Identification, Authentication and Authorization on the World Wide Web[1]

An ICSA White Paper

M. E. Kabay, PhD [,CISSP-ISSMP]

[formerly] Director of Education,
International Computer Security Association[2]

Executive summary

The buying public are leery of engaging in electronic commerce largely because they worry that their electronic transactions will be insecure. Observers of the growing field of e-commerce concur that lack of consumer confidence is the key stumbling block to continued growth of business on the World Wide Web.

Both merchants and clients need to be confident of the identity of the people and institutions with which they are doing business. At a technical level, these concerns focus on *identification, authentication and authorization.* Identification consists of providing a unique identifier for automated systems; authentication consists of correlating this electronic identity to a real-world, legally-binding identity; and authorization consists of assigning rights to the authenticated identifier.

Encryption technologies play a crucial role in protecting confidentiality, integrity and authenticity in cyberspace. Standards for labeling Web sites' compliance with privacy policies help consumers judge where to do business. Digital certificates and electronic cash of various kinds allow authorization for purchases with varying degrees of assurance for customer privacy. Single sign-on systems allow clients to establish and prove their identity once and then shop at several electronic locations without further inconvenience. Systems for extending the content and flexibility of digital certificates allow Web sites to tailor their services more closely to the needs and demands of their clientele.

---

1 This paper was published in 1997. Ten years later, colleagues asked me to ensure that it would be available on my Web site, so I dug it out of my archives and reformatted it and converted the end-notes to footnotes. If I were writing this today, I would have used a different style of reference involving cross-references rather than duplicate footnotes. However, I chose not to spend the time required to revamp the references. I have also removed the embedded html links which are duplicated in the footnotes.

2 Currently [2007] CTO & Program Director of the MSIA, School of Graduate Studies, Norwich University. For contact information see < http://www2.norwich.edu/mkabay >

When users communicate securely with a merchant online on the Web, they may establish a *session* using any of a variety of authentication procedures such as giving a password, using a physical device (a *token*) or providing other evidence of their identity (e.g., *biometric* authentication). During the session that they establish, it is assumed that only the authorized person will transact business with the merchant. One practical problem for customers is that buying more than one object or service may require communications with many Web sites, each of which currently requires a separate identification, authentication and authorization cycle. This report discusses several approaches to providing a secure, convenient shopping experience for consumers on the Web.

Table of Contents

1. Introduction 5

2. Identification, Authentication and Authorization 7

2.1 Identification 7

2.2 Authentication 7

2.3 Authorization 8

2.4 The Role of Encryption 9

3. Frameworks for Secure E-commerce 11

3.1 Privacy 12

3.1.1 P3 12

3.1.2 TRUSTe 12

3.1.3 SSL 13

3.2 Identification 13

3.2.1 Tokens 13

3.2.2 FIPS 196 13

3.2.3 vCard 14

3.3 Authentication 15

3.3.1 Digital certificates 15

3.3.2 CCITT (ITU) X.509v3 Standard for Digital Certificates 15

3.3.3 SESAME -- European Standard for Digital Certificate Authentication 16

3.3.4 Third-party Certification Authorities 16

3.3.5 SET -- Authorization and Non-Repudiation 16

3.3.6 OFX -- Open Financial Exchange 17

3.3.7 Gold Standard 17

3.4 Authorization and Single Sign-On 17
3.4.1 Kerberos 17
3.4.2 OPS -- Open Profiling Standard for Authorization and Single Sign-On 18
3.5 Interoperability 18
4. Products 20
4.1 VeriSign Digital IDs 20
4.2 DigiCash 22
4.3 CyberCash 22
4.4 Xcert Sentry CA 23
4.5 Auric Systems ASA 23
4.6 Security Dynamics SecurID & ACE/Server 23
4.7 Bellcore's S/KEY 24
4.8 Internet Mall 24
4.9 Extending the Usefulness of Certificates 24
4.9.1 VeriSign Digital Certificates 24
4.9.2 NCR TrustedPASS 25
5. Concluding remarks 27
6. Appendix: Basics of Cryptography for E-commerce 28
6.1 Symmetrical Encryption Algorithms 28
6.2 Asymmetrical Encryption Algorithms: the Public Key Cryptosystem 29
6.3 Using the PKC to Protect Confidentiality 29
6.4 Using the PKC to Establish Authenticity 30
6.5 Using the PKC to Establish Integrity 31

1. Introduction

Internet commerce is a strategic tool for business today and all evidence is that it will grow rapidly in the coming years if potential customers can gain confidence in the safety of electronic commerce. E-commerce is widely seen as threatening the privacy of the individual[3] <http://www.digicash.com/news/archive/bigbro.html>. Several surveys indicate considerable concern by users about their privacy online[4] <http://www.etrust.org/webpublishers/privacypays_studiesresearch.html>. For example, in March 1997, the Boston Consulting Group (BCG) surveyed 9,300 people about privacy concerns. BCG found 76% of respondents expressed concern about sites monitoring browsing on Net; 78% said privacy assurance would increase their willingness to disclose private information on Net. Without privacy assurance, BCG expect $6B of Web business compared with $12B if privacy were assured. The Lou Harris organization surveyed 1,009 computer users in a national sample; more than 50% of users are concerned about the release of their e-mail address by those responsible for the Web sites they visit[5] <http://www.etrust.org/webpublishers/studies_BCG.html>.

In general, observers feel that lack of consumer confidence is seriously limiting growth of e-commerce. In one large survey, 70% of respondents were worried about safety of buying things online; 71% were more worried about Internet transfer of information than phone communications; and 42% said they refused to transmit registration information via the Internet[6] <http://www.etrust.org/webpublishers/studies_BCG.html>. Several other observers report that lack of perceived privacy is a major block to the growth of e-commerce[7] <http://www.digicash.com/news/room/art/gartners01.html> and that security is essential for e-commerce[8] <http://www.verisign.com/products/sites/serverauth.html>. Barriers to more effective e-commerce include poor security standards[9] <http://www.jcp.co.uk/research.html>. Indeed, the lack of confidence may be measurably slowing progress of e-commerce: the percentage of online purchases was roughly the same in 1996 as in 1995 according to a study by Dataquest, and consumers seem to think the Internet is not secure enough to give their credit-cards to a Web site[10] <http://www.zdnet.com/pcmag/news/trends/t970221a.htm>.

One of the vexing problems faced by consumers is the "cookies.txt" file in which browsers such as Internet Explorer and Netscape Navigator store information sent from Web servers to the

---

3 <http://www.digicash.com/news/archive/bigbro.html> Security without Identification: Card Computers to make Big Brother Obsolete. By David Chaum.

4 <http://www.etrust.org/webpublishers/privacypays_studiesresearch.html> Privacy Studies and Research Reveal Concern.

5 <http://www.etrust.org/webpublishers/studies_BCG.html> TRUSTe/BCG Survey.

6 <http://www.etrust.org/webpublishers/studies_BCG.html> TRUSTe/BCG Survey.

7 <http://www.digicash.com/news/room/art/gartners01.html> Future of Web Success Relies on Converging Micro-Payment Model with Privacy Technology. Gartners Group Leaders Online, September 1997. Michael Nash.

8 <http://www.verisign.com/products/sites/serverauth.html> Digital IDs for Servers: High-level Security at a Low Cost.

9 <http://www.jcp.co.uk/research.html> Electronic commerce; Analysis of a new business paradigm.

10 <http://www.zdnet.com/pcmag/news/trends/t970221a.htm> Ready, Set, Shop: New technologies inch us closer to cybershopping.

client. These records of client activity can be abused; for example, a Web server offering clothing might determine that a particular client had previously visited a Web site dealing with new car sales and accordingly pipe the user's name to a service sending junk mail or junk e-mail offering cars for sale11 <http://www.epic.org/privacy/internet/cookies/default.html>.

According to an independent group that monitors government activities, US federal Web sites are failing to protect user privacy. OMB Watch said, "There is no government-wide policy regarding privacy concerns on federal Web sites... Agencies collect personal information about visitors to their Web sites, but fail to tell them why that information is being collected and what it is being used for." After the report, three agencies that were collecting cookies files stopped doing so12 <http://www.techweb.com/se/linkthru.cgi?WIR1997082713>.

As for the economic consequences of this general lack of confidence, the evidence warrants serious investment in whatever is required to improve public confidence. According to a summary by JCP Computer Services[13] <http://www.jcp.co.uk/research.html> that summarizes several other studies, by the year 2000, KPMG says that the top 100 UK companies will have 20% of their revenue from e-commerce. Killen & Associates say in another report that by the year 2005, worldwide Internet e-commerce will be ~U$27M, about 50% of the revenue from credit-card sales at that time. JPC studied the average online transactions per household and by the year 2000, they expect online transactions per household will rise from 9 per year in 1997 to 120 per year. IDC, in a report published in *PC Magazine*, estimates that one of every three Internet users already buys goods over the World Wide Web and predicts that e-commerce revenues will double between 1997 and 2001[14] <http://www.zdnet.com/pcmag/news/trends/t970221a.htm>. In addition, micropayments mediated by secure electronic forms of payment may help Web-based businesses such as magazines become profitable; currently they are experiencing customer resistance to paying for annual subscriptions, but micropayments are expected to help users by allowing small fees for use of individual articles[15] <http://www.digicash.com/news/room/art/gartners01.html>. Similar micropayments may revolutionize the music and video business.

---

11 <http://www.epic.org/privacy/internet/cookies/default.html> Electronic Privacy Information Center: THE COOKIES PAGE.

12 <http://www.techweb.com/se/linkthru.cgi?WIR1997082713> Federal Websites Faulted For Privacy Practices. By David Braun.

13 <http://www.jcp.co.uk/research.html> Electronic commerce: Analysis of a new business paradigm. Introduction; What is Internet Electronic Commerce? What type of business is conducive to Internet Electronic Commerce? What is the business benefit of Internet Electronic Commerce? Where is Internet Electronic Commerce today? What are the barriers to achieving the benefits of Internet Electronic Commerce? The way forward: What should organisations be doing about Internet Electronic Commerce? Summary of JCP research findings.

14 <http://www.zdnet.com/pcmag/news/trends/t970221a.htm> New technologies inch us closer to cybershopping. (2/21/97)

15 <http://www.digicash.com/news/room/art/gartners01.html> Future of Web Success Relies on Converging Micro-Payment Model with Privacy Technology. Gartners Group Leaders Online, September 1997. Michael Nash.

2. Identification, Authentication and Authorization

Whether users know it or not, their concerns about e-commerce security are fundamentally those of remote access controls. Any time someone needs to transact business, whether online or face-to-face, the client and the merchant must both provide identification, authentication and authorization. Users need to be sure that they know exactly who is running the Web server with which they intend to transact business. Merchants need identification of their clients to be sure they get paid for their products and services.

In a startling case of breach of identification, authentication and authorization in 1996 and 1997, viewers of pictures on several Web sites were in for a surprise when they got their next phone bills. Victims who downloaded a "special viewer" were actually installing a Trojan program that silently disconnected their connection to their normal ISP and reconnected them (with the modem speaker turned off) to a number in Moldova in central Europe. The phone call was then forwarded to an ISP in North America which continued the session. The long-distance charges then ratcheted up until the user disconnected the session -- sometimes hours later, even when the victims switched to other, perhaps less prurient, sites. In New York City, a federal judge ordered the scam shut down; however, the site persists on the Web and includes warnings that law enforcement officials and those intending to bring legal action against the owners are not to log in (we do NOT recommend that you risk connecting to it). Later in 1997, the FCC ordered $2.6M in fraudulently obtained charges to be refunded to the embarrassed victims16 <http://www.businessknowhow.com/newlong.htm>.

2.1 Identification

Identification, according to a current compilation of information security terms, is "the process that enables recognition of a user described to an automated data processing system. This is generally by the use of unique machine-readable names"[17]. In human terms, client and merchant engage in mutual identification when they -- for example -- tell each other their names over the phone. In the Moldovan Trojan case, the violation of identification occurred when there was no provision at all for ascertaining the identity of the company running the scam.

2.2 Authentication

Authentication is "A positive identification, with a degree of certainty sufficient for permitting certain rights or privileges to the person or thing positively identified." In simpler terms, it is "The act of verifying the claimed identity of an individual, station or originator"[18]. In a human contact by phone, the client and merchant might recognize (authenticate) each other by their familiar voices. The Moldovan Trojan fraudulently violated the principle of authentication by claiming that its software was a file-viewer when it was actually an ISP-switcher as well.

16 <http://www.businessknowhow.com/newlong.htm> New Long Distance Phone Scam Hits Internet Surfers.

17 Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization) <glossary@sdsc.isu.edu> or <jlisi@romulus.ncsc.mil>.

18 Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization) <glossary@sdsc.isu.edu> or <jlisi@romulus.ncsc.mil>.

The classic methods for correlating virtual and physical identities in cyberspace are parallel to methods used for authenticating human beings in the physical world. The four categories of authenticating information are:

What you know -- the password or passphrase, for example;

What you do -- e.g., how one signs one's name or speaks;

What you are -- e.g., one's face or other biometric attributes such as fingerprints;

What you have -- e.g., a token such as a key or a certificate such as a driver's license.

All of these categories of authentication are used in cyberspace. The last example is particularly interesting: certificates play a crucial role in authenticating people (or programs or machines) in the world of e-commerce. The driver's license, for example, if assumed to be real, tells a merchant that at some time in the past, a certification authority -- the issuing department of motor vehicles -- has undertaken some measures to ensure that the information on the license is (or was) correct. In cyberspace, verifying the legitimacy of a certificate can be easier than in real space.

Authentication leads to an related concept, that of *non-repudiation.* A formal definition of non-repudiation is "Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data." Non-repudiation, as we shall see in the section below on encryption, depends on asserting that authenticity has not been violated when identifying the source of that transaction or message.

2.3 Authorization

Authorization is "The granting to a user, program, or process the right of access"[19]. In the real world, we experience authorization every time a merchant queries our VISA or MasterCard service to see if we are authorized to spend a certain amount of money at their establishment.

The Moldovan Trojan violated authorization by fraudulently appropriating the right to disconnect a phone call and initiate an expensive long-distance call without notification to or permission from the victim.

In the mainframe environment, authorization depends on the operating system and the level of security that system administrators have imposed. Identification and authentication (I&A) begin when a session is initiated. A session is "An activity for a period of time; the activity is access to a computer/network resource by a user; a period of time is bounded by session initiation (a form of logon) and session termination (a form of logoff)"[20]. However, on the Web, most interactions

19 Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization) <glossary@sdsc.isu.edu> or <jlisi@romulus.ncsc.mil>.

20 Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization) <glossary@sdsc.isu.edu> or <jlisi@romulus.ncsc.mil>.

are *sessionless*; for example, there is no identification and authentication when an *anonymous* user accesses a *public* page on a Web site. There is no logon and no logoff under such circumstances. Web interactions require I&A only when the user and the Web owner agree to establish a secure session. Typically, secure Web transactions do require some form of logon and logoff even if these steps are not explicitly labelled as such.

Sessions integrity and authenticity can be violated in a number of ways. Piggybacking is the unauthorized use of an existing session by unauthorized personnel. This problem is difficult to imagine in the real world, where it would be unlikely that someone could, say, cut into the middle of a phone conversation to order goods and services using someone else's good name and credit card. In cyberspace, though, it is quite commonplace for users to initiate a transaction on a terminal or workstation and then to walk away from their unprotected session to go do something else. If a dishonest person sits at their place, it is possible to misuse the absent person's session. A common problem of piggybacking is the misuse of someone else's e-mail program to send fraudulent messages in the absent person's name. Another example might have the thief stepping into a session to change an order or to have goods sent to a different address but be paid for by the session initiator's credit card. Such examples of fraud can have disastrous consequences for the victims; in general, every news story about this kind of abuse reduces confidence in the security of e-commerce.

A more technical attack is called session hijacking: "Hijacking allows an attacker to take over an open terminal or login session from a user who has been authenticated by the system. Hijacking attacks generally take place on a remote computer, although it is sometimes possible to hijack a connection from a computer on the route between the remote computer and your local computer"[21]. "*Hijacking* occurs when an intruder uses ill-gotten privileges to tap into a system's software that accesses or controls the behavior of the local TCP [Transmission Control Protocol] . . . . A successful hijack enables an attacker to borrow or steal an open connection (say, a telnet session) to a remote host for his own purposes. In the likely event that the genuine user has already [been] authenticated to the remote host, any keystrokes sent by the attacker are received and processed as if typed by the user"[22].

In summary, identification, authentication and authorization are normal components of any business transaction and must be guaranteed by the communications systems and software mediating the relationship between supplier and customer.

2.4 The Role of Encryption

All of the technologies being proposed by competing companies and consortia, including tokens, secure protocols for data transmission, digital certificates, and standards for trusting Web sites involve some form of encryption. *Encryption* is "the process of transforming data to an unintelligible form in such a way that the original data . . . be obtained without using the inverse

21 Chapman, D. B. & E. D. Zwicky (1995). _Building Internet Firewalls_. O'Reilly & Associates (Sebastopol, CA). ISBN 1-56592-124-0. xxvi + 517. Index. See p. 352 ff.

22 Hughes, L. J., Jr (1995). _Actually Useful Internet Security Techniques_. New Riders Publishing (Indianapolis, IN). ISBN 1-56205-508-9. xv + 378. Index. See p. 37 ff.

decryption process.23" See the Appendix (section 6) for a brief overview of the basics of encryption as used in electronic commerce.

23 Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization) <glossary@sdsc.isu.edu> or <jlisi@romulus.ncsc.mil>.

3. Frameworks for Secure E-commerce

E-commerce security is currently under rapid and uncoordinated development. Many manufacturers, industry associations and standards bodies have proposed an implemented different solutions for the problems of ensuring confidentiality, identification, authentication, and authorization for e-commerce. This section summarizes some of the key initiatives and provides pointers for further details.

The frameworks discussed below emphasize various aspects of e-commerce security. Table 1 shows how these frameworks fit together in meeting the needs of users and businesses seeking to establish secure business relations through the Internet and the Web.

Framework	Privacy	Identification	Authentication	Authorization	Single Sign-On
P3	Y				
TRUSTe	Y				
SSL	Y	Y	Y		
Tokens		Y	Y		
FIPS 196		Y	Y		
vCard		Y			
Digital certificates		Y	Y		
X.509v3		Y	Y		
SESAME		Y	Y	Y	
Certification authorities		Y	Y	Y	
SET		Y	Y	Y	
OFX		Y	Y	Y	
Gold Standard		Y	Y	Y	
Kerberos		Y	Y	Y	Y

OPS	Y	Y	Y	Y	Y

Table 1. Frameworks for Privacy, Identification, Authentication, Authorization and Single Sign-On.

3.1 Privacy

3.1.1 P3

The Platform for Privacy Principles (P3) is backed by the World Wide Web Consortium, the Direct Marketing Association & (originally) Microsoft24 <http://www.zdnet.com/intweek/print/970609/inwk0040.html>. This standard helps describe and define limitations on the collection and use of private information from users of Web sites.

3.1.2 TRUSTe

TRUSTe (formerly known as eTRUST) is non-profit initiative25 <http://www.etrust.org/> that certifies the respect for users' privacy by Web sites26 <http://www.zdnet.com/intweek/print/970609/inwk0040.html>. Users are empowered to control how much information about themselves will be revealed while they are online. The TRUSTe trustmark indicates that a Web site is committed to protecting user privacy; its privacy assurance program is backed by periodic reviews by TRUSTe, which also seeds the site with personal user information to see if it is misused. In addition, Coopers & Lybrand and KPMG Peat Marwick audit sites randomly; TRUSTe also receives feedback from users about trustmarked sites27 <http://www.etrust.org/users/program.html>. The Trustmark from TRUSTe helps users feel confident about their personal privacy. There are three levels of Trustmark:

Third-party exchange is the lowest TRUSTe level: the vendor shares information with other vendors;

One-to-one exchange: vendor keeps information at the Web server but uses it only for interactions with that specific client;

No-exchange warranty is highest TRUSTe level: vendor does not capture or keep client data at all28 <http://www.zdnet.com/pcmag/issues/1612/pcmg0022.htm>.

24 <http://www.zdnet.com/intweek/print/970609/inwk0040.html> FTC Summit To Kick Off Privacy Programs. By Will Rodger.

25 <http://www.etrust.org/> TRUSTe home page.

26 <http://www.zdnet.com/intweek/print/970609/inwk0040.html> FTC Summit To Kick Off Privacy Programs. By Will Rodger.

27 <http://www.etrust.org/users/program.html> About the TRUSTe Privacy Program: Why It Matters to You.

28 <http://www.zdnet.com/pcmag/issues/1612/pcmg0022.htm> Whom Can You Trustmark? By Jim Seymour

3.1.3 SSL

Netscape Communications Corporation, creators of the widely-used Netscape Navigator browser, created the Secure Sockets Layer (SSL) protocol to protect information being transmitted through the Internet. In addition, the SSL provides for authentication of Web servers[29] <http://search.netscape.com/newsref/std/SSL_old.html>.

3.2 Identification

3.2.1 Tokens

Many identification and authentication methods rely on tokens[30] <http://www.zdnet.com/pcmag/features/inetsecurity/authentication.htm>. These devices are encapsulated microprocessors in a tamper-resistant package usually the size of a thick credit card. One-time password generators have an LCD panel to display an alphanumeric string that consists of their own serial number combined with the time and date and encrypted appropriately so that only the host software can deduce the serial number of the token that generated that particular string. Such devices currently cost about $30 or so.

Smart cards are similar to the hand-held one-time password generators and can also be used for authentication; however, they require specialized readers[31] <http://www.zdnet.com/pcmag/features/inetsecurity/authentication.htm>. Some tokens have been created to interact with the common floppy drive apparatus. PC-card (formerly "PCMCIA") based authentication is available but these devices are more expensive than smart cards, costing about $60[32] <http://www.zdnet.com/pcmag/features/inetsecurity/authentication.htm> not counting the readers. Tokens are usually owned by issuing organizations; however, a new approach involves smart-cards owned by user[33] <http://www.digicash.com/news/archive/bigbro.html>. Such user-owned devices can function as electronic purses and play a role in anonymous payment schemes designed to protect user privacy.

3.2.2 FIPS 196

The US Government's Federal Information Processing Standard (FIPS) 196 defines how the PKC is to be used for user authentication with challenge-response systems34. Suppliers aiming at government procurement will have to take FIPS 196 into account in their system designs.

---

29 <http://search.netscape.com/newsref/std/SSL_old.html> THE SSL PROTOCOL

30 <http://www.zdnet.com/pcmag/features/inetsecurity/authentication.htm> Internet Security: Authentication

31 <http://www.zdnet.com/pcmag/features/inetsecurity/authentication.htm> Internet Security: Authentication

32 <http://www.zdnet.com/pcmag/features/inetsecurity/authentication.htm> Internet Security: Authentication

33 <http://www.digicash.com/news/archive/bigbro.html> Security without Identification: Card Computers to make Big Brother Obsolete. By David Chaum.

34 Menke, S. M., K. Power & S. Graves (1997). New FIPS defines key use. Government Computer News 16(7):3 (Mar 17)

3.2.3 vCard

The vCard specification is managed by the Internet Mail Consortium; it allows "electronic business cards" to be exchanged. The vCard protocol has been submitted to IETF for approval as an open standard35 <http://www.zdnet.com/pcweek/news/0526/26apro.html>.

35 <http://www.zdnet.com/pcweek/news/0526/26apro.html> Standard for exchanging personal info moves forward. By Michael Moeller.

3.3 Authentication

3.3.1 Digital certificates

Digital certificates are growing in importance for Internet commerce[36] <http://www.zdnet.com/pcweek/reviews/0428/28cert.html>. Basically, to generate digital certificates, users and merchants use secret keys in concert to establish trust[37] <http://www.digicash.com/news/archive/bigbro.html> and devices can authenticate each other using digital certificates[38] <http://www.zdnet.com/pcweek/reviews/0428/28cert.html>. Digital certificates are being used to authenticate e-mail and other electronic messages; in addition, corporations can issues digital certificates to employees, obviating the need for user IDs and passwords to gain access to Intranets and other corporate networks. However, using certificates outside a single business can be complicated because digital certificates issued under different protocols are in general still not interoperable[39] <http://www.zdnet.com/pcweek/reviews/0428/28cert.html>.

3.3.2 CCITT (ITU) X.509v3 Standard for Digital Certificates

Most digital certificates are based on the CCITT (ITU) X.509v3 standard[40] <http://www.zdnet.com/pcweek/news/0526/26apro.html>. Groupware vendors are agreed that X.509 is the best way to secure information for Internet transfer; Lotus, Microsoft and Novell agreed to support X.509 (used by VeriSign and GTE Service Corp) and X.509 compliance is believed to enhance interoperability and simplification of security protocols[41] <http://www.zdnet.com/pcweek/news/0804/04cert.html>. Other supporters of X.509 include Lotus (Domino 4.6 will support X.509 certificates) and Microsoft (the next version of MS Exchange will support X.509 certificates). Novell's NDS directory services will support X.509 by 1998. The X.509-compliant Public Key Infrastructure is sometimes known as the PKIX[42] <http://pubsys.cmp.com/nc/813/813hrb.html>.

---

36 <http://www.zdnet.com/pcweek/reviews/0428/28cert.html> Role of digital certificates looks secure: But roadblocks to use include no interoperability, too many issuing authorities. By Dave Kosiur.

37 <http://www.digicash.com/news/archive/bigbro.html> Security without Identification: Card Computers to make Big Brother Obsolete. By David Chaum.

38 <http://www.zdnet.com/pcweek/reviews/0428/28cert.html> Role of digital certificates looks secure: But roadblocks to use include no interoperability, too many issuing authorities. By Dave Kosiur.

39 <http://www.zdnet.com/pcweek/reviews/0428/28cert.html> Role of digital certificates looks secure: But roadblocks to use include no interoperability, too many issuing authorities. By Dave Kosiur.

40 <http://www.zdnet.com/pcweek/news/0526/26apro.html> Standard for exchanging personal info moves forward. By Michael Moeller.

41 <http://www.zdnet.com/pcweek/news/0804/04cert.html>. Paper version: J. & C. Walker (1997). Groupware gets secure: major vendors pledge to standardize on X.509 spec for digital certificates. PC Week 14(33):1 (Aug 4)

42 <http://pubsys.cmp.com/nc/813/813hrb.html> Paper version: Hudgins-Bonafield, C. (1997). Mapping the rocky road to authentication. Network Computing 8(13):26 (Jul 15)

3.3.3 SESAME -- European Standard for Digital Certificate Authentication

In Europe, BULL, ICL and Siemens Nixdorf are pushing the SESAME standard for digital certificates. SESAME certificates expire after minutes or days to control access to system privileges. SESAME may eventually incorporate X.509 protocols43 <http://pubsys.cmp.com/nc/813/813hrb.html>.

3.3.4 Third-party Certification Authorities

The authenticity of digital certificates can be displayed by having each certificate signed by an entity (or person) that is trusted by both parties in the transaction. In one popular model of authentication of certificates, a web of trust among people and organizations ensures that every public key is signed by someone who knows that the public key is authentic. In a more hierarchical model, public keys used to sign certificates are authenticated by certification authorities (CAs) that are themselves authenticated by higher levels of CA[44] <http://www.zdnet.com/pcweek/reviews/0428/28cert.html>.

Organizations needing their own certification infrastructure can buy software from vendors; linking certificates to a directory structure facilitates single-logon systems, where users need to identify and authenticate themselves to a system only once to gain access to all authorized system services[45] <http://www.zdnet.com/pcweek/reviews/0428/28cert.html>. However, CAs have failed to take into account the importance and history of bilateral trading relations; today's CA products are "complex, hard to manage and scare the hell out of people"[46] <http://pubsys.cmp.com/nc/813/813hrb.html>. Perhaps as a result of this complexity, a survey in Dec 1996 by Netcraft and O'Reilly & Associates which examined 648,613 sites on the WWW found fewer than 1% of WWW sites offering both SSL and third-party authentication[47] <http://www.zdnet.com/pcmag/news/trends/t961220a.htm>.

3.3.5 SET -- Authorization and Non-Repudiation

The Secure Electronic Transactions (SET) protocol requires digital certificates for each use of a credit card by a user trying to pay a merchant48 <http://www.zdnet.com/pcweek/reviews/0428/28cert.html>. MasterCard and Visa announced the SET standard in February 1996; SET is also supported by GTE, IBM, Microsoft, Netscape,

43 <http://pubsys.cmp.com/nc/813/813hrb.html> Mapping The Rocky Road To Authentication. By Christy Hudgins-Bonafield.

44 <http://www.zdnet.com/pcweek/reviews/0428/28cert.html> Role of digital certificates looks secure: But roadblocks to use include no interoperability, too many issuing authorities. By Dave Kosiur.

45 <http://www.zdnet.com/pcweek/reviews/0428/28cert.html> Role of digital certificates looks secure: But roadblocks to use include no interoperability, too many issuing authorities. By Dave Kosiur.

46 <http://pubsys.cmp.com/nc/813/813hrb.html> Paper version: Hudgins-Bonafield, C. (1997). Mapping the rocky road to authentication. Network Computing 8(13):26 (Jul 15)

47 <http://www.zdnet.com/pcmag/news/trends/t961220a.htm> What's Holding Up E-Commerce? A survey says Web businesses still need security tools.

48 <http://www.zdnet.com/pcweek/reviews/0428/28cert.html> Role of digital certificates looks secure: But roadblocks to use include no interoperability, too many issuing authorities. By Dave Kosiur.

SAIC, Terisa, and VeriSign49 <http://www.zdnet.com/pcmag/news/trends/t960201d.htm>. SET-compliant sites protect merchants from unauthorized payments and repudiation by clients; banks using SET are protected against unauthorized purchases using their cards; and consumers are protected from merchant imposters and theft of credit card numbers50 <http://www.cybercash.com/cybercash/about/set.html>. Supporters say SET will allow consumers to relax about security on the Web51 <http://www.zdnet.com/pcmag/news/trends/t970221a.htm>.

3.3.6 OFX -- Open Financial Exchange

The Open Financial Exchange (OFX) is supported by Microsoft, Intuit, Checkfree and others. The standard governs digital certificates to be exchanged among financial institutions to authenticate transactions. VeriSign, currently the most important third-party CA, has issued a new type of digital ID called the Financial Service ID that is usable by institutions supporting the OFX specification. The Financial Service ID will secure transactions such as home banking applications52 <http://www.news.com/News/Item/0,4,15222,00.html>.

3.3.7 Gold Standard

In direct competition with OFX, Integrion (a joint venture of IBM, Visa and 17 North American banks) is creating a separate financial certificate protocol called "The Gold Standard"53 <http://www.news.com/News/Item/0,4,15222,00.html>.

3.4 Authorization and Single Sign-On

3.4.1 Kerberos

Kerberos was developed at MIT in the 1980s as part of an extended scheme for user identification, authentication and authorization. The system's security depends strongly on protection of a Kerberos server that talks to both users and computer services such as printers and file servers. Once a user has been securely enrolled in the Kerberos server, the user's passwords never travel the Kerberos authentication server. Each subsequent request for a bilateral relation with a service by an authenticated user is itself authenticated by the Kerberos server which issues digital certificates (called tickets) to allow use of specific services by specific users. Kerberos requires applications and servers to be Kerberized -- modified for use with Kerberos; most off-the-shelf software does not support Kerberos[54] . However, Microsoft defines Kerberos as its Windows NT v5 default authentication mechanism[55]

---

49 <http://www.zdnet.com/pcmag/news/trends/t960201d.htm> MasterCard and Visa Join Forces for Electronic Commerce: SET promises to be a global standard.

50 <http://www.cybercash.com/cybercash/about/set.html> CYBERCASH SET COMPLETE PAYMENT SOLUTION.

51 <http://www.zdnet.com/pcmag/news/trends/t970221a.htm> Ready, Set, Shop: New technologies inch us closer to cybershopping.

52 <http://www.news.com/News/Item/0,4,15222,00.html> Locking up home banking. By Tim Clark.

53 <http://www.news.com/News/Item/0,4,15222,00.html> Locking up home banking. By Tim Clark.

54 Elledge, D. (1997). Keep out prying eyes. InformationWeek (629):102 (May 5)

55 < http://pubsys.cmp.com/nc/813/813f2.html > Paper version: Hudgins-Bonafield, C. (1997). Bridging The Business-to-Business Authentication Gap. Network Computing 8(13):62 (Jul 15)

<http://pubsys.cmp.com/nc/813/813f2.html> and there is considerable interest in extending Kerberos to other applications as part of the Distributed Computing Environment (DCE) supported by a consortium of computer manufacturers.

3.4.2 OPS -- Open Profiling Standard for Authorization and Single Sign-On

The Open Profiling Standard, backed by Netscape, Firefly, and VeriSign56,57 <http://www.zdnet.com/intweek/print/970609/inwk0040.html>, <http://www.zdnet.com/pcweek/news/0526/26apro.html> removes the need for users to re-enter their identifying information more than once on Web sites. It is also designed to allow Web sites to tailor their presentation to a user by reading personal information that has been authorized by that user and is transmitted to the server via vCards and digital certificates58 <http://www.zdnet.com/pcweek/news/0526/26apro.html>. The OPS is supported by privacy activists such as the EFF, EPIC and also eTRUST/CommerceNet (now TRUSTe).

3.5 Interoperability

Competing standards make it difficult for users and corporations to communicate effectively; many observers hope that the field will develop standards for interoperability of the different certificates and protocols. Most of the directory/certificate linkage schemes that relate certificates to specific users and servers generally use LDAP, the Lightweight Directory Access Protocol[59] <http://www.zdnet.com/pcweek/reviews/0428/28cert.html>, and there is some talk of merging OFX and The Gold Standard, but as of Oct 1997 there had been no progress reported60 <http://www.news.com/News/Item/0,4,15222,00.html>.

Application Programming Interfaces (APIs) allow different programs to interoperate. It is frustrating that several API frameworks are under development by competing vendor groups and that the proposed standards do not spell out how to progress from authentication to authorization. Gradient Technologies, a Kerberizing specialist, supports integration of the Public Key Infrastructure (PKI) with Kerberos/DCE[61] <http://pubsys.cmp.com/nc/813/813f2.html>. The SecureOne framework integrates APIs for anti-virus programs, authentication, encryption, and

56 <http://www.zdnet.com/intweek/print/970609/inwk0040.html> FTC Summit To Kick Off Privacy Programs. By Will Rodger.

57 <http://www.zdnet.com/pcweek/news/0526/26apro.html> Standard for exchanging personal info moves forward. By Michael Moeller.

58 <http://www.zdnet.com/pcweek/news/0526/26apro.html> Standard for exchanging personal info moves forward. By Michael Moeller.

59. <http://www.zdnet.com/pcweek/reviews/0428/28cert.html> Role of digital certificates looks secure: But roadblocks to use include no interoperability, too many issuing authorities. By Dave Kosiur.

60 <http://www.news.com/News/Item/0,4,15222,00.html> Locking up home banking. By Tim Clark.

61. < http://pubsys.cmp.com/nc/813/813f2.html > Paper version: Hudgins-Bonafield, C. (1997). Bridging The Business-to-Business Authentication Gap. Network Computing 8(13):62 (Jul 15)

digital certificates; RSA, VeriSign, McAfee, Security Dynamics support SecureOne62 <http://www.zdnet.com/pcweek/news/0804/04cert.html>.

62 <http://www.zdnet.com/pcweek/news/0804/04cert.html>. Paper version: J. & C. Walker (1997). Groupware gets secure: major vendors pledge to standardize on X.509 spec for digital certificates. PC Week 14(33):1 (Aug 4)

4. Products

This section includes a few products thought to be particularly significant in the developing field of Web commerce security. Inclusion does not imply endorsement by the NCSA, nor does exclusion imply criticism.

Products	Privacy	Identity	Authenticity	Authorization	Single Sign-On	Extended Information
VeriSign Digital IDs		Y	Y			
DigiCash	Y			Y		
CyberCash	Y			Y		
Xcert Sentry CA			Y			
Auric Systems ASA	Y	Y	Y	Y		
Security Dynamics SecurID		Y	Y	Y		
Bellcore S/KEY		Y	Y	Y	Y	
Internet Mall		Y	Y	Y	Y	
VeriSign Private Label Digital ID Services		Y	Y	Y	Y	Y
NCR Smart EC TrustedPASS		Y	Y	Y	Y	Y

Table 2. Functionality of Some E-Commerce Security Products.

4.1 VeriSign Digital IDs

VeriSign has established itself as the supplier of digital certificates with the largest base of commercial and individual customers among the third-part y CAs. The Digital IDs use RSA cryptography with 1024-bit key length and are are being used by more than 16,000 Web servers and over 500,000 individuals. VeriSign's Server Digital IDs enable organizations to establish secure sessions with visitors; the Server Digital IDs authenticate the Web site and ensure that customers will not be fooled by unauthenticated Web sites of unscrupulous con-artists who make their sites look as convincing as those of real businesses.

Digital IDs dispense with the need for users to memorize individual user IDs and passwords for different Web sites. Digital IDs are issued by CAs and securely exchanged using SSL. VeriSign verifies a server operator's identity using Dun & Bradstreet, InterNIC and others authenticating information such as articles of incorporation, partnership papers, and tax records. VeriSign (or other CA) signs a Digital ID only after verifying the site's authenticity in these ways63 <http://www.verisign.com/products/sites/serverauth.html>. AOL offers VeriSign Digital IDs to let customers and merchants authenticate each other64 <http://www.zdnet.com/pcmag/news/trends/t961220a.htm>.

In use for a specific transaction between user and Web site, the server generates a random session key that is encrypted by the secret key from the server's Digital ID; this session key expires in 24 hours and each session uses a different session key, making it impossible for a captured certificate to be misused65 <http://www.verisign.com/products/sites/serverauth.html>.

From the user perspective, Digital IDs are easy to use. The Web user clicks on a credit-card icon on the Web site. The user then fills out a form that automatically provides the merchant's Web server with the user's public key, a list of desired purchases and the user's digital certificate. The merchant's software decodes the user authentication and corresponding bank identification to process the order66 <http://www.zdnet.com/pcmag/news/trends/t960723a.htm>.

Generally, Digital IDs are implemented for automatic use by Web browsers and e-mail software <http://digitalid.verisign.com/id_intro.htm>. However, currently, the VeriSign smart card system requires a card reader on the client system67 <http://www.zdnet.com/pcmag/news/trends/t970221a.htm>.

VeriSign announced plans for SET compliance in its digital authentication certificates in July 9668 <http://www.zdnet.com/pcmag/news/trends/t960723a.htm>.

VeriSign has been working on new digital certificates including new attributes to extend personalization of Web sites; the current version of Digital IDs have limited fields for user information that can be used to personalize Web site responses[69] <http://www.zdnet.com/pcweek/news/0526/26apro.html>.

---

63 <http://www.verisign.com/products/sites/serverauth.html> Digital IDs for Servers: High-level Security at a Low Cost.

64 <http://www.zdnet.com/pcmag/news/trends/t961220a.htm> What's Holding Up E-Commerce? A survey says Web businesses still need security tools.

65 <http://www.verisign.com/products/sites/serverauth.html> Digital IDs for Servers: High-level Security at a Low Cost

66 <http://www.zdnet.com/pcmag/news/trends/t960723a.htm> Virtual Plastic: VeriSign will give banks encoded digital certificates for Visa cardholders.

67 <http://www.zdnet.com/pcmag/news/trends/t961220a.htm> What's Holding Up E-Commerce? A survey says Web businesses still need security tools.

68 <http://www.zdnet.com/pcmag/news/trends/t960723a.htm> Virtual Plastic: VeriSign will give banks encoded digital certificates for Visa cardholders.

69. <http://www.zdnet.com/pcweek/news/0526/26apro.html> Standard for exchanging personal info moves forward. By Michael Moeller.

One of the limitations of the VeriSign scheme is that each Web site visited by a user must request the client Digital ID for re-authentication. If access control lists (ACLs) are to be linked to Digital IDs, every authorized user for a specific site must be entered into a database for ACL implementation70 <http://www.verisign.com/repository/clientauth/clientauth.html>.

4.2 DigiCash

DigiCash provides smart-card payments and software ecash using the PKC71 <http://www.digicash.com/digicash/digicash/profile>. This system is designed to enhance user privacy; for example, a user can use a different digital pseudonym (account identifier) for every organization. These tokens may contain personal information about the user, but the user can exert control over which data are sent to which server. Traditional security measures necessarily trace individual identity but the DigiCash approach ensures anonymity of each user while simultaneously ensuring data integrity and non-repudiation of transactions. Certificates of receipt are digitally signed to prevent repudiation of the transaction. The DigiCash system allows purchases to be subject to "cooling-off periods" during which they can be reversed. DigiCash protocols require a secret authorizing number (PIN) that would make use of a stolen or lost smart card difficult.

DigiCash is open to implementation on any device and hopes that this open system can allow merchants to take advantage of the best solutions available rather than be tied to a single supplier.

Merchants can lock out individuals who abuse their relationship; this locking function would allow the new system to be extended to polling and voting with security and anonymity[72] <http://www.digicash.com/news/archive/bigbro.html>.

DigiCash's ecash is a software-based payment system for use on any computer and network. The ecash system requires DigiCash software to be installed on each user's workstation. Such a system makes micropayments for services and products delivered via the Web economically feasible73 < http://www.digicash.com/ecash/>.

4.3 CyberCash

CyberCash customer information is sent encrypted to a merchant Web server, which signs and forwards it to CyberCash as a secure intermediary. The merchant never sees the customer's credit card number because it remains encrypted while on the merchant's server. CyberCash securely decrypts and reformats the transaction and sends the information securely to the merchant's bank. The merchant's bank securely forwards a request for authorization of the purchase to the customer's bank. The customer's bank sends a digitally-signed authorization back to CyberCash which then securely returns the authorization (or denial) to the merchant. The merchant in turn

70 <http://www.verisign.com/repository/clientauth/clientauth.html> Digital IDs: The New Advantage.
71 <http://www.digicash.com/digicash/digicash/profile> DigiCash Profile.
72. <http://www.digicash.com/news/archive/bigbro.html> Security without Identification: Card Computers to make Big Brother Obsolete. By David Chaum.
73 < http://www.digicash.com/ecash/> Electronic Payments With ecash.

notifies the customer of the acceptance or rejection of the purchase74 <http://www.cybercash.com/cybercash/shoppers/shopsteps.html>. The secure exchange depends on non-Internet communications between CyberCash and the financial institutions.

CyberCash is integrating its electronic cash system with the SET protocol75 <http://www.cybercash.com/cybercash/about/set.html>. AOL is an example of a large vendor that offers CyberCash authentication for its Web-hosting services[76] <http://www.zdnet.com/pcmag/news/trends/t961220a.htm>.

4.4 Xcert Sentry CA

Xcert, a Canadian company, provides a CA proxy to retrofit legacy systems so they can generate and interpret digital certificates[77] <http://pubsys.cmp.com/nc/813/813hrb.html>. Xcert's Sentry CA allows cross-authentication between CAs, although the current implementation requires Sentry CA 1.1 on all servers for cross-authentication. Later versions of Sentry CA will cross-authenticate to other types of CAs. In initial evaluations, Netscape Navigator used Sentry CA certificates flawlessly but Microsoft Explorer 3.02 did not78.

4.5 Auric Systems ASA

Auric Web Systems has announced Automatic and Secure Authentication (ASA). ASA allows any Web site to identify and authenticate a customer browsing its site; Web surfers do not need to type in any data for I&A by the Web server. To authorize a purchase, server queries an ASA server where customer and server are registered; the ASA server authenticates both sides of transaction and communicates with banks/credit services. Interestingly, customers need no special software or hardware ☞ any browser works with ASA. ASA essentially creates a Virtual Proprietary Network (VPN, usually called a Virtual Private Network) over the Internet. The Web site needs only to add a single plug-in software module to its dial-up user authentication to use ASA. Several ISPs are interested in ASA79 <http://www.auricweb.com/ecgateway.htm>.

4.6 Security Dynamics SecurID & ACE/Server

Security Dynamics is the leading provider of token-based authentication using the SecurID & ACE/Server80 <http://www.zdnet.com/pcmag/features/inetsecurity/authentication.htm>. These systems are widely used for I&A within corporations. However, penetration of the wider

---

74 <http://www.cybercash.com/cybercash/shoppers/shopsteps.html> SIX STEPS OF A SECURE INTERNET CREDIT CARD PAYMENT.

75 <http://www.cybercash.com/cybercash/about/set.html> CYBERCASH SET COMPLETE PAYMENT SOLUTION.

76. <http://www.zdnet.com/pcmag/news/trends/t961220a.htm> What's Holding Up E-Commerce? A survey says Web businesses still need security tools.

77 <http://pubsys.cmp.com/nc/813/813hrb.html> Paper version: Hudgins-Bonafield, C. (1997). Mapping the rocky road to authentication. Network Computing 8(13):26 (Jul 15)

78 Rapoza, J. (1997). Sentry CA cross-checks certificates; Review: Xcert uses LDAP directory secured via SSL for flexible authentication between authorities. PC Week 14(15):46 (Apr 14)

79 < http://www.auricweb.com/ecgateway.htm> EC Gateway: The Best Solution for E-Commerce.

80 <http://www.zdnet.com/pcmag/features/inetsecurity/authentication.htm> Authentication.

commercial market is problematic because of the capital cost of the hardware. It remains to be seen how the public will accept having to pay for and carry such tokens.

4.7 Bellcore's S/KEY

The S/KEY v2.6 from Bellcore is a system for one-time password authentication via software only. S/KEY uses a challenge-response system and the one-time password is never stored on the client or on the server and it never crosses the network. S/KEY complies with the Internet Engineering Task Force (IETF) standard RFC 1938 on One Time Passwords81 <http://www.bellcore.com/BC.dynjava?SkeyPDGeneralProductDescription>.

4.8 Internet Mall

How can a customer buy things from a number of vendors without repeatedly having to re-authenticate? Internet Mall Inc. provides for a single validation for all purchases in a series among any of the vendors signed up at the Mall82 <http://www.zdnet.com/pcweek/news/0317/21mimall.html>.

4.9 Extending the Usefulness of Certificates

Since customers and vendors are exchanging digital certificates, there has been considerable interest in extending the format of the certificates to allow additional information to be carried. Currently, digital certificates are being extended by developers to include more information; certificates with extended fields could help users by carrying personal details or preferences that would allow Web software to adjust the content presented so as better to suit each customer. For example, extended fields including an authenticated birth date could easily limit access to certain Web pages to adults, thus helping to reduce the problem of exposing children to pornography or other dangers on the Web[83] <http://www.zdnet.com/pcweek/reviews/0428/28cert.html>.

4.9.1 VeriSign Digital Certificates

VeriSign's Digital IDs are currently rigidly defined following the CCITT (ITU) X.509 standard. Digital IDs include the owner's public key, name, expiration date, CA name, serial#, and CA signature84 <http://digitalid.verisign.com/id_intro.htm>. VeriSign says that attribute extensions to certificates will have to enter the PKIX eventually. Some analysts believe that privilege and policy attributes will migrate from certificates to the LDAP. However, auto-industry expert argues that it is unacceptable to put privileges in a certificate because changing privileges would require revoking the certificate, and such a computationally- and I/O-intensive process would not be scalable.

---

81 <http://www.bellcore.com/BC.dynjava?SkeyPDGeneralProductDescription> S/KEY One-time Password Authentication System: Introduction.

82 <http://www.zdnet.com/pcweek/news/0317/21mimall.html> One-stop buying coming to the Web. By Margaret Kane.

83. <http://www.zdnet.com/pcweek/reviews/0428/28cert.html> Role of digital certificates looks secure: But roadblocks to use include no interoperability, too many issuing authorities. By Dave Kosiur.

84 <http://digitalid.verisign.com/id_intro.htm> Digital IDs Introduction.

Netscape's CA already attaches some privileges to its certificates and Consensus Development Corp. is building privilege/authority plug-ins for Netscape and Microsoft servers. Entrust also puts non-identity attributes in its certificates85 <http://pubsys.cmp.com/nc/813/813f2.html>.

Recent news suggests that VeriSign's Digital Certificates will include any type of data that can be programmed on servers. Corporations will customize VeriSign Digital Certificates to their own specifications. Customers using the "Private Label Digital ID Services" will be able to add their own customized fields at will. Such new expandable certificates could replace cookies (the text records stored in the cookies.txt file by browsers). VeriSign will offer free upgrade to its Private Label Digital Certificates to its 500,000 current customers using the older, fixed-format certificates; corporate users will also be able to upgrade their server software easily to be able to use the expandable certificates86,87 <http://www.verisign.com/pr/pr_large.html>.

4.9.2 NCR TrustedPASS

Another interesting new product is NCR's SmartEC TrustedPASS, originally developed as part of a system designed to allow telecommunications companies to control access by their customers to their own billing records. This software features an extendible certificate (called the TrustedPASS) format that includes fields for issuer, server port, originating IP address, time of expiration for the TrustedPASS, a flexible area for additional data, and a digital signature for the whole TrustedPASS. This design requires no software changes on the user side and there are no plug-ins for the client browser. An TrustedPASS authentication server on the server side uses whatever I&A the merchant chooses to impose. However, once the user is authenticated in compliance with the Web site's criteria, the TrustedPASS authentication server sends the client an TrustedPASS. If the customer repeatedly fails the authentication phase (e.g., by giving the wrong password too many times) the authentication server can invalidate the customer record in its public-key database and the customer can be instructed to call for help.

The TrustedPASS is described as extendible because there are no limits to how much information can precede the digital signature field. Such information could easily include personal details and permission fields controlling which data should be used for which purposes. The system would fit very well into many other frameworks and could help solve the problem of tailoring authorization privileges to a user's characteristics or displaying different views of Web site information.

The TrustedPASS system explicitly allows configuration of an expected lifetime for the TrustedPASS. If the authentication server notices that the current TrustedPASS being used for a specific session is reaching its limit, it issues another TrustedPASS. This feature allows an active user to continue to access a Web site without manual re-authentication. In addition, if the user holding a valid TrustedPASS accesses a different Web site that also has TrustedPASS software

85 < http://pubsys.cmp.com/nc/813/813f2.html > Paper version: Hudgins-Bonafield, C. (1997). Bridging The Business-to-Business Authentication Gap. Network Computing 8(13):62 (Jul 15)

86 Moeller, M. (1997). Digital IDs: offering an expanded view of users: VeriSign's next digital certificates extend electronic IDs to include personal data. PC Week 14(5):2 (Feb 3)

87 <http://www.verisign.com/pr/pr_large.html> VERISIGN PROVIDES CUSTOM DIGITAL ID SERVICES TO LARGE CORPORATE CUSTOMERS: NOVUS Services and Toppan Printing of Japan Among Those to Select VeriSign to Provide Digital Authentication Services for Internet Customers.

running, the new server can accept a valid TrustedPASS from a trusted site that it explicitly knows because of entries in its public-key database. If the user reaches expiration of the valid TrustedPASS from the first site, the second site can issue a new TrustedPASS that will in turn be respected by any other Web site that is running TrustedPASS and has a trust relationship with the second Web site. This is an unusual feature that permits a user to browse among many Web sites without reauthentication and without requiring a visit to a limited electronic mall where the vendors are required to pay a service fee to the mall owner88 <http://www.ncr.com/press_release/pr101497.html>.

88 <http://www.ncr.com/press_release/pr101497.html> Press Release: NCR Announces Internet Access to Telecommunications Bills.

5. Concluding remarks

Identification, authentication and authorization are recognized as critically important for the future of e-commerce on the World Wide Web. There are many competing initiatives and technologies currently under development and it will be important for all involved to cooperate fully in coming to agreements on interoperability as a minimum requirement for the good of the buying public and of vendors.

With the technologies described in previous sections, it should be increasingly acceptable for consumers and business people to to business securely on the Internet. Methods for evaluating each Web site's adherence to different levels of privacy policy will allow the marketplace, rather than governments and bureaucrats, to define the importance of protecting consumers' private information. Those wishing to protect their privacy to the utmost will favor electronic cash solutions, where funds will be expended without having to convey details of any kind about the identity of the purchaser. Such anonymous transactions may be especially useful for those businesses looking at micropayments as a method for selling access to publications, music, films, and other services where long-term subscriptions have so far remained unattractive to the public. Other developments such as single sign-on systems and customized contents in digital certificates will contribute to the ease with which ordinary consumers will be able to shop online.

We hope that this White Paper provides a basis for more extensive reading in the field of electronic commerce security. The field is developing rapidly and we will periodically revisit the paper for appropriate updates as conditions warrant. In the meantime, you will find below the list of recent papers and Web sites consulted during the analysis that led to this report. You will also find a visit to the NCSA Web site <http://www.ncsa.com> valuable as you explore the world of electronic commerce security.

Finally, do not hesitate to contact the NCSA by e-mail for help in any aspect of information technology security. Appropriate e-mail addresses are listed in each section of the NCSA Web Site.

6. Appendix: Basics of Cryptography for E-commerce

There are two major classes of encryption: symmetrical and asymmetrical. It is the asymmetrical class that has helped e-commerce the most in recent years.

6.1 Symmetrical Encryption Algorithms

The following diagram illustrates a simple *symmetric* encryption technique such as the Digital Encryption Standard (DES):

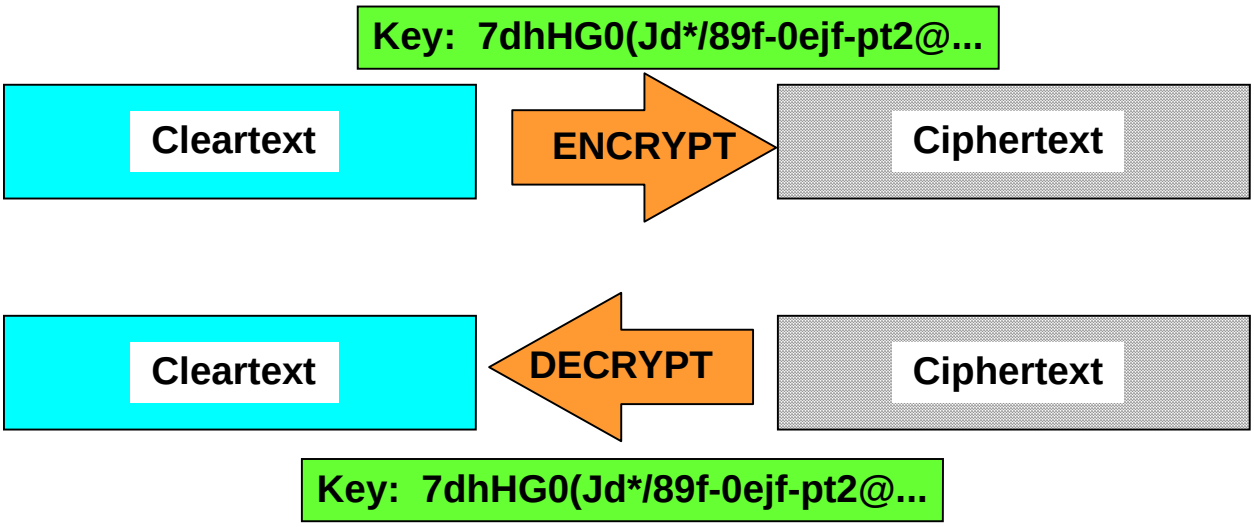

Figure 1. Symmetric Encryption and Decryption.

In this figure, the original text (or *cleartext*) is run through an *encryption algorithm* using a specific *encryption key*. This *encryption* process generates a garbled form of the text called a *ciphertext*. To retrieve the original cleartext after encryption using a symmetric algorithm, one uses the same key and algorithm to *decrypt* the ciphertext.

The symmetric encryption algorithms -- and there are many -- are usually very fast and they play an important role in securing information against detection. However, symmetric algorithms do require both sides of a transaction to know the same key, leading to risks if either sender or recipient compromise the secrecy of the key. In addition, every pair of correspondents that want to have purely confidential transactions has to generate a unique key known by no one else. This requirement for secret keys for each pair of correspondents leads to a *combinatorial explosion* because the number of pairs climbs approximately as the square of the number of correspondents. For example, three people need 3 x 2 / 2 = 3 unique keys for the three possible pairs of people (AB, AC and BC). Four people need 4 x 3 / 2 = 6 unique keys to protect the confidentiality of all possible pairs of correspondents (AB, AC, AD, BC, BD, CD). But a thousand people need 1000 x 999 / 2 = 499,500 or almost half a million unique pairs for all the possible combinations of correspondent pairs.

6.2 Asymmetrical Encryption Algorithms: the Public Key Cryptosystem

One of the most powerful tools invented to help protect information is the asymmetric encryption algorithms used in the *Public Key Cryptosystem* (PKC) first developed by Rivest, Shamir and Adleman in the 1970s[89] <http://www.rsa.com/rsalabs/newfaq/>.

Asymmetric encryption algorithms, unlike symmetrical encryption algorithms, use two keys for encryption and decryption. Instead of creating a single key that handles both encryption and decryption, key generation creates two different keys at once that are peculiarly complementary. One key is used to encrypt the cleartext and a different key is used to decrypt the ciphertext. Whatever is encrypted by one of the asymmetric keys can be decrypted only by the *other* key -- and vice versa, since one can encrypt with either key and then decrypt successfully with the other key. Figure 2 shows this principle.

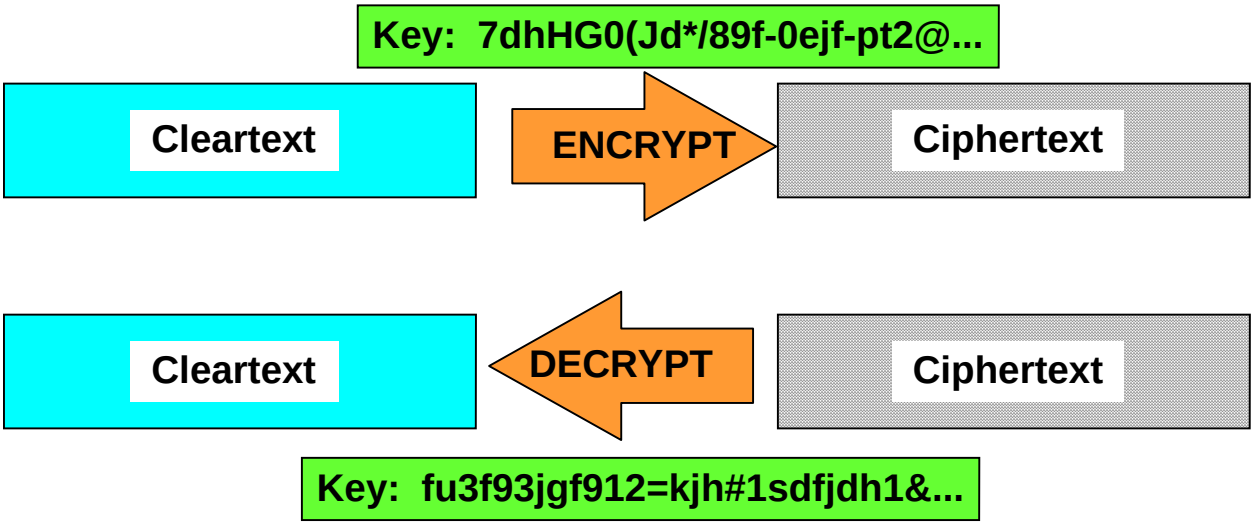

Figure 2. Asymmetrical Encryption and Decryption.

The PKC uses the fact that complementary keys can decrypt only what each keys complement encrypted. One of the pair is declared as a public key (known to anyone who wishes to use it) and the other is kept as a secret (or private) key.

6.3 Using the PKC to Protect Confidentiality

To send messages that can be read only by a specific holder of a public key, one encrypts the cleartext using the recipient's public key to produce a ciphertext; only the corresponding private key (known only, one hopes, to the recipient) can decrypt the ciphertext. Decrypting the message with any other key but the appropriate private key results in unusable garbage text, as shown in Figure 3.

89 <http://www.rsa.com/rsalabs/newfaq/> FAQ 3.0 on Cryptography.

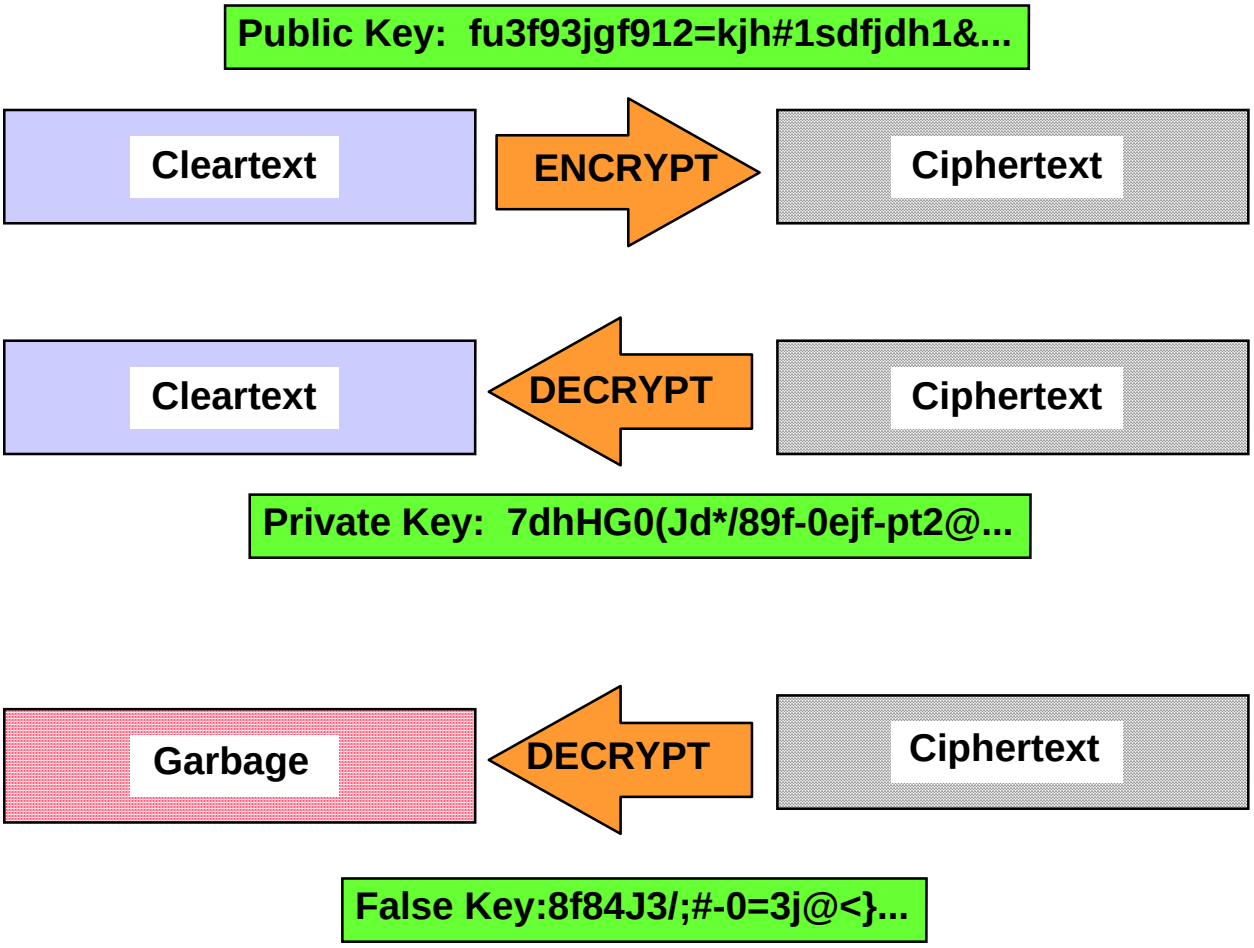

Figure 3. How the PKC Protects Confidentiality.

6.4 Using the PKC to Establish Authenticity

Similarly, to prove the authenticity and integrity of a message, the sender can encrypt the cleartext using the sender's *private* key; any recipient can verify both the integrity and authenticity of the cleartext by decrypting the ciphertext using the *sender's public key*. If the ciphertext can successfully be decrypted using the sender's public key, then only the user of the corresponding private key could have created the ciphertext. Figure 4 illustrates the demonstration of authenticity using the PKC.

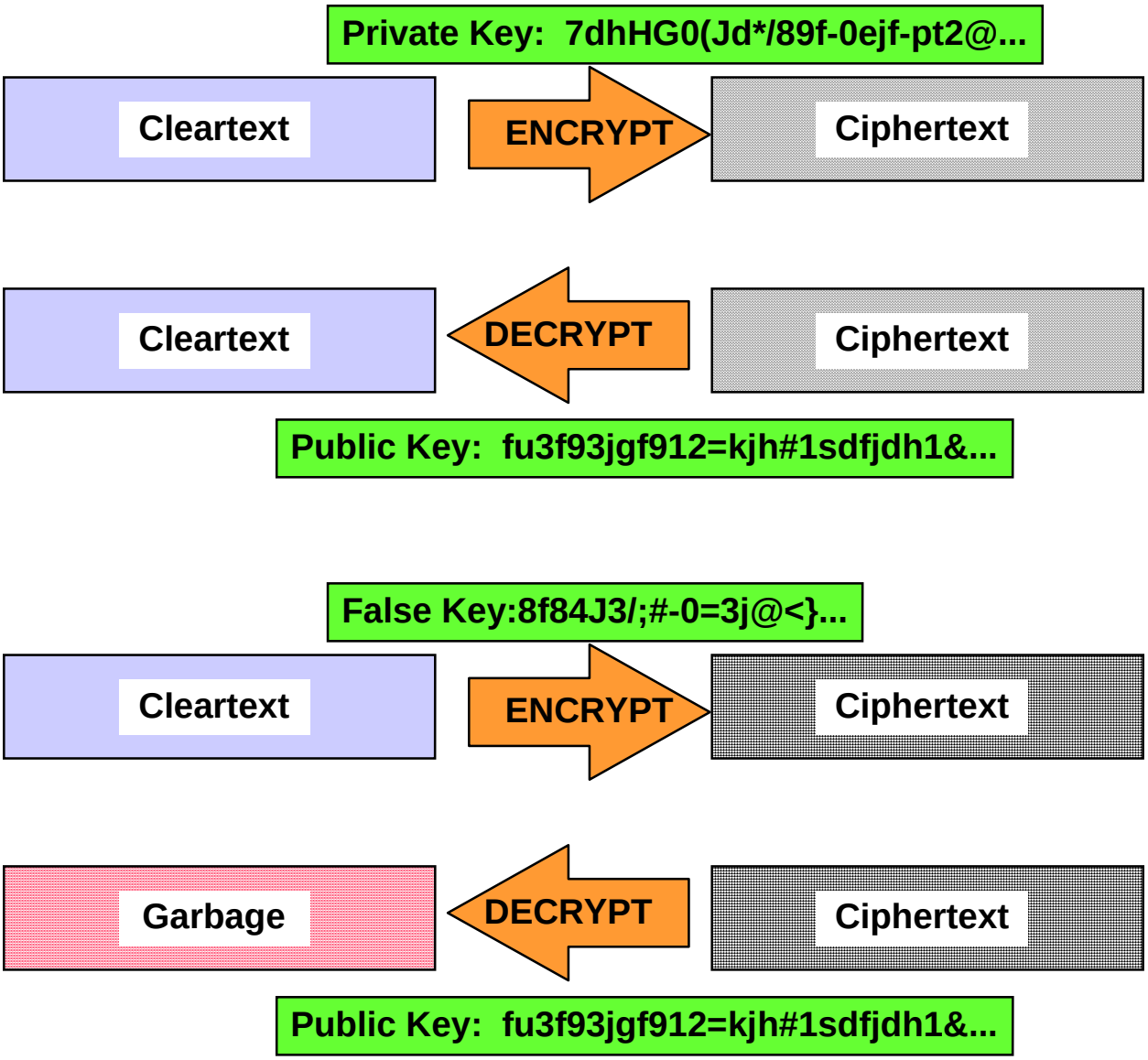

Figure 4. How the PKC Prevents Forgery

6.5 Using the PKC to Establish Integrity

In addition, if the ciphertext has been successfully deciphered, then the received text must be identical to what was originally sent. Figure 5 shows how the PKC (or any encryption method) helps ensure integrity of transmitted information.

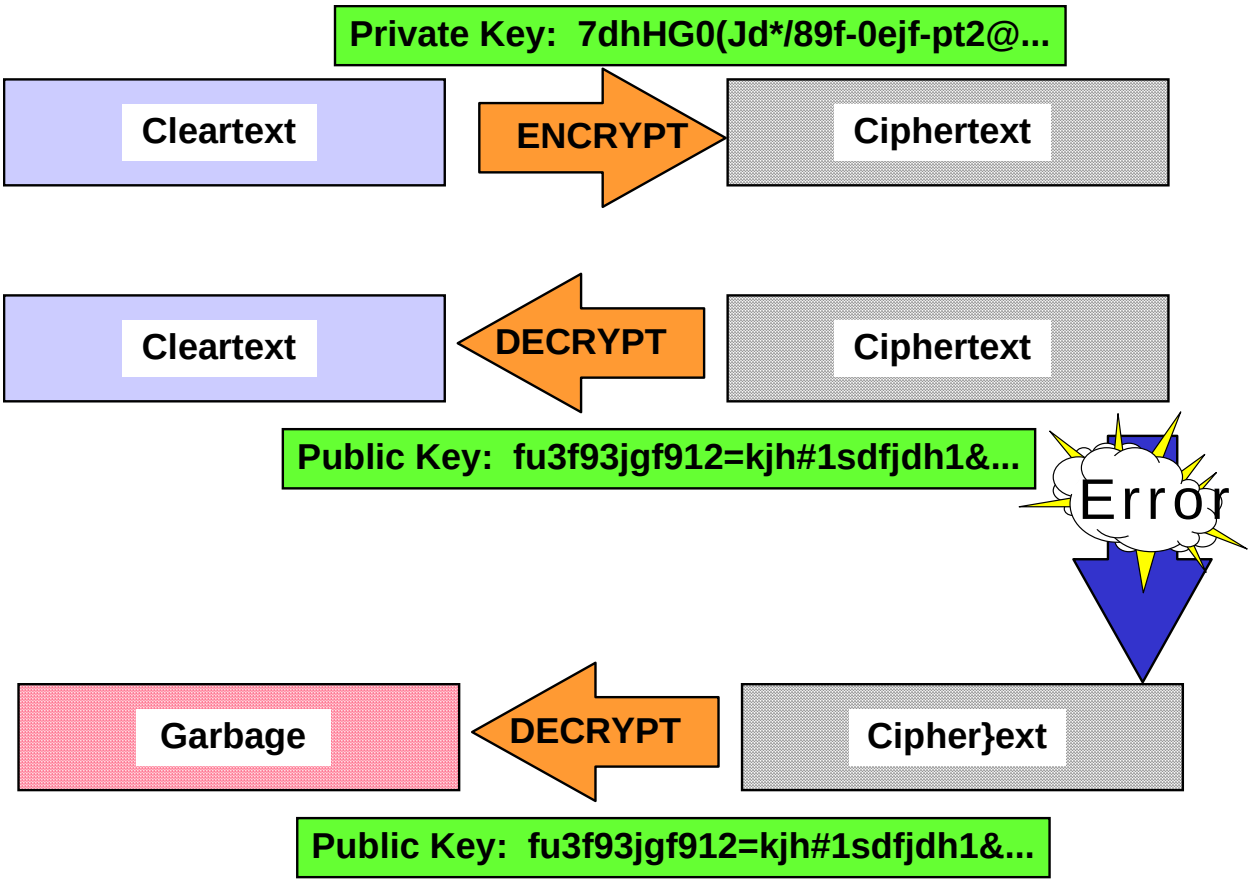

Figure 5. Error in transmission ruins decryption.

6.5.1.1 Use of Both Symmetric and Asymmetric Algorithms in the PKC

Typically, the asymmetric algorithms used in the PKC take a long time for encryption and decryption. In addition, longer messages naturally take longer to encrypt than short ones. To reduce the time required for tedious asymmetric encryption and decryption, one creates a *digital signature* under the PKC by generating a mathematical *hash* of the cleartext.

A hash function is any method that creates a short sequence of data to be used in verifying the integrity of its source; a *checksum* is an example of a hash total. For instance, the last four digits of most credit cards are a checksum. The algorithms for generating a hash are selected to generate a very different value for the cleartext modified by even so little as a single character. For example, if someone makes a mistake in reading their credit card number out over the phone so that one of the digits is wrong, it is very unlikely that the original four-digit checksum will be correct; when the incorrect card number is checked by the credit-card company, the erroneous checksum instantly identifies the mistake.

To shorten the time required for systems to check message integrity, the PKC usually does not encrypt the entire message. Instead, the PKC implementations create a hash total and it is the *hash* that is encrypted using the sender's private key. The recipient can decrypt the hash using the sender's public key and then independently calculate the hash value; if the recalculated hash

matches the decrypted hash, then the message is unchanged and it authentically originated with the holder of the corresponding private key. Figure 6 illustrates how the PKC uses hashes to check for authenticity and integrity.

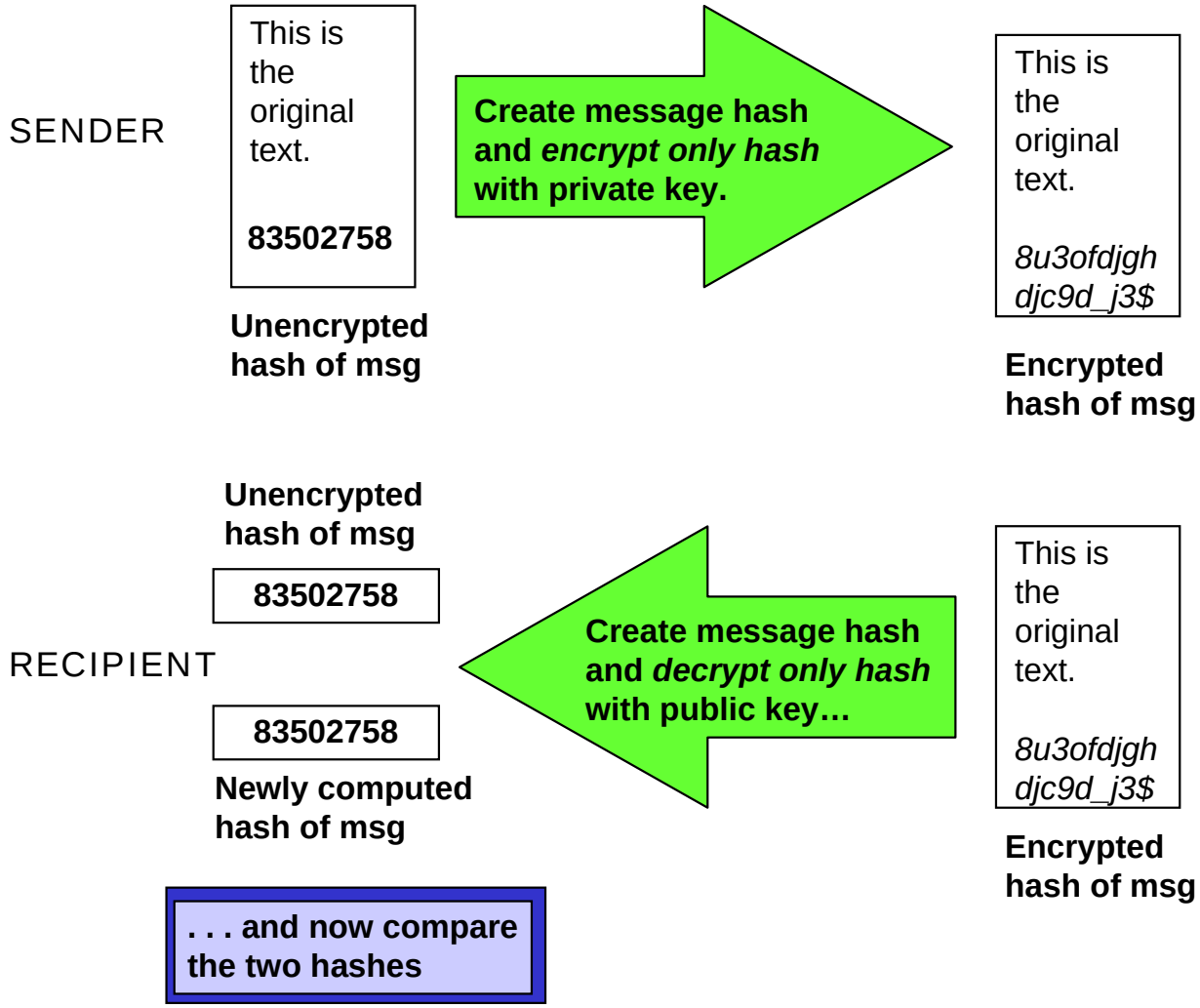

Figure 6. How the PKC Uses Hashes to Check Authenticity and Integrity.