(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0068251
(43) 공개일자 2017년06월19일

(51) 국제특허분류(Int. Cl.)
H04W 12/08 (2009.01) *H04L 9/32* (2006.01)
H04W 12/04 (2009.01) *H04W 12/06* (2009.01)
(52) CPC특허분류
H04W 12/08 (2013.01)
H04L 9/0825 (2013.01)
(21) 출원번호 10-2015-0175221
(22) 출원일자 2015년12월09일
심사청구일자 없음

(71) 출원인
송지훈
경기도 성남시 분당구 효자길 13 (서현동)
(72) 발명자
송지훈
경기도 성남시 분당구 효자길 13 (서현동)

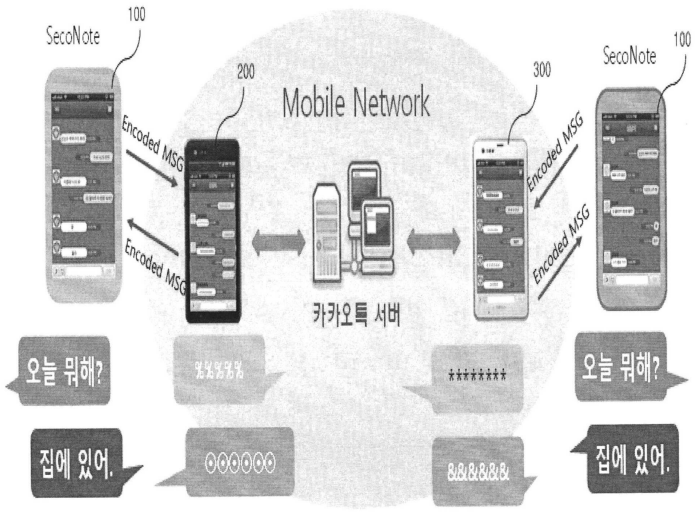
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 **보안 단말기**

(57) 요 약

본 발명은 암호화 대화내용이나 개인정보를 스마트폰으로부터 수신하여 해독하고 해독한 대화 내용을 화면상에 표시하는 보안 단말기에 관한 것이다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0861 (2013.01)
H04L 9/30 (2013.01)
H04L 9/3226 (2013.01)
H04W 12/04 (2013.01)
H04W 12/06 (2013.01)

명 세 서

청구범위

청구항 1

암호화 대화내용이나 개인정보를 스마트폰으로부터 수신하여 해독하고 해독한 대화 내용을 화면상에 표시하는 보안 단말기.

발명의 설명

기 술 분 야

[0001] 본 발명은 휴대폰이나 노트북 또는 테블릿 PC 등의 스마트폰을 이용한 대화 내용을 해독하는 보안 단말기에 관한 것이다.

배 경 기 술

[0002] 최근 도청 및 해킹 기술 발달로 휴대폰에 스파이웨어를 심어 스마트폰에 저장된 정보와 대화내용 및 도청을 하는 사례가 증가하고 있고, 공권력에 의한 문자대화 내용이 저장된 서버의 압수수색 등이 증가하고 있다. 이런 경우 휴대폰만 보안을 강화해서는 해결할 수 없으며, 모바일 OS 자체의 보안취약성으로 소프트웨어적으로 해결할 수 없다. 이런 이유로 개인간 통신의 비밀보장이 현실적으로 불가능한 실정이다.

발명의 내용

해결하려는 과제

[0003] 본 발명이 해결하고자 하는 과제는 휴대폰이나 노트북 또는 테블릿 PC 등의 스마트폰을 이용한 대화 내용을 해독하는 보안 단말기를 제공하는 것이다.

[0004] 상기 과제 이외에도 구체적으로 언급되지 않은 다른 과제를 달성하는 데 본 발명에 따른 실시예가 사용될 수 있다.

과제의 해결 수단

[0005] 상기 과제를 해결하기 위한 본 발명의 하나의 실시 예는 암호화 대화내용이나 개인정보를 스마트폰으로부터 수신하여 해독하고 해독한 대화 내용을 화면상에 표시하는 보안 단말기를 제공한다.

발명의 효과

[0006] 본 발명의 하나의 실시예에 따르면 스마트폰에 암호화되어 표시된 대화내용이나 개인정보를 별도로 해독하고 표시함으로써 도청 및 해킹을 방지할 수 있게 한다.

도면의 간단한 설명

[0007] 도 1은 본 발명의 하나의 실시예에 따른 보안 단말기의 사용 예를 보인 도면이다.

도 2는 본 발명의 다른 하나의 실시예에 따른 보안 단말기의 사용 예를 보인 도면이다.

도 3은 본 발명의 하나의 실시예에 따른 보안 단말기의 블록 구성도이다.

도 4는 본 발명의 하나의 실시예에 따른 보안 단말기의 보안키 사용 예를 보인 도면이다.

도 5는 본 발명의 하나의 실시예에 따른 보안 단말기의 동작을 보인 순서도이다.

도 6은 본 발명의 다른 하나의 실시예에 따른 보안 단말기의 동작을 보인 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0008] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대해 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며 명세서 전체에서 동일 또는 유사한 구성요소에 대해서는 동일한 도면부호가 사용되었다. 또한, 널리 알려져 있는 공지기술의 경우 그 구체적인 설명은 생략한다.

[0009] 본 명세서에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "…부", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0010] 도 1은 본 발명의 하나의 실시예에 따른 보안 단말기의 사용 예를 보인 도면으로, 일반 스마트폰(200, 300) 간에 카카오톡을 통해 문자 대화하는 경우를 보이고 있다.

[0011] 도 1에 도시된 바와 같이 일반 스마트폰(200, 300)의 통신 구간에는 암호화된 문자대화 메시지만 전달되고, 암호화된 문자대화 메시지는 그대로 화면상에 표시된다. 이에 따라 일반 스마트폰(200, 300)의 화면에는 대화 내용이 암호화처리되어 표시됨에 따라 육안으로 식별하지 못하는 기호나 문자, 이모티콘 등으로 표시된다.

[0012] 보안 단말기(100)는 일반 스마트폰(200 또는 300)과 유선 또는 무선으로 통신을 하여 일반 스마트폰으로부터 암호화된 문자대화 내용을 수신한다. 그리고 보안 단말기(100)는 암호화된 문자대화 내용을 복호화하고 복호화한 문자대화 내용을 화면상에 표시한다. 화면상에 표시되는 복호화된 대화 내용은 육안으로 내용 파악이 가능한 글자나 그림 등으로 표시된다.

[0013] 한편, 카카오톡 서버 등과 같은 채팅앱 서버에도 암호화된 대화 메시지가 저장된다.

[0014] 도 2는 본 발명의 다른 하나의 실시예에 따른 보안 단말기의 사용 예를 보인 도면으로, 일반 스마트폰(200, 300) 간에 카카오톡을 통해 음성 대화하는 경우를 보이고 있다.

[0015] 도 2에 도시된 바와 같이 일반 스마트폰(200, 300)의 통신 구간에는 암호화된 음성대화 메시지만 전달되고, 암호화된 음성대화 메시지는 그대로 스피커로 출력된다. 이에 따라 일반 스마트폰(200, 300)의 화면에는 대화 내용이 암호화처리되어 출력됨에 따라 이해할 수 없는 내용으로 들리게 된다.

[0016] 보안 단말기(100)는 일반 스마트폰(200 또는 300)과 유선 또는 무선으로 통신을 하여 일반 스마트폰으로부터 암호화된 음성대화 내용을 수신한다. 그리고 보안 단말기(100)는 암호화된 음성대화 내용을 복호화하고 복호화한 음성대화 내용을 스피커를 통해 출력한다. 스피커로 출력되는 복호화된 음성대화 내용은 사람이 이해할 수 있는 언어로 출력된다.

[0017] 이상과 같이 문자 또는 음성을 별도의 보안 단말기를 통해 복호화함에 따라 스마트폰의 통신 구간이나 스마트폰을 해킹하더라도 암호화된 문자 또는 음성만이 유출된다.

[0018] 도 3은 본 발명의 하나의 실시예에 따른 보안 단말기의 블록 구성도이다. 도 3에 도시된 보안 단말기의 구성은 다음의 내용을 기반으로 설계된 것이다.

[0019] 먼저 보안성을 높이기 위해 공개키/비밀키(비대칭키) 방식으로 암호화/복호화한다. 암호화는 공개키로 암호화하고, 복호화는 각 단말기에 하드코드 형태로 저장되어 있는 비밀키(개인키)로 복호화한다.

[0020] 키교환 방법은 암호화서버를 운영하여 암호화서버를 통해 키교환을 하게 하거나, 직접교환 방법을 통해서 한다.

[0021] 즉, 암호화서버운영 방법은 공인인증서와 유사함,각자의 공개키를 서버에 등록하여, 통신이 필요한 상대방이 서버에서 상대방의 공개키를 획득하여 메시지를 암호화한다. 그리고 직접교환 방법은 암호화가 필요한 두 당사자가 직접 단말기를 가지고 만나서, NFC,블루투스, 유선연결로 직접 단말기를 1:1로 연결하여 각자의 공개키를 상호 교환한다.

[0022] 도 4는 본 발명의 하나의 실시예에 따른 보안 단말기의 보안키 사용 예를 보인 도면이다. 도 4에 도시된 키교환 방법은 암호화서버운영 방법이다. 도 4에 도시된 바와 같이, A가 B와 통신하기 위해서 A의 ID를 가지고 인증서버에 미리 등록된 B의 공개키를 요청한다. 그리고 인증서버는 A의 ID를 확인한 후 B의 공개키를 A에게 전달한다. 이에 따라 공개키는 유출되어도 비밀키(개인키)를 알지 못하면 암호화된 메시지를 풀지 못하게 된다.

[0023] 도 5는 본 발명의 하나의 실시예에 따른 보안 단말기의 동작을 보인 순서도이다. 도 5에 도시된 바와 같이 A와

B의 ID 및 공개키는 인증서버에 미리 저장된다. 그리고 블루투스 연결 요청은 앱(App)->비화단말, 비화단말->앱(App) 모두 가능하다. 스마트폰 메신저 화면에는 암호화된 의미없는 문자가 표시된다.

[0024] 도 6은 본 발명의 다른 하나의 실시예에 따른 보안 단말기의 동작을 보인 순서도이다. 도 6에 도시된 바와 같이 A와 B의 ID 및 공개키는 인증서버에 미리 저장된다. 블루투스 연결 요청은 App->비화단말, 비화단말->App 모두 가능하다. 스마트폰으로 전달되는 음성은 암호화된 음성신호로 의미를 알 수 없는 소리이다.

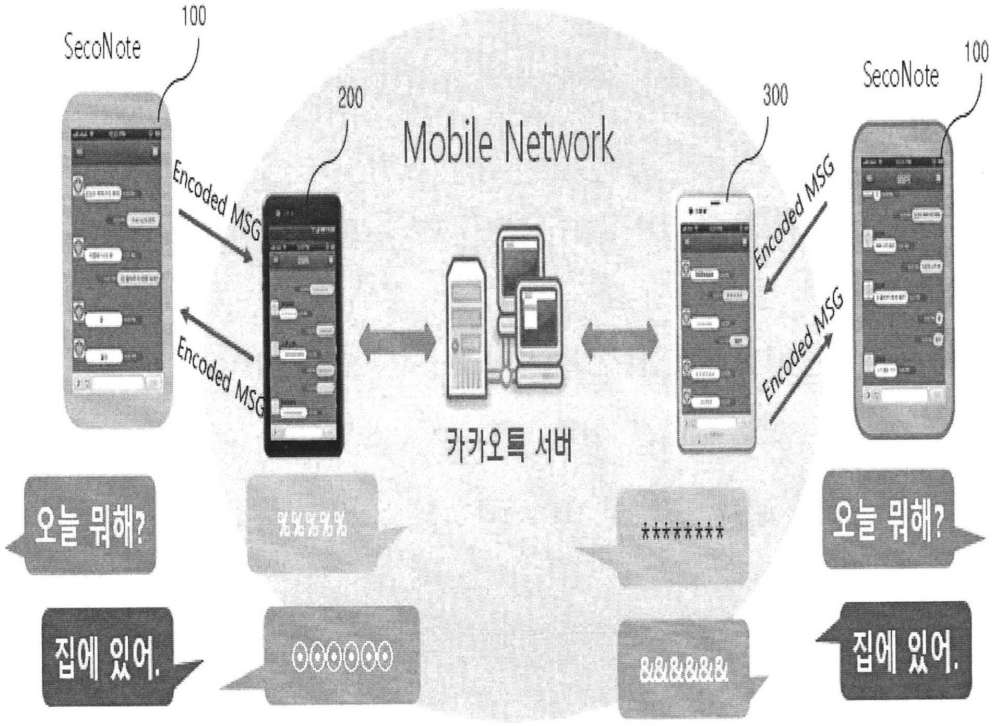
[0025] 이상에서 본 발명의 실시에에 대하여 상세하게 설명하였으나, 본 발명의 권리범위가 이에 한정되는 것은 아니며 본 발명이 속하는 분야에서 통상의 지식을 가진 자가 여러 가지로 변형 및 개량한 형태 또한 본 발명의 권리범위에 속한다.

부호의 설명

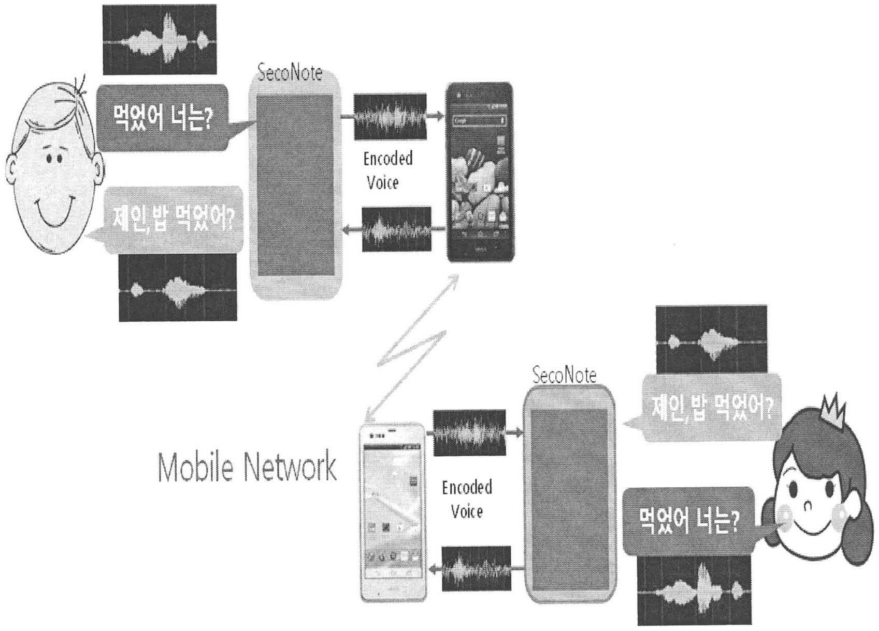
[0026] 100 : 보안 단말기

도면

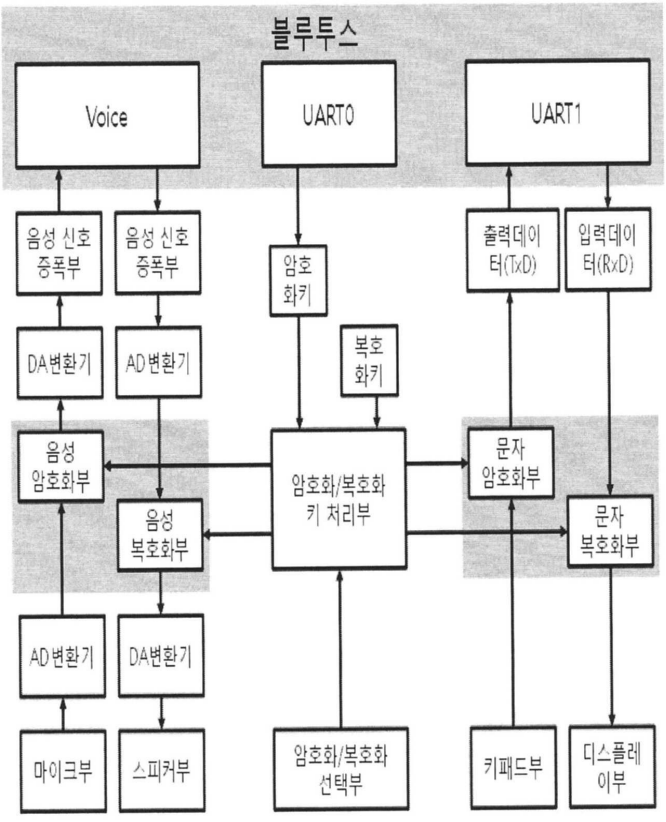
도면1



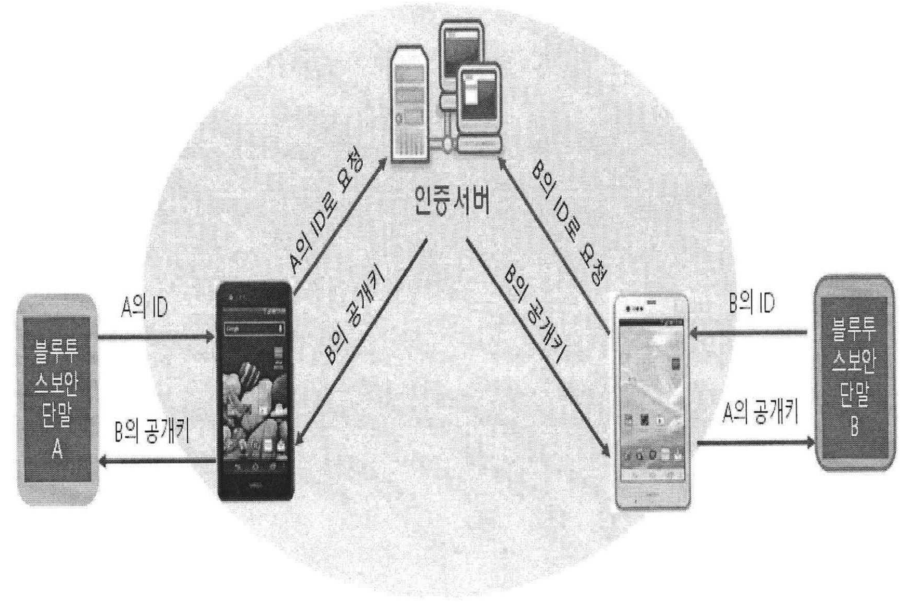
도면2


SecoNote
먹었어 너는?
제인,밥 먹었어?
Encoded
Voice
Mobile Network
SecoNote
제인,밥 먹었어?
Encoded
Voice
먹었어 너는?

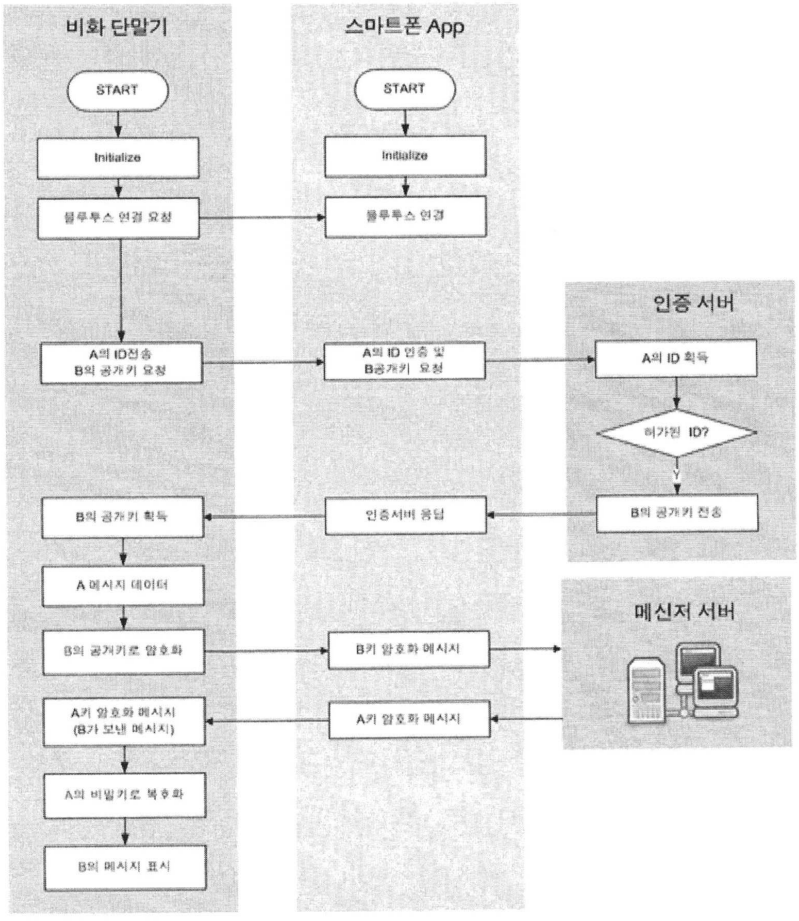
도면3


블루투스
Voice
UART0
UART1
음성 신호 증폭부
음성 신호 증폭부
암호 화키
출력데이터(TxD)
입력데이터(RxD)
DA변환기
AD변환기
복호 화키
음성 암호화부
암호화/복호화 키 처리부
문자 암호화부
음성 복호화부
문자 복호화부
AD변환기
DA변환기
마이크부
스피커부
암호화/복호화 선택부
키패드부
디스플레이부

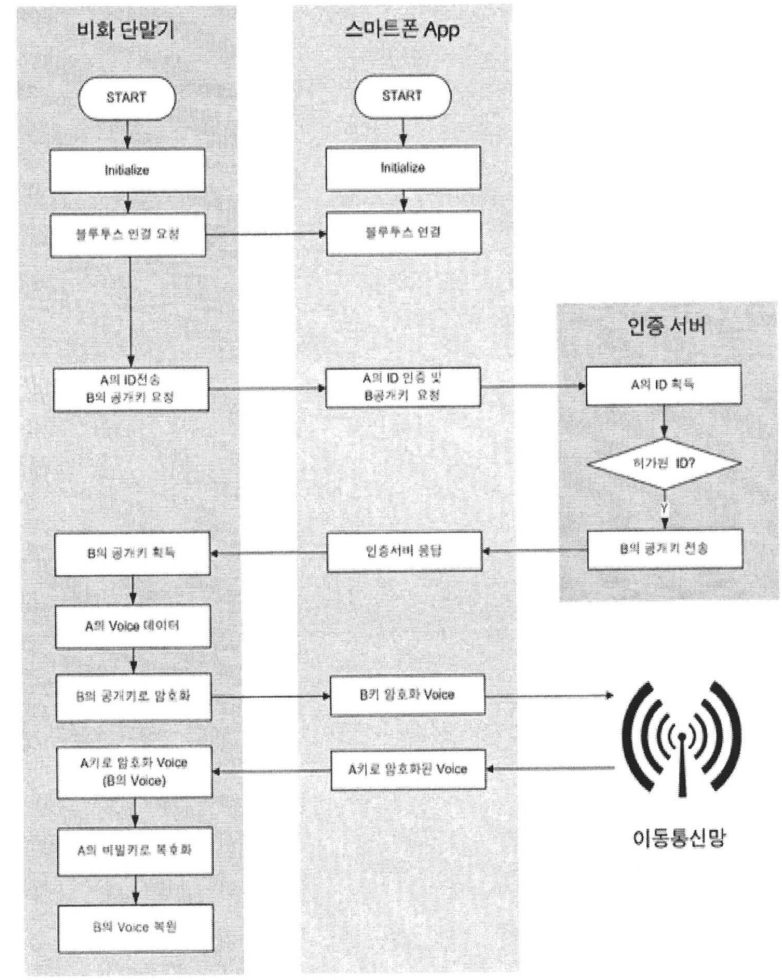
도면4


인증서버
A의 ID로 요청
B의 공개키
B의 ID로 요청
B의 공개키
블루투스 보안 단말 A
A의 ID
B의 공개키
B의 ID
A의 공개키
블루투스 보안 단말 B

도면5


비화 단말기
스마트폰 App
인증 서버
메신저 서버
START
Initialize
블루투스 연결 요청
블루투스 연결
A의 ID전송
B의 공개키 요청
A의 ID 인증 및
B공개키 요청
A의 ID 획득
허가된 ID?
Y
B의 공개키 획득
인증서버 응답
B의 공개키 전송
A 메시지 데이터
B의 공개키로 암호화
B키 암호화 메시지
A키 암호화 메시지
(B가 보낸 메시지)
A키 암호화 메시지
A의 비밀키로 복호화
B의 메시지 표시

도면6


비화 단말기
스마트폰 App
인증 서버
START
Initialize
블루투스 연결 요청
블루투스 연결
A의 ID전송
B의 공개키 요청
A의 ID 인증 및
B공개키 요청
A의 ID 획득
허가된 ID?
Y
B의 공개키 전송
인증서버 응답
B의 공개키 획득
A의 Voice 데이터
B의 공개키로 암호화
B키 암호화 Voice
A키로 암호화 Voice
(B의 Voice)
A키로 암호화된 Voice
A의 비밀키로 복호화
B의 Voice 복원
이동통신망