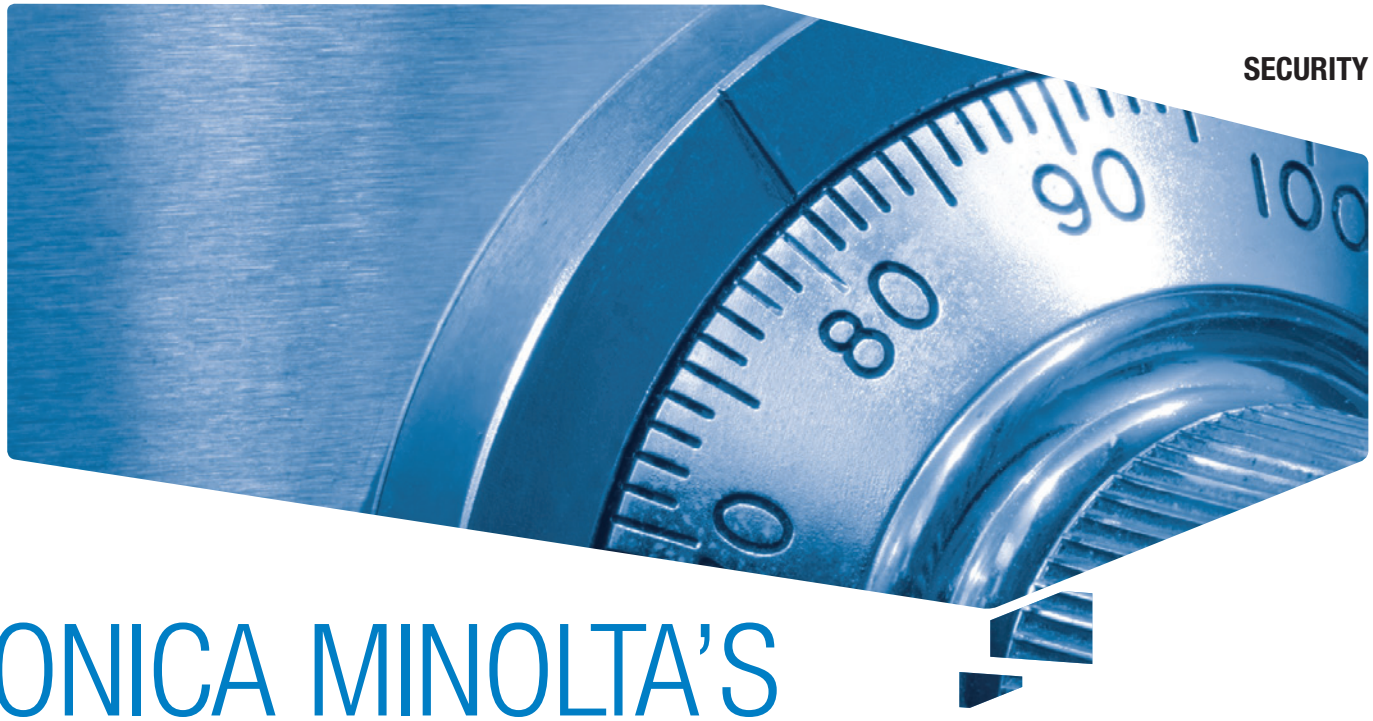
KONICA MINOLTA

SECURITY

Konica Minolta's industry-leading security standards

In the digital age, we have seen global communications undergo unprecedented growth – and the potential for damaging security breaches has soared in parallel. In any business environment, the day-to-day use of copying, print, scan and fax systems, as the elementary components of work processes and workflows, makes MFPs (multifunctional peripherals) indispensable at many levels. As a consequence, it is paramount that these devices are given the protection needed to withstand on-going threats to security.



KONICA MINOLTA'S SECURITY STANDARDS

Konica Minolta's comprehensive range of standard security features and options form a powerful source on which professional solutions can be based: solutions to both detect and prevent security violations, and avoid knock-on financial and/or reputational damage at corporate as well as private individual level.
Konica Minolta has pioneered this field and remains the industry's leader.

Generally MFPs offer a huge range of combined and single functions and choices. Therefore they represent a similarly wide range of potential security loopholes. The scope of MFP security can be grouped into three main sections:

- **Access control/Access security**
- **Data security/Document security**
- **Network security**

Konica Minolta security functions at a glance

Access control	Copy/print accounting
	Function restriction
	Secure printing (lock job)
	User box password protection
	User authentication (ID + password)
	Finger vein scanner
	IC card reader
	Event log
Data security	Data encryption (hard disc)
	Hard disc data overwrite
	Hard disc password protection
	Data auto deletion
Network security	IP filtering
	Port and protocol access control
	SSL/TLS encryption (HTTPS)
	IP sec support
	S/MIME
	802.1x support
Scanning security	User authentication
	POP before SMTP
	SMTP authentication (SASL)
	Manual destination blocking
Others	Service mode protection
	Admin mode protection
	Data capturing
	Unauthorised access lock
	Copy protection via watermark
	Encrypted PDF
	PDF signature
	PDF encryption via digital ID
	Copy guard/Password copy

COMMON CRITERIA AND ISO 15408 EAL3

Konica Minolta devices are certified almost without exception in accordance with the Common Criteria/ISO 15408 EAL3 standard.

These are the only internationally recognised standards for IT security testing for digital office products. Printers, copiers and software compliant with ISO 15408 EAL3 certification have all passed a strict security evaluation and are able to satisfy and deliver the kind of security levels that a prudent business operation should seek and rightfully expect.

Konica Minolta is the industry leader, setting the benchmark for standard security features!

Common Criteria Validated

"Security is the key element of Konica Minolta's overall strategy…

Konica Minolta has a comprehensive range of print and document security features, many of which are standard features for their bizhub range of devices. Rather than certifying optional security kits, Konica Minolta claims to have the widest range of ISO 15408 fully certified MFPs in the market."

Source: Quocirca (2011), Market study "Closing the print security gap. The market landscape for print security", p. 11. This independent report was written by Quocirca Ltd., a primary research and analysis company specialising in the business impact of information technology and communications (ITC).

ACCESS CONTROL/ ACCESS SECURITY

Despite security being high on the agenda in both public and corporate domains, the security risk posed by MFPs is often ignored entirely. While some risks are perhaps identified, they are often simply neglected, especially where sensitive documents and information is concerned. This is especially risky for those MFPs and printers located in public areas, where they can be accessed by staff, contractors and even visitors.

Because of the advanced features available on today's MFPs it is easy for information to be copied and distributed within and beyond actual and virtual corporate boundaries. The first logical step is to prevent unauthorised persons being able to operate an MFP. Preventive measures are needed to firstly control access to MFPs, and secondly to establish some kind of security policy reflecting how the devices are actually used in real life – Konica Minolta achieves this while ensuring that none of these measures restrict or limit the user-friendliness of the systems.

User authentication

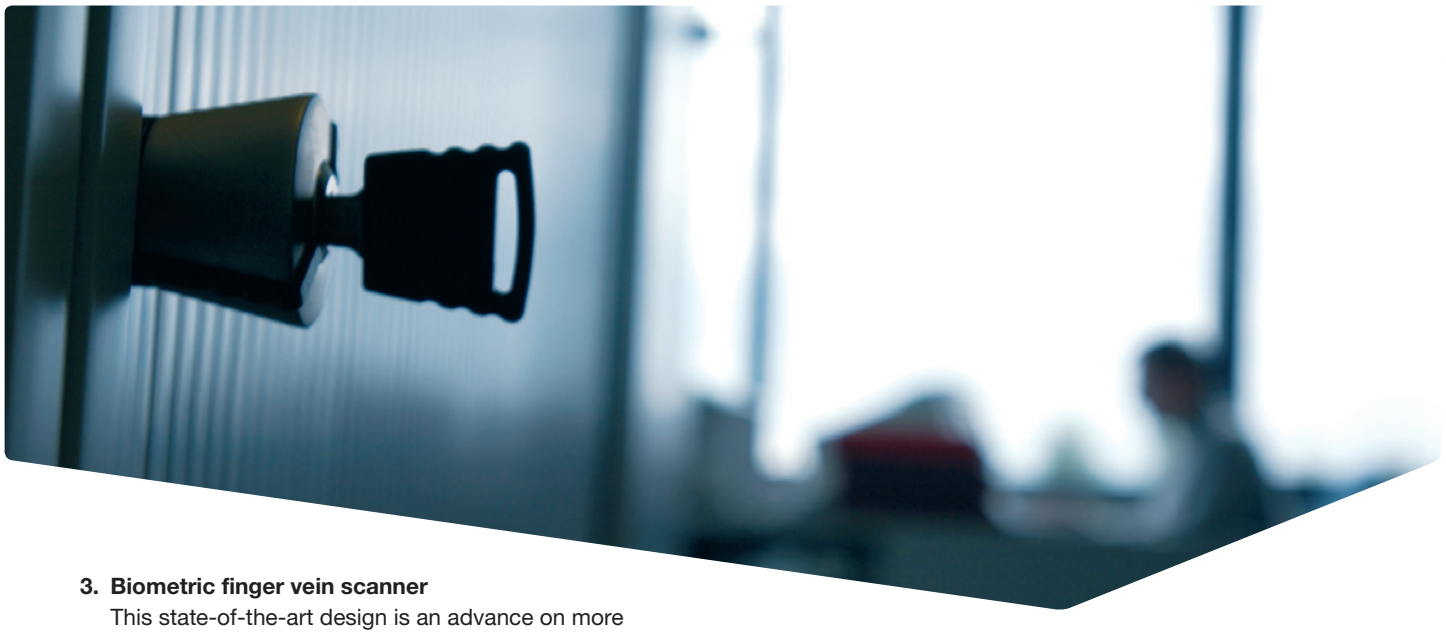
The authentication path starts by setting down a policy defining and configuring users and groups of users allowed to work with an MFP device. This can include limitations to access rights; basically that some users are authorised, while others are not, to use various functions such as colour printing.

Konica Minolta provides three basic technologies for user authentication:

1. **Personal password:**
   The password, an alphanumeric code with up to 8 characters, is entered at the MFP panel. These codes can be created for administrators and users. An important aspect is that they can be centrally managed.

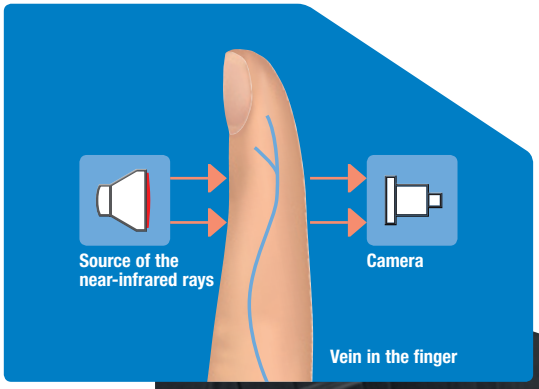
2. **IC card authentication**
   Most Konica Minolta devices can be fitted with an IC card reader. These are designed for convenience and speed; it is simply a matter of placing the IC card on or near the reader interface.

User authentication



3. **Biometric finger vein scanner**
   This state-of-the-art design is an advance on more common fingerprint scanners. This system works by comparing the image of the scanned-in finger vein patterns with those in the memory. The finger vein is a biometric which is almost impossible to falsify, and is therefore a means of identifying a person based on an individual physical feature. Unlike fingerprint systems, the finger vein cannot be scanned without the person actually being present and alive.
   The biometric finger vein scanner means there is no need for people to remember passwords or carry cards.

The authentication information can be stored either on the MFP (encrypted) or draw on existing data from the Windows Active Directory.
Ongoing information logging of access and usage for each individual device means that any security breaches are detected immediately and flagged.



Account tracking

Since user control/security requires every user to log in to the output device, the data generated represents an efficient means of monitoring at a number of levels such as user, group and/or department. Whichever of the device functions is used, monochrome or colour copy, scan or fax, b/w or colour printing, they can all be tracked individually, either at the machine or remotely. Analysis and trending of this data provides robust information about MFP usage from a number of different viewpoints: the data can be applied to ensure compliance and to trace unauthorised access; above all it allows usage to be monitored across the whole fleet of printers and MFPs in a corporate/business/office landscape.

Function control/Function restriction

It is possible for various MFP functions to be limited on an individual user basis. All of the Konica Minolta access control and security functions not only offer greater security against threats which can result in damage in financial and reputational terms, they can also be used as the basis for better governance and enhanced accountability.

DOCUMENT/DATA SECURITY

Reflecting the fact that MFPs and printers are often located in public areas, where they can be easily accessed by staff, contractors and visitors, it is necessary to implement appropriate data security policies. The situation is that confidential data, for example stored on the MFP hard disc over a period of time or simply confidential documents lying in the MFP output tray as printouts, are initially unprotected and could fall into the wrong hands. Konica Minolta offers a range of tailored security measures to ensure document and data security.

HDD security

Most printers and MFPs are equipped with hard discs and memory which can retain many gigabytes of possibly confidential data, collected over long periods.
Dependable safeguards must therefore be in place to ensure the safekeeping of sensitive corporate information.
With Konica Minolta a number of overlapping and intermeshing features provide this assurance:

- **Auto delete function:**
  The auto delete function erases data stored on the hard disc after a set period.

- **Password protection of internal HDD:**
  The read-out of data, obviously including confidential data, on the hard disc requires password entry after HDD removal. The password is linked to the device. The data is therefore not accessible after the HDD is removed from the device.

- **HDD overwriting:**
  The most secure method of formatting a hard disc is that of HDD data overwriting. This is performed in accordance with a number of standards.

- **HDD encryption:**
  On HDDs fitted to Konica Minolta devices the data can be stored in encrypted form based on a 128-bit algorithm encryption system. This feature satisfies corporate data security policies. Once an HDD is encrypted, the data cannot be read/retrieved, even if the HDD is physically removed from the MFP.

Secure print

Output devices are considered a security risk, a risk which should not be underestimated: at the simplest level, documents lying in the output tray can after all be seen and read even by passers-by. There is no simpler way for unauthorised persons to gain access to confidential information.
Secure print functionality is a way of ensuring document confidentiality as it specifies that the author of any print job must set a password as a security lock prior to the printing process itself. The secure print function requires the password to be entered directly at the output device, otherwise printing will not start. This is a simple and effective way of preventing confidential documents from falling into the wrong hands.

Touch & Print/ID & Print

Touch & Print is based on authentication via finger vein scanner or IC card reader while ID & Print requires user authentication via ID and password. The printing of the job at hand is immediate at the device, but only after the user at the MFP has been authenticated via an IC card being placed on the unit card reader or by ID confirmation using the finger vein scanner. The advantage of this particular feature is that it waives the need for additional security print ID and password.

Copy protection

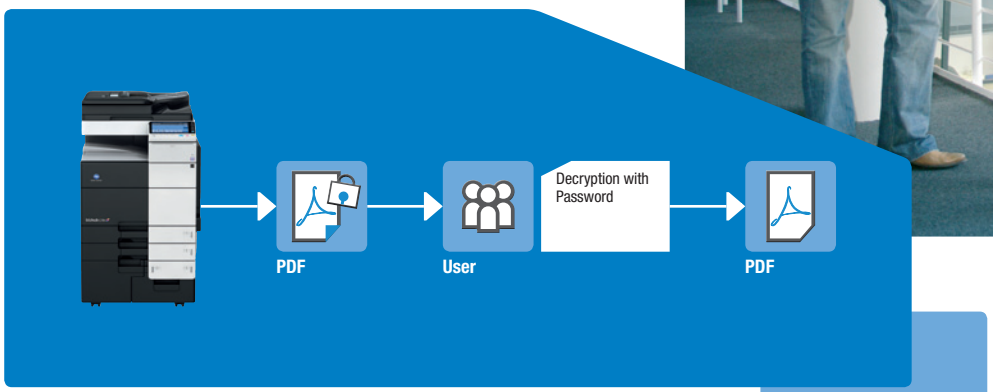
The copy protection feature adds a watermark to printouts and copies during the printing process. The watermark is barely visible on the original print, but if the document is copied, it moves from the background into the foreground to indicate that it is a copy.

Copy guard/Password copy

This feature adds a concealed security watermark to the original during printing to prevent copies of the document from being made. While barely visible on the protected original document, it is not possible to copy this document again, because the device is blocked for this operation. The password copy feature can override the copy guard and allows copies to be made when the correct password is entered at the MFP panel.

PDF encryption

Encrypted PDFs are protected by a user password: permission to print or copy the PDF and permission to add PDF contents can be configured during the scanning phase at the MFP.



Encrypted PDF

PDF digital signature

This feature allows a digital signature to be added to the PDF during scanning. After a PDF is written, this allows any changes to be monitored.

Fax reception

When activated, any faxes received can be kept confidential in a protected user box.

User box security

User boxes are available for single persons and for groups and allows for any documents to be securely stored on the MFP hard disc before output of the print or copy job. User boxes can be protected using an eight-digit alphanumeric password. When the right password is entered, it is possible to access/view documents in the box. This system effectively ensures that confidential documents and data can only be viewed by authorised persons.

NETWORK SECURITY

In today's corporate environment, indeed in today's business world, communications and connectivity are indispensable. Konica Minolta office devices are designed to integrate into network environments. For example, network printers and multi-functional peripherals (MFP) have evolved to the point that they act as sophisticated document-processing hubs integral within the network, with the ability to print, copy and scan documents and data to network destinations, as well as send e-mails. This scenario also means that this office technology must cope with and comply with the same security risks and policies as any other network device, and represents a risk if unprotected. In order to avoid any vulnerability from both internal and external network attacks, Konica Minolta ensures that all equipment complies with the strictest security standards. This is achieved by a number of measures including:

IP address blocking

A basic internal firewall provides an IP address filtering capability and appropriate control of protocol and port access.

Port disabling

The administration mode allows for ports and protocols to be opened, closed, enabled and disabled either directly at the machine or from a remote location.

S/MIME

Most Konica Minolta MFPs support S/MIME (secure/multi-purpose internet mail extensions) in order to secure e-mail communications from the MFP to specified recipients. S/MIME is used to ensure secure e-mail traffic by encrypting the e-mail message and its content using a security certificate.

SSL/TLS communication

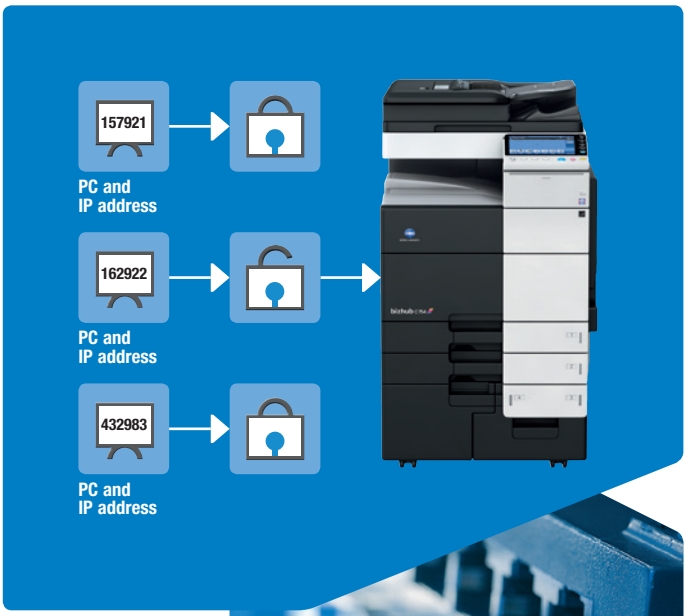
This is a protocol which provides protection to communications to and from the device, covering online administration tools and Windows Active Directory transmissions, for example.

IPsec support

Most bizhub devices also support IPsec to ensure complete encryption of any network data transmitted to and from an MFP. The IP security protocol encrypts all network communications between the local intranet (server, client PC) and the device itself.

IEEE 802.1x support

The standards described in the IEEE802.1x family are the recognised port-based authentication standard for network access control to WANs and LANs. These standards ensure a secure network by shutting down any network communications (e.g. DHCP or HTTP) to unauthorised devices with the exception of authentication requests.



IP address filtering