PKI International Scan
_____

October 31, 2004

PKI International Scan

International PKI Scan

Introduction

This report represents ongoing research conducted by the Government of Canada (GoC) to keep abreast of developments in secure electronic transactions and service delivery. The primary focus is on how federal governments are addressing the requirement to ensure a trusted environment to enable electronic delivery of services to the public. The document is compiled using information gathered from web sites, news reports, presentations from visiting delegations, and ongoing information exchanges with internal and external parties. Since most of the research has been compiled through secondary sources, the information in this document reflects how the profiled organizations present their situation, rather than a detailed and vetted analysis of actual progress. Also, due to the rapid pace of change in this area, new developments are happening all the time. The report should not be considered a final report, but rather an evolving source of compiled information for reference purposes.

Global/Multi-nation Activities

e-Government Beyond 2005: CoBrA Recommendations For Modern and Innovative Public Administrations By 2010 [1] *(e-Government)*

During a meeting held September 28th, 2004 in Amsterdam on "e-Government beyond 2005", leaders and representatives of national e-Government initiatives from 30 European countries, issued a set of recommendations for modernizing and stimulating innovation in European administrations between now and 2010. The main recommendations are that modern and innovative administrations are essential to achieve the "Lisbon" goal of: (1) making Europe the world's most competitive knowledge-based economy by 2010; (2) e-Government is the way forward and a catalyst for innovation, and should now deliver on its promise; (3) citizens and businesses should be at the very centre of e-Government; (4) e-Government is at least as much about people, organization, and institutions as about technology that enables better public services; (5) the focus is on how public administrations must be transformed to achieve these goals?, and joint European targets should be defined for progress by 2010; (6) examples could be reducing the administrative burden for citizens and business, society-wide take-up of on line public services, etc.

A Matter of Trust: Privacy and Security Issues in the Information Age [2] *(Privacy)*

Citizens must be able to maintain their privacy online. However, many are unaware of their rights and how to protect themselves. Information Society Technologies (IST) funded research into issues related to Privacy and Identity Management (PIM). Surveys have shown that some Europeans feel their privacy is at risk from identity theft. Others are concerned about the erosion of individual rights. One thing is sure, people want to be able to interact securely and safely in cyberspace while maintaining control of their personal data. Such trust is fundamental if citizens are to embrace new services.

Secure Online Transactions Worth Talking About [3] *(Authentication / Smart Card)*

---

[1]
http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/04/1167&format=HTML&aged=0&language=EN&guiLanguage=en

[2] http://istresults.cordis.lu/index.cfm/section/news/tpl/article/BrowsingType/Features/ID/70244

[3] http://istresults.cordis.lu/index.cfm/section/news/tpl/article/BrowsingType/Features/ID/70301

Trials of European Information Society Technologies (IST) Prize-winning Vocalid® technology, based on crypto-acoustic smart cards that ensure secure, online transactions over any phone or computer, have shown strong support. So far, there are just two ways to use a card online. Users can connect cards readers to terminals, such as PCs and telephones, or they can transmit card numbers online. Passwords or banking details may also be used for securing miscellaneous online services. IST project iPROVED provides a secure alternative. Its crypto-acoustic smart card - Vocalid® - transmits dynamic acoustic authentication codes via any telephone or PC, with no need for a dedicated card reader. Cardholders therefore may use their card through any terminal, anywhere and at anytime with the same high level of security. This means that mobility is no longer restrictive in terms of online security.

Experts Concerned With Premature Introduction of Biometric Identifiers [4] *(Biometrics)*

Four experts warned Members of the European Parliament (MEPs) against the risks of a premature introduction of biometrics in European passports during a hearing held October 6th, 2004 by the European Parliament Committee on Civil Liberties, Justice and Home Affairs. Arguing that biometric technologies are not yet ready for widespread implementation from both points of view: technical and societal, the experts invited were skeptical about the potential benefits of quick introduction of biometric technologies in European travel documents. Julian Ashbourn, who has advised the UK, US and Japanese governments on biometric technologies, warned that certain false assumptions were being made regarding the possibility of accurately identifying people through biometrics. He said, "[H]istory will show that certain assumptions involving biometrics will prove to be ill-founded". Adding that if biometric identification systems were poorly conceived states risked the alienation of citizens that a 25-year timeframe for implementation would be needed before biometrics had sufficient acceptance to be widely implemented.

A Finger for Europe [5] *(Biometrics)*

Following an agreement by European Union (EU) ministers, by the end of 2007, citizens will need to have their fingerprints scanned to get a passport. Indeed, Justice and Home Affairs Council of Ministers, meeting in Luxembourg October 25th and 26th, 2004 agreed to add digitized fingerprint scans to the microchips which will be embedded within passports produced by member states. EU countries had already agreed to add such chips for digitized photographs, following an agreement negotiated through the International Civil Aviation Organisation (ICAO) that all passports worldwide would include this feature. The UK retains an opt out from EU justice and home affairs measures, despite a move from consensus to qualified majority voting at the Luxembourg meeting. The Home Office could not immediately confirm its intention in this case.

Building a Pan-European Public Health Portal [6] *(Interoperability / e-Services)*

The creation of the European Union (EU) Public Health Portal (HEALTHGATE) is an initiative taken under the EU Public Health Programme 2003-2008, adopted by the European Parliament and the Council in September 2002. Its main objective is to provide citizens, patients, health professionals, policy makers, and other interested stakeholders with a single pan-European access point to data and information on public health from the Europeen Commission as well as from national and regional sources. A wealth of content will be made available through the portal, including a thematic presentation of Community activities related to public health. The public health work and activities carried out by Member States' administrations at national and regional/local level will be made accessible throughout Europe. The design and development of the portal and its functionalities are currently underway. A prototype should be available for testing in early 2005, and the fully functional version is due to go online by the end of that year.

---

[4] http://europa.eu.int/ida/en/document/3385/194
[5] http://www.kablenet.com/kd.nsf/Frontpage/0962C0C879BC953D80256F3A00318055?OpenDocument
[6] http://europa.eu.int/ida/jsps/documents/dsp_showPrinterDocument.jsp?docID=3346&lg=en

Defining an Enterprise Architecture for Pan-European e-Government Services [7]
(Interoperability / e-Services)

In order to start defining the "enterprise architecture" needed for pan-European e-government services, the Interchange of Data between Administrations (IDA) has launched a conceptual study that will determine the functionalities required at European level to facilitate the exchange of electronic information between administrations and to enable the emergence of cross-border e-government services. The study, based on an analysis of national e-government architectures, will start with a functional analysis of key requirements and will produce a description of the components of the future IT architecture for pan-European e-government services. To this end, it will address issues including reliable communications, messaging, identity management or semantic standardisation in a multi-organisational environment. Member States' experts are being consulted during the various phases of the study and industry will also be invited to comment via the IDA website. The first intermediate results of this study are expected in October 2004. The final step in preparing for the Interchange of Data between Administrations Business case (IDABC) will be to translate this European e-government enterprise architecture into a set of actions under the future programme, to set specific targets and dates and to assess budgetary requirements. This work will start in the final months of 2004 and conclude with the adoption of the first comprehensive Cross Border e-Government Services work programme in the summer of 2005.

IDA eLink: a Middleware Solution for Pan-European e-Government [8] *(Interoperability)*

The harmonisation of national legislations within the single market and the increasing need for cooperation and joint work between European Union (EU) Member States' administrations are facing considerable obstacles: different languages, administrative structures and infrastructures, legal contexts, processes and procedures, etc. By networking public administrations across Europe, Interchange of Data between Administrations (IDA) plays a key role in the process of removing such obstacles. One of its key projects in this respect is IDA eLink, which aims to define the specifications of a new communications middleware to be used by both EU and member states' administrations for the delivery of electronic public services at European level. A "middleware" can be defined as a software layer that mediates between distributed and heterogeneous applications or information systems while providing a set of generic services (messaging, directories, security, authentication, transaction, etc.) that can be used by multiple applications. IDA eLink is built up on the basis of the Government eLink (GeL) project developed in Sweden and of the German Online Services Computer Interface (OSCI).

Africa (Continent of)

No new item to report

South Africa

No new item to report

Argentina

No new item to report.

---

[7] http://europa.eu.int/ida/jsps/documents/dsp_showPrinterDocument.jsp?docID=3347&lg=en
[8] http://europa.eu.int/ida/jsps/documents/dsp_showPrinterDocument.jsp?docID=3348&lg=en

Austria

No new item to report.

Australia

Slow Move to e-Government [9] *(e-Gover nment)*

The latest survey of how Australians make first contact with queries to public agencies and departments has found that only 6 % do it online (5 % via a web site and only 1 % by e-mail), and this in spite the fact that about 70 % of Australians have Internet access. The survey found that the low use of online channels to government "can be ascribed to a lack of confidence in being provided with an immediate or timely response or the inability to use the technology". Avaya's product director, Asia-Pacific, Rosemary Durand, believes Australians are unwilling to make first contact with agencies online because they have tried and found it unsatisfactory. "[P]eople weren't using the lower-cost channels, probably because of bad experiences in the past and because they didn't trust them," Ms Durand said. However, the Commonwealth agency, responsible for promoting e-government, believes citizens use a mix of the communication channels when they need to contact their governments.

Govt Says No Plans for Australia Card [10] *(Smart Card)*

The Australian Government said there were no plans to introduce an Australia Card-style national identification system to tackle identity fraud. A spokesman for Justice Minister Chris Ellison said the government acknowledged identity crime was a growing problem and had passed laws earlier this year to outlaw the possession of credit card skimming equipment. He added "we have no plans to introduce any sort of Australia Card-style, national ID card. A bill went through at the end of August which specifically outlawed the possession and use of credit card skimming equipment and that's one of a few initiatives we've got underway on identity crime, working with industry, like the banking industry, to crack down on this problem."

Australia Losing Ground On e-Government [11] *(e-Government)*

Australia has lost ground in the latest study of global e-government by Brown University, going from fourth to seventh place in a ranking of countries' progress in putting services and information online. The study of global-e-government finds 21 percent of government agencies around the world are now offering online services, up from 16 percent in 2003, 12 percent in 2002, and eight percent in 2001. It names Taiwan and Singapore as the two outstanding performers, closely followed by Canada, and with Monaco and China both ahead of Australia in overall e-government performance. Australia's overall score of 36.7 is significantly below its 2003 score, of 41.5. And the country does even worse in the percentage of Web sites showing a security policy. The report found the countries most likely to show a visible security policy are Iraq (100 percent of its sites), Singapore (93 percent), the United States (67 percent), Taiwan (54 percent), Great Britain (41 percent), China (35 percent), Saint Lucia (25 percent), Belize (25 percent), Germany (23 percent), and Australia (23 percent). Likewise Australia falls behind Malta, the Bahamas, Saint Vincent, Togo, Dominica and Iraq, where 100 percent of Web sites sport a privacy policy, to tie with Singapore (97 percent) yet beat Canada (90 percent), and the United States (82 percent).

Biometrics: 'The Deal' at the Heart of Privacy Sacrifice [12] *(Privacy / Biometrics)*

---

[9]

http://canberra.yourguide.com.au/detail.asp?class=news&subclass=local&category=general%20news&story_id=338907&y=2004&m=9 CIOB News 2004-10-05

[10] http://www.theage.com.au/articles/2004/10/15/1097784020208.html?oneclick=true

[11] http://www.cio.com.au/index.php/id;187731422;fp;4;fpid;21

At the Biometrics conference held in Wellington on the dynamics of a relationship between sacrifice of privacy and gaining technologically assisted benefits, exaggeration, fears, gradual acceptance, trust and deal making were identified. Discussion ranged beyond biometrics to citizens' confidence in "joined-up government" and the shock of finding an Indian helpdesk apparently in possession of personal information entrusted to a US company's Australian branch. A rational person might find it very difficult to be opposed to the alleged privacy invasion of a biometric "when we've already accepted that we're safer with Security Camera Surveillance Equipment (CCTV) in our streets," says privacy lawyer John Edwards. On the other hand, a significant number of citizens had raised objections to their driver's license photographs being digitized. "At the heart of it is the deal," says Australian code of practice coordinator Terry Aulich "it's a matter of the privacy citizens are prepared to give up, including their perception of the possibility of subsequent abuse, in return for increased convenience in the transaction or some other kind of "reward".

ABS To Trial Online Stats Hub [13] *(Online Transactions)*

Next year, the Australian Bureau of Statistics (ABS) will begin trialing a new one-stop online data hub for requesting information from a range of government agencies. Australian statistician for the ABS, Dennis Trewin, said a demonstration version of the National Data Network, which is estimated to cost about $500,000 to $750,000 a year to build, was currently under development. At the moment, some government agencies collect their own statistics independent of the ABS. "[I]n a sense, we see our website as being the window to Australia's statistics rather than having to find out exactly where everything is. The hub would ensure statistics were consistent in the way that they were defined and classified." Mr. Trewin said.

Belgium

 No new item to report.

Bermuda

Bermuda Takes e-Government to the Next Stage [14] *(PKI / Online Transactions)*

The Government of Bermuda has retained QuoVadis Limited to provide digital identity services as part of its ongoing e-Government Portal Project. In the first phase of the project, Bermuda introduced a central portal uniting the informational websites of more than sixty government agencies. Under the agreement, QuoVadis will operate a digital certificate authority for the Government under the provisions of applicable local laws and regulation. Digital certificates are a form of non-forgeable electronic ID that may be used to identify online users and resources, to create legally binding electronic signatures, and to encrypt data for privacy.   QuoVadis is the first Authorised Certification Service Provider under Bermuda's *Electronic Transactions Act 1999*. This regulatory standard synthesizes elements of international security standards including BS7799, WebTrust for Certification Authorities, and the European Electronic Signature Standards Initiative. The QuoVadis Trust/Link operation is a global certification authority with users in more than 20 countries.

Bosnia-Herzegovina

No new item to report.

---

[12] http://www.cio.com.au/index.php/id;690486693;fp;4;fpid;21
[13] http://australianit.news.com.au/articles/0,7204,11214218%5E15306%5E%5Enbv%5E,00.html
[14] http://www.quovadis.bm/corporate/article.asp?newsid=78

Brazil

No new item to report.

Brunei

No new item to report.

Bulgaria

No new item to report.

Canada

US.Patriot Act Raises Canadian Privacy Fears [15] (Privacy)

A Canadian province has opened a fractious debate over whether a US anti-terrorism law invades its citizens' privacy, a move that could affect how American firms do business with Canada. British Columbia's top privacy official is probing complaints that the *US Patriot Act* allows the FBI to use US firms, and their foreign subsidiaries to gain access to Canadians' medical and financial records. The law gives the FBI broad powers to collect information from companies without the subjects of the probe knowing they are under investigation. Civil libertarians in both countries say Canada must take steps to protect its citizens' private information, but US security officials and firms that collect and store personal data say the fears are overblown. British Columbia is one of the first foreign jurisdictions to examine the *Patriot Act*'s implications outside US borders, and the study has drawn submissions from across Canada, the United States and Europe.

Online Banking Pays Dividends for Canadians [16] *(Online Transactions)*

In August 2004, 11.8 million Canadians, or 64 percent of all Internet users, visited sites in the Banking category. This is an impressive jump from the 8.7 million Canadians that visited a banking site in May 2003; an increase of over 36 percent in the past 15 months. To this regard, Brent Lowe-Bernie, president of comScore Media Metrix Canada said, "the days of standing in line at your financial institutions to complete a simple banking transaction are over. The Internet has revolutionized the way that Canadians bank and access their financial information. The web has also drastically changed the way that we buy and sell stocks and bonds, apply for credit cards, pay bills, and much more." An analysis of growth in the banking category since last year found significant strides among nearly every major entity.

Cabinet OKs Biometric Data on Passports: Critics Raise Privacy, Liberties Concerns Over Use of Facial Recognition System [17] *(Biometrics / Privacy)*

The federal government has approved the contentious use of biometric facial data on Canadian passports. The cabinet passed an order allowing the Passport Office to compile facial recognition data from photographs submitted with a passport application. The photos can be converted into a "biometric template" of a person's face and stored on an electronic chip in a passport booklet or

---

[15] http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=6370340 CIOB News 2004-10-01
[16] http://www.newswire.ca/en/releases/archive/October2004/04/c6675.html
[17] http://intranet/tbnews/stories/2004/20041006i0005.htm

added to database. The Passport Office is already planning to add digitized versions of passport photographs to its new "ePassports," But the addition of biometric data would make the process more elaborate and, critics say, raise new privacy and civil liberties concerns. Under the ePassport system in development, immigration officers would visually compare the digital photograph stored on the passport to the traveler. But under a biometric system, the traveler would be scanned by a camera, with the facial data compared electronically to the information encoded on the passport chip.

Ministry Loses Track of $587M Due To Errors in EI Payouts: Error Rate Almost 5%, Would Be Reduced With New Online Program, Internal Report Urges [18] (*e-Government*)

In a memo sent to Treasury Board President Reg Alcock, Treasury Board Secretary Jim Judd said the current rate of error in the Employment Insurance Program (EI) is running at about 5% of a total of $12.6 billion in payout benefits. "[I]n dollar terms, a 4.66% error rate represents a dollar value of $587 million in overpayments and underpayments combined," Mr. Judd suggests that the Department of Human Resources and Skills Development (HRSD) could potentially reduce its error rate to below 2% by 2007-2008 by bringing in "a fully mature automated EI adjudication process." He encourages the use of the secure channel since its increased use by departments will result in savings "through the migration of some of the government's existing programs." For example, HRSD's EI related (government online) applications could realize approximately $200 million per year in savings by 2007 through reduced operating costs and lower error rates," Mr. Judd wrote in the memo. He also notes Human Resources estimates that within its EI program, it could also pick up annual savings of about $40 million once all of its government online projects are fully functional. However, this estimate will be refined over time depending upon the take-up rates of electronic services and the back-end efficiencies due to automation, which are linked to electronic service take-up rates."

Privacy Law Perversely Protects Those Who Break It [19] *(Privacy)*

With Canada's national privacy law now nearly four years old, the Canadian privacy community has begun to assess the law's strengths and weaknesses. A recent ruling from the Privacy Commissioner of Canada's office involving an inadvertent e-mail disclosure provides a good case study for why the law's fundamental principles remain sound but that enforcement - both in terms of the Commissioner's approach and in limitations found in the law - remain a persistent shortcoming. The case involved an unnamed Canadian loyalty program that mistakenly revealed the e-mail addresses of 618 people when it sent an e-mail message about a contest. The error was a relatively common one - rather than hiding the names in the e-mail message, the e-mail operator placed all the addresses in the "to" field. The company quickly sent an apology to the affected parties, but eleven recipients still chose to launch a complaint with the federal privacy commissioner. The assistant privacy commissioner, who assumed responsibility for the complaint, concluded that it was "well founded." Canada's privacy legislation requires consent before the disclosure of personal information and it also compels organizations to provide adequate security safeguards to protect the personal information they collect. In this particular case, the e-mail addresses constituted such personal information. Despite the existence of a privacy policy and some security safeguards, the loyalty program failed to comply with both the disclosure and security principles and thus ran afoul of the law.

Government Must Provide 'Seamless' Experience For Online Service: Official [20] *(e-Government)*

---

[18] http://intranet/tbnews/stories/2004/20041012i0004.htm CIOB News 2004-10-12

[19]

http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&call_pageid=971358637177&c=Article&cid=1098010864947

[20] http://intranet/tbnews/stories/2004/20041019i0001.htm CIOB News 2004-10-19

On the first day of the Government Technology Exhibition and Conference (GTEC), Helen McDonald, the Treasury Board's acting chief information officer says the federal government must learn to operate as an integrated enterprise with a unified service face as it wraps up its ambitious project to transfer services online by 2005, "citizens and businesses are looking for a seamless service experience. They don't want to know who operates what service. They want us to integrate those services for them." The government has invested $880 million since 2000 in Government On-line, which aims to transfer most federal services online by next year. That has led to the creation of a centralized web portal, www.canada.gc.ca , which offers three service "gateways" for citizens and residents, businesses and non-Canadians. The government now delivers about 130 of its most commonly used services online, and has developed a security platform for online services, called Secure Channel. Canada who ranks first among 22 countries in overall e-government maturity, according to consulting firm Accenture falls to fourth in terms of users accessing e-government websites, suggesting clients have been slow to take up online services. One reason may be the dizzying number of entry points for clients, who must navigate over 1,600 points of service across nearly 30 ministries. To make its services more accessible, the government must create a common interface for clients, integrate business functions and develop common performance benchmarks, said Ms. McDonald. For example, sharing half of all information-technology services would save the government $300 million to $400 million a year, she added. The government currently shares only 5% of its Information technology (IT) services. Various departments have rolled out online initiatives as part of the Government On-Line (GoL) project.

Feds Eye Internet Obstacle [21] *(e-Government)*

David Marshall, deputy minister of Public Works, said during his opening remarks at GTEC Week that the federal government is looking to use technology to change the way it does business by putting the needs of citizens first. However, the biggest obstacle to bringing government online and allowing citizens to access and interact with government more easily isn't technology, "technology was going to be the easy part. The bigger challenge is the need to re-think how government operates," he said.

Public Sector Experts Urge Customized GOL Approach [22] *(e-Government)*

According to Dan Danagher, Director of Internet and service delivery innovation at Foreign Affairs Canada, a client-centric approach to online government makes a measurable difference in the quality of service to citizens, but the focus can't solely be on the client, "client-centric service is almost the grape Kool-Aid of the day," In addition to a client need, there has to be a public policy purpose for delivering a service online, he said "we have to have a shared view" of what those policy purposes are. The "we" he spoke of was the representatives of the three client groups of Canada's Government On-Line: Canadians and residents, non-Canadians and Canadian businesses. Peter Oberle, director of service integration with the Treasury Board Secretariat added "we need visions that are customized to the three client groups," Canadians don't just want services online, they want better-quality, more seamless services, a sophisticated Canadian "brand" to represent them to others and responsiveness when they are abroad.

Health Canada Launches First Electronic Pesticide Regulatory System [23] *(PKI / e-Services)*

Health Canada's Pest Management Regulatory Agency (PMRA) announced the development of the world's first web-based service for conducting pesticide regulatory transactions. The PMRA Electronic Regulatory System, dubbed e-PRS, offers a new approach to information management and will enable the PMRA to continue the evolution from a completely paper-based system to a sophisticated system using information technology. The electronic system will also strengthen the PMRA's ability to process, review and report to the public on pesticide information as required under the new *Pest Control Products Act*, which will come into force as soon as possible in 2005.

[21] http://www.canoe.ca/NewsStand/OttawaSun/Business/2004/10/19/675527.html CIOB News 2004-10-19
[22] http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=57037
[23] http://www.pmra-arla.gc.ca/english/highlights/20041020-e.html CIOB News 2004-10-19

The electronic system fulfills the PMRA's commitment to deliver on-line transactional services to stakeholders by 2005, under Canada's Government On-Line initiative.

US Patriot Act's Reach Is A Concern For Canadians [24] *(Privacy)*

A recent series of events has led Canadians to wonder how much of their personal information stored in computer databases is vulnerable to the FBI and CIA eyes, and who knows who else? The source of worry is the *Patriot Act*, that aims "to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes." The US Congress is now debating whether to expand or loosen the Act's far-reaching empowerment of law enforcement agencies. The *Patriot Act* lets US agencies obtain access to any and all "tangible things" from any individual or organization in order to investigate "international terrorism or clandestine intelligence activities." [T]he access order must be approved by a special court or magistrate, which does so in secret, while the order does not disclose the purpose of the investigation. Those served by the order must not disclose it, or risk fine or imprisonment. The Act provides some limited overriding protections, like free speech under the US Constitution. But these protections apply only to US residents. Canada, allows specific defined exceptions for police investigations, generally ambles in the opposite direction. Harmonized federal and provincial privacy legislation provides detailed guidelines and follow-up mechanisms to ensure that firms and government agencies obtain consent before collecting, using or disclosing someone's personal information

Canadians' Privacy at Risk, Masse says [25] (Privacy)

Windsor West Member of Parliament (MP) Brian Masse told the House of Commons that Windsor Star has cost Canadian taxpayers an extra $5 million to protect their private census data, which is being handled by an American company. The government awarded the census contract to Lockheed Martin last year, and because Lockheed Martin is an American company, the information it handles is vulnerable according to the *Patriot Act* that allows agencies such as the FBI and CIA access to personal records. To this regard, Masse says, "the processing of private information is increasingly being outsourced, but the government hasn't acted to protect that information," Banks and other private companies that outsource work to US companies also make information such as credit card records vulnerable, he says. "How many Canadians are being affected?" Masse asked the government. "Has he (Prime Minister Paul Martin) raised this with (US Homeland Security secretary Tom Ridge) and US counterparts? and what other nations could have access to Canadians' private information?" Treasury Board president Reg Alcock acknowledged that it's an important question and said he has been assured by privacy commissioner Jennifer Stoddart that Canada has the authority to protect its information and is reviewing its public sector contracts. This said, MP Keith Martin last spring questioned the government's decision to give the work to Lockheed Martin, calling it "strange and undesirable" in a letter to chief statistician of Canada Ivan Fellegi. "This information should be highly protected," Martin wrote, and added, "This census should be done in-house at the very least, and at the worst, contracted out to a Canadian company." The government has said that Lockheed Martin will have no access to completed 2006 census returns. The company will only provide scanning hardware and software.

Ottawa Approves BorderWare System [26] (*e-Services*)

The Communications Security Establishment (CSE), the Canadian Government's IT security watchdog, has approved BorderWare's MXtreme Mail Firewall for use by the Government of Canada. The system ensures that e-mail will not get tagged as spam, consumed by virus attacks or lost by a system malfunction. BorderWare Technologies Inc., a provider of messaging security systems, has confirmed that MXtreme has been added to the Information Technology Security Product Pre-qualification Program (IPPP) list of approved products for the Government of Canada. The CSE's endorsement is based on the recent awarding of a Common Criteria security

---

[24] http://intranet/tbnews/stories/2004/20041014g0321.htm CIOB News 2004-10-20
[25] http://intranet/tbnews/stories/2004/20041029i1647.htm CIOB News 2004-10-29
[26] http://www.theglobeandmail.com/servlet/story/RTGAM.20041019.gtborder1019/BNStory/Technology

certification of the MXtreme product at Evaluation Assurance Level 4+ (CC EAL4+). The Common Criteria is a set of international standards for evaluating the security of IT products. The standard not only grades products on their security and reliability, but also evaluates an IT vendor's development and support processes.

Alberta: Enhanced Protection for Albertans a Highlight for Government Services in 2003-04 [27] *(Authentication / e-Services)*

More consumer protection, better security against identity theft and new privacy legislation stood out as key achievements for Alberta Government Services in its work for Albertans in 2003-04, as highlighted in the ministry's annual report. Government Services Minister David Coutts said "Albertans see privacy, identity theft and fraud as critical issues for this ministry to address, and some of our greatest successes over the past year have come from our response to those priorities. We are also continuing to lead two major service improvement initiatives for the Alberta government: Service Alberta, through which we are ensuring Albertans' interactions with government are as convenient as possible, and the Alberta Corporate Service Centre, through which government is achieving further efficiencies through streamlining." In 2003-04, Government Services investigated nearly 2,000 consumer complaints and returned more than $780,000 in restitution to victims who lost money to fraudulent businesses. The ministry also laid charges that resulted in some of the most severe penalties ever imposed for marketplace misconduct in Canada.

British Columbia: Introduces Legislation to Hobble *US Patriot Act*: Privacy Law Designed to Prevent Disclosure of Personal Information [28] *(Privacy)*

The British Columbia government brought in new legislation designed to protect British Columbians' personal information from the US *Patriot Act*. The amendments to the *Freedom of Information and Protection of Privacy Act* prohibit companies from storing or disclosing sensitive information outside Canada and require them to report any foreign demands for unauthorized disclosures of personal information. The amendments also protect whistle blowers that report such demands, and call for fines of up to $500,000 for companies and $2,000 for individuals that break the rules. Government Management Services Minister Joyce Murray said the changes "really toughen up the provisions protecting personal information." In the meantime, New Democratic Party (NDP) house leader Joy MacPhail said it's particularly troubling that the BC law presumes to trump a US law, which forbids companies from disclosing the fact that they've been asked to turn over personal information. He arguing "that's the fundamental question that we're facing. We have companies that this government is now using that are subject to American law, and I guess they're being put in a situation where they either break the law in British Columbia or they break the law in the United States. And that's extremely troubling and doesn't answer any of the concerns of British Columbians."

British Columbia: Personal Information Law Takes Precedence [29] *(Privacy)*

Management Services Minister Joyce Murray and Information and Privacy Commissioner David Loukidelis said that Federal government found substantial similarities between the British Columbia *Personal Information Protection Act* (PIPA) and federal legislation. This finding clarified that the provincial law rather than the federal law governs the collection, use and disclosure of personal information by private organizations in British Columbia. When the federal government proposed the *Personal Information Protection and Electronic Documents Act* (PIPEDA), it offered to exempt organizations in the provinces that passed equivalent legislation. The provincial government responded to broad concerns from across the province and developed the PIPA, passed in 2003, that ensures BC's businesses and non-profit organizations operate under a workable, made in BC law. To this regard, Murray said "I am pleased that British Columbia is once again seen as a leader

---

[27] http://www.gov.ab.ca/acn/200409/17130779645FB-E5B7-4FAF-88FF2012D29C9061.html
[28] http://intranet/tbnews/stories/2004/20041008i0023.htm CIOB News 2004-10-08
[29] http://www2.news.gov.bc.ca/nrm_news_releases/2004MSER0022-000895.htm CIOB News 2004-10-08

in privacy protection. PIPA complements our recent improvements to the *Freedom of Information and Protection of Privacy Act* and was developed to meet the particular needs of British Columbians. Privacy Commissioner Loukidelis. Although federal privacy law still affects federally regulated organizations in BC, PIPA is now the central private sector privacy law in the province. I welcome this clarity around the role of PIPA's clear, common sense simple privacy rules."

British Columbia: Businesses Benefit From Innovative Online services [30] *(e-Services)*

National Revenue Minister John McCallum and John Les, BC Minister of Small Business and Economic Development, announced that in partnership with the Canada Revenue Agency and the Workers' Compensation Board, the province launched the OneStop Business Registry, an improved e-government service. McCallum said "this integrated online service is an excellent example of how federal, provincial and municipal partners are working together to create a more streamlined business environment in British Columbia. " Mr. Lee added "small business owners told us they needed a more efficient way to interact with public agencies. As part of our commitment to revitalize the economy, we modernized BC's business legislation to enable these kinds of innovative e-government services." The OneStop Business Registry lets people starting, moving or expanding a business deal with a wide range of public agencies at one website as well as a single number that identify the business to various levels of government, avoiding duplication and speeding up service. "This OneStop service is particularly valuable to small businesses which are the backbone of our economy, accounting for 98 per cent of BC business and employing nearly one million British Columbians," said Les.

New Brunswick: Biometric IDs Are in The Cards [31] *(Biometrics)*

A biometric security system will be arriving at the Moncton International airport before next fall, said Renee Fairweather, spokeswoman for the Canadian Air Transport Security Authority. Indeed, the federal government announced they had begun implementing a biometrics security system for restricted access areas in airports across the country. Under the airport system, an employee with a restricted area access card will have either their fingerprints or iris scanned by a biometric reader when entering a restricted area. The card would hold a chip with a number that is connected to the unique algorithm produced by a fingerprint or iris scan. Acadie-Bathurst New Democratic Party (NDP) Member of Parliament (MP) Yvon Godin said he worries that the government is preparing Canadians for the eventual implementation of national ID cards.

Ontario: McGuinty Government Protecting Personal Health Information [32] *(Privacy)*

George Smitherman, Health and Long-Term Care Minister, announced that the McGuinty government will strengthen protection of Ontarians' personal health information when *the Personal Health Information Protection Act, 2004* becomes law November 1st. He said, "we will have the strongest and clearest rules ever in this province on how personal health records are to be used and protected. The people of Ontario will know that their health information is protected, and they will have better access to their private records." Ontario residents will have the right to give consent to how their personal information is collected, used and shared. They will also have the right to request access to their personal records from health care providers and to correct faulty or incomplete information in their files. In this connection, Ann Cavoukian, Information and Privacy Commissioner said, "the act will provide essential privacy protection for the most sensitive personal information of Ontarians. I congratulate the government for making this much-needed legislation a reality."

---

[30] http://www2.news.gov.bc.ca/nrm_news_releases/2004FIN0033-000830.htm
[31] http://intranet/tbnews/stories/2004/20041025c0566.htm CIOB News 2004-10-22
[32] http://ogov.newswire.ca/ontario/GPOE/2004/10/26/c4629.html?lmatch=&lang=_e.html

Québec : Services gouvernementaux en ligne; Les Québécois frileux devant la divulgation de certains renseignements [33] **(Privacy)**

Le Centre Francophone d'Informatisation des Organisations (CEFRIO) a rendu publics les résultats de la seconde édition de l'enquête NetGouv 2004 portant sur les services gouvernementaux en ligne au Québec. Le sondage mené, du 16 avril au 24 mai dernier, auprès de 3000 citoyens et 1000 entreprises révèle que 54 % des adultes québécois ont accès à Internet à la maison et que plus de la moitié d'entre eux navigue à partir d'une connexion haute vitesse. Quant aux résultats de l'enquête, ils sont comme suit. Les Québécois sont "à l'aise" avec le fait que les ministères et organismes du gouvernement du Québec puissent se partager entre eux des informations contenant leur nom, leur date de naissance et leur adresse dans le but d'établir un code d'identification unique leur permettant d'accéder à tous les services transactionnels offerts par l'État. Toutefois, ils sont plus frileux à l'égard de la circulation dans l'univers gouvernemental de leur numéro de permis de conduire, d'assurance-maladie et d'assurance sociale. Par rapport aux informations biométriques et médicales et aux renseignements sur leur revenu, les Québécois préfèrent, dans une proportion de plus de 55 %, que les ministères et organismes chargés de traiter ces données ne les fassent pas circuler.

Québec : Big Brother inc.; Devons-nous fournir nos papiers d'identité aux courtiers? [34]
(Privacy, e-Commerce)

Depuis le 11 septembre, et pour essayer de contrer le financement des activités terroristes, les gouvernements des pays industrialisés ont, à la demande de la Maison-Blanche, uni leurs efforts pour adopter la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, laquelle est entrée en vigueur le 12 juin 2002. Cette loi oblige les courtiers en valeurs mobilières à vérifier l'identité de leurs clients, tant les particuliers que les personnes morales, les sociétés de personnes et autres entités d'exploitation d'entreprises. Pour ce faire, la vérification de l'identité des clients des maisons de courtage doit se faire par l'entremise soit d'un certificat de naissance, du permis de conduire, du passeport, de la carte d'assurance maladie du Québec. Une telle demande de pièces d'identité contrevient à la *Loi sur la protection des renseignements personnels* dans le secteur privé.

Saskatchewan: Keep this SIN a Secret [35] *(Authentication / Privacy)*

Canadians should know that they are not obliged to reveal their Social Insurance Number (SIN) just because a business asks for it. A computer was stolen at a Regina dentist's office that contains such information as names, addresses, phone numbers, birth dates and Saskatchewan health card numbers. It also contained the SIN of some patients whose claims are submitted electronically to insurance companies. Such information can be used for identity theft. As a result, the dentist has undertaken to warn anyone who has been a patient of her office in the last 10 years that their private information could be in the hands of the thieves. She's also warning them to keep an eye on their bank and credit card statements, even though the computer held no banking or credit card information. Saskatchewan Privacy and Information Commissioner Gary Dickson said what is most disturbing about the case is that it shows some private health insurance firms are using social insurance numbers to identify people. He says they should be creating unique identifying numbers for their clients rather than using their SIN, because the SIN can be used to gather data that will allow access to bank accounts or credit. Banks are supposed to "make a reasonable effort to obtain" the SIN of anyone who opens an interest-bearing account for income tax reporting purposes. Banks will open accounts if someone refuses to provide their SIN, but under the *Income Tax Act*, the person can be fined $100 for each refusal.

---

[33] http://intranet/tbnews/stories/2004/20041001c0653.htm CIOB News 2004-10-21
[34] http://intranet/tbnews/stories/2004/20041024c0397.htm CIOB News 2004-10-21
[35] http://intranet/tbnews/stories/2004/20041024i0282.htm CIOB News 2004-10-21

Chile

No new item to report.

China

No new item to report

Croatia

e-Government in Croatia [36] *(e-Government)*

The Croatian e-government strategy is set in the e-Croatia 2007 Programme, based on the principles and priorities outlined in the *e*Europe 2005 Action Plan. The e-Croatia strategy sets the objective of providing online access to key services in public administration, health, education and the justice system by 2007. To drive the implementation of this e-strategy, a Central Government Office for e-Croatia was established in December 2003, headed by a cabinet-level State Secretary directly responsible to the Prime Minister. The primary task of this new body is to reinforce strategic planning and develop stronger coordination between government departments for the use and the deployment of computer systems. Insufficient coordination has been identified as one of the main causes of the country's relatively slow e-government progress over the past years, especially as e-communications and interoperability remain constrained by the heterogeneity of systems and software in use across the government.

Denmark

No new item to report.

Dubai

Dubai e-Government Launches New Payments Portal [37] *(e-Government)*

A new application architecture designed by Dubai e-Government running on a new technology platform will help Dubai achieve its vision to "ease the lives of people and businesses interacting with the Government." So far, the Dubai e-Government portal hosts 14 Ministries including the Department of Health and Medical Services (DOHMS), Dubai Development Board (DDB), Land Department (LD), Dubai Civil Defense (DCD), Dubai Women's Association (DWA), and others. The portals, their architecture, the 'look and feel', and all web interfaces were designed and developed by Dubai e-Government and rolled out across the network and security infrastructure implemented by eHosting Data Fort (EHDF), a regional provider of managed hosting and security services.

Estonia

Estonia Is Central Europe's e-Government Champion, Says New Study [38] *(e-Government)*

---

[36] http://europa.eu.int/ida/jsps/documents/dsp_showPrinterDocument.jsp?docID=3327&lg=en
[37] http://www.pstm.net/article/index.php?articleid=388
[38] http://europa.eu.int/ida/en/document/3314/194

According to a report released by the Economist Intelligence Unit (EIU) September 28th, 2004 and sponsored by Oracle, e-Government in Central Europe, Estonia, Czech Republic and Slovenia have gone beyond e-government "window dressing" and compare favorably with the rest of the European Union. Coherent strategies and precise action plans, clear and centralized responsibility for implementation and the operation of modern digital transaction laws set the e-Government leaders apart from the rest of the region. However, poor infrastructure remains a massive impediment to the realization of the e-Government goals of most Central European Governments. Based on a comprehensive model comprising 35 qualitative and quantitative indicators, EIU researchers produced a set of e-Government rankings covering ten new EU members and candidate countries from Central Europe, as well as Turkey. The ranking model generates scores for each of the countries across seven inter-related sets of criteria, such as connectivity, technology infrastructure, relevant business and legal environment, and the development of online services for citizens and businesses.

Finland

No new item to report.

France

79% of French Internet Users Would Welcome Online Voting [39] *(e-Government)*

According to the survey, carried out for the 5th Worldwide Forum on Electronic Democracy held September 30th, 2004, 79% of French Internet users are in favor of Internet voting. Some of the most important results of the survey aiming at identifying the perceived impact of Internet on politics and democracy, include the following: 92% of survey respondents believed the Internet would allow citizens to increasingly express their political views. 89% believed the Internet was a good tool for obtaining information on candidates and their programmes. 86% of respondents believed France was late in terms of e-democracy development. 74% would like to communicate with their representatives via the Internet. 71% believed the Internet could lead to a better democracy. 70% believed the Internet will help fight abstention. 56% believed the Internet could contribute to more transparency in politics.

Secure Exchange Infrastructure For e-Government Presented in France [40] *(PKI / e-Government)*

Fournisseur d'Accès Sécurisé Transactionnel (FAST), or 'Secured Transactional Access Provider' represents a major step for the digitization of administrative processes, allowing public bodies to securely exchange authenticated electronic documents and acts, was officially launched September 30th, 2004. FAST consists in an exchange platform for electronic delivery and receipt of documents with legal value. It has as a strategic goal to enable a complete dematerialization of government communications and document exchange, as well as the use of electronic signatures, features a time-stamp function, and encryption of data exchange

French Government Launches Consultation On e-Signature Framework Policy [41] *(PKI)*

The second version of the Politique de Référencement Intersectorielle de sécurité (PRIS), or Intersectoral Referencing Security Policy is designed to provide a clear framework for the use of electronic signatures in e-government services. Initially published in October 2003 by the Agency of Development and Electronic Administration (ADAE), the PRIS provides certification authorities for public and private organizations that delivering e-services with a clear framework concerning the conditions under which digital certificates being acceptable for public administrations. The policy framework is based on the principle that certification services are provided by private players

---

[39] http://europa.eu.int/ida/en/document/3315/194
[40] http://europa.eu.int/ida/en/document/3357/194
[41] http://europa.eu.int/ida/en/document/3379/194

competing in a market where users are free to choose their suppliers. As for the framework is a comprehensive document that covers the whole "trust services" area, including confidentiality, identification and authentication, electronic signatures, time stamping, and archiving. It identifies different security levels to be applied to different trust services, and determines mandatory technical, legal and organizational specifications for the relevant service providers and product vendors. Version 2.0 of the framework, which is now being submitted to public consultation, should be published before end 2004.

Germany

Take-Up of Electronic Signatures Remains Low in Germany [42] *(Digital Signatures)*

According to a study on "Electronic signatures in e-government" released by Mummert Consulting October 1st, 2004, the take up of digital signatures by German municipalities, citizens and businesses remains very low, making paperless government a distant vision. Though, the study found that so far, only 8% of German municipalities are using electronic signatures, while both citizens and businesses are failing to take advantage of the limited number of e-government services for which documents may be signed electronically. Furthermore, the study points out that the low take-up of digital signatures by citizens and businesses, combined to the limited offer of e-government services allowing users to sign electronically, seems to be creating a vicious circle that prevents the widespread use of this fundamental e-government enabler. German citizens have to deal with public authorities on average twice a year. Because it costs about EUR 30 to be able to sign electronically, in the first year the average citizen would pay EUR 15 per transaction. The relatively high cost for the user may thus be a deterrent to the adoption of e-signatures, a point of view shared by most local authorities. According to the study, 75% of municipalities believe that citizens should be provided with digital signatures free of charge in order to overcome the price barrier.

Hong Kong

Promoting e-Govt Channels in Hong Kong [43] *(e-Government)*

Speaking at a conference in Singapore, Betty Fung, deputy CIO of Hong Kong, has made the case for penalising citizens who use more expensive offline channels to access government services. She said that the Hong Kong government's strategy was to use incentives and penalties to encourage residents to use more cost-effective service channels. Fung pointed out the example of the Government Electronic Trading Services (GETS) initiative that covered the submission of common trade-related documents to government. In fact, since 2001 there has been mandatory electronic submission of documentation, and the service counters were closed down in order to push companies to move the document submission process online. In doing so, she is expecting a substantially reduce in the department operating costs.

Hungary

Attaining Ambitious e-Government Goals in Hungary [44] *(Authentication)*

The formulation and the coordination of the implementation of Hungary's e-government strategy is the responsibility of the Electronic Government Centre within the Prime Minister's Office. This strategy, presented in 2002, is based on the vision of a service-providing State. By contributing to making public services customer-focused, e-government acts an important catalyst for the modernisation of public administrations. The primary focus of the strategy is the delivery of electronic services to citizens and businesses. In addition to providing information, the Government

[42] http://europa.eu.int/ida/en/document/3358/194
[43] http://www.pstm.net/article/index.php?articleid=409
[44] http://europa.eu.int/ida/jsps/documents/dsp_showPrinterDocument.jsp?docID=3342&lg=en

Portal is intended to act as a single entry point to interactive and transactional services. Currently, the legislation allows electronically delivery only when user's identity authentication is not required. However, a Bill has been presented to Parliament, which will make it possible for all public services to be provided electronically, with the same legal force as with traditional methods. The electronic service gateway will handle user authentication based on a number of identification methods: an electronic ID card, a mobile phone-based electronic ID, a certified electronic signature or a special ID and password obtained from the Registry Office and available to every citizen.

Smart cards have potential to become Big Brother's little helper, says inventor [45] *(Smart Card / Privacy / Encryption)*

Hong Kong is now part of the People's Republic of China, and it's replacing its national identity cards with multi-application, biometric-based smart cards. The Smart Identity Card System (SMARTICS) is one of the most ambitious projects of its kind in the world. When complete, seven million Hong Kong residents will use a smart ID card for mandatory government functions and optional business functions (through e-Cert). The credit card-sized piece of plastic will include personal data such as name, birth date, gender, residential status and photo, as well as a digital template of both thumbprints. A driver's license application will be introduced in 2006. The data is stored in a microchip and protected by encryption. While some believe Hong Kong is taking the lead in smart card implementation, others, namely civil libertarians warn that the use of such technology can backfire, causing human rights abuses by allowing governments to better control citizens.

India

No new item to report.

Ireland

 No new item to report.

Israel

No new item to report.

Italy

No new item to report.

India

No new item to report.

Japan

 No new item to report.

---

[45] http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=56991&adBanner=Security

Kenya

No new item to report.

Korea

No new item to report.

Malaysia

No new item to report.

Malta

 No new item to report.

Mexico

No new item to report.

Netherlands (the)

No new item to report.

New Zealand

Privacy Impact Assessment - April 2004 Update [46] *(Authentication / Privacy)*

A Privacy Impact Assessment (PIA) is an evaluation of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated. In this respect, in April 2002, the Cabinet formally recognized the need for the online E-authentication initiative to give full consideration to privacy concerns and issues. March 2003, feedback from public's consultation demonstrated a strong desire for security and privacy to feature prominently in any model that was adopted for implementation. This fact was reinforced by the conclusions of a Preliminary PIA that was completed in parallel by the E-government Unit. Further than influencing the identification of a preferred model for implementation, the debate is leading Cabinet's direction on giving precedence to security and privacy, and how a formal PIA should be undertaken.

29 Per Cent of New Zealanders Used e-Govt in Past Year [47] *(e-Government)*

A survey of New Zealanders conducted by Auckland University shows 29 per cent had communicated with government agencies by email or via the web during the past year, versus 41 per cent who did so by phone and 16 per cent in person. About half of those surveyed couldn't think of additional government information or services they wanted online. Most of the remainder asked

---

[46] http://www.e-government.govt.nz/authentication/privacy.asp CIOB News 2004-10-12
[47] http://www.pstm.net/article/index.php?articleid=385

for services that are already available over the web, such as Inland Revenue forms and information on job opportunities held by Work and Income Department.

Norway

New Ministry of Modernisation to Step-Up e-Government Efforts in Norway [48] *(e-Government)*

The Ministry of Modernisation, formally established October 1st, 2004, is meant to be a spearhead for the Norwegian Government's efforts to modernise the public sector. Among other things, it will have responsibility for IT policy and the e-government drive therefore, responsible for the Government's administration and personnel policy, competition policy, national policy for development and coordination of the use of information technology and measures to make government more efficient and service-oriented. The Ministry has 200 employees and five departments, one of which is in charge of IT policy. It oversees a number of public bodies, including the Data Inspectorate that is in charge of enforcing data protection legislation, and Statskonsult, a state-owned limited company providing research, consultancy and advisory services on all aspects of public management, including the use of Information Communication Technology (ICT) in public administrations. It will also be responsible for the operation and management of the country's e-government portal, Norge.no, which as of January 1st, 2005 will become a public agency subordinate to the Ministry.

Pakistan

No new item to report.

Poland
No new item to report.

Portugal

No new item to report.

Russia

No new item to report.

Singapore

Singapore Adds Online Access Channel for e-Govt Password [49] *(Authentication / e-Government)*

Singaporean residents can request or reset their unique SingPass password online. The password that provides authentication for 136 e-government services was launched in March 2003 allowing users to access government e-services at www.eCitizen.gov.sg, and various government websites. Previously the password could only be applied for or reset at Community Development Council (CDCs) offices, selected Community Centres or at Central Provident Fund (CPF) branches. Now

---

[48] http://europa.eu.int/ida/en/document/3408/194
[49] http://www.pstm.net/article/index.php?articleid=338

users can apply for a new password online, which will then be mailed directly to the applicant within a week of the request. This service is available to Singaporeans, employment and dependant pass holders. Loh Khum Yean, Deputy Secretary at Ministry of Finance said "[W]e are pleased that so many e-service users are now using SingPass, and our goal is to make government e-services intuitive and easy to use. The ease with which users can apply for their SingPass online makes it even simpler and more convenient for the public to transact electronically with the government."

Singapore Shares Smart Card Experience [50] *(Smart Cards / Biometrics)*

From first trials in 1996, the Singapore government's implementation of smart card technology to manage national security and ease the flow of travelers across the country's borders have come a long way. According to Mr. Wong Kan Seng, the Home Affairs Minister the initial trial used biometrics to automate immigration clearance for frequent foot travelers at the Woodlands Checkpoint. These early efforts later developed in 1997 into a permanent system called the Immigration Automated Clearance System (IACS) that is currently deployed at all checkpoints and clears 40,000 transactions daily at an average clearance time under 12 seconds per transaction. To this regard, Mr. Wong said "we also tested using iris biometric recognition technology for 3000 long-term pass holders who travel daily to and from Singapore on motorcycles. The reliability results have been very positive, and we will be hosting inter-operability testing for e-passports in Singapore during the entire month of November."

Government Revamps Online Services [51] *(Online Transactions / Authentication)*

The Government has revamped its online portal services to bring about a unified gateway to all Government services and information online. Acting Second Minister for Finance, Raymond Lim, said the revamp puts the user as the focus of attention. In doing so, the e-Government Action Plan-II that is about to bring improvements in e-Government activities, wants also to delight customers and connect citizens. He cited the Online Business Licensing Service (OBLS), where applying for licenses is now a breeze. An applicant now only needs to complete one integrated form and perform a single payment for many licenses, instead of a series of forms and separate payments.

Slovak Republic

New Slovak Driving Licences Pave the Way for Future e-ID Cards and Passports [52] *(Smart Car / Biometrics)*

By the end of 2004, more than 300,000 drivers in Slovakia will carry forge-proof driving licenses, complying with the security requirements laid down by the European Union. The IT infrastructure for capturing the data necessary for the personalization and issuing of the cards is being set up by Siemens Business Services (SBS) under contract with the Slovakian Ministry of the Interior. Project logistics include 80 fixed and 10 temporary sites across the country, were photos and signatures of the drivers are collected in digital form and embedded in the new driving licenses. In addition, SBC is running a helpdesk providing telephone support for government staff. The EUR 6 million project is a first step towards the delivery of a new generation of ID and travel documents in Slovakia; while the IT infrastructure used for the production of the driving licenses will be used to create high-tech ID cards and passports, which will most likely feature one or more biometric identifiers.

Slovenia (Republic of)
No new item to report.

---

[50] http://www.pstm.net/article/index.php?articleid=406
[51] http://business-times.asia1.com.sg/sub/latest/story/0,4574,133860,00.html
[52] http://europa.eu.int/ida/en/document/3406/194

Spain

Spanish Government Kicks-Off Ambitious e-Government Plan [53] *(Smart Cards / e-Government)*

Public Administration Minister Jordi Sevilla said "the Public Administration Technological Modernisation Plan 2004-2007 budgeted at EUR 84 million for the modernization of public administrations comprises 43 projects that aims to connect administrations and people and to reduce bureaucracy, simplify procedures and eliminate unjustified delays." To achieve this objective, an electronic system for the secure interchange of data between administrations will be put in place. Among the projects, there are some major initiatives such as the future electronic ID card, to be phased in from 2005, and expecting to allow citizens to sign electronically and conduct online transactions with Government, which, according to Mr Sevilla, will oblige the public administration to transform itself radically.

Sweden

 No new item to report

Switzerland

No new item to report

Taiwan

No new item to report

Tanzania

No new item to report.

Thailand

No new item to report.

Turkish

No new item to report

United Kingdom

Government Biometric ID Cards Could Be Vulnerable To Fraud, Warn Experts [54] *(Biometrics)*

---

[53] http://europa.eu.int/ida/en/document/3316/194

A leading biometrics expert has warned the government that biometric ID cards, due to be rolled out from 2007, could be vulnerable to fraud unless it invests in more sophisticated iris recognition technology. Professor John Daugman, who pioneered the developed of iris recognition at Cambridge University said that the biometric systems under test by the government were not sophisticated enough to distinguish between real and fake eye images. "I am quite worried about the way that national ID cards will work out if the wrong camera is chosen. This is a technology that depends on choosing the right camera," he said. Daugman was speaking after a Japanese academic revealed new research at the Biometrics 2004 conference in London, demonstrating that commercial iris recognition readers can be fooled by using eye images printed on paper.

Devil's Advocate: Does The UK Need ID Cards? [55] *(Smart Cards)*

A question worth asking is whether the ID card is driving the need for a database of all citizens, or vice versa? Usually, the assumption is that ID cards are justified and that to make them practical, a huge database has to be built. Nevertheless, the IT people are running around thinking about the practical issues. If the construction of a huge national database is required solely to support ID cards, then there is certainly a very large cost at stake. Also, there are considerable concerns about personal privacy and community relations. While the cited benefits are tenuous, the favorite justification for almost any government scheme nowadays is that it combats terrorism. Other justifications include cutting fraud and crime. What is ignored is that ID cards create a whole new business for organized crime through the sale of forged cards. In countries where cards are in use, this has happened, sometimes on a massive scale. Only the most sophisticated, and therefore costly, cards would be proof against forgery. Indeed in countries that have ID cards, nobody has ever offered proof that the cited benefits can be realized. Without proven benefits, what can be the justification for the cards?

Doubts Over Passport Face Scans [56] *(Biometrics)*

Serious doubts are being raised about a new secure identity system being incorporated into new UK passports from the end of 2005. Biometric facial recognition will be brought in as part of an international agreement to target terror and fraud. But trials suggest the technology has a 10% failure rate, the BBC has learned. Some experts say the technology could be unsuitable for the high volume of travelers, and may fail to improve airport security.

Blunkett Poised To Open ID Scheme Offensive Tomorrow [57] *(Smart Card)*

David Blunkett is to publish his response to the Home Affairs Committee (HAC)'s report on his ID card scheme. The HAC report found very little positive to say about the scheme, but concluded that "the Government has made a convincing case for proceeding with the introduction of identity cards, and gave it the green light." Blunkett's mission riposte is therefore primarily not to make the case for an ID scheme, but to provide a convincing explanation of how it will work and how it can be successfully implemented. The convincing explanation and the case are inextricably entwined, because you can't possibly have made a case for something you've neither adequately defined or explained, but from a parliamentary perspective he can get away with proceeding on the assumption that the payroll vote and enough others accept that a scheme is both useful and inevitable.

54
http://www.computerweekly.com/articles/article.asp?liArticleID=134258&liArticleTypeID=1&liCategoryID=2&liChannelID=22&liFlavourID=1&sSearch=&nPage=1)
55 http://comment.silicon.com/0,39024711,39125057,00.htm
56 http://new s.bbc.co.uk/1/hi/uk/3762398.stm
57 http://www.theregister.co.uk/2004/10/26/blunkett_prepares_hac_response/

ID Cards: MP Committee Glad That Home Office Will Re-Think Its Plans [58] *(Smart Cards)*

The House of Commons Home Affairs Committee Chairman John Denham MP welcomed the Government's response to the Committee's recent report on ID cards. Mr Denham described it as a very significant move to address the concerns raised by the Select Committee. In particular, he welcomed: (1) the move towards a single free-standing ID card which would enable the selection of the most appropriate technology; (2) the development of a simple on-line verification process; (3) independent advice on biometrics from the chief scientific adviser of the Government; (4) the rationalization of current database proposals and the dropping of the Citizen Information Project; (5) agreement to put the aims of the ID card scheme into primary legislation; (6) agreement to give the Commissioner oversight of the whole scheme. Mr. Denham said: "while there are many detailed issues still to be clarified, and further work needs to be done on costing, the Government's response makes it much more likely that this essential scheme will succeed. "

United States

Expert Pans Quality of Government's Biometric ID System [59] *(Biometrics)*

In prepared testimony for the House Homeland Security Infrastructure and Border Security Subcommittee, Stanford University professor Lawrence Wein said that the Homeland Security Department's US-VISIT system for crosschecking incoming foreign travelers against its biometric database is producing inadequate results. He added, "on the surface, biometric appears to be highly effective. However, an examination of the details shows it is very difficult to accurately match poor-quality images." Furthermore, he disputed the government's claim of 96 percent success in matching terrorists listed in the database by saying "the currently implemented strategy has only a 53 percent chance of detecting a terrorist during US entry. There is a serious but reparable vulnerability."

Electronic Government: Smart Card Usage is Advancing Among Federal Agencies, Including the Department of Veterans Affairs [60] *(PKI / Smart Cards)*

As the unique properties and capabilities of smart cards have become more apparent, federal agencies, including the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the General Services Administration (GSA), have acted to advance the government wide adoption of smart card technology. In turn, numerous smart card projects that offer a variety of uses and benefits have been launched. As of June 2004, 15 federal agencies reported 34 ongoing smart card projects. Further, agencies' actions toward the adoption of smart cards continue to evolve as understanding of the technology grows. Agencies are aiming mostly to show the value of using smart cards for identification to larger, more integrated, agency wide initiatives involving many thousands, or even millions of users, and that are focused on physical access to facilities and logical information systems access to computer systems and networks. The Department of Veterans Affairs (VA) is one of 9 federal agencies currently pursuing large-scale agency wide smart card initiatives. VA's project involves using, among other technologies, the One-VA Identification smart card to provide an agency wide capability to authenticate users with certainty and grant them access to information systems essential to accomplishing the agency's business functions. VA estimates that this project will cost about $162 million between 2004 and 2009, and enable it to issue 500,000 smart cards to its employees and contractors. The full report is available at: http://www.gao.gov/highlights/d0584thigh.pdf

Intense Focus on Identity Standards Encourages e-Authentication [61] *(Authentication / e-Government)*

---

[58] http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=1989
[59] http://www.govexec.com/dailyfed/0904/093004tdpm2.htm
[60] http://www.gao.gov/highlights/d0584thigh.pdf CIOB News 2004-10-07

For years US federal agencies have been hard at work figuring out ways to offer citizens fast access to services via the Internet, as well as making it easy for contractors and suppliers to connect with government business opportunities. But in their quest for simplicity, many agencies ended up complicating the issue, building individual systems tailored to specific needs rather than working together to develop a unified e-government system capable of securely sharing information across agencies. Therefore, lesson learned are, (1) there is no true interaction without standards; (2) there are now several standards-based plans underway to bring disparate federal networks together, enabling, controlling and securing access to online resources.

GAO: Beware Managed PKI [62] *(PKI)*

The Government Accountability Office (GAO) warned that in certain situations, managed public key infrastructure services could be more trouble than they're worth to government agencies. Writing to Republican Tom Davis, chairman of the House Committee on Government Reform, the GAO's chief technologist, Keith Rhodes, said several agencies had looked to GAO for informal advice on managed PKI services. GAO's position was that agencies might face a greater burden in using managed services, specifically contract certification authorities, than they would if they implemented technology themselves. In a PKI deployment, the certification authority issues and manages the digital certificates that authenticate users and systems in a PKI environment. GAO is especially concerned about managed services when it comes to using PKI for financial transactions. "If the certification authority is compromised, the impacts can be catastrophic to an agency's operations," Rhodes wrote. The full report is at:
http://www.gao.gov/new.items/d041023r.pdf

Human Chip Implants Approved [63] *(e-Services / Privacy)*

The US Food and Drug Administration has approved Applied Digital Solutions to market the VeriChip, an implantable computer chip about the size of a grain of rice, for medical purposes. With the pinch of a syringe, the microchip is inserted under the skin in a procedure that takes less than 20 minutes and leaves no stitches. Silently and invisibly, the dormant chip stores a code that releases patient-specific information when a scanner passes over it. The VeriChip itself contains no medical records, just codes that can be scanned, and revealed, in a doctor's office or hospital. With that code, the health providers can unlock that portion of a secure database that holds a person's medical information, including allergies and prior treatment. The electronic database, rather than the chip, would be updated with each medical visit. The microchips have already been implanted in 1 million pets, but the chip's possible dual use for tracking people's movements, as well as speeding delivery of their medical information to emergency rooms has raised alarm. The critics said it could pave the ways to imperil the confidentiality of medical records.

Veterans Affairs Smart Card Rollout Begins With a Trickle [64] *(PKI / Smart Card / Authentication)*

The Veterans Affairs (VA) Department is pinning its plans to roll out smart cards to all users while 950 OneVA identification cards have been distributed to employees at the Fayetteville Veterans Affairs Medical Center for the first phase of its Authentication and Authorization Infrastructure Project. Pedro Cadenas Jr., VA's deputy associate deputy assistant secretary for cyber and information security said, "Fayetteville is important because from an enterprise approach, we'll have a better understanding and feel of what is required and what some of our challenges are to better equip our multiple teams for deployment." The smart cards that contain chips with digital certificates for use in a public-key infrastructure provide building and computer access, is a pilot project which runs until February.

---

[61] http://www.sun.com/br/0904_ezine/gov_eauth.html
[62] http://www.washingtontechnology.com/news/1_1/security/24501-1.html
[63] http://australianit.news.com.au/articles/0,7204,11069347%5E15306%5E%5Enbv%5E,00.html
[64] http://www.gcn.com/23_31/news/27715-1.html

Keeping Data Sources Confidential [65] *(e-Commerce / Privacy)*

Statistical data is a challenging matter for the Energy Department. On the one hand, the department must offer definitive data on energy use trends nationwide, but at the same time, it must keep the data confidential. For agencies that gather statistical information, protecting participants' identities has always been a concern that's why the Office of Management and Budget (OMB) will issue a guide to help agencies make sure they are securing their statistical data against privacy invasions, as required by a provision of the *E-Government Act* of 2002. On the technology side, agencies have worked to perfect techniques to obscure the origin of data. On the legal side, Title V of the *E-Government Act,* the *Confidential Information Protection and Statistical Efficiency Act* (CIPSEA), set the rules for protecting the sources of that data. Now, the administration's CIPSEA guidance will make sure agencies gathering statistical data comply with the privacy regulations set forth by Congress. OMB expects to issue the CIPSEA guide by year's end. It will standardize the language federal agencies should use when collecting data for statistical purposes.

NRC Library Goes Off-Line [66] *(e-Services / Privacy)*

It could take several weeks before the Nuclear Regulatory Commission (NRC) restores public access to its online library, which was shut down after officials learned that potentially sensitive documents were found on the site. In addition to take offline the Agency wide Documents Access and Management System (ADAMS), NRC officials suspended access to the Electronic Hearing Docket and staff documents referring to the high-level waste repository.NRC spokesman David McIntyre said "we envision that just because of the sheer volume and number of documents involved that it will be a few weeks before ADAMS can be partially restored, and at that point a review of documents will continue and more will be added as they are determined not to contain sensitive information." ADAMS is the NRC's massive searchable online library that provides access to the full text of regulatory and technical documents, including regulatory guides, reports, correspondence, inspection reports and other documents written by agency officials, its contractors or licensees.

Banking On e-Authentication [67] *(Authentication)*

Speaking at the Federal Information Assurance Conference in Adelphi, Maryland, Steven Timchak, director of the initiative at the General Services Administration said that banks are getting behind the federal government's e-Authentication initiative, giving a significant push to federal efforts to use electronic identities for e-government and e-commerce. In this regard, he added "we're meeting daily with major banks to talk about e-Authentication and will announce soon the extent of the banks' participation. Federal officials plan to rely on the rigorous identity proofing that banks conduct on customers as a basis for identity credentials that people can use to do business online with the federal government. Other credential providers such as universities, airlines and states also will be involved in the e-Authentication initiative. We want to trust many credential providers. Much work remains to reach crucial agreements on business and policy issues, such as how much banks will charge the federal government for using the credentials and how disputes will be resolved,"

Security, But Only If It's Convenient [68] *(Authentication / Online Transactions)*

The US Federal Trade Commission reported that consumers continue to repeat the mistakes that resulted in nearly 10 million identity theft victims in the United States last year. The 2004 Identity

---

[65] http://www.gcn.com/23_31/news/27691-1.html
[66] http://www.fcw.com/fcw/articles/2004/1025/web-nrc-10-26-04.asp
[67] http://www.fcw.com/fcw/articles/2004/1025/web-timch-10-27-04.asp
[68] http://ctv.globetechnology.com/servlet/story/RTGAM.20041027.gtsecurity1027/tech/Technology/techBN/ctv-technology

Management Survey, commissioned by Texas-based Electronic Data Systems Corp. and the International Association of Privacy Professionals, based in Maine, have confirmed this information. It has been found that consumers are not taking enough security precautions to protect themselves despite repeated warnings of identity theft. According to the survey, more than 70 per cent of consumers are too ready to share information such as their names, addresses, postal codes, phone numbers, account numbers or give the answer to a security question to an unsolicited call or e-mail. In other findings, the survey said that a majority of 61 per cent does not want to be forced to change passwords to increase security. More than half of respondents 57 per cent do not want their accounts locked down after three failed attempts to provide identification verification information. Finally, two-thirds of consumers 66 per cent believe it is worse to endure the inconvenience of being denied access due to a systems glitch than it is to be given access without proving their identity.

Venezuela

No new item to report.

Viet Nam

No new item to report.

Miscellaneous

Cyberspace Confidential: Protecting Your Words Certificates, Encryption And Biometrics Secure The New Wave of Digital Documents [69] *(Cryptography / Privacy)*

Corporal Jacques Boucher, a member of the Royal Canadian Mounted Police (RCMP)'s Atlantic Tech Crime Unit says "more and more home PC owners are using tax software. Your tax return contains a wealth of personal information for identity thieves. What would happen if someone hacked into your home computer and was able to access those files? Or suppose your hard drive crashes and you drop your computer off for repairs. How many people will handle that drive and have the opportunity to extract personal information from it?" He recommends encrypting sensitive computer files, a system of encoding and decoding messages to keep information secure. But he warns that won't protect against keyboard sniffers that track keystrokes, save them to a file and send the file off to destinations unknown. He says larger companies are more aware of these perils but residential and small business users need to take them seriously. Most corporate security experts say that even some larger firms needed prodding, although security is now firmly on the radar.

Who's Trustworthy? Canadians, Americans Disagree [70] *(Privacy / Online Transactions)*

What is the most trusted company in Canada when it comes to customer privacy? Over the years we've seen many studies ranking the country's most environmentally responsible companies, or the best employers. But there's never been a similar study dealing with the issue of privacy until now. Larry Ponemon, chairman of the Ponemon Institute in Scottsdale, Arizona, and an adjunct professor at Carnegie Mellon University, asked 6,300 US consumers earlier this year to rank the companies they believed were most trustworthy. The highest pick turned out to be eBay, followed by American Express, Procter & Gamble, Amazon.com, and Hewlett-Packard. Companies in the Top 10 were generally Internet companies, financial institutions or health-care organizations. Those that received the lowest scores came from the hospitality and retail food store industries. Based on the interesting results of that survey, Ponemon decided to conduct a similar poll in September asking Canadian consumers what they thought. Specifically, he asked respondents to name one to five companies they trusted with their personal information out of a list of 20 industries. What companies are honouring their privacy commitments, such as not sharing your information without your consent? Which ones are keeping your information safe and secure? The names of companies were not provided in advance. People were allowed to pick any organization they wanted, keeping in mind that the poll aimed to measure perception rather than whether a company truly did measure up to its privacy promises. The highest score went to IBM Corp., which only ranked seventh in the US survey.

Fourth Annual Global e-Government Study: Taiwan, Singapore Lead US, Canada in Online Government [71] *(e-Government)*

 A new study of global e-government undertaken by researchers at Brown University shows that 21 percent of government agencies around the world are offering online services, up from 16 percent in 2003, 12 percent in 2002, and 8 percent in 2001. Taiwan and Singapore now lead the United States and Canada in overall e-government performance. The fourth annual survey, conducted by Darrell M. West, professor of political science and director of the Taubman Center for Public Policy

---

[69] http://intranet/tbnews/stories/2004/20041007g0788.htm CIOB News 2004-10-07

[70]
http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&call_pageid=9713 58637177&c=Article&cid=1097446808504 CIOB News 2004-10-12

[71] http://www.ascribe.org/cgi-bin/spew4th.pl?ascribeid=20040910.084729&time=21%2000%20PDT&year=2004&public=1

at Brown University, and a team of researchers at the Taubman Center, measures the online presence of governments in 198 countries. The research evaluates government Web sites on two-dozen criteria, including the availability of publications, databases, disability access, privacy, security, and the number of online services. Previous studies of global e-government were released in 2001, 2002 and 2003. This year's study reviews 1,935 government Web sites during June, July, and August 2004. Among the sites analyzed are those of executive offices, legislative offices, judicial offices, cabinet offices and major agencies serving crucial functions of government, such as health, human services, taxation, education, interior, economic development, administration, natural resources, foreign affairs, foreign investment, transportation, military, tourism and business regulation. Researchers find that 89 percent of Web sites have online publications and 62 percent have links to databases. Only 14 percent (up from 12 percent in 2003) show privacy policies and 8 percent present security policies (up from 6 percent in 2003). According to automated software provided by Watchfire Inc., government Web sites are lagging on disability access. Only 14 percent of sites provide some form of disability access, such as assistance for the vision or hearing impaired. That figure is unchanged since 2003.

Microsoft Opens Up To Governments [72] *(e-Services)*

In Paris on September 20th, 2004, Microsoft made public its plans to open up aspects of the source code for its Office 2003 suite of applications, saying the it will be added to the Redmond, Washington based software maker's Government Security Program (GSP). Known as the Microsoft Shared Source Initiative, the program was launched in 2003 to address growing security concerns, giving government agencies access to a secure systems source code for key Microsoft programs, including the most recent versions of the Windows operating system. The decision was no great shock to open-source software providers and government users. And as Microsoft continues its experiment with open licensing, many are wondering what technologies they will open source next and when.

Aladdin eToken Supports OATH OTP Standard [73] *(Authenti cation)*

Aladdin Knowledge Systems, Ltd. announced that its eToken user authentication key now supports the One-Time Password (OTP) Algorithm submitted to the Internet Engineering Task Force (IETF) by the initiative for Open AuTHentication (OATH). OATH is an industry initiative with the mission to drive the ubiquity of strong authentication across all networks, applications and devices. OATH member companies endorsed the submission of a new algorithm for the generation OTPs. Aladdin eToken now supports this new algorithm and illustrates Aladdin's commitment to the establishment of this important framework. More information on the OTP algorithm can be found at: http://www.ietf.org/internet-drafts/draft-mraihi-oath-hmac-otp-01.txt

New Technology Would Support Both Privacy And Data Sharing [74] *(Privacy / Interoperability)*

A maker of identity recognition software has come up with a scheme to allow organizations to share and compare data without compromising the privacy of individuals. Anonymous Entity Resolution software, dubbed ANNA, uses a standard hashing algorithm to create a unique identifier for each piece of data about a person in an organization's files. Identifiers from different lists can be compared to discover matches without revealing the identity of the individual. John Slitz, CEO of Systems Research and Development Inc. said "this is a technique that allows us to look at large quantities of data, and only evaluate ones that are common to both sets. We've got it out in beta right now and we expect a commercial release in January. "

Entrust Congratulates GTEC WEEK 2004 Distinction Award Winning [75] *(e-Government)*

---

[72] http://www.canadait.com/cfm/index.cfm?It=902&Id=19293&Se=2&Sv=&Lo=2
[73] http://biz.yahoo.com/prnews/041027/cgw029_1.html CIOB News 2004-10-27
[74] http://www.gcn.com/vol1_no1/daily-updates/27735-1.html

Entrust, Inc. a world-leading provider of Identity and Access Management solutions, offered its Congratulations to the Distinction Award Winners of Government Technology Exhibition Conference (GTEC) WEEK 2004. A total of 38 awards were given in four groups, encompassing 14 categories and 3 sub-categories. These groups included Federal Awards (Group I), Provincial Awards (Group II), Municipal Awards (Group III) and National E-Government Awards (Group IV). Kevin Simzer, Senior Vice President, Marketing at Entrust said. "Entrust is pleased that GTEC recognized and celebrated the accomplishments of a number of our customers using Entrust's leading technology in government applications. Our goal was to simplify deployment and improve return on investment for our customers. On the basis of these results and feedback, we believe that we have made significant strides toward achieving that goal." Three out of the top four eGovernments, as ranked by the latest Accenture global study, are standardized on Entrust(R) security solutions, while the governments include Canada, Singapore and Denmark. For additional information on the winners and finalists, visit
http://www.gtecweek.com/ottawa2004/english/distinction_awards/

The primary source for the information contained in this document is the Internet – most articles are footnoted with links to source documents on various web sites. The reader is reminded that much of the information on Internet news sites is transitory and may only exist on a site for a short period of time. Readers wishing to maintain copies of the source information are encouraged to capture the text in a word processing application. Where possible, the date that an article appeared on a web site is provided following the link. Please do not report "broken links".

---

[75] http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/10-20-2004/0002289491&EDATE=