

HOW TO CONNECT AN EXTERNAL READER TO THE SIGMA FAMILY



ACRONYMS

MWC=MORPHO WAVE COMPACT

UP=USER POLICY

BDP=BIOMETRIC DEVICE PROFILE

MM=MORPHO MANAGER

PHYSICAL CONNECTION

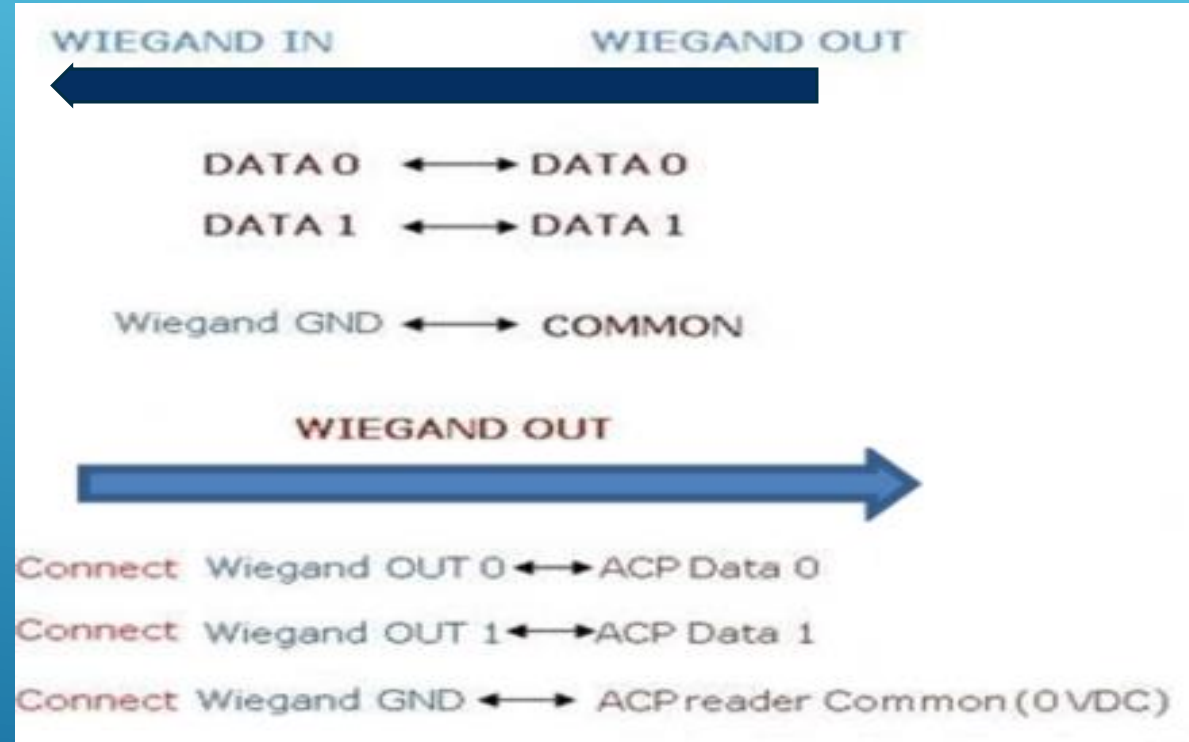


THEY ARE TWO EXAMPLES IN THE NEXT PAGES BUT THE WIRING IS BASICALLY ALL THE SAME WITH ALL THE SIGMA FAMILY INCLUDING THE MWC AND VIP

PHYSICAL CONNECTION BETWEEN A SIGMA READER



PHYSICAL CONNECTION BETWEEN A SIGMA READER AND EXTERNAL READER



Take the External reader's Wiegand OUT to the Wiegand IN of the Sigma



PHYSICAL CONNECTION BETWEEN A SIGMA READER AND EXTERNAL READER



Access Control Panel



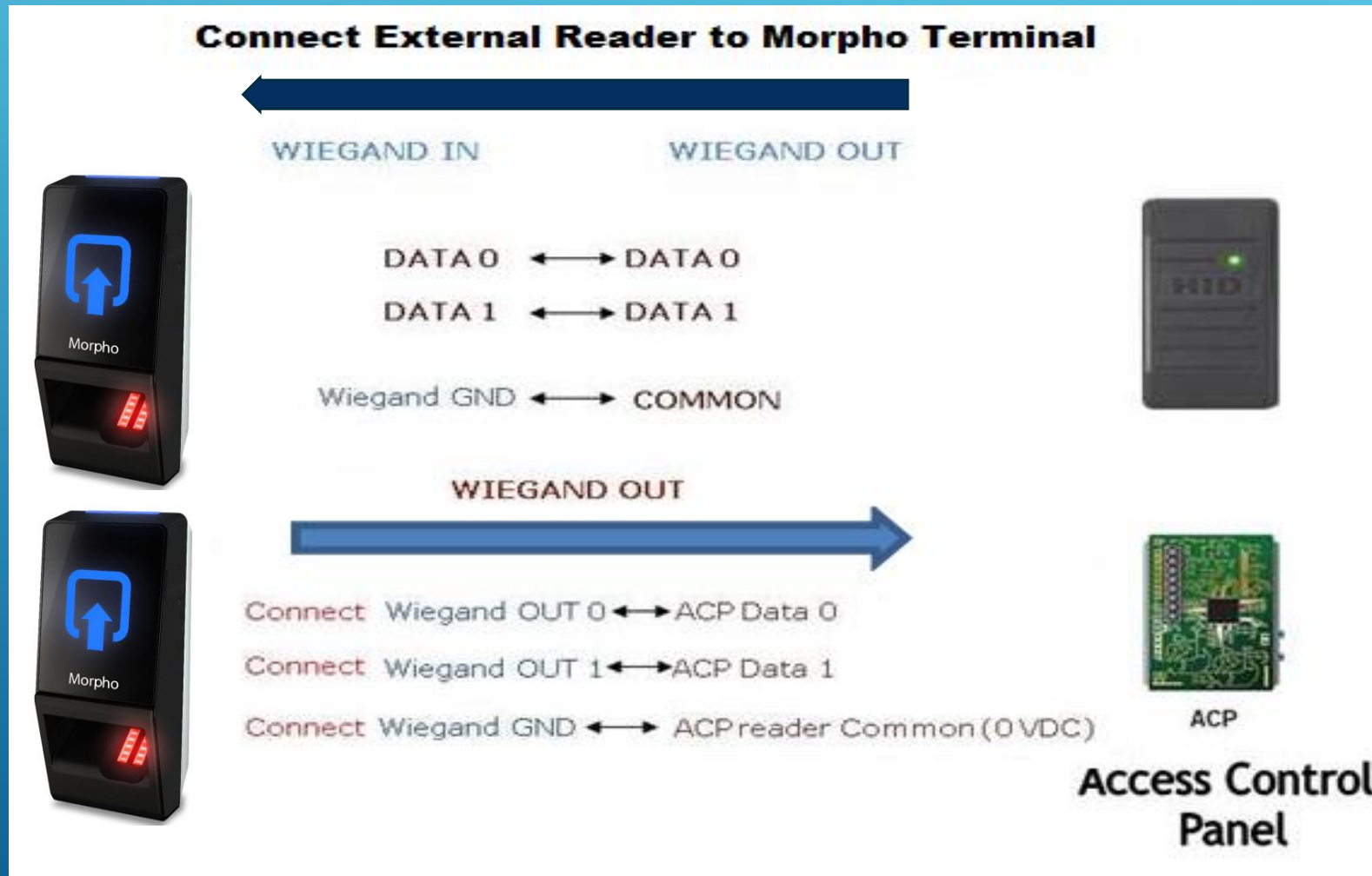
From Wiegand OUT from the Sigma to your ACP



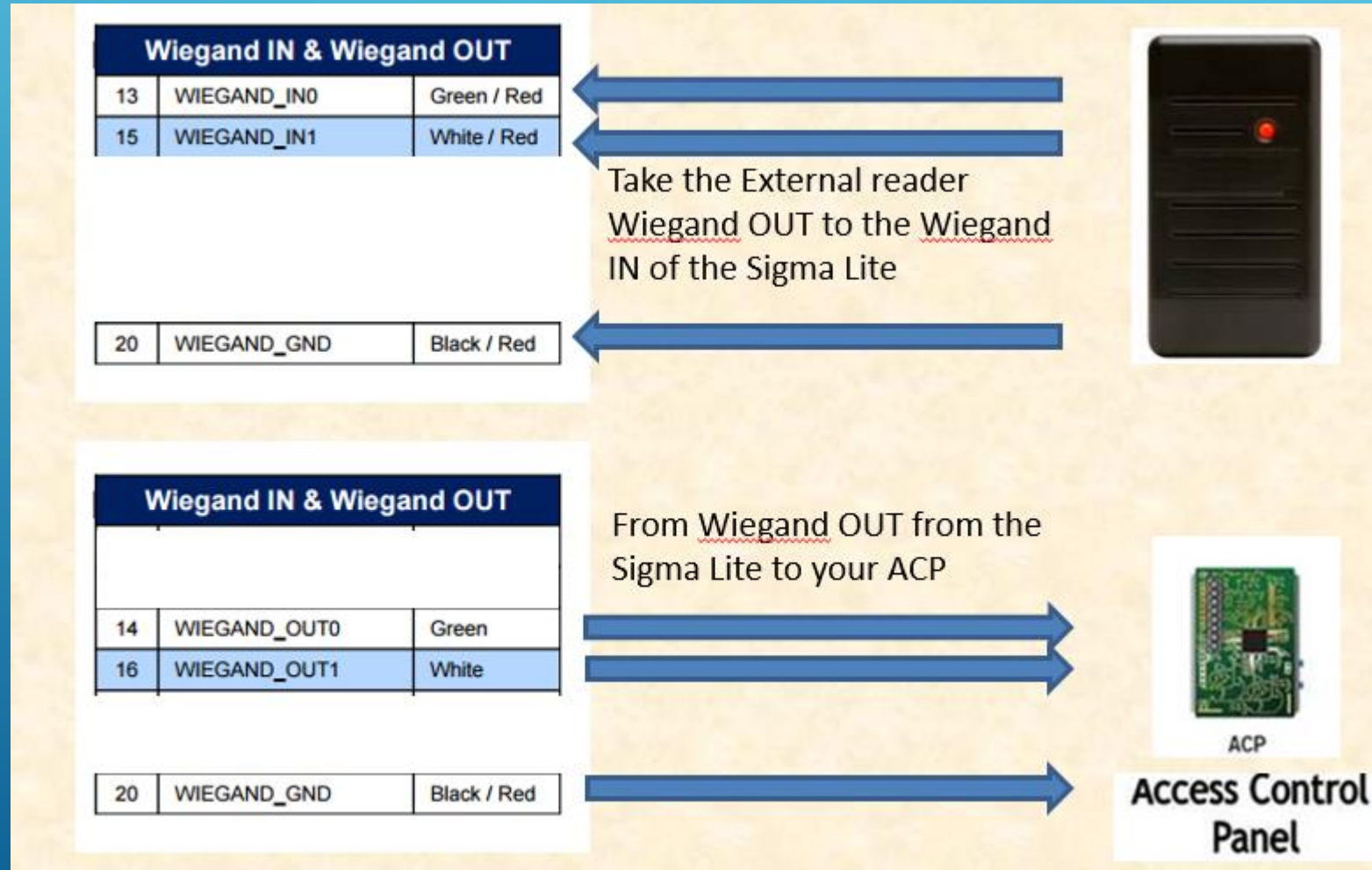
PHYSICAL CONNECTION BETWEEN A SIGMA LITE READER



PHYSICAL CONNECTION BETWEEN A SIGMA LITE AND EXTERNAL READER



SAME WIRING STRUCTURE FOR ALL SIGMA PRODUCTS INCLUDING MWC AND VIP



MORPHOMANAGER

MORPHOMANAGER DEFAULT LOG IN

USERNAME-ADMINISTRATOR

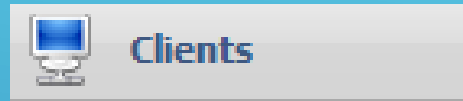
PASSWORD-PASSWORD

ADD AN BIOMETRIC DEVICE

Administration>Biometric Device

Biometric devices from three different hardware families can be added here; the MA 100, MA J, MA 500, and MA VP family, the MA Sigma, MA Sigma Lite And MA Sigma Lite + MA Sigma Extreme, the Morpho 3D Face, the MorphoWave Tower, MorphoWave Compact, and the Morpho Tablet Terminal.

CLIENTS



Path Administration>Clients

Clients are computers that have the MorphoManager Client software installed and communicate with a MorphoManager server

ADD YOUR DEVICE TO YOUR CLIENT

The screenshot shows a software interface with a left-hand navigation pane and a main content area. The navigation pane lists various settings: Operator, Key Policy, Biometric Device Profile, Biometric Device, Wiegand Profiles, User Policy, Access Schedules, User Distribution Group, User Authentication Mode, Operator Role, Notifications, and Clients. The 'Clients' item is highlighted with a blue arrow pointing to it. The main content area is titled 'Enter the details for this client' and contains three input fields: 'Name:' with the text 'This PC', 'Description:', and 'Location:'. A red callout box at the bottom right contains the text 'Click Next until you get to Enrollment devices'.

Operator

Key Policy

Biometric Device Profile

Biometric Device

Wiegand Profiles

User Policy

Access Schedules

User Distribution Group

User Authentication Mode

Operator Role

Notifications

Clients

Enter the details for this client

Name: This PC


Description:

Location:

Click Next until you get to Enrollment devices

SEARCH FOR YOUR DEVICE UNDER CONTACTLESS ENROLLMENT OR CAN BE A CONTACT READER OR A FACE READER

Contact Enrollment	
Morpho Finger biometric enrollment:	<input type="text" value="Selected MorphoAccess"/>
Morpho Finger enrollment MorphoAccess:	<input type="text" value="Sigma Iclass"/>
<input type="button" value="Search"/>	
Contactless Enrollment	
Morpho Contactless Finger biometric enrollment:	<input type="text" value="Selected MorphoWave Compact (IP)"/>
Morpho Contactless Finger enrollment MorphoAccess:	<input type="text" value="Work MWC"/>
<input type="button" value="Search"/>	
5G Face Enrollment	
Morpho face biometric enrollment:	<input type="text" value="Selected MorphoAccess"/>
Morpho face enrollment MorphoAccess:	<input type="text" value="Work VIP"/>
<input type="button" value="Search"/>	
Smartcard Encoding	
Morpho Smartcard encoding:	<input type="text" value="Selected USB card reader"/>
Morpho Smartcard encoding PC/SC device:	<input type="text"/>
Morpho Smartcard encoding MorphoAccess:	<input type="text"/>
<input type="button" value="Search"/>	



BIOMETRIC DEVICE PROFILE



Biometric Device
Profile

Path Administration>Biometric Device Profile

The Biometric Device Profile will define common settings and parameters for one or more biometric devices. This profile can be applied when adding units into the system from the Biometric Device section of Administration

BIOMETRIC DEVICE PROFILE

CREATE OR EDIT THE BIOMETRIC DEVICE PROFILE

Operator

Key Policy

Biometric Device Profile

Biometric Device

Wiegand Profiles

User Policy

Access Schedules

User Distribution Group

User Authentication Mode

Enter details for the Biometric Device Profile

Name:

Description:

Configuration Mode:

Log Retrieval Enabled:

Log retrieval interval: (seconds)

Duplicate check on biometrics: (Does not apply to Morpho 3D Face or MorphoTablet. Only applicable to new user adds or rebuild operations)

MorphoAccess heartbeat interval: (seconds)

Key Policy:

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MA Sigma VP Only Settings

Allow Remote Enrollment:

Default User Policy for Remote Enrollment:



Next

BIOMETRIC DEVICE PROFILE

Biometric Device Settings

General Settings

Wiegand Profile: Standard 26 bit

Language: English

Realtime logging enabled:

Biometric Threshold Settings


Biometric Threshold: Recommended

MorphoAccess Vein Print Mode: Universal Fast


MorphoAccess Fingerprint Threshold: 3

Morpho 3D Face Identification Threshold: Medium

Morpho 3D Face Verification Threshold: Low

 It is recommended the mode set in User Policy for enrollment should be the same mode or a more restrictive mode than the mode set in Biometric Device Profile. Using a less restrictive mode in User Policy than in Biometric Device Profile is likely to increase the False Rejection Rate (FRR) of biometric devices.




Next 

WIEGAND PROFILE: THIS VALUE WILL BE SENT BACK TO YOUR ACP

BIOMETRIC DEVICE PROFILE

Multi-Factor Mode Settings

Multi-Factor Mode: 

Contactless Smart Card Mode:

Morpho 3D Face Multi-Factor Mode

Mode:

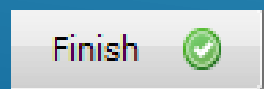
MA 100, MA J, MA 500, MA VP Multi-Factor Mode

Mode:

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MA VP MD, VisionPass, and Mor

Biometric:	<input type="checkbox"/>	Mifare Classic:	<input type="checkbox"/>
Proximity Card:	<input type="checkbox"/>	Mifare DESFire 3DES:	<input type="checkbox"/>
Wiegand In:	<input checked="" type="checkbox"/>	Mifare DESFire AES:	<input type="checkbox"/>
Clock and Data In:	<input type="checkbox"/>	Keypad:	<input type="checkbox"/>
HID iClass:	<input type="checkbox"/>		
HID iClass SEOS:	<input type="checkbox"/>		

SET THE MULTI-FACTOR MODE TO WIEGAND IN AS EXACTLY AS SHOWN



USER POLICY



Path Administration>User Policy

Create new User Policy

Select the User Policy that this user will belong to. This is an important selection, as the policy will determine Biometric Device access and other access control and time & attendance settings.

USER POLICY

CREATE A NEW USER POLICY

- Operator
- Key Policy
- Biometric Device Profile
- Biometric Device
- Wiegand Profiles
- User Policy**
- Access Schedules
- User Distribution Group
- User Authentication Mode

Enter the details for this User Policy

Name:

Description:

Access Mode:

Allow MA 500 database selection during user enrollment

Access Schedule:

Extended User Details: Display extended user details

Wiegand Profile:

User Authentication Mode:

Show Photo Capture Page:

Next 


**WIEGAND PROFILE- WILL BE WHAT ASSIGN TO THIS USER
UAM- SELECT WEIGAND IN AND BIOMETRIC(1-1)**

USER POLICY FINGER

CLICK TWO OR SELECT NONE DEPENDING IF YOUR USING FOR CARD AND FINGER
FOR EXAMPLE

Enter the details for finger biometric options

Finger Biometric Enrollment Minimum Fingers:	Two
Preferred Finger One:	Left Index Finger
Preferred Finger Two:	Right Index Finger
Preferred Duress Finger:	Left Middle Finger
Vein / Print Mode:	Universal Fast

 It is recommended the mode set in User Policy for enrollment should be the same mode or a more restrictive mode than the mode set in Biometric Device Profile. Using a less restrictive mode in User Policy than in Biometric Device Profile is likely to increase the False Rejection Rate (FRR) of biometric devices.



USER POLICY HAND

CLICK TWO OR LEAVE UNCHECKED DEPENDING IF YOUR USING FOR CARD
AND HAND FOR EXAMPLE

Enter the details for wave biometric options

Wave Enrollment Minimum Hands:

Two

Show Wave Biometric Capture Page:



Finish



USER POLICY FACE

CLICK FACE CHECK BOX OR LEAVE UNCHECKED DEPENDING IF YOUR USING
FOR CARD AND FACE FOR EXAMPLE

Enter the details for face biometric options

Require face biometric enrollment:



Show face biometric capture page:



Finish





USER MANAGEMENT



Users are people who will have their biometric data sent to the selected Biometric Device for identification purposes for either access control or time and attendance.

USER MANAGEMENT

 Home


 Administration

 User Management

CREATE A NEW USER WITH THE USER POLICY CREATED EARLIER

Enter details for this User

User Policy:

External Reader and Bio Reader 

Enabled:



First Name:

Joe

Middle Name:

Last Name:

Smith

Date of Birth:

Use M/d/yyyy eg. 3/24/1986.



Next

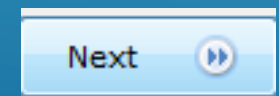


USER MANAGEMENT

THE USER ID NUMBER WOULD BE THE CARD NUMBER IF YOU WERE PRESENTING A CARD TO THE EXTERNAL CARD READER THEN BIOMETRICS

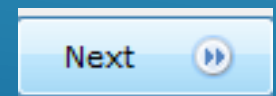
Wiegand Values

User ID	12345
---------	-------



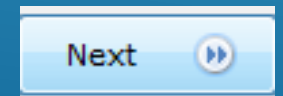
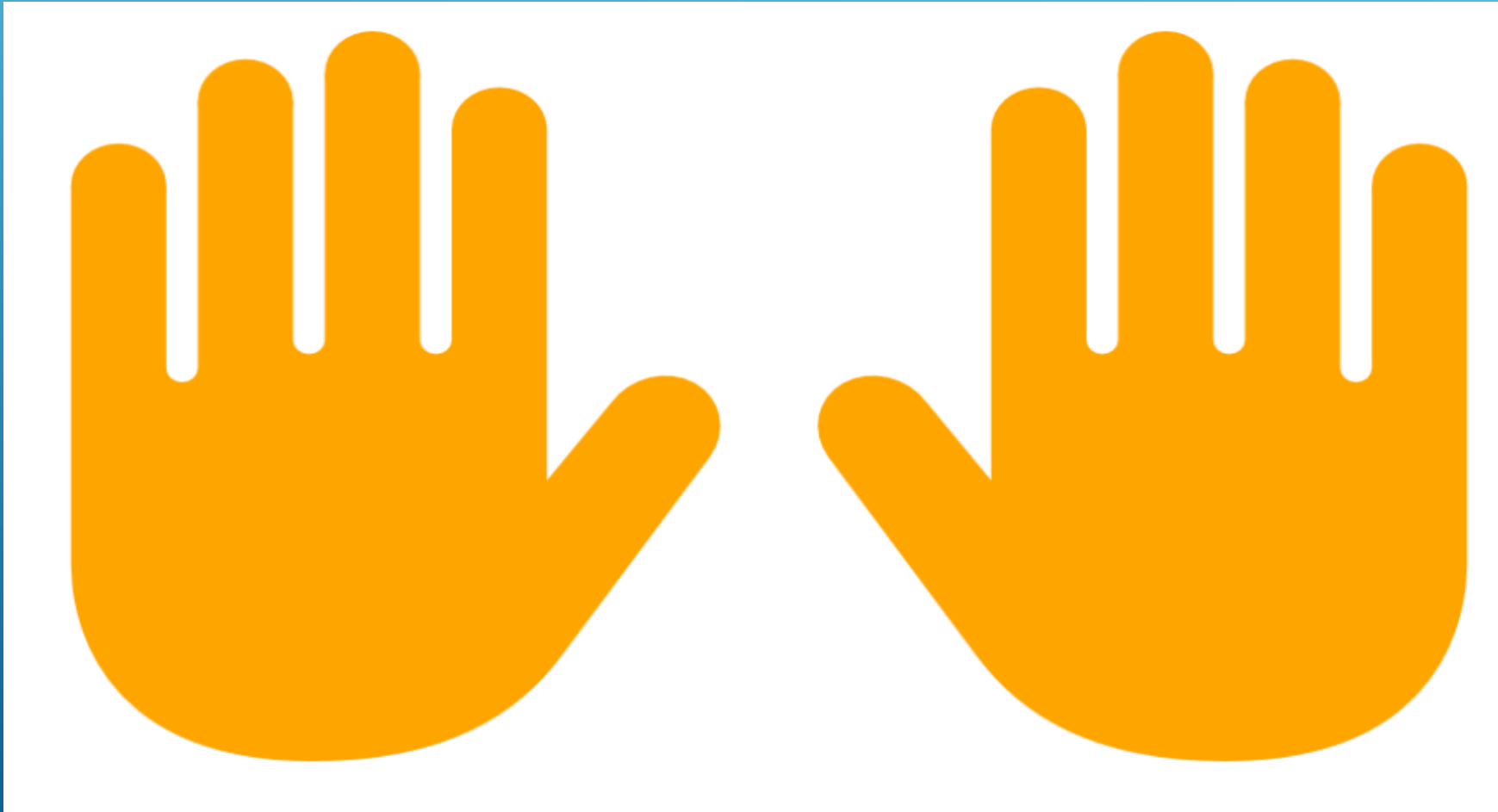
USER MANAGEMENT

THE NEXT STEPS ALL DEPEND WHAT DEVICE YOUR CONNOTED TO:
FOR THE MWC YOUR GOING TO CAPTURE HANDS
FOR THE SIGMA FAMILY YOUR GOING TO CAPTURE FINGERS
FOR THE VIP READER YOUR GOING TO CAPTURE FACE
THIS WAS DETERMINE ON WHAT WAS SET UP IN THE USER POLICY EARLIER



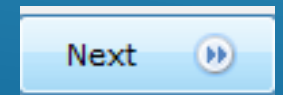
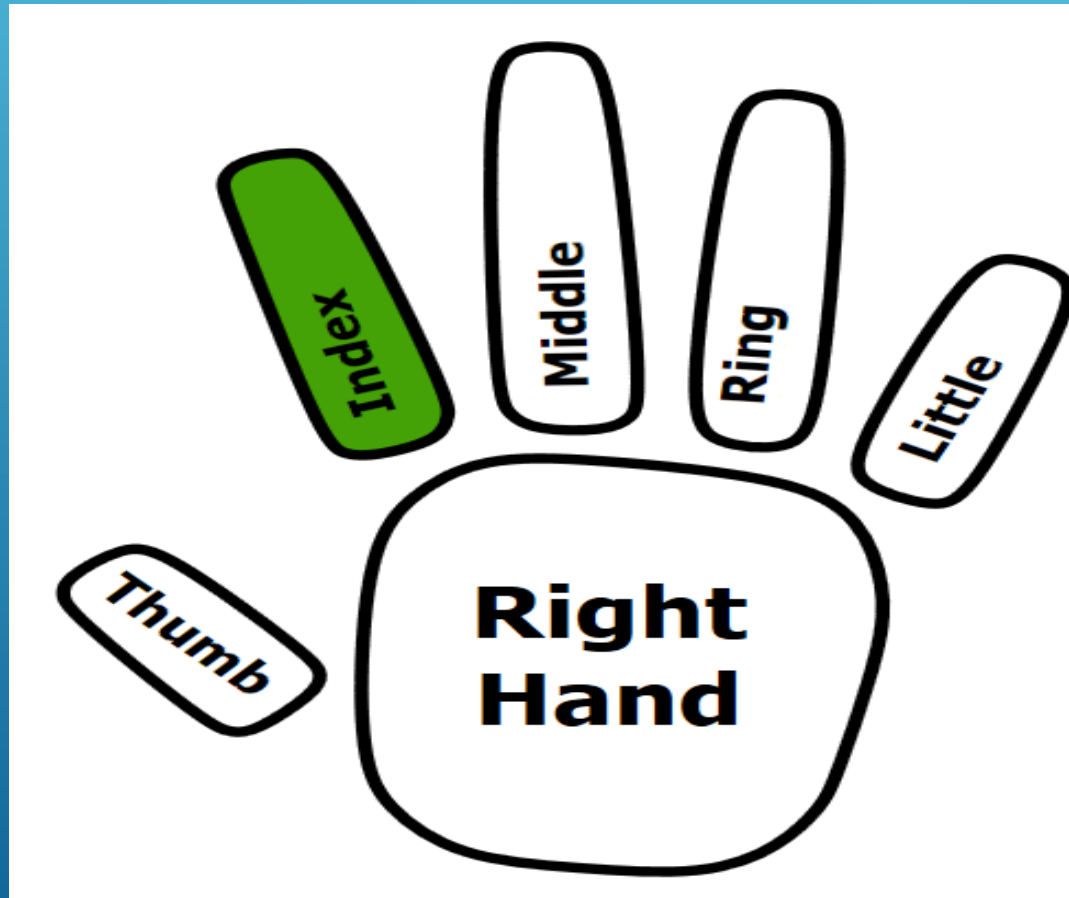
USER MANAGEMENT

FOR HAND ENROLLMENT CLICK ON THE FLASHING HANDS TO START CAPTURING



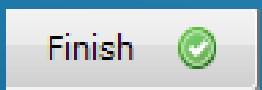
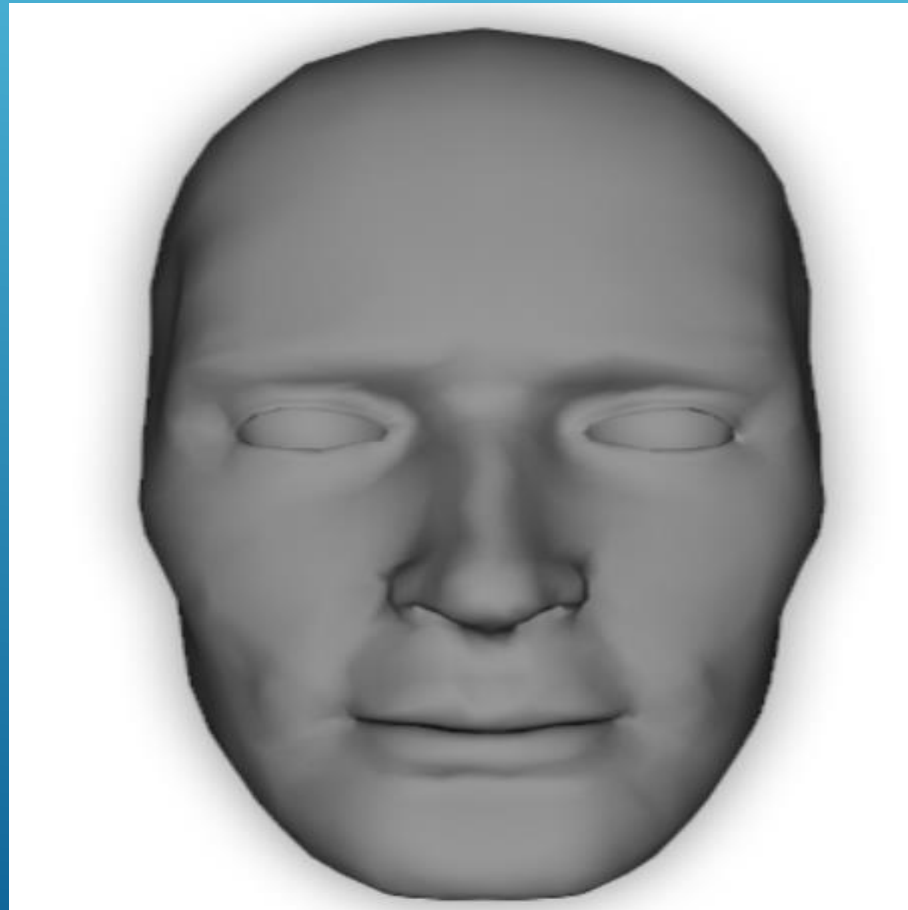
USER MANAGEMENT

FOR FINGER ENROLLMENT CLICK ON THE FLASHING FINGERS TO START CAPTURING



USER MANAGEMENT

FOR FACE ENROLLMENT CLICK ON THE FLASHING FACE TO START CAPTURING



WEBSITE

Please visit our website,
service.morphotrak.com for
software, firmware, videos and
PDF'S