Encryption Export Controls: A Comparative Analysis between the EU and the US

John F. McKenzie
Baker & McKenzie – San Francisco

Jasper Helder
Baker & McKenzie – Amsterdam

Friday, November 8, 2013
Amsterdam, Netherlands
UNITED STATES
Encryption Export Controls: Key Concepts

- Export Controls imposed on Products that are designed or modified to use “cryptography” employing digital techniques performing a cryptographic function
  - “Cryptography” is the discipline that embodies, principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, or prevent its unauthorized use.
- Products are controlled because of the capability to encrypt data, regardless of other functions and features
Encryption Export Controls: Key Concepts (cont’d)

– The United States takes a very broad view of the scope of the encryption controls, including:
  – Products that make calls to the encryption functionality of a third party product
  – Activation codes to activate “dormant” encryption functionality

– Encryption products specially designed or modified for military use are subject to export control under the separate ITAR munitions export control program
The Encryption Export Control Hierarchy

- Products without encryption functions or features are not subject to the encryption export controls
  - Exception: Products that make calls to, or interoperate with, the encryption functionality of third party hardware or software
The Encryption Export Control Hierarchy

- Items with encryption functionality but excluded from the encryption export controls
  - Products with dormant encryption that requires “cryptographic activation” (Note (j) to 5A002)
  - Activation keys for dormant encryption are themselves treated as controlled encryption products
The Encryption Export Control Hierarchy (cont’d)

– Items with encryption functionality but excluded from the encryption export controls (cont’d)
  – Ancillary encryption (Note 4)
  – Mass market encryption products (Cryptography Note: Note 3)
    – The United States BIS takes the position that the mass market exception applies only to products distributed to individual consumers
  – Products that use encryption exclusively for: (i) authentication and access control; (ii) digital signature; or (iii) execution of copy protected software
  – Low level encryption (e.g., using a symmetric encryption algorithm with a key length of 56 bits or less
The Encryption Export Control Hierarchy (cont’d)

- Controlled Encryption Products
  - 5A002: Encryption Commodities utilizing (i) a symmetric encryption algorithm with a key length greater than 56 bits; (ii) an asymmetric algorithm with a key length greater than 512 bits; or (iii) elliptical curve encryption with a key length greater than 112 bits
  - 5D002: Encryption software having the characteristics, or performing or simulating the functions, of controlled encryption commodities
  - 5E002: Technology for the development, production or use of controlled encryption commodities or software
Unique Features of the United States Implementation of the Encryption Export Controls

– Extraterritorial Application: The United States Export Controls extend to the reexport from one country to another of United States origin encryption products, and products developed and produced abroad with United States origin encryption components

– Encryption Products excluded from the Encryption Controls remain subject to U.S. Export Controls for Anti-Terrorism Reasons
Unique Features…(cont’d)

– Regulatory Formalities Apply to the Export of Mass Market Encryption Items covered by the Cryptography Note
  – Previously an Encryption Classification Ruling from BIS was required
  – Now, the Exporter must file an encryption registration statement, receive an encryption registration number (ERN) and file annual self-classification reports with BIS
Unique Features…(cont’d)

– Exports/reexports of controlled encryption products to foreign subsidiaries of U.S. corporations are authorized without export licenses and without regulatory formalities under license exception ENC

– Most other exports/reexports of controlled encryption commodities, software and technology are authorized without export licenses under license exception ENC, subject to compliance with a series of regulatory formalities specified in Section 740.17 of the Export Administration Regulations
Exports of Controlled Encryption Items under License Exception ENC

- For purposes of License Exception ENC, the Export Administration Regulations make a key distinction between (i) unrestricted encryption items; and (ii) restricted encryption items
  - Examples of restricted encryption items include
    - Network infrastructure products
    - Encryption source code
    - Encryption Items designed or modified for government end-users or to a customer specification, or that have cryptographic functionality that is user-accessible
    - Products that provide functions necessary for quantum encryption
...Items under License Exception ENC (cont’d)

– For purposes of License Exception ENC, the Export Administration Regulations make a key distinction between (i) unrestricted encryption items; and (ii) restricted encryption items (cont’d)

  – Examples of Restricted Encryption Items include (cont’d)
    – Encryption Products that provide network penetration capabilities
    – Cryptanalytic Products
    – Products with an Open Cryptographic Interface
    – Encryption Technology Classified under 5E002
...Items under License Exception ENC (cont’d)

- For purposes of License Exception ENC, the Export Administration Regulations make a key distinction between (i) unrestricted encryption items; and (ii) restricted encryption items (cont’d)
  - Examples of Restricted Encryption Items Include (continued)
    - Chips, chipsets, electronic assemblies and FPLDs
    - Cryptographic libraries and development kits and toolkits
    - ASIC development kits implementing cryptography
    - Encryption commodities and software that provide or perform vulnerability analysis, network forensics or computer forensics
    - Automated network analysis, virtualization or packet inspection
    - Investigation of data leakage, network breaches or malicious intrusion activities
Regulatory Formalities under the Export Administration Regulations to Export/Reexport Controlled Encryption Products under License Exception ENC

- Unrestricted Encryption Products (including most consumer, business and commercial software applications)
  - File an Encryption Registration Statement with, and receive an Encryption Registration Number (ERN) from, BIS
    - The ERN is the Authorization to Export Encryption Products under License Exception ENC
  - Self-Classify the Encryption Products
- File an Annual Self-Classification Report for Each Encryption Item Exported during the Calendar Year under License Exception ENC
Regulatory Formalities...under License Exception ENC (cont’d)

- Restricted encryption products
  - Obtain an encryption classification ruling (CCATS) from BIS
  - License exception ENC is nonetheless not available, and specific export licenses from BIS must be obtained for:
    - Exports of restricted items to government end-users located in any country other than the “Supplement No. 3” countries (i.e., Canada, European Union, NATO, other close allies)
    - Exports of encryption technology to customers located in country group D:1 countries (e.g., Russia, China)
    - File semi-annual sales reports with BIS (exports from the United States only)
EUROPEAN UNION
Encryption Export Controls: Key Concepts

– Like the U.S., the EU takes a broad view of the scope of encryption controls, including:
  – Activation codes to activate “dormant” encryption functionality
  – Unlike the US: components for ‘mass market’ encryption items remain controlled

– Encryption products specially designed or modified for military use are subject to export control under national regulations of the EU member states in respect of military items
  – Categories ML 11.a (sub e, inter alia data processing equipment), ML 21 a and b.4 (software designed/modified for ML items, C3I & C4I software)
Encryption Export Controls: EU catch up (?)

– However, the EU has not yet enacted 2011 & 2012 Wassenaar changes. Relevant (2012) Wassenaar changes are:
  – Addition of paragraph b to Cryptography Note for decontrol of hardware components for decontrolled “mass market” items
  – Note to Cryptography Note which provides guidance on “mass market” concept
  – Decontrol of personal area network equipment with a range up to 100 meters and max of 7 connections (EU: 30 meters)
  – Note to 5E002 explicitly controls technical data from procedures carried out to evaluate or determine the implementation of category 5 controlled encryption
Some key EU v US Differences

- EU export controls do not apply extraterritorially, so no re-export controls

- EU export controls do not have a ‘deemed export’ concept: ‘export’ requires transfrontier movement
Some Key EU v US Differences (cont’d)

– No up-front formal classification or registration requirement
  – However, some EU countries maintain import controls, which require registration before import/use:
    ▪ Bulgaria (registration requirements for imports from outside the EU)
    ▪ France (registration requirements, plus reporting requirements for exports)
    ▪ Latvia (import licensing requirements for certain goods)
    ▪ Poland (reporting requirements)
Some Key EU v US Differences (cont’d)

– Generally EU controls are a bright line: controlled or not controlled
  - We have no equivalent to US anti-terrorism controls such as 5A992, 5D992, 5E992
  - But: bear in mind that some EU countries may introduce national controls in addition to the EU Dual Use Regulation
  - Generally there is increased impact of human rights considerations for export licensing decisions
Some Key EU v US Differences (cont’d)

- Many EU licensing authorities consider encryption for gov’t use to be potential human rights issue
  - Impact of human rights related criteria for military items
  - EU Parliament resolution 23 October 2012 proposed:
    - end use controls for items not on EU control list which “are or may be intended (…) for use in connection with a violation of human rights, democratic principles of freedom of speech (…) by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of internet use (…)”
    - Mandatory licensing requirement for non-control list items if there are human rights considerations.
  - Restriction for UGEA005 (Telecoms Equipment)
Some Key EU v US Differences (cont’d)

– Examples of encryption related human rights impact:
  – Netherlands brokering controls require individual pre-notification of brokering for the supply of controlled items for ‘sensitive countries’ (Afghanistan, Angola, Belarus, Birma, Congo, Egypt, Eitrea, Guinee, India, Irak, Iran, Israel, Ivory Coast, Lebanon, Liberia, Libya, North-Korea, Pakistan, Sudan, Syria, Zimbabwe, South-Sudan)
  – Increased scrutiny by Dutch authorities of encryption exports to inter alia Lebanon
  – German unilateral controls: 5A991 and 5D991 hardware and software for Terrestrial Trunked Radio (‘TETRA’) for Sudan. TETRA typically also applies encryption
  – UK license refusals for encryption communications equipment
  – The exception for the supply of certain encryption items to Iran under the EU sanctions was limited to 15 April 2013
EU Export Licensing

- Export is transfrontier transfer to non-EU destination
  - ‘Annex IV’ items also require license for intra-EU transfer
    - Equipment, software and technology with/for cryptanalytic functions
- Transfers within EU may also require licence if known that the final destination is outside the EU and no processing or working is to be performed within the EU
EU Export Licensing

– The EU system has 2 types of licences:
  ▪ EU-level licences (i.e., the UGEA)
  ▪ National licences

– The national licences are subdivided into:
  ▪ “Global” (UK has specific OGEL for encryption items, Germany has AG16)
  ▪ Individual

– UGEA EU001 permits export of crypto hardware and software (excluding Annex IV) to Australia, Canada, Japan, Liechtenstein, New Zealand, Norway, Switzerland, and the US
EU Encryption Administrative Points

– EU: Article 20 - records of dual-use exports to be kept for at least 3 years (but national rules usually impose longer period)
– EU: Article 22 – Control statement on commercial documents for intra-EU transfers
– EU: Article 22 - Member States may request additional information in respect of intra-EU transfers of information security items
  ▪ UK: maintain records for intra-EU transfers
  ▪ France: ‘declaration’ required for certain encryption items when transferred to EU country
Tips

– License exception ENC does not mean re-export of US items from the EU do not require an EU license

– Components for ‘mass market’ encryption items still require an EU export license, although decontrolled in the US

– EU authorities do tend to follow US CCATS, but be mindful of the differences between EU and US Wassenaar implementation
Questions?

John F. McKenzie
San Francisco/Palo Alto
+1 415 576 3033
john.mckenzie@bakermckenzie.com

Jasper Helder
Amsterdam
+31 6 46 17 94 82
jasper.helder@bakermckenzie.com