Väljaandja:	Vabariigi Valitsus
Akti liik:	välisleping
Teksti liik:	algtekst
Jõustumise kp:	26.01.2007
Avaldamismärge:	RT II 2007, 9, 28

Eesti Vabariigi ja Hispaania Kuningriigi salastatud teabe kaitse kokkulepe

Vastu võetud 11.11.2005

Vabariigi Valitsuse 21.07.2005 korraldus nr 467 kokkuleppe eelnõu heakskiitmise kohta

Välisministeeriumi teadaanne välislepingu jõustumise kohta

Eesti Vabariigi ja Hispaania Kuningriigi salastatud teabe kaitse kokkuleppe muutmise kokkulepe

Eesti Vabariik ja Hispaania Kuningriik, edaspidi «pooled», et kaitsta omavahel või oma avalik- või eraõiguslike isikute vahel vahetatavat salastatud teavet,

on kokku leppinud järgmises.

Artikkel 1. Kohaldatavus

(1) Kokkuleppega sätestatakse poolte vahel vahetatava ja nende julgeoleku volitatud esindajate vastutusalasse jääva salastatud teabe kaitse kord.

(2) Kumbki pool ei või kasutada kokkulepet, et saada salastatud teavet, mida teine pool on saanud kolmandatelt isikutelt.

Artikkel 2. Mõisted

Kokkuleppes kasutatakse järgmisi mõisteid.

1) *Salastatud teave*– teave (s.t mis tahes vormis edasiantavad teadmised) või materjal, mida on vaja kaitsta loata avalikustamise eest ja mis on märgistatud vastava salastatuse tasemega.
a) *Materjal*– ese või aine, millest on võimalik saada teavet, sealhulgas dokumendid ning masinate, seadmete, relvade ja relvasüsteemide valmis või tootmisjärgus osised.
b) *Dokument*– mis tahes füüsilisel kujul ja omadustega salvestatud teave, näiteks kirjutised ja trükised (sealhulgas kirjad, joonised, plaanid), elektroonilised andmekandjad (sealhulgas kõvakettad ja disketid, kiibid, magnetlindid, laserkettad), fotod ja videod, nende optilised ja elektroonilised reproduktsioonid.

2) *Leping*– kahe või enama lepinglase kokkulepe, millega nähakse ette nendevahelised õigused ja kohustused.

3) *Salastatud leping*– leping, mis sisaldab salastatud teavet või on sellega seotud.

4) *Riigi julgeoleku volitatud esindaja*– asutus, mille kumbki pool on määranud vastutavaks käesoleva kokkuleppe täitmise ja selle järelevalve eest.

5) *Lepinglane*– füüsiline või juriidiline isik, kellel on õigus sõlmida lepinguid.

6) *Ehitis*– juriidilise isiku või riigiasutuse või -ettevõtte seade, tehas, vabrik, labor, kontor, ülikool või muu haridusasutus või äriruumid (sealhulgas nendega seotud laod, hoiualad, tarvikud ja komponendid, mis ehitisega funktsiooni ja asukoha poolest seotuna moodustavad toimiva üksuse).

7) *Päritolupool* –pool, kellelt salastatud teave pärineb.

8) *Vastuvõttev pool*– pool, kellele edastatakse salastatud teavet.

9) *Kolmas isik*– rahvusvaheline organisatsioon või riik, kes ei ole kokkuleppe pool.

10) *Füüsilise isiku juurdepääsuluba*– dokument, mille poolte asjaomased asutused väljastavad isikule ja mis võimaldab juurdepääsu salastatud teabele kooskõlas poolte asjakohaste riigisiseste õigusaktidega.

11) *Juriidilise isiku juurdepääsuluba*– dokument, mis tõendab, et juriidiline isik ja tema ehitised on reaalselt ja organisatoorselt sobilikud salastatud teabe kasutamiseks ja hoidmiseks kooskõlas riigisiseste õigusaktidega.

12) *Põhjendatud teadmisvajadus* –salastatud teabele võimaldatakse juurdepääs üksnes isikule, kellel on tõestatud vajadus saada sellist teavet oma teenistus- ja ametikohustuste tõttu, mille raames teave vastuvõtvale poolele väljastati.

Artikkel 3. Salastatuse tasemed

(1) Salastatud teave märgistatakse ühega järgmistest üksteisele vastavatest salastatuse tasemetest:

HISPAANIA KEELES	INGLISE KEELES	EESTI KEELES
SECRETO	TOP SECRET	TÄIESTI SALAJANE
RESERVADO	SECRET	SALAJANE
CONFIDENCIAL	CONFIDENTIAL	KONFIDENTSIAALNE
DIFUSIÓN LIMITADA	RESTRICTED	PIIRATUD

(2) Vastuvõttev pool ja/või tema füüsilised või juriidilised isikud ei vähenda saadud teabe salastatuse taset ega kustuta teabe salastatust ilma päritolupoole eelneva kirjaliku nõusolekuta. Päritolupool teatab vastuvõtvale poolele kõik edastatud teabe salastatuse taseme muudatused.

(3) Vastuvõttev pool märgistab saadud salastatud teabe salastatuse taseme omakeelse vastega. Tõlked ja koopiad märgistatakse sama salastatuse tasemega kui originaalid.

Artikkel 4. Riigi julgeoleku volitatud esindajad

(1) Riikide julgeoleku volitatud esindajad, kes vastutavad kokkuleppe täitmise ja selle järelevalve eest, on järgmised:

Eesti Vabariigis: Riigi julgeoleku volitatud esindaja
Kaitseministeeriumi julgeolekuosakond, Eesti Vabariik, Sakala 1, 15094 Tallinn, EESTI;

Hispaania Kuningriigis: Välisminister, Riikliku Luurekeskuse direktor
Riiklik Julgeolekubüroo, Avda. Padre Huidobro, s/n, 28023 Madrid, HISPAANIA.

(2) Kummagi riigi julgeoleku volitatud esindaja annab teise riigi julgeoleku volitatud esindajale tolle taotlusel teavet oma julgeolekunõuete kohta ning võimaldab volitatud ametiisikute vastastikuseid külastusi.

Artikkel 5. Salastatud teabe kaitse

(1) Pooled võtavad kooskõlas oma õigusaktidega meetmeid, et kaitsta salastatud teavet, mida edastatakse, saadakse, koostatakse või töötatakse välja tulenevalt poolte või nende füüsiliste või juriidiliste isikute vahelistest kokkulepetest või suhetest. Pooled tagavad kooskõlas kokkuleppe artikliga 3 kogu edastatud, koostatud või välja töötatud salastatud teabele samasuguse kaitse nagu oma samaväärsel tasemel salastatud teabele.

(2) Poolte julgeoleku volitatud esindajad aitavad vastava taotluse korral ja oma õigusaktidest lähtudes teineteisel kontrollida oma riigi füüsilisi ja juriidilisi isikuid, kes elavad või asuvad teise poole territooriumil, enne juurdepääsulubade väljastamist.

(3) Pooled tunnustavad teise poole õigusaktide kohaselt väljastatud füüsiliste ja juriidiliste isikute juurdepääsulube. Juurdepääsulubade tasemed peavad olema kooskõlas kokkuleppe artikliga 3.

(4) Riikide julgeoleku volitatud esindajad teatavad teineteisele kõigist muudatustest seoses füüsiliste ja juriidiliste isikute juurdepääsulubadega, eeskätt aga nende tühistamisest või nende taseme alandamisest.

Artikkel 6. Salastatud teabe avalikustamine

(1) Pooled ei loovuta, avalikusta ega luba loovutada või avalikustada kokkuleppe alusel saadud salastatud teavet kolmandatele isikutele, nende kodanikele ega avalik- või eraõiguslikele isikutele ilma päritolupoole eelneva kirjaliku nõusolekuta. Salastatud teavet, mida üks pool edastab teisele poolele, kasutatakse üksnes määratud eesmärgil.

(2) Kokkuleppega ei lubata ega reguleerita intellektuaalse omandi õigusi sisaldava teabe loovutamist, kasutamist, vahetamist või avalikustamist selliste õiguste omaniku eelneva selgesõnalise kirjaliku loata, olenemata sellest, kas nende õiguste omanik on üks pooltest või kolmas isik.

Artikkel 7. Juurdepääs salastatud teabele

Juurdepääs salastatud teabele ja aladele, kus toimub salastatud tegevus või kus hoitakse salastatud teavet, võimaldatakse üksnes isikutele, kellel on nõuetekohane juurdepääsuluba ja põhjendatud teadmisvajadus.

Artikkel 8. Külastused

(1) Poolte kodanike vastastikused külastused, millega kaasneb juurdepääsuvajadus salastatud teabele, võivad toimuda vastuvõtva poole julgeoleku volitatud esindaja eelneval kirjalikul loal.

(2) Kolmandate isikute esindajate külastused, millega kaasneb juurdepääsuvajadus salastatud teabele, on lubatud üksnes päritolupoole kirjalikul nõusolekul.

(3) Lähetava poole julgeoleku volitatud esindaja teatab kavandatavast külastusest vastuvõtva poole julgeoleku volitatud esindajale kokkuleppe lisas määratud korras. Kõnealune lisa on kokkuleppe lahutamatu osa. Lisas määratud külastuskorda võib muuta mõlema poole julgeoleku volitatud esindajate kirjalikul nõusolekul.

Artikkel 9. Lepingud

(1) Pool, kes soovib sõlmida salastatud lepingut teise poole lepinglasega või volitada oma lepinglast sõlmima teise poole territooriumil salastatud projekti põhjal salastatud lepingut, hangib oma riigi julgeoleku volitatud esindaja kaudu teise poole julgeoleku volitatud esindajalt eelneva kirjaliku kinnituse selle kohta, et pakutud lepinglasel on nõuetekohase tasemega juriidilise isiku juurdepääsuluba ning sama tasemega salastatud teabe käsitlemiseks ja hoidmiseks sobivad ehitised.

(2) Poolte füüsiliste või juriidiliste isikute ja/või eraettevõtete vahel käesoleva kokkuleppe kohaselt sõlmitud salastatud lepingud peavad sisaldama asjakohast julgeolekuosa, mis sisaldab järgmist:
a) salastamisjuhend ja salastatud teabe loend;
b) teabe salastatuse muutmisest teatamise kord;
c) sidekanalid ja elektromagnetside vahendid;
d) salastatud materjali vedamise kord;
e) lepinguga seotud salastatud teabe kaitse kooskõlastamise eest vastutavad asutused;
f) kohustus teatada salastatud teabe kadumisest, lekkest või ohtusattumisest või sellekohasest kahtlusest.

(3) Alltöövõtja peab täitma samu julgeolekukohustusi kui lepinglane.

(4) Teade salastatud projektide, kokkulepete ning pea- ja alltöövõtulepingute kohta edastatakse eelnevalt selle riigi julgeoleku volitatud esindajale, kus töö tehakse.

(5) Salastatud lepingu julgeolekuosa koopia edastatakse selle poole julgeoleku volitatud esindajale, kelle territooriumil töö tehakse, et tal oleks võimalik jälgida julgeolekunõuete täitmist.

Artikkel 10. Teabevahetus

(1) Salastatud teavet vahetavad pooled harilikult diplomaatiliste või sõjaväekanalite kaudu.

(2) Kui nende kanalite kasutamine ei ole otstarbekas või aeglustab tarbetult salastatud teabe edastamist, võivad teavet edastada nõuetekohase juurdepääsuloaga isikud, kellel on salastatud teavet edastava poole väljastatud kulleritunnistus.

(3) Pooled võivad salastatud teavet vahetada elektrooniliselt, pidades kinni asjaomaste asutuste vastastikku kokkulepitud julgeolekunõuetest.

(4) Suurte esemete või salastatud teabe koguste vahetamiseks annavad mõlema poole julgeoleku volitatud esindajad iga kord eraldi loa.

(5) Salastatud teabe vahetamiseks võib mõlema poole julgeoleku volitatud esindajate heakskiidul kasutada muid võimalusi.

Artikkel 11. Salastatud teabe kaitse nõuete rikkumine

Salastatud teabe kaitse nõuete rikkumise korral, mis on seotud teise poole koostatud või temalt saadud salastatud teabe kadumise, lekkimise ja ohtusattumisega või kahtlusega, et salastatud teave on avalikustatud vastava juurdepääsuloata isikutele, teatab selle poole julgeoleku volitatud esindaja, kelle territooriumil julgeolekunõuete rikkumine toimus, teise poole julgeoleku volitatud esindajale võimalikult kiiresti juhtunust ning võtab meetmeid juhtunu nõuetekohaseks uurimiseks. Teine pool võtab vajaduse korral uurimisest osa. Teise poole julgeoleku volitatud esindajale teatatakse uurimise tulemustest ning edastatakse lõpparuanne julgeolekunõuete rikkumise põhjuste ja ulatuse kohta.

Artikkel 12. Kulud

Kumbki pool kannab kokkuleppe täitmisega ja selle järelevalvega seotud enda kulud.

Artikkel 13. Vaidluste lahendamine

Vaidlused kokkuleppe tõlgendamise ja kohaldamise üle lahendavad konsultatsioonide teel poolte julgeoleku volitatud esindajad või, kui sel viisil kokkuleppele ei jõuta, poolte täievolilised esindajad.

Artikkel 14. Lõppsätted

(1) Kokkulepe sõlmitakse määramata ajaks. Kokkulepe tuleb kummagi poole õigusaktide kohaselt heaks kiita ning see jõustub kolmekümnendal päeval pärast seda, kui saabub viimane teade selle kohta, et kokkuleppe jõustumiseks vajalik riigisisene menetlus on lõppenud. Kumbki pool võib kokkuleppe igal ajal kirjaliku teatega lõpetada. Sellisel juhul lõpeb kokkulepe kuus kuud pärast teate saamist.

(2) Kokkulepet võib mõlema poole kirjalikul nõusolekul igal ajal muuta. Muudatused jõustuvad lõike 1 kohaselt.

(3) Kokkuleppe lõppemise korral tagastatakse kokkuleppe alusel saadud salastatud teave ja esemed võimalikult kiiresti teisele poolele. Ülejäänud salastatud teavet ja esemeid kaitstakse kokkuleppe kohaselt.

Koostatud 11. novembril 2005 Madridis kolmes originaaleksemplaris eesti, hispaania ja inglise keeles. Kokkuleppe erineva tõlgendamise korral lähtutakse ingliskeelsest variandist.

Eesti Vabariigi nimel	**Hispaania Kuningriigi nimel**
Herman SIMM	**Alberto SAIZ CORTÉS**

Eesti Vabariigi ja Hispaania Kuningriigi
vahelise salastatud teabe kaitse kokkuleppe
lisa

KÜLASTUSKORD

(1) Üks pool lubab teise poole isikute külastusi, millega kaasneb juurdepääsuvajadus salastatud teabele, üksnes juhul, kui:
a) lähetava poole julgeoleku volitatud esindaja või muu asjaomane asutus on nendele külastajatele väljastanud nõuetekohase füüsilise isiku juurdepääsuloa ning
b) nendel külastajatel on õigus saada salastatud teavet või juurdepääs salastatud teabele kooskõlas lähetava poole õigusaktidega.

(2) Lähetava poole julgeoleku volitatud esindaja teatab kavandatavast külastusest vastuvõtva poole julgeoleku volitatud esindajale külastustaotlusega, mis peab kätte saadud olema vähemalt kakskümmend (20) tööpäeva enne külastust või külastusi.

(3) Pakilistel juhtudel tuleb külastustaotlus saata vähemalt viis (5) tööpäeva varem.

(4) Külastustaotlus peab sisaldama järgmist:
a) külastaja ees- ja perekonnanimi, sünniaeg ja -koht, kodakondsus, passi või isikutunnistuse number;
b) selle asutuse, ettevõtte või organisatsiooni nimi, mida külastaja esindab või kuhu ta kuulub;
c) külastatava asutuse, ettevõtte või organisatsiooni nimi ja aadress;
d) tõend külastaja füüsilise isiku juurdepääsuloa olemasolu ja kehtivuse kohta;
e) külastuse või külastuste eesmärk ja otstarve;
f) külastuse või külastuste kavandatav kuupäev ja kestus. Korduskülastuste korral tuleb märkida külastuste koguperiood;
g) külastatava asutuse/ehitise kontaktisiku nimi ja telefoninumber, varasemad kontaktid ja muu teave, mis aitab otsustada külastuse või külastuste põhjendatuse üle.

(5) Külastusloa kehtivus ei tohi ületada 12 kuud.

(6) Kõik külastajad peavad täitma vastuvõtva poole salastatud teabe kaitset reguleerivaid õigusakte.

SECURITY AGREEMENT ON THE PROTECTION OF CLASSIFIED INFORMATION BETWEEN THE REPUBLIC OF ESTONIA AND THE KINGDOM OF SPAIN
Done in Madrid on November 11, 2005; in force as of January 26, 2007

The Republic of Estonia and the Kingdom of Spain hereafter referred to as the Parties, in order to safeguard the Classified Information exchanged directly between the Parties or through public entities or private companies.

Have agreed on the following provisions:

Article 1. Applicability

(1) This Agreement sets out procedures for the protection of Classified Information exchanged between the Parties and falling under the responsibility of the respective National Security Authorities.

(2) This Agreement may not be invoked by either Party in order to obtain Classified Information that the other Party has received from a Third Party.

Article 2. Definitions

For the purpose of this Agreement:

1) *Classified Information*means
any information (namely knowledge that can be communicated in any form) or "material", determined to require protection against unauthorised disclosure which has been so designated by security classification.
a) the term "*Material*" means any item or substance from which information can be derived. This includes "documents" and any item of machinery, equipment, weapon o weapon-systems either manufactured or in the process of manufacture,
b) the term "*Document*" means any form of recorded information regardless of its physical form or characteristics, e.g. written or printed matter (*inter alia*letter, drawing, plan), computer storage media (*inter alia*fixed disk, diskette, chip, magnetic tape, CD), photograph and video recording, optical or electronic reproduction of them.

2) *Contract*means
an agreement between two or more Contractors creating and defining enforceable rights and obligations between them.

3) *Classified Contract*means
a contract which contains or involves Classified Information.

4) *National Security Authority*means
the authority designated by a Party as being responsible for the implementation and supervision of this Agreement.

5) *Contractor*means
a natural person or a legal entity possessing the legal capability to undertake Contracts.

6) *Facility*means
an installation, plant, factory, laboratory, office, university or other educational institution or commercial premises (including any associated warehouse, storage areas, utilities and components which when related by function and location, form an operating entity) of a legal person, or any government department and establishment.

7) *Originating Party*means
the Party initiating the Classified Information.

8) *Receiving Party*means
the Party to which the Classified Information is transmitted.

9) *Third Party*means
any international organisation or state that is not a Party to this Agreement.

10) *Personnel Security Clearance*means
the document granted by the relevant authorities of the Parties to a person, that will allow the access to Classified Information, in accordance with the respective national laws and regulations;

11) *Facility Security Clearance*means
the document proving that a legal person and its facilities have the physical and organisational capability to use and deposit Classified Information, in accordance with the national laws and regulations.

12) "*Need-to-know*" means

that access to Classified Information may only be granted to a person who has a verified need to know such information in connection with his official and professional duties, within the framework of which the information was released to the Receiving Party.

Article 3. Security Classifications

(1) Classified Information shall be assigned one of the following equivalent security classification levels:

SPANISH	ENGLISH	ESTONIAN
SECRETO	TOP SECRET	TÄIESTI SALAJANE
RESERVADO	SECRET	SALAJANE
CONFIDENCIAL	CONFIDENTIAL	KONFIDENTSIAALNE
DIFUSIÓN LIMITADA	RESTRICTED	PIIRATUD

(2) The Receiving Party and/or entities from its State shall neither downgrade the classification nor declassify the received Classified Information without the prior written consent of the Originating Party. The Originating Party shall inform the Receiving Party of any changes in security classification of the transmitted information.

(3) The Receiving Party shall mark the received Classified Information with its own equivalent security classification. Translations and reproductions shall be marked with the same security classification as the originals.

Article 4. National Security Authorities

(1) The National Security Authorities responsible for the implementation and supervision of all aspects of this Agreement are:

In the Republic of Estonia: National Security Authority
Department of Security, Ministry of Defence, Republic of Estonia, Sakala Str. 1, 15094 Tallinn, ESTONIA;

In the Kingdom of Spain: Secretary of State Director of the National Intelligence Centre
National Security Office, Avda. Padre Huidobro, s/n, 28023 Madrid, SPAIN.

(2) Each National Security Authority shall, on request, pass to the other National Security Authority information about its security standards and shall enable mutual visits by certified officials.

Article 5. Security Protection

(1) In accordance with their national laws and regulations, both Parties shall take appropriate measures to protect Classified Information, which is transmitted, received, produced or developed as a result of any agreement or relation between the Parties or entities of their States. The Parties shall afford to all transmitted, produced or developed Classified Information the same degree of security protection as is provided for their own Classified Information of the equivalent level of classification, as defined in Article 3 of this Agreement.

(2) On request, the National Security Authorities of the Parties, taking into account their national laws and regulations, shall assist each other during the vetting procedures of their citizens or facilities living or located in the territory of the other Party, preceding the issue of the Personnel Security Clearance and the Facility Security Clearance.

(3) The Parties shall recognise the Personnel and Facility Security Clearance issued in accordance with the national laws and regulations of the other Party. The equivalence of the security clearances shall be in compliance with Article 3 of this Agreement.

(4) The National Security Authorities shall communicate to each other any information related to changes of the Personnel and Facility Security Clearances, particularly concerning cases of withdrawal or downgrading of their classification level.

Article 6. Disclosure of Classified Information

(1) The Parties shall not release, disclose or permit the release or disclosure of Classified Information received under this Agreement to Third Parties, or to their nationals or public or private entities, without the prior written consent of the Originating Party. Classified Information transmitted from one Party to the other Party shall be used for the specified purpose only.

(2) Nothing in this Agreement shall be taken as an authority for, or to govern the release, use, exchange or disclosure of information in which intellectual property rights exist, until the specific written authorisation of the owner of these rights has first been obtained, whether the owner is one of the Parties or a Third Party.

Article 7. Access to Classified Information

Access to Classified Information and to specific areas where classified activities are performed or where Classified Information is stored, shall be limited only to those persons who have been granted appropriate Personnel Security Clearance and who have a “need-to-know”.

Article 8. Visits

(1) Visits entailing access to Classified Information by nationals from one Party to the other Party are subject to prior written authorisation given by the National Security Authority of the host Party.

(2) Visits entailing access to Classified Information by a national of a Third Party shall only be authorised upon the written consent of the Originating Party.

(3) The National Security Authority of the sending Party shall notify the National Security Authority of the host Party of expected visitors in accordance with the procedures defined in the Annex to this Agreement. This Annex forms an integral part to this Agreement. Visit procedures as defined in the Annex can be changed on the basis of written consent of both National Security Authorities.

Article 9. Contracts

(1) One Party, wishing to place a Classified Contract with a Contractor of the other Party, or wishing to authorise one of its own Contractors to place a Classified Contract in the territory of the other Party within a classified project, shall obtain through its National Security Authority prior written assurance from the National Security Authority of the other Party that the proposed Contractor holds a Facility Security Clearance of an appropriate level and has the suitable Facilities to handle and store Classified Information of the same level.

(2) Every Classified Contract concluded between entities of the Parties and/or private companies, under the provisions of this Agreement, shall contain an appropriate security section identifying the following aspects:
a) Classification guide and list of Classified Information;
b) Procedure for the communication of changes in the classification of information;
c) Communication channels and means for electromagnetic transmission;
d) Procedure for the transportation of classified material;
e) Relevant authorities responsible for the co-ordination of the safeguarding of Classified Information related to the Contract;
f) An obligation to notify any actual or suspected loss, leak or compromise of the Classified Information.

(3) Any subcontractor must fulfil the same security obligations as the Contractor.

(4) Notification of any classified project, agreement, contract or subcontract shall be forwarded in advance to the National Security Authority of the State where the work is to be performed.

(5) Copy of the security section of any Classified Contract shall be forwarded to the National Security Authority of the Party where the work is to be performed, to allow adequate security monitoring.

Article 10. Communications and Transmissions

(1) Classified Information shall normally be transmitted between the Parties through the military or diplomatic channels.

(2) If the use of such channels would be impractical or unduly delay receipt of the Classified Information, transmissions may be undertaken by appropriately security-cleared personnel empowered with a courier certificate issued by the Party, which transmits the Classified Information.

(3) The Parties may transmit Classified Information by electronic means in accordance with security procedures mutually determined by the relevant authorities.

(4) Delivery of large items or quantities of Classified Information arranged on a case-by-case basis shall be approved by both National Security Authorities.

(5) Other means of transmission of Classified Information may be used if approved by both National Security Authorities.

Article 11. Breach of Security

In case of a breach of security concerning loss, leak and compromise of Classified Information originated by or received from the other Party or suspicion that Classified Information has been disclosed to unauthorised persons, the National Security Authority of the Party where the breach occurs shall inform the National Security Authority of the other Party as soon as possible and take appropriate action to ensure that such an incident is properly investigated. The other Party shall, if required, co-operate in the investigation. The National Security

Authority of the other Party shall be informed of the results of the investigation and shall receive a final statement on the reasons and extent of the security violation.

Article 12. Expenses

Each Party shall bear its costs in connection with the implementation and supervision of all aspects of this Agreement.

Article 13. Settlement of Disputes

Any dispute regarding the interpretation or application of this Agreement shall be resolved by consultations between the National Security Authorities of the Parties or, in the case that such a settlement is impossible to reach, between duly authorised representatives of the Parties.

Article 14. Final Provisions

(1) This Agreement is concluded for an indefinite period. This Agreement is subject to approval in accordance with the national laws and regulations of both Parties and shall enter into force thirty days after the last written notification has been received indicating that the necessary conditions for this Agreement to enter into force have been fulfilled. This Agreement may be terminated at any time by either Party with a written notification. In such a case the Agreement expires six months after receipt of this notification.

(2) Amendments to the present Agreement may be made at any time with the consent of both Parties in written form. Such amendments shall enter into force in accordance with paragraph (1) of this Article.

(3) In the event of termination, Classified Information and/or items transmitted under the terms of this Agreement shall be returned to the other Party as soon as possible. Remaining Classified Information and/or items shall be protected in accordance with the provisions of this Agreement.

Done in Madrid on the 11th of November 2005 in three originals in the Estonian, Spanish and English languages. In case of different interpretations the English version of the Agreement shall prevail.

On behalf of the Republic of Estonia	**On behalf of the Kingdom of Spain**
Herman SIMM	**Alberto SAIZ CORTÉS**

Annex
to the Security Agreement on the Protection
of Classified Information between the
Republic of Estonia and the Kingdom of Spain

VISIT REQUIREMENTS

(1) Visits entailing access to Classified Information shall be allowed by one Party to visitors from the other Party only if they have been:
a) granted appropriate Personnel Security Clearance by the National Security Authority or other relevant authority of the sending Party; and
b) authorised to receive or to have access to Classified Information in accordance with the national laws and regulations of their Party.

(2) The National Security Authority of the sending Party shall notify the National Security Authority of the host Party of the planned visit through a request for visit, which has to be received at least twenty (20) working days before the visit or visits take place.

(3) In urgent cases, the request for visit could be transmitted at least five (5) working days before.

(4) The request for visit shall include:
a) Visitor’s first and last name, place and date of birth, nationality, passport or ID card number;
b) Name of the establishment, company or organisation he/she represents or to which he/she belongs;
c) Name and address of the establishment, company or organisation to be visited;
d) Certification of the visitor’s Personnel Security Clearance and its validity;
e) Object and purpose of the visit or visits;
f) Expected date and duration of the requested visit or visits. In case of recurring visits the total period covered by the visits should be stated;
g) Name and phone number of the point of contact at the establishment/facility to be visited, previous contacts and any other information useful to determine the justification of the visit or visits;

(5) The validity of visit authorisation shall not exceed twelve months.

(6) All visitors will comply with the national laws and regulations on the protection of Classified Information of the host Party.