

SafeNet Authentication Client Compatibility Guide

Using SafeNet Authentication Client CBA for Dell Wyse

All information herein is either public information or is the property of and owned solely by Gemalto. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2010 - 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Doc Number: 007-013452-001 Rev. B

Release Date: February, 2017

Contents

Applicability	4
Environment.....	4
Validated Devices	4
Validated Use Cases with SAC	5
SAC Results.....	5
Validated Use Cases with IDGo800 Compatible mode	5
IDGo800 Compatible mode Results	5
Support Contacts	6

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC) Typical installation mode**— SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.
- **SafeNet Authentication Client (SAC) IDGo800 Compatible mode**— IDGo800 Minidriver based package, uses Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards.

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Client (SAC) - 10.2**
- **Dell Wyse 3010 T10 - Firmware 8.3.14**
- **Dell Wyse 5010 D10 - Firmware 8.3.14**
- **XenApp/XenDesktop - 7.6**

Validated Devices

SAC 10.2 was validated with the following devices:

- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 GA
- Gemalto IDprime MD 840
- Gemalto IDprime MD 830

Validated Use Cases with SAC

The following use cases were validated:

- Using the smart card to log into Wyse Client and then logging into Published App (Calculator) on Win Server 2008R2 virtual machine.
- Using the smart card to log into Wyse Client and then logging into XenDesktop Published Win 7 x32 virtual machine.

After Logging into XenDesktop Published Win 7 x32 virtual machine the following was tested:

- Sign/Encrypt Mail Outlook 2013
- SSL TLS 1.2

SAC Results

The following devices passed the above tests using SafeNet Authentication Client:

- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 GA
- Gemalto IDprime MD 840
- Gemalto IDprime MD 830

Validated Use Cases with IDGo800 Compatible mode

The following use cases were validated:

- Using the smart card to log into Wyse Client and then logging into Published App (Calc) on a Win Server 2008R2 virtual machine.
- Using the smart card to log into Wyse Client and then logging into XenDesktop on a Published Win 7 x64 virtual machine.

After Logging into XenDesktop on a Published Win 7 x64 virtual machine SSL TLS 1.2 was tested.

IDGo800 Compatible mode Results

The following device passed the above tests using SAC IDGo 800 compatible mode:

- Gemalto IDprime MD 830
- Gemalto IDprime MD 840

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	