SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for Stormshield Data Security

gemalto
security to be free

All information herein is either public information or is the property of and owned solely by Gemalto NV. 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.

© 2016 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.

Document Part Number: 007-013787-001 Rev. A

Release Date: June 2017

Contents

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Stormshield Data Security.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

Data protection poses both a security and a compliance challenge to IT organizations. The ability to positively identify users requesting access to resources is a critical consideration in achieving a secure data protection solution. Deploying a data protection solution without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat.

A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

Public Key Infrastructure (PKI) provides an effective strong authentication solution for the functional, security, and compliance requirements.

SafeNet Authentication Client (SAC) is a PKI middleware application that provides a secure method for exchanging information based on public-key cryptography, enabling trusted third-party verification of user identities. SafeNet's certificate-based tokens provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SAC. The SAC generic integration, with CAPI, CNG, and PKCS#11 security interfaces, enables out-of-the-box interoperability with a variety of security applications, offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

SafeNet Authentication Manager (SAM) provides your organization with a comprehensive platform to manage all of your authentication requirements, across the enterprise and the cloud, in a single, integrated system. SAM enables management of the complete user authentication life-cycle. SAM links tokens with users, organizational rules, and security applications to allow streamlined handling of your organization's authentication infrastructure with a flexible, extensible, and scalable management platform.

SAM is a comprehensive token management system. It is an out-of-the-box solution for Public Certificate Authorities (CA) and enterprises to ease the administration of SafeNet's hardware or software tokens devices. SAM is designed and developed to support the best practices of managing PKI devices in common PKI implementations. It offers a robust yet easy to customize framework that supports different organizations' PKI devices management workflows and policies. Using SAM to manage tokens is not mandatory, but it is recommended for enterprise organizations.

For more information, refer to the *SafeNet Authentication Manager Administrator Guide*.

Stormshield® Data Security Enterprise is a transparent solution that integrates into your usual communication tools to help your business teams create secure environments for collaborative working, regardless of the media (e-mail, USB sticks, etc.), terminals (work station, mobile or tablet) or applications (collaborative, intranet, network sharing, etc.) used.

This document describes the deployment of certificate-based authentication (CBA) for user authentication to Stormshield Data Security using SafeNet tokens.

It is assumed that the Stormshield Data Security environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

Stormshield Data Security can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with SafeNet products.

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, using Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards. For more details about different SAC installation modes, refer to the *SafeNet Authentication Client Administration Guide*.
- **Stormshield Data Security**

Environment

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

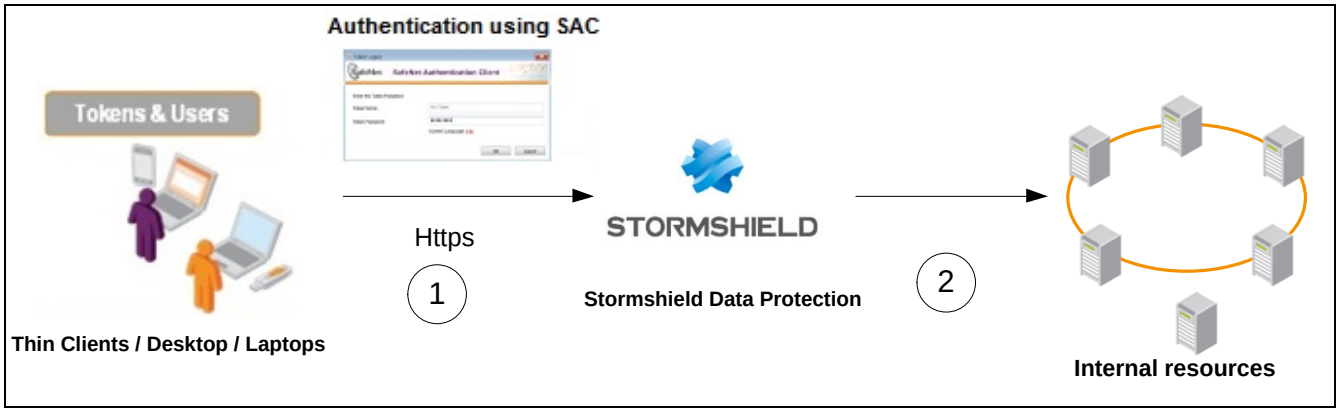
- **SafeNet Authentication Client (SAC)** - Version 10.3
- **Stormshield Data Security Suite** – Version 9.1

Audience

This document is intended for use by system administrators who are familiar with Stormshield Data Security, and are interested in adding multi-factor authentication capabilities using SafeNet tokens.

CBA/Encryption Flow using SafeNet Authentication Client

1. The user attempts to login to the Stormshield Data Security client application. The user inserts the Gemalto token or smart card on which his certificate resides, and when prompted, enters the token/smart card password.
2. After successful authentication, the user is allowed access to the encrypted data.



Prerequisites

This following must be installed and configured before implementing certificate-based authentication for Stormshield Data Security using SafeNet tokens:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. Any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) must be configured with an MS CA Connector. For further details, refer to the *SafeNet Authentication Manager Administrator's Guide*.
- Users must have a SafeNet token enrolled with the appropriate certificate.
- SafeNet Authentication Client (SAC version 10.3) must be installed on all client machines.

Tokens Supported by SafeNet Authentication Client

SafeNet Authentication Client (SAC) supports a number of authenticators that can be used as a second authentication factor for users authenticating to Stormshield Data Security.

SafeNet Authentication Client 10.3 (GA) supports the following tokens:

Certificate-based USB tokens

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

Smart Cards

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840

For a complete list of supported authenticators, refer to *SafeNet Authentication Client Customer Release Notes*

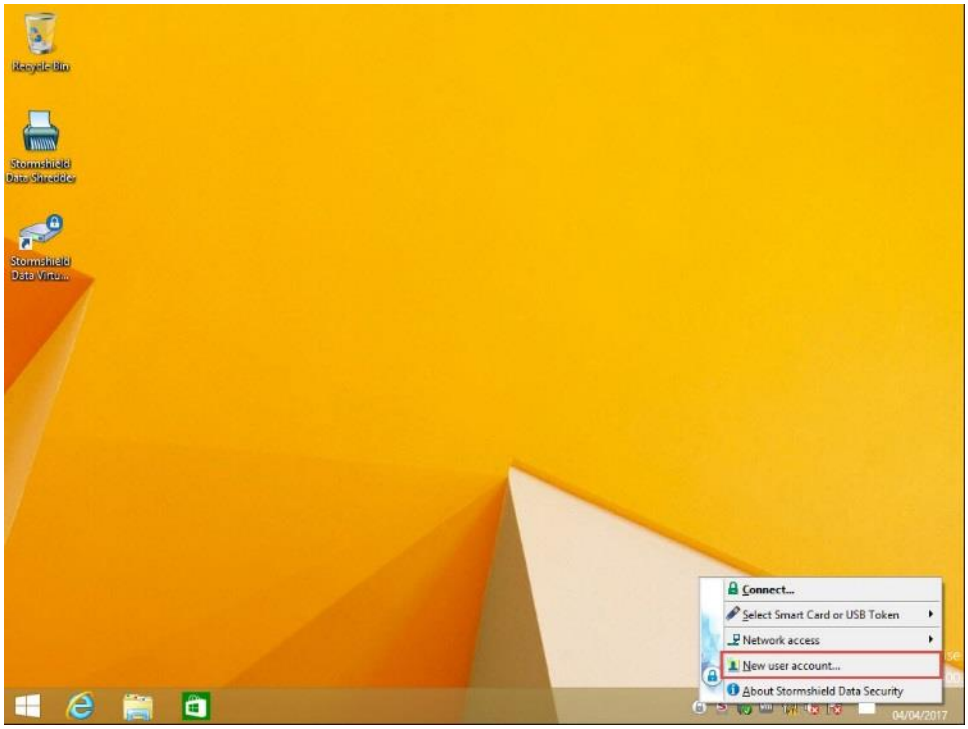
Configuring Stormshield Data Security

This section describes the basic configuration of Stormshield Data Protection, enabling the user to access to the protected data using a smart card.

Stormshield Data Protection supports Gemalto's tokens and smart cards out of the box.

To set up basic configuration:

1. Insert a Gemalto token or smart card. Right click on the Stormshield Data Security icon and select **New user account…**

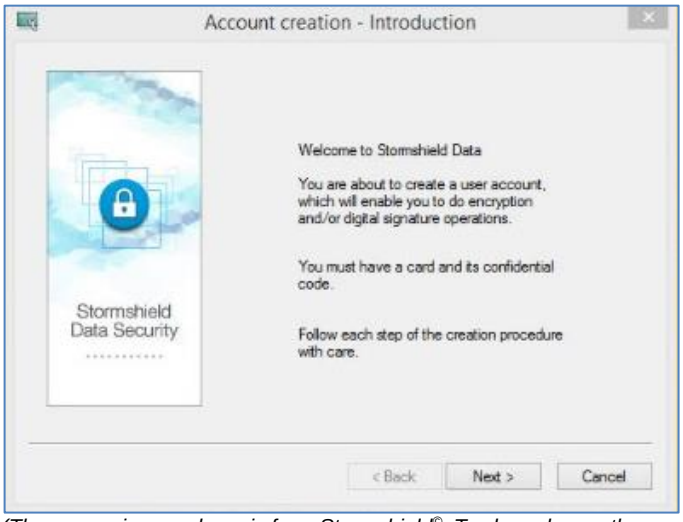


   The Stormshield Data Security window opens.

2. Select **Account 'Smart Card/USB Token"** and click **Create Account**

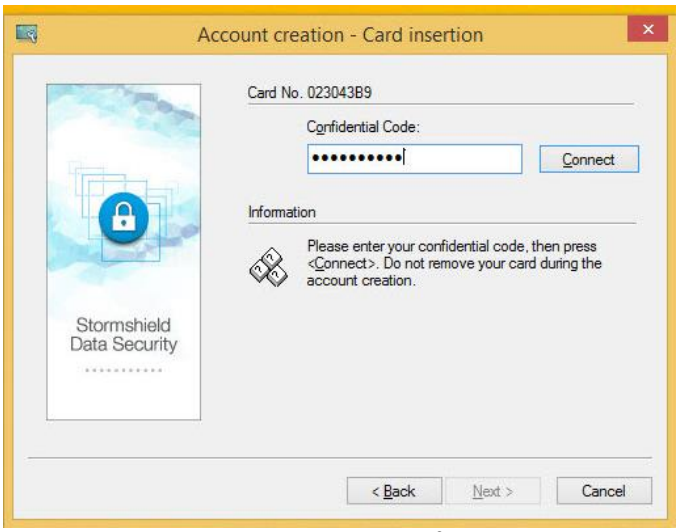
(The screen image above is from Stormshield©. Trademarks are the property of their respective owners.)

3. On the **Account creation – Introduction** window, click **Next.**



(The screen image above is from Stormshield©. Trademarks are the property of their respective owners.)

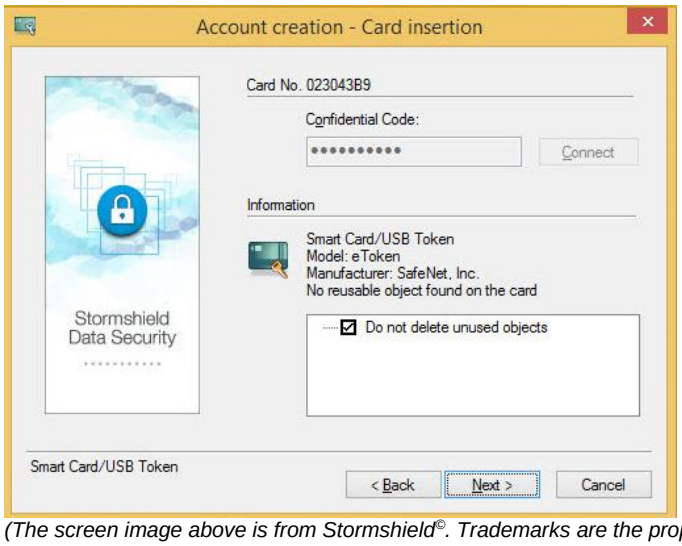
4. On the **Account creation – Card insertion** window, enter the token/smart card PIN code and click **Connect.**



(The screen image above is from Stormshield©. Trademarks are the property of their respective owners.)

Once connected, the token information is displayed.

5. Click **Next**



(The screen image above is from Stormshield©. Trademarks are the property of their respective owners.)

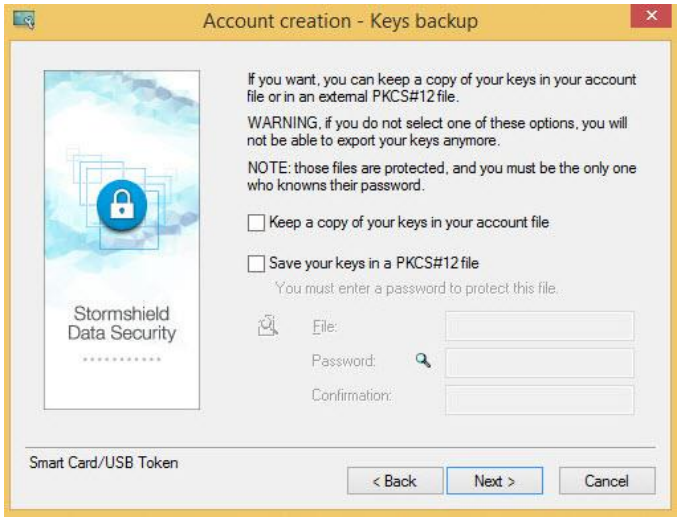
6. On the Account creation – Encryption key window, select **Generate your encryption key** or **Import your encryption key** and click **Next**

(The screen image above is from Stormshield©. Trademarks are the property of their respective owners.)

7. After generating/importing the keys, on the **Account creation – User information** window enter the user details and click **Next**

(The screen image above is from Stormshield©. Trademarks are the property of their respective owners.)

8. On the **Account creation – Keys backup** window select the desired configuration and click **Next.**



9. On the **Account creation – Summary** window click **Finish**.

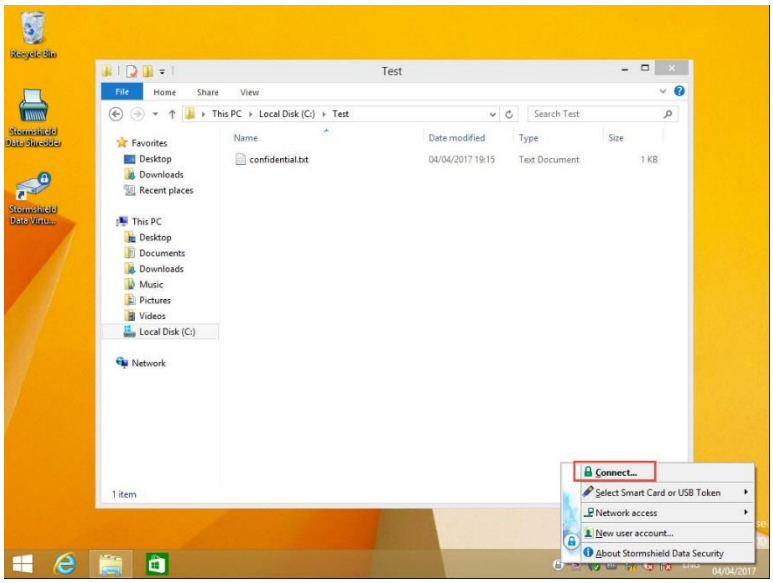
(The screen image above is from Stormshield©. Trademarks are the property of their respective owners.)

The account is being created and the keys are deployed on the Gemalto token/smart card.

Running the Solution

The following section demonstrates a file encryption using Stormshield Data Security and Gemalto token/smart card.

1. Right click the Stormshield Data Security icon and click **Connect**

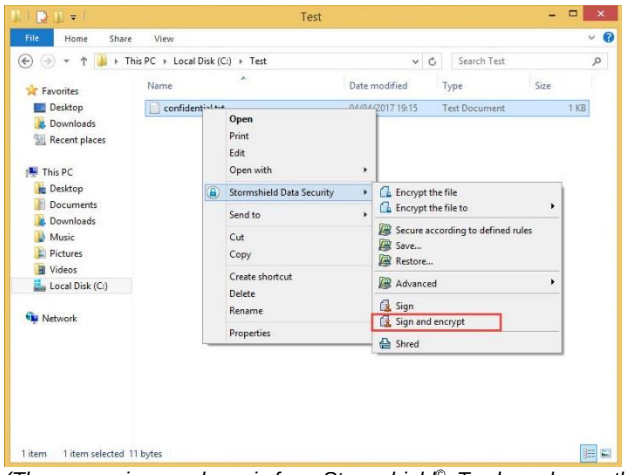


The **Stormshield Data Security – Connection** window opens.

2. Enter the token/smart card PIN in the **Enter your secret code** field and click **Validate**

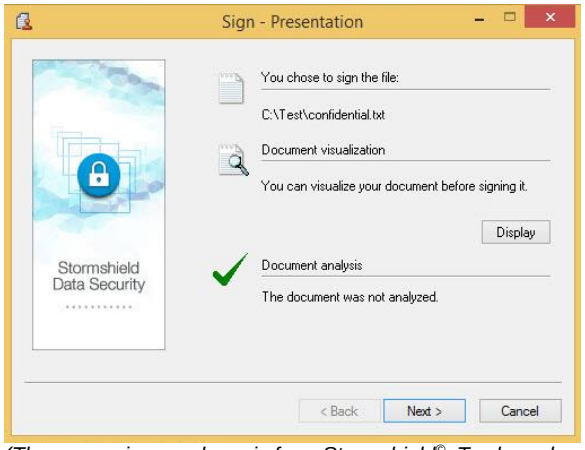
(The screen image above is from Stormshield©. Trademarks are the property of their respective owners.)

3. After a successful validation, right click on the file to be encrypted and select **Stormshield Data Security > Sign and encrypt.**



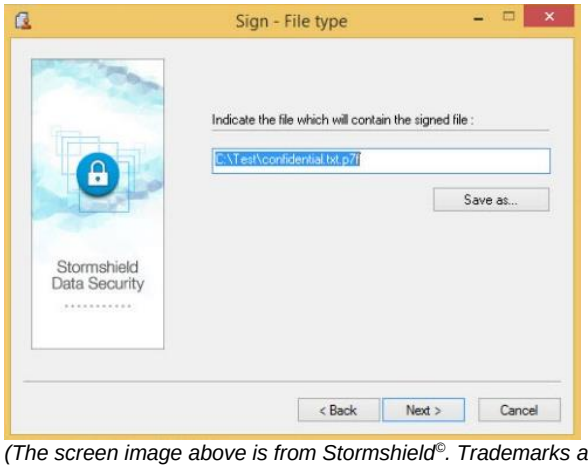
(The screen image above is from Stormshield©. Trademarks are the property of their respective owners.)

4. On the **Sign – Presentation** window, click on **Next**



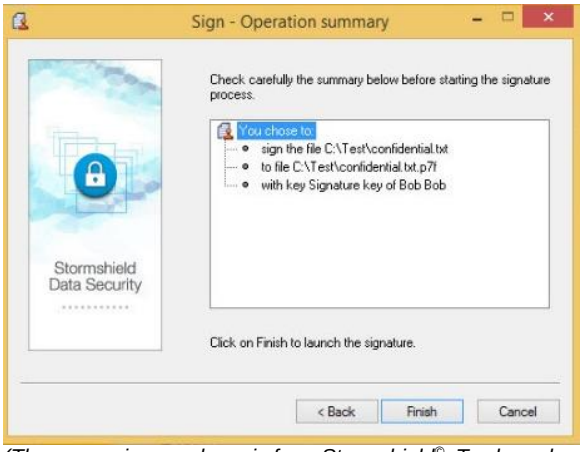
(The screen image above is from Stormshield©. Trademarks are the property of their respective owners.)

5. On the **Sign – File type** window**,** indicate the file which will contain the signed file and click **Next.**



(The screen image above is from Stormshield©. Trademarks are the property of their respective owners.)

6. On the **Sign – Operation summary** window click **Finish.**



(The screen image above is from Stormshield©. Trademarks are the property of their respective owners.)

The **secret code** window opens.

7. Enter your Gemalto token/smart card PIN and click **Validate**.

(The screen image above is from Stormshield©. Trademarks are the property of their respective owners.)

On successful validation, an encrypted file is created.

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
Customer Support Portal	https://supportportal.gemalto.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.
Technical Support contact email	technical.support@gemalto.com