동양네트웍스(주)
TONGYANG Networks Co.,Ltd.

스마트 모바일 오피스 소개

Smart mobile Office

Maket Designer Innovative Value Creator

TONGYANG Networks



동양네트웍스(주)
TONGYANG Networks Co.,Ltd.

CONTENTS

1 모바일오피스 구축시 Key Point

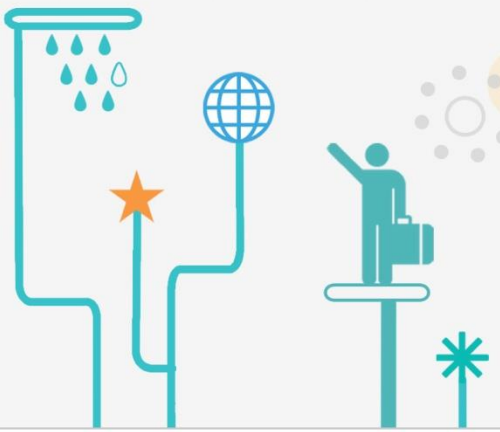
2 스마트 모바일 오피스 서비스 개요

3 서비스 개요

4 서비스 특징

5 도입 효과

6 별첨







동양네트웍스(주)
TONGYANG Networks Co.,Ltd.

1

모바일오피스 구축시 Key Point

- 1. Mobile Platform
- 2. Device Trends
- 3. App 개발 아키텍처
- 4. Security

TONGYANG

1. Mobile Platform

모바일 도입 기업의 고민

기업의 고민

- 모바일을 도입해야 할 업무 시스템이 다양한데 모바일도 시스템이 다양해진다.
- Smart Phone, Tablet PC 등 화면 해상도도 다양한데 비용은 한정적이다.
- OS도 다양하고, 버전도 너무 다양한데 이를 모두 지원하기가 어렵다.
- 모바일 디바이스에 대한 보안 대책은?
- 지속적으로 늘어나는 사용자 관리와 업무 시스템 관리에 대한 방안은
- 우리가 직접 시스템을 개발하면 조금 더 효율적이지 않을까?

시사점

- 다양한 Legacy System
- 다양한 Device
- 다양한 OS와 Version
- Device 보안
- 시스템 및 사용자 관리
- 업무 생산성 및 효율성

Key is Mobile Platform

Multi-OS Support	• One source Multi Use • 유연한 신규 단말 기기 적용
보안	• 이중화 사용자 인증 • 첨부 및 전송데이터 보안
유연한 Legacy 연동	• Legacy 상황에 따른 연동방법 제공
관리 및 운영	• App별, 사용자 권한 관리 • OS별 App 등록 및 배포관리

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

2. Device Trends

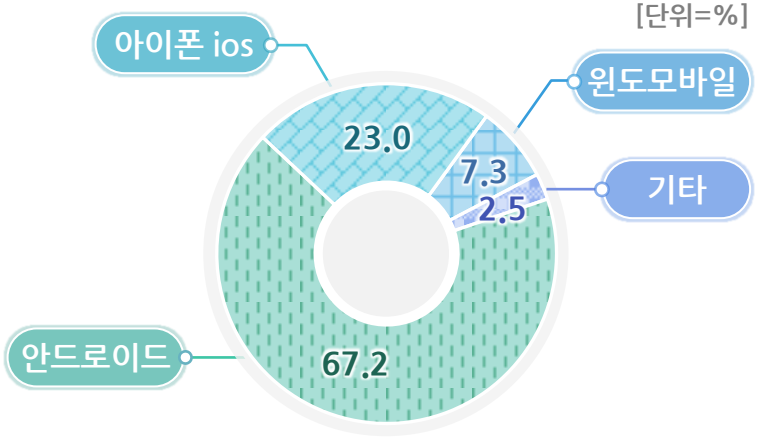
단말 OS 시장이 Android와 iOS 위주로 양분되고 있어 이를 고려한 Muti-OS Support 구축고려가 필요함

- 다양한 화면크기, 해상도, OS의 기기 출시
- Smart Phone : 2012년2월 현재 국내 판매중인 모델 79종(Size 18종, 해상도 10종)
- Smart Pad : 2012년 2월 현재 국내 판매중인 모델 44종(Size 8종, 해상도 7종)
- OS : Android, iOS, Windows, Bada, Palm, Symbian …

주력 O/S 및 단말기 선정 필요

스마트 운영체제 한국 점유율

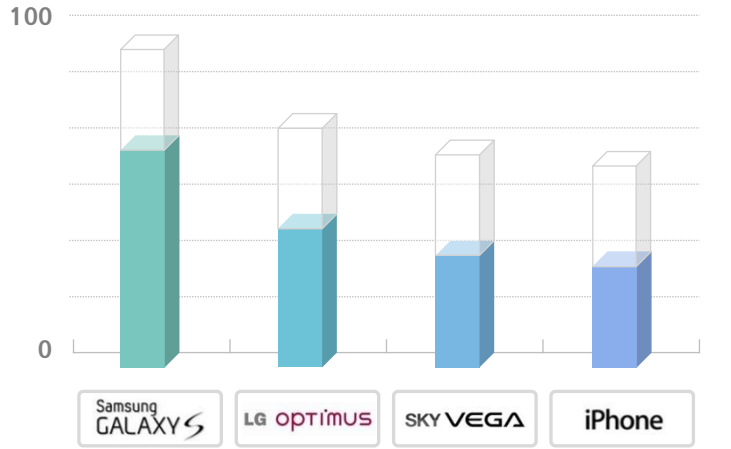
[단위=%]



※ 2011년 2월, 총897만대, 자료=각 사 통합

국내 스마트폰 점유율

[2011. 09]



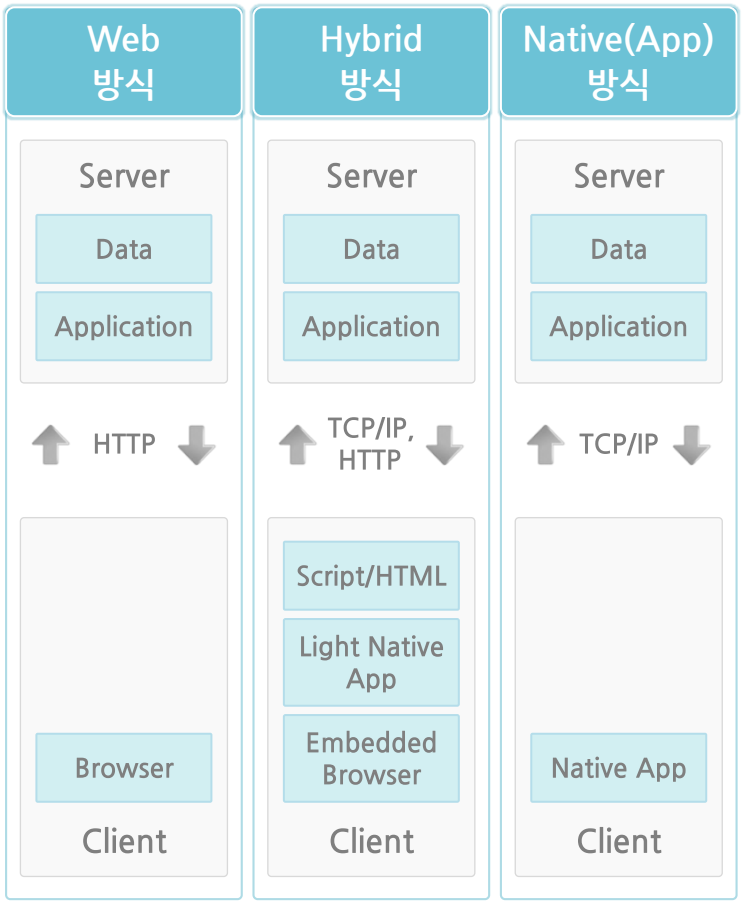
Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

3. App 개발 아키텍처

Mobile Application 구조는 크게 Web, Hybrid, Native의 3가지로 구분되며, Enterprise환경에서는 특성에 따라 선택되고 있음

개발업무특성에 따른 Mobile 개발아키텍처 선정필요

Mobile App 개발구조



App개발 아키텍처 별 특징

구분	Mobile Web	Hybrid App	Native App
Multi-OS	우수	보통	O/S별 개발
개발용이성	높음	높음	낮음
UI 표현 능력	낮음	중간	높음
실행속도	실행속도 보통	실행속도 우수	실행속도 빠름
그래픽성능	낮음	보통	높음
App Update	해당 페이지 재로딩	수정부분만 업데이트	재설치
아키텍처	Web (HTML, Script,)	Web(HTML5 ,CSS3,Script) + Native	Native

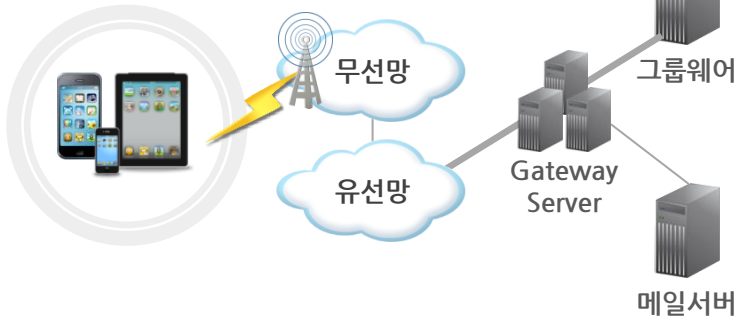
Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

4. Security

기업보안 실현을 위해 단말보안, 플랫폼 보안, 네트워크 보안, 컨텐츠 보안관점에서 보안정책 수립 및 보안 솔루션 도입을 검토 해야 함

보안 분류

① 응용프로그램 및 플랫폼 보안



② 단말 보안 ③ 네트워크 보안 ④ 서버 보안

- 모바일오피스의 보안은 악성 코드 등에 의한 Application의 보안과 단말의 분실 등에 따른 단말 보안, 네트워크, 서버의 보안 영역으로 분류할 수 있음

영역별 보안 대책

① Application 및 플랫폼 보안 대책

- Application 등록 > 검증 > 배표 시 보안 점검 체계 확립
- 플랫폰(OS 등)의 보안 취약점을 정기적으로 체크하고, 보안패치가 필요한 경우, 자동 업데이트를 통한 보안 강화

② 단말 보안 대책

- 도난·분실 대책으로 스마트폰 잠금 기능(원격 잠금)및 원격 파일 삭제 기능 등 물리적 보안책 마련
- 정책·업무 자료는 스마트폰에 저장되지 않도록 하며, 플랫폼에서 편집이 불가능한 형태로 병환하여 스트리밍 방식을 사용하여 스마트폰에 전송

③ 네트워크 보안 대책

- 모바일 플랫폼은 상용 인터넷망을 경유하지 않고, 이동통신망에서 전용 회선으로 직접 연결
- 데이터의 유출 방지를 위해 암호화 기능 및 네트워크 VPN(Virtual Private Network, 공중망 상에 사설망을 구축하여 전용망처럼 이용할 수 있는 방식)적용

④ 서버 보안 대책

- 모바일 플랫폼은 보안 적책 수준에 따라 전용 플랫폼을 구축하거나, 사업자 시설 등을 활용하여 공동 활용
- 데이터 입출력 시 DES(64bit), 3DES(192bit) 등 표준화된 암호화 기능을 적용하여 보호

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

동양네트웍스(주)
TONGYANG Networks Co.,Ltd.

2

스마트 모바일 오피스 서비스 개요

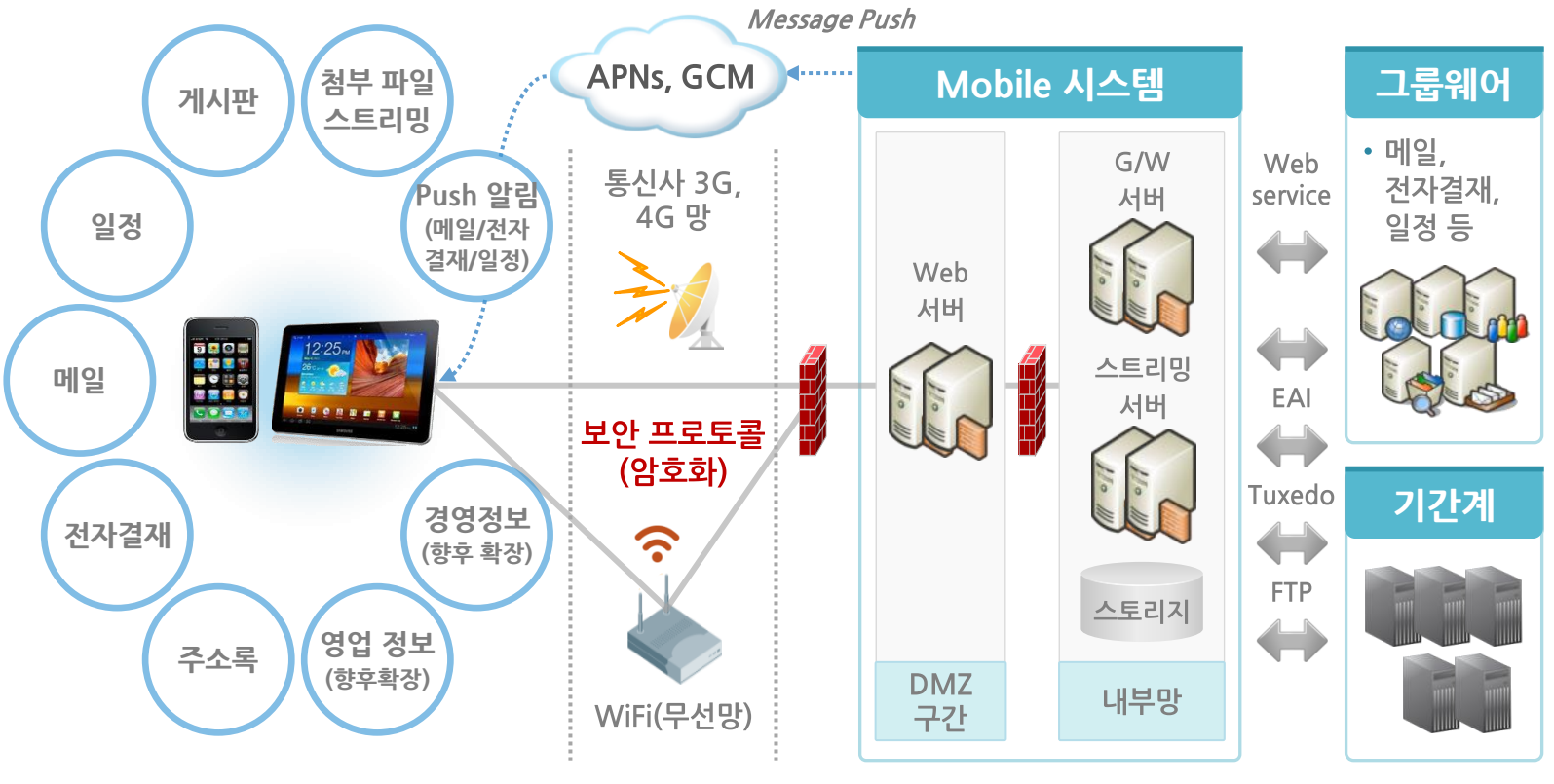
> 스마트 모바일 오피스 서비스 개요

TONGYANG

1. 스마트 모바일 오피스 서비스 개요

SMARTOffice는 임직원들에게 언제, 어디서나 업무수행이 가능한 환경을 제공하기 위해, 다양한 스마트폰을 대상으로 보안성이 뛰어난 서비스를 제공하며, 용이한 다양한 Legacy 시스템과의 연계 및 기존 업무의 모바일 서비스로의 확장을 지원합니다.

모바일 오피스 서비스구성도



서비스 제공 단말 종류

- iOS : iPhone 3GS, 4, 4S, 5, iPad1, 2, iPad mini
- Android : Galaxy S/S2/HD LTE/Note, Optimus 폰 외 Galaxy Tab 10.1, Note 10.1

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

3 서비스 개요

> 1. 서비스 기능

TONGYANG

1. 서비스 기능

구 분	주요 기능
메일	• 받은 메일함/안읽은 메일함/중요메일함/보낸 메일함/임시 저장함/메일 보관함/휴지통, 메일함 목록 조회, 메일목록 편집, 메일목록 조회, 메일쓰기, 메일상세 조회, 메일검색, 첨부파일 조회
전자결재	• 결재대기문서 목록 조회, 결재진행문서 목록 조회, 결재반려문서 목록 조회, 결재완료문서 목록 조회, 결재문서 상세 조회, 결재의견조회, 결재완료함 검색 , 결재 승인/반려/합의, 첨부파일 조회
일정	• 월간 일정관리, 주간 일정관리, 일간 일정관리, 일정 목록 조회, 타인 일정 조회, 일정 검색, 일정 편집 , 일정 등록, 일정 상세조회, 캘린더 변경
게시판	• 게시판 목록 조회(전체, 사내알림, 인사공지, 경조사 등), 게시글 조회/편집, 댓글달기
주소록	• 팀원 목록 조회, 조직도 조회, 메일그룹 조회, 개인주소록 조회, 계열사 변경, 임직원 검색 , 개인주소록 그룹 조회, 개인주소록 편집, 개인 프로필 조회
Push 서비스	• 메일, 일정, 전자결재 컨텐츠 실시간 알림을 위한 Push 서비스 제공
공통	• 사용자 신청/해지, 안내 SMS 전송(연동), 안내 Email 전송, 로그인, 첨부파일 스트리밍, 단말기 관리(사용 신청/정지/해지),
G/W 관리	• 단말기관리, App등록/배포 관리, 로그인, 결재서식관리, 로그조회, 연동 서버 URL 관리, 서버 환경설정 관리, 사용자별 메일 URL 관리

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

동양네트웍스(주)
TONGYANG Networks Co.,Ltd.

4

서비스 특징

- 1. 서비스 특징
- 2. 뛰어난 보안성
- 3. 개발 아키텍처
- 4. App 관리 및 Legacy연동이 용이한 Gateway
- 5. 통합 개발환경
- 6. 빠르고 직관적인 UI/UX

TONGYANG

1. 서비스 특징

설계단계부터 보안성 강화를 고려하여 구축하였으며, 모바일 플랫폼(MEAP)기반의 Hybrid App 방식으로 시스템을 개발하여 유지보수성이 뛰어나며 , 빠르고 직관적인 UI/UX 를 적용하였습니다.

모바일 보안

» 뛰어난 모바일 보안성

- 이용자 단말 보안 : 단말기/사용자 이중 인증, 데이터 저장 방식
- 네트워크 보안(암호화)
- 첨부파일 스트리밍 서비스
- App/서비스/사용자 단위 권한 관리
- 단말기 분실시 접속 차단
- 사용자/단말기별 추적성 제공

HTML5 기반 Hybrid App

» HMLT5기반의 Hybrid App

- Native(디바이스 통제) 와 Web(업무개발)을 결합한 아키텍처
- 웹 표준 HTML5 개발로 One-Source Multi-Use 지향
- 유지보수성이 뛰어남 : Web 표준 적용



편리한 Legacy 연동

» App 관리 및 Legacy연동이 용이한 Gateway

- App별 버전/등록/승인/배포 관리 제공
- 단말기 관리 : 지원 O/S 및 Version, 지원 Device 종류 관리
- 다양한 Legacy연동 Adaptor지원 (HTTP, Webservice, EAI, Tuxedo, EAI)

UI/UX 설계

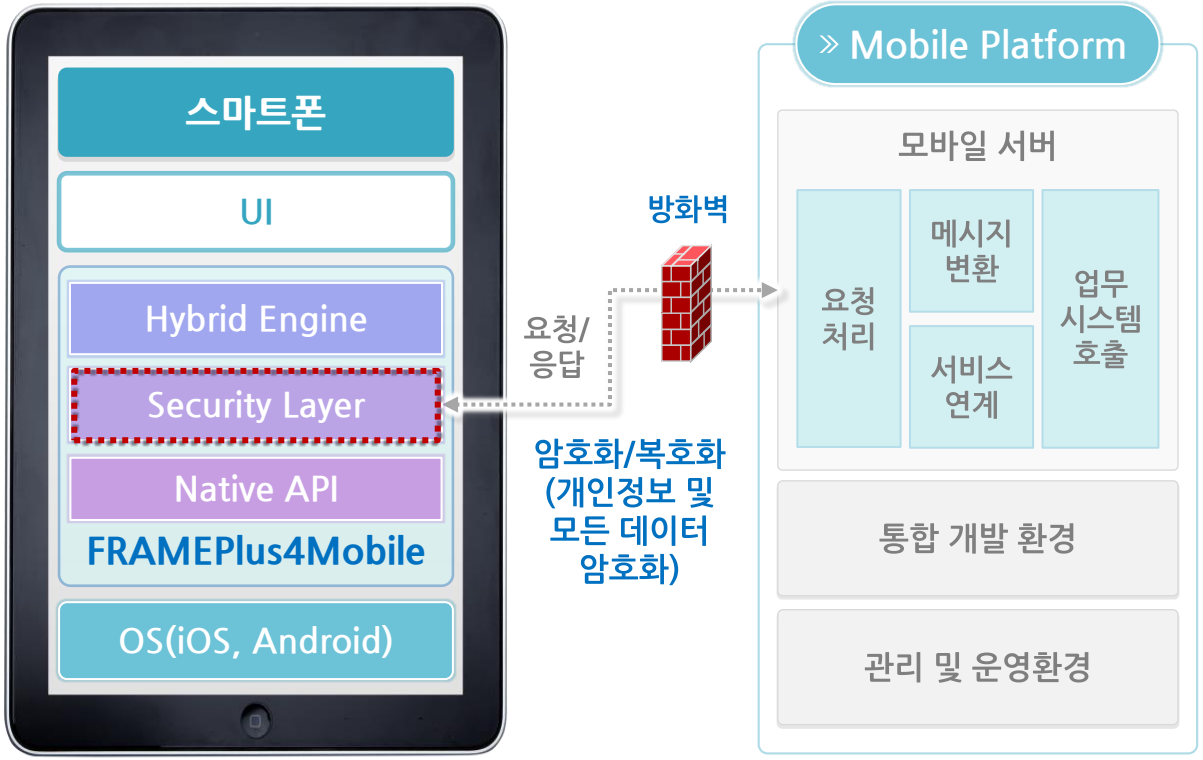
» 빠르고 직관적인 UI/UX

- O/S 및 디바이스별 UI/UX 통일
- 직관적이고 빠르게 접근 할 수 있는 GNB 메뉴
- OS간의 동일한 표준 UI 적용
- 고급 양장 다이어리 느낌의 디자인



Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

2. 뛰어난 보안성 - 아키텍처



단말보안

- 도난, 분실 대책으로 업무자료는 단말기에 저장되지 않으며, 분실시 해당 단말기 접속 차단기능 제공
- 첨부파일은 스트리밍 방식 사용
- 복합인증 방식 : 단말기 + 사용자 인증
- 루팅/탈옥폰에 App 수행방지

네트워크 보안

- 데이터 유출방지를 위해 전문 송수신시 암호화 적용(AES 128bit / RSA 512bit)
- 사용자 인증시 Token 방식 사용

App 및 서버 보안

- 그룹 보안기준에 따른 서버 구성 및 검증된 Framework 사용(생명 기 사용 Frameplus)
- App 배포시 검증된 App만 배포될수 있도록 등록/ 검증/ 배포 기능 제공

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

2. 뛰어난 보안성 - 첨부파일



통합뷰어

- 다양한 문서 지원 : Microsoft Office, 아래한글, 훈민정음, PDF, TIF, Auto CAD 등
- 다양한 단말기 지원 : iOS, Android 지원



문서보안

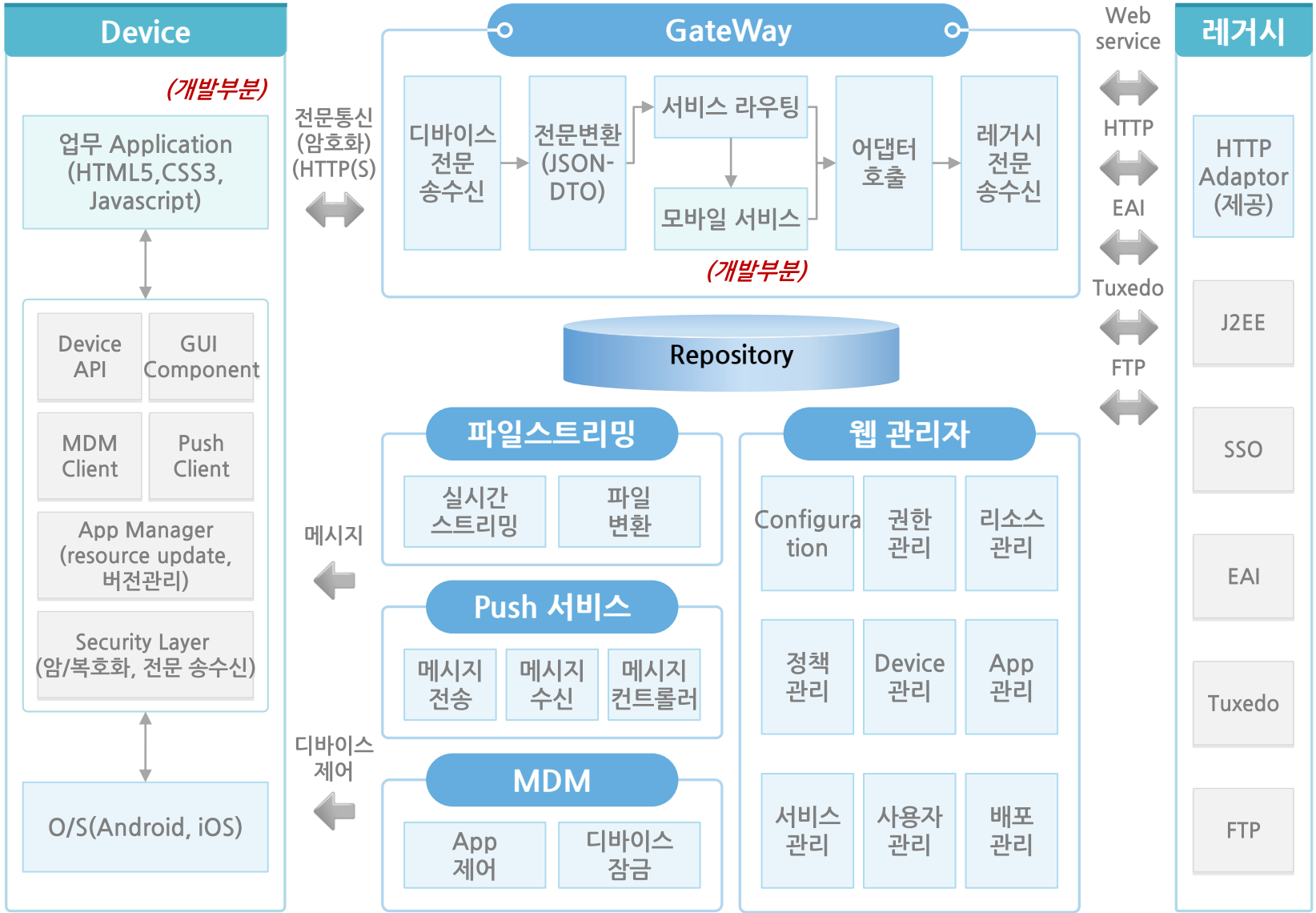
- 실시간 스트리밍 : 문서 다운없이 단말기 휘발성 메모리에 실시간 스트리밍하여 Viewing 제공
- 첨부파일을 DRM 암호화/복호화 적용(DRM 적용 계열사 한정)



Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

3. 개발 아키텍처

FRAMEPlus4Mobile 는 기업의 Enterprise system과 사용자의 Mobile 단말을 연동하여 모바일 어플리케이션의 개발, 배포, 관리가 가능한 통합 플랫폼을 적용하였으며, 개발생산성과 유지보수성이 우수한 Hybrid App 아키텍처로 개발되었습니다.



Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

4. App 관리 및 Legacy연동이 용이한 Gateway

검증된 기존 금융/기간계 프레임웍(FramePlus)을 기반으로한 FRAMEPlus4Mobile 는 Hybrid 형태의 모바일 어플리케이션 구축을 위한 다양한 기능을 제공하고 있습니다.

FRAMEPlus4Mobile

HTML5기반의 Hybrid 아키텍처

- Native App과 Web을 결합한 아키텍처
- Web을 이용한 신속한 배포 및 UI구현이 용이
- One-Source Multi-Use 지향

다양한 Adapter를 이용한 Legacy 연계

- FRAMEPlus, FTP, Tuxedo, EAI 등의 Adapter 제공
- 표준 DTO를 이용하는 Adapter 추가 용이

Open 아키텍처 기반의 Light 전문 송수신

- JSON 전문채택으로 사용이 용이하며, 전문 데이터 Size가 작아 통신속도가 빠르며 통신부하가 적음
- iOS, Android 기반의 Device 지원

Push 서비스 제공

- OS 기반의 PushService를 이용한 경량 메시지 전송
- Google C2DM, Apple APNs 사용

통합 개발환경 제공

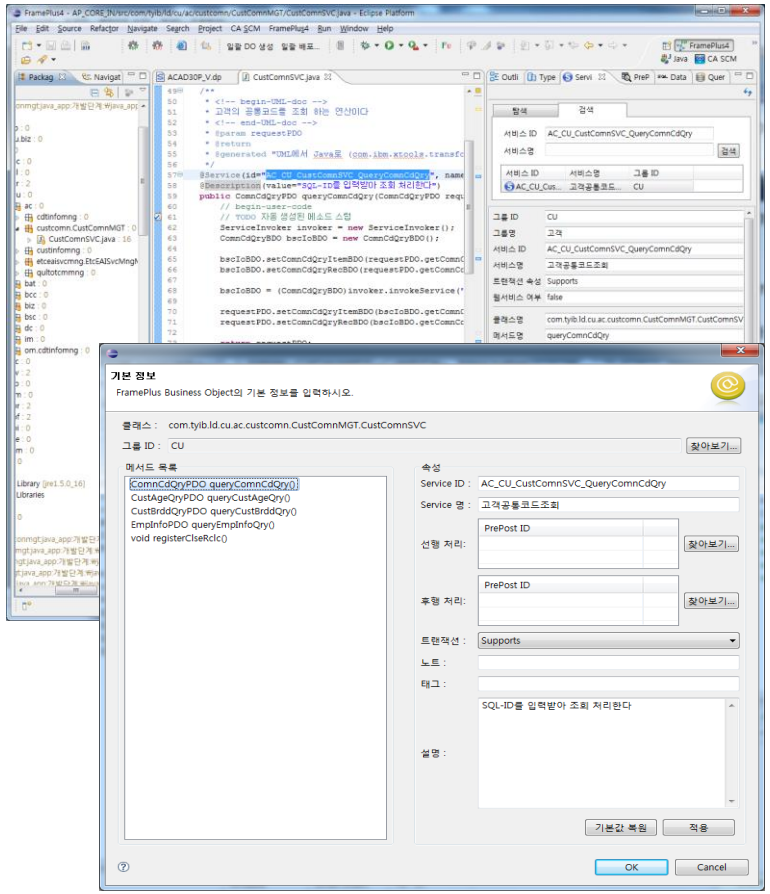
- Mobile Service 구현을 위한 IDE 제공
- 표준 DTO 사용
- FRAMEPlus for Java Framework과의 호환이 용이

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

5. 통합 개발환경

FRAMEPlus4Mobile은 모바일용 서비스를 정의하고 배포하기 위하여 FRAMEPlus4에서 지원되는 것과 동일한 통합개발환경 Studio를 제공합니다.

통합 개발환경 Studio



Source Editing
- Eclipse Java Editor를 그대로 사용 가능
- 일반 Java 개발과 동일하기 때문에 Java 개발자에 의한 손쉬운 개발이 가능
- 코드 레벨의 세밀한 제어가 가능

Annotation
- Service 메타 정보의 작성을 위하여 Annotation 기술 활용

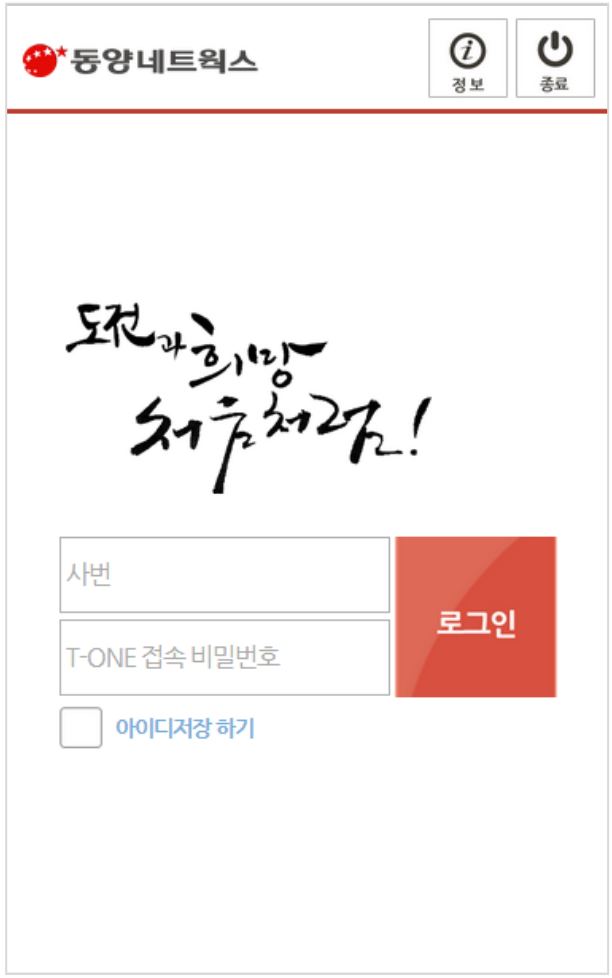
Service
- 하나의 Business Object에 여러 Service 구현 가능

Service View
- 기존 배포된 Service의 검색을 위한 Service View 제공

Service Meta Plug-in
- Service 메타정보 작성도구를 Eclipse Plug-in으로 제공
- 서비스 메소드는 public 이고 입출력이 FRAMEplus 4 지원 타입
- Annotation 입력도구를 제공하여 일반 메소드의 손쉬운 서비스 노출이 가능

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

6. 빠르고 직관적인 UI/UX





디자인 컨셉

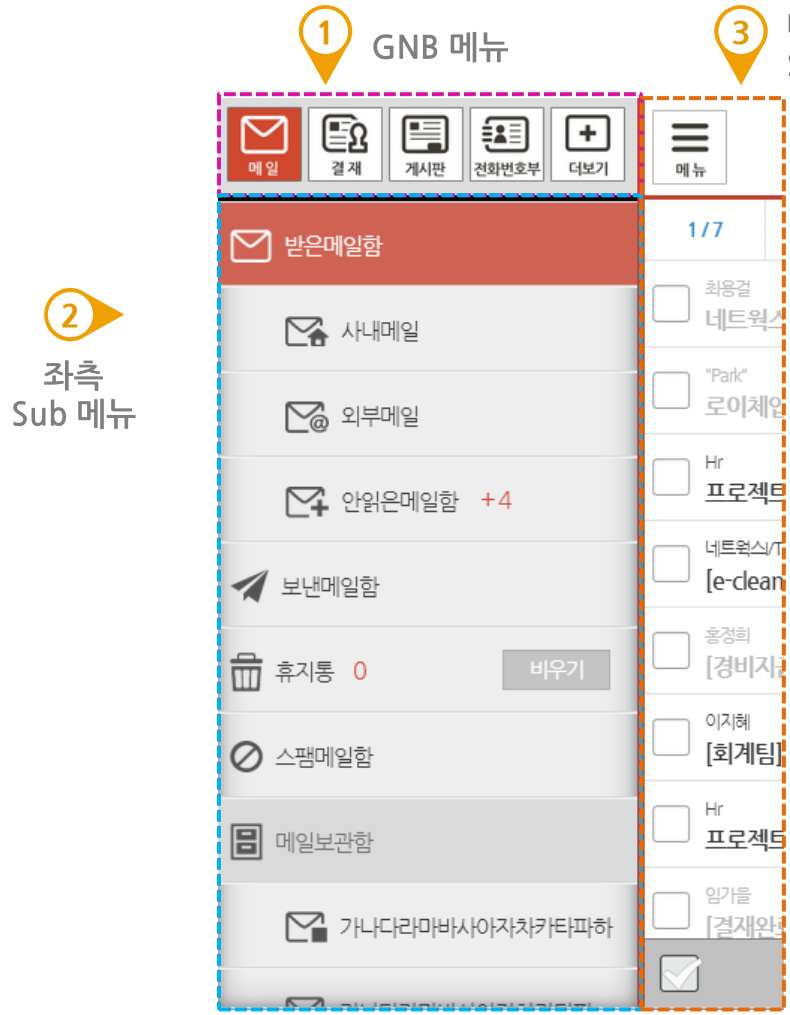
- 플랫디자인 컨셉
- 빠르고 직관적인 UX



Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

6. 빠르고 직관적인 UI/UX

동양 모바일오피스는 GNB 및 Side 메뉴 및 Pull-down/Pull-up UX제공을 통해 직관적인 빠르고 편리한 UX 제공합니다.



UX 특징

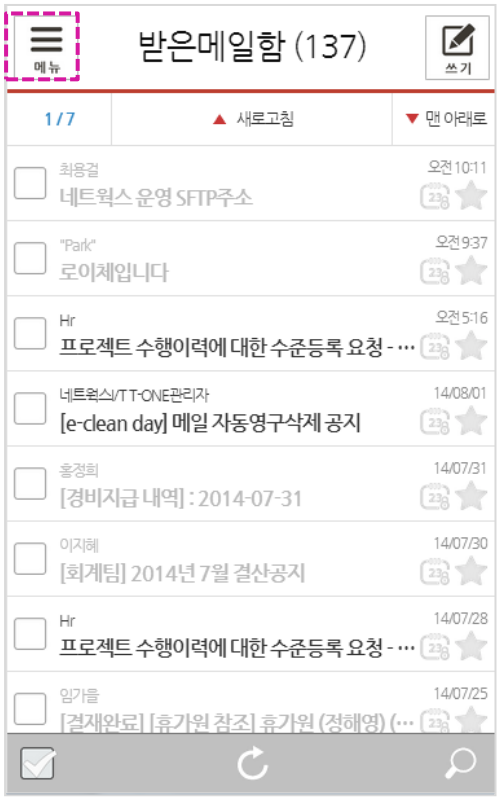
1. 좌측 상단에는 GNB(Global Navigation Bar) 제공
   - 메일, 일정, 전자결재, 주소록, 기타
2. 좌측에 GNB에서 선택한 Sub 메뉴 제공
3. Sub 메뉴에 대한 데이터 목록 Slice View 제공



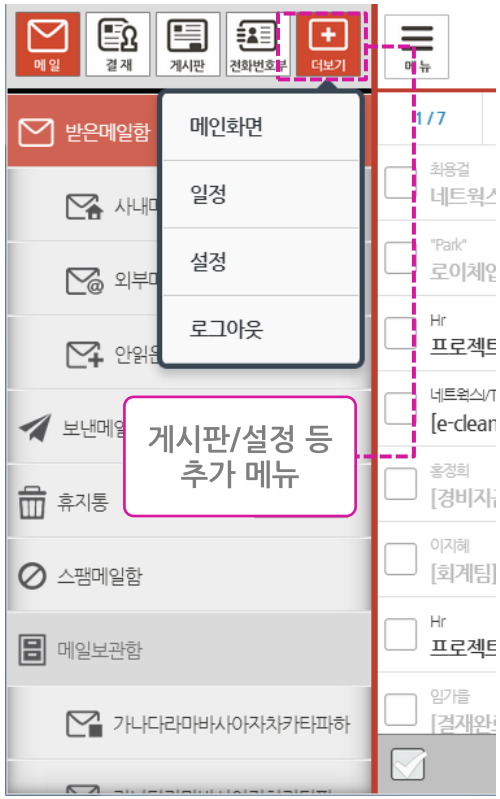
Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

6. 빠르고 직관적인 UI/UX

④ 목록 View에서 GNB 메뉴 노출 버튼 Click



GNB 및 Side Sub 메뉴 노출



UX 특징

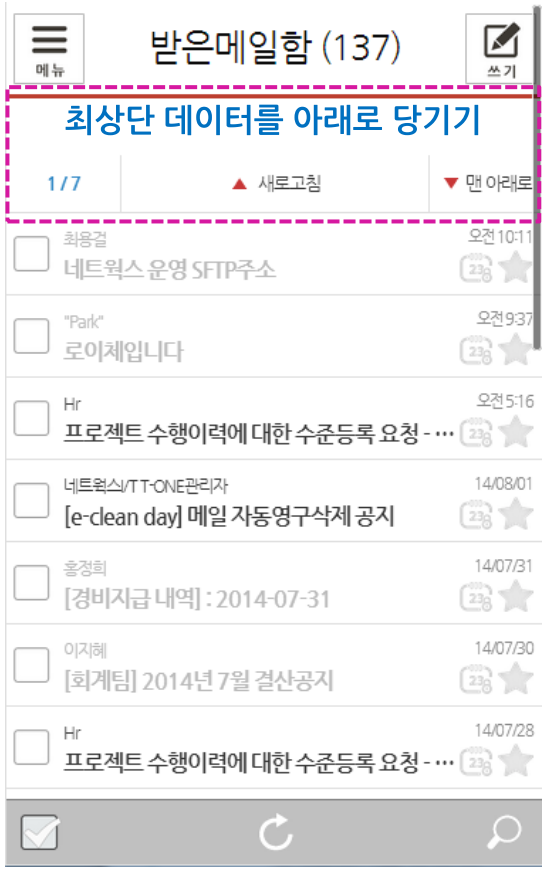
④ GNB 및 좌측 Side 메뉴 노출 버튼 제공

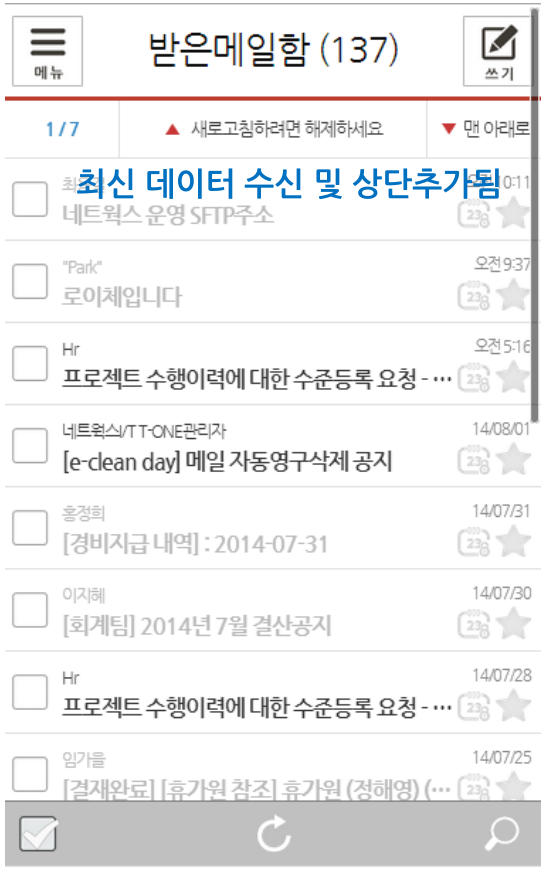


Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

6. 빠르고 직관적인 UI/UX

5 최신 데이터 새로 고침 UX - 최상단 목록 데이터 아래로 당기기





UX 특징

5

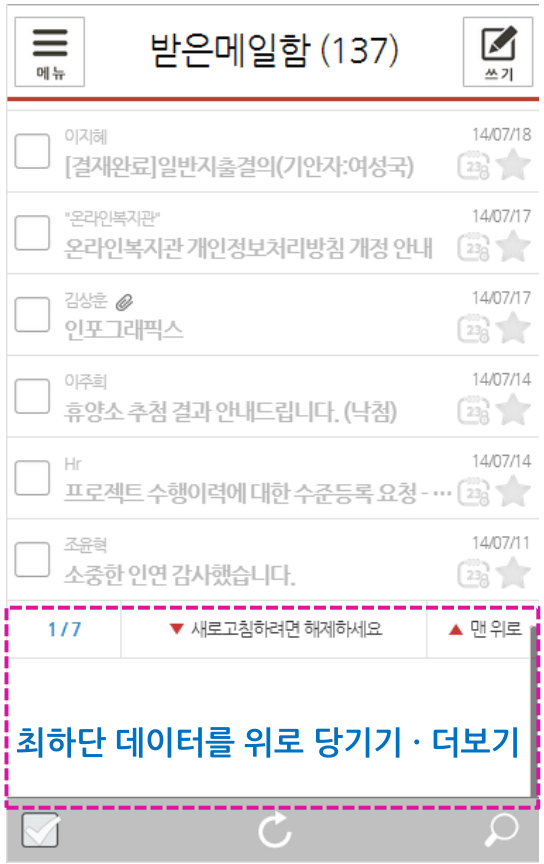
편리한 목록 데이터 View
새로고침, 더보기 UX
pull- down(아래로 당기기)
pull-up (위로 당기기)

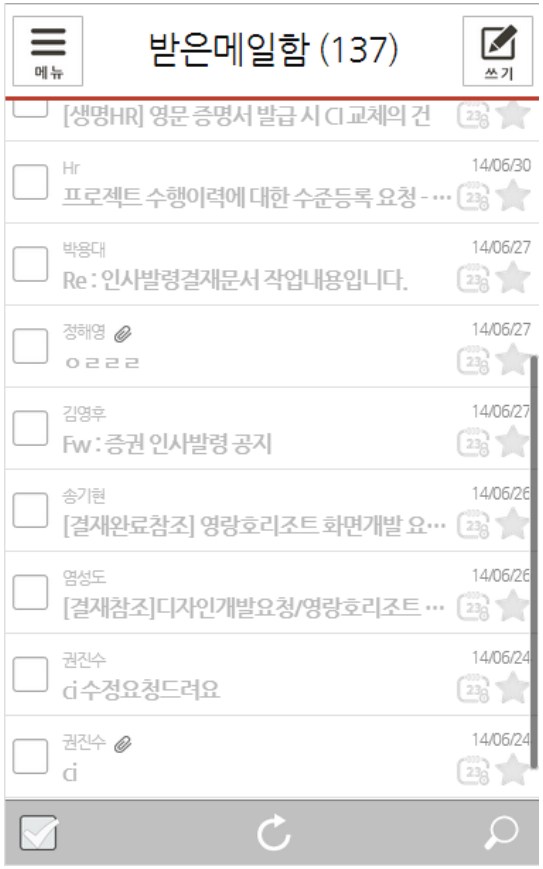


Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

6. 빠르고 직관적인 UI/UX

5 이전 데이터 목록 더 보기- 최하단 목록 데이터 위로 당기기





최신 데이터 수신 및 하단 추가됨

UX 특징

5 편리한 목록 데이터 View
새로고침, 더보기 UX
pull- down(아래로 당기기)
pull-up (위로 당기기)



Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

동양네트웍스(주)
TONGYANG Networks Co.,Ltd.

5

도입 효과

> 1. 도입효과

> 2. 스마트 모바일오피스 및 Mobile Platform 국내 고객

TONGYANG

1. 도입효과

최고의 보안성을 기반으로 급변하는 모바일 시장 환경에 유연하게 대응할 수 있는
성공적인 모바일 시스템 구축

SMART Mobile 서비스 구축

다양한 단말 대응 및 효율적인 App관리

- One-Source Multi-Use가 가능하여 O/S 별 Device별 개발이 필요않음
- 화면 개발을 위한 다양한 컴포넌트를 제공
- App실행시 단말기에 데이터를 저장하지 않으며, Gateway를 통한 단말기 통제 및 관리기능을 통해 분실시 문제가 발생않음
- 자체 App버전 관리 및 배포/업데이트 기능 제공하여 쉽고 효율적인 App관리 가능

개발생산성 향상 및 유지보수 편리

- Multi OS, 단말기 지원으로 중복 운영 비용 절감 및 App 개발의 단순화를 통해 비용절감 효과큼
- HTML5기반의 표준 Web 기술을 사용으로 기존 Web 개발자 활용이 매우 용이
- 모바일 서비스 개발이 용이한 Eclipse기반의 통합 개발환경을 지원
- 웹 기반 관리 콘솔을 제공하여 프레임워크의 효율적 관리가능

유연한 모바일 업무 확장

- 메일, 결재 등 단순 영역에서 SFA, FFA, 경영정보 등의 특화 영역으로 확장 용이(다양한 Adaptor제공, 연동 기능 제공)
- 향후 시스템 증설 시 프레임워크 및 개발된 서비스를 변경 없이 적용 가능
- 다양한 Legacy 연동 Adaptor 및 서비스 연동 관리 기능 지원

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

2. 스마트 모바일오피스 및 Mobile Platform 국내 고객

2012년 2월 출시되어 동양 그룹사의 모바일오피스(동양증권, 동양생명, 네트웍스 등)에 적용되었으며, Mobile Platform은 현대라이프 및 동양생명 모바일 전자청약, SFA 적용되어 보안성 및 안정성을 검증받았습니다.

동양그룹

» 모바일오피스

- 동양증권(주)
- 동양생명보험(주)

금융

» 모바일 SFA

- 동양생명보험(주)
- Hyundai Life

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

동양네트웍스(주)
TONGYANG Networks Co.,Ltd.

6

별첨

- 1. 스마트 모바일 오피스 보안성
- 2. 모바일 플랫폼 보안성 설계시 고려사항
- 3. 행안부 KISA 스마트워크 활성화

TONGYANG

1. 스마트 모바일 오피스 보안성

FRAMEPlus4Mobile 기반의 네트웍스의 모바일오피스는 금감원의 보안 기준을 충족합니다.

보안 기준	FRAMEPlus4Mobile 보안 적용(안)
인증	• AES 128bit / RSA 512bit 암호화 적용 사용자 인증처리 • 자체 세션 Key 를 통한 인증 및 세션 타임아웃에 따른 자동 로그아웃 기능 • 공인 인증서 모듈 연동 가능(3rd-Party 연동이 가능한 개방형 구조임) • Client 타임 아웃에 따른 화면 잠금 기능
악성코드 대응	• 루팅 및 탈옥폰에서 App이 실행되지 않도록 제어함 • 백신/MDM 연동 가능(3rd-Party 연동이 가능한 개방형 구조)
개발/아키텍처 보호	• 검증된 개발 아키텍처 적용 (FramePlus4)
접근통제	• App/컨텐츠 별 접근 통제 및 권한관리 기능 제공 - 관리 콘솔의 설정을 통한 접근 통제 및 권한관리 기능을 제공
데이터 변조/유출 방지	• 송/수신 데이터의 암호화 기능 제공(AES 128bit / RSA 512bit) - 암호화 설정에 따른 구간 암호화 제공 - 부분 암호화를 위한 암호화 API 제공 • 보안을 고려하여 단말기에 업무데이터를 저장하지 않음 • 첨부파일의 경우 DRM 복호화 연동 지원 및 스트리징 서비스 제공
분실/도난	• 단말기 관리기능을 통해 분실시 즉시 해당 단말기 접속 차단이 가능함 • 단말기에 업무데이터 저장을 하지 않아 유출방지
디바이스 통제	• MDM 연동 가능(3rd-Party 연동이 가능한 개방형 구조)
무선통제	• 내부 AP 통제 • Ad-Hoc 네트워크 탐지 및 차단 ➔ 향후 제공 예정
배포/패치 및 모니터링	• APP/컨텐츠의 설치 및 배포 관리 기능 제공 • 사용자별 단말기 정보, App 배포버전, 접속 로그 관리 기능 제공 • 자체 배포 사이트를 통해 배포가 가능하며 App 패치/업그레이드시 App 실행시 버전체크 및 자동업그레이드 기능을 제공함

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

2. 모바일 플랫폼 보안성 설계시 고려사항

모바일 상세 보안위협 및 통제기준

• 컨텐츠, App, 플랫폼, 단말기, 무선통신, 인프라 등의 모바일 보안영역별 상세 보안위협과 예상피해를 분석하여 공통적인 9개의 보안 통제기준 도출하여 대응하도록 구현하였습니다.

구분		위협요소
컨텐츠	사용자 인증	• 비인가 사용자 접근(임직원 사칭) • 인증 우회/사용자 가장 • 인증정보 평문저장 • 악성코드 감염 단말기 인증
	일정/메일 전자결재..	• 첨부파일 저장 • 이해상충부서간 정보교류 • SMS/SNS 위협
App.	악성코드	• 악성코드/스팸 • 다운로드 감염 • 브라우저 취약점
	개발/ 아키텍처	• 스파이웨어, 백도어 등 포함 • 인증우회/유출 • 입력값 검증 부재 • 부적절한 클래스, 메서드 사용 • 예외처리 부재 • 개발 소스 검증 부재
	접근통제	• 비인가 App. 접속
	배포/이력관리	• 설치 및 배포관리 미흡 • 불법 접근 사용자 추적 문제
무선 통신	WIFI	• 비인가 AP • 패킷 스니핑(도청)
	Ad-Hoc	• Ad-Hoc 사용
	Wibro	• 무선신호(Jamming) • 공격자 관리 메시지 변조

구분		위협요소
플랫폼	악성코드	• OS취약점 • 펌웨어 및 플랫폼 위변조
	단말기 인증	• 사용자 부주의 • 단순한 암호(passcode) 사용 • 화면잠금 미설정
	패치,루팅/ 탈옥 관리	• OS 보안패치 관리 미흡 • 루팅/탈옥
단말기	데이터 변조/유출	• 데이터 평문 저장 • 데이터 동기화 • 화면 캡처
	분실/도난	• 분실/도난
	디바이스 통제	• 이동식 저장매체 연결(안드로이드) • GPS 활성화 • 카메라/마이크 기능 활성화 • 무선장치 활성화(블루투스 등) • 데이터 로밍 활성화 • 테더링 사용
	Life Cycle관리	• 퇴직자 관리 부재
인프라	데이터 변조/유출	• 스니핑(도청) • KEMP 직원정보 및 데이터 저장 • 평문 저장
	로깅/모니터링	• 사용자 행위 기록 미흡

통제기준

- 인증(사용자/플랫폼)
- 악성코드
- 개발/아키텍처 보호
- 접근통제 /권한관리
- 데이터 변조 /유출
- 분실/도난
- 디바이스 통제
- 무선통제
- 배포/패치, 로깅/모니터링

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

3. 행안부 KISA 스마트워크 활성화

정보보호 권고 사항 충족도

보안 기준	권고사항	FRAMEPlus4Mobile 보안 적용 내역	충족도
단말기 인증	• 단말기 인증 : 단말기의 이용자별 고유인증키를 서버에서 부여하여 인증수행	• 단말기별 자체 세션 Key(인증 Token발행) 를 통한 인증 및 세션 타임아웃에 따른 자동 로그아웃 기능	●
	• 단말기 인증시 사전/사후 관리 정보 - 단말기 고유번호 - 단말기 사용자 인적관리(성명, 부서명, 사번 등) - 단말기 발급일시 - 단말기 사용목적 및 서비스 내용 - 단말기 네트워크 서비스 현황 - 단말기 운영체계 및 패치 버전	• 데단말기 관리 정보 - 단말기 고유번호 - 단말기 사용자 인적관리(성명, 부서명, 사번) - 단말기 서비스 사용신청 일시 - 단말기 서비스 내역 - 단말기별 접속로그 관리(접속일시, 요청기능, 요청/응답내역 등) - 단말기 운영체계 및 패치 버전 : 요청시 매번 로깅됨	●
이용자 인증	• 모든 사용자는 개인적인 사용만을 위해 유일한 식별자(사용자 ID)를 가져야 하며 사용자의 신원을 확인하기 위해 적절한 인증기법을 선택하여야 한다. • 이 통제는 사용자의 모든 유형(예) 기술지원자, 운영자, 네트워크 관리자, 시스템 프로그래머 및 데이터 베이스 관리자)을 위해 적용하여야 한다. • 사용자 계정(ID)은 책임이 있는 개인의 활동의 추적에 사용되어야 한다. 정규 사용자 활동은 특권을 가진 계정으로 실행되지 않는다.	• 사용자별 로그인 ID관리 및 단말기 관리 및 모바일오피스 Legacy를 통해 ID/Password 방식 또는 SSO(option)를 통해 인증 수행 • Role 정의 및 권한 관리 수행 가능 : 서비스/메뉴별 권한관리 수행 가능 • 서비스 요청별 .로깅 및 정보관리 수행 : 사용자 ID별, 디바이스별, 매 서비스 요청시 접속일시, 요청기능, 요청/응답내역	●
	• 강력한 인증과 신원확인 검증이 요구되는 경우, 암호화 수단, 스마트카드, 토큰, 생체 수단 등을 패스워드에 대한 대안의 인증방법으로 사용하여야 한다	• 공인인증서 등 신원검증 요구시 연동 지원 • AES 128bit / RSA 512bit 암호화 적용 사용자 인증제공, 암호화 API 제공	◐

보안충족도 만족 : ● 보통 : ◐ 미흡 : ○

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

3. 행안부 KISA 스마트워크 활성화

정보보호 권고 사항 충족도

보안 기준	권고사항	FRAMEPlus4Mobile 보안 적용 내역	충족도
통신보안 기능	• 스마트워크 인프라 및 프레임 워크에 접근하기 위해서 사용자 인증, 데이터 암호화 등의 방법 및 절차등이 수립되어야 한다 - 서비스 접근을 위해서는 사용자는 항상 인증을 통해서 엑세스 포인트에 접속할 수 있도록 한다 - 전송되는 데이터의 암호화만 이루어져도 무선랜 구간에서 발생하는 대부분의 해킹을 차단할 수 있으므로, 이에 대한 보안조치가 이루어져 있는지 확인하도록 한다. - 아이디, 비밀번호를 통한 기본 인증 외에 접속권한을 가진 사용자의 MAC(Media Access Control)주소를 등록하여, 지정된 MAC 주소의 랜카드를 장착한 단말기에서만 접속할 수 있도록 제한하여야 한다.	• AES 128bit / RSA 512bit 암호화 적용 사용자 인증(ID/Password)처리 및 단말기 인증관리를 통해 인가된 사용자, 단말기만 접속 가능하도록 복합인증 수행 - 인증 이후 사용자는 단말기별 인증 토큰을 서버에서 발급받아 매 요청시마다 인증 수행 - 모든 전송/수신 컨텐츠는 - 아이디, 비밀번호를 통한 기본 인증 외에 접속권한을 가진 사용자의 MAC(Media Access Control)주소를 등록하여, 지정된 MAC 주소의 랜카드를 장착한 단말기에서만 접속할 수 있도록 제한하여야 한다.	●
	• 모바일 오피스가 무선랜서비스를 제공하고 있는경우 접속 시스템과 액세스 포인트간의 적적한 프로토콜 사용 및 128 bit 이상의 암호화 사용하도록 권장한다.	• 데이터 송수신시 AES 128bit / RSA 512bit 암호화 적용 • 서버 공인 인증서 가반의 SSL 프로토콜 제공(https)	●
단말기내 암호화	• 휴대 단말기내 민감 개인정보, 계좌번호 등이 저장되지 않도록 하여야 한다 • 개인정보 등의 주요정보는 이동저장장치에 별도 보관하고, 필요시 연결 사용하도록 하여야 하며, 특히 주요정보를 휴대단말기에 저장할 수 밖에 없는 경우는, 단말기의 암호화 기능을 활용하여 암호화하여 저장하여야 한다 - 단말기 로그온 정지 - 단말기 저장 데이터 삭제	• 개인 정보 저장 없음 • 아키텍처 구조상 단말기내 데이터 저장없음 • 첨부파일을	●

보안충족도 만족 : ● 보통 : ◐ 미흡 : ○

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

3. 행안부 KISA 스마트워크 활성화

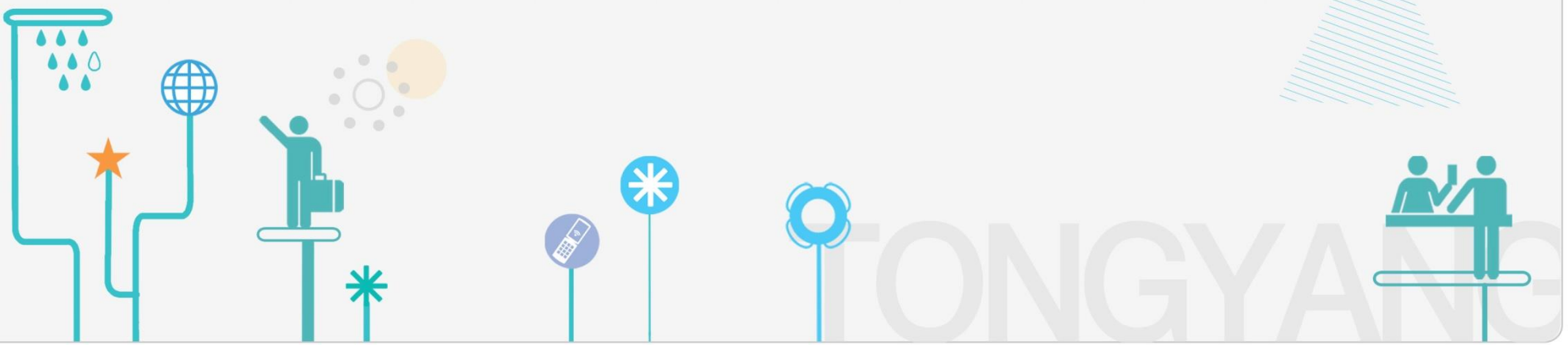
정보보호 권고 사항 충족도

보안 기준	권고사항	FRAMEPlus4Mobile 보안 적용 내역	충족도
악성코드 대응	• 상용 모바일 백신 등 연계를 통해 App실행전 악성코드 검사	• 루팅 및 탈옥폰에서 App이 실행되지 않도록 제어함 • 백신/MDM 연동 가능(3rd-Party 연동이 가능한 개방형 구조)	◐
개발/아키텍처 보호	• 애플리케이션 아키텍처 보안성 검증	• 금감원 보안기준 충족 및 외부 보안업체 검증완료 • 검증된 개발 아키텍처 적용 (FramePlus4)	●
접근통제		• App/컨텐츠 별 접근 통제 및 권한관리 기능 제공 - 관리 콘솔의 설정을 통한 접근 통제 및 권한관리 기능을 제공	●
침해사고 대응절차 마련 및 데이터 변조/유출 방지	• 콘텐츠 보안으로 이기종 단말기 간에 호환이 되는 DRM 및 데이터 암호화 등의 콘텐츠 보호 조치 요구 • 스마트워크에 활용되는 PC 및 휴대단말기는 분실 및 도난 발생시 제 3자의 데이터 접근을 차단해야 한다 • 분실 단말기의 기능을 정지시키기 위한 원격제어 기술을 고려요구 - 원격지에서 일부 및 전체 기능정지 - 단말기 로그온 정지 - 단말기 저장 데이터 삭제	• 송/수신 데이터의 암호화 기능 제공(AES 128bit / RSA 512bit) - 암호화 설정에 따른 구간 암호화 제공 - 부분 암호화를 위한 암호화 API 제공 • 보안을 고려하여 단말기에 업무데이터를 저장하지 않음 • 단말기 관리기능을 통해 분실시 즉시 해당 단말기 접속 차단이 가능함 - 원격지에서 단말제어는 MDM(3rd-Party) 연동을 통해 가능 - 단말기별 접속 차단 기능 제공 - 단말기에 데이터 저장 없음	●

보안충족도 만족 : ● 보통 : ◐ 미흡 : ○

Copyright© 2013 TONGYANG Networks Co.,Ltd. All rights reserved

Thank You



동양네트웍스(주)

