General Intelligence and
Security Service
*Ministry of the Interior and
Kingdom Relations*

# Deployment Advisory BSPA of datAshur PRO models

Date 25 November 2025

Colophon


| | | |
|---|---|---|
| Our reference number | : | 9fd68dc2-or1-1.0 |
| | : | T +31 (0)79 320 50 50 |
| | : | F +31 (0)70 320 07 33 |
| | : | P.O. Box 20010 2500 EA The Hague The Netherlands |
| Copy number | : | |
| Author(s) | : | NLNCSA |
| Number of enclosures | : | 0 |

# 1 Table of contents

## 2 Statement of Conformity

*Hereby is stated that evaluation has demonstrated that the product:*

**datAshur PRO+A and PRO+C model**
*from*
iStorage Ltd.

*is in conformity to:*
BSPA Security Evaluation Target for iStorage datAshur PRO+ C, Version 1.0, 19.11.2024 [1]

as demonstrated by:
Bureau Veritas Cybersecurity (formerly known as Secura), located in Amsterdam, Netherlands

*Applying:*
NL Scheme for Baseline Product Assessment, 07.08.2020

This Statement of Conformity (SoC) is part of the Deployment Advisory (DA) and is only valid if the recommendations and obligations in the DA are being followed.

The DA determines the conformity of the product with its Security Evaluation Target (SET) and the effectiveness of the security features offered by the product.

This SoC relates only to a specific version of a product. If the product is changed, this SoC is not applicable anymore. Newer versions of the products need to undergo the Baseline Security Product Assessment (BSPA) process anew to obtain a new Statement of Conformity.

Issuance of a SoC is no guarantee that the product is free from security vulnerabilities. Also, a SoC is not an endorsement of the IT product by NLNCSA and no warranty of the IT product by NLNCSA or by any other organisation, is either expressed or implied.

Issue date: 25 November 2025

Kind regards,

The National Security Authority of the Netherlands,
The minister of the Interior and Kingdom Relations of the Netherlands,
p.p.,

F. van Tongeren
Head of the National Communications Security Agency of the
General Intelligence and Security Service

[1] The original Security Evaluation Target document was created for the PRO+C model only. The PRO+A model was added to the scope later on. A comparative analysis was conducted to ensure that the two models presented identical security functions.

# 3 Introduction

## 3.1 Scope

| | |
|---|---|
| Product name | datAshur PRO+A and PRO+C model<br>(referred to as "datAshur PRO models" in the rest of this document) |
| Product version | Firmware version: 2.00.0 |
| Product category | 07 – Hardware and embedded software |
| Evaluation criteria and version | BSPA_D_01_NL_Scheme_for_Baseline_Product_Assessment<br>07.08.2020 |
| Vendor | iStorage Ltd. |
| Overseer | General Intelligence and Security Service<br>Ministry of the Interior and Kingdom Relations<br>Netherlands National Communications Security Agency<br>(NLNCSA)<br>P.O. Box 20010<br>2500 EA The Hague<br>The Netherlands |
| Evaluation facility | Bureau Veritas Cybersecurity Europe B.V.<br>Vestdijk 59,<br>5611 CA EINDHOVEN<br>The Netherlands<br><br>Herikerbergweg 15 (Apollo Building, 3rd floor),<br>1101 CN AMSTERDAM,<br>The Netherlands |

The goal of this Deployment Advisory is to inform consumers on:

- the specific use case for which the product has been tested,
- the manner in which the product has been tested and the limitations of this test process,
- the level of security provided by the product when used according to the prescribed use case,
- the residual risks of the product when used according to the prescribed use case.

This Deployment Advisory also gives guidance to users on how to securely use and configure the product.

### 3.2 Disclaimer

This advisory and associated Statement of Conformity applies only to the specific version of the product in its evaluated configuration (see section 4.1).

The Statement of Conformity is not a guarantee that the product is free from security vulnerabilities. Neither is it a guarantee that the product protects against adversaries with a high attack potential like (for example) intelligence organisations, organised (cyber-) crime organisations, terrorist organisations and capable security researchers.

Exploitable vulnerabilities may be discovered after issuance of the Statement of Conformity. The organisation or individual using the product should check regularly if security vulnerabilities have been discovered and whether updates are provided by the vendor. Installation of updates must be compliant with the risk management policy and risk appetite of the organisation or individual using the product. Updates should only be installed if there is sufficient trust or assurance that they improve the security of the product.

This advisory is supplementary to the instructions and documentation of the vendor. It is still necessary to consult these before installing and using the product.

All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

### 3.3 Certification scheme

The Dutch *Baseline Security Product Assessment* evaluates the security features of hardware and software security products for use in the "internal but unclassified" domain. The main goals of the evaluation are:

- Establishing that the product conforms to the security specification in the Security Evaluation Target,
- Establishing the effectiveness of the security features offered by the product,
- Establishing that the product has a limited impact on the security of the host system.

A positive Statement of Compliance and Deployment Advisory enables a government organization to make a better substantiated decision if these products are applicable in an ICT-infrastructure at the BBN1 or BBN2[2] level of the Government Baseline for Information Security (Baseline Informatiebeveiliging Overheid, BIO, Versie 1).

BSPA is intended for "internal but unclassified" information where there is no need for the product to be resistant against adversaries with a high attack potential[3], like intelligence organisations, organised (cyber-) crime organisations, terrorist organisations and capable security researchers

Documentation and procedures of the Baseline Security Product Assessment scheme are available at the following Internet site: www.aivd.nl search for "BSPA".

### 3.4 Copyright information



### 3.5 Contact information

All correspondence regarding this Deployment Advisory should be addressed to:

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations
NLNCSA
P.O. Box 20010
2500 EA The Hague
The Netherlands
bspa@nlncsa.nl

[2] To attain the BIO BBN2 level, a government organization will at least need:
- additional measures for detection of cyber-attacks by adversaries with high attack potential (BIO 12.4.1.3 and BIO 13.1.2.1),
- an additional and deeper assessment of the cryptography of the product (BIO 8.3.1.2 and BIO 13.1.2.3).

[3] BSPA is not designed and intended for the BIO BBN3 level (and higher classifications and threat levels). For the assessment security products for the BIO BBN3 level a national evaluation scheme exists, with different characteristics.

# 4 Product overview

## 4.1 Product version

This Deployment Advisory is limited to the following versions of the datAshur PRO models:

- PRO+A model
  Firmware version: 2.00.0
- PRO+C model
  Firmware version: 2.00.0

## 4.2 Product identification

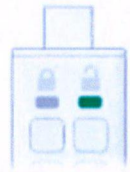
For both models, the product version can be identified in the following manner:

- **Model identification**
  Depending on the model (either PRO+A or PRO+C), and the storage capacity of the drive, there will be slight deviations in the model labelling. Two valid examples are stated below:
  - An example of a PRO+A model with a storage capacity of 64GB:
    IS-FL-DA3**A**-256-**64**
  - An example of a PRO+C model with a storage capacity of 32GB:
    IS-FL-DA3**C**-256-**32**

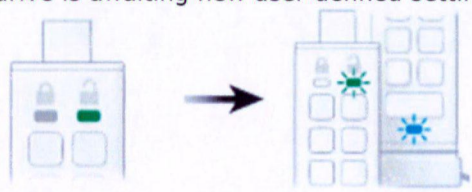
  An illustrative visual is added to this document:


*Figure 1: Illustrative visual of model labelling*

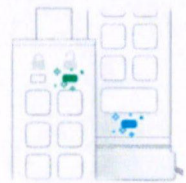
- **Determine the device Version** [4]
  - Determine the device Version Number in **User mode**
    - Unlock the datAshur PRO+C with your User PIN.
      GREEN LED will be solid indicating successful User PIN entry.



    - Press the KEY button THREE times (triple-click).
      Solid GREEN LED switches to blinking GREEN and BLUE LEDs indicating the drive is awaiting new user defined settings.

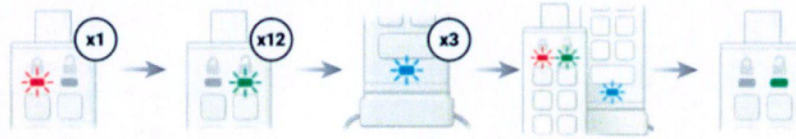


    - Press button number 8 followed by the number 6 button (86) GREEN and BLUE LEDs will continue to blink.



    - Press the KEY button once and then the following happens;
      - a. All LEDs (RED, GREEN & BLUE) will flash together once.
      - b. RED LED blinks indicating the integral part of the firmware revision number.
      - c. GREEN LED blinks indicating the fractional part.
      - d. BLUE LED blinks indicating the last digit of the firmware revision number.
      - e. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
      - f. RED, GREEN & BLUE LEDs switch to a solid GREEN LED.

      For example, if the revision number is '1.12.3', the RED LED will blink once (1) and the GREEN LED will blink twelve (12) times and the BLUE LED will blink three (3) times. Once the sequence has ended the RED, GREEN & BLUE LEDs will blink together once and then to solid GREEN.

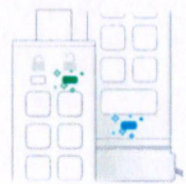



[4] Due to the fact that there are small deviations in the light indication for User mode and Admin mode, both modes are being described in a separate manner. The device version identification steps are derived directly from the official DataShur PRO+C user manual, available at: https://istorage-uk.com/wp-content/uploads/2023/05/datAshur-PROC_User-Manual_Multilingual_v1.0.pdf

- Determine the device Version Number in **Admin mode**
  - Unlock the datAshur PRO+C with your Admin PIN
    GREEN LED will flicker indicating successful Admin PIN entry.

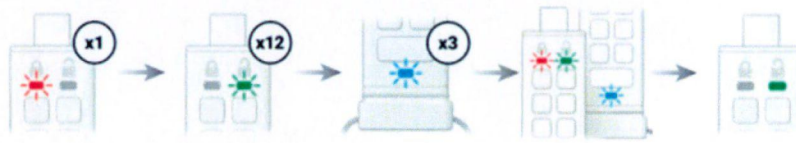
  - Press the KEY button THREE times (triple-click)
    GREEN and BLUE LEDs flicker together.

  - Press button number 8 followed by the number 6 button (86)
    GREEN and BLUE LEDs continue to flicker together.



  - Press the KEY button once and then the following happens;
    - a. All LEDs (RED, GREEN & BLUE) will flash together once.
    - b. RED LED blinks indicating the integral part of the firmware revision number.
    - c. GREEN LED blinks indicating the fractional part.
    - d. BLUE LED blinks indicating the last digit of the firmware revision number.
    - e. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
    - f. RED, GREEN & BLUE LEDs switch to a solid GREEN LED.

    For example, if the revision number is '1.12.3', the RED LED will blink once (1) and the GREEN LED will blink twelve (12) times and the BLUE LED will blink three (3) times. Once the sequence has ended the RED, GREEN & BLUE LEDs will blink together once and then to solid GREEN.



### 4.3 Assumptions

The following assumptions are considered relevant for the environment:

- **AS.PIN_Strength.** Authentication strength of Admin/User is determined by PIN that is between 8-15 digits long.
- **AS.PC_secure.** The device that the USB is plugged into is sufficiently secure and does not contain malware.
- **AS.USER.Secure.** The user is trustworthy.
- **AS.Setup_completed.** The first time use steps from the datAshur PRO models manual are expected to be followed to configure the User, Admin PIN and lockout mechanism.

### 4.4 Security functions

The following security functions of the datAshur PRO models have been verified by a time-boxed and lightweight pentest:

- **SF.Encryption**. The AES scheme encryption protects stored data on the device.
- **SF.Key_generation_wrapping.** Reliable generation and wrapping of data encryption key.
- **SF.Brute_force_resistance.** Reliable protection against all forms of brute force attacks.
- **SF.USB_lock.** Reliable locking of the devices after a time of inactivity, when the device will be unplugged from the host computer or when power to the USB port is turned off.
- **SF.USB_sanitization.** Reliable sanitization after a 'delete all data' in Admin mode Drive Reset.
- **SF.Write_protect.** Ensures reliable, restrictive data access when the device is set to write-protect mode.
- **SF.Best_effort_physical_security.** The epoxy encased board protects against attackers with physical access to the device's board and security controller.
- **SF.Best_effort_controller_access_protection.** Best-effort protection against attackers with physical access to the security controller.
- **SF.No_use_traces.** Hardware wear resistant keypad. It is not visible which PIN has been used often.
- **SF.Tamper_evidence.** Hardware tamper-evident. The user finds evidence of tampering with the hardware.
- **SF.Delete_Data**. If an Admin enters an incorrect Admin PIN ten (10) consecutive times, then both the User and Admin PINs, the encryption key and all data will be deleted.

## 4.5 Product description

The datAshur PRO models are encrypted storage devices that provide a secure way to store and transfer data. User authentication is performed through the onboard keypad. User data is protected by hardware-based 256-bit AES encryption to secure sensitive information in the event that the drive is lost or stolen.

### *4.5.1 Typical usage*

The user sets up an administrative PIN, and a standard User PIN during the first-time use. By entering the correct PIN, the user can view the protected storage media from the host, and write the data to, or read data from, the media. Only the user knows the PIN, therefore having the exclusive privilege to access the protected storage media. The drive goes to admin mode when the user executes the admin mode entering procedures using a valid administrative PIN. In the admin mode, the user can set up unattended auto lock time, standard User PIN policy, set the drive as write protect, etc. These administrative features offer different access levels thus improving the drive overall security.

When either the Admin or User PIN are incorrectly entered ten (10) consecutive times, the system activates a brute force hacking detection mechanism. In such a scenario, the PIN will be automatically deleted. If a User PIN is deleted, all data will remain on the datAshur PRO device and can only be accessed by the admin entering the correct Admin PIN. If the admin enters an incorrect PIN ten consecutive times, then both the User and Admin PINs, the encryption key and all data will be deleted.

## 4.6 Product category

The product belongs to the following BSPA category:
07 – Hardware and embedded software

## 4.7 Product configuration

No configuration options were altered unless it was necessary to test one of the security features in scope of the assessment.

# 5 Tested security features for the product

The security features that are part of the BSPA for the datAshur PRO models are listed in Table 1:

| Security features part of the datAshur PRO models | Security feature part of BSPA scope | Additional information |
|---|---|---|
| **SF.Encryption** | Yes | One of the security functions (SF.Tamper_evidence) reached a fail verdict as of result of the BSPA.<br><br>The NLNCSA and the test laboratory (Bureau Veritas Cybersecurity) reached a consensus that if the Deployment Advisory is strictly followed, the BSPA resulted in a pass.<br><br>The formal response issued by iStorage was as follows:<br><br>The datAshur Pro +A/+C samples were designed and built to meet FIPS 140-3 Level 3 physical security requirements. The drives were awarded a FIPS 140-3 Level 3 certificate in January 2025 and therefore passed the physical security tests.<br><br>In addition to this, iStorage proposed design refinements to enhance the existing models. See section 7.4 for more information. |
| **SF.Key_generation_wrapping** | Yes | |
| **SF.Brute_force_resistance** | Yes | |
| **SF.USB_lock** | Yes | |
| **SF.USB_sanitation** | Yes | |
| **SF.Write_protect** | Yes | |
| **SF.Best_effort_physical_security** | Yes | |
| **SF.Best_effort_controller_access_protection** | Yes | |
| **SF.No_use_traces** | Yes | |
| **SF.Tamper_evidence** | Yes | |
| **SF.Delete_Data** | Yes | |

Table 1. datAshur PRO models security features that have been part of this BSPA.

# 6 Scope and limitations of the evaluation

## 6.1 Evaluation facility

The security test has been performed by:
Bureau Veritas Cybersecurity Europe B.V.
Vestdijk 59,
5611 CA EINDHOVEN
The Netherlands

Herikerbergweg 15 (Apollo Building, 3rd floor),
1101 CN AMSTERDAM,
The Netherlands

https://cybersecurity.bureauveritas.com

## 6.2 Test duration and time used

The evaluation process has been performed in the period of 7th of August to 11th of September 2025.

## 6.3 Evaluation process and scope

The following time-boxed evaluation process was employed:

- Security Evaluation Target analysis.
- Product installation and deployment analysis.
- Compliance analysis by documentation review.
- Compliance analysis by product testing.
- Vulnerability analysis.
- Usability analysis.

## 6.4 Product procurement, installation and configuration for evaluation

The datAshur PRO models are available for purchase through iStorage's official web shop: https://istorage-uk.com

iStorage supplied the test devices required for this BSPA.

# 7 Instructions and recommendations for users

The datAshur PRO models distinguishes between a User PIN and an Admin PIN.
The Admin PIN is a useful feature for corporate deployment, by allowing:

- Recovering data from a drive and configuring a new User PIN in the event an employee has forgotten their PIN.
- Retrieving data from a drive if an employee leaves the company.
- Setting admin defined user policies.
- The Admin PIN can be used to override all user settings

As users can potentially assume both roles, this Deployment Advisory does not provide separate recommendations for administrators. The user recommendations are outlined in the subsequent sections.

## 7.1 Procurement of the product

Users are advised to only use the product when it has been procured, provisioned, or distributed by a trusted source. Disregarding this recommendation will expose the device to the risk of compromise if it has been handled by any untrusted party during any stage of its lifecycle, from initial production through distribution to end-user.

Please note that this recommendation should always be performed in conjunction with the 'Visual inspection' recommendation that is stated within section 7.4.

iStorage was asked to provide rebuttal on the matter, which was as follows:

> In relation to "Trusted Device Acquisition and Use," we propose supplying both the datAshur PRO+A and datAshur PRO+C models with the suffix **"-BL"** appended to their part numbers. This convention would be used exclusively for customers in the Netherlands and has already been applied for several years to all drives **[REDACTED]** under the datAshur PRO line. In addition, the packaging for both products includes anti-tamper labels (see attached images).

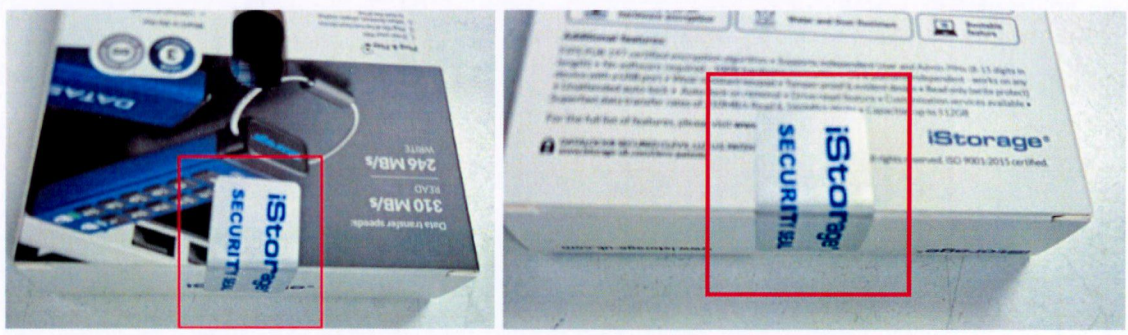



*Figure 2: Additional evidence provided by iStorage regarding anti-tamper labels*

Original packaging verification was not feasible throughout the assessment due to the fact that procured devices were not shipped in their original packaging. However, the provided response from iStorage demonstrates considerable credibility.

## 7.2 Installation of the product

No installation recommendations were identified throughout the assessment.

## 7.3 Configuration of the product

In a corporate environment, it is recommended to set an Admin PIN prior to device distribution. This approach enables organizational access to the device in scenarios such as user PIN recovery, implementing time lockout settings, or facilitating device ownership transitions without necessitating complete data erasure.

iStorage supplemented the initial recommendation with additional information:

> With regards to "Set the Admin PIN", there is no reason why the Administrator should ever disclose the Admin PIN to the User. The Admin PIN is normally configured before a drive is given to the User.

## 7.4 Security risks and countermeasures

Recommendations for secure usage:

- Users are advised to carefully inspect the device for signs of physical tampering or unauthorized modifications, as attackers can disassemble and reassemble the devices with minimal visible evidence. Tamper detection measures, such as holographic security seals, can be proactively added by users to verify device integrity.

  iStorage was asked to provide rebuttal on the matter, which was as follows:

> If a "visual" tamper evident is needed, one option is to modify the nameplate on the endcap. The existing nameplate is soft plastic, but they can change it to a hard plastic with "legs" and insert it into the endcap. Please see below.

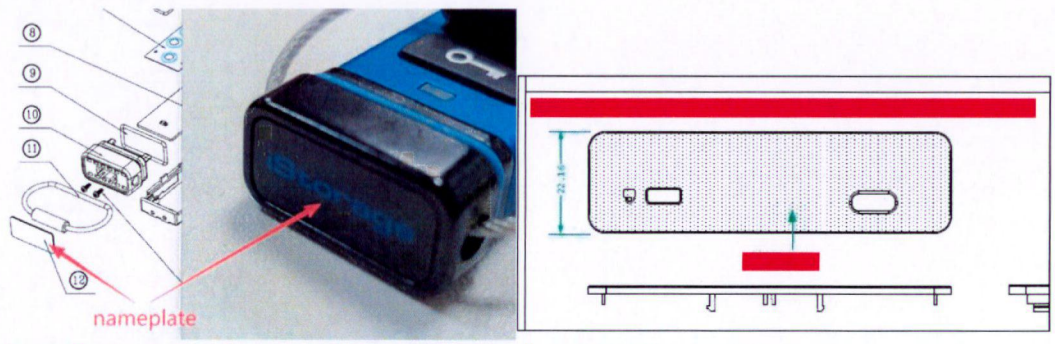



*Figure 3: Conceptual proposal for product enhancement*

While Bureau Veritas Cybersecurity supports the intent of iStorage to implement design refinements, the proposed enhancements do not impact the initial recommendation. This remains unaltered.

- Ensure that no intermediate devices with power retention capabilities are positioned between the device and the host system. Specifically, avoid using USB hubs with external power sources. If the device is supplied power through an intermediate hub, it fails to lock immediately upon disconnection from the host system, which allows an attacker a short period of time in which they can plug the device into their own computer without the need of re-entering a PIN. An example could be an employee leaving the device in the USB hub at their desk to go to a meeting. Then another employee may connect the hub to their laptop and have unrestricted access to the contents of the device.

  iStorage was asked to provide rebuttal on the matter, which was as follows:

> *Powered hubs can sometimes allow device access after detachment from the host, which is expected USB behaviour. Users are responsible for keeping the drive in their possession while drive is unlocked.*

After review of the submitted rebuttal, the initial recommendation remains unchanged. The original risk continues to be valid and applicable.

### *7.4.1 Publicly known vulnerabilities*

No exploitable publicly known vulnerabilities were identified for the datAshur PRO models throughout the evaluation.

### *7.4.2 Independent vulnerability analysis*

An independent vulnerability analysis on the datAshur PRO models was conducted during the evaluation. The following activities were in the scope of the investigation:

- **Attack scenario 1: Attacking the USB controller firmware**
  To test whether vulnerabilities could be discovered within the USB controller firmware.
- **Attack scenario 2: Remnants reconstruction**
  To determine whether remnants of data could be left on the device after a factory reset or data deletion operation.
- **Attack scenario 3: Attacking the security chip**
  To assess potential security weaknesses for the security chip, multiple attack scenarios were evaluated. These scenarios included attempts to activate the bootloader, observe the key exchange mechanism, and attempts to interact with the device through a debug interface.
- **Attack scenario 4: Chip-off forensics**
  A forensic examination was conducted through chip-off analysis of the storage chip to assess whether stored data is stored securely.
- **Attack scenario 5: One key ghost**
  Utilizing a configuration file, an attempt was made to rewrite and potentially manipulate the content of the storage chip.

Bureau Veritas Cybersecurity identified two areas of potential concern when testing scenarios 3 and 5. Due to the time limitations of the BSPA, these points were not subjected to further detailed investigation. A request was made to iStorage to provide further insights into these observations. The response was shared with both Bureau Veritas Cybersecurity and the NLNCSA.

Given the complexity of the observations, and considering that the performed tests did not result in new user-related recommendations, a decision was made to omit further elaboration from this Deployment Advisory.

### 7.5 Summary of recommendations

The following recommendations on actions are given to users of the datAshur PRO models:

**Procurement**

- Users are advised to only use the product when it has been procured, provisioned, or distributed by a trusted source. See section 7.1 for more information.

**Configuration**

- In a corporate environment, it is recommended to set an Admin PIN prior to device distribution. See section 7.3 for more information.

**Secure use**

- Users are advised to carefully inspect the device for signs of physical tampering or unauthorized modifications. See section 7.4 for more information.
- Ensure that no intermediate devices with power retention capabilities are positioned between the device and the host system. See section 7.4 for more information.