GNS
Gabinete Nacional de Segurança

NORMA TÉCNICA – B 03

ACREDITAÇÃO E AVALIAÇÃO DE PRODUTOS CRIPTOGRÁFICOS.

Lisboa, 17 de Julho de 2016

A Autoridade Nacional de Segurança

(José Torres Sobral)

1. REFERENCIAS

a. Decreto-Lei nº 3/2012, de 16 de Janeiro;

b. AC/35-D/0047 - Cryptographic Security and Cryptographic Mechanisms Directive;

c. AC/35-D/1019 - Guidelines for the Evaluation and Certification of ADP Systems.

2. SITUAÇÃO

O uso massivo das tecnologias de informação e comunicação (TIC) em todos os âmbitos da sociedade, criou um novo espaço, o ciberespaço, donde terá origem conflitos, agressões e onde existem as ciber ameaças que sem a menor dúvida atentarão contra a segurança nacional, o Estado de Direito, a prosperidade económica, o bem estar social e o normal funcionamento da sociedade, da administração publica e do Estado.

O decreto-lei 3/2012 de 16 de Janeiro, lei orgânica do Gabinete Nacional de Segurança resulta que cabe ao GNS determinar a avaliação, a acreditação e a certificação de produtos e sistemas de comunicações, de informática e de tecnologias de informação que sirvam de suporte ao tratamento, arquivo e transmissão de informação classificada dos quais se inclui a acreditação de produtos criptográficos

3. OBJECTO/FINALIDADE

O objectivo do presente documento é o de detalhar o processo de avaliação e elaborar para um determinado produto criptográfico, a síntese da informação e material que se considera imprescindível para poder avaliar e certificar em termos de segurança criptográfica um determinado produto de cifra.

A aquisição de um produto de cifra também chamado produto ou equipamento criptográfico, especialmente quando utilizado para cifrar informação classificada, obrigatoriamente tem de ser sujeito a uma comprovação e adequação dos mecanismos criptográficos implementados no produto de cifra para proteger a dita informação.

A avaliação e certificação de um produto de cifra, são processos que permitem valorar e acreditar a capacidade de um produto de processar informação de forma segura. Em Portugal estas funções cabem ao Gabinete Nacional de Segurança.

A avaliação e certificação de um produto de cifra deve abarcar tantos os aspectos relativos à segurança criptográfica dos algoritmos utilizados, como aos aspectos relacionados com a sua implementação nos equipamentos onde são inseridos, assim como os aspectos relacionados com a eficácia dos seus mecanismos de autoprotecção.

Por este motivo, a informação referida neste documento é tanto aquela que se considere necessária para avaliar a segurança do algoritmo (descrição do mesmo, simulação, resultados de testes, etc) como aquela documentação técnica adicional que seja precisa para comprovar que a cifra da informação se realiza de acordo com o algoritmo e as chaves utilizadas, e também se efectua segundo os procedimentos descritos na documentação.

A informação disponibilizada deve permitir comprovar que a partir da informação de saída do produto de cifra, se pode verificar que as tramas de dados de informação cifradas, aparecem conforme o algoritmo utilizado, conforme a chave seleccionada e que no restante das tramas de dados de informação auxiliar não aparece nenhum tipo de informação que comprometa a segurança da informação no seu global.

Também será necessário dispor-se de informação sobre a descrição funcional do produto de cifra e sobre a implementação dos requisitos funcionais de segurança no dito produto, assim como os testes realizados para comprovar as funções e mecanismos de segurança do produto.

Assim é necessário conhecer e verificar a eficácia dos mecanismos de segurança inseridos no produto de cifra para proteger os elementos criptográficos.

No caso de o produto de cifra seja software e esteja implementado sobre uma plataforma, deverá ser implementada segurança nessa plataforma de modo a salvaguardar a segurança do produto de cifra impedindo assim a manipulação do produto a avaliar.

O produto de cifra será certificado para uma versão concreta do produto, em função de uma configuração concreta e de acordo com umas normas de utilização que serão descritas no procedimento de emprego do produto.

A empresa fabricante do produto certificado deverá distribuir este procedimento de emprego junto com o produto de cifra certificado criptograficamente.

4. ÂMBITO

A presente norma destina-se a ser do conhecimento de todos os Chefes de Órgão de Segurança, Sub-Registos e Postos de Controlo, bem como dos Responsáveis pela Segurança dos Serviços, Órgãos ou Organismos, públicos ou privados, quer dentro, quer fora do país que tenham acesso a matéria classificada, de grau de classificação igual ou superior a RESERVADO, bem como a Universidades, Forças Armadas e fabricantes de produtos criptológicos que os pretendam acreditar nas marca nacional nas diferentes classificações de segurança.

A presente norma técnica também se aplica aqueles produtos de cifra que venham a ser adquiridos pela administração pública e pelo Estado para proteger a informação nacional classificada ou aquela que normativamente pela sua sensibilidade requer protecção.

No caso do produto de cifra necessitar de outros produtos associados para o seu funcionamento, como por exemplo um centro de gestão, geradores aleatórios, dispositivos de transporte e carregamento de chaves, estes produtos terão também de ser avaliados e certificados criptograficamente pelo Gabinete Nacional de Segurança

5. EXECUÇÃO DESCRIÇÃO DOS PROCESSO DE APROVAÇÃO PARA CERTIFICAÇÃO DE PRODUTOS CRIPTOGRÁFICOS

Áreas que deverão ser sujeitas a avaliação:

Avaliação "common Criteria" feita por laboratório certificado ou indicado pelo GNS. Certificação elaborada pelo GNS.

Análise de vulnerabilidades feita por laboratório certificado ou indicado pelo GNS. Certificação elaborada pelo GNS.

Avaliação Criptologica feita por laboratório certificado ou indicado pelo GNS. Certificação elaborada pelo GNS.

Avaliação "Tempest" feita por laboratório certificado ou indicado pelo GNS. Certificação elaborada pelo GNS.

O processo de avaliação e acreditação de produtos criptográficos que sirvam para cifrar informação classificada é um processo que resulta de diversas avaliações a que se submete um produto e entre elas se inclui a avaliação criptográfica.

O processo de avaliação criptográfica começa com o pedido de acreditação criptográfica do produto a avaliar (ver Anexo A). Este pedido deve ser acompanhado por um pedido formal da necessidade do produto por parte de um organismo da administração publica ou Estado (ver Anexo B).

Devido à complexidade do processo de avaliação criptográfica e a consumir uma grande quantidade de recursos, este processo só se realizará aqueles dispositivos que tenham previamente superado uma avaliação funcional e uma análise de vulnerabilidades.

Para detectar possíveis vulnerabilidades e funções de segurança que à priori não cumpram com robustez necessária para proteger a informação nacional classificada do nível esperado, é conveniente que ao iniciar-se o processo de avaliação funcional e de análise de vulnerabilidades se faça entrega ao laboratório criptográfico designado pelo Gabinete Nacional de Segurança o pacote inicial de documentação e material descrito no anexo C.

Uma vez concluída a avaliação funcional e análise de vulnerabilidades do produto criptográfico, terá de realizar-se uma reunião entre a empresa que propôs a acreditação e a equipa multidisciplinar de Garantia da Gabinete Nacional de Segurança e o laboratório que fez a avaliação, na qual se fará a entrega da restante documentação e material para certificação criptográfica (ver anexo C), dando-se inicio à avaliação criptográfica do produto.

Após a conclusão da avaliação criptográfica e em caso de esta ter sido favorável, será redigido uma informação técnica de avaliação (ITE) e o procedimentos de emprego do equipamento de cifra ou sistema de cifra. Depois de ter sido feita a revisão e estudado todos os relatórios técnicos de avaliação das diferentes áreas de análise (funcional, análise de vulnerabilidades, criptográfica e *tempest*) o GNS expede um certificado de acreditação com a aprovação para, processar e transmitir informação nacional para segurança das TIC, onde figura o máximo nível de classificação que está autorizado a processar, tal como a data desde que é válida a acreditação.

Certificado de acreditação:

O certificado de acreditação criptográfica do produto leva o selo branco do GNS e é assinado pela Autoridade Nacional de Segurança que como director do Gabinete Nacional de Segurança é a autoridade de acreditação criptográfica.

Uma vez finalizado o processo de acreditação, será comunicado à empresa fabricante que o produto superou o processo de acreditação criptográfica. Também se incluirá o produto no catálogo de produtos criptográficos acreditados pelo GNS e publicado na página WEB do GNS.

6. DESCRIÇÃO DOS PROCESSO DE AVALIAÇÃO CRIPTOGRÁFICA

23. A avaliação criptográfica consiste em verificar os aspectos de segurança física, criptográfica que proporciona ao produto criptográfico em função dos resultados obtidos por esta avaliação atribuir a máxima classificação de segurança da informação que estão autorizados a processar.

24. Os possíveis resultados da avaliação dos activos de segurança são:

POSITIVO: As condições para ter um veredicto positivo são que depois de se realizar a avaliação do activo, o avaliador determine que o activo avaliado cumpre os requisitos definidos para o activo avaliado. As condições para que um elemento passe na avaliação define-se como: todas as provas necessárias para realizar a avaliação do activo são coerentes, não tem inconsistências internas ou inconsistências com outras provas de avaliação.

NEGATIVO: As condições para ter um veredicto negativo são que depois de realizada a avaliação do activo, o avaliador determine que o activo avaliado não cumpre ou não satisfaz os requisitos definidos para o activo avaliado, ou que o resultado das provas realizadas são incoerentes ou que se tenha detectado alguma contradição na provas realizadas.

Não conclusivo: Inicialmente todos os veredictos são não conclusivos e continuam assim até que haja o veredicto de positivo ou negativo.

O veredicto global da avaliação é positivo só e só se todos os veredictos dos activos avaliados forem positivos.

Em caso de que durante a avaliação do equipamento se descubra alguma vulnerabilidade ou mal funcionamento do produto de cifra, deverá ser comunicado á empresa esse facto. O fabricante deverá eliminar essa vulnerabilidade no mínimo tempo possível desde a sua comunicação.

7. DOCUMENTAÇÃO A APRESENTAR PARA O PROCESSO DE AVALIAÇÃO CRIPTOGRÁFICA

Esta Norma Técnica deve ser divulgada a todos os responsáveis por SIC.

Esta Norma técnica aplica-se após a sua difusão e será oportunamente complementada.

Para realizar a avaliação criptográfica de um produto é necessário a entrega de documentação por parte do fabricante do produto. Esta informação é necessária para o conhecimento em detalhe do equipamento por parte do avaliador.

A informação fornecida pelo fabricante será utilizada exclusivamente pelo GNS para realizar o processo de avaliação criptográfica do produto, salvaguardando-se a confidencialidade e a propriedade da dita informação. Em caso em que se solicite uma certificação externa internacional (NATO, UE) a informação será entregue directamente ao organismo que realize a certificação.

É a seguinte a informação mínima obrigatória a fornecer:

DESCRIÇÃO FUNCIONAL DO PRODUTO

A descrição funcional do produto de cifra incluirá informação sobre especificação funcional do dito produto, assim como o desenho de alto nível e desenho detalhado. A descrição funcional do produto de cifra é uma descrição completa e precisa do comportamento das diferentes interfaces externas do produto, efeitos com diferentes entradas e possíveis erros.

INFORMAÇÃO TÉCNICA

Deverá ser entregue informação sobre o hardware do produto. Esta informação sobre o hardware deverá poder identificar todos os blocos e componentes do produto de cifra.

A informação deverá permitir a localização física dos diversos elementos funcionais até ao nível de componente no caso do hardware e a posição lógica ao nível do código fonte no caso do hardware.

A informação sobre o hardware incluirá pelo menos os seguintes dados:

a) Esquemas das placas de circuito impresso
b) Datasheets dos componentes fundamentais do circuito
c) Identificação de cada um dos blocos do circuito
d) Descrição de caixa negra de cada um dos blocos do circuito, com os sinais de entrada, de saída, características dos sinais, largura de banda, tolerância, etc
e) Se um bloco for formado por blocos menores, deverá ser feita a descrição de caixa negra para cada um desses sub blocos.
f) Esquemas do circuito, começando pelo circuito completo e descendo até ao nível de blocos, sub blocos terminando no nível de componente.
g) Se o hardware utilizar elementos programáveis, o seu código de programação deverá ter o mesmo nível de detalhe do restante software

Além disso deverá ser fornecida informação sobre as ferramentas de desenvolvimento e verificação utilizadas pelo fabricante, as suas versões, configuração dessas ferramentas e do sistema de desenvolvimento, e parâmetros de compilação caso seja necessário no processo de avaliação.

SOFTWARE DO PRODUTO

O fabricante deverá entregar a seguinte informação sobre o produto de cifra:

Código fonte do software desenvolvido para o produto de cifra. Junto com o código fonte deverá ser fornecido as ferramentas de desenvolvimento utilizadas no desenho e desenvolvimento do produto de cifra, assim como as instruções necessárias à sua compilação.
Documentação da estrutura e funcionalidade e características técnicas do software do produto de cifra.
Funções, diagramas de bloco e diagramas de fluxo de dados, bem como a interacção entre eles e descrição sucinta das interacções entre os blocos e sub blocos. Descrição de parâmetros, dados de entrada e de saída

MEDIDAS DE PROTECÇÃO FISICA

Este capitulo versa sobre as medidas de protecção física que deverá ser proporcionada:

A protecção física é as medidas implementadas para garantir a protecção física dos diferentes elementos do produto criptográfico.

Resposta implementada no produto ao detectar-se que haja uma vulnerabilidade relacionada com uma medida de protecção física

Deverá entregar-se a descrição dos procedimentos para verificação do correcto funcionamento do produto de cifra ou do sistema (teste da correcta operação do equipamento, protecções anti-tampering, protecções contra picos de tensão, protecção contra excesso de temperatura, etc)

MEDIDAS DE PROTECÇÃO LÓGICAS

Este capítulo versa sobre as medidas de protecção lógica que deverá ser proporcionada:

Medidas que o produto de cifra implementa para garantir a segurança dos diferentes elementos criptológicos.

Resposta implementada no produto ao detectar-se que haja uma vulnerabilidade relacionada com uma medida de protecção lógica.

Deverá entregar-se a descrição dos procedimentos para verificação do correcto funcionamento do produto de cifra ou do sistema (teste da correcta operação do equipamento, protecções do software, protecções do firmware, protecção dos parâmetros críticos de segurança, etc)

CRIPTOGRAFIA

Este capítulo versa sobre a informação criptológica que deverá ser fornecida pelo fabricante do produto de cifra que vai ser avaliado criptologicamente. Em particular informação sobre os algoritmos empregues.

Essa informação incluirá a descrição completa e detalhada dos algoritmos criptográficos utilizados, e a informação detalhada para ter uma compreensão total da forma como funciona o algoritmo de cifra, pelo menos: A descrição geral dos algoritmos utilizados e de cada um dos elementos que o formam, assim como a interligação e funcionamento conjunto dos ditos elementos.

Incluirá também informação sobre os diferentes modos de operação do algoritmo e sobre todas as operações necessárias para se efectuar o correcto funcionamento do algoritmo.

Diagrama com todos os passos para transformar a informação em claro a informação cifrada.

Em caso de o produto de cifra empregar algoritmos definidos em normas publicas, ter-se-á de fazer referencia à norma empregue.

GESTÃO de CHAVES

A informação incluirá a descrição completa e detalhada da gestão das chaves utilizadas de maneira a que permita a completa compreensão do funcionamento da mesma e deverá conter pelo menos:

a. Descrição do processo de pedido de chaves.

b Descrição completa e detalhada da criação de chaves e formato das mesmas.

c. Descrição do processo de transporte de chaves e medidas de proteção.

d.. Descrição da transmissão da chave ao dispositivo destinatário.

e. Descrição do processo de registos e auditoria.

f. Descrição do armazenamento de chaves.

g. Descrição do processo de substituição e revogação de chaves.

h. Descrição do processo de destruição de chaves.

i. Descrição dos períodos criptográficos das chaves.

INICIALIZAÇÃO

A informação incluirá a descrição completa e detalhada da inicialização do equipamento criptográfico e dos processos de comprovação da sus segurança antes de estar inicializada para uso.

GERADOR DE NUMEROS ALEATÓRIOS

Descrição detalhada do gerador de números aleatórios (a nível de software e hardware) e as provas que se efetuaram para verificar o seu correto funcionamento. O fabricante deve incluir uma ferramenta de teste que permita por parte do GNS a saída de dados e geradores físicos e lógicos que implemente o sistema a avaliar.

AUTENTICAÇÃO DOS UTILIZADORES

Descrição detalhada das diferentes regras de autenticação que tem o equipamento e as funções permitidas por cada regra.
Descrição detalhada dos algoritmos e processos utilizados para autenticação de utilizadores.

8. PROVAS DE VALIDAÇÃO E QUALIFICAÇÃO

Esta Norma Técnica deve ser divulgada a todos os responsáveis por SIC.

Esta Norma técnica aplica-se após a sua difusão e será oportunamente complementada.

9. MANUAIS DO PRODUTO

Esta Norma Técnica deve ser divulgada a todos os responsáveis por SIC.

Esta Norma técnica aplica-se após a sua difusão e será oportunamente complementada.

10. MATERIAIS PARA AVALIAÇÃO

GNS – Gabinete Nacional de Segurança

NT – Norma Técnica

11. REFERÊNCIAS

GNS – Gabinete Nacional de Segurança

NT – Norma Técnica

12. ACRÓNIMOS

GNS – Gabinete Nacional de Segurança

NT – Norma Técnica

SIC – Sistema de Informação e Comunicação

13. ANEXO

Nada a referir.