『kt is 통합계정권한관리시스템 구축』

과업내역서

2017.10

kt is

[목 차]

I. 개요

1. 추진목표

- 관련법 준수를 위한 내·외부계정의 DB 분리 및 접근 제어로 컴플라이언스 이슈를 제거한다.
- 접근 사유 없는 사용자의 시스템 접근을 원천 차단함으로 개인/기업정보 유출을 사전에 예방한다.
- 분산되어 있는 권한 부여/회수절차를 일원화하고 접근 권한/인증 부여절차를 통합하여 사용자 및 담당자에 업무 편의성을 제공한다.

2. 추진방침

- 연계 시스템에 대한 계정 및 권한관리 시스템과 협력사 관리 시스템을 통합 구축한다.
- 現 운영중인 SSO 서비스의 호환성 유지를 위해 동일 업체의 접근제어솔루션을 적용한다.
- 기존의 업무시스템과 연계하여 구현되어야 하며, 추후 연계시스템 추가 및 변경에 대해 유연하게 설계되어야 한다.
- 사용자 이용 편의성과 적응성이 우수한 시스템을 구축을 위해 웹 표준, 웹 접근성 및 표준 지침을 준수한다.
- 시스템이 처리하는 정보는 내, 외부의 위협으로부터 안전하게 보호되어야 한다.

3. 용역일반

- 사업명 : kt is 통합계정권한관리시스템(IAM) 구축
- 발주부서: 경영기획총괄 IT 개발팀
- 수행부서 : 경영기획총괄 IT 개발팀
- 계약방법 : 공개입찰
- 사업기간 : 2017 년 11 월 01 일 ~ 2017 년 12 월 31 일(이후 4 주 안정화)
  개발수행사와의 계약 및 일정조율에 따른 사업기간 변동 예상
- 사업범위
  1) 공통사항
  2) 통합계정권한관리시스템 구축
  3) SSO 접근제어 솔루션 적용

- 운영환경(kt ucloud 서비스 이용)
  - OS: Cent OS 6.x 이상
  - WEB/WAS: Apache Http Server 2.2.x / WildFly 9.x 이상
  - DB: Mysql, PAS

- 개발언어
  - JSP, JAVA (JDK 1.7x 이상, Spring Framework 4.x 이상)

- 기타 상용
  - NETS * Single Sign On v5.0 ACL Add On Pack (SSO 접근제어솔루션)

II. 과업 내역

1. 공통사항

- ❍ 유지보수, 운용, 사용의 효율성과 용이성에 기반한 시스템 개발
- ❍ 사용자 중심의 기능구현 및 요구사항 반영
- ❍ 다양한 환경에서의 운용성 제공(OS, MultiBrowse 지원)
- ❍ 보안규정 및 Application 보안성 기준 준수

구분	내역
Jenkins	❍ **지원기능** ■ 자동화 배포 관리 및 분산빌드 환경 구축 ■ 지속적인 자동화 빌드 및 테스트 버전관리 ■ 웹 인터페이스를 통한 간편한 설정 ■ 코드 품질 감시
모의해킹 및 웹 취약점 점검	❍ **단순정보노출** ■ 불필요 파일 노출 취약점 ■ 부적절한 로그인 실패, 메시지 노출 취약점 ■ 주석처리 중요정보 노출 취약점 ■ 에러메세지 및 Default Page 노출 취약점 ❍ **중요정보노출** ■ 중요정보 평문 전송 취약점 ■ 파일 다운로드 취약점 ■ 디렉토리 리스팅 취약점 ■ 소스코드 노출 취약점 ❍ **취약한 인증 및 권한** ■ 추측 가능한 계정/패스워드 취약점 ■ Brute-Force 허용 취약점 ■ 쿠키 인증 취약점 ■ 세션관리 취약점 ■ 인증우회 취약점 ■ Cross-Site-Script 취약점 ■ 크로스 사이트 요청 변조(CSRF) 취약점 ■ 관리 페이지 접근 제어 취약점 ❍ **원격 명령 실행**

	■ Command Injection 취약점 ■ SQL Injection 취약점 ■ Remote File Inclusion 취약점 ■ 파일 업로드 취약점

2. 통합계정권한관리시스템 구축

구분	내역
계정관리	❍ 내, 외부 사용자 데이터 분리 ■ 외부사용자: 협력사직원 정보 및 계정 등록, 관리 기능 ■ 내부 사용자: E-HR 의 인사정보 및 기타 시스템과의 동기화를 통한 계정 동기화 지원 ❍ 대상업무시스템의 권한정보를 통합관리 할 수 있는 기능 제공 ■ 목록 조회, 일관된 정책 설정, SMS 발송 등 ❍ 부서와 사용자의 속성정보를 바탕으로 복수의 규칙에 만족하는 사용자를 추출하여 그룹핑하고 계정 부여/회수 기능 제공 ❍ 결재 워크플로우(요청/결재/승인)를 통한 계정 생성 ❍ 접근 권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무/부서 변경)의 적정성 여부 정기 점검 자동화 등
사용자기능 (Self Service)	❍ 웹 UI 로 사용자 스스로 자신의 계정을 관리(조회/신청/변경/삭제)할 수 있는 기능 제공
감사 및 통계 기록	❍ 계정관리 작업에 대한 이벤트 저장 ❍ 감사기록 이벤트를 바탕으로 계정관리업무 내역에 대한 통계 제공 ❍ 자원 별, 사용자, 조직 통계 등 제공
시스템 간 동기화	❍ 대상업무시스템 별 동기화 정책 제공 ❍ 조직도, 사용자, 직무, 입퇴사, 휴직 등 통합계정권한관리에 영향을 미치는 정보의 동기화 기능 제공 ❍ 동기화 이력관리, 성공/오류 정보 상세 확인과 추적, 오류동기화의 재동기화 등을 관리할 수 있는 UI 제공
보안관련 기능구현	❍ 중요 정보 전송 시 암호화 전송 구현 ❍ 패스워드오류에 대한 정책 설정(N 회 이상 로그인 실패 등) ❍ 로그인 제한 후 해제 기능 구현

3. SSO 접근 제어 솔루션 적용

구분	내역
접근제어	❍ 사용자 업무권한에 따른 접근 제어 구현 ❍ 현재 kt is 업무지원시스템에 적용 된 통합인증(SSO) 솔루션과 연계 보장

4. 기타사항

가. SW 구성 및 품질관리

ktis_IT SW표준 프로세스 v1.0.pdf

"ktis_IT SW 표준 프로세스" 지침을 준용한다.

나. UI/UX 개발관리

ktis UXUI표준 가이드

"ktis UXUI 표준가이드" 지침을 준용한다.

III. 계약 일반 사항

1. 프로젝트 관리 요구사항

가. 수행방법론

1) 프로젝트 관리 절차 및 방법을 반영하여 프로젝트 수행에 적합하다고 판단되는 수행방법론을 제시하고 "회사"와 최종 협의 후 반영, 관리하여야 한다.

나. 시스템별 추진일정

구분		1M				2M				3M			
		1W	2W	3W	4W	5W	6W	7W	8W	9W	10W	11W	12W
보고		착수				1 차 오픈				2 차 오픈			
기능 개선	분석												
	설계												
	구현												
	테스트												
	안정화												

※ 1 단계 사용자워크플로우 구축 및 SSO 접근제어 적용, 2 단계 협력사관리 기능 개발

※ 1 차오픈 완료 후 4W 안정화 기간

※ 추진일정은 최종 협의 후 변경 될 수 있음

다. 의사소통관리(보고사항)

1) "과업상대자"은 시스템 개발과 관련하여 사업의 착수에서 종료까지 주간 및 월간 보고를 이행 하여야 하며, "회사"의 요구가 있을 시 회의 및 실사에 참여하여야 한다

구분	내용	시기
월간보고	ㅇ 해당월 업무보고 • 주요 이슈 사항	매월 말일
주간보고	ㅇ 주간 보고 • 계획/실적 관리 사항 정리 • 금주간 이슈 사항 정리	매주 수요일
수시보고	ㅇ 이슈 사항 해결을 위한 특별 보고	필요 시

라. 품질보증

1) "과업상대자"은 체계적이고 효과적인 사업추진을 위하여 적절한 품질보증에 관한 검토 및 평가를 수행하여야 하며, 보완이 필요한 경우는 조정기준, 조정내용, 조정사유 등을 관련근거로 하여 명확하게 제시하여야 한다.

마. 납품 조건

1) "과업상대자"은 납품하는 적법한 라이선스의 제품을 납품하여야 한다.

2) 추후 사용자 증가 등으로 인한 사용자 라이선스 추가 구매 시 현 사업의 계약단가에 물가상승률을 고려한 금액으로 납품하여야 한다

바. 공정관리

1) 프로젝트 업무 영역별 수행업무를 명확히 정의하고, 수행방법 및 수행절차에 의거 시행한다.

2) 주어진 기간 내 목표 시스템을 구축 완성하기 위한 업무 영역별로 밀접한 선후 관계를 고려하여 종합일정을 수립 실시한다.

3) 일정 계획 수립 시 영역별 품질보증 활동 계획을 고려하여 수립한다.

사. 사업 진행관리

1) "회사"은 사업 수행 전 과정에 대하여 관리감독을 하며, 시정 요구 시 "과업상대자"은 즉시 조치하여야 한다.
2) "과업상대자"은 "회사"과의 계약내용을 충실히 이행하여야 하며 사업 수행과 관련하여 취득한 정보에 대한 필요한 보안조치를 강구하고 이를 위반할 경우에는 모든 법적 책임을 진다.
3) "과업상대자"은 구축 작업에 필요한 기술, 인력을 확보하여 사업 수행에 성실히 임하여야 한다.
4) 사업 수행 시 의견이 상충되는 부분은 협의 후 비용이나 일정에 영향을 주지 않는 경우 "회사"의 의견에 따른다.

아. 변경관리

1) "과업상대자"은 "회사"과의 협의를 통해 계약 내용과 다른 방향으로의 사업 진행 내용에 대해서는 반드시 기록하고 "회사"의 확인을 받아야 한다. 이와 관련하여 이견이 발생하였을 경우 그 입증 책임은 "과업상대자"에게 있다.
2) "과업상대자"은 본 사업을 진행함에 있어 구조의 변경이나 커스트마이징을 위한 원천 프로그램 수정 시 해당 내용을 기록하여야 한다. 이 경우 내용은 변경자, 변경일시, 변경이유, 변경내용 등으로 한다.

자. 사용자/운영자 교육

1) "과업상대자"은 시스템 구축 내용을 활용할 수 있도록 사용자에게 교육하여야 한다.
2) 교육은 사용자 참여를 유도하기 위해 집합 교육이나 온라인 교육으로 진행되어야 하며 교육 시 필요한 자원은 원칙적으로 "과업상대자"의 부담으로 한다.
3) 교육 시에는 사용자에게 이해를 돕고 추후 기능 사용 시 참고할 수 있는 별도의 교재 또는 매뉴얼이 제공되어야 한다.
4) "과업상대자"은 시스템 운영자에게 시스템 운영에 전반적인 사항을 교육하여야 한다.
5) "과업상대자"은 시스템 운영자에게 시스템 오작동 및 장애 시 신속히 대처할 수 있도록 비상 상황에 대한 조치 매뉴얼을 제공하여야 한다.

차. 시스템 운영방안

1) 시스템 구축 후 시스템 이용 및 관리·운용에 관한 전반적인 방안을 제시해야 한다.

2) 발생 가능한 장애 요소들을 유형별로 구분하여 제시하고, 각 유형별로 대처 방안을 제시하여야 한다.

3) 장애 발생 시 장애 원인을 신속하게 분석할 수 있도록 로깅 등의 방법을 이용하여 시스템의 상태가 기록되어야 한다. 특히 타 시스템과 연동 부분에 있어서는 발생된 장애의 포인트를 명확하게 파악할 수 있도록 구성되어야 한다.

카. 유지보수

1) 무상하자유지보수 기간은 최종 검수일로부터 1 년으로 하며, 동 기간 중 하자발생 시 무상으로 지원하여야 한다.

2) 무상유지보수 기간 중 치명적인 시스템 오류로 인하여 시스템 사용이 불가능할 경우 즉시 사업 수행 시 개발인력을 문제발생 인지 시부터 해결 시까지 투입하여 지원하도록 하여야 한다.

3) 모든 소프트웨어 및 성과물에 대한 충분한 유지보수 지원방안을 분야별로 구분하여 구체적으로 제시하여야 하며, 무상이 아닌 경우 비용부담 조건 등을 계약서에 명시하고 계약 시 해당 내용에 대해 담당자에게 설명하여야 한다.

2. 산출물 및 지적재산권

가. 모든 산출물 일체는 감독관의 검사를 받아 사업추진 일정에 맞추어 제출하여야 한다.

나. 단계별 산출물 제출 목록

단계	단계별 활동	산출물
추진계획	계획 수립	프로젝트 추진계획서(WBS 등)
분석/기획	요구사항 분석	요구사항정의서
	기능 정의	기능 정의서

단계	단계별 활동	산출물
설계	데이터베이스 설계	ERD (논리/물리), 테이블정의서
	프로그램 설계	프로그램 목록
	인터페이스 설계	인터페이스 정의서, UI 설계서 요구사항 추적 매트릭스
구현	프로그램 코딩 및 리뷰	단위시험 명세서/결과서
	단위시험 및 결과 확인	프로그램 소스코드
	프로그램 배포	
시험	시험결과서 작성 및 확인	통합시험 명세서/결과서
	매뉴얼 작성 및 교육	운영 매뉴얼(사용자/운용자)
업무적용	상용전환	전환(운용) 계획서
종료	프로젝트 완료보고	업무전환 완료보고서, 준공계 프로젝트 완료보고서

※ 상기 산출물은 고객 협의 후 추가/변경 될 수 있음.

※ 용역 종료 후 검수 시 본 산출물 내역에 명시된 산출물 제출 여부를 확인하여야 한다.

다. 전산자료

1) 상기 산출물 수록 USB 2ea

2) 개발된 프로그램 1 조 (원시/목적) 수록 USB 2ea

(용역수행 시 개발된 프로그램에 한함)

라. 모든 산출물은 지적재산권과 관련된 사항을 주의해서 작성해야 하며, 지적재산권과 관련된 문제 발생시 지적재산권 소유자와의 분쟁해결 및 본 사업의 추진과정에서 오는 모든 손해배상 등의 책임은 "과업상대자"에게 있다.

마. 모든 산출물의 지적재산권은 "회사"에 귀속된다. 단. 다음의 경우는 제외한다.

1) 상용 소프트웨어 등 제 3 자 소유의 지적재산권과 본 계약 체결 이전 "과업상대자"이 소유하거나 향후 소유하게 될 지적재산권 (경험 및 노하우 포함하며 이에 한정 하지 않는다)

2) "과업상대자"이 기존에 보유한 지적재산권의 추가적인 개선 또는 파생되는 결과물(단, 본사업에 필요할 경우 무상의 사용권을 제공한다)

3. 정보보호 검토사항

가. 시스템의 설계 시부터 보안 취약점의 최소화가 고려되어야 하며 시스템은 "소프트웨어 개발보안(시큐어 코딩) 관련 가이드(안전행정부)"를 기준으로 구현되어야 한다.

나. 시스템의 보안성과 관련하여 설계의 변경이 발생되거나 설계 시 고려되었던 기능의 구현이 어려울 경우 대체 가능한 기능이 구현되어야 하며 이 또한 위의 가항의 내용이 준수되어야 한다.

다. 본 시스템의 설계 시 개인정보 처리 등 정보보호 관련 프로세스가 적절히 반영되고 검토되었는지 정보 처리 절차에 대한 보안성 검토가 수반되어야 한다.

라. 본 시스템의 업무 적용 전, 개인정보보호 OWASP TOP10 에서 제시된 웹서비스 취약점에 대한 내성 등 시스템 기능에 대한 정보보호에 대한 보안성 검토가 선행되어야 한다.

마. 설계 및 구현 중 본 사업 범위 이외의 것으로 인해 발생할 수 있는 보안 취약점을 인지하였을 경우 완료보고서 등 산출물에 그 가능성에 대해 명시하여야 한다.

바. 구현 시 어플리케이션 프로그램(코드 부분)과 데이터 영역(유통정보, 정책정보, 첨부파일 등)은 엄격히 분리하여 관리되어야 한다.

사. 정보보호와 관련된 세부 사항은 양측 협의된 내용에 한하여 요구사항 관리대장, 사업수행계획서, 설계서에 기록, 관리되어야 한다.

아. 기타 보안 관련 제반 사항은 첨부된 자료를 준용하여야 한다.

4. 보안유지 사항

가. "과업상대자"은 본 건과 관련하여 알게 된 "회사"의 시스템 환경, 운영 및 시설 등에 관한 정보를 외부에 누설하여서는 안되며, 만일 이를 위반하였을 경우 민・형사 상의 책임을 진다.

나. "과업상대자"은 사업 프로젝트팀 출입 등에 필요한 제반 보안사항을 충실히 이행하여야 하며, "회사"이 요구할 경우 프로젝트 수행인력의 재직증명, 신원조사와 관련된 서류를 제출하여야 한다.

다. 사업수행 과정에서 취득한 자료와 정보에 관해서는 사업수행 전·후 "회사"의 승인 없이 외부에 유출 또는 누설하거나 다른 용도로 이용할 수 없으며 이를 위반하여 발생하는 민·형사 상의 책임, 그에 따른 유·무형의 손해배상 책임을 져야 한다.

라. 납품하는 하드웨어 및 소프트웨어의 자체 보안상 문제점이 발견될 시 "과업상대자"은 즉시 그 대책을 수립하여 해결하며 모든 민·형사 상의 책임을 지고 보상하여야 한다.

5. 기타사항

가. 기능 변경 추가 시 각 소프트웨어의 수정이 용이하여야 한다

나. 서비스 진화 및 기술발전에 따른 새로운 기능추가와 변경이 용이한 모듈 구조로 설계 되어야 한다.

다. 오류 수정 및 개량 개선 시 서비스 중지가 발생하지 않도록 소프트웨어를 설계하여야 하며, 불가피하게 서비스 중지가 발생하는 경우 최소한의 정지 시간을 갖도록 하여야 한다.

라. 소프트웨어의 추가, 변경으로 기존 시스템의 성능 저하 및 연동성에 문제가 없어야 한다.

마. 본 프로젝트에 사용되는 모든 소프트웨어는 "회사"의 상업용으로 사용하는데 아무 런 지장이 없어야 한다. 단, 사전승인을 받거나 권한을 이양 받아야 하는 경우에는 "회사" 명의의 권한획득 업무 일체를 수행사에서 이행한다.

바. 납품(준공)시 제조업체의 기술지원확약서를 제출 하여야 한다

사. 개인정보 및 기업정보 보호를 위해 다음의 서류를 제출하여야 한다.

- 정보보호 서약서(협력사 대표자용 / 협력사 임직원용)
- 개인정보 취급위탁(제공) 계약 보안 서약서