ARTICLE 29 Data Protection Working Party

10054/03/EN
WP 68

Working Document on on-line authentication services

Adopted on 29 January 2003

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC.

The secretariat is provided by Directorate E (Services, Intellectual and Industrial Property, Media and Data Protection) of the European Commission's, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.
Website: www.europa.eu.int/comm/privacy

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

HAS ADOPTED THE PRESENT WORKING DOCUMENT:

1. INTRODUCTION: THE EXPANSION OF ON-LINE AUTHENTICATION SERVICES

The growing use of on-line authentication services has changed the Internet landscape[2]. More and more websites propose or require visitors to register, for instance because they provide confidential information, they offer the possibility of registering the preferences of the user, they provide a service for which they demand remuneration or because the object of their service is to deliver goods. All these sites require the user to supply some form of identification, often including an e-mail address, and a form of verification, often a password.

The use of "user-id/password" combination can pose some challenges to the service-providers:
- Users tend to forget their password. An increasing number of helpdesk calls or mails concern forgotten passwords. The costs of resetting passwords become an increasing burden on the websites.

- More and more users use different access methods to the Internet, yet require the same service from the service providers. The access methods may vary in their technology, from access from a pc to WAP, but more often the Internet is accessed from different personal computers, at Internet-cafes or public libraries. So users have to remember multiple passwords.

- Finally, some users do not like typing user-ID and passwords as they feel it interrupts their user-experience. Users tend to minimise the effort they need to take, which results in short passwords that are not secure and are often synchronised over many websites.

Any solution to the three issues mentioned above requires the user to delegate a part of the authentication. Currently, there are four possibilities available:

- The password management is delegated to the browser on the pc of the user, as is done for instance by the Mozilla password manager.

[1] Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

[2] As the Working Party has already said in previous documents, the principles of the Directive also apply to on-line activities. See for instance: Working Document Privacy on the Internet- An integrated approach to On-line Data Protection, adopted on the 21st November 2002, WP 37.

- The password management is delegated to a proxy-server on the Internet, possibly provided by the ISP
- Authentication is provided by a third party using a specific authentication protocol. This is done by Microsoft .NET Passport.
- Authentication is done by a contract party within a "circle of trust". A specific protocol is used, like for instance the one of the Liberty Alliance project.

These possibilities are analysed in the following paragraphs:

1. A password manager on the pc

Having a password manager as a part of the Internet browser solves only part of the problem. It will relieve the user from typing passwords, thereby minimising the risk that a password is lost. However, it does not solve the problem for roaming users that access services from different pcs.

From a data protection point of view, the situation is fairly simple. All the software is running on the pc of the user and under the control of that user. There is no external company that controls the data. The user is asked if the information should be incorporated into the database of the password manager. The password manager fills in the password, but does not yet send it, thereby ensuring the user's consent. From the security viewpoint it is necessary to take adequate measures to make sure that storage is secured from attacks.

2.Using a proxy-server

Instead of using a password manager in the user-agent (i.e. the browser), the same functionality may be built into a proxy-server on the Internet. The functionality is comparable to the better known anonymising proxies. A proxy-server may serve many users; it therefore needs to register passwords, for each user in respect of each per target site. The registration must be trusted by the users; this trust is very explicit because a user must make a conscious decision to use a specific proxy (there is no default service). A user must log in to the proxy if he wants to use his passwords. Once logged in, the user experiences the same benefit from the proxy as he does from the built-in password manager. The advantage of the proxy is that it may be accessed from different pc's and/or other devices.

These proxies should never divulge information about a user to a third party without the user's consent. If they do, they lose the trust of their clients and therefore their basis for existence. There will normally be a contract between the proxy provider and the client. The service will probably be paid by other sources than advertising, possibly in combination with the service provided by an ISP.

3. On-line authentication services with special protocols

None of the solutions described earlier requires any change to the website of the service provider. Another possibility is to carry out the authentication using a special authentication protocol. The basic architecture for these protocols is the same: there are three parties: an end-user, a service provider and an authentication provider. Before being served by the service provider, the end-user has his identity verified by the authentication provider. The service provider trusts the authentication provider and accepts the introduction of a user.

The .NET Passport architecture uses a single authentication server, which is operated by Microsoft. The Passport contains some identification and authentication information plus some profiling information. In the future, these two sets of information are expected to be increasingly separated . A user who has logged on to Passport has a unique identifier, a PUID. If the user wants to log on to a service provider, he instructs the Passport server to provide the PUID in a form that is readable by the service provider, currently symmetrically encrypted.

The Liberty Alliance uses a federated model. A user may federate his account to two service providers. Once an account has been federated, a service provider will accept the introduction of the other service provider; the other service provider will act as the authentication service.

The Working Party is aware of the expansion of on-line authentication services and decided therefore some months ago to examine the data protection implications of operating these systems[3]. While being conscious of the importance of secure authentication mechanisms to ensure the security and in particular the integrity of some electronic transactions, especially those involving on-line payments, the Working Party wishes to stress that the development of these services needs to respect the data protection principles laid down in the European Data Protection Directive[4] and in the national laws implementing this Directive.

2. CASE- STUDY 1: MICROSOFT .NET PASSPORT

.NET Passport is at present an initiative of considerable importance in this field. Consequently, the Working Party carried out an initial study of this system as its first priority in the spring of 2002[5]. After a first analysis, the Working Party concluded that, although Microsoft had put in place some measures to address data protection concerns, a number of elements of the .NET Passport system raised legal issues and therefore required further consideration.

In the months following, the Working Party engaged in a dialogue with Microsoft in order to improve the understanding of the working of the system, to discuss the different issues at stake and in particular to assess whether the European data protection principles are correctly complied with and, where appropriate, to identify elements of the system that require changes. As a result of this very open and fruitful dialogue Microsoft has committed itself to make changes to the system delivering improvements from the data protection perspective.

The commitment of Microsoft to put in place all the measures discussed with the Working Party has been documented in several letters to the chairman of the Working Party, Professor Rodotà[6], and in a timetable that fixes time frames for taking each step. The varying length of the implementation period is justified by the different nature of the steps. Some of the measures agreed, such as revising the text of the .NET Passport Privacy Statement and providing additional information on registration pages, are simple and can be implemented quickly. Others, such as the new information flow described

[3] See WP 60, Working Document First Orientations of the Article 29 Working Party concerning on-line authentication services, adopted on 2 July 2002.

[4] Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

[5] See WP 60, Working Document First Orientations of the Article 29 Working Party concerning on-line authentication services, adopted on 2 July 2002.

[6] Letters dated 19 September and 25 November 2002.

below, entail significant recoding of the .NET Passport service, and so require additional time to implement.

The Working Party has taken note of the timetable presented by Microsoft to address the concerns of the Working Party. This timetable includes three categories of time frames: first category (0-4 months), second category (4-8 months) and third category (8-18 months). The timeframe will be indicated in brackets after each measure. Some of the discussed measures have in the meantime already been put in place and are indicated subsequently in this text as current practice.

2.1. Short description of the Microsoft .NET Passport system

NET Passport is an Internet-scale authentication service providing single sign-in across multiple participating websites in order to help users to save time and avoid repetitive data entries when surfing on the Internet. It is not an authorisation or identification service but an authentication service, aiming at uniquely and securely authenticating a user by verifying the credentials presented[7].
It was created in 1999 and it was renamed .NET Passport in the summer of 2000. Presently there are over 250 million accounts worldwide (a user can have several accounts, surely if he has several Hotmail accounts). Over 40 million accounts belong to EU residents.

There are several ways of obtaining a Passport:
- At www.passport.net
- At a participating site
- By obtaining a Hotmail account

About 87% of the users sign up via a participating site or Hotmail, not directly at the Microsoft site. About 120 million accounts belong to Hotmail account holders and another significant number of users sign up through Window Messenger . Hotmail is an e-mail service used world-wide and totally managed by Microsoft Corporation or by other companies controlled by Microsoft.

Three predetermined blocks of personal data are currently collected:
1. Minimal information: user-name (e-mail address) and password.
2. Credentials: secret question and answer, phone number and pin, security key and three additional questions and answers. These are necessary in the cases when the user has forgotten his password.
This information is not part of the profile and is not communicated to other sites.
3. Maximal profile information: the above-mentioned information plus first name, last name, time zone, gender, date of birth, occupation and accessibility.
Participating sites can decide to collect directly from the user and to process additional information. Presently 69 external (not Microsoft related) websites participate in .NET Passport, 22 of them are EEA sites.

.

[7] It should be kept in mind that, in addition to the Data Protection Directive, other Directives might also apply to these services such as the e-commerce or e-signatures directives.

2.2. Legal issues at stake and outcome of the dialogue with Microsoft

In its July 2002 document the Working Party identified a number of issues that required further consideration. In the following paragraphs attention will be paid to each one of these issues and to the outcome of the dialogue with Microsoft concerning each matter at stake.

It is important to note as a general point that in addition to the specific measures that will be described in the following paragraphs, Microsoft has decided to change the .NET Passport information flow. In essence, the service will be recoded to clearly separate the creation of a .NET Passport account from the storing of personal data in the Passport profile. This new information flow should have, as will be explained in greater detail when dealing with proportionality issues, a positive impact on the fairness of the collection and processing of personal data. The Working Party notes this fact with satisfaction.

2.2.1. The information given to the data subjects at the moment of collecting, further processing the data or transferring it to a third party, possibly located in a third country

When beginning to study the working of the .NET Passport service the first problem faced by the Working Party was the lack of clear and transparent information about this system. Some of the existing information about the system was unclear, failed to give information as to the main data protection matters (identity of the controller, purpose of the processing, rights of the data subject, recipients of the data, what is necessary to ensure fair processing) and sometimes contained contradictory statements.
Two issues that particularly worried the Working Party were the lack of adequate information about the transfer of personal data to a third country and about the link between Hotmail and Passport.

In the meantime Microsoft has made the commitment to take the following measures in order to address the Working Party's concerns about this:
- Microsoft will provide, as recommended by the Article 29 Working Party in its recommendation 2/2001[8], a prompt box containing the information required by Article 10 of the Directive in a highly accessible and user friendly way. A link for the prompt box will be displayed to users who identify themselves as residing in the European Union right at the point on the registration page where they indicate their country of residence. Users who click on the link will then receive the prompt box in a side window. This feature will be available no later than April 2003.
- Users will be informed when they sign into a participating site of the country in which that site is located (8-18 months), and will have access, via the prompt box, to a link to the European Commission’s page listing countries whose data protection laws have been found to be adequate under EU standards (4-8 months).
- Microsoft will inform EU users, via the prompt box, of the length of time it retains log data (currently, no longer than 90 days) (0-4 months).
- Users will be clearly informed right at the beginning of the process exactly how they can open a .NET Passport account without using their real e-mail address, a functionality that the Working Party recommended be included on several occasions. At the same

[8] Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union, adopted on 17 May 2001, WP 43.

time, users will be advised of the limitations of pseudonymous accounts so that they can make an informed decision (8-18 months).

- Microsoft has made a commitment to update all language versions of the .NET Passport Privacy Statement at the same time, except where local considerations required an immediate change to a particular language version. In those cases, which are expected to be very rare, Microsoft will include a statement in the other language versions of the Privacy Statement indicating that they will be updated shortly (0-4 months).
- Microsoft has made a commitment to take a number of actions concerning the information given to Hotmail users to ensure that when users sign up for Hotmail they are also informed that they are simultaneously getting a Passport account (current practice); that when users sign up for Hotmail they are also informed that they must get a Passport account in order to access Hotmail, and that they cannot close their Passport account without also closing their Hotmail account (0-4 months).

2.2.2. The value and quality of the consent given by the data subjects to these operations.

After its initial analysis of the system, the Working Party had some questions about the validity and the quality of consent as a ground for processing as required by article 2h of the Directive[9]. In other words, it was not convinced that the consent given by the users was sufficiently informed, freely given and specific, particularly for those users registering through Hotmail, or for the transmission of personal data to participating sites.

As has just been explained, Microsoft has taken and is committed to implementing a package of information measures aimed at ensuring that fair information is provided to users. Moreover, concerning the possibilities of users deciding whether or not to provide personal information to Passport, the new information flow will allow users to communicate personal information to a participating site without storing it in their Passport profile and to obtain a pseudonymous Passport account with no collection of additional personal information (8-18 months).

As far as Hotmail users are concerned, in addition to the improvement of the provision of information, measures are being taken to clarify to users that when they sign up for a Hotmail account their personal data will be used for the purpose of sending them advertisements (0-4 months). This will be done by making explicit on the Hotmail registration page that users are opting in to receive Hotmail advertising when they agree to the Hotmail terms and conditions. As with any participating site, users who register for a .NET Passport at the Hotmail site will have the option of providing their personal information only to Hotmail, and not having it stored it in their .NET Passport profile (8-18 months).

The Working Party had also discussed with Microsoft the possibility of Hotmail users opting-out from targeted advertising. Microsoft has explained that once users have a Hotmail account, they can opt-out of receiving targeted advertising free of cost, but this involves the closing of their Hotmail account. Users can not retain a free Hotmail account without receiving targeted advertising because targeted advertising generates the revenue stream which makes it possible to provide the Hotmail account for free.

[9] The data subject's consent shall mean any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

The Working Party still considers that there is question of conformity of this practice with European legislation and will continue to reflect on this issue in the future. It considers however that this matter is related to a specific issue, i.e. the practice of several companies of linking the provision of a service to an obligation for the user to accept the use of his data for a marketing purpose without opt-out possibility. This issue, being distinct from the specific one of on-line authentication services that is the subject of this working document, will be dealt with in a broader context in the future.

Regarding the consent of the users given to the participating sites, the new registration flow will give users a Passport that contains only username and password by separating the creation of a Passport account from the decision to communicate personal data to participating sites or to store it in the profile (8-18 months). Users will be informed that they can register for a Passport at the Passport website by providing only a username and password, and that if they register through a participating site, other information may be mandatory for the purposes of the activities of that site (information to be included in the prompt box in 4-8 months). A new functionality will also be included to enable users to decide on a site-by-site basis whether they want to communicate their profile data or not. The user profile will be reconfigured to allow users to fill out the fields they choose, while leaving others blank (8-18 months).

The new information flow will also enable users, each time they register with a participating site, to revise profile information, to amend profile information, to decide whether or not to save those amendments in their Passport profile, and to determine what information they send to the site (8-18 months).

2.2.3. The proportionality and quality of data of the data collected and stored by .NET Passport and further transmitted to affiliated sites.

The Working Party was concerned about the amount of data collected through Passport, especially the profile data, and about the fact that once the data subject creates a .NET Passport the personal data included would, if the data subject has clicked in the sharing boxes, be transmitted to all participating sites he visits and signs in to, regardless of whether it is necessary for the site in question. At the moment of undertaking the first study of the system it was not possible for the user to authorise the transmission of a part of the data, all profile information was seen as a block.

The new information flow to be put in place by Microsoft will clearly separate creation of a .NET Passport account from the user's decision to communicate personal information to the participating site and possibly to .NET Passport. Users will be able to choose, on an opt-in basis, whether or not to store information they choose to communicate to a registering site in their .NET Passport profile. When a user who has stored information in his .NET Passport profile visits other participating sites, he will be able to alter or delete that information, on a field-by-field basis, before communicating it to the participating site. The user will also have the choice, on an opt-in basis, to have those alterations and deletions stored in his .NET Passport profile (8-18 months).

These changes, in addition to the fact that the user can decide not to use his real e-mail address in some cases, will, once implemented, meet the concerns of the Working Party, although the Working Party would like to continue monitoring this issue, in particular taking into account the role of Microsoft as controller of personal data and other valuable information submitted by the users.

2.2.4. The data protection rules applied by the websites affiliated to .NET Passport.

Another concern of the Working Party related to the lack of clarity concerning the level of protection ensured by the participating sites.

In its discussions with the Working Party Microsoft has clarified that they do not control the data protection practices of participating sites but that, through their contracts with such sites, they impose a number of safeguards, for example obliging them to have a prominent and readily accessible privacy policy that conforms to industry practices, to take adequate security measures, to comply with applicable laws, and not to use data beyond the provision of specific services without user consent.

Microsoft has made a commitment to take a number of additional steps:
- To revise the privacy statement to state clearly that Microsoft does not control the data protection practices of the participating sites (0-4 months).
- Microsoft will encourage participating sites to join TRUSTe, BBBOnLine, or similar services (0-4 months).
- Participating sites will be offered the opportunity, both on the page that collects personal information and, in a more detailed form, via a link from that page, to inform users of the purposes for which the site will use the data, its recipients and how long it will retain the data (8-18 months).

The Working Party advises Microsoft to inform the participating sites with the shortest possible delay of its recommendation on certain minimum requirements for collecting personal data on-line in the European Union.[10].

It should be clarified in any case that, apart from of the role that Microsoft plays within the .NET Passport system, all participating sites are to be considered as data controllers in respect of their own processing operations. They have therefore their own responsibility to comply with privacy legislation.

2.2.5. The necessity and conditions of use of a unique identifier.

From the moment it started its analysis of the Passport system, the Working Party was concerned about. NET Passport’s use of a single identifier – the PUID – for each user.

The Passport unique identifier (PUID) is generated at registration and persists for the life of the account. It is 64 bits in length and composed of two parts: 16 bits to identify the data centre from which it was generated and 48 bits to identify a specific account. The primary requirement for generating the PUID is that it be unique. The PUID is not based on any information provided by the account holder and there is no information about the account holder information that can be derived from the PUID.

The PUID is primarily used as an index into site-specific data stores. A PUID alone does not permit login access or access to a user’s profile information. Only a correctly formed authentication ticket (which includes the PUID), encrypted in the key assigned to the Participating Site, can be used as a session token. Any user can have one or more PUIDs since there is a PUID for each Passport account and users can have more than one Passport account.

[10] Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union, adopted on 17 May 2001, WP 43.

The Working Party was principally concerned that use of the PUID would enable participating sites to communicate to each other information about .NET Passport users and build user profiles. The contracts between Microsoft and affiliated sites prohibit selling PUID registers to third parties or cross-site linking without user consent and impose severe restrictions on the use of the PUID but, notwithstanding this fact, a risk always exists when the technical possibility is available. Another issue raised by the Working Party was the possibility for users of having access to his own PUID.

Concerning the second point, Microsoft has made a commitment to allow users to access their PUIDs on request (8-18 months). The Working Party would like to draw attention to the excessive delay for the possibility of exercising the access right to the PUID. Even if the access is not provided on-line, other means should be provided to users to exercise their right from now on.

Extensive discussions have taken place between Microsoft and the members of the Internet Task Force regarding the use of a single identifier at all. Microsoft understands the concerns of the Working Party and has agreed to continue to explore alternative identification architectures for .NET Passport. It has been agreed with Microsoft that the discussion about this issue will continue in the future in order to see if an adequate alternative can be found.

2.2.6. The exercise of the rights of the data subjects.

The Working Party was concerned about existing problems relating to the rights of the data subjects and in particular of problems encountered when trying to unsubscribe from Passport.

During its contacts with the Working Party Microsoft has recognised that some problems existed in the past and has agreed to put in place several measures to facilitate users' exercise of their rights .

- To provide a prominent, readable summary of the information required by Article 10 of the Directive in the prompt box, including information as to the rights of the data subject (no later than April 2003).
- To inform the users in the privacy statement and in the introductory mail that they should direct inquiries and requests to passpriv@microsoft.com (current practice and 0-4 months).
- To respond to inquiries and requests from Passport users in the customer's language, provided it is one of the languages in which Passport is available (0-4 months).

Since September 2002 the users have been able to close their .NET Passport account easily by going to passport.net and clicking on the "Member Services" link. The user will then be guided through the steps of how to close his particular Passport account. For accounts created at passport.net, the process is completely automated. The user is presented with a page describing the consequences of closing the account and is provided with a button to click to close it. For accounts created at Hotmail, the process is very similar: the user is first directed to the Hotmail site, which presents the closure page.

2.2.7. *The security risks associated to these operations*

The Working Party also examined the possible security risks, especially those associated to the concentration of data in two big databases, that the system could bring with it. These concerns were also due to the fact that Microsoft is a high-profile target for hackers.

The Working Party has taken note of the fact that Microsoft has put in place an Information Security Program in the framework of the Consent Order issued by the Federal Trade Commission in 2002. . Major requirements are:
- Inclusion of appropriate administrative, technical, and physical safeguards, including a revised security policy based on ISO 17799. Standard operating procedures for each major group will be modified as necessary to ensure compliance with the Information Security Program. These procedures will be updated as necessary according to technology and business evolution.
- Designation of an employee or employees who will co-ordinate and be accountable for the Information Security Program. Key stakeholders within all involved groups will assist in the creation and implementation of standard operating procedures that implement the Information Security Program.

Several programs are being formalised and documented in parallel with the implementation of the revised ISP. These programs include:
- Security Training for Operations & Application Development Teams.
- Incident Response & Escalation Procedures
- Creation of a divisional Security Oversight Group.

2.3. Conclusion

The Working Party welcomes the important steps that Microsoft has taken and is going to take in the next months in order to ensure the compliance of the .NET Passport system with the European Data Protection Directive. Needless to say, the Working Party will closely follow the evolution of the system during the following months in order to observe how the measures announced by Microsoft are being implemented.

The Working Party also takes note of the concerns, expressed also by NGOs, about the setting up of a centralised system of personal data storage. The Working Party will continue monitoring the issue, also with regard to the security features.

Therefore, due to the evolving nature of the .NET Passport service, to the possible developments of its future architecture and to the need for continuos reflection on a number of the above-mentioned issues, and particularly the PUID, the Working Party will continue to monitor the deployment of the system and its future development, where necessary in dialogue with Microsoft. Microsoft has agreed to report to the Working Party about the steps taken regarding the .NET Passport system.

3. CASE- STUDY 2: THE LIBERTY ALLIANCE PROJECT

3.1. Short description of the system

Formed in December 2001, the Liberty Alliance Project is a contract-based group, now comprised of more than 100 companies, non-profit organisations and governments world wide. The Liberty Alliance Project is not a legal entity, but an ad hoc project in which different companies participate, pursuant to the terms of an agreement.

The mission of the Liberty Alliance Project is to establish open standards for federated network identity through open technical specifications. Simplified sign-on and federated network identity (a system for binding multiple accounts for a given user) are key elements of the system. Single sign-on is the ability of the consumer to authenticate once in a session with an Identity Provider and later on navigate to various Service Providers within a Trust Domain without having to re-authenticate.

The system will work within trusted domains or circles of trust, these are a federation of Service Providers and Identity Providers that have business relationships based on the Liberty Alliance architecture and operational agreements and with whom Principals can transact business in a secure and apparently seamless environment.

The Liberty Alliance Project specifications are still in a very preliminary phase of development and hardly any implementation exists at the moment[11]. It is expected that in the future the LA specifications will be implemented by technology companies to create Liberty-enabled technologies.

3.2. Analysis of the present situation

- The protocol as it presently stands allows compliance with the requirements of the Directive. The Working Party would like to emphasise the fact that the Liberty Alliance bears responsibility as far as the technical development of the project is concerned. They should make sure that the specifications and protocol they design allow those using them to comply with the Directive. In addition to that, each of the participating companies are data controllers when they operate a Liberty-enabled site and will also bear the responsibility of complying with the existing data protection legislation in this context.

- The Liberty Alliance protocol is neutral regarding data protection. It allows compliance with the Directive but certainly does not require it and no measures are taken concerning enforcement. The Working Party wishes to encourage the Liberty Alliance to develop recommendations and guidelines that motivate companies to use the specifications in a privacy-compliant or even enhancing way. The system could also include specific features linked to the specificity of the European legislation in this field. This might be especially important concerning the identity providers who will be in the possession of a vast amount information about the users.

- The Working Party has noted that many companies within the Liberty Alliance are American-based and the expectation is that the use of the specifications will in practice mean that quite a lot of personal data will be transferred from Europe to the US.. The Working Party encourages the US companies participating to the Liberty Alliance project to guarantee an adequate level of protection for the personal data transmitted to them.

- Presently, given the very limited development of the Liberty Alliance and the fact that is not yet used in practice, it is difficult to foresee exactly what the consequences of using pair-wise identities will be. The Working Party would like to stress however that the system of pair-wise IDs has the advantage of not creating one unique identifier for the user, however, it is necessary to continue considering this issue from the data protection perspective, in particular concerning the technical possibility of sites sharing personal data of the user without his consent.

[11] Sun One is Liberty-enabled.

Even thought pair-wise identities appear to be a looser identifier than one general identifier, the technical possibility to share them among participating sites remains an issue which raises some concerns.

3.3. Some considerations of the possible issues at stake in the future

At this moment, the Liberty Alliance specifications are just a prototype that have hardly been used in practice and will certainly undergo many changes in the future.

The Working Party would therefore like to continue to follow this development in the future in order to make sure that the requirements of the Directive are taken into account. In this regard, consideration should be given to, for instance, the use of cookies, the possibility for the users to actively refresh the handle[12], the automated federation[13], the role of the identity providers[14], the notion and the functioning of the "circles of trust" and the contracts that will be signed between the companies using a federated identity.

The Working Party would like to invite Liberty Alliance to reflect about the issues raised in case-study 1 and to bear in mind the conclusions of the Microsoft discussions when reflecting about similar issues with respect to their specifications. In particular, all considerations given to the PUID issue should be considered when dealing with the opaque handles and pair-wise identities in the Liberty Alliance context.

4. COMPARISON OF THE PRESENTLY EXISTING ON-LINE AUTHENTICATION SYSTEMS

Mozilla Password manager	**Authentication by Proxy**	**Microsoft Passport**	**Liberty Alliance**
No third party identity provider	Third party identity provider chosen by the end user	Microsoft as third party identity provider	Third party identity provider chosen by the service provider (mutual contracts)
Access via own PC only	Access via the channels offered by the authentication provider	Possible access via different devices, currently mainly PC-like	Possible access via different devices, among which mobile phones.
Currently available and widely used	Limited availability	Currently available and used by all Microsoft services	First implementation stages.
User ID and password per site	User ID and password per site	Single user ID and password	Password and user ID per site
User is identified with user ID and password	User is identified with user ID and password	Single unique identifier for a user (PUID)	Different handle per pair of sites

[12] The opaque handle is the means used for the account linking of multiple local accounts within the trust Domain. It is recognised by any two providers in a trust domain. a "handle", It is a random complex character sequence, which each provider associates with its own record of the user.

[13] The Liberty Alliance project uses account federation to enable users to link or terminate accounts. Automated federation can raise specific issues.

[14] A Liberty-enabled entity that creates, maintains, and manages identity information for Principals and provides Principal authentication to other Service Providers within a "circle of trust".

No contract needed	Contract between end user and provider	Contract between Microsoft and service provider	Contract between every site in a circle of trust
-	Authentication protocol requires proxy provider to know which sites with authentication are visited (storage of UID/password combination per site)	Microsoft uses a unique PUID per user	Unique handle per user per federated pair of site. Authentication provider needs to know only sites where the identity is federated.
Using different user ID's, end user can prevent service providers from combining data among themselves	Using different user ID's, end user can prevent service providers from combining data among themselves	Unique PUID identifies the user. Contractual agreements prevent service providers to combine their data	Data on users can be combined by pairs of sites only. Sites determine their own mutual contracts.
Service provider is the only data controller	Both service provider and proxy provider are data controller	Service provider dealing with authentication requests and Microsoft are data controller	Service providers within a circle of trust become data controllers at the time users visit their sites.
No data transfer between controllers	Authentication information is passed between controllers	Authentication and in some cases profiling information is passed between controllers	Authentication information is passed between controllers
User controls all communication	User consent needed	User consent needed (required by MS's implementation and contracts)	Normally, user consent is needed twice per federation, but automatic federation is possible
Authentication protocol does not require cookies	Authentication protocol does not require cookies	Current implementation uses cookies	Current implementation uses cookies

5. CONCLUSION

The Working Party would like to emphasise that the conclusions reached through the two case-studies should be considered as being of general application to any on-line authentication system when dealing with similar issues. The two case-studies have been chosen taking into account the present development of the on-line authentication market but any similar services should bear in mind the same data protection considerations. This could be summarised as follows:

- Both those who design and those who actually implement on-line authentication systems (authentication providers) bear responsibility for the data protection aspects, although at different levels. Websites making use of these schemes (service providers) also have their own responsibility in the process. It is advisable for the different players

to have clear contractual agreements between them where the obligations of each party are made explicit.
- All possible efforts should be made to allow anonymous or pseudonymous use of on-line authentication systems. Where this would inhibit full functionality, the system should be built to require minimal information only for the authentication of the user and to give the user full control over decisions concerning additional information (such as profile data). This choice should exist both at the level of the authentication provider and of the service providers (the sites making use of the system).
- It is vital to provide adequate information to the users concerning the data protection implications of the system (controller identity, purposes, data collected, recipients and so on). This information should be provided in an easily accessible and user-friendly way, preferably through the collection form or via a prompt box that would automatically open on the screen of the user, and in all the languages in which the service is offered.
- When personal data are to be transferred to third countries, authentication providers should work with service providers who take all necessary measures to provide adequate protection[15] or that put in place sufficient safeguards to ensure the protection of the personal data of the users of the system, by using contracts or binding corporate rules. This should be the general rule. If in particular cases consent is used as a basis for the transfer, sufficient information and choice should be given to the users. They should have the option to agree or not to the transfer on a case by case basis.
- The use of identifiers, whatever form they take, entails data protection risks. Full consideration should be given to all possible alternatives. If user identifiers are indispensable, the possibility of allowing the user to refresh the identifier should be considered.
- The adoption of software architecture that minimises the centralisation of personal data of the Internet users would be appreciated and encouraged as a means of increasing the fault-tolerance properties of the authentication system, and of avoiding the creation of high added-value databases owned and managed by a single company or by a small set of companies and organisations.
- Users should have an easy means to exercise their rights (including their right to opt-out) and to have all their data deleted if they decide to stop using an on-line authentication system. They should also be adequately informed about the procedure they should follow if they have enquiries or complaints.
- Security plays a fundamental role in this context. Organisational and technical measures that are appropriate to the risks at stake should be taken.

Due to the evolving nature of both the .NET Passport service and the Liberty Alliance project and of other similar authentication services, the Working Party will continue to monitor future developments in this field, in **particular to ensure that the commitments made by Microsoft are honoured within the proposed timeframe, as outlined in** chapter 2 of this document.

Done at Brussels, 29 January 2003
For the Working Party
The Chairman
Stefano RODOTA

[15] This is possible for instance in the United States for those companies eligible for the safe harbor, that should be encouraged to join this scheme. This obviously only applies in the cases in which the company in the third country does not fall under the scope of application of the Directive.