DEVELOP

Dynamic balance

www.develop.eu

Security
you can count on!

Develop's security standards

data security

data security

Industry-leading security standards

In today's business company data has to cross a lot of different data highways. These different highways offer a lot of opportunities for digital attacks by hackers or viruses. Good to have antivirus software, network administrators and other tools which helps securing your environment! But what about your digital office system? Have you secured your multifunctional system as well as your PC?

Nearly every work process and workflow starts, ends or is somehow related to your multifunctional office device. A lot of your business data is running through your multifunctional system. This is the reason why the multifunctional office system as a main element of your business work processes and workflows has to withstand ongoing threats to security.

Develop'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 the corporate as well as the private individual level. Develop has pioneered this field and remains the industry's leader. Develop systems 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 the ISO 15408 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.

Common Criteria Validated

Data stay where they belong – in the right hands!

ineo systems offer a huge range of functions and features. All these features represent a wide range of potential security leaks. Therefore a lot of security mechanisms are included in the system offering secure access control, document and data security and network security. With ineo systems data stay where they belong to.

Access control/Access security

Despite the topic of security being high on the agenda in both public and corporate domains, multifunctional systems are often ignored as being any kind of security risk. This is especially risky for those systems and printers located in public areas, where they can be accessed by staff, contractors and even visitors. Because the advanced features available on today's systems deliberately make it 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 a multifunctional system. Preventive measures have to control access to multifunctional systems.

For this reason Develop offers various security features and solutions enabling access control and security.

Document security/ Data security

Reflecting the fact that multifunctional systems and printers are often located in public areas where they can easily be accessed, confidential data or documents stored in the HDD or printouts lying in the output tray could fall into the wrong hands. For this reason it is important to implement security policies which guarantee documents and data will not leave your company. In order to ensure document and data security Develop offers a huge range of tailored security features!

Network security

Today's business environment is characterised by connected systems, automatic data collection and transmission to downstream systems handling the data afterwards. Just like the scan send to a PC-folder or via E-Mail. Develop office devices are designed to work in network environments which enables fast processing workflows with the ability to scan data to network destinations or receive print jobs from different devices and destinations. There are a lot of connections from or to the multifunctional system which have to be secured. Otherwise they represent a potential risk.

Therefore Develop ensures that all equipment complies with the strictest security standards which are achieved by multiple features in order to close potential security leaks by using the network connection.

With its comprehensive range of security features, Develop provides professional solutions for the detection and prevention of security leaks.

Access control & security – safe path to DEVELOP multifunctional systems

Available features of the multifunctional systems make it very easy to operate them. The first logical step is to prevent unauthorised persons being able to use the system. This is the reason why authentication is needed including definition of users and user groups and limitations to access and usage rights. So some users are authorised to use specific functions, while others are not.

User authentication methods

DEVELOP offers various access control methods which are enabling access to the multifunctional system via authentication. Therefore only authorised persons can access and use the systems functionalities.

› Biometric finger vein authentication

Biometric finger vein authentication employs cutting edge technology by working with images of finger vein patterns that are captured by scanning the finger. Using an individual human feature for identification, this biometric measurement is virtually impossible to falsify. This authentication method is a lot more secure than fingerprint systems. And it's fast and simple, since there's no need to remember passwords or carry a card.

› Non-contact IC card

Authentication by non-contact IC card is also available for most ineo systems. This method is also designed for convenience and speed – it is simply a matter of placing the IC card on or near the reader interface.

› Password or user code

The simplest form of user authentication is to restrict access by personal password or user code which has to be entered at the panel. This internal authentication at the system supports up to 1,000 user accounts. Passwords are alphanumeric with up to 64 characters, can be created for administrators and users, and are maintained by an administrator.

Further authentication features

Encryption of authentication information

Authentication information can be stored in encrypted form on the multifunctional system, or existing access information can be used, e.g. from the Windows Active Directory. In addition, the authentication can be centrally managed via the Enterprise Suite Authentication Manager. This ensures no unauthorised person can read out authentication information or manage access rights.

Automatic reset

If you forget to logout the system is normally free for use. In consequence all ineo systems can be programmed to automatically reset in order to require password input after a specified period of inactivity. This ensures that the multifunctional system will reset to a secure state if a user forgets to log off when finished. Password protection can also be used to limit access to documents on system from remote workstations. Many DEVELOP devices offer the ability to remotely access print and scan jobs. This feature can be either password-protected or disabled altogether.

Unauthorised access lock

Like a cash terminal, each ineo system can be programmed to reject a user who attempts to authenticate with a wrong password. After a specified number of wrong attempts, the machine will block access for a chosen time period. This unauthorised access lock function can also be applied to the system user box for confidential documents (secure print box). This feature protects the multifunctional system against brute-force-attacks by trying lots of passwords in a short period of time done by hacking-tools.

Limitation of functionalities

An advanced level of user security governs the availability of specific features, allowing or prohibiting their use. A key operator or administrator can control these features as needed throughout an organisation of any size. The specific features are:

- Copying from the ineo as a walk-up function, including the restrictions of only b/w copying or only colour copying or neither b/w nor colour copying
- Printing as a remote function via the printer driver, including the restrictions of only b/w printing or only colour printing or neither b/w nor colour printing
- Scanning from the ineo as a walk-up or a remote function
- Faxing from the ineo as a walk-up or a remote function
- User box from the ineo as a walk-up or a remote function
- In addition, it is possible for various functions to be limited on an individual user basis. This could be directly linked with the authentication methods mentioned above.

Log information

Log information for access and usage of individual devices not only enables immediate detection of security breaches, it also facilitates accounting and cost allocation to users and departments. The administrator can individually review audits and job logs for different machine functions, including b/w and colour printing and/or copying, incoming and outgoing faxes, and scanning. Many print controllers on DEVELOP systems contain electronic job logs that record all print jobs sent to the output device. In addition, DEVELOP's Job Log Utility provides comprehensive electronic tracking logs of user activity.

Account tracking

Account tracking requires a user login at the output device and provides efficient monitoring at user level, group level and/or departmental level. Monochrome and colour copies, scans, faxes, b/w and colour printing can all be tracked locally at the machine or remotely via DEVELOP software such as Web Connection, Device Manager and Enterprise Suite Account Manager. When logged in, the user's activities are electronically recorded onto a log file inside the system, which can be accessed by the administrator or key operator. This feature provides efficient support, e.g. for invoicing departments or to audit employees' copier activities.

Document security & Data security – Confidential data and information secured by DEVELOP

When the multifunctional system is located in a public area confidential data can be accessed by staff, contractors or even visitors. These data may be available via printouts lying in the output tray or stored on the systems HDD. DEVELOP's comprehensive security functionality secures user details and output content, helping to prevent sensitive corporate information from falling into the wrong hands.

Secure printing

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 be seen and read even by passers-by. There is no simpler way for unauthorised persons to gain access to confidential information. The secure print functionality keeps documents confidential by requiring the author of the print job to set a password as a security lock prior to printing. Protected documents cannot be printed until the password set in the driver is entered directly at the output device. This guarantees that such documents are available only to those intended to read them. Each password connected to a confidential print job is encrypted. As further protection, the ineo systems can be configured to delete all unopened secure print jobs after a designated time period.

Secure printing is also available via the convenient Touch & Print or ID & Print functionality. Touch & Print is based on authentication via finger vein scanner or IC card reader, while ID & Print requires the user's authentication via ID and password. With these features, no additional secure print ID and password are required; instead the user authentication data is used to identify a stored secure print job and release the job immediately after authentication at the device.

Alternatively, print jobs can be protected by secure printing to the user box. The user box functionality on ineo systems enables users to store their documents in personal boxes that are only visible after authentication and only accessible with an additional individual user password. To access such print jobs for outputting or forwarding via fax or email, the user has to enter both the correct user ID and the password. At the same time the protected user boxes also enable confidential fax receipt.

PDF encryption

The content of PDFs can be encrypted by standard 40- or 128-bit encryption. Encrypted PDFs are protected by a user password that can have up to 32 characters. As part of the encryption, it is possible to specify permissions to print or copy the PDF or even edit its contents.

Encryption by Digital ID

PDF data that is attached to an email or sent to an FTP or SMB folder can be encrypted by Digital ID. Such PDF encryption makes the interception of PDF information impossible. Digital ID encryption is based on the S/MIME encryption and requires a public key for encryption plus a private key for decryption.

Digital signature

To prevent tampering with PDFs created on an ineo system, a digital signature can be added to the PDF. This monitors any changes made to the PDF after writing it. The digital signature clearly indicates all changes in the PDF security information. In addition to preventing documents from being tampered with, the digital signature provides details on the document source, helping to recognise if this is unsafe.

Copy protection

With copy protection, which is available on certain ineo models, a concealed security watermark is placed on the original document during printing. The security watermark can consist of several phrases and/or patterns. When a protected document is copied on any other system, the security watermark will appear, indicating to the recipient that this document has been copied and/or distributed without authorisation.

Copy Guard/Password Copy

The optional Copy Guard/Password Copy feature adds a concealed security watermark to the original during printing to prevent the copying of documents. While barely visible on the protected original document, it is not possible to copy this document again. 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 systems panel.

Hard Disk protection

Most printers and multifunctional systems have access to hard disks and memory which can retain many gigabytes of confidential data, over long periods. Dependable safeguards must therefore be in place to ensure the safekeeping of sensitive corporate information. At Develop a number of overlapping and intermeshing features provide this assurance.

HDD encryption

Develop offers HDD encryption for most of the multifunctional devices. This is of interest to companies that are concerned about the security of documents stored as electronic data in password-protected boxes on the system's hard drive. The stored data can be encrypted using the Advanced Encryption Standard (AES) supporting 128-bit key size. Once a HDD is encrypted, its data cannot be read even if the HDD is removed.

HDD data auto-delete

An auto-delete function erases data stored on the internal hard disk after a set time. This format/erase hard drive feature protects the sensitive electronic information stored on the hard disk drives of ineo systems. The stored data can be deleted by the user who first stored the document.

HDD overwrite

For added safety, a key operator, administrator or technician can physically format the HDD, for example if the system needs to be relocated. The hard drives can be overwritten using a number of different methods conforming to various (e.g. military) specifications. In addition, administrators can program the ineo to automatically erase any temporary data remaining on the HDD on a per job basis. If the automatic overwrite is set to 'on', then jobs manually deleted from a user box will be overwritten three times as well.

HDD password protection

Password protection of the internal HDD prevents its unauthorised removal; this password is linked with the device so that data is not accessible if the hard disk is removed and installed on other devices like a PC etc.

Network security – safe network communication with DEVELOP

DEVELOP's office devices are based on a concept of communication and connectivity. This complies with strict security standards concerning user access, encryption of data and protocols used for information transmission so you can ensure your data will arrive to the desired destination secure and trustworthy.

User Authentication

Besides governing access to output devices, user authentication also prevents unauthorised users from accessing the network. With this feature, which can be configured to authenticate to the network or locally at the machine, every authorised user has a unique user ID and password.

SSL/TLS encryption

SSL and TLS encryption protects communication to and from output devices, covering online administration tools, the Enterprise Server and Active Directory transmissions, for example. This communication type prevents from man-in-the-middle-attacks where the attacker would be able to record the data communication.

IPsec

ineo devices also support IPsec for the complete encryption of any network data transmitted to and from the multifunctional system. The IP security protocol encrypts the whole network communication between the local intranet (server, client PC) and the device itself.

IP address filtering

An internal basic firewall provides IP address filtering and control of protocol and port access. IP address filtering can be set at the machine: the network interface card of the multifunctional system can be programmed to only grant access to the device to a specific IP address range from client PCs.

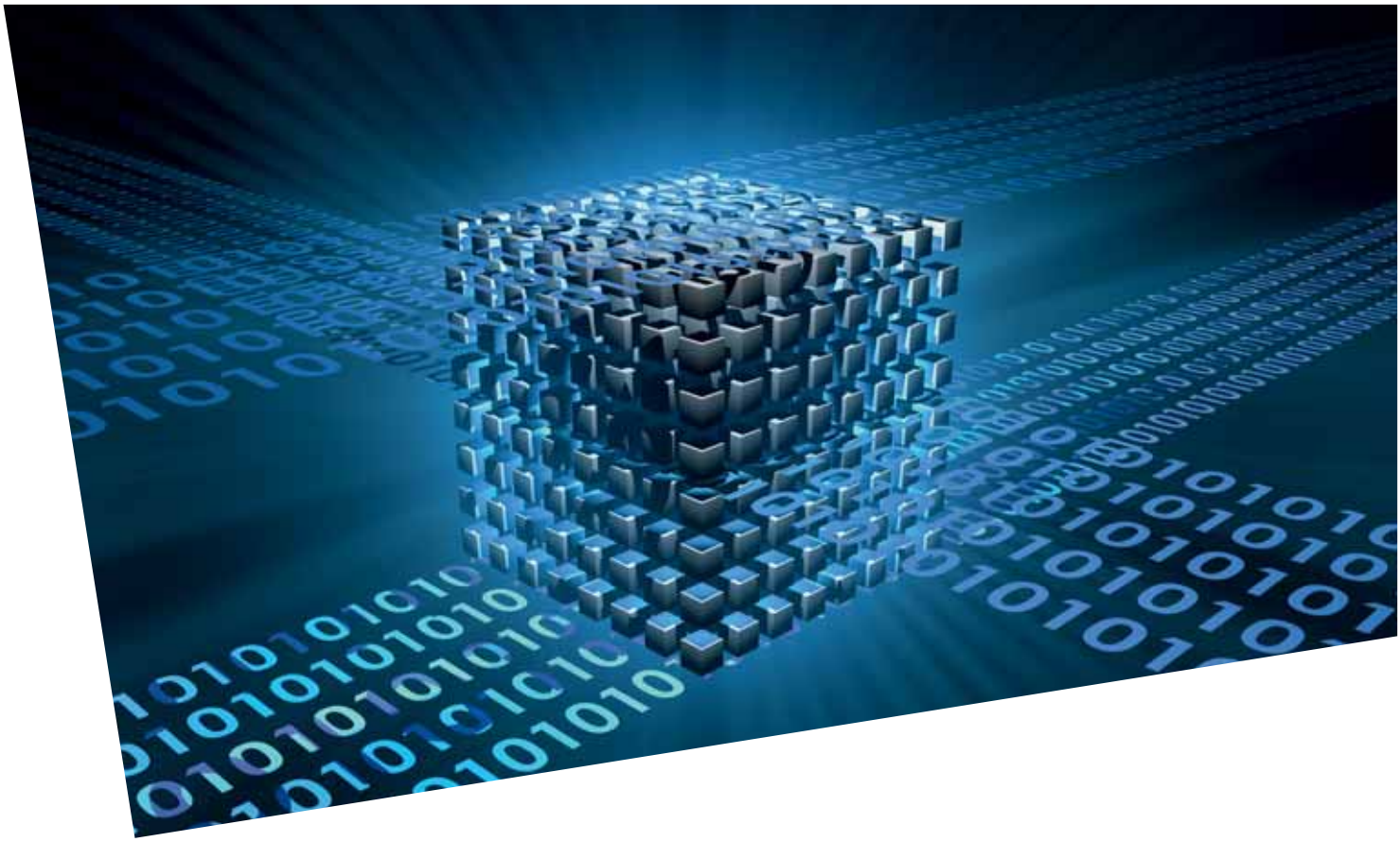
Ports and protocols secured by administrator

Ports and protocols can be opened, closed, enabled and disabled via the administration mode at the machine or remotely via Web Connection or Device Manager. As protection against unauthorised tampering with machine and network settings, the administrator mode itself is accessed by an 16-digit alphanumeric password, which can only be changed by the service engineer or from within the administrator area.

Where required, a web interface closing functionality allows the disabling of the web interface, i.e. Web Connection, for all users. This limits web access to administrators, providing reliable protection against unauthorised persons tampering with settings, configurations, etc.

SMTP Authentication

SMTP Authentication (Simple Mail Transfer Protocol) provides advanced email security. When activated, SMTP will authorise a machine to send email. For those customers who do not host their email services, the use of an ISP mail server is possible and is supported by the machine. SMTP authentication is required by AOL and for the prevention of spam. For secure communication it is also possible to combine POP before SMTP, APOP, SMTP authentication or encryption using SSL/ TLS.



S/MIME encryption

To secure email communication from the multifunctional system to certain recipients, the system supports S/MIME (Secure/ Multipurpose Internet Mail Extensions). S/MIME encrypts the email message and content with a security certificate. S/MIME certificates or encryption keys (public key) can be registered for email addresses stored in the systems address book. S/MIME encrypted emails can only be opened by the owner of the decryption key (private key).

Changing "From" address

When user authentication is activated, it is not possible to change the 'From' address. Despite the 'Changing From Address' function being enabled, The 'From' address of a scan-to-email job will always be the logged-in user's email address. This feature prevents spoofing and provides audit trails for administrators.

Manual Destination Prohibit

With the 'Manual Destination Prohibit' function, the direct input of an email address or scan destination is impossible. If this function is activated, only registered destinations from the internal system address book or LDAP can be used.

Fax line security

Advanced fax line security is ensured by the ineo fax connection using only the fax protocol for communication – no other communication protocols are supported. Develop products block any intrusion attempts as threats, including intrusions of a different protocol over public telephone lines, as well as any attempt to transmit data that cannot be decompressed as fax data.

Fax rerouting

Fax rerouting allows automatic forwarding of incoming faxes to any destination within the internal ineo address book, including for example email addresses, or to the user boxes on the ineo's internal HDD. Storing incoming faxes in a user box is considerably safer, as there are no printed faxes to be seen in the output tray. This rerouting can also make the communication faster, as faxes reach their recipients sooner. Last but not least, it also helps save paper – recipients can decide whether printing a fax is really necessary.

Network access control

Most Develop devices support the IEE802.11x 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.

Be prepared for the everyday security risks!

It is important to remain aware of the fact that today no company or organisation is immune to security risks – security breaches happen everywhere, all the time! But prudent businesses look ahead and take the necessary precautions before it's too late. They ensure that the confidential data held by the hard disk and memory of digital printers, copiers and all-in-one equipment cannot be accessed in the first place, let alone tampered with.

Security-conscious company owners and managers ensure that their network is protected and that unauthorised access to information on the company's intranet is barred. Conscientious managers are also aware that the printers and copiers installed throughout the company can easily constitute the most serious of security gaps. If left unattended in the output tray, confidential information might get into the wrong hands and could easily leave the company, for example via scan to email or fax transmissions. But prudent managers and IT specialists guard against these risks by reliably limiting access to devices to those authorised and by guarding against the unattended output of any kind of prints.

DEVELOP supports its customers' efforts to protect against security risks by allocating extensive engineering resources to the advanced development of security-related features for ineo systems and printers. DEVELOP thus provides customers with the technology required in today's security-conscious environments. Whether a customer is concerned about network intrusion, data theft or compliance with regulations, or whether the issue centres on limiting access to devices or functionalities, DEVELOP ineo technology offers professional solutions for the detection and the prevention of security breaches. This is the level of comprehensive protection that customers from all industries and public authorities now expect.

Overview security features and availability

Features	Multifunctional colour systems				Multifunctional b/w systems						Print systems		
	ineo +25	ineo +35	ineo +224 +284 +364 +454 +554	ineo +654 +754	D 240F	ineo 36 42	ineo 215	ineo 223 283 363 423	ineo 552 652	ineo 501 601 751	ineo +35P	ineo +353P	ineo 40P
Access Control/Access Security													
Copy/print accounting	—	●	●	●	●	●	●	●	●	●	—	●	○
Function restriction (copy/print/scan/fax/box/colour)	●**	●	●	●	●	●	—	●	●	●	○	●	—
Secure printing (lock job)	●	●	●	●	●	●	●	●	●	●	○	●	○
User box password protection	—	—	●	●	●	—	—	●	●	●	—	●	—
User authentification (ID + password)	○	●	●	●	●	●	●	●	●	●	○	●	○
Finger vein scanner	—	—	○	○	—	—	—	○	○	○	—	○	—
IC card reader	—	○	○	○	—	○	—	○	○	○	—	○	—
Event log	—	—	●	●	—	—	—	●	●	●	—	●	—
Data Security/Document 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	—	●	●	●	—	●	—	●	●	●	—	—	—
IEEE 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	—	—	○	○	—	—	—	○	○	—	—	—	—
ISO 15408 certification													
ISO 15408 EAL 3 certified	—	●	●*	●*	—	●*	—	●	●*	●	—	●	—

● = standard ○ = option — = not available * in evaluation ** with reservations

Please contact your dealer for further information.

Your Develop Partner:

January 2013

Konica Minolta Business Solutions Europe GmbH
Europaallee 17 30855 Langenhagen Germany Phone +49 511 7404-0 **www.develop.eu**