

ATUG's Focus this week is on the development of Australia's Digital Economy enabled by the NBN. The article looks at elements of the Digital Economy – services, applications and trust. A number of issues arise for ATUG:

- The emergence of a new class of applications service providers such as education service providers, health service providers, business service providers, who will need access over the NBN for delivery of their services.
- In E-Security Awareness Week the need for a trusted, secured environment for transactions – and not just financial transactions, as explained by the examples from France and UK below

The core material for this ATUG Focus has been provided by Adjunct Professor at Murdoch University, Perth and ATUG Director, Dr Walter B Green. Some expanded material has also been included and is referenced.

Key Components of the Digital Economy

The Digital Economy is dependent on applications, services, and the ability to have the same level of security, comfort and legal evidence that applies in the paper transactions that are in use at present.

Discussions about the Digital Economy are difficult, due to many interpretations of the words, applications, services, and trust. This note attempts to define these terms, and show their interdependence.

Services

Definition from Wikipedia

Services (Economics context)

A **service** is the... non-material counterpiece of a physical good. A service provision comprises a sequence of activities that does not result in ownership of the outcome, and this is what fundamentally differentiates it from furnishing someone with physical goods. Service provision is a process that creates predetermined benefits by effectuating either a change of service consumers, a change in their physical possessions or a change in their (in)tangible assets.

By composing and orchestrating the appropriate level of resources, skill, ingenuity, and experience for effecting specific benefits for service consumers, service providers participate in an economy without the restrictions of carrying stock (inventory) or the need to concern themselves with bulky raw materials. On the other hand, their investment in expertise does require consistent service marketing and upgrading in the face of competition which has equally few physical restrictions.

Providers of services make up the Tertiary sector of the economy.

Service Providers (communications context)

A **service provider** is an entity that provides services to other entities. Usually this refers to a business that provides subscription or web service to other businesses or individuals. Examples of these services include Internet access, Mobile phone operator, and web application hosting.

- Application service provider (ASP)
- Internet Service Provider (ISP)
- Managed Service Provider (MSP)
- Master Managed Service Provider (MMSP)
- Telecommunications Service Provider (TSP)
- Managed Internet Service Provider (MISP)

Services enable the exchange of information but in a fully operational Digital Economy would include the additional business and legal requirements of validation, proof of delivery, proof of receipt and non-repudiation.

The exchange of information maybe bidirectional, or unidirectional, with the additional possibility that information exchange can be a simultaneous exchange between multiple parties in both 1 to N (e.g. broadcast, webcast) and N to N environments (e.g. group conference calls). Early internet transactions were mainly downloads (or uni-directional) however WEB 2 services are based on services enabling users to provide the content and information. The increase in use of Web 2 services increases the need for symmetrical Broadband links to customers.

It should also be noted that the information can be distributed for free, (typically advertising) or procured where a user buys information or products. Free information may also be classified as advertising or for community benefit (e.g. government information or health information).

It is possible to protect information (eg data, music, videos applications, etc) so that a user cannot modify or on sell the information. Existing Protection applications also enable the seller to block the use of the data after a specified time. (Many of the piracy problems of today could be solved now, if suppliers used a protection scheme that are available on the market today.)

Applications

From Wikipedia:

In computer science, an application is a computer program designed to help people perform a certain type of work. An application thus differs from an operating system (which runs a computer), a utility (which performs maintenance or general-purpose chores), and a programming language (with which computer programs are created). Depending on

the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements. Some application packages offer considerable computing power by focusing on a single task, such as word processing; others, called integrated software, offer somewhat less power but include several applications.

A simple, if imperfect analogy in the world of hardware would be the relationship of an electric light bulb (an application) to an electric power generation plant (a system). The power plant merely generates electricity, not itself of any real use until harnessed to an application like the electric light that performs a service that benefits the user.

Typical examples of 'software applications' are word processors, spreadsheets, media players and database applications.

Applications enable users to display, modify and create new information based on one or more sources (mash ups). This new information can then be sold or distributed as part of a service. Applications also provide some of the management features for computers and networks.

In some instances, applications may be required to visualise or display the information (e.g. images, pdf files). A key enabler to the Digital Economy is an application that is able to display information that is received in a variety of formats, with in-built ability to support the secure receipt and management of the information.

Typical applications in use today are Adobe with "pdf" files, and more recently the Open Document Standard, that are attempts to make a single application capable of displaying a wide range of information. Each has their own limitations, because the producer of the information has to be able to save the information in a specific format (even if the source data may come from a spreadsheet, database, image etc).

Interesting insights to the development of secured applications for the Digital Economy can be found from the following article on a recently developed European/French protocol called FAST which has been developed to provide a secure online platform to handle electronically the many transactions between local communities, or collectives, and the central government and particularly the interior ministry:

In all sorts of dealings and transactions between government departments, between businesses and government bodies, and between individual citizens and government, verification of identity and proof of what has transpired is needed.

As a rule, this has usually meant forms to fill in, signatures dated and physically posting or delivering the completed forms.

A few years ago, a French government initiative set out to develop a secure online platform to handle electronically the many transactions

between local communities, or collectives, and the central government and particularly the interior ministry.

These include the 'collectives' having to inform the ministry of all decisions they take, and also to notify the central government of all births, deaths and marriages that occur.

Automated, secure document exchange

The system is able to provide automated and secure document exchange, legally recognised acknowledgement of receipt, electronic certificates and signatures, secure encryption of information, as well as traceability, time-stamping and archiving of electronic documents.

This means collectives all over France no longer have to post off copies of life-event certificates to Paris, but simply file them electronically via the FAST platform. Individual citizens benefit in a number of ways, such as no longer having to provide a physical copy of a birth certificate when making a benefit application.

The EU-funded project, which got underway in 2008, has two very different trials of the platform's capabilities on the go.

One is in the Spanish region of Valencia, where it is being used with the local government's e-procurement platform to provide a new level of security by generating legally binding proof of both calls for proposal and of transactions.

The second is in the English city of Sheffield, and the objective here is to develop from scratch a new procedure for the management of contacts within organisations. This is being done by a pilot system to manage the contacts between schools and parents.

Jonathan Gay, the project partner in charge of the Sheffield trials, said: "We took stock of the paperwork being used in the local school system to see what could be put onto the FAST platform to reduce the need for parent-based signatures". Then ten schools were selected to trial a cross-selection of applications.

One of the applications being trialled is parental consent for events, such as school outings. Instead of posting or giving children consent forms for parents to fill in, a teacher can put the detail of an event onto the platform which will then contact all the parents, and send reminders to those who do not respond. Parents log onto a website to give consent via an electronic signature. Parents who do not have access to a PC at home can use a token with an electronic signature on it at a public terminal.

For full details go to:

<http://cordis.europa.eu/ictresults/index.cfm?section=news&tpl=article&BrowsingType=Features&ID=90609>

Trust

The major weaknesses of internet transactions today, especially browsers, are the security issues and the ability to validate, and manage the transfer of data. At present, the most relevant example of the need for security are financial transactions, however these security solutions are generally not available to other types of transactions.

At present, a large number of internet and email transactions are wide open to abuse, which in turn creates problems for the business, end users and the legal profession.

Consider how many specifications, drawings, tender documents, quotations, purchase orders, etc are transmitted over the internet, without any solid proof that the:

- recipient has received a valid copy, and
- sender cannot deny sending the document.

Many businesses have not made a complete transformation from the business processes dependent on signed memos or documents, to the modern day environment where emails have replaced the old style memo. Many of the issues of repudiation, validity, tampering, etc have not been carefully considered (it is very easy to modify a back-up copy) leaving organisations open to significant liability in the event of a dispute. (No wonder many lawyers prefer to have paper copies). Modern day computer forensics are able to solve some of the problems, however the use of validation, and non-repudiation features would solve most of the problems we experience today.

It should be noted, with the Internet in its present form, that it is possible for a file to become corrupted while in transmission. This means that any validation process must be capable of identifying any changes due to corruption in transmission, and deliberate tampering and/or modification.

It is also important for any validation process to cover applications, so that the user can be sure that the application has not been modified, either in delivery, or after prolonged periods of use. As many applications are updated regularly there is also a requirement to validate any upgrades.

The development of new business models for a fully operational Digital Economy needs the support of advanced security solutions. One example of the work being done to develop these is the EU-funded ECRYPT project.

This network of researchers across Europe aims to deepen research into cryptography, and, through one so-called 'virtual lab' called WAVILA in

Belgium to study methods and applications for digital watermarking and perceptual hashing.

Watermarks have been used for centuries to prove the authenticity of bank notes, postage stamps and documents. The European researchers are considering them as a new tool in the fight against digital piracy and to authenticate and verify the integrity of digital media.

Though not a new concept, digital watermarking is starting to gain favour among content producers as one of several emerging anti-piracy measures. Earlier this year, for example, record companies Sony and Universal started embedding anonymous watermarks into songs not protected by other DRM methods. That will allow them to trace the origins of illegally copied material, potentially generating important empirical evidence on the scale of the piracy problem as they seek tighter copyright protection laws.

Other uses include authenticating information and ensuring data integrity, as well as making content easier to identify and find.

For further details go to:

<http://cordis.europa.eu/ictresults/index.cfm/section/news/tpl/article/BrowsingType/Features/ID/90264/highlights/security>

ATUG is interested in other topics of interest to members re-thinking their business operations and business models ahead of the transformation to a digital economy, email patrick.sinclair@atug.org.au or go to ATUG's Blog <http://www.atugblog.com.au>

The core material for this ATUG Focus has been provided by Adjunct Professor at Murdoch University, Perth and ATUG Director, Dr Walter B Green, PhD, MScEng, CEng, CPEng, CITP, FAIM, FIEAust, FIET, FBCS.

Dr Green would like to acknowledge the contributions to this paper by Murdoch University colleagues and researchers in the e-Commerce section from 2000 to 2002, and especially the contributions made by Assoc Prof Richard Joseph.