

NUS 2FA Guideline

By NUS ITS

Version 1.0

Apr 2017

CONTENTS

1. OBJECTIVE	2
2. SCOPE.....	2
3. AUDIENCE.....	2
4. DEFINITION.....	2
5. REQUIREMENTS	2
6. IMPLEMENTATION	3

APPENDIX A

EXEMPTION REQUEST FORM

1. OBJECTIVE

- 1.1 The objective of this document is to provide guidance on the usage of Two-Factor Authentication (2FA) with reference to NUS IT Security Policy version 3.6.

2. SCOPE

- 2.1 This guideline applies to any user access to applications containing NUS Confidential or personal data, or supporting critical business operations (i.e. breakdown or failure of the systems would likely result in major disruption to the University's mission critical functions or operations).

3. AUDIENCE

- 3.1 The intended audience are System owners and IT staff.

4. DEFINITION

- 4.1 NUS Confidential data examples (refer to NUS Data Management Policy version 2.3 clause 3.1.1):
- a. Salary and appraisal information of current and former staff
 - b. Examination marks/grades
 - c. Admission data
 - d. Medical records
 - e. Donor records
 - f. NRIC/FIN number, credit card and bank account information
 - g. University initiatives or collaborations undergoing negotiations
- 4.2 Sensitive personal data:
- a. Address
 - b. Age
 - c. Bank and credit card details (e.g. Bank account no., expiry date, etc.)
 - d. Mobile number
 - e. Citizenship/Nationality
 - f. Country of birth
 - g. Date of birth
 - h. Family details
 - i. Gender
 - j. Marital status and date of marriage
 - k. Next of kin/guarantor/proxy details (e.g. name, email, etc.)
 - l. NRIC/FIN number
 - m. Passport Details (e.g. Passport number, Date of Issue & Date Of expiry etc.)
 - n. Photo
 - o. Race & ethnic group
 - p. Religion
 - q. Personal Contact Number
 - r. Personal Email Address

5. REQUIREMENTS

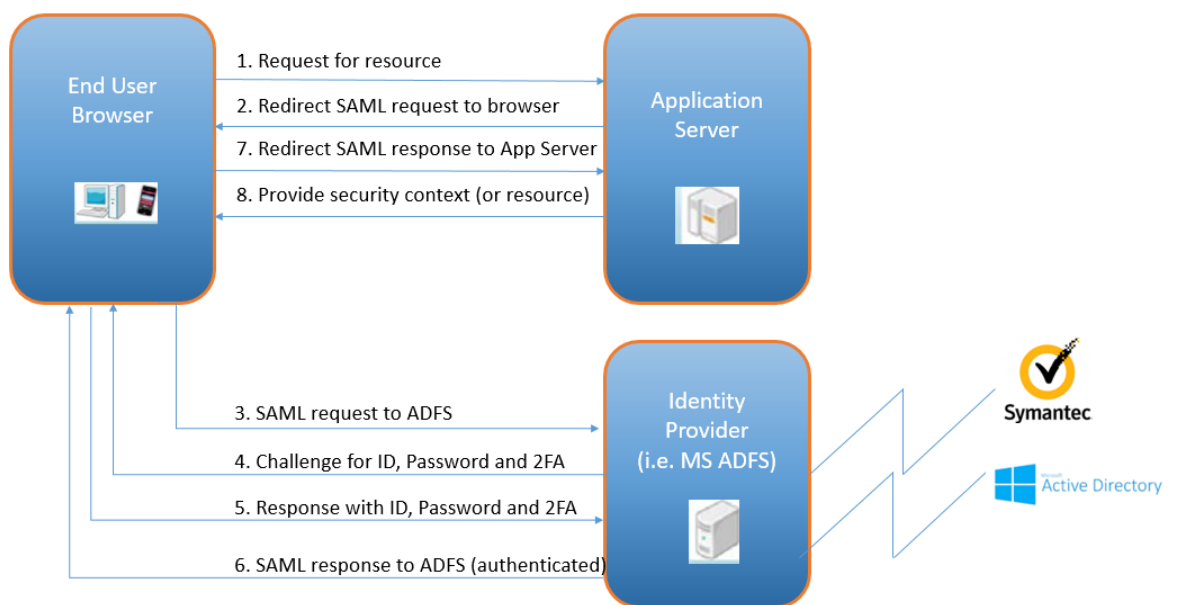
- 5.1 In addition to the username and password, 2FA requires a user to provide a separate piece of information, such as a security code, to login to a secured system. 2FA makes it much harder for an attacker to use stolen IDs and passwords to gain access to sensitive or confidential systems.
- 5.2 2FA shall be implemented for any user access to applications containing NUS Confidential or personal data, or supporting critical business operations (i.e. breakdown or failure of the

systems would likely result in major disruption to the University's mission critical functions or operations). Refer to the list of 2FA enabled applications/systems on NUS staff portal².

- 5.3 The System owner will carry out a risk assessment with inputs from IT staff, to decide on the need for 2FA implementation. Under certain circumstances, 2FA may be required but not implemented (see below). In such cases, appropriate risk mitigation controls must be identified and put in place.
- a. The systems are due for decommission within half a year.
 - b. The systems have reached end of support and cannot be enhanced.
 - c. The systems are Commercial Off The Shelf (COTS) and cannot be customized.
- 5.4 Exemption request form is given in Appendix A. Exemption granted is for the exemption period specified. Request for exemption shall be reviewed and sought thereafter.

6. IMPLEMENTATION

- 6.1 NUS' 2FA solution comes in the form of a Security Code generated by a software-based token that can be installed in any smart device or computer. In addition to the NUSNET ID and password, a Security Code must be entered to login and access those applications that are 2FA-enabled. Refer to NUS Staff Portal² for the instructions on how to generate a Security Code from your smartphone, tablet or computer.
- 6.2 Below is an overview of the application authentication mechanism between NUS ADFS and NUS 2FA. An integration guide for technical implementation is available, and will be provided upon request³.
- 6.3 In situations where the applications contain NUS Confidential or personal data, or support critical business operations, and where NUS 2FA is unfeasible or impractical to implement, other industry-established 2FA mechanisms (e.g. one-time password via SMS) may be considered in consultation with NUS IT.



² <https://inetapps.nus.edu.sg/2fa/applications.html>