Enforced Security, new default configuration

Technical bulletin for Access and Time Biometric Terminals

Corporate Identity | Access and Time Biometric Terminals | December 2022

About IDEMIA

IDEMIA, the global leader in Augmented Identity, provides a trusted environment enabling citizens and consumers alike to perform their daily critical activities (such as pay, connect and travel), in the physical as well as digital space. Securing our identity has become mission critical in the world we live in today.

By standing for Augmented Identity, an identity that ensures privacy and trust and guarantees secure, authenticated, and verifiable transactions, we reinvent the way we think, produce, use and protect one of our greatest assets – our identity – whether for individuals or for objects, whenever and wherever security matters.

We provide Augmented Identity for international clients from the Financial, Telecom, Identity, Public Security and IoT sectors. With close to 15,000 employees around the world, IDEMIA serves clients in 180 countries.

| For more information, visit www.idemia.com / Follow @IdemiaGroup on Twitter

Warning

Information in this document is subject to change without notice and does not represent a commitment from IDEMIA.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without the express written permission of IDEMIA.

This legend is applicable to all pages of this document

Revision History

Version	Date	Content
1	September 21st 2022	Document creation
2	December 13th 2022	Update with links for MorphoManager “How to” guides

Introduction

Since the introduction of biometric terminals a few decades ago, IDEMIA has continuously improved the products security. In 2022, the improvements include a new default configuration of the devices. The purpose of this document is to provide an overview of this default configuration, its benefits and impacts on the ways products are configured before operations.

The products covered are:

- MorphoWave Compact / XP, from firmware 2.9
- MorphoWave SP, from firmware 1.1
- VisionPass, from firmware 2.9
- SIGMA Lite and Lite+, from firmware 4.12
- SIGMA Wide, from firmware 4.12
- SIGMA Extreme, from firmware 4.12

Table of contents

Focus for installers

Background: a few words about cybersecurity

Over the last past years the importance of cybersecurity has kept on increasing, in various contexts and for all industries, covering a large spectrum of aspects, such as regulation, standards and policies. This naturally lead to growing expectations from customers.

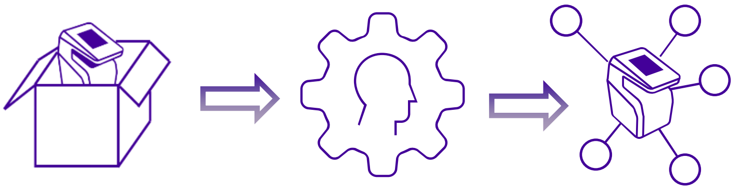
In the ecosystem of access control, meeting these expectations may represent a challenge, going through the various stakeholders involved, from the manufacturer (IDEMIA) to the end customer, via the distributor, the Embedded Solution Partner and Security System Integrator.

The purpose of cybersecurity is to protect individuals and assets. A category of assets have a specific importance: Personal Identifiable Information (PII). In an increasing number of countries, PII are subject to regulations, like the European GDPR (General Data Protection Regulation). In many ways, protecting assets in general with cybersecurity solutions is efficient to preserve Personal Data in particular.

IDEMIA addresses cybersecurity on biometric terminals with three levers:

- Integrating it in the product development cycle
- Considering it in the usage environment
- Designing the product set-up

Security by default evolution is part of this last lever.



To summarize, the new default configuration of biometric terminals, enforcing security, will help compliance in general, for instance to internal policies or to PII directives, like GDPR.

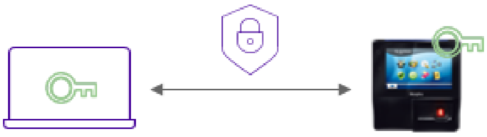
Terminals evolutions: security by default

Evolution purpose

IDEMIA biometric terminals propose a very large area of different use cases, features and options. From a historical perspective, these were all available, and were to be configured at installation depending on the system. Features and configurations related to security were optional.
The new default configuration reverses this principle: security configuration is now mandatory, and required before functional set-up.

As we will illustrate below, ensuring secure communication is key: TLS protects data that are transferred between the terminal and the machine (laptop, server…) interacting with it, providing:

- Confidentiality (data cannot be stolen)
- Integrity (data cannot be modified)



Terminal interfaces

The modifications in the default configuration, compared to the previous one, are derived from a two-angled approach:

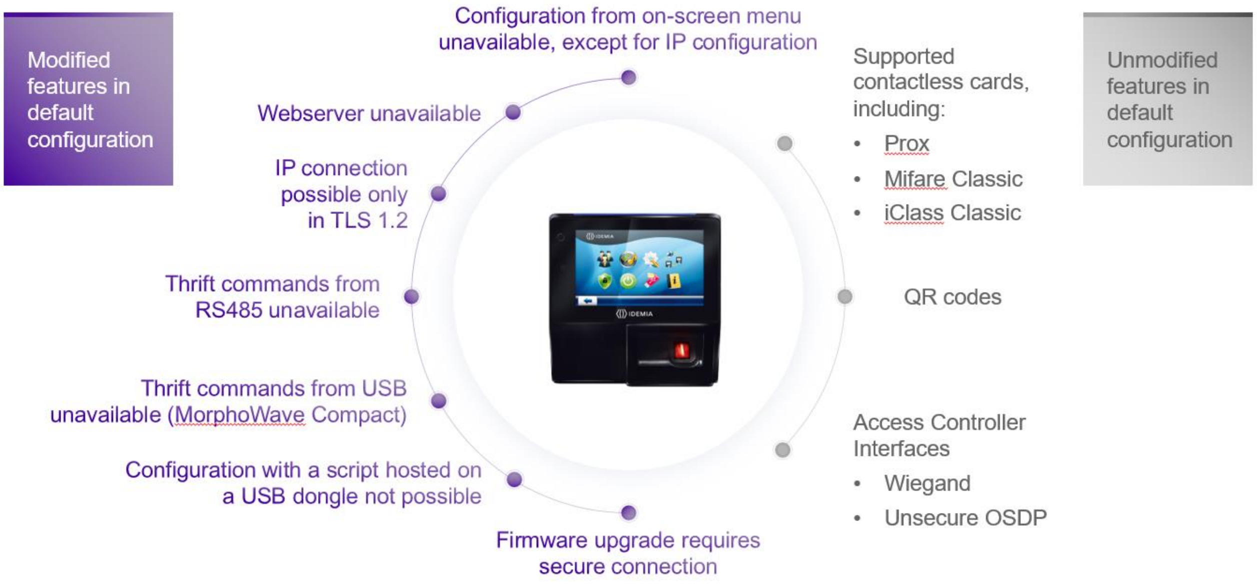
- Minimize the attack surface, meaning the number of entry points an attacker could leverage to try and intrude in the system
- Disable the features that are not recommended for security reasons (as defined in the previous versions of the Recommendations for a secure installation document).

The modifications resulting from this approach are:

- Communication with the terminal is mandatorily secured with TLS. Clear communication over IP is not possible. This includes communication:
  - with MorphoBioToolBox (MBTB)
  - with MorphoManager
  - for firmware upgrade
- The configuration of the terminal from on-screen menu is not possible any more, except for IP configuration
- The webserver is not active
- The configuration of the terminal from a USB dongle (hosting scripts) is not possible any more.

Please note the considered attack surface and features were analyzed from the standpoint of the IDEMIA technology only. Some interfaces are known not to be state-of-the-art in terms of security (Wiegand connection, legacy contactless cards, QR codes, etc.). We have chosen to keep them available in the secure configuration, as they are imposed by the access control system the terminal is integrated in.

Modified and unmodified features are summarized in the below diagram:



Modified features in default configuration

Configuration from on-screen menu unavailable, except for IP configuration

Webserver unavailable

IP connection possible only in TLS 1.2

Thrift commands from RS485 unavailable

Thrift commands from USB unavailable (MorphoWave Compact)

Configuration with a script hosted on a USB dongle not possible

Firmware upgrade requires secure connection

Unmodified features in default configuration

Supported contactless cards, including:

- Prox
- Mifare Classic
- iClass Classic

QR codes

Access Controller Interfaces

- Wiegand
- Unsecure OSDP

Terminal Security state

The new default configuration will be the one for:

- newly shipped terminals
- terminals upgraded with the latest firmware version.

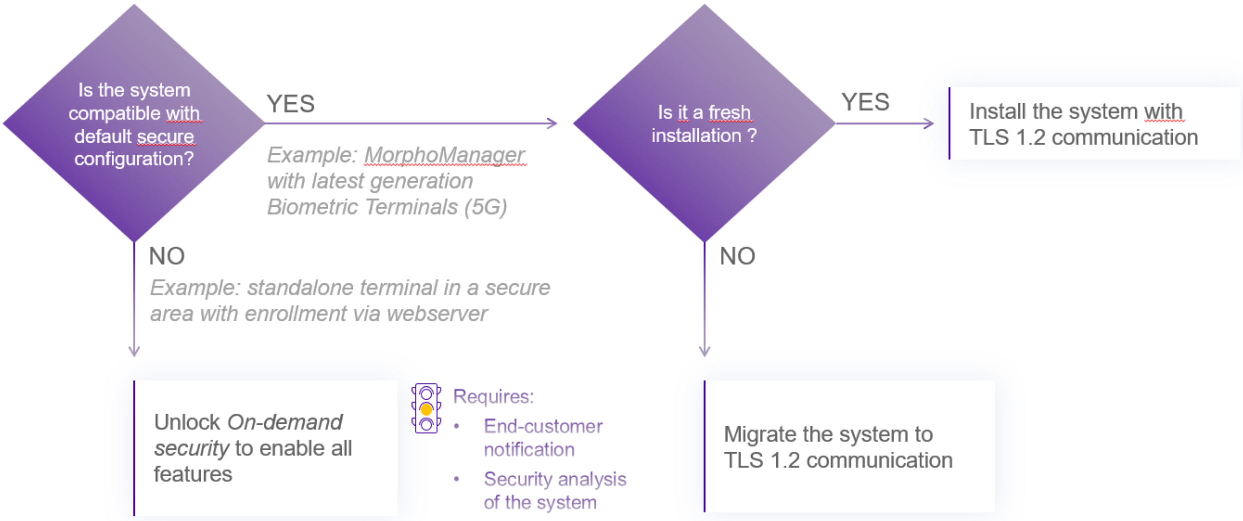
It is the configuration recommended by IDEMIA. If the system in which the terminal is integrated requires features that are out of this default configuration, these features can be unlocked switching the terminal from the Enforced Security state to the On-demand security state.

As the *On-demand security* state may affect the security of the full system, unlocking it requires:

- an impact analysis on the security of the system
- the end-customer to be notified, as they are the ones possibly affected by a system vulnerability.

End customers scenarios

The below diagram illustrates how to adapt to the security by default configuration:


Is the system compatible with default secure configuration?
YES
Example: MorphoManager with latest generation Biometric Terminals (5G)
NO
Example: standalone terminal in a secure area with enrollment via webserver
Is it a fresh installation ?
YES
Install the system with TLS 1.2 communication
NO
Unlock On-demand security to enable all features
Requires:
End-customer notification
Security analysis of the system
Migrate the system to TLS 1.2 communication

New installer journey: security set-up

As described above, the first set-up step for a terminal is its security configuration. This step consists in

- either configuring the TLS communication
- or unlocking the *On-demand security* state

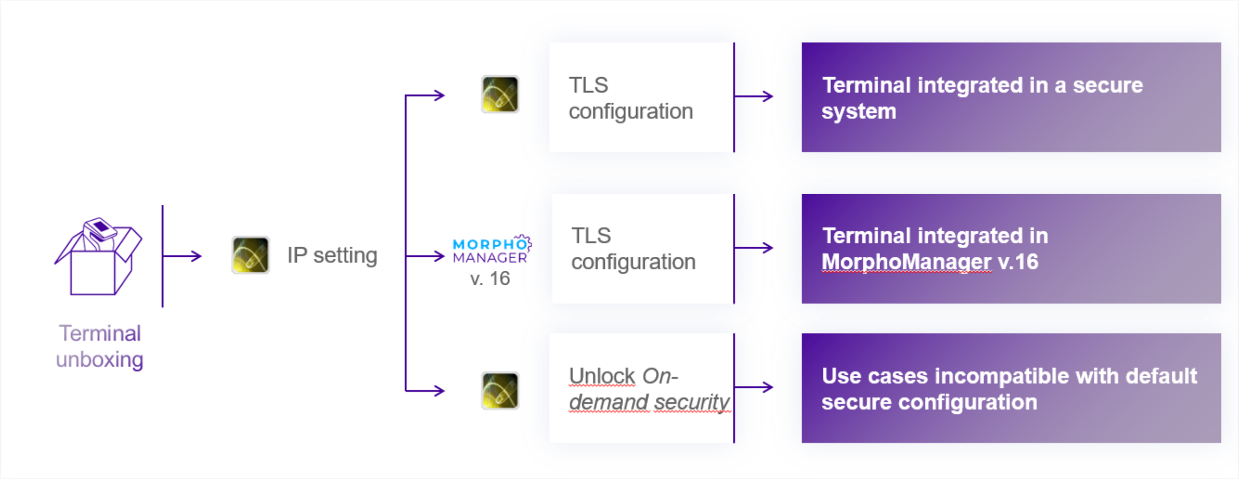
Setting the IP address of the terminal is a pre-requisite for either of these paths.

The below table describes what software can be used for each of these operations:

Operation	Software	Comment
Set IP address	MorphoBioToolBox	Or via the on-screen menu, if available
Configure TLS	MorphoBioToolBox or MorphoManager v16 or higher (*)	No other option is available for a newly shipped terminal
Switch to On-demand security state	MorphoBioToolBox	

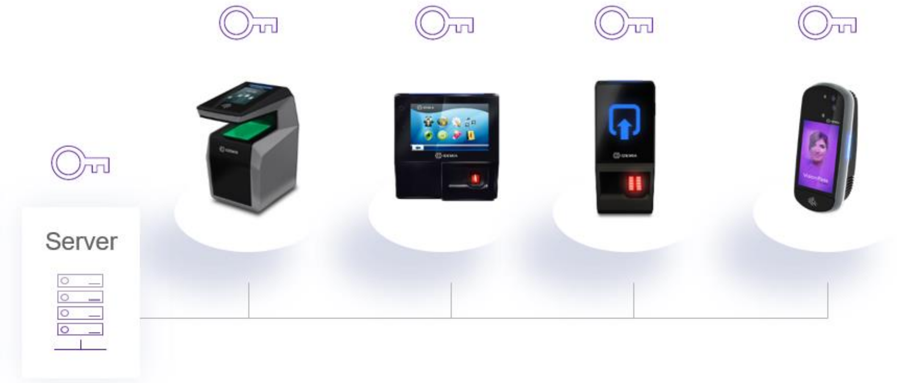
(*) MorphoManager v16 is not released when this bulletin is being written.

The below diagram summarizes the security set-up process:

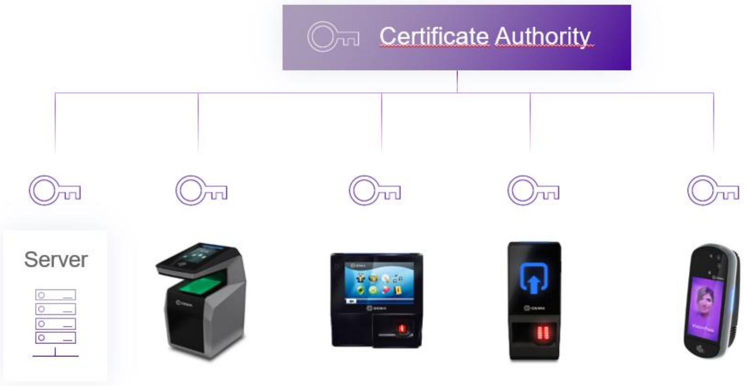

Terminal unboxing
IP setting
MORPHO MANAGER v. 16
TLS configuration
TLS configuration
Unlock On-demand security
Terminal integrated in a secure system
Terminal integrated in MorphoManager v.16
Use cases incompatible with default secure configuration

Basics about TLS secure communication

In a TLS system, each component (a terminal or a computer) has a unique TLS key. The latter is used to secure the communication of the component with the other component(s).



All TLS keys are signed by the Certificate Authority:



The certificate authority shall be specific to one installation, in order to ensure that a component of a system will not trust the component of another system.

Keys and certificate authorities have a validity period and require renewal in order for the system operations to continue after this validity period expires.

MorphoManager

Version 15

Version 15 is compatible with terminals default secure configuration. TLS keys are to be generated with MBTB, and then manually imported into the software.

Version 16 or higher

To improve security, smoothen installation and ease compliance while providing better control, MorphoManager 16 introduces a new configuration: Secure Communication Policy. Three policies are possible:

Policy	Description	Terminal Compatibility
Enforced security, self-generated certificates	TLS mandatory TLS certificates automatically generated Only policy in the Express Configuration wizard	• MorphoWave Compact / XP • MorphoWave SP • VisionPass • SIGMA Lite and Lite+ • SIGMA Wide • SIGMA Extreme
Enforced security, Imported certificates	TLS mandatory TLS certificates managed outside MorphoManager	
On-demand security	Same as version 15	Same as version 15

Selecting a policy is a mandatory step at installation or upgrade from version 15.

The Enforced security, self-generated certificates policy is recommended for systems without specific requirements on secret management or for administrators unfamiliar with TLS.
This configuration automatically:

- creates the necessary Certificate Authority and TLS keys;
- dispatches them to the system components (computer, terminals).

MorphoBioToolBox

Security set-up

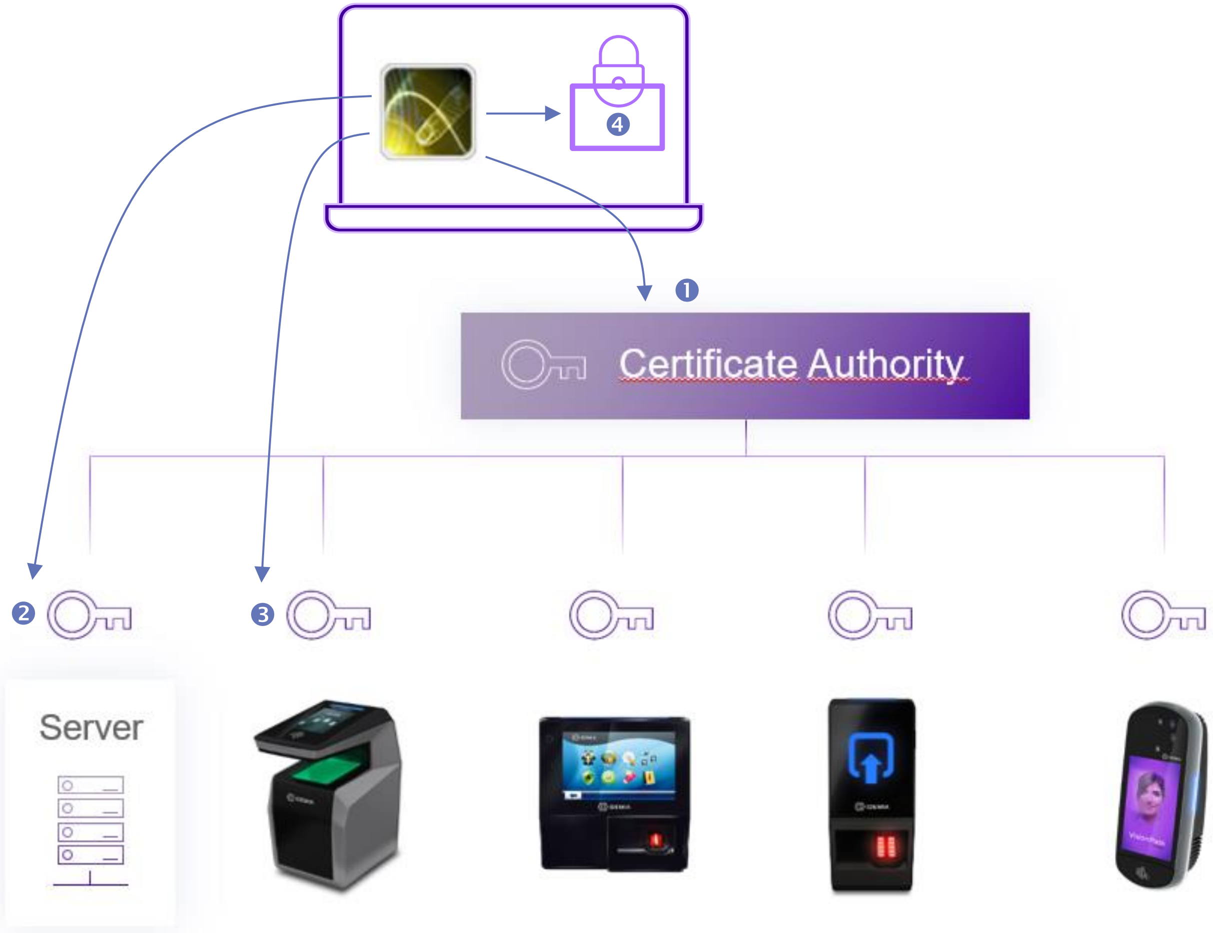
MorphoBioToolBox version 4.6 introduces 3 new features:

Feature	Typical targeted system
Generation of TLS keys	MorphoManager 15
Dispatch of TLS keys into a group of up to 100 terminals	MorphoManager 15
Unlock On-demand security state	Incompatible with Enforced Security state (no TLS, enrollment via Webserver, etc.)

Generation of TLS keys

This MBTB feature proposes the following operations:

1. Generation of Certificate Authority for a full system
2. Generation of TLS key for the PC communicating with the terminals (signed by the Certification Authority)
3. Generation of TLS key for each terminal of the system (signed by the Certification Authority)
4. Local storage of keys, with password protection



The password for the local storage of TLS keys is required during the full lifecycle of the system, to add terminals or to renew certificates after expiration. For this reason, it shall be recorded with care, as it cannot be retrieved: in case it is lost, all system components need to be reset to default factory settings.

"*How to*" guidelines

To go further and have step by step guides for the installation, our knowledge base, available on the IDEMIA portal, provides full details and documentation, depending on what you want to achieve with the terminal:

MorphoManager:

- How to install MorphoManager with Enforced Security (imported certificates)
- How to install MorphoManager with Enforced Security (self-generated certificates)
- How to install MorphoManager with On-Demand Security
- How to upgrade MorphoManager to 16.x with Enforced Security (imported certificates) from a version with TLS
- How to upgrade MorphoManager to 16.x with Enforced Security (imported certificates) from a version without TLS
- How to upgrade MorphoManager to 16.x with Enforced Security (self-generated certificates) from a version with TLS
- How to upgrade MorphoManager to 16.x with Enforced Security (self-generated certificates) from a version without TLS
- How to upgrade MorphoManager to 16.x with On-Demand Security from a version with TLS
- How to upgrade MorphoManager to 16.x with On-Demand Security from a version without TLS

MorphoBioToolBox:

- How to configure TLS communication (self-generated certificates)
- How to configure TLS communication (imported certificates)
- How to upgrade a terminal with Enforced Security firmware
- How to add a license on terminals with Enforced Security firmware

Miscellaneous:

- How to unlock the On-demand Security state
- How to enable the Enforced Security state
- Frequently Asked Questions - Enforced Security firmware