

Suprema Webinar

BioStar 2 v2.8.0 and Cybersecurity

Speaker

Michael Lee

BioStar 2 Product Manager | Suprema

Date: Tuesday, May 12, 2020

Time: 08:00 AM (GMT+9), Seoul

Contents

1. Cybersecurity
2. Security Features on BioStar 2 v2.8.0
3. Upcoming Features
4. Q&A

DISCLAIMER

This presentation is solely for the use of Suprema's employees. No part of this material may be circulated, quoted, or reproduced for distribution outside the customer's organization without prior written approval from Suprema Inc. This material was prepared by Suprema Inc. solely for informative purpose and was not independently verified. No representations or warranties, express or implied, are made as to, and no reliance should be placed on, the accuracy, fairness or completeness of the information presented or contained in this presentation. © 2020 Suprema Inc. All rights reserved.

Cybersecurity

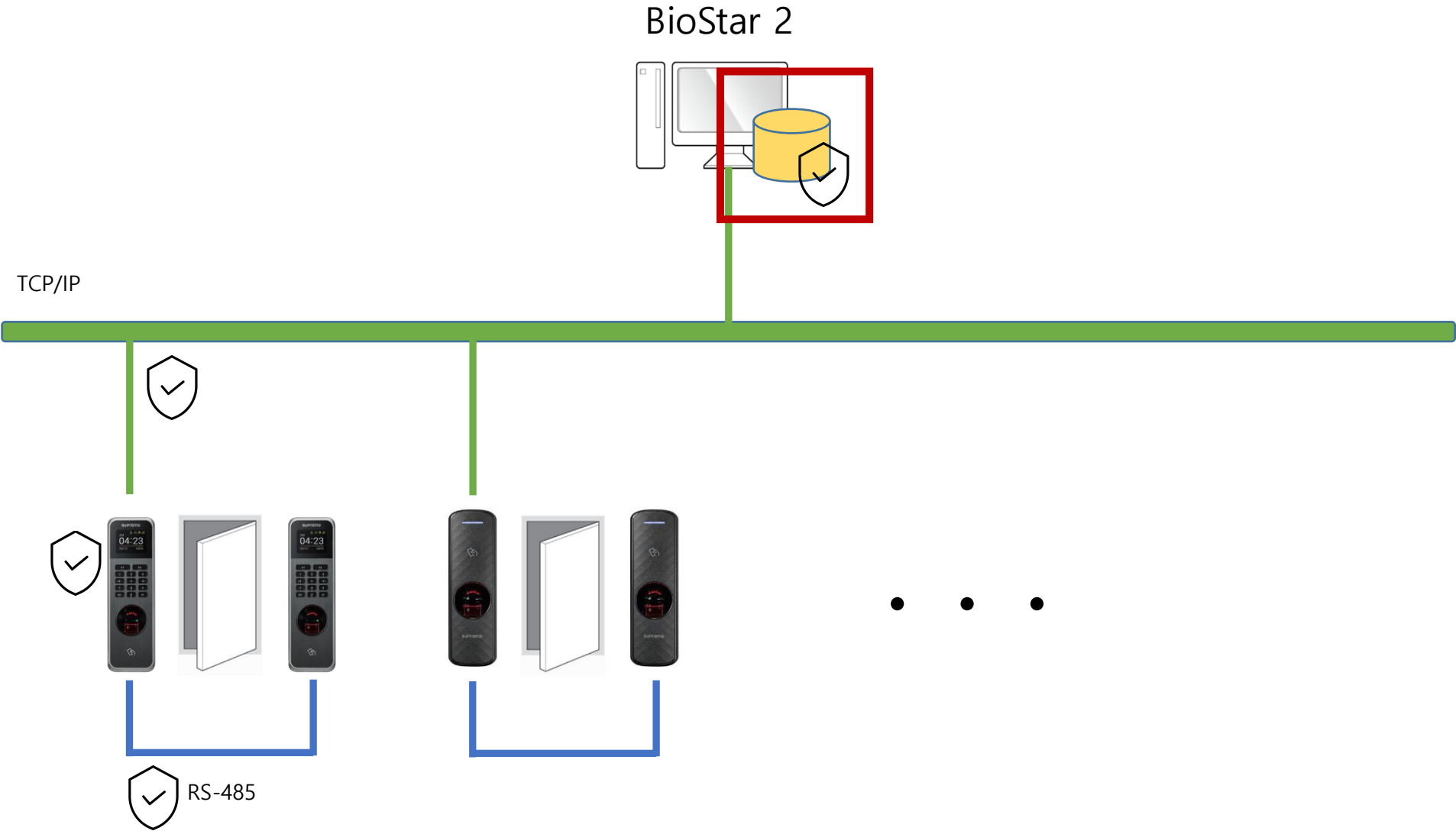
**Access
(Theft)**



Modify

Destroy

BioStar 2 System



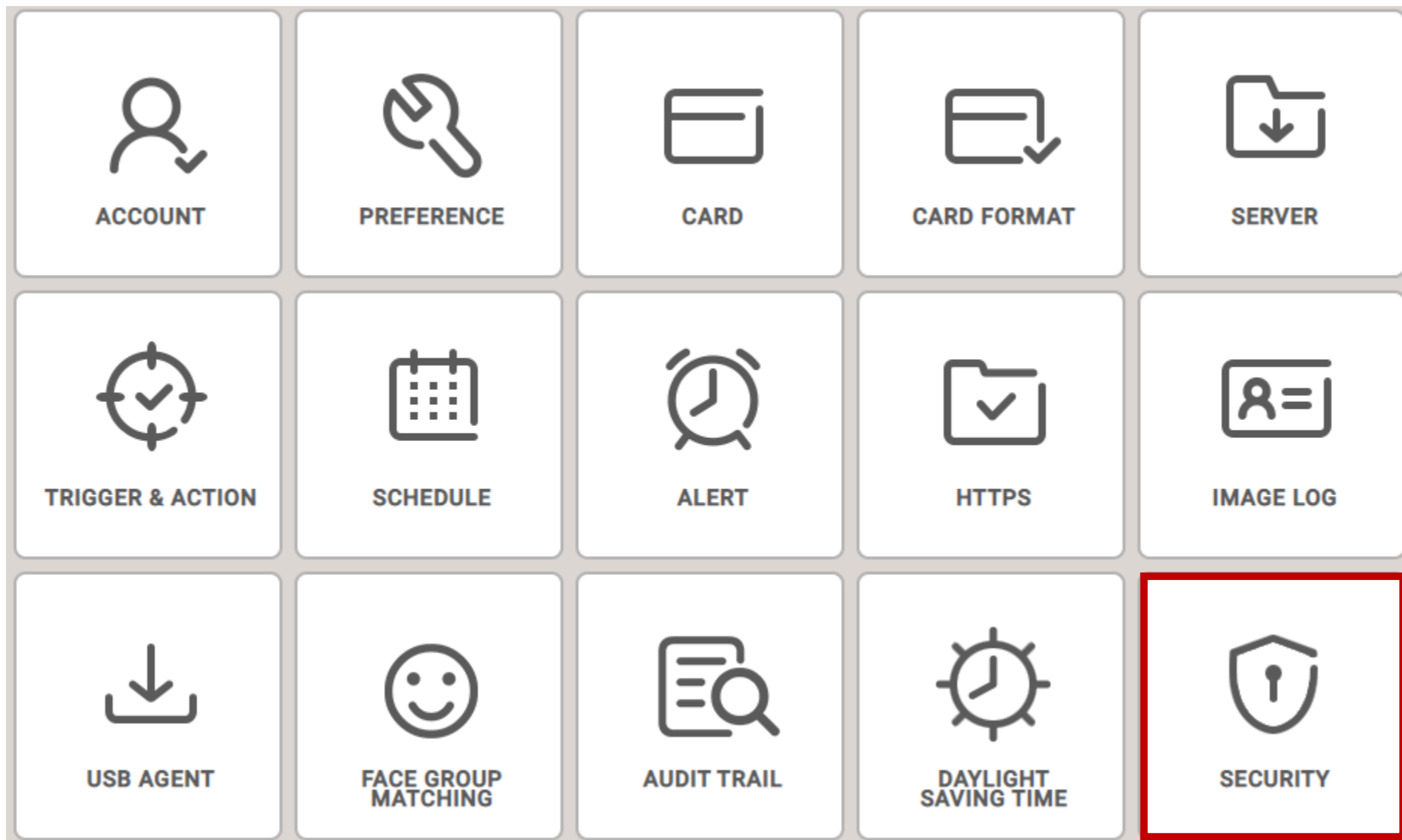
Security Features on BioStar 2 v2.8.0

BioStar 2 v2.8.0 Security Features

✓ Where did this start?

- BioStar 2 security was focused on the fact that biometric templates cannot be reversed to real images
- Data protection of BioStar 2 was leaning on the fact most sites are on-premise

BioStar 2 v2.8.0 Security Features



- ✓ Encrypt Sensitive Data on Database
- ✓ Secure Communication with Device
- ✓ Hash Key Management

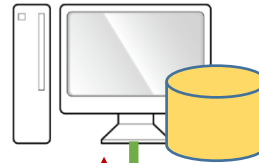
✓ Sensitive Data?

- A data or combination of data considered as personal information and information that can be a security threat when leaked
- User ID, Name, Mobile, E-mail, PIN, Login Account, Password, Profile Image and more.
- Card configuration such as key for data access

- ✓ Encrypt Sensitive Data on Database
- ✓ Secure Communication with Device
- ✓ Hash Key Management

Encrypt Sensitive Data on Database

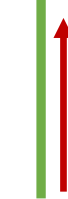
BioStar 2



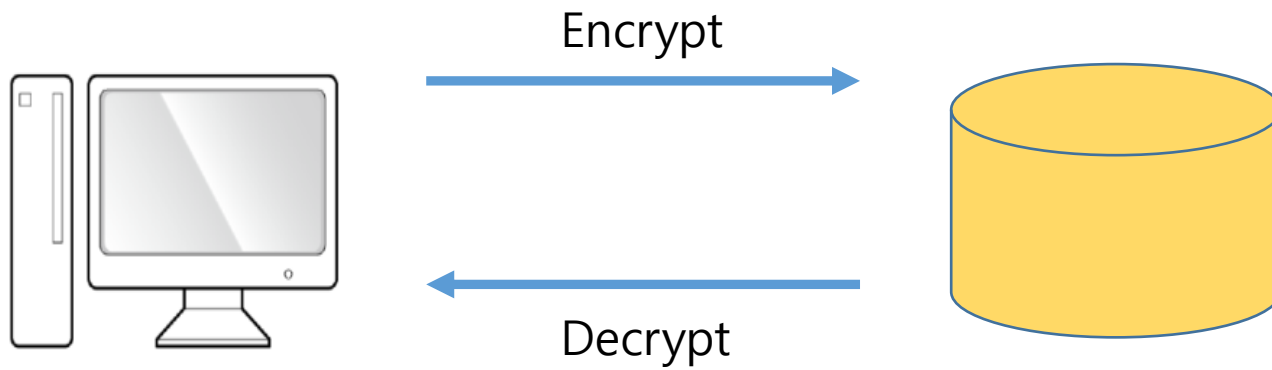
TCP/IP



RS-485



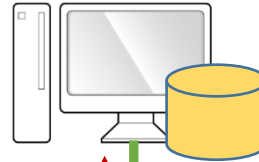
Encrypt Sensitive Data on Database



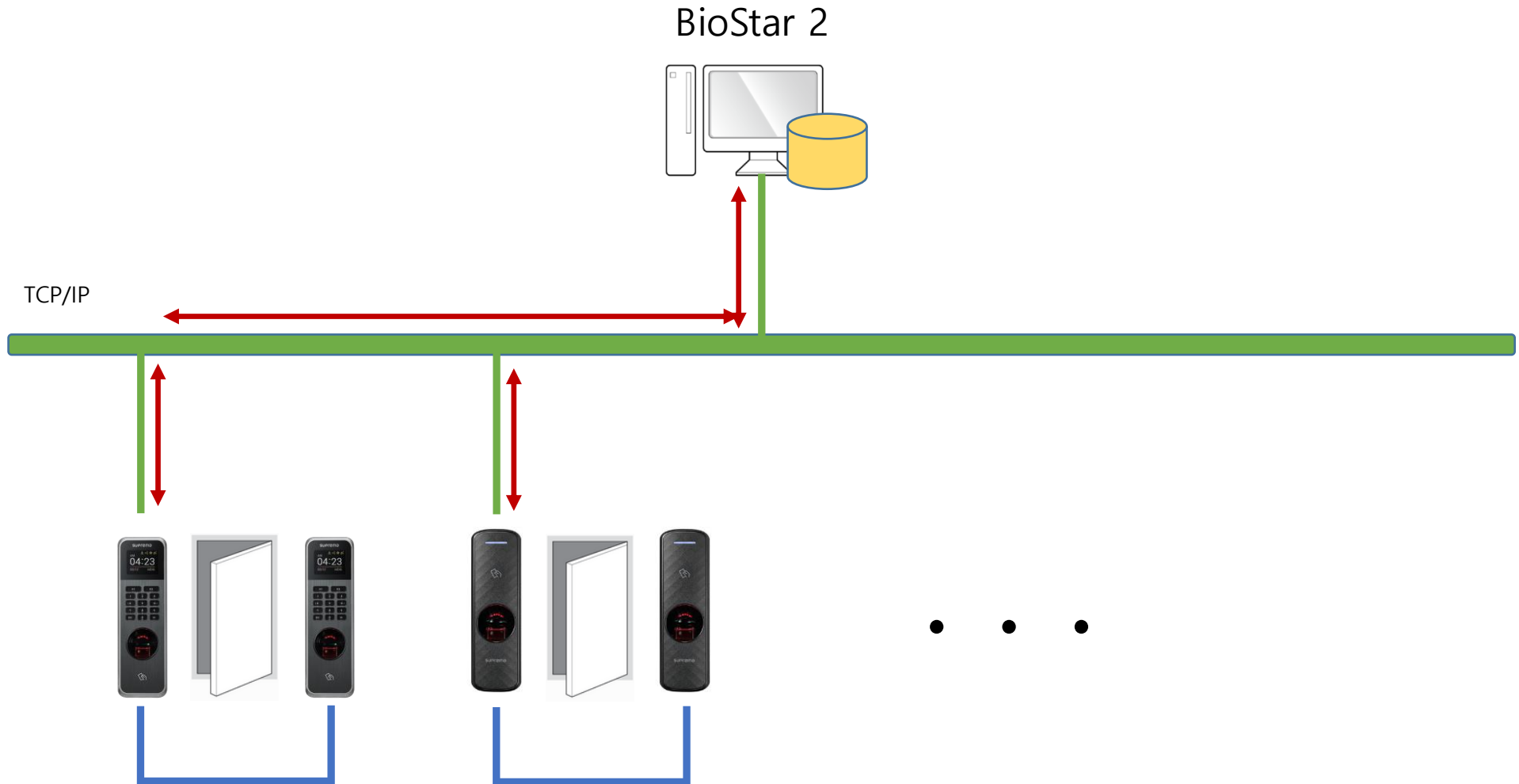
- ✓ Encrypt Sensitive Data on Database
- ✓ Secure Communication with Device
- ✓ Hash Key Management

Secure Communication with Device

BioStar 2



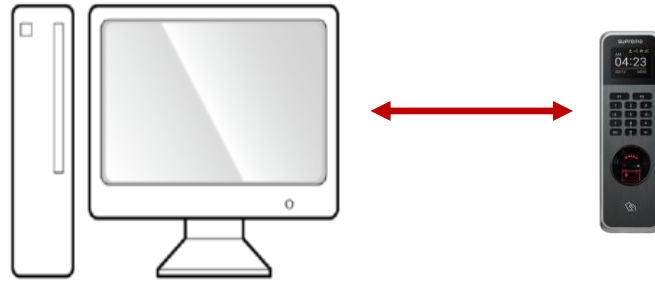
TCP/IP



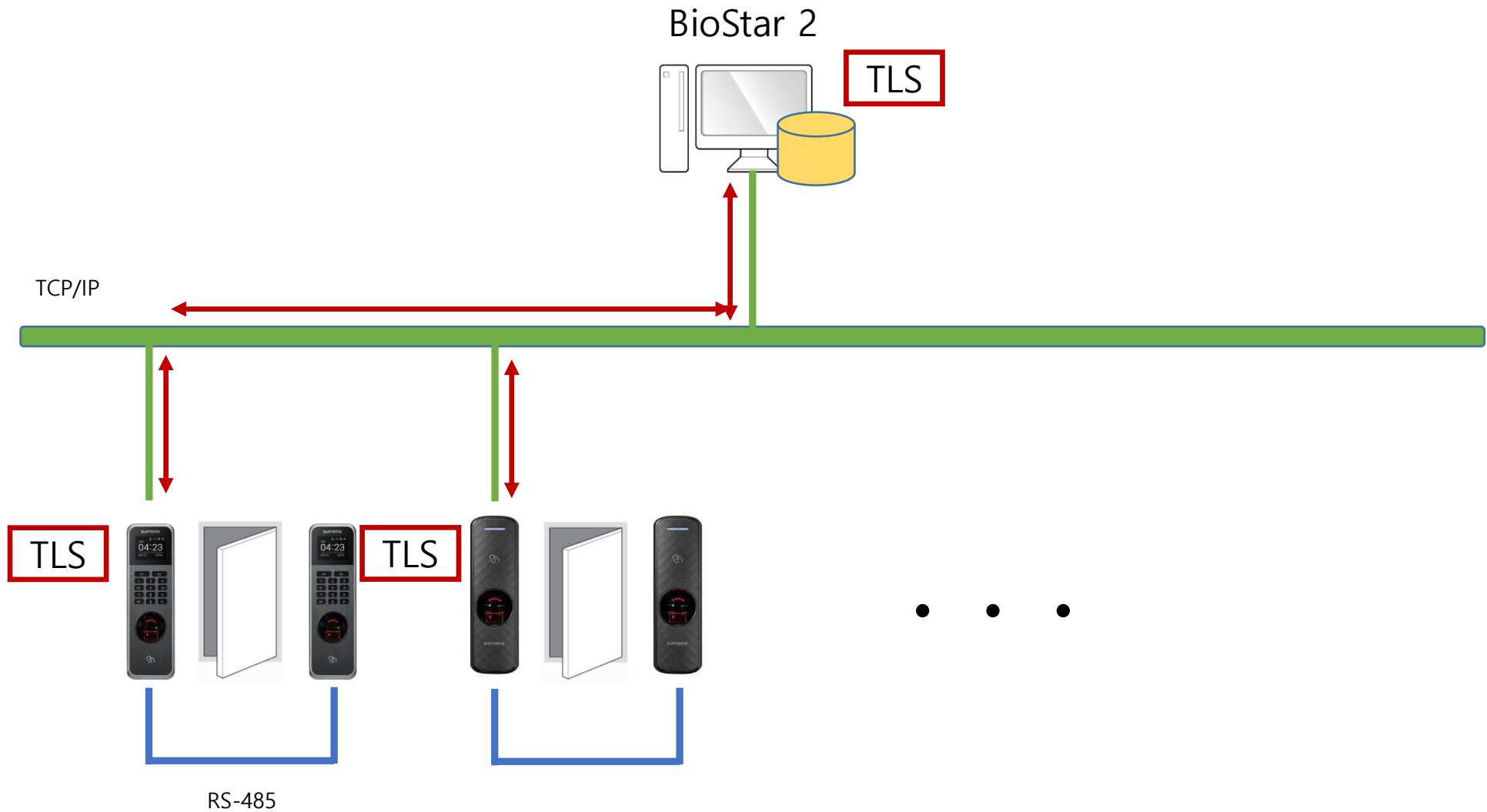
RS-485

Secure Communication with Device

Attacker's BioStar 2

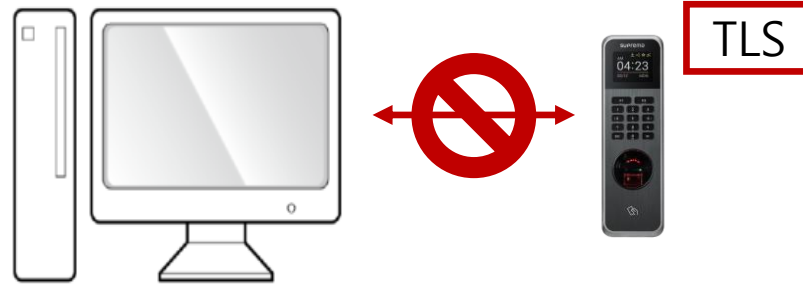


Secure Communication with Device



Secure Communication with Device

Attacker's BioStar 2



- ✓ Encrypt Sensitive Data on Database
- ✓ Secure Communication with Device
- ✓ Hash Key Management

Hash Key Management

- ✓ When does the hash key get used?
 - Hash key is used to encrypt PIN and PW
 - Hash key needs to be shared to support users created from devices and other servers

- ✓ What is hash key management?
 - An option to be able to set a unique hash key for a specific site

Upcoming Features

- ✓ Enhanced Data Storage on Device
- ✓ BioStar 2 Key Management
- ✓ Replace Oracle Java to Open JDK Environment



Q&A

Thank you!