디지털 인증 분류 프레임워크의 개발과 적용: 상황적 관점

Development and Application of a Digital Certificate Classification Framework: A Configuration Perspective

김 창 수 (Changsu Kim) 영남대학교 교수
딜셔드가푸로프 (Dilshodjon Gafurov) 영남대학교 대학원생

요 약

본 논문은 현재 전자거래에서 폭넓게 활용되고 있는 디지털인증 기술에 대하여 초점을 집중하고 있다. 즉, 현재 다양하게 활용되고 있는 디지털인증 기술들을 체계적으로 분류하기 위한 프레임워크의 개발과 적용 그리고 시사점에 대하여 고찰하였다. 먼저, 본 연구에서는 디지털 인증의 상황적인 흐름을 제공자에서부터 사용자까지 소프트웨어, 하드웨어, 네트워크 측면으로 구분하여 제시하였다. 이어서, 디지털인증의 다섯 가지 구성요소와 주요 요소기술 클래스 그리고 인증유형과 수준에 근거하여 디지털인증 분류 프레임워크를 개발하였다. 본 연구에서 개발된 디지털인증 분류 프레임워크를 베리사인의 디지털 인증 메커니즘에 적용하여 그 유용성을 검증하였다. 실제 사례에 본 연구에서 개발한 디지털 인증 분류 프레임워크를 적용한 결과 디지털 인증 기술의 세부적인 분류와 응용을 이해하는데 유효하다는 것을 알 수 있었다. 마지막으로 본 연구의 강점과 약점 그리고 시사점 및 향후 연구 방향에 대하여 논의하였다.

키워드 : 디지털 인증, 디지털 인증 기술, 분류 프레임워크.

Ⅰ. Introduction

The appearance of the World Wide Web (WWW) in 1995 has triggered the mass adoption of the Internet for public access to digital communications throughout the world (Mott, 2000). Although the Internet has enabled vastly increased information access and availability, it has also generated wholly new security challenges (Hunt, 2001; Laudon, 2002). Traditional computer security is dwarfed by the problems inherent to the containment of active attacks using phishing and Trojan horses (Schneier, 2005). Additionally, hackers have developed software that enables them to "sniff" a password being sent over the Internet (Venter, 2003; Wiedenbeck *et al*., 2005).

The promise of e-commerce is offset by the security challenges associated with the disintermediation of data access (Wiedenbeck *et al*., 2005). Security challenges result from cutting out the middleman, and from the expansion of the user community from a small group of vetted users to thousands of potentially untrustworthy users. Overall,

the success of e-commerce is primarily dependent on trust (Hunt, 2001). Trust plays a central role in helping consumers overcome perceptions of risk and insecurity (McKnight, 2002; Wiedenbeck *et al*., 2005). Digital certificate technologies are critical to trust-building (Chau, 2005). This study is motivated by the fact that, while we use digital certificates every day, we do not fully understand them. The principal objective of this study, then, is to provide a brief outline of the relevant concepts and principles of digital certificates, and to develop a framework by which they may usefully be classified.

Ⅱ. Overview of Digital Certificates

2.1 Understanding Digital Certificates

Digital certificates are issued by a trusted third party, which is referred to as a certification authority (CA). A digital certificate is an electronic document containing a copy of someone's public key, their relevant identification and business details, and the name of the certification authority (CA) (Wilson, 1999; Venter, 2003; Chau, 2005). Digital certificates are a central component of e-commerce, because they ensure the security of Internet transactions (Chau, 2005). They are required for a variety of purposes, including signing documents, authenticating servers, and creating secure channels between a company and its trusted third parties (Chau, 2005; Wiedenbeck *et al*., 2005).

Digital certificates are most commonly employed to secure transactions over the Internet, including purchasing goods, selling a product by online auctions, monitoring online bank accounts, or subscribing to a Web site (Jaweed, 2003). All of these transactions require sensitive personal information. Digital certificates perform the essential functions of authentication, encryption, identification, and data integrity (Hunt, 2001; Chau, 2005).

Authentication is the process by which the identities of parties in a communication are verified and confirmed (Wilson, 1999; Mott, 2000; Nambiar, 2004; Chau, 2005; Wiedenbeck *et al*., 2005). *Encryption* is a process of transforming data or information by using an algorithm, so as to make it unreadable to anyone except the designated senders and receivers. *Identification* is a signing process by which individuals and organizations augment the confidence of the transacting entities (Chau, 2005). *Data Integrity* provides evidence that the data has not been altered since it was signed, and also confirms the identity of the person or entity who signed the data (Wilson, 1999; Mott, 2000). A digital signature helps to ensure both the integrity and the origin of the data (http15). Digital certificates provide other services relevant to secure transactions, including confidentiality and non-repudiation.

Digital certificates are created by a certification authority or CA, as previously mentioned. The CA digitally signs the data record and thereby attests to the ownership of the public key (Ward, 1998).

2.2 Overview of Previous Classifications

What is taxonomy? According to Wikipedia.org, "*taxonomy* is the practice and science of classification." There are many strategies for the classification of digital certificates. For example, one common practice involves the definition of classes of certificates according to the quality of the registration process(es) (Lopez, 2005). Moreover, digital certificates can be classified in accordance with the purpose they serve and the storage device (e.g. USB

tokens, smartcards, routers, etc.) in which they are embedded. Here, we provide a brief review of some common examples of digital certificate classifications.

2.2.1 Classification by IBM

IBM classifies digital certificates according to the manner in which the certificate is used (http5). Their classification scheme involves certificate authority certificates, server and client certificates, object signing certificates, signature verification certificates, and user certificates. A certificate authority certificate (CAC) is a digital credential used to validate the identity of the Certificate Authority (CA) that owns the certificate. The CAC contains identifying information about the CA, in addition to its public key. A server or client certificate (SCC) is a digital credential which identifies the server or client. The SCC contains identifying information about the organization that owns the application. The certificate also includes the system's public key. An object signing certificate (OSC) verifies both the object's integrity and the origination or ownership of the object. A signature verification certificate (SVC) is a copy of an object signing certificate without the certificate's private key. People utilize the SVC's public key to authenticate the digital signature created with an object signing certificate. Finally, a user certificate (UC) is a digital credential which validates the identity of the client or user who owns the certificate. Many applications employ user certificates, instead of user names and passwords, to authenticate users' access to resources.

Whereas the IBM classification exhaustively describes five types of certificates, all of these types focus solely on technical aspects. Organizational and human issues known to be important to digital certificates are not included.

2.2.2 Classification by VeriSign

VeriSign provides three types of digital certificates: Server Certificates (SC), Developer Certificates (DC) for software publishers, and Personal Certificates (PC) for use with Web Browsers and S/MIME applications (http6, http9).

Server Certificates enable Web servers to operate in a secure mode. An SC unambiguously identifies and authenticates the user's server and encrypts any information passed between the server and a Web browser. *Developer Certificates* are used in conjunction with Microsoft AuthenticodeTM Technology (software validation), and provide customers with the information and assurance they require when downloading software from the Internet. *Personal Certificates* are used by individuals when they exchange messages with other users or online services.

Although the VeriSign method has been extensively explained in terms of technical digital certificate issues, certain matters of great concern to people, particularly users and providers, have been neglected.

2.2.3 Classification by Levi and Koç

Levi and Koç (2001) have classified three common classes of digital certificates in accordance with the method of their issuance. Class-1 certificates provide online processes for enrollment application and certificate retrieval. There is no real identity check, and it is possible to use a bogus name-the PIN sent by email to complete the application merely connects the applicant to an email address (Levi, 2001). Class-2 certificates are more secure than this. They are issued by CAs after both online and offline controls. CAs automatically check the applicant's identity and address against the database of a third party, such as a credit card company or DMV (Levi, 2001). Class-3 certificates are consid-

ered to be the most secure of all, as they require the in-person presence of an applicant for strong identity control prior to the issuance of the digital certificate by the CA.

Levi and Koç's digital certificate classifications are more or less concentrated on secure processes, which are relatively narrowly focused. This poses a limit on the explanation of complex digital certificate processes. Thus, broader perspectives on digital certificates should prove to be valuable in more clearly explaining the complicated activities inherent to digital certificate processes.

2.2.4 Classification by Usage in Electronic Payment Systems

Now, we briefly discuss the types of digital certificates that are utilized in some electronic payment systems, including SWIFT, CHAPS, EMV, and SET. Basically, this type of classification is based on the size and content of the information that may be contained in the digital certificate (Ward, 1998).

SWIFT and CHAPS operate over private networks and use certificates based on ISO 11166[1], which essentially come in three sizes *short, medium,* and *long* although all are relatively short as compared to other certificates.

Long certificates specify dates and time in the form YYMMDDHHMMSS, whereas the short and medium certificates use the form YYMM. Additionally, with long certificates, the certificate owner is identified by 16 alphanumeric characters, whereas short certificates use four decimal digits and medium certificates use an eight-character Bank Identifier Code (Ward, 1998).

1) ISO 11166 Banking-Key management by means of asymmetric algorithms.

EMV also uses short certificates because of the scarcity of ICC memory. EMV certificates are more generic than SWIFT and CHAPS certificates (Ward, 1998). By way of contrast, SET does not suffer from these limitations, and can utilize relatively long certificates based on X.509 that support a broad variety of participants.

These classifications tend to be concentrated in electronic payment systems. Thus, more general classifications would be required to gain a better understanding of the components and relevant applications of digital certificates.

2.3 Summary

In order to provide further insight, this study attempts to organize the above review into <Table 1>, as shown below:

The above review of previous digital certificate classifications provides insights that may be useful in further research into the new digital certificate classification framework. It appears that previous classifications of digital certificate have tended to underrate the role of human beings, which is a matter with some relevance to the subject of digital certificates. This perspective appears limited in terms of its capacity to clearly explain the characteristics of digital certificates. This is because human beings are an essential factor in the successful function and operation of digital certificates. Therefore, the principal objective of this study is to develop a novel classification framework for digital certificates, with a focus on human factors as the fundamental component of digital certificates. This perspective may prove to be of interest to researchers and practitioners who wish to understand how digital certificates interact with both human factors and technical components.

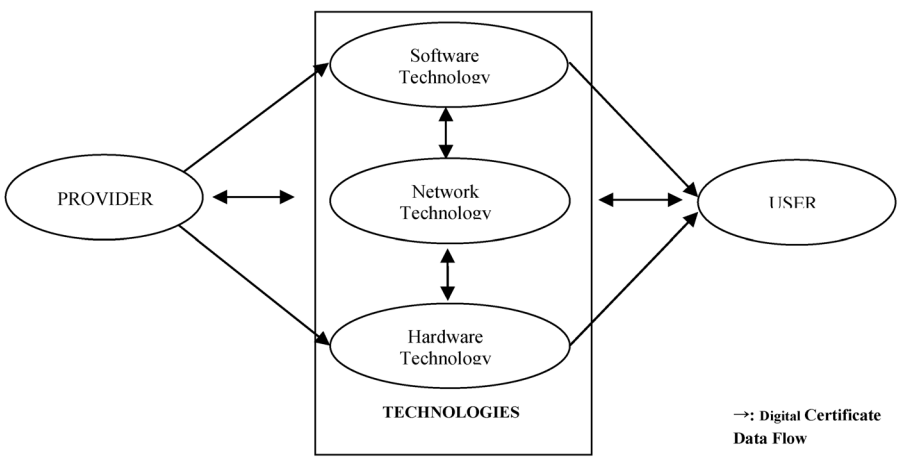
〈Table 1〉 Summary of Previous Classification of Digital Certificate

Category	Criteria	Classification
IBM	Use Method	◦ Certificate Authority Certificates ◦ Server and Client Certificates ◦ Object Signing Certificates ◦ Signature Verification Certificates ◦ User Certificates
VeriSign	Certificate User	◦ Server Certificates ◦ Developer Certificates ◦ Personal Certificates
Levi and Koc (2001)	Issue Way	◦ Class-1 Certificates ◦ Class-2 Certificates ◦ Class-3 Certificates
Electronic Payment Systems	Information Size	◦ Short Certificates ◦ Medium Certificates ◦ Long Certificates

Ⅲ. Development of a Digital Certificate Classification Framework

3.1 Configuration of Digital Certificate Flows

We can view a digital certificate as a type of system that accepts data as input and processes them into information as output. We can also see that all digital certificates utilize hardware, software, networks, and people to conduct input, processing, and output activities. With regard to these components of digital certificates, digital certificates flow from providers to users through software, hardware, and network technologies by traversing the links in the con-



〈Figure 1〉 Configuration of Digital Certificate Flows

figuration shown in <Figure 1>. Providers are those with the authority to issue digital certificates. Users are those who require digital certificates in their daily transactions. Software, network and hardware technologies are also required for the proper functioning of digital certificates. The five

〈Table 2〉 Technology Classes of Digital Certificates

DOMAIN	CLASS	REFERENCES
Software	◦ OS(Operating System)	(Lopez, 2005)
	◦ Certificate Managers	(http5)
	◦ Internet Browsers and Web Applications (online banking and shopping, credit card transaction over the internet)	(Josang, 2002)
	◦ E-mail and Groupware(S/MIME, PEM, IBE, PGP, Lotus Notes Groupware)	(Gerck, 2000); (Hunt, 2001); (Gerck, 2007)
	◦ Documents: XML, MS office, Adobe PDF, etc.	(Josang, 2002); (VeriSign, 2005)
	◦ Electronic Payment System(SET, SWIFT, EMV)	(Ward, 1998); (Mott, 2000)
	◦ Software and other applications	(http6)
Hardware	◦ Computers	(VeriSign, 2004)
	◦ Mobile devices(cellular phones, PDAs, etc.)	(Nambiar, 2004)
	◦ Web Servers/Clients	(VeriSign, 2004)
	◦ Routers	(Cisco, 2003)
	◦ Smartcards	(Ward, 1998); (http13)
	◦ USB tokens	(IdenTrust, 2007); (http13); (http14)
	◦ Cable Modems	(Hancock, 2000); (VeriSign, 2005a)
Network	◦ WAP	(Nambiar, 2004)
	◦ Internet	(http14)
	◦ Intranet	(http14)
	◦ VPN(operating with IPSec, PPTP, etc.)	(Cisco, 2003); (Jaweed, 2003)
	◦ Extranet	(http14)
User	◦ Personal	(http6)
	◦ Business	(Jaweed, 2003)
	◦ Organization	(http6); (http5)
	◦ Government	(http6); (VeriSign, 2004); (IdenTrust, 2007)
Provider	◦ CA	(Venter, 2003); (VeriSign, 2004)
	◦ Financial Institution(e.g. banks, etc.)	(Mott, 2000)
	◦ Government	(http7)

domains and the configuration of digital certificate flows guide our review of the characteristics of digital certificates.

3.2 Elements of Classification Framework

We conducted a literature review in order to identify the major classes of digital certificate technologies within five domains <Table 2>. The technological characteristics of selected classes are described in the following sections.

3.2.1 Software Technology

In this domain, digital certificates are issued or integrated with specific applications. If a customer purchases any software from a store, the customer obviously will know who produced the software. However, when he/she downloads software from the Internet, there is a high level of risk that the software may be inauthentic. One solution to this security issue is the VeriSign Digital Certificate. VeriSign is the preferred provider of digital certificate services for Microsoft's Technology Platform (including Windows 95, Windows NT Workstation, Windows NT Server, etc.) (http8). Via the use of digital signatures, software developers can include information about themselves and their code within their programs.

Digital signatures can also be signed by users by using certain software or applications. For example, in Microsoft Word, Excel, PowerPoint, and Outlook, VBA code supports the signing and verification of digital signatures. Third-party applications also employ VBA 7.0 to support their digital signatures (VeriSign, 2005b).

The most frequently utilized software technologies are web browsers such as Internet Explorer, Netscape Navigator, Firefox, or Google Chrome. These browsers perform duties such as encryption, decryption, and data signing via the use of digital certificates. However, this is an irreducibly complex area, and the recent proliferation of security attacks shows that a digital signature created with a software-based private key is no guarantee that the signature was actually created by the legitimate owner (http15). Thus, additional classes of digital certificates are required.

3.2.2 Hardware Technology

To alleviate security concerns, new technologies have been developed that can embed digital certificates in hardware. Digital certificates are currently being used to provide security and validation for wireless connections, and hardware manufacturers are one of the latest groups to adopt them. For instance, in July of 2000, VeriSign Inc. (Mountain View, CA), announced its Cable Modem Authentication Services, which allow hardware manufacturers to embed digital certificates into cable modems in order to help prevent the pirating of broadband services via device cloning (Hancock, 2000). Additionally, hardware producers generate cryptographic keys and corresponding digital certificates which can be utilized by manufacturers or cable service providers to identify individual modems automatically.

Recently, Cisco IOS Release 12.3(4)T introduced a Certificate Server that offers functionality for issuing digital certificates, enabling router-based network security. This new feature allows a Cisco IOS software router to issue and revoke x.509 digital certificates, thus eliminating the requirement for a costly and difficult-to-administer third-party certification authority. The initial phase of the certificate server fulfills the need for certificates to be issued to other Cisco IOS Systems (Cisco, 2003).

A certificate server supports the distribution of a Certificate Revocation List (CRL) to smaller networks via the Cisco IOS SCEP server. For larger networks, an external server for CRL distribution is encouraged, so as to reduce the load on the certificate server router. The certificate server can issue large volumes of certificates limited only by the contents of the X.509 serial-number. Different platforms are selected depending on the router load, processor speed, and memory availability. Certificate validation does not, therefore, induce additional load on the certificate server router, beside that required to respond to CRL retrieval requests (Cisco, 2003).

While personal computers and servers are the main players with regard to digital certificate use, the use of digital certificates in other devices is increasing. Examples include mobile devices, smartcards, and USB tokens. For instance, EMV is a specification developed by Europay, and is targeted toward MasterCard and Visa credit and debit card payments, which would be carried out using an IC chip embedded on the card. These chips can store digital certificates and symmetric keys for MAC and encryption, and also have the power to digitally sign and verify messages (Ward, 1998).

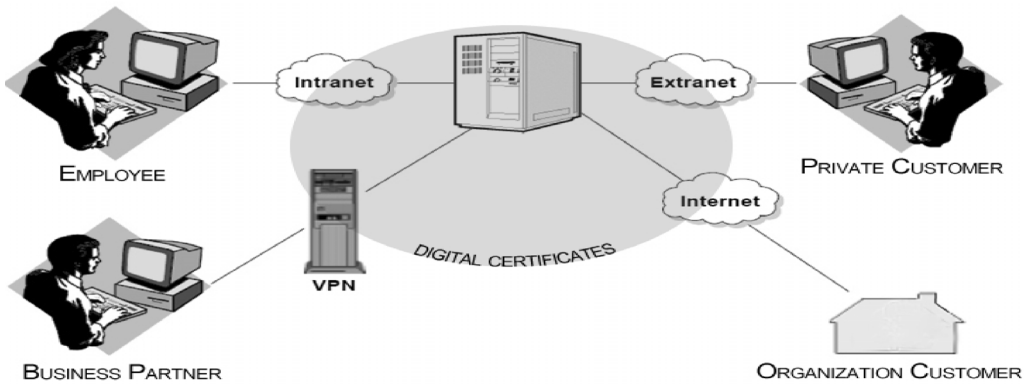
Another example are the certificates issued by PremierAccess, Entrust, and VeriSign that can be installed onto smart cards, as well as other digital certificate storage devices produced by Aladdin, Datakey, Gemplus, Rainbow, Axalto, and Sony. Once these certificates are enrolled in PremierAccess, they can be used for user authentication and access authorization (http13).

Aladdin provides the world's number one USB authenticator token, which is called the eToken PRO Anywhere. It is a portable, reader-less, smartcard-based token that enables secure access to the Web, authentication, digital signatures, encryption, decryption, and secure e-mail from any computer with a USB port and an Internet connection. Using eToken PRO Anywhere, users can access their networks and critical data easily, conveniently and most of all, securely, from just about anywhere (http14). In conclusion, digital certificates can be embedded in computers and related hardware, such as smartcards and microprocessor chips. Digital certificates enable the highest level of security by generating Public Key Infrastructure (PKI) and conducting cryptographic operations on the secure device itself, without exposing the private key.

3.2.3 Network Technology

Digital certificates can be employed in different networks. Some digital certificates support only Virtual Private Networks (VPN). Remote access using an IPSecVPN uses digital certificates to provide a high level of assurance regarding the authenticity of clients (Jaweed, 2003). <Figure 2> demonstrates how people employ digital certificates over different networks.

<Figure 2> shows that digital certificates can be employed using the Intranet, Extranet, Internet, and Virtual Private Networks. The objectives of digital certificates may differ according to the networks. For example, an employee may utilize an Intranet digital certificate to log onto a company desktop. Extranet digital certificates may be used when a private customer dials in. VPN digital certificates are designed for a variety of specific purposes. For example, a corporate partner may use a VPN digital certificate when remotely accessing corporate information. In such applications, digital certificates must provide strong authentication, as well as secure connections and data exchanges conducted between servers and clients.



〈Figure 2〉 Usage of Digital Certificate over Different Networks

Digital certificates are also used with mobile devices. WAP is an open international standard for application layer network communications within a wireless communication environment. Its primary use is to enable access to the Internet (HTTP) from a mobile phone or PDA (http12). In WAP, security is provided through the Wireless Transport Layer Security (WTLS) protocol (in WAP 1.0) and the IETF standard Transport Layer Security (TLS) protocol (in WAP 2.0) (Nambiar, 2004). The WTLS protocol is a PKI-enabled security protocol, which is designed to secure communications and transactions over wireless networks. It is used with the WAP transport protocols to provide security on the transport layer between the WAP server in the WAP gateway. The security services provided by the WTLS protocol are authentication, confidentiality, and integrity (Nambiar, 2004).

3.2.4 Users

This domain characterizes digital certificates on the basis of user characteristics. Four classes of users are recognized-Personal, Business, Organizations, and Government.

Personal certificates are issued to individuals primarily for the purpose of securing their email and constructing secure SSL online transactions. The transmitted data may be either personal private information or any other sensitive data.

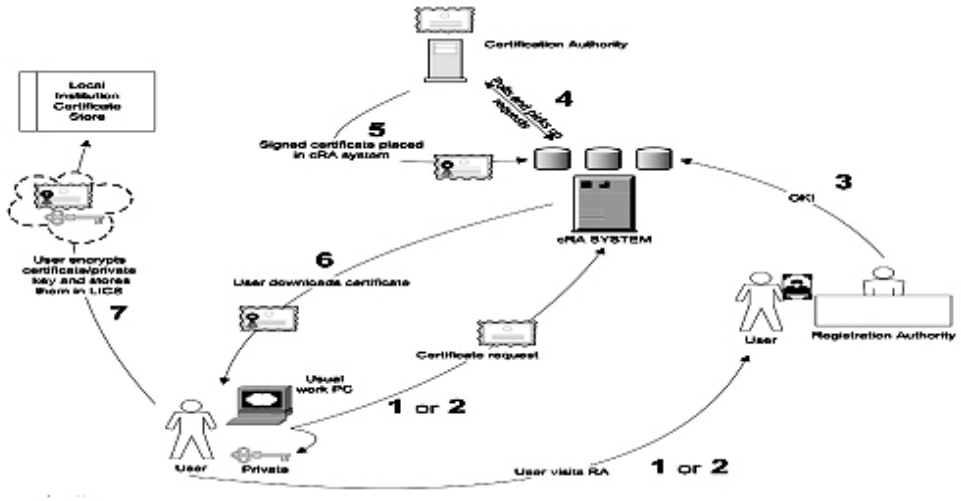
Businesses purchase digital certificates on a yearly or long term basis, both to render their company transactions more secure and to gain consumer trust. Retaining consumer trust is difficult, because trust can only be established slowly, but can be destroyed almost instantly (Lopez, 2005).

Organizations exchange data between other entities, and provide digital certificates for their consumers to ensure strong authentication and secure transactions.

The government employs digital certificates to ensure national security. For example, IdenTrust provides a complete hardware and software certificate service to streamline and strengthen identity authentication for DoD (Department of Defense) industry partners and for other related organizations (IdenTrust, 2007).

3.2.5 Providers

This domain characterizes digital certificates based on the characteristics of providers. Three classes of providers are recognized-Certificate Authorities (CA's), Financial Institutions (e.g. banks, etc.), and



〈Figure 3〉 Procedures for Requesting and Downloading a Digital Certificate

Government. <Figure 3> illustrates the issuance of a digital certificate. This process can be readily understood by following the numbered steps.

The CA is an entity which issues and revokes certificates. An in-house server or a TTP (Trusted Third Party) such as Entrust, Baltimore, or VeriSign, can function as a CA. The CA provides a basis for trusting a Public Key Infrastructure (PKI), because it manages public key certificates over their entire life cycle (Hunt, 2001). There are two types of CA's: Private and Public. Some CA's, such as GeoTrust, delegate the control of the SSL certificates to the entity that purchased them, whereas others provide a centralized certificate purchasing and lifecycle management service.

The management of SSL certificates is a critical competency for any enterprise security team. These certificates essentially provide today's secure e-business applications. Their management requires no additional hardware or software, and may be undertaken by entities of any and all sizes.

GeoTrust Europe's Enterprise SSL is used by businesses of all sizes as a cost-efficient replacement for the purchase of multiple individual SSL certificates via retail sites. Enterprise SSLs are also utilized by some of the world's leading companies and many European government organizations as a convenient and cost-effective alternative to the management of expensive in-house PKI software and hardware (http4). Financial institutions that desire to be a CA because they see trust as their business may be somewhat put off due to the expenses inherent to full deployment.

3.2.6 Digital Certificate Classification Framework

Our framework for digital certificate classification integrates the five domains described in sections 3.2.1-3.2.5 with the VeriSign types and levels of assurance described in section 2.2.2. We adopted the VeriSign method into our framework because it is quite common and has been well-characterized in terms of the assurance level of digital certificates. Within each domain, classes of digital certificates are classified according to the VeriSign type and the level of assurance <Table 3>.

〈Table 3〉 Digital Certificate Classification Framework

DOMAIN	CLASS	TYPE AND LEVEL OF ASSURANCE		
		SERVER CERTIFICATE	DEVELOPER CERTIFICATE	PERSONAL CERTIFICATE
Software	OS(Operating System)			
	Certificate Managers			
	Internet Browsers and Web Applications (online banking and shopping, credit card transaction over the internet)			
	E-mail and Groupware(S/MIME, PEM, IBE, PGP, Lotus Notes Groupware)			
	Documents: XML, MS office, Adobe PDF, etc.			
	Electronic Payment System(SET, SWIFT, EMV)			
	Software and other applications			
Hardware	Computers			
	Mobile devices(cellular phones, PDAs, etc.)			
	Web Servers			
	Routers			
	Smartcards			
	USB tokens			
	Cable Modems			
Network	WAP			
	Internet			
	Intranet			
	VPN(operating with IPSec, PPTP, etc.)			
	Extranet			
User	Personal			
	Business			
	Organization			
	Government			
Provider	CA			
	Financial Institution(e.g. banks, etc.)			
	Government			

Assurance Level: ● - high ◉ - medium ○ - low

Ⅳ. Application of Digital Certificate Classification Framework

To demonstrate the adequacy of our digital certificate classification framework, we populated it with VeriSign's extensive range of digital certificates. Our classification framework accommodates VeriSign's extensive range of digital certificates, and reports the assurance level associated with each <Table 4>.

Within each domain, VeriSign's digital certificates are organized by class, VeriSign type, and level of assurance. It can be clearly observed that personal certificates provide a high level of assurance to the greatest number of classes (15), followed by server certificates (12) and developer certificates (7). This overall ranking is reflected in the ranking of all of the domains except the following. Only in the user domain did personal certificates provide a high level of assurance to less classes (1) than did server certificates (3). Only in the network domain did server certificates provide a high level of assurance to less classes (0) than did developer certificates (0) or personal certificates (4).

<Table 4> also identifies the application of VeriSign type and assurance levels of individual classes of digital certificates. For instance, server certificates are principally utilized via Internet browsers and web applications (online banking and shopping, credit card transaction over the internet) using SSL sessions or other types of security systems. Additionally, server certificates and personal certificates are used with hardware more frequently than are developer certificates.

Ⅴ. Discussion and Conclusion

In this paper, a classification framework for digital certificates based on a broad conceptual review of digital certificate technologies was developed. This taxonomy is innovative, and is useful in a variety of situations. First, the taxonomy assists organizations, enterprises, or individuals in understanding what types of digital certificates are available. Second, the supporting descriptive review facilitates a better understanding of digital certificate technologies. Third, the taxonomy is predicated on concepts of class, type, and assurance level in matching the characteristics of the technology to the needs of the user. Fourth, the taxonomy devised herein may assist future researchers to compare and contrast digital certificates and identify opportunities for improvement.

The digital certificate taxonomy discussed in this paper provides a state-of-the-art overview of current digital certificate technologies. We anticipate that this broad overview of the rapidly developing domain of digital certification technologies and the resultant taxonomy will prove useful for both researchers and practitioners. First, the development and adoption of such a taxonomy of digital certificate technologies will stimulate and foster new research. For example, new initiatives might be researched, such as combining various digital certificate technologies to deal with increasingly secure security functions. Second, one of the strengths of our framework is the focus on the data flow of the digital certificates from providers to users. According to our classification framework, it is important for an organization to know which digital certificate technologies are currently available.

In addition to these contributions, this study opens the door to many new research opportunities. Perhaps the most obvious way to extend this research would be to address the study's limitations. First, our review of digital certificate technologies lacks

〈Table 4〉 Application of the Digital Certificate Classification Framework

DOMAIN	CLASS	TYPE AND LEVEL OF ASSURANCE		
		SERVER CERTIFICATE	DEVELOPER CERTIFICATE	PERSONAL CERTIFICATE
Software	OS (Operating System)	●	◉	●
	Certificate Managers	◉	◉	◉
	Internet Browsers and Web Applications (online banking and shopping, credit card transaction over the internet)	●	●	●
	E-mail and Groupware (S/MIME, PEM, IBE, PGP, Lotus Notes Groupware). (Hunt, 2001)	●	-	●
	Documents: XML, MS office, Adobe PDF, etc.	○	◉	●
	Electronic Payment System (SET, SWIFT, EMV)	●	-	○
	Software and other applications	○	●	◉
Hardware	Computers	●	●	●
	Mobile devices (cellular phones, PDAs, etc.)	●	◉	●
	Web Servers	●		◉
	Routers	◉	◉	◉
	Smartcards	-	-	●
	USB tokens	-	-	●
	Cable Modems	◉	-	○
Network	WAP	◉	●	●
	Internet	◉	●	●
	Intranet	◉	◉	●
	VPN (operating with IPSec, PPTP, etc.)	◉	○	●
	Extranet	◉	○	-
User	Personal	-	-	●
	Business	●	●	○
	Organization	●	◉	○
	Government	●	○	○
Provider	Certification Authority	●	●	●
	Financial Institution (e.g. banks, etc.)	●	○	●
	Government	◉	○	○

Assurance Level: ● - high ◉ - medium ○ - low

the detail required to support specific initiatives. More detailed study would clearly be required in order to identify more practical applications for the digital certificate classification framework proposed herein. Second, we included only the common technology classes. More research to extend this study will also

be required to analyze and define alternative digital certificate technologies. For example, a Delphi approach might be used to evaluate the framework. Finally, future research concerning design science is recommended to extend the finding of this study, as our research constituted only a conceptual framework.

In conclusion, despite the acknowledged limitations, we believe that the classification framework addressed in this paper will facilitate a more detailed and deeper understanding of the applications of digital certificates, and should provide a blueprint for the application of digital certificate concepts and principles in e-commerce and e-business organizations.

References

Aladdin, Using Entrust™ Digital Certificates with eToken, 2001, www.eAladdin.com.

Bosworth, K. P. and N. Tedeschi, "Public Key Infrastructures-The Next Generation", *BT Technology Journal,* Vol.19, No.3, July 2001, pp. 44-59.

Chau, J., "Digital Certificates-Is Their Importance Underestimated?", *Computer Fraud and Security*, December 2005, pp. 14-16.

Chheda, N., The Governing Dynamics of Digital Certificates: The Evaluation of the Adoption of Digital Certificates in the E-Business Environment., *Temple University*, Fox School of Business, Unpublished research, 2004.

Cisco Systems, Inc., "Certificate Server: Simplifying IPSec VPN Deployment with Digital Certificates", *Data Sheet*, 2003, pp. 1-2.

Gerck E., "Overview of Certification Systems: X. 509, PKIX, CA, PGP and SKIP", *THE BELL*, Vol.1, No.3, July 2000, pp. 3-8, (continued on http://www.thebell.net/papers/certover.pdf).

Gerck, E., Comparison of Secure E-Mail Technologies X.509/PKI, PGP, and IBE. *ICFAI University Press*, 2007, pp. 171-196.

Hancock, B., "Digital Certificates Get Creative", *Computers and Security*, Vol.19, No.6, 2000, pp. 480-482.

Hunt, R., "Technological Infrastructure for PKI and Digital Certification", *Computer Communications*, Vol.24, 2001, pp. 1460-1471.

IdenTrust, IdenTrust ECA Digital Certificates, *The IdentTrust ECA Program*, 2007.

Jaweed, S., "Could There Ever Be a Unitary Digital Certificate?", *Information Security Technical Report*, Vol.8, No.3, 2003, pp. 36-44.

Josang, A., D. Povey, and A. Ho, "What You See is Not Always What You Sign", *In the proceedings of AUUG2002*, Melbourne, September 2002. Vol.4, No.6.

Laudon, K. C. and P. Jane, Management Information Systems, *Prentice-Hall, Inc*., 2002.

Levi, A., and C. K. Koç, "Inside Risks: Risks in Email Security", *Communications of the ACM*, Vol.44, No.8, August 2001, p. 112.

Lioy, A., M. Marian, M. Moltchanova, and M. Palapast, "PKI Past, Present and Future", Vol. 5, No.1, January 2006, pp. 18-29.

Lopez, J., R. Oppliger, and G. Pernul, "Why Have Public Key Infrastructures Failed so Far?", *Internet Research*, Vol.15, No.5, October 2005, Emerald, Bradford, England.

Mott, S., "The Second Generation of Digital Commerce Solutions", *Computer Networks,* Vol.32, 2000, pp. 669-683.

McKnight, D. H., V. Choudhury, and C. H. Kacmar, "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology", *Information Systems Research,* Vol.13, No.3, September 2002, pp. 334-359.

Nambiar, S., C. H. Lu, and L. R. Liang, "Analysis of Payment Transaction Security in Mobile

Commerce", *Information Reuse and Integration*, Proceedings of the 2004 IEEE International Conference, Vol.8, No.10, 2004, pp. 475-480.

Oracle, Managing E-Business Security Challenges. *White Paper*, 2002.

Schneier, B., "Two Factor Authentication: Too Little, Too Late", *Communications of the ACM*, Vol. 48, No.4, April 2005, p. 136.

Venter, H. S., J. H. P. Eloff, A Taxonomy for Information Security Technologies, *Elsevier,* 0167-4048/03, 2003, pp. 299-307.

VeriSign, Digital ID: A Brief Overview, *White Paper*, 2004.

VeriSign, VeriSign Cable Modem Authentication Service, *Data Sheet*, 2005a.

VeriSign, VeriSign Microsoft Office/Visual Basic for Applications (VBA) Code Signing Digital Certificates, *Business Guide*, 2005b.

VeriSign, What Every E-business Knows About SSL Security and Consumer Trust, *Business Guide*, 2005c.

VeriSign, Maximizing Site Visitor Trust Using Extended Validation SSL, *White Paper*, 2007.

VeriSign, The Latest Advancements in SSL Technology, *White Paper*, 2008.

Ward, M., "Digital Certificates and Payment Systems", *Information Security Technical Report*, Vol.2, No.4, 1998, pp. 23-31.

Weise, J., Public Key Infrastructure Overview, *SunPSSM Global Security Practice Sun BluePrintsTM OnLine*, 2001.

Wiedenbeck, S., J. Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System", *International Journal of Human-Computer Studies*, Vol.63, 2005, pp. 102-127.

Wilson, S., "Digital Signatures and Future of Documentation", *Information Management and Computer Security,* Vol.7, No.2, 1999, pp. 83-87.

http1, http://www.arx.com/digital-signatures-faq.php

http2, http://www.computerworld.com/printthis/2001/0,4814,61990,00.html.

http3, http://www.computerworld.com/action/article.do?command = viewArticleTOC&special ReportId = 11&articleId = 62002.

http4, http://www.geotrusteurope.com/enterprise_ssl/enterprise-ssl.htm.

http5, http://publib.boulder.ibm.com/iseries/v5r2/ic2924/index.htm?info/rzahu/rzahutypesofcerts. htm.

http6, http://en.wikipedia.org/wiki/Digital_certificates.

http7, http://www.gsa.gov/aces.

http8, http://www.techagreements.com/agreement-review.aspx?num = 23724&title = Microsoft%20/%20VeriSign%20~%20Preferred%20Provider%20Agreement.

http9, https://www.verisign.com.au/repository/tutorial/digital/intro1.shtml.

http10, https://www.verisign.com/products-services/index.html.

http11, http://www.verisign.com/ssl/buy-ssl-certificates/secure-site-services/index.html.

http12, http://en.wikipedia.org/wiki/Wireless_Application_ Protocol.

http13, http://www.securecomputing.com/index.cfm?sKey = 664.

http14, http://www.aladdin.com/etoken/devices/pro-anywhere.aspx.

http15, http://technet.microsoft.com/en-us/library/cc758348.aspx.

http16, http://technet.microsoft.com/en-us/library/cc778623.aspx.

Information Systems Review
Volume 11 Number 3
December 2009

Development and Application of a Digital Certificate Classification Framework: A Configuration Perspective

Changsu Kim* · Dilshodjon Gafurov**

Abstract

In this paper, we review digital certificate technologies and their applications in e-commerce. Current digital certificate technologies are evaluated and their importance is explained. The configuration of certificate flows from providers to users through software, hardware, and network technologies is described. These five domains and the configuration of digital certificate flows guide our review of the characteristics of digital certificates. We then develop a framework for the classification of digital certificates that integrate these five domains with VeriSign's types and levels of assurance. In order to demonstrate the adequacy of our digital certificate classification framework, we populated it with VeriSign's digital certificates. Within each domain, VeriSign's classes of digital certificates are classified in accordance with the VeriSign type and level of assurance. The results of our analysis suggest that the framework is a useful step in developing a taxonomy of digital certificate technologies. The strengths and weaknesses of the study are discussed, and opportunities for further research are identified and discussed.

Keywords: Digital Certificates, Digital Certificate Technology, Classification Framework

* Professor, School of Business, Yeungnam University
** Graduate student, School of Business, Yeungnam University

◐ 저 자 소 개 ◑

김 창 수 (c.kim@yumail.ac.kr)

영국 London School of Economics(LSE)의 정보시스템학과(Information Systems Department)에서 전자상거래 박사학위를 취득하고, 현재 영남대학교 경영학부 교수로 재직하고 있다. 미국 University of Texas at Austin의 McCombs Business School과 영국 런던대학교(University of London)의 School of Computer Science and Information Systems에서 객원교수를 역임하였다. 주요 연구분야는 e-비즈니스, 디지털콘텐츠 비즈니스 그리고 정보시스템 분석 및 설계이다. 주요 저서로는 [e-비즈니스 원론], [경영정보시스템], [정보시스템 분석 및 설계], [디지털콘텐츠 비즈니스], [고객관계관리], [인터넷 비즈니스 창업과 경영] 등이 있다.

딜셔드 가푸로프 (dgafurov2001@yahoo.com)

영남대학교에서 경영학 학사를 취득하고 현재 경영정보관리 전공으로 경영학 석사과정에 재학중이다. 주요 연구관심분야는 e-비즈니스이다.

논문접수일 : 2009년 05월 26일 **게재확정일 : 2009년 10월 06일**
1차 수정일 : 2009년 07월 22일 **2차 수정일 : 2009년 09월 15일**