DATA SECURITY INFORMATION
COMMON CRITERIA ISO-IEC15408 / IEEE 2600-1
TASKALFA 3252Ci / 2552Ci w. HD-12

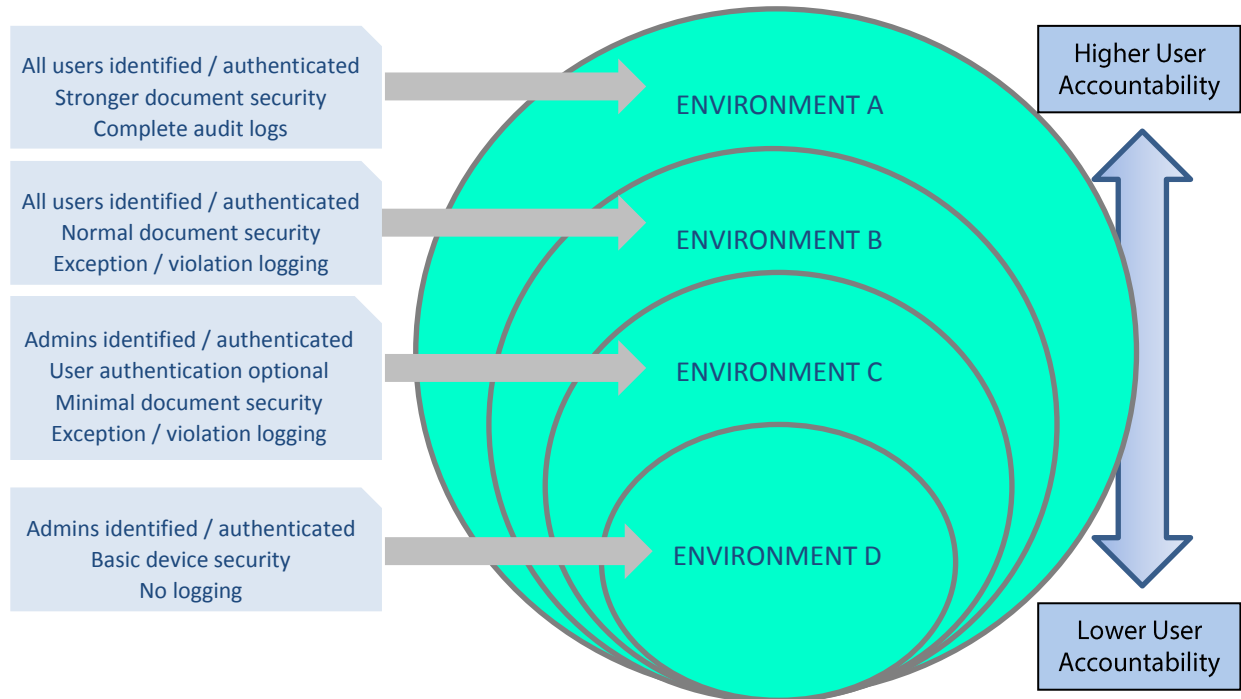**KYOCERA**
Document Solutions

Contents

1. IEEE 2600-1 Operational environments

1.1. Graphical overview

All users identified / authenticated
Stronger document security
Complete audit logs

All users identified / authenticated
Normal document security
Exception / violation logging

Admins identified / authenticated
User authentication optional
Minimal document security
Exception / violation logging

Admins identified / authenticated
Basic device security
No logging

ENVIRONMENT A

ENVIRONMENT B

ENVIRONMENT C

ENVIRONMENT D

Higher User Accountability

Lower User Accountability

1.2. IEEE 2600 operational environments are based on market segments

- A. For use with highly proprietary or legally regulated documents
- B. For general enterprise use
- C. For public-facing use
- D. For small office / home office use

The security requirements for environment are hierarchical:

- A is a superset of B
- B is a superset of C
- C is a superset of D

The main difference between environments is the level of accountability for individual user actions.

1.3. The two ways to evaluate products using Common Criteria

A) Without a Protection Profile:

- o A manufacturer writes a Security Target document that describes the security claims of their product.

- o Evaluation is based solely on the manufacturer's claims, not on a standard: it certifies only that the product performs what the manufacturer claims.

B) With a Protection Profile:

- o Somebody writes a Protection Profile document that describes the security requirements for a class of products.

- o Manufacturers write Security Target documents that make security claims conforming to those requirements.

- o Evaluation ensures that the product performs as the manufacturer claims, **and that the <u>manufacturer's claims fulfill those requirements</u>**.

1.4. IEEE 2600 – series Protection Profiles

The working group has also developed four Common Criteria Protection Profiles,one for each of the typical operating environments that are defined in IEEE 2600:

- IEEE 2600.1 - 2009 Standard Protection Profile for Hardcopy Devices in Operational Environment A (published and certified in 2009)

- IEEE 2600.2 - 2009 Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600 - 2008 Operational Environment B (published in 2009, certified in 2010)

- IEEE 2600.3 - 2009 Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600 - 2008 Operational Environment C (published in 2010 , not certified)

- IEEE 2600.4 - 2010 Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600 - 2008 Operational Environment D (published in 2010, not certified)

2. TASKalfa 3252ci - TASKalfa 2552ci

Configuration: HD-12, Data Security Kit (E), FAX System 12; Certification No. : C0540

2.1. IEEE 2600 certification level

The Kyocera TASKalfa devices described in this document have been certified according to **IEEE 2600.1 - 2009** Standard Protection Profile for Hardcopy Devices in Operational **Environment A.** Version of Common Criteria: 3.1 Release4, Conformance Claim : EAL3 Augmented with ALC_FLR.2

2.2. PRODUCT DESCRIPTION

Description of Target of Evaluation (TOE)

The TOE is a Multi-Function Printer, which has Copy, Scan, Print, FAX and Document Box functionality.
This TOE provides security functionalities, which conform to IEEE Std 2600.1™-2009 that is a protection profile for Hardcopy devices, for a purpose of preventing unauthorized disclosure and alteration of user document data.

2.3. Target of Evaluation (TOE) security functionality

This TOE provides the following security functionalities.

- User Authentication: The functionality that performs user identification and authentication.

- Job Authorization: The functionality that restricts the available functions of a user.

- Document Access Control: The functionality that restricts access to user document data to authorized users only.

- Hard Disk Data Encryption: The functionality that encrypts data stored in hard disk drive.

- Data Overwrite: The functionality that overwrites data stored in a product, and disables the data to be re-used.

- Audit Logs: The functionality that records audit logs relevant to the security functionalities.

- Security Management: The functionality that restricts management of the security functionalities to authorized users only.

- Self-Test: The functionality that verifies the integrity of executable codes of security functionality and setting data.

- Network Data Protection: The functionality that encrypts communication data, and prevents unauthorized transmission to an internal network via external interfaces such as public lines.

2.4. Security functional requirements

This TOE implements the following security functional requirements.

Security audit	Non-repudiation of origin/receipt	Cryptographic functionality	Access control
Data authentication	Export data protection	Information flow control	Import data protection
Internal transfer data protection	Residual information protection	Rollback	Stored data integrity
Transfer data confidentiality	Transfer data integrity	Identification and authentication	Security management
Privacy Control	Security functionality protection	Resource utilisation management	TOE access control
Trusted path/channels			

3.   Disclaimer & Contact

KYOCERA Document Solutions does not warrant that any specifications mentioned will be error-free. Specifications are subject to change without notice. Where application information is given, it is only advisory and does not form part of the specification. Information is correct at time of going to press. All other brand and product names may be registered trademarks or trademarks of their respective holders and are hereby acknowledged.

KYOCERA Document Solutions Europe B.V.

Branch Office Germany

Otto-Hahn-Strasse 12 * D-40670 Meerbusch * Germany

Contact:

Hans Gerd Schmidt, Software Product Manager / GSD

info@deu.kyocera.com

All information as of July 17th, 2017