digital.security

« IoT Qualified as Secured » :

IoT Solutions Security Labeling

IQS Label Regulations

January 1, 2019

Document version : 1.0

© 2019 digital.security • all rights reserved

DEVELOPMENT HISTORY

Version	Date	Paragraph	Action	Type of development
1.0	01/01/2019	All	Validation	Final version 1.0

© 2019 digital.security • all rights reserved

SUMMARY

© 2019 digital.security • all rights reserved

1. INTRODUCTION

The "IQS: IoT Qualified as Secured" Labeling program (abbreviated to "IQS" in the rest of the document) is offered by digital.security to Internet of Things (IoT) players wishing to have their IoT Solutions verified by an independent third party.

The IQS Label is awarded only to IoT Solutions that have demonstrated that they meet a set of published security requirements; it is a reliable indicator that enables future purchasers of IoT Solutions, private or professional, to be informed objectively about the security of connected objects and related services available on the market.

To this end, the IQS label is delivered by digital.security only to IoT Solutions that have demonstrated that they meet a set of security requirements published in this document, which constitutes the IQS Label's Security Requirements Standards: IoT Qualified as Secured.

These requirements are established regarding the targeted level of labeling:

- « Standard Level » certification for which the evaluation of the IoT Solution is based on :
  - its compliance with each of the security requirements qualified as standard [STD] in this Standards and constituting the state of the art of security measures that are applicable in the field of IoT;
  - its compliance, in addition, with certain safety requirements imposed by any regulatory provisions to which the IoT Solution is subject, specifically identified as such [REG] in this Standards.

- « Advanced Level » certification for which the evaluation of the IoT Solution focuses on:
  - its compliance with all the requirements specified at the "Standard Level"
  - its compliance with each of the security requirements qualified as advanced[AVC] in this Standards, allowing to strengthen the protection of the IoT Solution and to deliver an additional level of confidence deemed necessary by its supplier.

© 2019 digital.security • all rights reserved

2. STRUCTURE OF THE SECURITY REQUIREMENTS STANDARDS

ISSUES :		REQUIREMENTS :		
PED. Data exchanges protection				
	PED.1. Data exchanges encryption			
		PED.1.01. Sensitive data exchanges encryption	☑ STD ☐ AVC	☐ REG
		PED.1.02. Encryption of all data exchanges	☐ STD ☑ AVC	☐ REG
		PED.1.03. Robustness of encryption keys	☑ STD ☐ AVC	☐ REG
	PED.2. Integrity control of exchanges			
		PED.2.01. Integrity control of sensitive data exchanges	☑ STD ☐ AVC	☐ REG
		PED.2.02. Integrity control of all data exchanges	☐ STD ☑ AVC	☐ REG
		PED.2.03. Mutual authentication of data exchanges	☐ STD ☑ AVC	☐ REG
		PED.2.04. No replay of all data exchanges	☑ STD ☐ AVC	☐ REG

© 2019 digital.security • all rights reserved

PST. Protection of technical bases				
	PST.1. Hardening of hardware configurations			
		PST.1.01. Protection of debugging interfaces	☑ STD ☐ AVC	☐ REG
	PST.2. Physical protection of equipment			
		PST.2.01. Detection of box opening	☐ STD ☑ AVC	☐ REG
	PST.3. Hardening of software configurations			
		PST.3.01. Consideration of vulnerabilities published by OWASP	☑ STD ☐ AVC	☐ REG
		PST.3.02. Restriction of services	☑ STD ☐ AVC	☐ REG
	PST.4. Maintaining safe conditions			
		PST.4.01. Correcting device for technical vulnerabilities	☑ STD ☐ AVC	☐ REG
		PST.4.02. Notification of security updates	☑ STD ☐ AVC	☐ REG
		PST.4.03. Checking the reliability of software updates	☑ STD ☐ AVC	☐ REG
		PST.4.04. Protection of secrets contained in software updates	☑ STD ☐ AVC	☐ REG

© 2019 digital.security • all rights reserved

PAD. Data access protection					
	PAD.1. Control and partitioning of data access				
		PAD.1.01.	Systematic control of access to sensitive data	☑ STD ☐ AVC	☐ REG
		PAD.1.02.	Partitioning access to user data	☑ STD ☐ AVC	☐ REG
	PAD.2. Strong authentication				
		PAD.2.01.	Support for soft-tokens or hard-tokens devices	☐ STD ☑ AVC	☐ REG
	PAD.3. Personalization of passwords and secrets				
		PAD.3.01.	Systematic personalization of user passwords	☑ STD ☐ AVC	☐ REG
		PAD.3.02.	Definition of technical passwords and secrets during installation/configuration of the solution	☑ STD ☐ AVC	☐ REG
	PAD.4. Securing of password management procedures				
		PAD.4.01.	Non-disclosure of user attributes	☑ STD ☐ AVC	☐ REG
		PAD.4.02.	Prior identity check for password recovery	☑ STD ☐ AVC	☐ REG
		PAD.4.03.	Prior identity check for changing the password	☑ STD ☐ AVC	☐ REG
	PAD.5. Secure storage of passwords and secrets				
		PAD.5.01.	Storage of passwords in condensate or encrypted form	☑ STD ☐ AVC	☐ REG
		PAD.5.02.	Condensate robustness	☑ STD ☐ AVC	☐ REG
		PAD.5.03.	Storage of secrets in a security element	☐ STD ☑ AVC	☐ REG

© 2019 digital.security • all rights reserved

	PAD.6.	Deleting of user data		
			PAD.6.01. Device for deleting user data	☑ STD ☐ AVC ☐ REG
TRA. Traceability				
	TRA.1.	Logging of events		
			TRA.1.01. Existence of an event log	☑ STD ☐ AVC ☐ REG
			TRA.1.02. Accountability of logged events	☐ STD ☑ AVC ☐ REG
	TRA.2.	Trace protection		
			TRA.2.01. Access control to logged events	☑ STD ☐ AVC ☐ REG

© 2019 digital.security • all rights reserved

3. DESCRIPTION OF SECURITY REQUIREMENTS

3.1. Protection of data exchanges

Issue	PED 1.	Protection of data exchanges ➥Data encryption		
Requirement	PED 1.01	▸ Encryption of exchanges of sensitive data	☑ STD ☐ AVC	☐ REG
Description :	The confidentiality of sensitive exchanged data via the means of communication implemented by the IoT solution must be preserved by an encryption device that complies with the standards described below for each type of encryption mechanism chosen: symmetric or asymmetric. Symmetric encryption algorithms considered as standard should have the following characteristics : - in the case of block cipher algorithms, the block size should be at least of 128 bits and the algorithm must be widely tested in the academic environment (such as AES); - in the case of flow encryption algorithms, it shouldn't have vulnerabilities that would break it in less than 2128 calculations. Asymmetric encryption algorithms considered as standard should have the following characteristics: - the encryption algorithm used should have proof of security. The use of unencrypted communication channels is acceptable provided that all sensitive data passing through them are themselves encrypted.		
Perimeter :	This requirement applies to any exchange of sensitive data using the IoT solution, but not to all data exchanged.		

Issue	PED 1.	Protection of data exchanges ➥Data encryption		
Requirement	PED 1.02	▸ Encryption of exchanges of sensitive data	☐ STD ☑ AVC	☐ REG
Description :	The confidentiality of sensitive exchanged data via the means of communication implemented by the IoT solution must be preserved by an encryption device that complies with the standards described below for each type of encryption mechanism chosen: symmetric or asymmetric. Symmetric encryption algorithms considered as standard should have the following characteristics : - in the case of block cipher algorithms, the block size should be at least of 128 bits and the algorithm must be widely tested in the academic environment (such as AES); - in the case of flow encryption algorithms, it shouldn't have vulnerabilities that would break it in less than 2128 calculations. Asymmetric encryption algorithms considered as standard should have the following characteristics: - the encryption algorithm used should have proof of security. Note: End-to-end encryption systems are strongly recommended as part of this requirement, as they ensure the security of the communication channel regardless of the nature of the data passing through it...		
Perimeter :	This requirement applies to all data exchanges using the IoT solution, regardless of their sensitivity.		

© 2019 digital.security • all rights reserved

Issue	PED 1.	Protection of data exchanges ➥Data encryption		
Requirement	PED 1.03	‣ Robustness of encryption keys	☑ STD ☐ AVC	☐ REG
Description :	The choice of encryption keys must comply with the following criteria: - symmetric encryption keys must have a minimum size of 128 bits; - asymmetric encryption keys must have a minimum size of 3072 bits; - encryption keys must be unique per equipment and per user; - encryption keys must not be generated from public data (serial numbers, hardware addresses, etc.).			
Perimeter :	This requirement applies to any key generation mechanism, whether very temporary (e. g. session-related) or of longer duration.			

Issue	PED 2.	Protection of data exchanges ➥ Integrity control of exchanges		
Requirement	PED 2.01	‣ Integrity control of sensitive data exchanges	☑ STD ☐ AVC	☐ REG
Description :	The integrity of the exchanges of sensitive data carried out within the framework of the IoT solution must be ensured, in particular by one of the following specific mechanisms: - a checksum recognized as reliable, its robustness not having been questioned (SHA256 or equivalent); - a reliable cryptographic checksum (MAC); - an error-correcting code (EEC) system. Note: this requirement only concerns the integrity control of exchanges of sensitive data; it can nevertheless be satisfied by a mechanism providing guarantees of integrity and authenticity such as the use of cryptographic checksums or asymmetric signatures.			
Perimeter :	This requirement applies to any exchange of sensitive data using the IoT solution, but not to all data exchanged.			

Issue	PED 2.	Protection of data exchanges ➥ Integrity control of exchanges		
Requirement	PED 2.02	‣ Integrity control of all data exchanges	☐ STD ☑ AVC	☐ REG
Description :	The integrity of all data exchanges performed as part of the IoT solution must be ensured by at least one of the following specific mechanisms: - a checksum recognized as reliable, its robustness not having been questioned (SHA256 or equivalent); - a reliable cryptographic checksum (MAC); - an error-correcting code (EEC) system. Note: this requirement concerns only the integrity control of data exchanges and not the verification of data authenticity; it can nevertheless be satisfied by a mechanism providing guarantees of integrity and authenticity such as the use of cryptographic checksums or asymmetric signatures.			
Perimeter :	This requirement applies to all data exchanges using the IoT solution, regardless of their sensitivity.			

© 2019 digital.security • all rights reserved

Issue	PED 2.	Protection of data exchanges ➥ Integrity control of exchanges		
Requirement	PED 2.03	▸ Mutual authentication of data exchanges	☐ STD ☑ AVC	☐ REG
Description :	Data exchanges between the various components of the IoT solution must be subject to mutual authentication by means of mechanisms recognised as reliable (their robustness has not been compromised) such as : - a cryptographic checksum; - a digital signature. Note: the vast majority of these authentication mechanisms also ensure the integrity of exchanges.			
Perimeter :	This requirement applies to all types of communication protocols, some of which offer adapted mechanisms (such as TLS for example).			

Issue	PED 2.	Protection of data exchanges ➥ Integrity control of exchanges		
Requirement	PED 2.04	▸ No replay of all data exchanges	☑ STD ☐ AVC	☐ REG
Description :	Data exchanges between the various components of the IoT solution must be protected against replay attacks by means of mechanisms recognized as reliable, such as: - challenge-response authentication; ; - a suitable encryption operation mode (EAX, CCM, GCM, etc.).			
Perimeter :	This requirement applies to all data exchanges using the IoT solution, regardless of their sensitivity.			

© 2019 digital.security • all rights reserved

3.2. Protection of technical bases

Issue	PST 1.	Protection of technical bases ➥ Hardening of hardware configurations		
Requirement	PST 1.01	▸ Protection of debugging interfaces	☑ STD ☐ AVC	☐ REG
Description :	Access to debugging interfaces must be made extremely complex for an unauthorized person (attacker) because of: - disabling hardware debugging features (enabling a fuse); - the implementation of a password control restricting access to debugging interfaces. The non-wiring of hardware debugging interfaces is not enough, but is considered a plus if they are made inaccessible to an attacker.			
Perimeter :	This requirement applies to all electronic components that provide one or more hardware debugging interfaces: JTAG, SWD, etc.			

Issue	PST 2.	Protection of technical bases ➥ Physical protection of equipment		
Requirement	PST 2.01	▸ Detection of housing opening	☐ STD ☑ AVC	☐ REG
Description :	The equipment must have at least one opening detection system that triggers one of the following safety actions: - erasing secrets from storage memories; - sending a silent alert through a communication channel. The equipment may provide a means for authorized persons to disable the mechanism for detecting the opening of the housing (e. g. for inspection or maintenance purposes), subject to prior authentication.			
Perimeter :	This requirement applies to material equipment containing secrets or sensitive data.			

Issue	PST 3.	Protection of technical bases ➥ Hardening of software configurations		
Requirement	PST 3.01	▸ Consideration of vulnerabilities published by OWASP	☑ STD ☐ AVC	☐ REG
Description :	The configuration of web interfaces and services must comply with the best practices defined by the Open Web Application Security Project (OWASP) concerning in particular the consideration of the Top 10 security risks published on its website (www.owasp.org) and currently covering : - injection vulnerabilities (injection of SQL code, commands, etc.); - failed authentication mechanisms; - exposure of sensitive data; - XML external entities (XXE); - failed access control mechanisms; - configuration errors; - code injections by third party sites; - unsecured de-serialization of content; - the use of vulnerable components; - insufficiency/absence of logging.			
Perimeter :	This requirement only applies to web interfaces and mobile or desktop applications based on web interfaces (such as Cordova for example).			

© 2019 digital.security • all rights reserved

Issue	PST 3.	Protection of technical bases ➥ Hardening of software configurations		
Requirement	PST 3.02	▸ Restriction of services	☑ STD ☐ AVC	☐ REG
Description :	Network services exposed by systems and applications must be restricted to only those services necessary for the solution to work properly.			
Perimeter :	This requirement applies to equipment with systems or applications using the IP protocol.			

Issue	PST 4.	Protection of technical bases ➥ Maintaining in secure conditions		
Requirement	PST 4.01	▸ Correcting device for technical vulnerabilities	☑ STD ☐ AVC	☐ REG
Description :	At least one device must be in place to fix published software vulnerabilities, through a software update (including software and firmware). It may be a question of: - an update deployment system (via USB connection, memory card or over-the-air); - the replacement of fallible equipment by equipment with updated software and firmware.			
Perimeter :	This requirement applies to hardware devices, mobile applications based on the underlying application deployment system (iOS, Android, Blackberry, Windows Phone) and web applications hosted in the cloud and supported by the IoT solution provider.			

Issue	PST 4.	Protection of technical bases ➥ Maintaining in secure conditions		
Requirement	PST 4.02	▸ Notification of security updates	☑ STD ☐ AVC	☐ REG
Description :	A notification device must notify the user of the availability of any new security updates when action is required on his part for its implementation within the solution. This device may consist of: - a notification triggered by an application (mobile or web); - the sending of an email or SMS specifying the availability of the update; - a warning light on the equipment. The mechanism(s) chosen must be proportionate and sufficient to the information provided to the user. Thus, the e-mail addresses and telephone numbers used to notify the latter must be regularly checked. The joint use of several mechanisms is strongly recommended.			
Perimeter :	This requirement applies to hardware equipment, mobile applications based on the underlying application deployment system (iOS, Android, Blackberry, Windows Phone).			

© 2019 digital.security • all rights reserved

Issue	PST 4.	Protection of technical bases ➥ Maintaining in secure conditions		
Requirement	PST 4.03	▸ Checking the reliability of software updates	☑ STD ☐ AVC	☐ REG
Description :	A control system must be implemented to verify the reliability of software updates applicable to the IoT solution. It can be based on: - a transmission mechanism including mutual authentication (authentication by client and server certificate for example); - a public key signature mechanism.			
Perimeter :	This requirement applies to all software components of the solution, including those embedded in the equipment, which can be updated by any means, such as : - software and firmware for microcontrollers and System-on-Chip; - mobile and desktop applications; - embedded operating systems.			

Issue	PST 4.	Protection of technical bases ➥ Maintaining in secure conditions		
Requirement	PST 4.04	▸ Protection of secrets contained in software updates	☑ STD ☐ AVC	☐ REG
Description :	The content of software updates must be made intelligible when it includes secrets whose disclosure could compromise the security of the IoT solution. The measures implemented to do this may be based on the use of encryption mechanisms that comply with the PED.1.X requirements of these standards.			
Perimeter :	This requirement applies to all software components of the solution, including those integrated into the equipment, whose updates may contain secrets (encryption keys, algorithms, configuration parameters, etc.).			

© 2019 digital.security • all rights reserved

3.3. Data access protection

Issue	PAD 1.	Data access protection ➥ Control and partitioning of data access		
Requirement	PAD 1.01	▸ Systematic control of access to sensitive data	☑ STD ☐ AVC	☐ REG
Description :	Sensitive data must be systematically protected by an access control device: - consisting of at least one authentication device; - possibly supplemented by an access rights management system. No sensitive data must be publicly accessible.			
Perimeter :	This requirement applies to mobile, web and desktop applications and related web services.			

Issue	PAD 1.	Data access protection ➥ Control and partitioning of data access		
Requirement	PAD 1.02	▸ Partitioning access to user data	☑ STD ☐ AVC	☐ REG
Description :	Access to each user's data must be restricted to the user and the applications that handle it.			
Perimeter :	This requirement applies to mobile, web and desktop applications and related web services.			

Issue	PAD 2.	Data access protection ➥Strong authentication		
Requirement	PAD 2.01	▸ Support for soft-tokens or hard-tokens devices	☐ STD ☑ AVC	☐ REG
Description :	The solution must support the implementation of a strong authentication device, based on tokens generated by a dedicated system, whether specific hardware (e. g. RSA-SecurID) or software (e. g. Google Authenticator). The user must be informed of the existence of this device and be in a position to do so: - enable and disable two-factor authentication; - to manage its tokens (creation, revocation).			
Perimeter :	This requirement applies to mobile, web and desktop applications.			

Issue	PAD 3.	Data access protection ➥ Personalization of passwords and secrets		
Requirement	PAD 3.01	▸ Systematic personalization of user passwords	☑ STD ☐ AVC	☐ REG
Description :	The solution must require the user to define or modify the password(s) to protect the technical bases or applications from the configuration phase. The user must be alerted by the solution to the need to choose strong passwords by respecting the following principles in particular: - the password should be unique to the service it controls access to, if possible. - the password must be complex (not trivial or easy to guess);			
Perimeter :	This requirement applies to all components of the solution using a password, especially if it is preconfigured.			

© 2019 digital.security • all rights reserved

Issue	PAD 3.	Data access protection ➥ Personalization of passwords and secrets		
Requirement	PAD 3.02	▸ Definition of technical passwords and secrets during installation/configuration of the solution	☑ STD ☐ AVC	☐ REG
Description :	The solution must use technical passwords and secrets unique to each device, including: - providing them at the end of the production line; - generating them during the installation or configuration phase; - downloading them from an online service and installing them in the equipment.			
Perimeter :	This requirement applies to all components of the solution using technical passwords or secrets, especially if they are preconfigured.			

Issue	PAD 4.	Data access protection ➥ Securing password management procedures		
Requirement	PAD 4.01	▸ Non-disclosure of user attributes	☑ STD ☐ AVC	☐ REG
Description :	Devices for requesting the recovery or renewal of user passwords (in particular in the event of forgetting them) must not be used to obtain information that could be used for illegal access to the solution, such as: - the user names; - the email address of users.			
Perimeter :	This requirement applies to any interface used to manage a user account.			

Issue	PAD 4.	Data access protection ➥ Securing password management procedures		
Requirement	PAD 4.02	▸ Prior identity check for password recovery	☑ STD ☐ AVC	☐ REG
Description :	Devices for retrieving or renewing user passwords (in particular in the event of forgetting them) must verify the identity of the users making this request by means such as: - sending an SMS message containing a verification code (if the user's telephone number has been previously registered and stored by the service provider); - sending an email containing a one-time use link to renew the password (if the user's email address has been previously registered and stored by the service provider); - check of the answer to a secret question previously defined by the user. If the user's identity cannot be verified, a password reset mechanism by local access to the equipment may be implemented, provided that it results in the deletion of sensitive data.			
Perimeter :	This requirement applies to any interface used to manage a user account.			

© 2019 digital.security • all rights reserved

Issue	PAD 4.	Data access protection ➥ Securing password management procedures		
Requirement	PAD 4.03	▸ Prior identity check for changing the password	☑ STD ☐ AVC	☐ REG
Description :	Password change devices must verify the identity of users requesting this operation by one of the following means: - entry of the current password by the user and verification; - sending an SMS message containing a verification code (if the user's telephone number has been previously registered and stored).			
Perimeter :	This requirement applies to any interface used to manage a user account.			

Issue	PAD 5.	Data access protection ➥ Secure storage of passwords and secrets		
Requirement	PAD 5.01	▸ Storage of passwords in condensate or encrypted form	☑ STD ☐ AVC	☐ REG
Description :	Since confidentiality and the legitimate use of passwords must be preserved, the following precautions must be applied. In the event that an application only needs to verify the knowledge of a password, the application must store only a condensate of the password, resulting from a condensation (hashage) operation of the password and complying with requirement PAD.5.02 of these guidelines. In the case where an application needs to reuse a password and only in this case (mainly for authentication operations), it can be stored in an encrypted form, provided that the provisions required by the PED.1.X requirements of this repository are met. The reversibility of the encryption then allows the password to be retrieved, provided that the appropriate key is held, while ensuring its confidentiality.			
Perimeter :	This requirement applies to any application storing a password or its condensate on any medium (database, file system, memory...), including but not limited to : - mobile applications; - firmware; - software deployed on equipment that can be physically compromised			

© 2019 digital.security • all rights reserved

Issue	PAD 5.	Data access protection ➥ Secure storage of passwords and secrets		
Requirement	PAD 5.02	▸ Condensate robustness	☑ STD ☐ AVC	☐ REG
Description :	The password condensate generation mechanisms must have the following characteristics: - the minimum size of the generated condensates is 256 bits; - the best known attack to find collisions must require about 2h/2 condensate calculations, where h denotes the bit size of the condensate ; - the use of a grain of salt is mandatory, in order not to reveal information in the event of compromise; - the number of iterations must be in accordance with the state of the art in the case of iterative condensate calculation (e.g. bcrypt, scrypt or PBKDF2). Note: hash algorithms such as SHA-256 or SHA-512 comply with this requirement.			
Perimeter :	This requirement applies to any software that performs a condensate calculation on sensitive data.			

Issue	PAD 5.	Data access protection ➥ Secure storage of passwords and secrets		
Requirement	PAD 5.03	▸ Storage of passwords in a security element	☐ STD ☑ AVC	☐ REG
Description :	In order to preserve the security of cryptographic functions, the secrets used in the equipment must be buried within a recognized security element (HSM, Hardware Security Module) (Common Criteria, FIPS 140).			
Perimeter :	This requirement applies to all IoT solution equipment using cryptographic functions.			

Issue	PAD 6.	Data access protection ➥ Deleting user data		
Requirement	PAD 6.01	▸ Device for deleting user data	☑ STD ☐ AVC	☐ REG
Description :	A feature for permanently deleting user data must allow it to be deleted without rendering the application or equipment that used it inoperative.			
Perimeter :	This requirement applies to all equipment and applications storing user data.			

© 2019 digital.security • all rights reserved

3.4. Traceability

Issue	TRA 1.	Traceability ➥ Logging of events		
Requirement	TRA 1.01	▸ Existence of an event log	☑ STD ☐ AVC	☐ REG
Description :	An event log must be continuously supplied with at least the computer traces required to: - to know the nature of the operations carried out within the functional framework of the solution; - to date these operations. Under no circumstances should these traces mention the content of secrets, passwords, or any other information whose confidentiality must be preserved.			
Perimeter :	This requirement applies to the equipment and applications that make up the IoT solution.			

Issue	TRA 1.	Traceability ➥ Logging of events		
Requirement	TRA 1.02	▸ Accountability of logged events	☐ STD ☑ AVC	☐ REG
Description :	The computer traces generated by the solution must make it possible to attribute the logged events (operations or attempted operations) to their origin (physical persons, technical equipment, application, etc.).			
Perimeter :	This requirement applies to the equipment and applications that make up the IoT solution.			

Issue	TRA 2.	Traceability ➥Trace protection		
Requirement	TRA 2.01	▸ Access control to logged events	☑ STD ☐ AVC	☐ REG
Description :	Computer traces recorded in event logs must be protected by an access control device.			
Perimeter :	This requirement applies to all event logs supplied by the various components of the solution.			

© 2019 digital.security • all rights reserved

4. GLOSSARY

Sensitive data :	The data considered as "sensitive" for the purposes of these requirements are personal data, data classified as sensitive by the GDPR, all data subject to sectoral regulation (health data, bank data, financial data, etc.) and remote monitoring data from the IoT solution. The secrets used in the IoT solution are also considered "sensitive" data.
Secrets :	Secrets include certificates and keys used in a cryptographic context.
Technical passwords :	Any password used by the IoT solution that is not intended for its users is considered a technical password.

© 2019 digital.security • all rights reserved