10054/03/IT
WP 68

Documento di lavoro relativo ai servizi di autenticazione *on-line*

adottato il 29 gennaio 2003

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995[1],

visti gli articoli 29 e 30 paragrafi 1, lettera a), e 3 di detta direttiva,

visto il proprio regolamento interno, in particolare gli articoli 12 e 14,

HA ADOTTATO IL PRESENTE DOCUMENTO DI LAVORO:

1. INTRODUZIONE: L'ESPANSIONE DEI SERVIZI DI AUTENTICAZIONE ON-LINE

Il frequente ricorso a servizi di autenticazione on-line ha cambiato il paesaggio di Internet[2]. Sempre più siti web propongono o chiedono ai visitatori di registrarsi, ad esempio perché forniscono informazioni riservate, oppure offrono all'utente la possibilità di registrare le proprie preferenze, forniscono un servizio che richiede una remunerazione o perché scopo del loro servizio è la fornitura di beni. Tutti questi siti chiedono all'utente di identificarsi, spesso mediante l'indirizzo e-mail, e di confermare la registrazione con una password.

L'uso della combinazione "nome utente/password" può creare dei problemi ai fornitori di servizi:
- gli utenti tendono a dimenticare la password. Un numero crescente di chiamate o di e-mail che giungono ai centri di assistenza riguarda password dimenticate. I costi dell'attivazione di nuove password stanno diventando un onere gravoso per i siti web;

- sempre più utenti si connettono a Internet in modi diversi, ma esigono lo stesso servizio dal fornitore. I vari tipi di accesso possono fondarsi su configurazioni tecniche diverse, dall'accesso da un PC al WAP, ma spesso la connessione a Internet avviene da computer diversi, in "Internet caffè" o biblioteche pubbliche. In tal modo gli utenti sono costretti a ricordare diverse password;

- alcuni utenti infine non amano inserire nome utente e password in quanto lo considerano un ostacolo alla navigazione. Gli utenti tendono a minimizzare lo sforzo richiesto scegliendo password brevi che non risultano sicure e spesso sono utilizzate per accedere a diversi siti.

Qualsiasi soluzione ai tre problemi citati comporta una delega parziale del processo di autenticazione da parte dell'utente. Attualmente esistono quattro possibilità:

- la gestione della password è delegata al browser sul PC dell'utente, come nel caso del gestore di password Mozilla;

---

[1] Gazzetta ufficiale L 281 del 23/11/1995, pag. 31, disponibile sul sito: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

[2] Come il gruppo di lavoro ha già rilevato in precedenti documenti, i principi della direttiva si applicano anche alle attività *on-line*. Vedere per esempio il documento di lavoro "Tutela della vita privata su Internet - Un approccio integrato dell'UE alla protezione dei dati on-line", adottato il 21 novembre 2002, WP 37.

- la gestione della password è delegata a un proxy server su Internet, messo eventualmente a disposizione da un fornitore di servizi Internet;
- l'autenticazione è gestita da terzi che utilizzano un protocollo di autenticazione specifico, come avviene nel caso di Microsoft .NET Passport;
- l'autenticazione è effettuata da una parte contraente nell'ambito di un "circuito di fiducia". Viene utilizzato un protocollo specifico, come quello del "Liberty Alliance project".

Queste possibilità sono analizzate nei paragrafi che seguono.

1. Gestione della password sul PC

Un gestore di password integrato nel browser di Internet risolve solo parte del problema. Non dovendo più inserire la password l'utilizzatore non rischia di dimenticarla. Questa forma di autenticazione non risolve tuttavia il problema di utenti mobili che accedono ai servizi da PC diversi.

Dal punto di vista della protezione dei dati la situazione è abbastanza semplice. Tutti i software sono installati sul PC dell'utente e sono sotto il suo controllo. Nessuna impresa esterna controlla i dati. Il sistema chiede all'utente se le informazioni vanno integrate nella base di dati del gestore di password, che inserisce la password, ma non la invia senza il consenso dell'utente. Per quanto concerne la sicurezza è necessario prendere provvedimenti adeguati per accertarsi che i documenti siano protetti da attacchi esterni.

2.Utilizzo di un proxy server

Anziché utilizzare un gestore di password installato sul PC dell'utente (ossia il browser), si può ricorrere alla stessa funzione integrata in un proxy server su Internet. Si tratta di una funzione paragonabile al più noto sistema del proxy anonimo. Un proxy server può servire numerosi utenti; perciò è necessario registrare una password per utente e per sito visitato. L'utente deve avere fiducia nel processo di registrazione; una fiducia espressa in modo esplicito in quanto la decisione di utilizzare uno specifico proxy deve essere pienamente consapevole (non c'è servizio di default). L'utente deve identificarsi sul proxy per utilizzare le sue password. Dopo l'identificazione il proxy offre all'utente gli stessi benefici del gestore di password installato sul PC. Il vantaggio del proxy consiste nella possibilità di accedervi da diversi PC e/o da altri dispositivi.

Questi proxy non dovrebbero mai trasmettere a terzi informazioni relative a un utente senza il consenso di quest'ultimo. Facendolo, perdono la fiducia dei clienti e di conseguenza la loro ragione d'essere. In genere viene stipulato un contratto tra il fornitore del proxy e il cliente. Il servizio probabilmente è pagato mediante fonti alternative alla pubblicità, eventualmente in combinazione con il servizio di un fornitore di servizi Internet.

3. Servizi di autenticazione on-line con protocolli speciali

Nessuna delle soluzioni descritte comporta modifiche al sito web del fornitore di servizi. Un'altra possibilità consiste nel procedere all'autenticazione ricorrendo a un protocollo speciale di autenticazione. Si tratta di protocolli con la stessa architettura basilare che consiste in tre parti: utente finale, fornitore di servizi e provider di autenticazione. Prima di accedere al fornitore di servizi, l'utente finale deve far verificare l'identità al provider di autenticazione. Il fornitore di servizi si fida del provider di autenticazione e consente l'accesso all'utente.

L'architettura di .NET Passport fa ricorso a un unico server di autenticazione, prodotto da Microsoft. Passport contiene dati di identificazione e di autenticazione come pure informazioni relative al profilo. In futuro queste due serie di dati verranno sempre più separate. All'utente che si connette a Passport è assegnato un identificatore unico, o PUID. Se l'utente vuole connettersi con un fornitore di servizi dà istruzioni al server Passport di trasmettere il PUID in una forma leggibile per il fornitore di servizi, in quanto di solito è criptato simmetricamente.

Il sistema "Liberty Alliance" utilizza un modello federato. L'utente può registrarsi congiuntamente presso due fornitori di servizi. Quando l'account è stato registrato, un fornitore di servizi accetta l'integrazione con l'altro, che funge da servizio di autenticazione.

Il gruppo è consapevole dell'espansione dei servizi di autenticazione on-line, pertanto alcuni mesi fa ha deciso di esaminare l'impatto di tali sistemi sulla protezione dei dati[3]. Consapevole anche dell'importanza di disporre di meccanismi sicuri di autenticazione per garantire la sicurezza e l'integrità di alcune operazioni elettroniche, in particolare di quelle connesse ai pagamenti on-line, il gruppo desidera tuttavia sottolineare che lo sviluppo di tali servizi deve rispettare i principi in tema di protezione dei dati stabiliti dalla direttiva relativa alla tutela dei dati personali[4] e dalle leggi nazionali che l'hanno recepita.

2. CASO N. 1: MICROSOFT .NET PASSPORT

.NET Passport è al momento un'iniziativa di considerevole importanza in questo settore. Per questa ragione il gruppo di lavoro ha proceduto in primo luogo a uno studio iniziale di tale sistema nella primavera 2002[5]. Dopo una prima analisi il gruppo ha concluso che nonostante alcuni provvedimenti adottati da Microsoft in risposta alle preoccupazioni relative alla tutela dei dati, numerosi elementi del sistema .NET Passport sollevavano problemi giuridici e richiedevano pertanto un ulteriore approfondimento.

Nei mesi successivi il gruppo di lavoro ha avviato un dialogo con Microsoft al fine di comprendere meglio il funzionamento del sistema, di discutere i diversi problemi sorti e in particolare di valutare la piena ottemperanza ai principi europei in merito alla tutela dei dati e, se necessario, individuare gli elementi dei sistemi suscettibili di modifiche. In seguito a questo dialogo molto aperto e positivo Microsoft si è impegnata a modificare il sistema apportando miglioramenti in termini di protezione dei dati.

L'impegno di Microsoft in merito all'attuazione tutti i provvedimenti discussi con il gruppo di lavoro è stato documentato da diverse lettere al presidente del gruppo, il professor Rodotà[6], e da un calendario che fissa le scadenze relative a ciascuna misura. Il carattere diverso delle misure giustifica le differenze dei periodi di esecuzione. Alcuni dei provvedimenti concordati, quali la revisione del testo concernente la dichiarazione di privacy di .NET Passport e l'aggiunta di informazioni nella pagina di registrazione, sono

[3] Cfr. WP 60, Documento di lavoro "Primi orientamenti del gruppo "articolo 29" in merito ai servizi di autenticazione on-line", adottato il 2 luglio 2002.
[4] GU L 281 del 23/11/1995, pag. 31, disponibile sul sito: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

[5] Cfr. WP 60, Documento di lavoro "Primi orientamenti del gruppo "articolo 29" in merito ai servizi di autenticazione on-line", adottato il 2 luglio 2002.
[6] Lettere datate 19 settembre e 25 novembre 2002.

semplici e possono essere attuati in tempi brevi. Altri, come il nuovo flusso informativo descritto di seguito, comportano considerevoli modifiche alla configurazione del servizio .NET Passport per cui richiedono tempi di attuazione aggiuntivi.

Il gruppo di lavoro ha preso atto del calendario presentato da Microsoft per rispondere alle preoccupazioni espresse. Sono stati fissati tre tipi di scadenze, che verranno indicate tra parentesi dopo ogni provvedimento: a breve termine (0-4 mesi), a medio termine (4-8 mesi) e a lungo temine (8-18 mesi). Nel frattempo alcuni dei provvedimenti discussi sono già stati attuati e nel presente testo vengono indicati in seguito come prassi attuale.

2.1. Breve descrizione del sistema Microsoft .NET Passport

NET Passport è un servizio di autenticazione su Internet che consente di accedere ai diversi siti partecipanti con un'unica registrazione, al fine di aiutare gli utenti a risparmiare tempo ed evitare loro l'inserimento ripetitivo di dati nel corso della navigazione su Internet. Non si tratta di un servizio di autorizzazione o di identificazione, ma di un servizio di autenticazione, con l'unico scopo di autenticare in modo univoco e certo l'identità di un utente mediante verifica delle credenziali fornite[7].
Realizzato nel 1999 il sistema è stato denominato .NET Passport nell'estate 2000. Attualmente in tutto il mondo esistono oltre 250 milioni di account (un utente può averne più d'uno, soprattutto se ha già diversi account Hotmail). Oltre 40 milioni di account appartengono a cittadini dell'UE.

Un Passport si può ottenere utilizzando:
- il sito www.passport.net
- un sito partecipante
- un account su Hotmail

Per registrarsi circa l'87% degli utenti si serve di un sito partecipante o di Hotmail, senza rivolgersi direttamente a Microsoft. Circa 120 milioni di account sono intestati a utenti di Hotmail e un'altra significativa percentuale di utenti si iscrive mediante Window Messenger. Hotmail è un servizio e-mail utilizzato in tutto il mondo gestito totalmente dalla Microsoft Corporation o da altre imprese controllate da Microsoft.

I dati personali raccolti attualmente sono suddivisi in tre categorie predeterminate:
1. informazioni minime: nome dell'utente (indirizzo e-mail) e password;
2. credenziali: domanda e risposta segrete, numero di telefono e codice PIN, codice di sicurezza e tre ulteriori domande e risposte di sicurezza, necessarie nel caso in cui l'utente dimentichi la password.
Tali dati non fanno parte del profilo e non vengono comunicati ad altri siti;
3. Informazioni complete sul profilo: i dati di cui sopra nonché nome, generalità, fuso orario, sesso, data di nascita, professione, reperibilità.
I siti partecipanti hanno la possibilità di chiedere direttamente all'utente ulteriori informazioni e trattarle. Attualmente 69 siti esterni (non collegati a Microsoft) partecipano a .NET Passport, di cui 22 appartenenti all'SEE.

.

[7] E' opportuno ricordare che oltre alla direttiva sulla protezione dei dati, altre direttive, come quelle sul commercio elettronico o sulla firma elettronica, possono essere applicate a questi servizi.

2.2. Aspetti giuridici del problema e risultati del dialogo con Microsoft

Nel documento del luglio 2002 il gruppo di lavoro ha individuato alcuni problemi giuridici che richiedevano un ulteriore approfondimento. I paragrafi successivi sono incentrati su ciascuno di questi problemi e sui risultati del dialogo con Microsoft relativo alle questioni sollevate.

Da un punto di vista generale è importante sottolineare che oltre ai provvedimenti specifici descritti nei successivi paragrafi Microsoft ha deciso di cambiare il flusso informativo relativo a .NET Passport. Essenzialmente il servizio sarà riconfigurato al fine di separare con chiarezza la creazione di un account .NET Passport dall'archiviazione dei dati personali nel profilo Passport. Come si spiegherà più dettagliatamente nel capitolo dedicato ai problemi di proporzionalità, il nuovo flusso informativo dovrebbe avere un impatto positivo sulla correttezza della raccolta e del trattamento dei dati personali. Il gruppo di lavoro ne prende atto con soddisfazione.

2.2.1. Informazioni fornite alle persone interessate al momento della raccolta, del successivo trattamento o del trasferimento dei dati personali a terzi, eventualmente ubicati in un paese terzo

Quando il gruppo di lavoro ha iniziato a studiare il funzionamento del servizio .NET Passport il primo problema affrontato è stata la mancanza di informazioni chiare e trasparenti relative a tale sistema. Alcune delle informazioni erano poco chiare, non fornivano ragguagli sulle principali questioni in tema di protezione dei dati (identità del responsabile, motivazioni del trattamento, diritti della persona interessata, destinatari dei dati, condizioni necessarie a garantire la correttezza del trattamento) e talvolta contenevano affermazioni contraddittorie.
Due punti in particolare preoccupavano il gruppo di lavoro, ossia l'assenza di informazioni precise sul trasferimento dei dati personali verso un paese terzo e sul collegamento tra Hotmail e Passport.

Per rispondere alle preoccupazioni del gruppo di lavoro nel frattempo Microsoft si è impegnata a prendere i seguenti provvedimenti:
- come ha raccomandato il gruppo di lavoro “articolo 29” nella raccomandazione 2/2001[8], Microsoft proporrà una finestra di dialogo che contenga le informazioni richieste dall'articolo 10 della direttiva presentandole in forma altamente accessibile, semplice e diretta. Un link verso la finestra di dialogo comparirà agli utenti che si identificano come residenti nell'Unione europea indicando il paese di residenza nella pagina di registrazione. Gli utenti che cliccano sul link vedranno apparire le informazioni in una finestra laterale. Questa funzione sarà disponibile entro l'aprile 2003;
- gli utenti che si iscrivono su un sito partecipante saranno informati sul paese in cui tale sito è ubicato (8-18 mesi), e attraverso la finestra di dialogo accederanno a un link verso la pagina web della Commissione europea con l'elenco dei paesi la cui legislazione in tema di tutela dei dati è stata dichiarata conforme alle norme dell'UE (4-8 mesi);
- mediante una finestra di dialogo Microsoft informerà gli utenti dell'UE in merito alla durata di conservazione dei dati di registrazione (attualmente non oltre 90 giorni) (0-4 mesi);
- sin dall'inizio della procedura gli utenti saranno chiaramente informati sulle modalità per aprire un account .NET Passport senza utilizzare il loro vero indirizzo e-mail, una

[8] Raccomandazione 2/2001 relativa ai requisiti minimi per la raccolta di dati on-line nell'Unione Europea, adottata il 17 maggio 2001, WP 43.

funzionalità che il gruppo di lavoro ha raccomandato di includere in diverse occasioni. Al tempo stesso gli utenti saranno avvisati dei limiti degli account pseudonimi in modo da poter prendere una decisione consapevole (8-18 mesi).
- Microsoft si è impegnata ad aggiornare contemporaneamente tutte le versioni linguistiche della dichiarazione sulla riservatezza dei dati di .NET Passport, eccettuati i casi in cui il contesto locale richieda modifiche immediate a una versione linguistica particolare. In simili eventualità, che dovrebbero presentarsi molto raramente, Microsoft segnalerà nelle altre versioni linguistiche della dichiarazione sulla riservatezza dei dati che le versioni mancanti saranno aggiornate entro breve (0-4 mesi).
- Microsoft si è anche impegnata ad intraprendere una serie di iniziative relative agli utenti di Hotmail al fine di garantire che nel momento in cui tali utenti si iscrivono a Hotmail siano anche informati che simultaneamente ottengono un account Passport (prassi attuale) e che quando si iscrivono a Hotmail siano consapevoli che devono ottenere un account Passport per poter accedere a Hotmail, e che non possono chiudere l'account Passport senza cancellare anche quello di Hotmail (0-4 mesi).

2.2.2. Valore e qualità del consenso accordato dalle persone interessate a tali operazioni.

In seguito all'analisi iniziale del sistema il gruppo di lavoro ha formulato alcuni interrogativi in merito alla validità e alla qualità del consenso come base giuridica per un trattamento conforme alle disposizioni dell'articolo 2 della direttiva[9]. In altri termini, il gruppo non era convinto che il consenso accordato dagli utenti fosse sufficientemente informato, libero e specifico, in particolare per quanto concerne gli utenti che si iscrivono attraverso Hotmail o la trasmissione dei dati personali ai siti partecipanti.

Secondo quanto spiegato, Microsoft ha preso e si è impegnata a prendere una serie di provvedimenti volti a garantire la correttezza delle informazioni fornite agli utenti. Inoltre per quanto concerne la possibilità che gli utenti decidano di non fornire i loro dati personali a Passport, il nuovo flusso informativo consentirà di comunicare i dati personali a un sito partecipante senza che vengano trasmesse al profilo Passport e di ottenere un account Passport pseudonimo che non implica la raccolta di ulteriori dati personali (8-18 mesi).

Per quanto riguarda gli utenti di Hotmail, oltre ai miglioramenti relativi alla qualità delle informazioni, vengono presi provvedimenti per avvisare gli utenti che quando aprono un account Hotmail i loro dati personali saranno utilizzati a fini pubblicitari (0-4 mesi). A tal fine sulla pagina di registrazione di Hotmail si spiegherà chiaramente agli utenti che accettando i termini e le condizioni del servizio opteranno per ricevere pubblicità da Hotmail. Come per tutti i siti partecipanti, gli utenti che si registrano su .NET Passport da un sito Hotmail potranno scegliere di fornire i propri dati personali solo a Hotmail senza conservarli nel proprio profilo .NET Passport (8-18 mesi).

Il gruppo di lavoro ha anche discusso con Microsoft la possibilità per gli utenti di Hotmail di non accettare pubblicità mirate. Microsoft ha spiegato che gli utenti con un account Hotmail possono scegliere liberamente di non ricevere pubblicità mirata, ma questo comporta la chiusura dell'account. Gli utenti non possono mantenere un account

[9] Per consenso della persona interessata s'intende ogni indicazione data liberamente, specifica ed informata dei suoi desiderata mediante la quale la persona interessata esprime il proprio accordo per il trattamento dei dati personali.

Hotmail gratuito senza ricevere pubblicità da Hotmail in quanto la pubblicità mirata è la fonte delle entrate che consentono la gratuità dell'account.
Il gruppo di lavoro continua a interrogarsi sulla conformità di questa prassi con la legislazione europea e in futuro continuerà a riflettere su questo punto. Va considerato tuttavia che la questione è connessa con un problema specifico, ossia la prassi seguita da diverse società in base alla quale la prestazione di un servizio è legata all'obbligo per il cliente di accettare l'utilizzo dei suoi dati a fini pubblicitari senza potersi opporre. Poiché il problema è distinto da quello specifico dei servizi di autenticazione on-line, oggetto del presente documento di lavoro, sarà affrontato in futuro in un contesto più ampio.

Per quanto concerne il consenso accordato dagli utenti ai siti partecipanti, la nuova procedura di registrazione consentirà agli utenti di ottenere un Passport che contiene solo nome dell'utente e password separando la creazione di un account Passport dalla scelta di comunicare i dati personali ai siti partecipanti o di conservarli nel profilo (8-18 mesi). Gli utenti saranno informati della possibilità di ottenere un Passport dal sito Passport fornendo unicamente nome dell'utente e password, e che se si registrano da un sito partecipante possono essere obbligati a fornire altre informazioni necessarie alle attività del sito (informazioni da includere nella finestra di dialogo tra 4-8 mesi). Sarà aggiunta anche una nuova funzione che consentirà agli utenti di decidere sito per sito se comunicare i dati rilevati dal loro profilo. I profili degli utenti saranno riconfigurati per consentire loro di cancellare i campi che desiderano e di lasciarne altri vuoti (8-18 mesi).

Il nuovo flusso informativo permetterà anche agli utenti, ogni volta che si registrano su un sito partecipante, di rileggere i dati del profilo, di modificarli decidendo se salvare le modifiche sul profilo Passport e di scegliere quali informazioni inviare al sito (8-18 mesi).

2.2.3. Proporzionalità e qualità dei dati raccolti e conservati da .NET Passport e successivamente trasmessi ai siti affiliati.

Il gruppo di lavoro era preoccupato per il volume dei dati raccolti attraverso Passport, in particolare dei dati relativi al profilo e per il fatto che se la persona interessata optava per la condivisione in seguito alla creazione di un .NET Passport, i dati personali rilevati erano trasmessi a tutti i siti visitati in cui l'utente si registrava, a prescindere dalla necessità di tali dati per i siti in questione. Quando è stato intrapreso il primo studio del sistema l'utente non aveva la possibilità di autorizzare la trasmissione di una sola parte dei dati, le informazioni del profilo erano considerate un blocco unico.

Il nuovo flusso informativo che sarà attivato da Microsoft separerà chiaramente la creazione di un account .NET Passport dalla decisione dell'utente di comunicare le informazioni personali al sito partecipante ed eventualmente a .NET Passport. Gli utenti avranno la possibilità di decidere, accordando il loro consenso, se conservare nel profilo .NET Passport i dati che scelgono di comunicare al sito su cui si registrano. Quando un utente che ha archiviato i suoi dati nel profilo .NET Passport visita altri siti partecipanti avrà la possibilità di modificare o di cancellare tali dati campo per campo prima di comunicarli al sito. L'utente potrà anche scegliere, accordando il suo consenso, di salvare le modifiche nel suo profilo .NET Passport (8-18 mesi).

Queste modifiche, unite al fatto che l'utente può decidere in alcuni casi di non utilizzare il suo vero indirizzo e-mail risponderanno alle preoccupazioni del gruppo di lavoro quando saranno attuate, sebbene il gruppo desideri continuare a monitorare la situazione,

specialmente per quanto concerne il ruolo svolto da Microsoft quale responsabile del trattamento dei dati personali e di altre importanti informazioni fornite dagli utenti.

2.2.4. Disposizioni a tutela dei dati applicate dai siti affiliati a .NET Passport.

Un'altra preoccupazione del gruppo di lavoro riguardava l'assenza di chiarezza relativa al livello di tutela garantito dai siti partecipanti.

Nel corso delle discussioni con il gruppo di lavoro Microsoft ha spiegato che non controlla le prassi dei siti partecipanti in merito alla protezione dei dati ma che i contratti conclusi con tali siti impongono alcune garanzie. I siti partecipanti sono tenuti per esempio ad attuare una politica di tutela della privacy efficace, facilmente accessibile e conforme alle prassi del settore, a prendere idonei provvedimenti di sicurezza, a rispettare la normativa applicabile in vigore, e a non usare i dati per scopi che trascendano la fornitura di determinati servizi senza il consenso dell'utente.

Microsoft si è impegnata a prendere alcuni provvedimenti supplementari:
- la dichiarazione di privacy sarà modificata al fine di indicare chiaramente che Microsoft non controlla le prassi dei siti partecipanti in merito alla protezione dei dati (0-4 mesi);
- Microsoft incoraggerà i siti partecipanti ad aderire a TRUST e, BBBOnLine, o a servizi analoghi (0-4 mesi);
- i siti partecipanti avranno la possibilità (tanto sulla pagina che raccoglie le informazioni personali quanto in forma più dettagliata, attraverso un link presente nella pagina) di informare gli utenti in merito allo scopo del trattamento dati, ai destinatari e alla durata di conservazione dei dati (8-18 mesi).

Il gruppo di lavoro consiglia a Microsoft di informare il più presto possibile i siti partecipanti dell'esistenza della raccomandazione relativa ai requisiti minimi per la raccolta di dati on-line nell'Unione europea.[10]

Occorre tuttavia precisare che, a prescindere dal ruolo svolto da Microsoft all'interno del sistema .NET Passport, tutti i siti partecipanti vanno considerati responsabili dei dati in rapporto alle loro operazioni di trattamento. Tali siti hanno pertanto una responsabilità diretta per quanto concerne il rispetto della legislazione sulla tutela della vita privata.

2.2.5. Necessità e condizioni d'impiego dell'identificatore unico.

Sin dall'inizio dell'analisi del sistema Passport il gruppo di lavoro era preoccupato per l'uso di un identificatore unico per ciascun utente, il PUID, da parte di . NET Passport.

L'identificatore unico di Passport (PUID) è generato all'atto della registrazione e ha una durata pari alla vita dell'account. Esso ha una lunghezza di 64 bit e si compone di due parti: 16 bit per identificare il centro dei dati dal quale è stato generato e 48 bit per identificare un account specifico. Requisito primario per generare un PUID è la sua unicità. Il PUID non si basa su alcuna informazione fornita dal titolare dell'account e dal PUID non può essere dedotta alcuna informazione sul titolare.
Il PUID è usato primariamente come indice in basi di dati specifiche per ogni sito. Un PUID da solo non permette né registrazione né accesso ai dati del profilo utente. Solo un

[10] Raccomandazione 2/2001 relativa ai requisiti minimi per la raccolta di dati on-line nell'Unione europea, adottata il 17 maggio 2001, WP 43.

ticket di autenticazione correttamente impostato (che include anche il PUID), criptato con la chiave assegnata al sito partecipante, consente di aprire una sessione. Ogni utente può avere uno o più PUID, poiché esiste un PUID per ogni account Passport e gli utenti possono avere più di un account Passport.

Una delle principali preoccupazioni del gruppo di lavoro concerneva l'utilizzo del PUID e il fatto che consentisse ai siti partecipanti di scambiarsi informazioni sugli utenti di .NET Passport e di costituire profili degli utenti. I contratti tra Microsoft e i siti affiliati non autorizzano la vendita degli elenchi PUID a terzi o collegamenti incrociati tra siti senza il consenso dell'utente ed impongono severe restrizioni all'utilizzo del PUID; tuttavia non è possibile eliminare i rischi, dato che la possibilità tecnica esiste. Un altro problema evidenziato dal gruppo di lavoro riguardava la possibilità degli utenti di accedere al proprio PUID.

Per quanto concerne il secondo punto Microsoft si è impegnata a consentire agli utenti di accedere ai propri PUID su richiesta (8-18 mesi). Il gruppo di lavoro desidera richiamare l'attenzione sul lungo periodo di attuazione relativo al diritto di accesso al PUID. Anche se non viene fornito l'accesso on-line, si dovrebbero mettere a disposizione altri strumenti per consentire agli utenti di esercitare sin d'ora il loro diritto.

Microsoft e i membri della *task force* "Internet" hanno discusso a lungo sulla necessità di utilizzare un identificatore unico. Microsoft capisce le preoccupazioni del gruppo di lavoro ed ha accettato di continuare a studiare architetture di identificazione alternative per .NET Passport. E' stato concordato con Microsoft che le discussioni su questo punto saranno portate avanti in futuro per valutare la possibilità di trovare un'alternativa adeguata.

2.2.6. L'esercizio dei diritti da parte della persona interessata.

Il gruppo di lavoro era preoccupato per l'esistenza di problemi relativi ai diritti delle persone interessate, in particolare per le difficoltà incontrate nel tentativo di cancellare l'iscrizione a Passport.

Durante i contatti con il gruppo di lavoro Microsoft ha riconosciuto l'esistenza di alcuni problemi in passato ed ha accettato di prendere provvedimenti per consentire agli utenti di esercitare più agevolmente i propri diritti.

- Introdurre nella finestra di dialogo una sintesi chiara e leggibile delle informazioni richieste dall'articolo 10 della direttiva, così come informazioni relative ai diritti delle persone interessate (entro aprile 2003).
- Informare gli utenti nella dichiarazione sulla privacy e nella e-mail iniziale che possono inviare domande e richieste all'indirizzo passpriv@microsoft.com (prassi attuale e 0-4 mesi).
- Rispondere a domande e richieste degli utenti di Passport nella loro lingua, a condizione che si tratti di una lingua nella quale Passport è disponibile (0-4 mesi).

Dal settembre 2002 gli utenti hanno avuto la possibilità di cancellare la propria iscrizione a .NET Passport facilmente, recandosi sul sito passport.net e cliccando sul link "servizio utenti". L'utente viene poi guidato attraverso diverse tappe a chiudere il suo specifico account Passport. Per gli account aperti sul sito passport.net, la procedura è completamente automatizzata. L'utente accede a una pagina che descrive le conseguenze

della chiusura dell'account e deve cliccare su un bottone per chiuderlo. Per gli account aperti su Hotmail la procedura è molto simile: l'utente viene prima indirizzato al sito di Hotmail dove accede alla pagina di cancellazione.

2.2.7. *Rischi per la sicurezza associati a tali operazioni*

Il gruppo di lavoro ha esaminato anche i potenziali rischi per la sicurezza, in particolare quelli associati alla concentrazione dei dati in due grandi basi di dati che il sistema può comportare. Tali preoccupazioni erano anche legate al fatto che Microsoft è un obiettivo di alto profilo per gli *hacker*.

Il gruppo di lavoro ha preso atto del fatto che Microsoft ha realizzato un programma per la sicurezza delle informazioni (*Information Security Program*) nel contesto dell'ordine di consenso (*Consent Order*) emanato dalla commissione federale per il commercio nel 2002. Le principali esigenze sono:
- l'introduzione di appropriate garanzie a livello amministrativo, tecnico e fisico nonché di una revisione delle politiche di sicurezza in base alla norma ISO 17799. Le procedure operative standard di ciascun gruppo principale saranno modificate, all'occorrenza, per garantire la conformità con il programma per la sicurezza delle informazioni. Tali procedure saranno aggiornate se necessario in funzione degli sviluppi tecnologici ed economici;
- la designazione di uno o più impiegati responsabili del programma per la sicurezza delle informazioni e del suo coordinamento. I principali rappresentanti di tutti i gruppi coinvolti contribuiranno all'elaborazione e all'applicazione delle procedure operative standard relative al programma per la sicurezza delle informazioni.

Parallelamente all'attuazione di un nuovo programma relativo ai fornitori di servizi Internet diversi programmi sono in fase di completamento, tra cui:
- formazione alla sicurezza per gruppi responsabili dello sviluppo di operazioni ed applicazioni,
- procedure di intervento e di ripristino in caso di incidenti,
- costituzione di un gruppo di supervisione della sicurezza settoriale.

2.3. Conclusioni

Il gruppo di lavoro è soddisfatto per gli importanti provvedimenti che Microsoft ha preso o sta per prendere nei prossimi mesi per garantire la conformità del sistema .NET Passport alla direttiva europea sulla protezione dei dati. Naturalmente il gruppo seguirà con attenzione l'evoluzione del sistema nei prossimi mesi per vedere come vengono applicati i provvedimenti annunciati da Microsoft.
Il gruppo di lavoro prende atto anche delle preoccupazioni espresse da organismi non governativi in rapporto all'istituzione di un sistema centralizzato di archiviazione dei dati personali. Il gruppo continuerà a monitorare il problema, anche per quanto concerne le funzionalità relative alla sicurezza.
A causa della natura evolutiva del servizio .NET Passport, dei possibili sviluppi della sua architettura e della necessità di continuare la riflessione su alcuni dei problemi citati (in particolare il PUID) il gruppo di lavoro continuerà pertanto a seguire la revisione del sistema e i suoi futuri sviluppi, se necessario in contatto con Microsoft. Microsoft ha accettato di riferire al gruppo di lavoro i provvedimenti presi in rapporto al sistema .NET Passport.

3. CASO N. 2: IL "LIBERTY ALLIANCE PROJECT"

3.1. Breve descrizione del sistema

Costituito nel dicembre 2001, "Liberty Alliance Project" è un consorzio che attualmente comprende più di 100 società, organismi senza scopo di lucro e governi in tutto il mondo. Il "Liberty Alliance Project" non ha personalità giuridica, ma costituisce un progetto *ad hoc* al quale partecipano diverse società conformemente ai termini di un accordo.
Obiettivo del progetto Liberty Alliance è definire standard aperti per un'identità federata sulla rete attraverso specifiche tecniche non proprietarie. L'autenticazione semplificata (*simplified sign-on*) e l'identità federata sulla rete (un sistema per collegare diversi account a un dato utente) rappresentano elementi chiave del sistema. L'autenticazione unica (*single sign-on*) consente al cliente di identificarsi una sola volta presso un provider di identità per navigare poi sui siti dei diversi fornitori di servizi all'interno di un dominio di fiducia senza doversi identificare nuovamente.

Il sistema funzionerà nell'ambito di domini o circuiti di fiducia; si tratta di una federazione di fornitori di servizi e provider di identità le cui relazioni commerciali si basano sull'architettura di Liberty Alliance e su accordi operativi e con i quali i committenti possono effettuare transazioni in un ambiente sicuro e privo di ostacoli.

Le specifiche del progetto Liberty Alliance si trovano ancora in una fase di sviluppo preliminare e al momento non esistono sostanzialmente forme d'implementazione[11]. Si ritiene che in futuro le specifiche di Liberty Alliance saranno implementate da imprese tecnologiche al fine di mettere a punto tecnologie compatibili con Liberty.

3.2. Analisi della situazione attuale

- Nella sua forma attuale il protocollo consente di rispettare le prescrizioni della direttiva. Il gruppo di lavoro desidera sottolineare che Liberty Alliance è responsabile dello sviluppo tecnico del progetto. Liberty Alliance deve garantire che le specifiche e il protocollo progettati consentano a coloro che li utilizzano di rispettare la direttiva. Ciascuna delle società partecipanti è inoltre responsabile dei dati quando utilizza un sito Liberty e sarà anche tenuta a rispettare la legislazione in vigore relativa alla protezione dei dati.

- Il protocollo di Liberty Alliance è neutro in rapporto alla protezione dei dati; consente l'ottemperanza alla direttiva ma sicuramente non la impone, inoltre non vengono presi provvedimenti per farne rispettare l'applicazione. Il gruppo di lavoro desidera incoraggiare Liberty Alliance a formulare raccomandazioni e linee guida che motivino le società a utilizzare le specifiche rispettando o promuovendo la tutela della sfera privata. Il sistema potrebbe anche integrare caratteristiche connesse con la specificità della legislazione europea in questo ambito. Si tratta di un aspetto che può dimostrarsi particolarmente importante per i provider di identità che si troveranno in possesso di una notevole quantità di dati relativi agli utenti.

- Il gruppo di lavoro ha constatato che numerose imprese partecipanti a Liberty Alliance sono ubicate negli Stati Uniti per cui si prevede che l'utilizzo delle specifiche implicherà in sostanza il trasferimento di una notevole quantità di dati personali dall'Europa agli Stati Uniti. Il gruppo di lavoro incoraggia le imprese statunitensi che partecipano al

[11] Sun One è compatibile con Liberty.

progetto Liberty Alliance a garantire un livello adeguato di protezione dei dati personali loro trasmessi.

- Attualmente, dato lo sviluppo estremamente limitato di Liberty Alliance e il fatto che tale sistema non sia ancora stato utilizzato, è difficile prevedere con esattezza le conseguenze dell'uso di "identità a coppie" (*pair-wise identities*). Il gruppo di lavoro desidera comunque sottolineare che il sistema delle identità appaiate presenta il vantaggio di non costituire un identificatore unico per l'utente; è tuttavia necessario continuare a studiare il problema dal punto di vista della protezione dei dati, in particolare per quanto concerne la possibilità tecnica dei siti che condividono i dati personali dell'utente senza il suo consenso.
Sebbene le identità appaiate sembrino un sistema più flessibile rispetto a quello dell'identificatore unico, la possibilità tecnica di comunicare i dati ai siti partecipanti desta alcune preoccupazioni.

3.3. Alcune considerazioni sugli eventuali problemi futuri

Attualmente le specifiche di Liberty Alliance sono semplicemente un prototipo che non è ancora stato verificato nella pratica e certamente subirà numerose modifiche in futuro.

Il gruppo di lavoro desidera pertanto continuare a seguire gli sviluppi futuri al fine di garantire che le prescrizioni della direttiva siano rispettate. Da questo punto di vista occorre prendere in esame l'utilizzo dei *cookies*, la possibilità per gli utenti di aggiornare il descrittore (*handle*)[12], il carattere automatico della federazione[13], la funzione dei provider di identità[14], il concetto e il funzionamento dei "circuiti di fiducia" nonché i contratti che saranno conclusi tra società che utilizzano un'identità federata.

Il gruppo di lavoro invita Liberty Alliance a riflettere sui problemi menzionati nell'analisi del caso n. 1 e a tenere conto delle conclusioni delle discussioni con Microsoft relative a problemi analoghi in rapporto alle specifiche del sistema. In particolare, i descrittori "opachi" e le identità a coppie nell'ambito di Liberty Alliance andrebbero studiati alla luce delle considerazioni formulate per il PUID.

4. CONFRONTO TRA GLI ATTUALI SISTEMI DI AUTENTICAZIONE ON-LINE

Gestore di password Mozilla	**Autenticazione mediante proxy**	**Microsoft Passport**	**Liberty Alliance**
Nessun provider di identità costituito da terzi.	Provider di identità costituito da terzi, scelto dall'utente finale.	Il provider di identità costituito da terzi è Microsoft.	Provider di identità costituito da terzi, scelto dal fornitore di servizi (contratti

[12] Il descrittore (*handle*) opaco è utilizzato per collegare tra loro diversi accout locali all'interno del dominio di fiducia. E' riconosciuto da ogni coppia di fornitori di servizi nell'ambito di un dominio di fiducia. Un "descrittore" è una sequenza casuale di caratteri complessi, che ogni fornitore di servizi associa al proprio file dell'utente.

[13] Il progetto Liberty Alliance utilizza la federazione degli account per consentire agli utenti di collegare o di cancellare account. La federazione automatica può porre problemi particolari.

[14] Si tratta di un'entità compatibile con Liberty che produce, conserva e gestisce dati relativi all'identificazione per i committenti e fornisce l'autenticazione dei committenti ad altri fornitori di servizi nell'ambito di un "circuito di fiducia".

			reciproci).
Accesso unicamente dal proprio PC.	Accesso mediante i canali offerti dal provider di autenticazione.	Accesso possibile da sistemi diversi, attualmente soprattutto PC.	Accesso possibile da sistemi diversi, tra cui il cellulare portatile.
Attualmente disponibile e ampiamente diffuso.	Disponibilità limitata.	Attualmente disponibile e utilizzato da tutti i servizi Microsoft.	Fasi iniziali di implementazione.
Nome dell'utente e password per sito.	Nome dell'utente e password per sito.	Nome dell'utente e password unici.	Password e nome dell'utente per sito.
Utente identificato mediante nome dell'utente e password.	Utente identificato mediante nome dell'utente e password.	Identificatore unico per utente (PUID).	Handle diverso per coppie di siti.
Nessun contratto necessario.	Contratto tra utente e fornitore.	Contratto tra Microsoft e fornitore di servizi.	Contratto tra tutti i siti nell'ambito di un circuito di fiducia.
-	Il protocollo di autenticazione richiede al fornitore di proxy di sapere quali siti sono visitati con l'autenticazione (archiviazione della combinazione nome dell'utente/password per sito).	Microsoft utilizza un PUID unico per utente.	Handle unico per utente per ogni coppia di siti federati. Il provider di autenticazione deve conoscere solo i siti dove l'identità è federata.
Usando diversi nomi dell'utente, l'utente finale può impedire ai fornitori di servizi di unificare i dati.	Usando diversi nomi dell'utente, l'utente finale può impedire ai fornitori di servizi di unificare i dati.	Un PUID unico identifica l'utente. Accordi contrattuali impediscono ai fornitori di servizi di unificare i dati.	Dati relativi agli utenti possono essere unificati solo da coppie di siti. I siti determinano i propri contratti reciproci.
Il fornitore di servizi è l'unico responsabile dei dati.	Il fornitore di servizi e il fornitore di proxy sono entrambi responsabili dei dati.	Il fornitore di servizi che gestisce le richieste di autenticazione e Microsoft sono responsabili dei dati.	I fornitori di servizi nell'ambito del circuito di fiducia diventano responsabili dei dati quando gli utenti visitano i loro siti.
Nessun trasferimento di dati tra servizi responsabili.	I dati relativi all'autenticazione sono trasmessi tra i servizi responsabili.	I dati relativi all'autenticazione e in alcuni casi al profilo sono trasmessi tra i responsabili dei dati.	I dati relativi all'autenticazione sono trasmessi tra i servizi responsabili.
L'utente controlla l'intera comunicazione.	Consenso dell'utente necessario.	Consenso dell'utente necessario (richiesto dall'implementazione di MS e dai contratti).	Normalmente il consenso dell'utente è richiesto due volte per federazione, ma la federazione

			automatica è possibile.
Il protocollo di autenticazione non richiede l'uso di *cookies.*	Il protocollo di autenticazione non richiede l'uso di *cookies.*	L'attuale implementazione utilizza *cookies.*	L'attuale implementazione utilizza *cookies.*

5. CONCLUSIONE

Il gruppo di lavoro desidera sottolineare che le conclusioni raggiunte a proposito dei due casi analizzati dovrebbero essere considerate globalmente applicabili a tutti i sistemi di autenticazione on-line quando verranno affrontati problemi analoghi. I due casi analizzati sono stati scelti in considerazione degli attuali sviluppi del mercato dell'autenticazione on-line, ma tutti i servizi simili dovrebbero tenere conto delle stesse considerazioni in tema di protezione dei dati, che si possono sintetizzare come segue:

- Tanto coloro che progettano quanto coloro che implementano i sistemi di autenticazione on-line (provider di autenticazione) sono responsabili degli aspetti relativi alla protezione dei dati, sebbene a livelli diversi. Anche i siti web che utilizzano tali sistemi (fornitori di servizi) hanno una loro responsabilità nel processo. E' opportuno che i diversi soggetti concludano tra loro chiari accordi contrattuali in cui siano esposti in modo esplicito gli obblighi di ogni parte in causa.
- Occorre impegnarsi a fondo per consentire l'utilizzo anonimo o sotto pseudonimo dei sistemi di autenticazione on-line. Nel caso in cui tale libertà ostacoli la piena funzionalità, il sistema dovrebbe essere concepito in modo da richiedere informazioni minime solo per l'identificazione dell'utente lasciando a quest'ultimo il pieno controllo delle decisioni relative alle informazioni supplementari (quali i dati del profilo). Questa opzione dovrebbe esistere a livello di provider di autenticazione e di fornitori di servizi (i siti che utilizzano il sistema).
- E' essenziale fornire agli utenti informazioni adeguate relative alle implicazioni del sistema in tema di protezione dei dati (identità dei responsabili del trattamento, scopi, dati raccolti, destinatari, ecc.). Tali informazioni dovrebbero essere fornite in forma facilmente accessibili e diretta, preferibilmente nel modulo di raccolta dei dati o mediante una finestra di dialogo che si apra automaticamente sullo schermo dell'utente, e in tutte le lingue in cui è offerto il servizio.
- Quando i dati personali devono essere trasferiti verso paesi terzi, i provider di autenticazione dovrebbero collaborare con fornitori di servizi che prendano tutti i provvedimenti necessari per assicurare un'adeguata protezione[15] o che offrano sufficienti garanzie relative alla protezione dei dati personali degli utenti del sistema, ricorrendo a contratti o a regole d'impresa vincolanti. Questa dovrebbe essere la regola generale. In casi particolari, in cui il trasferimento è legato al consenso dell'utente, quest'ultimo dovrebbe disporre di sufficienti informazioni e libertà di scelta. Gli utenti dovrebbero avere la possibilità di scegliere, caso per caso, se acconsentire od opporsi a un trasferimento.
- L'uso di identificatori, qualunque sia la loro forma, comporta rischi alla protezione dei dati. Occorre studiare attentamente tutte le possibili alternative. Se gli identificatori si

[15] Questo è possibile per esempio negli Stati Uniti per le imprese conformi al principio dell'approdo sicuro, che dovrebbero essere incoraggiate ad aderire al sistema. Evidentemente tale possibilità è pertinente solo nei casi in cui l'impresa del paese terzo non rientra nella sfera di applicazione della direttiva.

dimostrassero indispensabili si dovrebbe considerare la possibilità di consentire agli utenti di aggiornarli.
- L'adozione di un'architettura software che minimizzi la centralizzazione dei dati personali degli utenti di Internet sarebbe apprezzata ed incoraggiata sia per accrescere le proprietà di tolleranza ai guasti del sistema di autenticazione, sia per evitare la creazione di basi di dati ad elevato valore aggiunto controllate e gestite da un'unica impresa o da un piccolo gruppo di imprese ed organizzazioni.
- Gli utenti dovrebbero avere la possibilità di esercitate i loro diritti senza difficoltà (compreso il diritto di opporsi) e di far cancellare tutti i loro dati se decidono di interrompere l'utilizzo di un sistema di autenticazione. Essi dovrebbero anche essere adeguatamente informati sulla procedura da seguire in caso di domande o reclami.
- La sicurezza svolge un ruolo essenziale in questo contesto. Occorrerebbe prendere provvedimenti di carattere organizzativo e tecnico adeguati ai potenziali rischi.

A causa della natura evolutiva del servizio .NET Passport, del progetto Liberty Alliance e di servizi di autenticazione analoghi, il gruppo di lavoro continuerà a monitorare gli sviluppi futuri in questo ambito, in **particolare per garantire che gli impegni presi da Microsoft siano onorati entro i termini proposti, secondo quanto descritto nel** capitolo 2 del presente documento.

Fatto a Bruxelles, 29 gennaio 2003
per il gruppo di lavoro
il presidente
Stefano RODOTÀ