PassLogic has been adopted as an authentication option for Fujitsu’s managed infrastructure virtual desktop service, VCC.

Fujitsu’s VCC is a comprehensive cloud-based desktop service that utilizes Citrix client virtualization software Citrix Virtual Apps and Desktops. The virtual client cloud (VCC) features compatibility with Microsoft products (including support for Windows 10 version updates) and a high-performance graphics option (vGPU). The VCC focuses on high performance and reliability and provides a convenient and secure Virtual Desktop Infrastructure (VDI) platform to users. The VCC service is hosted in a highly secure Fujitsu data center.

PassLogic has been adopted as one of the authentication options for the VCC service. Users can secure access to their VDI environments with PassLogic’s tokenless one-time password authentication method.

We spoke to Ume-san from the VCC Business Department of Fujitsu’s Digital Service Business Unit. He is in charge of the basic design and operation of the VCC and the business negotiations relating to it.

Background Issues and Reasons for Introduction

- A desire to strengthen the type of user authentication that is required for connecting to a virtual desktop via the Internet.

- A desire to provide an authentication system that is comprised of a range of options that does not depend on any specialized authentication devices, unlike existing authentication systems which require specialized devices such as hardware tokens or smartphones with software tokens.

Benefits of Introduction

- The introduction of PassLogic’s tokenless one-time password authentication method strengthened authentication and improved convenience for users.

Working Style Reform with Virtual Desktops

In recent years, Telework is one of the work styles which companies have introduced in response to the government’s Work Style Reform program. Telework utilizes information and communications technology (ICT) to provide flexible working conditions that are not restricted by time or location; VDI is a key technology in this regard. The VCC utilizes Citrix Virtual Apps and Desktops to provide a one-stop VDI service that covers everything from deployment to monitoring and operational support of the VDI platform.

The VCC VDI service is hosted on servers located in a Fujitsu data center. The service facilitates both connections on a dedicated line from the company’s intranet and connections made via the Internet, which allow employees to access the service from home or when working remotely.

When a connection is made via the Internet an appropriate level of authentication is required in order to prevent unauthorised access. It is for this reason that a security policy will typically disallow user authentication that requires only a basic password. The VCC provides optional forms of authentication in addition to password authentication in order to enhance security and facilitate connections to the VDI service via the Internet. PassLogic is one of these options.

Reasons for Adopting PassLogic

PassLogic had been adopted as an authentication option for the FENICS II Universal Connect remote access service before it was adopted for the VCC virtual desktop service. PassLogic demonstrated its effectiveness and reliability to us on the FENICS service.

PassLogic’s distinguishing feature is that it is a one-time password authentication method which does not require the use of tokens. The user is only required to remember a pattern in order to use the one-time passwords - that is the reason why the PassLogic method is sometimes called “Pattern Authentication”. Typically, one-time passwords require the user to carry a hardware token or a software token installed on a smartphone, but PassLogic does not require such tokens. There are other forms of authentication like IC card authentication and biometric authentication, but these require a reader or scanner.

PassLogic’s tokenless one-time password method eliminates the need for specialized authentication devices such as tokens and readers, reducing device installation costs and operational management costs. We evaluated that this feature would be particularly beneficial to companies that have introduced telework.

For these reasons, we adopted PassLogic for the VCC service.
Tokenless One-Time Password Method

1. The user creates a pattern by selecting a sequence of cells from a grid. In the example above, the user has selected a V-shaped pattern.

2. For every login, the grid is displayed on the login page and each cell of the grid is filled with a random number. The user extracts the sequence of random numbers which corresponds to his or her pattern and inputs it into the password field.

3. Since the grid of random numbers is refreshed at every login the user's password will change for each login.

4. If the login is successful, a menu of available applications will be displayed. Select NetScaler.*

5. The Citrix Storefront portal screen will then be displayed. Select the desktop that you would like to use from the available desktops displayed and begin using it.

Cooperation and Operation of PassLogic and Citrix Virtual Apps and Desktops

If PassLogic authentication is selected, the PassLogic server will be hosted in the same data center as the Citrix Virtual Apps and Desktops server. PassLogic acts as a RADIUS server against which RADIUS authentication can be carried out on connection requests to the Citrix Virtual Apps and Desktops server.

The operations management of PassLogic can be fully managed by Fujitsu or it can be controlled on the customer side with a management screen supported by Fujitsu. In addition to the tokenless one-time password authentication method, PassLogic also supports hardware and software tokens and it is possible to assign different authentication methods and policies to different users and groups.

It is also possible to restrict access based on the device by adding client certificate authentication.

Fujitsu VCC virtual desktop service introduction page:
https://www.fujitsu.com/jp/services/infrastructure/virtualdesktop/vcc/