

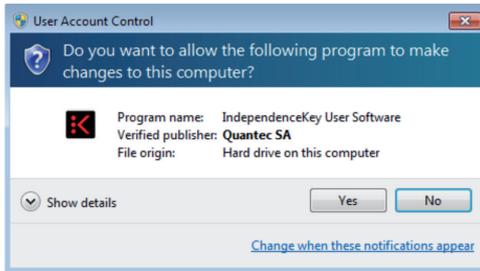
INDEPENDENCEKEY
User manual



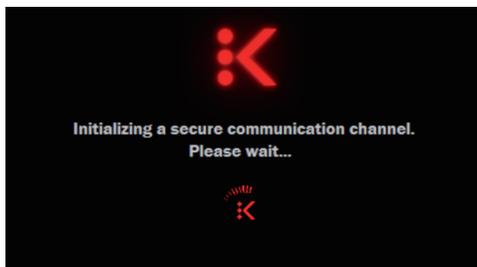
INDEX

Installation and Initialization	04
How to Use IndependenceKey to Make Your Data Safe	06
Initial Settings	07
How to Encrypt – Open – Modify – Decrypt a File	08
• How to Encrypt a Directory	09
QDisk: How to Create an Encrypted Disk	10
Safe Cloud Storage with IndependenceKey	12
Association with Other Users	14
• Remote Association	14
• Physical Association	16
Safe Information Sharing	18
How to Use the USB Host Port	20
• How to Make an Encrypted Backup on External Supports	20
How to Use the Security Cap	22
How to Use the Data Bank	27
Keylogger and Master Password	28
Programs and Authorizations	29
How to Remove IndependenceKey	31
Reset and Migration	32
Technical Support and Assistance	33
Troubleshooting	34
Technical Appendix	38
Software Licence Terms and Conditions	40
Hardware Guarantee	42
Privacy Terms	44

- 01 Download the setup program last version from the IndependenceKey site at the following address: <http://www.independencekey.com/download> in order to download the software, it is necessary to have the authorization code which is either printed on the instruction sheet inside the IndependenceKey box or which you have received via email.
- 02 Install the software (the administrator rights are needed) and accept any request of authorization from antivirus and/or firewall applications operating on your computer, or manually enable IndependenceKey software in the above mentioned applications after the installation. The IndependenceKey software is digitally signed with a certificate issued by a Certification Authority. This states that the software produced by Quantec SA is genuine. For Windows XP users, read the technical appendix at the end of this manual before proceeding.



- 03 Once you have installed the software, you don't need to restart the computer, plug the Security Cap in your IndependenceKey and then plug your IndependenceKey in your computer.
- 04 Windows will look for the driver already installed to connect it to the device. This operation may take one or more minutes and is carried out only once.
- 05 The following screen will appear:



indicating that your IndependenceKey has been recognized by your computer and that the communication channel between the computer and the device is being ciphered.

TECHNICAL ASPECTS

What is IndependenceKey made of?

IndependenceKey is a high-integration device. It is the smallest portable cryptographic device in the world that can reach and exceed 100 cryptographic Mbps in real time. Equipped with a USB host port, it can fulfil numerous applications. It is made of an aluminium alloy and the outer coat is treated with a special treatment named PVD, entirely non-toxic and nickel-free.

What happens during the initialization?

Both inside IndependenceKey and inside its Security Cap there is a cryptographic authentication chip from the TPM (Trusted Platform Module) safety platform. Thanks to these chips and to the high-performance hardware cryptographic engines housed in both devices, IndependenceKey and its Security Cap create an unbreakable mutual association during the association phase, making all the necessary anti-cloning checks, encrypting the communication channel and memorizing specific combinatorial secrets derived from the Master Password.

Where is the Master Password memorized?

The Master Password is never memorized anywhere but a series of combinatorial secrets is derived from it, partly residig inside IndependenceKey and partly memorized in the Security Cap. Neither device can individually access the cryptographic database inside containing all the IndependenceKey data. Only the person who knows the Master Password can complete part of these secrets by unlocking one of them.

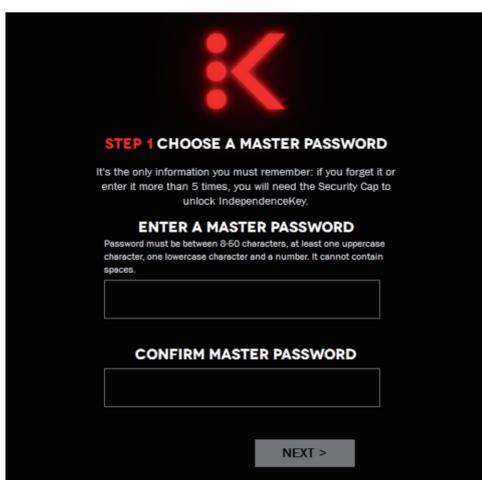
What if I forget the Master Password?

Just connect your IndependenceKey to its Security Cap and together they will unlock the cryptographic database because they have the necessary secrets to do it. Now you can change your Master Password as you wish.

What is the Alias?

The Alias is the device digital print. It is an alphanumeric code derived both from the cryptographic chip Serial Number and the manufacture's combinatorial secrets. Thus, it can neither be modified nor cloned. Once you have activated your IndependenceKey, the Alias accompanies the user during the device entire lifespan also in case of upgrade to further versions.

06 After a few seconds, the IndependenceKey initialization procedure will start:



07 Follow the video instructions by typing in a Master Password of at least 8 characters containing at least one capital letter, one small letter and a number (the software will check its congruity). Once you have confirmed your Master Password, type in your Nickname which will be useful for your further associations with other users.

Make a note of the ALIAS of your IndependenceKey which appears under the Nickname. **This code is the exclusive ID of your product and can be neither modified nor cloned.** This is the code that you will have to give to other users if you want to create an association via Internet (see the chapter dedicated to the association procedure).

The product initialization has to be carried out only once and takes nearly a minute, just the time for both devices to make the authenticity and anti-cloning checks, to encrypt the communication channel and create the main database which will contain the cryptographic keys and the Password Manager data.

You will find a detailed description of what happens during this phase in the chart aside.

At the end of the initialization, when the message indicating that the procedure has been completed appears, remove the Security Cap, even leaving your IndependenceKey plugged in, and keep it in a safe place. IndependenceKey is ready for use.

TECHNICAL ASPECTS

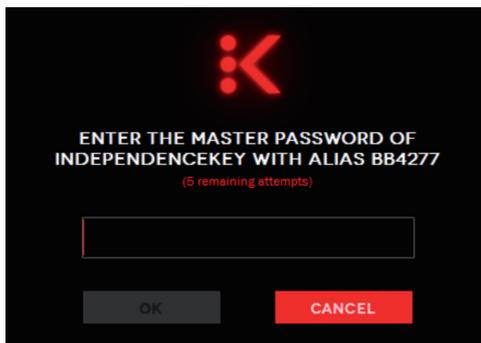
NOTE: IndependenceKey does not work if the Security Cap is plugged in as this is the safety and backup device which is to be kept in a safe place, far away from your IndependenceKey.



How to Use IndependenceKey to Make Your Data Safe

TECHNICAL ASPECTS

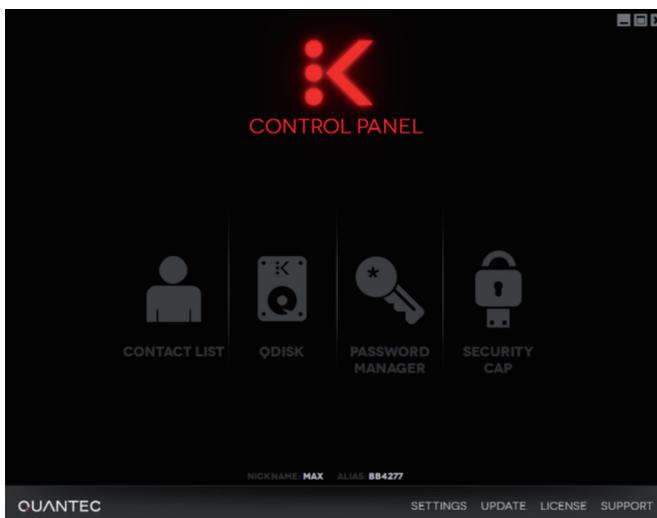
 IndependenceKey is very easy to use. After plugging it in your computer, just unlock it before use. This can be done in two ways: by typing in your Master Password or plugging in it the Security Cap with which your IndependenceKey has been initialized. This second procedure is useful in case you didn't want to type your Master Password for any special reason.



Once your IndependenceKey has been unlocked, the “K” icon on the bottom right of the System Tray Bar changes from “grey” to “red”. If this icon is not visible, click on the triangle-shaped Windows key “▲” to widen the list of icons.



In order to open the main interface, just double click on the “K”-shaped icon.



What happens when IndependenceKey is plugged in a PC?

Every time IndependenceKey is plugged in a computer, it starts a new copy of its own operative system, identical to the original one, that is to say that it starts from a known and predetermined condition in order to maximise the device safety levels.

What type of cryptography does IndependenceKey use?

IndependenceKey is equipped with a hardware accelerated cryptographic engine that can reach very high performance levels with the most modern cryptographic standards such as 3DES, AES256, AES-XTS, AES-GCM. By using AES, Quantec has developed from this engine a further cryptographic engine, characterized by “ mobile windows “ , that **can adapt dynamically to any type of data to be protected**, be it a file, a disk, a VoIP stream.

How is the cryptographic key created and where is it located?

The cryptographic keys are created inside the device by a cryptographic chip from the TPM safety platform expressly dedicated to this task. These keys are unique, universal and cannot be replicated but, most of all, **these cryptographic keys never leave the device!** This is a unique and extremely important feature of IndependenceKey.

What type of files can I protect? Which size must they be?

IndependenceKey has no limitations about the size of the file or information to be encrypted. It can work with files, folders, disks, as well as with VoIP stream and high definition A/V streams in real time.

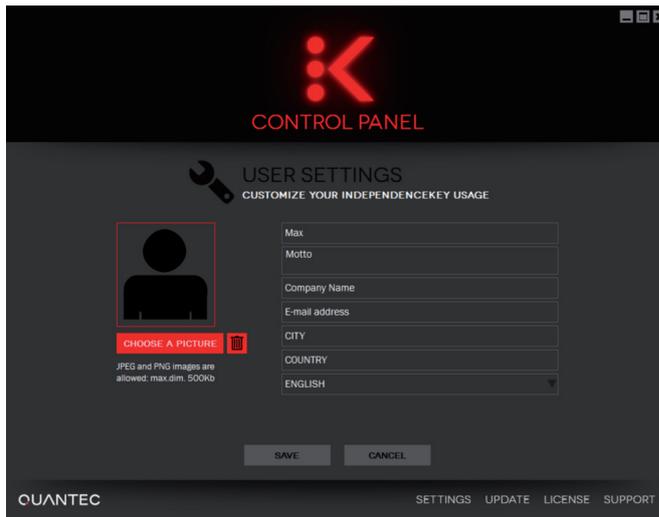
What is the device encryption speed?

IndependenceKey reaches and goes beyond the cryptographic speed of 100 Mbps in real time. The next versions will exceed 150-160 Mbps in real time. These values make IndependenceKey so effective and efficient that, once it has been connected to the computer, there is no difference with the usual working habits.

How does IndependenceKey communicate with the computer?

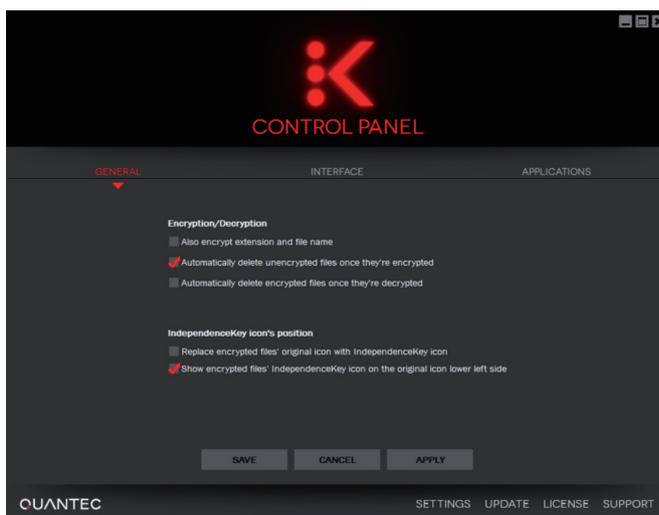
When you plug your IndependenceKey in your computer, the device starts operating and the communication channel protection is immediately activated between the device and the computer. This is done by using the most modern PKI cryptographic techniques (public-private key). **The entire communication channel is encrypted**, also on the computer side, but the most significant thing is that IndependenceKey uses the cryptographic keys only inside itself, without ever letting them out. This maximises its safety level at the best. Besides, IndependenceKey is like an NIC interface to the computer where it is plugged in. This will allow the IndependenceKey users to have advanced VPN hardware services.

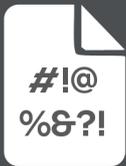
 In order to modify the settings of the program relevant to you user profile, preferred language, etc., just click on "Settings" and select the "Edit your Profile" option. From here you can change the interface language choosing among the ones available.



By clicking on the "Preferences" option, you can adjust your IndependenceKey behaviour according to your needs; for example, you can scramble file names when they are encrypted or keep an unencrypted copy of the encrypted file and use the other available options as you wish.

IndependenceKey can automatically and permanently wipe the original files once they have been encrypted. Due to its ability to operate directly on encrypted files without leaving any trace, it is advisable to proceed keeping this option always enabled.

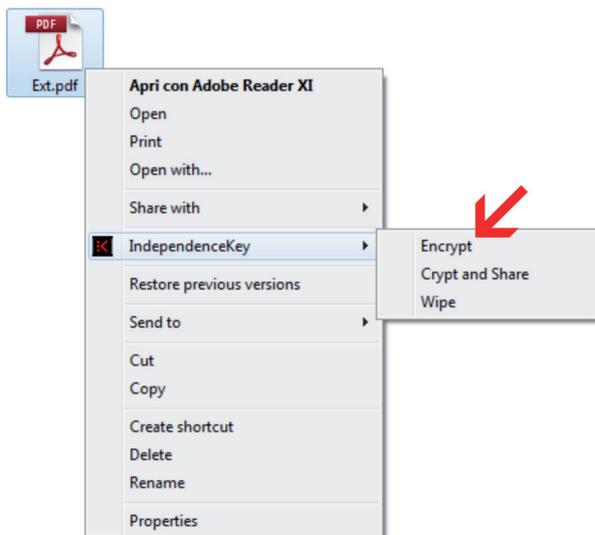




How to Encrypt, Open, Modify, Decrypt a File

HOW TO ENCRYPT A FILE

You just need to right click on the file you want to encrypt.



Then select "IndependenceKey" -> "Encrypt". This operation will enable you to encrypt your files. The progress of the procedure can be visualized through the "Encryption Crate" option from the IndependenceKey interface ("Settings" menu -> "Encryption Crate"):



TECHNICAL ASPECTS

When an encrypted file is opened, are any unencrypted copies made?

Absolutely NOT! Unlike all other software cryptographic systems but not only these, high level applications (Microsoft Word, Excel, Power Point and any type of application that can be executed on a computer including CAD/CAM and RAD systems, authoring environments, etc..) **work directly on the encrypted data; these files will never have an unencrypted copy anywhere.** IndependenceKey decrypts and encrypts in real time the data required by the application respectively when it reads and writes in the computer storage memory on the encrypted file itself. Everything happens in real time in the application memory.

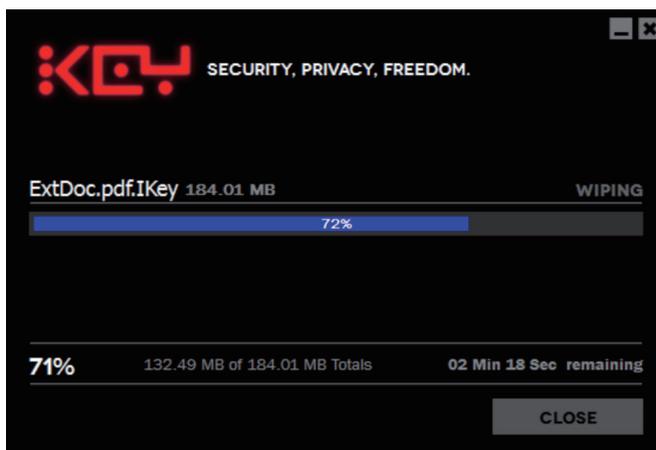
Even the temporary files created by Microsoft Office applications are encrypted and there is no trace of them in the computer storage memory. This remarkably improves safety levels, together with the fact that the secrets necessary to access encrypted files reside only and exclusively inside your IndependenceKey.

How does it work?

IndependenceKey operates under the operative system file system, that is between this one and the storage devices recognized by one's computer, be these disks, devices, USB devices, network disks, NAS and on-line Cloud storage systems.

Thanks to specific drivers at kernel level, every time an application requires access to an encrypted file or disk, if authorized, IndependenceKey decrypts and encrypts in real time the data buffers (parts of a file) that the application requires while it is working. The applications believe they are always and exclusively working on unencrypted files but, in fact, they are working on encrypted files with no need for modification or update: **any application installed on the computer, even if old-fashioned, can directly and safely work on its files.** The files are never decrypted anywhere.

If you select the automatic cancellation option for the files being encrypted, IndependenceKey will carry out a complete wiping of the file unencrypted version.



HOW TO OPEN OR MODIFY A FILE

In order to open an encrypted file with IndependenceKey, it is necessary for it to be plugged in your computer and unlocked. **The file DOES NOT NEED to be decrypted first, just double click on the file to open it.** You can work on your file, make modifications as usual without changing your working habits and going on using the same tools you have always used. **The file will open automatically with the application related to it** (for example, a “.docx” file will open with Microsoft Word, Wordpad or with the text editor installed on your computer) **and you can work directly on your encrypted file.** When you close an application, IndependenceKey records the modifications made and automatically updates the encrypted file.

No unencrypted copies of the file will be created in your computer: the application used works directly on the encrypted file thanks to IndependenceKey.

DECRYPT

In order to decrypt a file, you just need to right click on one or more encrypted files and select the “IndependenceKey” option -> “Decrypt”. The files will be automatically decrypted.

HOW TO ENCRYPT A DIRECTORY

Just as you can encrypt one or more files, the same applies to an entire directory. Just right click on the directory and select the “IndependenceKey” option -> “Encrypt”. The entire content will be automatically encrypted. Should it contain other directories with other files, these will in turn be automatically encrypted.

WARNING: If you add an unencrypted file inside an encrypted directory, the file will not be automatically encrypted because the “Encrypt” function encrypts files only when it is executed.

In order to have the content of a directory always encrypted, even though some unencrypted files are added at a later stage, it is better to use the IndependenceKey encrypted disks (see the chapter dedicated to the QDisk service).

More in detail

IndependenceKey can access encrypted files and disks following the high level application requests. For example, if you open an encrypted video file reproducing it with Windows Media Player or another multimedia software and you execute the “seek”, that is the forward search, skipping from a position to another along the A/V file, **IndependenceKey follows the application requests, accessing dynamically the encrypted file and aligning itself in real time to the closest cryptographic input** and then starting to decrypt what required. The algorithm developed by Quantec, based on the AES 256, **dynamically adapts these inputs on the basis of the type of file.** This improves the random access times to protected files and disks and optimizes their synchronization during the update on Cloud storage systems or company servers, **transferring only the strictly necessary modifications** (reduction of the data transferred, of the band and of the necessary time).

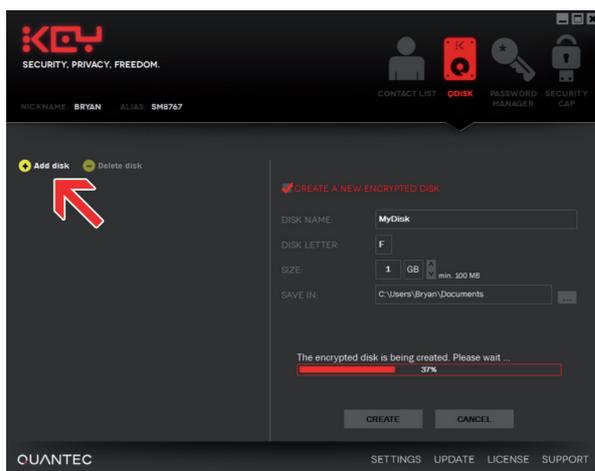


QDisk: How to Create an Encrypted Disk

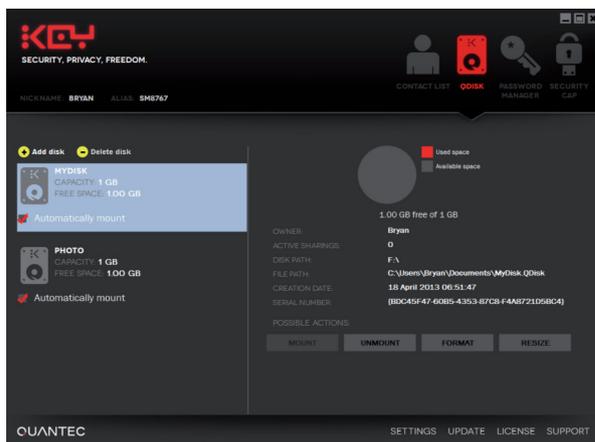
TECHNICAL ASPECTS

In order to create an encrypted disk, open the user interface and click on the QDisk icon.

Then select the “Add Disk” option and fill in the gaps opening on the right of the interface as you wish, choosing a preferential letter for the disk with which IndependenceKey will try to mount it onto the local system if available (if not, IndependenceKey will use the first letter available).



After clicking on “Create”, at the end of the procedure the disk will be created and it will appear in Windows as a common disk, just as you plug any USB storage device in a computer USB port.



Now the disk is ready for use and you can use it as any other disk : you can either copy files, create folders, move files, rename them, etc.

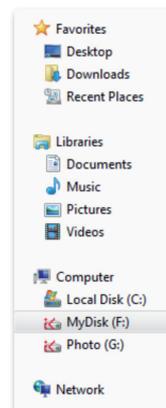
If you want to use a protected disk already created with IndependenceKey, you need to mount it. This can be done through the QDisk interface or by simply **double clicking on the encrypted image file that contains the disk (this file contains the disk entire structure and it is accessible through Windows Explorer. For any further information, please refer to the technical notes aside)**. The disk has also the extremely useful “Automount” option that, if enabled, allows the user to mount it automatically after typing one’s Master Password, that is after unlocking one’s IndependenceKey. This a very useful option in order to make procedures automatic when accessing one’s own encrypted files.

How does a disk encrypted with IndependenceKey work?

A disk is organized on the basis of data filing blocks, named “clusters”. The computer file system organizes and manages these storage areas on behalf of the operative system, automatically and invisibly to the user as well as to the applications. Inside the disk image file also named “file container”, IndependenceKey creates and manages the disk physical architecture, that is the indexing and management of the clusters. There are several types of clusters, some of them gather data about the file structure, others about the directories, others contain the real data also of more files, and so on, as it happens with any storage device. **IndependenceKey works directly and in real time on the clusters and in a totally encrypted way.** As it happens with the files and with the applications installed on a computer, (see chapters above), in this case the file system of the **operative system has direct access to the encrypted clusters without realizing that it is working on encrypted clusters!** IndependenceKey places itself in the middle and makes the entire process completely automatic and crystal clear to the operative system.

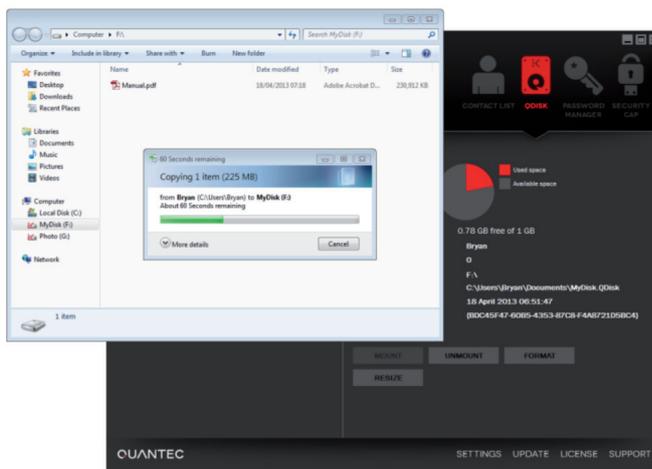
What size can the disk be?

The disk has no limitations of space. During the creation or the downsizing phase, it is possible to define its maximum size (of course it has to be lower than the free space available on the real disk that hosts it). It is not possible to reduce the size of a disk which already contains data if the new size chosen is lower than the size of all the data saved on it. In this case, it is necessary to create the required space by wiping some files.



TECHNICAL ASPECTS

The disk content is totally hardware encrypted thanks to IndependenceKey and without it no-one can access it. As for any storage device, IndependenceKey must not be removed while operating on the disk, otherwise the files on which you are working may be corrupted. The IndependenceKey engine QDisk shows the disk operativeness through Windows Explorer standard advance progress bars:



For example, when the progress bar reaches 100% during the copying of a file, the relevant window closes, meaning that the disk has ended its job and the file has been completely copied and encrypted.

Should you, by any chance, unmount a disk while a file is being copied inside it, IndependenceKey will first end the operation and then unmount the disk automatically. In this case, the information appears with a balloon hint on the system tray bar on the bottom right.

The IndependenceKey QDisks can be downsized, defragmented and repaired, exactly as any other real disk, only through the program main interface. If you want to downsize a disk by reducing its dimensions and also need to defragment it, IndependenceKey will carry out the entire procedure automatically. This operation may be quite long as the disk clusters are completely encrypted.

In the future, IndependenceKey will also be able to support variable-sized disks that adapt their dimension on the basis of the files and folders saved therein. In order to use them on Cloud systems, the use of fixed size disks is recommended. This way, IndependenceKey can optimize the “cluster chain” every time you work on the disks and the third parties synchronization services (i.e. Dropbox, Google Drive, Power Folder, etc..) can operate effectively, synchronizing only the modifications made time by time. The same can be said for variable size disks but their effectiveness is lower.

It is worth remembering that, **when you remove your IndependenceKey, the system unmounts all the active disks automatically.** The effect is that the disks disappear from Windows Explorer. Although this operation is possible, always carry out a “Safe Remove” of your IndependenceKey (see specific chapter) before extracting it or before unmounting a disk. If disks are not active, it is always possible to remove your IndependenceKey without making a safe removal. On the contrary, if the device is forcibly removed while a file is being copied or a program is saving some data onto a protected disk, the files may turn out to be corrupted while writing them, just as it happens with any other removable storage device. Therefore, **always remember to make a safe removal of your IndependenceKey or unmount the disks before removing it.**

What will be of the disk if I remove IndependenceKey?

The protected disks, regardless of their content, are organized and managed by IndependenceKey through “file containers”, that is “image files” containing the entire structure of the clusters that form the various disks. These files are **QDisk files** and contain a totally encrypted image of every disk. Every disk corresponds to a file container.

Once IndependenceKey has been unplugged from the computer, only these totally encrypted files will remain on the storage device where there are the QDisk image files (the computer main disk, a network disk, a NAS, a Cloud storage system, etc..). For example, if you create a 10 GByte disk named “My Disk”, on your computer desktop, there will be a 10 GB file in “C:\Users\User.Company\Desktop” named “My Disk.QDisk”. The same can be said if the disk is created in the Dropbox folder or anywhere else where you have access to.



Safe Cloud Storage with IndependenceKey

TECHNICAL ASPECTS



I file possono essere criptati e copiati in qualunque spazio Cloud. The files can be encrypted and copied in any Cloud system. In order to access encrypted files, just double click on them as if they were not encrypted and leave the rest to IndependenceKey. In order to open the protected files and/or disks uploaded on the Cloud it is necessary for the IndependenceKey software to be installed.

Thanks to IndependenceKey, you will be able to access your Cloud storage area, open the documents and work on them without leaving any trace. It is always possible to scramble file names too. This way, not only the content of a single file but also its name will be completely incomprehensible. Just plug in your IndependenceKey and you will be able to visualise the file real name.

HOW TO SYNCHRONIZE FILES AND DISKS IN DROPBOX

Cloud storage systems like Dropbox, Power Folder and others, make on their servers a differential copy of the files which the user uploads in his/her on-line storage area. **IndependenceKey protects the content of these files** thanks to an advanced and intelligent use of cryptography, **at the same time allowing the user to continue working on one's files without changing one's working habits.**

First of all, it is necessary to have a Cloud storage area of one's own. Dropbox, for example, offers up to 2 GByte for free. Follow the procedures indicated by the supplier's software to create your Cloud storage area. Once you have created it, your Cloud area is generally accessible through Windows Explorer in the shape of a folder, preferred link or disk. In order to use your Cloud safely, just upload your encrypted files or encrypt the already existing unencrypted files by right clicking on them with the mouse right button and selecting the "IndependenceKey" option -> "Encrypt".

The same applies to the disks protected with IndependenceKey. Just create your encrypted QDisks inside your Cloud area or transfer into it the already existing ones, always paying attention to the storage area size available according to your contract. It is worth reminding that moving a QDisk means unmounting it first ("unmount" option from the user interface, QDisk section), which means that it must not be in use. The shift can be made as usual by clicking on CTRL+X and CTRL+V or by Drag & Drop choosing the "Move here" option.

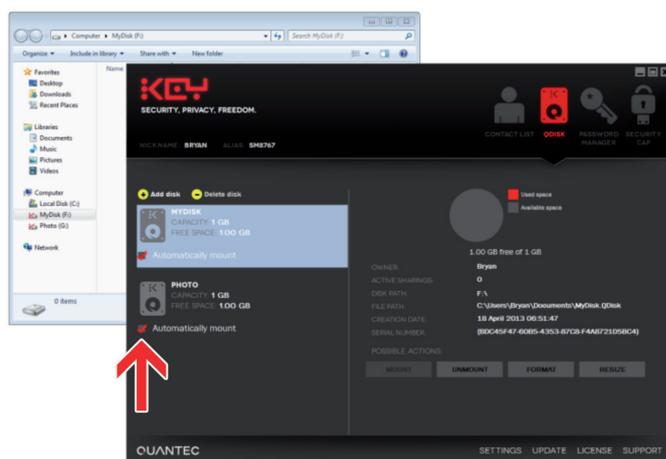
Once the disk has been created or shifted within the Cloud storage area, just double click on the QDisk file to mount it. It is also possible to use the "Automount" option so that the disk will be automatically opened and mounted every time you plug your IndependenceKey in the computer and you unlock it with your Master Password. The "Automount" option is available through the user interface, in the QDisk section, in the disk properties.

What is the Cloud Storage?

It is an on-line system for filing and accessing one's data, requiring the presence of an Internet connection. The user can memorize one's data in one's Cloud storage area to be able to access it at any time, sometimes even with a web browser, even from more than one computer or device in order to have an ever updated backup copy. Some Cloud storage services also offer the file versioning that is they incrementally memorize the different modifications of the files allowing the user to recover the previous versions of one's files and documents within the storage limits purchased. The most famous and most functional of them is Dropbox, but there are also others such as Power Folder, etc..

How does it work?

As for Dropbox, an area managed and monitored by the Cloud storage service is created in the user computer: every time a file is put in this area, or a directory is created, or a file is renamed or similar, the underlying system synchronizes the differences on the provider's server making the updated file available to all the computer synchronized with the user account. The synchronization generally takes place when a single modified file is released by the application. .



What is the role of IndependenceKey?

IndependenceKey makes the content of the files and disks hosted in the Cloud storage provider's servers totally inaccessible. Most of all, thanks to its variable blocks adaptive cryptographic engine, it grants absolute secrecy in AES 256 and, at the same time, the possibility **to incrementally update these files and disks**. When a file is encrypted, given an "X" cryptographic key, this becomes completely different from its original, that is it is turned into a sequence of high entropy bits (chaotic), substantially with no sense. The cryptographic process that leads to the generation of this sequence is, by its own nature, a chained type process, that is, it works by sequential blocks. The block in position 1 influences the cryptography of the block in the following "n" position. This is the reason why, if the content of the first block changes, with the same cryptographic key ("X" in the example), the entire bitstream is completely different from the previous one. Now think of a large-sized file, or of a database, or better of a protected QDisk image (file container): if we worked only in "chained" mode, adding only a small document to the disk, the cryptographic process would modify the entire bitstream from the cluster in which it has been added, making the Cloud synchronization of the disk practically impossible. For example, if the disk were 1 GByte and only 100 kBytes of data were added at the beginning, the entire bitstream forming the disk would change. Here lies the difference with IndependenceKey: **its cryptographic engine only modifies the necessary blocks and the neighbouring ones**, keeping the cryptographic integrity inside the file. When the files is released by the application (for example, you close Word in case of a single file or you unmount a QDisk), the differential synchronization service of the Cloud storage area provider only detects the small differences and, therefore, carries out the synchronization rapidly . Also the synchronization of the files protected by IndependenceKey and stored on the Cloud takes advantage of this when the access rights to the files (share) are modified. If a user wants to enable another user to open an encrypted file which has already been stored on a common space on the Cloud in order to be shared, just like on a company server, NAS and so on , just wait a few seconds and the authorization will be automatically extended to all the service subscribers.

Cloud storage services like Dropbox make a differential copy of the files contained in the Cloud storage area and save it in their servers. When an encrypted file is updated or you work on a protected disk, the relevant modifications are applied to the data structure and they are automatically transferred by the Cloud storage service as the file is released by the application with which you have worked on it (for example, Microsoft Word will be closed after saving your job on a document). In order to carry it out with disks as well, you need to unmount them.

Going back to the example, if you create a 2 GByte protected disk within Dropbox and work on it, during its use 10 MBytes of data will be copied in this disk and once it has been unmounted, Dropbox will synchronize it by sending a little more than 10 Mbytes of data to its servers, completely encrypted. By plugging your IndependenceKey in another computer synchronized with the same Dropbox account and mounting the disk, this last will appear among the computer local sources with the added data exactly as they had been left. **The files and the disks are now completely encrypted and protected by your IndependenceKey**. Now you can use your Cloud storage area safely, at last.



Association with Other Users

TECHNICAL ASPECTS

 IndependenceKey can be associated with other IndependenceKeys. Associating two IndependenceKeys means enabling two users to share files safely as well as open and modify them without any worry. Some additional services will be available in the future such as the possibility to make VoIP phone calls and exchange safe messages.

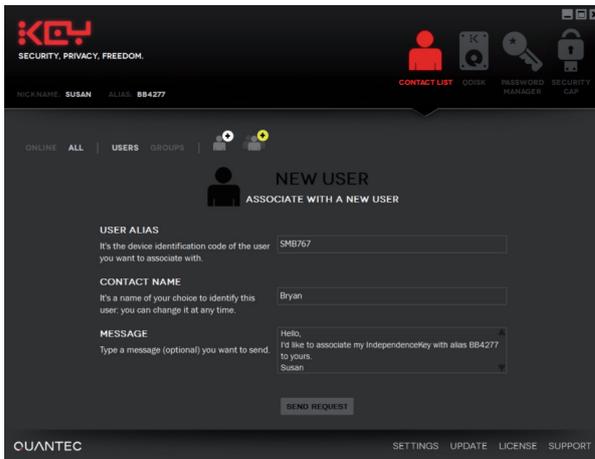
An association with another user does not mean granting him/her access to any protected file, disk or data. It only means that the other user can appear in your “Contact List” and you can choose, time by time, whether to share a file or not **The access authorizations to a file can be removed at any time only by the user who has created that file**, that is by the person who encrypted it the very first time.

The association operation can be carried out in two different ways :

REMOTE ASSOCIATION

The users have no chance to meet

Open the interface -> Select “Users” from the menu -> then select “Contact List” and, in order to add a user, click on the icon indicated in the picture below :



The screenshot shows the IndependenceKey user interface. At the top, there is a navigation bar with the logo and the slogan "SECURITY, PRIVACY, FREEDOM." Below the navigation bar, there are several icons: "CONTACT LIST", "DISK", "PASSWORD MANAGER", and "SECURITY CHIP". The main content area is titled "NEW USER" and "ASSOCIATE WITH A NEW USER". It contains three input fields: "USER ALIAS" with the value "SMB767", "CONTACT NAME" with the value "Bryan", and "MESSAGE" with the value "Hello, I'd like to associate my IndependenceKey with alias BB4277 to yours. Susan". A "SEND REQUEST" button is located at the bottom of the form. The footer of the interface includes the text "QUANTEC" and "SETTINGS UPDATE LICENSE SUPPORT".

A window will open. Now type in the Alias of the person you are looking for (for example, the user named Susan is trying to send a request for association to the user named Bryan who has already given his Alias to Susan).

The Alias is a univocal code that can be also derived from the cryptographic authentication chip serial number inside IndependenceKey and from the manufacturer’s combinatorial secrets. Each user has its own Alias which can be communicated to other users in order to activate a remote association. The Alias, together with the Nickname, is always visible in the user interface as it is positioned on the top left under the IndependenceKey logo.

How does the association process work?

The association between two users i.e. between two IndependenceKeys is a mathematic process based on cryptographic and authentication algorithms. IndependenceKey has both a cryptographic engine and a dedicated authentication cryptographic chip inside belonging to the TPM platform (Trusted Platform Module). Thanks to this chip and to its cryptographic engine, when two IndependenceKeys associates, first of all they check their originality. Only after this check they exchange the univocal secrets that enable them to recognize each other, set up safe communication channels and exchange reserved and protected files and information.

Is the remote association less safe than the physical one?

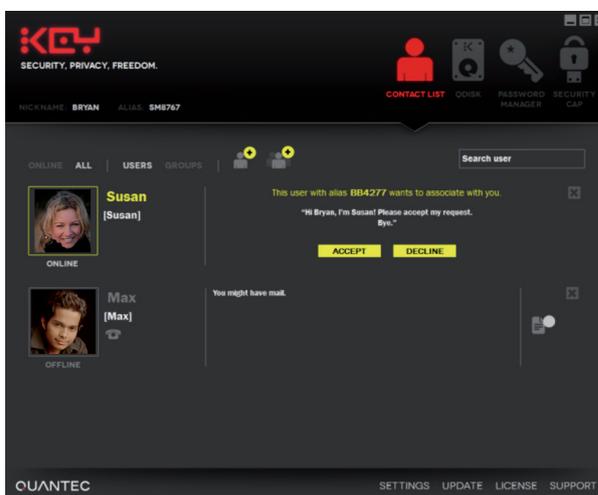
No, it isn't. IndependenceKey can associate with other IndependenceKeys both physically, thanks to their interconnection through the USB host port, and remotely via Internet. In both cases, the cryptographic authentication chips inside allow the two devices to set up a safe hardware communication, to make the necessary checks, to encrypt the communication channel and to generate as well as exchange the univocal combinatorial secrets necessary to complete the association.

TECHNICAL ASPECTS

The Alias can be communicated also publicly to the other person with whom we want to create an association as it is not part of sensitive data and should it be read by third parties, it couldn't be used to falsify an identity.

Once the Alias of the remote IndependenceKey with which we want to create an association has been typed in, it is possible to type the Nickname of the person with which we want to recognize the other person in our "contact list" and then type a brief text message. Then click on -> "Send" to send your request.

As soon as the other person is on-line with his/her IndependenceKey, he/she will receive your request for association by visualizing it thanks to his/her user interface :



What do Quantec servers do during the remote association?

Quantec makes available a communication packet relay service between two IndependenceKeys that replaces with the Internet the USB communication means used during the physical association. **Packets are materially encrypted in advance by each IndependenceKey and reach the servers that memorize them until the IndependenceKey to which you want to be associated with gets connected to the Internet. Quantec servers are not aware of the secrets that the two IndependenceKeys exchange,** but they only identify both devices thanks to their univocal ID which is the Alias. The servers aim is to allow two users to associate via Internet at any time, without them being on-line at the same time and without establishing a direct communication channel through the USB host back port.

Does associating mean giving a permanent access to all the protected files?

Absolutely not! Establishing an association with another user means generating the necessary combinatorial secrets in order to create, either at that moment or later, a real time safe communication session as well as safely share the files to which the user has given the authorization access thanks to the "Crypt & Share" function of IndependenceKey.

As soon as the addressee accepts the request, the sender (Susan, in the example) appears in his/her Contact List. The same applies to the sender's Contact List.

It is not necessary for both to be on-line at the same time. The operation can take place at different times, thanks to Quantec's servers. See the technical notes aside for further details.

It is also possible to create an association with infinite substantial number of users (several thousands) and it is always possible to cancel the associations that are no longer welcome. After cancelling an association with another user, it will be impossible for you to access the files which that user shared with you (but, of course, it is always possible to access the files which you decided to share with him/her, even though he/she has been cancelled from your Contact List).



Association with Other Users

PHYSICAL ASSOCIATION

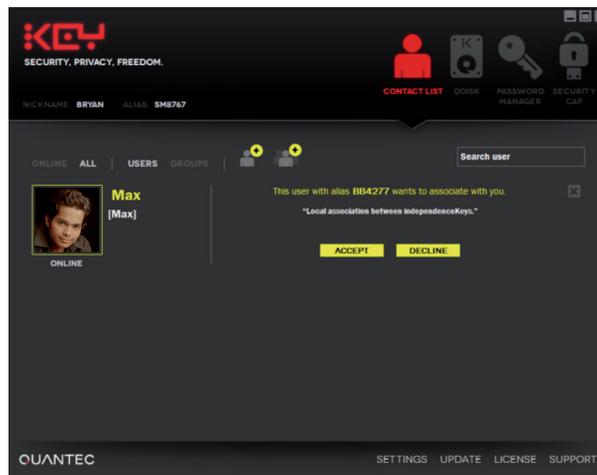
The users have the chance to meet

IndependenceKey can create a physical association with another IndependenceKey by plugging one IndependenceKey in the other's USB host port!

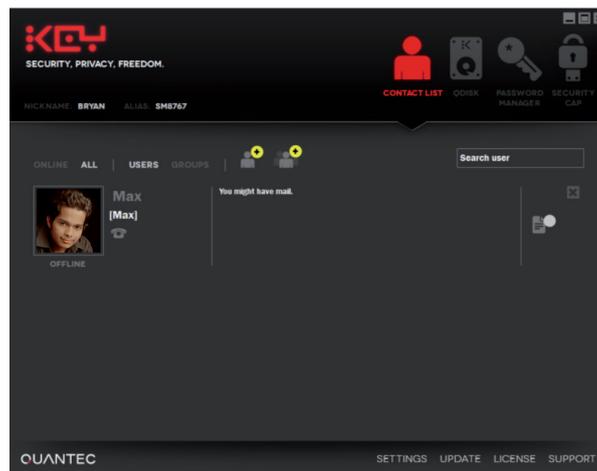


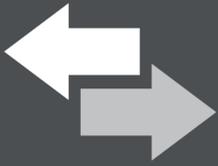
In order to create a physical association, plug your IndependenceKey in the computer and unlock it. Plug the IndependenceKey belonging to the person you want to create an association with in your IndependenceKey back port. After a few seconds, a window will appear on your computer asking for the Master Password of the IndependenceKey with which we want to associate, as the owner has to give his/her approval. If the Master Password is correct and the two IndependenceKeys haven't been already associated before, a box will appear on the screen of the computer asking for the authorization to proceed and, should the answer be positive, the procedure is finished.

In the example below, Bryan accepts the request for a local, physical connection made by Max who has plugged his IndependenceKey in Bryan's. The Master Password required by the system is the one of Max's IndependenceKey.



Now the two users appear in each other's Contact List and can start sharing files and communicating safely.





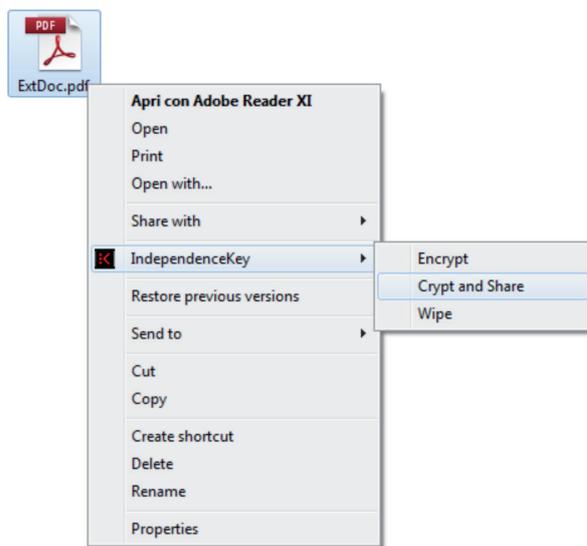
Safe Information Sharing

TECHNICAL ASPECTS

 From the moment you create an association with other users, it is possible to start sharing information, in particular files or group of files.

HOW TO SHARE A FILE

In order to share a file, right click on the file to open the related Windows menu and then select -> "IndependenceKey" -> then "Crypt & Share"



A screen indicating all the contacts in your Contact List will appear. Select the contacts you want to grant access to the file by clicking on them.



How can IndependenceKey regulate the access rights?

The files encrypted with IndependenceKey have their own structure of data, completely encrypted and specifically designed to allow the operative system to interact with them as with any other file in the computer. Every file protected with IndependenceKey is encrypted by Quantec's adaptive block algorithm by using the AES 256 and it contains several references to the file main data such as the file real name (we wish to remind our customers that, besides encrypting the files, they can always scramble their names with their IndependenceKey), the type of file, its dimensions etc. Among these elements there is the list of users that can access a single file. The users authorized to access a file are identified thanks to a univocal code generated during the association procedure. When a user tries to open a file encrypted with IndependenceKey, the system driver, installed on Windows thanks to the software supplied with IndependenceKey, has access to a small part of the file, decrypts it inside IndependenceKey and checks if the user knows the key with which the file has been encrypted. If the key is known, then the file is processed, that is opened, decrypted and sent to the application to which it refers. Otherwise, nothing happens. The cryptographic key is rebuilt starting from the combinatorial secrets of the association algorithm between users, secrets that are protected inside the IndependenceKey cryptographic chips. The procedure with which all this is carried out is entirely hardware based and is funded on the principle according to which the keys never leave IndependenceKey. This is the reason why any cryptographic, authentication and file integrity control operation takes place inside IndependenceKey. This solution not only allows a file to be decrypted but also to check its structural integrity.

IndependenceKey will automatically encrypt the file, if not already encrypted, and extend the access to the selected users. It is not necessary to encrypt files first and then extend the related access rights. **It is always possible to extend or deny the access rights to an already encrypted file.** The encrypted file can be safely sent by using the most common means, also the most unsafe ones like emails, Skype, file transfer sites or similar.

Thanks to IndependenceKey, it is not necessary to share any secret, password, cryptographic key or anything else. No longer access passwords sent by e-mail, SMS or read on the phone. The user who receives the file, has been given the authorization to access it and has his/her, IndependenceKey plugged in his/her computer and unlocked, has no need to decrypt the file. He/she only has to double click on the file in order to open and modify it. It is not necessary to change one's working habits : when you have finished working on the file, just save it as you are used to and IndependenceKey will automatically update the encrypted file.

IndependenceKey lets you always work directly on the encrypted file.

HOW TO SHARE MANY FILES

It is also possible to share many files and folders safely. For example, if you select 5 unencrypted files and you select the "Crypt & Share" option, these files will automatically be encrypted with a single operation. The IndependenceKey progress window will indicate the progress of each operation in real time.

If there is an already encrypted file among the selected ones, two windows will appear: the usual window asking the user to select the user/users with whom the 4 files to be encrypted are to be shared and an additional window specific for the already encrypted file. Actually, before modifying the access rights to already encrypted files, it is necessary to check with whom these files are already shared. This last operation can be made only by the user who has created the encrypted files.

HOW TO ADD/DENY ACCESS RIGHTS

An already encrypted and shared file can be further shared with new users by simply extending the access rights. Just repeat the above mentioned procedure, that is right click on the file -> "IndependenceKey" -> "Crypt & Share", without first decrypting the file.

Likewise, it is possible to remove the users from the access rights by following the same procedure.

OWNER USER OR RIGHTS OWNER

Only the user who has created the file can modify its access rights, which means that if user A creates an encrypted file and extends its access rights to users B and C, these last will neither be able to extend the file access rights to anyone nor remove one of the users : they will always have to refer to user A (the owner or file owner) to modify the sharing criteria.

In the future, IndependenceKey will also allow the user to open a file only in reading mode or to open it only for a certain number of times and to set an expiry date to the file beyond which no user will be able to open it except for the owner. (user A in the above example).

SYNCHRONISATION OF ENCRYPTED FILES AND RIGHTS

Following the same procedure above, the file owner can modify the rights at any time. It is worth remembering though that, if the file does not reside on a synchronised Cloud storage system (i.e. Dropbox or similar) or on a company server, the other users will always be able to open the previous versions of the encrypted files they have in their hands. From the synchronisation point of view, the use of a Cloud system makes the management of the access to protected sources more interactive and effective, mainly when several users have to access these data with different rights.

How to Use the USB Host Port

TECHNICAL ASPECTS

 IndependenceKey is equipped with a USB host port which can be used for several reasons :

- To connect another IndependenceKey
- To connect the Security Cap
- To connect the Data Bank
- To connect a digital VoIP headset
- To connect a USB storage memory
- And, in the future , to connect a USB keyboard or a USB microcamera

This peculiar function enables IndependenceKey to supply several useful cryptographic services.

You can connect or remove these devices to/from IndependenceKey even with IndependenceKey already plugged in the computer and unlocked.

HOW TO MAKE AN ENCRYPTED BACKUP ON EXTERNAL SUPPORTS

Thanks to IndependenceKey, the user can encrypt files and data on common mass-storage USB devices, apparently unsafe, be they common USB keys or USB hard disks without changing one's working habits. In order to do so, just plug these devices in the **USB host port of your IndependenceKey** previously plugged in your computer and unlocked.



What is a USB Host port?

The USB standards include several types of interfaces and connectors, all of them included in the USB devices world, which are really different one from the others. A USB “host” port is the one we find in a common computer, that is the port where common USB devices are usually plugged in like USB storage memories, USB hard disks, USB headsets etc.

IndependenceKey is equipped with both a USB device port to get connected to the computer and a USB host port to connect other USB devices.

Thanks to some specific solutions set up by Quantec, the electronic integration level reached with this device has led to a reduction of IndependenceKey dimensions to its minimum possible size, yet always keeping the same performances as a USB 2.0 High-Speed port that can reach up to a 480 Mbps. Through the “device type” USB port, IndependenceKey is considered by the computer as a high-speed network card thanks to its hardware engineering and to the drivers installed in the computer by the supplied software.

What are the limits of a USB host port?

The USB standards require a USB host port to supply a certain current to feed the device connected to it. This current is to be 500 mA 5 Volts at least. Nowadays, several computers supply from some ports, but not from all ports , more current than required by the minimum standards. For example, some USB hard disks, mainly old-generation ones, require an external power supply and make use either of USB double connectors (to increase the available current) or of external power supplier.

IndependenceKey is a low-power USB device that can dynamically adapt the consumption of energy on the basis of the jobs carried out. This feature not only allows two IndependenceKeys to be supplied, being one plugged into the other during the physical association phase , but it also supplies power to most mass-storage USB devices, USB headsets and similar. However, if after plugging your device in your IndependenceKey this should not turn on, it would be advisable to try the computer other USB ports or connect to the USB device its additional external power supplier.

If IndependenceKey has already been unlocked, as soon as a storage device is plugged in it, it appears on Windows interface as usual: the operative system does not detect the presence of IndependenceKey.

Now you can either Drag&Drop or click on CTRL+C & CTRL+V to copy and automatically encrypt the required files into the external support. At the end of the copying procedure, the external support will contain the data fully protected.

In order to further access these files, it is not strictly necessary to plug the mass-storage device in the IndependenceKey USB host port. You can go on in the traditional way by plugging the USB device in another USB port of the computer.

Access to data is as usual : double click to open a file, provided that your IndependenceKey is already plugged in the computer and unlocked.

Eventually, the files contained in the external supports can be shared with third parties thanks to the IndependenceKey "Crypt & Share" option by following the indications in the paragraph above. This way it will be possible for you to plug in a common USB storage device in your IndependenceKey, already unlocked, copy a file and share it with a colleague with which you had already established an association. Now disconnect the device and give it to your colleague who, in turn and with his/her own IndependenceKey, will be able to safely access the files at any time by simply plugging the mass-storage device in his/her IndependenceKey USB host port or in one of the other ports available on the computer where his/her IndependenceKey is already operative.

Before removing the mass-storage USB device from your IndependenceKey, unmount it just as it should be done when removing it from a generic USB port in your computer. However, should it be removed by force, IndependenceKey will, in turn, try to close the work session associated to this device also for the operative system (Windows). Nevertheless, make sure that there are no open files on the device or files being copied, otherwise they will be lost or will be inevitably corrupted.

TECHNICAL ASPECTS

Does the "Safe Unmount" have anything to do with the USB back device port ?

The "Safe Unmount" option, available by right clicking the IndependenceKey icon in the System Tray Bar on the bottom right, refers to the working session shutdown function in IndependenceKey. Please refer to the "How to remove IndependenceKey" chapter for further details. Before removing the USB device connected to IndependenceKey, unmount it just as it should be done when removing it from a generic USB port in your computer.



How to Use the Security Cap

CRYPTOGRAPHIC KEYS, ASSOCIATION AND PASSWORD MANAGER BACKUPS

While being used, IndependenceKey generates a series of unique cryptographic keys thanks to which the several cryptographic services available are managed. In addition, it also generates specific combinatorial secrets, starting from the initialization phase with the typing of one's own Master Password, and during the association procedure with other users. The cryptographic keys as well as the combinatorial secrets never leave IndependenceKey.

The Security Cap is the hardware solution, 100% encrypted and protected, thanks to which the user can easily backup the encrypted data contained into IndependenceKey, whenever and the way the user wants to, autonomously and safely.

The Security Cap does not backup files, disks and folders encrypted with IndependenceKey, yet it files the cryptographic keys and all the data which are necessary in order to access or decrypt these files. The backup of encrypted files is to be made by the user.

The Security Cap is exclusively associated to IndependenceKey during the initialization phase (for further details please refer to specific chapter in this manual). The Security Cap can only be unlocked by the owner with the same Master Password used with his/her IndependenceKey.

In order to carry out a backup, just plug the Security Cap in your IndependenceKey, be it already plugged in your computer and unlocked or still to be plugged in and unlocked.



TECHNICAL ASPECTS

Is the Security Cap associated to my IndependenceKey only or to others as well?

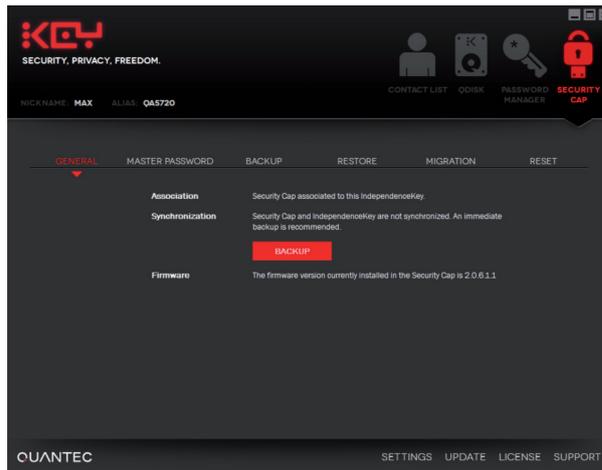
Inside IndependenceKey and inside its Security Cap there is an authentication cryptographic chip from the TPM (Trusted Platform Module) safety platform. Thanks to these chips, together with their relevant cryptographic engines, both IndependenceKey and the Security Cap create a mutual unbreakable link during the association phase, making all the necessary anti-cloning checks, encrypting the communication channel, and memorizing, each device, part of the combinatorial secrets derived from the Master Password. In this way, the Security Cap can be associated only to its IndependenceKey or to a new IndependenceKey in case of theft or loss of the old one. Warning: if you do not know the Master Password, the Security Cap cannot associate to any other new IndependenceKey.

Why doesn't it make a backup if I encrypt a file and then plug the Security Cap in ?

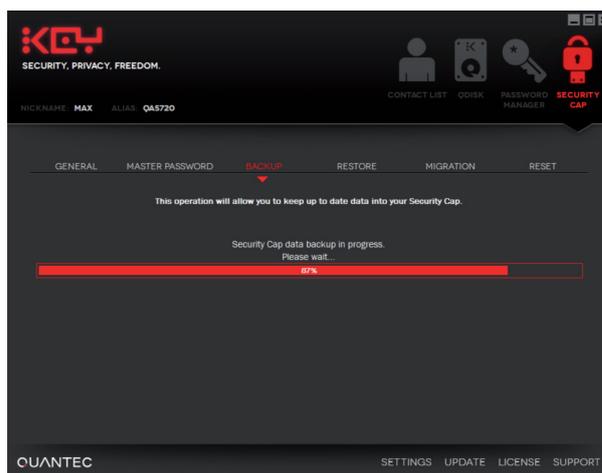
In order to optimize the use of the cryptographic engine and consequently the need to make frequent backups, IndependenceKey makes an indexed use of the file cryptography, which means that a file only contains a reference to the cryptographic key to be used, a reference which only the IndependenceKey user can understand. A specific algorithm inside IndependenceKey makes a smart use of these references, linking the cryptography of a single file or disk not only to a cryptographic key but also to other combinatorial secrets inside IndependenceKey. This procedure includes the creation of these secrets only during the initialization phase and any time it associates with new users. In these cases, it is always advisable to make a backup of one's IndependenceKey.

TECHNICAL ASPECTS

The user interface of the software supplied with IndependenceKey will set itself on the Security Cap screen indicating, if necessary, the possibility to carry out the backup. In order to do the backup, select the relevant option on the interface.



The backup is automatically suggested by the user interface in case IndependenceKey detects a difference in the database version contained in the Security Cap, or detects that IndependenceKey contains more updated data compared to the ones in the Security Cap. The procedure is such that it is impossible to plug in a Security Cap containing a backup more updated than the one inside the IndependenceKey to which it is associated.



The backup also includes the safe automatic filing of all the data in the Password Manager.

Is the Security Cap a mass-storage device?

Absolutely not! The Security Cap is in fact a cryptographic USB device equipped with both his own high-performance cryptographic microcontroller and TPM platform authentication chips, physically protected from any intrusion. It is in fact a device belonging to the same class and category as IndependenceKey and it is not limited to file data on a internal flash memory like a common mass-storage USB device. Indeed, it checks the full authenticity of the IndependenceKey to which it is connected and can in turn encrypt the local USB channel in AES 256, thus creating a safe connection with its IndependenceKey. Eventually, it memorizes the entire backup of the cryptographic keys in a completely encrypted way.

What happens if I lose the Security Cap?

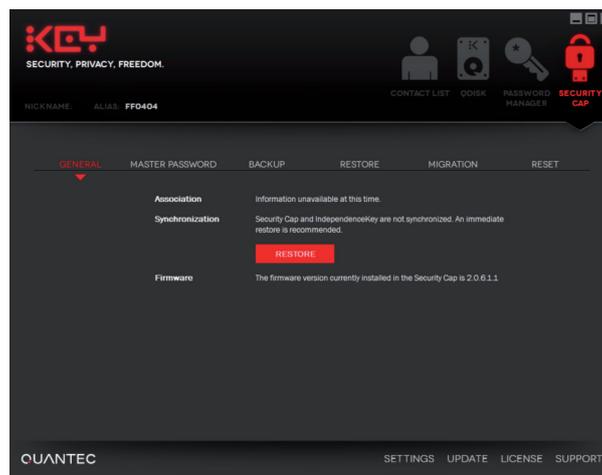
Nothing! The data contained in the Security Cap are totally encrypted and protected by the Master Password. If you lose it, you can purchase a new Security Cap and associate it to your IndependenceKey. From now on, your IndependenceKey will only and exclusively recognize the new Security Cap.



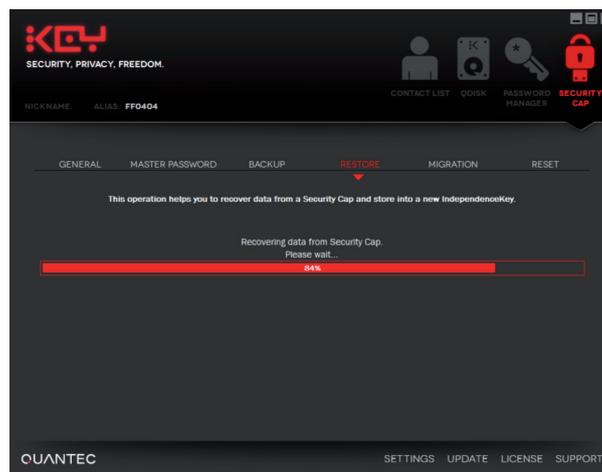
How to Use the Security Cap

RESTORE

If you plug a Security Cap with its own backup in a new IndependenceKey (or reset to its original status), the software will only suggest one possible option, that is to restore the data contained in the Security Cap inside IndependenceKey.



For safety reasons and in order to proceed with the restore operation, it is necessary to type in your Security Cap Master Password. This procedure allows the user to recover all the data from the last backup available in the Security Cap in case of theft or loss of one's IndependenceKey. In this case, just purchase a new IndependenceKey, plug the Security cap in its USB host port and follow the video procedure. Once it has been associated to the new IndependenceKey, the Security Cap will only be able to work with the new IndependenceKey, not with the previous one.

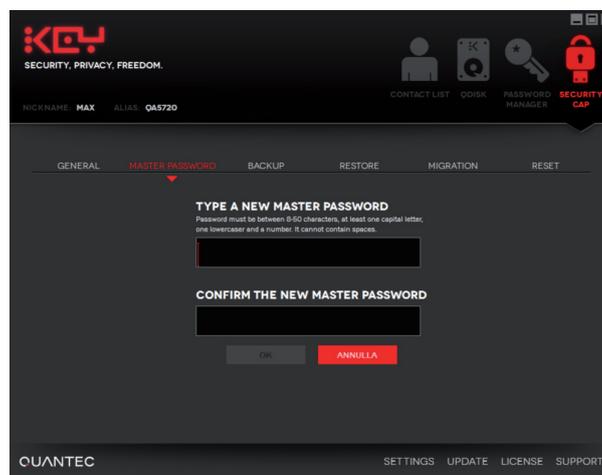


It is worth reminding that the Security Cap must always be removed from IndependenceKey in order to use this last again.

MODIFICATION OF THE MASTER PASSWORD

You may happen to forget your Master Password. IndependenceKey can safely deal with this event: **it is absolutely unnecessary to write down your Master Password on a piece of paper or other kind of supports!** The Security Cap will do everything.

Just plug your Security Cap in your IndependenceKey; the device will unlock and, thanks to the user interface, you will be able to modify your Master Password easily. From now on, the new Master Password will be operative.



NOTE: This way, IndependenceKey will be automatically unlocked by its Security Cap: when IndependenceKey is plugged in a computer together with its Security Cap, no Master Password is required. However, as the Security Cap is the backup safety device of the cryptographic data, IndependenceKey will not start working as long as the Security Cap is not removed.

CONTINUOUS BACKUPS

The Security Cap allows the user to restore in a new IndependenceKey the cryptographic keys, the data contained in one's Password Manager as well as the association data shared with other users and updated to the last backup. It is understood that if the last backup dates back to a month before, the new IndependenceKey will save data updated to that date. Should you have created an association with other users in the meantime, these associations will not be present in the backup: it will therefore be necessary to create an association again. The Password Manager data as well as everything else will not be updated.

In order to avoid this possible problem, Quantec makes the Data Bank service available for continuous data backups. Absolutely reserved and protected, 24 hours a day. Please refer to the following chapter for further details.

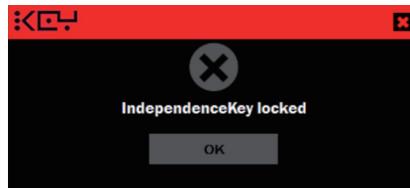


How to Use the Security Cap

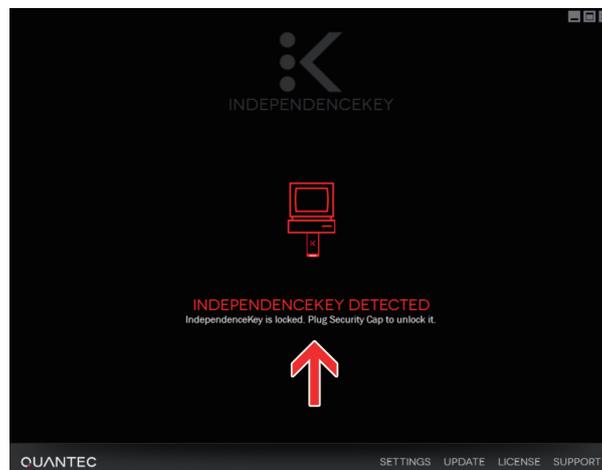
HOW TO UNLOCK INDEPENDENCEKEY

As mentioned in the first chapter concerning the initialization and in the technical notes aside, your IndependenceKey is indissolubly associated to its Security Cap. The Master Password is one of the key elements which enable to use either device separately from the other. When the two devices are linked, the Master Password is no longer necessary and can be modified. Another function of the Security Cap is to unlock the IndependenceKey to which it is associated in case this last gets blocked.

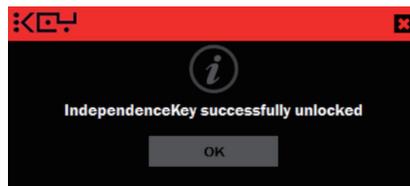
IndependenceKey can get blocked if the maximum number of consecutive attempts to type in the Master Password is exceeded, that is, when a wrong Master Password is typed more than 5 consecutive times.



IndependenceKey is equipped with a protection system against brute force attacks and the block allows the user to realize if someone has tried to forcibly access his/her IndependenceKey.



In case of block, just plug your Security Cap in the IndependenceKey to which it is associated in order to reactivate it immediately.



How to Use the Data Bank



The Data Bank is a further protection service which can be added to the one already supplied by the Security Cap.

Just like the Security Cap, the Data Bank allows the user to back up the cryptographic keys, the combinatorial secrets, the associations with other users and the Password Manager data contained in one's IndependenceKey.

The Data Bank has been thought for people who travel a lot and for a long time and have no opportunity to take their Security Cap with them, for people who are afraid that they may lose both their IndependenceKey and their Security Cap, thus losing access to all the data protected with their IndependenceKey and for all those people who need to make their protected data available to third parties (partners, associates etc..) in some particular cases. In order to meet all these requirements, the Data Bank allows the user to create an updated IndependenceKey at any time, with all the cryptographic data needed to access one's own restricted data.

The Data Bank is a device whose security level is the same as the one of the Security Cap's from which it differs in colour (blue) but most of all, in the functioning logic.

Once you have endorsed this service, the Data Bank is sent to the user who associates it to his/her IndependenceKey. Unlike the Security Cap, it doesn't need to be periodically plugged into the IndependenceKey to carry out a backup. It can be stored in a safe place and left there permanently.

Any time IndependenceKey detects an update of the cryptographic data, association data or Password Manager data contained in it, it carries out a hardware encrypted backup on Quantec's servers or on your company servers automatically (see technical description aside for details). This backup will be filed on Quantec's servers, in Switzerland, or it can be made directly on your company servers and is associated to one's own Data Bank serial number. The backup is automatically carried out when the computer where IndependenceKey is plugged in is connected to the Internet.

In case of loss of your IndependenceKey, just order a new one, plug your Data Bank in the IndependenceKey USB host port and that's all: nothing else is needed ! IndependenceKey will automatically recover the backup related to the Data Bank plugged in it and will send it to its Data Bank which decrypts it and updates itself to the last modification made. All the cryptographic modifications, the associations with other users, and the Password Manager data will be automatically restored inside the new IndependenceKey.

The former IndependenceKey will no longer be usable and it will be automatically locked by Quantec's servers as soon as it tries to connect to the Internet. The data contained will not be accessible unless the Master Password with which it had been initialized is known.

TECHNICAL ASPECTS

How does the Data Bank work?

When the Data Bank is plugged in your IndependenceKey, it creates an unbreakable link with it just as the Security Cap does but, in addition, it downloads into IndependenceKey a cryptographic key, which is specific and secret, that only that data Bank will be able to use. The key is memorized in the TPM cryptographic chip protected also against any external intrusion. Thanks to this cryptographic key, your IndependenceKey will carry out an encrypted backup of its cryptographic data on either Quantec's or your company's servers. The servers receive these bytes, completely incomprehensible to them as they do not know the Data Bank cryptographic key but they will only be able to associate this number of bytes to the Data Bank serial number. The Data Bank cryptographic key is created locally by the Data Bank during the association phase with your IndependenceKey.

Is the backup on Quantec servers safe?

On the basis of the reasons stated above, Quantec servers file a number of encrypted bytes, completely incomprehensible to anyone who does not have the cryptographic keys to decrypt them, strictly linked to the serial number of the Data Bank which can decrypt them. There is no other way to decrypt these data as they are hardware protected in AES 256.

Are Quantec servers safe?

Quantec has got its own server cluster in a data center in Switzerland, specialized in mission-critical applications for the banking and TLC systems. Quantec servers are protected inside an underground bunker and the data contained in them are daily backed up onto other systems. All the backups carried out by the Data Bank are subject to daily and constant backups made onto other systems positioned within the Swiss territory.

Is it possible to make a backup on one's own ? For example, on one's company servers?

On the basis of its customers' specific needs, Quantec allows its customers to make backups anywhere they are thanks to an optional software module which can be installed on one or more dedicated server of his/her company. In this way, the filing of the backups made with the Data Bank and with the IndependenceKey Commander version, created for companies as well as mission-critical governmental applications, is granted even in case of physical disaster recovery scenarios (it is also possible to automatically have all the required backups anywhere you wish).



Keylogger and Master Password

 Should you be afraid that there may be a keylogger in your PC, it is also possible to connect a USB keyboard to the IndependenceKey USB host port and type the Master Password directly into the device.

Now you can go on working, leaving the keyboard connected to IndependenceKey USB host port.

This function will be released in the near future with a product upgrade.

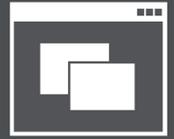
You can always unlock your IndependenceKey by plugging in the Security Cap with which it has been initialized. In this case, it is worth reminding that, in order to use your IndependenceKey, it is necessary to remove the Security Cap after unlocking your IndependenceKey.

TECHNICAL ASPECTS

What is a keylogger?

The keylogger is a particular IT malware, that is, a harmful program residing in a computer without the owner knowing it. Its task is to memorize all the keys pressed by the user while the computer is being used to allow unauthorized third parties to understand what the user is doing/writing, that is recreating emails, texts and passwords. If you believe your PC may be the object of such an attack, you can use an external USB keyboard. A fast and simple solution: just plug the keyboard in the IndependenceKey USB host port and type your Master Password. In this way, no malware of any kind will be able to understand what is being typed as IndependenceKey will not show the keyboard to the computer as long as the right Master Password is typed. Before that time, the keyboard will not be detected by the computer at a hardware level, therefore no malware will be able to detect it. **Once you have typed in your Master Password, IndependenceKey will unlock the keyboard so that it can be used as usual.** It is also possible to leave it connected at the back of your IndependenceKey. If your computer is part of a company network, it will be duly administered by your company's IT Manager and it will certainly be equipped with the suitable software programs as modern antivirus, so the possibility for such an event to happen is rather remote.

Programs and Authorizations

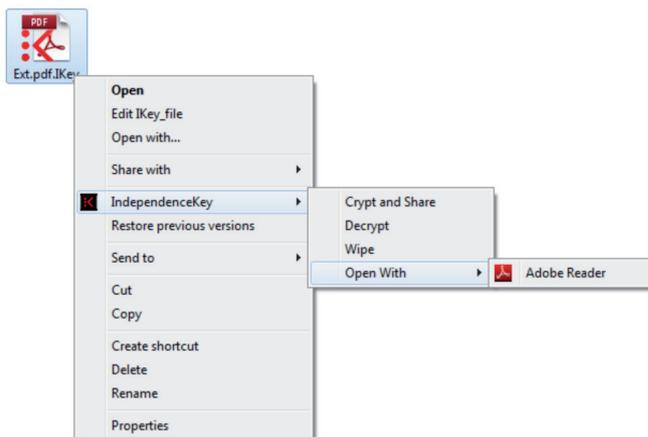


TECHNICAL ASPECTS

 IndependenceKey uses an easy and efficient system to enable the authorized applications to automatically access encrypted files. In this way, the access to encrypted files can be gained without changing one's working habits and, at the same time, **the user is always warned when an unauthorized program is trying to access a protected file.**

When opening a file with a double click, IndependenceKey access the file, automatically checks the parameters needed and recalls the related application. For example, if the file is a ".docx" one and Microsoft Word is installed on the computer, IndependenceKey will execute the Word program and work directly on the encrypted file.

It is always possible to open the encrypted files with Wordpad or other programs by clicking on the option "Open with" from the IndependenceKey menu. Just right click on the file and select "Open with" from the "IndependenceKey" menu. This applies to all the programs installed in the computer, not just to Word.



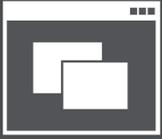
However, there may be other programs running in the computer aiming at accessing the encrypted files, for example an antivirus. In this case, it is necessary to enable the antivirus when opening the encrypted file as, should it not be done, the antivirus may be likely to forbid the execution of the program associated to the file as it is unable to recognize its content.

If a non-enabled program requires the access to an encrypted file, it will always be the user to decide if the access can be give or not by answering either yes or no to the pop-up appearing on the video. Should the answer be positive, the program will be inserted in a special list of enabled programs which can be accessed through the menu by selecting "Settings" -> "Preferences" -> "Applications".

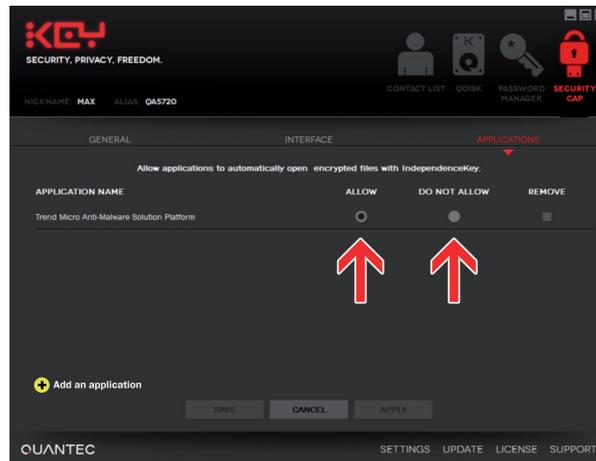
The IndependenceKey double click

One of the unique and successful features of IndependenceKey is its ability to open and manage encrypted files as if they were not encrypted. Thanks to this ability, the presence of IndependenceKey does not require to change one's working habits. This function, characterized by the usual "double click" on the file icon is indeed a basic function in any modern operative system. What happens when you double click on a file? The operative system has access to a specific inner area, the register, and understands what type of application is connected to this file (usually by identifying the file extension). If the application is known and it is installed in the computer, it will be executed in order to open the file. Otherwise, an error will be reported. In any case, it is always possible to use the "Open with" option to open the file even with applications which are different from the "default" one to which the file is associated. IndependenceKey operates under the file system of the operative system that is between the storage devices and the file system. When the user tries to open a file with a certain application, this last starts to require the file system the different parts of the file which are necessary for the opening. Now it's the turn of IndependenceKey which, on behalf of the application, access the file and decrypts only the required parts, sending them to the application afterwards. Vice versa, when the application requires the memorization of the updated parts inside the file, IndependenceKey encrypts the data received and memorizes them in the file already encrypted. Everything occurs in real time, absolutely invisible to the user and to the applications. In order to carry out the process described above, the application has to be authorized to open the file. All the applications already installed in a computer are authorized by default. Unauthorized applications are dealt with through a pop-up so that the user is the only one who can decide whether to authorize an application to access a specific file or not.

If the antivirus requires access to a file, it is advisable to give it the authorization to prevent it from blocking the main application. However, should an unknown application require access to an encrypted file, check the application first before giving it the authorization to access the file. If the answer is positive, IndependenceKey will make the non-codified parts of the file available to the application. This way the user has a thorough control over the encrypted files. Generally, once IndependenceKey has been installed, it is necessary to give authorization to the antivirus or antimalware software. Once the authorization has been given, it is always possible to deny it again through the user interface at any time .



Programs and Authorizations



Thanks to this interface, you can enable, disable or remove one of the enabled programs .

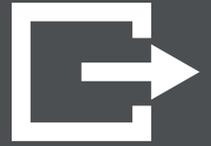
This function is also very useful for those programs like RAD, CAD/CAM development programs, authoring systems, etc.. which can open more than one file at the same time within the same project. In this case, it is necessary to enable the specific program to operate directly on the files encrypted by IndependenceKey.

By selecting “Authorize New Application” it is possible to manually authorize an application to access a file protected by IndependenceKey. Afterwards, to remove the application from the list of the authorized ones, just select the option “Remove” and chose “Apply”.

It is worth reminding that IndependenceKey can enable a program to access an encrypted file by simply double clicking on the icon of this file in Windows Explorer or by simply opening this file with the “Open with” option from the related “IndependenceKey” menu. You can’t open the file as usual from the specific internal options of the program. This is a one-off operation.

The use of IndependenceKey encrypted QDisks is recommended if the programs used have to work with many files at the same time. In this case, this is the most effective solution.

How to Remove IndependenceKey



 IndependenceKey is a device that can encrypt data, file, folders and disks as well as audio/video and VoIP streams in real time. If it is removed from the computer to which it is connected while working, some errors may occur while encrypting files and data in general, just as it may happen with a USB storage device if it is removed from the computer while copying files on it. As for IndependenceKey, the cryptographic operations will be interrupted.

However, IndependenceKey has been designed to be as safe as possible and “failsafe”. This is the reason why it can deal with particular situations like, for example, removing its Security Cap while a backup or a restore procedure are being run: nothing odd happens, just plug in your Security Cap and the operation will re-start from where it had been interrupted.

Should IndependenceKey be removed during the initialization phase, nothing irrecoverable would happen. In this case, once you have plugged in again your IndependenceKey with its Security Cap, the initialization re-starts from where it had been interrupted.

On the contrary, should IndependenceKey be removed while it is encrypting a file, all the data will be lost: the file which was being encrypted will be cancelled as it will be considered as an incomplete file. In this case, if the “Autowiping” function is enabled, the unencrypted file will not be cancelled as it has been impossible to encrypt it completely.

Should you be using an encrypted disk (Qdisk) and copying files inside it, if you unmount the disk (without removing the IndependenceKey), the system will first terminate the operations and then unmount the disk. Should you abruptly remove IndependenceKey from the computer during this operation, the files copied will be corrupted as it happens with any other disk and mass storage device when forcibly removed while copying data on it.

In any case, **in order to operate safely, it is highly recommended before removing IndependenceKey from the computer, to click on the “K” icon at the bottom right on the system tray bar and select the option -> “Safe Remove”.**

Thanks to this procedure, the device will check if there are any operations being run and, should it be so, notifies the user about the need to terminate them before removing IndependenceKey. If there are no operations being run, IndependenceKey will be disabled and the user will be free to remove it safely. The flashing LED of the device turns off indicating that it is now possible to safely remove it. After disabling it, in order to use it again, it is necessary to remove it and plug it in the computer again.



Moreover, if you are copying files on disks protected by IndependenceKey, or if you are working on encrypted files with one or more applications (e.g. an encrypted document opened by Microsoft Word or by another application) it will not be possible to safely remove IndependenceKey. In this case, the user interface will invite you to close the protected files.

If you try to turn your computer off or to put it on standby while IndependenceKey is operating, Windows will notify, on the list of applications to be closed, that IndependenceKey is still operating. In this case, it is advised to click on “Cancel” option, go back to the desktop, close encrypted files and/or disks and then repeat the operation safely.

It is always advisable to click on the “Safe Remove” option from IndependenceKey menu before putting the computer on standby either through Windows interface or through the automatic mechanisms made available by the hardware (for example when closing the display of a notebook or clicking on the standby option of the computer).

When resuming the work session after the standby, if your IndependenceKey had not been removed from the computer, you will be asked to insert the Master Password again in order to unlock it and continue to work.





Reset and Migration

TECHNICAL ASPECTS



IndependenceKey has been designed to preserve and at top security levels the cryptographic data necessary to access files, disks and encrypted information, both personal and shared with other users. It has also been designed to safely **backup and restore these data, always under the user control**. IndependenceKey memorizes all the cryptographic keys and combinatorial secrets created while being used, starting from its initialization and including the data related to the associations with other users. IndependenceKey also memorizes all the Password Manager data and makes a safe backup and restore operation of them.

RESET

You can reset your IndependenceKey to its original status, which means that you can cancel all the combinatorial secrets, the cryptographic keys and the Password Manager data contained in the device by following the “Reset” procedure through the user interface.

WARNING: once your IndependenceKey is restored to its original status, previously encrypted data will be impossible to access, be these files, disks or any other type of data or information protected by IndependenceKey.

In order to reset your device, make sure your Internet connection is active. Plug your IndependenceKey in your computer together with its Security Cap. Select option -> “Reset” on the user interface from the Security Cap menu.

Your IndependenceKey will be automatically restored to its original conditions thanks to Quantec servers. Once the procedure has been started it is impossible to interrupt it.

MIGRATION

The migration procedure is complementary to the reset one and allows the user to physically move the cryptographic data from one IndependenceKey into a new IndependenceKey. All autonomously. The migration allows the user either to make an upgrade of one's IndependenceKey to a new version or to replace it with a new IndependenceKey.

In order to start the migration, make sure your Internet connection is active, plug your old IndependenceKey in your computer and unlock it. Plug your new IndependenceKey in the USB host port of the old device and insert the old Security Cap in the USB host port of the new IndependenceKey. Follow the video instructions through the user interface so that all the encrypted data contained in the old IndependenceKey, together with the ones from the Password Manager, will migrate into the new IndependenceKey.

The old IndependenceKey Security Cap will be automatically and exclusively associated to the new IndependenceKey, whereas the old IndependenceKey will be reset and restored to its original conditions.

From now on, you can use your new IndependenceKey with the Security Cap of the old IndependenceKey. The Security Cap of the new IndependenceKey, which hasn't been initialized, will be assigned to the old IndependenceKey which has been reset and restored to its original status during the migration procedure.

For any question and clarification, please refer to the IndependenceKey Support Service integrated in the user interface (see following chapter).

How are secrets protected inside IndependenceKey?

IndependenceKey contains specific chips dedicated to cryptography as well as to the safe authentication, creation and management of cryptographic keys. These chips, belonging to the TPM (Trusted Platform Module) platform, enable the user not only to create and manage all the combinatorial secrets during the use of IndependenceKey, but also to protect them in sealed memory areas, protected from intrusions and analysis attempts based on weak currents and clock derivation.

What happens with the Reset?

The reset of IndependenceKey will cancel all the secrets contained in the cryptographic chips, thus eliminating all the cryptographic keys which have been used so far, the user primary key, the combinatorial secrets related to the associations with other users etc. including the data contained in the Password Manager. Everything will be **safely cancelled, block by block, at a low level and directly in the hardware**. A reset IndependenceKey cannot be distinguished from a brand new IndependenceKey as far as the data contained are concerned.

Why do I need an Internet connection?

In order to reset an IndependenceKey, Quantec requires the computer through which the reset will take place to be connected to the Internet so as to be able to lock the old one inside its database.

Is migration safe?

All the initialization cryptographic processes, association processes, backup and restore ones are carried out at firmware level inside the selfsame IndependenceKey and Security Cap devices. They can be interrupted at any time, even forcibly, for example by unplugging the Security Cap while a backup or restore procedure are being carried out. Also the migration takes place exclusively between IndependenceKey devices and is completely “failsafe”, which means that IndependenceKey can recover any error condition including the unplugging of the new IndependenceKey from the old one while the procedure is being carried out.

Once the migration is over, all the data contained in the old IndependenceKey are transferred into the new one and therefore they are permanently cancelled from the old IndependenceKey.

Technical Support and Assistance



IndependenceKey has been designed to be practically invisible to the user during most daily operations and services supplied.

We at Quantec believe technical support to be essential. This is why it has been integrated into the user interface of the software supplied with IndependenceKey.

In order to contact the technical service, just open the user interface, click on “Support “ on the bottom right and choose the option “Technical Support”. Now you can write your message in the box that opens. Click on “Send” and the message will be immediately addressed to our Technical Support department.

You can always either send an e-mail message to the following addresses, that is support@independencekey.com or support@quanteclab.com, or open a ticket on the IndependenceKey site using your account and indicating your Alias (written on the user interface under the IndependenceKey logo).

It is also possible to send suggestions and opinions concerning the products, the user interface, how useful our services are as well as ideas and proposals for any potential desiderata. Just click on “Support“ on the bottom right on the user interface, choose the option “ Suggestions“ then follow the instructions.

In order to send your enquiries, you just need an Internet connection and your IndependenceKey plugged in and unlocked in your computer.

TECHNICAL ASPECTS

What happens when I send an enquiry?

The IndependenceKey communication system with Quantec servers, is hardware encrypted by the device itself. Quantec servers do not allow connections if these are not from duly enabled and initialized IndependenceKey devices. In order to access the IndependenceKey on-line services , your IndependenceKey has to be plugged in your computer and unlocked . However, you can also send your request for assistance and support without your IndependenceKey being plugged in.



Troubleshooting

SECURITY AND PRIVACY

Can anyone recover my data after I erased them?

It's impossible! IndependenceKey will automatically wipe all unencrypted traces when you encrypt a file. When you erase a file through the "wipe" menu function, there will be no way to retrieve it. Besides, when you open an encrypted file it won't be decrypted in any temporary area or similar area! Everything happens in the memory, in real-time, and only for the parts of the file that the application requires from the operating system, both in reading and writing mode. For this reason, when you are working on an encrypted file there are no unencrypted parts of it on the system.

Can I make over my IndependenceKey to somebody else? Is there any reset function that makes my data impossible to access?

Yes. If you switch to a new product, a guided procedure will help you create a new IndependenceKey and will reset the old one, so that you can make it over to someone else without risks. You can also reset the IndependenceKey directly, if so, remember to previously decrypt your data. To wipe your IndependenceKey completely your Security Cap is needed.

Can IndependenceKey and SecurityCap be violated without my noticing?

No. Neither at the software level nor at the hardware level. Moreover, should someone try to open the hardware, the product will break.

What if I write a message in a file, instead of in the e-mail text field, then encrypt and attach it? Am I protected?

Yes, at 100%. We're thinking about a software tool to protect e-mails and work directly on Outlook, but, at the moment, the procedure you suggested is the only 100% safe one.

Who chooses the cryptographic keys?

The cryptographic keys are generated on hardware by the IndependenceKey and are all different one another. The Master Password is only one of the elements that give access to the cryptographic keys. Nobody knows the cryptographic keys, neither you, nor those you want to share files with: the only way other people can open your documents is by associating to you through their IndependenceKeys.

Is it possible to intercept communications between Security Cap and IndependenceKey, between IndependenceKey and the computer, or between/among IndependenceKeys?

No. Security Cap and IndependenceKey (as well as the different IndependenceKeys) are actually associated 1:1 on hardware: an encrypted channel is established to make communications absolutely safe. This will avoid any kind of attack ("Man in the Middle", "Replay Attack", etc.). Communications between the IndependenceKey and the computer are also encrypted with keys that vary from session to session.

What if I have a Malware or a Trojan in my computer? Can it detect my Master Password?

Yes, if you digit your password directly from the keyboard to the computer, and the Trojan is a "Key Logger". But there is something you can do if you think there could be a damaging software on the computer you are using: plug an USB keyboard directly in the USB port on the back of your IndependenceKey, digit your Master Password and you will unlock your key bypassing your PC!

INITIALIZATION AND USE

How do I initialize my IndependenceKey?

Once you have downloaded and installed the software, you will have to plug it in your computer's USB port and follow the guided procedure. After that, you will only need to plug it into your computer's USB port and unlock it with the Master Password you chose during the guided procedure. Refer to the user manual for the details.

IndependenceKey is plugged in but nothing happens. What can I do?

IndependenceKey works on x86 computers equipped with several versions of Microsoft Windows operating system: XP SP3, Vista, Windows 7 (both 32 and 64 bit). Your computer doesn't probably meet the minimum system requirements. Each IndependenceKey is 100% tested before delivery. Anyway, damage can be caused by something out of our control that happens during shipping. If that's the case, ask your distributor to open a ticket through IndependenceKey support service and then arrange to exercise your warranty rights.

Sometimes IndependenceKey seems to heat up. Is it OK?

Yes, it can happen during an intensive use of the product. Do not forget: this isn't an usual "USB key" but a high performance embedded computer. IndependenceKey holds, in just 45x25 mm, all the electronics contained in modern computers and smartphones. All devices heat up. Obviously, due to its very small size, IndependenceKey has a lower possibility to disperse heat, that's why it feels warmer. The metallic shell helps keeping the heat lower inside, to the detriment of the heat outside. All operating parameters are way under the functioning limit and this is not a product flaw.

I want to buy a new IndependenceKey, do I have to decrypt and encrypt all the documents again?

No. You have to follow the migration procedure to substitute your old IndependenceKey with the new one. Once you've completed it, the new

IndependenceKey is immediately operative, the old one is totally resetted and you can make it over to other people, friends, colleagues or relatives.

Can I store files on the IndependenceKey?

On the model equipped with internal memory, yes. On any other model, no. The data stored on the IndependenceKey are cryptographic keys and reserved information. The IndependenceKey model with internal memory (available with different memory sizes) is also a superfast storage “encrypted USB key” with two benefits: speed and a backup on your computer of the encrypted data it contains.

Can I use more than one IndependenceKey on the same computer?

Sure, but pay attention: these are different users’ IndependenceKeys, so the files encrypted by one cannot be accessed by the other, unless you associate the IndependenceKeys and share the files between them.

Can I temporary block a contact or do I have to cancel him and then associate again?

Contacts on your list cannot open or see anything, unless you grant them the access rights to files, folders and disks. For this reason, there’s no use in blocking them. As for the resources shared on company servers or Cloud systems, removing a user from the file or disk, will prevent him/her to open it anymore. Obviously, files already sent to users via e-mail or by other tools, can’t be blocked.

If I create a file and grant access to 3 users, can they grant the same right to other users?

No! IndependenceKey exploit the concept of “ownership”. The user who creates an encrypted file is the only one who can grant or deny the access right to other users. No one else can.

I unplugged IndependenceKey while it was executing an operation, did I damage it?

It depends on which kind of operation it was executing. When it comes to initialization, association to other users, backup, restore and migration, there’s no damage. These operations are executed by IndependenceKey in absolute safety. If you were encrypting one or more files, they would remain unencrypted. If you were working on an encrypted file (for example a Word document) there is the possibility that the entire file or parts of it might be corrupted. If you were writing on encrypted disks (for example copying a big size file), you may have lost it as it happens if you remove a standard USB mass-storage device. It’s always recommended to do the “Safe Remove” clicking on the red “K” in the system tray bar.

How should I remove the IndependenceKey?

Before removing the IndependenceKey, you need to “Safe Remove” it from the menu function on the system tray bar low to the right, by clicking the red icon “K”. Anyway, if you don’t execute the unmount and there are no operation in progress, nothing will happen. We highly recommend to always unmount the device correctly. In case of activities in progress, the users will be notified. User will be notified even in case of computer turn off without previous correct IndependenceKey unmount.

CLOUD COMPUTING

Can I upload data encrypted with IndependenceKey on Dropbox, Skydrive, Power Folder, Wuala, Carbonite, etc.?

IndependenceKey is just perfect for such usage. No one can access your information, and you can exploit the whole Cloud service. Attention: always remember to respect the service provider’s terms and conditions.

What’s the maximum file size I can encrypt?

When it comes to sizes, IndependenceKey has no limits. Actually, the bigger they are the fastest encryption and synchronization with Cloud will be performed. You can find further details in the technical information section.

Can I share files through Cloud?

Sure. Just remember that sharing Cloud access isn’t enough: users’ IndependenceKeys should also be associated in order to share files, documents and disks.

Can the IndependenceKey protect me also on social network platforms?

When you use a social network you decide to publicly share your information. Anyway, you can encrypt files and share them with other users using your social network as an exchanging tool for reserved information, always respecting their terms and conditions.



Troubleshooting

SECURITY CAP

Do I need to use Security Cap?

Have you ever thought about it? Whatever you do on the Internet, there's always someone who knows your data recovery password. Thanks to the revolutionary Security Cap we finally solved the problem. Everything is in your hand. The Security Cap is equipped with a cryptographic authentication chip, a hardware cryptographic engine and a memory capable of functioning as a safe and reliable backup system of the data stored on the IndependenceKey (cryptographic keys and associations with other users); it enables data recovery in case your IndependenceKey is lost or stolen or in case of amnesia. This patented solution opens a new era for private and company security.

How often should I connect it to my IndependenceKey to backup data?

It depends on how often you use your IndependenceKey. If you use it daily, in association to several users, we recommend to backup regularly. If you use it less, you can do the backup with lower frequency. When you use it and associate with new users, you create new cryptographic keys; if you don't do the backup and lose your IndependenceKey you could lose access to the last files you received from other users. Anyway, this operation is so simple and fast that you can easily do it frequently.

What happens if I lose the Security Cap?

Don't worry, you won't lose your data. You can buy a new one and, with your IndependenceKey and the Master Password, you can create a new Security Cap. Remember that you will always need two components: if you lose the IndependenceKey, you will need the Security Cap and the Master Password; if you lose the Security Cap, you will need the IndependenceKey and the Master Password. If you forget your Master Password, you will need the IndependenceKey and the Security Cap.

Then, if both my IndependenceKey and my Security Cap are stolen, the thieves can decrypt my data?

Yes. That's why you shouldn't keep them together: it's like they stole both your ATM card and your PIN. You need to keep them separate.

If someone gets my Security Cap, could he be able to open my files?

No. The device would be totally useless and he wouldn't be able neither to see nor to extract your unencrypted data. It's always also required your Master Password.

I lost the IndependenceKey and I really need to open encrypted files but my new IndependenceKey will arrive next week: what can I do?

Nothing. For your own security, you have to wait for the new device to arrive and the restore the data.

While the backup on Security Cap was in progress, power went out. Does IndependenceKey still work? Do I have to restart the backup?

Yes, IndependenceKey is built to resist this kind of inconveniences. Always check that the executed processes are completed.

ASSOCIATION AND SHARING

How does association occurs?

There are two ways: 1. PHYSICAL: plug the IndependenceKey of the user you want to associate with into your IndependenceKey USB back port. Now, follow the instructions. 2. REMOTE: you can associate with remote users, through the unique ALIAS of every IndependenceKey (it's written in the IndependenceKey cryptographic chip).

If I associate with someone, does it mean the he can see/read my files and folders?

No. You can associate with anyone in total security. Association only means that from now on you can grant someone access to a specific file, folder or disk. You can associate with clients, providers, colleagues, friends, and share only the files you want with whoever you want. The association process creates a universal and unambiguous cryptographic key between you and the user you are associated with. Later, through this cryptographic key, you will be able to extend file access rights to file, folders and disks. The user will be able to access only the files you chose to share with him. The rest of the files, folders and disks is safe.

If a user to whom I'm already associated sends me a file, do I have to decrypt it to open it or save it into a specific memory area?

No. You can store it wherever you like and it will stay encrypted. With the IndependenceKey plugged in and unlocked (through your Master Password) you can open the file with a simple double-click and you can work on it as usual. You won't need to make an unencrypted copy of it on you PC because only the parts you are working on are decrypted in real-time exclusively on the memory. Obviously, when IndependenceKey is unplugged nobody can open both your and the other users' documents.

THE DATA BANK

What do I have to do when I receive Data Bank?

Plug it in your IndependenceKey USB host port and store it safely. That's all. Keep making regular backups with your Security Cap, knowing that Data Bank will give you an extra protection twenty-four hours a day.

When Data Bank Cap is associated, which information is stored and where?

The stored information is the one generated by IndependenceKey, i.e. the cryptographic keys and the associations. This information is encrypted in hardware through Data Bank's unambiguous cryptographic key and, when IndependenceKey is connected to the Internet, it is sent encrypted to Quantec's servers. In case both your IndependenceKey and your Security Cap are lost or stolen, thanks to Data Bank you will be able to recover everything and lose nothing.

Can Quantec open the backup files it receives?

In no way. Your backup is meaningless for us: it's encrypted in hardware with AES 256-bit at high entropy.



Technical Appendix

SOFTWARE INSTALLATION WITH WINDOWS XP

In order to install the IndependenceKey Software with Windows XP, the operative system has to be updated to the Service Pack 3 version. This is an essential pre-requisite for the software to operate correctly.

The IndependenceKey software and its drivers are digitally signed with a certificate issued by a trustworthy Certification Authority. This certificate (Microsoft Authenticode) guarantees, from the setup start-up, the software origins thanks to the digital certification of all the program key components. Windows XP does not recognise this certificate therefore it is necessary to carry out some manual operations. This operation occurs automatically with the other operative systems that can be used with this application, with no further user intervention.

The following screen can be visualized in Windows XP SP3 when the setup is started. Click on "Continue Anyway" to proceed. Do not interrupt the setup although it may take some minutes to complete.



Install the setup, restart the computer, plug in your IndependenceKey. The following message will appear on the system tray bar (bottom right) :



Select the first option available in the two following screens and click on "Next":



Photo 1



Photo 2

Windows XP will automatically detect the right driver to be used with IndependenceKey (Photo 1 and 2). Click on “Continue Anyway” on the following screen to proceed (Photo 3).

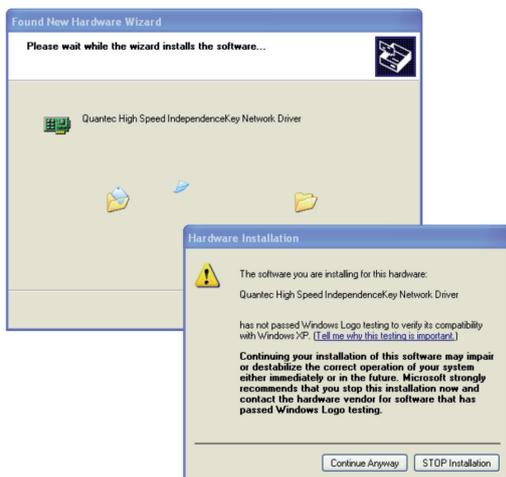


Foto 3



Foto 4

The IndependenceKey driver is now installed. Click on “Finish” (Photo 4).

Software Licence Terms and Conditions

QUANTEC SA

SOFTWARE LICENCE TERMS AND CONDITIONS

IMPORTANT: USE OF THE INDEPENDENCEKEY BINDS THE USER TO THE FOLLOWING TERMS AND CONDITIONS.

PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THE INDEPENDENCEKEY DEVICE OR DOWNLOADING THE SOFTWARE OR SOFTWARE UPDATE ACCOMPANYING THIS LICENCE. By using IndependenceKey or downloading the software, you accept the terms and conditions of this licence. If you do not wish to accept the following terms and conditions, please do not use the device and do not download the software or its updates.

1. TERMINOLOGY AND REFERENCES

Product: The hardware and software that make up the IndependenceKey.

User: The individual or legal entity that uses the product.

Software: The original software and software updates.

Software Updates: Software updates downloaded from the website or the internet in general, including automatic updates sent by the Quantec server.

IndependenceKey or IKEY: Generally refers to the product.

Data: The content, documentation, interfaces and all data supplied by Quantec with the IndependenceKey, as well as those upgraded or replaced by added features, both in read-only memory, on any other media or in any other form.

Security Cap: The IndependenceKey back-up and restore device

Services: The features made available to the product.

Hardware Warranty: The warranty referred to in the "Hardware Warranty" document, which shall be deemed an integral and binding part of the terms and conditions.

Privacy: It is not dealt with in these terms and conditions, but in the "Privacy" document which shall be deemed an integral and binding part of the terms and conditions.

2. LIMITATIONS AND PERMITTED USES OF INDEPENDENCEKEY

IndependenceKey can be used to encrypt and decrypt files, folders, create encrypted disks and encrypt material in general, share encrypted material with third parties, load encrypted material into the cloud and the user's company enterprise servers. IndependenceKey also allows real-time encryption and decryption of digital data (streams), whether audio or audio/video and also perform, by means of the appropriate optional extensions, VoIP calls that cannot be accessed by unwelcome third parties, as well as digitally sign data files of any kind and check their structural integrity, to make sure that they have not been tampered with and/or modified.

The user expressly agrees to the following:

1. The use of IndependenceKey is limited to material for which the user holds the copyright or which is not protected by copyright and that, in any case, cannot cause harm to public safety or to third parties in general and is not contrary to law.
2. Since Quantec can in no way access or decrypt the user's material, by purchasing the product the latter agrees to comply unreservedly with each request, invitation, order or injunction issued by any authority in relation to the material itself, in order to exempt Quantec from any burden in this regard.
3. In the event that the user makes use of cloud or file transfer services or any other internet service, the user agrees to observe the terms and conditions of the service provider, in order to exempt Quantec from any burden in this regard.
4. To record his/her contents (files, data and digital information) on IndependenceKey (the version with internal storage memory), performing regular back-up copies on some other mass storage device (alternatively, when available, the user can use the IndependenceKey optional software plug-in for automatic back-ups of data stored in the IndependenceKey internal mass storage memory on the computer to which the device itself is connected).
5. The user agrees to use the product, Software and services under the terms of the licence granted by Quantec and in compliance with all applicable laws, including local laws of the country or region in which the user resides, purchases the product, downloads the software or uses the software and services.
6. The user shall faithfully observe the terms in the "Controlled Export" paragraph, below.
7. Improper use is the sole responsibility of the user.

3. SOFTWARE LICENCE

1. Quantec grants the user a personal, limited, non-transferable and non-exclusive licence to use the software and data, on one or more computers owned by the user (the "Licence"). The licence also includes the right to download any software updates that may be made available by Quantec.
2. The terms and conditions of the licence govern the use of the services and the software, including any software updates that may be provided and/or made available by Quantec to replace and/or supplement the software, unless such updates are governed by a separate licence, in which case the terms and conditions of the latter will apply.
3. Quantec is the sole owner of the software and reserves all the rights not expressly granted to the user by the licence.

4. LIMITATIONS OF THE SOFTWARE LICENCE

1. Software updates downloaded by the user can only be copied for back-up purposes and as long as the copy includes all the information relating to copyright or other proprietary notices contained in the original.
2. The licence does not grant any rights to use the interfaces owned by Quantec nor other intellectual property rights regarding the manufacture, development, design, licensing or distribution of third-party devices and accessories or third-party applications to be used with the devices.
3. It is forbidden to copy, modify, create derivative work from the source code, reverse engineer, disassemble or try to discover the code by other means, sell, assign, sub-licence, pledge or otherwise transfer any right in the software, unless such activity is expressly permitted or required by law or expressly authorised in writing by Quantec. The user agrees not to carry out any of the actions mentioned above, acknowledges and agrees that carrying out or even just attempting to carry out any of them constitutes an infringement of Quantec's industrial and intellectual property rights.

5. TRANSFER

Notwithstanding the provision in point 4 of the preceding paragraph, the user may permanently transfer all rights in the software to third parties, in the event of a transfer of ownership of IndependenceKey, provided that:

1. The transfer regards the IndependenceKey device and all its components, including software, original media, printed materials and the licence;
2. The user performs a "reset" of the IndependenceKey device and the Security Cap associated to it by following the procedure laid down in the software or through an internet connection. In this way, the cryptographic chips of the device can be completely erased and both devices set to factory configurations;
3. No partial or full copy of the software is kept, including any copies stored on a computer or other IndependenceKey data storage device;
4. The party receiving the software reads and agrees to the terms and conditions of the licence and any separate licence for the software updates.

6. CONSENT TO USE OF DATA

1. The user agrees and acknowledges that Quantec may collect, store, process and use diagnostic information, use, techniques and other related information, in particular (but not exclusively) information about the IndependenceKey device, the computer, the system and application software as well as any external devices in use. This data will be collected from Quantec periodically to allow and facilitate the preparation and provision of software updates, technical support and other services related to the software and to verify compliance with the terms and conditions of the licence. Quantec will use this data in a form such that it is not possible to discover the identity of the person to whom it belongs, with the sole aim of providing and improving our products and services. To enable Quantec's partners and third party developers to improve their software, hardware and services intended for use with the products provided, Quantec can forward to such partners and third party developers a subset of diagnostic information relevant to their software, hardware and/or services, as well as diagnostic information, in a form such that it is not possible to identify you personally.
2. The data will be treated at all times in accordance with the policy of protecting the privacy of Quantec, integrated as a reference to the licence and which can be consulted at <http://www.independencekey.com/blog-en/privacy/>

7. USE OF SERVICES

L'Utente riconosce e accetta che i Servizi ed il Software contengano informazioni proprietarie e riservate, di esclusiva proprietà di Quantec e protette dalle leggi applicabili in materia di proprietà intellettuale e da ogni altra norma - di legge o non - applicabile, ivi compresa, a titolo esemplificativo ma non esaustivo, la normativa in materia di copyright.

1. The user acknowledges and agrees that the services and the software contain proprietary and confidential information, the exclusive property of Quantec and protected by the applicable laws on intellectual property and all other applicable regulations - judicial or not - including, by way of example and by no way of limitation, the laws on copyright.
2. The user agrees not to modify, rent, lease, hire, sell or distribute, in whole or in part, the services or the software and not to create derivative work based on the proprietary content of the services and the software, unless explicitly authorised in writing by Quantec.
3. The user agrees not to use the services in ways that are not permitted, including, by way of example and by no way of limitation, the use of services for the transmission of Trojans, worms, viruses or other malware.
4. The user agrees not to use the services in any way to harass, stalk, abuse, defame, threaten, infringe or breach third party rights in any other manner.
5. Quantec is in no way responsible for any uses not permitted or put in place by the user to the detriment of third parties, as well as the consequences thereof, including, but not limited to, harassment, violations, defamation, threats, offensive or illegal messages.
6. Quantec does not guarantee that the software updates it provides and/or makes available include all existing software features or new features provided by Quantec for other or newer IndependenceKey models.
7. Quantec is not responsible for the adequacy of third party services and materials to which the user may have access using IndependenceKey.
8. Quantec reserves the right to modify, suspend, discontinue or disable access to one/some/all of the services, as well as to restrict the use and/or access at any time and from time to time, with or without notice. The user agrees that, in any case, Quantec shall not be liable to him/her or to any third party for such modifications, suspensions or interruptions of the services.

8. REVOCATION OF THE LICENCE

In the event of failure to comply with even one of the clauses in the terms and conditions of the licence, it shall immediately be deemed automatically revoked without notice by Quantec, resulting in loss of the rights it granted to the user, while the use of the software and services by the latter must stop with immediate effect.

In the event of a failure to comply with the terms and conditions of the licence, Quantec reserves the right, at any time and without notice, to disable all installations of the software carried out by the user and the IndependenceKey device(s) being used.

The responsibilities and limitations to which the user is subject will continue even after the licence has been revoked.

9. DISCLAIMER OF OTHER WARRANTIES

The user acknowledges and accepts the following:

1. To the extent permitted by applicable law, the use of the product and services is at the sole risk of the user, even in terms of quality, accuracy, performance and satisfactory employment. Services are provided in the state in which they are found and depending on their availability. Quantec specifically disclaims any warranty and/or condition of any kind, whether express or implied, including, but not limited to, the implied guarantees and conditions of merchantability, fitness for a particular purpose and non-infringement of third party rights;
2. Quantec does not guarantee that the services and features of the software will be suitable for the needs and expectations of the user nor that the services will be free from interruptions, that they will be timely, secure or error free;
3. Quantec does not guarantee that the software is compatible with applications, services or third party software and that services will continue to be available and, in case of interference with the operation of third party software, Quantec reserves the right to assess from time to time any changes to be made to its software, evaluate the time and manner of application and, in any case, decide at its discretion whether or not to carry them out;
4. Any material downloaded or otherwise obtained through the use of the services is at the risk and discretion of the user, who shall be solely responsible for any damage to their computer systems or other devices, as well as the loss of data resulting from the download of such material;
5. The user acknowledges, assuming sole responsibility in this regard, that the use of the IndependenceKey and services is not suitable for situations or environments in which failure, delays, errors or inaccuracies of content, data or information provided by the product and services may result in death, physical or environmental damage, including, but not limited to, situations which use nuclear equipment, flight or aircraft communication instrumentation and systems for air traffic control, assistance or weaponry, including military uses. For these applications, Quantec provides a specific version of the IndependenceKey;
6. Any information or advice, whether oral or written, obtained by the user from Quantec or their authorised representatives, shall in no case be regarded as a form of guarantee by Quantec. In the event of defects in the software or services, the costs of interventions, fixes and repairs that may be required will be fully borne by the user;
7. The limitations referred to in this paragraph shall be construed as being valid and enforceable to the extent compatible with the applicable law, as specified in paragraph 11, below.

10. LIMITATION OF LIABILITY

To the extent permitted by applicable law, Quantec is absolved from any liability for any personal injury or any damages, whether direct or indirect and of every type and kind, including, but not limited to, damages for loss of earnings, interruption of activity, data loss or damage, errors in the transmission or reception of data or other commercial damages or loss, arising out of or related to: (i) Disruption of software operations due to a lack of power supply or the forced removal of the IndependenceKey device from the computer or a mass storage memory device connected to the port at the back of the IndependenceKey while it was operational or without having first carried out the proper "unmount" procedure using the software, (ii) use or misuse of the Software, services or of any third party software or application in conjunction with the Software or (iii) any other aspect related to the services.

In no event shall the liability of Quantec to user exceed the amount of five Swiss francs (CHF 5.-) for the damage as a whole.

The limitation of Quantec's liability herein described applies regardless of the cause of the damage and the origin of responsibility (interruption of the contract, tort or otherwise) and even in cases where Quantec had been advised of the possibility of such damages occurring.

The limitations referred to in this paragraph shall be construed valid and enforceable to the extent compatible with the applicable law, as specified in paragraph 11, below.

11. EXCLUSIONS

Some jurisdictions do not allow the exclusion of certain guarantees or conditions or the limitation or exclusion of liability for personal injury, loss or damage caused by negligence, breach of contract, breach of implied terms or incidental or consequential damages. Therefore, the limitations referred to in paragraphs 9 and 10 are understood as only being applicable to the extent they are not prohibited by the laws applicable where the user is located and/or where the product is used.

CONTROLLED EXPORT

It is forbidden to use, export or re-export the product except in accordance with the laws of the United States of America or the country in which the product was purchased. In particular, but without limitation, it is not possible to purchase, export or re-export the product:

1) In any country embargoed by the United States;

2) To anyone on the Specially Designated Nationals list of the United States Treasury Department or the Denied Person's List or Entity named List of the United States Department of Commerce (detailed information available at <http://www.bis.doc.gov/entities/entitylistfaq.html>).

By using the product, the user expressly states and guarantees that he/she does not appear on the lists mentioned above and is not located in one of those countries. In addition, the user agrees not to use the software for any purposes prohibited by law, including, but not limited to, the development, design, manufacture or production of weapons, nuclear, chemical or biological weapons and missiles.

OTHER RIGHTS

Rights which have not been published are protected by the Swiss Federal laws on copyright, available at the address http://www.admin.ch/ch/i/rs/231_1/index.html.

GOVERNING LAW AND THE POSSIBLE INVALIDITY OF ONE OR MORE CLAUSES

The terms and conditions of the licence are subject to the laws of the Swiss Confederation and will be applied and construed in accordance with them.

The possible inapplicability and/or invalidity and/or unenforceability of one or more clauses or parts of the terms and conditions of this licence do not imply inapplicability and/or invalidity and/or unenforceability of the other clauses or parts of clauses, which, being fully valid and enforceable, will continue to be applied.

INTEGRITY OF THE AGREEMENT

This licence supersedes all prior agreements and constitutes the entire agreement between the user and Quantec regarding the use of the software and services. Any amendments or changes shall be valid and effective only if they are set down in writing and signed by one of Quantec's authorised representatives.

Any translation of this licence is provided solely for convenience and does not have legal value.

Should the Italian version of the licence and the translated version differ, the Italian version shall be deemed the correct one, to the extent permitted by the laws applicable where the user is located and/or where the product is used.

The above English text named 'Software Licence Terms and Conditions' should be considered indicative. For all legal intents and purposes it is valid only and exclusively the document 'USO DEL SOFTWARE' in Italian which you can find on our web site www.independencekey.com

Copyright ©2012 Quantec SA. All rights reserved.

Quantec SA, Corso San Gottardo 86, CH-6830 Chiasso, Ticino.

Updated on 05/03/2013

For more information, contact info@quantecclub.com

Hardware Warranty

HARDWARE WARRANTY

This warranty gives the user specific rights, in addition to those under the laws of the user's state (country or region) and does not exclude, limit or suspend any of the user's rights, including those that may result from non-conformity with the contract of sale.

We invite the user to consult the regulations of his/her country, region or state.

Limitations

To the extent permitted by law, this warranty and the remedies set forth are exclusive and in lieu of all other warranties, remedies and conditions, whether express, implicit, verbal, written or statutory. Quantec specifically disclaims any statutory guarantees, including, by way of example, guarantees of merchantability and fitness for a particular purpose or for hidden or latent defects. Where applicable laws do not allow Quantec to disclaim these warranties, Quantec limits the duration and remedies of this warranty to the period of its duration and, at its discretion, the repair and replacement service. In countries, states and regions that do not allow limitations on the duration of implied conditions and warranties, the limitations mentioned here may not apply.

Coverage

Quantec guarantees that the hardware products and accessories in the original packaging ("Quantec Products") are free from material and manufacturing defects for two (2) years from the date of purchase by the end user ("Warranty Period") when used in accordance with the guidelines provided by Quantec. By way of example, the guidelines include the information contained in the user manual, technical specifications, website and the communications service.

NOT guaranteed coverage

Quantec does not guarantee that the operation of the product will be interruption or error free. Quantec is not liable for damage caused by not following the operating instructions of the product. For further information of user rights regarding use of the software, please refer to the Quantec Software Licence.

The warranty does not apply to:

- 1) Consumable components, such as protective coatings that wear over time, unless the problem is caused by a manufacturing defect or poor workmanship;
- 2) Damage caused by use with products that are not made by Quantec;
- 3) A product whose serial number has been removed or rendered illegible;
- 4) Damage caused by services (including enhancements and upgrades) performed by anyone who is not a representative of Quantec or one of its authorised service providers;
- 5) A product that has been modified to alter its functionality or capability without the written consent of Quantec;
- 6) Damage caused by accidents, abuse, misuse, liquid contact, fire, earthquakes or other external causes;
- 7) Damage caused by the use of the product not in accordance with the used intended or described by Quantec;
- 8) Cosmetic damage, including but not limited to, scratches or dents on all metal or plastic surfaces;
- 9) Defects caused by normal wear and tear or otherwise caused by normal aging.

Important limitations

Quantec reserves the right to limit the warranty service in the country in which Quantec or its authorised distributors originally sold the product.

User responsibility

Il dispositivo crittografico portatile IndependenceKey (d'ora in avanti "IKEY") è un apparato elettronico progettato per applicazioni nel solo ambito consumer. L'utente deve prestare attenzione a quanto descritto nel manuale di istruzioni ed evitare di collegare alla presa USB presente sul retro del prodotto dispositivi non conformi USB e non rientrati nelle specifiche funzionali del prodotto IKEY. IKEY consente di The portable cryptographic device called IndependenceKey (henceforth "IKEY") is an electronic device designed for applications in the consumer sphere only. The user must pay attention to what is written in the instruction manual and avoid using the USB port at the back of the product to connect non-compliant USB devices and those that are not included in the functional specifications of the IKEY product. IKEY allows the USB port at the back to be used to connect common USB data storage flash "drives", only USB Hard Disks that are externally powered via their own adaptor, USB keyboards, USB mouse and all the IKEY range of accessories, including the "Security Cap" device, the "Data Bank" and specific digital USB headsets.

The "Security Cap" device allows the recovery of information in the event of amnesia or the loss, theft or malfunction of the main IKEY device. It is therefore recommended that a back-up should be carried out using Security Cap, as expressly stated in the instruction manual accompanying the product, or that the optional Data Bank automatic back-up service should be used when available.

Before performing the warranty service, it may be necessary to provide proof of purchase, reply to direct questions by the support service for the diagnosis of possible problems and follow set procedures for obtaining the warranty service. Before delivering the product to the warranty service, the user should: Contact the service centre to identify the nature of the problem with the IKEY or the Security Cap and only then proceed with the shipment of the product as instructed.

IKEY contains, in an encrypted form which is not accessible without the user's Master Password, all the identification elements of the user, the cryptographic keys generated during use of the device itself and the associations with other users and data relating to the Password Manager (data on access to websites, third party services, e-mail, home banking and so on). The version with internal mass storage also contains its own storage, which is also fully encrypted, like a traditional flash drive USB device.

Following the repair service, the product or a replacement product will be returned to the user, where possible, with the user data or in the configuration in which the original product was purchased, appropriately updated and without user data. In this case, Quantec and its agents are not responsible for damage or loss of software programs, data files or any other information contained on that media or of any part of the product covered by this warranty. The user is responsible for restoring data. In this case, the product returned to the user without the user's original data can be reset using the appropriate procedures related to the product using its own back-up device called "Security Cap", following the product's procedures.

In this case, when the content of the Quantec device is lost or reformatted/reset during the warranty service, in order to restore content, the user must have the Security Cap back-up device in the event of a malfunction of the IKEY or the IKEY in case of a malfunction of the Security Cap. In the absence of both, Quantec cannot under any circumstances guarantee the restoration of lost data, user's identification data, cryptographic keys generated during use of the device itself, associations with other users or data related to the Password Manager. In addition, the user can still subscribe to the "Data Bank" on-line service and, therefore, use the "Data Bank" device to restore. This service is optional and is not included in the standard IKEY package.

The recovery and restoration of data on the user's IKEY are the responsibility of the user and are not covered by this warranty. Please note that failure to restore such data on the part of the user, due to not having the Security Cap device in the case of the IKEY being repaired/replaced under warranty, not having the IKEY in the case of the Security Cap being repaired/replaced under warranty or not having either device belonging to the user makes it impossible to recover the user's data, cryptographic keys, data associated to other users and data related to Password Manager and the subsequent impossibility of accessing files, folders and disks that have been previously encrypted. With this in mind, it is always recommended that the user place the Security Cap in a safe place that can only be accessed by the user, with a temperature that is preferably between 0°C and 30°C and under controlled conditions of humidity. In addition, the user can use the automatic and continuous on-line back-up service by using the "Data Bank" (optional), with the possibility of having a third device for the recovery of the data mentioned above in case of loss, damage or repair/replacement under warranty of either the IKEY or the Security Cap.

Important: Do not try to open the product and/or unsolder parts. Attempting to open the product causes damage which is not covered by the warranty. Only Quantec or a service staff member can provide assistance on this product. Unauthorised opening of the product immediately renders the warranty invalid.

Warranty

In the case of a valid request being received within the warranty period, Quantec may, at its discretion:

- 1) Repair the product using new or reconditioned parts that are equivalent to new ones in terms of performance and reliability;
- 2) Replace the product with another having the equivalent minimum functions, made of new or used parts that have the same performance and reliability as a new product;
- 3) Refund the purchase price of the product (excluding original shipping costs and any duties) upon it being returned.

Quantec guarantees the product for two (2) years.

Replacement parts will be guaranteed either for the remaining warranty of the product or for one (1) year from the date of replacement or repair, whichever is longer. Following replacement, the replacement product or part becomes the property of the user and the product or part which has been replaced becomes the property of Quantec.

Warranty service

Before requesting the warranty service, the user is invited to consult the on-line help resources (FAQ, FORUM, BLOG) at the www.independekey.com site. In the event that the product still fails to work properly even after having followed the instructions in the on-line help resources, the user may contact Quantec according to the information below. A Quantec representative and/or Quantec support technician will assist the user in order to ascertain whether the product requires the assistance service and, if so, will explain how Quantec provides the warranty service.

Quantec will provide the warranty service in one or more of the following ways:

- Purchase from an authorised dealer. The user may deliver the product to a Quantec dealer. When the user receives notice that the service has been carried out, the user shall be required to pick up the product promptly from the dealer. Any shipping charges will be borne by the user.
- On-line purchase. The user may ship the product to Quantec at the user's expense. Once the service has been carried out, Quantec will ship the product to the user, bearing the shipping charges and informing the user immediately.

Quantec reserves the right to modify the conditions of the warranty service to the user and the availability of certain types of services on the product. The types of service will be limited to the options available depending on the country from which the warranty service request is received. The service options, availability of parts and response times may vary from country to country. If the product cannot be repaired or replaced in the country in which it is located, the user will have to bear the cost of shipping and handling related to the service. If the warranty service is requested in a different country to the one in which the product was bought, the user must comply with the applicable laws and regulations governing import and export, bear the cost of customs duties, VAT and any other associated taxes and charges. In the case of the international warranty service, Quantec may repair or replace defective products and parts with comparable ones that comply with local regulations.

Limitations on liability

Except as provided in this warranty and up to the maximum extent permitted by law, Quantec is not liable for any direct, special, indirect or incidental damages arising from a breach of the warranty or its provisions, including those imposed by any other legal principle, including, but not limited to, damage to reputation; loss, damages, alteration or destruction of data; loss of use, loss of revenue, loss of

actual or contractual profit; loss of cash flow; loss of expected savings; loss of business; loss of opportunities; loss of goodwill; or any loss or indirect or incidental damages regardless of the cause, including the replacement of equipment and property, costs of data recovery, reprogramming or reproduction of programs or data stored or used by the product.

Quantec does not specifically guarantee that it will be able to repair or replace any product covered by this warranty without risk or loss of programs or data stored on the product, including the identification of the user, cryptographic keys, data associated to other users and Password Manager data, nor can it be held responsible for the loss of any type of data, information or files contained therein or the impossibility in such cases of accessing data, files, folders and disks that have been previously encrypted using IKEY.

The limitations and exclusions mentioned above may not be applicable in countries, regions and provinces that do not allow exclusions or limitations in cases of incidental or consequential damages.

Privacy

Quantec commits to maintaining and using customer information in compliance with the Privacy Policy, available on page <http://www.independencekey.com/blog-en/privacy/>

Miscellaneous

Quantec dealers, agents or employees are not authorised to make any modifications, extensions or additions to this warranty. In the event that some of the conditions of this warranty are held to be invalid, void or unenforceable, all remaining provisions will remain in full force and effect. This warranty is subject to the governing law of the place in which the product was purchased and it must be interpreted on this basis.

Quantec or its assignees are providers of the warranty service on the basis of this warranty.

The above English text named 'Hardware Warranty' should be considered indicative. For all legal intents and purposes it is valid only and exclusively the document 'GARANZIA HARDWARE' in Italian which you can find on our web site www.independencekey.com

Copyright ©2012 Quantec SA. All rights reserved.

Quantec SA, Corso San Gottardo 86, CH-6830 Chiasso, Ticino.

Updated on 05/03/2013

For more information, contact info@quantecclab.com

Privacy Terms

The Privacy Policy govern the modalities and limits of the collection, use, retention, disclosure, transfer and storage of data by Quantec and clarify the tools available to the user of Quantec's services (the "User" and/or "Users") for the protection of their privacy.

We encourage users to read this document carefully and contact Quantec should there be any questions.

1. Introduction

Quantec **has no way of detecting encryption keys or accessing encrypted data user**. Therefore:

1. The user is solely responsible for the material that he/she decides to encrypt and must do so in accordance with local governing laws.
2. Upon user access, Quantec stores the date and time of access, the user IP address and related geographic data on its servers. For user accounting services regarding websites and assistance (trouble ticketing), Quantec stores the user's account and related optional data provided solely for purposes of ensuring safe and secure access to restricted areas and assistance services.
3. If the user makes use of Quantec advanced services (for example, secure file transfer or streaming connections with other users), Quantec will merely be aware of when information is being shared between identified users (knowledge which is necessary for the provision of advanced services); the type and content of the information shared will remain completely unknown to Quantec. Any file and/or collection of data in transit through Quantec servers is encrypted with the user's encryption keys (the "Keys"), which are managed exclusively by the user. The Keys reside in the user's IndependenceKey device, which can be unlocked only (i) by connecting the Security Cap to which the device is uniquely associated or (ii) using the User Master Password known only to the user.
4. The optional data referred to in point 2 and what has been specified in point 3 constitute the only information available to Quantec, which Quantec will therefore make available when ordered, faced with an injunction or requested to do so by any public authority or government agency. Quantec will not be able, in any way, to disclose the type and content of information that users can exchange directly and/or through their own servers, because they will have been encrypted at source using the application of cryptographic keys known only to the users. Unless clearly necessary to deliver advanced services, Quantec will not store or maintain the data in transit, except for the minimum time necessary; under no circumstances will Quantec store and maintain data in transit related to real-time streaming services such as VoIP services.

2. DATA COLLECTED

Type of data collected by Quantec:

Personal data: Any information concerning an individual or legal entity, whether identified or identifiable, (using the same data or) even indirectly, by reference to any other information, including a personal identification number (for example, name and surname);

Non-personal or anonymous data: Data not clearly pertaining to a particular subject and therefore unfit to allow, either directly or indirectly, its identification (it covers so-called aggregate data: Data grouping en masse information on multiple users, with a statistical/business aim: for example, the detection of websites and Quantec products of the greatest interest to users).

2.A Method of data collection

The collection of user data (personal or otherwise) by Quantec has the purpose of improving the products and services that Quantec offers the user. To do this, Quantec reserves the right to combine the personal data collected with other data.

Method of data collection:

a) Personal data provided by users

Coming into contact with Quantec, the user may be required to provide their personal data: The purchase of products and the use of Quantec services may require the creation of an account by the user. When creating the account, the user may be required to provide certain personal information, such as name and surname, e-mail address, telephone number (optional) and VAT No. in the case of business users.

b) Personal data collected through the use of Quantec services by the user

Through the activation and use of the IndependenceKey, downloading of software updates, access to forums on the product's websites, Quantec will collect:

- (i) The user's nickname and alias, the serial number of the product, the serial number that identifies the user and any additional optional data the user has entered into the management software that comes with the product (name, surname, e-mail, company, website, etc.);
- (ii) The information data of the machine on which the software is installed (for example, microprocessor type and speed, screen resolution, type of operating system, amount of RAM available to applications and disk capacity)..

c) Non-Personal data collected from the use of Quantec services by the user

Quantec can collect information on services used by the user and how they are used. For example, Quantec may collect data regarding the activities of users on the Quantec website, forums and IKey Store, or activities recorded by other Quantec products and services.

2.B Purposes and methods of use of the data collected

Quantec uses the data collected within the terms referred to in paragraph 2A above:

- 1) To ensure that the user is continually updated, for example on the latest Quantec products, software updates and any events promoted by Quantec;
- 2) For the purpose of marketing: Commercial and advertising strategy;
- 3) For communications relating to the contractual relationship with the user: for example, communications relating to the purchase of products and any modification to the terms and conditions of the Quantec licence;
- 4) To increase the compliance of Quantec products and services with the needs and expectations of the user, even in terms of assistance and web content;
- 5) For internal purposes of analysis, testing and research, with the aim of continually upgrading the quality Quantec products and services. It is reiterated that Quantec has no way of detecting encryption keys, cannot open files, folders or drives that have been encrypted using IKEY. The data collected during analysis and research is therefore confined to the performance of the device.

Cookies and other anonymous identifiers

Il sito web, i servizi online, le applicazioni interattive, i messaggi email e le pubblicità di Quantec potrebbero avvalersi di "cookie" o altri identificatori anonimi (ad esempio pixel tag e web beacon) per raccogliere e memorizzare informazioni relative all'accesso e/o utilizzo dei servizi e siti web Quantec da parte dell'Utente.

Come accade nella magThe website, on-line services, interactive applications, e-mail messages and advertisements by Quantec may use "cookies" or other anonymous identifiers (such as pixel tags and web beacons) to collect and store information on the access and/or use of Quantec services and websites users.

As is the case for most of websites, some data is collected automatically and stored in log files. Thus data includes Internet Protocol (IP) addresses, browser type and language, Internet Service Provider (ISP), input/output pages, operating system, date, time and clickstream data.

The data collected through cookies or other anonymous identifiers helps to understand the behaviour, trends, expectations and the goals of users. It allows detection of which parts of the site are most frequently visited, which services are used the most and allow the effectiveness of the advertising and marketing strategies adopted to be tested. Through this data it is possible to improve and "customise"

the Quantec experience for each user (for example, if a user were to save a language preference, it would be possible to view the services in that user's preferred language) and to increase the overall quality of Quantec services.

Data collected using cookies or other anonymous identifiers are treated as non-personal information. Nevertheless, to the extent that Internet Protocol (IP) or similar identifiers are considered personal data by local law, these identifiers will be treated as personal data. Similarly, to the extent that non-personal data is aggregated with personal data, such aggregated data will be treated as personal data.

2.C Accessing and updating personal data

Users who elect to use Quantec services are put in a position where they have access to their personal data. If the user points out that the data is incorrect, Quantec will allow it to be updated or deleted, unless it needs to keep it for legitimate business or legal purposes. In the case of updating personal data, users will initially be asked to confirm their identity.

Quantec reserves the right to refuse any requests to update and/or delete the data collected, where such requests require unduly burdensome and/or disproportionate technical effort (for example, the development of a new system or the significant modification of an existing practice), jeopardize the privacy of others or if they cannot actually be carried out (for example, requests concerning information residing on backup devices).

In order to avoid any malicious or accidental destruction of data, once the user has decided to remove his/her data from Quantec services, Quantec may not immediately eliminate the remaining copies on the active servers and may not remove the information from the backup systems.

2.D Dissemination of collected data

Quantec does not provide the user's personal data, without consent, to companies, organisations or third parties, subject to the following exceptions:

(i) Quantec shares your personal data with companies that carry out user orders, deliver products and provide logistical assistance. These companies may be located wherever Quantec operates and are obliged to protect the user's personal data under the terms set out in this policy, with the utmost care and diligence;

(ii) According to law, prosecution, disputes, and/or requests from public and governmental authorities within or outside the country of residence, reasons of national security, law enforcement or other issues of public importance, Quantec may be required to disclose the serial number of the product used by a given user and any available history of connections to other users. No other data will be disclosed by Quantec under these circumstances. As already mentioned, any files or data in transit through Quantec servers cannot be decrypted without the IKEY device and its Master Password and/or Security Cap, which are possessed by and are exclusively available to the user. Any information disclosed by Quantec in the cases mentioned herein is therefore not suitable, under any circumstances, for accessing the encryption keys, nor does it allow the decryption of the user's data.

(iii) In the case of restructuring, merger or sale, Quantec reserves the right to transfer all collected data to a third party.

2.E Protection of collected data

Quantec takes precautions, technical, physical and administrative procedures adopted according to normal professional diligence, in order to protect personal data against loss, theft and misuse, as well as unauthorised access, disclosure, alteration and destruction.

On-line services such as Quantec IKEY Store use Secure Sockets Layer (SSL) encryption systems on all web pages where personal data is collected. To make purchases through using these services, the user is asked to use an SSL-enabled browser such as Safari, Firefox or Internet Explorer, for greater protection of personal data transmitted over the internet.

WARNING: Using certain products, services or applications, publishing on forums, chat rooms or social networking service provided by Quantec, shared personal data is visible to other users and may be read, collected or used by them. On such occasions, the user has sole responsibility for the personal data submitted.

The services provided by Quantec servers are subject to the channel's hardware encryption and authentication, obtained directly from the IndependenceKey device and the servers themselves. Communications are, therefore, all encrypted and the data itself is stored in the Quantec data centre in a building physically located in Switzerland, secured and protected in special rooms equipped with biometric authentication. The telematics connection to these servers is, therefore, managed directly between the servers and the IndependenceKey device via the host computer in which the device itself is inserted. Therefore, all communications between IndependenceKey and the servers are encrypted at a hardware level, communications designed to provide the services of first connection and activation, remote association between users, file sharing and VoIP telephony through advanced Quantec services. It is reiterated that Quantec servers can also never ever access the contents of files, data and VoIP streams exchanged between users because they, in turn, have been encrypted at the source using unique cryptographic keys known only to the IndependenceKey devices belonging to the users themselves.

2.F Storage of collected data

Quantec stores personal data in a careful, complete and updated manner for the time necessary to achieve the purposes of the services provided in accordance with this Privacy Policy, unless a longer retention period is required or permitted by law.

3. EXCLUSIONS

Minors

Quantec does not collect personal data from and/or relating to persons under the age of 13 years. Should such an event occur, Quantec will immediately eliminate said data as soon as it becomes aware of the situation.

Third party sites and services

Quantec internet sites, products, applications and services may contain links to internet sites, products and services of third parties to which this Privacy Policy is not applicable. The user is therefore advised to consult the privacy regulations of these third party providers.

4. CHANGES

The Privacy Policy referred to herein may be subject to occasional changes. Quantec is committed in any case not to reduce the rights of users without their express consent. Any changes to this Privacy Policy will be posted on this page. Earlier versions of this Privacy Policy will be archived and will remain accessible by users at all times.

The above English text named 'Privacy Terms' should be considered indicative. For all legal intents and purposes it is valid only and exclusively the document 'PROTEZIONE DEI DATI' in Italian which you can find on our web site www.independencekey.com

Copyright ©2012 Quantec SA. All rights reserved.
Quantec SA, Corso San Gottardo 86, CH-6830 Chiasso, Ticino.

Updated on 05/03/2013

For more information, contact info@quantecclub.com

Microsoft Windows XP SP3, Windows Vista 32 & 64 bit,
Windows 7 32 & 64 bit compatible.



Norms and Technical References : EN 55022, EN 61000-4-2, EN 61000-4-4,
EN 61000-4-6. FCC PART 15 SUBPART B CLASS B



Copyright © Quantec SA 2013
IndependenceKey™ is a Trademark of Quantec SA
International PCT Patent Pending

Patents pending in Switzerland with international extension procedure PCT
in 138 countries # 0021212 of 17/02/2012 and # 0075312 of 01/06/2012

QUANTEC

QUANTEC SA
Corso San Gottardo, 86
6830 Chiasso
Switzerland
Telephone: +41.(0) 91.696.16.16
Email: info@quanteclub.com

