정부주도 샵메일 서비스의 문제점

김 기 창

사단법인 오픈넷

2014.6.3

위인설관 , 억지춘향 : “ 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

구 분		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 ?

샵메일의 기술적 얼개

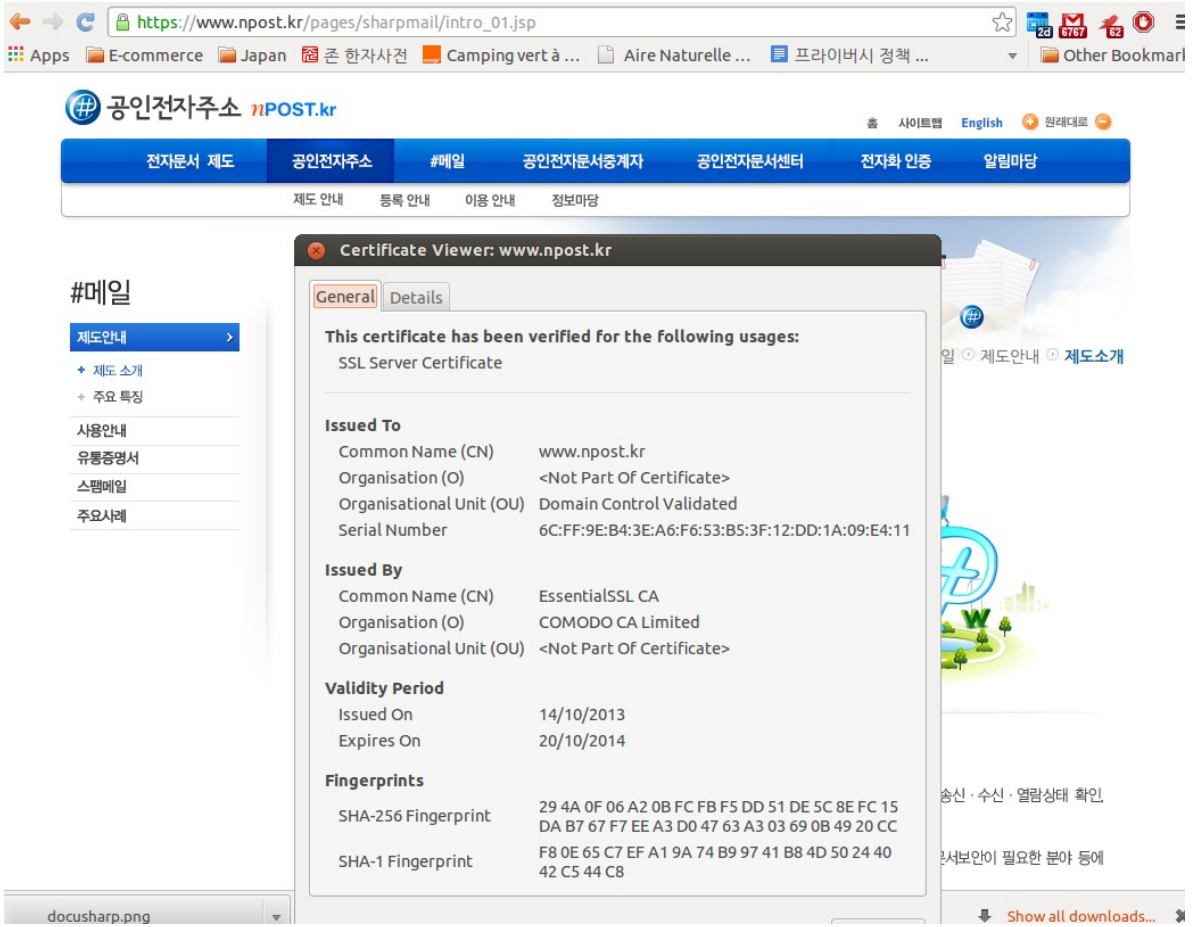
- ebXML (e-business XML)
- ebMS (e-business Message Service Specification)
- HTTP

- 별도 클라이언트 사용하거나 , ‘ 웹메일’ 형태의 UX 제공
- SMTP 사용하지 않을 이유 ?

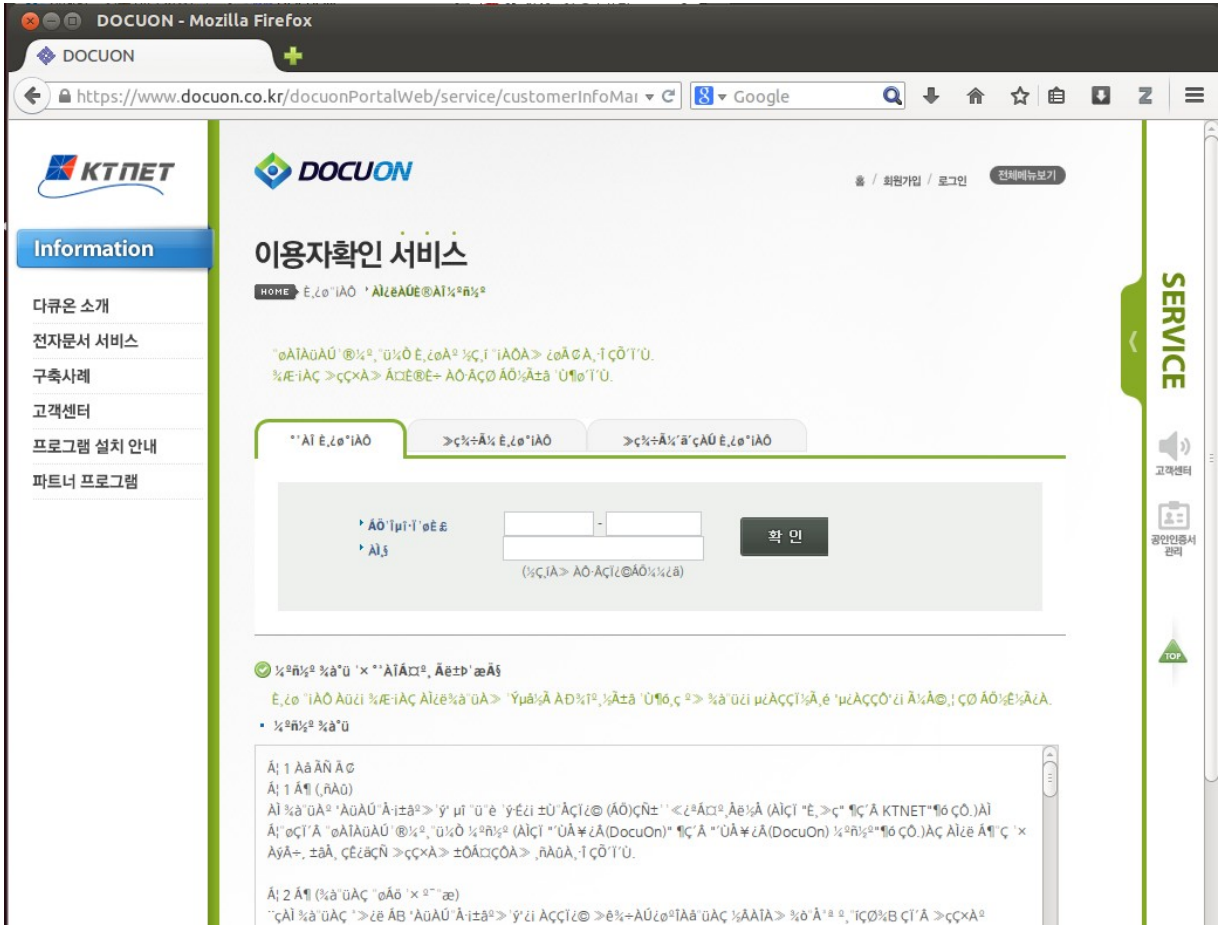
샵메일의 현실적 문제

본 연결은 신뢰할 수 없음
Firefox가 안전하게 www.docusharp.com로 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

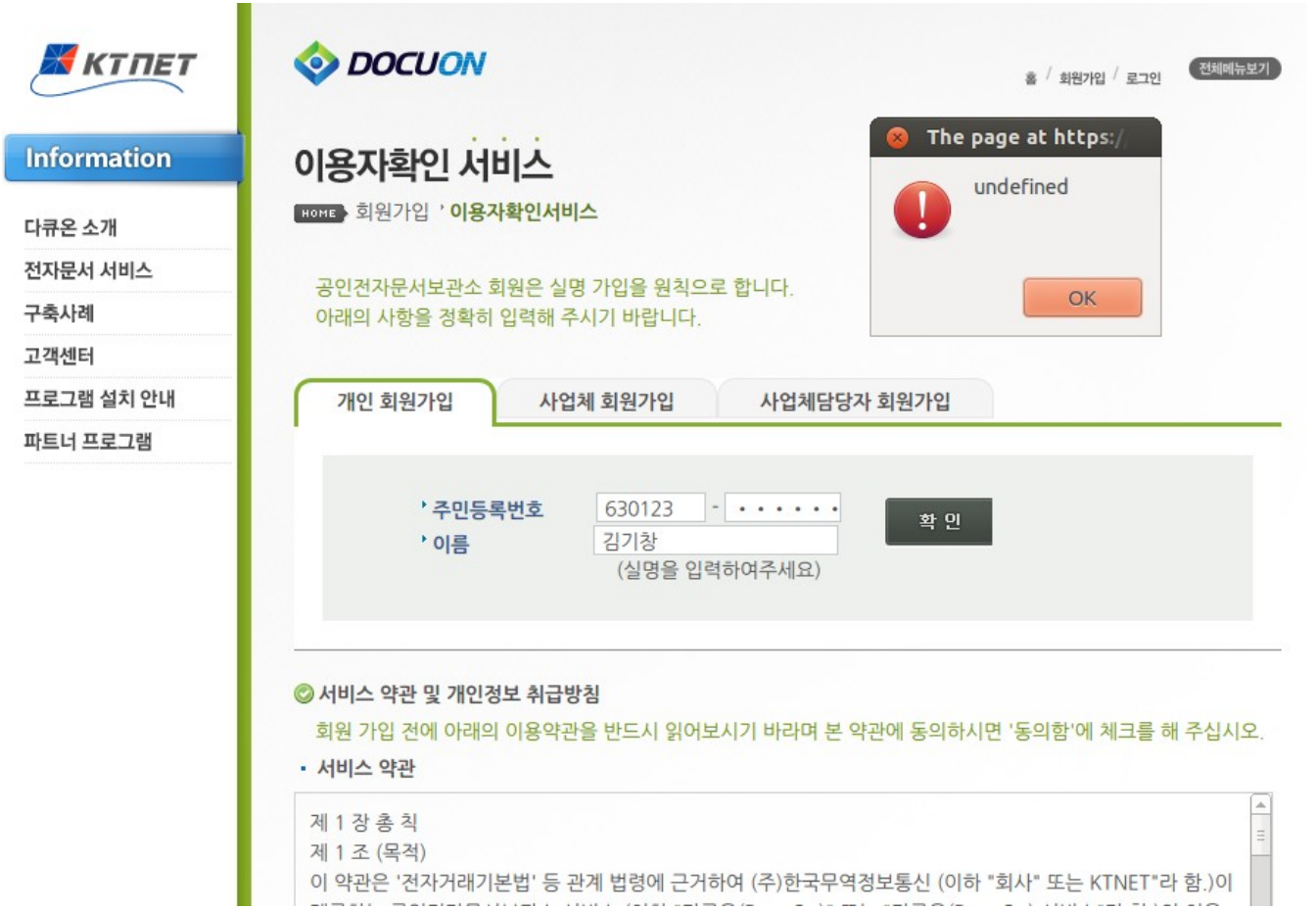
nPost 만 예외


https://www.npost.kr/pages/sharpmail/intro_01.jsp
Apps
E-commerce
Japan
존 한자사전
Camping vert à ...
Aire Naturelle ...
프라이버시 정책 ...
Other Bookmarks
공인전자주소 nPOST.kr
English
전자문서 제도
공인전자주소
#메일
공인전자문서중계자
공인전자문서센터
전자화 인증
알림마당
제도 안내
등록 안내
이용 안내
정보마당
#메일
제도안내
제도 소개
주요 특징
사용안내
유통증명서
스팸메일
주요사례
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
제도안내 제도소개
송신 · 수신 · 열람상태 확인
Show all downloads...
docusharp.png

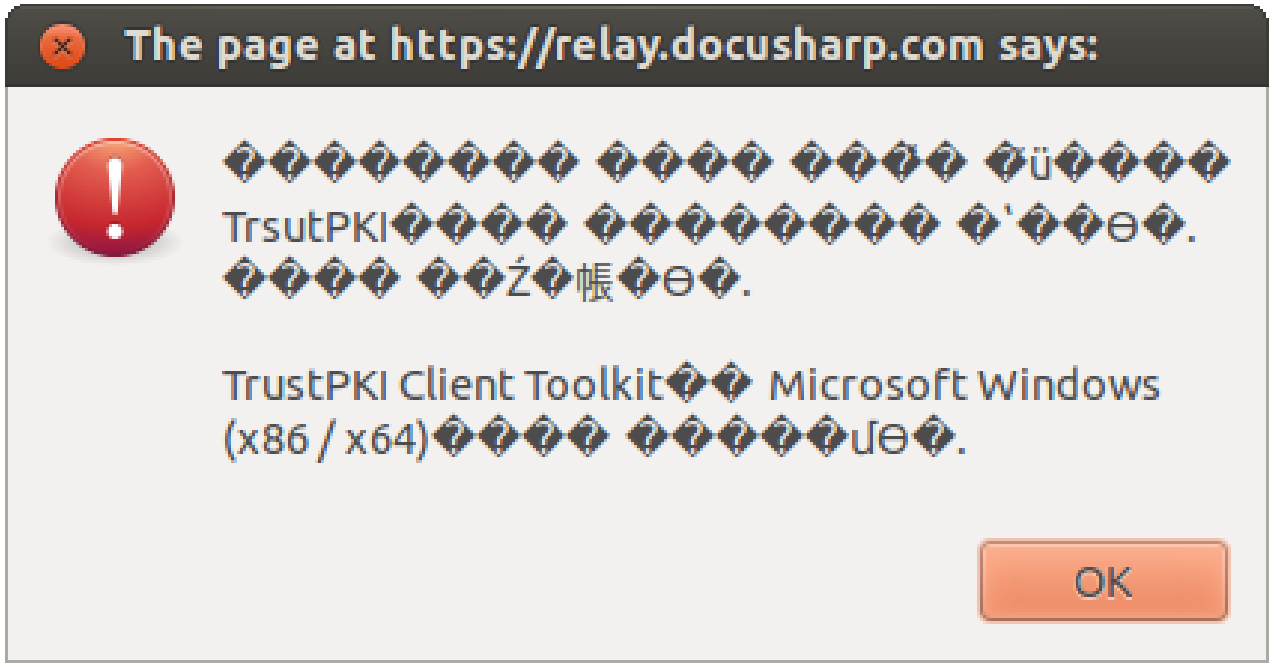
국내전용 서비스


DOCUON - Mozilla Firefox
DOCUON
https://www.docuon.co.kr/docuonPortalWeb/service/customerInfoMai
Google
KTNET
Information
다큐온 소개
전자문서 서비스
구축사례
고객센터
프로그램 설치 안내
파트너 프로그램
DOCUON
홈 / 회원가입 / 로그인
전체메뉴보기
이용자확인 서비스
HOME
확 인
SERVICE
고객센터
공인인증서 관리
TOP

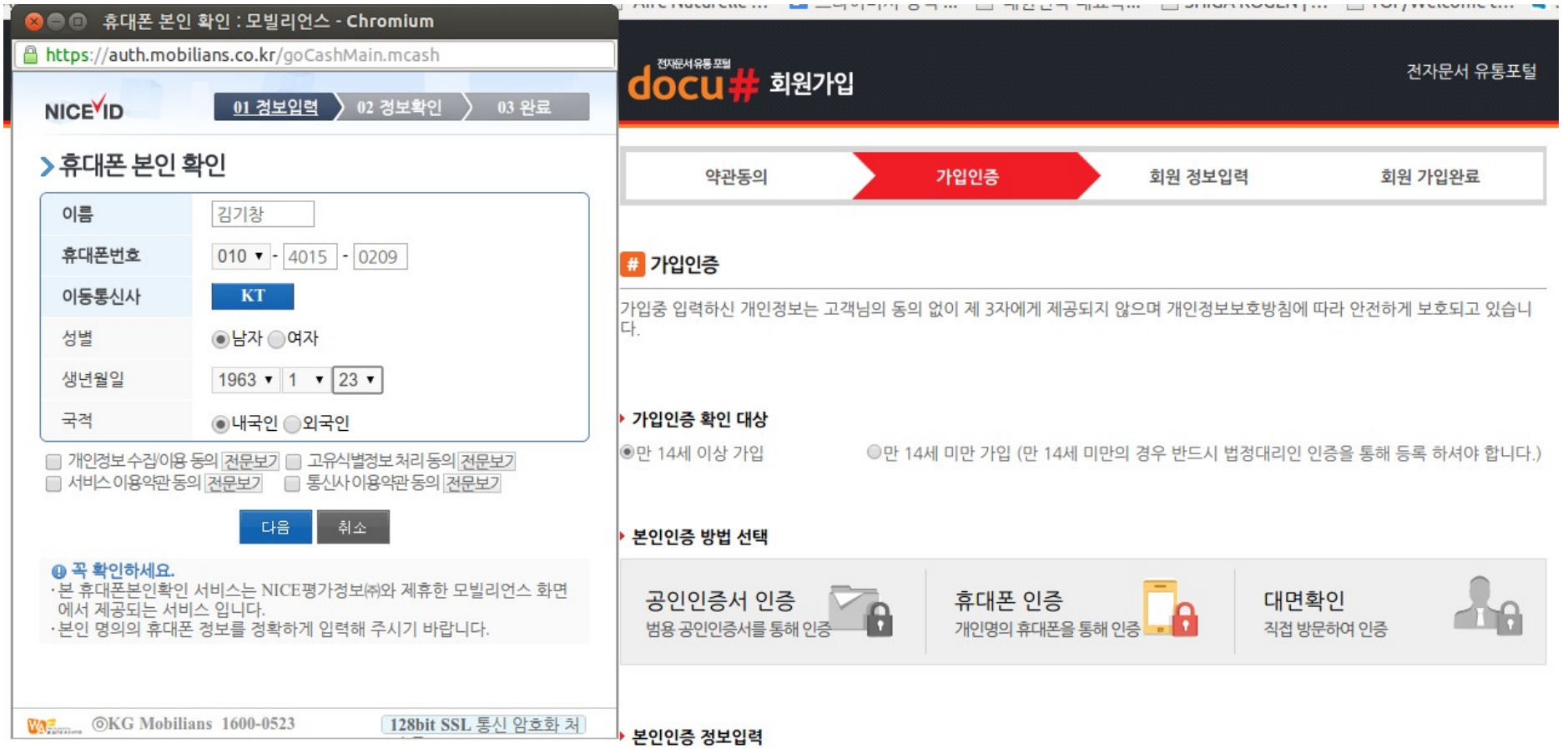
윈도우 Only 서비스


KTNET
Information
다큐온 소개
전자문서 서비스
구축사례
고객센터
프로그램 설치 안내
파트너 프로그램
DOCUON
홈 / 회원가입 / 로그인
전체메뉴보기
이용자확인 서비스
HOME 회원가입 ' 이용자확인서비스
공인전자문서보관소 회원은 실명 가입을 원칙으로 합니다.
아래의 사항을 정확히 입력해 주시기 바랍니다.
The page at https:/
undefined
OK
개인 회원가입
사업체 회원가입
사업체담당자 회원가입
주민등록번호
630123 - • • • • • •
이름
김기창
(실명을 입력하여주세요)
확 인
서비스 약관 및 개인정보 취급방침
회원 가입 전에 아래의 이용약관을 반드시 읽어보시기 바라며 본 약관에 동의하시면 '동의함'에 체크를 해 주십시오.
서비스 약관
제 1 장 총 칙
제 1 조 (목적)
이 약관은 '전자거래기본법' 등 관계 법령에 근거하여 (주)한국무역정보통신 (이하 "회사" 또는 KTNET"라 함.)이

플러그인 의존 서비스

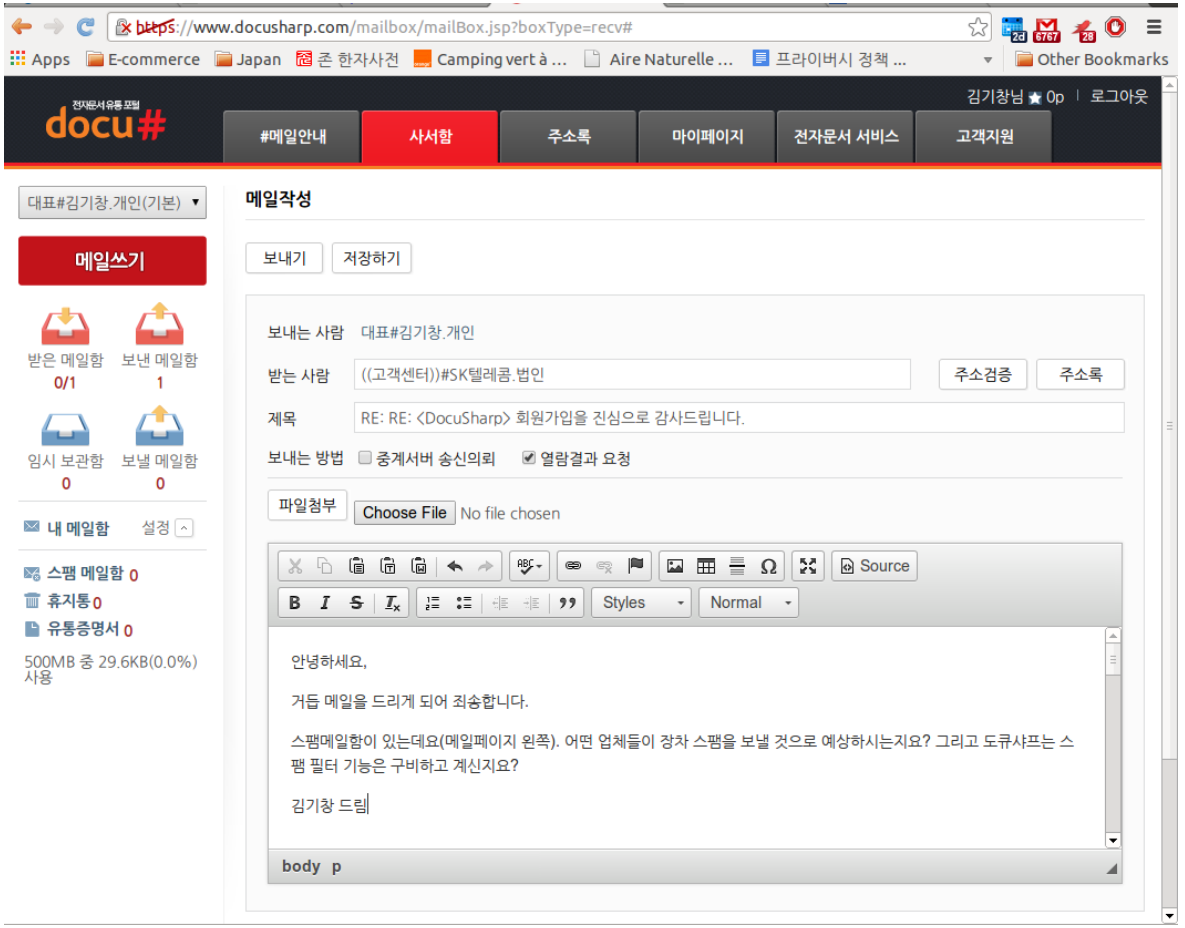

The page at https://relay.docusharp.com says:
TrsutPKI
TrustPKI Client Toolkit Microsoft Windows
(x86 / x64)
OK

발신자 , 수신자 본인확인 ?

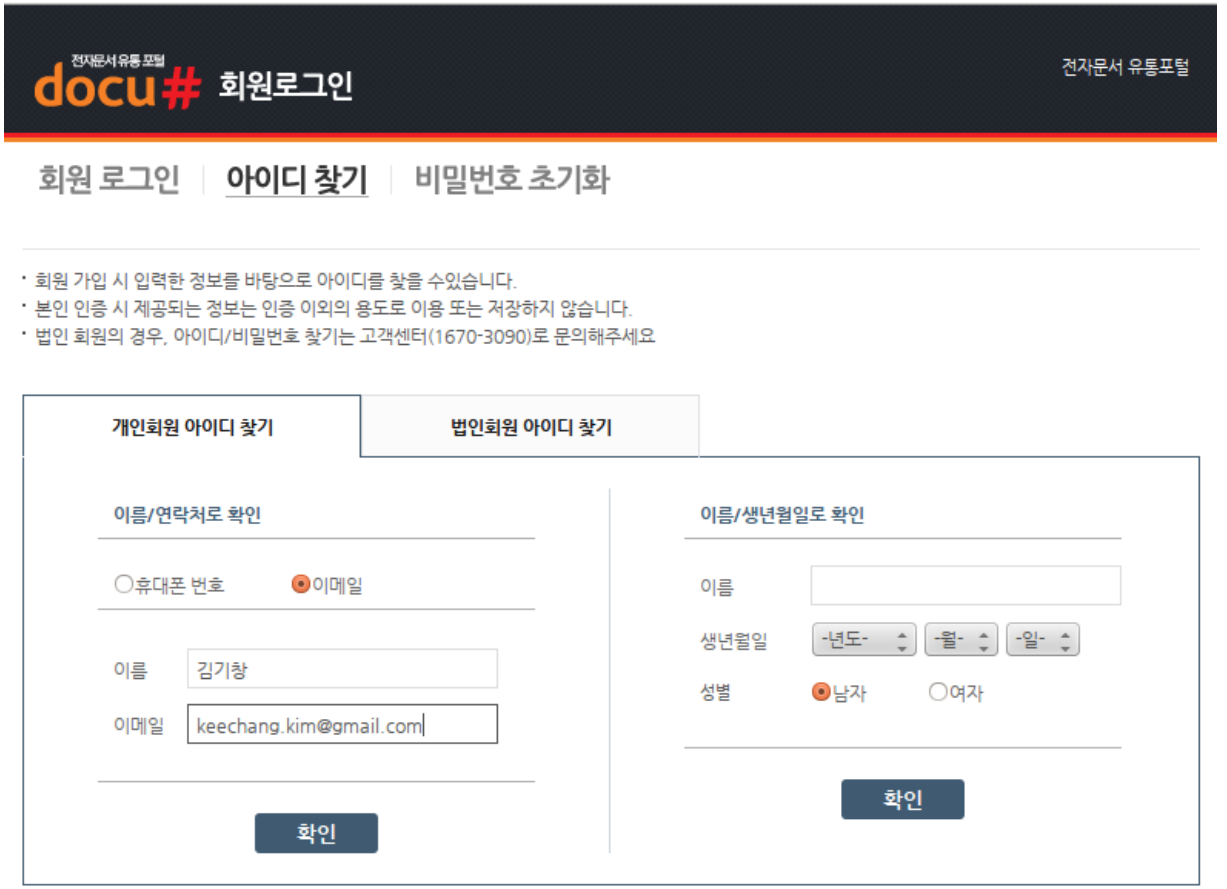


- 휴대폰 + 주민번호 이용한 본인 확인 ?
- 이메일 계정 발급시 본인 확인하면 안될까 ?

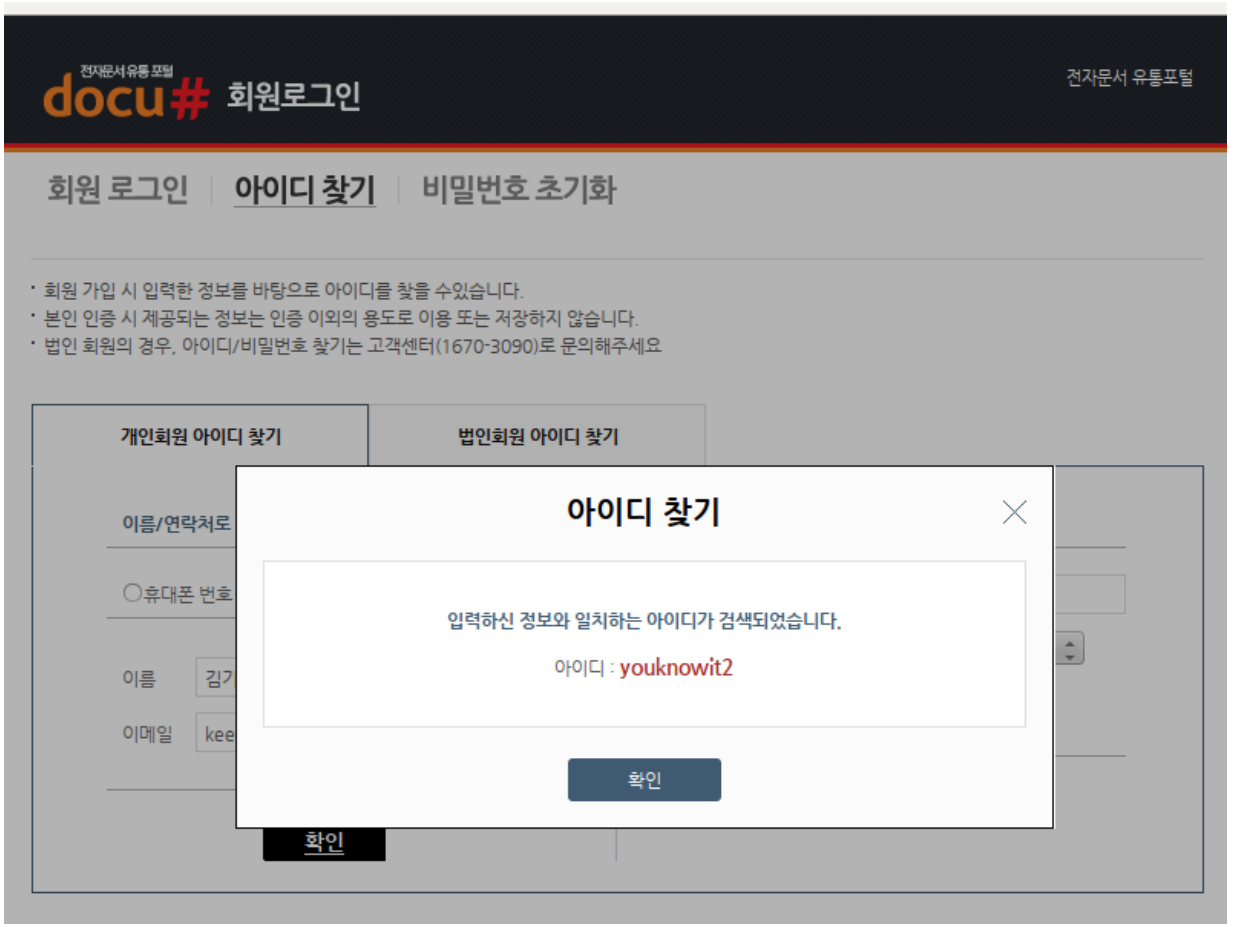
스팸 #메일


https://www.docusharp.com/mailbox/mailBox.jsp?boxType=recv#
Apps
E-commerce
Japan
존 한자사전
Camping vert à ...
Aire Naturelle ...
프라이버시 정책 ...
Other Bookmarks
docu#
김기창님 0p | 로그아웃
#메일안내
사서함
주소록
마이페이지
전자문서 서비스
고객지원
대표#김기창.개인(기본)
메일쓰기
받은 메일함 0/1
보낸 메일함 1
임시 보관함 0
보낼 메일함 0
내 메일함
설정
스팸 메일함 0
휴지통 0
유통증명서 0
500MB 중 29.6KB(0.0%) 사용
메일작성
보내기
저장하기
보내는 사람 대표#김기창.개인
받는 사람 ((고객센터))#SK텔레콤.법인
주소검증
주소록
제목 RE: RE: <DocuSharp> 회원가입을 진심으로 감사드립니다.
보내는 방법 중계서버 송신의뢰 열람결과 요청
파일첨부
Choose File No file chosen
Source
Styles
Normal
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
body p

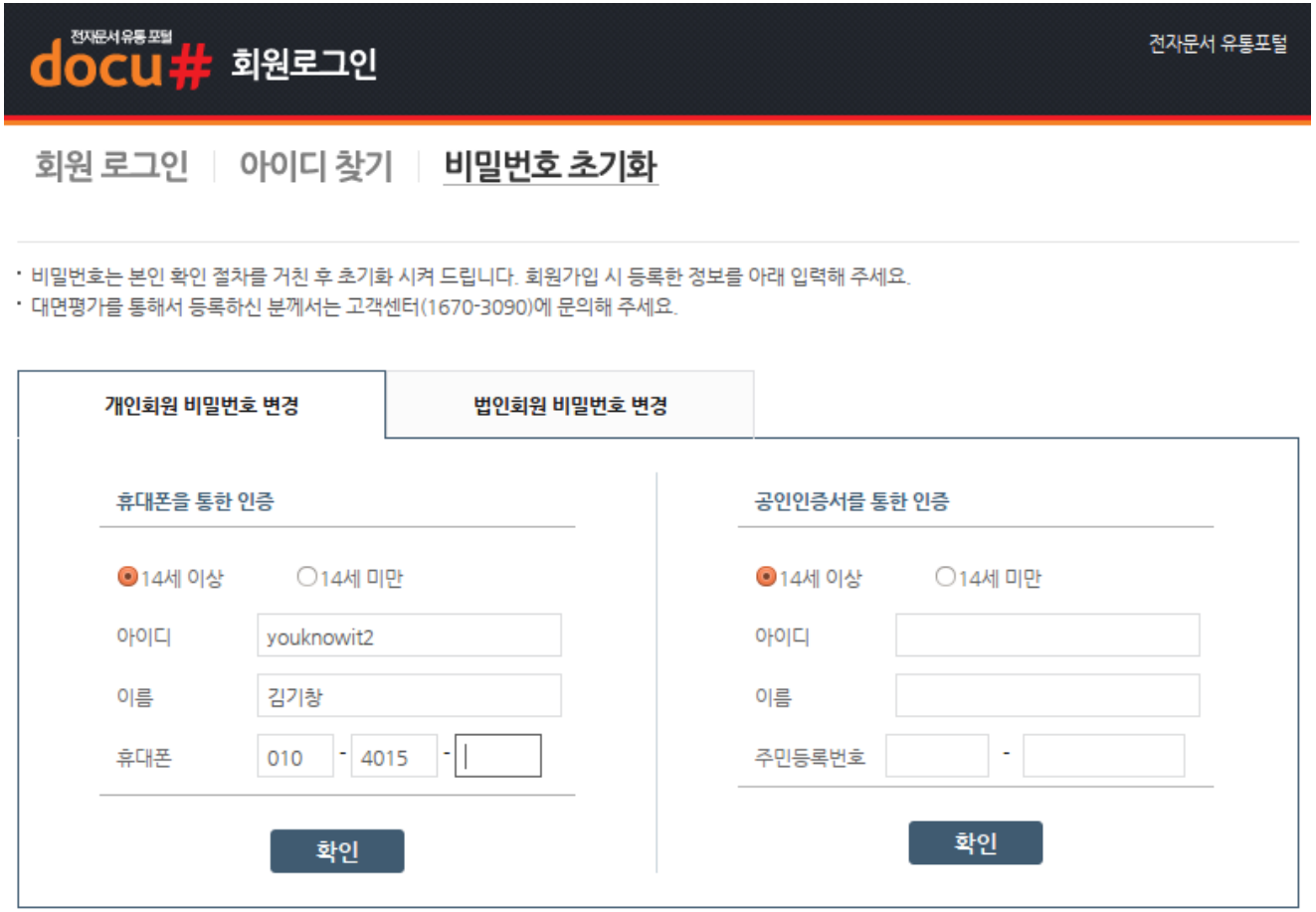
메일 '본인확인' 취약점


전자문서유통포털
docu# 회원로그인
전자문서 유통포털
회원 로그인
아이디 찾기
비밀번호 초기화
· 회원 가입 시 입력한 정보를 바탕으로 아이디를 찾을 수있습니다.
· 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
이름/연락처로 확인
휴대폰 번호
이메일
이름
김기창
이메일
keechang.kim@gmail.com
확인
이름/생년월일로 확인
이름
생년월일
-년도-
-월-
-일-
성별
남자
여자
확인

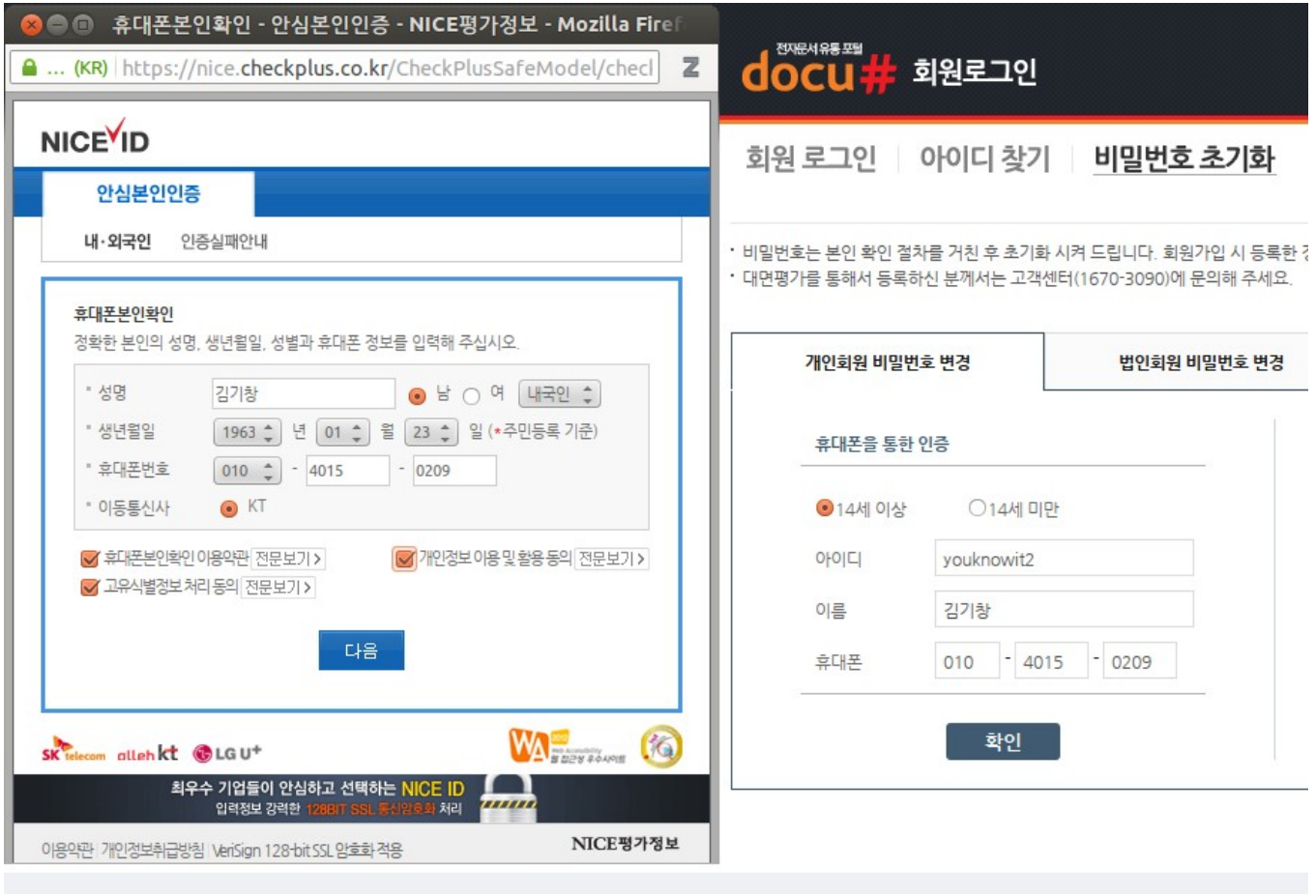
“# 메일 ID” 쉽게 노출


전자문서유통포털
docu# 회원로그인
전자문서 유통포털
회원 로그인 | 아이디 찾기 | 비밀번호 초기화
· 회원 가입 시 입력한 정보를 바탕으로 아이디를 찾을 수있습니다.
· 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
이름/연락처로
휴대폰 번호
이름
이메일
확인
아이디 찾기
입력하신 정보와 일치하는 아이디가 검색되었습니다.
아이디 : youknowit2
확인

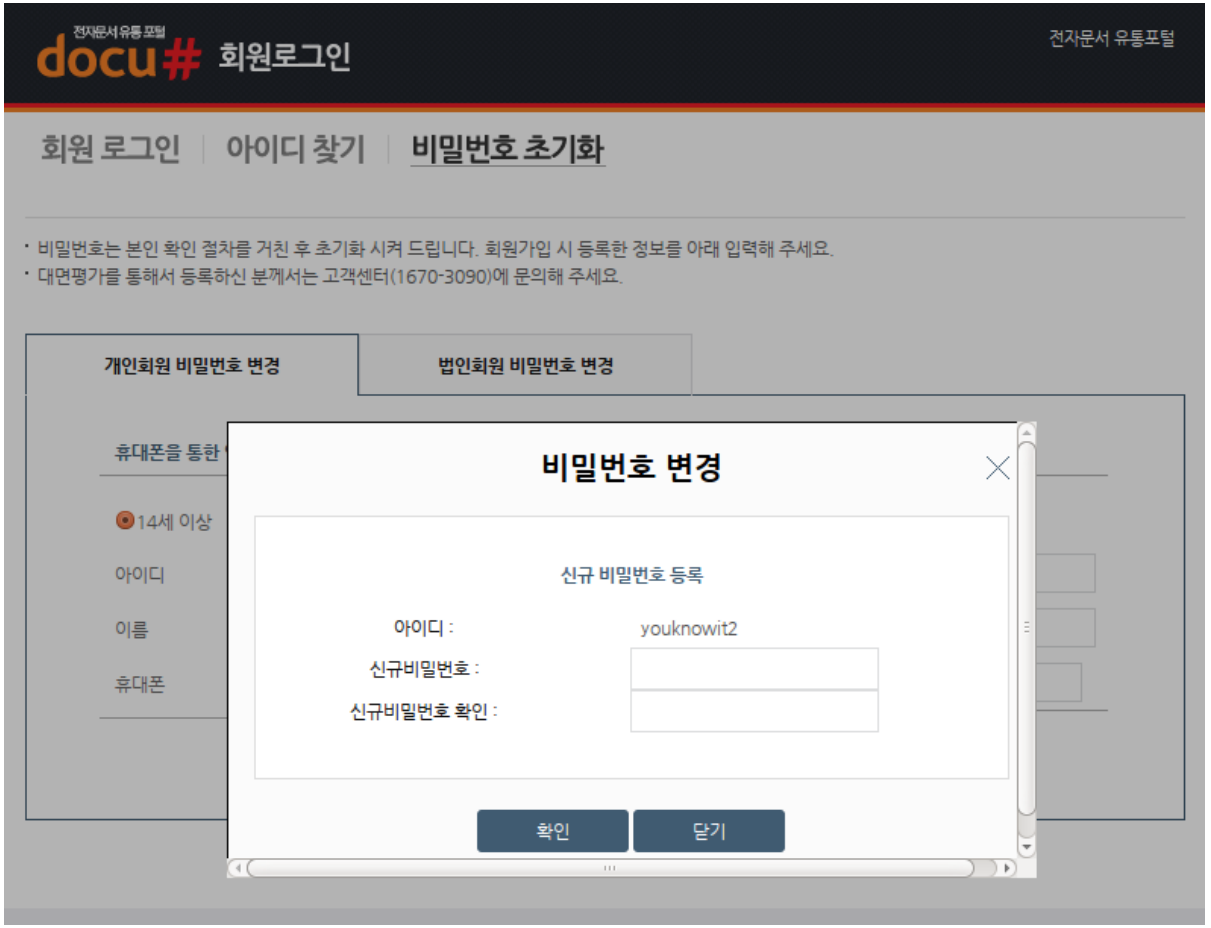
메일 비밀번호 reset



메일 비밀번호 = 휴대폰인증



비밀번호 reset 완료



메일의 본인확인 기능 ?

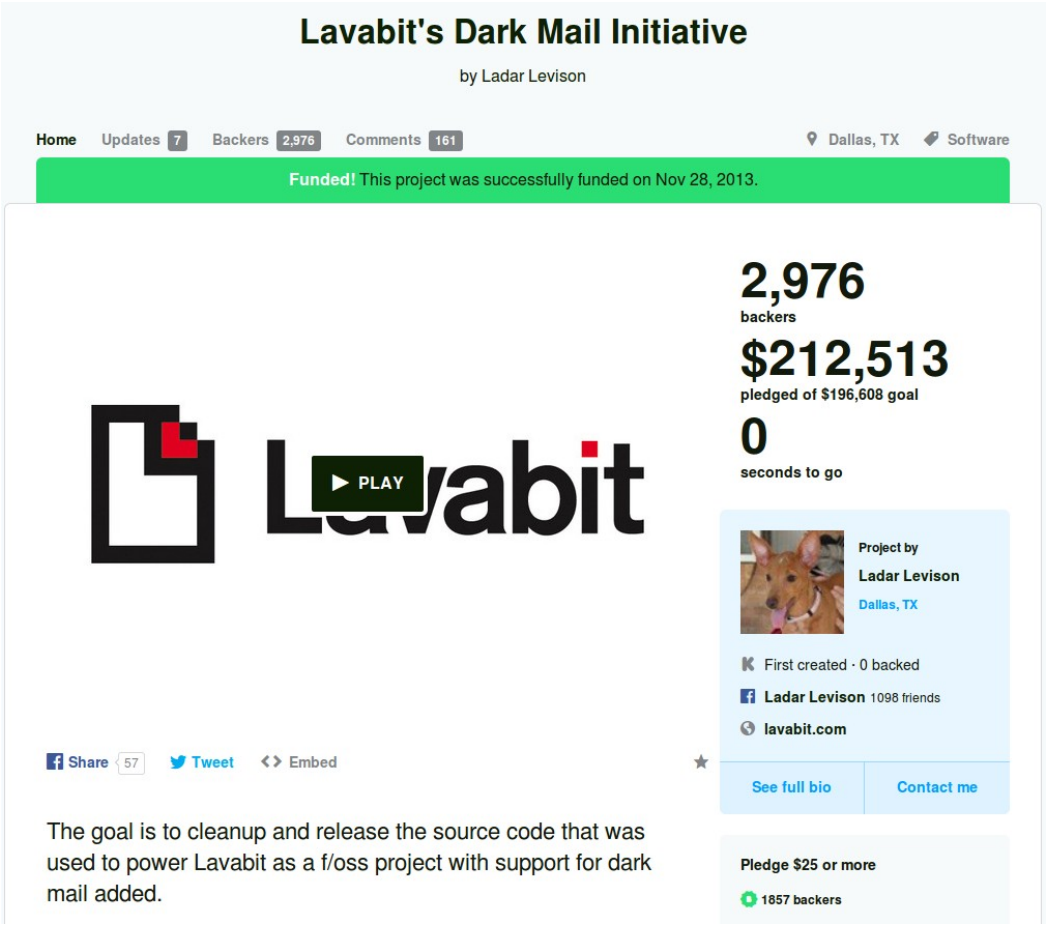
- # 메일 계정의 보안 수준 = 휴대폰인증 수준
- ID 유출과 비밀번호 재설정은 매우 쉬움
- # 메일 발신자 , 수신자의 “본인확인”은 계정 탈취 당하지 않았을 경우에만 가능
- “ 이론적”인 본인확인 기능일 뿐 , 실제로는 피해자만 양산할 것 .

‘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
“샵 메일” 유감… (지경부 임성민 서기관께) http://openweb.or.kr/?p=7079
샵메일… 결국 이런 식으로 http://opennet.or.kr/4615
[왜이러는걸까요] #메일 http://www.bloter.net/archives/124750
[e말뚝] 공인인증서·샵메일, 그분들의 인증 강박 http://www.bloter.net/archives/163707
“샵메일은 내가 메일 받은 걸 어떻게 알까요?” http://www.bloter.net/archives/187823

국제무대에서 승부합시다 !



@ 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.