Authentication Solution Optimized for Smart Devices

IKEYA Ryohei, OKADA Hideaki, KOUDA Keito, TEZUKA Yukiko

Abstract

Recently, users of smart devices such as smartphones and tablet terminals have been increasing both in the business and individual markets. In the business environment, the innovative use of smart devices has already begun and situations in which employees perform business tasks from outside the office by using smart devices are increasing. With regard to the individual market, various smart devices have already been released by the mobile carriers. This paper introduces an authentication solution that has been developed at NEC to support users to enjoy smart devices safely, securely and simply under the current trend for use with various terminals, regardless of the chosen OS or network.

Keywords

cloud, smartphone, multi-device, 3A Secure Token, software certificate, device authentication
ID integration, ID federation single sign-on, integrated management, user identification

1. Introduction

The introduction of smart devices in the business domain is increasing year on year and the number of shipments is expected to grow even more in the future.

Businesses are promoting the use of smartphones in support of their day to day activities because of the high portability, sophisticated appearance and for the cost reduction that results from paperless operation. In the individual market too, the number of smart device contracts of each mobile carrier increases every year.

In recent years the product configurations of terminal manufacturers have also been changed in order to focus more on smart device usage. Accordingly, the services provided for end users are also becoming smart device compatible.

These market trends are backed by the fact that smart devices have evolved into terminals that are usable by a wider range of users. This is due to the improved performance of smart devices, the enhanced user-friendly interfaces made possible by touchscreen panels, etc., and by the drop in prices.

Nevertheless, the use of smart devices is associated with several issues that should be solved by applying certain measures. This paper introduces the issues that mainly involve security in the use of smart devices as well as discussing the solutions proposed by NEC.

2. Businesses Utilizing Smart Devices

2.1 Purpose of Introduction of Smart Devices

In general, the devices used to support the business procedures of corporate enterprises have been PCs, but the advance of smart devices has been shifting work styles to those that utilize smart devices. The representative changes in work styles are as listed in the following:

1) Execution of business operations by remote access from outside the office.
2) Promotion of paperless meetings by adoption of electronic data.
3) Customer explanations and PR using a touchscreen panel.
4) Multi-device operations using PCs as well as smart devices.

Common to these changes is the “capability of executing operations with a single smart device.” We believe that this is also the main reason for the introduction of smart devices by multiple enterprises.

2.2 Issues with Smart Devices

One of the issues of the execution of business operations from outside the office is access control in cases when the Internet is used. With operations inside the office, terminals such as PCs are connected to a LAN, so access to various business systems is possible by simply logging in using the employee's ID and password. If such a system is opened to use outside the office, there is a risk of access by persons who have obtained the ID and password illegally.

One of the existing methods of preventing illegal access is the two-factor authentication that uses hardware or software tokens. The mobile PC is used to implement the two-factor authentication by using hardware tokens such as a one-time password generator or USB token. With smart devices, however, hardware connection is not as easy as for a PC because of the small number of connection ports for micro-USBs, etc. In addition, as the smart devices are operated in the hand, the usability is downgraded considerably if certain hardware has to be kept connected to it.

On the other hand, the two-factor authentication using software-based tokens is possible by adopting one-time password generation via an application or a software certificate. In this case, smart devices can be used with high convenience and without the need for additional equipment or facilities. However, with regard to the software certificate, the security itself is weaker than for the hardware tokens, which may easily result in an illegal access issue if the certificate is stolen.

As described above, the business use of smart devices is accompanied by the issue of "compatibility of security and convenience."

2.3 Multi-device Authentication

The NC7000-3A is an NEC product equipped with the "3A Secure Token" that achieves compatibility of security and convenience as discussed above. The features of this product are as follows:

1) Software certificate without the need of additional equipment
2) Camouflage technology providing protection against abuse in use, even in the case of theft
3) Multi-device compatibility regardless of OS for Windows PC, iOS or Android OS

(1) Software certificate without the need for additional equipment

The 3A Secure Token utilizes a software-based, an X.509-base software certificate in which the NC7000-3A adds original security features. The software certificate does not need special equipment such as a hardware token, so the costs of procurement and operation can thereby be reduced.

The 3A Secure Token can be used in two ways; the first method performs authentication based on the ID and password that an end user inputs and the second method performs authentication without the ID and password input.

The two methods have a trade-off relationship between security and convenience. It is therefore necessary to select the optimum method according to each service and/or use case.

(2) Camouflage technology protecting against abuse even in the case of theft

Due to the mechanism of the ordinary software certificate, it has been weak against the offline brute force attacks in cases when the certificate has been stolen. The 3A Secure Token has solved this problem by means of its camouflage technology (**Fig. 1**).

If an ordinary software certificate is used, a brute force attack can identify the secret key information, which is used illegally by a malicious attacker. With the camouflage technology of the 3A Secure Token, information seeming like a secret key is output every time and, if the attacker wants to find the real secret key, the attacker has to send an authentication request directly to the authentication server. Before the attacker completes checking all of the billion items of camouflaged secret key information, the authentication server locks the authentication when wrong attempts occur several times, so illegal access can be prevented.

In this way, the 3A Secure Token is a software certificate that is capable of achieving a security strength equivalent to that of the hardware tokens.

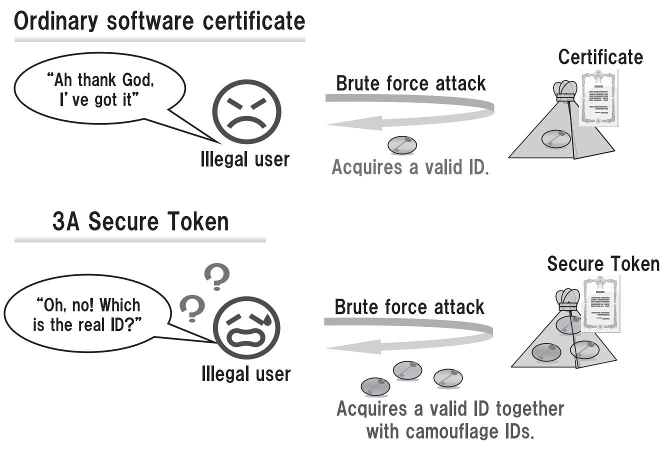

Ordinary software certificate
"Ah thank God, I' ve got it"
Illegal user
Brute force attack
Certificate
Acquires a valid ID.
3A Secure Token
"Oh, no! Which is the real ID?"
Illegal user
Brute force attack
Secure Token
Acquires a valid ID together with camouflage IDs.

Fig. 1 Camouflage technique of 3A Secure Token.

(3) Multi-device compatibility

Multi-device operations with which a single person uses several terminals including smart devices and PCs are increasing. Even in such cases authentication of the 3A Secure Token is possible by using the same ID and password.

The 3A Secure Token can be used on various terminals irrespective of OS choice, such as for the Windows PC, Android OS and iOS. There is also freedom from network restrictions and authentication is possible so far as the terminal in use is online.

In addition, installation of the software certificate is possible by online downloading from anywhere that you happen to be. There is no need to gather the terminals for the setting.

2.4 NEC Cloud Authentication

The multi-device authentication using the 3A Secure Token described above is provided as a cloud-based authentication service for corporations by "NEC Cloud Authentication". Provision of this service as a cloud service enables early startup of the service and reduction of the installation and operation costs (**Fig. 2**).

The usage situations in which the NEC Cloud Authentication can be applied are as described in the following.

- **Corporate system access from outside the office**
  Secure access from outside the office to a business-purpose web system is possible using the multi-device authentication facility.
- **Substitute to hardware token**
  Although the hardware token offers high security, its cost is very high. The NEC Cloud Authentication can be used to replace it with a software token, which offers an equivalent security level at a lower cost.

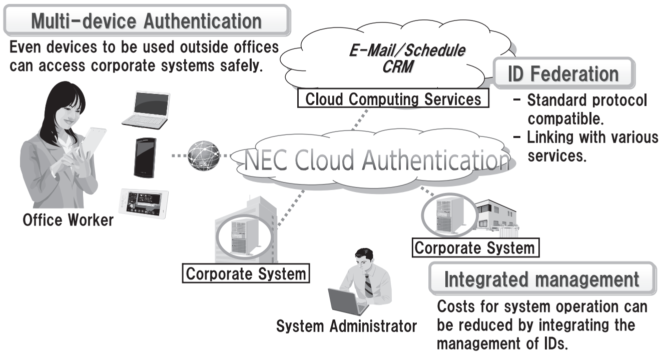

Multi-device Authentication
Even devices to be used outside offices can access corporate systems safely.
E-Mail/Schedule
CRM
Cloud Computing Services
ID Federation
- Standard protocol compatible.
- Linking with various services.
NEC Cloud Authentication
Office Worker
Corporate System
Corporate System
System Administrator
Integrated management
Costs for system operation can be reduced by integrating the management of IDs.

Fig. 2 Outline of NEC Cloud Authentication.

- **SSL-VPN authentication**
  The multi-device authentication is compatible with the RADIUS authentication. The RADIUS authentication is necessary when connecting an SSL-VPN device of the Juniper Series, etc. The NEC Cloud Authentication supports the RADIUS authentication, so that it can be used in SSL-VPN authentication.
- **Single sign-on between systems or cloud services**
  The compatibility with standard protocols such as OpenID 2.0, SAML 2.0 and OAuth 2.0 makes possible a single sign-on between services in different domains. A user is required to input ID and password only once when he/she accesses several services in different domains. Because the services share authentication results securely, a user is authenticated without inputting ID and password to all of them.
- **LDAP linkage**
  Linkage with an LDAP server of the enterprise is possible.

3. Authentication Service for Consumers

Consumer-oriented services also involve the security issue derived from the differences between smart devices and feature phones.

The 3G and LTE networks provided by the mobile carriers are capable of authenticating users by linking the SIM card of each user with the terminal. However, smart devices connect to the Internet, including Wi-Fi, in addition to mobile networks. This means that the Internet-based "open" world is now asked to implement the user security equivalent to the network authentications of mobile carriers (**Fig. 3**).

The means for enhancing security may include the use of hardware tokens or an increase in the number of password digits, but both of these solutions compromise the convenience of users.

Consequently, authentication using the 3A Secure Token is regarded as being promising.

The 3A Secure Token has high security in spite of the use of software a certificate, and it may be used regardless of terminal types and networks. It can be used by simply installing it without adding hardware and authentication of users is possible using a 4-digit PIN code in consideration of the appropriate usability. With its compatibility of security and convenience, it can be used safely even by consumers who do not have a high IT literacy level.

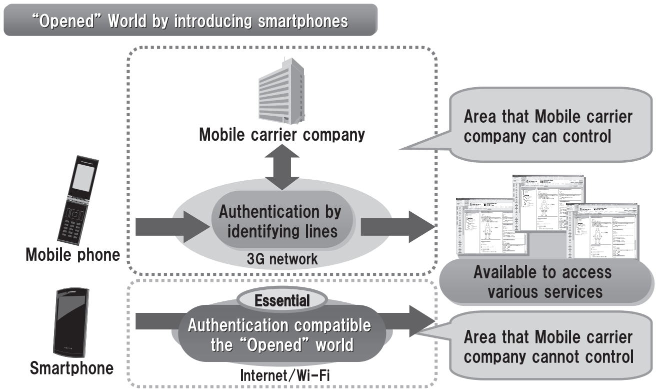

"Opened" World by introducing smartphones
Mobile carrier company
Area that Mobile carrier company can control
Mobile phone
Authentication by identifying lines
3G network
Available to access various services
Essential
Authentication compatible the "Opened" world
Smartphone
Internet/Wi-Fi
Area that Mobile carrier company cannot control

Fig. 3 Authentication method in the "opened" world.

The multi-device authentication facility makes it possible to assign an identifier to the accessing user in order to distribute a recommendation or personalized information to that user. The consumer-oriented cloud-based authentication makes it possible to use these features, and the service NEC provides is the "Smart Cloud Sign."

4. Conclusion

In this paper we discussed the security issues in the use of smart devices and proposed our authentication platform product and cloud authentication service as solutions. Smart devices are expected to be used actively in operations that involve confidential systems of enterprises. In this case, it will be necessary to develop solutions that place more emphasis on security. At NEC, we will continue to expand the services in this field and provide solutions for issues experienced by enterprises and consumer service providers.

*Android is a trademark or registered trademark of Google Inc.

*iOS is a trademark of Cisco Systems, Inc. in the U.S. and other countries and is used under license.

*LTE is a registered trademark of European Telecommunications Standards Institute□ETSI□.

*OpenID is a registered trademark of OpenID Foundation.

*Wi-Fi is a registered trademark of Wi-Fi Alliance.

*Windows is a registered trademark of Microsoft Corporation in the U.S. and other countries.

Authors' Profiles

IKEYA Ryohei
3rd Carrier Services Division
Carrier Services Operations Unit

OKADA Hideaki
Manager
3rd Carrier Services Division
Carrier Services Operations Unit

KOUDA Keito
Ubiquitous Network Systems Division
NEC Soft, Ltd.

TEZUKA Yukiko
3rd Carrier Services Division
Carrier Services Operations Unit

Information about the NEC Technical Journal

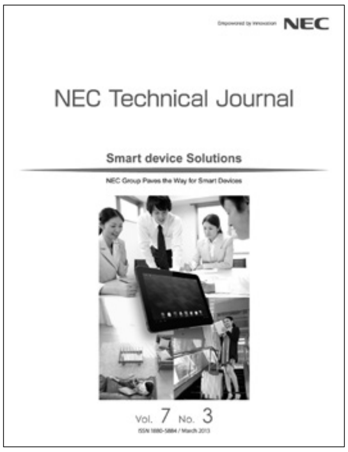
Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.7 No.3 Smart Device Solutions



Vol.7 No.3

March, 2013

Special Issue TOP