KONICA MINOLTA

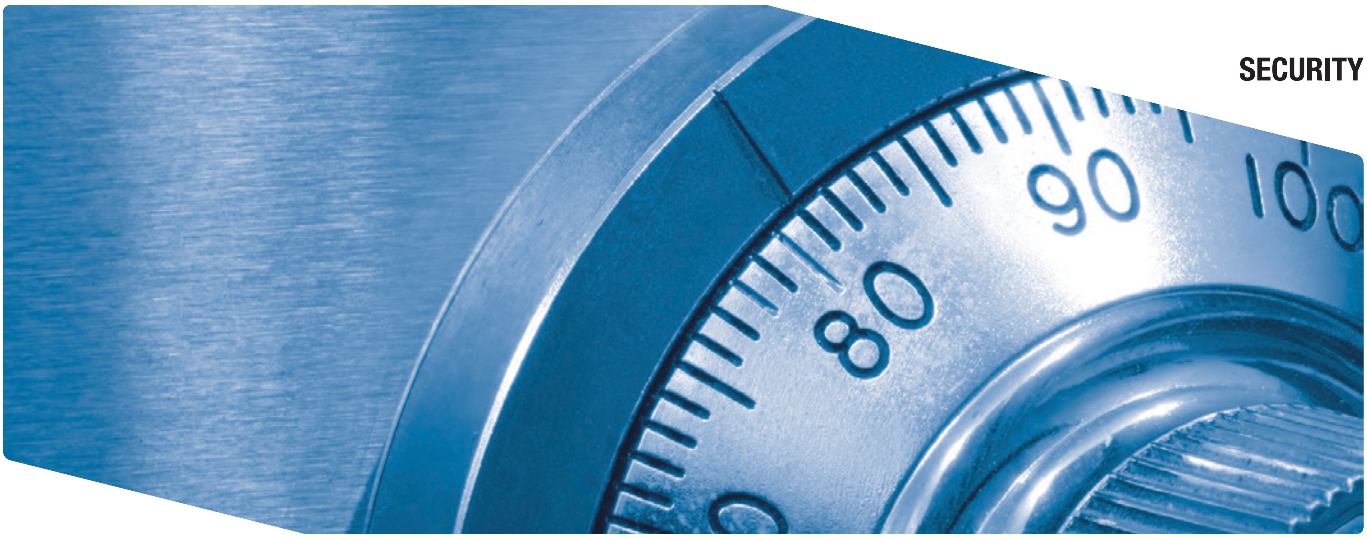
SAFEGUARD YOUR COMMUNICATION

With security standards from Konica Minolta

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 daily activities of printing, copying, scanning, e-mailing and faxing as the elementary communication applications in work processes and workflows make multifunctional peripherals (MFPs) 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.

Giving Shape to Ideas

SECURITY



RELIABLY DETECT & PREVENT **SECURITY BREACHES**

If you want solutions to both detect and prevent security violations, and want to avoid knock-on financial and/or reputational damage at corporate as well as private individual level, trust the industry leader Konica Minolta who offers a comprehensive range of standard security features and options.

Generally MFPs give their users a huge range of combined and single functions and choices. As a consequence, 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 disk)
	Hard disk data overwrite
	Hard disk 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

PROVEN SECURITY EVALUATION THAT YOU CAN TRUST

You want to be able to truly rely on your output devices guaranteeing you the security you need? With printers and MFPs from Konica Minolta you can relax, because almost without exception they are certified in accordance with the Common Criteria / ISO 15408 EAL3 standard and IEEE 2600.1.

The Common Criteria certification conforming to ISO 15408 EAL3 is the only internationally recognised standard 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 can rightfully expect.

The Common Criteria certification according to IEEE 2600.1 acknowledges Konica Minolta‘s office information security standard. This certification is an international IT security standard and confirms that the security features in the certified MFPs conform to the high standards of the Institute of Electrical and Electronic Engineers (IEEE). From daily office tasks to the handling of highly confidential information and documents – all data saved on corporate level need reliable protection, which this certification guarantees you.

Setting the benchmark for standard security features, Konica Minolta is the industry leader in this field.

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 option- al 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).

INDIVIDUAL ACCESS CONTROL FOR ALL-ROUND SECURITY

Although these days, security generally is high on the agenda in both public and corporate domains, the security threats from MFPs are often ignored entirely. While most companies might recognise some of the risks, these frequently are simply neglected, especially where sensitive documents and information are concerned. This is especially risky for any MFP or printer located in a public area, as this 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 from operating an MFP at all. Preventive measures are needed firstly to 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 without restricting the user-friendliness of the systems in any way.

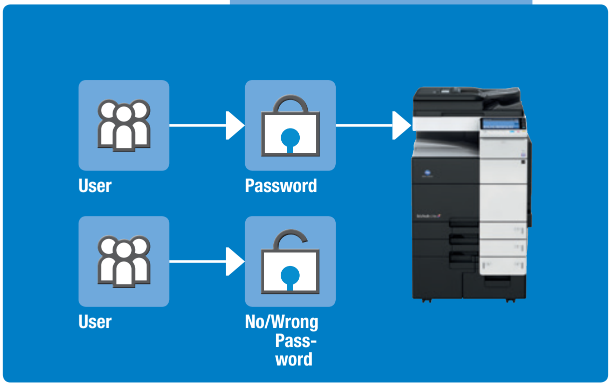
Comprehensive user authentication

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, namely 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. **ID card authentication**
   Most Konica Minolta devices can be fitted with an ID card reader. ID cards offer convenience and speed; it is simply a matter of placing the ID card on or near the reader interface to access and also to log out of the system.



User authentication

3. **Biometric finger vein scanner**

   This state-of-the-art design is an advance on more common fingerprint scanners. The system works by comparing the image of the scanned-in finger vein patterns with those in the memory. The finger vein is a biometric characteristic that is almost impossible to falsify, which makes it extremely reliable to identify 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.

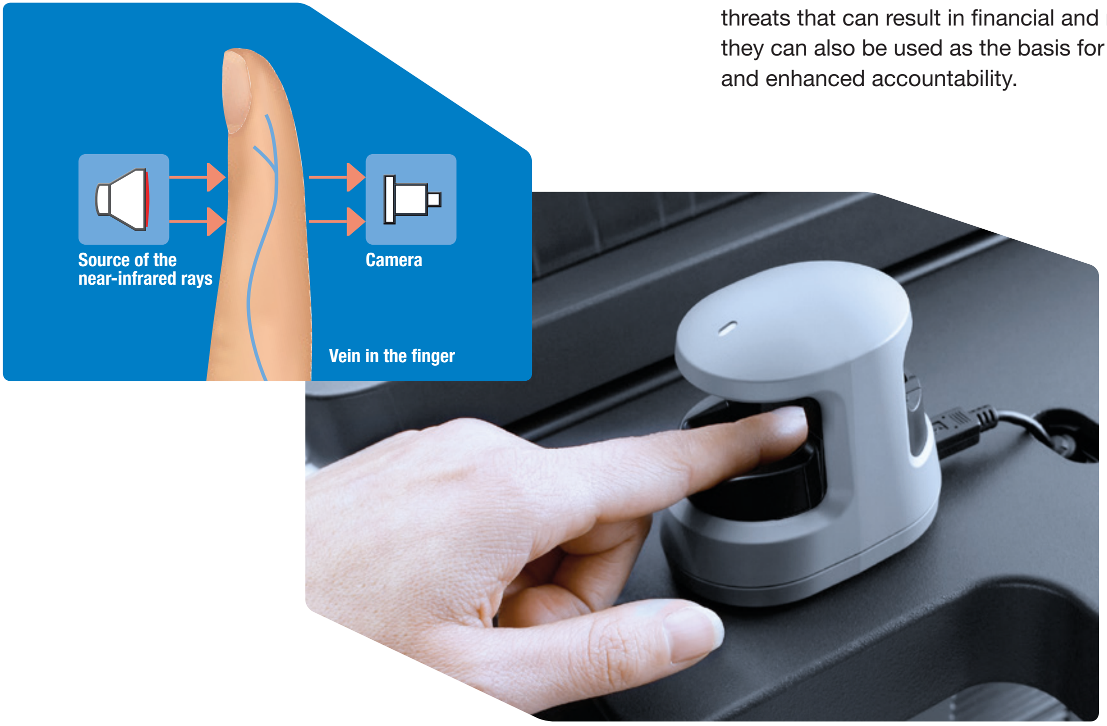
Ongoing information logging of access and usage for each individual device means that any security breaches are detected immediately and flagged.

Account tracking for more transparency

Since user control for 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.

Individualise access with function restrictions

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



COMPREHENSIVE SECURITY FOR DATA AND DOCUMENTS

As MFPs and printers are often located in public areas, where they can be easily accessed by staff, contractors and visitors, implementing appropriate data security policies is essential. Sensitive data stored on the MFP hard disk over a period of time as well as confidential documents lying in the MFP output tray as printouts, are initially unprotected and can easily fall into the wrong hands. To avoid this and ensure complete document and data security, Konica Minolta offers a range of tailored security measures.

No loopholes with HDD security

Most printers and MFPs are equipped with hard disks and memory that 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. In Konica Minolta systems, a number of overlapping and intermeshing features provide this assurance:

- **Auto delete function**
  The auto delete function erases data stored on the hard disk after a set period.
- **Password protection of internal HDD**
  The read-out of data, obviously including confidential data, on the hard disk 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 disk 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.

Protect documents with secure printing

Output devices are considered a security risk that 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 easier way for unauthorised persons to gain access to confidential information. The 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. Following that, printing can only be started by entering this password directly at the output device. This is a simple and effective way of preventing confidential documents from falling into the wrong hands.

Printing with individual authentication

Touch & Print is based on authentication via finger vein scanner or ID card reader while **ID & Print** requires user authentication via ID and password. The job at hand is printed immediately after the user authenticates at the MFP by placing his ID card on the unit card reader or by ID confirmation using the finger vein scanner. The advantage of this particular feature is its speed: it waives the need for additional security print ID and password.

Curb unauthorised copying

The **copy protection** feature adds a watermark to prints 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.

Remain in control with Copy Guard

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

Smart 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.

Useful PDF digital signature

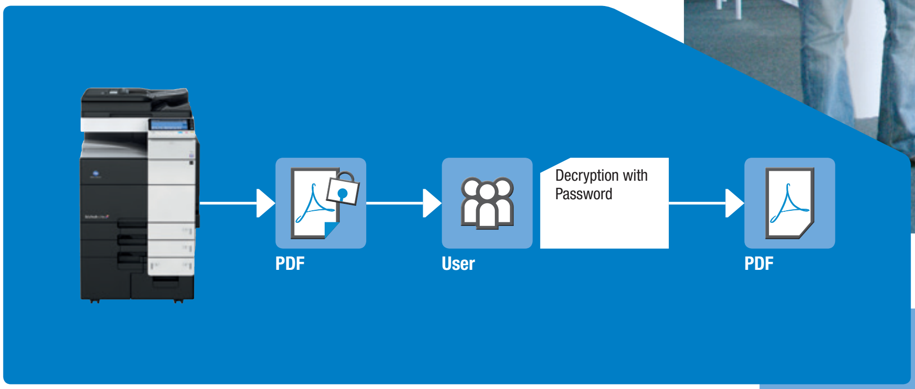
With this feature, a digital signature can be added to the PDF during scanning. After a PDF is written, this allows monitoring any changes.

Secure fax reception

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

User box security

User boxes are available for single persons and for groups and allow for any documents to be securely stored on the MFP hard disk 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 limits access to confidential documents and data to those authorised.



Encrypted PDF

SECURE **YOUR NETWORK**

Communication and connectivity are indispensable in today's business world. Office devices from Konica Minolta account for this and provide easy integration into network environments. No doubt, you are aware that network printers and multifunctional 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.

For your office, this or a similar scenario means that such technology represents a risk if unprotected and must therefore cope with the same security threats and policies as any other network device. In order to avoid any vulnerability from both internal and external network attacks, Konica Minolta helps you ensure that all your equipment complies with the strictest security standards. In Konica Minolta devices, this is achieved by a number of measures including:

IP address blocking

Control protocol and port access with this basic internal firewall that includes an IP address filtering capability.

Port handling

Your administrator can open, close, enable and disable ports and protocols either directly at the machine or conveniently from a remote location.

Secure e-mail communication

Most Konica Minolta MFPs support S/MIME (secure/multi-purpose internet mail extensions) in order to secure the e-mail communication from your MFPs to specified recipients. S/MIME secures your e-mail traffic by encrypting e-mail messages and their content using a security certificate.

Network authentication

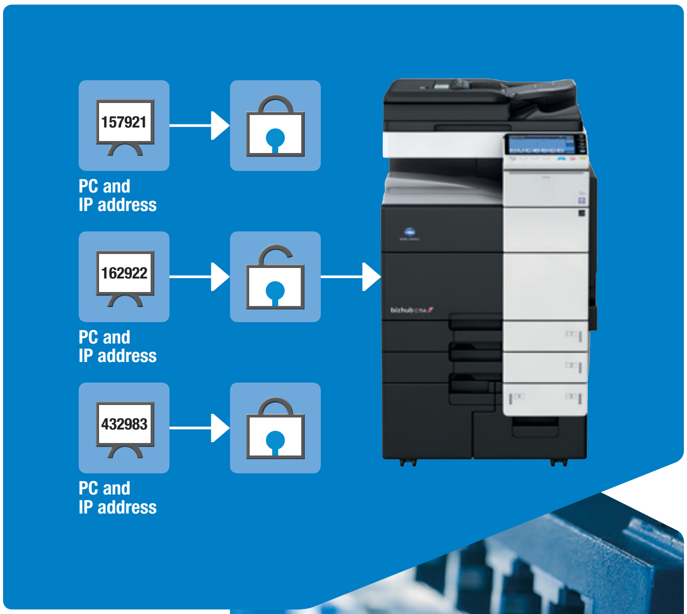
The standards described in the IEEE802.1x family are the recognised port-based authentication standard for network access control to WANs and LANs. These standards effectively secure your network by shutting down any network communication (e.g. DHCP or HTTP) to unauthorised devices, except for authentication requests.

Protected communication

This protocol gives you protection for all communication to and from devices, covering online administration tools and Windows Active Directory transmissions, for example.

Encrypted network communication

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



IP address filtering

02/2014