MBANK 、 OTP、Mobile Signature、eID Security Solution by Overlay SIM

New Generation of 2 Way Authentication Hardware Devices - Mobile Phones

The mobile phone meets the requirement of new generation of two way authentication hardware devices:

1、A daily necessities for people work and live.

2、Three trends of mobile phones as tools:

A、 Calling function

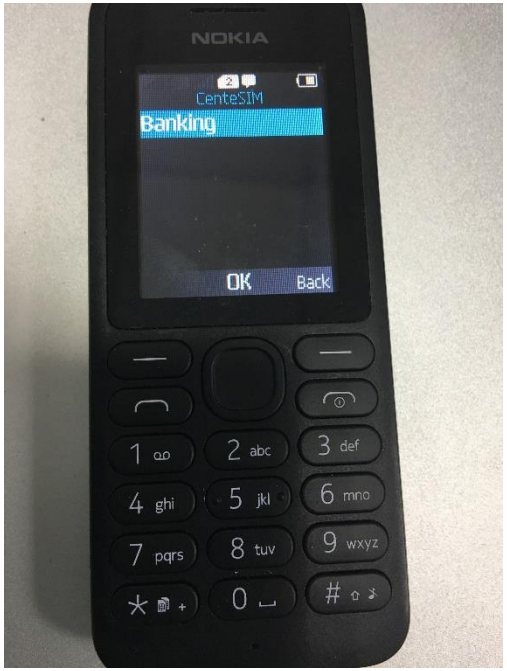
B、Mobile bank service

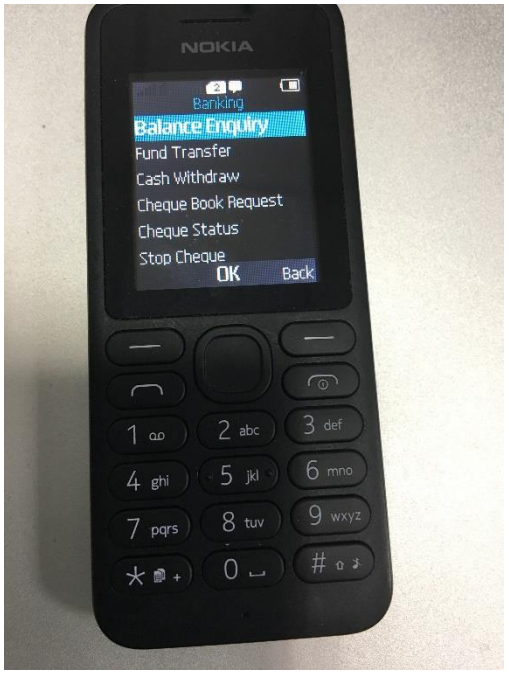
Mobile wallet
Mobile phone transportation card
Mobile payment

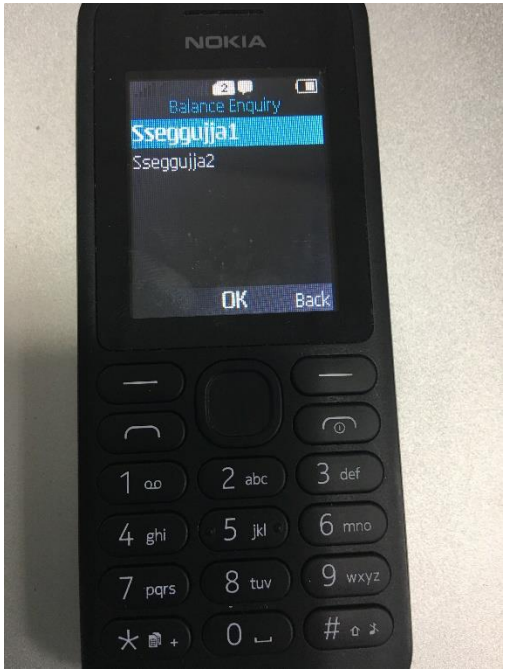
C、 Mobile phone network ID card

Chilitag 齊|耀|科|技

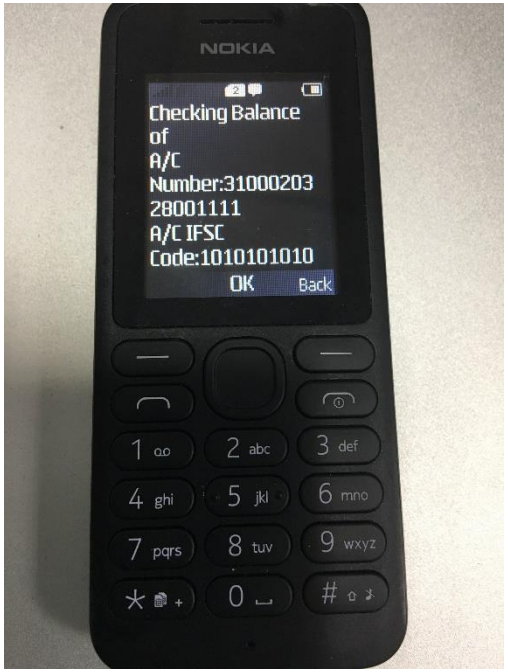
STK Banking function

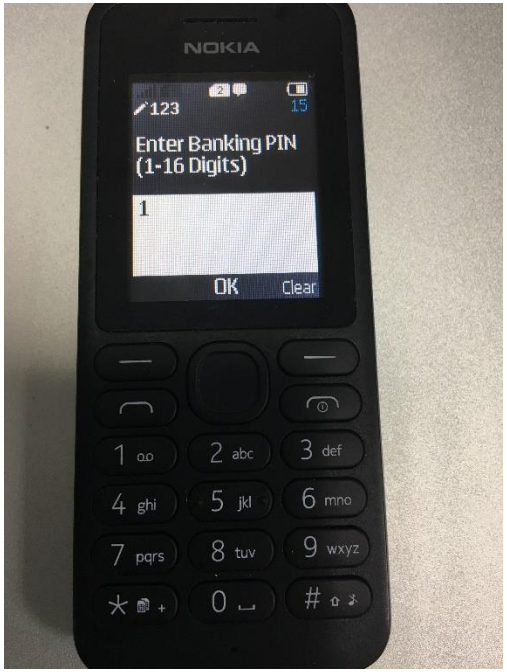






SMS Preview & Send

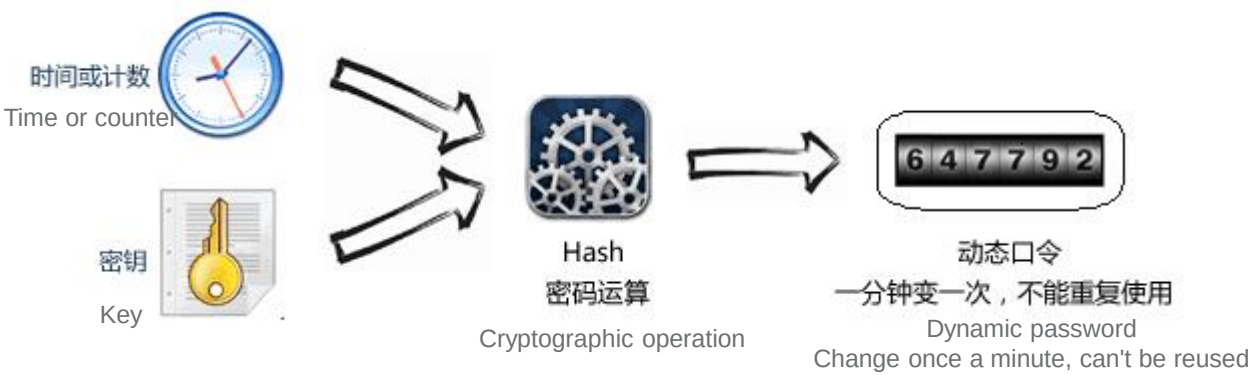




Overlay card OTP principle

There are the following modes:

- Time synchronization
- Event synchronization (counter synchronization, etc.)
- Challenge response



The OTP algorithm generally does not use symmetric encryption and decryption algorithms, such as: 3DES, AES, etc. A one-way hash algorithm is used. The reason is this, with the time-type scepter, the key + time (dynamic factor) = OTP, the time is known, the dynamic password generated every minute can be known through hardware, the 3DES algorithm is also public, so there is the possibility of launching a counter. The one-way hash algorithm, even if it knows the result of the calculation of the algorithm, OTP, because the algorithm guarantees one-way, it fundamentally cuts off the way to reverse the key.

Chiitag 齊|耀|科|技

What are OTP and mobile signature ?

Based on PKI technology, uses SIM card as a security carrier to achieve the industry-wide security technology for digitally signing business critical data.

Password

Log-In with OTP generated by overlay card or with the mobile signature

Digital certificate

China Mobile Certificate

B bank
USBKey

Bank A
WebBank

C Bank
K Key

D Bank
Mobile
Certificate

Put the key in each USB-key into your phone

Overlay card preset security algorithm key

Cell phone in hand, the network is worry-free!

Chilitag 齊|耀|科|技

Securities industry certificate

Subcontractor CA certificate

Bank A WebBank

B bank K Key

C Bank USBKey

Dedicated Overlay SIM card storage certificate and private key

Core：

✓Based on the PKI/CA system, with legal basis, Compliance with the Electronic Signature Act

✓Store user digits in mobile devices such as mobile phones, Certificate and private key for signature operation

✓With the help of the communication network, independent of the trading system Certificate channel

① Complete encryption, decryption, and signature in a dedicated overlay card operation, can be used in any mobile terminal

②Assist CA to manage user certificates and keys, online application, loss reporting, update, etc.

③Trigger the network when a user needs to sign. The network side sends the data to the user's mobile phone and signs the data using the private key in the mobile phone.

Chinitag 齊|耀|科|技

Business Frame

Application

Operation terminal

User

Financial industry

Government industry

Medical industry

Online game industry

E-commerce industry

Media industry

Generate and manage private keys and digital signatures

Docking application system, raw Random code, number of checks accordingly

Customer side unified authentication platform

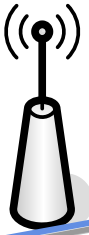
Industry CA

Certificate service

Moving side

Authentication

Dedicated overlay SIM card storage certificate & private key



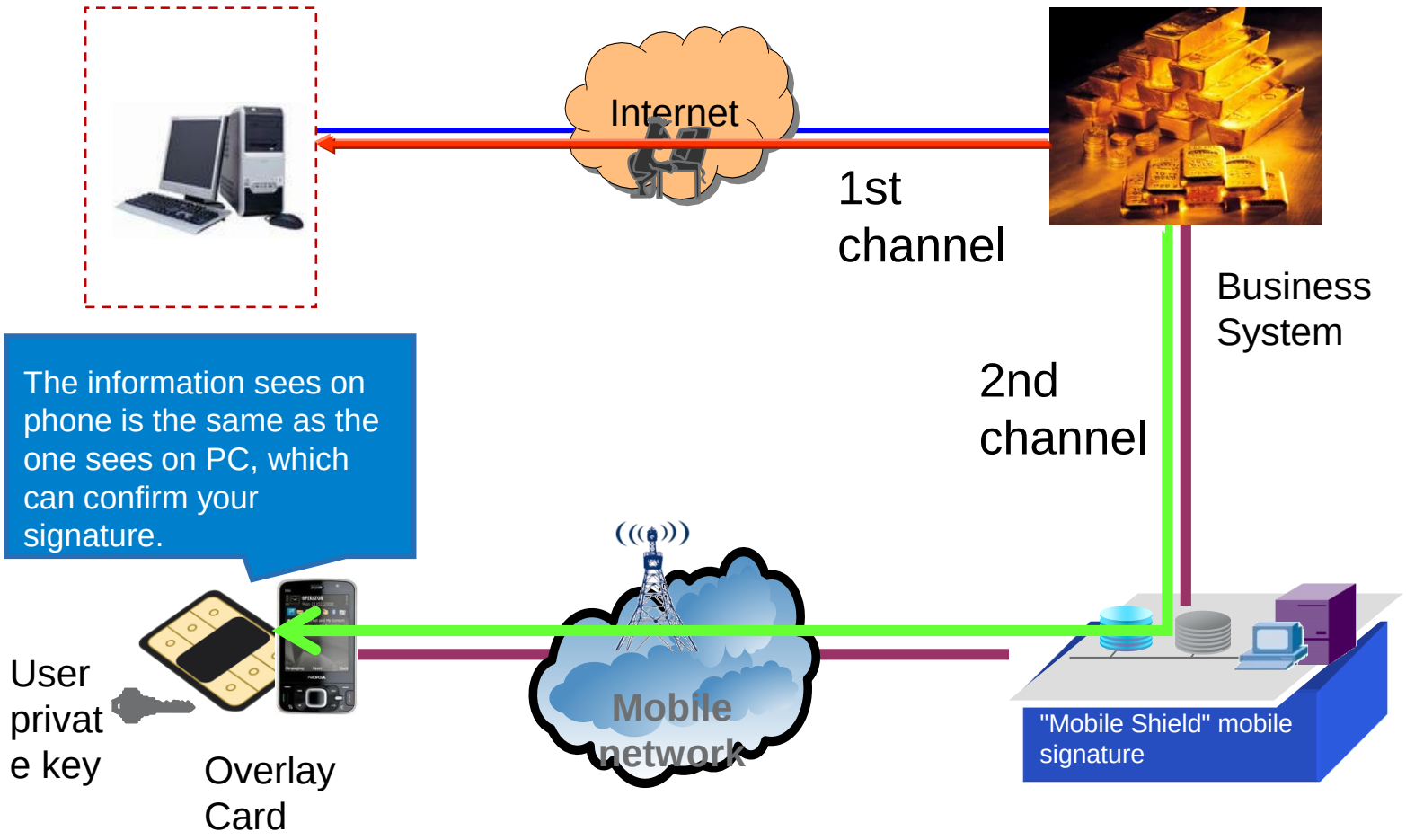
Mobile signature service platform

Manage mobile signature services:

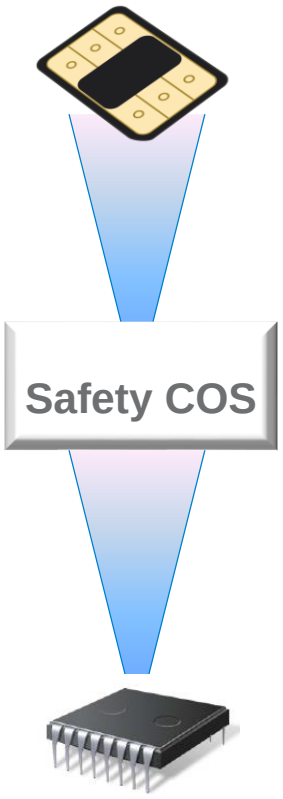
User, application, CA management

Chilitag 齊|耀|科|技

Core Advantage 1: Separation of Trading Channels & Certification Channels



Core Advantage 2 : Overlay Card as a Security Carrier



Safety Chip

- The overlay card interacts with the mobile CA service platform through a baseband module

- Secure closed system, no Subcontractor malware
- Secure communication guarantee, all data entering and leaving the card must be verified by MAC to ensure that the card only accepts data from the mobile signature service platform.
- Only the key pair generation, decryption, and signing operations are provided, and the private key remittance instruction is not provided, the private key never comes out of the card.

- Built-in password algorithm to generate public and private key pairs, encryption, decryption, signature, verification, etc.
- Built-in secure storage area for storing multiple pairs of keys for multi-CA support
- Anti-intrusion attack, anti-DPA/SPA design, secure private key

Chiitag 齊|耀|科|技

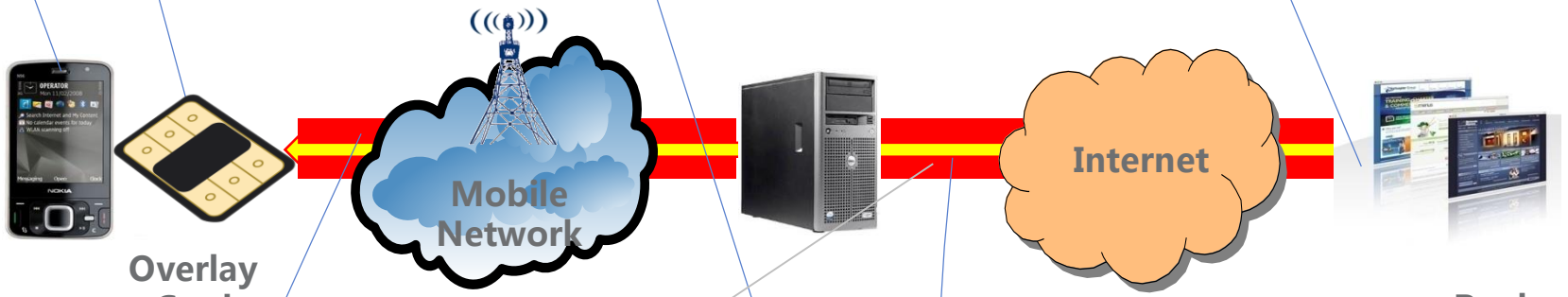
Core Advantage 3： End-to-end Security

Terminal: Baseband module directly supports STK application, so all terminal support

Overlay Card：Support des, RSA public key algorithm to achieve transaction data decryption and digital signature

Mobile signature service platform: realizes transaction management and security management of signatures, and the platform and card are authenticated by pre-shared key

Application: Interact with the mobile signature service platform through Web Service, no special requirements



Terminal

Overlay Card

Mobile signature service platform

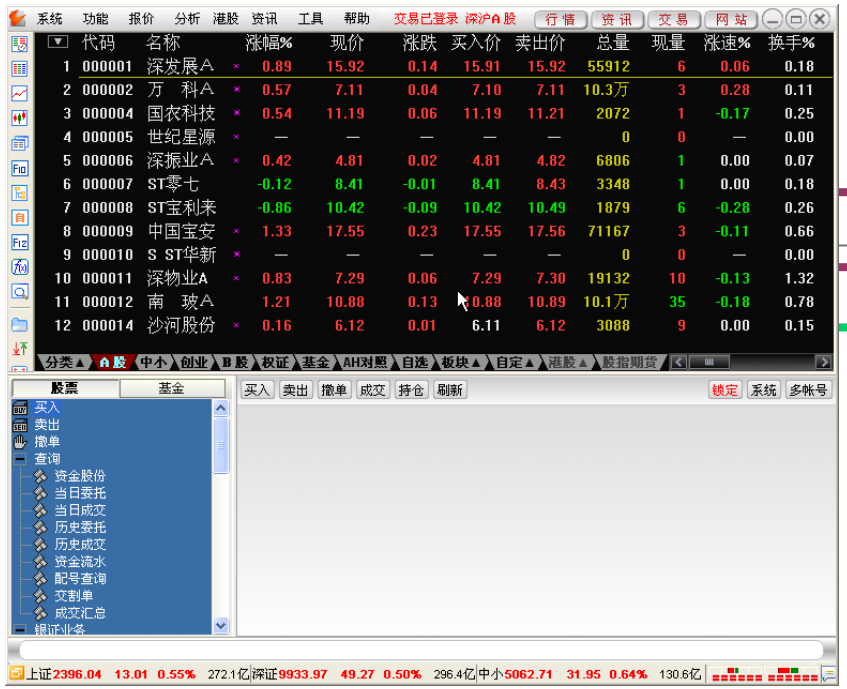
Bank core business system

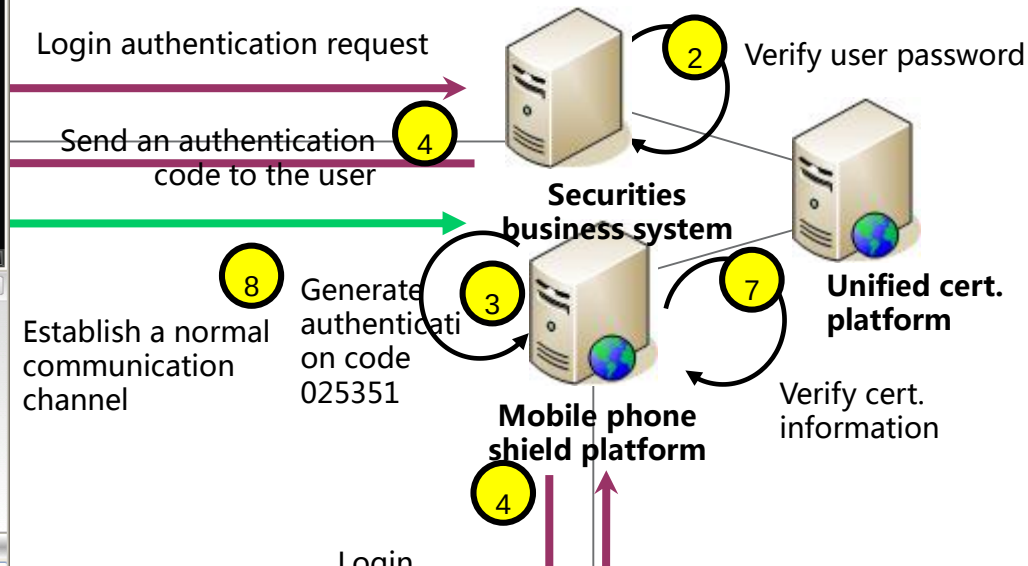
- **Two-way SSL between the platform and the system**，Implement two-way authentication;
- **MAC authentication mechanism between platform and overlay card**，Implement two-way authentication;

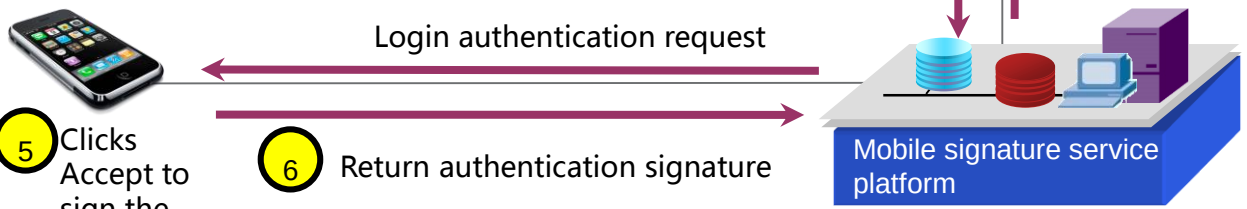
The transaction data is encrypted in the business system and sent to the overlay card in cipher text.，Only users and applications can see the data for end-to-end security protection

Chiitag 齊|耀|科|技

Delivery Deployment & Demo (e.g. securities industry)



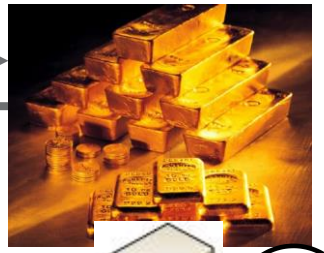




One-time Public-Private Key Pair Solution Based on smart phone

1

8



Business system

7

Verify certification information

Mobile phone shield platform

2

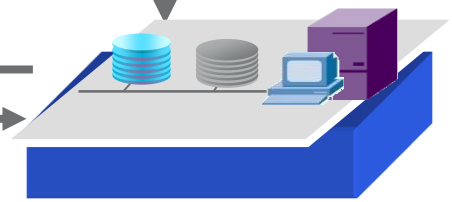
6

Generate a one-time public-private key pair

4

3

5



1 User access to system

2 System submits authentication request

3 Mobile signature service platform Forward the information to be signed to user

4 5 User's mobile phone generates a public-private key pair. Then use the private key to sign the signature data and return the signature result

6 Mobile signature service platform forwards signature results to mobile shield server

7 Mobile shield platform verification signature, return the verification results to the business system

8 After system receives the verification result, Passing or failing the user authentication

Chitag 齊|耀|科|技

User Innovation Experience

Numerous application systems in work & life

Work	Funds	Government affairs	Business	Healthy
OA	Pay bank	File tax	Online shop	Online registration
ERP	Accumulation fund	Accumulation fund inquiry	Online securities	E- medical record
CRM	Mortgage	Social security inquiry	Travelling	Medical report
SCM	Credit Card	Traffic violation	Group buying	

Securities industry certificate

Medical industry certificate

E-government certificate

Online game CA certificate

Subcontractor CA certificate

Web back USB KEY

Dedicated overlay SIM card storage certificate & private key

Chiitag 齊耀科技

User operation, management simplification

The user uses the mobile phone overlay SIM card to realize the mobile signature, reduce the cost of purchasing Ukey and token, no hardware requires, the investment in system construction and operation and maintenance is reduced, the process is simplified, and easily to maintain.

The comparison of current solutions for application service providers:

	Overlay card (mobile signature)	USB-KEY	token
Security Level	• Independent security authentication channel and process, hardware encryption, high security level • National policy support	•Hardware encryption, high security level •National policy support	• There are security vulnerabilities, easy to be phishing attacks, and the security level is relatively weak. • No National policy support
Application	• Cross-platform certification • The overlay card can store multiple user certificates, serve multiple business applications.	• Only for IE browser business applications • a USB-Key service for a business	• Cross-platform certification • A dynamic password token to serve a business
Marketing	• Mobile signature can implement product standardization, the market is large •Customer demand is tight, it takes time to form a product	• Has a certain market in the use of banks and enterprises	• There is a certain demand in industries with low security requirements. • Standardization of certified products cannot be achieved, Low security level, no promotion value.
Cost	• The lowest user opening cost • Have a certain cost of use	• Low opening cost • Usage cost can be ignored	•higher cost of use, and need to replace the cost every 3 to 5 years.
Convenience	• Only one overlay card is required to achieve identity authentication for multiple contracted services.	• Need to carry USB-Key device. •Only windows systems allow.	• Need to carry dynamic mouth stick equipment •Need to enter a dynamic password within the specified time

Chi 齊|耀|科|技

∞

無線生活　無限自由

anytime anywhere

http://www.chilitag.com.tw