AirCUVE

• Multi-Factor Authentication

• Wireless (Wi-Fi) Authentication

2017
AirCUVE Introduce

✓ 15 years Expertise
  - Established in 2002

✓ Network Device Authentication Solution
  - Wired / Wireless consolidated Auth.
  - Multi Factor Auth.
  - VPN, WEB authentication

✓ Excellent Inter-Operability with Network Equipment
  - Good Inter-Operability with various AP, Switch, WIPS.

✓ Proven Quality with over 700+ Customer
  - Meet customer requirement
  - Prompt customer service
AirCUVE Introduce - Reference

- Expertise with Major Telcos: SKT, KT, LG U+
- Global Clients: 760 Reference including SAMSUNG, LG, Hyundai.
- Proven Reference for Key Industries

<table>
<thead>
<tr>
<th>760 Reference</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>336</td>
</tr>
<tr>
<td>Enterprise</td>
<td>245</td>
</tr>
<tr>
<td>School</td>
<td>130</td>
</tr>
<tr>
<td>Hospital</td>
<td>17</td>
</tr>
<tr>
<td>Banks, Insurance</td>
<td>22</td>
</tr>
<tr>
<td>Military</td>
<td>10</td>
</tr>
<tr>
<td>Patent</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Authenticate system Detailed log treatment process</td>
<td></td>
</tr>
<tr>
<td>Wired/wireless network quarantine and policy based network access</td>
<td></td>
</tr>
<tr>
<td>Wireless network security control equipment (WIPS related patent)</td>
<td></td>
</tr>
<tr>
<td>Private IP based - Remote device control using SIP</td>
<td></td>
</tr>
<tr>
<td>Multi-Factor authentication</td>
<td></td>
</tr>
<tr>
<td>Location based Security control for high mobility device</td>
<td></td>
</tr>
</tbody>
</table>
AirCUVE Introduce - Main Products

**AirCUVE**

**V-FRONT**
Multi-Factor Authentication
(Mobile OTP, PKI)

**AirFRONT**
WLAN(Wi-Fi) Authentication
Multi Factor Authentication
(2 FA)
V-FRONT
One Factor Authentication is not good enough for your security control

V-FRONT is Multi-Factor Authentication Platform.
V-FRONT Need & Benefit

Need

- ID BASED Authentication cause many Network Security Accident.
- High DEMAND on Multi-Factor Stronger Authentication for VPN Access, Web server, VDI, Device Management, Banking Service

Benefit

  - CA, OTP, QR Code, Finger Printing
- More RELIABLE Authentication with Multi-Channel Authentication.
  - Separate Service CH. From Authentication CH.
V-FRONT Overview

V-FRONT strengthens Web server, VPN, Network access authentication

- Base VPN device
- RADIUS Standard Protocol
- OTP, SMS Strong 2Factor Authentication

- Supports ODBC such as Oracle/Active Directory/LDAP
- Multiple types of DB support

- Telnet Login
- Server Access (Linux/Unix based RADIUS account interface)
- Network switch
- RAIDUS Proxy role

- Existing mail server, groupware
- Provides standard API
- OTP, SMS Strong 2Factor Authentication system
Multi-Factor Authentication - Configuration

1st: OTP Key request (ID/PW need)

2nd: ID+OTP PW Authentication

3rd: Web Server (Mail, Groupware etc.)

User

OTP Key creation Request for using mobile OTP Application

Authentication Server

Corporate Employee DB Server

Network diagram

Switch

Internet

Web Server (Mail, Groupware)

Employee DB Server

SMS Server

Authentication Server
V-FRONT Architecture

- V-FRONT offers Various IT Service

**VPN Interface**

- Groupware Interface
- VDI Interface
- Server access control
- SSO Interface
- Network Equipment
- Mail Solution
- Account Management
We can support multiple authentication token.

Authentication Platform Business

(Platform name is V-FRONT)
2 Factor Authentication Process

Activate personal policy by sending group policy attribute values with authentication success message to the VPN device depending on product’s function.
V-FRONT Solution Reference

- Portal Service: Naver (Line)
- Insurance Company: Samsung Insurance
- TV Broadcasting center: KBS
- Electronic Company: Samsung
V-FRONT Solution Reference

1st Authenticate

ID

PW

✓ Enter  Cancel

2nd Authenticate Selection

- QRCord
- OTP
- SMS  010-9099-9724
- E-mail  abc@naver.com

✓ Enter  Cancel

2nd Authenticate

OTP Choice

ID  aircuve
PW  ********
2nd Authenticate  102569874

✓ Enter  Cancel

Network Access connected.
1. Access to SSL VPN login page.
Enter your ID / Password and click the “Sign in” button.

Example: VPN Login

Welcome to the Junos Pulse Secure Access Service

Username
Password

Please sign in to begin your secure session.
Example: VPN Login

2. Enter OTP code created by AirOTP. And then click the “Sign in” button.

[VPN Login Page - Enter OTP]
Example: VPN Login

You completed to access “SSL VPN”.

[VPN Login Page – Login Success]
V-FRONT Monitoring

System status
- AAA Process: on
- MariaDB: on
- OCSPD: on
- DBMS Process: off
- Fallback Process: off

Hardware status
- CPU: 16

Trend Analysis
- Hourly: Success, Fail
- Daily: Success, Fail
- Monthly: Success, Fail
Wi-Fi (Wireless LAN) Authentication Solution

AirFRONT
AirFRONT : Wi-Fi Authentication Solution

Existing Terminal Environment

• **Wired Terminal**
  - Fixed terminal
  - Gradually disappearing form

• **Wireless Infra Introduction**
  - Trend of expansion
  - High-speed wireless technology such as 11n
  - Security recognition with security reinforced technology

• **Wireless Terminal**
  - Desktop substituting terminal
  - Expand by targeting employees with high mobility
  - Network connection change from wired to wireless connection
  - Use wired connection certification/wired data encryption

Changed Environment

• **Wired Terminal**
  - Existing desktops will be substituted by notebooks and terminals

• **Wireless Infra Introduction**
  - Introduce wireless infra to the entire region
  - Introduce 11n high-speed wireless product
  - Introduce wireless certification system
  - Introduce wireless control system
  - Introduce wireless IPS

• **Wireless Terminal**
  - Use 2 terminals including notebook, smartphone/tablet per person
  - Establish a work environment without location problems (SmartWork)
  - Communication environment (FMC) without distinguishing internal/external lines
  - Consolidation of various terminals
  - Short terminal replacement period
AirFRONT Need & Benefit

**Need**

- Spread of Wireless Infra: Existing desktops will be substituted by notebooks and smart Device
- Increase of Mobile office environment
- Consolidation of various smart terminals

**Benefit**

- Provide Wired / Wireless integrated authentication solution
- Data encryption of the devices in the wireless LAN environment
- Support the integrated authentication application of smart devices (Android, iOS)
AirFRONT - Configuration

Inside wired network
- FireWALL
- IPS

Inside wireless network
- AP
- AP

Authentication & Security System
- Authentication Server
- Authentication System
- WIPS Management server
- WNMS Management server

Mobile Device
- Mac
- iOS
- Android
- Mobile

Wireless authentication system
## AirFRONT Architecture & Monitoring UI

<table>
<thead>
<tr>
<th>Details</th>
<th>Type</th>
<th>Product</th>
<th>Detail function description</th>
</tr>
</thead>
</table>
| Smart Mobile Integrated Authentication server                          | Smart Mobile Integrated Authentication server | AirFRONT                                     | • Support standard protocol of IEEE802.1x  
• IEEE802.11i security (support higher than WPAv2)  
• Follow TLS v1.2 : AES256/SHA256/RSA2048  
• Support AAA standards  
• Support RADIUS IPv6                                                  |
| Private Certificate Tool                                               | Private Certificate Tool               | Certificate Tool                              | • Issue private CA  
• Private CA  
• Public certificate authority link                                   |

### GS Certified Products (AirFRONT)

### CC Certified Products (AirFRONT)

### Certificate Tool

#### Issue private CA

#### Private CA

#### Public certificate authority link

---

### Admin Log

<table>
<thead>
<tr>
<th>Access IP</th>
<th>Administrator ID</th>
<th>Time</th>
<th>ACTION</th>
<th>table to be change</th>
<th>Items to be modified</th>
<th>EVENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.102</td>
<td>aaa</td>
<td>2015/11/24 14:17:25</td>
<td>member</td>
<td>member</td>
<td>bbi</td>
<td>Insert</td>
</tr>
<tr>
<td>10.10.102</td>
<td>aaa</td>
<td>2015/11/25 15:55:34</td>
<td>memberINFOR</td>
<td>member</td>
<td>test1</td>
<td>Insert</td>
</tr>
<tr>
<td>10.10.102</td>
<td>aaa</td>
<td>2015/11/27 17:47:31</td>
<td>memberINFOR</td>
<td>member</td>
<td>sdl</td>
<td>Insert</td>
</tr>
<tr>
<td>Local</td>
<td>aaa</td>
<td>2015/11/27 18:03:23</td>
<td>memberINFOR</td>
<td>member</td>
<td>sdl</td>
<td>Delete</td>
</tr>
</tbody>
</table>

### System Management

#### Preferences

#### System Settings

#### NAS Registration

#### Personal Page Setting

---

### DHCP Status

#### DHCP Log

### Static IP List
Customer References

- National Outlet: emart
- Government: Seoul City Hall, NIPA (National IT Industry Promotion Agency)
- School: Smart e-Learning
- Public Org.: KEPCO (elect. Power)
- TV Broad Casting: KBS
- Hospital: General Hospital
WiFi Authentication Reference – Outlet E-MART

- Free WiFi service and Outlet Promotion for Outlet customers
  - Web Authentication
  - Wireless access

Customer Marketing System

Outlet promotion and Web authentication

A Branch

B Branch

C Branch
Nationwide smart school student authentication project

- 12,000 school: 7 million student
- WiFi based each classroom: 2 WiFi APs per classroom
- Intelligent WiFi Auth.: Teacher Net. / Student Net.
- Smart Edu-Roaming: Student Edu Roaming

Net Aggregation Point

City 1

City 2

City 3

City 4

City 5

City 6

City 7

City 8
“Seoul City Hall” Reference

- **Customer**: Seoul City Hall
- **Enterprise type**: government city hall
- **No. of License**: 15,000 License
- **Service launch**: November 2011
Customer : KEPCO (Korea Electric Power Company)
Enterprise type : Nationwide public organization
Service launch : February 2012
“KBS” TV Reference

- Enterprise type: Korea Broadcasting Station
- No. of users: 15,000 users
- No. of branch office: 22
- Service launch: December 2010
“Hanwha Life Insurance” Reference

- Enterprise type: Nationwide Insurance company
- No. of users: 20,000 users
- No. of branch office: 84
- Service launch: January 2006
“Hospital” Reference

- "SOONCHUNHYANG UNIVERSITY HOSPITAL"
- Enterprise type: General Hospital
- No. of users: 10,000 users
- No. of branch office: 4
- Service launch: July 2012
“Telecom Carrier” Reference

- “SK Planet”
- Enterprise type: Telecom carrier
- No. of users: 6,000 users
- Service launch: January 2012
CONTACT POINT

- GS AHN : Executive Vice President
- Mobile : +(82)10-3703-1648
- E-Mail : gsahn@aircuve.com

- Sophia PARK : Marketing manager
- E-Mail : sophia@aircuve.com

- Office : Suite 606, Gangseohankang XI Tower B,
  Yangcheon-ro 401, Gangseo-gu, Seoul, 157-801, Korea
Thank you

Authentication On Everything