Entendendo o Ciclo de Vida das Chaves Criptográficas

Mario Luiz Bernardinelli *(mariolb@gmail.com)

11 de janeiro de 2009

Resumo

As chaves criptográficas possuem um papel importantíssimo na segurança dos dados, pois elas são os insumos para que os algoritmos criptográficos possam garantir um ou mais requisitos básicos da segurança da informação: a autenticidade, a confidencialidade, a integridade e o não-repúdio de acordo com as necessidades das aplicações e transações eletrônicas.

Desde a sua criação até a sua destruição, as chaves criptográficas passam por várias fases, cada uma delas contendo características próprias. As fases descrevem de uma forma geral e de alto nível a situação da chave. Em cada fase, as chaves criptográficas passam por ou mais estágios. A transição de estágios é comandada por eventos característicos que definem para qual será o novo estágio da chave como, por exemplo, o comprometimento da chave, a expiração do criptoperíodo etc.

Neste artigo são apresentadas as fases do ciclo de vida das chaves criptográficas, suas características, os estágios que compõem cada uma das fases e os eventos que promovem a transição entre os mesmos.

Dada a importância das chaves criptográficas na segurança da informação, o conhecimento do seu ciclo de vida é essencial para que se possa elaborar e gerenciar o conjunto de chaves criptográficas utilizadas pela organização em seus sistemas computacionais. Falhas de gerenciamento aparentemente simples, como simples fato de se deixar o criptoperíodo de uma chave expirar pode trazer vários transtornos e prejuízos para a organização.

Palavras-chave: criptografia, gerenciamento de chaves criptográficas, ciclo de vida das chaves criptográficas.

[1]Mario Luiz Bernardinelli é Tecnólogo em Processamento de Dados pela Faculdade de Tecnologia de Americana, possui os títulos de Especialista em Engenharia de Sotware e Especialista em Redes de Computadores, ambos pela Unicamp, e as certificações Linux LPI-C1 e LPI-C2. Atualmente, trabalha como desenvolvedor de software em ambiente Linux e administrador de redes para uma empresa do ramo de sistemas de automação.

1 Introdução

A criptografia é uma ferramenta importantíssima para a segurança dos sistemas de informação, porém, nem o mais poderoso algoritmo criptográfico pode prover alguma segurança se as chaves criptográficas forem comprometidas. O comprometimento das chaves criptográficas pode ocorrer de várias formas: as chaves podem ser capturadas, modificadas, corrompidas ou até mesmo disponibilizadas para pessoas (ou entidades) não autorizadas. Dada a importância das chaves criptográficas, deve haver um mecanismo ou técnica que permita protegê-las de forma adequada.

Além dos riscos já mencionados, as chaves podem ser simplesmente perdidas. Se uma informação for cifrada e a chave de decifrамento for perdida, pode ser impossível recuperar a mensagem se não houver uma cópia da chave de decifrамento armazenada em algum lugar (*backup*). Por outro lado, se as cópias de segurança das chaves não forem protegidas, corre-se o risco das mesmas serem comprometidas pelo acesso indevido.

Surge então o gerenciamento de chaves criptográficas como um conjunto de técnicas e procedimentos que visa permitir o estabelecimento e a manutenção dos relacionamentos de chaves entre entidades autorizadas ou, de uma maneira mais simples: garantir a segurança das chaves. O gerenciamento de chaves é um processo complexo e não envolve apenas controles tecnológicos, mas uma combinação de:

- Controles tecnológicos, tais como *hardware* e soluções de segurança.
- Controles físicos, tais como alarmes e salas seguras.
- Procedimentos que, normalmente, necessitam da interação humana.

O tipo de gerenciamento a ser empregado depende do tipo da chave utilizada. Por exemplo, uma chave de sessão, que é tipicamente de curta duração, pois é trocada a cada sessão de comunicação, não exige nenhum gerenciamento durante a sua curta vida. Por outro lado, uma chave mestre deve ter um nível de proteção e gerenciamento diferenciado e mais cuidadoso, já que esta chave pode ser utilizada para cifrar várias outras chaves e é utilizada por muito mais tempo.

Discutiremos aqui o ciclo de vida das chaves criptográficas com o objetivo de oferecer uma visão geral de cada uma das fases pelas quais uma chave criptográfica passa, desde a sua criação até a sua destruição, de forma que seja possível o entendimento de todo o processo e os cuidados necessários em cada fase.

2 As fases do ciclo de vida da chave

Quando falamos em gerenciamento de chaves, a primeira coisa que imaginamos é que devemos cuidar da integridade e autenticidade daquele conjunto de caracteres a princípio sem nenhum nexo, que constitui a chave criptográfica propriamente dita. No entanto, o gerenciamento de chaves preocupa-se com algo mais: apesar do nome referir-se diretamente apenas ao termo chave, o gerenciamento envolve também os atributos que acompanham uma chave criptográfica, como, por exemplo, os valores de inicialização da chave e a pessoa ou sistema relacionado com a referida chave. Assim, durante o gerenciamento de chaves muitas vezes utilizamos o termo **material criptográfico** para nos referirmos tanto à chave criptográfica quanto aos demais atributos relacionados.

Podemos dividir o ciclo de vida de uma chave em quatro fases gerais, conforme descrito em (BARKER *et al.*, 2007, p.90):

Fase pré-operacional: Nesta fase o material criptográfico ainda não está disponível para uso, mas estão em processo de criação ou ativação.

Fase operacional: Nesta fase o material criptográfico está disponível para uso normal.

Fase pós-operacional: O material criptográfico não está mais disponível para uso normal, mas o acesso ao mesmo ainda é possível em determinadas circunstâncias.

Fase de destruição: Nesta fase, as chaves são destruídas, assim como todos os registros de sua existência devem ser destruídos também. Apesar das chaves propriamente ditas serem destruídas nesta fase, os seus atributos (nome, tipo, criptoperíodo e período de uso) podem ser mantidos (arquivados).

A figura 1 apresenta as fases do ciclo de vida das chaves e as transições entre as mesmas.

Se observarmos atentamente o diagrama vamos perceber que uma, uma vez ocorrida a transição de fase, a chave nunca volta à fase anterior. As transições de fase apresentadas no diagrama são as seguintes:

1. Quando a chave é criada, ele passa automaticamente a fazer parte da fase de pré-operacional.
2. Quando uma chave é criada, mas decide-se que ela não será utilizada, ela passa da fase pré-operacional diretamente para a fase de destruição.
3. Quando uma chave que esteja na fase pré-operacional é comprometida, ela passa para a fase pós-operacional, para que as ações pertinentes às chaves comprometidas possam ser executadas, como, por exemplo, a revogação do certificado digital relacionado.

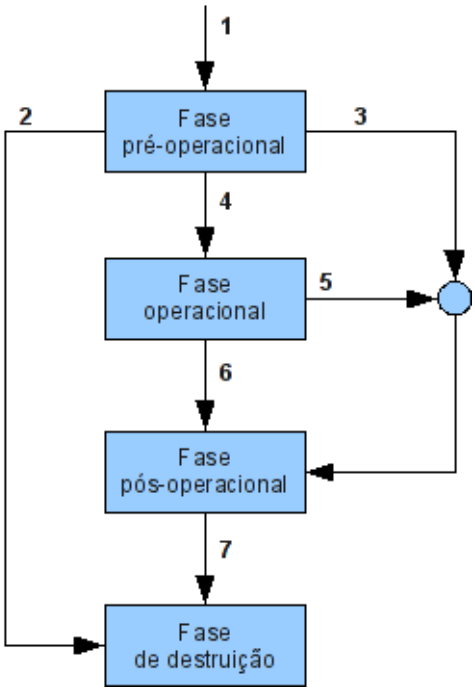

Figura 1: Fases do gerenciamento de chaves

4. Após criação da chave e dos atributos necessários e do estabelecimento das associações necessárias, a chave está pronta para ser utilizada e ela pode passar para a fase operacional.

5. Quando uma chave que está na fase operacional é comprometida, ela passa para a fase pós-operacional, onde existem ações adequadas para o tratamento de chaves comprometidas.

6. Quando as chaves não mais devem ser utilizadas em operações normais, mas podem ser necessárias sob circunstâncias especiais, elas passam da fase pós-operacional.

7. As chaves passam para a fase de destruição quando elas realmente não são mais necessárias e não devem ser utilizadas sob nenhuma circunstância. Uma vez na fase de destruição, todos os registros referentes à chave serão destruídos.

2.1 Os estágios da chave

As fases apresentadas nos dá uma visão geral de alto nível do ciclo de vida das chaves criptográficas, não oferecendo uma visão detalhada do que ocorre realmente com a chave.

Em cada fase do ciclo de vida, as chaves passam por estágios específicos. A figura 2, descrita por (MENEZES; OORSCHOT; VANSTONE, 1996, p.579), apresenta de forma

detalhada cada um dos estágios pelos quais uma chave passa durante a sua vida útil, além das fases já descritas.

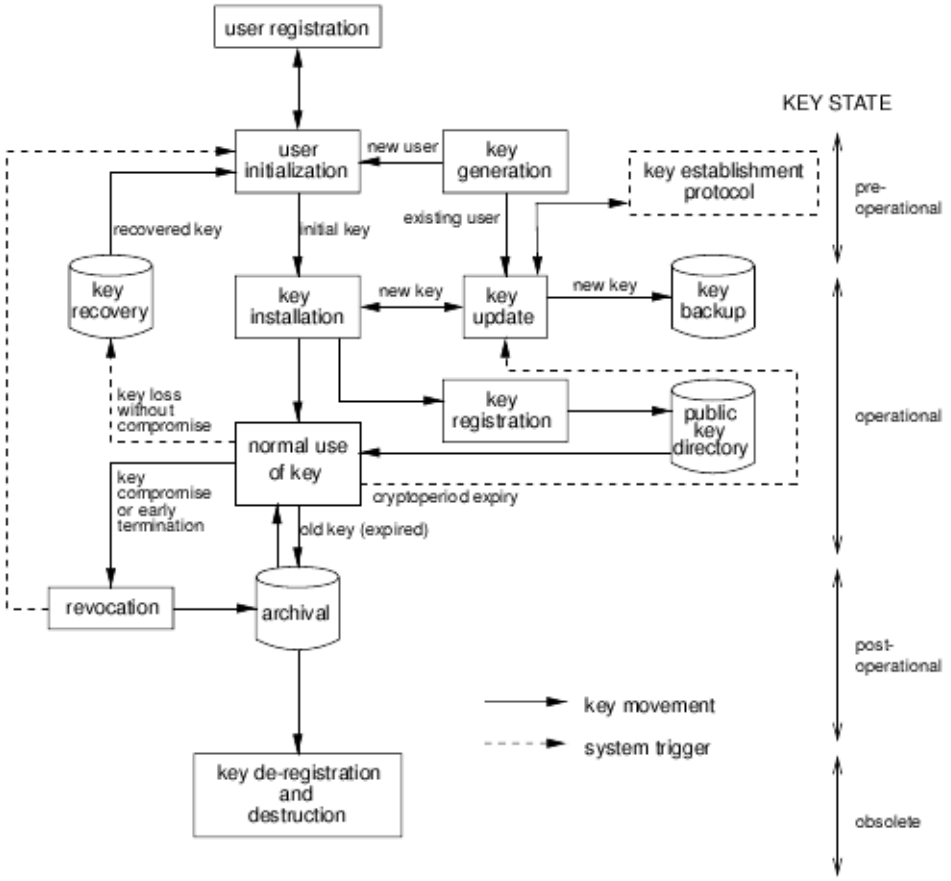

Figura 2: Gerenciamento do ciclo de vida da chave

No diagrama da figura 2, os retângulos representam os estágios pelos quais a chave passa durante a sua vida útil, as linhas contínuas representam as transições de estágio da chave e as linhas tracejadas representam eventos que disparam ações que provocam a mudança de estágio.

Registro do usuário (*user registration*). Durante esta fase uma entidade, que pode ser um indivíduo, organização, dispositivo ou processo; interage com uma autoridade de registro com a finalidade de tornar-se um membro autorizado do domínio de segurança. Nesta fase, é criado um identificador para a entidade que será utilizado para identificar o novo membro do domínio nas transações futuras. Vários atributos podem ser estabelecidos nesta fase como, por exemplo, o endereço de *email* ou alguma outra informação relacionada ao usuário (ou corporação, no caso de empresas). Todos estes atributos fazem parte da entidade e são relacionados ao ao identificador criado, permitindo que as aplicações utilizem-se da infra-estrutura de

segurança para suportar serviços mais seguros, baseados na possibilidade de verificação da autenticidade destes atributos. É importante salientar que a interação com a entidade de registro deve ser efetuada de forma segura como, por exemplo, troca pessoal do material necessário, carta registrada etc.

Inicialização (*user initialization*). Uma entidade inicializa sua aplicação criptográfica (instala e inicializa o *software* ou o *hardware*), operação esta que envolve o uso ou a instalação do material criptográfico obtido durante o processo de registro do usuário.

Geração da chave (*key generation*). A geração das chaves deve garantir as propriedades adequadas para a aplicação e uma aleatoriedade que torne baixíssima a probabilidade da chave ser previsível. A entidade dona da chave deve gerar suas próprias chaves ou usar as chaves obtidas através de um componente confiável do sistema.

Instalação da chave (*key installation*). Todo o material criptográfico necessário (chaves e demais atributos) são instalados no *software* ou *hardware* da entidade. Esta instalação pode ocorrer de várias maneiras, tais como: entrada de senha ou PIN (*Personal Identification Number*), transferência de disco, dispositivos não graváveis (somente leitura), *chipcard* etc.

Registro da chave (*key registration*). Além da instalação da chave, o restante do material criptográfico deve ser oficialmente associado ao identificador único que distingue a entidade das demais. Para o caso de chaves públicas, os certificados podem ser criados por uma autoridade certificadora, a qual servirá como garantia da associação, e tornada pública através de algum diretório público na rede ou qualquer outro meio disponível.

Uso normal (*normal use*). Nesta fase, o material criptográfico é disponibilizado para uso conforme necessário, ficando disponível durante todo o criptoperíodo da chave ou até que ocorra algum evento específico, como comprometimento, perda ou simplesmente a finalização de seu uso. O material criptográfico deve ser protegido, devendo ser armazenado num dispositivo adequado (módulo ou mídia) que esteja disponível para leitura quando necessário.

Cópia de segurança (*key backup*). Consiste na cópia de segurança de todo o material criptográfico em um meio de armazenamento seguro, de forma a oferecer uma fonte de recuperação em caso de desastre. Observe que esta cópia de segurança é de curto prazo, pois deve durar apenas enquanto a chave estiver em uso operacional.

Atualização da chave (*key update*). A substituição das chaves é realizada numa das seguintes situações:

- Comprometimento da chave.
- O criptoperíodo da chave encontra-se próximo da expiração.
- Há muito material protegido pela chave e deseja-se limitar este volume criando uma nova chave para proteger os materiais a serem produzidos a partir de então.

Arquivo (*archival*). Todo o material criptográfico que não estiver mais em uso pode precisar ser arquivado a fim de prover a uma fonte de recuperação necessária em determinadas circunstâncias. Apesar de ter basicamente a mesma função da cópia de segurança (*backup*), o arquivamento refere-se ao armazenamento de longo prazo efetuado após o término de uso operacional do material criptográfico. Da mesma forma que a cópia de segurança, o arquivamento deve oferecer integridade e controle de acesso.

Destruição da chave (*key de-registration and destruction*). Passadas as fases operacional e pós-operacional, a chave deve ser definitivamente cancelada e destruída. Isto significa que todas as cópias da chave devem ser removidas de forma segura de todos os dispositivos de armazenamento. Uma remoção segura neste caso refere-se à remoção de todo e qualquer traço da existência da chave. Por exemplo, quando o registro de uma chave é removido do disco, é desejável que a área do disco onde a chave estava armazenada seja sobrescrita com outras informações, de forma a eliminar qualquer possibilidade de recuperação da chave caso o dispositivo de armazenamento venha a ser comprometido.

Recuperação da chave (*key recovery*). Uma vez que a cópia de segurança ou o arquivamento tenham sido executados, deve haver um mecanismo que permita a recuperação do material criptográfico armazenado na cópia de segurança. Observe que uma operação de restauração da chave que reinstale uma chave que esteja em uso operacional só deve ser realizada se a chave foi perdida sem que a sua autenticidade tenha sido comprometida. Exemplos de perda da chave sem o seu comprometimento são a quebra do *hardware* de armazenamento ou o simples esquecimento da mesma.

Revogação da chave (*key revocation*). Por razões diversas, pode ser necessário remover uma chave do uso operacional antes do previsto. É o caso, por exemplo, do comprometimento da chave: neste caso, a revogação da mesma deve ser efetuada imediatamente, sob pena de comprometer a segurança dos dados e sistemas dependentes da chave. No caso das chaves que fazem parte de certificados digitais, o certificado deve ser revogado.

O ciclo de vida da chave apresentado refere-se principalmente à chaves assimétricas. O ciclo de vida de chaves simétricas costuma ser mais simples, mas não menos importante. Por exemplo, as chaves de sessão normalmente não possuem cópias de segurança, nem são registradas, arquivadas ou revogadas devido à sua natureza: elas são chaves efêmeras, ou seja, de curta duração.

3 Conclusão

As chaves criptográficas são a base os sistemas criptográficos pois, segundo o Princípio de Kerckhoffs (KERCKHOFFS, 1883), "A segurança de um sistema deve residir no desconhecimento da chave.". Sendo esta premissa verdadeira, então as chaves criptográficas constituem um artigo que deve ser muito bem protegido. Uma chave comprometida pode comprometer toda a segurança de um sistema.

Imagine o que pode acontecer se uma chave privada utilizada para assinar documentos digitais de uma grande organização for comprometida: todos os documentos assinados por esta empresa estarão comprometidos, pois quem dispor da chave privada de tal organização pode alterar qualquer documento emitido por ela e assiná-lo novamente, tornando-o autêntico perante a chave pública da organização. Como se todo este problema não bastasse, imagine como ficaria a imagem da organização perante seus usuários e clientes. E se tal organização fosse uma instituição financeira, como um banco?

Sendo peças cruciais para a segurança dos sistemas, as chaves criptográficas precisam de cuidados especiais. Desde a sua criação até a sua destruição, as chaves precisam ser acompanhadas e gerenciadas de maneira a permitir que sejam organizados os procedimentos e as ações necessárias a cada etapa da vida útil das mesmas. É preciso que hajam controles e meios de verificar o estágio atual das chaves, tornando possível o planejamento dos passos a serem dados no futuro.

Portanto, o conhecimento de cada uma das fases da vida útil das chaves criptográficas é essencial para que se possa efetuar o gerenciamento eficiente das chaves criptográficas, permitindo que as etapas normais da vida da chave sejam alcançadas de maneira tranquila, sem percalços, e também que os eventuais problemas inerentes aos sistemas computacionais, tais como quebra de dispositivos de *hardware* ou mesmo ações de *crakers* possam ser contornadas através do uso de técnicas e procedimentos bem definidos e documentados.

Referências

BARKER, E. *et al. Recomendation for Key Management - Part 1: General*. USA: NIST National Institute os Standards and Technology, 2007. 89-113 p.

MENEZES, A.; OORSCHOT, P. v.; VANSTONE, S. *Handbook of Applied Cryptography*. Boca Raton, Florida, USA: CRC Press, 1996. 577-581 p.

KERCKHOFFS, A. *La Cryptographie Militaire*. France: Journal des Sciences Militaires, vol. IX, 1883. 161-191 p.