Assinando a aplicação

[[Category:]]

Por que é necessário assinar as aplicações ?

O termo "assinar as aplicações" significa que as aplicações são assinadas com uma chave privada. Para cada chave privada, existe uma chave pública e um **certificado**, por exemplo, um certificado de desenvolvedor (*developer certificate*), um certificado emitido por alguma autoridade certificadora, ou um certificado criado localmente (também chamado de certificado "auto-assinado" ou *self-signed*).

Quando se instala um aplicação assinada em um dispositivo, o instalador usa um **root certificate** ("certificado raiz") que foi fornecido com o dispositivo para checar a assinatura e também o certificado da chave pública. Se for possível rastrear o certificado fornecido (ou quem quer que tenha assinado a aplicação), de maneira a se chegar em certificado raiz válido, a aplicação é considerada **confiável** no domínio onde o certificado raiz é considerado confiável. Se a aplicação for assinada com uma chave que possui somente um certificado do tipo *self-signed*, então não existirá um certificado raiz correspondente. Dessa forma, a aplicação é considerada **não-confiável**.

Aplicações seguras recebem menos mensagens de aviso e podem ter acesso a capacidades mais poderosas. No caso do Java ME, os MIDlets assinados irão gerar menos pedidos de confirmação do usuário quando precisarem usar APIs Java restritas.

Termos e definições

É importante não confundir "assinar" com "certificação", ou "certificação" com "certificados", ou "emissão de certificado" com "certificação de aplicação". Esses termos são muitas vezes usados como sinônimos, mas eles possuem significados diversos.

- **Assinar** é o termo técnico para o ato de se criar uma assinatura digital para um pacote de *software* usando uma chave privada (arquivo SISX em S60, *signed JAR* em Java). O par de chaves (pública e privada) pode ter um certificado emitido por uma autoridade certificadora ou emitido localmente ("self-signed"). A diferença entre essas opções refere-se ao nível de confiança que a assinatura confere, mas na assinatura em si não há diferenças.
- **Certificado** é uma prova de que alguém realmente possui determinadas chaves pública e privadas. Um certificado é emitido por alguma autoridade certificadora ("emissor", como Nokia ou Verisign), indicando que o par de chaves pública e privada pertence à entidade especificada no certificado. Se o certificado por criado localmente ("self-signed"), o certificado não possui nenhum tipo de confiabilidade, tendo sido criado apenas por mera necessidade técnica.
- **Certificação** significa que uma aplicação passou por algum teste cujas regras foram pré-estabelecidas e aceitas, tendo sido certificada por tal feito. A aplicação é assinada com uma determinada chave e certificado, que são compatíveis com o certificado raiz presente nos dispositivos. Dessa forma, quando o usuário instala uma aplicação (que possui o certificado raiz correto), fica estabelecido que essa aplicação é confiável para o dispositivo. O instalador de aplicações checa a assinatura de modo a conferir se a aplicação possui uma fonte confiável. Se a aplicação não for certificada (ou seja, não existe um certificado raiz correspondente no dispositivo), o usuário receberá um aviso no momento da instalação, dizendo que a aplicação não tem origem confiável.
- **Emissão de certificado** é o ato de uma autoridade certificadora emitir um certificado ligado a um determinado par de chaves pública e privada. Isso não é a mesma coisa que "certificar aplicações", e a autoridade certificadora também não corresponde à entidade que realiza certificação de aplicações.
- Uma aplicação **confiável** é alguma coisa que foi assinada com uma chave cujo certificado corresponde a algum certificado raiz confiável. Aplicações assinadas com certificados do tipo "self-signed", ou não-assinadas, são **não-confiáveis**.

Considerações para S60

Um aspecto importante a ser entendido em relação a S60 3ª Edição é que a **assinatura de aplicações é obrigatória, mas a certificação não é**. A aplicação precisa ser assinada, em termos técnicos, mas o certificado usado nesse procedimento não necessariamente precisa ter sido emitido por uma autoridade certificadora. Entretanto, o uso de capacidades pode requerer que a aplicação também seja certificada (assinada por uma chave que possui um certificado confiável).

Processo de assinatura em programas de teste

Quando uma aplicação é testada através de um programa de grande âmbito e reconhecido pela indústria (como "Symbian Signed" ou "Java Verified"), a entidade que realiza os testes de certificação (que, para reforçar, não é a mesma que emite o certificado) é responsável por realizá-la (ou seja, assinar a aplicação com uma chave que possui um certificado confiável) depois que aplicação for aprovada.

(C) Copyright Nokia 2013. All rights reserved.

(C) Copyright Nokia 2013. All rights reserved.