MICROSOFT AUSTRALIA

Inquiry into the Management and Integrity of Electronic Information in the Commonwealth

Responses to questions posed by the Joint Committee of Public Accounts and Audit
July 2002

1) What is the scope of Microsoft's engagement with DSD?

Microsoft has been interfacing with DSD at various levels for more than 5 years. Recently, our major engagement has been around getting Microsoft products onto the Australian EPL (Evaluated Products List). This has lead to discussions including:

- The 2 methods to get products on EPL
    1. Via DSD Evaluations, or;
    2. Via Mutual Recognition:
        - And the Mutual Recognition process requiring the US Government to finish their publishing of Common Criteria (CC) testing;
        - The requirement under CC for each country to do its own Crypto evaluation;
        - The requirements for DSD to have access to source code to be able to do the crypto evaluation.

DSD has recently finished the Mutual Recognition assessment with the exception of the cryptography components which they need source code to do, and are advancing in their negotiations with Microsoft about access to the source code, which we will be providing through the Government Security Program (GSP). GSP is explained in greater detail in the following question.

Once DSD and Microsoft complete the discussions around GSP, Microsoft will invite DSD to visit development laboratories and meet key people over in Redmond, WA USA. Additionally, other issues that have recently been discussed between Microsoft and DSD include:

- possibility of Common Criteria evaluations being conducted in Australia;
- other possible markets for DSD's AISEP program (the evaluation program);
- which Microsoft products are in higher demand for use in secure areas and therefore have more demand that they undergo Common Criteria evaluations;
- related discussions about the Security level required of the products;
- Microsoft's international security executives visiting Canberra;
- Discussion about the methods of distribution of patch update, and;
- DSD like many agencies also attend a number of the routine technical briefings MSFT holds from time to time.

Microsoft plans to continue open and constructive engagement with DSD.

2) ***What is the Government Security Program? How does it work? What benefits will it afford the Australian Government?***

Microsoft Government Security Program: Overview

In recent years, security has emerged as one of the most pressing concerns for every user of information technology, from the largest multinational corporation to the individual online shopper. No technology consumers, however, face more challenging security threats than national governments and their principal agencies. Microsoft recognizes that in matters ranging from national defense to the protection of citizens' personal data, governments must place security at the forefront of their information-technology requirements. They must be able to trust that their computing environments are secure.

The Government Security Program (GSP) is one crucial element of Microsoft's efforts to address the unique requirements of governments around the world. The GSP provides national governments with information they need to be confident in the security of the Microsoft® Windows® platform. In 2001, Microsoft launched the Shared Source Initiative, expanding its long-standing efforts to make Windows source code more transparent to trusted partners and customers. In 2002, the company announced its Trustworthy Computing Initiative, placing security at the core of all Windows development efforts. The principles of these two critical directives are embodied in the GSP, which is built upon the cornerstones of *transparency* and *partnership*.

Transparency
Through the GSP, Microsoft offers participating governments zero-cost online "smart-card" access to source code for the most current versions, beta releases and service packs of Windows 2000, Windows XP, Windows .NET Server 2003 and Windows CE. In addition, subject to requirements such as U.S. export approval, qualified GSP participants may also obtain access to cryptographic code and development tools.

Access to the source code is provided via MSDN® Code Center Premium for the Government Security Program, an online resource that enables authorized government employees to access source code from approved locations. The service provides just-in-time access and the ability to browse, search and access code through a smart-card-based, Secure Sockets Layer connection. Feedback channels enable communication and collaboration with Microsoft professionals.

In addition to source access, the GSP provides transparency through an expansive disclosure of Microsoft technical information. This engineering-level understanding of Windows architectural design as it relates to security imparts greater insight regarding the platform's integrity and enhances the government's ability to design and build demonstrably secure computing infrastructures.

Partnership
The GSP fosters partnership between the government and Microsoft based on mutual trust and fortified through ongoing interaction, collaboration and information exchange. As part of the program, representatives of participating government agencies may opt to visit Microsoft development facilities to review various aspects of Windows source-code development, testing and deployment processes, to discuss existing and potential projects with Microsoft security experts, and generally to interact with Microsoft staff. For the government participants, this represents an occasion for gaining valuable insights into Windows security. For Microsoft, the visit offers an invaluable opportunity to receive feedback from agency representatives. Visiting

agencies will be asked to outline specific projects and objectives prior to arrival, so that Microsoft can best develop a customized, rewarding itinerary.

The GSP also engenders opportunities for cooperation with Microsoft on projects identified by the participating government agencies in their GSP Authorizations (discussed below). The relationship of trust cultivated in the course of GSP participation, moreover, serves as a solid foundation for future technical collaborations in furtherance of designing, developing and implementing an optimally secure government computing environment.

GSP Code Agreement and GSP Authorization

The *GSP Source Code License Agreement* (or, simply, the GSP Agreement) establishes the legal framework for participation in the Government Security Program. It is the means by which Microsoft extends source-code access and other GSP benefits to the participating nation, while protecting the valuable intellectual property rights that have fostered innovation throughout the software industry for more than a quarter-century. The GSP Agreement's terms are straightforward, deliberately avoiding endless pages of complex, legalese provisions. They are also uniformly applied among participating nations.

The GSP Agreement establishes a standard three-year relationship, and sets forth all the basic elements of program participation. It describes the available types of license grants to access and use Microsoft source code, and establishes certain limitations to those grants. It defines the process of smart-card access via MSDN Code Center Premium for the Government Security Program. It also provides for protection of government information and Microsoft intellectual property, and invites feedback and communication. The GSP Agreement's terms apply both to employees and to approved agency contractors, and the document takes effect upon the signing of at least one project-oriented GSP Authorization.

To facilitate coordination of the government security review, the GSP Code Agreement envisions a single national government division or authority as the sponsoring agency within each participating nation. This agency executes the three-year GSP Code Agreement and may conduct the security review on behalf of the national government. The sponsoring agency has direct access to MSDN Code Center Premium for the Government Security Program, and may authorize other government agencies for annual, project-specific source-code access during the term of the GSP Agreement. Within such project-specific authorizations, Microsoft-approved contractors of sponsored agencies may be afforded code-access privileges identical to those of authorized agency employees.

The *GSP Authorization* establishes the license grant and more specifically defines each security project launched under the GSP by the sponsoring agency or any agency it has authorized. It is executed by the agency undertaking the project. The term of a GSP Authorization is one year, and is renewable. There is no fee associated with an Authorization unless it is warranted by the particular requirements and circumstances of the project. The GSP Authorization defines the specific purpose for the agency's license to access and use Microsoft source code, and identifies the products and government facilities that will be involved in the project.

Microsoft looks forward to helping governments respond to today's unprecedented security challenges. Through the GSP, key public agencies gain access to source code and information they need to be confident in the security of Windows.

Government Security Program: Fact Sheet

Overview The Government Security Program (GSP) is one important facet of Microsoft's efforts to help address the unique security requirements of governments around the world. The GSP provides national governments access to Windows® source code and information they need to be confident in the security of the Microsoft® Windows platform. This program embodies the principles of Microsoft's Trustworthy Computing and Shared Source initiatives, and is built upon the cornerstones of transparency and partnership.

Benefits Participation in the GSP affords national governments the following benefits:

- Online access to source code for the most current versions, beta releases and service packs of Windows 2000, Windows XP, Windows Server 2003 and Windows CE.Net;
- Engineering-level understanding of Windows architecture through expansive disclosure of Microsoft technical information;
- Enhanced ability to conduct security and privacy audits and to design, build and maintain demonstrably secure computing environments;
- Access to cryptographic code and development tools, subject to U.S. export regulations;
- Source code training;
- Communication and collaboration with Microsoft security professionals; and
- Opportunities for visits by agency representatives to Microsoft development facilities in Redmond, Washington.

Program Details The program provides zero-cost "smart-card" access to source code via MSDN® Code Center Premium for the Government Security Program, an online resource that enables authorized government personnel to browse, search and access source-code files from approved locations.

- *GSP Source Code License Agreement*: The GSP Agreement sets forth all basic elements of the program, and specifies the parties' respective rights and obligations. Its terms are straightforward and applied consistently among participating nations. It is valid for a period of three years.
- *Sponsoring Agency and Authorized Agencies*: Typically, one national government authority or department in each participating nation serves as the sponsoring agency. This agency signs the GSP Agreement, typically conducts the security review on behalf of the national government and has direct access to MSDN Code Center Premium for the Government Security Program. The sponsoring agency may authorize other government agencies for annual, project-oriented source access during the term of the GSP Agreement.
- *GSP Authorizations*: The GSP Authorization establishes the license grant and sets forth more specific terms defining each security project launched under the GSP by the sponsoring agency or any authorized agency. It is executed by the agency undertaking the project. The term of the authorization is one year, and is renewable. Each GSP Authorization becomes part of the GSP Agreement.
- *Visit to Microsoft Facilities*: Representatives of licensee agencies may opt to visit Microsoft development facilities in Redmond to discuss critical projects with Microsoft security experts and to review the Windows source-development process. Visiting agencies are asked to outline specific projects and objectives prior to arrival, so that their representatives' itineraries may be optimized.

Questions Additional questions regarding the Government Security Program should be directed to the Microsoft GSP Team at GSPTeam@microsoft.com.

3) ***What is Microsoft's liability re patch deployment? If a department does not get a patch deployed in time and gets compromised, is there any liability on Microsoft***?

Microsoft takes great responsibility for the quality and reliability of its products. Microsoft is constantly striving to make products more reliable and secure and with each successive product release we have seen this. Recently Microsoft spent $100 million to clean over 100 million lines of code and make its software more secure and reliable. Microsoft invests $5 billion in research and development each year. This is a long term investment in the future to ensure that our software delivers new features and innovations but at the same time is the most reliable and secure it can be.

Software development is a dynamic process. It is an imperfect science and there is no such thing as perfect software. Software is also part of a broader IT ecosystem and is just one part of a complex set of technologies and functions. Microsoft recognises that computing is an increasingly essential part of the lives of many Australians and there is some way to go before people trust it as they trust electricity, the telephone or other services. However, as long as there are individuals involved in malicious activity we feel we have a responsibility to inform customers of security issues and to provide patches and service packs. We also engage in a broad range of education initiatives and publicly announce any vulnerabilities or flaws that are discovered so that consumers and business can protect their IT systems and valuable data.

Microsoft is working on improving its patch management system and we refer the Committee to the White Paper on patch management we inserted into the record on June 16, 2003. This will be a constantly evolving and improving process.

The question of liability for software vulnerabilities remains a complex one. Already, Microsoft warrants our products to be fit for the purpose for which they are intended currently. In addition, we believe that Australian consumers are adequately protected under existing Australian legislation. Consumers can rely on a host of legislation designed to protect their interests including the Fair Trading Act and the Trade Practices Act.

If stricter liability were introduced, the cost of producing software would certainly increase but there is also the question of usability and the richness of features that would be provided by software developers. If further liability were introduced this would have a negative impact on innovation and would likely result in a reduction in software usability and easy of use.

From a company perspective, this is an issue we are closely examining. To this end, we refer the Committee to a response made by Microsoft Chief Security Strategist Scott Charney in an interview with the U.S. PBS on March 20, 2003:

"The product liability question is actually a very difficult one. People tend to think, "Well, we should just impose liability for software that has some sort of vulnerability." The reason it's so difficult is: What does that regulation or liability look like, and can you deploy it fairly?

So, first of all, it would be completely inappropriate to say you should have liability if there's any bug in software, because that's beyond any reasonable standard. But also, in terms of fairness, there's a huge difference between the software industry, for example, and other industries with liability, like the automobile industry. There is no group of automobile manufacturers who give

away cars for free. There is no open source of automobile movement. There is, by contrast, an open source software community.

So if you were going to impose liability on the software industry, how do you do it in a fair way? Or are you only going to impose liabilities on companies that actually pay a lot of taxes and create a lot of jobs? Can you do this equitably? No one has answered that question yet."

Ultimately, we believe that to successfully create a new era of computing – one which provides a safe, private and reliable computing experience for everyone, the entire software industry must work together to deliver a' trustworthy computing' environment and that this will involve rethinking our industry from the ground up. That means addressing issues with today's software and services as well as building fundamentally secure and reliable technologies for tomorrow.

4) ***How does Australia compare on the process and cost of getting products onto the EPL? What is the view of other countries with comparable standards and are there any best practices we can learn from***?

We canvassed these questions with our Redmond-based colleagues and we have not conducted any kind of comparative study or assessment of respective evaluation and EPL processes. Because receiving Common Criteria recognition is such a costly and time and resource-intensive process, we have focused on achieving CC recognition through the U.S. system and are then seeking Mutual Recognition agreements with the national signatories, including Australia. Conducting separate evaluations for hundreds of countries may not be the most feasible, efficient or cost-effective way of approaching this.

Security begins with good software code and high-quality testing of that code, and it continues with the process used to identify, correct and patch security vulnerabilities, and with third-party auditing based on recognized standards. Because of this, Microsoft submitted the Windows 2000 family of operating systems for a through, independent evaluation based on the new Common Criteria for Information Technology Security Evaluation.

Ratified as an international standard in 1999, the Common Criteria replaces the old evaluation schemes, the US TCSEC, which provided the well-known C2 rating, and the European ITSEC. The nations that embrace the Common Criteria believe that it will improve the availability of security-enhanced IT products, help customers evaluate IT products when making software purchase decisions, and contribute to higher levels of consumer confidence in IT product security.

Below, we are providing our view on the benefits of certification, the Microsoft Windows 2000 scenarios that have been certified, and resources available to help customers configure and administer a secure Windows 2000 environment based on the Common Criteria evaluation.

What is the Common Criteria Security Evaluation Process?

The United States federal government maintains a set of evaluation criteria for judging the security of computer systems. Many of its agencies, and many private-sector companies, will only buy systems that meet specified sets of these evaluation criteria. The well-known C2 rating of the US Trusted Computer Systems Evaluation Criteria (TCSEC) was one such level. The European counterpart to the TCSEC, the Information Technology Security Evaluation Criteria, specified a comparable rating. Both the US TCSEC and the European ITSEC have been updated. To reflect the increased sophistication of technologies and the growing need for more international standards for evaluation, a group of nations joined forces through the International Organization

for Standardization (ISO) to design a new security evaluation process, known as the "Common Criteria for Information Technology Security Evaluation (CCITSE). In this paper well abbreviate it to the Common Criteria.

Under the Common Criteria, classes of products (such as operating systems) are evaluated against the security functional and assurance requirements of "Protection Profiles." Protection Profiles may be developed to apply to operating systems, firewalls, smart cards, or other products that can be expected to meet security requirements. For example, the Controlled Access Protection Profile applies to operating systems and replaces the old C2 evaluation requirements. The Common Criteria also specify a series of Evaluation Assurance Levels (EALs) for evaluated products. A higher EAL certification specifies a higher level of confidence that a products security functions will be performed correctly and effectively.

While the Common Criteria was ratified as a standard in 1999, the stringent and lengthy testing requirements mean that test results for operating systems submitted for evaluation then are only now available. Testing for Microsoft Windows 2000 was recently completed and as a result of these tests, Windows 2000 achieved (EAL 4 + Flaw Remediation). The certification of Windows 2000 covers the broadest set of real world scenarios and the highest level of evaluation yet achieved.

What the Common Criteria Means for You

The existence of the Common Criteria impacts everyone that uses, deploys, and manages IT systems.

First, the Common Criteria provides a certain level of quality assurance by, among other things, allowing customers to apply a consistent, stringent, and independently verified set of evaluation requirements to their IT purchases. This raises the quality bar for products customers deploy, and it ensures a higher level of truth in advertising. This is not to imply that all products that are certified through the Common Criteria are free of all security vulnerabilities; however, it does provide a higher level of assurance that the product is secure.

Second, the Common Criteria program provides customers with a wealth of information enabling higher security in their actual implementation and deployment of evaluated products. Vendors that embrace the opportunities afforded by the Common Criteria can help customers build more secure IT systems.

The remainder of this paper will discuss the benefits of the Common Criteria, and then go into more detail on the specific evaluations performed on the Windows 2000 family and conclude with information on how customers can make real improvements to their configuration and implementation plans using the information provided by evaluators.

The fourteen nations[1] that have embraced the Common Criteria did so because they recognized that their common endorsement of a uniform set of IT security standards would improve the availability of evaluated, security-enhanced IT products. These nations also recognized that the Common Criteria would contribute to higher levels of consumer confidence in IT product security and would improve the efficiency and cost-effectiveness of the evaluation and certification process.[2]

Enables Customers to Make Informed Decisions

The Common Criteria help customers make informed security decisions in several ways:

- Customers can compare their specific requirements against the Common Criteria, consistent and universal standards to determine the level of security they require.
- Customers can more easily determine whether particular products meet their security requirements. Because the Common Criteria require certification bodies to prepare detailed reports about the security features of successfully evaluated products, consumers can use those reports to judge the relative security of competing IT products.
- Customers can depend on Common Criteria evaluations because they are not performed by the vendors, but by independent testing labs. The Common Criteria is, however, increasingly used as a purchasing benchmark; for example, the U.S. Department of Defense recently announced plans to use only Common Criteria-evaluated systems.
- Because the Common Criteria is an international standard, it provides a common set of standards that customers with worldwide operations can use to help choose products that meet their local operations security needs.

Helps Vendors Build Secure IT Products

By providing a detailed set of security standards, the Common Criteria effectively create an IT product security language that both vendors and consumers can understand. Vendors can draw upon this language to describe the security features included in their products by describing which Common Criteria evaluations their products have passed. Similarly, consumers can use this language to identify and communicate their security needs, which enables vendors to design products that meet those needs.

Furthermore, the Common Criteria language enables vendors to build their IT products in such a way that they can more easily demonstrate that their products meet specified security requirements, and the evaluation process allows them to have their product security evaluations performed by an impartial third party.

Microsoft has supported and embraced the Common Criteria from the beginning. Microsoft submitted Windows 2000 for evaluation by the Science Applications International Corporation (SAIC), an independent, accredited evaluator for evaluation under the Common Criteria. Microsoft and SAIC have worked together before: SAIC performed the C2 evaluations of both Windows NT 4.0 and SQL Server 2000.

Using the Controlled Access Protection Profile (which, you will recall, replaces the C2 set of evaluation requirements), SAIC determined through exhaustive testing that the Windows 2000 family achieved a rating of EAL 4 + Flaw Remediation under the Common Criteria.

To better understand where EAL 4 fits within the seven levels, it is helpful to know that, according to the Common Criteria drafters, EAL levels 5-7 are targeted toward the evaluation of products built with specialized security engineering techniques. As such, these levels are generally less applicable to products built with commercial distribution in mind. EAL 4, then, represents the highest level at which products not built specifically to meet the requirements of EAL 5-7 ought to be evaluated. To meet the Flaw Remediation requirement over and above EAL 4, as Windows 2000 did, the developer/vendor must establish flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution

of corrective action information to customers. The Microsoft Security Response Center fulfills these roles for Windows 2000.

According to SAIC, the Windows 2000 Common Criteria EAL 4 evaluation was, as yet, the most challenging evaluation project conducted by SAIC's Common Criteria Testing Lab from both technical and project management perspectives.

Other Windows 2000 Evaluations

The Windows 2000 family includes Windows 2000 Professional for desktop systems and the Windows 2000 Server family. Because Windows 2000 has such a broad range of features and abilities, it was submitted for evaluation against CC requirements that are beyond the Controlled Access Protection Profile. The result is that Windows 2000 is now evaluated with the following Information Assurance (IA) enabled information technology (IT) product features:

Sensitive Data Protection Device. Encrypting File System (EFS) protects sensitive data against tampering or theft by encrypting it on the local system. EFS protection meets the Common Criteria standards for certification as a Sensitive Data Protection Device.

Directory Service. Active Directory provides a robust, distributed enterprise directory service. The Common Criteria evaluation covers LDAP-based access and management of Active Directory objects; Windows 2000 meets the evaluation requirements by providing secure directory access and administration.

Virtual Private Network (VPN). VPNs make it possible for organizations to provide secure connectivity to remote servers and users without opening their networks to the world. Support for VPNs in Windows 2000 includes an integrated client and server services for two industry-standard protocols: L2TP+IPsec; the Windows VPN components have been evaluated for compliance with the Common Criteria standards.

Software Signature Creation Device. Digital signatures provide valuable integrity protection and authentication services, but only if the signature creation systems are secure against tampering or interference. Federal Information Processing Standard (FIPS) 140-1 sets out the requirements for secure signature creation; Windows 2000 provides security services that meet the FIPS 140-1 requirements, including a protection service that uses strong cryptography to protect users private signature keys and a FIPS 186-2-compliant implementations of the RSA and DSA signature algorithms.

Single Sign On. Many enterprises want to allow users to sign on to multiple network systems with a single set of security credentials. Windows 2000 supports this by providing application programming interfaces (APIs) so that third-party developers can use authentication services in Windows 2000 directly. While not described by a Protection Profile in itself, Single Sign On, as a capability, is composed of evaluated components.

Network Management. Windows 2000 provides several powerful network management tools, including the Windows Management Instrumentation (WMI) Services for monitoring and controlling system performance and operations and Active Directorys Group Policy engine for applying security and application policies to computers on a network. Network management tools in Windows 2000 have been evaluated against the Common Criteria requirements for network management systems and software.

Desktop Management. Desktop management services allow efficient and secure policy application for desktop computers in an enterprise network. Group Policy provides these critical services for Windows desktops; accordingly, Windows 2000 has been evaluated as a Common Criteria Desktop Management product.

In the context of the Common Criteria, Windows 2000 provides the clear advantage of a multi-purpose platform whose evaluated components satisfy many of an organizations needs. From the operating systems security technologies, to network management security, to VPN security, Windows 2000 provides the key (and evaluated) pieces in one package.

To reiterate, one of the key tangible benefits of the Common Criteria Certification is that it provides customers with guidance that simplifies the deployment and operations of Windows 2000 in a secure networked environment. Toward that end, Microsoft has worked to make sure that the evaluation data gathered in accordance with the Common Criteria are presented in a useful, actionable manner. As a result of this effort, customers have specific resources available to them - resources that meaningfully present architectural and configuration recommendations and best practices.

Microsoft is deeply committed to ensuring the security of its products and services. As part of that commitment, Microsoft strongly supports the Common Criteria certification program — a commitment that is directly reflected in its successful effort to design Windows 2000 to meet and exceed the security requirements specified for commercially available systems. The efforts by Microsoft are rooted in the conviction that the Common Criteria evaluation and certification system creates a reliable, internationally recognized way for consumers to evaluate and gain confidence in the security of IT products. By defining clear, robust security standards and establishing an independent security evaluation process, the Common Criteria promote the benefits and efficiencies that secure computing environments can provide to individuals, businesses, and governments.

Addendum:

There was significant discussion centered around Gatekeeper, authentication and PKI. We would like to share with the Committee, to insert into the record, our earlier submission to NOIE on their discussion paper, "***Towards a National Authentication Technology Framework*"**

1. Introduction

1. Microsoft Australia (herein, "Microsoft") commends the Government for opening discussion of this important issue to the public and welcomes the opportunity to discuss any security, trust or privacy related issues with NOIE in any forum that is made available.

2. In particular, Microsoft welcomes the opportunity to participate in the proposed Digital Signature Management Council. Ultimately we believe that key stakeholders in government and industry are best-placed to advise on new PKI accreditation and cross-recognition arrangements.

3. Furthermore, Microsoft believes that the domain of "security claims" is far more reaching than today's PKI technologies. Indeed Microsoft recommends that such

activities look carefully at other forms of authentication with multifactored claims technologies (biometric, Kerberos, Assertion based (eg. XrML, SAML), PKI as well as new evolving high volume technologies.

4. Microsoft shares the NOIE view that solutions to security and related issues require resolution before there will be broad take up of an e-services environment for significant transactions. Such resolution should, we believe, be conscious of the commercial and technical aspects of such potential standards.

5. Microsoft technology is widely used by Australian consumers,, by Australian businesses and by a broad range of government agencies to develop solutions to assist their clients engage in the business of government

6. The recent figures collected by the Business Entry Point (BEP) indicate the impact that Microsoft technology as on the IT community and hence we believe that it is important that we take a responsible position in advising relevant agencies regarding the decisions that the company is making with regard to security issues as these will most likely have an impact in the broader market.
.
7. Microsoft continues to be significantly engaged with a number of federal agencies working on security related projects and has provided those agencies with ready access to corporate decision makers regarding the technology that Microsoft is developing, standards being adopted, standards bodies that it is participating in and technology under consideration as well as general time frames for delivery to the market place of these projects. We believe that this information would be of value to NOIE.

8. Microsoft has been exposed to the Gatekeeper standards and the Angus Project as well belatedly and indirectly to the TAC trial. These experiences have led us to form some opinions that we believe may assist any further discussion on this topic.

9. It is important to recognize, in the context of these discussions, that the real objective must be e-enabling the community of users. While it is important that the systems that government supports are technically secure we must always be mindful of the impact on the users. It is in this context that Microsoft has a lot to offer as it is one of our imperatives that the user experience in their interaction with technology is simple and readily comprehended.

2. General Comments

1. We acknowledge the importance of the issues around this topic as being critical if the wider adoption of the Internet for transactions is to occur. We see many issues relating to the elements that NOIE has identified around identity, privacy, security and authentication and will cover these briefly in this response.

2. We also see other key issues around cost, ease of use, digital rights management and capacity of older platforms that should be considered as well.

3. Microsoft has placed a substantial effort and resources into this topic. This ranges from a significant project to educate all of its developers and testers on the topics relevant to writing secure code and identifying security holes in existing code and an associated security audit of current developments. We have also entered into discussions with the tertiary institutions who provide basic education in IT about the security implications of existing courses. This has significant implications for our recruiting practices as we believe that the issue must be tackled at the most fundamental levels.

4. Microsoft is also pursuing two key initiatives to make the PC platform an outstanding secure platform, viz:
    i. Hardware. The WinHEC industry wide initiatives with Windows OEMs (such as IBM, HP and Intel) is targeted at defining the most secure platform possible to base a full security operating system such as trusted Windows. Detail of the hardware requirements for such a hardware platform are documented on http://www.TrustedPC.Org/ This initiative formally began almost two years ago and currently has a membership in excess of 170.
    ii. Palladium. This project (called Trusted Windows by the press) is around making additional changes to the Windows Operating system to innovate a large number of security technologies. Microsoft would welcome the opportunity to discuss and present such activities on a confidential basis.

5. Currently we see the solution being built around PKI technology and no vendor of security technology covers all platforms. This results in high costs for any PKI solution from the development as well as support perspective. We do not believe that users will adopt PKI until:
    i. Costs are substantially reduced
    ii. Ease of use is dramatically improved

6. Microsoft has concerns that Government policy that is too prescriptive in this area could impede uptake and growth electronic transactions and could ultimately pose a barrier for global online trade with Australia. Given the global nature of Microsoft's business, we believe that we could be well-placed to work with government to help develop solutions for interoperability between overseas agencies as well as between the private and public sectors in Australia

3. Identity/Authentication/Trust Management

1. Microsoft announced a number of enhancements in this area on July 24th (US time). Whilst it is true that there are a number of new innovations as a part of the .Net Strategy there are other aspects that are very relevant to this response also. In particular, Microsoft has listened very carefully to Organizations and Partners around a number of apprehensions and has changed strategy in a variety of areas.

2. Microsoft has experience with a web-based identity (authentication) service, Microsoft .NET Passport (herein, "Passport"). This has had a significant take up rate in the open market and has provided Microsoft with valuable insight into the challenges that the provision of such a service can bring.

3. Microsoft's .Net Strategy will continue to accept and encourage Passport authentication (which is evolving) however many other forms of authentication are also to be fully supported.

4. In order for federation to work, authentication and trust must be able work between systems that are implemented on any number of technology platforms, including those with no Microsoft software or licenses involved. It is Microsoft's goal to be interoperable with these authentication systems by adopting open standards.

5. Towards this goal, Microsoft, IBM, and VeriSign announced on April 11, 2002 the publication of a new Web services security specification to help organizations build and secure broadly interoperable applications. The three companies jointly developed the new specification, known as WS-Security, and plan to submit it to a standards body.

6. WS-Security is the foundation for a broader road map and additional set of proposed Web services security capabilities outlined by IBM and Microsoft to tackle the growing need for more interoperability between authentication systems. The proposed road map outlines additional specifications the companies plan to develop along with key customers, industry partners and standards organizations.

7. While the .NET Passport is moving to an authentication architecture that is based on the open and established Kerberos v5.0 standard, WS-Security will allow it to interoperate with other styles of authentication, including PKI.

8. For government transactions, NOIE should consider the proposition that it establish an optional, federally issued identity smart card that was required for secure on line transactions. NOIE could take advantage of the fact that all identifiers currently used for significant transactions are based on government-issued identifiers such as birth certificates, passports and drivers licenses. It may instances these are mandatory for participating in certain activity (?). For example a government-issued drivers license is required if an individual wishes to drive a vehicle on the public roads. This analogy could be applied to on line government transactions.

9. This would enable agencies to significantly reduce costs of development of web based services and provide citizens with a high level of confidence in the security and privacy of those transactions.

10. We understand that these are complex issues but this is a forum in which the options open to government should be canvassed.

11. This is more fully canvassed in section 6 of this response.

Privacy

12. One of the central tenets of the .NET Passport service is that the user is in control of their personal information and ultimately, their privacy. The .NET Passport privacy statement underscores our commitment to consumer privacy and serves as a public declaration to this effect. The .NET Passport privacy statement clearly states that .NET Passport does not share, sell, or use personal information in a manner that differs from what is described in the privacy statement, unless the user has granted their consent.[1]

13. No user information flows from participating sites to Microsoft. All data on user activity at participating sites—such as items purchased, pages viewed, and data entered—is solely the property of the participating site and is not seen by Microsoft. Participating sites that choose to collect information in addition to that which is stored in the .NET Passport profile are free to do so This information is stored at the participating site and is never stored with Microsoft. The relationship between the participating site and the user remains intact.

14. When going live with .NET Passport all participating sites must contractually agree to post a privacy statement, follow legal privacy requirements, and industry standards.

15. .NET Passport makes it possible for users to obtain an account while providing only two pieces of information, a unique e-mail address and password, nothing more. This gives the user the ability to create a useful account while maintaining a degree of anonymity.

16. Microsoft is a strong supporter of the privacy initiatives of the Federal Government and works diligently to comply with the privacy laws of Australia and other nations globally.

Security

17. Microsoft takes security very seriously. .NET Passport employs multiple layers of security technologies and systems that are designed to prevent unauthorized access to the system.

18. We believe that secure operations are an imperative. The user's sensitive data must be protected between the client machine and the data centre, through encryption, personnel management and other means.

19. These privacy and security considerations also need to be balanced with concerns about reliability, availability and usability and are all part of Microsoft's commitment to consumer confidence, trust and safety as embodied in our "Trustworthy Computing Initiative."

[1] We encourage you to review the entire .NET Passport privacy statement at http://www.passport.com/Consumer/PrivacyPolicy.asp.

4. Gatekeeper

1. As NOIE has pointed out there are many issues that fall under the security heading and Microsoft has a point of view on many of them that we believe NOIE should have better access to.

2. We are generally supportive of the Gatekeeper approach as being appropriate for the time it was introduced and certainly has started down a standards based approach. We believe that keeping close to international standards is a key element of the Gatekeeper Project if it is to attract widespread adoption.

3. We have some concerns that the price of entry into Gatekeeper is such that the qualified organisations may not adopt industry standards with the speed required in an e-enabled world as they will be driven by cost recovery models based on older, obsolete technology.

4. This will require close monitoring from NOIE to ensure that Gatekeeper keeps in step with industry standards. This will be particularly important if NOIE is to influence one of the important barriers to widespread adoption of PKI, that of high cost of entry.

5. Microsoft will provide products for evaluation under the common criteria regime. This is the most appropriate forum for having new technologies evaluated by the security community. Product groups are now made aware of common criteria requirements and we participate in industry groups establishing appropriate standards.

6. We urge NOIE to maintain its focus and awareness of open industry standards in the security community. It is not only existing standards but also emerging standards that are important for this success. Microsoft is a leading advocate of the development of open industry standards and have committed to adopting them in its products as soon as practicable. Microsoft is happy to share its knowledge of these developments with NOIE for use in its forums with other interested parties.

7. With regard to Gatekeeper implementation, we believe that NOIE should re-visit the option for a National Authentication Authority as out lined in section 6 of this response. In our view this would rapidly accelerate the roll out of PKI solutions in both private and public sector organisations.

8. There are still significant issues to be resolved around ease of use. Currently digital signing of documents and associated key management issues make the user experience challenging.

9. Given the difficulty of doing this accurately and the complexity of the technology involved in associated processes
    i. Rendering,
    ii. digital time stamping
    iii. notarisation
    iv. certificate profiles
    v. playback and intent mechanisms

Authentication

10. The Federal Government should consider that it establish the Australian National Identity Transaction Authority for this purpose. The benefits of such a body would be to be a
    i. single fortress for low cost PKI enablement
    ii. vehicle for single sign on and authentication
    iii. mechanism for isolating foreign keys
    iv. central point for user auditing
    v. unified source for court ordered access to information.

11. While the discussion paper does not make it clear that such a concept would be well received, Microsoft believes that formation of this authority is in step with governments that modify their business models to become the wholesalers of appropriate services.

12. This fits in with the government wholesaler of an essential service. In keeping with that direction such an authority as a wholesale service provider appears to fit with broad government policy. Banks have established points of proof requirements for the establishing of an identity to participate in their transactions. The highest proof points are based on government issues identifiers such as birth certificates and tax file numbers. A formal wholesale service could reduce costs and drive adoption in the community.

13. With appropriate legislation such a wholesale service could be provided. Given that the contentious issues around liability have been discussed at length, legislation could be drafted that removed this barrier from government consideration.
    i. The provision of the actual service could well be contracted to the private sector but to succeed it would require strong government authority.

14. In this context, we submit that the Electronic Transactions Act of 1999 (ETA) should be reconsidered and revised. In our 1999 submission on the ETA, Microsoft expressed concern that the bill would only serve to promote legal certainty in electronic commerce in a very limited way. This concern has largely been born out and we are concerned that this lack of clarity and certainty will serve as an impediment to e-commerce uptake. As a participant in electronic commerce on a global basis, Microsoft is faced with regulatory uncertainties arising under different national laws and the uncertainties and risks increase if there are varying laws within a country's domestic jurisdictions. If left unchanged we would expect legal challenges to increase with subsequent reduction in confidence in the electronic transaction process.

Other Issues

15. We have been fortunate to work with a number of federal agencies in the context of The Business Authentication Framework Project, Gatekeeper and Project Angus. Based upon this work and other activities elsewhere around the world :-
    i. We have concerns around the cost of PKI certificates and the management of such certificates.
    ii. We believe that current technology can provide the platform for a certificate validation service based on current open industry standards
    iii. We see the challenge as the client signing interface. Currently the systems that are built to accommodate all platforms in the market place are complex and bring significant support costs to the hosting agency.
        1. This is made more challenging by the requirement that all platforms that work on the internet must provide the same level of security protection.
        2. NOIE should consider that as more modern technology is developed with a focus on security and released into the consumer market, the provision of secure environment will become cheaper on more modern platforms. This may require additional policy consideration in the context of IT and equity of access. The issue of optional authentication cards may be a mechanism to reduce the technologies between older and newer platforms.
        3. We expect to have a version of a client signing interface as a part of the next major release of our operating system (can we explain the implications of this for govt in greater detail?).
    iv. We have been impressed with the BAF team's approach to the practicalities associated with how this must all fit into an existing paper based legal system.
        1. This has led to discussion around other related topics such as digital rights management technologies and partial signing of documents which we are addressing and will continue to work with the BAF team in conjunction with development groups in Redmond

16. We have observed the challenges involved in the use of ABN-DSC's with platforms that have not been intended for use in a secure environment.
    i. Unfortunately, Microsoft Australia was consulted very late in the TAC project when the challenges had become critical.
    ii. We have committed to resolving some identified issues to assist the trial but believe that earlier consultation would have been preferable.
    iii. We respectfully suggest that NOIE take a role in advising agencies undertaking key pilots or projects, of the potential to receive advice from Microsoft technical staff where the project has a significant Microsoft component.