# Módulo Cifrador de Documentos Eletrônicos

**Ricardo Felipe Custódio**[1] **, Júlio da Silva Dias**[2*]
**Fernando Carlos Pereira**[1] **, Adriana Elissa Notoya**[1]

[1]Laboratório de Segurança em Computação – Universidade Federal de Santa Catarina
Caixa Postal 476 – 88040-900 Florianópolis, SC

[2]Universidade do Estado de Santa Catarina
Av. Madre Benvenuta, 2037 – 88035-001 Florianópolis, SC

{custodio,jdias,fcarlos,elissa}@inf.ufsc.br

***Abstract.*** *Electronic documents are relevant for many applications and users. Doctors, lawyers or bankers requires information confidentiality. However, the solutions found cannot provide the confidentiality required, presenting high costs and limited functions. This paper presents the security requirements that were obtained through the analysis of several applications. Based on this security requirements we propose the implementation of a new architecture for a secure encipherment module.*

***Resumo.*** *O sigilo de documentos eletrônicos é essencial em aplicações que envolvem informações críticas, como no comércio eletrônico e aplicações bancárias. Entretanto, as soluções existentes para prover o sigilo ainda não são satisfatórias, devido ao alto custo de suas implementações e por atender o sigilo sob uma ótica restrita. Este trabalho apresenta um levantamento de requisitos necessários ao sigilo de documentos eletrônicos e propõe a implementação de um Módulo Cifrador que visa disponibilizar um método com custo acessível e abranger todos os requisitos estabelecidos, ainda não contemplados nas propostas existentes.*

## 1 Introdução

O surgimento de técnicas que permitem imprimir aos documentos eletrônicos os mesmos requisitos de segurança existentes no documentos papel tem auxiliado a disseminação de seu uso. Estes requisitos são autenticidade, integridade, tempestividade, não-repúdio e sigilo. O atendimento dos requisitos autenticidade e integridade são alcançados através do uso de assinaturas digitais [Stinson, 1995]. As autoridades

*Apoiado pela Universidade do Estado de Santa Catarina e CAPES.

de datação fornecem a referência temporal necessária para atender ao requisito tempestividade [Buldas and Lipmaa, 1998, Ansper et al., 2001, Dias et al., 2003]. O não-repúdio, composto pela irrefutabilidade e irretratabilidade, tem sido amplamente discutido [Austrália et al., 2003], tendo soluções desenvolvidas baseadas em software e hardware [Balacheff et al., 2001]. O sigilo pode ser alcançado com o uso de criptografia [Schneier, 1995, Stinson, 2002].

O sigilo do documento eletrônico é obtido pela sua cifragem e o armazenamento seguro da chave de deciframento. A decifragem do documento depende diretamente da técnica de cifragem utilizada: se simétrica, é necessário o conhecimento da chave de sessão; se assimétrica, é necessária a posse da chave privada correspondente a chave pública usada na cifragem. Entretanto, a perda da chave de decifragem impossibilita o acesso e inutiliza o documento cifrado. A gerência da chave de deciframento e do documento cifrado não é trivial.

A chave de decifragem deve ser armazenada de forma segura enquanto existir a necessidade de manutenção do sigilo. Várias estratégias têm sido usadas para gerir este problema. Uma delas consiste em cifrar o documento também com a chave pública de uma terceira parte confiável. Assim, caso o destinatário do documento cifrado perca a chave de decifragem, existe a possibilidade de recorrer à terceira parte para realizar a decifragem. Outra estratégia consiste em também cifrar o documento com uma chave pública, cuja chave privada será distribuída, em partes, a um grupo de entidades através de técnicas de compartilhamento de segredos. Assim, caso o destinatário perca a chave privada, pode-se solicitar, a um sub-grupo autorizado do grupo que recebeu as partes da chave de decifragem, a recuperação desta.

Na prática, a cifragem de documentos eletrônicos é feita usando-se cifras simétricas, uma vez que estas são, em geral, mais eficientes que as cifras assimétricas. A chave de sessão $K_S$, produto de um gerador de números aleatórios, utilizada na cifra simétrica é cifrada com a chave pública do destinatário. Desta maneira somente o destinatário, de posse da sua chave privada, é capaz de decifrar o documento, pois somente ele é capaz de decifrar a chave de sessão. Este esquema é bastante conhecido e utilizado em diversos sistemas de informação que cifram suas informações. No entanto, é ineficaz no atendimento de alguns requisitos de segurança. Isto é demonstrado pelo fato de que nada impede que a entidade que cifra um documento mantenha uma cópia da chave $K_S$. Com isso, qualquer entidade de posse de $K_S$ pode decifrar o documento sem possuir a chave de decifragem de $K_S$. Isso mostra que é necessário um esquema de ciframento que não permita ao usuário o controle sobre a chave de sessão. E isso só pode ser realizado por um módulo externo e independente da plataforma computacional do usuário. Este é o mesmo conceito utilizado por um HSM - *Hardware Security Module*.

Um HSM consiste de um dispositivo de hardware desenvolvido para executar serviços específicos, tais como a geração e armazenamento de chaves e a realização de operações criptográficas, em aplicações que exigem elevado grau de segurança. O projeto

e a implementação de um HSM deve atender a requisitos de segurança e funcionamento estabelecidos pela recomendação FIPS 140-2 [NIST, 2002] ou ISO [ISO, 1999]. Um dos requisitos é a exigência de que o HSM deve ser lacrado e protegido contra violações que possam comprometer o sigilo dos dados que mantém. O HSM gera, usa e destrói chaves criptográficas sem que entidades externas tenham acesso as mesmas.

O serviço de ciframento, apesar de previsto nas funcionalidades de um HSM, não atende às necessidades de capacidade de processamento, quantidade de memória e de políticas de cifragem mais flexíveis e abrangentes, normalmente exigidas pelas mais diversas aplicações. Este trabalho propõe a arquitetura de um Módulo Cifrador - MC que atende estas necessidades. Os MC devem ter elevada capacidade de processamento e memória suficiente para receber grandes documentos.

Os requisitos de segurança e funcionalidade do MC são apresentados na seção 2. Os requisitos são atendidos por blocos funcionais, também apresentados na seção 2, que uma vez reunidos irão compor o Módulo Cifrador Completo. Estes blocos são: cifrador básico, cifrador utilizando compartilhamento de segredos, selo, janelas públicas e prova de conteúdo e origem. A seção 3 discute o atendimento dos requisitos de segurança e funcionalidade. E a seção 4 apresenta uma discussão sobre o resultado do trabalho e trabalhos futuros.

## 2 Módulo Cifrador

Uma análise das aplicações que utilizam documentos eletrônicos sigilosos, tais como licitação pública, aplicações financeiras e votação digital, proporcionaram o levantamento dos requisitos de segurança e funcionalidade que um MC deve atender. Estes requisitos são:

Req-1. deve ser possível controlar o acesso ao conteúdo do documento cifrado. A chave de deciframento só pode ser liberada para os destinatários que possuem direito de acesso ao documento sigiloso;
Req-2. chaves criptográficas de deciframento podem somente ser exportadas se cifradas ou protegidas por esquemas de compartilhamento de segredos;
Req-3. não deve ser possível armazenar o documento em claro após a execução do processo de cifragem;
Req-4. não deve ser possível conhecer o conteúdo completo de um documento;
Req-5. não deve ser possível determinar qual documento cifrado corresponde a um documento original.

Os vários blocos funcionais do MC são apresentados na seqüência.

### 2.1 Módulo Cifrador Básico

O MC básico é responsável pelo recebimento do documento $DOC$ a ser cifrado e os certificados digitais dos usuários que poderão decifrar o documento, conforme ilustrado na Figura 1. O MC básico, utilizando um Gerador de Números

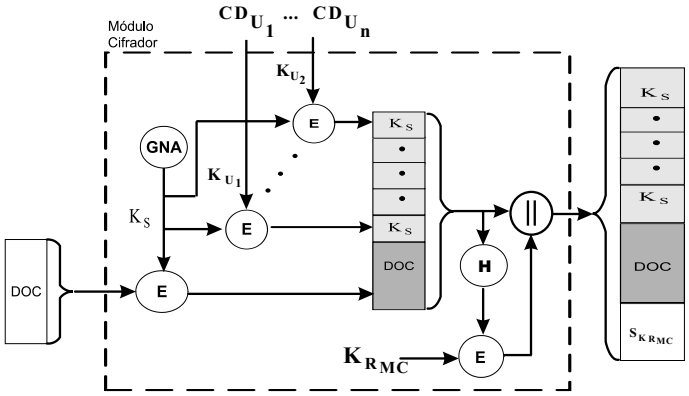


Figura 1: Módulo Cifrador Básico.

Aleatórios - GNA, gera uma chave simétrica $K_S$ para cifrar o documento $DOC$, gerando $E_{K_S}[DOC]$. A chave simétrica $K_S$ é então cifrada utilizando-se cada uma das $n$ chaves públicas $K_{U_i}$ e posteriormente destruída. Os diferentes arquivos contendo a chave de sessão cifrada são concatenados com $DOC$ cifrado produzindo $DS = [E_{K_{U_1}}[K_S], ..., E_{K_{U_n}}[K_S], E_{K_S}[DOC]]$. Por fim $DS$ e sua assinatura, $E_{K_{R_{MC}}}[H(DS)]$, são entregues ao requisitante do ciframento. O conjunto $\{DS, E_{K_{R_{MC}}}[H(DS)]\}$ é referenciado por envelope, em analogia à forma utilizada para manter sigiloso um documento papel através de um envelope lacrado. No envelope são adicionadas todas as informações necessárias ao correto procedimento de recuperação da chave de deciframento.

A revelação do conteúdo de um documento cifrado só pode ser realizada por um dos destinatários que possuem uma chave privada $K_{R_i}$ correspondente a uma das chaves públicas $K_{U_i}$, utilizadas no processo de ciframento do documento.

O deciframento do documento pelo destinatário é mostrado na Figura 2. Primeiro é necessário verificar a integridade e autenticidade do envelope. Deve-se verificar também se envelope foi produzido por um MC confiável. Em seguida, destinatário utiliza a sua chave privada para decifrar a chave de sessão $K_S$ e, através do uso desta, decifrar $DOC$.

## 2.2 Módulo cifrador utilizando compartilhamento de segredo

A política de deciframento de um documento cifrado pelo MC básico é muito simples: o destinatário, de posse da chave privada, usa-a para decifrar o documento. Entretanto, em várias situações práticas, esta política não é adequada. São necessários mecanismos que propiciem políticas mais complexas, adequadas a cada tipo documento. Uma forma suprir esta necessidade é prover tal política através de esquemas de compartilhamento de segredos. Estes trabalham com um conjunto $P$ de participantes, onde partilha-se a chave de deciframento em diversas partes e entrega-se cada uma delas a um membro diferente de $P$. Seja $\Gamma$ o conjunto dos subconjuntos de $P$. Os subconjuntos em $\Gamma$ são os subconjuntos de $P$ capazes de reconstruir a chave de deciframento. $\Gamma$ é chamado

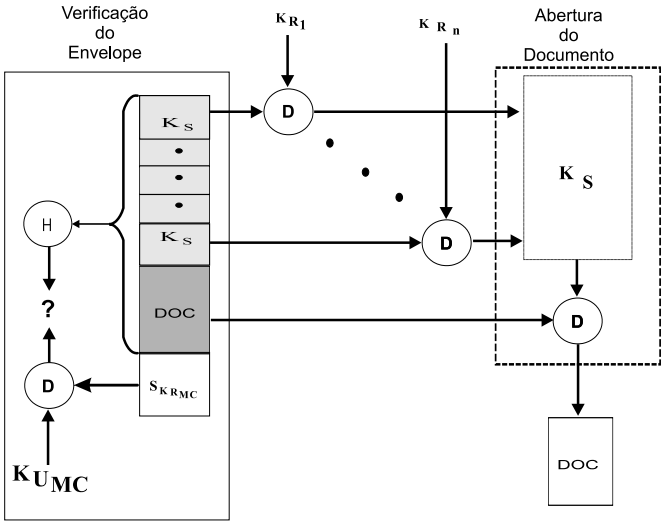


Figura 2: Recuperação de $DOC$, cifrado pelo MC básico.

de estrutura de acesso e os subconjuntos em $\Gamma$ são denominados de subconjuntos autorizados. Para a reconstrução da chave de deciframento é necessário que um subconjunto autorizado de participantes $B \subseteq P$ reúnem suas partes [Stinson, 1995]. Vários têm sido os algoritmos propostos na literatura que implementam este esquema. O mais simples é o particionamento de segredos em $m$ partes usando a operação Ou-exclusivo $\bigoplus$. Seja $x$ o segredo que se quer partilhar em $m$ partes. Gera-se, de forma aleatória $y_i$, para $i = 1 \ldots m-1$. Faz-se $z = x \bigoplus y_1 \bigoplus \ldots \bigoplus y_{m-1}$. As partes serão $z, y_1, ..., y_{m-1}$. Para se reconstruir o segredo faz-se $x = z \bigoplus y_1 \bigoplus \ldots \bigoplus y_{m-1}$. Neste esquema $B = P$, o que implica que todos os participantes devem contribuir para a reconstrução do segredo.

Outro esquema bastante conhecido é baseado na interpolação polinomial [Shamir, 1979]. Neste esquema um polinômio $F(x) = a_0 + a_1.x + ... + a_{n-1}.x^{n-1}$ de grau $(n-1)$ é construído de tal forma que o coeficiente $a_0$ seja o segredo. Seja $m \geq n$ o número de participantes que receberão as partes do segredo. Cada participante recebe um ponto $(F(x_i), x_i)$ com $x_i \neq 0$. Para se reconstruir o segredo são necessários os pontos de $t$ participantes com $m \geq t \geq n$. Com estes $t$ pontos, pode-se obter o segredo $a_0$, por interpolação polinomial [Press et al., 1994].

A Figura 3 ilustra a arquitetura proposta para o funcionamento do MC utilizando esquemas de compartilhamento de segredo.

Um aspecto normalmente considerado ao se partilhar segredos é a necessidade de se verificar a validade das partes produzidas e as utilizadas no processo de reconstrução do segredo. Os esquemas de compartilhamento de segredos, tais como o Ou-exclusivo e a interpolação polinomial, normalmente não atendem este requisito. É necessário a utilização de artifícios como aqueles propostos por Gennaro [Gennaro, 1998] para se

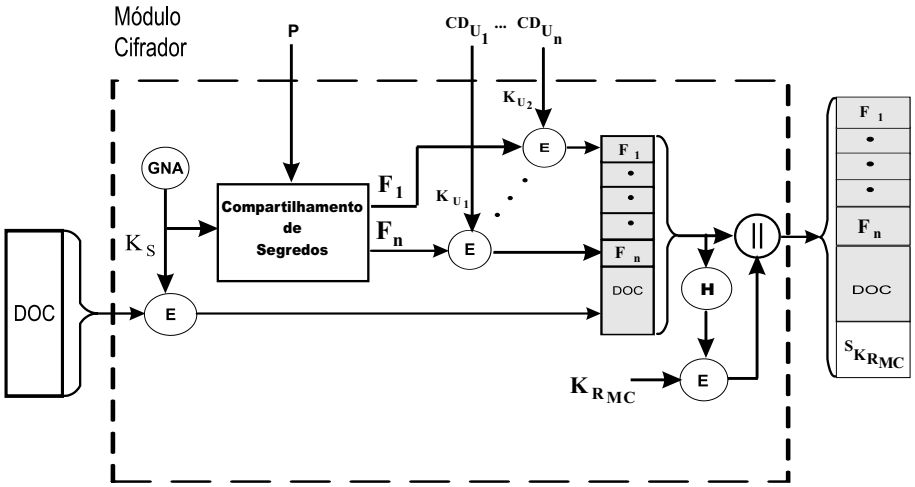


Figura 3: Módulo Cifrador Utilizando Compartilhamento de Segredo

garantir tal verificabilidade. Entretanto, como as partes cifradas são anexadas ao documento cifrado e todo o conjunto é assinado pelo MC, não há a necessidade aqui do uso destes esquemas mais elaborados.

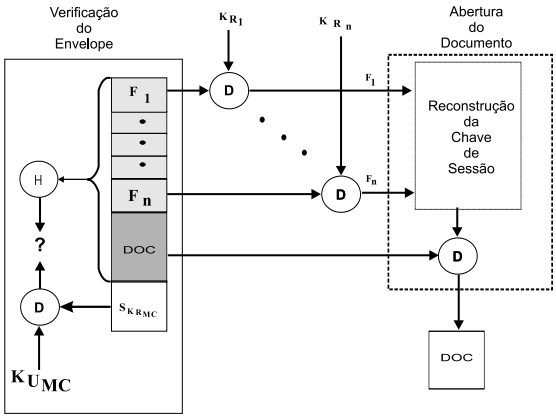


Figura 4: Recuperação de $DOC$ utilizando esquema de compartilhamento de segredos.

O destinatário, após verificar a assinatura do MC, pode escolher um subconjunto de partes e enviá-las para os proprietários das chaves privadas capazes de decifrar cada uma destas partes. Ao receber uma parte decifrada, o destinatário, pode facilmente conferir se a parte recebida corresponde a parte cifrada, uma vez que possui a chave pública utilizada no ciframento da parte. De posse das partes decifradas, o destinatário pode reconstruir a chave $K_S$ e proceder o deciframento de $DOC$. Este processo é representado na figura 4.

## 2.3 Selo

Com o objetivo de propiciar um maior controle aos usuários interessados na manutenção do sigilo de documentos propõe-se a utilização de uma informação externa, denominada selo. O MC concatena o resumo criptográfico deste selo à chave de sessão $K_S$. O resumo criptográfico desta concatenação, $K_S^*$, é utilizado como chave para cifrar $DOC$, conforme é ilustrado na Figura 5. Para ter-se acesso a $DOC$, é necessário primeiro decifrar-se $K_S$ e em seguida, obter $K_S^*$ para decifrar-se $DOC$.

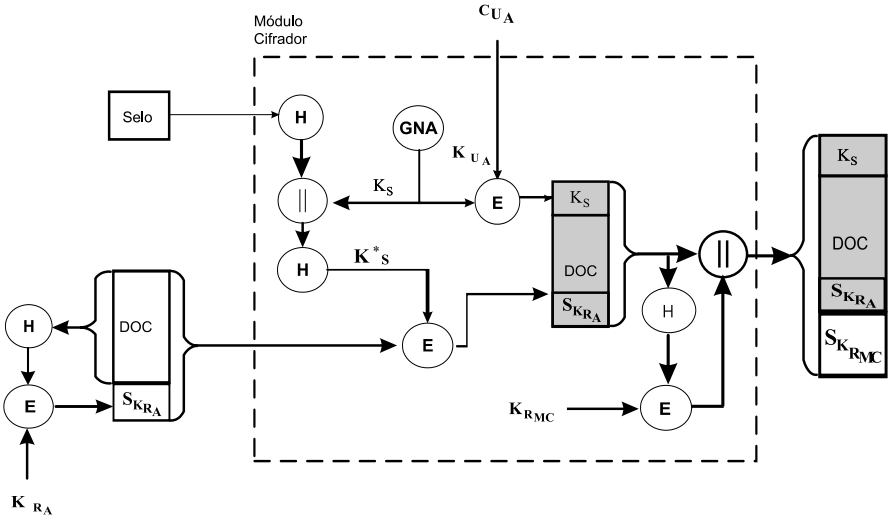


Figura 5: Selo

O selo pode ser mantido em segredo ou tornado público. Quando mantido em segredo, fornece um segundo mecanismo de controle de acesso ao conteúdo de documento: o destinatário, além de necessitar da chave de sessão $K_S$, precisa também do selo para poder decifrar o documento. Quando público, pode ser utilizado como controle de acesso aos serviços da infra-estrutura. Neste caso, o selo é fornecido pela entidade prestadora do serviço. O cliente da infra-estrutura deve adquirir o selo que será utilizado pelo MC na geração da chave simétrica de cifragem do documento. Somente selos válidos seriam aceitos pelo MC para permitir acesso ao processo de ciframento.

## 2.4 Janela Pública

Janelas públicas são informações anexadas ao documento ou ao envelope que não são cifradas, conforme ilustra a Figura 6. Isso é importante para facilitar a gerência do documento cifrado. A janela anexada ao documento é chamada janela interna. A anexada ao envelope é a janela externa.

A janela interna, é anexada ao documento através da assinatura do conjunto janela interna e $DOC$. Somente $DOC$ e a assinatura são cifrados pelo MC. Ao $DOC$ e assi-

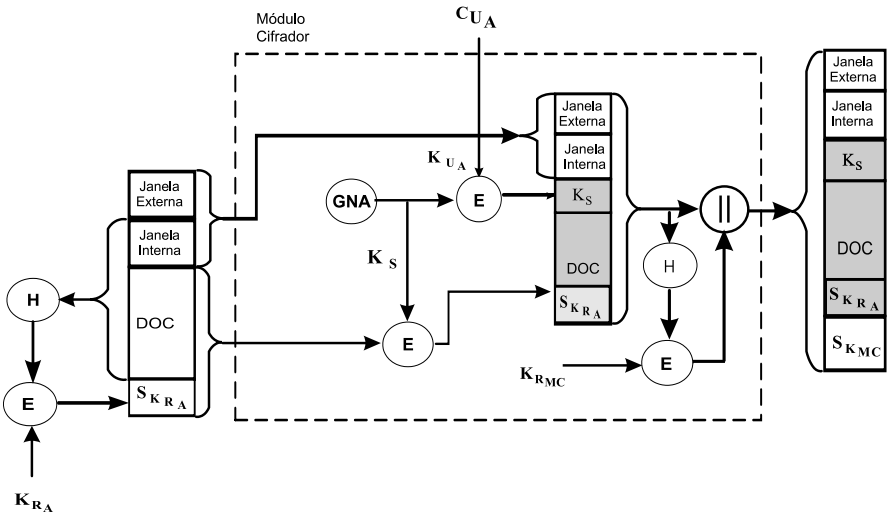


Figura 6: Janelas Públicas

natura cifrados são anexadas as janelas externa e interna. Todo o conjunto é então assinado pelo MC.

## 2.5 Módulo Cifrador Completo

O MC completo agrega todas as funcionalidades do MC básico, compartilhamento de segredos, selo e janela pública conforme ilustra a Figura 7.

A unidade de controle é responsável pela recepção e interpretação das políticas de ciframento. A interpretação das políticas gera sinais de controle aos componentes internos do MC ditando o seu comportamento.

Para contornar a possibilidade de um agente externo obter acesso ao conteúdo de um documento através do uso de um cifrador malicioso, é necessário eliminar possíveis evidências que permitam a quebra do sigilo por parte do autor ou por parte de outra entidade com acesso à plataforma computacional do proprietário do documento eletrônico. Propõe-se a utilização do módulo em conjunto com um software cliente capaz de dividir o documento em blocos menores. Estes blocos menores são submetidos a vários MC de forma aleatória, conforme ilustra a Figura 8. Desta forma um MC não tem acesso ao conteúdo completo do documento eletrônico.

O acesso ao conteúdo completo é possível somente se todos os módulos cifradores envolvidos agissem em conjunto e mesmo assim, soubessem a ordem correta de todas os blocos cifrados. Isso é improvável pela característica proposta para estas entidades: cada MC assina suas partes, deve ser confiável e não deve estar submetido a uma mesma administração. A comunicação entre o solicitante e o MC é realizada utilizando canais seguros garantindo o sigilo na comunicação. Uma vez que o cliente recebeu todas as partes cifradas de um documento, estas são re-ordenadas para o envio aos destinatários.

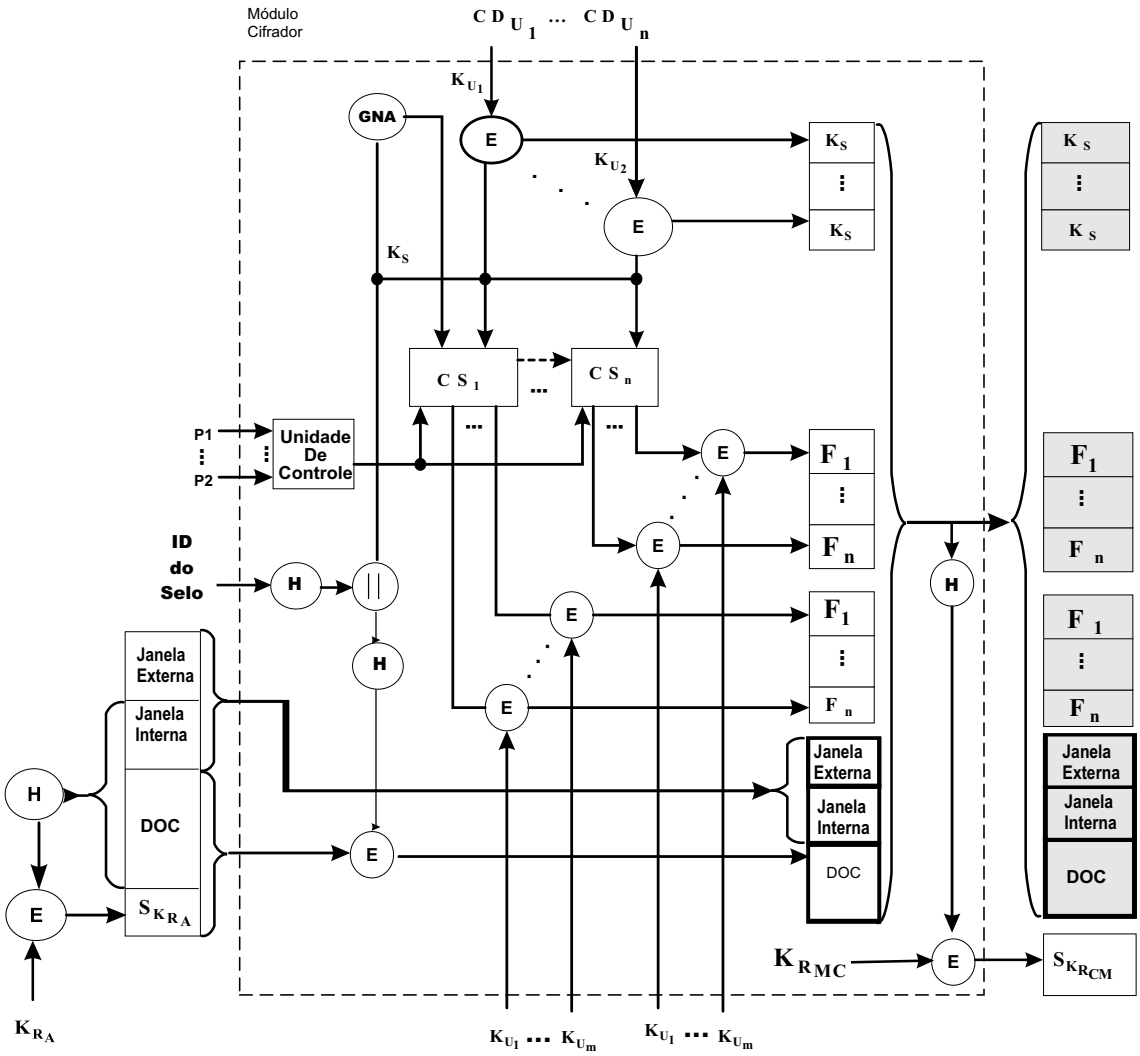


Figura 7: Módulo Cifrador Completo.

## 2.6 Gerenciamento do Módulo Cifrador

O gerenciamento do MC é possível através de funções de configuração e de auditoria. Estas funções são disponíveis exclusivamente para o administrador do módulo.

Ao iniciar pela primeira vez o MC, deve-se definir o administrador e os usuários, seja através de senhas ou de certificados digitais. Uma vez definido o administrador, este ativa o procedimento de geração do par de chaves criptográficas de assinatura, que é realizado em duas etapas. A primeira consiste na geração de um par de chaves assimétricas e de uma requisição no formato PKCS#10 contendo a chave pública deste par. Esta requisição deve ser encaminhada, pelo administrador, a uma Autoridade Certificadora. A segunda etapa consiste na importação do certificado digital emitido. A chave

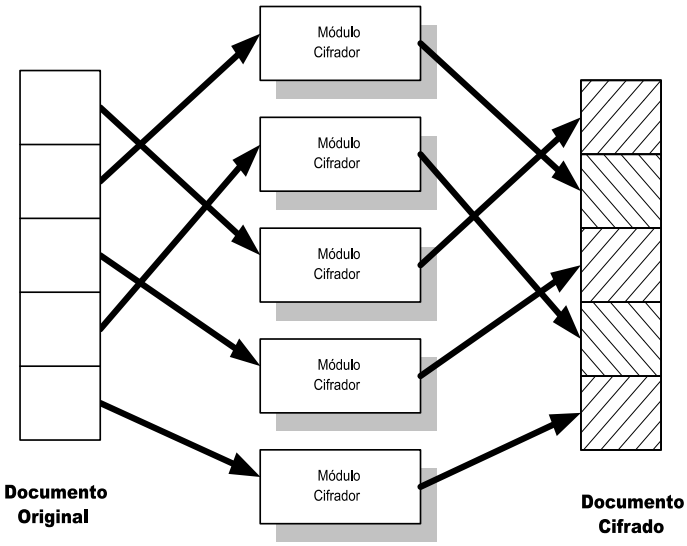


Figura 8: Uso de Múltiplos Módulos Cifradores. Um documento tem seu conteúdo dividido em várias partes. Cada uma das partes é enviada a um diferente MC, escolhido de forma aleatória. O requisitante recebe de cada um dos MC as partes cifradas e monta o documento cifrado, inserindo as informações necessárias para que o destinatário possa remontar o documento original, assim que tiver acesso à chave de deciframento.

privada do par é mantida interna ao módulo e será utilizada para assinar os envelopes. Também devem ser inseridos a lista certificados digitais das autoridades certificadoras que o MC deve confiar bem com suas respectivas listas de certificados revogados. Finalmente, o administrador estabelece políticas de funcionamento. Estas podem ativar e desativar funcionalidades de acordo com a necessidade da aplicação que fará uso do seu serviço.

Periodicamente, o administrador deve realizar algumas operações de rotina: renovar o certificado de assinatura do MC; verificar o estado de funcionamento interno; definir novos usuários; gerenciar a lista de autoridades certificadoras confiáveis e listas de certificados revogados e caso necessário, realizar auditoria nos registros internos.

As informações para a verificação da validade de certificados digitais devem ser fornecidas pelo solicitante ao utilizar o módulo, evitando assim que o MC necessite acessar entidades externas.

## 3 Análise do Módulo Cifrador

O MC foi desenvolvido visando atender a todos os requisitos de segurança levantados na seção 2. Nesta seção é apresentada a análise do MC proposto em relação aos requisitos levantados.

Ao cifrar a chave de sessão, utilizada no ciframento de um determinado docu-

mento, com as chaves públicas dos respectivos destinatários deste, o MC assegura que somente estes serão capazes de acessar o documento mantido em sigilo. Desta forma o MC atende ao requisito *Req-1*. Só conseguirá decifrar o documento os que tiverem a posse da chaves privadas.

O MC utiliza três tipos de chaves criptográficas em suas operações. Dentre estas somente a chave pública do MC é extraída do módulo na sua forma original. As chaves de sessão somente saem do MC cifradas com as chaves públicas dos respectivos destinatários destes. Com isto o MC atende ao requisito *Req-2*.

O requisito *Req-3* é atendido através da arquitetura do MC, a qual não permite o armazenamento dos documentos após o término da operação de cifragem. Já o requisito *Req-4* é garantido através da ação conjunta de vários módulos cifradores independentes com um software cliente que realize a divisão do documento em blocos e submissão aleatória aos módulos.

A destruição pelo MC da chave de sessão utilizada no ciframento de determinado documento permite a eliminação de qualquer possibilidade de correlação entre o documento original e o documento cifrado. Esta característica permite o atendimento do requisito *Req-5*.

Esta análise permitiu constatar que o MC atende a todos os requisitos levantados.

## 4 Considerações Finais

Neste trabalho foi proposto um módulo cifrador para realizar o ciframento de documentos eletrônicos de forma confiável. Os requisitos de segurança e funcionalidade que o módulo cifrador deve atender foram levantados a partir da análise de diferentes tipos de aplicações que requerem este tipo de serviço.

O módulo cifrador trata-se de uma plataforma computacional segura, que recebe de um solicitante: um documento a ser cifrado; as políticas de deciframento; e as chaves públicas dos destinatários do documento sigiloso. O módulo cifrador foi concebido para ser flexível e robusto de tal forma que possa ser facilmente incluído em uma infra-estrutura de prestação de serviços que necessite proteger o acesso a documentos eletrônicos.

## Referências Bibliográficas

Ansper, A., Buldas, A., Roos, M., and Willemson, J. (2001). Efficient long-term validation of digital signatures. *Lecture Notes in Computer Science*, 1992:402–415.

Austrália, A. M., Caelli, W., and Little, P. (2003). Electronic signatures - understand the past to develop the future. http://www.law.edu.au/unswlj/ecommerce/mccullagh.html.

Balacheff, B., Chen, L., Plaquin, D., and Proudler, G. (2001). A trusted process to digitally sign a document. In *Proceedings of the 2001 Workshop on New Security Paradigms*, pages 79–86. ACM Press.

Buldas, A. and Lipmaa, H. (1998). Digital signatures, time-stamping and corresponding infrastructure. Technical report, Küberneetika AS.

Dias, J., Demétrio, D. B., Custódio, R. F., and De Rolt, C. R. (2003). Reliable clock synchronization for electronic documents. In *Proceedings of III IEEE Latin American Network Mangment Systems*, pages 550–559.

Gennaro, R., R. M. O. R. T. (1998). Simplified vss and fast-track multiparty computations with applications to threshold cryptography. *Proceedings of the 1998 ACM Symposium on Principles of Distributed Computing.*

ISO (1999). Information technology - security techniques - evaluation criteria for it security - part 1: Introduction and general model.

NIST (2002). Fips pub 140-2 security requirements for cryptographic modules. Disponível em <http://csrc.nist.gov/cryptval/140-2.htm>. Acesso em 18 de Dezembro de 2002.

Press, W. H., Teukolsky, S. A., Vetterling, W. T., and Plannery, B. P. (1994). *Cambridge University Press*. New York, 2 edition.

Schneier, B. (1995). *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition*. John Wiley and Sons, 2 edition.

Shamir, A. (1979). How to share a secret. *Communications of the ACM, Volume 22, pages 612-613*.

Stinson, D. R. (1995). *Cryptography : Theory and Practice*. CRC Press.

Stinson, D. R. (2002). *Cryptography - Theory and Practice*. Chapnan & Hall, 2 edition.