안심본인인증
서비스
개발 가이드

Version 2.2JSP

2020년 08월 14일

NICE평가정보㈜ 디지털개발실

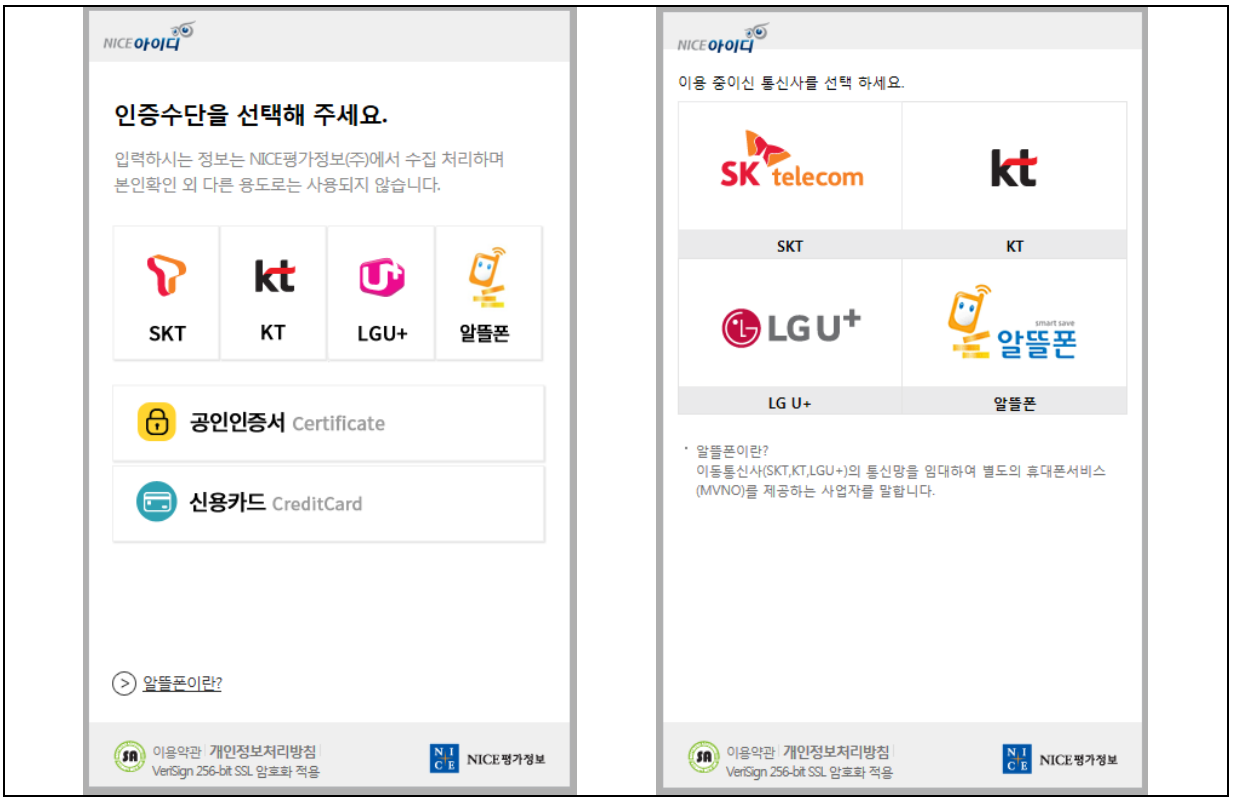
목차

1. 안심본인인증

1.1. 안심본인인증 서비스 개요

1.1.1. 안심본인인증 서비스는 개인의 등록된 정보를 기초로 휴대폰, 신용카드, 공인인증서를 이용하여 온라인상에서 본인을 확인하는 서비스 입니다. **(*신용카드인증은 신규계약 불가*)**

[그림1 – PC 서비스 페이지 예시]



[표1 – 본인인증 시 전달되는 주요정보]

인증결과	전달되는 정보
인증성공	CP요청번호, 인증수단, 처리결과 고유번호, 이름, 생년월일, 성별코드, 내/외국인코드, ***중복가입 확인값(DI), *연계정보 확인값(CI), *통신사정보, *휴대폰번호**
인증실패	CP요청번호, 인증수단, 에러코드

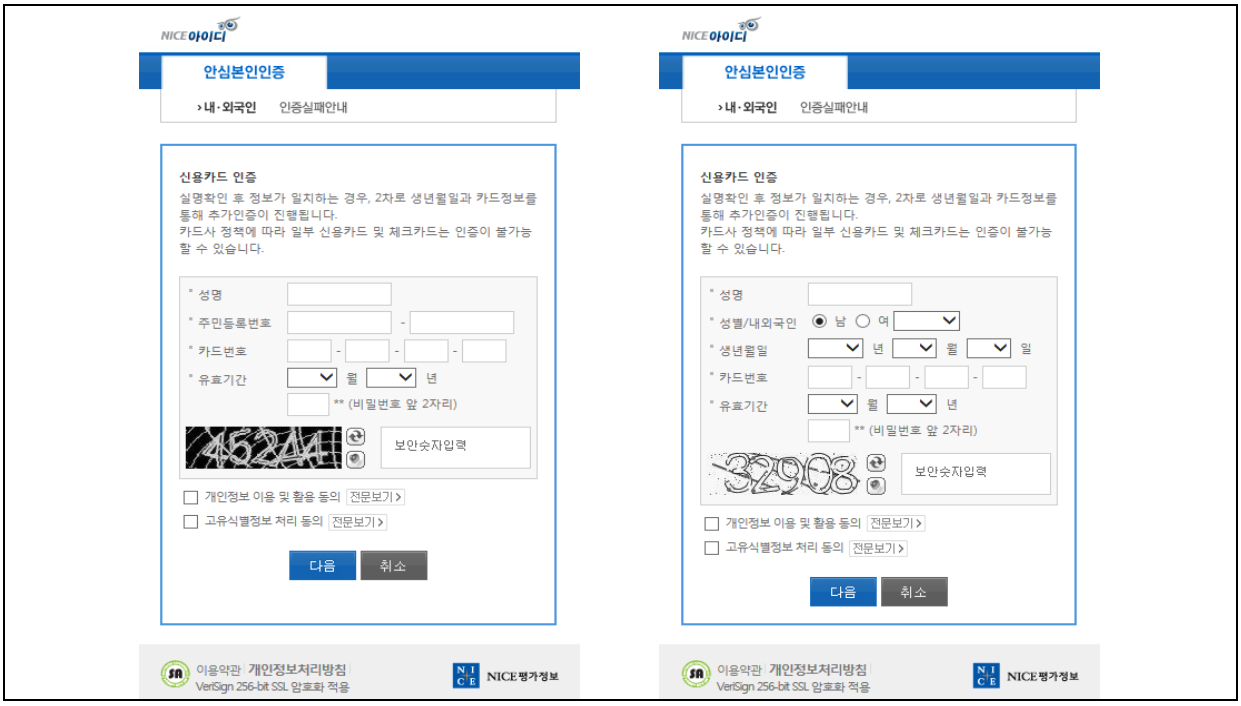
* 일부 항목은 인증결과와 인증방식에 따라 전달 여부가 결정됩니다. (3.결과추출 참조)

1.1.2. 신용카드 및 공인인증서 인증은 인증하는 방식에 따라서 DI, CI 제공이 가능합니다.

인증수단	주민번호 방식	생년월일 방식
카드	DI, CI 제공 가능	**DI, CI 제공 불가**
공인인증서	DI, CI 제공 가능	DI, CI 제공 가능

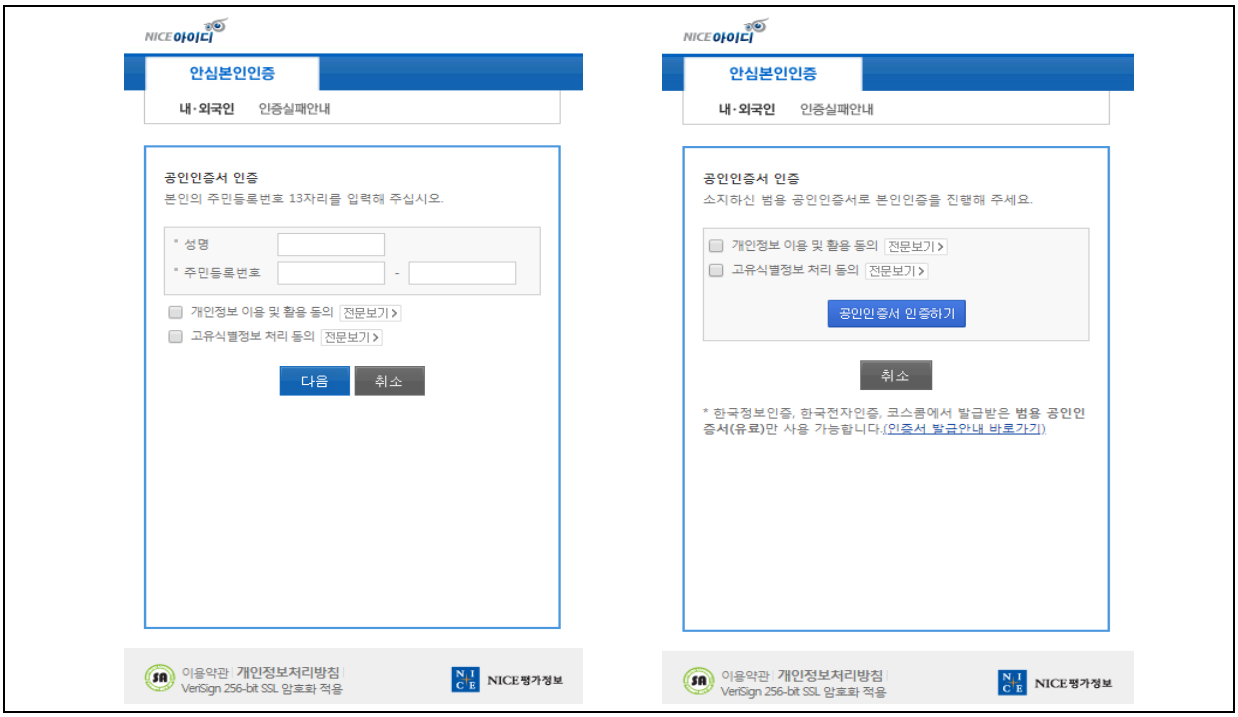
* 인증수단은 당사 계약 담당자를 통해 실시간으로 이용여부(사용/미사용) 변경 가능

[그림2 - 신용카드 인증예시]



1.1.3. 화면의 왼쪽은 주민번호를 활용한 신용카드인증이고, 화면의 오른쪽은 생년월일을 활용한 신용카드 인증입니다.

[그림3 – 공인인증서 인증 예시]



1.1.4. 공인인증서는 모바일에서 사용 불가능 합니다.

(왼쪽 – 주민번호방식 , 오른쪽 – 생년월일방식)

[그림4 – 모바일 휴대폰인증 예시]

1.1.5. 맨 왼쪽은 첫화면입니다. 가운데, 오른쪽 화면은 가운데 화면과 동일한 프로세스에 들어있는 화면입니다. (스크롤로 제어 가능)

[그림5 – 모바일 카드인증 예시]

1.1.6. 화면의 왼쪽은 주민번호를 활용한 주민번호방식이고, 화면의 오른쪽은 생년월일을 활용한 생년월일 방식입니다.

2. 개발연동 시 수정사항

2.1 서비스연동

2.1.1 파일구성

- 모듈 : NiceID.jar(Sun/Oracle) , NiceID_ibm.jar(IBM)
- 샘플페이지 : checkplus_main.jsp, checkplus_success.jsp, checkplus_fail.jsp
- 이 외 : 안심본인인증_응답코드.xlsx, 안심본인인증_사용자메뉴얼.doc

2.1.2 모듈설치

환경에 맞는 모듈을 1개만을 올려 적용해주시기 바랍니다.

2개의 모듈을 동시에 올릴 시 에러가 발생하실 수 있습니다.

- NiceID.jar : JDK 1.4.2이상
- NiceID_ibm.jar : JDK 1.4.2이상

* 모듈이 제대로 올라가지 않을 경우 (환경에 맞지 않는 모듈 사용 등)

- ClassNotFoundException, NoClassDefFoundError 등 오류 발생
- JDK가 지원하는 버전보다 낮은 경우 기술지원 담당자에게 문의 (02-2122-4873)

2.1.3 네트워크 및 방화벽 설정

: 사용자의 PC에서 방화벽을 사용 중인 경우 아래 IP가 등록되어야 합니다

- URL : nice.checkplus.co.kr
- IP : 121.131.196.215
- Port : 80 , 443

2.1.4 checkplus_main 수정사항

해당 값들은 checkplus_main의 필수 입력(수정)값입니다.

변수명	설정내용
sSiteCode	NICE평가정보로부터 부여받은 사이트코드 // ex) XC123
sSitePassword	NICE평가정보로부터 부여받은 사이트패스워드 // ex) 000000000000
sReturnUrl	성공시 이동될 full URL // success페이지 절대 URL
sErrorUrl	실패시 이동될 full URL // fail페이지 절대 URL

부모창의 주소와 자식창의 주소는 동일해야합니다.

(부모창 : http://www.~ , 자식창 : http://www.~)

- 부모창과 자식창의 주소가 다를경우 Cross Domain 오류 발생

<세션을 이용한 부정이용방지>

안심본인인증의 경우 악의적인 인증결과(암호화) 가로채기를 막기 위해 암호화데이터 내에 요청고유번호를 반영하고 있습니다. 안전한 고객관리를 위하여 반드시 반영해 주시기 바랍니다.

함수명	이용방식
session.setAttribute	해킹등의 방지를 위하여 세션을 이용

샘플페이지에 들어있는 값은 임의로 저희쪽에서 반영해드린 소스입니다. 업체에서 다른 값으로 지정 하셔도 변경하셔도 무방합니다.

입력한 정보를 암호화 하여 NICE평가정보로 넘겨줍니다. sEncData 는 회원사 정보를 암호화 하여 NICE평가정보 페이지 호출시 POST 방식으로 넘겨주셔야 하는 값입니다.

변수명	설정내용
sEncData	업체정보 (사이트코드 외 설정사항에 대한 정보)

<암호화 결과코드>

암호화 결과코드	내용	조치
없음	정상	-
-1	암호화 시스템 오류	시스템 환경 확인 및 최신 모듈 적용
-2	암호화 처리 오류	시스템 환경 확인 및 최신 모듈 적용
-3	암호화 데이터 오류	시스템 환경 확인 및 최신 모듈 적용
-9	입력 정보 오류	main 페이지의 입력값 확인 및 수정 (2.1.4 참조)

<안심본인인증 팝업 오류>

안심본인인증 팝업 오류 내용	조치
입력값 오류	main 페이지의 입력값 확인 후 문의 (2.1.4 참조)
잘못된 요청 오류	1) 인증팝업 호출 form의 URL이 정확한지 확인 2) 인증팝업 호출 form의 요청모드 정확한지 확인 (FAQ "잘못된 요청" 관련 참조)
파싱 오류	main 페이지에서 생성된 plaindata 가 정상인지 확인 (문의 시 plaindata, enc_data, sitecode를 메일로 발송)
IP 차단 안내	IP 차단해제 요청 (반복 시 약관/계약 담당에게 상담)
빈 화면 (ERR_EMPTY_RESPONSE)	1) 네트워크 및 방화벽 설정 확인 : **121.131.196.215 (Port: 80, 443)** 통신 가능해야 2) IP 차단 여부 문의

* 조치 후에도 오류가 지속될 경우 기술지원 담당자에게 문의 (02-2122-4873)

2.1.5 checkplus_success.jsp 수정사항

해당 값들은 checkplus_success의 필수 입력(수정)값입니다.

변수명	설정내용
sSiteCode	NICE평가정보로부터 부여받은 사이트코드 // ex) XC123
sSitePassword	NICE평가정보로부터 부여받은 사이트패스워드 // ex) 000000000000

<사용자 정보 확인 변수>

변수명	내용
EncodeData	NICE평가정보로부터 받은 암호화된 사용자 결과 데이터
PlainData	암호화된 결과 데이터의 복호화 (키의길이:키:값의길이:값)

결과코드	내용	조치
없음	정상	-
없음	세션값 불일치	1) main 페이지의 설정 및 세션 저장 처리 확인 2) success 페이지의 세션 상태 및 비교처리 확인 *** 조치 안 되는 경우 success 페이지의 데이터 위변조 검사 구문 주석처리 후 이용**
-1	복호화 시스템 오류	1) 시스템 환경 확인 및 최신 모듈 적용 2) 결과 데이터 확인 (아래 설명 참조)
-4	복호화 처리 오류	
-5	복호화 해시 오류	
-6	복호화 데이터 오류	1) 인증 시 세션 유지 여부 확인 2) 결과 데이터 확인 (아래 설명 참조)
-9	입력 정보 오류	각 페이지 입력값 확인 및 수정
-12	CP 비밀번호 불일치	결과페이지의 패스워드 설정값 확인 및 수정

* 조치 후에도 오류가 지속될 경우 기술지원 담당자에게 문의 (02-2122-4873)

<결과 데이터 확인 방법>

암호화된 결과데이터는 base64 인코딩을 거치게 되므로 아래와 같은 문자열이 포함됩니다. 복호화 처리에 실패하는 경우 결과데이터에서 아래 문자가 누락되거나 아래 문자열 이외의 문자가 포함되는 확인해주십시오.

- 알파벳 대문자: [A-Z]
- 알파벳 소문자: [a-z]
- 숫자: [0-9]
- 특수기호: [+ / =]

문자열에 문제가 있는 경우 귀사 시스템 상에서 변조되고 있는 것입니다. 웹 방화벽이나 웹서

버의 설정(필터링, 문자 치환 등)을 확인하시기 바랍니다. 결과 데이터를 GET 방식으로 전달하는 경우에도 인코딩이 변경될 수 있습니다. 디버그 코드나 로그를 이용해 변조 지점을 찾아주십시오.

문자열은 정상이지만 복호화 처리에 실패하는 경우 따로 확인이 필요합니다. 입력한 사이트코드, 사이트 패스워드, main에서 생성된 암호화 데이터, 리턴받은 결과데이터를 메일로 발송해주시기 바랍니다. *메일발송 시 당사 홈페이지 www.niceid.co.kr 의 전산 문의 담당자 이메일 참조

2.1.6 checkplus_fail.jsp 수정사항

변수명	설정내용
sSiteCode	NICE평가정보로부터 부여받은 사이트코드 // ex) XC123
sSitePassword	NICE평가정보로부터 부여받은 사이트패스워드 // ex) 000000000000

3. 결과 추출

인증이 정상적으로 완료된 경우 아래와 같이 결과를 추출할 수 있습니다. 값은 모두 String 형태로 전달되며 일부 값은 인증결과와 인증방식에 따라 전달여부가 결정됩니다.

인증결과	명칭	키값	비고
공통	CP요청번호	REQ_SEQ	최대 30 Byte (생성/임의값)
	인증수단	AUTH_TYPE	M: 휴대폰 C: 카드 X: 인증서 P: 삼성패스
인증성공	처리결과 고유번호	RES_SEQ	24 Byte
	이름	NAME	50 Byte, EUC-KR
	UTF-8 이름	UTF8_NAME	50 Byte, UTF-8, URLDecode 처리 필요
	생년월일	BIRTHDATE	YYYYMMDD
	성별 코드	GENDER	0: 여성, 1: 남성
	내/외국인 코드	NATIONAINFO	0: 내국인, 1: 외국인
	중복가입 확인값 (DI값)	DI	64 Byte, **카드-생년월일 인증 시 리턴X**
	연계정보 확인값 (CI값)	CI	88 Byte, **카드-생년월일 인증 시 리턴X**
	통신사정보	MOBILE_CO	3 Byte, **핸드폰 인증 전용**
	휴대폰번호	MOBILE_NO	24 Byte, **핸드폰 인증 전용**
인증실패	에러코드	ERR_CODE	4 Byte, 응답코드 문서 참조

* 일부 항목이 인증결과/방식 맞는데도 NULL로 들어오는 경우 당사 계약/관리담당자에게 문의 (해당 값이 리턴 되도록 신청 필요)

3.1 결과 추출 방식

3.1.1 결과페이지에 전달된 인증 결과데이터(EncodeData)를 복호화 하면 아래와 같이 구성된 복호화데이터 (plaindata)가 생성됩니다. 항목의 키값과 추출함수를 이용해 실제값을 추출합니다.

추출함수	복호화 데이터 구성
GetValue	[키값 길이] : [키값] [실제값 길이] : [실제값] ... 예) 9:**BIRTHDATE**8:**19890123**6:**GENDER**1:**1** ...

3.2 결과 항목 안내

3.2.1 CP요청번호 (REQ_SEQ)

추가적인 보안을 위한 변수입니다. main 페이지에서 설정 시 인증결과 데이터와 함께 전달됩니다. 세션에 저장된 값과 비교해 데이터 위/변조를 검사하거나, 사용자를 특정하는데 이용할 수 있습니다. (위/변조 검사는 필수사항이 아닌 보안 권고사항)

- 모듈 함수로 생성 가능
- 임의의 값 정의 가능 (최대 30 Byte, 공백문자 이용불가)

3.2.2 인증수단 (AUTH_TYPE)

인증 팝업창 화면에서 선택한 인증수단 정보입니다.

본인확인수단코드	본인확인수단
M	핸드폰
C	카드
X	공인인증서
P	삼성패스

* 삼성패스의 경우 사용설정이 되어있는 경우 지원하는 기기에서만 표시됩니다.
  (사용 설정 시 당사 계약 담당자에게 문의)

3.2.3 처리결과 고유번호 (RES_SEQ)

당사에서 인증수단, 사이트코드, 요청 시간에 기반해 부여하는 고유번호입니다.

- 형식: AA0000000000000000000000 (24 Byte)

3.2.4 이름 (NAME)

인증한 사용자의 실명입니다. 값이 깨지는 경우 EUC-KR로 변환하거나 UTF-8 이름을 이용해주시기 바랍니다.

3.2.5 UTF-8 이름 (UTF8_NAME)

UTF-8 형식의 인증 사용자 실명입니다. URL인코딩된 값이므로 URL디코딩 후 이용해주십시오.

3.2.6 성별 코드 (GENDER)
인증한 사용자의 성별 코드입니다.

성별코드	성별
0	여성
1	남성

3.2.7 생년월일 (BIRTHDATE)
인증한 사용자의 생년월일입니다.

- 형식: YYYYMMDD (예: 19990123)

3.2.8 내/외국인 코드 (NATIONAINFO)
인증한 사용자의 국적 정보입니다. 내/외국인 여부만 판별 가능합니다.

내/외국인 코드	국적
0	내국인
1	외국인

3.2.9 중복가입 확인정보 (DI: Duplicate Info) *카드-생년월일 인증 시 리턴 불가
사용자의 주민번호와 CP코드(계약된 서비스의 12자리 키 값)를 암호화한 개인 식별값입니다.

- 주민번호 + CP코드 ➔ 해쉬 ➔ DI값 (64 Byte)

여러 인증서비스를 이용하는 경우에도 **CP코드를 동일하게 맞춰주면 DI가 같아집니다**. 아이핀이나 타사 인증 모듈도 DI는 동일한 방식으로 생성되므로, CP코드를 맞춰 DI를 맞추실 수 있습니다.
DI가 같아지면 동일인임을 인식할 수 있으므로 중복가입 방지가 가능합니다.
* CP코드의 확인 및 설정이 필요한 경우 계약/약관 담당자에게 요청해주십시오.

3.2.10 연계정보 (CI: Connecting Information) *카드-생년월일 인증 시 리턴 불가
이용자의 주민번호를 암호화한 개인 식별값입니다.

- 주민번호 ➔ CI값 (88 Byte)

사이트 간 서비스 연계를 위한 값이며, 주민번호 기반이므로 서비스에 관계없이 값이 일정합니다.

아이핀이나 타사 인증 모듈에서도 동일한 값으로 생성됩니다. (**CI 리턴 신청 시 이용 가능)**

3.2.11 통신사정보 (MOBILE_CO) *핸드폰 인증 전용
인증 시 이용한 팝업창 화면에서 선택한 인증수단 정보입니다.

통신사코드	통신사정보
SKT	SKT
KTF	KT
LGT	LGU+
SKM	SKT 알뜰폰
KTM	KT 알뜰폰
LGM	LGU+ 알뜰폰

3.2.12 핸드폰번호 (MOBILE_NO) *핸드폰 인증 전용
인증한 사용자의 핸드폰번호입니다.

- 형식: 00000000000 (최대 24 Byte)

3.2.13 에러코드 (ERR_CODE)
인증에 실패한 경우 실패 사유에 따라 에러코드가 리턴됩니다. 자세한 사유는 응답코드 문서를 참조해주시기 바랍니다.
* 응답코드 문서에 정의되지 않은 에러코드의 경우 기술지원 담당자에게 문의 (02-2122-4873)

4. 자주 묻는 FAQ

Q. 팝업창에 하얀화면이 나오는경우

1)인증전 하얀화면
- 암호화데이터가 생성이 되었는지 확인 (환경에 맞는 모듈 – Build path 참고)
- JDK 버전 확인 (2.1.2 참고)

2)인증후 하얀화면
- sReturnUrl , sErrorUrl 설정 확인

(부모창과 자식창의 프로토콜 포함한 도메인이 정확히 일치해야합니다. - 절대주소)
(부모창: www.~~~.co.kr 자식창: www.~~~.co.kr)

Q. 특정값들이 나오지않는 경우 (CI, 휴대폰번호 등)

기본적으로 당사에서 제공되는 리턴값은 이름, 생년월일, 성별, 내외국인, DI값이 제공되고 있습니다. 그 외에 값들이 나오지 않는 경우 당사 관리담당자(계약)에게 문의해주시기 바랍니다.

Q. 법인폰 인증

법인폰에 경우 개인에 대한 정보등록이 되어야 인증이 가능합니다.
정보등록에 대해서는 각 통신사에 문의바랍니다.

Q. " 해당 인증서는 본 사이트에서 사용이 불가능합니다. " 공인인증서 오류

공인인증서에 대한 인증은 개인/사업자로 나뉘고 또 그에 따라 사용할 수 있는 인증서 기관도 다릅니다. (한국정보인증 , 한국전자인증 , 코스콤 외 은행권)
업체에서 진행한 계약에 따라 사용 가능한 인증서가 다르오니 계약형태에 맞는 인증서를 사용해 주시기 바랍니다.

Q. SMS인증문자가 안오는 경우

인증문자가 안오는 경우에는 2가지 경우가 있습니다.
- 사용자 인증정보가 틀렸을 경우
- 고객번호에 스팸번호(1600-1522)가 들어가 있는경우

위 와 같은 경우에는 SMS인증문자가 오지 않으므로 고객센터(1600-1522)에 문의 해주시거나 담당자에게 문의바랍니다.

Q. "세션값이 다릅니다" 오류

서버 및 프레임워크 설정에 따라 프로토콜이 자동적으로 변경되거나 URL 리다이렉션이 일어나는 경우가 있습니다. 이 경우 세션값이 바뀌어 결과 데이터를 받지 못하게 됩니다. 세션 정보를 확인하시고 관련 설정을 수정해주시기 바랍니다.

Q. 웹뷰 구현 시 intent주소의 URL Schema 오류 발생

웹뷰 구현 시 Pass앱 or 스토어로 이동될 수 있는 URL에 대하여 분기처리가 구현되어 있지 않으면 나는 오류입니다.

당사에서 모듈파일과 같이 전달드린 파일을 참고하여 해당 분기처리에 대해 진행해주시기 바랍니다.
해당 파일이 없으시다면 당사 담당자에게 문의바랍니다.

Q. 팝업창 iframe 혹은 layer popup으로 구현 시 오류 발생

안심본인인증은 독립적인 도메인으로 구현되어 있으므로 iframe으로 구현 시 도메인에 대한 제어를 잃어버릴 수 있습니다.

예를 들어, 브라우저 보안정책에 위배되어 부모창과의 값 전달에 실패하거나 보안모듈 (키보드, 보안문자 등)이 오동작할 수 있으며. iOS 13 이상에서는 safari 쿠키처리 정책이 변경되어 오류가 발생합니다. 반드시 독립적인 popup창으로 구현해주시기 바랍니다.

Q. “잘못된 요청이거나 서비스처리중 오류가 발생했습니다.” 팝업 오류

form으로 넘기는 데이터 중 필수데이타가 빠졌거나 값이 변형되어 넘어올 때 나는 오류입니다. 하기 내용의 데이터가 빠졌는지, 페이지를 여는 URL 확인바랍니다.

- <input type="hidden" name="m" value="checkplusService">
- <input type="hidden" name="EncodeData" value="<%= sEncData %>">
- URL : https://nice.checkplus.co.kr/CheckPlusSafeModel/checkplus.cb

Q. GET/POST 방식

기본적으로 success/fail 페이지로 enc_data는 POST 방식으로 전달이 됩니다.

크롬 80이상인경우 https://www.niceid.co.kr/front/contactus/popNoticeChrome.jsp 에 안내되어 있는 것과 같이 크롬의 쿠키정책에 따른 GET 방식으로 전달하고 있습니다.

다만, 윈도우 업데이트에 따라 Internet Explorer에서 samesite=lax으로 설정 될 경우 세션이 유실할 가능성이 있습니다.

이러한 경우 샘플에서 제공된 checkplus_main 페이지의 “form_chk”에 아래와 같이 recvMethodType input box를 추가하여 GET 방식으로 전달이 가능합니다.

<input type ="hidden" name="recvMethodType" value ="get"> //값은 get, post 선택

(단, param1,2,3 파라미터 값이 있는 경우 post로 변경 됩니다.)

Q. 이 외 오류

본인인증 오류화면	내용
[오류안내] 죄송합니다. 요청된 암호화정보에 오류가 있습니다. 입력된 정보를 확인해 주시기 바랍니다.	NICE에서 발급받은 사이트 코드와 사이트 패스워드의 오류입니다. 사이트 코드는 대문자와 소문자를 구분합니다.