
Java Cert Path

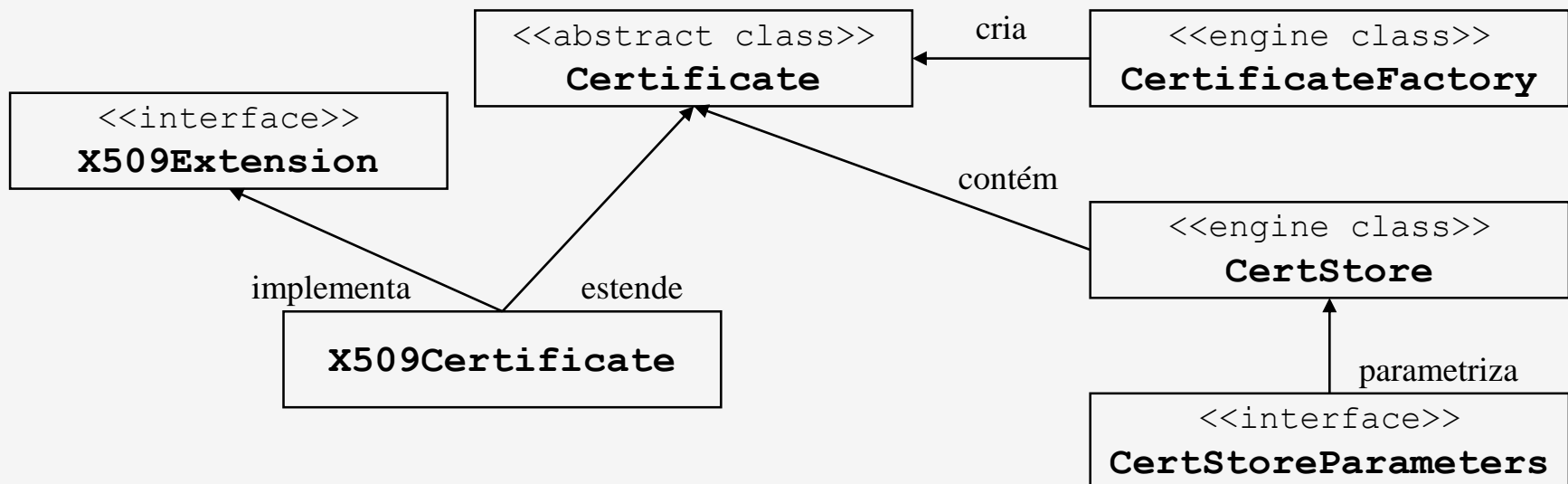
Pedro Félix (pedrofelix@cc.isel.ipl.pt)
[Instituto Superior de Engenharia de Lisboa](#)

Sumário

- Java Certification Path API
 - Criação e verificação de cadeias de certificados
 - Arquitectura baseada em *providers*
 - Implementações para certificados X.509 e perfil PKIX

Classes *Certificate* e *CertificateFactory*

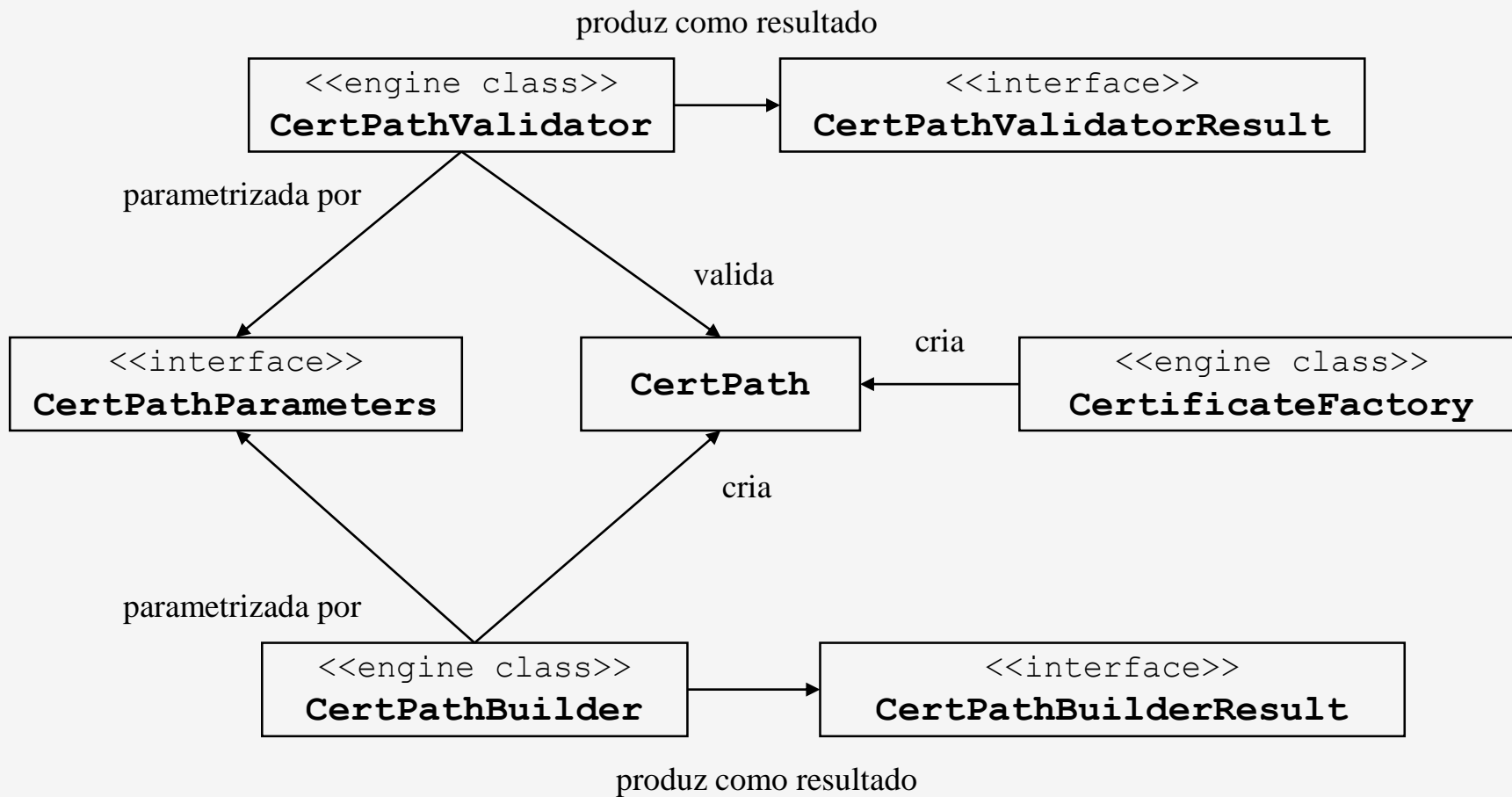
- **Certificate** – classe para a representação abstracta de certificados
- **X509Certificate** – estende a classe **Certificate** para o caso concreto de certificados X.509
- **CertificateFactory** – *engine class* para a criação de certificados ou cadeias de certificados com base na sua representação codificada, tipicamente em *stream*.
- **X509Extension** – Interface com métodos de acesso a todas as extensões presentes num certificado X.509



Cadeia de certificação

- Uma cadeia (caminho) de certificação é uma sequência de n certificados onde
 - $\forall i \in \{0, n-2\}$: **C[i].subject = C[i+1].issuer**
 - **C[0]** é um certificado emitido pelo *trust anchor*
 - **C[n-1]** é o certificado a validar
- Na plataforma Java, uma cadeia de certificados é representada pela classe abstracta **CertPath**
 - é imutável
 - contém uma lista de certificados
 - No caso de certificados X.509, o primeiro é o de *end-entity* e o último é o emitido pelo *trust anchor* (não inclui o *trust anchor*)
- Construção:
 - **CertificateFactory** – a cadeia existe em forma codificada
 - **CertPathBuilder** – constrói uma cadeia com base num conjunto de *trust anchors*, um conjunto de certificados e um critério de selecção para o certificado final (*end entity*)
- Validação: **CertPathValidator**

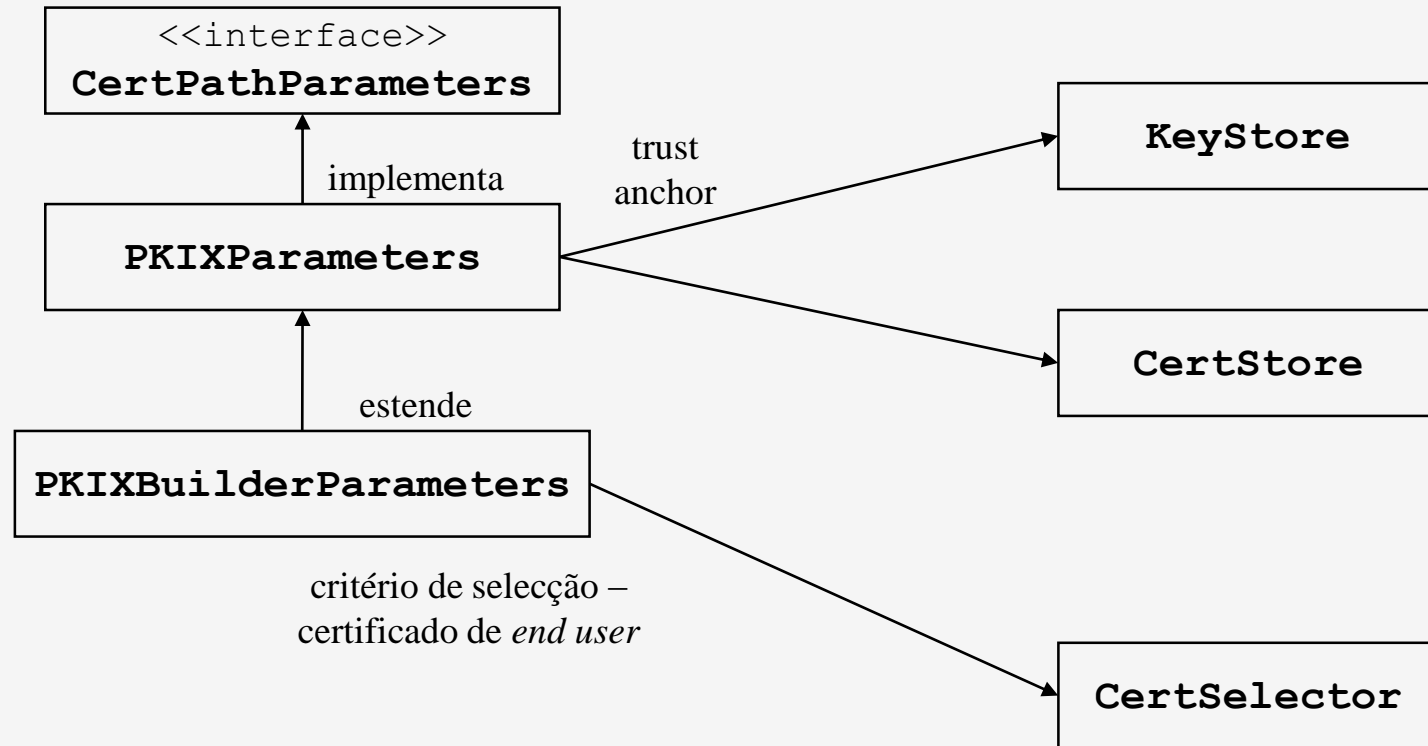
Construção e validação de cadeias (1)



Construção e validação de cadeias (2)

- **CertPathValidator**
 - public final **CertPathValidatorResult**
validate (**CertPath** certPath, **CertPathParameters** params)
throws **CertPathValidatorException**,
InvalidAlgorithmParameterException
- **CertPathBuilder**
 - public final **CertPathBuilderResult**
build (**CertPathParameters** params)
throws **CertPathBuilderException**,
InvalidAlgorithmParameterException

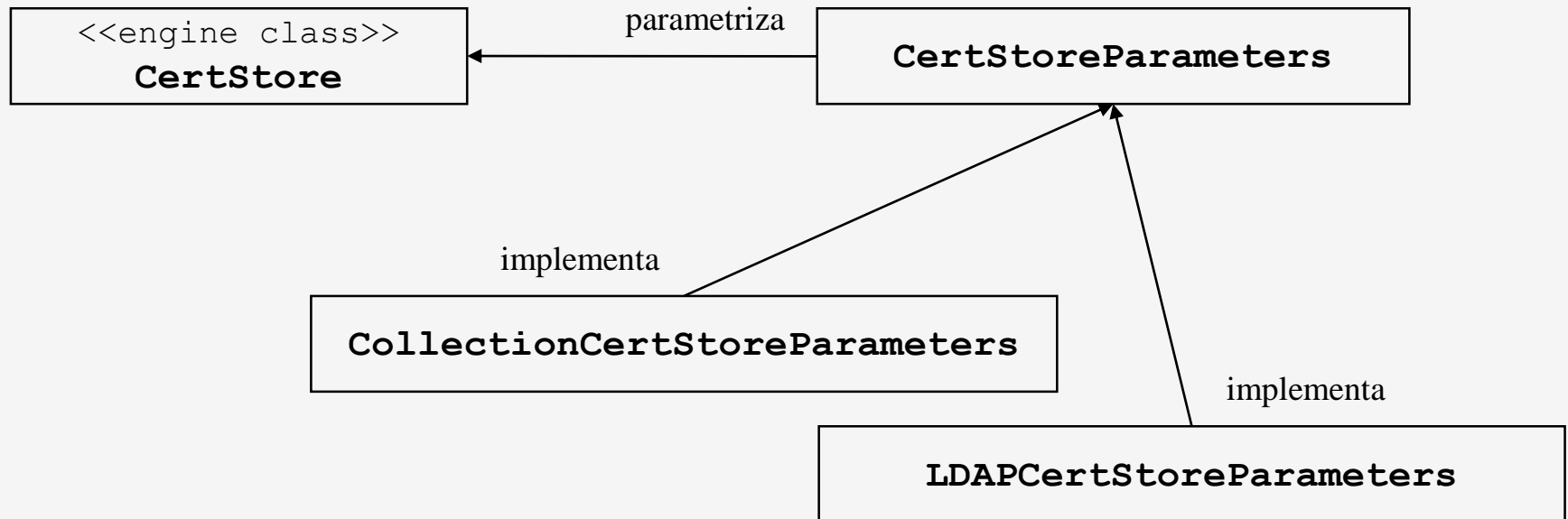
Parametrização (1)



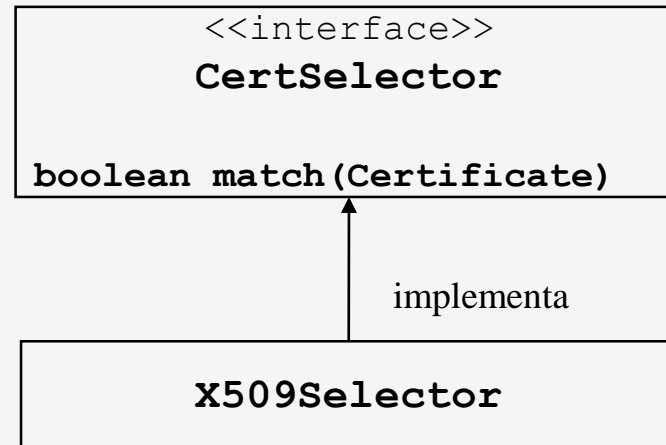
Parametrização (2)

- Construção:
 - Conjunto de *trust anchors* – define os *issuers* dos certificados iniciais da cadeia
 - Conjunto de certificados (**CertStore**) – define os certificados que podem constituir a cadeia
 - Selector (X509CertSelector) – define os requisitos (ex. nome do *subject*) para o certificado final (*end user*)

Classe *CertStore*



Classe *CertSelector*



Debugging

- Parâmetros da máquina virtual: **-Djava.security.debug=certpath**
- Coloca informação adicional no *standard error*