Geracao de Chaves e Certificados Digitais

Requisitos

As chaves privadas e os certificados digitais utilizados no OpenBus seguem formatos bem definidos:

- a chave privada deve ser do tipo **RSA** e deve estar codificada no formato **PKCS8**, não criptografado.
- o certificado digital utilizado deve ser do tipo **X.509** e deve estar codificado no formato **DER**.

Estas chaves e certificados podem ser geradas por quaisquer ferramentas, desde que estes requisitos sejam atendidos. Abaixo, seguem as instruções para geração utilizando o OpenSSL. O OpenSSL já está disponível por default em máquinas Linux; se for necessário usar uma versão para Windows ou outras plataformas, consultar o site oficial.

Chave Privada

A geração de uma chave privada é feita com o seguinte comando:

```
openssl genrsa -out chave_privada.key 2048
```

- `genrsa` — solicita a geração de uma chave privada RSA
- `-out <arq>` — define <arq> como o nome do arquivo onde será gerada a chave privada (no exemplo acima, `chave_privada.key`)
- `2048` — o tamanho da chave

Para converter a chave privada para o formato PKCS8, fazer:

```
openssl pkcs8 -topk8 -in chave_privada.key -nocrypt > chave_pkcs8.key
```

- `-in <arq>` — define <arq> como o arquivo de entrada (no exemplo acima, `chave_privada.key`)
- `chave_pkcs8.key` — arquivo onde será gerada a chave PKCS8

Certificado Digital

A geração dos certificados digitais depende de uma chave privada no formato PKCS8:

```
openssl req -new -x509 -key chave_pkcs8.key -out certificado.crt -outform DER
```

- `-key` — arquivo com a chave PKCS8 (gerado pelo comando anterior)
- `-out <arq>` — define <arq> como o arquivo onde será gerado o certificado (no exemplo acima, `certificado.crt`)

O comando acima tipicamente é suficiente para geração do certificado. Porém, pode ser necessário fornecer um arquivo de configuração diferente do default para o OpenSSL; se for este o caso, este deve ser fornecido (com path) via parâmetro `-config` :

```
openssl req -new -x509 -key chave_pkcs8.key -out certificado.crt -outform DER -config
<path>/openssl.cnf
```

Script de geração de chaves.

Caso prefira, este script gera o par de chaves sem a necessidade de executar os comandos separadamente.
Para gerar a chave basta executar o script passando como parâmetro o nome da chave. Exemplo:

```
$ ./openssl-generate.ksh -n <nome>
```

Para visualizar todos os parâmetros suportados, use o parâmetro `-h`:

```
$ ./openssl-generate.ksh -h

Uso: openssl-generate.ksh [opcoes]

  onde [opcoes] sao:

  -h      : ajuda
  -c arq  : arquivo de configuracao do OpenSSL
  -n nome : nome do arquivo com o certificado

OBS.: se o nome nao for fornecido via '-n' sera obtido interativamente
```
