# Java domínios de segurança

**Este artigo não atende os padrões de qualidade da wiki:** Este artigo não atende aos padrões de qualidade do wiki: Por favor, ajude a melhorá-lo acrescentando links ou informações relevantes para solucionar o problema da qualidade. Após isso ser resolvido, por favor retire do artigo o modelo {{NeedsMoreWork}}, para que este aviso seja removido.

**Motivos:** - lpvalente
(14 Oct 2011) A tradução parece que foi feita com uma ferramenta de tradução automática. O artigo precisa ser reescrito.

## Introdução

O acesso a chamada de certos métodos e APIs de MIDlets tem algumas restrições. É possível que o usuário seja solicitado para permitir á chamada a certos métodos ou poder bloquear o acesso totalmente, que resultará no lançamento de uma SecurityException.

Fazendo estas solicitações, sem aparentar, frequentemente requisita do desenvolvedor assinar o MIDlet (e o usuário para manualmente trocar as configurações de acesso a API). Somente a assinatura do domínio operador ou produtor removerá completamente as solicitações (prompts), embora esses requeiram estrita colaboração com estas partes.

## Domínio de segurança

O MIDP 2.0 define quarto especificações de domínios de segurança em que o MIDlet pode ser instalado:

- Domínio de proteção para aplicações de terceiros (aplicações não confiáveis)
- Domínio de proteção para aplicaçoes de terceiros identificados (aplicações confiáveis)
- Domínio de proteção da operadora
- Domínio de proteção do produtor

## Grupos de proteção de API

Cada um dos domínios de proteção tem certo nível de proteção à acesso (APIs sensíveis). Os acessos corretos estão agrupados para um grupo de funções:

- Net Access (MIDP spec também define baixo-nível para o Net Access, mas este tem sido combinado em muitos aparelhos para o Net access function group)
- Messaging (MIDP spec também define messaging como restrita)
- Aplicação auto-inicializável
- Conectividade local
- Gravação multimídia
- Ler dados do usuário (incluindo arquivos e PIM)
- Escrever/editar dados do usuário (incluindo arquivos e PIM)
- Localização
- Armazenamento Landmark
- Comunicação com Smart card
- Autenticação
- (Controle de chamada)
- (Chamada telefônica)

O MIDlet terá configurações de acesso definidas para cada um dos grupos de funções acima mencionados, que são suportados pelo telefone. A configuração pode ser uma das definidas a seguir pela política de domínio de segurança do aparelho:

- Sempre permitido / Acesso direto
- Pergunta a primeira vez / pergunta uma vez por sessão
- Pergunta todas as vezes
- Não permitido

## Definições de acesso à API nos padrões do Java ME

As especificações do Java incluem um número de versões para o acesso a API disponíveis (note que ali pode não ser um simples dispositivo disponível que suportaria o acesso a API, uma vez que as diretrizes deles são definidas na especificação).

- MIDP 2.0 API access rights
- MIDP 2.0.1 API access rights
- MIDP 2.1 API access rights (o mesmo que na MSA)
- JTWI API access rights (somente define acesso à API para domínio de terceiros confiáveis)

NOTA: A especificação define que mesmo aplicações confiáveis de terceiros podem não ter permissões de rede e auto-inicializar, simultaneamente, com sempre permitido.

Um MIDlet que não tem sido assinado será localizado no domínio não confiável. Que possui mais restrições para acessar certas APIs. Se o MIDlet tem sido assinado e o certificado correspondente esta armazenado no certificado do aparelho, o MIDlet será reconhecido no domínio de proteção para que o certificado seja integrado. (Existem algumas verificações complexas que são feitas no momento da instalação, veja a especificação do MIDP 2 para mais


(C) Copyright Nokia 2013. All rights reserved.

informações).

## Certificados para assinar domínio confiáveis de terceiros

Se sua aplicação passar no teste Java Verified, ela será assinada com o certificado UTI root, que reconhecerá seu MIDlet com o domínio de aplicação confiáveis de terceiros. Outros certificado comuns que reconhece o seu MIDlet com o domínio de aplicação confiável de terceiro estão disponíveis em:

- Thawte
- Verisign – instalação test MIDlet para este certificado.

Note que existe diferença entre diferentes modelos de aparelhos em que os certificados são instalados. Adicionalmente alguns modelos de aparelhos podem ter diferentes tipos de certificados dependendo em que região ele foi vendido. E finalmente, as operadoras também podem disponibilizar certificados adicionais.

Também note que, a especificação do MIDP não permite novos certificados adicionados no dispositivo móvel para permitir assinatura de domínio de aplicações confiáveis de terceiros. Isto é, entretanto é possível nos dispositivos da segunda edição da S60 devido ao incorrect implementação (instructions). Veja ainda , que algumas operadoras tem implementado ainda chamadas de certificados de desenvolvedor para seus dispositivos (Sprint e China Unicom). Consequentemente, para ter certeza check the available code-signing CA-certificates (ou verifique this posting).

## Política de domínio de segurança para um número de transportadores, desviando do padrão

Como a política de domínio de segurança do MIDP spec é apenas uma recomendação, algumas operadoras têm definido seus próprios domínios de segurança para acesso a API. Estas incluem:

- AT&T Java security domains (Cingular) (entry on FN blogs)
- China Unicom Java security domains
- Hutchinson 3G security domains(entry on FN blogs) - note que a Orange Israel segue o guia da Hutchinson 3G também
- Sprint Java security domains (entry on FN blogs)
- T-Mobile U.S. Java security domains (entry on FN blogs)

## Informação de domínio de segurança de outros fabricantes exceto Nokia

- Motorola Java ME Developer Guide (requer se registrar gratuitamente)
- Sony Ericsson Developers' Guidelines Java ME CLDC (MIDP 2) and [developer.sonyericsson.com/getDocument.do?docId=99421 Java ME Permission settings in Sony Ericsson phones]

## Configurações de acesso a API em dispositivos reais

Mesmo aparelhos genéricos têm diferentes versões de acesso a API implementadas.

- API access rights on phones, S60 2nd FP2, no genérico 6630 (2.39.126)
- API access rights on phones, S60 2nd FP2 ver2, nos genéricos 6680, 6630 (6.03.40)
- API access rights on phones, S60 2nd FP3, no genérico N72
- API access rights on phones, S60 3rd, no genérico E61i
- API access rights on phones, S60 3rd FP1, no genérico N95
- API access rights on phones, S60 3rd FP2, no genérico 6210 Navigator
- API access rights on phones, S60 5th, ainda apenas um lugar proprietário
- API access rights on phones, Series 40 3rd FP1, no genérico 6131
- API access rights on phones, Series 40 3rd FP2, nos genéricos Nokia 5300, 6300, 7373
- API access rights on phones, Series 40 5th FP1, no genérico Nokia 6500 slide

Algumas trocas de configurações padrões podem no aparelho, mas depois da instalação do MIDlet é possivel trocar as configurações padrões de acesso a API de alguns(nem todas opções estão disponíveis para MIDlets não confiáveis).

- S60 instructions
- Series 40 instructions

## Referências

- MIDP 2.0: Signed MIDlet Developer's Guide


(C) Copyright Nokia 2013. All rights reserved.

(C) Copyright Nokia 2013. All rights reserved.