**REVISTA CIENTÍFICA ELETRÔNICA DE SISTEMAS DE INFORMAÇÃO**
**PERIODICIDADE SEMESTRAL – EDIÇÃO NÚMERO 1 – AGOSTO DE 2004**

# PADRÃO DE CRIPTOGRAFIA BASEADA NO PKCS

Fernando Augusto Garcia MUZZI
Docente da Faculdade de Ciências Juridicas e Gerenciais – FAEG/GARÇA
Rodrigo Yoshio TAMAE
Docente da Faculdade de Ciências Juridicas e Gerenciais – FAEG/GARÇA

## RESUMO

O PKCS é uma série de especificações produzidas pelos Laboratórios RSA em cooperação com desenvolvedores de sistemas de segurança de várias partes do mundo que visa acelerar, através de padronização, a utilização e o desenvolvimento de algoritmos de chave pública. A necessidade de padronização para sistemas de criptografia é importante para garantir a troca segura de informações entre sistemas não padronizados.
**Palavra chave:** PKCS; Criptografia.

## ABSTRACT

PKCS is specifications produced by the RSA Labs associated with system's developers of several safety of all world thats look for accelerate, through standardization, use and development of algorithms of public key. The standardization's necessity for cryptograph systems is important for secure information's exchange not patterned.
Key words: PKCS; Criptography.

## 1. INTRODUÇÃO

O PKCS é uma coleção de padrões proposta pela *RSA Data Security*, Inc, utilizando sistemas assimétricos para realizar as seguintes tarefas: assinatura digital, envelopamento digital (onde uma mensagem é "selada" de tal forma que só pode ser lida por um destinatário especificado), certificação digital (onde uma autoridade de certificação assina uma mensagem especial contendo o nome de algum usuário) e sua chave pública, de tal forma que qualquer um possa ter confiança na chave pública desse usuário e concordância de chave, onde duas entidades, sem arranjo prévio, trocam mensagem de tal forma a concordar com uma chave privada conhecida apenas por elas, que pode ser usada no futuro como chave para um sistema simétrico (RSA Labs, 2003A).

O algoritmo de chave pública, isto é, para criptografia assimétrica, mais difundido é o RSA (significa o nome dos autores: Rivest, Shamir e Adleman). A segurança do algoritmo se baseia na intratabilidade da fatoração de produtos de dois números primos (STALLINGS, 1996).

A assinatura digital é o ato capaz de verificar e garantir a origem e a integridade de um documento reproduzido em meio digital, similar a estrutura de autenticação de cartório – muito utilizada no sistema legal brasileiro.

Tendo sido realizado pela empresa possuidora da patente do RSA, não é de se espantar que o sistema de chave pública descrita nesses padrões seja o próprio RSA.

Os objetivos globais do PKCS são manter compatibilidade com Internet PEM (*Privacy-Enhanced Mail Protocol*), estender o Internet PEM para lidar com qualquer tipo de dados e tratar um número maior de atividades e servir como proposta para ser parte dos padrões OSI (RSA Labs, 2003B).

A empresa *RSA Data Security*, formada pelos inventores das técnicas RSA de criptografia de chave pública, tem um papel importante na criptografia moderna.

Nomeadamente, a sua divisão RSA *Laboratories* mantém uma série de padrões (*standards*) denominados de *Public Key Cryptography Standards* (*PKCS*) muito importantes na implementação e utilização de PKIs (*Public-Key Infrastructure*).

Os PKCS visam preencher o vazio que existe nas normas internacionais relativamente a formatos para transferência de dados que permitam a compatibilidade/interoperabilidade entre aplicações que utilizem criptografia de chave pública.

Existem doze standards deste tipo: PKCS#1, #3, #5, #6, #7, #8, #9, #10, #11, #12, #13 e #15 (RSA Labs, 2003A).

Os objetivos da RSA na publicação destes padrões são, segundo eles próprios, os seguintes:

– Manter a compatibilidade com os standards existentes, nomeadamente com PEM (*Privacy-Enhanced Mail Protocol*).

– Ir além dos padrões existentes, para permitir uma melhor e mais completa integração entre aplicações, normalizando a troca segura de qualquer tipo de dados.

– Produzir um padrão que possa ser incluído numa futura versão dos padrões OSI (*Open Systems Interconnection*).

Os PKCS descrevem a sintaxe de mensagens de uma forma abstrata, utilizando o ASN.1, e não restringem a sua codificação.

Como pode ser visto na Tabela 1, a especificação do PKCS responsável pela padronização da criptografia/verificação de assinatura e pela descriptografia e geração de assinatura utilizando o criptossistema RSA. Existem 12 tipos de especificações gerados pelo PKCS.

**Tabela 1** - Temas tratados pelas especificações PKCS.

| **Número** | **Tema** |
|---|---|
| 1 | • PKCS #1 – Como cifrar e assinar usando sistemas criptográficos RSA |
| 3 | • PKCS #3 – Padrão de Normalização de chave Diffie-Hellman |
| 5 | • PKCS#5 – Como cifrar com chaves secretas derivadas de um password |
| 6 | • PKCS#7 – Sintaxe de mensagens cifradas contendo assinaturas digitais |
| 7 | • PKCS #8 – Formato da informação de uma chave privada |
| 8 | • PKCS #9 – Tipos de atributos e sua utilização nas normas PKCS |
| 9 | • PKCS #10 – Requisição de certificados |
| 10 | • PKCS #11 – Define API de criptografia (Criptoki) |

| | |
|---|---|
| 11 | • PKCS #12 – Formato portável para armazenamento ou transporte (exportação/importação de certificados) |
| 13 | • PKCS #13 – Como cifrar e assinar com criptografia de curva elíptica |
| 14 | • PKCS #14 – Padrão para geração de números pseudo-random |
| 15 | • PKCS #15 – (está ainda em desenvolvimento... Tem em vista propor uma norma para armazenamento de credenciais em “token-based devices” (incluindo smart cards) |

## 2. PKCS: COMO FUNCIONA

O sistema consiste em gerar uma chave pública (geralmente utilizada para cifrar os dados) e uma chave privada (utilizada para decifrar os dados) através de números primos grandes, o que dificulta a obtenção de uma chave a partir da outra.

Quanto maior os números primos utilizados para a criação da chave, maior é a segurança proporcionada por esse algoritmo. Hoje em dia os números primos que são utilizados têm geralmente 512 bits de comprimento e combinados formam chave de 1024 bits. Em algumas aplicações como, por exemplo, bancárias que exigem o máximo de segurança a chave chega a ser de 2048 bits.

Com o passar do tempo, a tendência é que o comprimento da chave aumente cada vez mais. Esse fenômeno acontece, em grande parte, pelo avanço nos sistemas computacionais que acompanham o surgimento de computadores que são capazes de fatorar chaves cada vez maiores em um tempo muito baixo.

Os algoritmos para a geração da chave pública e privada usadas para cifrar e decifrar as mensagens são simples. Observe-os a seguir:

- Escolhe-se dois números primos grandes (p e q);
- Gera-se um número n através da multiplicação dos números escolhidos anteriormente (n = p . q);
- Escolhe-se um número d, tal d é menor que n e d é relativamente primo à (p-1).(q-1);
- Escolhe-se um número e tal que (ed-1) seja divisível por (p-1).(q-1). Para realizar esse cálculo é necessário o algoritmo de Euclides estendido.
- Os valores e e d são de expoentes públicos e privados, respectivamente. O par (n,e) é a chave pública e o par (n,d) é a chave privada. Os valores p e q devem ser mantidos em segredo ou destruídos.
- Para cifrar uma mensagem com esse algoritmo é realizado o seguinte cálculo : $C = T^e \bmod n$, onde C é a mensagem cifrada, T é o texto original, e o n são dados a partir da chave pública (n,e).
- A única chave que pode decifrar a mensagem C é a chave privada (n,d) através do calculo de: $T = C^d \bmod n$.

## 3. CONCLUSÕES

O PKCS é um padrão de segurança baseado no modelo RSA e no conceito de chave pública, sendo considerado o principal padrão para implementação de módulos de segurança baseados criptografia assimétrica.

Através dele são descritos os modelos de implementação para criptografia em hardware em sistemas reconfiguráveis baseados em SoC (System on-Chip) ou não, em transações bancárias seguras através de Smart-Cards, transporte ou armazenamento de dados em geral pela Internet, cifragem e assinatura de curva elíptica, requisição de certificados de segurança e para definir formatos de chaves privadas.

Com o advento da Internet e World Wide Web, dispositivos reconfiguráveis de hardware, a crescente utilização em larga escala das redes de computadores e a necessidade de interoperabilidade entre os diversos sistemas de informação existentes, fazem com que o uso de padrões certificados e amplamente aceitos pelo mercado sejam cada vez mais utilizados e garantindo o surgimento de mecanismos tecnológicos cada vez mais seguros.

## REFERÊNCIAS BIBLIOGRÁFICAS


RSA Labs. **Public Key Criptography Standards (PKCS).** Version 2.1 - 2002, Disponível em: <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html>. Acesso em: 02 Dez. 2003A.

RSA Labs. **Factorization of RSA-155.** Disponível em: <http://www.rsasecurity.com/rsalabs/challenges/factoring/rsa155.html>. Acesso em: 02 Dez. 2003B.

STALLINGS, William. **Cryptography and Network Security – Principles and Practice** – Second Edition, 1996.