Our Design and Implementation of Multi-Factor Authentication Deployment for Microsoft 365 in Kyushu University

Kasahara, Yoshiaki
Kyushu University

Shimayoshi, Takao
Kyushu University

出版情報：2022, pp.56-61, 2022-03. Association for Computing Machinery: ACM
バージョン：

Our Design and Implementation of Multi-Factor Authentication Deployment for Microsoft 365 in Kyushu University

Yoshiaki Kasahara
kasahara.yoshiaki.820@m.kyushu-u.ac.jp
Kyushu University
Fukuoka, Japan

Takao Shimayoshi
simayosi@cc.kyushu-u.ac.jp
Kyushu University
Fukuoka, Japan

ABSTRACT

In Kyushu University, Information Infrastructure Initiative manages a Microsoft 365 tenant for our university members. We started offering Office 365 in 2016 and migrated our university-wide email service to Microsoft 365 Exchange Online in 2018. Due to the recent outbreak of COVID-19, off-campus uses of Microsoft 365 have increased, and concerns about account security arose. We discussed how to deploy Multi-Factor Authentication (MFA) to protect our users. Microsoft 365 comes with Azure Active Directory (Azure AD), and it includes built-in MFA functionality. With the basic Azure AD MFA, individual users can register MFA information anytime but have no control to enable or disable MFA. Tenant administrators need to enable MFA for each account. For a gradual deployment, we want to allow users to enroll in MFA and register information at their convenience. In addition to that, we want to prevent malicious attackers from registering their MFA information if an account should be already compromised. Such control was difficult with the basic Azure AD MFA. Since 2020 our tenant subscribes to Azure AD Premium P2 licenses, which provides Azure AD Conditional Access. Conditional Access enables fine controls of MFA and other user access behavior with security groups. We designed an MFA self-enrolling and configuration system, and implemented it with Microsoft Forms, Power Automate, Conditional Access, and in-house web applications. By design, this system prohibits MFA information registration until user's self-enrollment in MFA, and requests the user to register MFA information upon the next sign-in after the self-enrollment. This is supposed to reduce the possible unauthorized registration of MFA information. We extensively discussed implementation of various measures and preparation of documents to counter users' troubles and complaints. We started deploying MFA in April 2021, but we have not yet fully mandated MFA due to a push back from some executives expressing concern about the adverse effects of enforcing MFA too quickly.

CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**; • **Software and its engineering** → *System administration*; • **Information systems** → *Collaborative and social computing systems and tools.*

KEYWORDS

Multi-Factor Authentication, Account Security, Microsoft 365, Azure Active Directory

ACM Reference Format:
Yoshiaki Kasahara and Takao Shimayoshi. 2022. Our Design and Implementation of Multi-Factor Authentication Deployment for Microsoft 365 in Kyushu University. In *Proceedings of the 2022 ACM SIGUCCS Annual Conference (SIGUCCS '22), March 28-April 8, 2022, Virtual Event, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3501292.3511569

1 INTRODUCTION

Kyushu University is one of the national university corporations in Japan, located in Fukuoka Prefecture, Kyushu Island. A virtual agency "Information Infrastructure Initiative" (to which the authors belong) provides university-wide network infrastructure and ICT (information and communication technology) services for staff members and students in Kyushu University. Our services support almost thirty thousand users, including ten thousand staff members and twenty thousand students. As a part of our services, all of the students and staff have accounts with Microsoft 365 (formerly known as Office 365) service. In Kyushu University, a unique ten-digit identifier called the SSO-KID is randomly assigned to each student or staff member, by the central identity management (IdM) system of the university[3]. Users can sign in to Microsoft 365 using their SSO-KID and the corresponding password.

We started offering Office 365 in 2016 and renovated the environment in 2018[15]. Our university-wide email service (called *Kyushu University Primary Mail Service*) was migrated to Microsoft 365 Exchange Online in 2018 after the renovation[4, 5]. By email migration, more users started to sign in to Office 365. Due to the outbreak of COVID-19 in 2020, we had to promote remote-working, and more users started to use OneDrive for Business and Microsoft Teams outside the campus network. High usage meant that more valuable data was stored in Microsoft 365.

The number of reported Microsoft 365 related incidents is increasing worldwide, and concern regarding the account security of our Microsoft 365 environment arose. Introducing Multi-Factor Authentication (MFA) is an effective measure to mitigate the risk of identity theft.

Since 2016 we researched Microsoft 365's security features including its built-in MFA and discussed how to deploy MFA in our tenant to protect our users without disrupting the usability too much. Based on our research, we started designing full-fledged MFA deployment and its implementation for our environment in 2020. The initial deployment plan was to start the voluntary enrollment period in January 2021 and to start the mandatory enrollment period from April 2021. But, there was a push back from some

SIGUCCS '22, March 28-April 8, 2022, Virtual Event, USA

executives expressing concern about the adverse effects of introducing MFA too quickly. Due to a technical difficulty found later, the start of the voluntary enrollment period was delayed to April 2021, and mandatory enrollment has not yet been enforced. We are still in a voluntary period and the further deployment timeline is not decided as of this writing.

In this paper, we'd like to share the design, implementation, and experience of our MFA deployment.

2 MULTI-FACTOR AUTHENTICATION IN MICROSOFT 365

In this section, we explain how MFA in Microsoft 365 with Azure Active Directory (Azure AD) works as far as we understood. Microsoft 365 and Azure AD are evolving rapidly and as a result, new features may emerge.

2.1 Azure Active Directory (Azure AD)

Azure AD is Microsoft's cloud-based identity and access management service[12]. Every Microsoft 365 tenant is bundled with an Azure AD tenant for user management.

When you use Microsoft 365 as a standalone service, you register all your user accounts to Azure AD and manage them using the Microsoft 365 admin portal and Azure AD admin portal. You can synchronize user account data with your on-premise Active Directory by Azure AD Connect, and also configure authentication federation with your on-premise AD Federation Service.

2.2 Azure AD MFA

Azure AD has a built-in MFA functionality, called Azure AD Multi-Factor Authentication. Azure AD requests a user to provide preregistered MFA information for personal identification in following to usual password under specified conditions. For example, a user has to answer a notification sent to the user's smartphone application (Microsoft Authenticator), enter the 6-digit time-based one-time password (TOTP) generated by an authenticator application or sent via SMS, or receive a phone call and push the pound key on the phone.

In general information and communication services such as Google, Twitter, and Facebook, any user can request to enable MFA for one's account, and then the service immediately requests that user to register one's MFA information such as a mobile phone number or an authenticator application. On the other hand, Azure AD doesn't allow individual users to enable MFA by themselves. Only an administrator can enable users' MFA through the Azure AD admin portal.

Another difference is when a user registers one's MFA information. A user may register one's MFA information anytime by accessing the MFA information registration page[1], even if MFA is not enabled for the account. MFA is not automatically enabled after the registration, so MFA is not required to sign in to Microsoft 365 (except the MFA information registration page itself to protect the registered MFA information). If MFA is enabled by an administrator but a user has not registered one's MFA information yet, that user is redirected to the MFA information registration page upon the next sign-in. That user cannot finish sign-in until the MFA information registration is finished.

There are a few ways to enable or enforce MFA for a user in Azure AD. *Per-User MFA Setting* and *Security Defaults* are available with free licenses. *Conditional Access* and *Identity Protection* are only available with premium licenses.

2.3 Free features

2.3.1 Per-User MFA Setting. There is a configuration screen in the Azure AD admin portal where an administrator can enable and disable the MFA of each account. By enabling MFA for a user, that user will always require to provide MFA information upon sign-in (with exceptions such as a connection from pre-defined trusted IP address ranges)[8].

Currently, Microsoft doesn't recommend using this setting unless your Azure AD licenses don't include Conditional Access and you don't want to use Security Default.

2.3.2 Security Defaults. Security Default is a collective setting of Azure AD to enable multiple security enforcement to the Azure AD tenant[11]. It includes requiring all users to register MFA information with the Microsoft Authenticator application and blocking legacy authentication protocols such as IMAP and POP with password authentication. This feature may be enabled by default in a new Microsoft 365 tenant created after October 2019.

This feature applies to all users and doesn't have any configuration option. It cannot be enabled simultaneously with Conditional Access.

2.4 Premium Features

2.4.1 Conditional Access. Conditional Access is a premium feature of Azure AD available with the Premium P1 licenses and above. It allows an administrator to define policies to control user access based on various conditions[7]. For example, a policy can take the following various conditions into account to make a decision. Conditions include user or group membership, the client's IP location, device platforms, applications, and sign-in risks (requires Identity Protection).

Based on these conditions, the policy can enforce decisions to user access. The decision includes blocking access and granting access with an additional requirement such as MFA verification. You can define multiple policies, and these policies are evaluated simultaneously and all decisions are enforced.

2.4.2 Identity Protection. Identity Protection is available with the Premium P2 licenses[13]. This is a risk-based authentication mechanism provided by Microsoft. The individual sign-in is evaluated and marked with a risk value (high, medium, low, or no risk). A Conditional Access policy can take the risk value into account and make a decision, such as blocking access entirely or require MFA.

Additionally, Identity Protection provides three preconfigured access policies including *User risk policy*, *Sign-risk policy*, and *MFA registration policy*. The first two are simple risk-based authentication policies. The last one is a policy to enforce users to register their MFA information during their sign-in. It has a unique and convenient feature that a user can postpone the required MFA information registration for 14 days. Unfortunately, you cannot

[1] https://aka.ms/mfasetup

change the length or reset the remaining grace period. This feature is not available with other MFA enforcement mechanisms such as the per-user MFA setting or a Conditional Access policy. A user must register MFA information during the next sign-in with these methods.

3 MFA DEPLOYMENT DESIGN AND IMPLEMENTATION

In this section, we explain how the design, implementation, and experience of our MFA deployment evolved in roughly chronological order. The implementation detail of some components will be explained in Section 4.

From the beginning, MFA has been considered a highly desirable feature to protect user accounts. Our ultimate goal should be to enforce MFA on all users without exception, but it cannot be done at once considering the size of our user base. We need a way of gradually introducing MFA by allowing users to enroll MFA at their convenience in the beginning. We call it *the voluntary enrollment period*.

As explained in 2.2, Azure AD doesn't allow users to change the MFA setting. We don't want to increase the administrative load by manually changing the MFA setting upon user requests. Therefore, a self-service system must be implemented outside of Azure AD.

After a certain deadline has passed or enough users have enrolled, we can enforce MFA on new users and remaining users who have not enrolled yet. We call it *the mandatory enrollment period*.

3.1 First MFA Trial with Self-Service MFA Switch

In 2016 we started offering Office 365 to our university members and immediately recognized that there was a built-in MFA feature. At that time our licenses were Office 365 for Education A1, so only per-user MFA setting (in 2.3.1) was available.

After an internal test of MFA, we tried to offer the MFA feature to early adapters as the voluntary enrollment period. We implemented a self-service MFA switch in the user profile page of our central IdM. Users could enable and disable the MFA of their Office 365 account with this switch. IdM would change their per-user MFA settings using the Azure AD PowerShell module. At first, it seemed working, but soon we realized our misunderstanding about the details of the setting. It is a three-state switch instead of two, and you have to know the previous state of the value before re-enabling MFA. The implementation was abandoned due to some unexpected behavior, and MFA deployment had been put on hold.

3.2 Exploring Premium Features for MFA deployment

In 2017, we were notified that the licenses of our Office 365 tenant would change in 2020 because our agreement with Microsoft would be discontinued. Microsoft proposed a new agreement covering Office 365 A3, which includes Azure AD Premium P1 licenses. That meant that we would be able to leverage Conditional Access (in 2.4.1) of Azure AD from 2020. We had not realized the flexibility provided by Conditional Access yet.

In SIGUCCS 2019, there was a presentation about avoiding phishing traps[14]. One of the topics was about a self-service MFA enrollment system and its deployment. After the session, we asked the author about the details and she kindly provided us the internal detail of the system. It was implemented using Microsoft services including PowerApps, Flow, SharePoint, Conditional Access, and Azure groups. We realized that a similar system could be implemented with our new licensing without purchasing a third-party service. The information greatly helped us toward designing our system for the voluntary enrollment period.

In 2019, we evaluated the Office 365 E5 trial licenses including Azure AD Premium P2 and explored the premium features of Azure AD and other Office 365 services. The purpose of the trial was to evaluate the benefit of additional features available in A5 (the educational equivalent of E5 licenses) before the change of the agreement with Microsoft and decided which licenses we should subscribe to considering the additional licensing cost.

Among premium features, the risk-based authentication mechanism of Identity Protection (in 2.4.2) seemed desirable, as it could effectively protect users while minimizing intrusion. Without Identity Protection, MFA is required with simple conditions (such as all off-campus accesses). Some ordinary users might feel it too disturbing. With Identity Protection, a user will only occasionally be prompted to validate their MFA session, and attackers without registered MFA methods will be blocked by the risk-based MFA request (if it works as advertised). In addition to that, email protocols such as IMAP and POP were not compatible with MFA at that time. Requiring MFA for these protocols blocks the sign-in entirely because MFA information cannot be provided using these protocols. Identity Protection was required to block only high-risk sign-ins while allowing legitimate access with these protocols.

By estimation, A5 licenses were too expensive to subscribe to, but there might be some room to add individual licenses to A3 licenses. The Identity Protection were highly desired as explained above. To propose these licenses be included in the agreement, we explained the benefit of the licenses and the importance for the flexible deployment of MFA. The proposal was accepted and the budget for Azure AD Premium P2 was secured.

In May 2020 we subscribed to Azure AD Premium P2 licenses and started experimenting with various MFA-related behavior of Azure AD including Conditional Access and Identity Protection. We gradually learned the details explained in Section 2.

3.3 A Design with Automatic MFA Enabling Flow

We first started designing and implementing a self-service MFA enabling mechanism for the voluntary period. Due to our lack of experience with PowerApps, we changed our design from the system presented in [14]. Our design was inspired by MFA deployment materials provided by Microsoft[10]. In this material, users are required to register their MFA information first before MFA is enabled. Unfortunately, a Conditional Access policy cannot check if a user has already registered one's MFA information or not, so an administrator has to enable MFA manually or in a batch, which may cause a significant delay between registration of MFA information and enabling MFA. During the voluntary enrollment period of our plan,

we also wanted to direct users to the MFA information registration page, and then enable MFA automatically after the MFA registration. Once enabled, users are unable to disable MFA for their accounts.

We anticipated that a Power Automate flow could be implemented which periodically collected the list of users who had registered their MFA information and added the users to a certain security group. MFA would be enabled for these users through a Conditional Access policy referring to the security group. The list of MFA registered users can be retrieved via Microsoft Graph API[9] using an HTTP connector of Power Automate.

There are group-related Azure AD connectors that can retrieve or modify the membership of a security group, but these are very slow especially when the group is large. To reduce the use of Azure AD connectors, the flow stored a list of members in a SharePoint file. When the flow was invoked the next time, it retrieved the SharePoint file and the new list of MFA registered users, took the difference of these two lists, and added the difference to the security group with Graph API instead of the Azure AD connector. It took several months of trial and error to fully implement the flow.

3.4 Self-Service MFA Configuration Form

In addition to the gradual deployment with the voluntary enrollment period, we were concerned about when and how often MFA information should be requested upon sign-in. Always requiring MFA is the most secure, but we felt that this might be too disruptive for an ordinary user. On the other hand, if MFA is required only with high-risk sign-ins from the beginning, an inexperienced user might forget about MFA and stop carrying a device required or forget how to provide one's MFA information. Consequently, we prepared a self-service MFA configuration form to provide a way for our user population to change preferences and set the initial setting to a stronger MFA requirement. The details are explained in 4.1.

We wanted users to get used to handling MFA requests in the beginning, so the default policy was decided that MFA was always required and the session timeout was 7 days. They may feel uncomfortable about the frequent MFA requests and change the configuration by this form. In addition to that, users are not allowed to stop using MFA entirely. At least requiring MFA under the high-risk condition should be remained to protect the user's account.

3.5 Preparing a Deployment Plan

While implementing them, we prepared a deployment plan. Our initial plan was to start the voluntary enrollment period in January 2021 and proceed to the mandatory enrollment period in April 2021.

The MFA registration policy of Azure AD Identity Protection would be used for the mandatory enrollment period. All users without MFA information will be required to register it upon the next sign-in (with a grace period of 14 days). In addition to that, we have a plan to limit off-campus access to the MFA information registration page to a certain period after the account is created. We want to protect user accounts without MFA information from malicious attackers by restricting the MFA registration period. Even a legitimate user may not sign in to Microsoft 365 from off-campus when the MFA information registration page is blocked. Administrator intervention is required to handle such a case.

In December 2020, our MFA deployment plan was rejected by some executives without a chance to explain, because they were concerned about the adverse effects of hasty MFA enforcement.

3.6 Documentation and Self-Service Recovery Support

The plan to enforce MFA from April 2021 was rejected, but we were allowed to start the voluntary enrollment period. We wrote an article about the preview of the MFA deployment in the 2021 spring newsletter of the Information Infrastructure Initiative.

We started compiling manuals to explain how to enable MFA and how to register MFA information in various scenarios. Our concern was how to support users who didn't have a smartphone or other mobile devices (such as a laptop). We had to consider such users because we want to require MFA for all users once we enter the mandatory enrollment period. All students should have a laptop because our university employs student BYOD[2], but there may be some staff members who have no mobile device.

While testing Conditional Access, we realized that once MFA information for a user was registered to Azure AD, this MFA information would be required to access the MFA information registration page regardless of existing Conditional Access policies. For example, once a user has registered one's office phone number, the user cannot register another MFA information at home because the MFA system calls the office phone, which is out of reach.

To resolve such a situation, we need to provide a way to register an arbitrary phone number without signing in to Microsoft 365. To achieve this, we decided to implement *the Alternative Phone Number Registration* form outside of Microsoft 365. The detail is explained in 4.2. In addition to the original intention, this form can be used for self-service recovery when a user has lost or changed a mobile phone and the registered phone number becomes invalid.

By leveraging this form, the recommended order for registering MFA information with or without a mobile device was prepared. To reduce the risk of losing MFA methods, we encourage users to register multiple MFA information including an authenticator app, an authenticator browser extension including laptop, home, and office desktop PCs, a mobile phone number, an office phone number, and a home phone number as much as possible. These recommendations were inspired by the MFA manual of Kyoto University[6].

3.7 A Setback

During the test of automatic MFA enabling flow, more than 500 users who had happened to register MFA information were found. To start the voluntary period using the flow, we had to remove the MFA information from them, because these users will be collected by the flow and MFA would be enabled unexpectedly. In February 2021, We temporarily prohibited users to access the MFA information registration page by a Conditional Access policy, sent a notification email about removing their MFA information to relevant users, and then cleared the MFA information of these accounts.

Then, an unexpected thing happened. We prohibited users to register MFA information, but soon new MFA registered users appeared out of nowhere. We checked the details of the information

and found that it was Windows Hello for Business. It seemed to be related to the mobile device management (MDM) in Azure AD. There was no plan to manage users' own devices with MDM in our tenant, so we had little knowledge about that. The behavior of this MFA registration couldn't be controlled with a Conditional Access policy at that time. We didn't have a Windows Hello capable device, so it was impossible to investigate further. We concluded that we couldn't deploy this flow at that time, and ended up abandoning this plan altogether.

3.8 A Design with Self-Service MFA Enabling Form

We needed another way to enable MFA and created a simple form containing only a "Yes" check box and a submit button with some explanation about enabling MFA. There is no option because we don't allow users to disable MFA later. A Power Automate flow will be triggered by the form and simply adds the submitted user to a security group referred by Conditional Access policies. Initially, we avoided this idea because it required additional action from users. A good side effect of this method is that we can make sure that users read the instruction on the form and agreed about the consequence of enabling MFA.

In addition, we added another Conditional Access policy only to allow MFA-enabled users to access the MFA information registration page. When we discussed MFA deployment with administrators of other universities, a frequent topic was how to avoid malicious attackers registering their MFA information before the legitimate user had registered it. In our plan, a user can register one's MFA information only after submitting the MFA enabling form. After the submission, that user will be directed to our MFA information registration manual and expected to register an MFA information immediately. We believe that this is a good measure to prohibit malicious attackers from registering malicious MFA information during the voluntary enrollment period.

3.9 Windows Virtual Desktop for Remote Workers

Due to the COVID-19 pandemic, the Administration Bureau ICT group in Kyushu University needed to provide a remote working environment to office workers. For remote working, access to the internal office LAN was required. To provide off-campus access, they decided to try Microsoft Windows Virtual Desktop (WVD) because the required licenses were included in Microsoft 365 A3.

In 2020, the WVD tenant was separately prepared and connected to the office LAN via Microsoft Azure ExpressRoute, and the user authentication was processed by our Microsoft 365 tenant. To protect the internal LAN, the ICT group decided to require MFA for users of WVD.

The trial for standard users was planned for February 2021 but postponed to May 2021 due to some technical difficulties. At that time, the voluntary enrollment period of Microsoft 365 MFA had been started, so the ICT group prepared a user's manual for the WVD based on our MFA manual, and WVD trial users were requested to enable MFA using our MFA enabling form. Some of the trial users didn't know well how MFA would work, so we had received some unexpected inquiries and trouble reports. These incidents were beneficial to improve our MFA deployment implementation and documents.

3.10 Current Status

We are still in a voluntary period and the further deployment timeline is not decided as of this writing. About 500 users had voluntarily enabled MFA at the end of September 2021. Our implementation seems working as expected because there were few inquiries from these users. We have not yet started the mandatory enrollment period, so we cannot discuss the outcome of our entire plan yet.

4 IMPLEMENTATION DETAIL

4.1 Self-Service MFA Configuration

The self-service MFA configuration form presents the following selection to a user. A user can change the condition when one's MFA information is required, and how often a sign-in session will be expired.

(1) Require MFA verification under the following condition(s)
   a. Only when the estimated risk of the sign-in is "high", such as a sign-in from an unfamiliar location
   b. Always except Kyushu University's campus network
   c. Always regardless of your location/network
(2) How often you need to sign-in again
   a. High frequency (once per 7 days)
   b. Normal (once per 90 days)

To reflect the user's preferences, five Conditional Access policies were prepared for each selection. Each policy looks up some security groups to determine if the policy is applied to a user. For our purpose, four security groups are enough to control the behavior.

After enabling MFA, users are always included in the security group *sg-mfa-enrolled* and never removed. The group membership of the other three will be modified according to a user's selection as shown in Table 1. For example, when a user changed the setting to (1) a. High-risk only and (2) b. 90 days, a Power Automate

Table 1: Group Membership Change by Configuration

	(1) Cond.			(2) Freq.	
Group name	a.	b.	c.	a.	b.
sg-mfa-highrisk	+	-	-		
sg-mfa-external	-	+	-		
sg-mfa-session				-	+

+: add -: remove

Table 2: Security Groups and Conditional Access Policies

	Conditional Access Policies				
Group name	*High-Risk*	*External*	*Always*	*7d*	*90d*
sg-mfa-enrolled	+		+	+	
sg-mfa-highrisk	+		-		
sg-mfa-external	+	+	-		
sg-mfa-session				-	+

+: include -: exclude

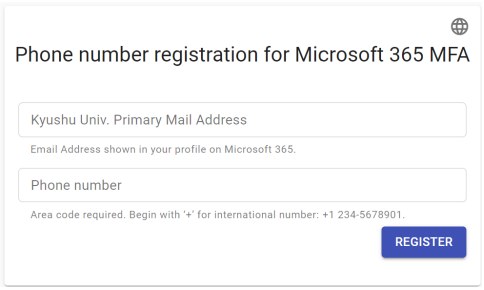

Figure 1: The Form to Register Phone Number

flow would be triggered and the user became a member of *sg-mfa-highrisk* and *sg-mfa-session*. Also, the user would be removed from *sg-mfa-external* if needed.

Each Conditional Access policy checks the membership of security groups as shown in Table 2. *High-Risk*, *External*, and *Always* policies require MFA for high-risk sign-ins, for sign-ins from the outside of campus network, and for all sign-ins, respectively. *7d* and *90d* policies expire MFA in 7 and 90 days, respectively. Initially, users belong to *sg-mfa-enrolled* only, so *Always*, *High-Risk*, and *7d* conditions will be applied. In a Conditional Access policy, *exclude* superseded *include*, so when a user becomes a member of both *sg-mfa-enrolled* and *sg-mfa-external* by the selection, the user is excluded from *Always* policy but included in *External* and *High-Risk* policies.

4.2 Alternative Phone Number Registration

We need a way to register an arbitrary phone number without signing in to Microsoft 365. We implemented the *Alternative Phone Number Registration* form shown in Figure 1 using our web hosting service.

This form is a single-page application with REST API to modify the Azure AD configuration. The client-side uses React[1] and the server-side uses Sinatra[16] on Ruby. To access this form, users need to sign in with Shibboleth IdP provided by our central IdM system. An authorized user can enter a phone number and the number is registered into one of three phone number slots of Azure AD MFA via Microsoft Graph API. To protect this form from abuse, off-campus access requires the matrix password on the staff ID card, which is a kind of MFA.

5 CONCLUSION

In this paper, we explained the design, implementation, and experience of our Microsoft 365 MFA deployment. We believe that the hardest part of the deployment is to enforce the use of MFA to all Microsoft 365 users, and we haven't started that process yet. We would like to report our experience in the future after our MFA deployment is completed.

Other than Microsoft 365, our central IdM also has a plan to deploy TOTP-based MFA in their Shibboleth IdP. It might be confusing for a user to use multiple MFA systems, so we need to continue discussing how we should improve user experience in our university ICT environment as a whole.

ACKNOWLEDGMENTS

The authors thank all of the other members of the Collaborative Infrastructure Working Group, Information Infrastructure Initiative, Kyushu University.

REFERENCES

[1] Facebook Inc. 2021. React – A JavaScript library for building user interfaces. Retrieved 2021-11-18 from https://reactjs.org
[2] Naomi Fujimura. 2013. Bring Your Own Computers Project in Kyushu University. In *Proceedings of the 41st Annual ACM SIGUCCS Conference on User Services* (Chicago, Illinois, USA) *(SIGUCCS '13)*. ACM, New York, NY, USA, 43–50. https://doi.org/10.1145/2504776.2504789
[3] Eisuke Ito, Yoshiaki Kasahara, and Naomi Fujimura. 2013. Implementation and Operation of the Kyushu University Authentication System. In *Proceedings of the 41st Annual ACM SIGUCCS Conference on User Services* (Chicago, Illinois, USA) *(SIGUCCS '13)*. ACM, New York, NY, USA, 137–142. https://doi.org/10.1145/2504776.2504788
[4] Yoshiaki Kasahara, Takao Shimayoshi, Eisuke Ito, and Naomi Fujimura. 2018. The Past, Current, and Future of Our Email Services in Kyushu University. In *Proceedings of the 2018 ACM on SIGUCCS Annual Conference* (Orlando, Florida, USA) *(SIGUCCS '18)*. ACM, New York, NY, USA, 103–106. https://doi.org/10.1145/3235715.3235737
[5] Yoshiaki Kasahara, Takao Shimayoshi, Tadayuki Miyaguchi, and Naomi Fujimura. 2019. Migrate Legacy Email Services in Kyushu University to Exchange Online. In *Proceedings of the 2019 ACM SIGUCCS Annual Conference* (New Orleans, LA, USA) *(SIGUCCS '19)*. Association for Computing Machinery, New York, NY, USA, 127–131. https://doi.org/10.1145/3347709.3347817
[6] Kyoto University. 2021. Multi-Factor Authentication User's Guide. Retrieved 2021-09-26 from https://sites.google.com/kyoto-u.ac.jp/mfa/
[7] Microsoft. 2021. Azure AD Conditional Access documentation. Retrieved 2021-09-21 from https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/
[8] Microsoft. 2021. Enable per-user Azure AD Multi-Factor Authentication to secure sign-in events. Retrieved 2021-09-21 from https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates
[9] Microsoft. 2021. List credentialUserRegistrationDetails. Retrieved 2021-09-21 from https://docs.microsoft.com/en-us/graph/api/reportroot-list-credentialuserregistrationdetails
[10] Microsoft. 2021. Multi-factor authentication rollout materials. Retrieved 2021-11-18 from https://aka.ms/mfatemplates
[11] Microsoft. 2021. What are security defaults? Retrieved 2021-09-21 from https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults
[12] Microsoft. 2021. What is Azure Active Directory? Retrieved 2021-09-21 from https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis
[13] Microsoft. 2021. What is Identity Protection? Retrieved 2021-09-21 from https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
[14] Katelin A Moul. 2019. Avoid Phishing Traps. In *Proceedings of the 2019 ACM SIGUCCS Annual Conference* (New Orleans, LA, USA) *(SIGUCCS '19)*. Association for Computing Machinery, New York, NY, USA, 199–208. https://doi.org/10.1145/3347709.3347774
[15] Takao Shimayoshi, Yoshiaki Kasahara, and Naomi Fujimura. 2019. Renovation of the Office 365 Environment in Kyushu University: Integration of Account Management and Authentication. In *Proceedings of the 2019 ACM SIGUCCS Annual Conference* (New Orleans, LA, USA) *(SIGUCCS '19)*. Association for Computing Machinery, New York, NY, USA, 135–139. https://doi.org/10.1145/3347709.3347819
[16] Sinatra. 2021. GitHub - sinatra/sinatra: Classy web-development dressed in a DSL (official / canonical repo). Retrieved 2021-11-18 from https://github.com/sinatra/sinatra/