ProtegeWX Compliance with GDPR

Application Note

ICTProtegeWX®

The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited. Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2018. All rights reserved.

Last Published: 25-May-2018 11:30

Contents

Background to GDPR ____ 4

What Constitutes Personal Data 4

General Requirements 4

How GDPR impacts on ProtegeWX ____ 5

Technical Protection Measures 5

Organizational Measures 5

End To End Data Encryption 6

Reference and More Information ____ 7

Contact ____ 8

Background to GDPR

The European Union General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to align data privacy laws across Europe, and to protect and empower all EU citizens to enable self-management of data privacy and to reshape the way organizations across the region approach data privacy.

The GDPR also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

What Constitutes Personal Data

Personal Data is defined as "any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person". It can be anything from a name, photo, an email address, bank details, medical information, IP address, or an RFID tag.

General Requirements

The GDPR requires personal data to be processed in a manner that ensures its security and includes protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organizational measures are used. The GDPR also details the rights of an individual regarding the provision, consent to use, upkeep, retention and deletion of their personal data.

How GDPR impacts on ProtegeWX

Within ProtegeWX, personal data items that are stored and used are usually First and Last names, and a card or tag number. Some installations may go further and add custom fields for data such as: Employee/Student ID number, DOB, Company, Department, Vehicle registration etc. All these items fall within the scope of GDPR, and therefore need to be safeguarded and managed within the GDPR's requirements.

Technical Protection Measures

Within the ProtegeWX system, the End to End transmission of data is secured using encryption and security features at many levels as outlined below.

- Controller - Server communications are carried out over an encrypted local area network or 3G mobile connection using NIST Certified AES 128, 192 and 256 Bit Encryption
- Controller - Module communications use an encrypted proprietary RS-485 module network
- Mobile application communications to the Mobile App Cloud Server utilizes the HTTPS protocol
- ProtegeWX operator logins are secured using username/password combination

Organizational Measures

ICT products are intended for use by organizations for the purpose of enabling access control and security services. Any organization administering the individual use of ICT products will need to manage the data privacy in line with any legislation, employee agreements, customer use and visitor obligations.

It is therefore the responsibility of the system owner (e.g. End user Company, Property management Company or Integrator) to implement procedural measures to obtain and manage the personal data for users within the system. Within the scope of GDPR this includes (but is not limited to) the following:

- The recording of what data is stored and transmitted
- Obtaining users' consent to obtain and use personal data
- Detailing the specific use of personal data
- Processes of personal data retention, update and deletion
- Protection and management of access to personal data (operator management and separation of duties)

Example of a Human Resource Statement or Consent Form

As part of the access control and security system in the building personal details of individuals are stored and used for event logging and tracking. The Personal information stored is used for this explicit purpose and is not transferred to any other party in any form.

The Personal data used are First Name and Last name (add others here as appropriate e.g. employee ID, Department etc)

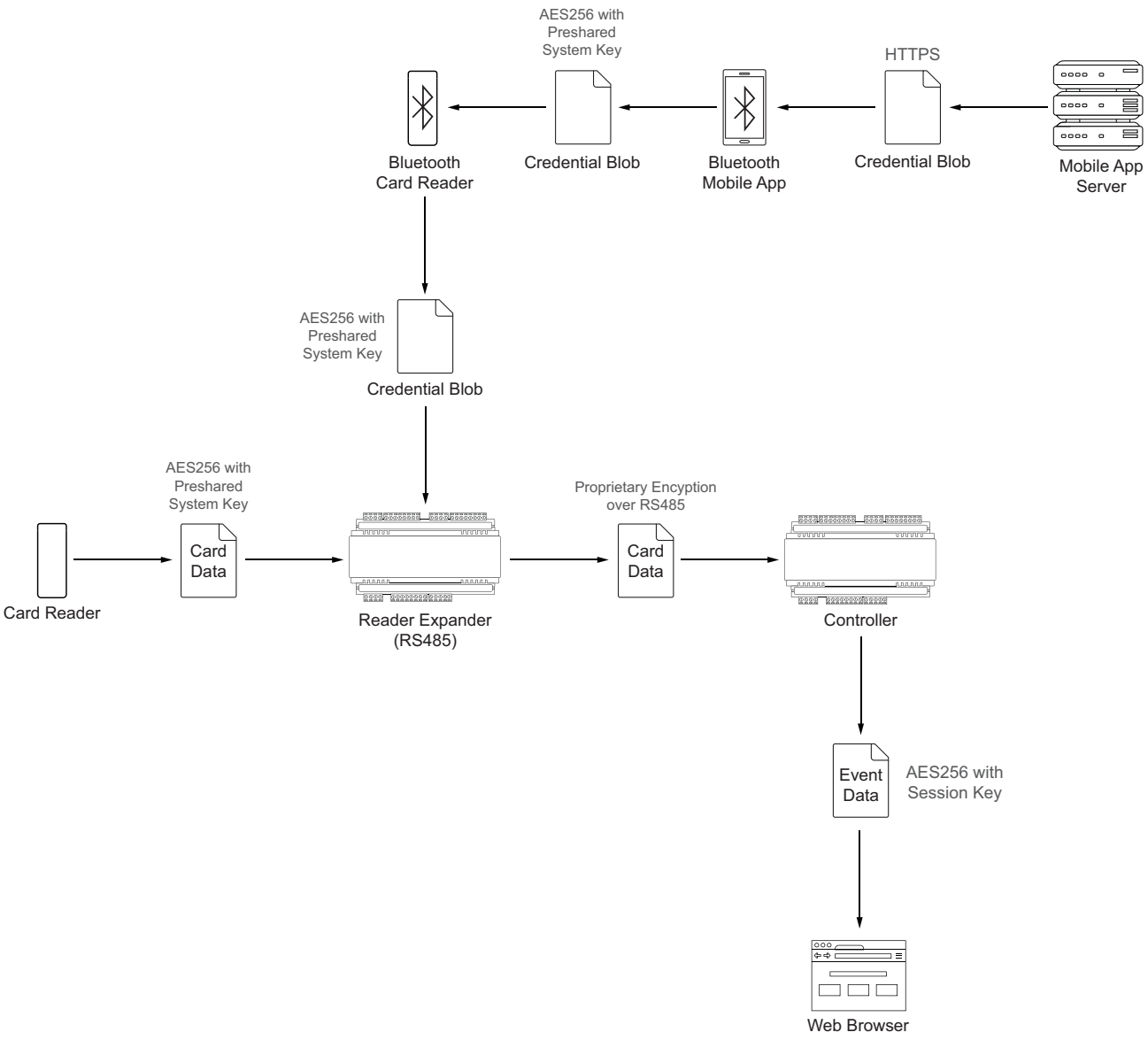
By signing below, you acknowledge and consent that your personal data can be stored and used in this manner

Signed: _____ *Date:* _____

End To End Data Encryption

The diagrams below show the end to end encryption of data for ProtegeWX and should help answer any questions regarding the security of data during transmission within the system.

ProtegeWX End to End Data Encryption



Reference and More Information

The United Kingdom's independent authority

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

General Data Protection Regulation

- https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Data Protection in the European Union

- https://ec.europa.eu/info/law/law-topic/data-protection_en

Contact

Integrated Control Technology welcomes all feedback.

Please visit our website (http://www.ict.co) or use the contact information below.

Integrated Control Technology

P.O. Box 302-340
North Harbour Post Centre
Auckland
New Zealand

4 John Glenn Ave
Rosedale
North Shore City 0632
Auckland
New Zealand

Phone: +64-9-476-7124

Toll Free Numbers:

0800 ICT 111 (0800 428 111) - New Zealand

1800 ICT 111 (1800 428 111) - Australia

1855 ICT 9111 (1855 428 9111) - USA/Canada

Email: sales@ict.co (mailto:sales@ict.co) or support@ict.co (mailto:support@ict.co)

Web: www.ict.co

APAC
Integrated Control Technology Limited
4 John Glenn Avenue, Rosedale, Auckland 0632
PO Box 302-340, North Harbour, Auckland 0751, New Zealand
Email: sales@ict.co Toll Free: (0800) 428 111 Phone: 64 (9) 476 7124

AMERICAS
Integrated Control Technology (USA) LLC
5265 S Rio Grande Street, Suite 201, Littleton, CO 80120
Email: ussales@ict.co Toll Free: (855) 428 9111 Phone: 720 442 0767

EMEA
Integrated Control Technology (Europe) Limited
St Mary's Court, The Broadway, Amersham, HP7 0UT, UK
Email: emeasales@ict.co Phone: 44 0 1494 590494

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2018. All rights reserved.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of these products, neither Integrated Control Technology Ltd nor its employees, shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the Integrated Control Technology policy of enhanced development, design and specifications are subject to change without notice

www.ict.co