DEVELOP

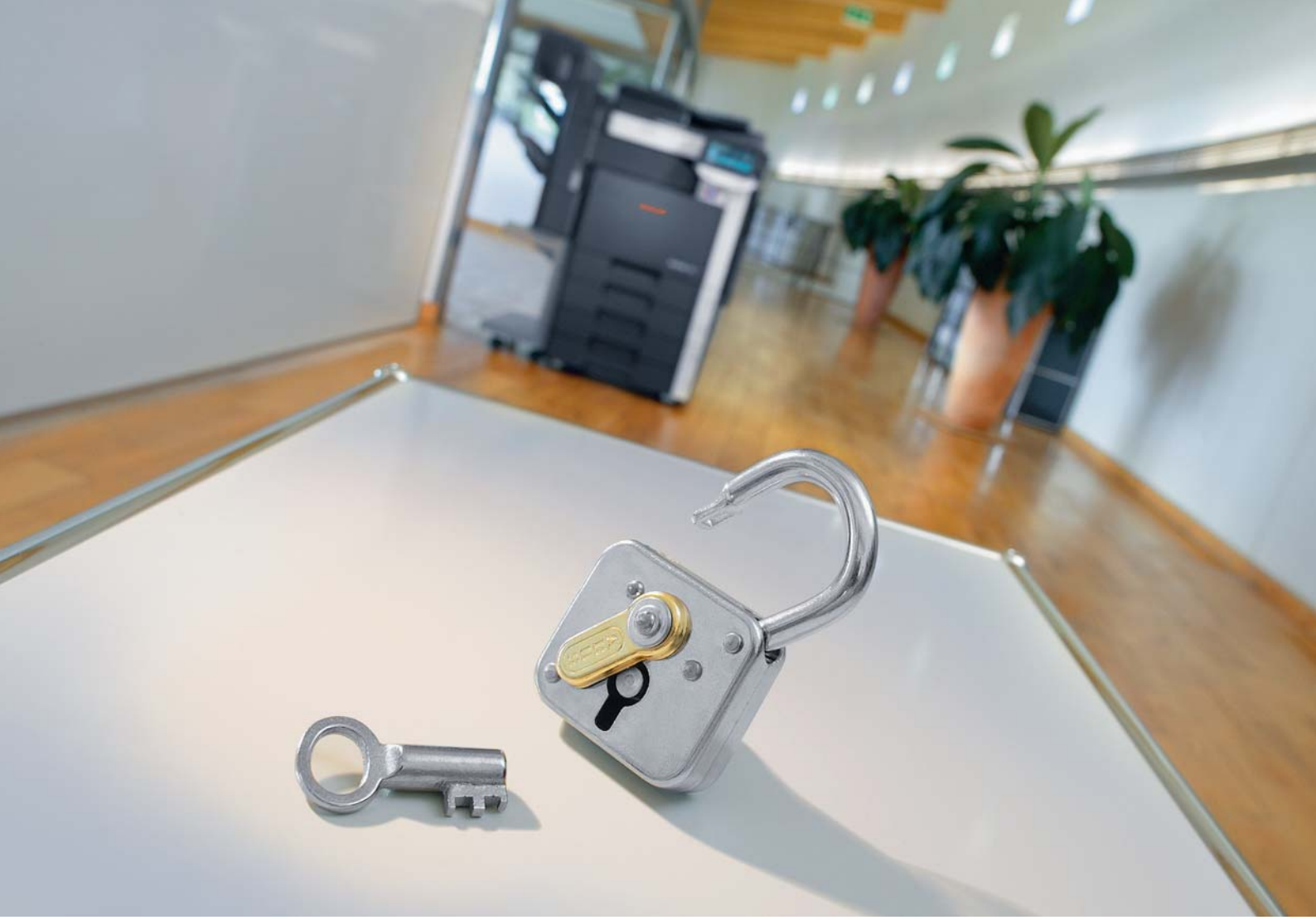
Dynamic balance

www.develop.eu

On the safe side

DEVELOP and data security

data security



Data abuse – a real risk

You know how important it is to protect your PC data from viruses and bugs, hackers and data thieves. But what about the data on your digital office machine? Are these data just as well protected?

The fact is that every organisation is at risk, for example when devices are replaced and the data on their hard disks are not properly deleted. Data theft or abuse can result in financial loss or damaged reputations, especially in organisations where sensitive data circulate freely. In today's information era, data are often an organisation's most valuable asset. And that is why we take the issue of data security very seriously at Develop. Our ineo office systems are equipped with all the latest security functions – and are certified as safe to ISO 15408.

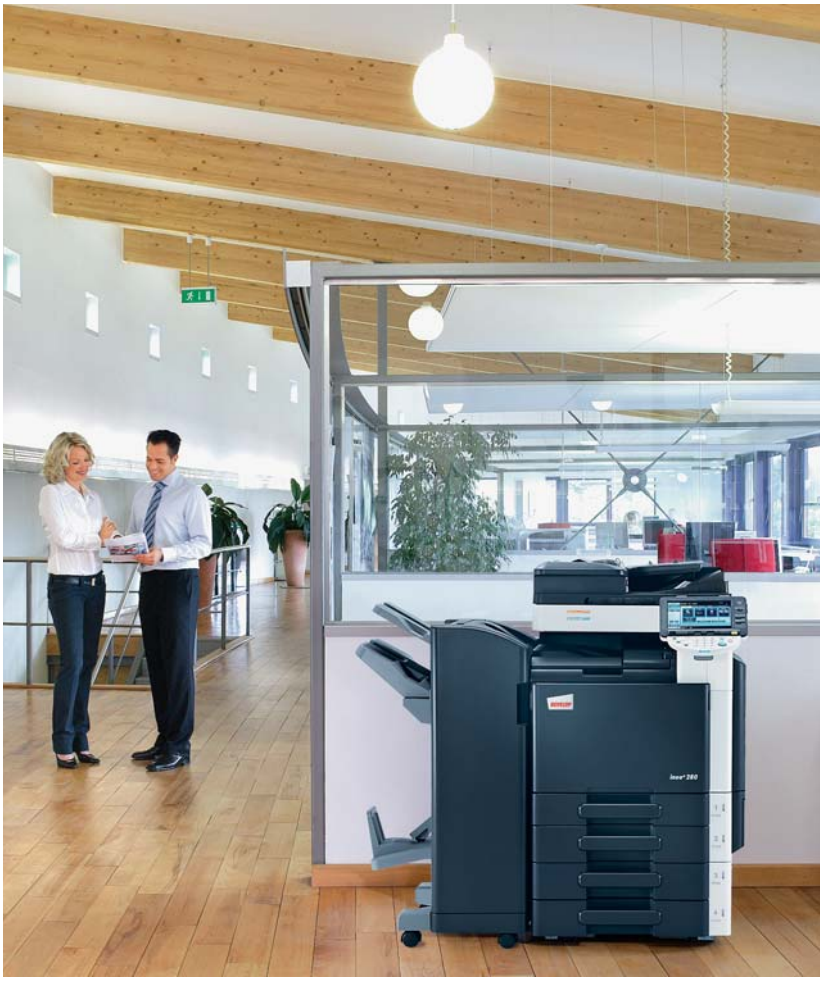
System certification to ISO 15408

ISO 15408 is the only internationally accredited safety standard for digital office machines. Most people know it as "the Common Criteria". Although many vendors of digital office machines claim certification to ISO 15408, in actual fact certification is limited to a specific security kit, data protection kit, software package or data deletion function. The ISO 15408 certificate applies to individual data security options, not the entire system. Develop, in contrast, has been awarded system certification to ISO 15408 EAL 3. In other words, when you invest in an ineo office machine, you can be sure that the entire system is safe.

Secure printing on an ineo system

Secure print

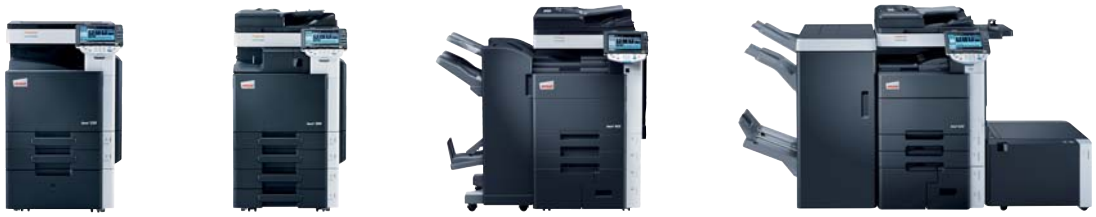
The digitalised office brings many benefits, but also various risks. Today's digital office machines – whether printers or multifunctional devices – offer networked access to every user from his or her PC. That is certainly convenient, but also raises the question of who has access to sensitive data on the system's hard disk. If sensitive information has to be printed or copied, there is always the risk that it will end up in the wrong hands – unless the digital office machine is equipped with data security functions that, for example, restrict access to authorised persons. Here, ineo systems offer a number of options that go well beyond the standard security functions. With DEVELOP you can be sure that confidential documents stay that way.



Automatically safe

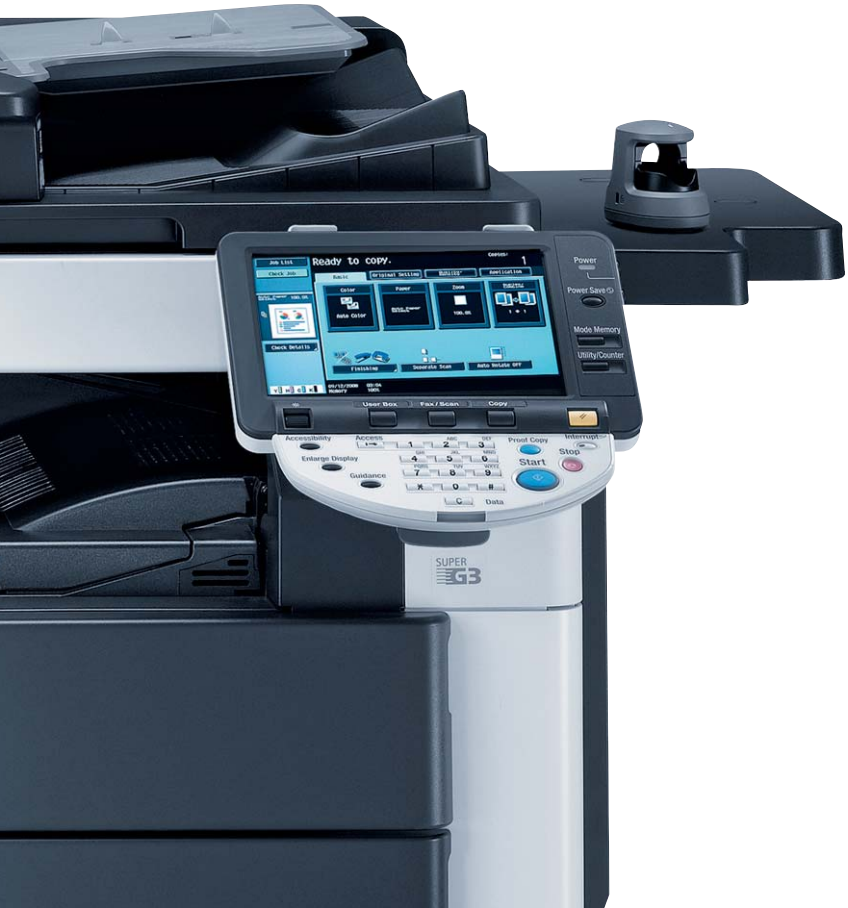
Automatic log-off

One of the simplest but most effective security features is the automatic reset/log-off function, which can be set to any time between 1 and 9 minutes. At the end of the preset period, you will be automatically logged off and can only access printing data by re-entering your password or other means of authentication. This ensures that no other user can access your documents, even if you simply forget to press the manual log-off key when you collect your documents from the printer. DEVELOP ensures automatic data security.



Safe through state-of-the-art technology

Encryption of sensitive information
Encrypting electronic data ensures they stay confidential. ineo office systems are equipped with a standard encryption function that ensures that only an authorised user can open a document for printing by entering a pre-defined password. The ultimate security feature for an ineo office system is the 192- or 256-bit encryption for even greater data security*. This Security Chip ensures that all the documents and data stored on the system's hard disk are encrypted to the Advanced Encryption Standard. With this option, you can be sure your sensitive data stay safe even if the hard disk is stolen or the ineo office machine is sold or returned to the dealer after a leasing contract expires.



High-tech authentication

Authentication
Who is allowed access to sensitive data? That is a critical security question. On ineo office machine's permission to print such documents can be restricted to authorised persons – and although the two options available are entirely safely, they are easy to use.

- **Card-based authentication:**
  This contactless smart card allows individual users fast and safe access to documents on an ineo office machine. The advantage here is that printing, copying, faxing and scanning functions can be restricted to authorised users, if required. This reduces the risk of data abuse and is also an effective means of controlling document production costs.

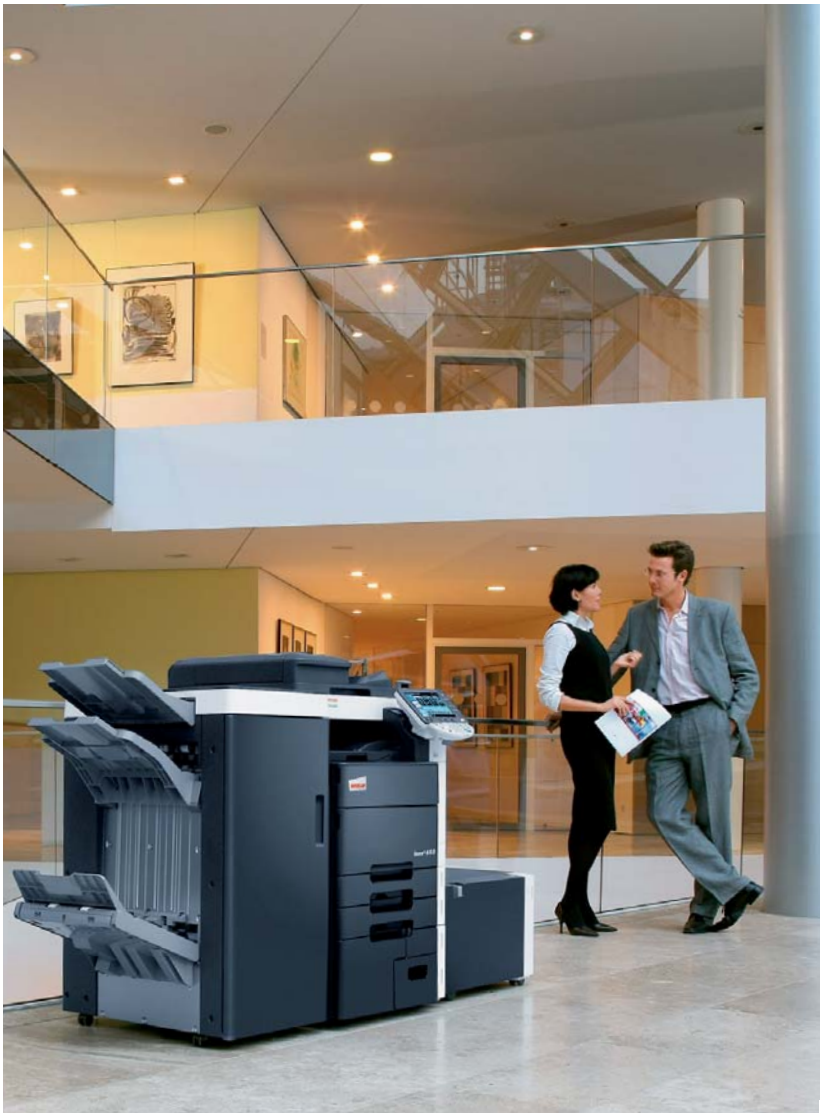
- **Biometrical authentication:**
  This method makes use of the pattern of the veins on your finger. An ineo machine equipped with an optional finger-vein scanner identifies you as the one and only person authorised to access your documents and specific functions. Since your vein pattern is unique, this method is absolutely safe. No need to remember your password, no need to carry an access card. Nothing could be easier – and safer.

DEVELOP not only ensures confidential documents stay that way, it also offers user-friendly solutions to the data security problem.

* optional for: ineo 501/601/751

Data security – any place, any time

Password-protected access to documents
In modern-day offices most workplaces have remote access to a digital office machine used by several employees. The advantage is you can print documents on the departmental printer from your workplace, for example. The disadvantage is that other users may remove your printed document before you get to the printer. Here, DEVELOP offers a simple but effective solution: password-protected access to documents on an ineo machine. So you can print or scan a document from your workstation and protect the document by means of your own PIN to prevent unauthorised access.



Data deletion guaranteed

Format/erase HDs on ineo office systems
Deleting data from a hard disk is actually more difficult than many people think. The good thing is that accidentally deleted data, e.g. on your PC, have not actually gone for good. Experts can recover such data with relative ease.

Unfortunately, the same is true of the hard disks in digital office machines. If the data are not deleted professionally, anybody can recover them after the machine is sold or returned at the end of a leasing contract. If the data are sensitive, their theft may well prove harmful to your organisation. At DEVELOP we ensure that the data on your hard disk are permanently protected from unauthorised access. In the case of documents stored on an optional hard disk, the data are automatically deleted. All ineo systems offer up to eight different write-over modes during sanitizing that ensure 100% data deletion. As an additional protection DEVELOP offers the feature of encryption with the optional Security Chip. This ensures that even if data are recovered, they cannot be read by anybody else – because the correct encryption code has to be entered to decode the data.

Preventing data abuse

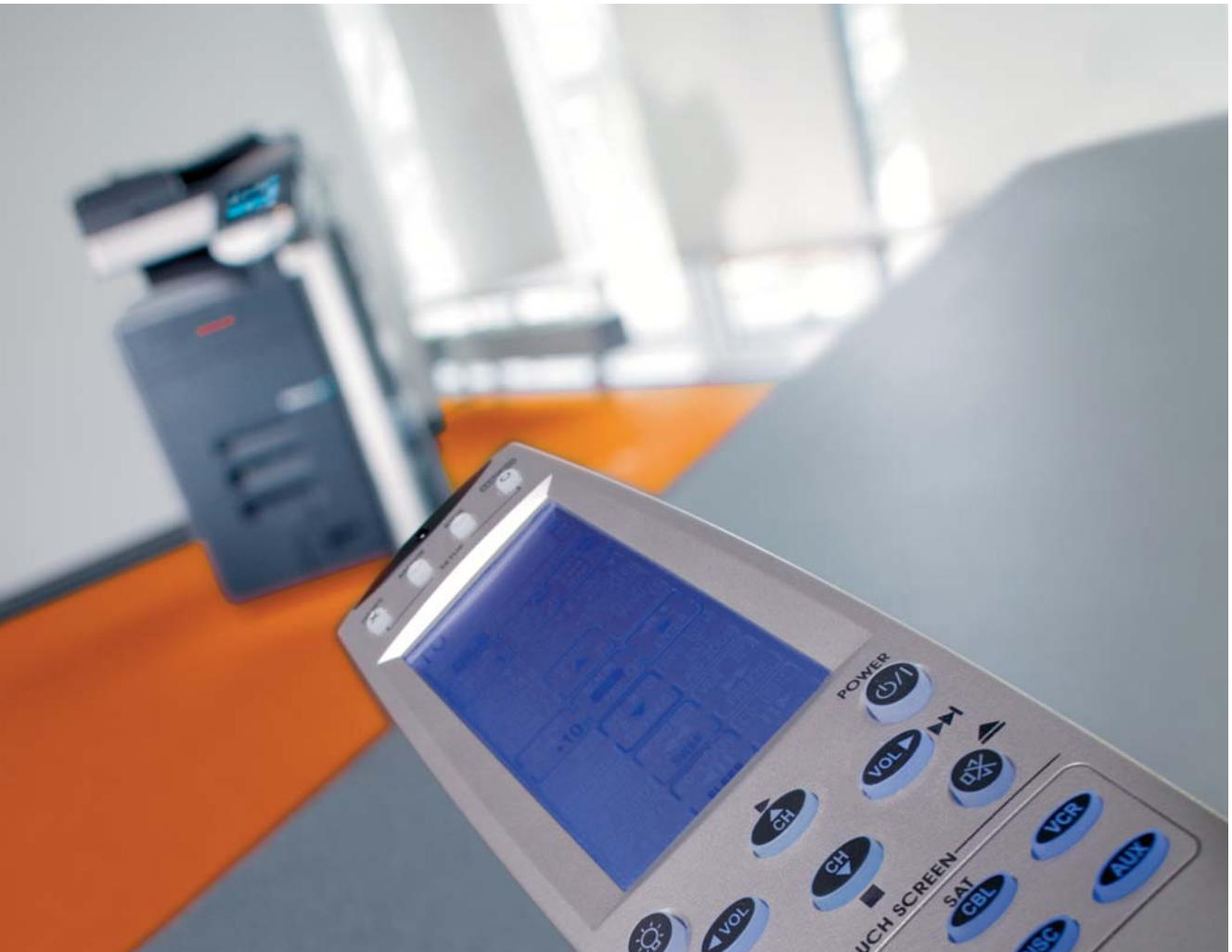
Bypassing HDs when printing

Most digital office machines are accessible to a number of users. That means that at busy times your print job may be placed on hold until it is your turn. This not only results in delays but also means that your document data are stored on the system's hard disk while waiting to be printed. If you want to prevent confidential data from reaching the hard disk, you can have your document printed via the system's RAM, which ensures automatic deletion after printing has been completed. Any abuse of your data is impossible. Password-protected documents can also be automatically deleted after a pre-determined period of time – another reassuring feature of ineo machines that prevents data abuse.

Safe office networks

Network security

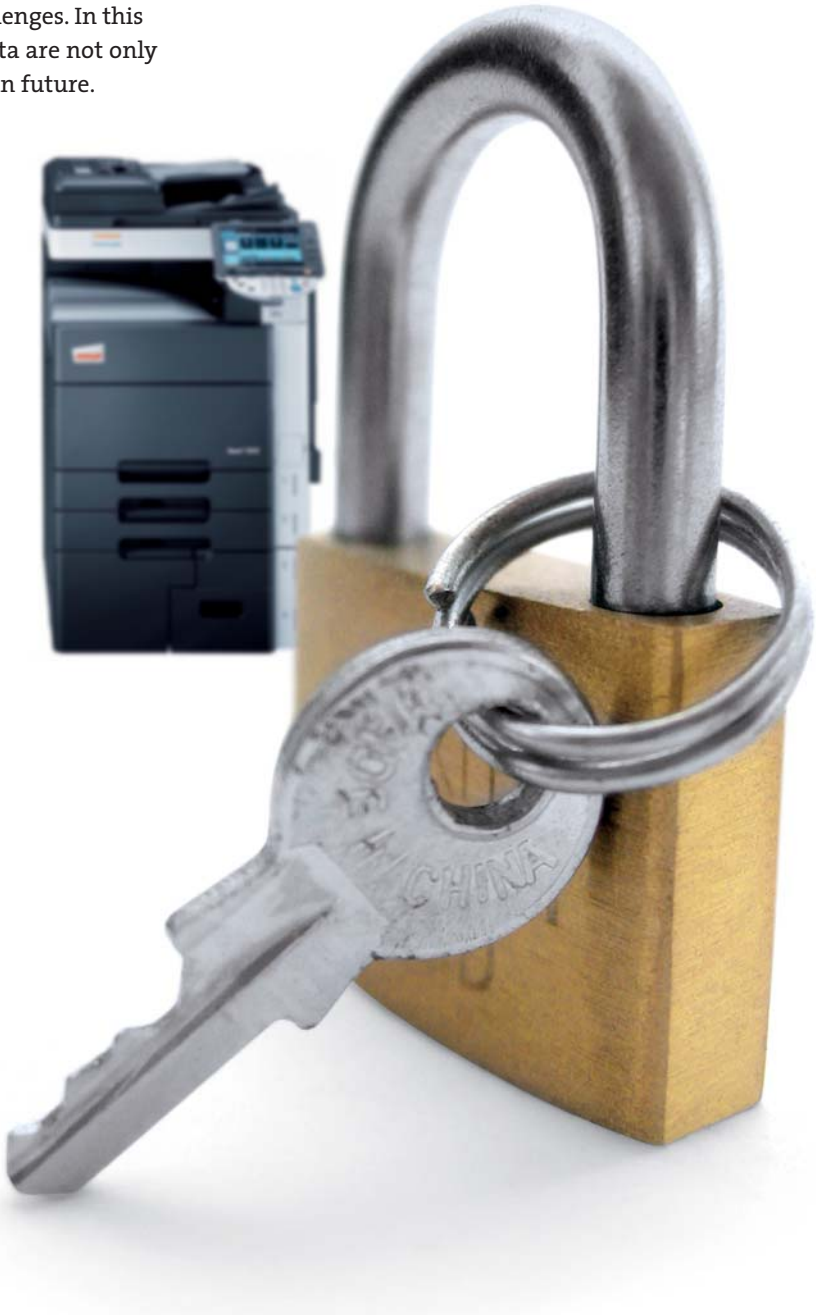
An ineo office machine is an integral part of an office network – and as any network administrator will tell you, a network is only as strong as its weakest link. At Develop we have taken great care to ensure that no ineo machine needs to be the weakest link. Today's ineo machines have a built-in security function that provides reliable data protection. Working with the IP filter, this security function offers safe logging and port access control, relying on the commonly used SSL encryption method. This provides an effective defence against hacker attacks – so your ineo office system can be made as safe as any networked PC.



Safe data – now and in future

DEVELOP uses state-of-the-art technology and reliable standards to protect your organisation from data thieves, financial loss or immaterial damage. Whatever your specific concern – network security, confidential documents or data theft – we ensure you don't need to worry about data security any more because ineo office machines offer the highest possible level of security to any organisation in the private or public sector.

But we are by no means resting on our laurels. True to our name, we are constantly developing the data security functions featured in our ineo machines to meet any future challenges. In this way, you can be sure that your data are not only safe right now, but also stay safe in future.



Overview

	ineo 223 ineo 283	ineo 363 ineo 423	ineo 501	ineo 601 ineo 751	ineo+35	ineo+220 ineo+280 ineo+360	ineo+452 ineo+552 ineo+652 ineo+652DS
Access Control							
Copy/print accounting	●	●	●	●	●	●	●
Function restriction (copy/print/scan/fax/box)	●	●	●	●	●	●	●
Secure printing (lock job)	○	●	●	○	●	●	●
User box password protection	○	●	●	○	—	●	●
User authentification (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	●	●	●	—	●	●	●
Scanning							
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	○	●	○	—	—	●	●
ISO 15408							
EAL 3 certified	●	●	●	●	●*	●	●

● = standard ○ = optional — = not available

*** expected in autumn 2010**

Please contact your dealer for further information.

Your Develop Partner:

Since changes in technical features are the order of the day in the world of digital copiers and printing technology, please note that the technical data provided in this material was issued in August 2010. We reserve the right to make changes to the technical design. Specifications refer to maximum performance under standard conditions and are only valid for the systems listed in the above overview. No guarantee is provided in relation to any of the data supplied.

Your Develop Marketing

August 2010