Smart Security Innovation!

A good partner for smart devices security solutions

Extrus Company Profile

www.extrus.co.kr

MOBILE
TOTAL
SOLUTION

ExTrus
Extreme Trust

ExTrus
Extreme Trust

CONTENTS

ExTrus
Extreme Trust

1. Extrus Introduction

1.1 Overview

Name	Extrus Inc.
CEO & Founder	Jung, Kyung Su
Establishment	2009, October
Capital	KRW 1,000 Million (about USD 1 million)
Major products	Mobile & Security solutions (Exafe MDM, Exafe AppDefence, Exafe KeySec, Exafe mPKI, TrusAP, and others)
Website	https://www.extrus.co.kr (☎ +82-2-6928-6774)

ExTrus
Extreme Trust

1.2 Business Areas

Mobile Security solutions

- MDM, AppDefence, KeySec, E2E
- Vaccine for Mobile OS
- Firewall for Mobile OS

EXAFE **MDM**™
EXAFE **KeySec**™
EXAFE **AppDefence**™
EXAFE **AppCodex**™
EXAFE **Vaccine**™
EXAFE **XCapture**™
EXAFE **mPKI**™
EXAFE **FaceAuth**™
TrusAP™

Business Areas

Mobile Security Solutions

Fintech solutions

Financial SI & Consulting

Fintech solutions

- Developed various solutions for Fintech
- User verification with face recognition for financial transactions
- Developed the Fintech open platform based on OAuth2.0

EXAFE **FaceAuth**
EXAFE **Auth**

Financial SI & consulting

- Financial SI projects and consulting
- Fintech
- Samsung Life Insurance,
- Samsung Fire & Marine insurance,
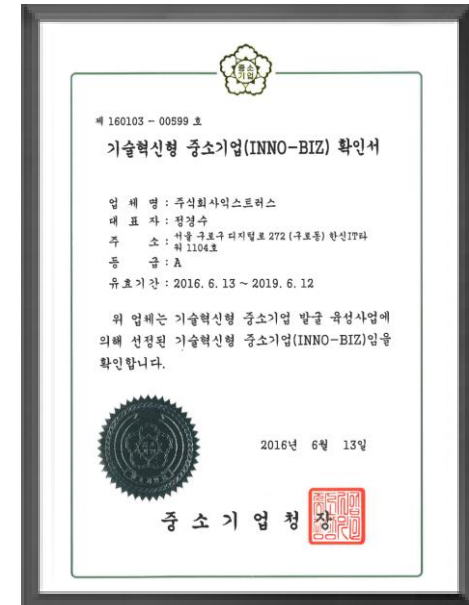- SBI savings bank
- FirstData (PG/Van)

1.3 Patents and Certificates

Acquired the venture business certificate

Recognized R&D Centre

INNO-BIZ

1.3 Patents and Certifications

Patents

❑ **Registered Patent**
- **Security and Access Controlling Device for Mobile Terminal and Financial trading method using the same**
- **Smishing Blocking Apparatus on Cloud Mobile Environments**

❑ **Applied Patents**
- **Apparatus and Method for Controlling Permission for an Application Using Reputation Information**
- **Method for Dynamic Modules Authentication and secure integrity**
- **System and Method for prevention of avoiding emulator analyzing for dynamic analysis**
- **Method for guaranteeing integrity and strengthening security using Block chain in app forgery detection**

SW certificates

NIS Certifications
(National Intelligence Service)

❑ **Obtained NIS's EAL2 CC certificate (Exafe MDM v4.5)**

❑ **NIS cryptography verification module CM -65- 2017.12 Exafe Crypto v 1.0**

❑ **GS certificates**

  GS Verification: 13-0105

  Company Name: Extrus

  Product Name: Exafe MDM v4.0

1.4 Major Customers - Government & Public enterprises

1.4 Major Customers - **General enterprises**

ExTrus
Extreme Trust

1.4 Major Customers - **Financial companies**

2. Exafe Solutions

ExTrus
Extreme Trust

2.1 Exafe Solutions

Mobile Security

Exafe MDM	• Mobile Device Management product for prevention of information leakage through mobile device, and asset management • Developed and applied MCM (Mobile contents management)	NIS's CC certificate GS certificate
Exafe KeySec, E2E	• Using security keypad, protect input data of personal information • Combined with E2E solution, support encryption of transmitted data. • Developed the next generation V2.0	
Exafe AppDefence	• Prevents from malicious code threats and protect personal information. • Developed the next generation V2.0	
Exafe mPKI	• Product for a construction of mobile-based PKI system • Provide public certification management, E2E, and keypad security	
Exafe Vaccine	• Detect mobile malignant code, real time monitoring, and prevention of OS forgery	
Exafe AppCodex	• is a code obfuscation solution and protects mobile apps against hacking threats by reverse engineering.	
TrusAP	• is a Security wireless AP(Access Point). • Security functions : OTA(One Time Authentication), SSL VPN, Blocking Harmful Websites.	

Fintech solutions

Exafe FaceAuth	• User authentication technology base on face recognition • Compatible with FIDO technology • The leading payment service provider, KG INICIS will apply it to K-Pay	FIDO UAF Ready
Exafe Auth	• Authentication solution based on OAuth 2.0 (M2M, Client to Server, Server to Server) • Applied to NH bank's Fintech open platform	Applied to Fintech open platform authentication

EXTrus Extreme Trust

2.2 Mobile security solutions

EXAFE MDM™

Exafe MDM provides a safe mobile environment and prevents information leakage by malignant application, data leakage through devices, and security accidents via network.
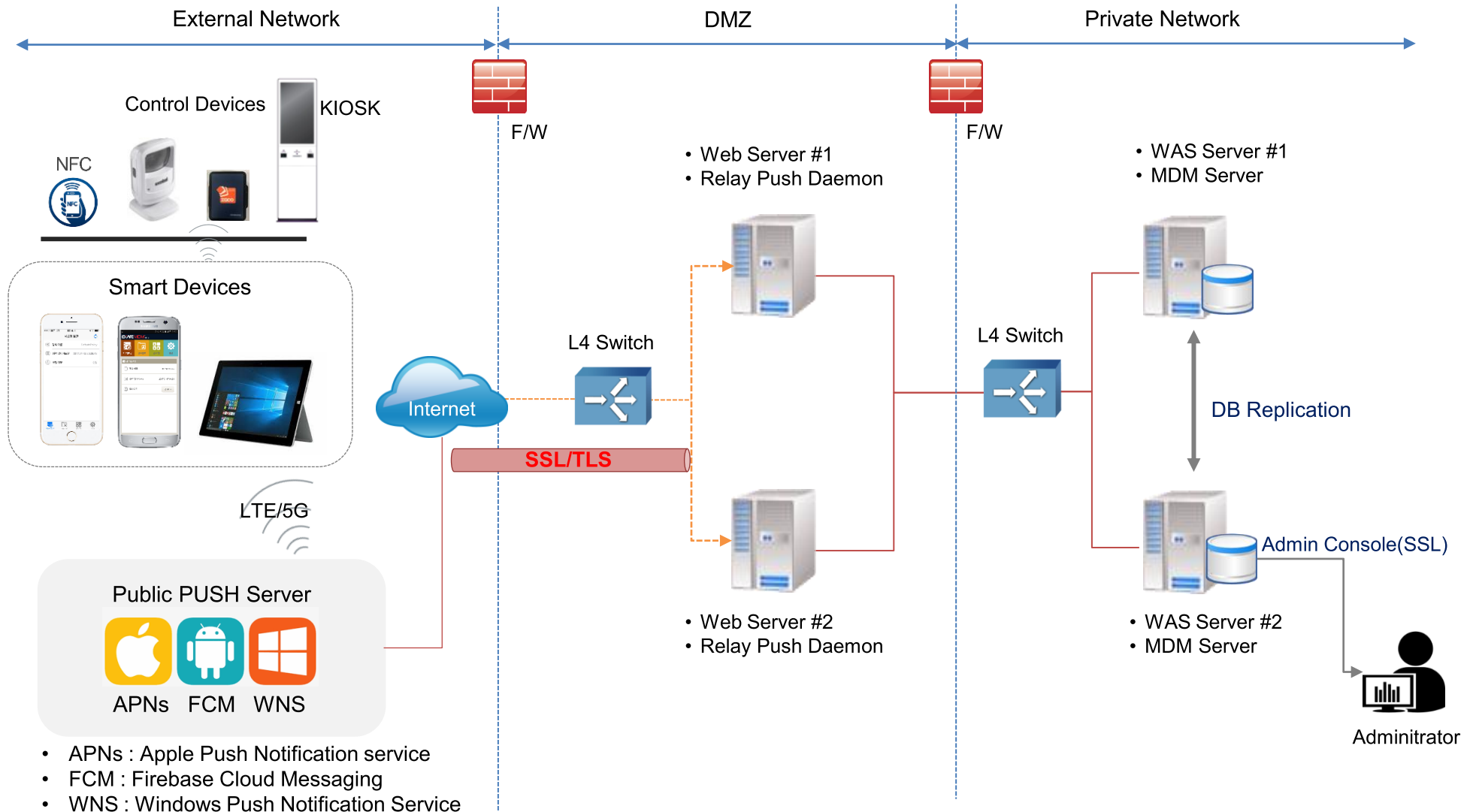
- ● **Mobile Device Management and Security**
- ● **Essential Mobile App Distribution (OTA-based Distribution Management)**
- ● **Smart Device Theft and Loss Management**
- ● **Smart Device Asset Management**
- ● **Android, iOS, Windows support (Tablet PC, Smartphone)**
- ● **Smart Device Location Tracking**

Category	Major features
Policy Server	• Exafe MDM S/W Manager - Device Management Policy Creation and Management for various Platforms - Information Backup/Recovery for Loss Management - Remote Command Transmission &History Management for Device Remote Management - Audit Log Management for audit - Self-Push Server & SMS Push Method for Remote Control
Administrator Console	• Exafe MDM Admin Console - Centralized Device Management - Security Policy Creation &Management (Policy Management) based on Group or Conditions - Smart Device Usage Status Management - Device Management with Remote Control - Theft and Loss Management, Mobile Office App Management - User/Organization/Administrator Information Management
Smart Device Agent	• Exafe MDM Agent - Android, iOS Smart Device Platform Support - Support MS **Window OS – the sole provider in Korea** - Theft and Loss Management - Information Backup/Recovery/Delete, Factory Initialization, - Device Location Information - Security Policy Reception & Execution (Device Use Control) - Corporate Mobile Office App Store Management - Log Creation & Transmission

2.2 Mobile security solutions – Service Architecture   EXAFE MDM™

External Network | DMZ | Private Network

External Network

Control Devices   KIOSK

NFC

Smart Devices

LTE/5G

Public PUSH Server

APNs   FCM   WNS

- APNs : Apple Push Notification service
- FCM : Firebase Cloud Messaging
- WNS : Windows Push Notification Service

Internet

SSL/TLS

DMZ

F/W

L4 Switch

- Web Server #1
- Relay Push Daemon

- Web Server #2
- Relay Push Daemon

Private Network

F/W

L4 Switch

- WAS Server #1
- MDM Server

DB Replication

Admin Console(SSL)

- WAS Server #2
- MDM Server

Administrator

- 출입관리 Groupware Server

ExTrus
Extreme Trust

2.2 Mobile security solutions – Application Cases **EXAFE MDM**™

Prevention of information leakage

- Information leakage through smart device camera, voice recording, screen capture, WiFi/Bluetooth, etc.
- Policy control using location information(GPS), Speed-gate and NFC/RFID tagging.
- Location tracking and device locking, remote wipe or factory reset, etc.

Prevention of National information leakage

- Control smart device of general soldiers to prevent leakage of military secrets through cameras.
- Track the location or movement of patrolling police officers and patrol cars.
- Prevention of leakage of military secrets through cameras in submarines and ships
- Collect health and body information of soldiers through smart watch

National Infrastructure Management System

- Traffic priority signal system for emergency vehicles (ambulance, fire engine, police car, etc.).
- Home gas remote meter reading system.
- National waterworks integrated management system.
- Structure remote inspection system through wearable camera.

Target Institution

- **General enterprises**
- **R&D center**
- **Governments & Public enterprise**
- **Financial companies**

- **National Police Agency**
- **Department of Defense**
- **Army, Navy, Air force Unit**
- **National Defense Research Institute**

- **Local Government Unit**
- **Fuel Supply Compay**
- **Water supply management institution**

ExTrus
Extreme Trust

2.2 Mobile security solutions

EXAFE mPKI Suit

Using electronic signature and virtual keypad, Exafe mPKI Suite prevents data leakage when a smart device needs user verification and input of important information. Combined with E2E solution, it also supports encryption of transmitted data.

mPKI™
+
KeySec™
+
E2E™

Smart device

- Linked to electronic signature
- Linked to security keypad for a important input data

HTTPS / SSL

- E2E data security : symmetric key coded algorithm ARIA (128/256 bit) / SEED (128 bit)
- Section security by using SSL(TLS1.0)

Security server

- Use Exafe mPKI toolkit API for web-based service
- Verify Electronic signature, decode input data of security keypad, decode/ code of E2E security

Electronic signature and identification
Corresponds to KSA verification system

Guarantee integrity
Provides various algorithms for authentication certificate

Guarantee confidentiality of transmitted/ received data
Provides various password decode methods

※ mPKI: mobile public key infrastructure

ExTrus
Extreme Trust

2.2 Mobile security solutions

EXAFE Application Protection Suit

Exafe Application Protection Suite consists of prevention of app forgery, blocking black list based malignant code, and white list based firewall solutions. It support trustworthy working environment by preserving App and OS.

AppDefence™ + Vaccine™ + Wall™

EXAFE AppDefence™

EXAFE AppDefence prevents to malicious code threats and protect personal information.
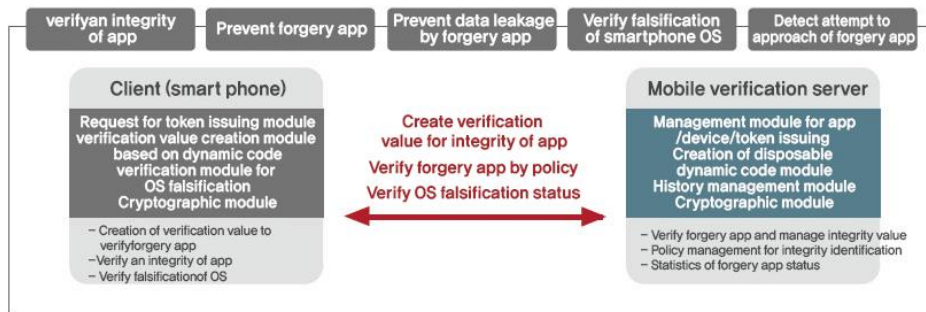
EXAFE Vaccine™

EXAFE Vaccine is an anti-malware solution for smart devices. It prevents possible threats from unauthorized programs and malignant code.

EXAFE Wall™

EXAFE Wall is a firewall protection for smart devices. Furthermore, by reading patterns it blocks dangerous apps and security treats.

ExTrus
Extreme Trust
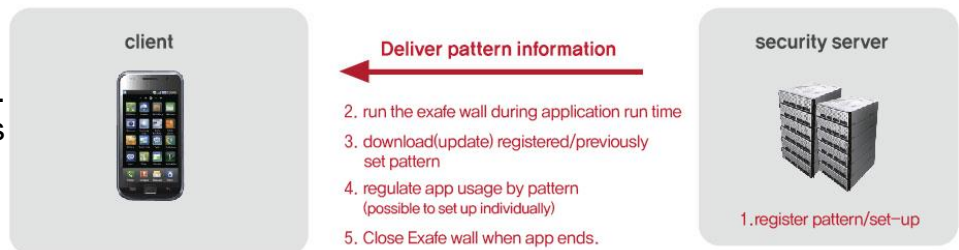
2.2 Mobile security solutions
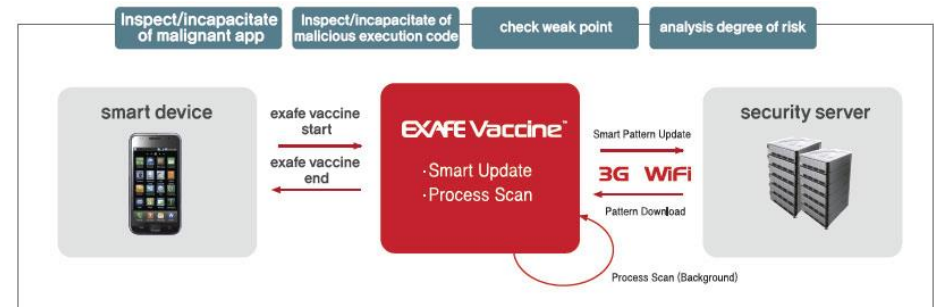
EXAFE AppCodex™

Exafe AppCodex is a binary code obfuscation solution and protects Mobile apps against hacking threats by reverse engineering.

It is simple and powerful mobile apps security solution that code obfuscation is applied to uploaded APK binary.

SCAN
Scans vulnerabilities of mobile apps

PROTECT
Obfuscation / encryption in binary level

TRACK
Detects tampering / hacking and monitoring

1등급
GOOD Software

Financial / Game / Enterprises / SNS / Health care / e-commerce / Digital media / public

ExTrus
Extreme Trust

2.3 Network security solution

TrusAP™

Through the establishment of a TrusAP-based wireless LAN security system, it is possible to increase the efficiency of work and smart life, such as strengthening authentication of the wireless work environment, improving security, improving performance, and managing functions.

[Trough Strengthening WirelessLAN security and providing convenience]

Increase Work and Smart life efficiency

WirelessLAN Security System

Strong Authentication

- WPA2,3 + PSK + OTA
  - **OTA(One-Time Authentication)**
- Support 3rd Party Authentication
  - Support FIDO-based biometric authentication
  - X.509v3-based PKI authentication, etc.

Increase Security

- Support TLS 1.2/1.3
- Provide **SSL VPN(Encryption channel) function**
- Provide HSM token function for console access
- Provide Embedded key management function

TrusAP™

Improve Performance

- Support Wi-Fi Certified 6
- Provide EasyMesh function
- Embedded Chip to improve encryption/decryption performance

Management Function

- Wireless terminal device registration & approval process
- **Blocking Harmful Websites**
- Real-time AP integrated control function

2.3 Network Security Solution

TrusAP™

The TrusAP solution is composed of TrusAP Server (authentication and AP management), Access Point (TA Series), and TrusAP Client. Through the client's device authentication request, a VPN security channel is configured to provide services.

TrusAP Server

OTA Auth. & Approval

TrusAP Client

- **Notebook / TabletPC**
- **Smart Device**
- **Wireless Printer**
  - •
  - •

BackBone

Firewall

L3 Switch

L2 Switch

AP (TA Series)

VPN Tunnel

2.4 Exafe solution strengths

ExTrus
Extreme Trust

Performance
- ✓ **R&D and sales experts in Fintech and mobile security**
- ✓ **Solutions for** Government, banks and digital payments **can be adopted promptly**
- ✓ **Professionals experienced various financial SI projects**
- ✓ **Provide ASP service for small and medium enterprises**

Line-up
- ✓ **Provide** comprehensive mobile & Network security solution
- ✓ **Easy to integrate into various Fintech solutions due to experience of accumulated financial SI projects**
- ✓ **Support** various mobile platform **- Android, iOS, Windows (the first and sole provider in Korea)** **EXAFE FaceAuth** fido Ready
- ✓ **Fintech authentication technology which is compatible with FIDO**
- ✓ **Fintech open platform authentication technology which is compatible with OAuth 2.0** **EXAFEAuth** ②

Core
- ✓ **Cryptography module is certified by NSRI (Korean National Security Research Institute)**
- ✓ **Consist of modularized functions based** on security framework
  - ➔ **prompt support for various customers' needs**

Thank you.

123, Digital-ro 26Gil, Guro-gu, Seoul, South Korea ☎ +82-2-6928-6774

ⓔ-mail : sales@extrus.co.kr