



BIOVISION

Report on legal and privacy issues

Project Number	IST-2001-38236
Project Title	BIOVISION Roadmap to Successful Deployments from the User and System Integrator Perspective
Deliverable Type	Document

Deliverable Number	BIOVISION: D 7.3 & D 7.5
Contractual date of delivery to Commission	
Actual date of delivery to Commission	28 August 2003
Title of the Deliverable	Final report on regulatory aspects and data protection requirements
Work Package contributing to the Deliverable	WP 7
Editor	Astrid Albrecht and Martin Walsh (Daon)

Abstract:

- This report carries out a first assessment of EU and Member State regulatory environments from a biometric viewpoint in light of legal and e-signature requirements
- Provides an outline of guidelines covering the data protection requirements of biometrics for users, suppliers manufacturers etc
- Provides a draft Code of Best Practice for the development, manufacture and use of biometrics from a legal and regulatory standpoint

History About this document

Any enquiries about this document should be directed to:

Martin Walsh

Daon
IFSC House
Custom House Quay
Dublin 1
Ireland
martin.walsh@daon.com

Dr. jur. Astrid Albrecht
Head of TeleTrusT Working Group 6 Biometrics
TeleTrusT Deutschland e.V.
Chamissostrasse 11
99096 Erfurt
Germany
<http://www.teletrust.de>
AAlbrechtLaw@aol.com

and

Steffan Wettig
Friedrich Schiller University Jena
Department of Computer Science
Ernst-Abbe-Platz 2
D-07743 Jena, Germany

wettig@informatik.uni-jena.de

Contents

1	INTRODUCTION.....	4
	The issues being faced	5
1.1.1	Travel, immigration and border control.....	7
2	REQUIREMENTS OF E- SIGNATURES UNDER EU LAW	12
2.1.1	Signatory	12
2.1.2	Signature-Creation Data	12
2.1.3	Signature Creation Device.....	12
2.1.4	Signature-Verification Data.....	13
2.1.5	Signature-Verification Device	13
2.1.6	Advanced Electronic Signature.....	13
2.1.7	Qualified Certificate.....	14
	Defining the Certification Service Provider as an Entity	14
	Summary of Terminology under electronic signature process	14
	Status report on Member States.....	15
	Seeking accreditation under the Directive	16
	Annex II of the Directive.....	17
2.1.8	Data Protection	18
2.1.9	Information Security Management System.....	18
3	Additional legal issues	19
	Software export licenses.....	19
	Protecting intellectual property rights when selling biometric software ..	22
4	Appendix C: References	24
5	Glossary.....	26

1 INTRODUCTION

Enterprises and governments are increasingly looking at biometrics and related technologies as potential solutions for some of the issues facing today's world. Among the issues facing governments and enterprises are those of requiring secure authentication, use of digital signatures, adoption of e-records and e-signatures, immigration and order control and effective information collection.

As compared with recent years the number of trials, deployments of biometrics are becoming increasingly common and widespread in certain sectors for example aviation and border control¹. Given the increasing consideration being given to these technologies as appropriate or potential solutions to address some of the issues facing today's world an awareness of legal and regulatory requirements is becoming increasingly relevant and crucial in instances where they are to be deployed and where they will interface with users.

As biometrics become more mainstream and prevalent it is important, and it is the intention of the research being carried out under the BIOVISION project, that due consideration is given to the legal and data protection considerations that arise in circumstances where they are being used.

Workpackage 7 was established to examine these and other issues. The overall Workpackage objectives were to assess the regulatory, legal and standards environment for biometric technology from an EU, Member State and non-EU perspective. This will involve:

- reporting the state and effects of the transposition of the E-Signatures Directive (99/93/EC) in EU Member States as well as in the accession countries
- reporting on the data protection/ privacy regimes in place in the EU and US
- examining and assessing other legal issues that may have an impact on the successful deployment of biometric technology in the EU

¹ As can be evidenced by the Biovision database of such activities

The issues being faced

Through the work of the Workpackage leaders and the contributors to Workpackage 7 on legal and data protection issues BIOVISION has tried to detail some of the more common issues faced in differing sectors and jurisdictions.

A practical example would be for example authentication/ non-repudiation in terms of who owns the legal liability - as more and more legal transactions are conducted via the Internet. The success of the electronic and future mobile commerce within the European Community and worldwide will strongly depend on identifying the issues of legal liability in electronic transactions. Many commentators believe that as yet many of the requirements that they need from biometric systems in terms of proper installation, associated network security and in essence trust are still absent - thus causing a hesitation on the part of some financial organisation to endorse widespread use of biometric system in these instances. The concern is around the ownership of legal liability - a thorny subject in the world of high finance.

It is believed that in the realm of e-commerce the application of biometrics can potentially help to achieve a greater legal binding e.g. with respect to electronic signatures. One important precondition here is the proven security and high technical quality of a biometric system. Moreover in the contractual area there is a great need for transparent, fair, comprehensive and non-discriminating conditions, and which is also valid for the necessary informed consent for data processing as contained within the EU Data Protection Directive.

Biometrics are a potential safeguard for achieving this important goal, but only with appropriate design of a biometric system. This means, in particular, the need to be compliant with security and technology requirements as well as privacy requirements. The juridical requirements e.g. in terms of judicial evidence also strongly depend on technical feasibility and sensible technological possibilities which have yet to be examined in detail.

There are many areas with which the existing law cannot yet deal. In some countries legislators have already noted the need for new rules concerning biometrics and introduced specific regulations on biometrics.

Data protection legislation is also an absolutely crucial area when discussing biometrics from a legal perspective and there are notable divergences in terms of the Member State requirements e.g. with regards to e-signatures and biometrics.

There are also jurisdictions where the application of biometrics may well be hindered as a result of certain laws and requirements. In some countries, laws with application to biometrics appear to be in place, e.g. in the USA.

In many sectors of federal activity for example biometrics have been after a fashion been promoted.

A classic example is that of the Food and Drug Administration. Recently they adopted a Coded Federal Regulation commonly called 21 CFR Part 11 which advocates the use of e-signatures and e-records - giving them parity in a legal sense with their handwritten and paperbased cousins. Mentioned clearly in that same regulation is the use of biometrics as an appropriate signature and authentication mechanism.

Similarly the Department of Health has adopted a regulation aimed at protection of data and personal information - this is called the Health Information Portability and Accountability Act. This piece of federal legislation also supports the use of biometrics for the protection of such data.

Many of these requirements do transfer across the Atlantic to EU companies doing business in the US or exporting their products there. It for example is a requirement for any EU company manufacturing drugs for the US market that they obey the requirements of 21 CFR Part 11.

However, there is a need for legal research on the European level to determine in which areas specific biometric legislation is required - both enabling, as well as limiting the use of biometrics.

To regulate or not to regulate?

More research needs then to be undertaken in the field of self regulation. This is only possible with a comprehensive understanding of the legal systems in each European Member State, the requirements of appropriate European directives and possible self-regulatory instruments which differ in each country. An example is the British T-Scheme in the field of electronic signatures.

Codes of conduct (which in particular must include the privacy aspects) will enable the biometric industry to meet the needs of the more vulnerable sections of society, i.e. the consumer and the end user. This will doubtless also provide a competitive advantage in the world-wide market. Such a Code of Conduct could be developed into a European Commission- and industry approved- quality seal (supported by the European Biometric Forum, for example), and which could be applied for and granted when a company fulfils the requisite criteria. We envisage a future extension world-wide. A significant part of the work of Workpackage 7 has been devoted to a proposed Best Practice and part of a future Code of Conduct.

Within potential governmental applications the legal requirements differ in each European member state. In particular for border crossing applications, e.g. for airport security or immigration control, the requirements need to be examined and negotiated on an cross-European

level. European standards on identification cards with biometric identification may be a goal.

1.1.1 Travel, immigration and border control

Background

September 11 2001 meant that none of us could be complacent about the core values of our society; namely peace, democracy and freedom. It provided us with unequivocal evidence that a root and branch review of many of the everyday services and sectors that we took for granted or had even possibly neglected was required.

One of the sectors that was thrust to the foreground of this review was that of the aviation sector – particularly in light of this newly evolved terrorist threat which had attacked us from our own skies. However, it certainly was not alone as a sector that was placed under the microscope as the rail, road and sea transport infrastructures were also put under the spotlight.

(a) The EU approach

In 2001 and 2002 the European Union took steps to introduce a tightening of the regulatory environment in the aviation sector. This came in the form of a Regulation of the European Parliament and of the Council aimed at establishing common rules in the field of civil aviation security. The objective of this Regulation is clear - *to adopt appropriate provisions and standards in the field of air transport policy to ensure that citizens travelling via civil aviation within the European Community would be protected from acts of unlawful interference.*

Aims of the Regulation

The Regulation contains a series of specific requirements, which apply to all Member States, which include:

- The adoption of a national civil aviation security programme which can allow for the swift detection and correction of security failures
- Creation and adoption of common basic standards for aviation security measures
- A quality control programme and a training programme, and
- each Member State must designate a single appropriate authority responsible for the coordination and the monitoring of the implementation of aviation security programmes with appropriate compliance monitoring mechanisms.

The Regulation also sets out the fact that the national civil aviation security programme shall be closely and regularly audited as well as the airports and aviation environment in which it applies.

Specific obligations

The Regulation is divided into a number of sections.

Airport security in general

There is a requirement that airports now needed to be planned in terms of the layout of airports, passenger and cargo terminals and other buildings having direct airside access so that security controls could effectively be applied to passengers, baggage, cargo, courier and express parcels, mail and air carrier catering stores and supplies as well as ensuring the protection and control of access to airside, security restricted areas and other sensitive airport areas and facilities.

Airports are required to ensure the protection of the boundaries of each airport using effective security equipment with clear protection for all security restricted areas.

The technology that is being looked as a possible panacea for some of the issues faced here is biometrics. Systems have been trialled at Heathrow, Gatwick and other airports and indeed are fully deployed in London city Airport and Schipol airport. In such instances biometrics can provide appropriate level of security for such facilities. In addition, some biometric systems can provide policy management enabling airport operators to manage access to certain sections of the airport in line with their required security policy.

Staff screening and security

All staff requiring access to security restricted areas have to be subjected to a minimum 5-year background check which shall be accompanied by training in aviation security. Part of the discussions that are underway at EU and national aviation level are around using biometrics in conjunction with such background checks to keep effective and non-repudiable records on the staff who are checked.

There is also a requirement that airport identification cards and vehicle passes shall be checked at all airside and security restricted area checkpoints. Recently in the US legislation was passed recognizing the use of biometrics in such instances and requiring non-repudiable checks at all perimeter points of access and egress.

1.1.1.1 Immigration and border control

The area of border control and immigration has also been an area of activity from a biometric perspective in the EU. One of the biggest evident concerns, which is also a political hot potato, is that of illegal immigrants and particularly those who are repeat offenders.

There were 3 significant problems that had to be faced. First, the extensive and very porous borders on the eastern perimeter of the EU which are extremely difficult to police. Secondly even if illegal immigrants were successfully expelled they could easily re-enter with no definitive method often to identify them as forged papers are commonly used. Finally, the European Union prides itself on freedom of movement and in recent years had put in place the Schengen zone which allowed for freedom of movement of persons – making surveillance and tracking and tracing of individuals difficult.

Among the steps taken was the installation of a Europe wide database and infrastructure for the registration and storage of the fingerprints of illegal immigrants. This database – EURODAC – has been in operation since January 2003.

In addition, on a national basis the majority of EU member countries, including Ireland, Germany and the UK passed legislation aimed at controlling and managing border crossings. In the UK the Government adopted 2 pieces of legislation known as Schedule 7 and the Anti-Terrorism Crime and Security Act 2001. This legislation requires that information must be gathered on all journeys to and from UK and within UK for passengers and goods. In addition, Under Para 17(4) of Schedule 7 to the Terrorism Act 2000 the following information must be collected on passengers and crew: full name and gender, date and place of birth, home address and nationality. Also with regard to the travel documents: the type of document used, its number, its country of issue and expiry date along with the number of items that a passenger has placed in the hold of an aircraft.

In Germany, the "Terrorismusbekämpfungsgesetz" (law fighting terrorism) was enacted in January 2001 and provides new regulations for implementing biometrics in national ID-cards and passports as well as in the area of foreigner legislation e.g. asylum seekers.

It can be fairly said that similar legislation is either in place or being adopted in many of the European Union countries. Indeed plans are under way for "Schengen Information System II" which will act essentially as an entry-exit system for the EU. The upcoming European visa will bear biometrics in order to be able to check identities of aliens against databases as well as to verify the carrier of a document.

A number of Governments have initiated tenders and Requests for Information to see what the art of the possible is for the use of biometrics as part of an overall border solution. These include the UK - biometric capture and recognition system and related services published on 9 May 2003.

In addition, a bold step is being pushed at EU level by DG Justice and Home Affairs for the Schengen System II which is intended to create a

free travel area for EU citizens inside the Schengen area. The tender process has been initiated on this issue as this document goes to press.

The G 8 countries have agreed on establishing a common working group on biometrics which is to be set off in September 2003 with a launch in Berlin, hosted by the German government.

(b) The US approach

Following 9/11 a raft of far reaching legislation was adopted in the US to control and regulate travel and transport. First adopted was the USA PATRIOT Act which set out the foundation for providing sufficient powers to provide appropriate tools and requirements to regulate areas such as travel and immigration.

This was swiftly followed by the Enhanced Border Security and Visa Reform Act 2002 that was signed into law by President George W Bush on 14 May 2002.

The Act provides approximately \$4bn over 3 years to be invested in, inter alia: computer security, infrastructure support, Information technology devt for border security and control and management of the flow of commerce and persons at ports of entry eg pre-enrolment and pre-clearance.

At the core of the Act it provides that:

- Not later than 26 Oct 2004 the Attorney General shall issue to aliens only machine readable tamper resistant visas and travel and entry docs that use biometric identifiers
- Not later than 26 October 2004 shall install in all US ports of entry equipment and software to allow biometric comparison of all US visas and entry documents issued to aliens and
- Not later than 26 Oct 2004 the government of each visa waiver country must certify (as a condition of continuation of their visa waiver status) that it has a program to issue its nationals with Machine Readable passports that are tamper resistant and incorporate biometric identifiers that comply with biometric identifier standards as established by the International Civilian Aviation Organisation (ICAO), an international forum of the UN focused on travel documents.
- After 26 Oct 2004 any alien applying for admission under the visa waiver programme shall present a passport that meets these requirements unless he already has an issued passport.

These measures are likely to have a very significant impact on the use of biometrics in the EU - there is the potential in this legislation that could become a 'tipping point' for the technology.

The implications from a legal and data protection perspective are around issues such as:

- what data will be collected,
- who will have access to such data,
- will biometric data be associated with other personal information to build profiles on individuals,
- how will such information be protected,
- what happens if data is compromised
- how biometric data be regarded from law enforcement purposes, etc.

These are among the most crucial issues, as well as being drivers, for biometrics going forward.

2 REQUIREMENTS OF E- SIGNATURES UNDER EU LAW

Electronic signatures are recognised under Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999, on a Community framework for electronic signatures (also known as the Electronic Signatures Directive).

Under the Directive an electronic signature is taken to mean “*data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.*”

There are a number of aspects to an electronic signature that encompasses a biometric aspect - these are listed below.

2.1.1 Signatory

The signatory as defined by the Directive is “*a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents.*” Within a biometric signing process the signatory would equate to the “user” of the technology. Typically this would be an individual within an organisation seeking to electronically sign data.

2.1.2 Signature-Creation Data

Within a standard PKI system signature-creation data would equate to a signatory’s private key, however the Directive defines signature-creation data to include, “*unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature*” (emphasis added).

Within a signing process the signatory creates an electronic signature by supplying a biometric to the signature-creation device, namely the system. Based on an authentication using a biometric the users private key is used as the basis for creating the signature. Thus, within the signatory’s biometric *and* private key together equates to signature-creation data as defined by the Directive.

Users private keys must be stored securely on a server or elsewhere in the normal fashion - it must be ensured that the administrators access will not be capable of compromising the system's implementation in order to steal the users key.

2.1.3 Signature Creation Device

A signature creation device is defined as “*configured software or hardware used to implement the signature-creation data.*” Within common signature

processes the system captures the biometric and utilises the users individual private cryptographic key to produce an electronic signature. The technology, both client and server, are considered the signature creation device.

2.1.4 Signature-Verification Data

Signature-verification data is defined as “*data, such as code or public cryptographic keys, which are used for the purpose of verifying an electronic signature*”.

Within a standard PKI system this would be interpreted as the signatory’s public cryptographic key. The signature verification data is regarded as the public cryptographic key held on file by the Certification Service Provider (CSP) and used for the purpose of authenticating a signatory’s electronic signature.

2.1.5 Signature-Verification Device

The signature-verification device means “configured software or hardware used to implement the signature-verification data”. Essentially this describes the device in which signature verification occurs. Depending on the system being used, the signature-verification device can be a server or client machine.

2.1.6 Advanced Electronic Signature

Under the Directive an advanced electronic signature, referred to as an AES, is one which meets the following requirements;

- it is uniquely linked to the signatory
- it is capable of identifying the signatory
- it is created using means that the signatory can maintain under his sole control
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

Within many signature processes, the use of a biometric as part of the signature-creation data to generate an electronic signature, and the characteristics of the signature produced as a result of this process, is designed to ensure that each electronic signature can be uniquely linked to a signatory.

The verification process conducted through the technology, verifies the signatory’s biometric against verification data held on file, and as such is capable of identifying the signatory.

The use of the users` biometric as signature creation data is designed to ensure that such signature creation data is maintained under the sole control of the signatory.

2.1.7 Qualified Certificate

Under the requirements of the Directive a qualified certificate must fulfil two requirements; 1) the certificate itself must be capable of meeting the ten requirements defined in Annex I, and 2) it must be issued by a CSP which fulfils the requirements of Annex II.

Such signature processes must generate a qualified certificate that conforms to the requirements of Annex I. An audit of the live environment at a customer location is required in order to qualify the degree of compliance that a potential CSP can demonstrate against the clauses of Annex II.

Defining the Certification Service Provider as an Entity

A CSP has been broadly defined by the Directive as “*an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.*”

Where a single organisation provides all relevant services related to the issuance of qualified certificates (including for example, registration, certificate generation, certificate dissemination, revocation and de-registration) then defining the CSP is a simple matter.

In the implementation of some systems, however, activities may be outsourced to a variety of ‘service providers’ each responsible for their own service. For example, the registration of signatories may be outsourced to a Registration Authority (RA), revocation of certificates and a directory of qualified certificates may be outsourced to a second service provider, and the generation of certificates may be the responsibility of a third service provider, i.e. a Certification Authority (CA). In such circumstances defining the entity which is the CSP may be more complicated.

In practice, the CSP is often deemed to be the organisation or entity which accepts responsibility for, and liability arising from, third parties relying on qualified certificates provided through its services (Article 6). This will often be the contracting party where a number of service providers have been brought together to provide qualified certificates, and the CSP is by definition the entity which signs its name to the qualified certificates in keeping with Annex I, Clause (b) of the Directive.

Summary of Terminology under electronic signature process

Interpretation Directive	under	Signature Process
-------------------------------------	--------------	--------------------------

Advanced Signature	Electronic	Signature created
Signatory		User
Signature-creation data		Biometric and users Private Key
Signature-creation device		Client and Server or other
Signature-verification data		Users Public Key
Signature-verification device		Server or other device
Qualified Certificate		Signature from Server or device
Certification Provider (CSP)	Service	Based on deployment options
Certification Authority (CA)		The entity responsible for the operation of technology.
Registration Authority (RA)		The entity responsible for the enrolment of new users.
Relying Party		Parties requiring signature verification

Status report on Member States

Status of electronic legislation in the Europe

Country	Name and date	Detail	Location
Austria	E-sig Act 99 (Bundesgesetz über Elektronische Signaturen).	Regarded as equivalence to handwritten sigs. Exceptions in area of probate and family law Regulated by the Telekom-Control-Kommission	www.rtr.at
Belgium	E-sig Act adopted on 22/12/00	Complete equivalence with handwritten signatures	http://www.mineco.fgov.be
Denmark	E-sig Act adopted on 31/ 5/ 00	Equivalent to handwritten signatures	www.retsinfo.dk
Finland			
France	E-sig Act adopted on 13/3/ 00	once e-sig is non-repudiable it is accepted	www.internet.gouv.fr
Germany	Conditions for	any exceptions where	www.bmwa.b

	Electronic Signatures adopted May 2001 Law concerning adaptation of private law form requirements and other provisions to modern commerce	handwritten sigs are required. Specific technology requirements for a signature to be approved. accepts AES for new electronic form and new prima facie evidence rule	und.de www.bmj.bund.de
Greece	E-sig act adopted 05/0601	regarded as equivalent apart from conveyancing and some financial instruments	www.eett.gr/g r_pages/index 2.htm
Ireland	E-Commerce Act 01/09/00	while regarded as equivalent consent of receiver is required to be valid. Not accepted on probate and conveyance documents and some court documents.	www.gov.ie/o ireachtas/frame.htm
Italy	24/ 12/00 adopted Testo Unico	acceptance is confirmation required from a notary public	www.innovazione.gov.it
Luxembourg	e-signature act 01/10/00	regarded as equivalent	http://www.etat.lu/OLAS/
Netherlands	E-Sig Act	regarded as equivalent	www.overheid.nl.
Portugal	Decree-Law 290-D/99 of 2/8/99	regarded as equivalent	
Spain	Real decreto-ley 14/1999, (lfe) de 17/ 9/ 99		http://www.mcyt.es/grupos/grupo_setsi.htm
Sweden	E-sig Act 1/1/01	generally equivalent except with regard to conveyancing	www.regeringen.se
UK	Electronic Communications Act 2000		http://www.legislation.hmso.gov.uk/acts/acts2000/20000007.htm

Seeking accreditation under the Directive

The European Commission introduced the provision for voluntary accreditation schemes for CSPs under Article 3, Clause 2 of the Directive. The purpose of such schemes, as explained in Recital 11, is to enable CSPs to credibly and independently demonstrate enhanced levels of service, and thereby establish the trust, security and quality expected by the marketplace. Successful certification under a recognised accreditation scheme is testimony to best practice on the part of the CSP.

As acknowledged by the Commission in Recital 4, divergent rules with respect to the legal recognition of electronic signatures has the to potential create a significant barrier to electronic commerce within the European Community. Independent certification through a recognised accreditation scheme is intended to prevent such barriers, and furthermore is likely to strengthen confidence in, and the general acceptance of, the new technologies involved in this emerging market.

Any entity defined as a CSP may apply for certification under a relevant accreditation scheme. To successfully achieve certification the CSP must be capable of demonstrating conformance with the following requirements:

- The CSP issues qualified certificates which conform to Annex I of the Directive,
- The CSP conforms to the requirements of Annex II of the Directive,
- The CSP must be capable of demonstrating compliance with the requirements of the Data Protection Directive (95/45/EC), and
- The CSP must operate a recognised information security management system (ISMS).

Annex II of the Directive

CSPs must be able to demonstrate conformance with the requirements of Annex II in order to successfully achieve certification. CSPs seeking guidance on how to demonstrate conformance with Annex II can utilise the European Telecommunications Standardisation Institute (ETSI) Standard ETSI TS 101 456 – Policy Requirements for CSPs. Certification Europe would note that while ETSI TS 101 456 provides useful text on how to demonstrate compliance with Annex II, it is intended for a PKI based system and thus specific clauses may have no direct relevance when applied to a biometric based system.

Annex II (f) requires a CSP to use trustworthy systems and products that are protected against modification and ensure the technical and cryptographic security of the process supported by them.

2.1.8 Data Protection

Article 8 of the EU-Data Protection-Directive requires that a CSP must comply with the requirements laid down in Directive 95/46/EC. A CSP seeking certification under the Directive will be audited to assess compliance with both the Data Protection Directive and applicable national legislation.

2.1.9 Information Security Management System

CSPs seeking certification under the Directive are required to demonstrate that they have a fully functioning and recognised information security management system (ISMS) in place in order to demonstrate the required levels of reliability and trustworthiness expected under Annex II.

Certification to IS 17799:2 2000, or BS 7799:2 1999 or 2002 are all accepted as recognised information security management systems for the purpose of demonstrating conformance with the Directive.

3 Additional legal issues

Software export licenses

In certain instances biometric products may require a software export licence. These licence requirements commonly arise when the technology being exported is classified as a dual-use good. A dual use good is essentially one where it can be used for normal business and every day activities but also for military or sensitive purposes.

This classification arises in the event that the product is a:

- military good
- is a highly sensitive dual-use item
- is being exported to a jurisdiction outside the EU
- is being exported to a jurisdiction where sanctions are in place.

The requirement applies not only to the physical export of such technology but also in the event that it is transferred electronically.

The controlling legislation from which the Member State provision derive is EU Regulation 1334/ 2000. It encompasses many categories of products ranging from telecom and IT security products to nuclear materials and micro-organisms. Also covered is encryption technology.

One area of export laws that has become more relevant in recent years is the "catch all" clause which implements the Missile Technology Control Regime (which is separate to the Wassener arrangement). It is potentially relevant where biometrics technology is used by the military, police or military contractors. It is set out in COUNCIL REGULATION (EC) No 1334/2000 of 22 June 2000.

Article 4 (1) provides as follows:

"An authorisation shall be required for the export of dual use items not listed in Annex I if the exporter has been informed by the competent authorities of the Member State in which he is established that the items in question are or may be intended, in their entirety or in part, for use in connection with the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological or nuclear weapons or other nuclear explosive devices or the development, production, maintenance or storage of missiles capable of delivering such weapons."

Article 4 (5) provides:

"If an exporter is aware that dual use items which he proposes to export, not listed in Annex I, are intended, in their entirety or in part, for any of the uses referred to in paragraphs 1, 2 and 3, he must notify the authorities referred to in paragraph 1, which will decide whether or not it is expedient to make the export concerned subject to authorisation."

The other manifestation of the Missile Technology Control Regime is found in the restriction on the Community General Export Authorisation which provides that the " general authorisation may not be used if the exporter has been informed by the competent authorities of the Member State in which he is established that the items in question are or may be intended, in their entirety or in part, for use in connection with the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological or nuclear weapons or other nuclear explosive devices or the development, production, maintenance or storage of missiles capable of delivering such weapons, or if the exporter is aware that the items in question are intended for such use". It is still possible to get a licence to export such technology.

With regard to Dual Use licences it is important to request the most up to date categories of controlled dual use goods directly from the relevant Government Department as the categories do change from time to time.

Required actions

The items in question, which may be classified as dual-use items should be notified to the relevant national government department - for example in the UK the Department of Trade and Industry and the Ministry of Defence and in Ireland the Department of Enterprise, Trade and Employment. This requirement occurs if the exporter believes that the technology in question may be intended in whole or part for military activities, for example connected with military installations or indeed weapons themselves.

Among the countries where sanctions are applicable are:

- Afghanistan
- Iraq
- Libya and Zimbabwe

Exporters should also examine the appropriate type of licence that is required. These include:

- A Community General Export Authorisation Licence
- A Single Licence
- A Global Export Licence

A final point worth noting is that in most EU countries significant penalties - both financial, corporate and criminal can apply for ignoring or breaching the export licence requirements.

In addition, the relevant Government Departments normally request the following commercial details:

Elements of company profile.

1. Name of company.
2. Address.
3. Telephone & fax numbers, e-mail addresses, web site addresses.
4. Contact names and addresses.
5. Date of establishment.
6. Parent company (if applicable).
7. Numbers employed.
8. Nature of business (manufacturer, distributor etc).
9. Business relationships (e.g. subsidiaries, parent companies, contracts with freight forwarders, exporters, suppliers etc)
10. Product details especially the dual use products for export (e.g. promotional material, technical material, website pages with product details)
11. Location of manufacture of goods.
12. The company's market and destinations.
13. Board of Directors
14. Authorisation on company headed paper permitting named employees to apply for dual-use export licences on behalf of the company. This authorisation should be signed by a director of the company and provide sample signatures of the authorised employees.

Protecting intellectual property rights when selling biometric software

Companies planning to export software/ hardware and indeed their technology products to the US should appraise themselves of many of the complex rules and potentially damaging and sometimes irreparable pitfalls that can impact the ownership and intellectual property rights of their products. Indeed it is fair to say that not only do you have to consider the procurement rules that would normally apply to US software/hardware vendors but also those issues that effect non-US companies such as Foreign Ownership, escrow and GSA schedules to name just a few.

Only by ensuring a full understanding of the legal environment into which the products are being placed can companies prevent such damage. The golden rule, which is accurate in a lot of cases is that if you fail to properly protect your products or your intellectual property rights then you run a serious risk of losing your rights in these products permanently. For a software/hardware company producing biometric products or indeed any similar products your intellectual property is the lifeblood of the your organisation.

One of the areas of greatest concern revolves around ensuring that you are adequately protected by the contracts that are used to licence your products or indeed those that are used by the purchaser of your product. Be aware that there may be at least 2 pitfalls in this scenario. The first one is the where you may be bound by referred terms in a contract to a prime or government contractor ie while terms or conditions may not be explicitly stated in your contract, but rather referred to obliquely, they may still bind you as they transfer via the prime's contracts. Be sure if at all possible to get full sight of all such relevant contracts.

One of the most recent infamous cases involved a company providing both hardware and software to a US Government Department. The products provided were a later or upgraded version than that referred to in the licence/contract. The court held that the products that were provided to the US Department were not covered under the protective terms of the providers contract. The result was that the licence terms did not apply and by default the US Government gained complete and unlimited rights in the product. This is obviously a disastrous verdict for a software company who would undoubtedly have invested significant time, money and resources into development of such a product.

This is commonly referred to in legal circles as "IP leakage" and is an occurrence that can irreparably damage a company.

Many of the purchasing rules that can apply in these situations can be found in the US Government's publication/tome entitled Federal Acquisition Regulation. The FAR as it is commonly referred to provides a

comprehensive source/ reference to view the uniform policies and procedures for acquisition by executive agencies of the federal government. The FAR is issued and maintained by the US Department of Defense, the US General Services Administration and the National Aeronautics and Space Administration.

Therefore in brief some of the key points to remember:

- Ensure you have had clear visibility of all contractual terms in the prime contractors contracts – terms may not always be explicit
- Ensure that the products you supply under contract/ licence agreements are indeed the self same products that you provide

4 Appendix C: References

Digital Signature Law Survey <http://rechten.kub.nl/simone/ds-lawsu.htm> (Simone van der Hof)

Anonymity Law Survey
<http://rechten.kub.nl/anonymity/index2.htm> (Miriam van Dellen)

Digital Signature Project
http://www.law.kuleuven.ac.be/icri/projects/digisig_lb_eng.htm
University Leuven (last update 2000!)

Elektronic Signature <http://www.internet4jurists.at/intern25a.htm>
Germany/Austria/EU

Privacy links
http://europa.eu.int/comm/internal_market/de/dataprot/index.htm
(European Commission)

Divers links to biometrics
<http://www.geocities.com/woodwardlaw/linksbiometrics.html>
John D. Woodward, Jr.

- [1] Albrecht, A. (1999). Biometrie, digitale Signatur und elektronische Bankgeschäfte zum Nutzen für Verbraucher, hrsg. von der Arbeitsgemeinschaft der Verbraucherverbände, Bonn
- [2] Albrecht, A. (2000) Biometrie zum Nutzen für Verbraucher?, DuD, S. 332 ff.
- [3] Albrecht, A. (2001). Biometrische Anwendungen aus verbraucherpolitischer Sicht: Wo sind die Chancen und Risiken für den Nutzer? S. 244 ff. in: Fluhr, Matthias (Hrsg.): Die Chipkarte: Neue Sicherheitskonzepte und Wertschöpfungsmodelle, Kongressdokumentation Omnicard 2001, inTIME, Berlin
- [4] Albrecht, A. (2001). Brennpunkt Biometrie, SicherheitsForum 5, S. 34 ff.
- [5] Albrecht, A. (2001). Brennpunkt Biometrie, SicherheitsForum 6, S. 56 ff.
- [6] Albrecht, A. (2000). Consumer Acceptance and Legal Frameworks, S. 68 ff. in: Lockie, Mark/Deravi, Farzin, The Biometric Industry Report, Elsevier Advanced Technology, Oxford Dezember
- [7] Albrecht, A. (2002). Relevanz biometrischer Verfahren im gesellschaftlichen Kontext, S. 85 ff. in: Nolde, Veronika/Leger, Lothar (Hrsg.): Biometrische Verfahren – Körpermerkmale als Passwort, Deutscher Wirtschaftsdienst Köln

- [8] Albrecht, A. (2002). Biometrie und Recht, S. 97 ff. in: Nolde, Veronika/Leger, Lothar (Hrsg.): Biometrische Verfahren – Körpermerkmale als Passwort, Deutscher Wirtschaftsdienst Köln
- [9] Albrecht, A. (2002). Verbraucherpolitische Bedeutung der Biometrie, S. 129 ff. in: Nolde, Veronika/Leger, Lothar (Hrsg.): Biometrische Verfahren – Körpermerkmale als Passwort, Deutscher Wirtschaftsdienst Köln
- [10] Albrecht, A. und T. Probst (2001). Biometrische Verfahren – im Einklang mit Verbraucher- und Datenschutz? AgV-Forum 1, S. 32 ff.

5 Glossary

BVN The EC's abbreviation for the BIOVISION project