Instalação Componentes

- "*Weak Names*" versus *Strong Names*
- Criptografia de chave pública
- Assinaturas e referências
  - O utilitário `sn.exe`
  - Asssinatura atrasada (*delayed signed assemblies*)
- Assemblies partilhados (shared)
  - GAC (Global Assembly Cache)
- Resolução de nomes
- Ficheiros de configuração
  - Controlo de versões
  - Parâmetrização de aplicações

"Weak Names" - problemas

- Questões relacionadas com os "*weak names*"
  - Como evitar que vários *assemblies* (não relacionados) tenham o mesmo nome?
  - Como manter várias versões do mesmo *assembly?*
  - Integridade dos *assemblies (não foram modificados durante e/ou após o deployment?)*
  - Como possibilitar a distribuição para diferentes *localizações/culturas* (*assemblies* com *resources)*

Strong Names

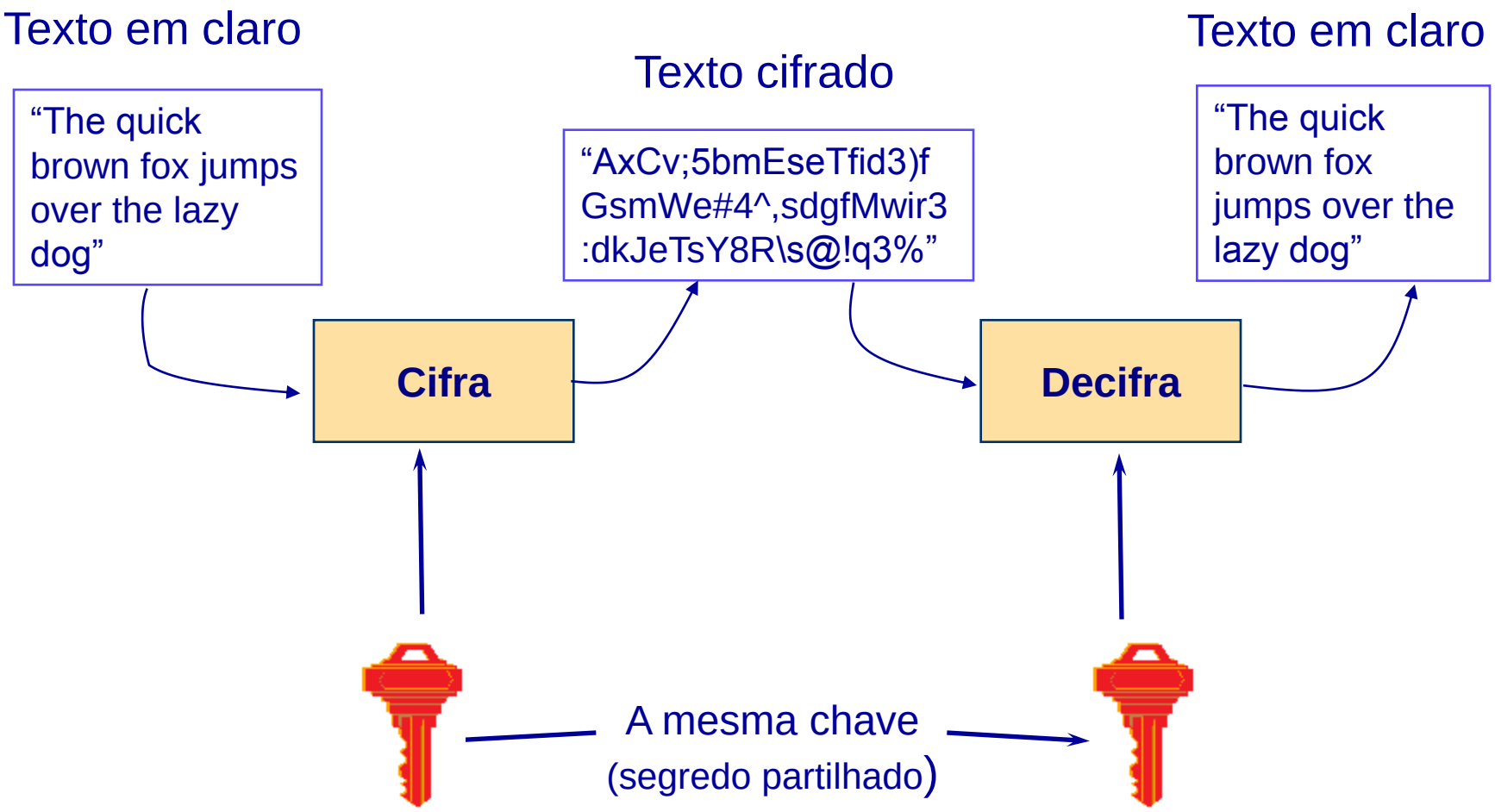
- *A solução .Net foi identificar assemblies com Strong Names*
  - Um strong name é composto por:

nome	*Corresponde ao nome do ficheiro que tem o manifesto (sem extensão)*
versão	(*major*, *minor*, *build*, *revision*)
cultura	localização dos recursos para uma linguagem e região
chave pública(token)	associa o *assembly* à entidade que o criou

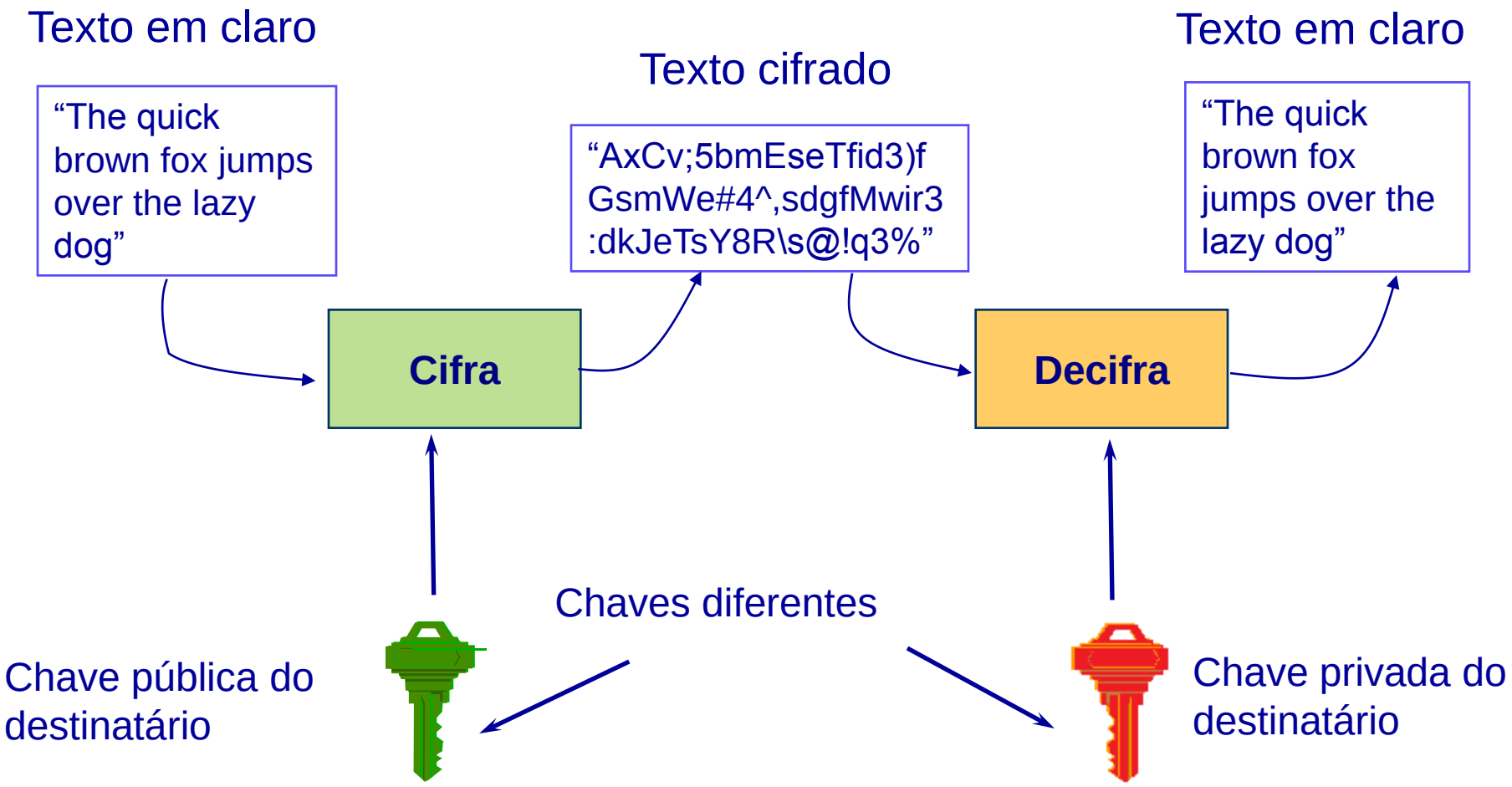
Exemplo de *strong name* *(formato legível)*

MyAssembly, **Version**=1.2.3.4, **Culture**=neutral, **PublicKeyToken**=1234123412341234

Cifra simétrica



Cifra assimétrica



Assinatura Digital

Mensagem a assinar

This is a really long message about Bill's…

Função de Hash (SHA, MD5)

Hash da mensagem

Py75c%bn&*)9|fDe^b
DFaq#xzjFr@g5=&nm
dFg$5knvMd'rkvegMs"

Cifra assimétrica

Assinatura Digital

Jrf843kjfgf*£$&
Hdif*7oUsd*&@:
<CHDFHSD(**

Cálculo de representante (*hash*) da mensagem através de função de sentido único. O *hash* tem um tamanho típico entre 16 e 32 bytes.

Chave privada do assinante

Verificação de assinatura digital

Assinatura Digital recebida

Jrf843kjf
gf*£$&Hd
if*7oUsd
*&@:<CHD
FHSD(**

Asymmetric decryption (e.g. RSA)

Hash da mensagem recebido

Py75c%bn&*)
9|fDe^bDFaq
#xzjFr@g5=
&nmdFg$5kn
vMd'rkvegMs"

Chave pública do assinante

Iguais?

Same hash function (e.g. MD5, SHA…)

Py75c%bn&*)
9|fDe^bDFaq
#xzjFr@g5=
&nmdFg$5kn
vMd'rkvegMs"

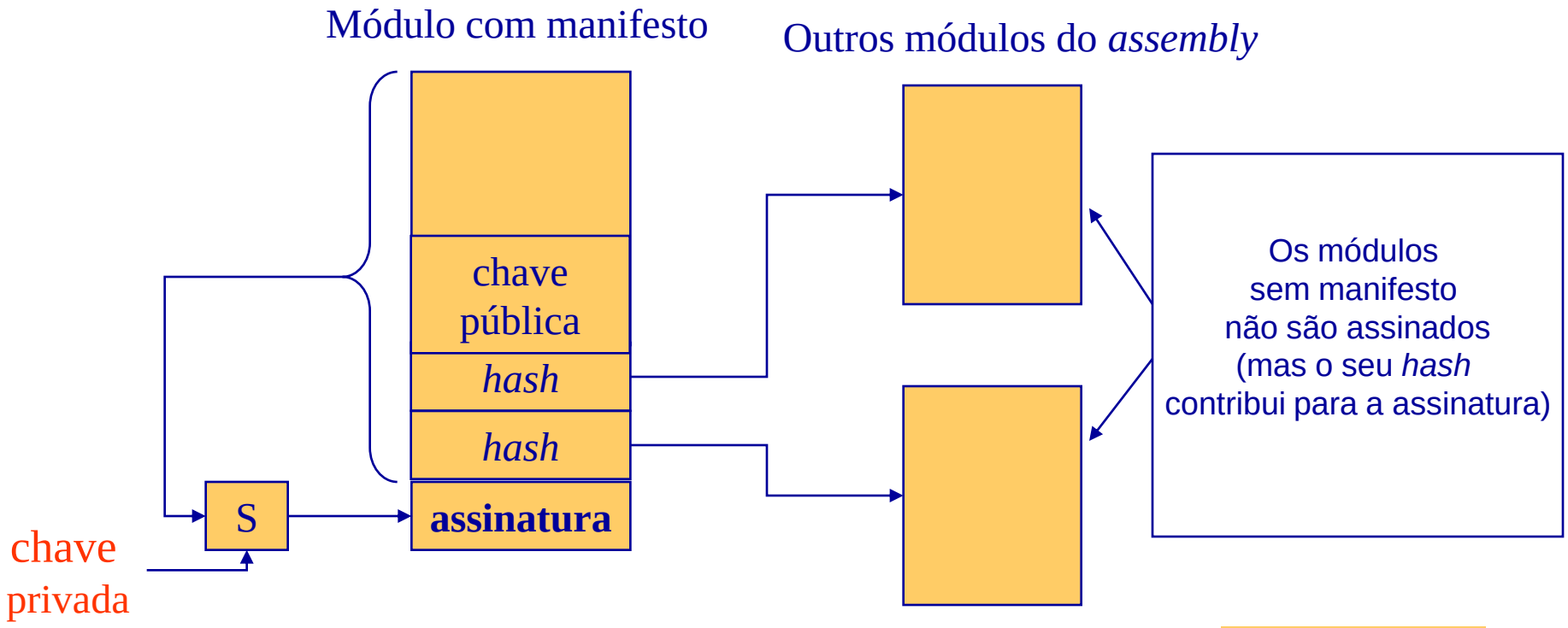
Mensagem recebida

This is a really long message about Bill's…

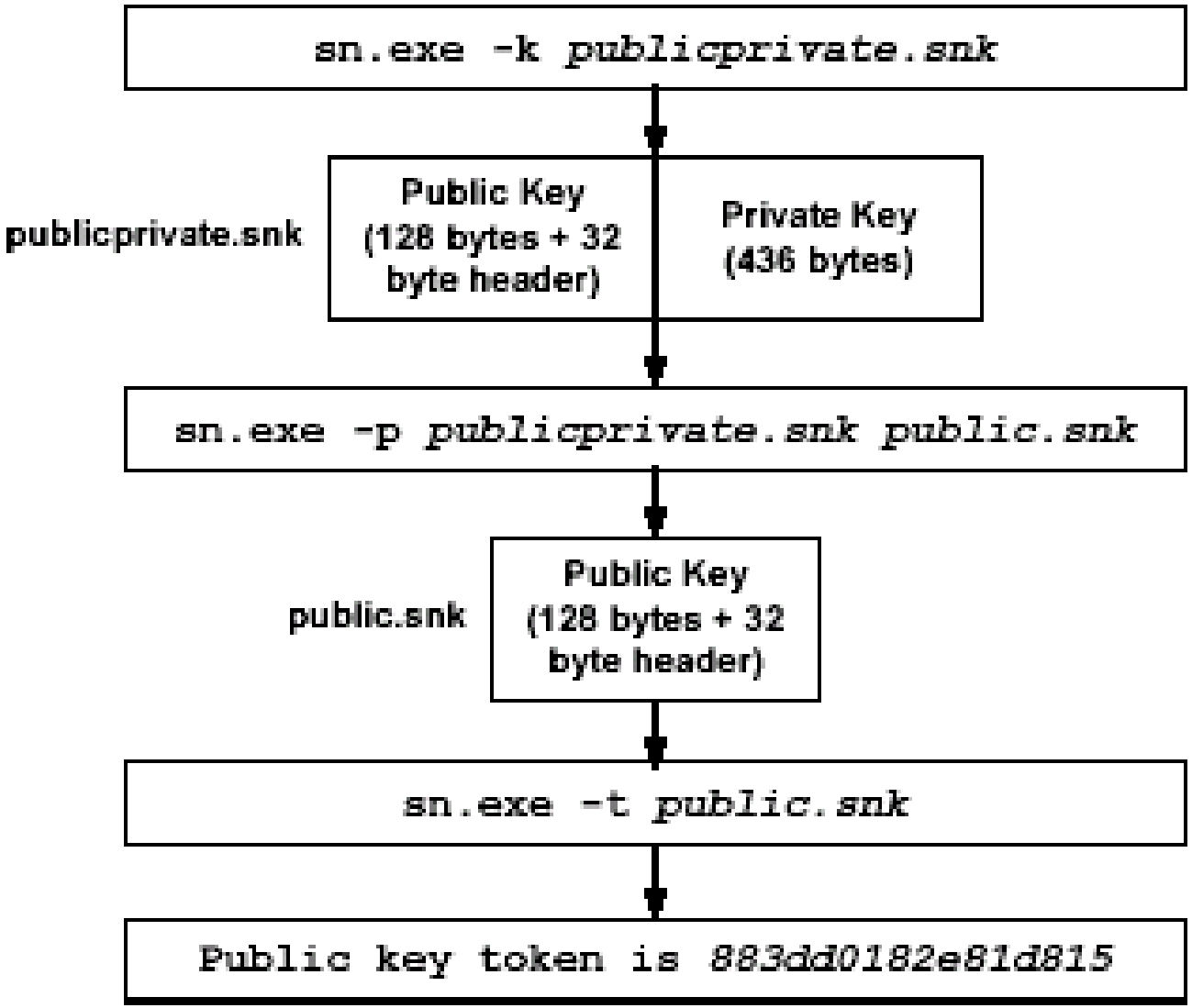
Hash da mensagem gerado no receptor

Assinatura digital em *assemblies strong name*

- O módulo com o manifesto é assinado com a chave privada associada à chave pública do seu nome
- A assinatura é incluída no módulo com o manifesto



Utilização do sn.exe



Geração de Assemblies Strong Name

- A criação de assemblies strong named é feita através da utilização de atributos e/ou opcões de compilação, que especificam a versão e o ficheiro com a chave pública ou o par chave pública/chave privada

- [assembly: AssemblyVersion("1.0.0.3")]
- [assembly: AssemblyKeyFile("keys.snk")]

Delay Sign

- Problema:
  - a geração da assinatura implica conhecimento da chave privada
  - a utilização desta chave na fase de desenvolvimento e teste compromete a sua privacidade

- Solução: *delay signing*

1. Desenvolvimento e teste - a chave pública é colocada no *assembly* e é reservado espaço para a assinatura. Contudo esta não é gerada. Apesar de não estar assinado, o *assembly* possui *strong name.* Outros *assemblies* que o referenciem utilizam este *strong name*

2. Publicação – o *assembly* é assinado, usando-se a chave privada. Esta acção deve ser realizada em ambiente protegido

Delay Sign (II)

- Geração sem assinatura
  - Atributo `AssemblyDelaySignAttribute` controla a realização de *delay sign*
    - [assembly: AssemblyDelaySign(true)]
  - Atributo `AssemblyKeyFileAttribute` indica o nome do ficheiro com a chave pública
- Utilização do *assembly* sem assinatura
  - Registar o *assembly* para que não seja verificada a sua assinatura

    ```
    sn –Vr <assembly>
    ```
- Geração da assinatura
  - Utilitário sn

    ```
    sn –R <assembly> <key_pair_file>
    ```

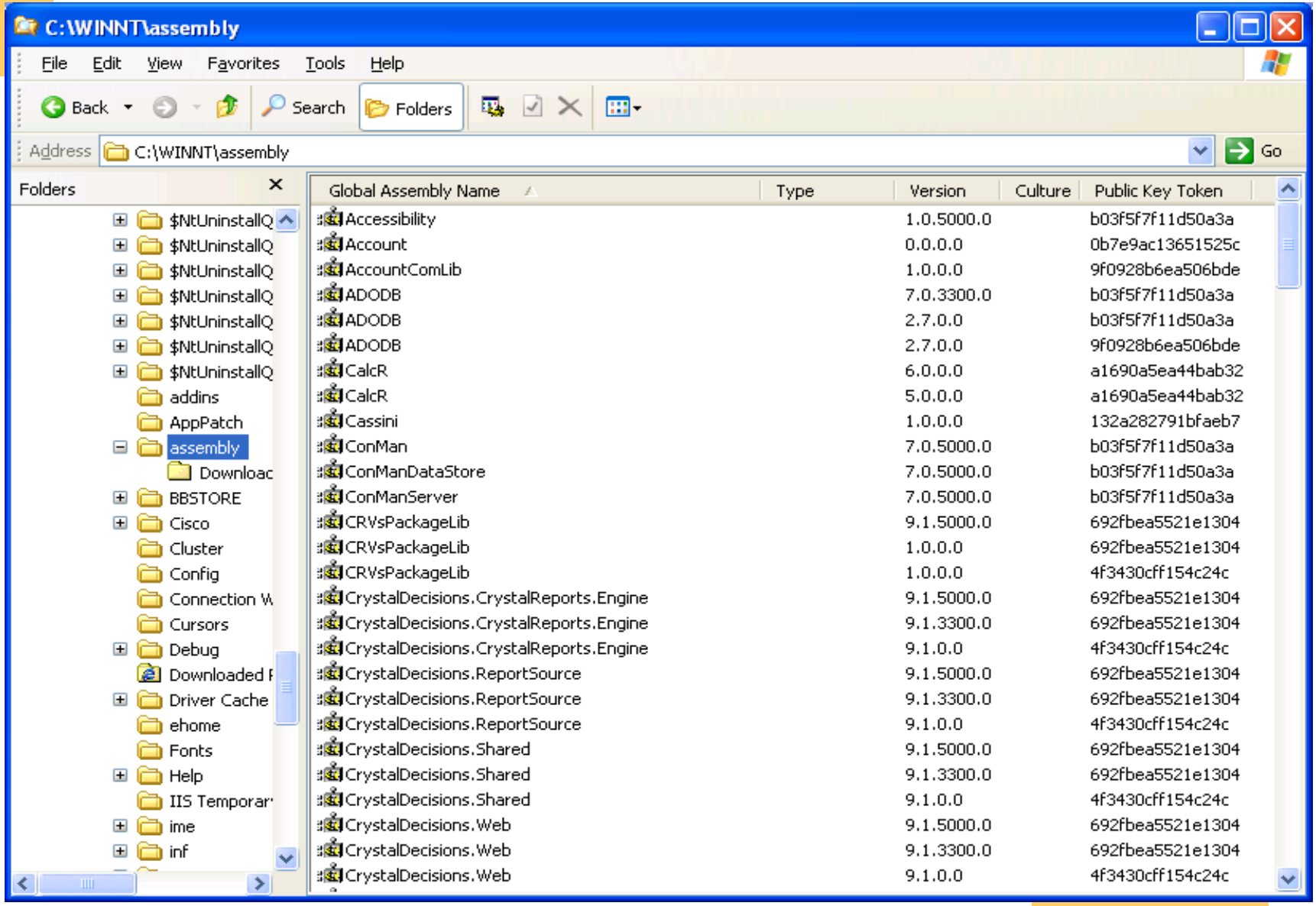
Carregamento com resolução de nome

```
using System;
using System.Reflection;

public class Utilities {
   public static Object LoadCustomerType()  {
      Assembly a = Assembly.Load(
                           "Test, Version=1.2.3.4," +
                           "Culture=neutral," +
                           "PublicKeyToken=9a33f27632997fcc“
                     );

      return a.CreateInstance(“CustomerA”);
   }
}
```

GAC

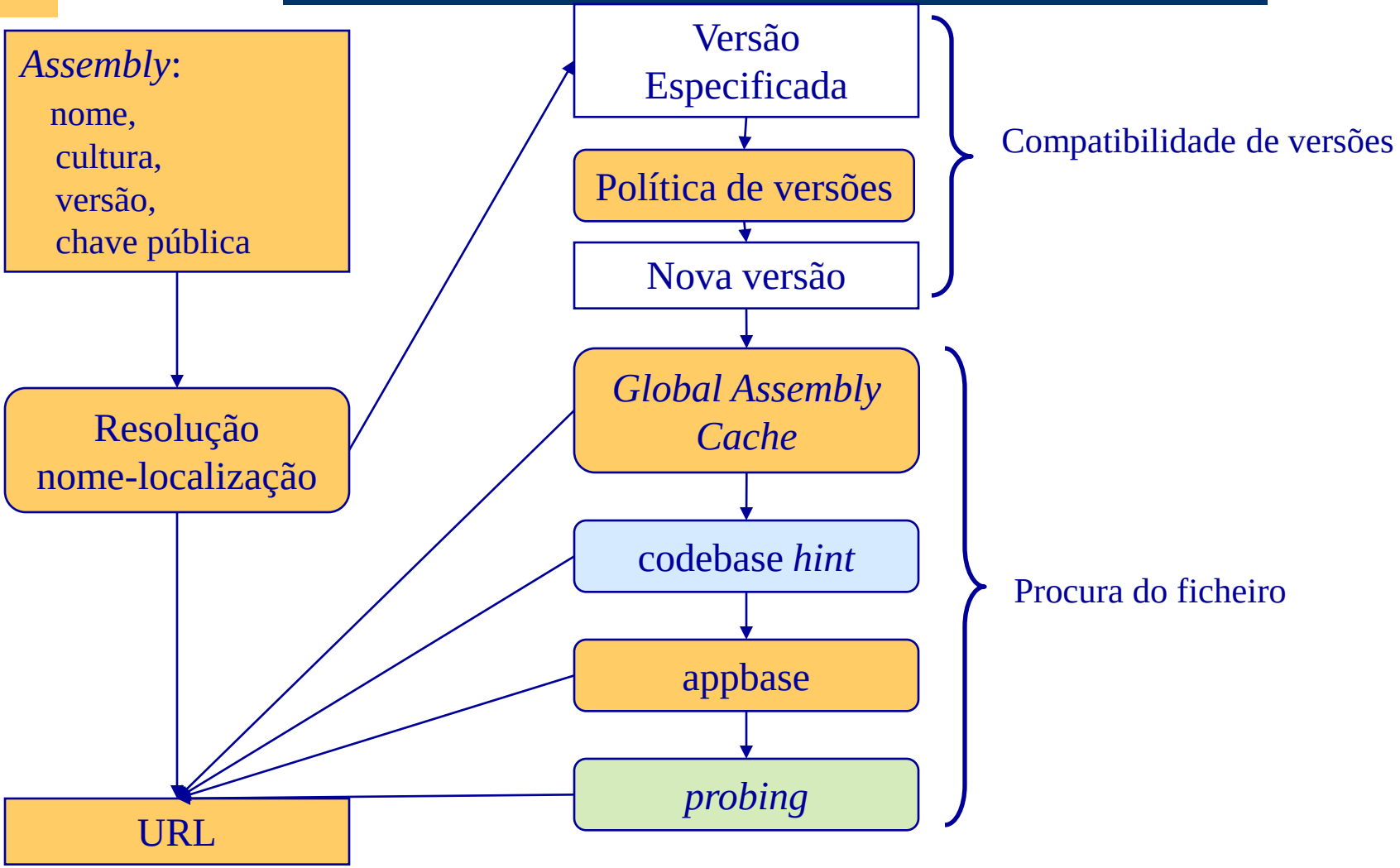

C:\WINNT\assembly
File Edit View Favorites Tools Help
Back Search Folders
Address C:\WINNT\assembly
Go
Folders
$NtUninstallQ
addins
AppPatch
assembly
Downloac
BBSTORE
Cisco
Cluster
Config
Connection W
Cursors
Debug
Downloaded F
Driver Cache
ehome
Fonts
Help
IIS Temporar
ime
inf
Global Assembly Name | Type | Version | Culture | Public Key Token
Accessibility 1.0.5000.0 b03f5f7f11d50a3a
Account 0.0.0.0 0b7e9ac13651525c
AccountComLib 1.0.0.0 9f0928b6ea506bde
ADODB 7.0.3300.0 b03f5f7f11d50a3a
ADODB 2.7.0.0 b03f5f7f11d50a3a
ADODB 2.7.0.0 9f0928b6ea506bde
CalcR 6.0.0.0 a1690a5ea44bab32
CalcR 5.0.0.0 a1690a5ea44bab32
Cassini 1.0.0.0 132a282791bfaeb7
ConMan 7.0.5000.0 b03f5f7f11d50a3a
ConManDataStore 7.0.5000.0 b03f5f7f11d50a3a
ConManServer 7.0.5000.0 b03f5f7f11d50a3a
CRVsPackageLib 9.1.5000.0 692fbea5521e1304
CRVsPackageLib 1.0.0.0 692fbea5521e1304
CRVsPackageLib 1.0.0.0 4f3430cff154c24c
CrystalDecisions.CrystalReports.Engine 9.1.5000.0 692fbea5521e1304
CrystalDecisions.CrystalReports.Engine 9.1.3300.0 692fbea5521e1304
CrystalDecisions.CrystalReports.Engine 9.1.0.0 4f3430cff154c24c
CrystalDecisions.ReportSource 9.1.5000.0 692fbea5521e1304
CrystalDecisions.ReportSource 9.1.3300.0 692fbea5521e1304
CrystalDecisions.ReportSource 9.1.0.0 4f3430cff154c24c
CrystalDecisions.Shared 9.1.5000.0 692fbea5521e1304
CrystalDecisions.Shared 9.1.3300.0 692fbea5521e1304
CrystalDecisions.Shared 9.1.0.0 4f3430cff154c24c
CrystalDecisions.Web 9.1.5000.0 692fbea5521e1304
CrystalDecisions.Web 9.1.3300.0 692fbea5521e1304
CrystalDecisions.Web 9.1.0.0 4f3430cff154c24c

Colocar assemblies no GAC (gacutil)

gacutil [*options*] [*assemblyName* | *assemblyPath* | *assemblyListFile*]

Option	Description
/i *assemblyPath*	Installs an assembly into the global assembly cache.
/u *assemblyName*	Uninstalls an assembly from the global assembly cache.

Fases associadas ao carregamento de *assemblies*



Ficheiro de configuração da aplicação para controlo de versões

```
<?xml version="1.0" ?>
<configuration  >
        <runtime>
                <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1" >
                        <!-- one dependentAssembly per unique assembly name -->
                        <dependentAssembly>
                                <assemblyIdentity
                                name="Acme.HealthCare" publicKeyToken="38218fe715288aac"
                                />
                                <!-- one bindingRedirect per redirection -->
                                <bindingRedirect oldVersion="1.2.3.4" newVersion="1.3.0.0" />
                                <bindingRedirect oldVersion="1-1.2.3.399" newVersion="1.2.3.7" />
                        </dependentAssembly>
                </assemblyBinding>
        </runtime>
</configuration>
```

Terá de existir na directoria da aplicação, com o nome **<appname>.exe.config**

Path de pesquisa privados

```
<?xml version="1.0" ?>
<configuration  >
        <runtime>
                <assemblyBinding  xmlns="urn:schemas-microsoft-com:asm.v1" >
                        <probing privatePath="shared;common" />
                </assemblyBinding>
        </runtime>
</configuration>
```

Terá de existir na directoria da aplicação, com o nome <appname>.exe.config

Funciona também em *weak named assemblies*

Definição de *codebase* em ficheiro de configuração

```
<?xml version="1.0" ?>
<configuration >
        <runtime>
                <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1" >
                        <!-- one dependentAssembly per unique assembly name -->
                        <dependentAssembly>
                                <assemblyIdentity
                                  name="Acme.HealthCare" publicKeyToken="38218fe715288aac" />
                                <!-- one codeBase per version -->
                                <codeBase version="1.2.3.4"
                                                href="file://C:/acmestuff/Acme.HealthCare.DLL"  />
                                <codeBase version="1.3.0.0"
                                                href="http://www.acme.com/Acme.HealthCare.DLL"  />
                        </dependentAssembly>
                </assemblyBinding>
        </runtime>
</configuration>
```

Terá de existir na directoria da aplicação, com o nome **<appname>.exe.config**

Publisher Policy Control

JeffTypes.config

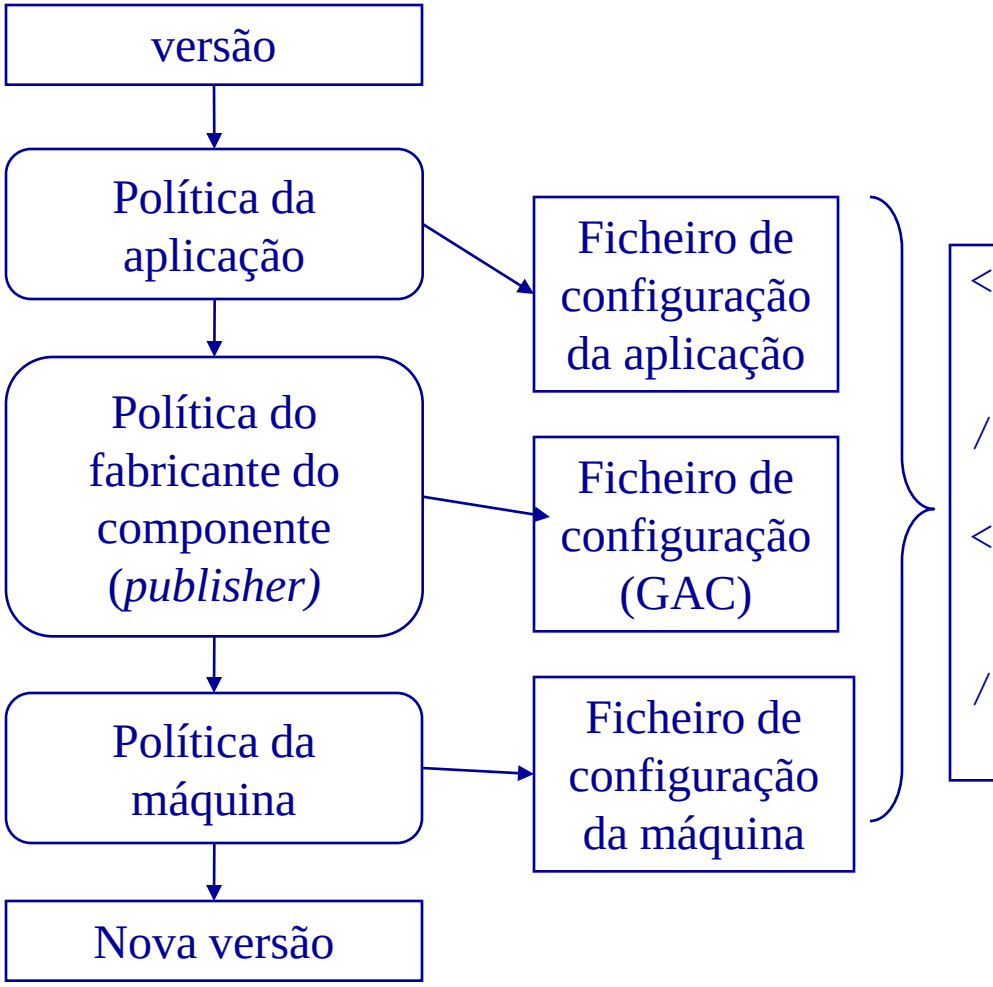
```
<configuration>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="JeffTypes" publicKeyToken="32ab4ba45e0a69a1"
           culture="neutral" />
        <bindingRedirect oldVersion="1.0.0.0" newVersion="2.0.0.0" />
        <codeBase version=2.0.0.0"
         href="http://www.Wintellect.com/JeffTypes.dll" />
      </dependentAssembly>
    </assemblyBindings>
  </runtime>
</configuration>
```

- Apenas podem ser definidos critérios para os *assemblies* criados pelo próprio. Além disso, os elementos aqui mostrados são os únicos elementos que podem constar num ficheiro deste tipo
- O ficheiro de configuração diz ao CLR para carregar a versão 2.0.0.0 do *assembly JeffTypes* sempre que seja referenciada a versão 1.0.0.0.
- Para criar o *assembly* que contém esta informação de configuração, deverá usar o *AL.exe* da seguinte forma:

```
AL.exe /out:policy.1.0.JeffTypes.dll
       /version:1.0.0.0
       /keyfile:MyCompany.keys
       /linkresource:JeffTypes.config
```

Nome do ficheiro
Identifica os elementos *major* e o *minor* da versão do *assembly* a que está associado

Política de versões – fases de aplicação



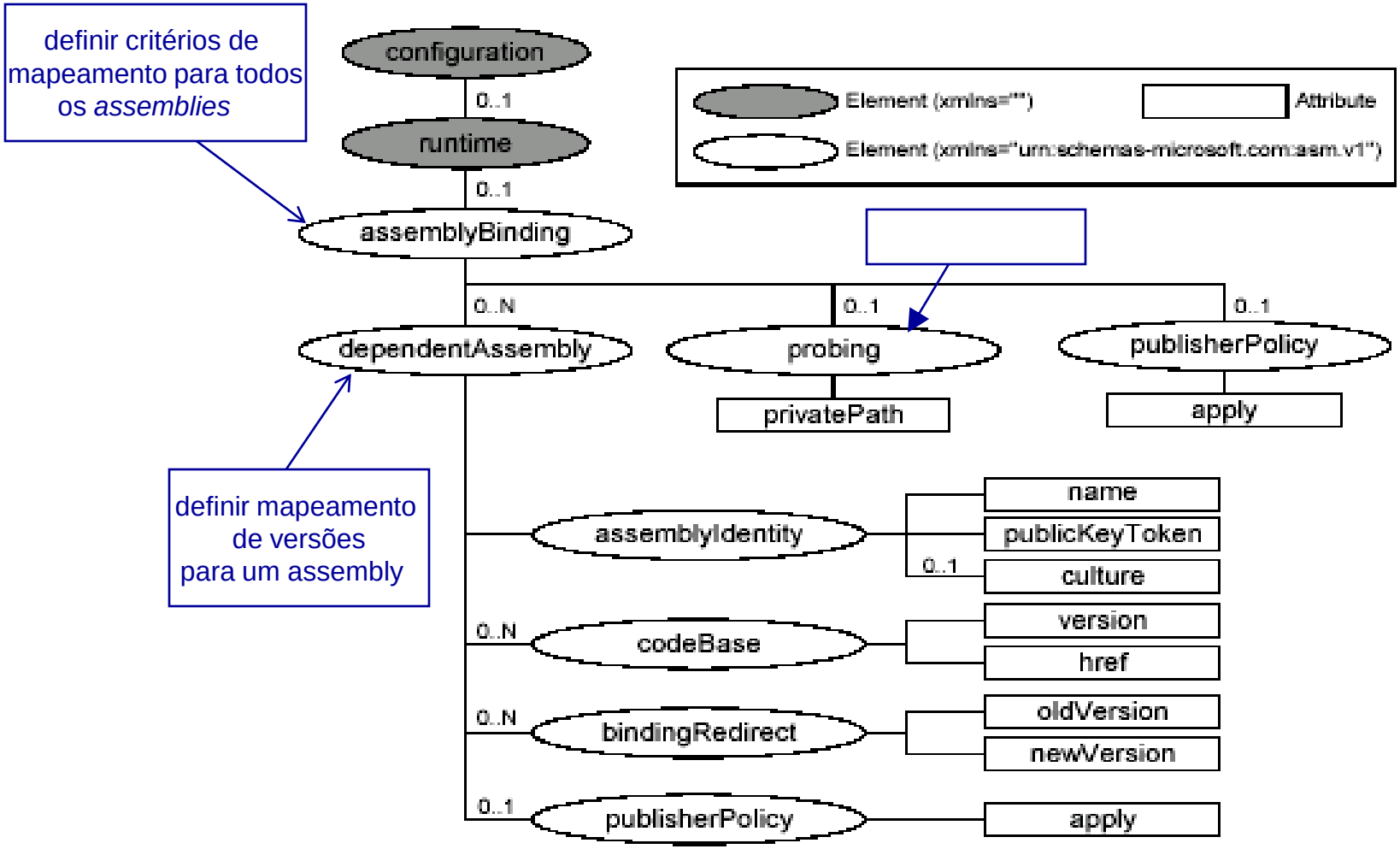

```
<bindingRedirect
    oldVersion = "1.2.3.4"
    newVersion = "1.3.0.0"
/>

<bindingRedirect
    oldVersion = "1-1.2.3.399"
    newVersion = "1.2.3.7"
/>
```

Publisher policies - o cliente do componente tem a última palavra

```
<?xml version="1.0" ?>
<configuration xmlns="urn:schemas-microsoft-com:asm.v1">
      <runtime>
            <assemblyBinding>
                <publisherPolicy apply="no" />
            </assemblyBinding>
      </runtime>
</configuration>
```

Excerto de schema de ficheiros de configuração



Secção *appsettings* do ficheiro de configuração

```
<configuration>
    <appSettings>
        <add key="key1" value="10" />
        <add key="assembName" value="a1" />
    </appSettings>
</configuration>
```

Secção *appsettings* do ficheiro de configuração

Acesso programático

Namespace

Classe

Colecção de pares nome/valor

indexer

```
String res=System.Configuration.ConfigurationManager.AppSettings["key1"]; //res="10"
```