Väljaandja:	Vabariigi Valitsus
Akti liik:	välisleping
Teksti liik:	algtekst
Jõustumise kp:	01.03.2008
Avaldamismärge:	RT II 2008, 17, 51

Eesti Vabariigi valitsuse ja Soome Vabariigi valitsuse salastatud teabe vastastikuse kaitse kokkulepe

"Eesti Vabariigi valitsuse ja Soome Vabariigi valitsuse salastatud teabe vastastikuse kaitse kokkuleppe" eelnõu heakskiitmine ja volituse andmine

Teadaanne välislepingu jõustumise kohta

Alla kirjutatud 5. juunil 2007. a Tallinnas, jõustus 1. märtsil 2008. a

Eesti Vabariigi valitsus ja Soome Vabariigi valitsus (edaspidi *pooled*),

soovides sätestada salastatud teabe vastastikuse kaitsmise korra,

on kokku leppinud järgmises.

Artikkel 1. Eesmärk ja kohaldamisala

Kokkuleppe eesmärk on kaitsta salastatud teavet, mida pooled vahetavad eelkõige välisasjade, kaitse-, julgeoleku-, politsei- või tööstusvaldkonnas või mida edastatakse salastatud lepingute ettevalmistamiseks või täitmiseks või mis luuakse vahetatud salastatud teabe põhjal või sellest tulenevalt.

Artikkel 2. Mõisted

Kokkuleppes kasutatakse järgmisi mõisteid:
a)*salastatud teave*– selle kokkuleppe alusel vahetatav või loodav teave või materjal, mille salajasust tuleb hoida ning mis on ühe poole riigisiseste õigusaktide kohaselt märgistatud salastusmärkega, et tagada teabe või materjali asjakohane kaitsmine;
b)*lepinglane*– ühe poole jurisdiktsiooni alla kuuluv füüsiline või juriidiline isik või ametiasutus, kellel on õigus sõlmida lepinguid;
c)*salastatud leping*– kahe või enama lepinglase vahel sõlmitud leping, mille täitmiseks on vaja salastatud teavet või juurdepääsu sellele või mille täitmise käigus või millest tuleneb salastatud teave;
d)*riigi julgeoleku volitatud esindaja*– asutus, kes vastutab kokkuleppe täitmise ja selle järelevalve eest;
e)*pädev asutus*– riigi julgeoleku volitatud esindaja või muu riigiasutus, kes riigisiseste õigusaktide kohaselt vastutab kokkuleppe täitmise eest;
f)*päritolupool*– pool, kellelt salastatud teave pärineb;
g) *vastuvõttev pool*– pool, kellele edastatakse salastatud teavet;
h)*riigisisesed õigusaktid*– seadused, määrused, ametlikud eeskirjad ja juhendid;
i)*füüsilise isiku juurdepääsuluba*– pädeva asutuse poolt riigisiseste õigusaktide kohaselt tehtud otsus, mille tulemusel antakse isikule juurdepääs salastatud teabele;
j)*juriidilise isiku juurdepääsuluba*– tõend selle kohta, et juriidiline isik ja tema ehitised sobivad füüsiliselt ja korralduslikult salastatud teabe kasutamiseks ja hoidmiseks riigisiseste õigusaktide kohaselt;
k)*põhjendatud teadmisvajadus*– tõendatud vajadus salastatud teabe järele.

Artikkel 3. Salastatud teabe kaitsmine

1. Pooled võtavad kooskõlas oma riigisiseste õigusaktidega kõik asjakohased meetmed salastatud teabe kaitsmiseks. Pooled tagavad sellele teabele samasuguse kaitse nagu oma samaväärsel tasemel salastatud teabele.

2. Pooled lubavad salastatud teabe juurde rahvusvahelisi organisatsioone ja riike, kaasa arvatud nende ametnikke ja füüsilisi või juriidilisi isikuid, kes ei ole käesoleva kokkuleppe pooled, üksnes teabe salastanud poole pädeva asutuse eelneval kirjalikul loal.

3. Salastatud teavet kasutatakse üksnes otstarbel, milleks see on edastatud.

4. Juurdepääs salastatud teabele võimaldatakse isikutele üksnes nende töö või kindla ülesande täitmise tõttu, lähtudes põhjendatud teadmisvajadusest.

5. Juurdepääs salastatud teabele, mille salastatuse tase on LUOTTAMUKSELLINEN/KONFIDENTSIAALNE või kõrgem, võidakse anda üksnes isikutele, kes on riigisiseste õigusaktide kohaselt saanud füüsilise isiku juurdepääsuloa.

6. Pooled tagavad oma territooriumil kokkuleppe täitmiseks vajaliku ehitiste julgeolekualase inspekteerimise ja isikute taustakontrolli nõuetekohase läbiviimise.

Artikkel 4. Salastatuse tasemed

1. Poolte salastatuse tasemed vastavad üksteisele järgmiselt:

Eesti Vabariik	Soome Vabariik
TÄIESTI SALAJANE	ERITTÄIN SALAINEN
SALAJANE	SALAINEN
KONFIDENTSIAALNE	LUOTTAMUKSELLINEN
PIIRATUD	KÄYTTÖ RAJOITETTU

2. Vastuvõttev pool tagab salastatud teabe ja selle koopiate märgistamise võrdväärsele riigisisesele salastatuse tasemele vastava märkega. Märgistatakse ka teave, mis on loodud edastatud salastatud teabe või salastatud lepingu põhjal või sellest tulenevalt.

3. Vastuvõtva poole riigi julgeoleku volitatud esindaja tagab, et salastatuse tase muudetakse või tühistatakse üksnes päritolupoole riigi julgeoleku volitatud esindaja taotlusel või loal.

4. Vastuvõtva poole riigi julgeoleku volitatud esindaja võib paluda päritolupoole riigi julgeoleku volitatud esindajal salastatuse taset muuta või see tühistada või põhjendada valitud salastatuse taseme määramist.

Artikkel 5. Salastatud lepingud

1. Päritolupool, kes sõlmib teise poole lepinglasega salastatud lepingu või volitab sellise lepingu sõlmimise, hangib selle poole pädevalt asutuselt tõendi lepinglase julgeolekukontrolli põhjal väljastatud juriidilise isiku juurdepääsuloa kohta. Tõend tuleb hankida enne, kui pakkumisel osalevale potentsiaalsele lepinglasele võimaldatakse juurdepääs salastatud teabele.

2. Pädevad asutused tagavad, et salastatud lepingutesse lisatakse sätted, mis käsitlevad lepinglase kohustust võtta salastatud teabe kaitseks asjakohaseid meetmeid, ning suunised salastatuse tasemete määramise kohta.

3. Pädevad asutused tagavad, et salastatud lepingutes nähakse ette keeld sõlmida salastatud lepinguid alltöövõtjatega enne, kui pädev asutus on selleks loa andnud. Alltöövõtjad peavad täitma samu julgeolekunõudeid kui põhilepingu sõlminud lepinglane.

4. Vastuvõtva poole pädevad asutused tagavad, et salastatud lepingute täitmisel peetakse kinni julgeolekunõuetest, mis on võrdväärsed poole enda sõlmitud salastatud lepingute suhtes kehtivate nõuetega. Selleks võtavad nimetatud pädevad asutused enne lepinglasele salastatud teabele juurdepääsu võimaldamist järgmisi meetmeid:
a) tagavad, et lepinglane suudab tagada salastatud teabe asjakohase kaitse;
b) väljastavad isikutele, kellel on töö või konkreetse ülesande täitmise tõttu vaja juurdepääsu salastatud teabele, asjakohase taustakontrolli alusel juurdepääsuloa tõendi;
c) tagavad, et kõik isikud, kellel on juurdepääs salastatud teabele, on teadlikud oma kohustustest, mis tulenevad kehtivatest riigisisestest õigusaktidest;
d) viivad selles artiklis nimetatud järelevalvekohustuse kohaselt läbi ehitiste julgeolekualase inspekteerimise.

Artikkel 6. Salastatud teabe edastamine

1. Teavet, mille salastatuse tase on ERITTÄIN SALAINEN / TÄIESTI SALAJANE, edastatakse üksnes ametlike valitsustevaheliste kanalite kaudu.

2. Teavet, mille salastatuse tase on SALAINEN/SALAJANE või LUOTTAMUKSELLINEN/ KONFIDENTSIAALNE, edastatakse harilikult ametlike valitsustevaheliste kanalite kaudu. Kiireloomulistel juhtudel või konkreetsetes projektides või programmides võib mõlema poole riigi julgeoleku volitatud esindajate heakskiidul kasutada ka muid kanaleid.

3. Niisuguse teabe edastamiseks, mille salastatuse tase on LUOTTAMUKSELLINEN/KONFIDENTSIAALNE või kõrgem, tuleb täita järgmisi nõudeid:
a) dokumenti või materjali vedaval isikul on asjakohase taustakontrolli põhjal väljastatud juurdepääsuloa tõend ja pädeva asutuse väljastatud kulleritunnistus;
b) päritolupool peab edastatud salastatud teabe kohta registrit ning esitab vastuvõtvale poolele selle taotlusel väljavõtte sellest registrist;
c) salastatud teavet sisaldavad dokumendid ja muud materjalid on nõuetekohaselt pakendatud ja pitseeritud;
d) salastatud teabe kättesaamist tuleb kirjalikult kinnitada.

4. Suurte salastatud teabe koguste edastamisel lepivad poolte riigi julgeoleku volitatud esindajad iga kord eraldi kokku kohaldatavates menetlustes.

5. Tasemel KÄYTTÖ RAJOITETTU / PIIRATUD salastatud teavet võib edastada ka posti teel või muu edasitoimetamisteenuse vahendusel, kui täidetakse päritolupoole riigisisestest õigusaktidest tulenevaid nõudeid.

6. Elektrooniliselt tohib salastatud teavet edastada üksnes täielikult krüpteerituna, kasutades selleks mõlema poole pädevate asutuste ühiselt kokku lepitud krüpteerimismeetodeid ja -vahendeid.

7. Poolte julgeolekuasutused võivad kooskõlas riigisiseste õigusaktidega operatiiv- ja/või luureteavet vahetada omavahel otse.

Artikkel 7. Salastatud teabe tõlkimine, paljundamine ja hävitamine

1. Tasemel ERITTÄIN SALAINEN / TÄIESTI SALAJANE või SALAINEN/SALAJANE salastatud teavet võib tõlkida või paljundada üksnes päritolupoole riigi julgeoleku volitatud esindaja eelneval kirjalikul nõusolekul.

2. Tasemel SALAINEN/SALAJANE või LUOTTAMUKSELLINEN/KONFIDENTSIAALNE salastatud teave tagastatakse päritolupoolele või hävitatakse riigisiseste õigusaktide kohaselt.

3. Kui vajadus tasemel ERITTÄIN SALAINEN / TÄIESTI SALAJANE salastatud teabe järele kaob, tagastatakse see päritolupoolele artiklis 6 ettenähtud korras, arvestades päritolupoole riigisiseseid õigusakte.

4. Kriisiolukorras, kui kokkuleppe raames loodud või edastatud salastatud teavet ei ole võimalik kaitsta ega tagastada, hävitatakse see viivitamata. Vastuvõttev pool teatab salastatud teabe hävitamisest päritolupoole riigi julgeoleku volitatud esindajale võimalikult kiiresti.

Artikkel 8. Külastused

1. Pooled lubavad teineteise esindajatel teha asutustes, kus töödeldakse või hoitakse salastatud teavet või kus toimuvad salastatud projektid, kontrollkülastusi üksnes vastuvõtva poole pädeva asutuse eelneval kirjalikul loal. Luba antakse üksnes isikutele, kellel on füüsilise isiku juurdepääsuluba ja põhjendatud teadmisvajadus.

2. Pooled lubavad teineteise valitsuste või lepinglaste esindajatel külastada enda või oma lepinglase neid ehitisi, kus külastajatel võib olla juurdepääs salastatud teabele. Külastajad peavad vastama artikli 3 lõigetes 4 ja 5 sätestatud nõuetele.

3. Külastajad peavad täitma vastuvõtvas asutuses ja selle ehitistes kehtivaid riigisiseseid julgeolekueeskirju ja -juhendeid. Külastajatele antud salastatud teave loetakse antuks sellele poolele, kelle valitsust need külastajad esindavad või kellel on jurisdiktsioon lepinglase üle, keda külastajad esindavad või kelle töötajad külastajad on; ning teavet kaitstakse vastavalt sellele.

4. Kui külastuse ajal soovitakse tutvuda teabega, mille salastatuse tase on LUOTTAMUKSELLINEN/ KONFIDENTSIAALNE või kõrgem, tuleb külastustaotlus esitada vastuvõtvale poolele üksnes ametlike valitsustevaheliste kanalite kaudu. Külastuste taotlemise kord kehtib üksnes tööstusliku julgeolekuga seotud ning julgeolekualase inspekteerimise külastuste kohta.

5. Külastustaotlus tuleb esitada vähemalt kaks nädalat enne kavandatava külastuse algust kas vastuvõtva poole riigikeeles või inglise keeles. Külastustaotluses tuleb esitada kokkuleppe lisas nimetatud andmed.

6. Pooled võivad oma pädevate asutuste vahel kokku lepitud tingimustel koostada nimekirjad isikutest, kellel on konkreetse projekti, programmi või hankelepingu raames õigus rohkem kui ühele külastusele. Sellised nimekirjad kehtivad kaksteist kuud. Poolte kokkuleppel võib niisuguste nimekirjade kehtivust pikendada korraga kuni kaheteistkümne kuu võrra.

7. Nimekirjade koostamises lepitakse kokku ja nimekirjad koostatakse vastuvõtva poole riigisiseste õigusaktide kohaselt. Kui nimekiri on koostatud, võib iga külastuse kooskõlastada otse külastatava lepinglase või asutusega.

Artikkel 9. Teatamine ja konsulteerimine

1. Pooled toetavad oma pädevate asutuste koostööd ning kokkuleppe täitmiseks teavitavad teineteist järgmisest:
a) salastatud teabe kaitset käsitlevad riigisisesed õigusaktid ja nende muudatused, kui need mõjutavad kokkuleppe alusel vahetatava või loodava või sellest tuleneva salastatud teabe kaitsmist;
b) riigi julgeoleku volitatud esindaja määramine ja selle muutmine.

2. Tiheda koostöö tagamiseks kokkuleppe täitmisel peavad poolte riigi julgeoleku volitatud esindajad üksteise taotlusel konsultatsioone.

Artikkel 10. Vaidluste lahendamine

Kõik pooltevahelised vaidlused kokkuleppe tõlgendamise või kohaldamise üle lahendatakse üksnes pooltevaheliste konsultatsioonide teel.

Artikkel 11. Salastatud teabe kaitse nõuete rikkumine

1. Kumbki pool teatab teisele poolele viivitamata kokkuleppes nimetatud salastatud teabe õigusvastase avaldamise või selle kaitse nõuete muu rikkumise kindlakstehtud juhtumitest või kahtlustest.

2. Pädev pool võtab oma riigisiseste õigusaktide kohaselt kõik meetmed, et piirata lõikes 1 osutatud rikkumiste tagajärgi ja hoida ära edasised rikkumised. Teine pool osutab esimese palvel rikkumise uurimisel abi; talle teatatakse uurimise tulemustest ja seoses rikkumisega võetud meetmetest.

Artikkel 12. Kulud

Pooled ei hüvita teineteisele kokkuleppe täitmisel tekkivaid kulusid.

Artikkel 13. Lõppsätted

1. Pooled teatavad teineteisele kokkuleppe jõustumiseks vajaliku riigisisese menetluse lõpetamisest. Kokkulepe jõustub viimase teate kättesaamispäevale järgneva teise kuu esimesel päeval.

2. Kokkulepe sõlmitakse määramata ajaks. Kokkulepet võib muuta poolte vastastikusel kirjalikul nõusolekul. Pooled võivad igal ajal teha ettepanekuid kokkuleppe muutmiseks. Asjaomase ettepaneku saamisel alustavad pooled konsultatsioone kokkuleppe muutmiseks.

3. Kumbki pool võib kokkuleppe lõpetada, teatades sellest teisele poolele ametlike valitsustevaheliste kanalite kaudu kirjalikult kuus kuud ette. Kokkuleppe lõppemise korral töödeldakse kokkuleppe alusel juba vahetatud ja kokkuleppest tulenevat salastatud teavet kokkuleppe kohaselt niikaua, kui on vajalik selle teabe kaitsmiseks.

Selle kinnituseks on poolte täievolilised esindajad kokkuleppele alla kirjutanud 5. juunil 2007. aastal Tallinnas.

Kokkulepe on koostatud kahes võrdselt autentses eksemplaris eesti, inglise ja soome keeles.
Tõlgenduserinevuste korral lähtutakse ingliskeelsest tekstist.

Eesti Vabariigi valitsuse nimel	**Soome Vabariigi valitsuse nimel**
Jaak AAVIKSOO	**Jyri HÄKÄMIES**

Lisa

KÜLASTUSTAOTLUSED

Kõik kokkuleppe artiklis 8 nimetatud külastustaotlused peavad sisaldama järgmisi andmeid:
1) külastaja perekonna- ja eesnimi, sünniaeg ja -koht, passi või isikutunnistuse number;
2) külastaja kodakondsus;
3) külastaja ametikoht või -nimetus ning selle asutuse nimi, kus külastaja töötab;
4) külastaja juurdepääsuloa tase, mis näitab, millises ulatuses on külastajal õigus juurdepääsuks salastatud teabele;
5) külastuse eesmärk ja kavandatav kuupäev;
6) asutused ja ehitised, mida soovitakse külastada, ning nende kontaktisikud.

AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC OF ESTONIA ANDTHE GOVERNMENT OF THE REPUBLIC OF FINLAND ON THE MUTUAL PROTECTION OF CLASSIFIED INFORMATION

Signed on the 5th of June, 2007 in Tallinn, in force as of the 1st of March, 2008

The Government of the Republic of Estonia and the Government of the Republic of Finland, hereinafter referred to as the “Parties”,

desirous of laying down an arrangement on the mutual protection of classified information,

have agreed as follows:

Article 1. Purpose and scope of application

The purpose of this Agreement is to protect classified information transmitted between the Parties particularly for purposes of foreign affairs, defence, security, police or industrial matters, or transmitted for the preparation or implementation of classified contracts, or produced on the basis of or arising from transmitted classified information.

Article 2. Definitions

For the purposes of this Agreement:
a)*classified information*means information or material transmitted or produced under this Agreement that is to be kept secret and has been marked with a classification marking under the national law of a Party so as to ensure that the information or material is appropriately protected;
b)*contractor*means an individual, a legal person or a public authority under the jurisdiction of one of the Parties possessing the legal capacity to conclude contracts;
c)*classified contract*means a contract between two or more contractors the implementation of which requires access to, or the use of, classified information or where classified information is produced to implement the contract or arises from the contract;
d)*National Security Authority*means the national authority responsible for the implementation and supervision of this Agreement;
e)*competent authority*means the National Security Authority or other national authority which, under the national law, is responsible for the implementation of this Agreement;
f)*originating Party*means the Party initiating classified information;
g)*recipient Party*means the Party to which classified information is transmitted;
h)*national law*means laws, subordinate regulations, official instructions and guidelines:
i)*personnel security clearance*means a determination by the competent authority that allows a person to access classified information, in accordance with the relevant national law;
j)*facility security clearance certificate*means a 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 relevant national law.
k)*need-to-know*means a verified need to access classified information.

Article 3. Protection of classified information

1. The Parties shall take all appropriate measures under their national law to protect classified information. They shall afford such information the same protection as they afford to their own information at the corresponding level of classification.

2. The Parties shall not grant access to classified information to any international organisation or any state, including its officials, citizens and legal entities, that is not a Party to this Agreement, without the prior written consent of the competent authority of the Party which determined the classification.

3. Classified information shall be used solely for the purpose for which it has been transmitted.

4. Access to classified information may only be granted to individuals on account of their work or performance of a given task, on a need-to-know basis.

5. Access to information classified as LUOTTAMUKSELLINEN/KONFIDENTSIAALNE or above may only be granted to individuals who hold a personnel security clearance in accordance with the relevant national law.

6. In their respective territories, the Parties shall ensure that the security inspections of facilities and the background checks of individuals necessary for the implementation of this Agreement are appropriately carried out.

Article 4. Security Classification Levels

1. The security classifications levels shall correspond to one another as follows:

Republic of Estonia	Republic of Finland
TÄIESTI SALAJANE	ERITTÄIN SALAINEN
SALAJANE	SALAINEN
KONFIDENTSIAALNE	LUOTTAMUKSELLINEN
PIIRATUD	KÄYTTÖ RAJOITETTU

2. The recipient Party shall ensure that any classified information and any copies of such information are marked with a marking designating the corresponding national security classification level. A marking shall be made also on information produced on the basis of or arising from transmitted classified information or a classified contract.

3. The National Security Authority of the recipient Party shall ensure that the security classification level is altered or revoked only when so requested or allowed by the National Security Authority of the originating Party.

4. The National Security Authority of the recipient Party may request the National Security Authority of the originating Party to alter the security classification level or revoke it, or to supply reasons for the choice of a given level of classification.

Article 5. Classified contracts

1. The originating Party, which concludes, or permits the conclusion of, a classified contract with a contractor of the recipient Party, shall obtain from the competent authority of that Party a facility security clearance certificate based on a security vetting of the contractor. The certificate shall be obtained before access to classified information is granted to a potential contractor participating in a tender process.

2. The competent authorities shall ensure that classified contracts contain both provisions on the duty of the contractor to undertake the necessary measures for the protection of classified information and classification instructions.

3. The competent authorities shall ensure that classified contracts contain provisions that prohibit concluding a classified contract with a subcontractor before the competent authority has granted a permission to do so. Subcontractors shall be subject to the same security requirements as the contractor which concluded the main contract.

4. The competent authorities of the recipient Party shall ensure that the same standard of security is observed in the implementation of classified contracts as would be the case with classified contracts concluded by that Party itself. To this end, these competent authorities shall undertake the following measures before access to classified information is granted to the contractor:
a) ensure that the contractor can offer appropriate protection to classified information;
b) issue personnel security clearance certificates to those persons who have a verified need for access to classified information for reasons of work or performance of a given task;
c) ensure that everyone with access to classified information is aware of his or her obligations under the applicable national law;
d) carry out security inspections in facilities subject to the duty of supervision referred to in this Article.

Article 6. Transmission of classified information

1. Information classified as ERITTÄIN SALAINEN/TÄIESTI SALAJANE shall only be transmitted through official Government-to-Government channels.

2. Normally, information classified as SALAINEN/SALAJANE or LUOTTAMUKSELLINEN/ KONFIDENTSIAALNE shall be transmitted through official Government-to-Government channels. In urgent cases or for specific designated projects or programmes, also other channels may be used, subject to the approval of the National Security Authorities of both Parties.

3. The transmission of information classified as LUOTTAMUKSELLINEN/ KONFIDENTSIAALNE and above shall meet the following requirements:
a) the person carrying the document or material holds a security clearance certificate issued on the basis of an appropriate background check and a courier certificate issued by a competent authority;
b) the originating Party maintains a register of transmitted classified information and, on request by the recipient Party, provides the latter with an extract of the register;
c) the documents and other materials containing classified information are appropriately packaged and sealed;
d) the receipt of classified information is confirmed in writing.

4. If a large volume of classified information is to be transmitted, the applicable procedures shall be agreed upon by the National Security Authorities on a case-by-case basis.

5. Information classified as KÄYTTÖ RAJOITETTU/PIIRATUD may be transmitted also by post or another delivery service, taking due note of the requirements of the national law of the originating Party.

6. Classified information may be transmitted electronically only in a fully encrypted mode, using encryption methods and devices jointly approved by the competent authorities of both Parties.

7. The security services of the Parties may exchange operative and/or intelligence information directly with each other in accordance with national law.

Article 7. Translation, copying and disposal of classified information

1. Information classified as ERITTÄIN SALAINEN/TÄIESTI SALAJANE or SALAINEN/SALAJANE may be translated or copied if the National Security Authority of the originating Party has given a prior written consent for it.

2. Information classified as SALAINEN/SALAJANE or LUOTTAMUKSELLINEN/KONFIDENTSIAALNE shall be returned to the originating Party or disposed of in accordance with national law.

3. Information classified as ERITTÄIN SALAINEN/TÄIESTI SALAJANE shall be returned to the originating Party in accordance with the procedure provided in Article 6 after it is no longer considered necessary, taking into account the national law of the recipient Party.

4. In case of a crisis situation which makes it impossible to protect and return classified information generated or transmitted according to this Agreement, the classified information shall be destroyed immediately. The recipient Party shall notify the National Security Authority of the originating Party about the destruction of classified information as soon as possible.

Article 8. Visits

1. Security inspection visits to premises where classified information is developed, handled or stored, or where classified projects are carried out, shall only be granted by one Party to visitors from the other Party if a prior written permission from the Competent Authority of the recipient Party has been obtained. Such permission shall only be granted to persons who have a personnel security clearance and a need-to-know.

2. Each Party shall allow visits by personnel of the administration or of a contractor of the other Party to its own or its contractor's facilities, where the visitors may have access to classified information. The visitors shall meet the requirements referred to in paragraphs 4 and 5 of Article 3.

3. The visitors shall abide by the national security instructions and guidelines applicable in the host agency and its facility. Classified information that has been provided to the visitors shall be deemed to have been provided to the Party whose administration the visitors represent or which exercises jurisdiction over the contractor whom the visitors represent or are employed by; the information shall be secured accordingly.

4. If, during a visit, information classified as LUOTTAMUKSELLINEN/KONFIDENTSIAALNE or above is to be accessed, the visit request shall be submitted to the host Party solely through official Government-to-Government channels. The visit request procedure shall be limited only to industrial security visits and security inspection visits.

5. The visit request shall be submitted at least two (2) weeks before the intended time of the visit, either in the national language of the host Party or in English. The visit request shall contain the information referred to in the Annex to this Agreement.

6. In accordance with conditions agreed upon by their competent authorities, the Parties may draw up lists of personnel who are entitled to more than one visit in the context of an individual project, programme or procurement contract. Such lists shall have a period of validity of twelve (12) months. However, the period of validity of such lists may be extended, by agreement between the Parties, for at most twelve (12) months at a time.

7. The agreement on the lists shall be concluded and the lists shall be drawn up in accordance with the national law of the host Party. Once a list has been drawn up, the particulars of a single visit may be agreed upon directly with the contractor or agency to be visited.

Article 9. Notification and consultations

1. The Parties shall promote the co-operation between their competent authorities and, in order to implement this Agreement, notify each other of the following:
a) national laws on the protection of classified information and amendments to such laws, when these may affect the protection of classified information to be exchanged, arising or produced under this Agreement;
b) the designation of National Security Authorities and any changes thereto.

2. In order to ensure close co-operation in the implementation of this Agreement, the National Security Authorities of the Parties shall consult each other at the request of one of these authorities.

Article 10. Resolution of disputes

All disputes between the Parties on the interpretation or application of this Agreement shall be resolved exclusively by means of consultations between the Parties.

Article 11. Violations of provisions on the protection of classified information

1. Each Party shall immediately notify the other Party of any suspicions or discoveries of unlawful disclosure of classified information referred to in this Agreement or of other violations of the protection of such information.

2. The Party with jurisdiction shall undertake all possible appropriate measures under its national law so as to limit the consequences of violations referred to in paragraph 1 of this Article and to prevent further violations. Upon request, the other Party shall provide investigative assistance; it shall be informed of the outcome of the investigation and of the measures undertaken as a result of the violation.

Article 12. Costs

The Parties shall not reimburse each other for the costs incurred in the implementation of this Agreement.

Article 13. Final provisions

1. The Parties shall notify each other of the completion of the national procedures necessary for the entry into force of the Agreement. The agreement shall enter into force on the first day of the second month following the receipt of the later notification.

2. This Agreement shall be in force for an indeterminate period of time. The Agreement may be amended by the mutual, written consent of the Parties. Either Party may propose amendments to this Agreement at any time. If one Party so proposes, the Parties shall begin consultations on the amendment of the Agreement.

3. A Party may terminate this Agreement by written notification to the other Party delivered through official Government-to-Government channels, observing a period of notice of six (6) months. If the Agreement is terminated, the classified information already transmitted and the classified information arising from this Agreement shall be handled in accordance with the provisions of this Agreement for as long as necessary for the protection of the classified information.

In witness whereof, the duly authorised representatives of the Parties have signed this Agreement, in Tallinn on the 5th day of June, 2007 in two originals, both in the Estonian, Finnish and English languages, each text being equally authentic. In case of any divergence of interpretation the English text shall prevail.

For the Government of the Republic of Estonia	**For the Government of the Republic of Finland**
Jaak AAVIKSOO	**Jyri HÄKÄMIES**

Annex

VISIT REQUESTS

All visit requests referred to in Article 8 of the Agreement shall contain the following information:
1. the given name and surname of the visitor, his or her date and place of birth, and the number of his or her passport or identity card;
2. the citizenship of the visitor;
3. the position or service designation of the visitor, as well as the name of the authority, agency or facility to whose personnel the visitor belongs;
4. the grade of the security clearance of the visitor, indicating the scope of his or her right to access classified information;
5. the purpose of the visit and its proposed date;
6. the agencies and facilities to be visited and the contact persons there.