

합의문 (초안)

신청인 김 기 창(金基昌)

서울 성북구 안암 5가 xxxxx (keechang@fastmail.fm)

피신청인 사단법인 금융결제원

(우)135-758, 서울 강남구 역삼동 717

소송 대리인 법무법인 광장(담당 변호사 정진영 등)

前 文

- 피신청인은 전자서명법령에 규정된 요건을 충족하는 가입자 소프트웨어를 제공할 의무가 있고,
- 가입자 소프트웨어는 공인인증서의 발급, 관리 및 이용에 필요한 설비이고,
- 전자서명법 제7조에 따른 피신청인의 의무는 공인인증서의 발급, 관리 및 이용에 모두 적용되는 것이긴 하나,
- 본 합의문은 이 사건 분쟁의 신속하고 원만한 해결을 위하여, 이용자가 클라이언트(client)의 지위에서 공인인증서를 “이용”하는데 필요한 소프트웨어(이하 “소프트웨어”라고만 한다)와 관련된 사항만을 정한다.

本 文

1. 피신청인은 다음 중 하나를 자유로이 선택하여, 그 소프트웨어(들)에 대한 최상위 인증기관의 심사 등 전자서명 법령에 규정된 요건을 구비하여 이용자들에게 제3조에 정한 방법으로 제공한다:
 - ① 인터넷 익스플로러 웹브라우저 이용자를 위하여는, 피신청인의 등록대행기관들이 현재 각각 제공하는 소프트웨어들 중 하나를 피신청인이 확보하거나, 이와 유

사한 소프트웨어를 마련하고, 파이어폭스, 사파리, 오페라 웹브라우저 이용자를 위하여는 별도의 소프트웨어를 마련한다, 또는

② 인터넷 익스플로러, 파이어폭스, 사파리, 오페라 웹브라우저 이용자들이 사용할 수 있는 하나의 소프트웨어를 마련한다.

2. 소프트웨어(들)의 제공은 이 합의문이 조정조서에 기재된 날로부터 8개월 이내에 이루어져야 한다. 단, 한국정보보호진흥원의 심사 및 정보통신부 장관의 확인에 소요된 기간 중 처음 2개월은 산입하지 아니한다.

3. 소프트웨어(들)은 다음과 같은 방법으로 제공한다:

① 피신청인이 배포자로서 코드사인을 하고, 적어도 5개 이상의 웹서버에서 내려받을 수 있도록 업로드 한 후, 그 서버들의 URL을 피신청인의 홈페이지에 게시하고,

② 소프트웨어(들)이 준수하는 프로토콜과 API는 피신청인의 홈페이지에 게시한다.

4. 소프트웨어(들)은 다음 환경에서 정상 작동하여야 한다:

① 인터넷 익스플로러 6.0 이상 (윈도우즈 98/2000/XP/Vista)

② 파이어폭스 1.5 이상 (윈도우즈 98/2000/XP/Vista, 매킨토시 OS X, 리눅스 Ubuntu/Debian¹)

③ 오페라 8.0 이상 (윈도우즈 98/2000/XP/Vista, 매킨토시 OS X, 리눅스 Ubuntu/Debian)

④ 사파리 1.3 이상 (매킨토시 OS X)

5. 피신청인이 마련한 소프트웨어(들)에 대하여 한국정보보호진흥원이 부적격 판정을 내리거나, 정보통신부 장관의 확인이 거절되어 위 제2조에 정한 기한 내에 소프트웨어(들)을 제공하지 못하게 되는 경우, 피신청인은 부적격 판정이 내려진 날 또는 확인 거절 처분이 내려진 날 중 앞선 날로부터 4개월 이내에 적절한 소프트웨어(들)을 위 제3조에 정한 방법으로 제공하여야 한다. 단, 추완 신청에 대한 심사 및 확인

1 테스트 시점의 current version을 뜻함.

에 소요된 기간 중 처음 1개월은 산입하지 아니한다.

6. 다음 각 호의 경우, 피신청인은 위약벌로서 금5억원을 신청인에게 지급한다:
 - ① 이 합의문이 조정조서에 기재된 날로부터 8개월이 만료되는 날까지 소프트웨어(들)에 대한 한국정보보호진흥원의 심사가 신청되지 아니하거나,
 - ② 제5조에 규정된 기한이 만료하는 날까지 소프트웨어(들)이 제공되지 아니하는 경우.
7. 제6조 각 항에 규정된 날로부터 소프트웨어(들)이 제공되는 날까지 피신청인은 하루 1,500,000원으로 계산한 위약벌을 신청인에게 지급한다. 단, 이 조항에 따른 위약벌은 5억원을 넘지 못한다.
8. 제2조 또는 제5조에 정한 기한내에 소프트웨어(들)이 제공되면, 신청인은 이 사건 조정신청서에 기재된 피신청인에 대한 모든 청구, 요구를 확정적으로 포기한다.
9. 이 합의문이 조정조서에 기재된 날로부터 15개월이 도과하도록 소프트웨어(들)이 제공되지 아니하는 경우, 신청인은 피신청인에 대한 재판상, 재판외의 일체의 청구권을 행사할 수 있다.

설 명

前文:

- 공인인증서를 “발급”받고, “관리”하기 위하여 윈도우즈를 이용하여야 하는 현 상황도 당연히 개선되어야 하겠으나, 우선 시급한 부분은 발급받은 공인인증서를 “이용”하는 부분이므로, 이 점에 대한 개선요구로 국한하였습니다.
- 현재 ActiveX 컨트롤을 사용하여 수행하는 작업은 “가입자 설비”가 수행하도록 전자서명 법령이 규정하고 있는 사항들을 넘어선 부분까지도 포함되어 있습니다. 즉, 서버와 클라이언트 간의 교신을 암호화하는 작업도 지금은 ActiveX로 수행하는데, 이 부분은 실은 전자서명법이 요구하는 바가 아닙니다. 전자서명법은 말 그대로 “전자서명”의 생성과 관련된 사항들과, 교신 상대방(서버)이 공인인증서(서버인증서)

를 제시하는 경우 이를 검증하는 기능에 대한 규정만이 있을 뿐입니다.

- 웹서버가 반드시 “공인”서버인증서를 이용해야 한다는 법규정은 없습니다.
Verisign 등 주요 웹브라우저들이 신뢰하는 사설인증기관이 발급한 서버인증서를 사용하여 암호화 교신을 해도 무방하므로, 이런 경우에는 서버-클라이언트 간의 교신 내용을 암호화하는 작업은 브라우저에 탑재된 ssl 모듈을 사용하더라도 법적으로 아무 문제될 것이 없습니다. 이때 사용해야 할 알고리즘이 반드시 SEED 또는 3-DES에 국한되는 것도 **아닙니다**.
- 관련 법령이 SEED 또는 3-DES를 요구하는 부분은 인증서 및 비밀키를 암호화하는 경우에 한합니다. 시설, 장비 규정 5.1.3 에서 말하는 “암호화 알고리즘”은 서버-클라이언트 간 교신을 암호화 할때의 알고리즘이 아닙니다. 규정 5.1.3.은 규정 “5. 전자서명키 생성·관리 설비” 의 하위 규정에 불과합니다. 규정 5는 서버-클라이언트 간의 교신에 관한 내용이 아닙니다.
- 현재 ActiveX로 수행하고 있는 작업들 중, 법의 규제를 받아야 할 부분과 그럴 필요가 없는 부분을 분리하여 이해할 필요가 있고, 합의문은 법의 규제를 받는 부분에 한정합니다. 나머지(서버-클라이언트 간 교신의 암호화)는 자율에 맡기면 됩니다.
- 따라서 합의문에서 말하는 클라이언트 소프트웨어는 시설, 장비 규정 중, 다음에 정해진 기능을 구현하는 소프트웨어를 말합니다:
 - 9.3 전자서명 생성 및 공인인증서 검증 기능
 - 9.4 식별번호를 이용한 본인확인 기능
 - 9.5 시점확인 기능
- 그리고, 전자서명법 제22조의2 제2항에 규정된 기능도 구비하여야 함은 물론입니다. 즉, 공인인증서 파일을 액세스 하여 그 정보를 이용자가 확인할 수 있게 하거나, SEED 또는 3-DES로 암호화된 비밀키 파일을 액세스 하여 가입자가 인증서 로그인 등의 용도로 사용하는 것을 지원해야 합니다.

本文:

제1조(단기 해결방안) 합의문은 즉시 실행가능한 “단기”해결 방안을 담고 있을 뿐입니다.

장기적으로는 PKI자체에 대한 대안, 다양한 디바이스 등에서 사용할 수 있는 인증 솔루션 등도 검토의 대상이 되어야 하겠지만, 합의문에서는 현재 즉시 채용 가능하고, 이미 개발이 완료된 대안들 중에서 피신청인이 자유로이 선택할 수 있도록 하고자 합니다. 따라서 ActiveX를 사용한 방법도 만일 피신청인이 원한다면 계속 유지할 여지를 열어 두고자 합니다. 다만, 나머지 웹브라우저들에서 작동가능한 추가적 대안은 반드시 제공되어야 합니다.

제2조(제공 시한) 오픈웹이 2006.5. 에 문제 제기를 하기 전에도 이미 2002년 경부터 무수히 많은 시정 요구가 거듭되어 왔습니다. 2006.6.30.에는 피신청인에게 분명하고도 자세하게 위법사항의 시정을 요구하였고, 소송이 제기될 것이라는 점도 안내하였습니다. 즉시 구입하여 실행할 수 있는 상용 솔루션도 시장에 이미 있고, 공개소스(GPL 또는 LGPL 조건)로 제공되고 있는 대안도 있습니다. 또한, “피신청인 역시 지원 가능한 운영체제와 웹브라우저의 범위를 넓히기 위하여 꾸준히 노력”해 왔다고 주장하고 있으므로,² 필요한 준비는 이미 상당히 되어 있을 것으로 봄이 합리적일 것입니다. 이러한 여러 사정을 감안하였을 때, 8개월은 충분하다고 판단됩니다. 심사 등에 필요한 기간 중 처음 2개월은 제외되므로 실제로는 8개월 이상의 여유가 부여되어 있습니다.

제3조(제공 방법) 소프트웨어(들)은 인터넷을 통하여 간편하게 배포됩니다. 은행, 전자정부, 쇼핑몰 등 공인인증서 이용을 요구하는 각종 웹서버³들이 자신의 웹페이지 소스를 작성할 때, 소프트웨어(들)의 배포 서버(repository) URL을 정확히 지정해 주기만 하면, 은행 등 웹서버에 접속하는 고객의 컴퓨터가 해당 소프트웨어를 배포 서버로부터 알아서 내려받습니다.

그러나, 클라이언트 소프트웨어를 이렇게 배포, 제공하더라도, 그 소프트웨어가 준수하는 프로토콜과 API 가 공개되지 않으면, 아무도 그 소프트웨어를 사용할 수 없습니다. 그 소프트웨어와 제대로 교신할 수 있는 서버측 인증 솔루션을 설계하기 위하여는 클라이언트 소프트웨어의 프로토콜과 API가 있어야 하기 때문입니다. 따라서 가입자 소프트웨어를 제공하여야 한다는 법 규정은 프로토콜과 API 공개를 당연히 전제하는 것입니다.

공인인증서(와 쌍을 이루는 비밀키)를 이용하여 수행하는 전자서명의 프로토콜은 원칙적

2 2007.3.5. 자 피신청인 답변서 제17면.

3 피신청인은 이를 “이용기관”이라 부르고 있습니다.

으로 KISA Guideline에 기초하여 마련하면 될 것입니다. 서명 대상이 되는 메시지 구성은 금융기관별로 이미 갖추고 있는 금융데이터 네트워크 송수신 스펙을 준용하여 적절히 정하면 될 것입니다. 금융기관이 아닌 웹서버(예를 들어 전자정부 또는 오픈웹 등이 공인전자서명을 접속자로부터 요구할 때)들이 자신의 필요에 맞게 서명대상 메시지를 적절히 구성하는 것도 가능하도록 메시지 관련 프로토콜을 확정지어야 합니다. 인증서 로그인이 구현되는 방법을 정하는 프로토콜도 확정, 공표되어야 합니다.

클라이언트 소프트웨어의 소스코드까지 공개된다면 이상적이겠으나, 소스의 공개를 강제할 근거는 없습니다. 합의문은 공개소스 소프트웨어(들)을 채용할 것을 강요하는 내용이 아닙니다.

서버측 인증 솔루션을 피신청인이 제공할 의무는 없습니다. 그것을 독점 공급할 “권리”는 더더욱 없습니다.

제4조(이용 환경) 공인인증 서비스도 공공 역무의 일종입니다. 외국의 경우, 공공성이 있는 인터넷 서비스는 합의문에 제시된 것의 두세배에 달하는 다양한 이용 환경에서 정상적으로 작동하는지를 테스트하는 것이 당연한 관례로 정착되어 있습니다. 예를 들어, 영국 전자정부 웹사이트는 다음과 같은 이용 환경에서 충분히 테스트 되었습니다:

Windows

MS Internet Explorer 7.05 (on Windows XP)

MS Internet Explorer 5.01 SP2 and 5.5 SP2 (on Windows 98, Windows NT 4 SP 6a, Windows 2000 SP4, Windows XP)

MS Internet Explorer 6.0 (on Windows 98, Windows NT 4 SP 6a, Windows 2000 SP4, Windows XP)

Netscape Navigator 6.x (on Windows 98, Windows NT 4 SP 6a, Windows 2000 SP4, Windows XP)

Netscape Navigator 7.0, 7.2 and 8.0 (on Windows 98, Windows NT 4 SP 6a, Windows 2000 SP4, Windows XP)

Opera 6.01, 7.2, 8.0 and 8.5 (on Windows 98, Windows NT 4 SP 6a, Windows 2000 SP4, Windows XP)

Lynx 2.8.3 (on Windows 98, Windows NT 4 SP 6a, Windows 2000 SP4, Windows XP)

JAWS 7.10 (on Windows 98, Windows 2000 SP4, Windows XP)

Browsealoud 6.0

Mozilla Firefox 1.07, 1.5

Mozilla 1.0 to 1.5, 1.6, 1.7

Macintosh

MS Internet Explorer 5.1 Mac Edition (on Mac OS 9 and OS X)

MS Internet Explorer 5.2 Mac Edition (on Mac OS X)

Netscape Navigator 6.2.2 Mac Edition (on Mac OS X)

Netscape Navigator 7.0, 7.2 and 8.0 (on Mac OS X)

Opera 6.01, 7.2, 8.0 and 8.5 (on Mac OS X)

Lynx 2

Safari 1.2 (OS X)

Safari 2.0 (OS X)

Mozilla Firefox 1.07, 1.5

Linux

Netscape Navigator 6.2.2 (on Linux RedHat 9)

Netscape Navigator 7.0.2 (on Linux RedHat 9)

덴마크의 공인인증기관이 제공하는 소프트웨어(자바 애플릿 형태)는 훨씬 더 다양한 이용 환경에서 정상 작동하고 있습니다.⁴ 그러나 우리의 현실을 고려하고, 본 합의안은 “단기” 해결 방안이라는 점을 충분히 감안하여 테스트 환경을 축소, 제한 하였습니다. 피신청인이 제공한 소프트웨어(들)이 만일 제4조에 열거된 이용 환경에서 정상 작동 되지 않는다는 점이 사후에 입증되는 경우, 피신청인의 의무 이행이 이루어지지 않은 것으로 평가받아야 할 것입니다.

제5조(부적격 판정시의 보완 기간) 최초의 신청과 비교하였을 때, 추완 신청은 경미한 개

⁴ http://www.openoces.org/opensign/supported_platforms.html

선과 시정이 필요한 경우일 터이므로, 4개월의 기간은 충분할 것입니다. 그 기간 내에는 추완 신청 회수의 제약은 없습니다. 그리고 추완 심사에 필요한 기간 중 처음 1개월은 역시 제외되므로, 실제로는 더 긴 여유기간이 주어지는 셈입니다.

제6조(위약벌) 신청인은 이 사건 분쟁의 당사자가 되고자 희망하는 분들을 대표하거나 대리할 권한이 없습니다. 제시된 액수는 손해액을 반영하는 것이 아닙니다.

피신청인은 공인인증기관이기도 하지만, 인터넷지로, 전자금융공동망(계좌이체, 송금, 금융거래정보 조회 등 서비스), 결제대행(Bankpay PG), 전자상거래 지급결제(BANK B2B) 등의 영리 사업을 수행하고 있습니다. 이들 거래는 모두 공인인증서가 반드시 이용되어야 합니다. 공인인증 및 전자서명 처리를 지금과 같이 ActiveX기술로 구현하는 경우, 그 폐쇄성(서버 솔루션과 클라이언트 소프트웨어를 하나의 업체가 모두 제작하고, 그 프로토콜과 API가 전혀 공개되지 않는 상황)과 비호환성으로 인한 lock-in 효과 때문에 신규 사업자의 시장참여가 매우 제약됩니다.

피신청인은 위에 나열한 여러 사업 분야에서 압도적인 시장 점유율을 누리고 있습니다. 전자서명법에 규정된 대로, 공인인증기관이 클라이언트 소프트웨어를 제공하고 공인인증서 처리 API와 프로토콜을 제대로 공개하였다면, 다양한 사업자들이 이 API와 프로토콜을 응용한 혁신적인 상품을 지속적으로 많이 내놓을 수 있을 것이며 이들 사업 분야의 활발한 경쟁과 기술진보가 가능하였을 것입니다.

다양한 웹브라우저를 지원하는데 비용이 많이 들거나, 기술적으로 어렵거나, 이용자에게 불편이 초래되거나, 다른 어떠한 장애도 생기지 않음에도 불구하고, 위법한 현 상황을 피신청인이 집요하게 유지하려는 이유를 선불리 짐작할 필요는 없습니다. 그러나 분명한 사실은, 현재로서는 위 사업 영역들에서 신규 경쟁자들이 혁신적인 기술을 이용하여 시장에 진입하는 것이 현실적으로 불가능하도록 되어 있다는 점입니다.

피신청인이 스스로 마련한 2006년 업무소개서⁵ 제21면을 보면, “개인정보 보호를 위하여 납부시 공인인증서 사용을 의무화하는 등 많은 개선을 하여 2005년도 인터넷지로 처리실적이 크게 증가하였다”고 합니다. 2005년 한해 동안 피신청인이 인터넷 지로로 처리한 액수는 33조원이 넘습니다.

위법한 현 상황을 개선하지 아니한 댓가로 지불되어야 할 위약벌 액수는 이러한 상황을 고

5 http://210.103.193.153/kftc/do/FileDownloader/ko2006.PDF?n=4787&d=GD&f=ko2006.PDF&t=board_pds

려하여 책정되어야 할 것입니다.

제7조(지연 위약벌) 일차적 기한은 실제로는 1년이 넘을 수도 있습니다. 그 기한을 지키지 않은 경우, 또 한차례의 기회를 부여하는 취지입니다. 다만, 지연 위약벌의 상한을 합리적인 수준에서 정하고 있습니다. 지연 위약벌의 산정에 있어서는 정보보호진흥원의 심사나 정보통신부 장관의 확인에 소요된 기한도 산입합니다. 그 이유는, 만일 이들 기관의 심사나 확인이 부당하게 지연되는 경우, 사태 해결의 길이 막히기 때문입니다. 충분한 시간이 허여 되었음에도 피신청인이 적법한 소프트웨어(들)을 제공하지 못하는 경우에는 피신청인보다 우월한 기술을 구비한 자가 공인인증기관이 되는 길을 막아둘 필요는 없을 것입니다.

[date]

신청인

김기창

피신청인

사단법인 금융결제원

서울 중앙지방법원 귀중