

정부주도 샵메일 서비스의 문제점

김기창

사단법인 오픈넷

2014.6.3

위인설관, 억지추항 : “공인”

- 전자문서 및 전자거래 기본법 개정 (2012)
 - 공인전자주소
 - 공인전자문서중계자
 - 미래부는 샵메일사업자 ‘지정권한’ 보유
 - 공인전자문서보관센터 보관문서의 ‘추정력’
 - 공인전자문서보관센터 발급 증명서의 ‘추정력’
 - 정보통신산업진흥원장 발급 유통증명서의 ‘추정력’

선전 내용

#메일의 수신효력

#메일로 전자문서가 수신되면 #메일을 열람하지 않아도 “전자문서 및 전자거래 기본법”에 의해 공인전자주소(#메일)는 수신자가 관리하는 정보처리시스템에 해당되어 전자문서가 수신된 것으로 법적효력이 있습니다. (민법상으로는 도달에 해당)

부정사용 방지

공인전자주소(#메일)는 “전자문서 및 전자거래 기본법”에 의해 주소의 무단 수집·판매·제공 및 스팸메일을 송신할 수 없습니다.

| 구분 | 내용 |
|---------|------------------------------------------------------------------------------------------------------------|
| 부정사용 방지 | - 자동 프로그램 및 기술적 장치를 이용하여 공인전자주소(#메일)를 수집하거나 판매,제공할 수 없음 - 수신자의 공인전자주소(#메일)에 영리 또는 홍보를 목적으로 광고를 송신할 수 없음 |
| 과태료 부과 | - 위 사항을 위반하면 “전자문서 및 전자거래 기본법”에 의해 3천만원 이하의 과태료를 부과 |

샵메일 선전

메일 특성 비교

| 구분 | 우편 | | 전자우편 | |
|----------|--------|-------------------|---------------|--------------|
| | 일반우편 | 내용증명 | e메일 | #메일 |
| 이용환경 | 우체국 방문 | 우체국 방문 | 인터넷 이용 | 인터넷 이용 |
| 발신자 본인확인 | × | ▲ | × | ● |
| 수신자 본인확인 | × | ● | × | ● |
| 송달과정 조회 | × | ● | × | ● |
| 수신확인 | × | ● | ▲ | ● |
| 열람확인 | × | × | ▲ | ● |
| 증명 | 내용 | ● | ▲ | ● (유통증명서) |
| | 시각 | ● | ▲ | ● (유통증명서) |
| | 배발 | ● | ▲ | ● (유통증명서) |
| 이용요금 | 270원 | 2,770원(보통 1,770원) | 50~60원 (대량발송) | 100원/송신 건 |

@ 메일의 '법적' 효력

| | @ 메일 | # 메일 | |
|---------------|------|------|---------------------|
| 의사표시, 계약체결 수단 | Yes | Yes | |
| 효력발생시기: 도달주의 | Yes | Yes | '실제로' 열람했는지 여부와는 무관 |
| 증거능력 | Yes | Yes | |
| 인증서 / 전자서명 사용 | Yes | Yes | |

제 4 조 (전자문서의 효력) ① 전자문서는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 전자적 형태로 되어 있다는 이유로 문서로서의 효력이 부인되지 아니한다.

“문서로서의 효력”이 무엇일까 ?

이른바 # 메일은 ‘문서’가 아닌가, 문서보다 우월한 그 무엇인가 ?

삽메일의 기술적 열개

- ebXML (e-business XML)
- ebMS (e-business Message Service Specification)
- HTTP
- 별도 클라이언트 사용하거나, '웹메일' 형태의 UX 제공
- SMTP 사용하지 않을 이유 ?

삽메일의 현실적 문제



본 연결은 신뢰할 수 없음

Firefox가 안전하게 **www.docusharp.com**로 연결하려고 하지만 실제 보안이 이루어지는지 확인할 수 없습니다.

일반적으로 안전한 연결을 할 때 웹 사이트는 신뢰된 인증 정보를 제공하여야 하지만 현재 사이트는 이러한 확인 정보를 제대로 보내주지 않고 있습니다.

고려할 사항

만일 지금까지 문제 없이 현재 사이트에 계속 접속했다면 이 오류는 누군가가 웹 사이트를 공격했을 수 있으므로 가급적 계속 접속하지 않기를 권장합니다.

사이트에서 나가기

- ▶ 상세 기술 정보
- ▶ 위험 사항 확인

nPost 만 예외

The screenshot shows the nPost website interface with a Certificate Viewer window open. The website header includes the nPOST.kr logo and navigation menus for '전자문서 제도' (Electronic Document System) and '#메일' (Mail). The Certificate Viewer window displays the following information:

Certificate Viewer: www.npost.kr

General | Details

This certificate has been verified for the following usages:
SSL Server Certificate

Issued To

| | |
|--------------------------|-------------------------------------------------|
| Common Name (CN) | www.npost.kr |
| Organisation (O) | <Not Part Of Certificate> |
| Organisational Unit (OU) | Domain Control Validated |
| Serial Number | 6C:FF:9E:B4:3E:A6:F6:53:B5:3F:12:DD:1A:09:E4:11 |

Issued By

| | |
|--------------------------|---------------------------|
| Common Name (CN) | EssentialSSL CA |
| Organisation (O) | COMODO CA Limited |
| Organisational Unit (OU) | <Not Part Of Certificate> |

Validity Period

| | |
|------------|------------|
| Issued On | 14/10/2013 |
| Expires On | 20/10/2014 |

Fingerprints

| | |
|---------------------|-------------------------------------------------------------------------------------------------|
| SHA-256 Fingerprint | 29 4A 0F 06 A2 0B FC FB F5 DD 51 DE 5C 8E FC 15 DA B7 67 F7 EE A3 D0 47 63 A3 03 69 0B 49 20 CC |
| SHA-1 Fingerprint | F8 0E 65 C7 EF A1 9A 74 B9 97 41 B8 4D 50 24 40 42 C5 44 C8 |

국내전용 서비스

DOCUON - Mozilla Firefox

DOCUON

https://www.docuon.co.kr/docuonPortalWeb/service/customerInfoMa

KTNET

DOCUON

홈 / 회원가입 / 로그인 / 전체메뉴보기

Information

다큐온 소개

전자문서 서비스

구축사례

고객센터

프로그램 설치 안내

파트너 프로그램

SERVICE

고객센터

공인인증서 관리

TOP

이용자확인 서비스

HOME > E,do'IAO > A,leAUE@AI%R%R

"oAIAUAU @%,"u%O E,coA% %C,I'IAOA> zoAQA,TiCO'T'U.
%R-iAC > c%XA> AOE@E+ AO'ACQ AO%Asa'U'oe'T'U.

"AI E,do'IAO > c%+A% E,do'IAO > c%+A%'a'cAU E,do'IAO

AO Tpi'oeE
A,ls
(%C,IA> AO'ACIz@AO%zA)

확인

✓ %R%R% %a'u' x' "AIAC, Ae±'aeAs
E,do'IAO AUzi %R-iAC A,le%a'UA> 'Yma%AD%t%,%Asa'U'io,c% > %a'u'zi μzACCT%ā,e'μzACQ'zi A%ā@;i cQ AO%E%zA.
• %R%R% %a'u'
A: 1 Aā AN A@
A: 1 A# (RAG)
AI %a'uA% 'AuAU'Ä±ā%> 'y' pi'ü'è 'y-Ezi ±U'ÄCIz@ (AO)CÑ±'i' <E'ÄCQ, Ae%Ä (AIC'I "E,>c" %C' A KTNET"%6 CQ.)AI
A: "oC'I'Ä" "oAIAUAU @%,"u%O %R%R% (AIC'I "ÜÄ#zÄ(DocuOn)" %C'Ä "ÜÄ#zÄ(DocuOn) %R%R% "%6 CQ.)AC A,le A#I'c' x
AyA-, ±ā, cEzäcN > c%XA> ±OÄCQOA> ,nAUÄ,TiCO'T'U.
A: 2 A# (%a'uAC' "oAó'x'ae)
"çAI %a'uAC' > zE AB 'AuAU'Ä±ā%> 'y'zi ACCTz@ > è%+AUzco'IAā'üAC %AAIA> %o'Ä" > "içQ%B C'I'Ä > c%XA"

윈도우 Only 서비스

The screenshot shows the DOCUON user authentication service page. The page title is "이용자확인 서비스" (User Authentication Service). The breadcrumb trail is "HOME > 회원가입 > 이용자확인서비스". The page content includes a notice: "공인전자문서보관소 회원은 실명 가입을 원칙으로 합니다. 아래의 사항을 정확히 입력해 주시기 바랍니다." (For certified electronic document storage service members, real-name registration is the principle. Please enter the following information accurately.) Below this, there are three tabs: "개인 회원가입" (Personal Registration), "사업체 회원가입" (Business Registration), and "사업체담당자 회원가입" (Business Representative Registration). The "개인 회원가입" tab is active, showing a registration form with fields for "주민등록번호" (Residence Registration Number) containing "630123" and "김기창" (Kim Gi-chang) for "이름" (Name). A "확인" (Confirm) button is present. A browser error message is displayed in the top right corner: "The page at https://... undefined". The left sidebar contains the KTFNET logo and an "Information" menu with items: "다큐온 소개", "전자문서 서비스", "구축사례", "고객센터", "프로그램 설치 안내", and "파트너 프로그램". At the bottom, there is a section for "서비스 약관 및 개인정보 취급방침" (Service Terms and Privacy Policy) with a "서비스 약관" (Service Terms) link. The terms section is partially visible, starting with "제 1 장 총 칙" (Chapter 1 General Provisions) and "제 1 조 (목적)" (Article 1 Purpose).

플러그인 의존 서비스



발신자, 수신자 본인확인?

The image displays two screenshots from a web browser. The left screenshot shows the '휴대폰 본인 확인' (Mobile Phone Self-Verification) page on the NICEVID portal. It includes a progress bar with steps: 01 정보입력 (Information Input), 02 정보확인 (Information Confirmation), and 03 완료 (Complete). The form fields are filled with: 이름 김기창, 휴대폰번호 010-4015-0209, 이동통신사 KT, 성별 남자, 생년월일 1963-1-23, and 국적 내국인. There are checkboxes for privacy policies and buttons for '다음' (Next) and '취소' (Cancel). A note at the bottom states: '꼭 확인하세요. 본 휴대폰본인확인 서비스는 NICE평가정보(주)와 제휴한 모빌리언스 화면에서 제공되는 서비스입니다. 본인 명의의 휴대폰 정보를 정확하게 입력해 주시기 바랍니다.'

The right screenshot shows the 'docu# 회원가입' (docu# Member Registration) page. It features a progress bar with steps: 약관동의 (Terms Agreement), 가입인증 (Registration Confirmation), 회원 정보입력 (Member Information Input), and 회원 가입완료 (Member Registration Complete). The '가입인증' step is highlighted. Below the progress bar, there is a section for '가입인증' (Registration Confirmation) with a warning: '가입중 입력하신 개인정보는 고객님의 동의 없이 제 3자에게 제공되지 않으며 개인정보보호방침에 따라 안전하게 보호되고 있습니다.' It also lists '가입인증 확인 대상' (Registration Confirmation Targets) as '만 14세 이상 가입' (Selected) and '만 14세 미만 가입 (만 14세 미만의 경우 반드시 법정대리인 인증을 통해 등록 하셔야 합니다.)' (Not Selected). Under '본인인증 방법 선택' (Self-Authentication Method Selection), three options are shown: '공인인증서 인증' (Public Certificate Authentication), '휴대폰 인증' (Mobile Phone Authentication), and '대면확인' (Face-to-face Confirmation). The '휴대폰 인증' option is selected. At the bottom, there is a section for '본인인증 정보입력' (Self-Authentication Information Input).

- 휴대폰 + 주민번호 이용한 본인 확인?
- 이메일 계정 발급시 본인 확인하면 안될까?

스팸 # 메일

The screenshot shows a web browser window displaying the DocuSharp webmail interface. The address bar shows the URL: <https://www.docusharp.com/mailbox/mailBox.jsp?boxType=recv#>. The page title is "docu#". The navigation bar includes links for "#메일안내", "사서함", "주소록", "마이페이지", "전자문서 서비스", and "고객지원". The user is logged in as "김기창님" with 0 points.

The left sidebar displays email statistics:

- 받은 메일함: 0/1
- 보낸 메일함: 1
- 임시 보관함: 0
- 보낼 메일함: 0
- 내 메일함: 설정
- 스팸 메일함: 0
- 휴지통: 0
- 유통증명서: 0

The main area is titled "메일작성" (Compose Email). It includes buttons for "보내기" (Send) and "저장하기" (Save). The "보내는 사람" (From) field is set to "대표#김기창.개인". The "받는 사람" (To) field is set to "((고객센터))#SK텔레콤.법인". The "제목" (Subject) field is set to "RE: RE: <DocuSharp> 회원가입을 진심으로 감사드립니다.". The "보내는 방법" (Send Method) section has checkboxes for "중계서버 송신의뢰" (unchecked) and "열람결과 요청" (checked). The "파일첨부" (Attachments) section shows "Choose File" and "No file chosen".

The email body text is:

안녕하세요,
거듭 메일을 드리게 되어 죄송합니다.
스팸메일함이 있는데요(메일페이지 왼쪽). 어떤 업체들이 장차 스팸을 보낼 것으로 예상하시는지요? 그리고 도큐샤프는 스팸 필터 기능은 구비하고 계신지요?
김기창 드림

The bottom of the composition area shows the HTML source code: `body p`.

메일 '본인확인' 취약점

전자문서유통포털
docu# 회원로그인

전자문서 유통포털

회원 로그인 | 아이디 찾기 | 비밀번호 초기화

- 회원 가입 시 입력한 정보를 바탕으로 아이디를 찾을 수 있습니다.
- 본인 인증 시 제공되는 정보는 인증 이외의 용도로 이용 또는 저장하지 않습니다.
- 법인 회원의 경우, 아이디/비밀번호 찾기는 고객센터(1670-3090)로 문의해주세요

| 개인회원 아이디 찾기 | 법인회원 아이디 찾기 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>이름/연락처로 확인</p> <p><input type="radio"/> 휴대폰 번호 <input checked="" type="radio"/> 이메일</p> <p>이름 <input type="text" value="김기창"/></p> <p>이메일 <input type="text" value="keechang.kim@gmail.com"/></p> <p><input type="button" value="확인"/></p> | <p>이름/생년월일로 확인</p> <p>이름 <input type="text"/></p> <p>생년월일 <input type="text" value="-년도-"/> <input type="text" value="-월-"/> <input type="text" value="-일-"/></p> <p>성별 <input checked="" type="radio"/> 남자 <input type="radio"/> 여자</p> <p><input type="button" value="확인"/></p> |

“# 메일 ID” 쉽게 노출

The screenshot shows the 'docu# 회원로그인' (docu# Member Login) page. At the top right, it says '전자문서 유통포털' (Electronic Document Distribution Portal). The main navigation includes '회원 로그인' (Member Login), '아이디 찾기' (Find ID), and '비밀번호 초기화' (Reset Password). Below this, there are instructions: '회원 가입 시 입력한 정보를 바탕으로 아이디를 찾을 수 있습니다.' (You can find your ID based on the information entered during registration.), '본인 인증 시 제공되는 정보는 인증 이외의 용도로 이용 또는 저장하지 않습니다.' (Information provided during self-authentication is not to be used or stored for any other purpose.), and '법인 회원의 경우, 아이디/비밀번호 찾기는 고객센터(1670-3090)로 문의해주세요.' (For corporate members, please contact the customer center (1670-3090) for ID/password search.).

There are two tabs: '개인회원 아이디 찾기' (Find ID for Individual Member) and '법인회원 아이디 찾기' (Find ID for Corporate Member). The '개인회원 아이디 찾기' tab is active. It contains input fields for '이름/연락처로' (Name/Contact Info), '휴대폰 번호' (Mobile Number), '이름' (Name) with the value '김기' (Kim Ki), and '이메일' (Email) with the value 'kee'. A '확인' (Confirm) button is at the bottom of the form.

A modal window titled '아이디 찾기' (Find ID) is overlaid on the form. It contains the message: '입력하신 정보와 일치하는 아이디가 검색되었습니다.' (A matching ID was found based on the entered information.) and '아이디: youknowit2' (ID: youknowit2). A '확인' (Confirm) button is at the bottom of the modal.

메일 비밀번호 reset

회원 로그인 | 아이디 찾기 | 비밀번호 초기화

- 비밀번호는 본인 확인 절차를 거친 후 초기화 시켜 드립니다. 회원가입 시 등록한 정보를 아래 입력해 주세요.
- 대면평가를 통해서 등록하신 분께서는 고객센터(1670-3090)에 문의해 주세요.

| 개인회원 비밀번호 변경 | 법인회원 비밀번호 변경 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>휴대폰을 통한 인증</p> <p><input checked="" type="radio"/> 14세 이상 <input type="radio"/> 14세 미만</p> <p>아이디 <input type="text" value="youknowit2"/></p> <p>이름 <input type="text" value="김기창"/></p> <p>휴대폰 <input type="text" value="010"/> - <input type="text" value="4015"/> - <input type="text" value=""/></p> <p>확인</p> | <p>공인인증서를 통한 인증</p> <p><input checked="" type="radio"/> 14세 이상 <input type="radio"/> 14세 미만</p> <p>아이디 <input type="text"/></p> <p>이름 <input type="text"/></p> <p>주민등록번호 <input type="text"/> - <input type="text"/></p> <p>확인</p> |

메일 비밀번호 = 휴대폰인증

The image shows a web browser window displaying the NICE ID mobile authentication and login interface. The browser address bar shows the URL: <https://nice.checkplus.co.kr/CheckPlusSafeModel/checl>. The page title is "휴대폰본인확인 - 안심본인인증 - NICE평가정보 - Mozilla Firefox".

The main content area is titled "안심본인인증" (Safe Self-Authentication) and includes a sub-section for "휴대폰본인확인" (Mobile Self-Authentication). The form fields are as follows:

- 성명 (Name): 김기창 (Kim Gi-chang), Gender: 남 (Male), Nationality: 내국인 (Domestic)
- 생년월일 (Date of Birth): 1963년 01월 23일 (January 23, 1963)
- 휴대폰번호 (Mobile Number): 010 - 4015 - 0209
- 이동통신사 (Mobile Carrier): KT

There are also checkboxes for "휴대폰본인확인 이용약관 전문보기" (View Mobile Self-Authentication Terms), "개인정보 이용 및 활용 동의 전문보기" (View Personal Information Usage and Utilization Consent), and "고유식별정보 처리 동의 전문보기" (View Unique Identification Information Processing Consent).

The bottom of the page features logos for SK Telecom, allnet kt, and LG U+, along with a security seal and the text "최우수 기업들이 안심하고 선택하는 NICE ID" (NICE ID, chosen with confidence by top companies) and "이동통신사 개인정보취급방침 VerSign 128-bit SSL 암호화 적용" (Mobile Carrier Personal Information Handling Policy VerSign 128-bit SSL Encryption Applied).

On the right side, there is a "docu# 회원로그인" (docu# Member Login) section with links for "회원 로그인" (Member Login), "아이디 찾기" (Find ID), and "비밀번호 초기화" (Reset Password). Below this, there are two tabs: "개인회원 비밀번호 변경" (Change Personal Member Password) and "법인회원 비밀번호 변경" (Change Corporate Member Password). The "개인회원 비밀번호 변경" tab is active, showing a form for "휴대폰을 통한 인증" (Authentication via Mobile Phone) with fields for "아이디" (ID: youknowit2), "이름" (Name: 김기창), and "휴대폰" (Mobile Number: 010 - 4015 - 0209). A "확인" (Confirm) button is at the bottom.

비밀번호 reset 완료

The screenshot shows the 'docu# 회원로그인' (docu# Member Login) page. At the top, there are navigation links for '회원 로그인' (Member Login), '아이디 찾기' (Find ID), and '비밀번호 초기화' (Reset Password). Below these, there are instructions: '비밀번호는 본인 확인 절차를 거친 후 초기화 시켜 드립니다. 회원가입 시 등록한 정보를 아래 입력해 주세요.' (We will reset your password after a self-verification process. Please enter the information you registered during sign-up below.) and '대면평가를 통해서 등록하신 분께서는 고객센터(1670-3090)에 문의해 주세요.' (Members who registered through a face-to-face evaluation should contact the customer center (1670-3090) for inquiries.)

The main content area has two tabs: '개인회원 비밀번호 변경' (Change Personal Member Password) and '법인회원 비밀번호 변경' (Change Corporate Member Password). The '개인회원 비밀번호 변경' tab is active. On the left, there are options for '휴대폰을 통한' (Via Mobile Phone) and '14세 이상' (14 years and over). Below these are fields for '아이디' (ID), '이름' (Name), and '휴대폰' (Mobile Phone).

A modal window titled '비밀번호 변경' (Change Password) is open. It contains the following fields and buttons:

- 신규 비밀번호 등록 (New Password Registration)
- 아이디 : youknowit2
- 신규비밀번호 :
- 신규비밀번호 확인 :
- 확인 (Confirm) button
- 닫기 (Close) button

메일의 본인확인 기능 ?

- # 메일 계정의 보안 수준 = 휴대폰인증 수준
- ID 유출과 비밀번호 재설정은 매우 쉬움
- # 메일 발신자, 수신자의 “본인확인”은 계정 탈취 당하지 않았을 경우에만 가능
- “이론적”인 본인확인 기능일 뿐, 실제로는 피해자만 양산할 것.

‘공인’

정부가 ‘공인’하면 만사 OK ?
정부가 ‘공인’하면 안전해 지는가?
언제까지 정부에 기대서 장사하려는가?
억지로 사용하게 할 경우 생겨날 ‘민폐’는?
공인인증서, WIPI, 공인전자주소 ...

세계최초의 이메일 삽질, 그리고 IT “콘트롤 타워?” <http://openweb.or.kr/?p=6760>
“삽 메일” 유감... (지경부 임성민 서기관께) <http://openweb.or.kr/?p=7079>
삽메일... 결국 이런 식으로 <http://opennet.or.kr/4615>
[왜이러는걸까요] #메일 <http://www.bloter.net/archives/124750>
[e말뚝] 공인인증서·삽메일, 그분들의 인증 강박 <http://www.bloter.net/archives/163707>
“삽메일은 내가 메일 받은 걸 어떻게 알까요?” <http://www.bloter.net/archives/187823>


국제무대에서 승부합시다!

Lavabit's Dark Mail Initiative

by Ladar Levison

Home Updates **7** Backers **2,976** Comments **161** Dallas, TX Software

Funded! This project was successfully funded on Nov 28, 2013.



2,976
backers

\$212,513
pledged of \$196,608 goal

0
seconds to go

Project by
Ladar Levison
Dallas, TX

First created · 0 backed

Ladar Levison 1098 friends

lavabit.com

[See full bio](#) [Contact me](#)

Pledge \$25 or more
1857 backers

[Share](#) **57** [Tweet](#) [Embed](#)

The goal is to cleanup and release the source code that was used to power Lavabit as a f/oss project with support for dark mail added.

@ 메일에서도 충분히 구현가능

The Summer of Snowden may have taken the Lavabit email service offline, but the lifeblood of the service is still alive and relevant to Dark Mail. The goal is to perfect and release its source code as a free and open-source software (F/OSS) project. The "magma" daemon supports access via SMTP, POP3, IMAP4 and HTTP. Magma can be clustered and transparently encrypts user data before storing it on disk. It includes a Javascript webmail system that uses a JSON-based API to provide secure mail access via the web.

Along with preserving existing functionality, the team will build in support for the Dark Mail protocol. Dark Mail, a newly developed messaging protocol, is designed to provide end-to-end encryption of both the message itself and the email in transit. Because encryption will be integrated into the protocol itself, it will be invisible to the user. Dark Mail users will get the security of PGP without the cognitive burden; if someone can use email today they will be able to use Dark Mail tomorrow.