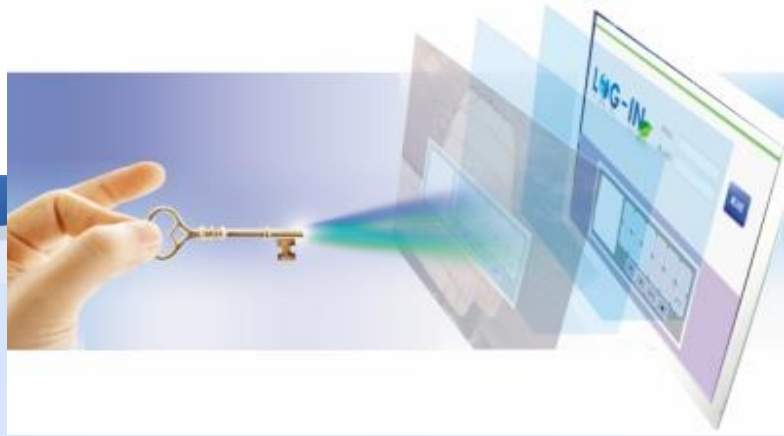


Supplement 1 : Details of Magic keyboard

ML Information Technology

CONTENTS

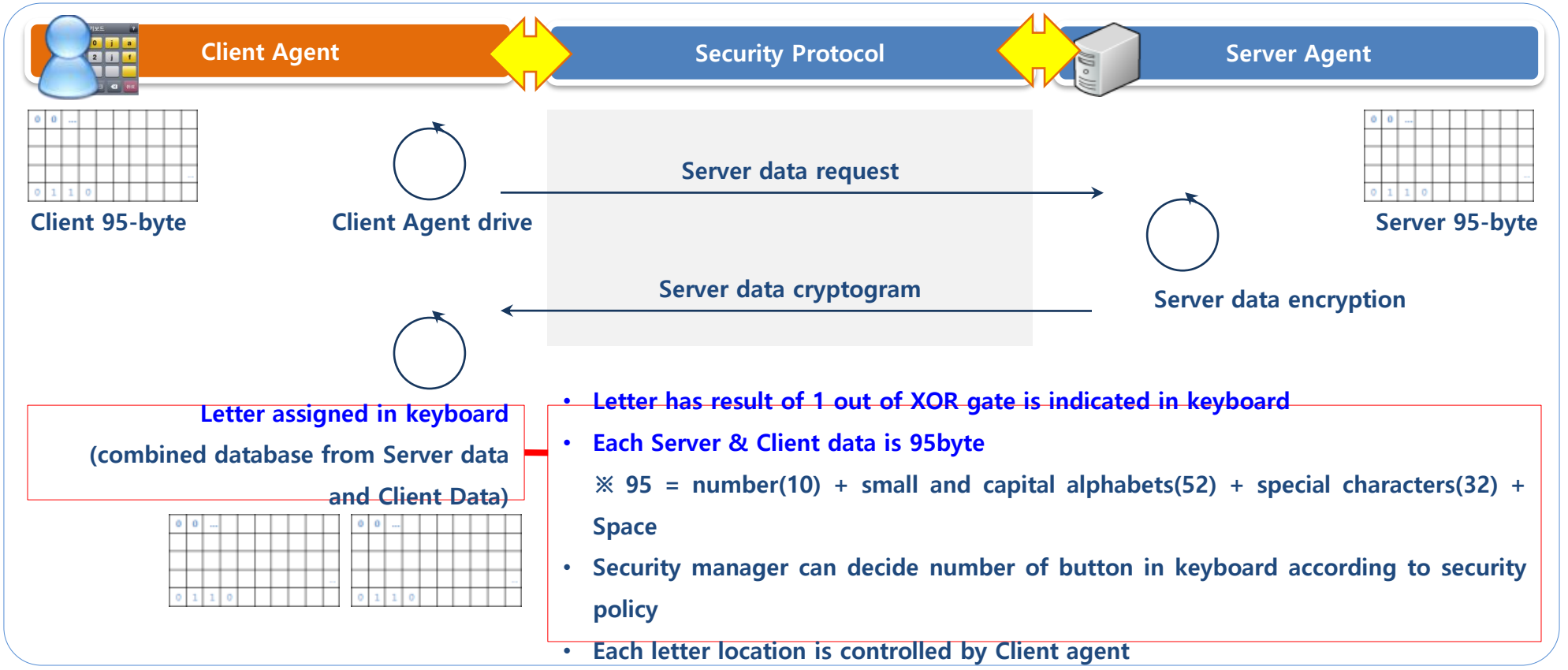
INDEX

1.1 Expended E2E case

Letter assigned in keyboard

Magic keyboard has assigned letters in keyboard using combined database from Server data and Client Data. Each data is 95byte.

Creative Protocol of Magic keyboard : Expended E2E case

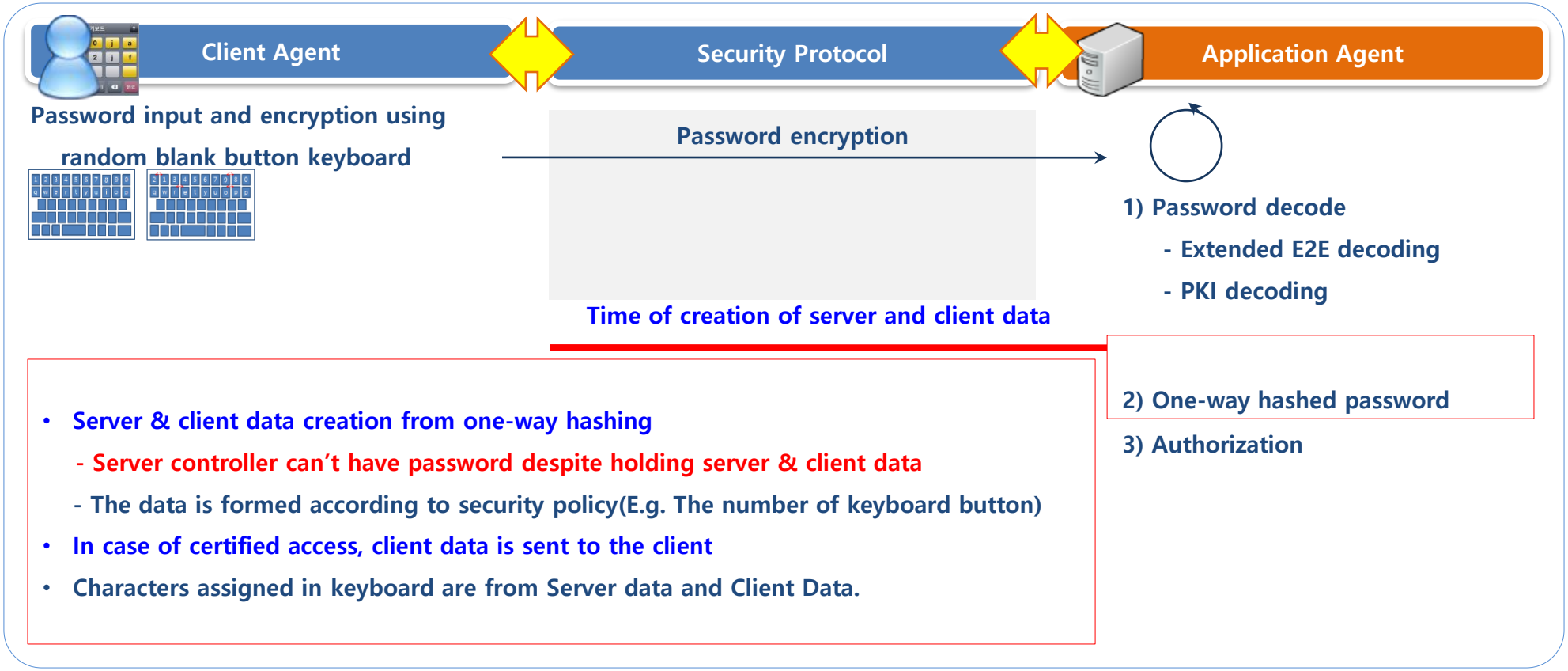


1.1 Expended E2E case

Time of creation of server and client data

Server creates server data & client data when password is hashed in one way. **So even if controller knows this data, password can't be known.**

Creative Protocol of Magic keyboard : Expended E2E case

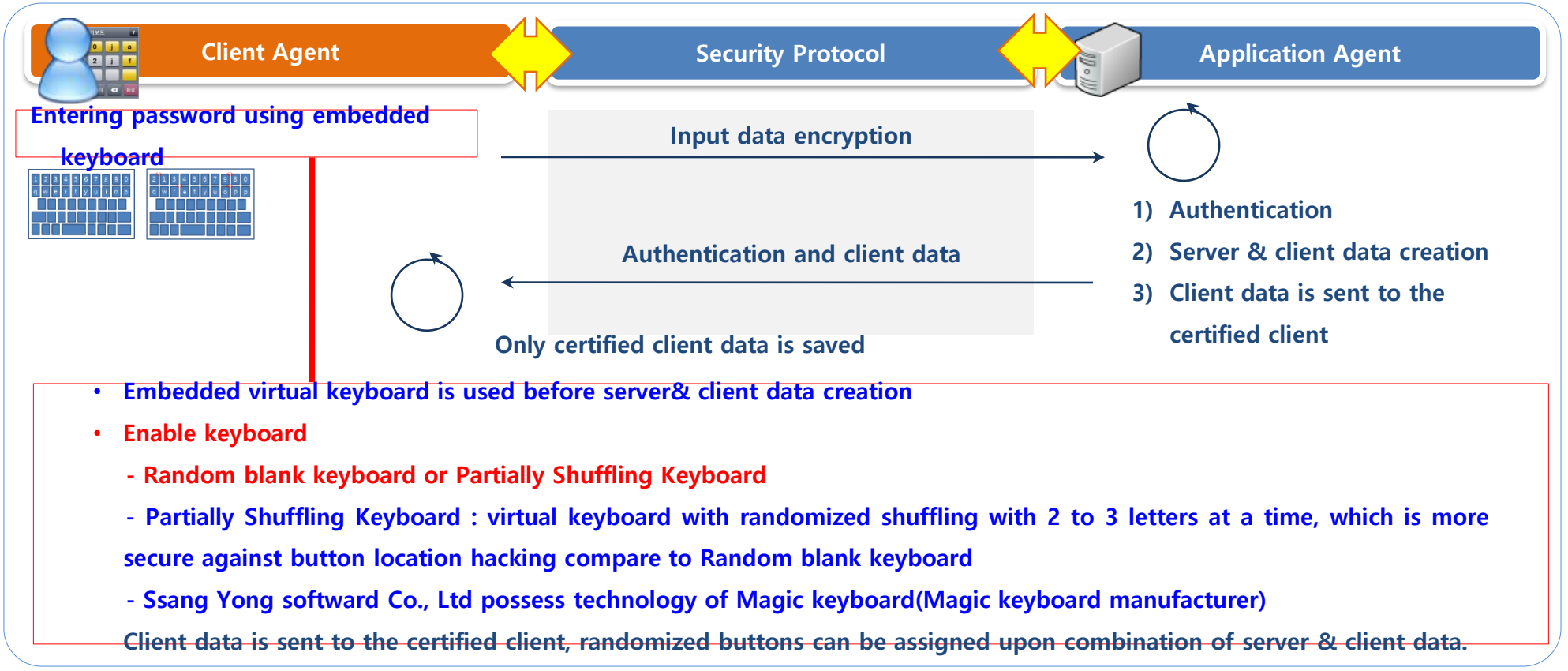


1.1 Expended E2E case

Before server & client data creation

After installation of Magic keyboard, embedded keyboard is used for initial Log-in.

Creative Protocol of Magic keyboard : Expended E2E case



- Embedded virtual keyboard is used before server& client data creation
- Enable keyboard
  - Random blank keyboard or Partially Shuffling Keyboard
  - Partially Shuffling Keyboard : virtual keyboard with randomized shuffling with 2 to 3 letters at a time, which is more secure against button location hacking compare to Random blank keyboard
  - Ssang Yong softward Co., Ltd possess technology of Magic keyboard(Magic keyboard manufacturer)

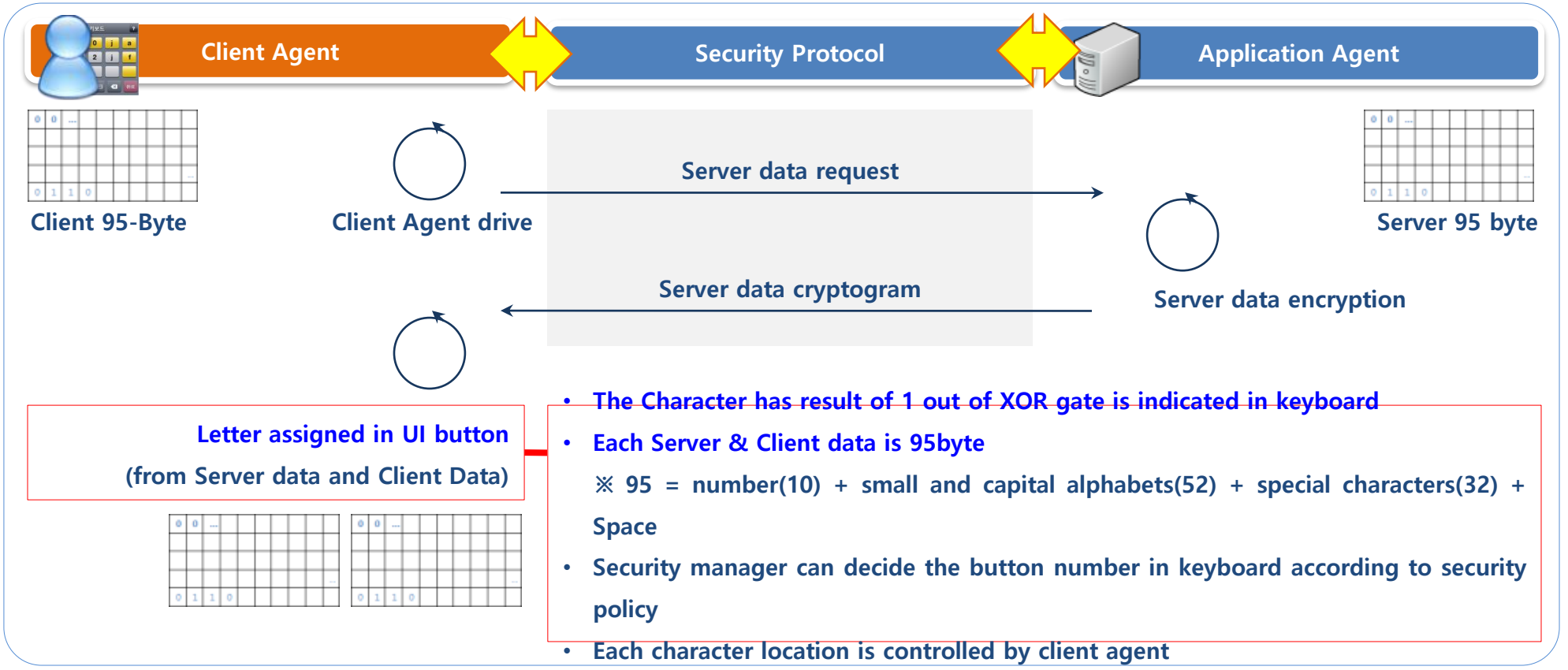
Client data is sent to the certified client, randomized buttons can be assigned upon combination of server & client data.

1.2 Unextended E2E case

characters assigned in keyboard(same as extended E2E case)

Magic keyboard decided characters appeared in keyboard from combined data from Server and Client Data. Each data is 95byte.

Letter in UI assignment protocol: Letter in UI assignment

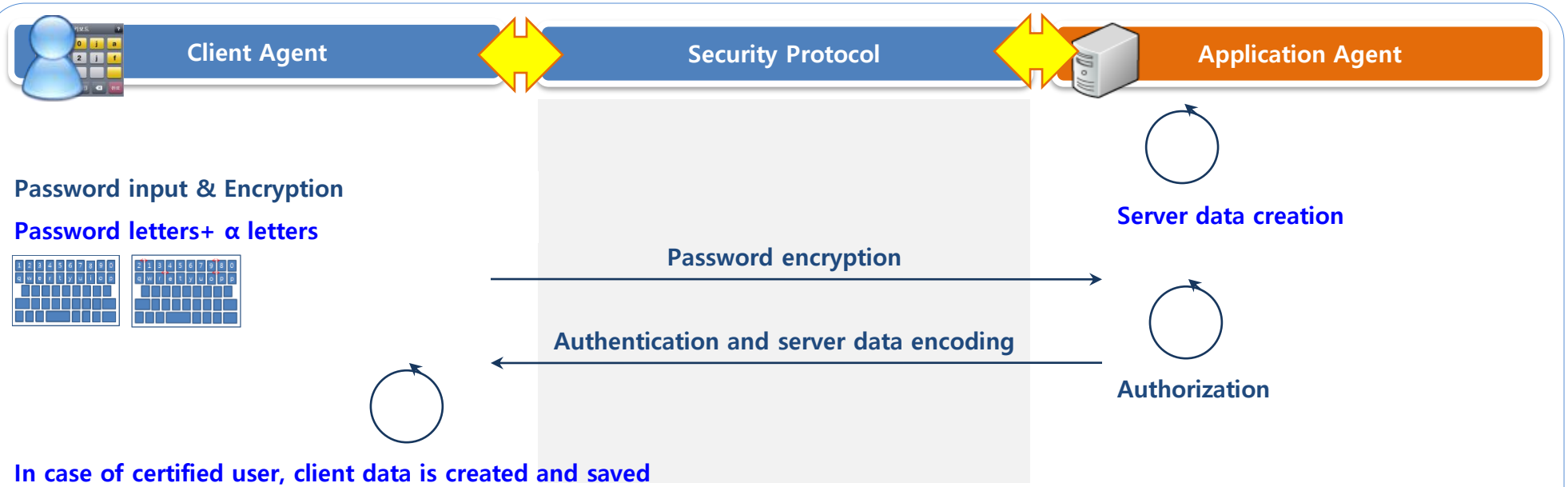


1.2 Unextended E2E case

Time of creation of server and client data

Server creates server & client data when password is hashed in one way. So even if controller know this data, password can't be known.

Letter in UI assignment protocol : Time of creation of server and client data



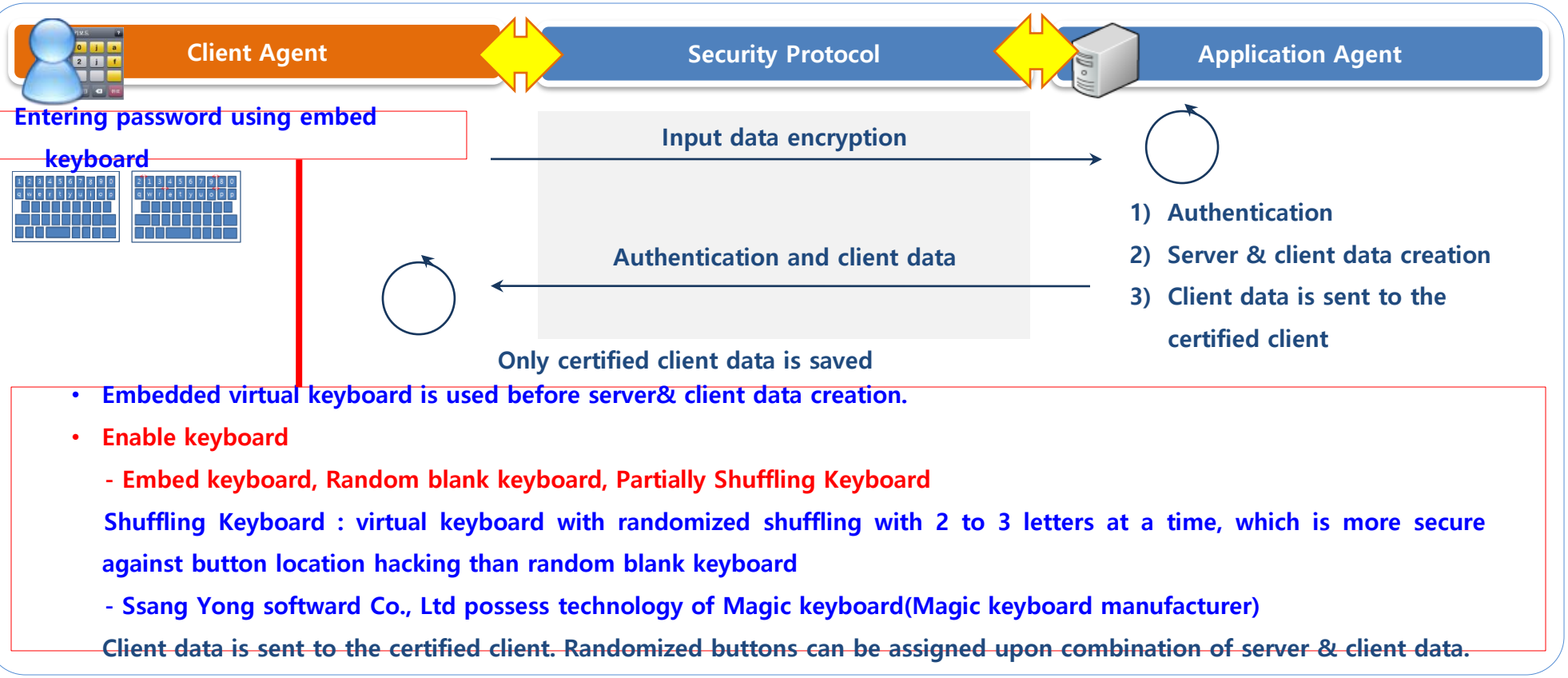
- Server :Randomly create 95 byte
- Client : In case of certified user, client data is created by referring to server data
- Impossible guessing password by having password +α letters, the number of randomized characters is decided by security policy (E.g.: the number of buttons in keyboard)

1.2 Unextended E2E case

Before server & client data creation

After installation of Magic keyboard, embedded keyboard is used for initial Log-in.

Creative Protocol of Magic keyboard : Expended E2E case



- Embedded virtual keyboard is used before server& client data creation.
- Enable keyboard

  - Embed keyboard, Random blank keyboard, Partially Shuffling Keyboard

  Shuffling Keyboard : virtual keyboard with randomized shuffling with 2 to 3 letters at a time, which is more secure against button location hacking than random blank keyboard

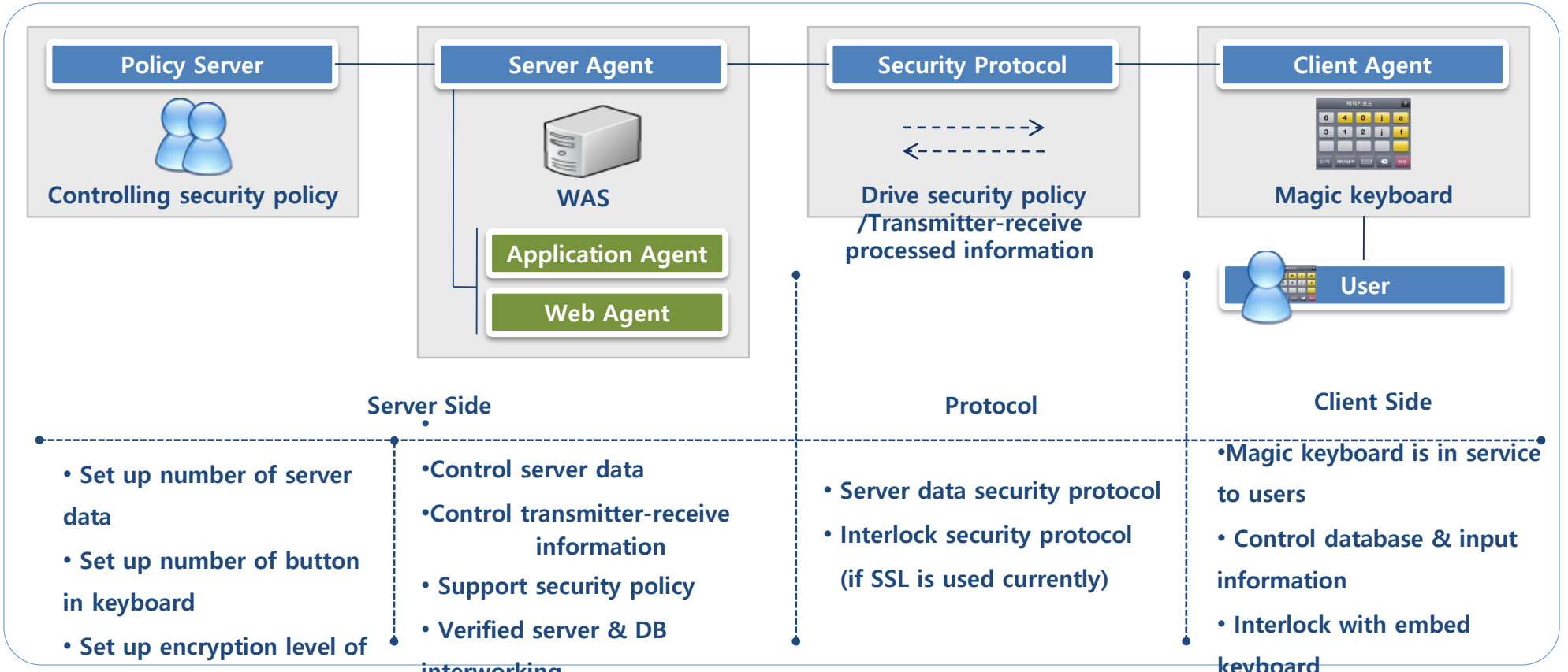
  - Ssang Yong softward Co., Ltd possess technology of Magic keyboard(Magic keyboard manufacturer)

  Client data is sent to the certified client. Randomized buttons can be assigned upon combination of server & client data.

2.1 Magic keyboard components

Magic keyboard is compromised of **Policy Server, Server Agent, Security Protocol and Client Agent.**

Magic keyboard contents: Magic keyboard components

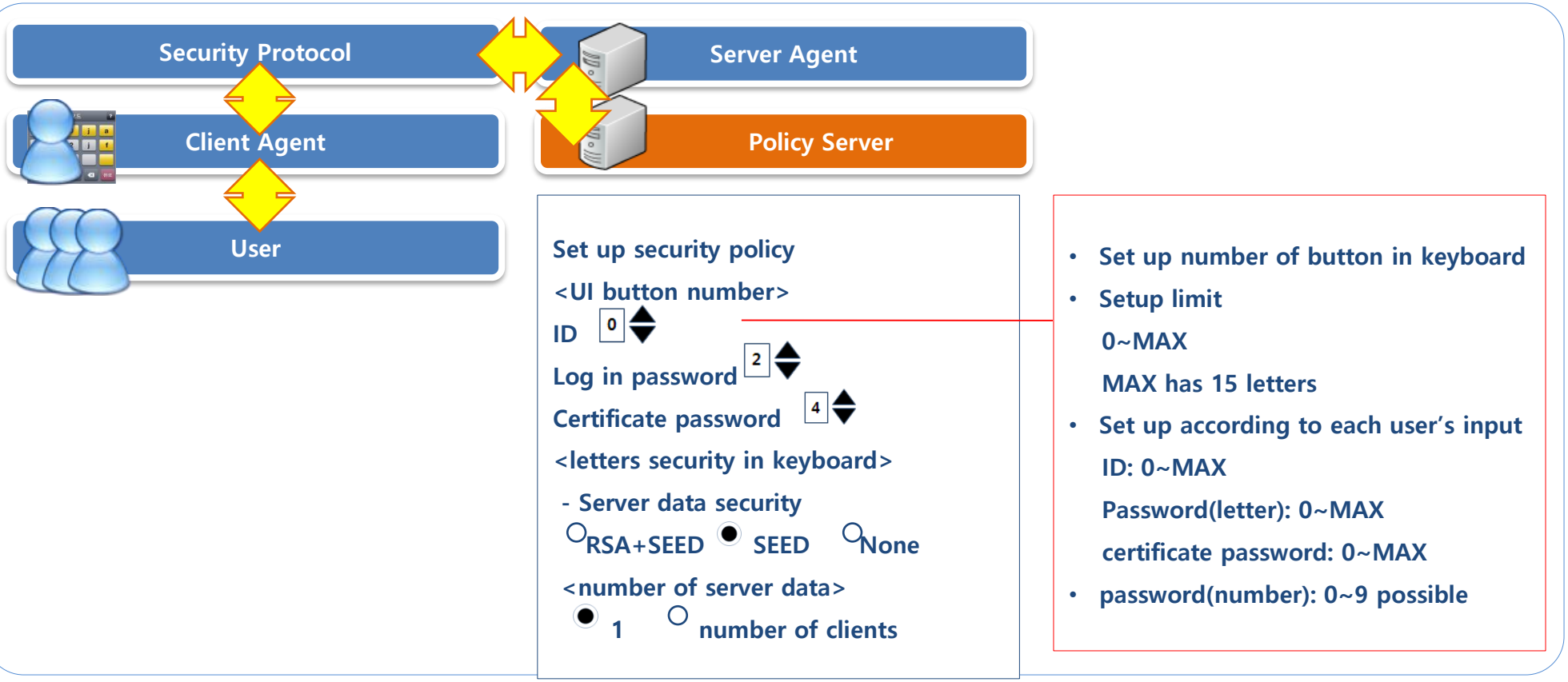


2.2 Policy Server

Driven security policy of Policy Server : the number of buttons in keyboard

Security manager can set up the number of buttons in keyboard on policy server separately for ID and password log-in process.

Magic keyboard contents : Policy Server

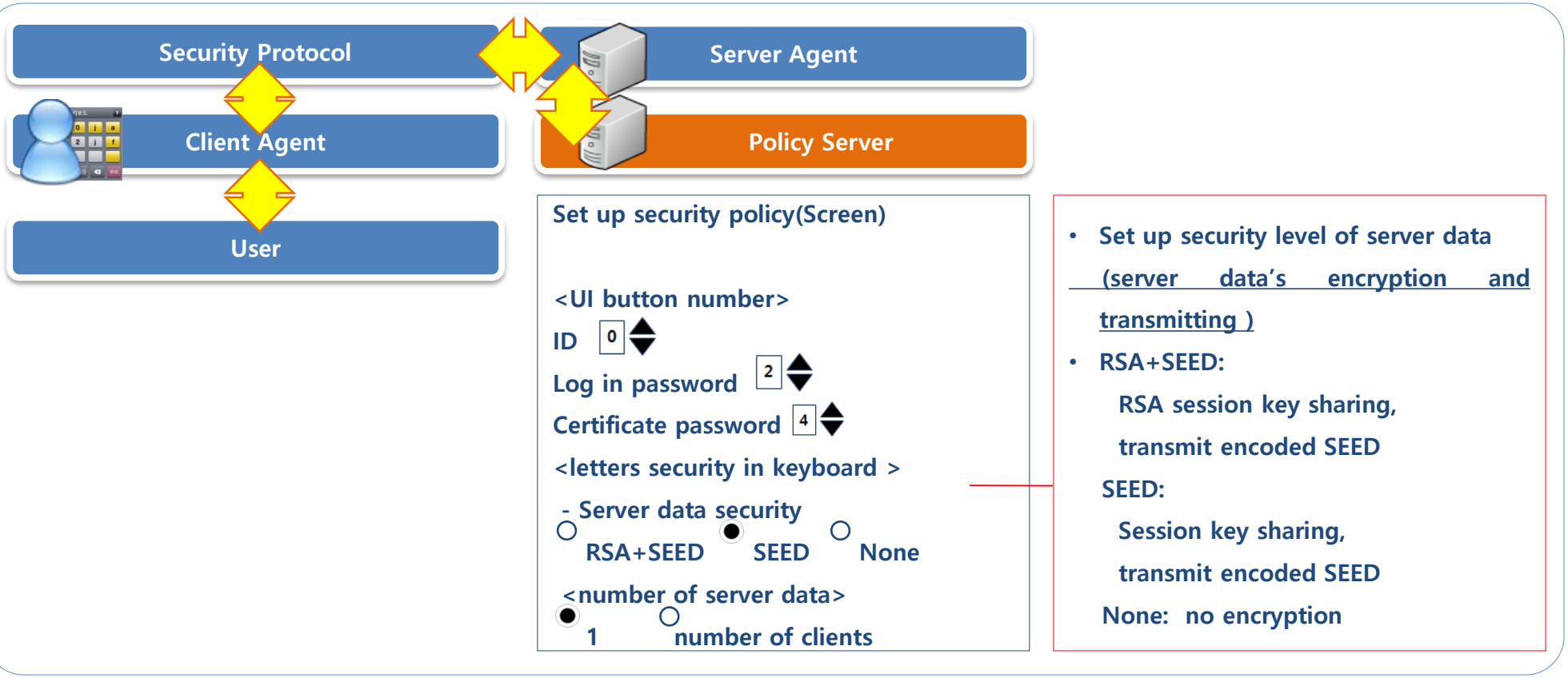


2.2 Policy Server

Driven security policy of Policy Server : set up level of data encryption transmission

How Server data is encrypted and transmitted to client is to be set. There are 3 set up modes which are RSA+SEED, SEED and None.

Magic keyboard contents : Policy Server

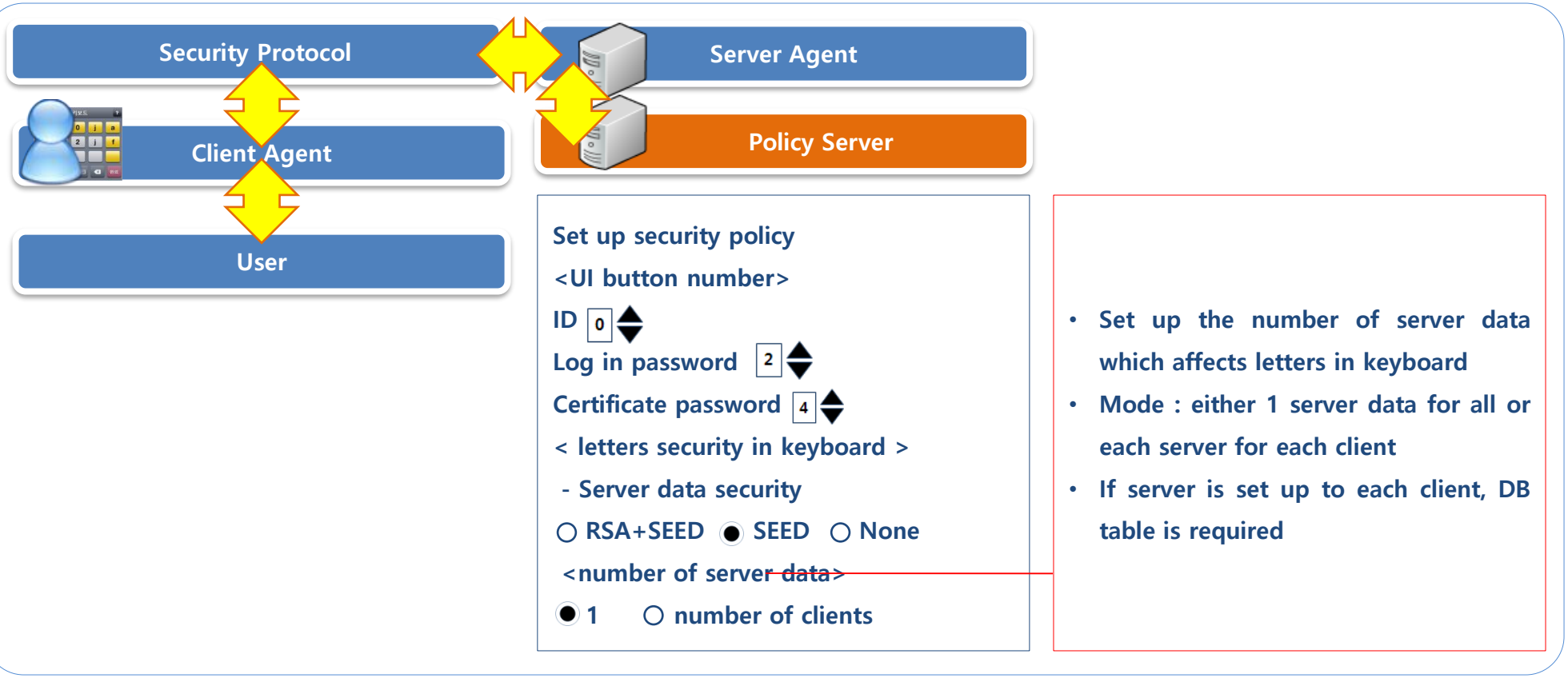


2.2 Policy Server

Driven security policy of Policy Server : set up the number of server data

Security manager sets up the number of server data in policy server. It can be 1 or 1 for each client.

Magic keyboard contents : Policy Server

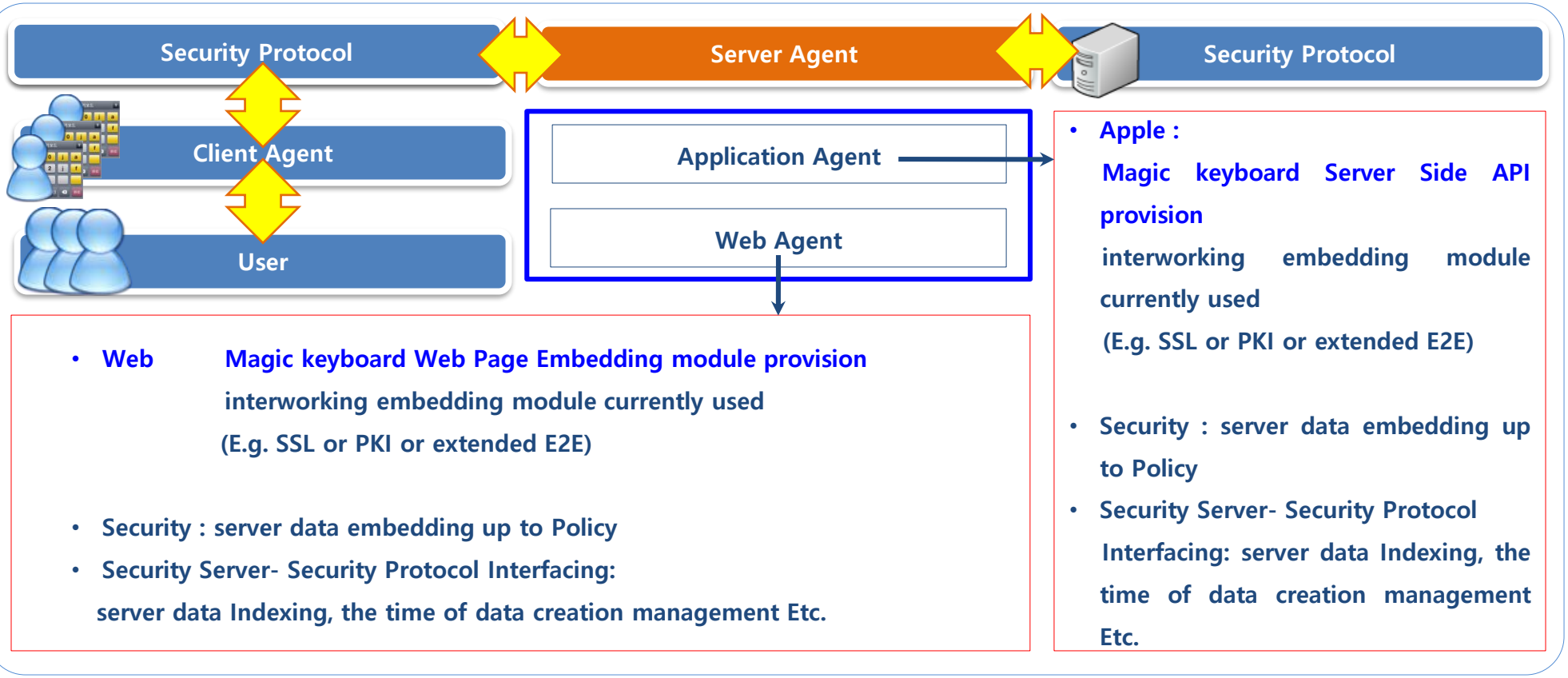


2.3 Server Agent

Apple Server Side API & Web Page Embedding module provision

Server agent consists of application agent and web agent. Application agent provides Server side API of Magic keyboard, web agent provides web page embedding Module.

Magic keyboard contents : Server Agent

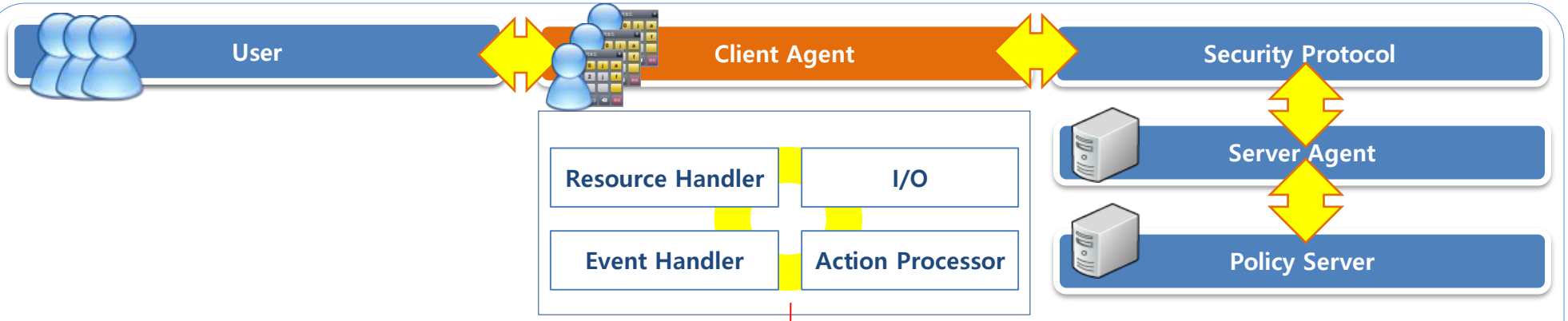


2.4 Client Agent

Apple Client Side API & Web Page Embedding module provision

Client agent consists of 4 modules. Among 4 modules, I/O module provides client side API for Apple and page embedding module for web.

Magic keyboard contents : Client Agent



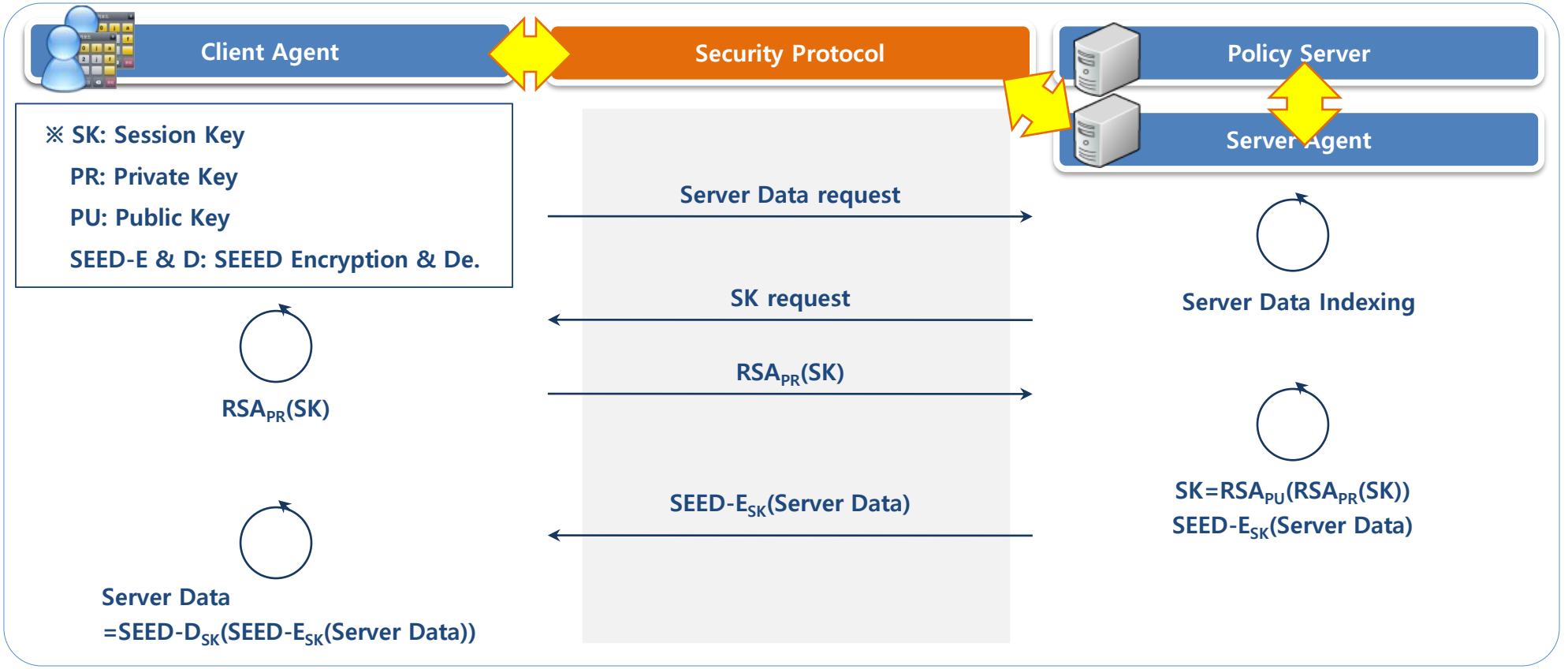
- I/O — **Apple Client Side API & Web Page Embedding module provision**
  Convey server data to action processor and input data to embedding protocol
- Resource Handler — UI processing
- Event Handler — the event occurred in Resource Handler upon button use and input data is delivered to action processor module
- Action Processor — Delivery of collective input result to I/O module, server & client data processing

2.5 Security Protocol

Encryption and transmission of server data

Security protocol encrypts and transmits server data to client agent. Embedding algorithms are RSA-1028 and SEED-128 and operating method is SSL(Secure Socket Layer).

Magic keyboard contents : Security Protocol



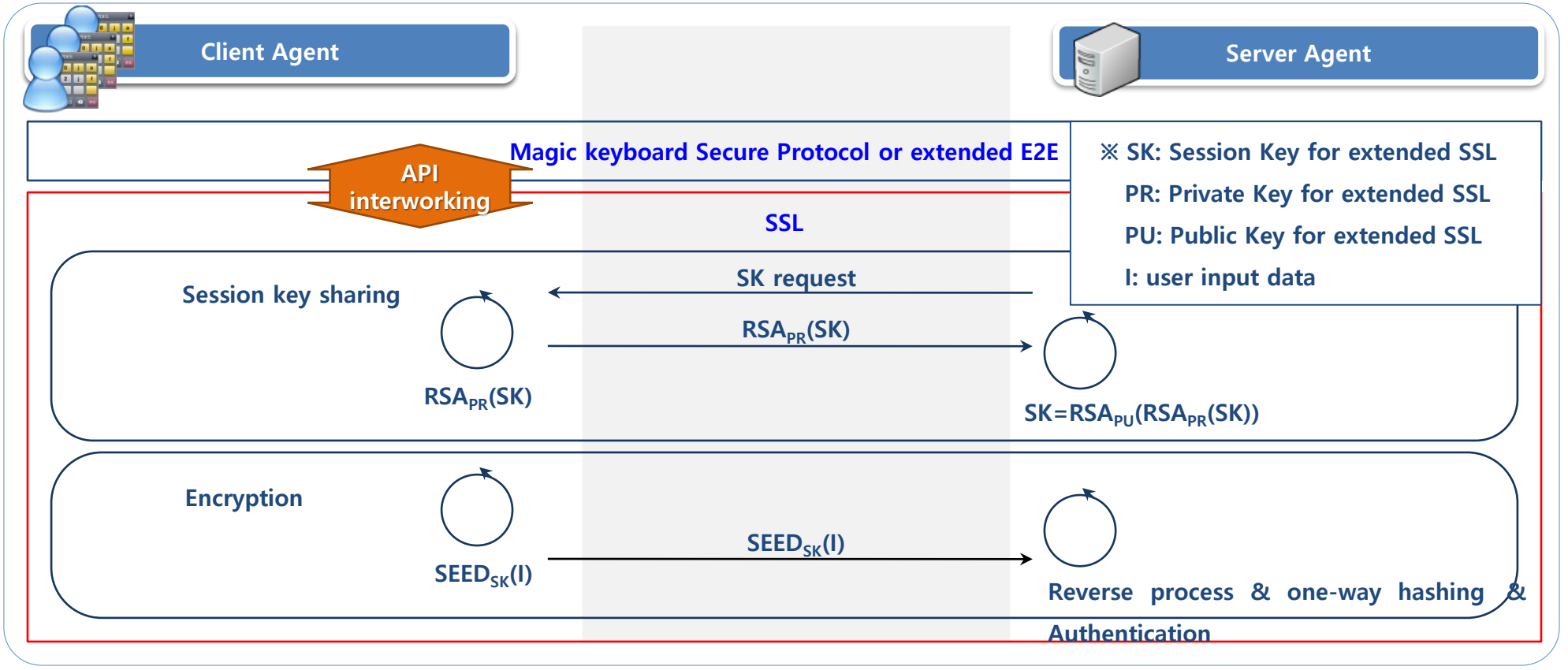
3.1 interworking protocol

Magic keyboard Secure Protocol - SSL interlocking

Server authentication and network confidentiality are provided with Secure Protocol or interworking protocol with extended E2E and SSL.

※ P.S. : SSL only work with Magic keyboard when it's interworked with extended E2E or Secure protocol.

Magic keyboard security processing: Magic keyboard Secure Protocol – SSL interworking

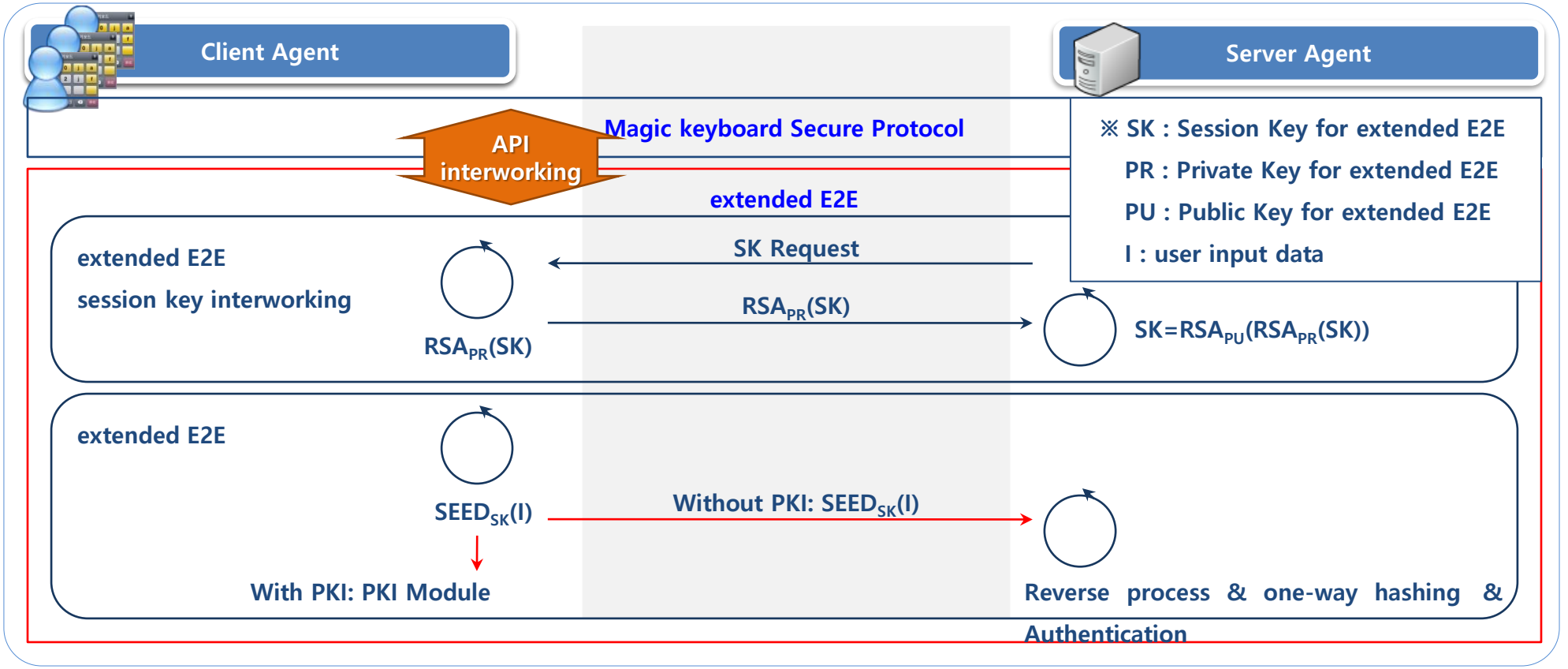


Magic keyboard Secure Protocol - extended E2E interworking

Magic keyboard Secure protocol interworks with extended E2E as API method. It is effective for prevention of memory hacking.

※ If system doesn't have extended E2E, extended E2E is able to be provided in Magic keyboard

Magic keyboard security process : Magic keyboard Secure Protocol – extended E2E interworking



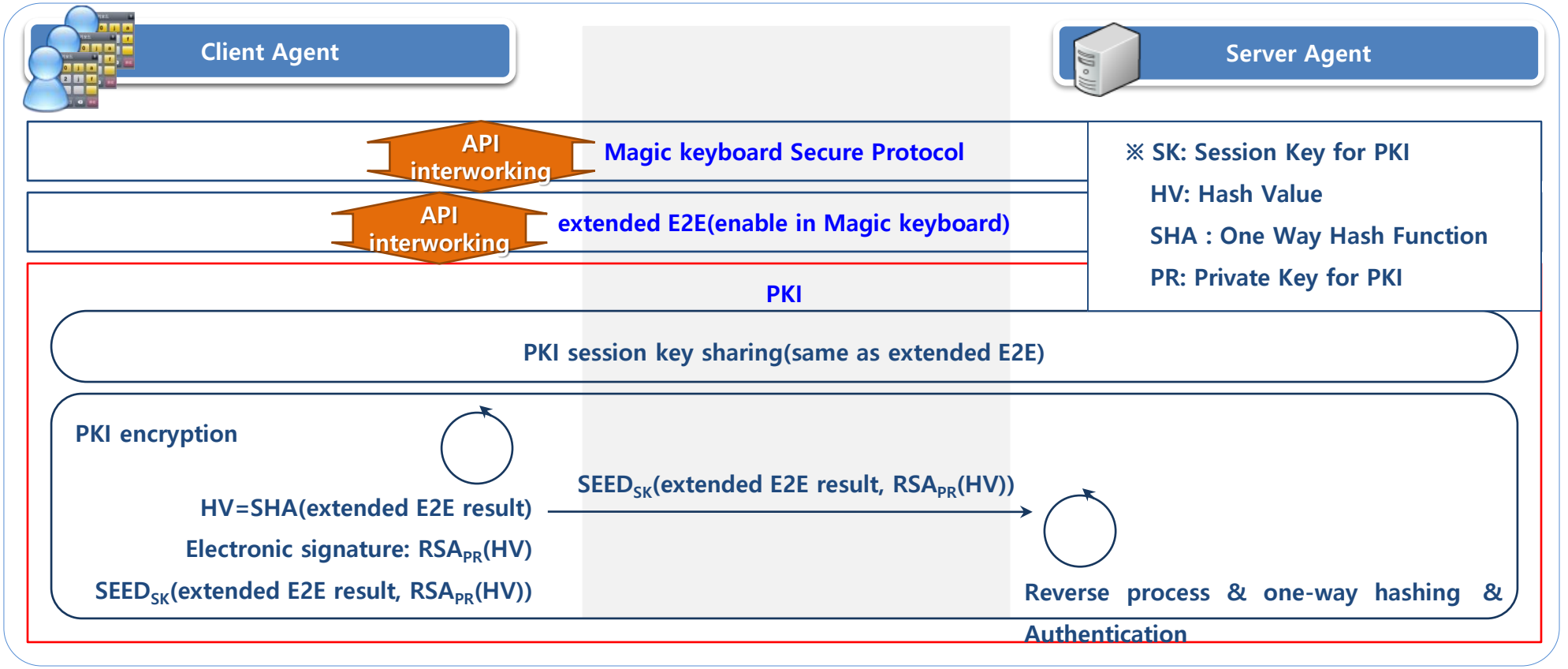
3.1 Protocol interworking

Magic keyboard Secure Protocol - PKI interworking

The protocol can be interworked with Secure Protocol and PKI. This is effective for non-repudiation and network forgery prevention

※ P.S. : PKI is based on certification, we don't offer PKI but interwork with Secure protocol.

Magic keyboard security process : Magic keyboard Secure Protocol – PKI interworking



3.2 Reverse-analysis prevention

Magic keyboard uses code obfuscation service provided by Korea Copyright Commission to prevent reverse-analysis.

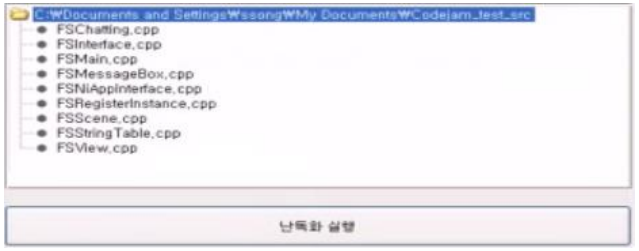
Magic keyboard security process : Reverse-analysis prevention

Code Jam introduction

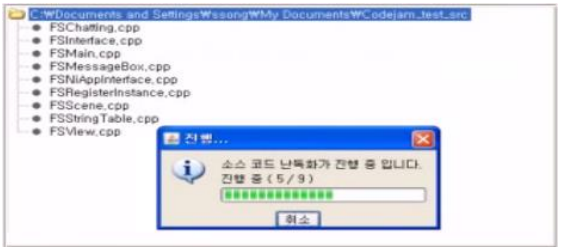
Product	content
Name	Codejam
Function	Code obfuscation (source code => obfuscated code) and program author identification (inserted program author identified database)
Organization	Korea Copyright Commission (www.codejam.or.kr)

Code obfuscation process

① select source code



② Obfuscation



③ Convert result

3.3 Cryptographic module summary

Avoidance of similar encrypted module overlap

Encrypted modules might be overlapped due to several protocol uses. It is necessary to refer to recommended priority of embedding algorithm to avoid overlap.

Magic keyboard Security process: Cryptographic module summary

MTS Algorithm

Secure Item	Encryption algorithm	Use
Magic keyboard	• RSA-1024 • SEED-128	• Server data protection • Extended E2E support(Optional)
SSL & extended E2E	• Open key Cryptosystem(Ex RSA-2048 , etc.) • Symmetric key Cryptosystem (Ex SEED-128, etc.)	• Session key sharing& prevention memory hacking • Server authentication(SSL)
PKI	• Open key Cryptosystem(Ex RSA-2048 , etc.) • symmetric key Cryptosystem (Ex SEED-128, etc.) • one-way hash function(Ex SHA2 etc.,)	Network forgery prevention Non-repudiation(electronic signature)

Priority of embedding algorithm

There is no need for users to use several embedding algorithms. Order of priority is as below;

1) SSL encrypted module should be used for SSL, extended E2E module should be used for extended E2E
2) PKI module should be used for PKI
3) Use Magic keyboard encrypted module

3.4 Magic keyboard security management

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

Magic keyboard security process : Magic keyboard security management

Compulsory quality for virtual keyboard

- Magic keyboard is proven to be the most secure virtual keyboard existing in the world regarding to button location hacking and screen hacking.
- Prevention of pharming
- Despite its simple design it is proven that it is not possible to guess a user password, (**Probability of guessing password is 0.0000000006977%**)

Magic keyboard eliminates security threats

Magic Keyboard tackles security threats such as memory hacking, reverse engineering, network forgery prevention.

Magic keyboard security result

As Magic keyboard satisfies all compulsory quality and security processes.

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