

THE PRIVACY RISKS OF PUBLIC KEY INFRASTRUCTURES

EXPOSING THE DANGERS THAT UBIQUITOUS DIGITAL SIGNATURES AND PUBLIC KEY INFRASTRUCTURES POSE TO INDIVIDUAL PRIVACY, AND EXPLORING SOME POSSIBLE SOLUTIONS

Austin Hill

and

Gus Hosein

Zero-Knowledge Systems, Inc.
Canada

Abstract

As we move closer toward the goal of ubiquitous public key infrastructures, we are encountering a growing number of serious dangers to individual privacy. Security and authentication of communications are essential to the growth of the Internet for commerce and social communications, but many problems exist that might create the infrastructure of a digital ID card that can be used to track individuals and infringe on their privacy.

This session will explore some of the existing tracking technologies and the dangers of adding widespread use of public key infrastructures to the Internet, and will also examine some technologies and techniques that balance privacy and individual rights with the requirements for authentication and security.

This session is non-technical and is geared toward policy makers and privacy advocates.

Specific topics to be discussed include:

- *Archiving of public speech.*
- *The true-identity certificate authority model.*
- *Marketing profiling technologies currently in use (e.g. Engage, DoubleClick).*
- *Private credential systems, private signature systems and pseudonymous certificate authorities.*

1.0 Toward the Public Key Infrastructure(s) and Essentials of Identity

The challenges for the Internet as we encounter the electronic marketplace and the digital society include security and privacy of communications and transactions. Before they purchase from a merchant on the Internet, users are demanding a level of security of their transaction; when dealing with merchants and portals, users would also like a level of residual privacy.

Experts traditionally discuss cryptography as the solution to these challenges. Cryptography conventionally introduces confidentiality into a transaction or communication. With the advent of public key cryptography in the 1970s came the opportunity for digital signatures, which provides for integrity checks. However, digital signatures involve public keys -- large numbers with no discernable owners. Thus entered the digital certificate: a public key with information that assists in identifying the owner. The integrity of the certificate is assured by a digital signature from a third party, often called the Certification Authority (CA). The collection of this set, the cryptographic algorithms and protocols, the keys, the certificates, and the CAs, is referred throughout this paper as a Public Key Infrastructure (PKI).

With this PKI, users can now traverse the World Wide Web or communicate via email securely, that is with *confidentiality*. Email and commercial transactions can be

effected with a level of security and certainty in the actual data that is being shared, i.e. with *integrity*. The certificate and the according Authority provide a level of security and certainty that email is being sent and received from known subjects (friends or colleagues), and products are being purchased from an authorized merchant by an authorized consumer and will always be verifiable in case of dispute, that is with *authentication* and *non-repudiation*. With this final phase of security -- authentication and non-repudiation -- a significant shift has occurred within the *spectrum of identity*: to an extent, the identity of people and institutions in the virtual world can be ascertained with near-true certainty.

While the spectrum of identity begins with anonymity and ends with true-identity, we have rarely been accustomed to this level of certainty in identity. In browsing, virtually and in reality, we are accustomed to anonymity to a large extent, while more practically we are in fact pseudonymous, and true-identity browsing occurs the least frequently, until recently at least. In communications, however, things are traditionally somewhat reversed. In the real world, identity is often revealed quickly and easily among companions and professional contacts, while in the marketplace, pseudonymity is practiced with credit card transactions, and anonymity is assured with cash.

The identity spectrum in Internet communications has always been an interesting dynamic. Anonymity is ever present, but in the case of communications, anonymous communication is deemed *pernicious*, as US Supreme Court Justice Scalia once wrote. The anonymous speaker is free from responsibility, while the identified speaker carries the full weight of complete responsibility for statements and actions. Although repudiation may exist in the real world for non-public figures to some extent, this is not the case in the virtual world with archived speech. In the middle of the spectrum lies pseudonymous communications, which sociologically is how the Internet community was built:

face to face communications never quite existed, and researchers and participants in discourse developed a reputation not only through their professional and accredited affiliations, but also through *reputation capital*. Over time, email addresses and userIDs in chat forums and email lists develop recognition for being wise or for being spammers, and so on, and develop a life and character.

Explicitly, this spectrum of anonymity--pseudonymity—true-identity can be applied on the Internet to electronic commerce, legal interchanges, information retrieval, and discourse. While other types of transactions may exist, for the purpose of illustrating the differences in amount of identity required and used, these will suffice.

In electronic commerce, users can browse through merchant sites with a level of anonymity: the merchants do not immediately know much about the browsing individual. However, marketing has become savvier with the introduction of profiling (of browsing consumers) and targeted advertising, with the assistance of techniques such as cookies, thus providing pseudonymous browsing. When the purchase occurs, often the consumer's identity is fully revealed upon payment or delivery; and even the browsing can occur with a true-identity divulging if the cookie, for example, is correlated with the purchase order.

Interaction with legal entities, such as governmental agencies, can be somewhat different. At the inquiry stage, mere browsing is occurring, such as the inquiring into social benefits and welfare. Profiling does not occur as often in these transactions, so pseudonymity is not often used overtly. However, plans on bringing social benefit administration to the Internet (such as with the US Social Security Administration¹) eventually incorporates a requirement for complete divulging of identity in order to receive benefits, and to change personal information on-line.

Researching or news retrieval on the Internet is again somewhat different. Free

information is available from many sites and browsing may be anonymous. However in some cases, cookies or IP addresses are used to track the movement of readers pseudonymously, where the cookie or IP address is not linked to a true-identity and is used for advertising, or maybe personalization of the news. However, some news sites, without necessarily requiring payment, do require registration (e.g. the *New York Times*), where users enter personal data and allows for a cookie to be placed on their systems to allow the information provider to monitor their reading habits.

Finally, in discourse, such as mailing lists, USENET groups, IRC, etc., the spectrum is balanced somewhat differently. Constructively, mailing lists and newsgroups have arisen through pseudonymous communications, where people from all over the world communicate with others through pseudonyms or by leaving behind an email address that means very little to participants outside of the discourse; and names and faces are often not important. Rather, reputations arise with time. Users can post anonymously to these discussion forums, but unless anonymous posters change anonymous-userIDs consistently, inevitably a reputation will develop. Meanwhile, rarely has the situation arisen where the members of a large discussion forum actually relied on true-identity.

The above examples were used merely as illustrations of the current state of affairs in the identity spectrum. However, this section began with the discussion of the need for security and privacy, and the introduction of cryptography as an infrastructure. This introduction (and not entirely inevitable development) of the Public Key Infrastructure will change the balance of the spectrum in each case. It is the purpose of this paper to argue that the PKI will in fact introduce an infrastructure of perfect true-identity, of security gained, and of privacy lost. Yet, privacy need not fall victim to advances in security, and coexistence is possible where many of the parties' interests are maintained and preserved.

2.0 Influences and Interests in PKI

The significant interests at play within the current security and privacy conflict include consumers and users, merchants and marketers, and government institutions. While there are no clear demarcations on specific intents and interests, and a high level of simplification is assumed, this section aims to provide some level of understanding as to what is being sought and what are the consequences of public key infrastructures.

2.1 Consumers and users

The interests of this group are that with electronic commerce and interaction with legal authorities, fraud is reduced and privacy is retained. Privacy is considered to include confidentiality of email and transactions, as well as control over personal information that is gathered and/or generated.

With the market in electronic commerce and information retrieval, the consumer interest does include personalization and ease of use. This can be achieved through merchants providing easy access to products and information that consumers wish to purchase, and for others, relevant or targeted advertising may be valued. Consequently, many consumers are also interested in gaining value for their personal information, and benefiting from loyalty schemes.

In discourse, the threat of archived speech and spam traditionally has participants concerned with the flow of personal information and the archiving of statements of opinion.

2.2 Merchants and Marketers

A synergistic relationship exists between the merchants and marketers on the Internet. Merchants would like to sell their products, and in order to assist them in this process, knowing the demands and desires of their customers would assist greatly. Thus they rely on marketing and

advertising companies to provide the merchants with customers, and some market information regarding these potential consumers.

This is advanced through customer profiling. Individual merchants can choose to track their site visitors with session-cookies² or with cookies that will be used when users return. While a lot can be learned from this, more advanced techniques exist that are not limited to learning from what customers review when they are visiting the site, and that will also provide targeted ads to people who browse consistent genres, i.e. *behavioral targeting*. To illustrate these techniques, let us examine more closely the leading marketing services providers on the Internet: DoubleClick and Engage Technologies.

2.2.1 DoubleClick

As of September 1998, DoubleClick has received over 3.2 billion requests for the delivery of ads generated by an aggregate of approximately 4,200 Websites or 440 Web publishers that are part of the DoubleClick 44-million-user worldwide network. From all of these sites and users, aggregate information is accumulated in a central database that assists DoubleClick in deciding on which banner advertising to place on the screen of a Web browser.

Using cookies under a technique entitled Dynamic Advertising Reporting and Targeting, DoubleClick can control the number of times a browser encounters the same advertisement, and decide on which particular ad would most appeal to a user.

With growing concerns in the market and among regulators regarding privacy and particularly cookies, DoubleClick is concerned that it will lose the ability to provide its service. DoubleClick is particularly uncertain about the future of the EU Data Protection Directive and its effects on transborder data flow.

2.2.2 Engage Technologies

Engage provides to merchants a service similar to DoubleClick. Engage recognizes itself as the world's largest database of *anonymous* Web-user profiles. Using a double-blind cookie management system, the identity of Web users is pseudonymized through a unique cookie to which merchant sites are oblivious, and to which only Engage has full access. Even then, acknowledging privacy interests, Engage does not relate true-identifying information with the cookie.

Engage manages to develop behavioral profiles on Web browsers based on long term browsing. The profiles are categorized among 22 different interests, such as Automobiles, Entertainment, Books, Hobbies, Stocks, etc. These profiles are stored centrally at the Engage data center and are released to merchants when required; however personally identifiable information such as name, e-mail, phone, etc., is reportedly not collected or stored, and therefore this is again a relatively pseudonymous collection of data. Assisting in profile development, clickstream data and registration demographics are also gathered.

Regarding privacy interests, in its Privacy FAQ, Engage promises:

"Engage Knowledge protects the privacy of Website visitors through anonymity. Web marketers do not need to know the personally identifiable information like name, address or e-mail address of a Website visitor. Instead, a Web marketer only needs the ability to distinguish one Website visitor from another and to recognize that visitor when they return to a site. By restricting the storage and access to the data collected, Engage prevents inappropriate use of the anonymous information and its association with personally identifiable information."

This is assisted by the difficulty in gathering such personally identifiable information. Like DoubleClick, however, Engage is concerned with the future where cookies are frowned upon and erased from hard drives by users.

Engage is thus looking for new techniques for gathering demographic and behavioral information.³

Meanwhile, Equifax, a firm that provides credit information on over 300 million people to companies world-wide, announced in April 1999⁴ that it was working on a new technique for online retailers to immediately gauge the credit-worthiness of Internet customers. Equifax's announced plan is to develop 'electronic ID cards.'

While cookies may or may not involve identity, anonymous cookies are in the interest of marketers and merchants. Pseudonymity thus exists largely through pseudonymous profiling, such as the service provided by Engage Technologies. Even multiple profiles exist, as profiles are destroyed and recreated, in effect multiple IDs. The *New York Times* Website, for example, requires cookie use for the free viewing of articles, as well as registration. According to the director of sales and marketing⁵:

"We follow two basic principles regarding gathering and using user data. First, we practice full disclosure so the user knows what their data will be used for. Second, we practice what we call 'optability'. This allows our users to **change profiles** and opt out of the process if they don't want to participate." [italics inserted]

Therefore, marketers and merchants are faced with multiple profiles, anonymous profiles, pseudonymous profiles, and **the need for** new techniques.

2.3 Government Agencies and Law Enforcement

Briefly stated, the interest of government and law enforcement agencies in particular tends towards perfect true-identity more frequently than it does towards sustaining privacy. Often contradictory efforts occur from governments, such as the EU as it passes its own Data Protection Directive, while also placing an interest in issues such as ENFOPOL.

Various governments have used the danger of immoral behavior as a reason to suppress anonymous speech, and on the Internet, legal and criminal cases have arisen due to anonymous and pseudonymous speech. Legal cases include the Raytheon case, and criminal cases include the sharing of child pornography on Bulletin Board Systems, etc.

The same applies for access to government services over the Internet: many governmental initiatives have assumed that access to services over the Internet will involve authentication of users first, information after.

At the same time, practically all governments have an interest in seeing their constituencies become the prime locations for electronic commerce, and therefore wish to pass laws and create policies that support this endeavor. If this can be done while meeting the interests of government agencies, then the situation can only be win-win for government. A good example of this is the discovery of FBI plans⁶ to develop a system to monitor activities on networks, to track 'patterns of patterns' of behavior, in order to prevent cracking attacks.

In summary for this section, various groups have different interests in privacy and security for the Internet, as well as the changing spectrum of identity. All groups, however, acknowledge that things are about to change. The development of PKI is one such change.

3.0 On Public Key Infrastructures

PKI, as it is being developed, consists of the transformation of public keys into certificates through the digital signatures of Certification Authorities, based on a hierarchical system of authorities. The X.509v3 standard for certificates is most common, and consists of numerous fields on top of the basic key and name, as follows:

This involves the creation of a global certificate authority, a central root to the hierarchy. According to a vice president at Chase Manhattan: "This venture seeks to address the key missing link in e-commerce today, particularly in the business-to-business environment. [...] That is establishing verifiably the identity of trading partners in open network."⁹

If it hasn't been governments trying to set up a national PKI, governments have been working hard on developing electronic commerce bills that support the legal validity of digital signatures under certain conditions. However, their interests, as briefly outlined in the previous section, comes clear in the specifications of their requirements, particularly any emphasis on identity. For example, consider the following national or multinational statements on digital signatures.

3.3 Singapore's Electronic Transactions Act 1998

The language of the act includes the defined 'subscriber,' that is "a person who is the subject named or identified in a certificate issued to him and who holds a private key that corresponds to a public key listed in that certificate."

The resulting digital signature will only be treated as secure and trustworthy if the "certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity."

And under enforcement, section 26 explains that any person who "knowingly misrepresents to a certification authority his identity or authorization for the purpose of requesting for a certificate [...] shall be guilty of an offence..."

In general the Act, and even press releases and general reports from the Singaporean government, hinge on establishing the *identity of the person* who owns the public key. A February 10, 1999 press release states:

"In the faceless world of the Internet, transacting parties may not be able to reliably verify each other's identity. A CA thus plays the important role of a trusted third party in vouching for the identities of holders of certificates that it issues (i.e. its subscribers). Parties participating in online transactions can, through the digital signatures created and the information contained in the certificates, reliably verify the identities of the transacting parties."

3.4 International Chamber of Commerce

Interestingly, this international group has very similar wording in its GUIDEC: General Usage for International Digitally Ensured Commerce report from 1997.

3.5 Canada

The Draft Uniform Electronic Commerce Act, as of March 15, 1999 defines an electronic signature as:

"information in electronic form that is associated with an electronic document by a person for the purpose of signing the electronic document; and/or information in electronic form that a person, directly or through an agent, associates with an electronic document for the purpose of establishing a connection between the electronic document and the person."

Thus, in order for legal status to be given to an electronic signature, the electronic signature must be reliable for the purpose of *identifying the person*.

Canada also has been working on developing a Government of Canada Federal PKI, with the following goal:

"To facilitate electronic commerce nationally and internationally and to achieve its goal of conducting business electronically whenever possible [...]. In order for electronic transactions to be seamless across Canada, it is important that similar infrastructures, policies and standards be adopted nationally."

The policy of true-identity as central to the value of a certificate and signature is thus

to be translated from Federal government initiatives to all recognized CAs in the country.

3.6 European Commission and European Union

In early work on digital signatures, the European Commission took a different approach to identity. In a 1997 Communication (Com97(503)), the Commission stipulated early that:

“Business partners sometimes do not have an interest in the precise identity of a particular person or entity, but only in the confirmation of previous contacts, in their affiliation to a defined group of persons, in their individual characteristics such as solvency and creditability or simply in unforged data.”

The Commission followed this with an example stating that credit card companies do not confirm the identity of the cardholder, but rather the presence of credit.

The Commission continues to state that in many cases people will have several key pairs corresponding to their different roles, in complete contrast with the X.500 philosophy. Moreover, the Commission states:

“Those persons not wishing or not obliged by law to communicate under their name can choose a pseudonym which safeguards their anonymity in transactions and communication (though the signatory is identified to the CA) whilst fully exploiting the integrity and authentication functions of digital signatures.”

Therefore, this creates a certificate relationship of *many user identities* to *many public keys*, in direct contravention to the notion of *one user identity* to *all applications* that is presented in the traditional x.500 worldview.

Thus, while some governments push for identity-based certification for use like a Social Security/Insurance Number for many, if not all, applications, others are

acknowledging that there may be a need not only for many certificates, but even pseudonymous certificates.

Beyond national and international policy, legislation, and government efforts, VeriSign is leading a significant commercial initiative.

3.7 An Identity-Intensive Commercial Implementation: VeriSign CA

VeriSign begins by stating clearly that its DigitalIDs address the problem of online impersonation, by providing an electronic means of verifying someone's *identity*.

VeriSign makes no effort to hide metaphors: the company continues to define DigitalIDs as the electronic counterparts to passports, driver licenses, and membership cards. Accordingly, VeriSign offers different classes of DigitalID akin to each level of identity verification.

Together -- the national policies, the Certification Authorities, the contents of the certificates -- this is what makes up a PKI. The following section combines this and previous sections to provide support to the argument that the PKI can be used as an infrastructure for surveillance.

4.0 Synthesis: Potential for Abuse

In Section 2, the interests and requirements of the consumer, the marketers, the merchants, and government institutions were briefly outlined. In Section 3, the PKI was presented. This section will synthesize these themes to argue that the PKI has a potential for abuse.

Our paper focuses on the issue of identity and the PKI rather than the confidentiality afforded by cryptography. The European Union recognized this difference in the process of creating its own policy on digital signatures, as outlined earlier. In an early policy statement, the Commission decided that pseudonymous certificates should be allowed for, and the reasoning for this was that:

“Without such a privacy safeguard, digital signatures could be abused as an efficient instrument for tracing individual on-line consumption patterns and communication or for intercepting, recording or misusing documents or messages.”¹⁰

The Commission thus acknowledged that the PKI could be used as an instrument of surveillance. The European Commission went through with implementing this in a *Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures*. The Committee of the Regions responded¹¹ with its opinion on the proposal with the following statement:

“The Committee expects the Commission ... to monitor from the point of view of privacy protection, that the technical ease of using electronic signatures does not lead to the introduction of recognition in transactions where it is not absolutely necessary. **Such a development could be regarded as posing a threat to, for example, transparency in administrative dealings by requiring recognition in situations where anonymity is appropriate.** Similarly, in electronic commerce, it would be enough in most cases to verify that a payment is effected by the client and received by the supplier.” [emphasis added]

Thus, the European Union is set to act on the idea that the PKI need not be true-identity based because it would threaten privacy; and in fact, there are occasions where anonymity is appropriate within an infrastructure that seems built and set on identity.

How exactly does it become an infrastructure for surveillance? Consider marketing and electronic commerce. In Section 2, both Engage and DoubleClick acknowledged concerns that the time may come when the method of cookies would become unacceptable to the consumer, and thus unprofitable. However, merchants would still want to know who is accessing their site, what exactly customers are interested in and what they

are looking for, while also providing advances in security and privacy to meet a market need.

Addressing these concerns, VeriSign published a white paper entitled *Digital IDs: The New Advantage*. In the white paper, VeriSign positioned the DigitalID, or the digital certificate, as the next replacement marketing tool for merchants.

First, VeriSign proposed that the certificate would replace the cumbersome username and password scheme that most sites have for registered users – one certificate could be used to access many merchant sites, while still uniquely identifying the customer in a way that is similar to a “driver’s license or passport.”

Second, VeriSign addressed cookies. Remarking that privacy concerns have been raised regarding cookies because users do not know when a cookie is passed or what information is in the cookie, and that cookies provide merchants with no mechanism for gathering information about first time visitors, VeriSign promotes the certificate again as the solution. VeriSign also states the following limitations **to cookies, as they:**

- “Offer no mechanism for third party verification of the identity of the user. Furthermore, everyone using a browser on a particular computer presents the same cookie to the server.
- Provide no way to track user information, such as demographic profiles, unless the site implements a full registration process.”

Yet, Engage Technologies even noted that it was not necessary for sites to have detailed personal information, because it was the practices and uniqueID that merchants truly sought, and not necessarily the name of each and every visitor to their site. But VeriSign argues that because the certificate provides security and encryption, it should be preferred over the cookie.

In a section entitled “A Better Solution: Using DigitalIDs to Identify Users”, VeriSign argues that the certificate allows for a unique identifier (the identity of the user) that allows the merchant to personalize information and advertising for each user, match behavioral patterns with a user’s profile, control a user’s access to a particular information or services, and secure email messages. The difference between then (section 2) and now (section 4) when it comes to electronic marketing, the merchants and marketers are given the identity of individuals who visit their site and present their certificates.

Just as the current US Government ACES certification policy admits that it is uncertain about the status of the specified digital certificates and how they fit under the EU Data Protection Directive, the VeriSign ‘solution’ is even more suspect.

5.0 Over-Emphasizing Identification

With the PKI, the type of profiling outlined in Section 1 becomes identity-based. Pseudonymity will no longer exist, and the only thing that will remain is the divulging of true-identity at every Internet purchase, every time information is accessed from government Web servers, at every newspaper article read on the Internet, and every time someone posts a message to a newsgroup. Repudiation, within the PKI, is gone.

The Public Key Infrastructure concept makes one very important and dangerous mistake very early in its establishment: it tends to assume that everything must revolve around the identity of the public key owner, and this identity is linked to some database. Relying on identity as a focal point, as the index, reveals far too much personal information, far more than is necessary, and in some cases, more than is legal.

As an alternative technology to PKI, being the Simple Public Key Infrastructure (SPKI)¹² outlines, “with the explosion of the Internet, it is likely that one will encounter keyholders who are complete strangers in the physical world and will

remain so. Contact will be made digitally and will remain digital for the duration of the relationship. Therefore, on first encounter, there is no body of knowledge to be indexed by any identifier.”

SPKI theorists argue that the X.509 type identifier is problematic. The consequence of the identifier is that it requires a GlobalID system in which people must be unable to repudiate an identifier, and must be unable to generate another (after all, why would someone who is not evil wish to change his or her name?). SPKI supporters argue that: “To make that scenario come true, one would have to have assignment of such identifiers (probably by governments, at birth) and some mechanism so that it is always possible to get from any flesh and blood person back to his or her identifier.” SPKI theorists argue that such a system only exacerbates the privacy situation by raising the possibility of using biometrics for that purpose. The concern is then that these certificates are required to purchase CDs and books online. SPKI then advocates the existence of multiple identities for one individual.

Another alternative scheme is AADS: Account Authority Digital Signatures. This scheme is idealized for financial transactions, and preserves privacy through its electronic commerce payment protocol x9.59. Arguing that it is not necessary for a merchant to know the identity of the consumer for payment, X9.59 would merely assure a merchant that payment is possible – that is the extent of the concerns for the merchant. As well, the certificates that exist will differ for each account held.

The likelihood of either of these alternative schemes becoming standard is not the point of the above discussion. Rather, the two alternative schemes show that not only is the implementation of X.509 PKI problematic, but its worldview is as well. Merchants do not need true identities, nor should a user be restricted to owning one certificate for use in multiple applications.

Furthering the SPKI notion of multiple certificates are the three types of digital certificates as outlined by Bohm, Gladman, and Ellison.¹³ The first type is the identity certificate, as outlined throughout this paper, but not relying on a unique identifier of a name. The second type is that of accreditation: a certificate that states that the owner is a member of a group without necessarily specifying the identity of the owner. So a certificate stating that the owner is a member of the Association for Computing Machinery should suffice for access to the ACM Digital Library, so long as there is a unique identifier such as a serial number. Finally, the third type is authorization and permission certificates: The CA delegates some form of authority to the key being signed (example given of a Bank authorizing the withdrawal of money using a certificate for account 742507). Again, no name is required; the account number should suffice.

The result is that not only are there many certificates to own such as in SPKI and AADS, but also not all the certificates relate back to personal information such as a true-identity, or a name. The existence of multiple identities also allows for the existence of multiple pseudonyms, since the identities need not relate directly to the true-identity, or the real name of the owner. There is no need for an x.500 type of *1 identity to 1 public key*. Rather it is safer to have *1 identity to many public keys*, or rather than *1 X.509 certificate to many applications*. The relationship can be reduced to *1 x.509 certificate based on pseudonym to each application*.

The EU recognized the dangers of a true-identity PKI in its policy statements and papers. A Memorandum by Members of the Global Internet Liberty Campaign to the UK Government was released in February 1999 that places the possibility of surveillance in an appropriate perspective. Although referring more to confidentiality and key escrow, the Memorandum had a key point: "Encryption has the power to authenticate the identity of these authors to their partners abroad, and protect their identity from despots at

home. [*To restrict encryption*] would mean a tremendous blow to international efforts to support the cause of human rights."

Conclusion

True-identity is not the panacea. Multiple IDs where some are pseudonyms is an alternative method to the surveillance infrastructure that the PKI may become. As a result, pseudonym management and pseudonymous certificates may meet the needs of the consumers, the market-sensitive merchants and marketers, and the government that wishes to support electronic commerce. Under this model, the only unhappy parties are marketers and merchants that gather hazardous amounts of personal data, and governments bent on creating an infrastructure of surveillance.

And the age-old balance between security and privacy is not the key issue. In the end, the essential endeavor is that the identity spectrum must remain balanced.

REFERENCES

- ¹ See *GCN Spotlight: Electronic Commerce*, by Richard W. Walker, in *Government Computing News*, May 3, 1999.
- ² Monitoring can also consist of tracking the IP addresses on each session, but this is assuming static IP addressing, which is a very large assumption.
- ³ Taken from the amended S-1 form for Engage Technologies, under Risks, at the Securities and Exchange Commission, dated July 19, 1999.
- ⁴ See *Equifax CEO: credit data to be sold online*, By Reuters, Special to CNET News.com, April 15, 1999, 4:00 p.m. PT.
- ⁵ Taken from *Got the Click-Through Blues?*, by Deborah Kania, in *Clickz Network Precision Marketing Column*, available at <http://www.searchz.com/Articles/0601991.shtml>.
- ⁶ See *Computer security readied, Targeting intruders: U.S. system, overseen by FBI, would protect vital government, industry data networks*, By John Markoff of the *New York Times*, July 27, 1999.
- ⁷ See *GCN Editorial: No risk, no gain*, *Government Computing News*, February 22, 1999.
- ⁸ As reported by Greg Woods, from the Minutes of the GiTS Meeting on May 6, 1999.
- ⁹ Taken from *Big banks back digital certificates*, By Tim Clark, Staff Writer, CNET News.com, October 21, 1998, 12:55 p.m. PT, URL: <http://www.news.com/News/Item/0,4,27800,00.html>
- ¹⁰ Taken from *Towards a common framework for electronic signatures*, Com(97)503, DGXIII, European Commission, 1997.
- ¹¹ Taken from *Opinion of the Committee of the Regions* on the 'Proposal for a European Parliament and Council Directive on a common framework for electronic signatures. (1999/C93/06), April 6, 1999, Official Journal of the European Communities.
- ¹² Taken from *SPKI Certificate Theory*, Internet Draft, Expires 3 December 1999, by Carl Ellison, Bill Frantz, Butler Lampson, Ron Rivest, Brian Thomas, Tatu Ylolen, May 28, 1999.
- ¹³ See *Digital Signatures, Certificates, and Electronic Commerce, ver 1.1*, by Brian Gladman, Carl Ellison, and Nicholas Bohm, June 8, 1999.