Security Insurance Plan

Protection of Personal Data
XB5S6-XB5S7

05/2019

MFR8402300_00

www.schneider-electric.com

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

You agree not to reproduce, other than for your own personal, noncommercial use, all or part of this document on any medium whatsoever without permission of Schneider Electric, given in writing. You also agree not to establish any hypertext links to this document or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the document or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

© 2019 Schneider Electric. All rights reserved.

Table of Contents

About the Book

At a Glance

Document Scope

This document describes the measures that Schneider Electric has implemented in the development and design of XB5S6/S7 to take into account the protection of Personal Data (DP), in its capacity as manufacturer of XB5S Harmony products. It is intended to help customers fulfill their compliance obligations.

In this document, actions are identified to be the responsibility of the customer / operator of XB5S Harmony products. For this purpose, the « ☞ » symbol is placed at the beginning of the paragraph containing the expected action.

Validity Note

REFERENCE DATA PROTECTION LAWS

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation: GDPR) repealing Directive 95/46 /EC

Text in English: **REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL** of 27 April 2016 on web site of European Union: **Access to European Union law**.

Related Documents

Title of documentation	Reference number
XB5S6/S7 biometric switch - Instruction Sheet	MFR3178001

You can download these technical publications and other technical information from our website at *www.schneider-electric.com/en/download*.

Chapter 1
Description

Description

Description

The XB5S AUTONOMOUS products allow the implementation of a biometric button. This button uses proven optical technology and benefits from excellent shock and vibration resistance (CEM protection, IP65).

Macro architecture of XB5S Harmony products:

Chapter 2
Processing of Personal Data

What Is in This Chapter?

This chapter contains the following topics:

Processing of Personal Data

Personal Data Collected and Data Minimization

Schneider Electric has considered the data minimization principle for the design of its XB5S6/S7. The data collected is the minimum necessary for the proper functioning of the products.

The XB5S6/S7 stores the following Personal Data:

- Fingerprint template, along with a number (automatically allocated),
- User role (Administrator or User).

The fingerprint template is an algorithmic representation of the fingerprint. The XB5S6/S7 does not store the actual fingerprint image.

No other information about users, such as their names, job titles, other identifiers, or time of authentication are processed by the product.

☞ If Customer processes other Personal Data in the course of the implementation of the product, the customer must ensure that the data collected are adequate, relevant, and limited to what is necessary for the specified purposes (art 5 GDPR).

Protected Individuals

The product processes data about two categories of individuals:

- User: person registered in XB5S6/S7, so that his/her fingerprint can be recognized,
- Administrator: any user authorized to manage other users.

Purposes

The XB5S6/S7 is a device for the authentication of persons who are granted specific access rights. It can be used for instance to control access to:

- Premises which require a high level of protection
- Dangerous process or machines,
- Hazardous materials,
- Funds or other valuables…

☞ Several technologies are available to ensure access control authentication. Customer determines whether biometrics is an appropriate measure in light of the risks at stake, including those for individuals.

Customer must take into account applicable regulation that may:

- Limit the use of biometrics data to certain high-risk scenarios.
- Prohibit the use of biometrics data for other purposes than access control authentication (such as, for example, for working hours management).

Operations

The processing operations in relation to the products XB5S6/S7 are as follows:

- Collection of users' fingerprint templates,
- Assignment of "Administrator" roles,
- Authentication of users, activation of the output (electrical information) according to fingerprint recognition,
- Deletion of a user,
- Removal of Administrator role.

The combination of these basic actions allows XB5S6/S7 to be used as specified in the associated operating instructions.

Data Controller and Data Processor

The data controller is the person who has taken the decision to implement the XB5S6/S7. It is generally the customer. The Data Controller:

- Determines the purposes and means of the processing operations,
- Is responsible for the lawfulness and compliance of the processing operations with applicable data protection laws,
- Ensures that the rights of protected individuals are respected,
- Provides documented instructions to its data processors, if any.

The data controller may resort to data processors. A processor is a person/entity who processes personal data on behalf of and under the instructions of the data controller.

☞ If Customer involves third parties in the implementation of the XB5S Harmony autonomous products, it is Customer's responsibility to ensure under appropriate contractual arrangements that these third parties act in compliance with data protection obligations (art 28 GDPR).

Schneider Electric is the manufacturer of the XB5S6/S7. Schneider Electric cannot be considered as a data processor, as it does not process any personal data.

Data Processing Register

To assist customers operating the XB5S6/S7, it is recommended to create a Record of Processing Activities *(see page 23)*.

☞ Data processing activities must be logged by Customer in a processing register (art 30 GDPR).

Data Protection Impact Assessment (DPIA)

GDPR subjects sensitive data processing activities to a prior assessment of their impact on the protection of personal data (DPIA). XB5S Harmony products involve the processing of biometric data which are considered as a "special category of personal data" (art 9 GDPR). The processing of special categories of data on a large scale triggers the requirement of a DPIA, unless it meets certain requirements determined by the competent Data Protection Authority, if any.

☞ Customer must check whether the contemplated project requires a DPIA and must perform it if required.

Rights of Individuals

- Information

  ☞ Customer must provide mandatory information to users of XB5S6/S7 before enrollment. An example of statement is provided under appendix Example of framework for information statement *(see page 22)*. Customer must ensure that the statement used is compliant with applicable national data protection laws.
- Access

  It is not possible to extract the fingerprint templates stored in the XB5S Harmony button. It is designed this way to ensure a high level of security for this sensitive personal data. Users may check whether his/her fingerprint templates are actually processed by the XB5S6/S7 device by authenticating themselves.

  ☞ Customer must have a procedure to address access requests. Users may require access to data processed by Customer in relation to the XB5S6/S7. For instance: any registers or logs that are used in conjunction with the XB5S6/S7, or with the processes/resources protected by XB5S6/S7.
- Rectification

  It is not possible to modify the fingerprint templates stored in the XB5S Harmony button. It has been designed this way to ensure a high level of security. A user has the possibility to unenroll and enroll again. The deletion process is detailed in the XB5S6/S7 Instruction Sheet *(see page 5)*.

  ☞ Customer must have a procedure to address rectification requests.
- Erasure

  It is possible to delete a fingerprint template on the condition that the user is physically present. The deletion process is detailed in the XB5S6/S7 Instruction Sheet *(see page 5)*. Deletion of a single template is not possible in the absence of the user. A reset to the "factory default" initial state is also possible, but this is equivalent to unenrolling all users, and it will therefore be necessary to re-register all authorized persons.

  ☞ Customer must have a procedure to address erasure requests.
- Restriction

  In the XB5S6/S7, the registration/deletion of fingerprint templates as well as the assignation/removal of roles both require positive actions. It is therefore possible to restrict processing using an operational procedure.

  ☞ Customer must have a procedure to address restriction requests. It entails (1) suspending the use of the XB5S6/S7 by the concerned user for the time necessary to address the user’s request, and (2) refraining from modifying or deleting any data relating to said user.
- Objection

  It is possible to manage the right to object using an operational procedure.

☞ Where the right to object applies, Customer must have a procedure to address objection requests. It entails suspending the use of the XB5S6/S7 by the user for the time necessary to check the balance of interests between (1) the user who objects to the processing, and (2) the customer. If, according to this assessment, Customer determines that data processing is infringing on the rights of the user, the customer will be able to delete the user's fingerprint templates as detailed under 'erasure' above.

Measures for the Security and Confidentiality of Personal Data

Overview

This paragraph lists the security measures protecting information processed by XB5S6/S7.

Data Measures

- Fingerprint data are stored in dedicated database. This database is stored in internal memory.
- The internal database is fully encrypted using the AES-128 algorithm.
- Internal component and communication are protected from external access and are not accessible from outside. The communication ports used for the development and manufacture of the fingerprint recognition module are burnt at the end of the production process. These ports cannot be reused after, even for maintenance.
- The key using to cipher internal database is unique by XBS5 product. This key generated at each reset factory. This key is stored in a dedicated storage on the main chipset, access protected by firmware authentication (only the signed firmware can access the key). Encryption keys are stored in an electronic safe of the recognition module.
- Data integrity of stored data is verified by an error-detecting code (CRC32).
- Fingerprint identification are processed in the CPU chipset in the button, without copy of the fingerprint data.
- At the time of collection, fingerprint data immediately undergo an irreversible transformation (one-way function).
- If a button is compromise, data still encrypted and cannot be read by anyone. The encryption key is isolated in an electronic safe of the recognition module. This mechanism prevents the disclosure of data.
- Erasing user data is achieved by freeing data space, with the following writing operations using free space. Even free space data is encrypted.
- Product maintenance can be done with or without reset factory, private data will not be accessible either way. Schneider Electric recommends doing a reset factory before return product in their services. A reset factory brings the advantage of replacing existing key using to cipher internal database by a new one and thus a better protection in case of loss of the product.
- ☞ Fingerprint in a button always allows the owner to activate the button. The data controller must erase the fingerprint when the user is not authorized to activate the XB5S6/S7 button.
- XB5S6/S7 can detect the case of use a dead finger to guard against attacks on the integrity of people.

Organizational Measures

- ☞ The data processor makes sure that the users have understood the operation of the button.
- ☞ Under customer responsibility, Schneider Electric is only responsible to inform customer about back-up solution. The data processor make available an alternative "emergency" device or used in exceptional circumstances, without any constraint or extra cost for persons not using the biometric solution; in particular, for persons who do not meet the constraints of the biometric device (enrollment or reading of the biometric data impossible) and in anticipation of the unavailability of the biometric device (such as a malfunction of the device), a "backup solution" must be implemented to ensure continuity of the proposed service, limited however to exceptional use.
- ☞ While authentication is not good, the XB5S6/S7 button is not activated. To prevent authentication failures due to pain, it is recommended to authenticate two fingerprints by user.
- ☞ The role of administrator must be controller in a registry. Refer to data processing register *(see page 11)*.
- ☞ The data processor makes sure that the administrator have understood the specific operation for administrator on the button. An administrator must add record when modifying user usage of the XB5S6/S7 button.
- ☞ When button integrity is broken (refer to Material Measure *(see page 15)*) the data processor must alert owner of fingerprint stored in button about this incident and potential impact on their personal data.
- ☞ The data processor must have a backup procedure to re enroll all persons in case of incident with out of order button. The data processing register *(see page 11)* must help to know impacted users.

Material Measures

- The button must be installed by Customer in a secure area. This security against theft is limited to areas where access is restricted to authorized persons (company premises with reception screening, etc.). The XB5S buttons are not protected from vandalism. In case of theft, data are protected by security at logical level.
- A sealed shell surrounds the biometric recognition module. This solid envelope guarantees fast detection of an intrusion by simple observation. This envelope must be damaged to access the biometric recognition module.
- All data and electronic process of data ran in a secure module integrated in the XB5S6/S7 button.
- Use certified equipment under the conditions of use and in terms of safety.
- The serial number is uniq and guaranty the traceability of the XB5S6/S7 button life cycle.
- An out-of-service product cannot be erased by a factory reset. Schneider Electric recommends destroying the product in accordance with the customer's procedure for secure destruction of out-of-service computer items.

Software Measures

- Software used in the XB5S6/S7 button is protected copyright reserved to Schneider Electric.
- The firmware used by the button is protected by electronic signature.
- Software electronic signature is verified by internal electronic module at each start.
- Software updates are managed by Schneider Electric through a standard procedure of product evolution
- Software checked to be at the state of art about security.
- Schneider Electric has strictly limited user action to decrease theirs impacts on security. The default configuration selected by Schneider Electric to guarantee the best security of usage.
- The XB5S6/S7 button internal software work only with internal data.

Flow Measures

- All internal channels are not accessible to users.

Location and Data Transfer

The location of the data is physically and only in the XB5S Harmony button, therefore the data is processed where the Data Controller is located.

Chapter 3
Restriction on the Use of Encryption Techniques

Restriction on the Use of Encryption Techniques

Restriction on the Use of Encryption Techniques

The XB5S Harmony button use encryption techniques. Encryption techniques used may be subject to authorization or prohibited in some countries.

Chapter 4
Procedure for the Development of the DC File

Procedure for the Development of the DC File

Procedure for the Development of the DC File

This document is in its original version. It will be developed by Schneider Electric in the following cases:

- Evolution of the functions of XB5S Harmony products,
- Recommendation by data protection authorities
- Changes in regulation

The revised version will be kept available for customers of XB5S Harmony products.

Chapter 5
Appendices

What Is in This Chapter?

This chapter contains the following topics:

Example of Framework for Information Statement

PRIVACY NOTICE

TO BE ADAPTED IN ACCORDANCE WITH CONTEMPLATED PROJECT AND APPLICABLE NATIONAL LAW

Purpose of the processing operation (purpose and legal basis):

[COMPANY ABCD] has implemented a biometric control access system to authenticate access to its sensitive premises.

The legal basis for the processing is… [for example: the legitimate interests of [COMPANY ABCD] (ensuring that …, protecting …)/compliance with a legal obligation (text n° xxx)].

Recorded data:

- Authorization register: Employee ID, duration of authorization, date of registration and deletion in the system,
- Access button: two fingerprint templates, automatically attributed reference number, role (user administrator)

Data recipients:

- Authorization register: Head of the department that owns the premises and the personnel department,
- Access button: there is no recipient, the data remains protected inside the device)

Data retention period:

- Authorization register: 5 years for persons with a long-term authorization, three months for persons with a one-off authorization,
- Access button: the erasure of fingerprint templates is performed by the users themselves at the end of their access authorization (or end of contract).

Rights of persons:

In order to exercise the data protection rights granted under applicable data protection law, such as the right to access, object, rectify, or request erasure or restriction of personal information, or if you have any questions about the processing of your data, you can contact our Data Protection Officer (DPO).

- Contact our DPO: dpo@abcd.fr
- Contact our DPO by post: The Data Protection Officer.
  Company ABCD
  Rue la Transparence
  96 000 CONFIANCE

If, after contacting us, you believe we might have processed your personal information in violation of applicable law, you may also lodge a complaint with a supervisory authority.

Record of Processing Activities

Description

To assist customers operating the XB5S6/S7, it is recommended to create a Record of Processing Activities.

For more details, refer to Data processing register *(see page 11)*.

Record of Processing Activities Example

Date (with hour)	Button	User's ID	Administrator's ID	Action
Fri 3-Aug-2018 09:12	Area no 2	AD258	AD258	Reset Factory
Mon 3-Sep-2018 00:00	Area no 1	LH028	AD258	Add administrator
Sun 2-Sep-2018 09:09	Process A	TF504	AD258	Delete user

Action list example:

Action
Add administrator
Add user
Delete user
Delete administrator
Reset Factory