

## FACTSHEET FS 2009-02

**Limits on cryptography: working with confidential information abroad.**

This factsheet reflects the situation from a Dutch perspective. This means that all the situations set out here apply to travellers going from the Netherlands to other countries.

The partners of the government and business community are increasingly situated abroad. It often happens that one takes abroad digital information of a confidential nature for the purpose of cooperating with foreign partners. Such confidential business or personal information, which may be found on laptops, USB sticks, PDAs or other data-carriers, is in many instances secured by means of cryptographic techniques.

Many people are not aware that there are restrictive laws and regulations in many countries concerning the possession and use of encryption tools. It is therefore not always permitted to make use of encryption in a country or to import encryption products. In addition, some countries reserve the right to demand access to information protected using cryptographic techniques.

This factsheet contains valuable information to remember when travelling to other countries with encryption tools or encrypted files. There are separate rules regarding classified information within the government covered by the Civil Service Information Security Regulations for Classified Information (VIR-BI).<sup>1</sup> This information falls outside the scope of this factsheet.

**Cryptography is everywhere**

Cryptography is widely used. We are usually aware of the fact that we are using encryption tools, but sometimes we use these without being directly aware of it. This includes:

- encryption of files or entire data-carriers (USB sticks, hard disks);
- protection against access to information on a data-carrier (computer, PDA etc.) with the use of, for example, a password;
- web surfing via a secure connection (https);
- setting up and using a secured VPN connection (for example, to create a secure connection from ones home or elsewhere to ones office);
- sending secure e-mail;
- creating a digital signature.

Some products using encryption are:

- web browsers, such as MS Internet Explorer, Mozilla Firefox, Opera and Safari;
- products for file or disk encryption, such as TrueCrypt and Safeguard;
- products for creating digital signatures or secure e-mails. Examples include 'Pretty Good Privacy' (PGP) and derived products, such as GPG or other techniques for securing e-mails, such as S/MIME;
- VPN-client software, included as standard in operating systems like Windows XP/Vista or Mac OS X, and other special products from e.g. Cisco.

In brief, cryptography is far more widely used than many believe.

**Overview of the most important facts:**

- > Confidential information is more and more often protected by means of cryptographic techniques.
- > Various countries impose restrictions on the use of and travel with cryptographic techniques.
- > It is not always permitted to make use of cryptography in a country or to import cryptographic products.
- > Foreign authorities may demand access to or decryption of information on laptops or other mobile data-carriers.
- > By granting access to third parties, you may lose control over the dissemination of your confidential information.
- > You need to consider in advance which information you wish to take with you and how you want to and are allowed to protect it.

<sup>1</sup>For the complete text of the VIR-BI (Dutch: Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie) please see (Dutch version) : <http://www.minbzk.nl/contents/pages/3811/voorschriftinformatiebeveiliging.pdf>

## Which legislation and regulations could affect you?

The legal and regulatory restrictions imposed by some countries on possession and use of cryptography can be divided into three main categories:

### 1. **Restrictions on the use of cryptographic products**

A number of countries impose restrictions on the use of cryptography. These restrictions are usually combined with import restrictions to prevent residents from gaining access to prohibited cryptographic tools. Such restrictions are usually based on the need for official bodies to monitor communication flows for the purposes of investigations and information.

Some well-known examples of countries that impose such restrictions are:

- France imposes restrictions on the use of cryptography by security service providers, such as trusted third parties (ttp's). In the past, France imposed greater restrictions, but these have been reduced in recent years.
- Poland places restrictions on the importation of cryptographic tools, but this does not cover standard cryptographic software for private and business use that complies with the requirements of the 'General Software Note'<sup>2</sup> in the Wassenaar Controls (see also box below).
- India places restrictions on cryptography used in hardware, but not in software.
- South Africa does not place restrictions on business or private use, but does restrict use by security service providers.
- Other countries such as China and the former Soviet republics prohibit all forms of cryptography, unless the authorities have given their explicit consent for its use.

### 2. **Legislation regarding granting access to data-carriers**

In certain cases authorities can demand access to your data-carrier or disclosure of passwords or keys, in order to inspect your data-carrier. This usually happens in the following two cases:

#### *When crossing an international border*

This is comparable to opening your suitcase, so that customs staff can search it for prohibited goods. Usually they simply want to be sure that your laptop is really just a laptop (and not a bomb, for example) and incidentally also whether you are carrying any prohibited information. For the purposes of greater clarity, the US customs for example have made their guidelines for border inspections of data-carriers publicly available, with explanations.<sup>3</sup>

#### *In the context of a criminal or other investigation*

The police, the courts or security services may request access to data-carriers or surrender of passwords in the context of a (criminal) investigation. It is best to be aware that your cooperation is compulsory in certain countries. Even the right not to incriminate yourself does not always apply. If you refuse to surrender a decryption key, you can be imprisoned for a maximum two years in Great Britain.

Countries that impose an obligation to decrypt include The Netherlands, Belgium, France, Great Britain, Australia and India. The USA does not impose any obligation to decrypt inside the country, but does operate strict border controls.

<sup>2</sup> <http://www.wassenaar.org/controllists/2008/>

<sup>3</sup> [http://www.eff.org/files/filenode/alc/071608\\_cbp\\_policy.pdf](http://www.eff.org/files/filenode/alc/071608_cbp_policy.pdf)

### 3. Export restrictions because cryptographic tools can also be used for military ends

Certain advanced cryptographic techniques are also designated 'dual-use goods' in many countries, meaning they can be used for military purposes, and are therefore subject to export restrictions. These restrictions are known as the 'Wassenaar Controls' and are imposed by a large number of countries. There are also comparable EU regulations in this field (see Council Regulation (EC) No 2432/2001). EU regulations allow almost completely free circulation within EU Member States and only impose restrictions on very advanced cryptographic and crypto-analysis tools. The 'Wassenaar Controls' also only apply to advanced forms of cryptography. They do not cover the use and possession of standard or freely available products intended for personal or business use.

#### The most important parts of the Wassenaar controls:

- > There are no export restrictions on: symmetric cryptography with a maximum key length of 56 bits, any asymmetric cryptography with a maximum key length of 512 bits and any other cryptography (including elliptical curves) up to 112 bits key length.
- > The export of products that utilize encryption in order to protect intellectual property is only permitted to a limited extent.
- > A licence is still necessary for the export of other cryptographic tools.
- > There are no restrictions on cryptographic products or algorithms that are freely available and in the public domain

There are restrictions on algorithms or software that contains such algorithms. For more information about the 'Wassenaar Controls' see [www.wassenaar.org](http://www.wassenaar.org).

#### What does this mean for you?

The legislation and regulations we have described regarding the use of cryptography involve risks for you as a traveller and for your organization. You could be breaking the rules in certain countries if you use or are in possession of cryptographic products.

What is more, the compulsory granting of access to your data-carrier or surrendering of your password may result in a breach of your confidential data. You should therefore watch out for (industrial) espionage, for example, if you are required to hand over data-carriers. From this point of view, you also need to be alert to copies being made of your information, as suspected by the AIVD (General Intelligence and Security Services of the Netherlands) and also described in a brochure on (industrial) espionage risks<sup>4</sup>. One can also find experiences on the internet describing border controls where laptops are seized and only returned to the owner after a long time (1 year). You need to keep in mind the above risks, although GOVCERT.NL has not as yet received any indications that these are standard practices.

Remember that by granting access, you may lose control over the dissemination of your confidential information. This may have serious consequences for the future security of your organisation. If you hand over an encryption key (instead of decrypting and only handing over a decrypted file) the risk arises that other files that can be decrypted with the same key will also become accessible, and that everything that you want to protect with that key in the future will also become accessible. If you surrender the key used to create your electronic signature, then other persons can use this to sign messages in your name. What if you are required to surrender an encryption key? Inform your organisation of this, so it can take countermeasures. Consider revoking the keys or encrypting the information again with other keys.

If you come into contact with authorities that try to gain access to your data-carriers, it is unwise to deny that you make use of cryptography or to try to hide this. As soon as there is a suspicion that you are trying to hide the use of cryptography or if you deny this, then the consequences can be serious, for example, confiscation of the data-carrier, enforced surrender of the encryption key(s) with the threat of serious punishment, or being placed on a blacklist so that it becomes impossible to re-enter that country in the future.

<sup>4</sup> Dutch version: <https://www.aivd.nl/contents/pages/96114/spionagerisicosbijreizenaarhetbuitenland.pdf>

## Recommendations with regard to dealing with confidential information abroad

The risks that we have set out indicate that when you travel abroad you could find yourself in a situation where you are required to grant access to your data-carriers. We have set out some recommendations in order to handle confidential information in the best possible way.

In the first place we advise you to secure your information in such a way that you can always cooperate with the authorities if they request access to your data-carrier. As an organisation you should not try to shift the risk to an individual employee by trying to conceal the use of cryptography.

Ask yourself or the organisation the following questions before you travel abroad:

1. Is the information that you are taking with you (or which you are going to receive at your destination), confidential in nature?
2. Are there statutory or other obligations to protect the information, for example in the context of the Personal Data Protection Act? (In Dutch: WBP)
3. Is there a risk in the destination country that you will be asked to allow data to be examined?

If you have to answer any of these questions in the affirmative, consider the following:

- Always use a *clean 'travel laptop'*, meaning that you should use a laptop or data-carrier that does not hold or has never held confidential information (unless the information has really been deleted; see box 'Total removal').
- Are you going to visit a branch of your own business/organisation? Enquire whether you can send the information in a secure form *via the company's network* (both from the Netherlands to another country or if need be the other way round) and then place this on your laptop or data-carrier when you arrive. An alternative is to create a secure connection (e.g. a VPN)<sup>5</sup> with the corporate network and to copy the confidential information to your laptop/data-carrier, so you can use or process this at your destination.
- *Clean up your data-carriers* before you return. This means sending the confidential information on your laptop or other data-carrier back to your own organisation in a secure manner (as described under the previous point). Then remove all the confidential information from your laptop/data-carrier (see box 'Total Removal'). Make sure that your laptop is in fact switched off while you are travelling! There may still be important information left behind if you are in stand-by mode. Do not forget the information on your PDA, Blackberry, mobile telephone and associated memory cards.

### Total removal - how can I do that?

Although many people are not aware of it, deleted files or formatted disks can almost always be restored, sometimes with the use of additional tools. This means that information can still be read later on. If you want to be sure that information has been definitively removed, then we advise you to make use of special tools such as PGP-shredder or Eraser. Such tools overwrite old data several times so that they are almost impossible to read, even with the use of specialized tools. Remember that this method of deletion can take a great deal of time (up to half a day with the current capacity of hard disks). If you want to reduce the deletion time, you can delete only files that hold confidential information. The risk here is that you will fail to delete some files.

You can find more instructions about how to clean up media among other places in NIST publications.<sup>6</sup>

## Conclusion

Legislation and regulations are constantly changing everywhere. Given the great number of countries and the fact that it is difficult to interpret legal wording precisely, this factsheet can only give a general idea of the issues and does not deal with specific situations in detail. GOVCERT.NL therefore recommends that you always seek legal advice for specific situations.

A good starting point is the 'crypto law survey' by Bert-Jaap Koops of the Tilburg University, which provides a global overview of countries with restrictive legislation and regulations. See <http://rechten.uvt.nl/koopscryptolaw>.

<sup>5</sup> Given that you will need to make a connection between your laptop and the internet for this purpose, it is important to ensure that your basic security (anti-virus and firewall) are in order.

<sup>6</sup> See for example [http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88\\_rev1.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)