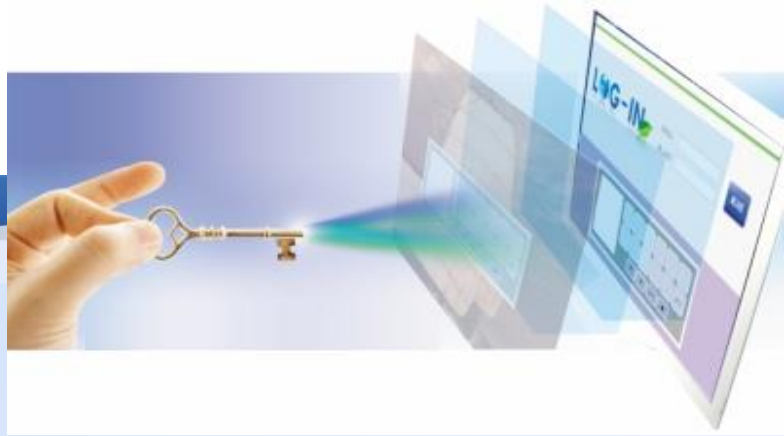


Magic keyboard

Ssang Yong Software Co., Ltd

CONTENTS

INDEX

1.1 Magic keyboard Before & After

The UI uses a password made up of a combination of randomized buttons

The Magic keyboard has simple and big sized buttons for the user's password, mixed with randomized buttons. The number of randomized buttons can be configured upon installation.

UI innovation : Magic keyboard Before & After

Before

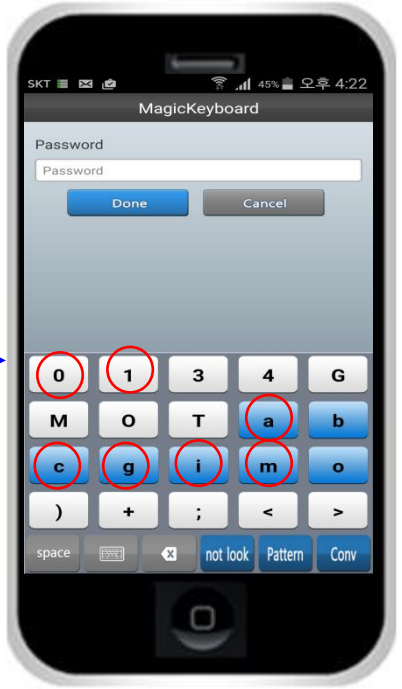
Magic keyboard

Small sized buttons

Big buttons, Big letters

(E.g. password is magic0001)

After



1.2 UI Structure

Magic keyboard can be configured using a maximum of 20 characters (letters, numbers and symbols). 6 function keys allow for the use of patterns as a password.

UI Innovation : UI Structure

Magic keyboard UI

Type : 3X5
4X5

20 characters

- Password mixed with randomized characters = up to 20 characters
- This is an example of a keyboard which has 11 randomized characters using the password (magic0001).
- If the password is longer than 20 characters, a new shuffled keyboard will appear.

Menu

space	Blank
⌨	Shuffling Keyboard I/F
⌫	Backspace
not look	Letter Shown ⇔ Letter Hidden
Pattern	Pattern design
Conv	Next pad (up to 4 pads with 3 randomize pads)

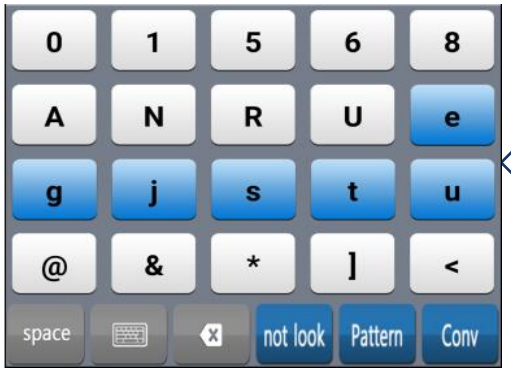
1.3 Buttons according to Input information

Different keyboard for ID and Password

The ID and password interfaces use a different keyboard. The number of randomized buttons can be configured upon installation.

UI Innovation : Keypad indicates input characters

For ID



Keyboard appears including characters of ID.

<= When ID is guest0001

The number of randomize buttons can be configured upon installation.

For Password

Keyboard appears including characters of a password.

When password is magic0001=>

The number of randomize buttons can be configured upon installation.

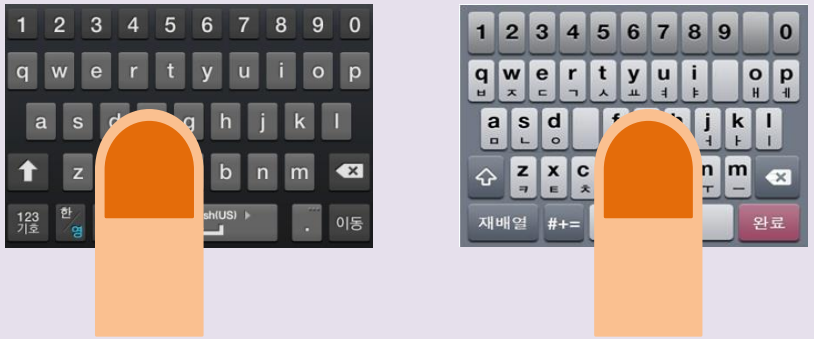
2.1 Convenience input design

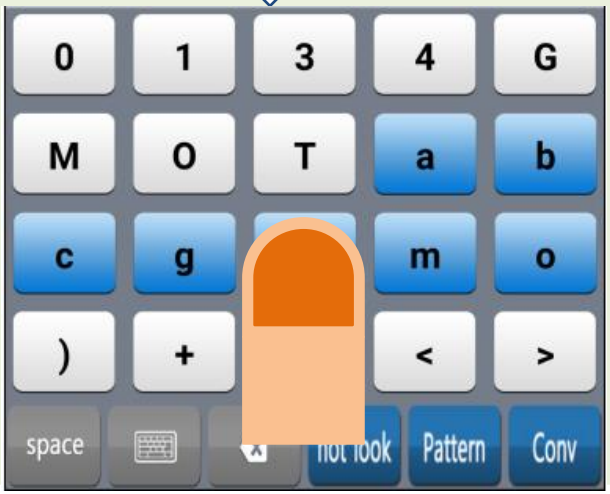
Bigger sized button with larger letters are more convenient. There's no mistyping!

Current keyboards have buttons which are too small and this is not convenient for many users who have thick fingertips.

UI Innovation : Convenience input

Other Keyboards	Magic keyboard
3 buttons are pressed at a time=> Difficult & Frustrating	Big sized buttons are as big as fingertips => Easy and no mistyping





2.2 Pattern input system

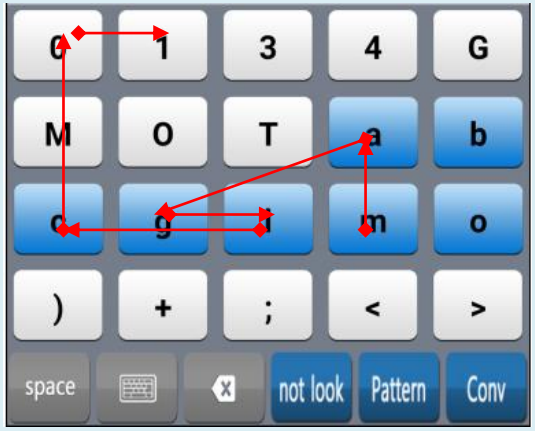
Entering ID/password by dragging pattern

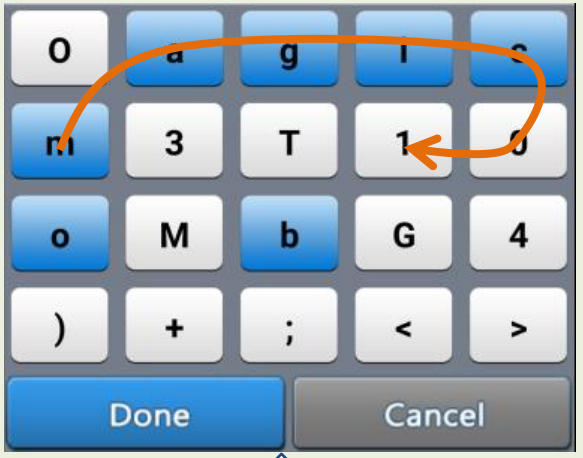
Magic keyboard provides a pattern design function which allows users to create passwords easily by dragging patterns.

UI Innovation : pattern input system

When the password is magic0001

Normal Keyboard	Magic keyboard	
	Without pattern set up	Pattern set up





- press buttons at a time
- takes time to find its location

Still faster than other keyboard

One drag only

2.3 Pattern Design

Simple swapping buttons

How to: Press “Pattern” Button. Select the first button that you want to swap then select the next button. The press “Done”.

UI Innovation : Pattern Design

Password is 82honara and it has pattern.

Before Setup	Pattern setting up	Pattern input
		
Select Pattern function	Changing button location	Aligned buttons for pattern will appear

2.4 Shortened data input time

Approximately 24 seconds OFF

Shortening the password input time is especially important in MTS(Mobile Trading System). Using Magic keyboard can save 10 seconds during ID input, 10 seconds during password input. An extra 4 seconds can be saved when compared with instances of mistyping.

UI Innovation: Shortening input time

ID Input: 1-2 seconds, ID & Password Input : 2- 4seconds

Less chance of mistyping

Shortening 10 seconds from ID input

Shortening 10 seconds from Password input

Shortening 4-8 seconds in compare with typo case

General the time required

Password : 10 seconds

ID + Password : 20 seconds

In case of mistyping : additional 4 seconds

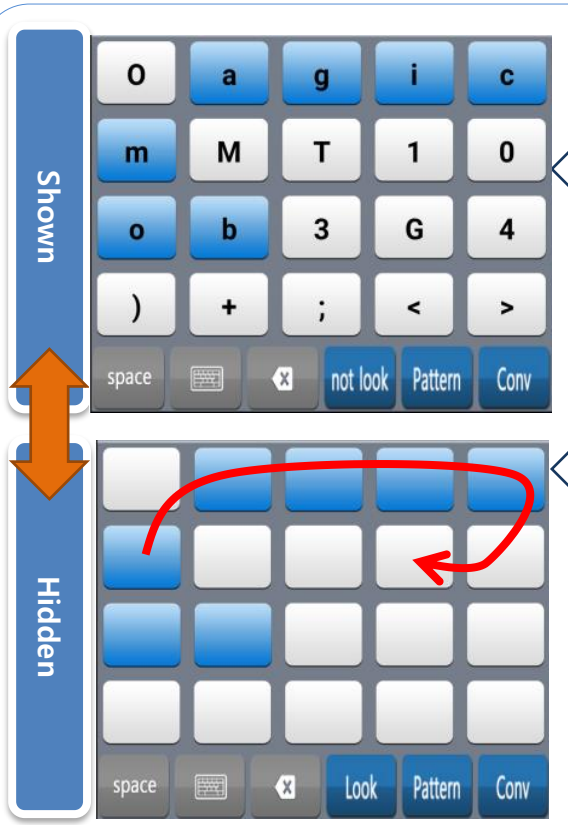
2.5 Pattern Shown⇔ Hidden

Password Input using Hidden status – Arouse user's interest

Magic keyboard has a hidden button function when using a pattern password.

It is secure from screen hacking.

UI Innovation : Button shown⇔ Hidden



Shown status

Pressing "Not Look" makes letters disappear

"not Look" key becomes "Look"

Hidden status

Drag pattern on Hidden keyboard

Pressing "Look" will makes letters appear

"Look" key becomes "not Look

Hidden button effect

Arouse User's interest

Security enhancement

3.1 Prevention of forgotten data complaint

Magic keyboard UI enables users to easily remember their data. For users, their input data is visually distinguishable and users seldom forget login details.

Complaint prevention : prevention of forgotten password

UI provides password with randomized letters

Input data aligned as pattern

=> Easy for user to guess password

=> No password forgotten

For ID input

=> Easy for user to guess ID

=> Knowing ID helps users to remind related password

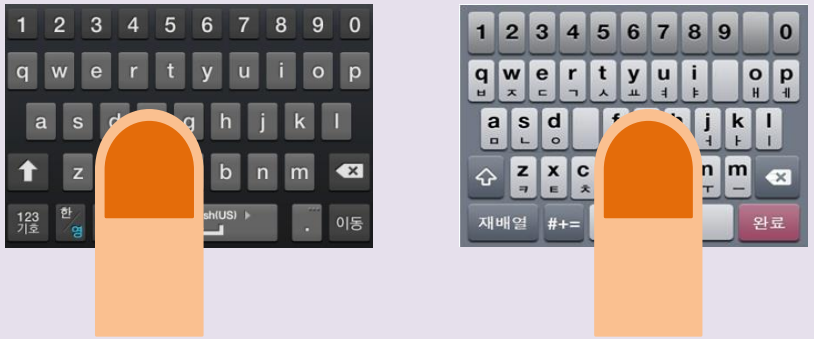
=> No forgotten ID & Password

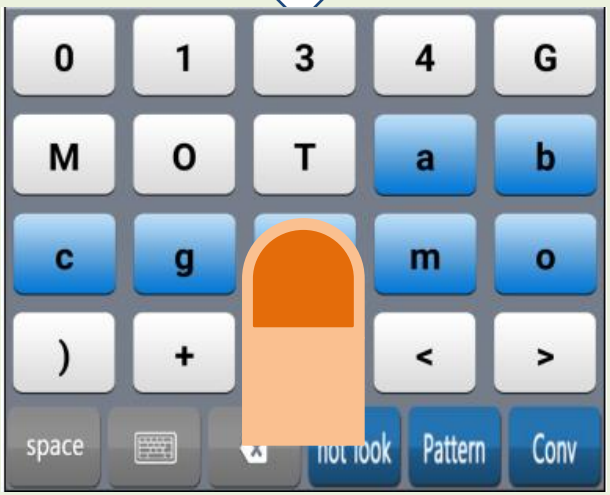
3.2 Prevention of Incorrect entering

Magic keyboard provides comfortable UI which uses bigger buttons that helps prevent pressing the wrong buttons.

3. Complaint prevention: Prevention of pressing wrong buttons

Other Keyboard	Magic keyboard
Small button => Incorrect password pressed => Verification required =>complaint of Inconvenience	Big button => easy and quick log-in => Good Feedback





4.1 Prevention of Pharming

Magic keyboard => User's identified keyboard => Anti-Pharming

Other keyboards may use personal images to protect against Pharming. As each magic keyboard user has a different keyboard, this keyboard automatically becomes a personalized image itself. The Magic keyboard therefore is simpler because it does not require personal image identification.

Security innovation : Prevention of Pharming

Personalized Image

Personal image set up => Indicate Personal image

Prevent of pharming (if there is no image, this may indicate pharming)

Magic keyboard

If Magic keyboard doesn't have your password characters, user will know that it is pharming

No need to verify personal image confirmation

4.4 Comparative safety – Random blank keyboard vs Magic keyboard

Other keyboards attempt to prevent button location hacking by using random blank buttons. Magic Keyboard uses random character assignment making it a more secure virtual keyboard.

Security Innovation: comparative safety - Random blank keyboard vs Magic keyboard

"Does Random blank keyboard looks more secure?"

Magic keyboard is the most secure virtual keyboard existing in the world.

Virtual keyboard security threat	Threats to virtual keyboard: button location hacking, screen hacking Threats prevented by virtual keyboard : Memory hacking, reserve-analysis, network falsification etc.
Virtual keyboard security evaluation	Virtual keyboard can be rated by safety ability against threats All virtual keyboard can tolerate threats of Memory hacking, reserve-analysis, network falsification etc.

Button location hacking	Applicable with PC keyboard, Action of taking password by hacking its button location
Screen hacking	Action of taking password by videotaping or sharpshooting of login page

4.4 Comparative safety - Random blank keyboard vs Magic keyboard

Magic keyboard : Safe from button location hacking

Random blank keyboard : no protection from button location hacking

It is proven theoretical basis.

Security Innovation: comparative safety - Random blank keyboard vs Magic keyboard

How to prevent button location hacking?

Random character assignment can prevent button location hacking

Random blank keyboard

no protection from button location hacking

-Reason-

81 = number of password case at 1 attempt of hacking

-Example-

password= 8digits, 1 blank button in each row

1) User : 4^{th} and 7^{th} in 1^{st} Row, 3^{rd} and 6^{th} in 2^{nd} row, 2^{nd} and 8^{th} in 3^{rd} row, 4^{th} and 6^{th} in 4^{th} row
2) Hacker : Hacking location of the button pressed
3) Number of case : 36, 46, 47 in 1^{st} row, wt, et, ey in 2^{nd} row, aj, sj, sk in 3^{rd} row, cb, vb, vn in 4^{th} row
   => 81 number of password case (81=3X3X3X3)

Magic keyboard

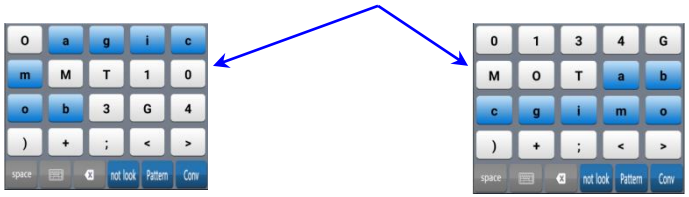
Magic keyboard

-Reason-

Each user has different combination of keyboard

-Example-

Totally different combination and location of button



User A User B

4.4 Comparative safety - Random blank keyboard vs Magic keyboard

Magic keyboard : Safe from screen hacking

Random blank keyboard : no protection from screen hacking

Magic keyboard has a hidden letter function without any distinguishing colors when buttons are pressed.

Security Innovation: comparative safety - Random blank keyboard vs Magic keyboard

Protection condition of button location hacking

1) No distinguishing color when button is pressed 2) Entering password in hidden keyboard

Random blank keyboard

Not safe from screen hacking

-Reason-

1) Color distinguished in pressed button
2) Letters shown in button

-Is it safe from screen hacking? "No Way!"-

1) What if there's no color change on pressed button?
   => not knowing about mistyping
   => Cause complaint of inconvenience
2) How about hide letters in keyboard? => unusable

-Result-

Random blank keyboard has no protection from screen hacking

Magic keyboard

Safe from screen hacking

-Reason-

1) Color distinguished in pressed button
2) Button can be hidden

-It is safe from screen hacking-

1) What if there's no color change on pressed button?
   => no affect to mistyping, but, less visual effects
   => protective from screen hacking
2) Button hidden function

-Result-

Safe from screen hacking
(Client have color option about pressed button)

4.4 Comparative safety - Random blank keyboard vs Magic keyboard

Magic keyboard is the most secure virtual keyboard existing in the world.

Despite its simple design, it is proven that it is the most secure virtual keyboard.

Security Innovation: comparative safety - Random blank keyboard vs Magic keyboard

- Reasons that you assume that Magic keyboard is not safe -

Due to its design : password mixed with randomize buttons

=> Assume that anyone easily can guess your password

=> Assume that it doesn't look safe from hacking

(Ex : Assume that password can be figured by screen hacking)

-Reality-

Magic keyboard is the most secure virtual keyboard existing in the world (with Functional shift)

4.4 Comparative safety - Random blank keyboard vs Magic keyboard

The conclusion of comparative safety

Random blank keyboard exposes confidential data on 3rd attempt of button location hacking. Magic keyboard can not be hacked even with thousands of attempts. Hacker only can guess password from keyboard UI.

Security Innovation: comparative safety - Random blank keyboard vs Magic keyboard

End of war : Magic keyboard definitely win!

1) Other keyboard — **3rd attempt of hacking**

=> password is exposed

2) Magic keyboard — **unlimited attempt of hacking**

=> Hacker can't get any clue

4.5 Preventing password inference (guessing)

It is proven that Magic keyboard is a secure virtual keyboard. Now we would like to demonstrate that no one can guess data in Magic keyboard UI.

Security Innovation : Prevent of password inference (guessing)

-Reason you think that Magic keyboard is not secure-

Proven to be

Magic keyboard combined password with random buttons

=> Assume that anyone can easily guess password in phone loss

=> Require to be proven

Proven

=> Assume that it might be week in security due to its design

=> Security against hacking is proven

4.5 Prevent of password inference

Example: When UI has 20 buttons and the password is 9 characters,

Probability of guessing password = 0.000000000000098%

Security Manager can configure the number of buttons in keyboard upon installation.

Security Innovation : Prevent of password inference

If someone stole my phone or phone is hacked,

they still need to figure password only based on keyboard UI

※ There are limited login attempts allowed, to prevent online Dictionary Attack. Online Dictionary Attack is different from Brute Force Attack which is an action of breaking into authentication mechanism by systematically entering every word in a dictionary.

※ Depends on user data, the pattern function can be less likely secure. The use of pattern is considered according to security policy.

< Prevent of password inference : Security Manager can configure the number of buttons in keyboard upon installation >

When UI has 10 buttons and the password is 8 characters, the number of possible passwords is $100000000=10^8$ and the probability of guessing the password is 0.00000003%

When UI has 2 additional randomize buttons, the number of possible passwords is $429981696=12^8$ and the probability of guessing the passwords is **0.0000000006977%**

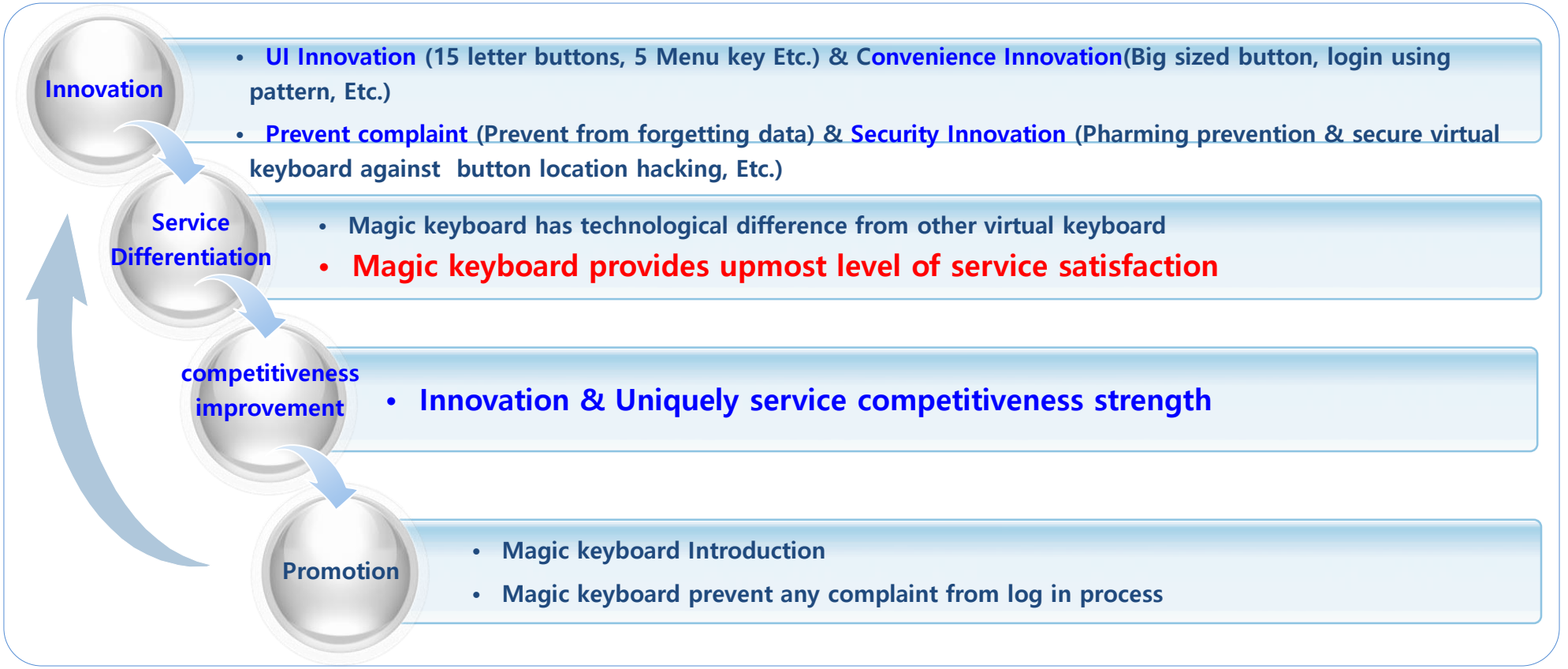
※ P.S : Probability of guessing Credit card passcode = 0.0003%

5.1 Service competitiveness reinforcement

Service competitiveness is reinforced by Innovated service

Innovated service of Magic keyboard is able to perform service differentiation and it strengthens service competitiveness.

Expectation of Magic keyboard effectiveness : Service competitiveness reinforcement

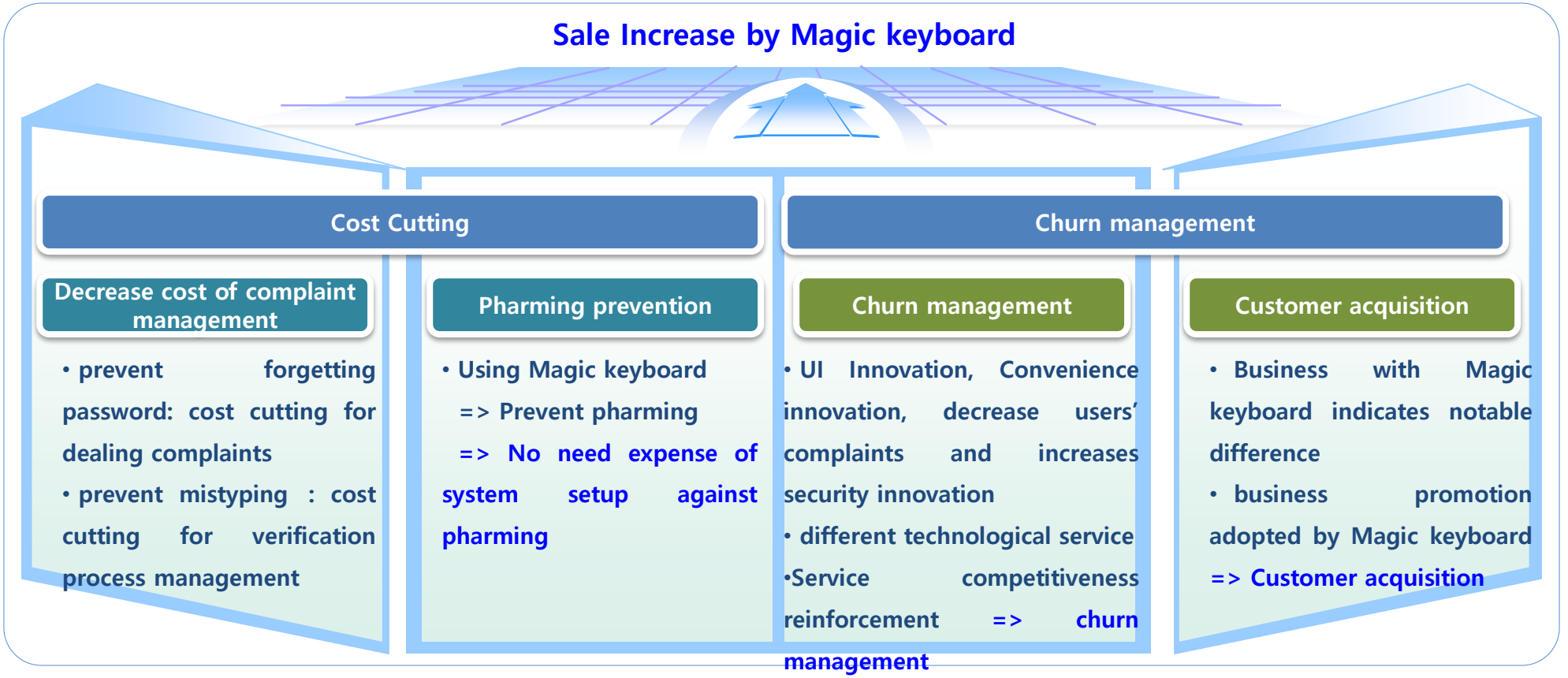


5.2 Cost Cutting and Churn management, it leads sale increase

Cost Cutting and Churn management, which brings sale increase

Magic keyboard saves you the expense of anti-pharming setup and handling client complaints. Innovated Magic keyboard strengthens competitiveness and manages churn easily. Eventually it will bring customer acquisition.

Expectation of Magic keyboard effectiveness : Cost Cutting and Churn management

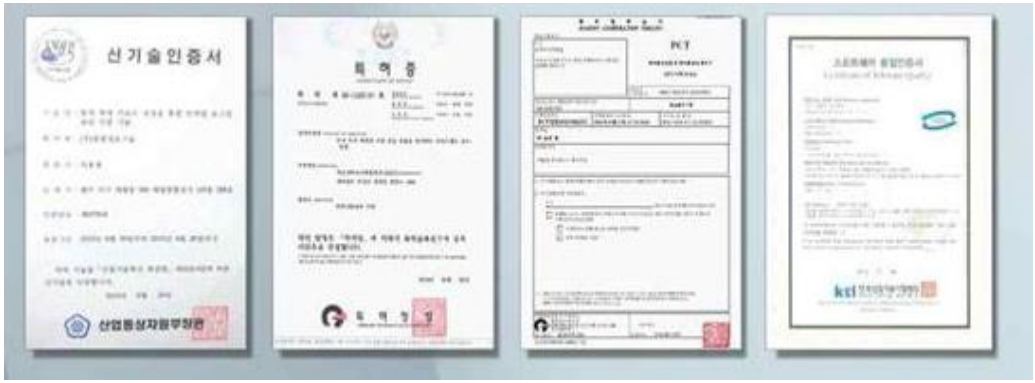


6.2 Patent

In Korea : 1 registered & 1 in progress,

International : PCT patent application(27th of March, 2013)

Patent :



7.1 Summary of supplement 1

Supplement 1 has details of elements and role of Magic Keyboard, etc.

Supplement 1 explains the protocols which determine the letters in the keyboard, interworking with SSL, enlarged E2E and PKI.

Summary of supplement : summary of supplement 1

Please note: Supplement is provided only upon request due to its volume.

Supplement 1 : Details of Magic keyboard

Supplement 1 contains the answers to most of the inquiries about Magic keyboard.

1. Magic keyboard creative protocol
   The protocol which determine letters in keyboard is explained in detail as classified into Application and Web.
2. Magic keyboard Formation
   Formation element of Magic keyboard is explained with details of its function. Specially, it includes number of buttons in keyboard UI and number of server data which can be affected by security policy.
3. Magic keyboard security processing
   It is about Magic keyboard protocol and interworking method of SSL & Extended E2E & PKI.
   Also, it explains how to prevent reverse engineering by using Code obfuscation service provided by Korea Copyright Commission.

7.1 Summary of supplement 2

Supplement2 has detailed Server operating environment for Magic keyboard

It explains suitable devices and compatible Browsers for use with the Magic keyboard, maintenance and quality assurance system and history of Ssangyong software Co. Ltd.

Summary of supplement : summary of supplement 2

Supplement 2 : application of Magic keyboard

Supplement 2 has content of application and technical support during application progress and corporation history.

1. Magic keyboard application
   Suitable devices and Browser for Magic keyboard are explained in detail as Application and Web.
   Plus, It has detailed explanation of Magic keyboard applying method and examples.
2. pre-post Installation client relationship
   Its about maintenance, its supporting system and quality assurance system
   Client relationship can be taken care of by Ssang yong Software(manufacturer) or BP(business partner) company.
   It explains each corporations' role and liability.
3. Corporation history
   It will helps you to understand major History of Ssang yong Softward Co., Ltd which is manufacturer of Magic keyboard.
   it also introduces the history of BP(business partner).(Ex : Stock Firm)