



PKI and the legal sector

<http://www.galexia.com.au/resources/>

Peter van Dijk, CEO, Galexia

- ◆ Introduction to PKI
- ◆ Digital Signatures
 - Authentication, integrity, confidentiality and non-repudiation
- ◆ The development of a trusted business environment
- ◆ Use of Digital Certificates by solicitors
 - Developments in other jurisdictions
- ◆ Practical example of a simple PKI pilot in NSW – court lodgment





What is PKI?

- ◆ Public Key Infrastructure (PKI) is the combination of **software, encryption technologies, and services** that enables organisations to protect the security of their communications and business transactions on the Internet
- ◆ PKIs integrate **digital certificates, public-key cryptography, and certificate authorities** into a shared network security architecture, including:
 - issuance of digital certificates to individual users
 - end-user enrolment software
 - integration with corporate certificate directories
 - tools for managing, renewing, and revoking certificates





What are some of the technical security issues with the internet?

- ◆ **Eavesdropping** - Information remains intact, but its privacy is compromised. For example, someone could learn your credit card number, record a sensitive conversation, or intercept classified information.
- ◆ **Tampering** - Information in transit is changed or replaced and then sent on to the recipient. For example, someone could alter an order for goods or change a person's resume.
- ◆ **Impersonation** - Information passes to a person who poses as the intended recipient. Impersonation can take two forms:
 - **Spoofing** - A person can pretend to be someone else. For example, a person can pretend to have the email address `pvd@galexia.com.au`, or a computer can identify itself as a site called `www.galexia.com.au` when it is not.
 - **Misrepresentation** - A person or organization can misrepresent itself. For example, suppose the site `www.dodgybros.com` pretends to sell software online when it is really just a site that takes credit-card payments but never sends any goods.





PKI provides four assurances

- ◆ **Authentication** - confirm who you are
- ◆ **Integrity** - what you sent
- ◆ **Non-repudiation** - you can't deny it
- ◆ **Confidentiality** - what you can see - enables the encryption and decryption of information sent between two parties

galexia



Components of a PKI

A PKI comprises the following components:

- ◆ **Certificate Authorities (CAs):** These are responsible for issuing and revoking certificates.
- ◆ **Registration Authorities (RAs):** These verify the binding between public keys and the identities of their holders.
- ◆ **Certificate holders (or subjects):** People, machines or software agents that have been issued with certificates and can use them to sign digital documents.
- ◆ **Clients:** These validate digital signatures and their certification paths from a trusted CA's public key.
- ◆ **Repositories:** These store and make available certificates and certificate revocation lists
- ◆ **Security policy:** This sets out and defines the organization's top-level direction on information security, as well as the processes and principles for the use of cryptography.

galexia



Components of a PKI

<http://www.baltimore.com>

A PKI should consist of:

- ◆ A Security Policy
- ◆ Certificate Authority (CA)
- ◆ Registration Authority (RA)
- ◆ Certificate Distribution System
- ◆ PKI-enabled Applications



The components of a PKI

galexia

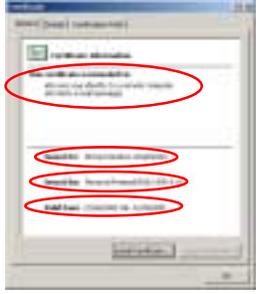
What is a Digital Certificate?

- ◆ A digital form of identification
 - Similar to a passport or driver's licence
 - Binds subject's public key (a mathematical value) to one or more attributes relating to their identity
- ◆ A certificate is valid for a period of time, (often one, three or ten years)
- ◆ Certificates can do different things. For example:
 - Encrypt a document
 - Sign a document – for non-repudiation
 - Secure a WWW server
 - Provide authentication - Enable the holder to access a corporate new work



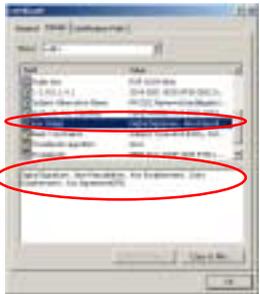
Example Certificate (1)

- ◆ Certificate Summary



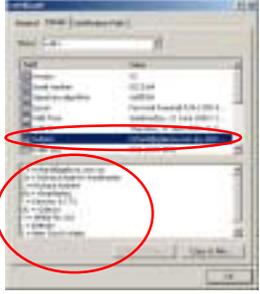
Example Certificate (2)

- ◆ Certificate Attribute details : Key Usage



Example Certificate (3)

- ◆ Certificate Attribute details : Subject



gaalexia

What are Certificate Authorities?

- ◆ CAs issue digital certificates and validate the holder's identity and authority
 - PKIs and digital certificates are most trustworthy when they are vouched for by a trusted certificate authority.
- ◆ CAs embed an individual's or an organisation's public key along with other identifying information into each digital certificate and then cryptographically "sign" it as a tamper-proof seal, verifying the integrity of the data within it and validating its use.

gaalexia

Why use a CA?

- ◆ PKI is based on the concept of a certificate hierarchy.
 - The "root key" of this hierarchy links all certificates issued by the hierarchy and identifies the CA.
 - The root key must be recognised by all the various software applications that must verify and accept digital certificates in order to verify the authenticity of the information in the certificate.



gaalexia



What is a Registration Authority?

- ◆ Performs subset of CA functions
- ◆ Establishes and confirms identity of an individual
- ◆ Initiates the certification process with a CA on behalf of individual end-users
- ◆ Performs key and certificate lifecycle management functions





Quality of Certification Services

- ◆ A digital signature is as good as a handwritten signature only if the digital signature is verified by reference to a reliable certificate. A certificate is reliable only if the relying party can trust its issuer.
- ◆ The value of a PKI is ultimately dependant upon the level of assurance that the CA provides -
 - verification of security policies
 - validating certificate requests
 - issuing certificates properly
 - managing certificates
 - managing certificate lifecycle
 - managing the private key
 - security of pass phrases





What does PKI mean to the legal sector?

- ◆ Enabling eBusiness for the profession
 - professional and individual practice,
 - firm and
 - client oriented
- ◆ Secure messaging and document exchange
- ◆ Court lodgement
- ◆ Authentication - for secure internet access (intranets, extranets)
- ◆ Issuing certificates to clients
 - Contract formation
 - Access to client extranets
 - Solicitor/client communications - encrypted, signed, audit trails





Making PKI work for the Legal Sector (1)

- ◆ 'Trusted Digital Credentials'
 - Digital Certificate
 - Confirmation of a professional status by a professional association - a professional regulatory body that has a mandate to confirm professional status of their members. Organisations like the Law Society of NSW have the ability to mandate and validate. They currently are a 'real world RA'.
 - Co-regulatory framework in which to operate
- ◆ A series of killer applications
- ◆ Integration of other online legal applications through a common authentication gateway
- ◆ Publicly accessible directory services - making the public key certificate openly available





Making PKI work for the Legal Sector (2)

- ◆ Online, on-mass certificate issuance - based upon professional or firm membership
- ◆ Certificate interoperability - will other PKIs accept 'legal sector' certificates?
 - Multiple jurisdictions
 - Multiple root CAs - possibly solved cross certification
- ◆ Conformance to standardised method of providing levels of assurance by differing RA's within the PKI - e.g. across state based law societies





Making PKI work for the Legal Sector (Issues)

- ◆ Multiple signings - sequential, contemporaneous, new contract for each signing?
- ◆ What objects are signed? - issues of document formats, meta data
- ◆ Managing revocation
- ◆ Key recovery
- ◆ Key escrow
- ◆ There may only be room for 1 legal PKI provider





Canadian Example - Juricert (1)

'Professional Authentication Online'

- Juricert is an initiative of the Law Society of British Columbia and other Canadian law societies to provide *Trusted Digital Credentials* to professional associations, their members, staff and clients for use with secure third party applications. Its operations are governed in the interests of the public and the professional integrity of the participating professional associations.
- Juricert will provide three services:
 - Systems for professionals, their staff and clients to obtain *Trusted Digital Credentials*;
 - Systems and practices for professional associations to participate in the authentication of their members; and
 - Access to a set of safe, PKI-secured third party applications that use these *Trusted Digital Credentials*.





Canadian Example - Juricert (2)

- The Law Societies in Canada have a legislated mandate to issue and maintain legal credentials and to authenticate members of the legal profession. Juricert's mission is to authenticate the on-line identity of Canadian lawyers, their staff and members of the public with whom the legal community wishes to carry out secure electronic transactions.
- Juricert acts as an electronic intermediary between professional societies, members of those societies, and software application or service providers that require evidence of members' identities in order to establish *Trusted Digital Credentials* within their software applications or services.





Canadian Example - E-reg

Land registration in Ontario

- Remote, electronic document registration (e-reg™), a paperless land titles registration system has been piloted by the Middlesex County real estate community in Ontario
- Extensive consultations with stakeholders were held and legislation was passed that set the framework for electronic registration. A joint committee of the Law Society of Upper Canada and the Canadian Bar Association Ontario reviewed existing practice standards and developed new ones to reflect the advent of e-reg in Ontario.
- Amendments to the Land Registration Reform Act remove the requirement for handwritten signatures and permit electronic signatures.
- Only users equipped with an encrypted digital signature that uniquely identifies them will be legally able to sign and register title documents.

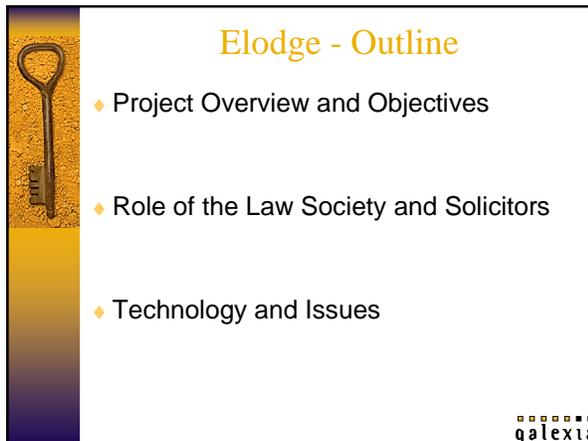




Elodge - Electronic Filing Case Study

NSW Land and Environment

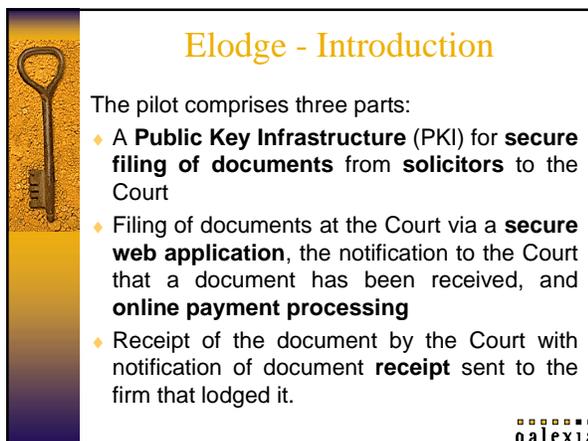
The Law Society of New South Wales galexia eSOLICITORS



Elodge - Outline

- ◆ Project Overview and Objectives
- ◆ Role of the Law Society and Solicitors
- ◆ Technology and Issues

galexia

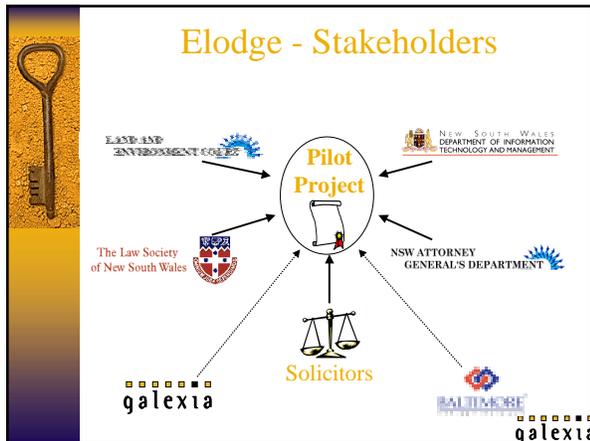


Elodge - Introduction

The pilot comprises three parts:

- ◆ A **Public Key Infrastructure (PKI)** for **secure filing of documents** from **solicitors** to the Court
- ◆ Filing of documents at the Court via a **secure web application**, the notification to the Court that a document has been received, and **online payment processing**
- ◆ Receipt of the document by the Court with notification of document **receipt** sent to the firm that lodged it.

galexia



-
- The diagram, titled "Elodge - Objectives", features a central circle labeled "Pilot Project" containing a document icon. Six arrows point towards this central circle from various stakeholders: "EASE AND ENVIRONMENT COLLEGE" (top left), "NEW SOUTH WALES DEPARTMENT OF INFORMATION TECHNOLOGY AND MANAGEMENT" (top right), "The Law Society of New South Wales" (middle left), "NSW ATTORNEY GENERAL'S DEPARTMENT" (middle right), "Solicitors" (bottom center, with a scales of justice icon), and "BALTIMORE" (bottom right). The "galexia" logo is present in the bottom left and bottom right corners of the slide.
- ◆ Primary Objective:
 - "proof of concept" for the electronic exchange of documents within the legal sector utilising PKI
 - ◆ Specific Objectives:
 - Provide mechanism for courts to define policies and standards for electronic document exchange
 - Identify court processes requiring re-engineering to exploit secure e-commerce transactions
 - Dispel fear barriers related to security for the growth of e-commerce within the legal sector
 - Prove PKI technical concepts & allow Law Society of NSW to evaluate issuing digital certificates to lawyers

-
- The diagram, titled "Elodge - Requirements", features a central circle labeled "Pilot Project" containing a document icon. Six arrows point towards this central circle from various stakeholders: "EASE AND ENVIRONMENT COLLEGE" (top left), "NEW SOUTH WALES DEPARTMENT OF INFORMATION TECHNOLOGY AND MANAGEMENT" (top right), "The Law Society of New South Wales" (middle left), "NSW ATTORNEY GENERAL'S DEPARTMENT" (middle right), "Solicitors" (bottom center, with a scales of justice icon), and "BALTIMORE" (bottom right). The "galexia" logo is present in the bottom left and bottom right corners of the slide.
- ◆ Simplicity
 - ◆ Digitally signed filing
 - ◆ Encrypted filing
 - ◆ Online payment for documents attracting filing fees
 - ◆ Digitally signed email receipts
 - ◆ Secure document retrieval
 - ◆ **Not** evaluating Court document processing



Elodge - Constraints

- ◆ Limited budget
- ◆ Short development timescale
- ◆ Short pilot phase
- ◆ Class 4 Court documents only
- ◆ Run in parallel with real manual system
 - Initiating
 - Online payments are not cleared





Elodge - Questions

- Was the pilot a successful proof of getting HTML forms and/or documents digitally signed?
- What issues did the pilot highlight with respect to digitally signing messages and/or documents?
- How will documents requiring multiple signatures be digitally signed?
- Could the project be extended to include other forms?
- Did solicitors successfully make payments online?
- Did users receive notification of receipt of the filed document?
- Were court clerks able to process documents efficiently?
- Was the court clerks' response to the pilot positive?
- What Court Rules need to be changed in order to allow for e-filing?





Elodge - Role of Law Society

- ◆ The Law Society of NSW acted as the Registration Authority
 - Generates keys
 - Registers certain end-user attributes
 - Submits public key and request to CA
 - Revokes certificates when required
- ◆ Coordinating and supporting solicitors during pilot
- ◆ Evaluating PKI technical concepts
- ◆ Assessing the feasibility of issuing digital certificates to lawyers and firms
- ◆ Reporting results and recommendations





Elodge - Issuance Certificates

- ◆ Baltimore Technologies selected as PKI vendor
- ◆ Law Society used Baltimore Registration Authority (RA) software
- ◆ Individual solicitors issued with certificates
 - Face-to-face
 - Approved by Law Society (peak sector RA)
 - Each certificate signed by Security Domain Pty Ltd
 - Issued as an electronic file on a floppy disk, containing **certificate** and **private key**
 - Each solicitor selects a pass phrase to secure the file
- ◆ Solicitors install cert and private key on their PC





Elodge - Problems/Issues

- ◆ Are digital certificates necessary in the lodgement of court documents?
- ◆ Do Law Societies have to be involved?
- ◆ How should certificates be issued?

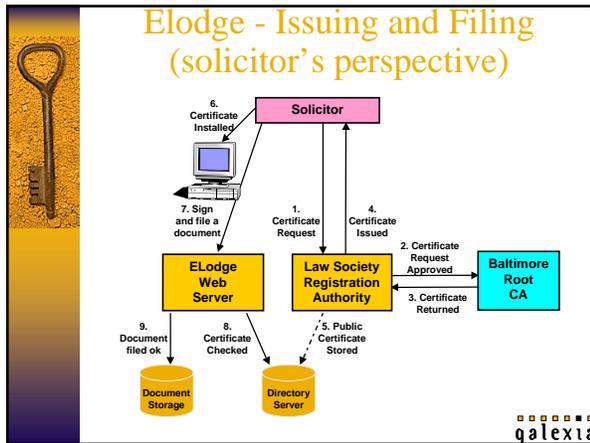


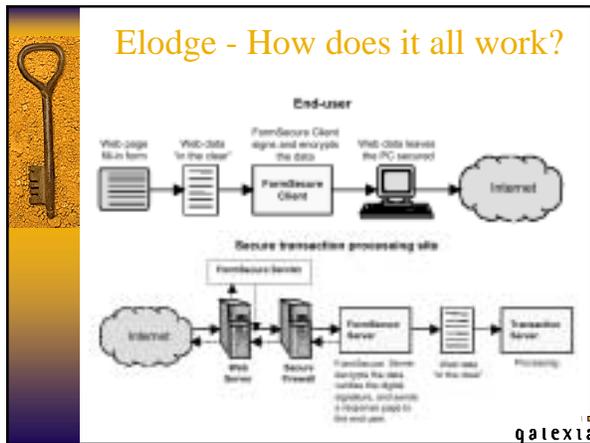


Elodge - Development

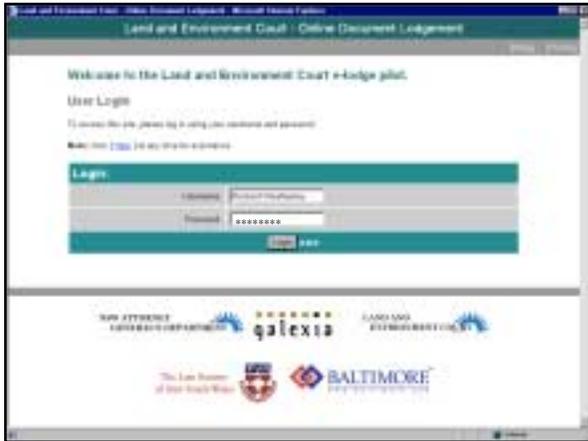
- ◆ Galexia was selected to develop “**ELodge**” system
- ◆ PKI software development, including integration of Baltimore Technologies FormSecure product
- ◆ Web-based user interface design
- ◆ Provision of a document repository
- ◆ Document storage and retrieval interface
- ◆ On-line payment processing software
- ◆ Server configuration
- ◆ Technical documentation



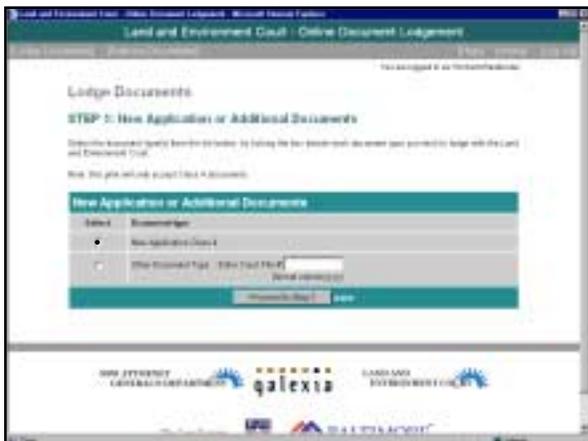






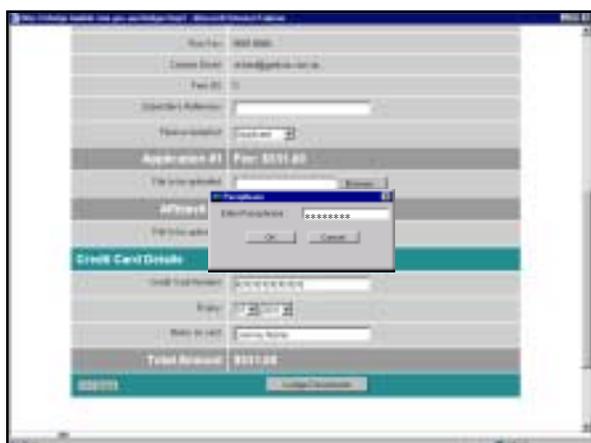


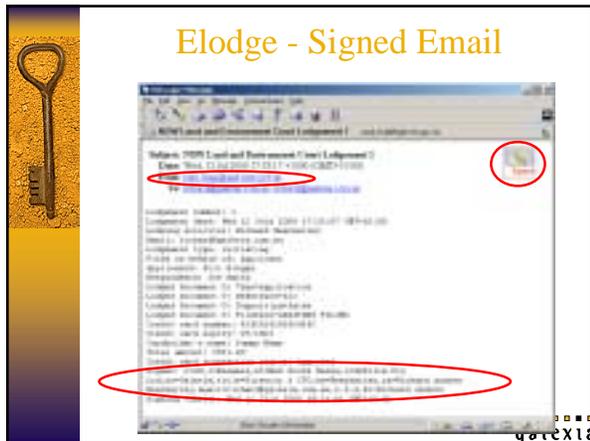


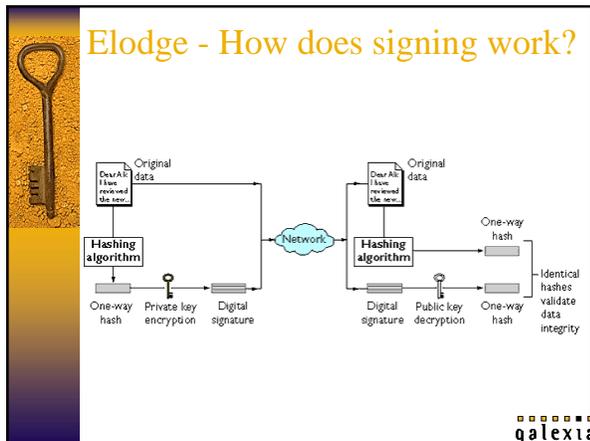












- 
- Elodge - Issues**
- ◆ Audit trail
 - Certificate expiry and document access
 - ◆ Certificate storage and key recovery
 - ◆ Multiple signatures, multiple documents
 - ◆ Browser-based lodgement
 - Thin-client PKI technology “work-in-progress”
 - Acceptable file formats
 - ◆ Is encryption/SSL really required?
 - ◆ Storing your certificates: smart cards, tokens...
 - ◆ The future: PDF, XML and e-forms plug-ins?



Elodge - Issues (2)

- ◆ Fifth level of PKI Assurance? -> contract formulation
 - Can digital signatures bind parties?
 - Varies by jurisdiction
- ◆ Quality of Certification Services
 - Reliable digital signature = reliable certificate
 - Reliable certificate = reliable issuer
- ◆ Reliance and Liability Limits
 - Some legislation permits certificates to include limits for relying on the certificate





Useful References (1)

- ◆ Introduction to Public-Key Infrastructure
 - <http://www.iplanet.com/developer/docs/articles/security/pki.html>
 - <http://www.baltimore.com/pki.html>
 - <http://verisign.netscape.com/security/pki/understanding.html>
 - <http://www.counterpane.com/pki-risks.html>
 - <http://www.iief.org/html/charters/pkix-charter.html>
 - <http://www.infosecurymag.com/jan2000/fundamentals1.htm>
- ◆ Some PKI Vendors
 - Baltimore: <http://www.baltimore.com/>
 - Verisign: <http://www.verisign.com/>
 - Thawte: <http://www.thawte.com/>
 - Entrust: <http://www.entrust.com/>





Useful References (2)

- ◆ Legal PKI initiatives
 - <http://www.juricert.com>
- ◆ Law Society Of Upper Canada - Electronic Registration of Title Documents ("e-reg") - http://www.lsuc.on.ca/edrintro_en.shtml
 - Practice Directives for Electronic Registration of Real Estate Title Documents - http://www.lsuc.on.ca/edrdraftdirectives_en.shtml
 - Document Registration Agreement (DRA) - <http://www.lsuc.on.ca/eddra99.doc>
 - Electronic Funds Bulletin - http://www.lsuc.on.ca/edrfundsbulletin_en.shtml
 - Extracts from the Joint Committee Report - http://www.lsuc.on.ca/edjointcommrpt_en.shtml
 - Practice Directives for Electronic Registration of Real Estate Title Documents - http://www.lsuc.on.ca/edrdraftdirectives_en.shtml





www.galexia.com.au ■

- ◆ End-to-end Internet solutions
- ◆ Portal & hub development
- ◆ e-Business consulting services
