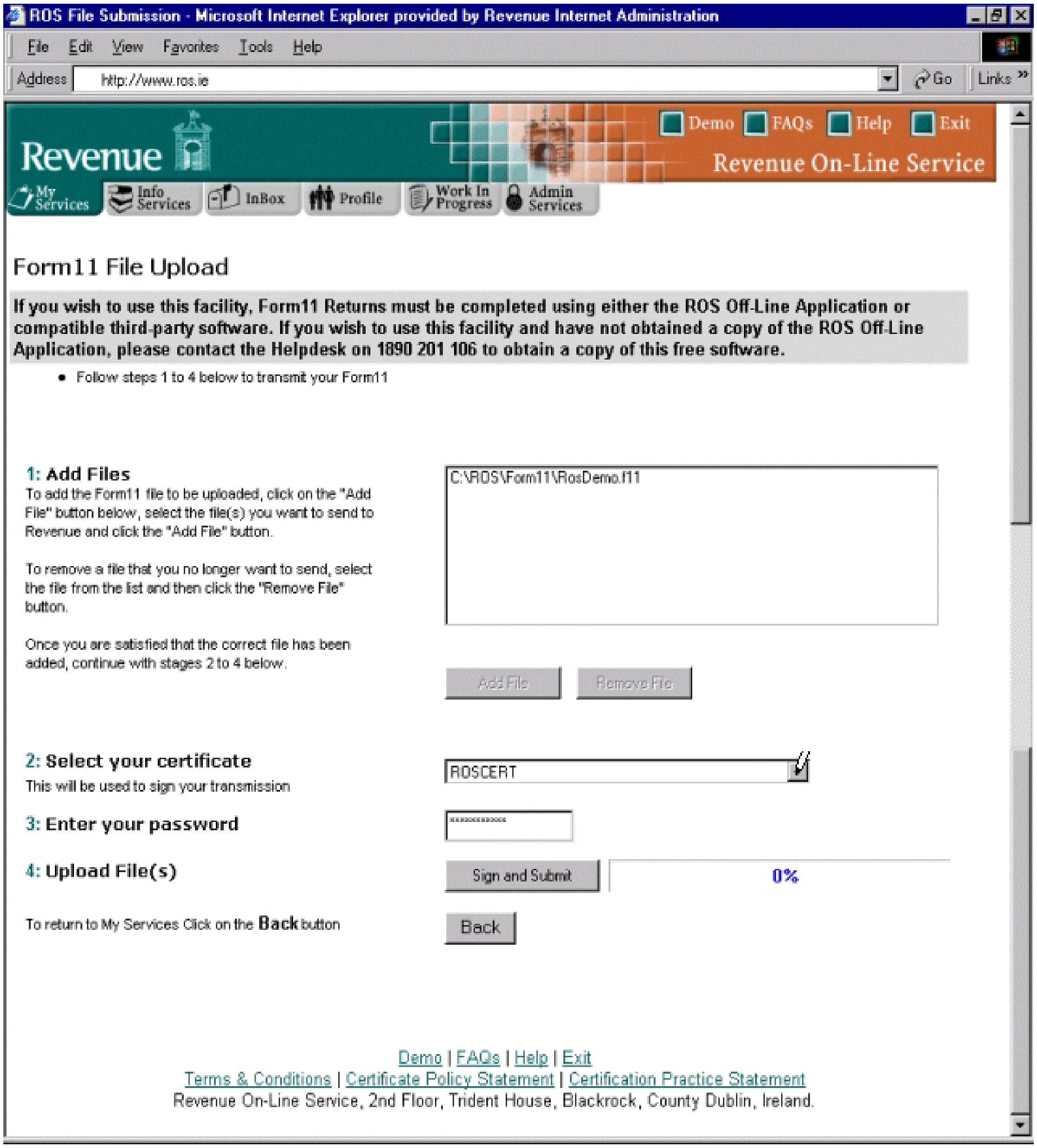
It should be noted that user error requires intervention at the Tax Office to correct discrepancies. ROS operates a 'Last Chance Check' displaying information to the user to recheck before signing and submitting. The system's error checking functionality is designed to detect invalid data, rather than human errors (e.g., entering €10,000 instead of €100,000).

Following formal submission, the ROS system immediately sends a copy of the submitted and signed record to the user's ROS Inbox for future reference.

Debit Instruction Forms

The ROS system accommodates two different options for completing RDI forms (see Figure 20): (1) online while signed on to the ROS system, and (2) offline by hand using a downloadable form.

1. **Online**. To complete an RDI online, a user or agent logs onto the ROS Web site and enters his/her RAN to gain access to the secure section of the Web site. An RDI is then filled out online via a series of Java-controlled form screens in which the users is required to enter his/her bank account details, select which tax type(s) and registration number(s) to apply the RDI to (a single RDI can be applied to more than one tax type and registration number), select the certificate to be used to sign the RDI, enter his/her password and click the 'Sign and Submit' button to formally submit the RDI to the ROS



Form11 File Upload

If you wish to use this facility, Form11 Returns must be completed using either the ROS Off-Line Application or compatible third-party software. If you wish to use this facility and have not obtained a copy of the ROS Off-Line Application, please contact the Helpdesk on 1890 201 106 to obtain a copy of this free software.

- Follow steps 1 to 4 below to transmit your Form11

1: Add Files

To add the Form11 file to be uploaded, click on the "Add File" button below, select the file(s) you want to send to Revenue and click the "Add File" button.

To remove a file that you no longer want to send, select the file from the list and then click the "Remove File" button.

Once you are satisfied that the correct file has been added, continue with stages 2 to 4 below.

C:\ROS\Form11\RosDemo.f11

2: Select your certificate

This will be used to sign your transmission

ROSCERT

3: Enter your password

****

4: Upload File(s)

To return to My Services Click on the **Back** button

Demo | FAQs | Help | Exit

Terms & Conditions | Certificate Policy Statement | Certification Practice Statement

Revenue On-Line Service, 2nd Floor, Trident House, Blackrock, County Dublin, Ireland.

Figure 21. ROS File Upload interface used to submit tax forms completed offline

system. Successful submission of an RDI results in a copy of the RDI being forwarded to the user's ROS Inbox immediately.

2. **Offline**. To complete an RDI offline, a user or agent logs onto the ROS Web site and enters his/her RAN to gain access to the secure section of the Web site. An RDI form in PDF format may then be downloaded to the user's computer and/or printed to hard copy, filled in by hand and mailed to Revenue for processing. Once processed, the user will be notified via e-mail that a copy of the RDI has been forwarded to the user's ROS Inbox.

It is noted that a tax liability payment does not necessarily need to accompany a return filed electronically. Therefore, it is not mandatory that an RDI be set up before a tax return can be filed in ROS. In fact, customers who file an electronic return can, if they wish, still use other more traditional forms of payment, such as a cheque, thereby negating the need for an RDI altogether.

Once an RDI is in place, a user must then submit an electronic payment instruction form to authorize specific payment amounts to be drawn from the user's bank account on specific dates. To complete an electronic payment instruction form, a user or agent logs onto the ROS Web site and enters his/her RAN to gain access to the secure section of the Web site. After clicking on the "Payment" button on the user's "My Services" page and selecting the applicable tax type(s) and registration number(s), the system will indicate whether an RDI is linked to the registration for the tax type(s) selected. In the absence of a valid RDI for the tax type selected, the user may choose instead to pay online using Laser by entering his/her Laser card number and expiration date. In cases where an RDI is linked to the registration for the tax type(s) selected, the payment instruction form will be pre-filled with the user's banking details (drawn from the user's RDI) and the amount of the user's relevant tax liability.

Whether paying via Laser or a linked RDI, the user must enter (or, if already pre-filled, confirm) the total payment amount and the payment date, then sign and submit the payment form. Immediately following a successful payment form submission, an electronic receipt is forwarded to the user's ROS Inbox.

The user's tax liability is calculated on the basis of the entries made on his/her tax return. The user can change the amount to be paid on the electronic payment form, if required. Any shortfall in what is paid is followed up via the back-office systems compliance processes.

7. To what other digital or non-digital entities are they connected in either a conceptual or a technical way? Is such connection documented or captured?

Digital Certificates and Signatures

ROS digital certificates are connected to Revenue's CA. In both Revenue and ROS's case, there is a link between their public and private keys. All Approved and Authorized Persons hold a public key as a component of their digital certificate and their private key resides on their computer.

As part of the process of acquiring a digital certificate, ROS causes paper outputs to be issued by the ITP system (i.e., the RAN and System Password letters mailed to users), so there is a formal relationship between the electronic application and these paper outputs.

Tax Forms

ROS is essentially a data collection and a data publishing system in which data is collected from customers and tax agents that would otherwise be submitted to Revenue on paper, and outputs are delivered to customers electronically that would otherwise be issued on paper by placing them in the customer's ROS Inbox. These inputs and outputs are processed by Revenue's back-office systems. Also, at the heart of ROS is a virtual copy of the ITP system database. In this way ROS is fully integrated with these back-office systems.

Revenue's integrated solution to tax collection and administration comprises four core internal elements, which are complemented and 'fed' in part by ROS.

> In putting together an integrated solution, Revenue focused on four core elements: (1) a common registration system whereby all taxpayers are registered on a single database; (2) a proactive intervention strategy which allows Revenue to act before customers become non-compliant; (3) a corporate information facility which provides for statistical forecasting and budgetary projections; and (4) an integrated taxation processing system which ensures a common platform for the issuing and processing of tax forms and payments, as well as linking with the other three elements in the system. A new Internet file and pay service complements these internal solutions.[44]

Debit Instruction Forms

Outputs from ROS in the form of debit instructions link to financial institutions and Revenue back-end systems. The successful payment of a tax liability triggers the updating of the information in the back-end systems, the debiting of the user's account and the generation and posting of a receipt to the user's ROS Inbox.

8. What are the documentary and technological processes or procedures that the creator follows to identify, retrieve, and access the digital entities

ROS uses UIDs and database structures to identify, retrieve and access digital entities.

What documentary processes are followed?

When a tax form is received from a user and validated by ROS, the data is exported to ITP and, if appropriate, the relevant financial institution. The data is then used to update a user's account with Revenue. All activities are time and date stamped in addition to using the security wrapper as a means of verification.

What technological processes are followed?

The technological processes used by ROS to oversee identification, retrieval and access to the digital entities in the system can be grouped into three general categories: (1) security-related processes, (2) administrative-related processes, and (3) generic Web-related processes. It should be emphasized that, to a large degree, the processes discussed below are from the perspective of the users of ROS, and only relate the creator's (i.e., Revenue) digital entity identification, retrieval and access activities in a tangential way. In fact, the processes

[44] See www.ca.com - client information sheet on Revenue (Accessed 18 Feb 2004).

and procedures used by the creator for identification, retrieval and access to the digital entities examined in this report appear, for the most part, to be largely restricted to the use of UIDs (to uniquely identify records in the ROS and Revenue databases) and various search and retrieval database structures.[45]

- **Security-related Processes**
  These include the PKI framework (Keys, Certificates and security software), the ACS, and the use of secure login procedures requiring a valid certificate and password. Each of these processes helps control which digital entities may be retrieved, viewed, edited, downloaded and/or printed to hard copy by the user or agent, and, in certain cases (e.g., user's Private Key), by Revenue.

- **Administrative-related Processes**
  These include the use of the dedicated ROS Information Services, Administrator Services and Inbox features (all accessible from within a user's secure ROS Web page), in conjunction with a user's official e-mail, to administer identification, retrieval and access to system notifications, receipts, reminders, filed returns and other records. They also include the use of sub-certificates, in conjunction with the Access Control System (ACS), to help manage and administer access privileges for agents (i.e., Approved Persons) acting on behalf of their clients (i.e., Authorised Persons). Finally, they include the back-end database management processes and procedures (e.g., the use of UIDs to uniquely identify records in the system) that are used to transfer data back and forth between the ROS database and Revenue's ITP back-office system, synchronize and update the data in the two systems.

- **Generic Web-related Processes**
  These include the navigational links and the online help documentation provided on the secure section of the ROS Web site that help facilitate identification, retrieval and access to the digital entities associated with a user's ROS account.

9. Are those processes and procedures documented? How? In what form?

From the perspective of the creator (i.e., Revenue), no documentation was identified during the interview process that refers to the digital entity identification, retrieval and access processes or procedures associated with the back-end systems of ITP and others as used by ROS to store and present data.

On the other hand, from the perspective of the users of ROS, most, if not all, of these processes and procedures are supported by copious documentation in the form of technical system specifications and guidelines, periodic news bulletins, online help documentation and links, animated ROS demonstration applets, and user FAQs.

[45] Presumably, Revenue has its own search and retrieval system in place to identify, retrieve and access the records in its databases (i.e., distinct from the ROS Web page interface used by ROS customers).

10. What measures does the creator take to ensure the quality, reliability and authenticity of the digital entities and their documentation?

Customers have their own personalized inbox, secured through a PKI environment. PKI is understood by Revenue to provide four attributes of authenticity: the guarantee of integrity of data, the guarantee of the identification and authentication of the communicator, the provision of an environment of non-repudiation, and the provision of the confidentiality of personal data at all times. External users must be authorized to use the ROS through a digital certificate.

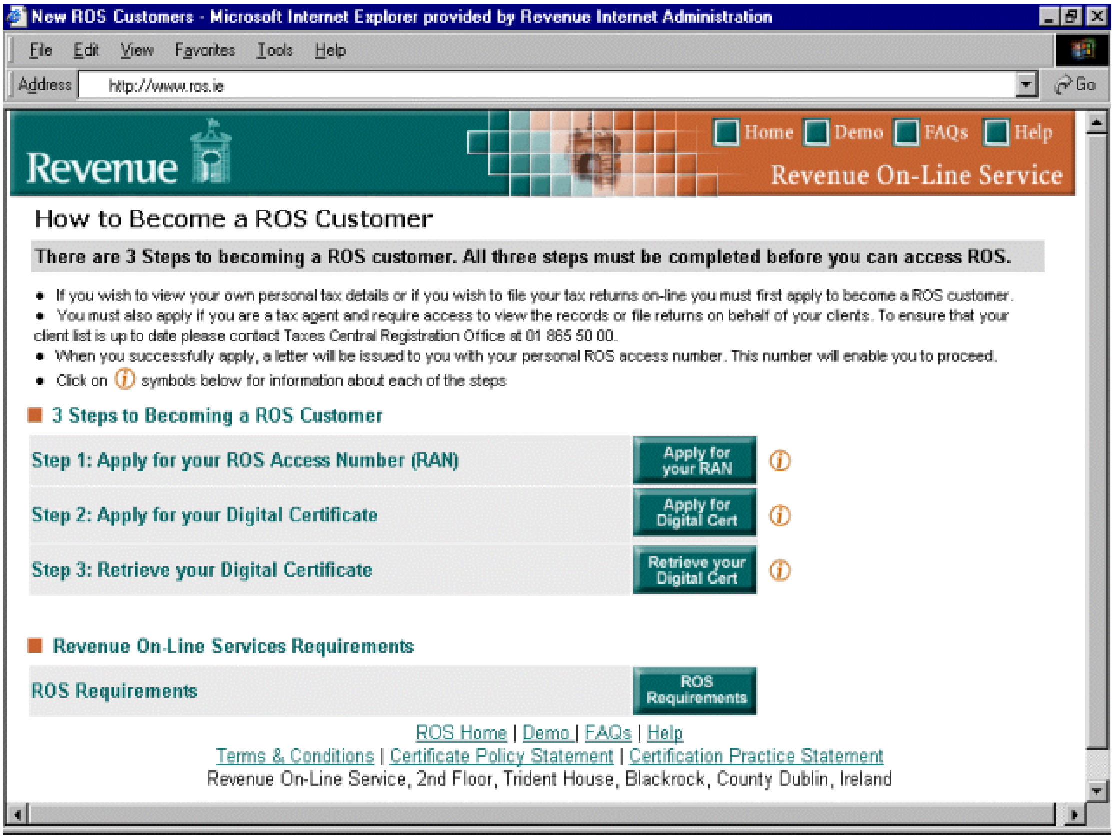
Access is also connected to the job responsibilities of Revenue employees. The Revenue Certification Practice Statement details the policy related to employee access to digital certificates and the PKI structure, and the RPS Access Control System ensures staff access is restricted based on job responsibilities.

The mirroring of the ITP system also offers greater security of Revenue's systems.

Digital Certificates and Signatures

The digital certificates themselves are used as a measure of authenticity for the tax forms and debit instruction forms, since only customers with a valid, password-protected, digital certificate can enter the ROS secure site.

The issuance of certificates is tightly controlled via a regimented series of both online and offline procedures and processes. To apply for and retrieve his/her certificate, a user must first obtain a RAN. As shown in Figure 22, this is identified as the first of three steps involved in registering as a ROS customer. This process is carried out entirely online using a series of Java-controlled forms into which users are required to enter and submit their tax registration number and their contact information (name and telephone number). Following successful completion of Step 1, ROS sends the applicant his/her RAN number via letter mail. Once received, the applicant must then return to the ROS Web site to apply for a digital certificate (Step 2 in the ROS customer application process). This process is also carried out entirely online using a series of Java-controlled forms into which users are required to enter and submit their RAN, their tax registration number and their official e-mail contact information. Following successful completion of Step 2 and verification of the user's RAN, Revenue notifies the ROS CA to issue a digital certificate for the applicant. A RAN system password is generated at the same time and mailed to the applicant. Once this password is received, the applicant must once again return to the ROS Web site to retrieve his/her digital certificate (Step 3 in the ROS customer application process). This final process is also carried out entirely online using a series of Java-controlled forms. To begin with, users are required to indicate their acceptance of the ROS system terms and conditions of use, provide their tax registration number and enter their system password. Users are then required to enter their name and provide their own personal password and click the 'Request Certificate' button. At this point, the certificate is downloaded and installed onto the hard drive of the user's computer under a ROS sub-directory.


New ROS Customers - Microsoft Internet Explorer provided by Revenue Internet Administration
File Edit View Favorites Tools Help
Address http://www.ros.ie
Go
Revenue
Home Demo FAQs Help
Revenue On-Line Service

How to Become a ROS Customer

There are 3 Steps to becoming a ROS customer. All three steps must be completed before you can access ROS.

- If you wish to view your own personal tax details or if you wish to file your tax returns on-line you must first apply to become a ROS customer.
- You must also apply if you are a tax agent and require access to view the records or file returns on behalf of your clients. To ensure that your client list is up to date please contact Taxes Central Registration Office at 01 865 50 00.
- When you successfully apply, a letter will be issued to you with your personal ROS access number. This number will enable you to proceed.
- Click on ⓘ symbols below for information about each of the steps

3 Steps to Becoming a ROS Customer

Step 1: Apply for your ROS Access Number (RAN)	Apply for your RAN	ⓘ
Step 2: Apply for your Digital Certificate	Apply for Digital Cert	ⓘ
Step 3: Retrieve your Digital Certificate	Retrieve your Digital Cert	ⓘ

Revenue On-Line Services Requirements

ROS Requirements	ROS Requirements

ROS Home | Demo | FAQs | Help
Terms & Conditions | Certificate Policy Statement | Certification Practice Statement
Revenue On-Line Service, 2nd Floor, Trident House, Blackrock, County Dublin, Ireland

Figure 22. Main ROS customer registration screen

Revenue has articulated a very strong position regarding its implementation of PKI. Two documents covering various policies and procedures detail the steps taken to ensure quality and integrity of digital certificates.[46] However, it should be noted that in the transaction to retrieve the certificate, the user must accept Revenue's terms and conditions, including 1.6, which states that "In the event of and in your transmitting material to Revenue using ROS, Revenue has no responsibility for the accuracy, veracity and completeness of same and for any errors in the manner of its input."

Tax Forms

Various validation controls are used to assist users in inputting data online. There is field validation in forms such as alphanumeric controls or date structures. Cross validation is used to ensure there is no logical inconsistency (e.g., a person checking a status box for 'Single' and then claiming a married allowance). The system also employs basic calculators to assist in calculating tax liabilities, as well as built-in logic and dynamic options to present a form based on choices made and to reduce the need for scrolling or presenting sections that are not applicable to the user.

[46] See: Office of the Revenue Commissioners Ireland (2000). "Revenue Public Key Infrastructure: Certification Practice Statement," and Office of the Revenue Commissioners Ireland (2000). "Revenue Online Service Certificate Policy Statement."

Mistakes or inaccuracies are minimized through the use of controlled fields that must contain accurate information to be accepted by the system. Should a user later identify mistakes that were not identified by the system prior to submission of the form to ROS, s/he must contact the relevant tax office directly to request that the mistakes be corrected.

The same type of validation functionality is built into the ROS Offline Application and the uploaded and signed forms are also validated on receipt by ROS (at the point of submission and subsequent acceptance by ROS as 'valid').

Revenue does not accept responsibility for faulty information but does, as part of any transaction, provide users with a final summary check to confirm that the data entered are correct. This data is time/date stamped and is securely transferred to the ROS system using PKI. The ROS system also retains a copy of all submitted forms in a user's ROS Inbox.

Debit Instruction Forms

The quality, reliability and authenticity of RDIs is tightly controlled via a regimented series of either online or offline processes and procedures (see Question 6, above). For RDIs created online, this level of control is achieved via a series of Java-controlled forms utilizing controlled data entry fields that must contain accurate information to be accepted by the system. Presumably, the data used in the offline process to create RDIs using paper forms submitted to ROS are either authenticated via manual processing, or are subjected to automated processing similar to that used for the online RDI application process once the data is entered into the system by a Revenue employee. These measures, as well as those outlined above for digital certificates and tax forms, help to ensure the authenticity of the system's users and the reliability and accuracy of the data they submit to ROS, which, in turn, serve to reinforce the authorization for a user's tax liability payment.

11. Does the creator think that the authenticity of his digital entities is assured, and if so, why

Revenue asserts that the use of its PKI assures, among other things, the identity, and hence authenticity, of all parties using the ROS system (including Revenue), as well as the non-repudiation of all transmissions that occur between ROS and its users through the use of a digital signature that binds the person making the transmission to what is received at the other end. This, in turn, implies that Revenue believes the digital entities created by ROS are indeed authentic.

The Revenue CA is the highest point of trust within the Revenue PKI and, as such, has articulated strong policies and procedures designed to ensure the continued trust and security of the Infrastructure. Security of the Revenue and ROS private keys is paramount. Consequently, Revenue has implemented extensive, stringent technological, physical, procedural and personnel security controls and obligations to minimize threats to the PKI.[47] In the words of Revenue, its PKI "has adopted and employs personnel and management practices to ensure the

[47] See: Office of the Revenue Commissioners Ireland (2000). "Revenue Public Key Infrastructure: Certification Practice Statement."

trustworthiness, integrity and professional conduct of all staff and agents involved in its operation.[48]

Revenue regards the use of PKI to offer twofold protection of the authenticity of its digital entities by ensuring: (1) the identification and authentication of all communicating parties, and (2) the non-repudiation of transmissions.[49]

- **Identification and Authentication**
  In the Revenue PKI, all Private Keys are unique to the persons to whom they are issued and serve the same function as a hand-written signature. The fact that the Public Key matches the Private Key used identifies the sender as the person who purportedly holds the Private Key. Thus, the use of matching Public and Private Keys allows a user to authenticate the identity of the ROS server, and have his/her own identity authenticated in turn by ROS. This authentication process results in the establishment of a 'secure session' by which encrypted communications can be trusted to arrive privately and unaltered to the specified recipient and no other.

- **Non-repudiation**
  It is essential that a secure system exists between the ROS system and its users whereby neither a user nor Revenue cannot repudiate a communication or transaction. This level of non-repudiation is achieved through a combination of the guaranteed integrity of the data transmitted to and from ROS, together with the uniqueness of the sender's Private Key and the time/date stamped security wrapper applied to all transmissions.

Legislation designed to cater to ROS activities was included in the 1999 *Finance Act*.[50] Among other things, the amendments to this Act allow for: (1) an Approved or Authorised Person to electronically transmit the information required on a return on behalf of a taxpayer without the need for the taxpayer's written signature, and (2) the recognition of electronic transmissions for legal purposes. Consequently, Revenue regards the digitally-signed electronic records as acceptable in law and believes that this claim is bolstered via a **chain of authenticity** created by compliance with the following steps:

1. Authentication and identification of users through the use of RANs and digital certificates;
2. Validation by ROS of all submitted data;
3. Retention, logging and archiving of all actions within ROS;
4. Prevention of the deletion or modification of entries from ROS Inboxes; and
5. Time/date stamping of all actions within ROS.

12. How does the creator use the digital entities under examination?

Revenue's use of the digital entities under examination here is entirely dictated by obligations imposed by statute and by Government and as a result of Ireland's membership in the European

[48] Ibid., p. 19.
[49] These are, in fact, two of the four functional requirements that the PKI is mandated to fulfill under the *Taxes Consolidation Act 1997*, Part 38, Chapter 6(3)(5). Available at: http://www.revenue.ie/services/foi/s16_2001/pt_38.pdf.
[50] See Part 7, section 209 (Electronic filing of tax returns). Available at: http://www.irishstatutebook.ie/ZZA2Y1999S209.html.

Union. Thus, in general terms, Revenue uses these digital entities to support its mandate and core business, which is the assessment and collection of taxes and duties.

Digital Certificates and Signatures

Revenue and ROS CAs create digital certificates to ensure data integrity through digital signing and user authentication through unique identification.

Tax Forms

ROS does not itself process data from tax returns. Instead, ROS is responsible for securely receiving, validating and authenticating all submissions, and forwarding the data to the appropriate back-end system for processing by Revenue. A key aspect of this processing activity is the issuing of various tax assessments, notifications, acknowledgements and receipts, which, in relation to returns submitted electronically, is carried out through transfer of relevant data from Revenue back-end systems to taxpayers via ROS. Thus, it is the ROS system that is responsible for providing users secure access to this information, as well as secure access to copies of their submitted returns (via their ROS Inboxes). It is also noted that data mining of Revenue/ROS-created data is used to audit tax details, improve efficiencies, increase customer service and enable fraud detection.

Debit Instruction Forms

Revenue uses the debit instructions as an efficient and secure means of facilitating the collection of tax liabilities due in line with Ireland’s taxation laws.

13. How are changes to the digital entities made and recorded

Digital Certificates and Signatures

Generally speaking, no changes can be made to a digital certificate once it is created. However, a certificate can be divided into sub-certificates in line with the ACS, allowing an Approved Person (e.g., tax agent) acting on behalf of more than one Authorised Person to manage multiple users and their rights in ROS (See Q.14).

Digital certificates have a fixed operational life that is determined by the relevant CP. Certificates automatically expire upon reaching their designated expiry date (generally two years), at which time they are archived by Revenue for a minimum period of ten years, or other such time as required to meet requirements of Revenue. In most situations, the life of a certificate cannot be extended, nor does the ROS CA support the routine renewal, re-issuing or rekeying of certificates.[51] Instead, a reminder to apply for a new certificate is automatically issued to a user’s official e-mail address by the ROS system at the appropriate

[51] Apparently, however, users may, in certain circumstances, request that the Revenue PKI renew their Keys and Certificates at the end of their standard life provided that: (1) the request is made prior to the expiry of the current Keys and Certificates, (2) material Certificate information has not changed, and (3) the current Keys and Certificates have not been revoked (Office of the Revenue Commissioners Ireland (2000). “Revenue Public Key Infrastructure: Certification Practice Statement,” pp. 16, 36).

time. Metadata related to the expired certificates, in addition to the security wrapper, is maintained within ROS. As alluded to above, Revenue has a separate Archiving Policy for certificates but this is considered beyond the remit of ROS.

Tax Forms

There is no versioning or updating. ROS considers a user's clicking of the 'Sign and Submit' button a formal declaration that the return being submitted is complete; consequently, no subsequent changes or revisions can be made to that submitted version. Whether working online or offline, a user can save, update, and resave a draft return as often as needed prior to formally signing and submitting the final version. While only the most current draft is retained in the online and offline ROS applications, users can save each draft on their own computer (outside of the ROS application), if so desired. It should also be noted that if a user proceeds with a new return whilst still holding a draft of a previous one in the ROS application, the earlier draft will be overwritten.

Once a return is signed and submitted, it is time/date stamped and forwarded to the appropriate Revenue back-end system to be retained as a record and processed, but ROS does no further action to it. However, when interfacing with other systems, ROS may restructure the data into a required format for ingest by the appropriate back-end system (e.g., XML or flat files in the case of Form 11). In some cases, ROS may perform basic calculations on the data prior to transfer but this is not regarded as changing or amending the return.

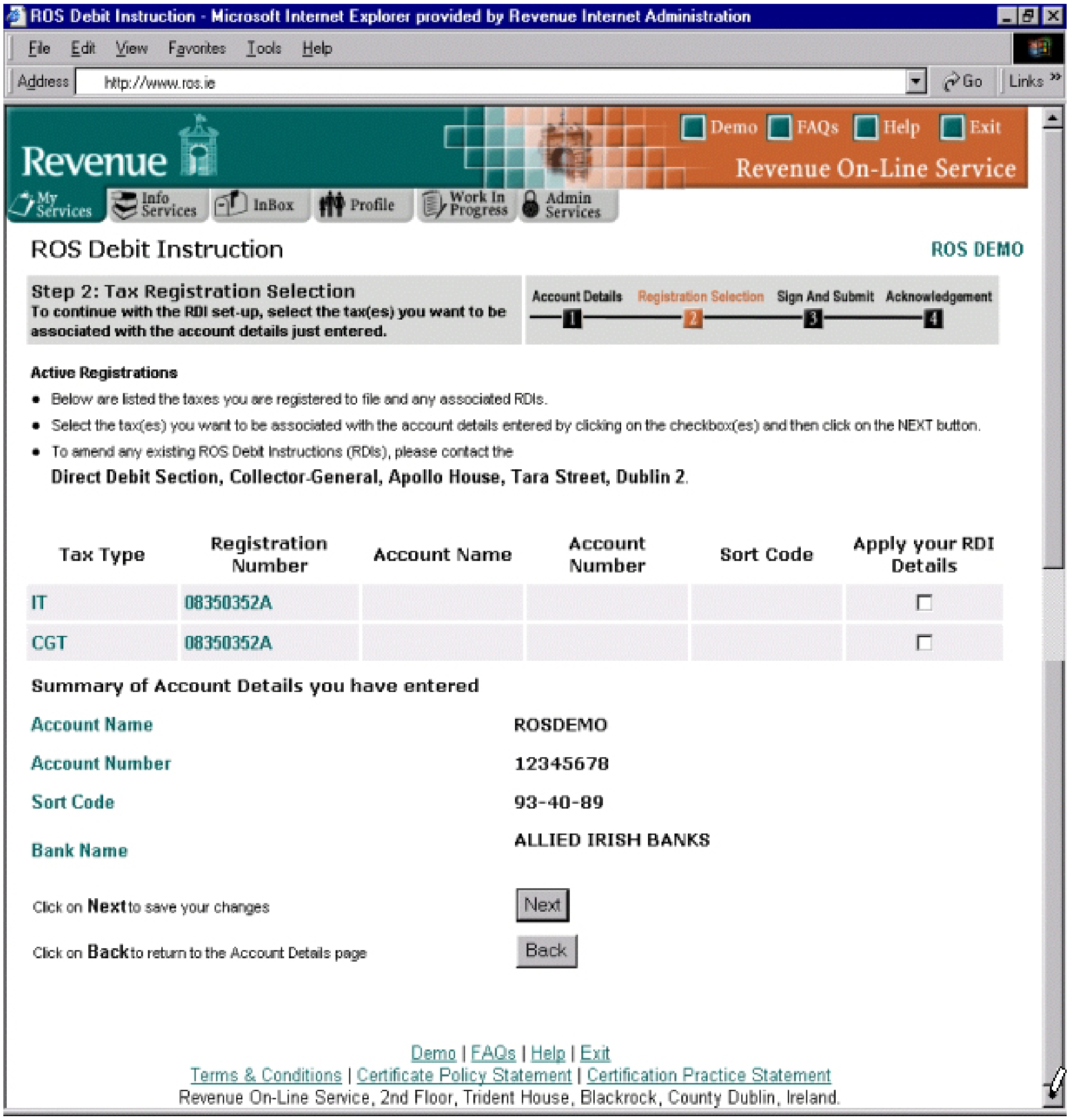
ROS staff may examine a submitted return if a customer makes a specific complaint, or to investigate a reported problem, but will not amend the record. Records are not deleted and any problems encountered are followed up directly by the person at the appropriate regional tax office.

ITP manages data processing and the system allows for both paper and electronic data to be used. It is important to note that the transaction history held in a user's
ROS Inbox only details actions and transactions that were made through ROS; no paper audit is available. However, the view of the ITP copy offers a god's eye view of all transactions either paper or electronic.

The only time when data in the ROS database is changed is following an update through the daily import of data from the ITP. Such action will include manual and electronic changes to the tax records.

Debit Instruction Forms

Generally speaking, an RDI can only be changed or revoked by its user. However, it appears that the user may, in some cases, authorize the Direct Debit Section of Revenue to amend an existing RDI (e.g., update the user's financial institution information) (Figure 23, see third bulleted item under Active Registrations). Once established, an RDI may be used indefinitely by the user to authorize electronic transfers of funds from the nominated bank account to



ROS Debit Instruction

ROS DEMO

Step 2: Tax Registration Selection
To continue with the RDI set-up, select the tax(es) you want to be associated with the account details just entered.

Active Registrations

- Below are listed the taxes you are registered to file and any associated RDIs.
- Select the tax(es) you want to be associated with the account details entered by clicking on the checkbox(es) and then click on the NEXT button.
- To amend any existing ROS Debit Instructions (RDIs), please contact the

Direct Debit Section, Collector-General, Apollo House, Tara Street, Dublin 2.

Tax Type	Registration Number	Account Name	Account Number	Sort Code	Apply your RDI Details
IT	08350352A				□
CGT	08350352A				□

Summary of Account Details you have entered

Account Name	ROSDEMO
Account Number	12345678
Sort Code	93-40-89
Bank Name	ALLIED IRISH BANKS

Click on **Next** to save your changes

Click on **Back** to return to the Account Details page

Demo | FAQs | Help | Exit
Terms & Conditions | Certificate Policy Statement | Certification Practice Statement
Revenue On-Line Service, 2nd Floor, Trident House, Blackrock, County Dublin, Ireland.

Figure 23. ROS Debit Instruction setup screen, Step 2 – Tax Registration Selection

Revenue. The user initiates such transfers by completing an online electronic payment instruction form (accessible by clicking on the 'Payment' button on the user's 'My Services' ROS Web page). This form is prefilled with the user's banking details using data drawn from the RDI, as well as the total amount of the user's relevant tax liability and the due date. All that is required from the user is confirmation of the amount to be transferred and the date on which the transfer should occur. Both the amount to be transferred and the date of transfer can be changed by the user to allow for incremental instalment payments, if desired.

14. Do external users have access to the digital entities in question? If so, how, and what kind of uses do they make of the entities?

"External users" is taken to mean Approved and/or Authorised Persons.

Digital Certificates and Signatures

A copy of each digital certificate is held in ROS and by each user. A user's private key is stored on his/her own computer and is completely separate from ROS. It is the intention of the Irish government that the Revenue CA will issue digital certificates for other e-initiatives. If this proceeds, then the ROS digital certificate may be used to confer authenticity and integrity on data submitted to other government departments or agencies.

Tax Forms

Approved or Authorised Persons can access stored records via the ROS Customer Information Service section of the ROS Web site. This service allows users to search for, retrieve and view data and records under the following headings:

- Payments (details of tax liability payments made by a user);
- Returns (listing of returns due and returns filed by a user);
- Refunds and Repayments;
- Taxhead Registration Details (detailed information about all of a user's Tax Registrations);
- Charges and Collections (listing of user's tax liabilities and payments);
- Event List (chronological list of activity on a user's Tax Registration);
- Statement of Account (provides an interface for user to request a Statement of Account on any Tax Registration be delivered to the user's ROS Inbox);
- Items Submitted via ROS (listing of all items submitted to ROS by a user); and
- Outstanding returns (tax agents only).

Management of external access is controlled by the ACS in conjunction with the granting of sub-certificates to identified persons and agents. The digital certificate identifies people who log onto the ROS system. Agents acting on behalf of tax clients can only view records of those clients who have requested that the agent act on their behalf. ROS uses previous client history to set up agents. Agents are given a special Tax Agent and Identification Number (TAIN) to enable them to gain access to their client's accounts. Customers and agents can restrict the level and degree of access their staff have, if required, by using sub-certificates and the ACS facilities. Each individual is responsible for his/her own digital certificate and its management. An Administrative Certificate allows a user to specify degrees and levels of access controls for sub-certificates, which can be given to other employees within the agency. For example, one person may only have access rights to view and not alter data in ROS, while another may have the right to input and submit returns for VAT but not payroll (PREM form). Given the nature of the operation (tax payment), there is little scope for financial gain by obtaining another taxpayer's digital certificate, but confidentiality is still a major concern.

Debit Instruction Forms

Banks and financial institutions receive copies of RDIs submitted by ROS users. Other payment options such as Laser (debit card) also result in the transfer of requests for payment authorizations from ROS users to their financial institution, submitted via ROS.

15. Are there specific job competencies (or responsibilities) with respect to the creation, maintenance, and/or use of the digital entities? If yes, what are they?

All job-specific employee training and support is administered through Revenue's Performance Management and Development System (PDMS), which became operational for all grades across all Revenue Regions and Divisions in 2003. The PDMS is designed to "clearly identity the role of each person in the organisation, and the range of competencies they need to fulfil this role." While specific job competencies and/or responsibilities related to the creation, maintenance, and/or use of the digital entities examined in this report likely exist, with the exception of those noted below for Keys and Certificates, documentation outlining the specifics of these competencies and responsibilities was not available for inclusion in this report.

For the most part, the creation, maintenance and use of the digital entities in question are automated where possible. ROS staff are responsible for business analysis, functional specification of ROS processing, and for assuring the quality of ROS front-end processing and interfaces with back-office systems, and also for ROS marketing. The objective of ROS is to remove the need for human intervention in filing tax returns and making associated payments.

With respect to the ROS system itself, it is noted that development and maintenance of the system has been outsourced to Accenture.[52] Development and maintenance of back-office systems to which ROS interfaces records input by customers is handled by a mixture of both in-house and outsourced staff, in the case of the ITP system, and by in-house development teams in the case of other back-office systems.

Digital Certificates and Signatures

Basic job competencies and responsibilities for Revenue PKI services personnel charged with various digital certificate administration functions are outlined in Section 5.3 "Personnel Controls" of the *Certification Practice Statement*.[53] As noted in this section, "recruitment and selection practices for Revenue PKI services personnel take into account the background, qualifications, experience and clearance requirements of each position…" All Revenue PKI services staff members receive appropriate training specific to their administrative functions. Certain Revenue PKI services personnel are, for example, responsible for ensuring that Approved and Authorised Persons understand their responsibilities for adhering to the possession, use and operation of their Keys and Certificates, as outlined in the Conditions of Use statements that apply to each.

To help ensure that one person acting alone cannot circumvent the PKI security system, the area where the servers and work stations that comprise the Revenue PKI is located is a

[52] http://www.accenture.com/xd/xd.asp?it=irweb&xd=locations\ireland\ireland_home.xml.

[53] Office of the Revenue Commissioners Ireland (2000). "Revenue Public Key Infrastructure: Certification Practice Statement," pp. 46-47.

declared “no lone zone,” meaning that all tasks carried out within these areas require oversight from two PKI services personnel. For example, in certain instances access to equipment requires that two keys be inserted and turned simultaneously to open the cabinet securing the equipment. Likewise, access to a work station requires that separate passwords be input by two employees, at which point one person performs the task while the other audits the task performance to ensure it is done properly.[54]

At a minimum, the following roles are established at each Revenue location with respect to management of the PKI:[55]

- System Administrator;
- Registrar (ROS CA); and
- Security Administrator.

Revenue PKI services staff also receive training in the use and operation of the CA and RA’s software whenever new versions of the software are installed and/or on an as-needed basis. Finally, it is noted that Revenue PKI services staff are required to have access to their relevant:

- Hardware and software documentation;
- Policy documents, including the Certification Practice Statement; and
- Operational practice and procedural documents, including a relevant CP.

Tax Forms

For security purposes, ROS does not require nor allow manual intervention by ROS staff following formal signing and submission of electronic tax returns. All newly submitted records are exported from the ROS system on a daily basis, and ROS staff have no further responsibility for them. The virtual copy of a user’s tax return residing in the ITP database is typically available in read-only form. Once in the ITP database, changes can only be made to a user’s return by authorized Revenue staff at the user’s local tax office. All such changes or corrections are logged and time/date stamped. Certain back-end systems and Revenue employees are authorized to use the submitted tax returns for compliance and audit purposes.

Debit Instruction Forms

Again, for security purposes, ROS does not require nor allow manual intervention by ROS staff following formal signing and submission of RDIs. Instead, the ROS system automatically exports these entities to the ITP database and forwards copies to the appropriate financial institution systems.

[54] Ibid., pp. 44-45.

[55] Ibid., p. 45.

16. Are the access rights (to objects and/or systems) connected to the job competence of the responsible person? If yes, what are they?

Digital Certificates and Signatures

Yes. To ensure the level of trust necessary for Revenue to function as a CA, a detailed policy statement notes the level and degree of access to digital certificates. Revenue's Certification Practice Statement goes into considerable detail about the procedures surrounding staff access to PKI structures (See Appendix 2).

> *In all cases, the Revenue PKI operates to:*
>
> *1. Generate Keys and Certificates securely and take appropriate precautions to protect against their compromise, modification, disclosure, loss or unauthorised use.*
>
> *2. Be able to detect and record unauthorised events and actions.*
>
> *These procedures extend to the Revenue PKI, which must ensure that only an Approved or Authorised Person is made aware of the Private Keys and any associated Pass-phrase values.*[56]

Tax Forms

No. Only authorized Revenue employees have access to ITP and other back-end systems that import tax forms from ROS. A feature of the ROS submission procedure is the need by Revenue to ensure that no intervention occurs and that non-repudiation of data can be claimed.

Debit Instruction Forms

As noted earlier in Question 13, certain employees in the Direct Debit Section of Revenue appear to have the authority to, upon request from a user, amend the user's existing RDI (e.g., update the user's financial institution information) (see Figure 23, third bulleted item under Active Registrations). Presumably, there is a level of record access competency that is concomitant with the record amendment competency of these employees.

17. Among its digital entities, which ones does the creator consider to be records and why?

Revenue considers all digital entities identified within this report to be records because of their relationship to the transaction of tax filing and payment. This is reinforced by the current commitment to retain the security wrapper and its contents in their original form.

[56] Ibid., p. 19.

18. Does the creator keep the digital entities that are currently being examined? That is, are these digital entities part of a recordkeeping system? If so, what are its features

The digital entities examined in this report are made and/or received and set aside (i.e., kept) by Revenue as records of an individual's tax history with the Irish state. All official copies of these records (both active and inactive) are retained, according to a records retention authority, within the ITP mainframe system, which is separate from the ROS system, and/or are securely stored within a facility approved by the PAA. The ROS system maintains a virtual sub-set of the ITP records for easy access by ROS users. As yet, there is no defined retention period for these record copies maintained within the ROS system.

Digital Certificates and Signatures

The Revenue PKI maintains an "archive collection system." As is more fully detailed in a separate Revenue document titled "Auditing and Archiving Policy," the Revenue PKI uses this system to maintain an archive of relevant records, including certain Keys and Certificates. For example, Approved and Authorised Persons' Private Keys are never held within the Revenue PKI or by Revenue, while the Revenue CA and ROS CA Confidentiality keys are archived. All entities are subject to record-specific retention authorities as outlined in the relevant CP. For example, as outlined in the ROS CA Certificate Policy Statement, the Revenue PKI's Confidentiality keys shall be archived within the back-end systems for a minimum period of ten years from the date when they expire or such other time as required to meet requirements of the Revenue Commissioners, after which time they are archived securely to a facility approved by the PAA.[57] It is noted, however, that certain components of these digital entities (e.g., the security wrappers generated when filing tax returns) appear to be retained only in the ROS system.

The Revenue PKI archive collection system is designed to meet the requirements of the *Certification Practice Statement* as set out in the relevant CP. Among these requirements are various procedures used to obtain and verify archive information and integrity. Under these procedures, the integrity of the Revenue PKI archives is verified:[58]

- Annually at the time of a programmed Security Audit;
- At any other time when a full security audit is required; and
- At the time the archive is prepared.

Tax Forms

Copies of tax forms submitted are retained in the ITP as well as in the ROS system. Revenue does not distinguish between current and non-current files. It was noted that even after a death, files might remain current if there is an outstanding payment due to the State on behalf of the deceased's estate. Following the discharge of any liability, records are held in the live system but classified as inactive. It should be noted, however, that these inactive records are not considered archival and will be destroyed after an as yet unspecified period of retention.

[57] Office of the Revenue Commissioners Ireland (2000). "Revenue Online Service Certificate Policy Statement," p. 35.
[58] Ibid., p. 36.

Debit Instruction Forms

Details of payments authorized and made are retained as an element of a user's tax return in the ITP as well as in the ROS system.

18a. Do the recordkeeping system(s) (or processes) routinely capture all digital entities within the scope of the activity it covers?

Yes. However, it is emphasized that ROS only considers signed and submitted documents to be the authoritative records of transactions between users and ROS. Interim documents, such as drafts retained offline on a user's personal computer, or online in a user's ROS Inbox do not hold record value. In instances where interim documents are retained (e.g., when a user chooses to save copies of different draft versions of his/her tax return prior to signing and submitting the final version), these are kept for reference purposes only [and for possible cross-reference and checking in case of a query?] and do not constitute authoritative records of transactions.

Nevertheless, it should be noted that, under Ireland's *Freedom of Information (FOI) Act 1997*, which, among other statutory rights, grants citizens the right "to obtain access, to the greatest extent possible, consistent with public interest and right to privacy, to records in the possession of public bodies (such as Revenue)," 'record' is defined broadly to include drafts, working notes, margin comments and copies of records. Because draft records have no special exemption status under the *FOI Act*, Revenue is required, whenever drafts are kept, to include them in FOI considerations.[59]

18b. From what applications do the recordkeeping system(s) inherit or capture the digital entities and the related metadata (e.g., e- mail, tracking systems, workflow systems, office systems, databases, etc.)?

The ROS/Revenue recordkeeping systems utilize various Java-based applications, Web and database servers to capture and/or inherit the digital entities and related metadata. See Revenue IT documentation for additional information.

18c. Are the digital entities organized in a way that reflects the creation processes? What is the schema, if any, for organising the digital entities?

The digital entities, at least as they are presented to users, are organized in reverse chronological order by issued date (i.e., most recently issued records listed first) within each tax type. At the back-end systems level, data flow (and presumably organization of digital entities) is dependent upon the type of tax record and system receiving records from ROS.

[59] Office of the Revenue Commissioners Ireland (2003). "Misc. 22: Record maintenance and Release of papers under Freedom of Information (inserted June 2002)," *Taxes Consolidation Act 1997: Miscellaneous*, Publication under Section 16, *Freedom of Information Act 1997*; Rules, Procedures, Practices, Guidelines & Interpretations, revised February 2003.

18d. Does the recordkeeping system provide ready access to all relevant digital entities and related metadata?

For the most part, the ROS recordkeeping system does provide ready access to all relevant digital entities to both Revenue employees and ROS users. However, for security reasons, not all entities or metadata are accessible to Revenue employees and ROS users. A user's Private Key, for example, is not accessible to Revenue employees. Likewise, access to certificate information within the Revenue X.500 Directory is limited to ensure that only authorized Revenue personnel have the ability to write to or modify entries in the Revenue X.500 Directory. In the case of certificates issued to Approved and Authorised Persons, access is restricted to a single named search enquiry by Revenue officers.[60]

18e. Does the recordkeeping system document all actions/ transactions that take place in the system re: the digital entities? If so, what are the metadata captured?

All automated system actions and transactions are automatically noted and logged with a time/date stamp. Actions initiated by Revenue employees are also noted and logged with both a time/date stamp and the name of the Revenue employee initiating the action. In the case of the Revenue PKI, due to heightened security requirements, very stringent procedures are used to document all changes to the system and/or the digital entities within it. For example, all keystrokes typed on a keyboard attached to a PKI work station are captured and recorded in an audit log.[61]

19. How does the creator maintain its digital entities through technological change?

Digital Certificates and Signatures

Certificates are issued every two years. It is unclear what happens to older public keys and certificates. Proprietary technology used to create digital certificates may have long-term implications.

While the Revenue CPS addresses numerous operational and administrative procedures and controls designed to safeguard the PKI system and its contents, it does not address the issue of technological change. The Revenue PKI has established and maintains detailed documentation covering its backup, archiving and offsite storage procedures.[62] Presumably, these procedures address technological change issues (e.g., system upgrades, data migration, etc.); however, this could not be confirmed. As well, it is noted that Revenue PKI services personnel receive training in the use and operation of the Revenue CA and RA's software whenever new versions of the software are installed.

[60] Office of the Revenue Commissioners Ireland (2000). "Revenue Public Key Infrastructure: Certification Practice Statement," p. 31.

[61] Ibid., p. 45.

[62] Ibid., pp. 41-42.

Tax Forms

It is reemphasized that these records are not considered archival and will be destroyed after an as yet unspecified period of retention. As necessary, records are migrated when back-end systems are being updated. The current block of data held in ITP is composed of new and migrated data. ROS uses XML as an export standard and this should enable migration to newer systems in the future. That said, there are no specific plans to migrate records in the future. In fact, it was noted that when migrating to new systems, Revenue may decide not to migrate all records and allow older, inactive records to remain on older system or else archived to offline storage.

Debit Instruction Forms

These are held as part of the tax form within ROS and ITP.

19a. What preservation strategies and/or methods are implemented and how?

Digital Certificates and Signatures

“Security wrappers” are held in ROS indefinitely.

According to the Revenue CPS, certain Revenue and ROS Keys, Certificates and supporting records (e.g., audit logs) are routinely preserved (archived). For example, the Revenue CA Confidentiality keys are archived (presumably within the live system) for a minimum period of ten years from the date when they expire, or such other time as required to meet requirements of the Revenue Commissioners, after which time they are archived securely to a facility approved by the PAA.[63]

Tax Forms

Tax return records are held in ITP indefinitely. The original system allowed users to view current and two years’ history. This has been extended to current and seven years’ history. It is unclear if this is in response to companies law or the statute of limitations. Revenue intends in the future to enable users to view an entire tax history to cut down on the number of requests it receives for manually-generated histories.

Work practices and increased use of IT are driving the retention and preservation of records, rather than any legislative need. Tribunal mentality has highlighted the need to present accurate financial records over time, and Revenue are conscious of this.

All tax records are held whilst active. Even following a death, a person’s estate may owe Revenue money and the record will not be closed. Inactive records are maintained in the ITP system but are not exported to ROS. Thus, the virtual image of ITP transferred to ROS only contains data for active ROS users and their clients.

[63] Ibid., p. 40.

Note that Standard IT backup and disaster recovery operations are in place.

Debit Instruction Forms

As 19.

19b. Are these strategies or methods determined by the type of digital entities (in a technical sense) or by other criteria? If the latter, what criteria?

Digital Certificates and Signatures

The need to reissue digital certificates routinely for security reasons requires that their life span be limited.

Tax Forms

The preservation strategy for tax form records within the ROS system is driven more by procedural considerations than anything else. Revenue intends offering seven years of history to users via the ROS Customer Information Service. The reasoning behind this action is procedural rather than legal, as Revenue does not regard the *Companies Act* as applicable to the retention of these records.

Preservation of tax form records is also, to a degree, driven by archival considerations. In fact, the long-term preservation of tax records is not appropriate given the level of personal information within the forms and their lack of suitability for archival purposes. It should be noted, however, that under Irish archival legislation, Revenue, when they elect to destroy these and other records will require authorization from the National Archives.

Debit Instruction Forms

As 19.

20. To what extent do policies, procedures, and standards currently control records creation, maintenance, preservation and use in the context of the creator's activity? Do these policies, procedures, and standards need to be modified or augmented?

Pre-existing paper form 'standards' have influenced the design of electronic forms. In fact, many of the forms in ROS are designed to emulate closely the environment of the paper-based forms including 'white space' emulation whereby forms are intuitive and allow for expressions of doubt to be inputted. Such expressions trigger an activity at the back-end systems and create an activity item for Revenue staff.

ROS is continually modifying its records management policies, procedures and standards in an effort to increase the amount of routine data that are processed automatically with little or no human intervention. In addition to freeing employees to perform more meaningful tasks, these efforts should help improve record reliability and accuracy by reducing the overall incidences of data input errors and omissions stemming from human input.

All personal data entered into ROS forms are held in accordance with Revenue's privacy policy and FOI and cannot be forwarded or disclosed to a third party.

ROS adheres to international Web standards affecting various content design and usability factors. These standards include *World Wide Web – Content Standard*, and *W3C (World Wide Web Consortium) Website Content Accessibility Guidelines*. ROS also provides a comprehensive range of services to individuals with special needs, including, for example, a Screen Reader compatible version of ROS to enable the visually impaired to use the system.

Digital Certificates and Signatures

There are very specific policies, procedures and standards currently controlling creation, maintenance, preservation and use of Keys and Certificates. These are addressed in considerable detail in two Revenue documents: the *ROS Certificate Policy Statement* (CP) and the *Certification Practice Statement* (CPS).

As stated in the CPS, this document provides factual information that describes the:

- Practices employed within the Revenue PKI to support the use of certificates issued by the Revenue CA; and
- Attendant use of technologies and processes to support the underlying operational infrastructure.

Together with the technologies and processes referred to in other Revenue documents (e.g., ROS CP, Revenue PKI Configuration Baseline), the practices described in the CPS "illustrate the trustworthiness and integrity of Revenue PKI's operations from Certificate generation and signing to expiry."[64]

In contrast, the information provided in the ROS CP is intended to:

- Inform recipients of certificates issued by the ROS CA of their rights and obligations; and
- Set out how the ROS CA discharges its obligations to those persons by describing the policies used by ROS CA to ensure the security and integrity of the ROS CA's operations and the certificates under its control.

As noted in the ROS CP, the information is provided "in accordance with the general provisions of the Irish Government's policy and guidelines on the protection of information and information technology environments."[65]

All Revenue and ROS certificate operations comply with documented internal security policies and practices, as well as published and internal privacy policies and practices, including the *Data Protection Act 1998*. From a technological perspective, all certificate operations comply with appropriate international recognized PKI conventions and standards.

[64] Ibid., p. 11.

[65] Office of the Revenue Commissioners Ireland (2000). "Revenue Online Service Certificate Policy Statement," p. 9.

21. What legal, moral (e.g., control over artistic expression) or ethical obligations, concerns or issues exist regarding the creation, maintenance, preservation and use of the records in the context of the creator's activity?

Legal Obligations

As stated in the Revenue Customer Service Charter, "[t]he effective and fair administration of tax and customs law requires Revenue and citizens to recognise certain basic rights and responsibilities."[66] These mutual expectations are detailed in the Customer Charter. In addition to the mutual Revenue <---> Taxpayer expectations outlined in the Customer Charter, there are a number of legislative conveyances that impact directly on Revenue's records creation, maintenance, preservation and use activities, including:

- *Data Protection Act 1988*
- *Official Secrets Act 1963* (esp., Revenue Certification Practice Statement - Section 1.1.9 Staffing Arrangements invokes the OSA in terms of Revenue employees)
- *Freedom of Information Act 1997*
- *E-Commerce Act 2000*
- *Taxes Consolidation Act 1997*
- *Official Languages Act 2004*

Moral Obligations

None identified.

Ethical Obligations

A number of ethical obligations are identified in Revenue's *Customer Service Action Plan*[67] and *Customer Service Standards*[68] documents. Some key obligations with the potential to impact directly or indirectly on Revenue's records creation, maintenance, preservation and use activities, include:

- Monitoring technical developments and providing users with integrated online access to the full range of public services offered by Revenue via its Web site.
- Ensuring compliance with Revenue PKI Policy and Practice documents.
- Treating all tax returns, electronic or paper, with similar weight and chance of audit.
- Adhering to specified efficiency standards for processing submissions via ROS.[69]
- Promoting official languages equality by providing services through Irish, English and/or bilingually.
- Facilitating access to ROS services for persons with disabilities and others with special needs.

[66] See: http://www.revenue.ie/aboutus/charter.htm. Also available in PDF format at http://www.revenue.ie/pdf/charter.pdf.
[67] Available at http://www.revenue.ie/pdf/cs_action.pdf.
[68] Available at http://www.revenue.ie/aboutus/standards.htm.
[69] Currently, these standards include the processing of returns, declarations and applications filed through ROS within five working days, and the processing of claims within five working days (subject to security checks) (See: Customer Service Standards at http://www.revenue.ie/aboutus/standards.htm).

22. What descriptive or other metadata schema or standards are currently being used in the creation, maintenance, use and preservation of the recordkeeping system or environment being studied?

Twenty-two schemas for the tax forms available via ROS are publicly available in XML DTDs for inclusion in ROS-compatible software developed by third parties.[70] Each schema includes a DTD and element definitions and explanations. An extract from a schema is available in Appendix 4. Although an Irish Public Service Metadata Standard exists,[71] it is not used with ROS.[72]

23. What is the source of these descriptive or other metadata schema or standards (institutional convention, professional body, international standard, individual practice, etc.?)?

From an administrative perspective, form design and structure is based largely on established institutional practice (i.e., on existing paper-based forms). From an operational perspective, form element selection and management are, in large measure, based on data flow and format requirements of the ITP and related back-end systems applications. Also, it is noted that the XML schemas used may include other descriptive standards, such as the ISO Year Standard.

E. Narrative Answers to Applicable Domain and Cross-domain Research Questions

Given that the scope of the ROS application is the creation and maintenance of electronic records, most attention will be given to Domain 1 Research questions and, where possible, Domain 2 and 3 will be addressed.

Please note: questions that were not relevant to the case study or for which no answer could be given are not listed here.

Domain 1 Research Questions (Record Creation)

1.1 (a) What types of documents are traditionally made or received and set aside (that is, created) in the course of artistic, scientific, and governmental activities that are expected to be carried out online?

ROS is an e-government application used to file and return tax forms and pay commensurate tax liabilities. The case study identified three main groups of electronic records being created by ROS: Digital Certificates, Tax Forms, and Debit Instruction Forms. Additional documents include the Web pages, database entries, PDF versions of forms and generic e-mails.

[70] See http://www.ros.ie/PublisherServlet/downloads.

[71] See http://www.gov.ie/webstandards/metastandards/index.html.

[72] In fact, a search on the word ‘metadata’ via the Revenue Web site search function returns zero hits.

(b) For what purposes?

The records are created by Revenue primarily to facilitate compliance with Irish and European tax legislation, and, secondarily, to facilitate efficient and effective user interaction with the ROS system.

(c) What types of electronic documents are currently being created to accomplish those same activities?

Digital certificates, generic e-mails, Adobe Acrobat PDF files, EDI (Electronic Data Interchange) financial interchange files.

(d) Have the purposes for which these documents are created changed?

No. However, it is noted that Revenue's requirement for a secure system dictated the use of PKI as an additional element.

1.2 (a) What are the nature and the characteristics of the traditional process of document creation in each activity?

Document creation occurs in a controlled environment, access to which is regulated using PKI. The tax forms are designed to visually replicate analogue paper-based forms. Debit Instruction Forms replace the use of cheques or the analogue provision of credit or debit card details.

(b) Have they been altered by the use of digital technology and, if yes, how?

While the look and feel of traditional paper-based forms are retained in the electronic versions, the electronic forms include additional functionality not present in traditional paper-based, such as the use of automated pre-population and validation to improve efficiency and minimize data entry errors. In addition, all forms can be downloaded in PDF format and printed off for hard copy filing, if preferred.

1.3 (a) What are the formal elements and attributes of the documents generated by these processes in both a traditional and a digital environment?

The formal elements and attributes of the documents generated in the digital environment are discussed in Question 4a, above. The only traditional (i.e., paper-based) documents routinely generated through interaction with the ROS system are the separate letter post mailings of a user's RAN and ROS System Password, both of which are required to facilitate access to the secure ROS environment. In addition, users have the option of downloading most of the forms in PDF format and printing them off for hard copy filing, if preferred.

In the digital environment, the overall appearance of many of the electronic forms mirrors analogous traditional paper-based forms. The security environment created and maintained by PKI and digital certificates is analogous to a person using his/her PPS Number and handwritten signature. The elements and attributes included in RDI and Electronic Payment forms are modelled on traditional financial transaction forms, such as cheques and direct debit instructions.

(b) What is the function of each element and the significance of each attribute?

See Question 4a, above.

(c) Specifically, what is the manifestation of authorship in the records of each activity and its implications for the exercise of intellectual property rights and the attribution of responsibilities?

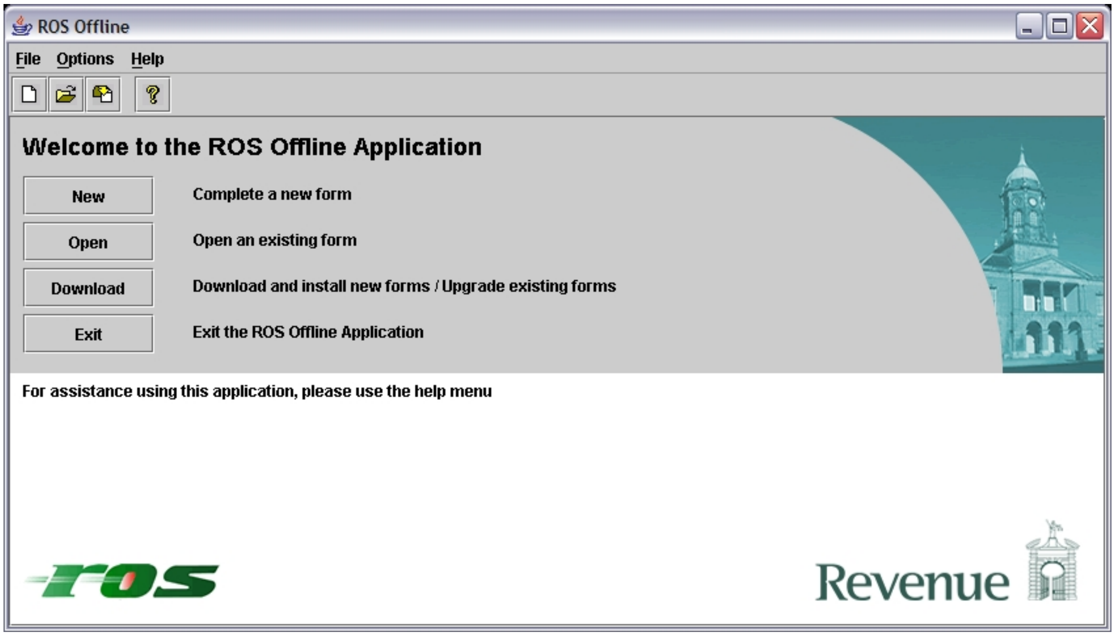
Authorship, which for this case study is understood to apply to the digital entities generated either online or offline and submitted electronically to Revenue via the ROS application, is manifested visually online through the use of: (1) the Revenue logo in the header section of each ROS Web page, (2) the ROS physical address information in the footer section of each ROS Web page, and (3) the www.ros.ie domain in all ROS Web page URLs (see Figure 23 for an example of an ROS Web page illustrating all three authorship elements). As shown in Figures 24 and 25, authorship is manifested in the ROS Offline Application through the use of the Revenue and ROS logos on the initial 'Welcome' menu screen, and through the use of the Revenue logo on all subsequent form screens. While the author[73] for each of the three classes of digital entities examined in this case study is the Revenue Commissioners for the Irish state, it is noted that the tax and debit instruction forms are filled out and completed by an individual or his/her agent and there is a level of personal responsibility in maintaining tax compliance that is attached to process of providing complete and accurate information on all forms submitted to Revenue via ROS.

1.4 (a) Does the definition of a record adopted by InterPARES 1 apply to all or part of the documents generated by these processes?

The InterPARES 1 Glossary defines "record" as "a document made or received and set aside in the course of a practical activity." This definition does apply to the three main classes of documents identified as originating from within ROS (i.e., digital certificates, completed and signed tax forms, and (corresponding) debit instruction forms).

That said, it is important to note, however, that although the electronic tax forms mirror the paper forms in look and feel, their evidential weight is dependant upon supporting documentation and technology (PKI and user set up and authorization). Revenue maintains that its ROS system offers and supports a chain of authenticity. In essence, ROS is seen as facilitating a service in the electronic environment by utilizing technology to minimize errors and enhance traditional Revenue services, rather than to radically alter or transform these same services.

[73] Author is used in this context in a diplomatic sense to refer specifically to the physical or juridical person having the authority and capacity to issue the record or in whose name or by whose command the record has been issued.



Welcome to the ROS Offline Application

New — Complete a new form

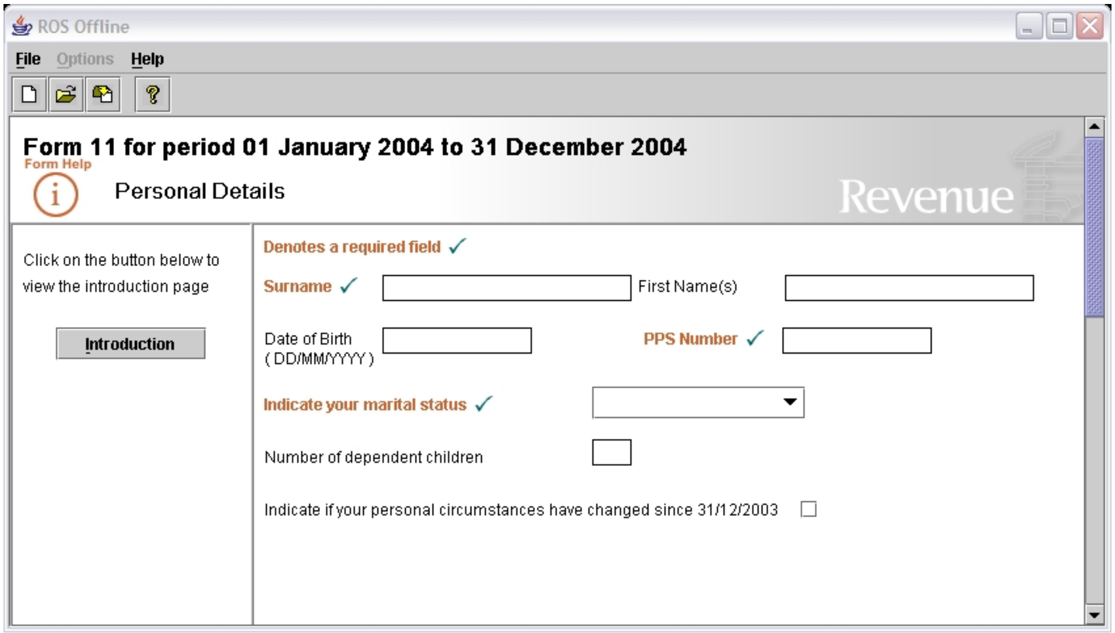
Open — Open an existing form

Download — Download and install new forms / Upgrade existing forms

Exit — Exit the ROS Offline Application

For assistance using this application, please use the help menu

Figure 24. ROS Offline Application 'Welcome' menu screen showing use of Revenue and ROS logos



Form 11 for period 01 January 2004 to 31 December 2004

Personal Details

Click on the button below to view the introduction page

Denotes a required field ✓

Surname ✓ First Name(s)

Date of Birth (DD/MM/YYYY) PPS Number ✓

Indicate your marital status ✓

Number of dependent children

Indicate if your personal circumstances have changed since 31/12/2003 □

Figure 25. ROS Offline Application Form 11 'Personal Details' screen showing use of Revenue logo

(b) If yes, given the different manifestations of the record's nature in such documents, how do we recognize and demonstrate the necessary components that the definition identifies?

Some components are common to both electronic and analogue records, but others, such as the PKI environment and the use of EDI elements for debit instruction forms, are particular to the electronic environment. More details are required to articulate the formal components.

(c) If not, is it possible to change the definition maintaining theoretical consistency in the identification of documents as records across the spectrum of human activities?

Not applicable.

(d) In other words, should we be looking at other factors that make of a document a record than those that diplomatics and archival science have considered so far?

ROS closely emulates paper-based forms and, as such, uses the paper-based form as the basis of the electronic record and offers, in effect, an electronic paper form. The main innovation offered by ROS is form management and ease of access and viewing, and the security functionalities supported by PKI.

1.5 As government and businesses deliver services electronically and enter into transactions based on more dynamic Web-based presentations and exchanges of information, are they neglecting to capture adequate documentary evidence of the occurrence of these transactions?

While ROS does capture documentary evidence, Revenue has not, as yet, articulated a process of ensuring the adequate medium-to-long-term preservation of this data. Revenue regards ROS as a means to provide for and present a 'snapshot' into the main ITP back-end tax processing system. This 'snapshot' is only a subset of the main database and does not immediately affect the contents of the ITP.

1.6 Is the move to more dynamic and open-ended exchanges of information blurring the responsibilities and altering the legal liabilities of the participants in electronic transactions?

Not as yet. ROS functions as both an intermediary and a buffer application blocking and controlling data access and data flow to the main Revenue back-end systems. If, in the future, more direct access is given to these systems by Revenue, greater control and recordkeeping will be required.

1.7 (a) How do records creators traditionally determine the retention of their records and implement this determination in the context of each activity?

Revenue has not articulated a strategy for the retention of records within and from ROS. ROS only maintains a subset of the main body of records. Presumably, the *National Archives Act* is consulted regarding the identification of archival documents and to provide guidance for establishing and agreeing upon retention periods and disposal arrangements. (Note, however, that the *National Archives Act* does not, itself, prescribe retention periods in relation to records.)

(b) How do record retention decisions and practices differ for individual and institutional creators?

ROS will only hold records of active users or agents. While ROS retains a copy of an active user's submissions and transactions in the user's ROS Inbox, it is unclear if there are limits to how long these records will be retained here. Users do not have the option of directly modifying or deleting these records.

(c) How has the use of digital technology affected their decisions and practices?

Digital technology has reduced errors by enabling pre-population of forms and a degree of real-time, automated data entry validation. It has also facilitated the retention and instantaneous distribution of copies and, via PKI technology, facilitated remote user authentication and secure transfer of completed forms.

Domain 2 Research Questions (Concepts of Authenticity, Accuracy, Reliability)

2.1 (a) What does record reliability mean in the context of artistic, scientific and government activities?

Record reliability, which is established by examining the completeness of a record's form and the amount of control exercised on the process of its creation, is, for the most part, conferred here by the use of PKI to control access to the system and by the use of automated validation routines built into the ROS form templates to: (1) ensure standardization of the forms presented to users, (2) prevent users, to a certain degree, from saving and/or submitting forms with invalid data, and (3) prevent users from submitting incomplete forms.

(b) To what extent can the electronic records created in the course of each type of activity be considered reliable and why?

Record reliability, which is established by examining the completeness of a record's form and the amount of control exercised on the process of its creation, is, for the most part, conferred on the records created in the ROS system by the use of PKI to control access to the system and by the use of automated validation routines built into the ROS form templates to: (1) ensure standardization of the forms presented to users, (2) prevent users, to a certain degree, from saving and/or submitting forms with invalid data, and (3) prevent users from submitting incomplete forms.

ROS is a system designed for tax collection. It facilitates the filing and uploading of tax returns and the electronic payment of associated monies. The nature of this business activity suggests that users will attempt to minimize their tax liability by avoiding penalties and will, therefore, seek to comply with all parts of the transaction process. There are legal and financial implications to misfiling a tax return or by not declaring all taxable income, which provide further incentive to users to ensure that the documents they submit are reliable and that the data those documents contain are accurate (Revenue has made a claim that the use of ROS does not increase nor decrease the likelihood of a tax audit being undertaken).

(c) What requirements on their form and controls on their creation would make us presume that they are reliable?

See previous question. In addition, it is emphasized that only Approved and Authorized Persons can access the secure section of ROS and submit documents. To this end, ROS incorporates an Access Control System based on user log-ins, passwords, profiles, permissions and a valid digital certificate.

2.2 (a) What does record accuracy mean in the context of each activity?

Accuracy is defined by the InterPARES 2 Glossary as:

> The degree to which data, information, documents or records are precise, correct, truthful, free of error or distortion, or pertinent to the matter.[74]

Within ROS, the concept of record accuracy refers to both the accuracy of the submitted records and the accuracy of the presented records (e.g., the PDF format copies of submitted records that are retained in a user's ROS Inbox). ROS cannot guarantee that submitted documents are accurate, as individuals or agents may submit incorrect details. The application, however, does attempt to minimize inaccuracies by incorporating a certain number of business rules and logic to check calculations prior to saving and/or submitting documents. Any inaccuracies that escape detection by the built-in validation routines, and which are subsequently identified by the taxpayer or the ITP system during processing require direct human intervention by Revenue staff to correct..

(b) To what extent can the electronic records created in the course of each type of activity be considered accurate and why?

Revenue incorporates a degree of pre-population and validation within ROS to maximize accuracy but for the most part, control of data accuracy is dependent upon the user inputting the data. Once submitted, the ability to query an inaccurate entry in a form and/or appeal a decision based on inaccurate information in a form requires human intervention and direct contact with a Revenue employee.

(c) What controls on their creation would make us presume that these records are accurate?

In one sense, ROS is a system designed to help facilitate compliance with tax obligations. To this end, it facilitates the filing and uploading of tax returns and the electronic payment of

[74] Accessed 12/08/04

associated tax liabilities. The nature of this business activity suggests that users will attempt to minimize their tax liability by avoiding penalties and will, therefore, seek to comply with all parts of the transaction process, including providing accurate information. There are legal and financial implications to misfiling a tax return or by not declaring all taxable income, which provide further incentive to users to ensure that the documents they submit are reliable and that the data those documents contain are accurate. Further incentives for submitting accurate documents are provided by the Revenue Charter of Rights, which, among other things, establishes:

1. A ‘presumption of honesty,’ whereby taxpayers are presumed by Revenue to have dealt with their “tax affairs honestly unless there is reason to believe to the contrary;” and
2. That “Revenue staff are entitled to expect that [taxpayers] will give them all the facts” they need to ensure that “every reasonable effort [can] be made to give [taxpayers] access to full, accurate and timely information about Revenue law and [the taxpayers’] entitlements and obligations under it.”

To some extent, the use of a PKI to restrict and control access to ROS and its document submission functions may indirectly impact the accuracy of the records by ensuring that the documents (and, hence, the data entered in those documents) are only submitted by those persons authorized or approved to do so.

2.3 (a) What does authenticity mean in the context of each activity?

As defined in the glossary to its *Certificate Policy Statement*, ROS defines “authenticity” as “[t]he property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.” It further defines “authentication” as “[t]he provision of assurance of the claimed identity of an entity.”[75] ROS presumes authenticity of received, signed and submitted tax forms from authorised users. Moreover, the E-Commerce Act 2000 confers the same evidential weight on an electronic transaction as that of a paper based one.

(b) To what extent is the definition of record authenticity adopted by InterPARES 1 relevant to the records resulting from each type of activity and from the use of increasingly complex digital technology?

InterPARES 1 defines authenticity as “[t]he quality of being authentic, or entitled to acceptance. As being authoritative or duly authorized, as being what it professes in origin or authorship, as being genuine.”[76] The researcher found no reason to question this definition with respect to the records created in the ROS system. Regardless of Revenue’s claims that ROS functions as a dynamic system, it was found that ROS is highly controlled and only confers evidential weight and authenticity on records at the moment of fixity (i.e., signing and submitting).

[75] Office of the Revenue Commissioners Ireland (2000). “Appendix D – Glossary: Revenue Online Service Certificate Policy Statement,” p. 46.

[76] InterPARES 1 Book Part 1- line 41.

2.4 (a) On what basis can the records created in the course of each activity be presumed authentic?

The InterPARES 2 Glossary defines "presumption of authenticity" as "[a]n inference as to the fact of a record's authenticity that is drawn from known facts about the manner in which that record has been created and maintained"[77]

On the one hand, ROS presumes, by virtue of the identification and authentication security provided by the Revenue PKI, the authenticity of the digitally signed documents it receives from Approved and Authorised Persons. However, whilst ROS is a secure record-creating environment, it is unclear if it is an authentic recordkeeping environment. Moreover, while Revenue presumes a chain of authenticity based on password-protected user log-ins, digital certificates and PKI, the researcher would require further information about ITP and other systems to asses them for their full impact on the creation an maintenance of record authenticity. It has been presumed in this case study that the repository with the most evidential weight is the ITP system.

(b) How, in the absence of such presumption, can their authenticity be verified?

The nature of the system suggests that they cannot. Revenue may argue that its continued custody confers authenticity on the electronic records contained within its back-end systems.

2.5 (a) How is the authenticity of these records affected by their transmission across space and time?

The Revenue PKI confers authenticity across space. Revenue retains the 'security wrapper' to confer authenticity and non-repudiation over time. More research is required into the longer term implications of this approach as measured by the number of claims against the ROS application, etc. There is no defined policy regarding the retention and management of these security wrappers. It would appear that Revenue is retaining these 'wrappers' as security against a future claim of wrongful repudiation and it is suggested that the wrappers offer evidence of submitted records. ROS requires the formal 'sign and submit' activity as both a procedural and technical process to confer diplomatic authenticity on the submitted transaction.

(b) What controls on the process of transmission would ensure that these records will continue to be recognised as authentic?

Controls are required at the point of reception rather than transmission to ensure that continued authenticity will be recognized. The Revenue PKI facilitates the transmission of authentic data into ROS but cannot be used to continue to confer authenticity. Internal controls and procedures illustrating the mechanisms by which data elements are removed from the security wrapper, ingested into ROS, and processed should be articulated and maintained.

[77] Accessed 12/08/04.

2.6 Are the conceptual requirements for reliability and authenticity developed by the UBC-MAS project [Duranti and MacNeil, 1999] and InterPARES 1 for administrative and legal records generated within databases and document management systems applicable to the records studied by InterPARES 2?

The researcher understands this question to relate to the electronic records contained in ITP and back-end systems, which are outside the scope of this research study. Nevertheless, it seems likely that the cited conceptual requirements for reliability and authenticity are indeed applicable to the records kept in Revenue's ITP and related back-end database systems.

2.7 (a) Do the participants in electronic transactions have shared access to reliable and accurate information about the terms and effects of the transactions?

Participants must sign up for a digital certificate accepting Revenue's terms and conditions. If the ROS Access Controls are set accordingly, it is possible for several people (agents, etc.) to view the same records. As part of a common ROS Web site template, the ROS Terms and Conditions are readily available for viewing via a hyperlink in the footer section on each ROS Web page.

(b) What would constitute reliable and accurate records of transactions in current electronic service delivery initiatives?

Reliable and accurate transaction records would include audit logs, and (certified) copies saved in ROS user Inboxes.

2.8 What would be the consequence of issuing guidelines for record creation on the nature of the records of each activity?

The core issues to be addressed for ROS and other e-government-type applications are: integrity of submitted data, security of delivery, user authentication, and authority of the creating agency.

Each activity creates records in very controlled environments. Guidelines would only serve to assist new users in learning how to use the system. A more intuitive software program might assist with personalization and user-definable preferences to minimize clutter and irrelevant data. This would require further developments in such areas as internal software business logic, integration of user-centred design principles, and greater agreement amongst agencies.

2.9 How can cultural differences, freedom of expression, freedom of inquiry, and right to privacy be reflected in those guidelines?

Not applicable.

2.10 What technological and intellectual tools would assist creators to generate records that can be authentically preserved over time?

Presumption of authenticity requires controls at points of transmission, reception and maintenance. Diplomatic tools are required to seal or fix the record at these points and create and maintain additional metadata supporting these actions.

ROS developers are continually releasing new XML DTDs for new tax forms or updating and improving existing ones. It is incumbent upon individuals or agents to download the latest versions of available forms. It is unclear if later ROS releases are technically backward-compatible such that the application will accept earlier versions of forms.[78] This also raises questions of authenticity and accuracy.

2.11 What legal or moral obligations exist regarding the creation, use and preservation of the records under investigation?

There are no moral obligations but Revenue and Irish and European citizens availing of the service must comply with a series of legislative obligations (see Section D, Question 21, above).

It is interesting to note that while other European countries have offered financial or other incentives to encourage citizens to switch to using online services, the Irish civil service has not, as yet, availed of such measures.

Domain 3 Research Questions (Appraisal and Preservation)

3.1 How do the appraisal concepts, methods and models developed by InterPARES 1 for the administrative and legal records created in databases and document management systems apply to the appraisal of the records of artistic, scientific and government activities resulting from the use of the technology examined by InterPARES 2?

There is no appraisal of records within ROS. Appraisal within ITP appears to distinguish between active and inactive records but there are no outlined procedures governing these actions. It would appear that this is conducted on a case-by-case basis, taking into account the nature of the tax relationship between each individual taxpayer and Revenue.

3.2 How do the preservation concepts, methods and models developed by InterPARES 1 for the administrative and legal records created in databases and document management systems apply to the preservation of the records of artistic, scientific, and government activities resulting from the use of the technologies examined by InterPARES 2?

All records created by Revenue are subject to the terms and conditions of the *National Archives Act*. However, no dedicated, formal appraisal has been made of ITP and other back-end systems. Revenue has, as yet, not instituted a retention policy for records in ITP, for which ROS is a subset.

In this light, it is difficult to answer questions about preservation policies. The issue of preservation and migration was raised as part of the interview process (See Question 19, above).

[78] However, the true consequence of this may be moot since it appears that users are required to always use the most current version of the application (at least as far as the online version is concerned), and thus do not have the option of choosing to use earlier versions of forms. As well, all earlier versions of forms that users have already submitted, and which they subsequently may wish to access, have been converted to PDF format. It is conceivable that access to these PDF forms may be compromised by future changes to the Adobe Reader application. As for the ROS Offline Application, users are reminded to periodically check for, and download, the latest versions of the available forms. When doing so, users are presented with a choice of forms to download (arranged by tax type and year). Presumably, if a form is included in the list of available choices, the application will be able to open it.

3.3 (a) What preservation paradigms can be applied across activities and technologies?

Whatever preservation paradigm is suggested, it should include or incorporate a comprehensive response to the issue of digital signatures and future claims of authenticity arising from such technology.

Policy Cross-domain Research Questions

4.1 (a) To what extent do policies, procedures, and standards currently control records creation, maintenance, preservation and use in each focus area?

The main policy issue affecting ROS is the enthusiastic push by Revenue for a larger number of users. Incentives were offered to self-employed individuals to use ROS instead of making a paper-based tax return.

Another policy issue that could, in the near future, impact records management activities includes the potential use of the Revenue PKI as part of the Irish Public Service Broker (PSB) being built by the Reach Agency, which acts as the centralized electronic gateway for all Government services (Figure 26).[79] This has implications for privacy and authenticity. It is interesting to note that the recent push by the Irish government to roll out electronic voting machines was impeded by software faults and the absence of a verifiable paper-receipt-based audit trail.

For further discussion of the Revenue and ROS procedures and standards impacting records management activities, see Questions 5a, 8, 10, 16, 18, and 20, above, and Appendix 2, below.

(b) Do these policies, procedures, and standards need to be modified or augmented?

The most obvious deficiency in the current system is the lack of formal appraisal and retention policies, especially with respect to the subset of ITP records and the security wrappers held in the ROS system. Also, should the Revenue PKI be expanded to serve as the exclusive PKI environment for e-government transactions and businesses, as part of the Reach Agency’s Irish PSB, it is likely that the current policies, procedures and standards will need to be modified.

4.2 Can an intellectual framework or frameworks be developed to facilitate the translation of policies, procedures, and standards into different national environments, sectors, and domains?

The current framework is based on the development of the Irish PSB. However, it is uncertain if this will be facilitated by the Revenue PKI.

[79] Office of the Revenue Commissioners Ireland (2004). “Request for Tender (RFT): IT Solution to Meet Customs Administration and Enforcement Requirements,” p. 8. Available at: http://www.revenue.ie/aboutus/procurement/rft.doc. For further information on the Reach Agency, see http://www.reach.ie.

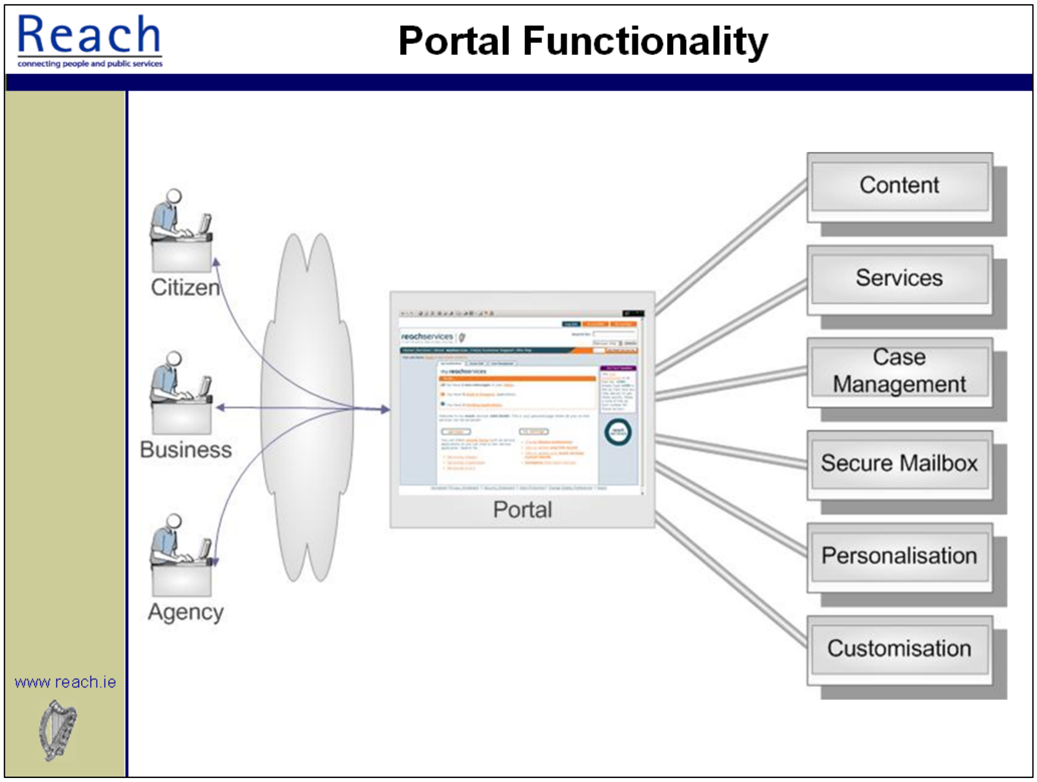


Figure 26. Schematic of proposed Irish Public Service Broker (PSB)

4.3 How can enhanced control over and standardisation of records creation, maintenance, preservation, access and use be balanced against cultural and juridical differences and perspectives on issues such as freedom of expression, moral rights, privacy, and national security?

Identity, security and privacy are key issues for ROS and Revenue, and in a wider context, the Irish public service (see Question 20, above).

As noted above, the Reach Agency is currently developing the Irish PSB and is articulating an Integrated Identity Management & Access Control System (IDMACS).

Reach describes the IDMACS as follows:[80]

1. Access to services and data will be controlled by IDMACS
2. Registered customers access their own PSB “accounts” by username and password
3. Public service agencies set their own access rules
4. Access rules are managed and applied by the IDMACS
5. Four levels of identity assertion

[80] Reach (2004). “Public Services Broker (PSB): Update on Progress,” 22 July 2004 PowerPoint presentation, slide 27, p. 14..Available at: http://www.reach.ie/publications/downloads/July22Website.pdf.

- Level 0 – users own assertion – no proof of identity – available end October
- Level 1 – Validated against PSI – “on the balance of probability” – available end November
- Level 2 – additional proofs “Substantial level of assurance” – work with agencies for delivery in 2005
- Level 3 – very substantial proofs – “Beyond reasonable doubt” – need to establish business case

The legislative obligations come from taxation legislation, specifically the *Finance Act 1999*, allowing for the introduction of electronic filing and tax returns, and the *E-commerce Act 2000*, in which Revenue contributed the sections dealing with strong encryption.

Unlike other e-government initiatives, ROS is not aimed at the e-citizen. The main focus has been on self-employed and business taxpayers who generate a large number of returns over the financial year.

4.5 (a) What principles should guide the formulation of policies, strategies and standards related to the creation of reliable, accurate and authentic records in the digital environments under investigation?

The need for policies to be government-wide suggests that there is a real need for information security, reliability, integrity and authenticity. ROS offers these elements in terms of records generation and transmission. Back-end systems require additional elements to ensure the electronic records remain authentic through time.

Revenue’s main warrant for developing ROS and actively encouraging its take-up is the organizational history and the body of knowledge developed and maintained through the history and practice of tax collection. This is transferred into the electronic environment, as exemplified in the creation of electronic forms mirroring analogue paper-based ones.

4.6 What principles should guide the formulation of policies, strategies and standards related to the long-term preservation of those records?

As mentioned above, there appears to be no long-term preservation plan for data in ROS/ITP.

It is noted that a search of www.balii.org did not result in any hit for ‘non-repudiation’ in the documented Irish case law. As this is the most contentious issue affecting PKI and the records environment maintained by this infrastructure, it may be appropriate to suggest that a coherent process be established for the treatment of electronic signatures and their long-term preservation, from both a legal and technical perspective.

4.7 What should be the criteria for developing national policies, strategies and standards?

Such criteria should include long-term accessibility, security of data, and maintenance of a demonstrable evidential weight to electronic records.

4.8 What should be the criteria for developing organizational policies, strategies and standards?

As Question 4.7, above.

Description Cross-domain Research Questions

6.1 What is the role of descriptive schemas and instruments in records creation, control, maintenance, appraisal, preservation, and use in traditional recordkeeping systems in the three focus areas?

No descriptive schemas were discovered in the ROS case study. XML DTDs were created for tax forms emulating the analogue versions (See Appendix 4). The forms are available for downloading at: http://www.ros.ie/app/available.html.
The DTD (Data Type Descriptors) for each form are available in XML Schema, PDF, or MS Word format at: http://www.ros.ie/PublisherServlet/downloads.

These are very detailed forms. For example, the f1103not.doc detailing the Form 11 self-assessment tax form (Version 4, for tax periods ending in 2003) for the self-employed is 59 pages in length.

6.2 (a) What is the role of descriptive schemas and instruments in records creation, control, maintenance, appraisal, preservation, and use in emerging recordkeeping systems in digital and Web-based environments in the three focus areas?

The Web components of ROS use HTML, XML, DTD, meta and alt tags. The application also requires Java and XML-compatible browsers to ensure that the schemas and forms can be viewed properly (authentically?).

(b) Do new tools need to be developed, and if so, what should they be?

It is unclear whether new tools need to be developed, but if the development of e-government services is based on interoperability issues, metadata and descriptive schemas will play an increasingly important role.[81]

[81] See, for example, the UK's e-Government Interoperability Framework, or e-GIF, at: http://www.govtalk.gov.uk/interoperability/egif.asp.

F. Bibliography and Sources

Public Key Infrastructure

PD0039, ROS Certificate Policy Statement, version 1.1, 7 April 2004.
PD0018, Revenue PKI Certification Practice Statement, version 1.1, 7 April 2004.

Revenue Commissioners

Revenue On-Line Service Privacy Policy Statement, 4 June 2003 (Note: no longer accessible, see instead 1 Feb 2005 version at: https://www.ros.ie/privacy_policy.pdf).

Irish Government

Interdepartmental IT Security Group (1999). *A Secure and Trusted Electronic Business Environment for Government* (internal report prepared for the Irish Government).

General Sources

MacNeil, Heather (2000). *Trusting records, legal, historical and diplomatic perspectives* (London: Kluwer Academic Publishers).

Web Sites

- **General**

  http://www.revenue.ie (Accessed 2004 Jun 01)

- **Policy**

  http://www.e-europeawards.org/ (Accessed 2004 Jun 01)

- **PKI**

  http://www.revenue.ie/pro_arc.htm (Accessed 2004 Aug 19) - Archive of Revenue's procurement documents.

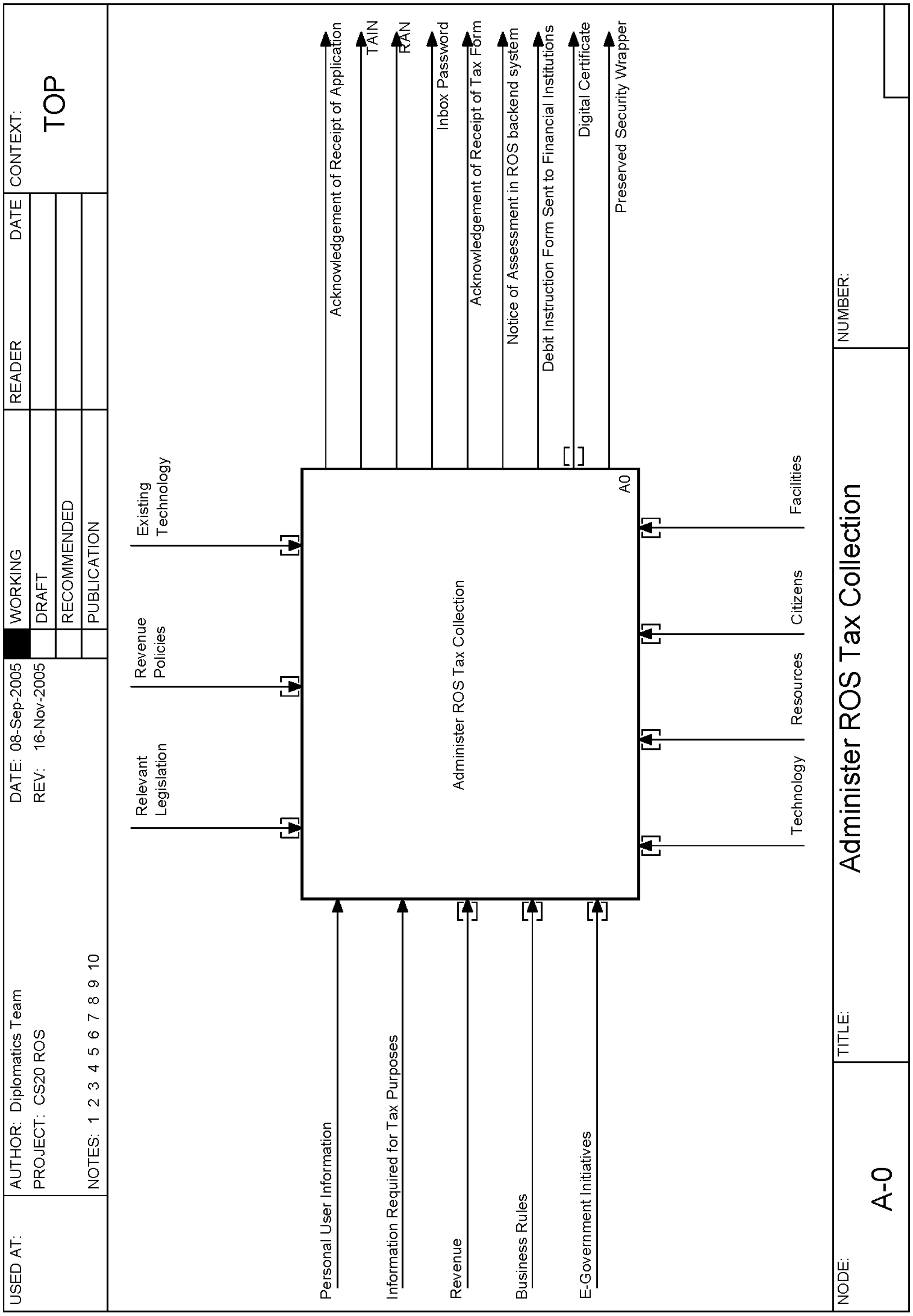
  http://www.ietf.org/rfc/rfc3647.txt (Accessed 2004 Aug 19) - Internet X509 Public Key infrastructure Certificate Policy and Certification Practices Framework.

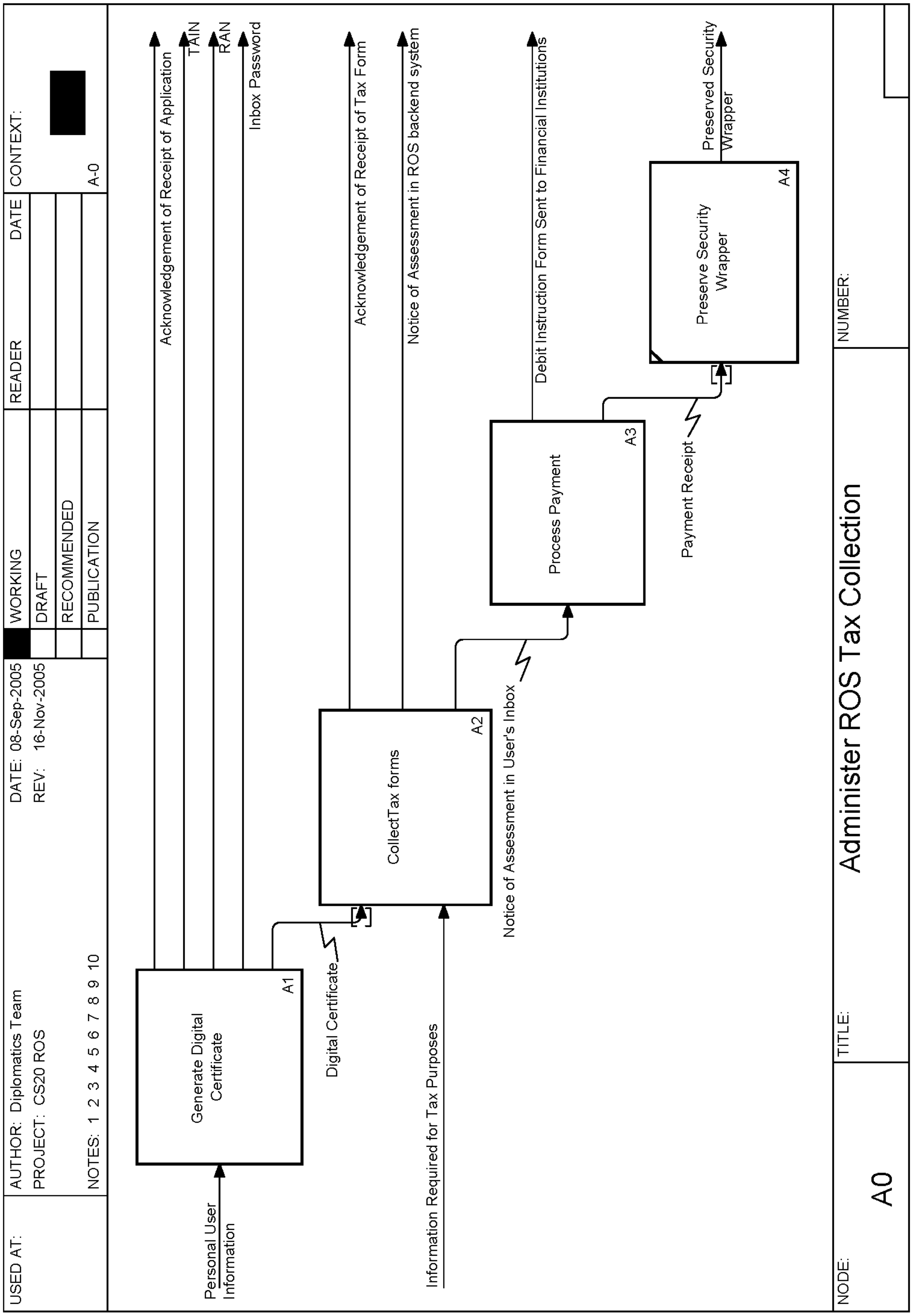
- **Legislation**

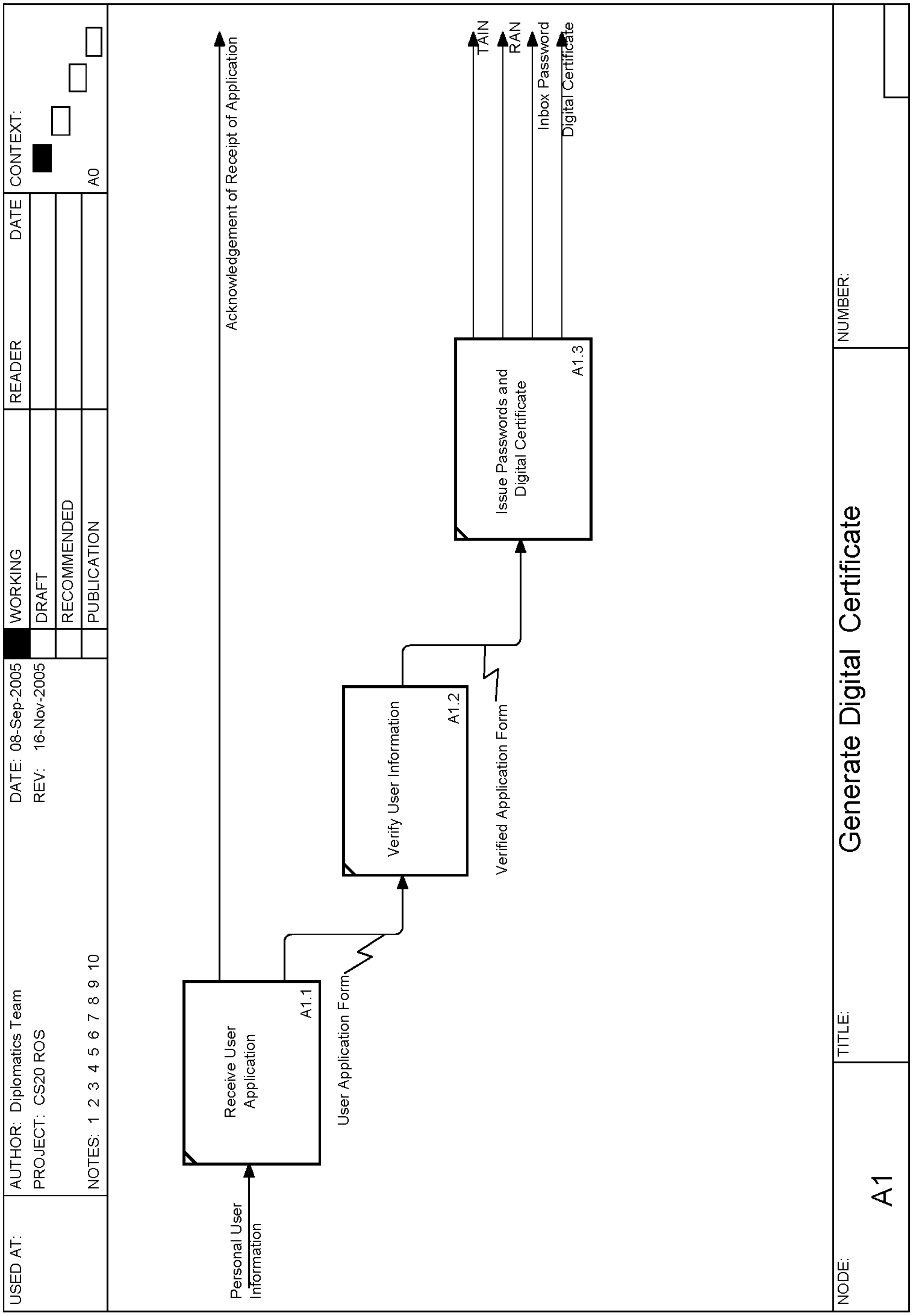
  http://www.bailii.org/ie/legis/num_act/tca1997222/s1.html - *Taxes Consolidation Act 1997* (Accessed 2004 Jun 01)

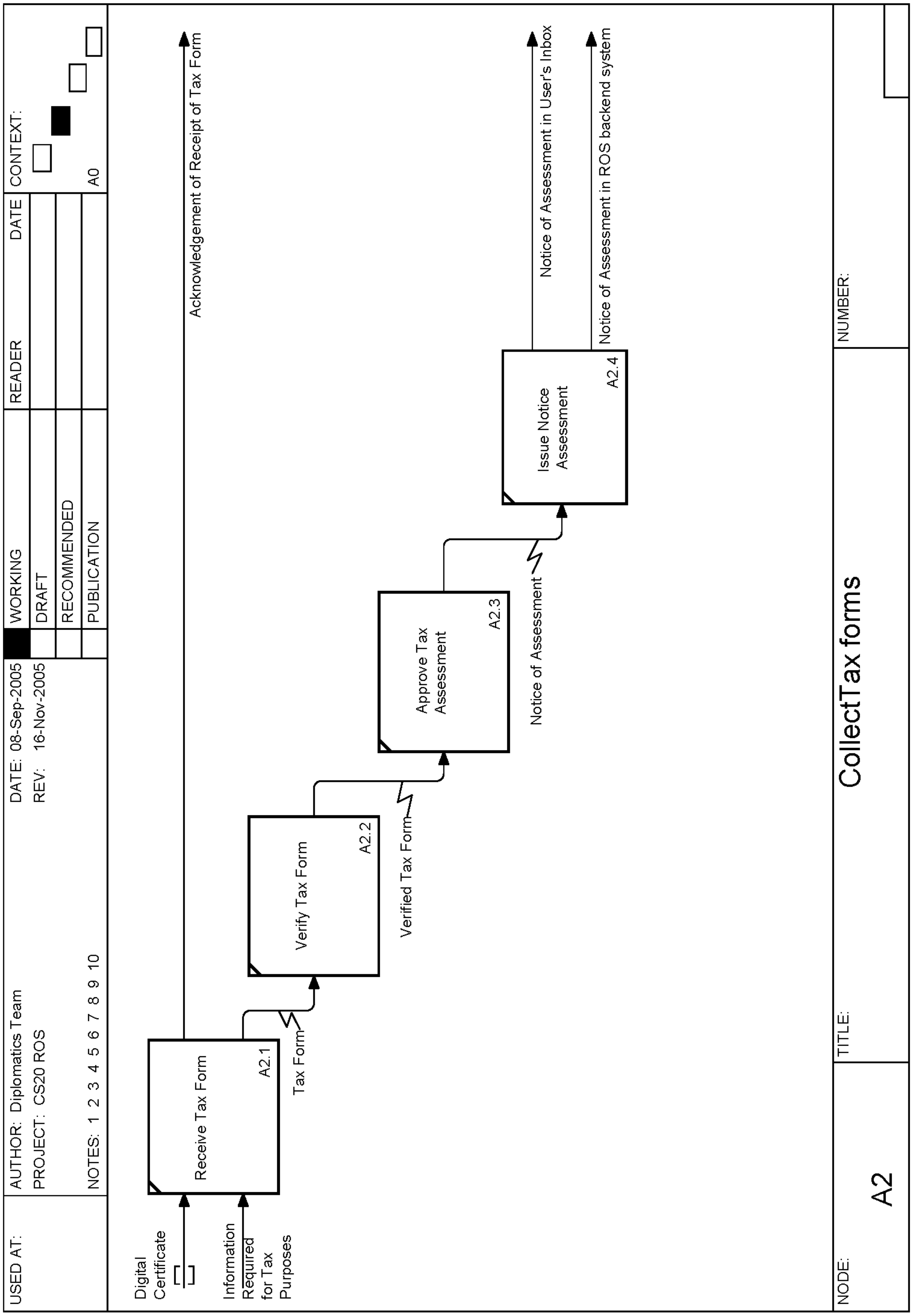
  http://www.bailii.org/ie/legis/num_act/eca2000182/s1.html - *E-Commerce Act 2000* (Accessed 2004 Jun 01)

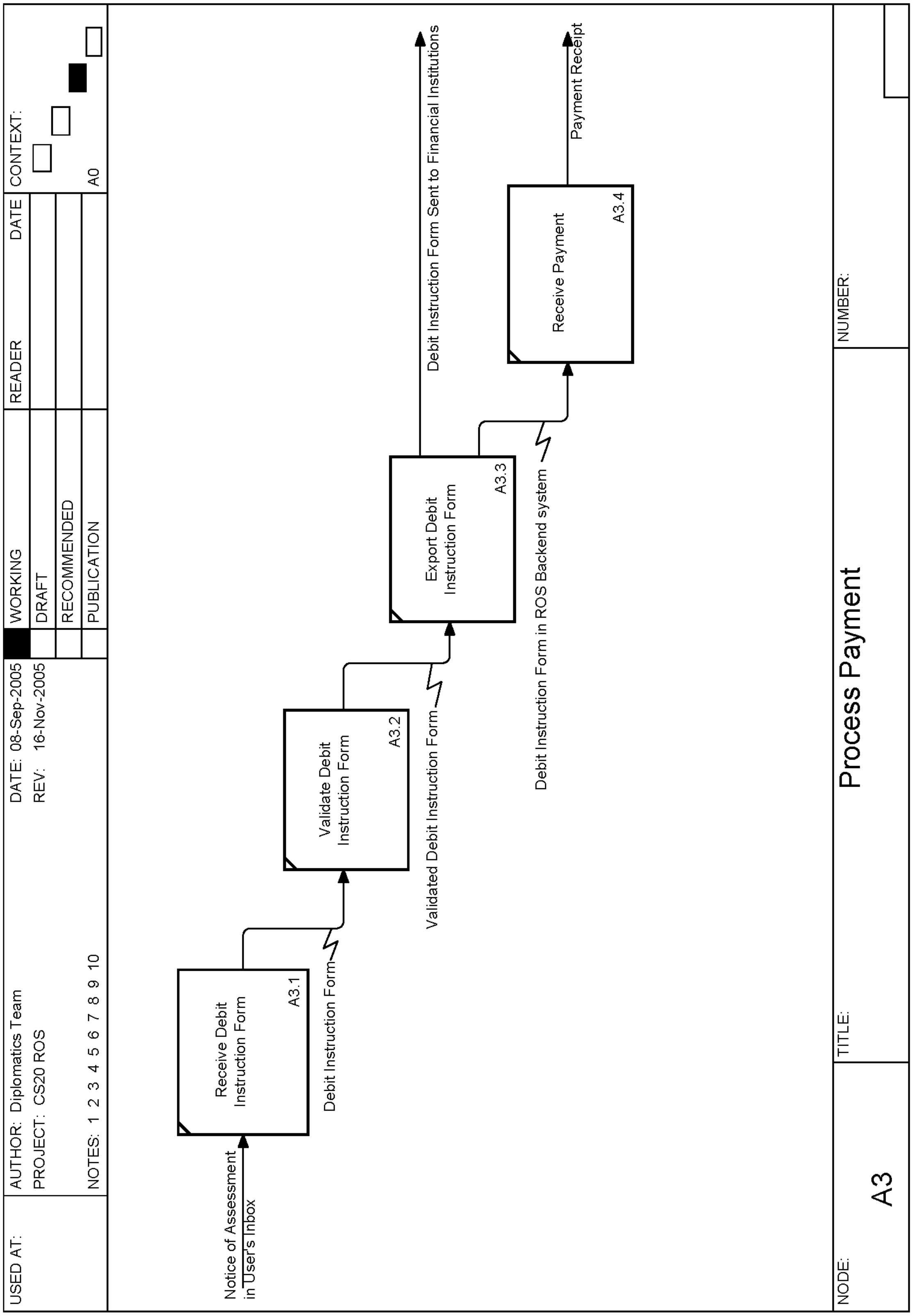
G. IDEF0 ACTIVITY MODEL

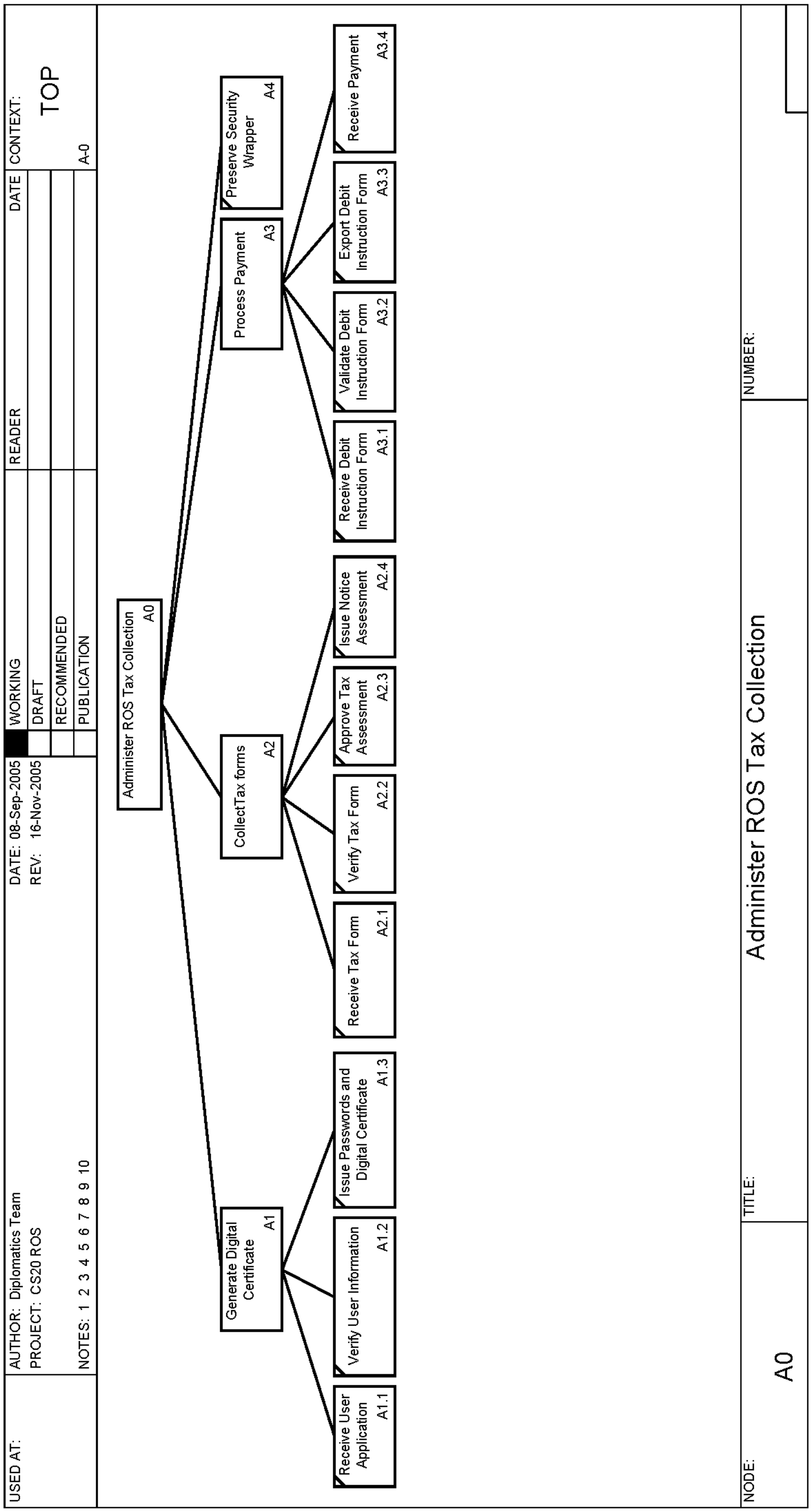

USED AT:
AUTHOR: Diplomatics Team
PROJECT: CS20 ROS
NOTES: 1 2 3 4 5 6 7 8 9 10
DATE: 08-Sep-2005
REV: 16-Nov-2005
WORKING
DRAFT
RECOMMENDED
PUBLICATION
READER
DATE
CONTEXT:
TOP
Relevant Legislation
Revenue Policies
Existing Technology
Personal User Information
Information Required for Tax Purposes
Revenue
Business Rules
E-Government Initiatives
Administer ROS Tax Collection
A0
Acknowledgement of Receipt of Application
TAIN
RAN
Inbox Password
Acknowledgement of Receipt of Tax Form
Notice of Assessment in ROS backend system
Debit Instruction Form Sent to Financial Institutions
Digital Certificate
Preserved Security Wrapper
Technology
Resources
Citizens
Facilities
NODE:
A-0
TITLE:
Administer ROS Tax Collection
NUMBER:


USED AT:
AUTHOR: Diplomatics Team
PROJECT: CS20 ROS
NOTES: 1 2 3 4 5 6 7 8 9 10
DATE: 08-Sep-2005
REV: 16-Nov-2005
WORKING
DRAFT
RECOMMENDED
PUBLICATION
READER
DATE
CONTEXT:
A-0
Personal User Information
Generate Digital Certificate
A1
Acknowledgement of Receipt of Application
TAIN
RAN
Inbox Password
Digital Certificate
Information Required for Tax Purposes
CollectTax forms
A2
Acknowledgement of Receipt of Tax Form
Notice of Assessment in ROS backend system
Notice of Assessment in User's Inbox
Process Payment
A3
Debit Instruction Form Sent to Financial Institutions
Payment Receipt
Preserve Security Wrapper
A4
Preserved Security Wrapper
NODE:
A0
TITLE:
Administer ROS Tax Collection
NUMBER:


USED AT:
AUTHOR: Diplomatics Team
PROJECT: CS20 ROS
NOTES: 1 2 3 4 5 6 7 8 9 10
DATE: 08-Sep-2005
REV: 16-Nov-2005
WORKING
DRAFT
RECOMMENDED
PUBLICATION
READER
DATE
CONTEXT:
A0
Personal User Information
Receive User Application
A1.1
User Application Form
Verify User Information
A1.2
Verified Application Form
Issue Passwords and Digital Certificate
A1.3
Acknowledgement of Receipt of Application
TAIN
RAN
Inbox Password
Digital Certificate
NODE:
A1
TITLE:
Generate Digital Certificate
NUMBER:


USED AT:
AUTHOR: Diplomatics Team
PROJECT: CS20 ROS
NOTES: 1 2 3 4 5 6 7 8 9 10
DATE: 08-Sep-2005
REV: 16-Nov-2005
WORKING
DRAFT
RECOMMENDED
PUBLICATION
READER
DATE
CONTEXT:
A0
Digital Certificate
Information Required for Tax Purposes
Receive Tax Form
A2.1
Tax Form
Verify Tax Form
A2.2
Verified Tax Form
Approve Tax Assessment
A2.3
Notice of Assessment
Issue Notice Assessment
A2.4
Acknowledgement of Receipt of Tax Form
Notice of Assessment in User's Inbox
Notice of Assessment in ROS backend system
NODE:
A2
TITLE:
CollectTax forms
NUMBER:


USED AT:
AUTHOR: Diplomatics Team
PROJECT: CS20 ROS
NOTES: 1 2 3 4 5 6 7 8 9 10
DATE: 08-Sep-2005
REV: 16-Nov-2005
WORKING
DRAFT
RECOMMENDED
PUBLICATION
READER
DATE
CONTEXT:
A0
Notice of Assessment in User's Inbox
Receive Debit Instruction Form
A3.1
Debit Instruction Form
Validate Debit Instruction Form
A3.2
Validated Debit Instruction Form
Export Debit Instruction Form
A3.3
Debit Instruction Form Sent to Financial Institutions
Debit Instruction Form in ROS Backend system
Receive Payment
A3.4
Payment Receipt
NODE:
A3
TITLE:
Process Payment
NUMBER:


USED AT:
AUTHOR: Diplomatics Team
PROJECT: CS20 ROS
NOTES: 1 2 3 4 5 6 7 8 9 10
DATE: 08-Sep-2005
REV: 16-Nov-2005
WORKING
DRAFT
RECOMMENDED
PUBLICATION
READER
DATE
CONTEXT:
TOP
A-0
Administer ROS Tax Collection
A0
Generate Digital Certificate
A1
CollectTax forms
A2
Process Payment
A3
Preserve Security Wrapper
A4
Receive User Application
A1.1
Verify User Information
A1.2
Issue Passwords and Digital Certificate
A1.3
Receive Tax Form
A2.1
Verify Tax Form
A2.2
Approve Tax Assessment
A2.3
Issue Notice Assessment
A2.4
Receive Debit Instruction Form
A3.1
Validate Debit Instruction Form
A3.2
Export Debit Instruction Form
A3.3
Receive Payment
A3.4
NODE:
A0
TITLE:
Administer ROS Tax Collection
NUMBER:

CS20 - Revenue On-Line Service (ROS)
IDEF0 Model Activity Definitions (20051014)

Activity Name	Activity No.	Activity Definition	Activity Note
Administer ROS Tax Collection	A0	To generate digital certificate, to collect tax forms, and to receive tax payments using ROS.	
Generate Digital Certificate	A1	To receive user application, verify user information, and issue passwords and Digital Certificates.	
Receive User Application	A1.1	To receive user application for password and ROS Access Number (RAN) or Tax Agent Identification Number (TAIN).	
Verify User Information	A1.2	To verify accuracy and completeness of user application form.	
Issue Passwords and Digital Certificate	A1.3	To issue inbox password, RAN or TAIN and Digital Certificate.	Although ROS issues the passwords and the Digital Certificates at the same time, the user receives the passwords first and then uses them to obtain the Digital Certificate.
Collect Tax forms	A2	To receive Tax Form, verify Tax Form, approve Tax Form and Export Tax Form.	
Receive Tax Form	A2.1	To receive completed and encrypted Tax Form.	
Verify Tax Form	A2.2	To verify accuracy and completeness of Tax Form.	This is done automatically by ROS. If the system detects an error, human invention by ROS might be required.
Approve Tax Assessment	A2.3	To approve assessed tax payment or refund.	
Issue Notice Assessment	A2.4	To send the Notice of Assessment to the user's inbox.	A copy is saved by ROS in the backend system.
Process Payment	A3	To receive, validate, and export the Debit Instruction Form, and receive payment.	
Receive Debit Instruction Form	A3.1	To receive completed Debit Instruction Form.	
Validate Debit Instruction Form	A3.2	Verify user identity, record authentication and content integrity as conducted by the PKI technology.	
Export Debit Instruction Form	A3.3	Send validated Debit Instruction Form to appropriate financial institution and to ROS' backend system.	
Receive Payment	A3.4	ROS receives payment from the user.	
Preserve Security Wrapper	A4	The Security Wrapper is the entire transaction data set received from the customer by ROS. This includes the transaction element, i.e. tax return and payment instruction, as well as the 'security packaging' element, i.e., digital signature, date/time stamp, etc. The Security Wrapper confers authenticity and non-repudiation over time.	Although this is an important stage, the exact procedure cannot be determined from the case study.

CS20 - Revenue On-Line Service (ROS)
IDEF0 Model Arrow Definitions (20051014)

Arrow Name	Arrow Definition	Arrow Note
Acknowledgement of Receipt of Application	A notice is automatically sent to users acknowledging that their application has been received.	
Acknowledgement of Receipt of Tax Form	A notice is automatically sent to users acknowledging that their Tax Form has been received.	
Business Rules	The creation, retention, and preservation of ROS records according to Best Practices.	
Citizens	Individuals who possess a PPS number and choose to file their taxes through ROS.	
Debit Instruction Form	Instructions on how to process payment.	
Debit Instruction Form in ROS Backend system	Forms saved in the ROS' backend system.	
Debit Instruction Form Sent to Financial Institutions	Forms sent to appropriate financial institutions.	
Digital Certificate	Digital Certificate containing user information and the user's Public Key.	
E-Government Initiatives	Resulting from the strong emphasis placed by the Irish government on the importance of electronic government and business transactions for the Irish and EU economy.	
Existing Technology	The capabilities of the technology available to the Revenue and users at any given time.	
Facilities	The physical space that hosts the server and the database.	
Inbox Password	Password for users' inbox.	
Information Required for Tax Purposes	The information needed from the user that is necessary to complete tax assessment.	
Notice of Assessment	ROS-approved tax assessment.	
Notice of Assessment in ROS backend system	Notice of Assessment saved in ROS backend system.	
Notice of Assessment in User's Inbox	Notice of Assessment sent to user's inbox.	
Payment Receipt	Receipt for payment issued to user.	
Personal User Information		
Preserved Security Wrapper	The preserved Security Wrapper is the entire transaction data set received from the customer by ROS. This includes the transaction element, i.e. tax return and payment instruction, as well as the 'security packaging' element, i.e. digital signature, date/time stamp, etc.	
RAN	ROS Access Number.	
Relevant Legislation	The 1923 Order 2/23, the Taxes Consolidation Act of 1997, the Irish E-Commerce Act 2000, and the National Archives Act.	Order 2/23 established the office of the Revenue Commissioners with the mandate to collect taxes.

CS20 - Revenue On-Line Service (ROS)
IDEF0 Model Arrow Definitions (20051014)

Arrow Name	Arrow Definition	Arrow Note
Resources	Available human and financial resources.	
Revenue	The department of the responsible for the collection of tax which includes the Revenue Certificate Authority (CA).	
Revenue Policies	The policies that dictate how ROS conducts its business including Revenue PKI Certificate Practice and Policy Document, the Certification Practice Statement, and the RFT for the PKI infrastructure.	These are administered by the Revenue Commissioners.
TAIN	Tax Agent Identification Number.	
Tax Form	Form containing information in required fields for the purpose of calculating a user's tax payment or refund.	
Technology	The n-tiered platform, Advantage Ingress 2.5 relational database, and the PKI environment.	
User Application Form	Form containing user information in required fields.	
Validated Debit Instruction Form	The instruction form that has been validated by ROS.	
Verified Application Form	Application form that has been verified by ROS.	
Verified Tax Form	Tax Form that has been verified by ROS.	

Appendix 1: Abbreviations

ACS	Access Control System
CA	Certification Authority
CP	Certification Policy Statement
CPS	Certification Practise Statement
IDMACS	Identity Management & Access Control System
ITP	Integrated Taxation Processing [System]
OID	Object Identifier
PAA	Policy Approval Authority
PKI	Public Key Infrastructure
PPA	Policy Approval Authority
PPS	Personal Public Service [Number]
PSB	Public Services Broker
PRSI	Pay Related Social Insurance
RA	Registration Authority
RAN	ROS Access Number
RDI	ROS Debit Instruction
ROS CA	ROS Certification Authority
ROS CIS	ROS Customer Information Service
ROS	Revenue On-Line Service
TAIN	Tax Agent Identification Number

Appendix 2: Extract from Revenue's PKI *Certification Practice Statement*

5.2 Procedural Controls[82]

5.2.1 Trusted Roles

In order to ensure that one person acting alone cannot circumvent the entire system, the area where the servers and work stations that comprise the Revenue PKI is located is a declared no lone zone where two people are required to carry out an operation. To gain access to a machine, two keys are required to be inserted and turned simultaneously to open the cabinet securing the machine. All actions carried out in the vicinity of a cabinet containing a machine is captured on video tape. When gaining access to a work station, one person enters the first half of the password and the second person enters the rest of the password. Once access is gained to the work station, one person performs the task while the other audits the task performance to ensure it is done properly. All keystrokes typed on a keyboard attached to a machine are captured and recorded in an audit log.

At a minimum, the following roles are established at each location:

1. System Administrator.
2. Registrar (ROS CA).
3. Security Administrator.

5.2.2 Number of Persons Required Per Task

Separate individuals fill each of the three roles described above. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over system operation. However:

1. A single individual may assume the roles of the System Administrator and Registrar.
2. The Security Administrator must always remain separate from the System Administrator in order to provide an independent review of the audit log.
3. Any task requiring the creation, backup or importation into a database of The Revenue CA's Private Key must involve two trusted persons, one performing the function and the second fulfilling a security monitoring role. Each of the operations that require dual control by two personnel within the Revenue PKI shall not be carried out by one person. Each person in a dual control shall be responsible for the integrity of the process they are performing. They will not disclose to the other person any parts of a password.

5.2.3 Identification and Authentication for Each Role

All staff are recruited in line with Irish Government recruitment procedures.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

The recruitment and selection practices for Revenue PKI services personnel take into account the background, qualifications, experience and clearance requirements of each position, which are compared against the profiles of potential candidates.

[82] Office of the Revenue Commissioners Ireland (2000). "Revenue Public Key Infrastructure: Certification Practice Statement," p. 45.

5.3.2 Background Check Procedures

Background checks are conducted on all persons selected to take up a trusted role in accordance with the designated security screening procedure, prior to the commencement of their duties.

5.3.3 Training Requirements

- All Revenue PKI services staff are provided with appropriate training, including:
- Basic PKI concepts
- For pertinent CA staff, how to explain to RA Certificate applicants the responsibilities adhering to the possession, use and operation of their key pairs
- How to explain to Approved and Authorised Persons, for example Approved and Authorised Persons, the responsibilities adhering to the possession, use and operation of their Keys and Certificates
- The meaning and effect of the Conditions of Use that applies to the Keys and Certificates

Note that additional software product specific training will be provided to Revenue PKI services staff, as and when deemed appropriate.

5.3.4 Retraining Frequency and Requirements

Revenue PKI services personnel will receive a security briefing update at least once a year. Training in the use and operation of the CA and RA's software is provided when new versions of the software are installed.
Remedial training is completed when recommended by audit comments.

5.3.5 Job Rotation Frequency and Sequence

The Revenue PKI may implement formal job rotation practices (for example through formal relief). Where formal job rotation is not implemented, cross-training activities are conducted to ensure operations continuity.

5.3.6 Sanctions for Unauthorised Actions

Unauthorised actions by Revenue PKI services personnel staff are submitted to appropriate authorities including, but not limited to, the Security Administrator.

5.3.7 Contracting Personnel Requirements

Revenue PKI services personnel may be contractors who are appointed in writing and given written notification of the terms and conditions of their position. They are normally assigned full-time to their responsibilities.

5.3.8 Documentation Supplied to Personnel

Revenue PKI services personnel shall have access to their relevant:

1. Hardware and software documentation.
2. Policy documents, including this CPS.
3. Operational practice and procedural documents, including a relevant CP.

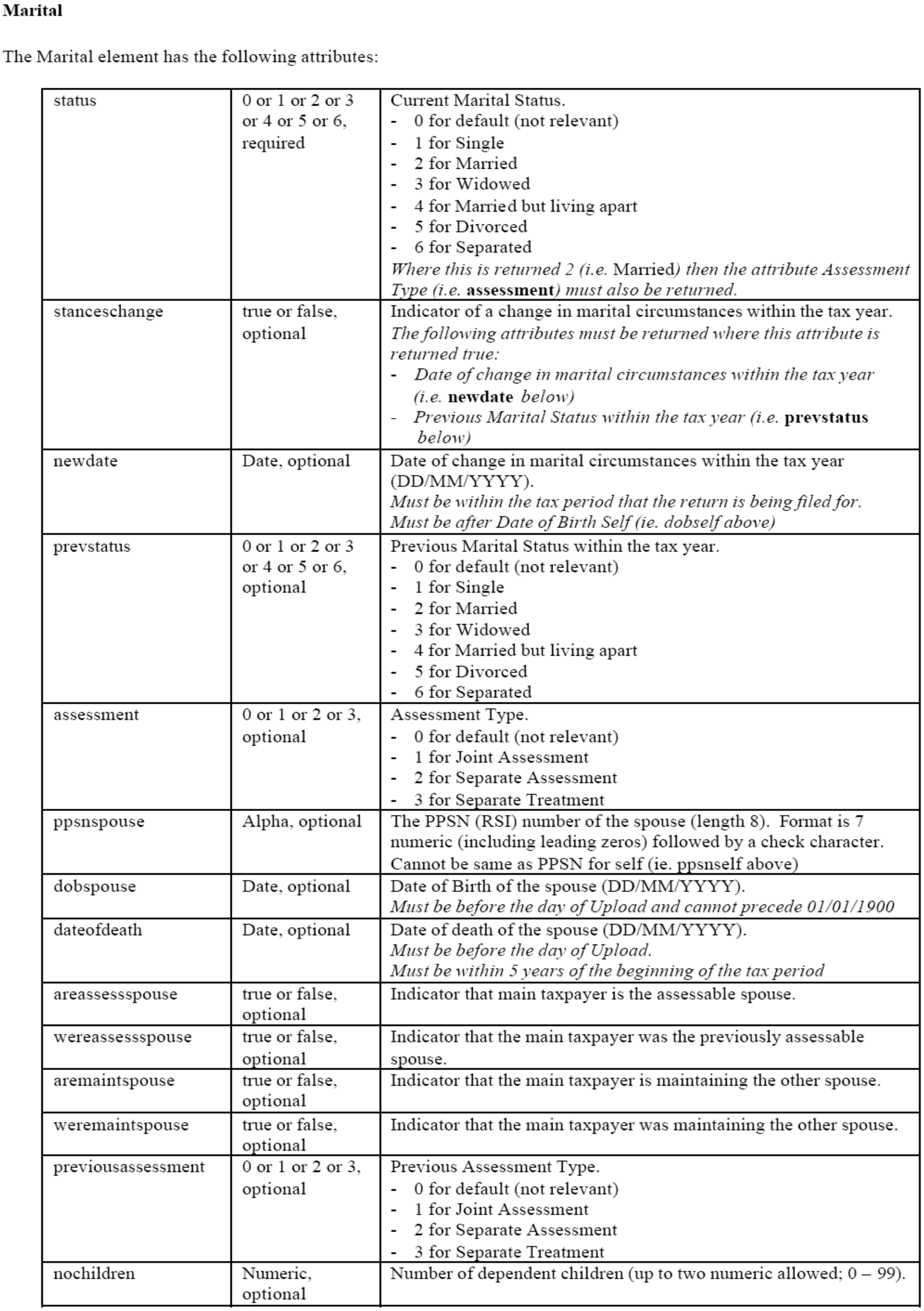
Appendix 3: Glossary extract from the *ROS Certificate Policy Statement*

Approved Person	Defined in S917G of the *Taxes Consolidated Act 1997*. An individual who applies for a digital certificate for their own use or on behalf of an Entity, and who applies for digital certificates for Authorised Persons.
Authentication	The process whereby a service provider satisfies him/her self to an appropriate level of confidence that a service requester is entitled to the service sought.
Authenticity	The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.
Authorised Person	Defined in S917G of the *Taxes Consolidated Act 1997*. An individual who receives a digital certificate applied for on their behalf by an Approved Person.
Certification Authority (CA)	(i) A centre trusted to create and assign Public Key Certificates. Optionally, the certification authority may create and assign keys to the entities. (ii) An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the user's keys. (iii) A trusted entity that verifies the identity of a user, allocates a Distinguished Name to that user, and verifies the correctness of information concerning that user by signing the data that constitutes the digital signature for that user.
Certification Policy Statement (CP)	A set of procedures to be followed by the CA when certificates are issued to an Entity
Certification Practice Statement (CPS)	A statement of the practices that the Revenue CA employs in issuing certificates
Cryptography	The discipline that embodies principles, means, and methods for the transformation of data to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.
Digital signature	Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery for example by the recipient.
Entity	For the Revenue PKI, the term Entity is used to describer a Revenue customer. For example, an Entity may be a company, trust, partnership, sole trader or individual taxpayer who is an employee of a company and pays tax through PAYE. NOTE: The term "entity" is also sometimes used in this glossary as a generic term to describe an Approved or Authorised Person and/or relying party within a PKI.
Hash	A computed number. A hash is used to compare versions of a calculated piece of data. If the hash results match, an assurance can be drawn that the data has not been tampered with.

Key pair	A complementary pair of encryption keys generated by the CA and formatted into a private key and public key. The public key is distributed within a certificate issued by the CA.
Non-repudiation exchange	A sequence of one or more transfers of non-repudiation information (NRI) for the purpose of non-repudiation.
Non-repudiation information	A set of information that may consist of the information about an event or action for which evidence is to be generated and validated, the evidence itself, and the non-repudiation policy in effect.
Non-repudiation policy	A set of criteria for the provision of non-repudiation services. More specifically, a set of rules to be applied for the generation and verification of evidence and for adjudication.
Policy Approval Authority (PAA)	The Policy Approval Authority established by Revenue, responsible for the policies that govern the management and operation of the Revenue PKI.
Privacy	The right of individuals to control or influence what information related to them may be collected and stored and to whom that information may be disclosed. NOTE - Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.
Private Key	That part of a key pair that is held by a logical or legal entity in an authentication system, protected by a password, and not made available to anyone else.
Public Key	(i) Public part, key or mathematical construct from a pair of keys which together form the basis of Public Key Technologies. (See Private Key). The key of an entity's asymmetric key pair that can be made Public. In the case of an asymmetric signature system, the Public Key and the associated algorithms define the verification transformation. [ISO/IEC 13888] (ii) (In a Public Key cryptosystem) that key of a user's key pair that is Publicly known. [ISO/IEC 9594-8:1990] [CCITT X.509: 1988] (iii) That key of an entity's asymmetric key pair that can be made Public. [ISO/IEC 9798-1 (2nd edition): 1997] [ISO/IEC 11770-1: 1997] [2nd DIS ISO/IEC 11770-3 (08/1997)] The following note is contained in ISO/IEC 9798-1 and in ISO/IEC 11770-3: NOTE - In the case of an asymmetric signature system the Public Key defines the verification transformation. In the case of an asymmetric encipherment system the Public Key defines the encipherment transformation. A key that is 'Publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.
Public Services Broker (PSB)	A centralized electronic gateway for all Government services.

RAN	ROS Access Number. A unique number allocated to each potential Approved or Authorised Person to the ROS CA as part of the registration process. The RAN forms part of the Distinguished Name on the Approved or Authorised Person's certificate and may not be re-used.
Registration Authority	An entity that establishes the identities of users and registers their certification requirements with a Certification Authority.
Revenue CA	Office of the Revenue Commissioners Certification Authority. The Revenue CA is the highest level of trust within the Revenue PKI.
Revenue PKI	The public key infrastructure established by Revenue.
ROS CA	The Certification Authority supporting the ROS application. The ROS CA is a sub CA from the Revenue CA within the Revenue PKI.

Appendix 4: Tax Form 11 Metadata Extract



Marital

The Marital element has the following attributes:

status	0 or 1 or 2 or 3 or 4 or 5 or 6, required	Current Marital Status. - 0 for default (not relevant) - 1 for Single - 2 for Married - 3 for Widowed - 4 for Married but living apart - 5 for Divorced - 6 for Separated *Where this is returned 2 (i.e.* Married*) then the attribute Assessment Type (i.e.* **assessment***) must also be returned.*
stanceschange	true or false, optional	Indicator of a change in marital circumstances within the tax year. *The following attributes must be returned where this attribute is returned true:* - *Date of change in marital circumstances within the tax year (i.e.* **newdate** *below)* - *Previous Marital Status within the tax year (i.e.* **prevstatus** *below)*
newdate	Date, optional	Date of change in marital circumstances within the tax year (DD/MM/YYYY). *Must be within the tax period that the return is being filed for.* *Must be after Date of Birth Self (ie. dobself above)*
prevstatus	0 or 1 or 2 or 3 or 4 or 5 or 6, optional	Previous Marital Status within the tax year. - 0 for default (not relevant) - 1 for Single - 2 for Married - 3 for Widowed - 4 for Married but living apart - 5 for Divorced - 6 for Separated
assessment	0 or 1 or 2 or 3, optional	Assessment Type. - 0 for default (not relevant) - 1 for Joint Assessment - 2 for Separate Assessment - 3 for Separate Treatment
ppsnspouse	Alpha, optional	The PPSN (RSI) number of the spouse (length 8). Format is 7 numeric (including leading zeros) followed by a check character. Cannot be same as PPSN for self (ie. ppsnself above)
dobspouse	Date, optional	Date of Birth of the spouse (DD/MM/YYYY). *Must be before the day of Upload and cannot precede 01/01/1900*
dateofdeath	Date, optional	Date of death of the spouse (DD/MM/YYYY). *Must be before the day of Upload.* *Must be within 5 years of the beginning of the tax period*
areassessspouse	true or false, optional	Indicator that main taxpayer is the assessable spouse.
wereassessspouse	true or false, optional	Indicator that the main taxpayer was the previously assessable spouse.
aremaintspouse	true or false, optional	Indicator that the main taxpayer is maintaining the other spouse.
weremaintspouse	true or false, optional	Indicator that the main taxpayer was maintaining the other spouse.
previousassessment	0 or 1 or 2 or 3, optional	Previous Assessment Type. - 0 for default (not relevant) - 1 for Joint Assessment - 2 for Separate Assessment - 3 for Separate Treatment
nochildren	Numeric, optional	Number of dependent children (up to two numeric allowed; 0 – 99).