

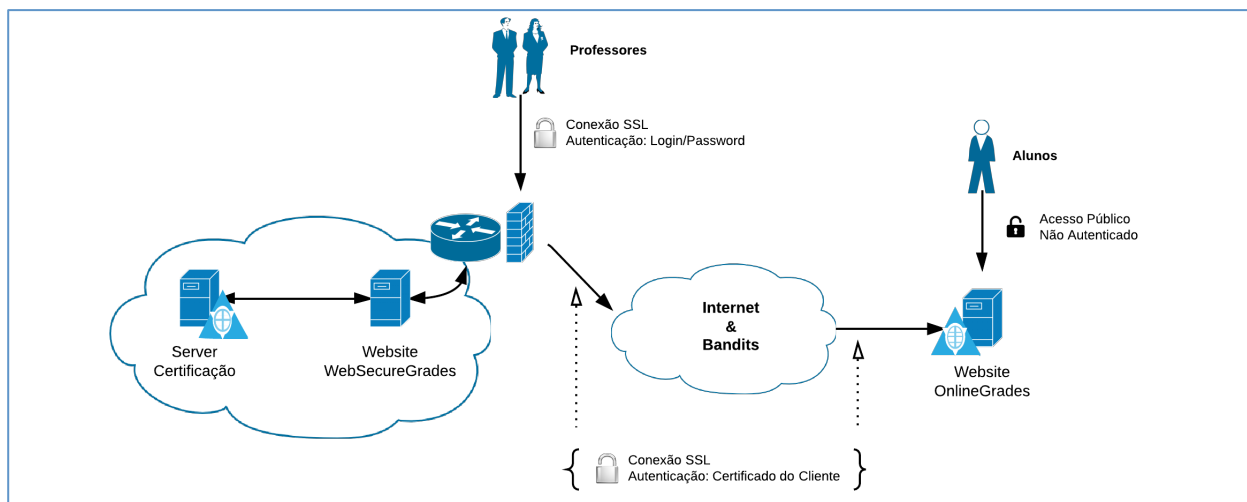


# Relatório - Projecto SIRS

## Módulo Assinatura de Pautas

GRUPO6 : 66047 – JOÃO PINHO | 68147 – FREDERICO MENDES | 68158 – JOÃO SOUSA

### Arquitectura do Projecto



### Problema

O problema que pretendemos resolver na nossa solução consiste, no desenvolvimento de um sistema que permita efectuar a publicação de notas de alunos pelos professores, a partir de um servidor seguro, para um servidor público de consulta de notas.

Para que o sistema seja considerado seguro tivemos os seguintes aspectos em atenção:

- A ligação HTTP ao Website WebSecureGrades é feita sobre SSL, com autenticação por Login (Username e Password);
- As notas carregadas no WebSecureGrades são assinadas antes de serem enviadas para o OnlineGrades (sistema de publicação) com a chave privada da escola/faculdade;
- A ligação entre o WebSecureGrades e o OnlineGrades é feito por HTTP sobre SSL com autenticação do cliente por certificado (e autenticação do sistema de publicação através do certificado usado na ligação SSL).

### Pressupostos à Solução Implementada

Na nossa solução assumimos que o atacante não consegue penetrar a firewall da rede onde se encontra o WebSecureGrades e assim falar com a máquina de certificação como se fosse o WebSecureGrades.

Por esse motivo a ligação entre a Máquina de Certificação e a WebSecureGrades não dispõe de qualquer autenticação.

### Detalhe da Solução por Componentes

Este processo de detalhe pretende provar, explicando e detalhando os detalhes da nossa implementação, de que o sistema é efectivamente seguro. Assim como identificar quando seja caso disso, possíveis vulnerabilidades que sejam do nosso conhecimento e que não tenham sido asseguradas na solução.

### Login

O login permite ao professor, ter acesso ao sistema de carregamento/publicação de notas. Os dados de acesso são fornecidos ao professor por carta, de forma segura (detalhe na conclusão).

Por sua vez, os dados de acesso ao website são guardados numa base de dados onde é guardado o hash por SHA1 da password juntamente com o seu salt, que consiste no seguinte:

Quando é gerada a password do utilizador é gerado também um salt através de um **Cryptographically Secure Pseudo-Random Number Generator (CSPRNG)**. O salt é único por cada par user/password.

No processo de armazenamento da password no sistema ocorrem as seguintes operações:

- Geração de um salt aleatório e tipicamente grande através de um CSPRNG;
- Hash através do SHA1 da concatenação da password+salt;
- Guarda-se no registo de login do utilizador o hash anterior e o salt.

No processo de validação da password:

- É obtido o salt e a hash da base de dados para o utilizador (username);
- Hash através do SHA1 da concatenação da password+salt;
- Comparação do hash obtido no passo anterior com o obtido da base de dados para o utilizador, se os hashes forem iguais o utilizador é autenticado com sucesso, caso contrário é negado o acesso ao sistema.

### Assinatura das Notas

Quando o professor termina a inserção das notas, efectua a submissão das mesmas – este processo é composto por três fases:

- Envio dos dados para o Webservice de Certificação das notas que se encontra na Máquina de Certificação;
- Solicitação final ao professor, para confirmação da publicação das notas;
- Envio das notas, junto com a respectiva assinatura.

O utilizador é informado do sucesso da operação após validação das notas enviadas para o sistema OnlineGrades.

## WebService Certificação de Notas

O webservice de certificação recebe um objecto do tipo `GradesPublication` e assina o seu conteúdo. A assinatura dos dados envolve as seguintes operações:

- Serialização do objecto para XML;
- Escrita do XML numa stream em memória;
- Aquisição de um vector de bytes contendo o XML, ao qual iremos chamar **dataBytes**;
- Cálculo do hash de **dataBytes**: `byte[] sha1Hash = sha.ComputeHash(dataBytes);`
- Assinatura do hash recorrendo ao algoritmo RSA com o algoritmo de hashing SHA-512:  
`X509Certificate2 keyCertificate = LoadPrivateKeyCert()  
RSACryptoServiceProvider rsa = (RSACryptoServiceProvider)keyCertificate.PrivateKey  
byte[] signedHash = rsa.SignHash(sha1Hash, CryptoConfig.MapNameToOID("SHA-512"))`
- Retorno da assinatura dos dados: `return Convert.ToBase64String(signedHash).`

O certificado encontra-se instalado na máquina de certificação (para mais informação, por favor consulte o Anexo I).

Um passo algo abstracto acima, é a conversão para XML do objecto, a conversão do objecto em XML obedece a algumas regras de formatação especificadas através de meta atributos nas propriedades da própria classe “GradesPublication”, sugere-se a consulta do código para melhor se perceber esta informação (CertificationFeature\Sources\EduMaterialCertificator\App\_Code\GradesPublication.cs + StudentEvaluation.cs).

Com base nesta especificação XML, imposta aos dados a assinar, foi gerado um XSD (WSG-GradesPublication\_1\_0\_0.xsd), partilhado com o sistema OnlineGrades, cuja utilidade será mencionada mais à frente, mas que basicamente permite fazer com que ambos os sistemas vejam os dados de acordo com um standard imposto por este XSD.

## OnlineSecureGrades

### WebService de Publicação das Notas

O sistema WebSecureGrades comunica com este webservice sobre HTTPS (HTTP sobre SSL) e efectua o envio dos dados assinados, após autenticação perante o sistema OnlineGrades via certificado (Client Certificate).

Após receber os dados, o webservice possui do seu lado um objecto (extraído apartir do corpo do objecto SOAP recebido por XML WebServices) e a assinatura dos dados recebidos. Com esta informação o webservice procede à execução das seguintes operações:

- Validação da Assinatura:  
`bool dataValid = ModelHelper.IsValidSignature(publication, signature);`
  - Conversão do objecto **publication** para XML e tradução para byte[]:  
`xs.Serialize(memStream, publication, ns);`  
`byte[] dataBytes = memStream.ToArray();`
  - Geração do SHA1 dos dados recebidos:  
`byte[] sha1Hash = sha.ComputeHash(dataBytes);`
  - Verificação do hash calculado anterior com o hash recebido:  
`X509Certificate2 publicKeyCert = LoadPublicKeyCert();`  
`byte[] signedHash = Convert.FromBase64String(signature);`  
`RSACryptoServiceProvider rsa = publicKeyCert.PublicKey.Key`  
`rsa.VerifyHash(sha1Hash, CryptoConfig.MapNameToOID("SHA-512"), signedHash);`
- Inserção dos dados na base de dados.

**Nota:** Na base de dados são inseridas publicações de notas, assinadas em nome de cada professor, ou seja, um professor pode publicar várias vezes as notas de uma determinada cadeira, a publicação actual poderia num sistema real ser mostrada apenas em função da data, para determinar a última publicação (mas isso já sai fora de âmbito, pelo que, no sistema OnlineGrades é possível visualizar somente as notas de cada publicação válida recebida pelo sistema WebSecureGrades).

Em relação ao ficheiro XSD (WSG-GradesPublication\_1\_0\_0.xsd) mencionado anteriormente, notem que o webservice de publicação é chamado pelo sistema WebSecureGrades. Neste contexto, acrescentamos ainda e tal como prometido anteriormente, que o webservice de publicação aceita a recepção de dados apenas no formato especificado no XSD (foi usada a ferramenta xsd.exe para se extrair uma representação em C# do XSD).

Por isso no webservice de publicação, garantimos assim que ao serem serializados os objectos de publicações de notas, o resultado em binário e posterior hash irá estar em sintonia com o sistema de certificação dos dados e assim ambos falam a mesma “língua”.

Este XSD é na verdade imposto aos três participantes na comunicação das notas, pois o WebSecureGrades ao falar com o webservice do sistema de publicação tem também de converter os

seus dados para um objecto do tipo solicitado por este (baseado no XSD).

## Conclusão

A nossa solução implementa assim um sistema onde os professores se autenticam de forma segura perante um sistema e trocam informações através de um canal seguro onde todas as comunicações são devidamente cifradas.

É garantida a autenticação do sistema WebSecureGrades, devido à existência de um certificado assinado pela VeriSign (no nosso caso usámos certificados self-signed, mas num sistema real seriam usados certificados confiáveis por uma CA acreditada), evitando desta forma que um atacante podesse efectuar um ataque de DNS Cache Poisoning e levar assim os utilizadores a tentarem autenticar-se numa máquina do atacante.

A protecção da máquina de certificação é também assegurada, uma vez que assumimos que a firewall da rede do sistema WebSecureGrades foi configurada por profissionais de segurança de forma a que sejam impossível um atacante penetrar a rede, e através de IP Spoofing fazer-se passar pela máquina do WebSecureGrades.

Entre o sistema WebSecureGrades e o sistema OnlineGrades a comunicação é cifrada através de um canal seguro por SSL e a autenticação é garantida ponto a ponto, quer por parte do WebSecureGrades com um certificado de cliente, que por parte do Online Grades através do certificado usado para estabelecer o canal SSL, ambos os certificados foram assinados pela. Para garantir que tudo isto é seguro ambas devem consultar as CRL's da VeriSign e garantir que os certificados estão dentro da validade, esta propriedade é garantida pelo WebServer utilizado (IIS – Internet Information Services) na utilização de canais seguros, quando configurado. No nosso projecto, não efectuamos essas configurações por estarmos a trabalhar com certificados self-signed.

O acesso ao sistema OnlineGrades para consulta de notas é público e inseguro, por se tratar de um sistema puramente de consulta de informação. Caso um atacante penetre a rede do sistema de publicação, não existe grande coisa que possa fazer, uma vez que este não tem nada de importante nele guardado, guarda somente notas. Eventualmente, poderá alterá-las, mas ao fazê-lo a publicação deixaria de ser válida por deixar de corresponder à assinatura guardada no sistema. Assinatura esta que, para ser recalculada necessita da chave privada do sistema WebSecureGrades, que está guardada a “sete chaves”, no servidor de certificação.

Desta forma, garantimos não repúdio por parte do sistema WebSecureGrades perante o sistema OnlineGrades uma vez que os dados são assinados com a chave privada do primeiro, e também confidencialidade dos dados comunicados entre eles, devido a existência de uma ligação SSL com autenticação de ambas as entidades.

Os professores garantem o não repúdio e a confidencialidade ao fazerem login no sistema WebSecureGrades sobre uma ligação por HTTPS, com credenciais solicitadas pelos mesmos na secretaria da escola, presencialmente e com assinatura manual, para a qual obtém em resposta um envelope opaco, selado por uma máquina própria. Em alternativa aqui poderia usar-se SmartCards, contendo uma chave privada atribuída especificamente ao professor, e que seria lido por um leitor especial sempre que este se quisesse autenticar no sistema WebSecureGrades. Desta forma, a segurança seria bastante forte, mas também mais dispendiosa e menos prática devido à necessidade de um leitor de cartões SmartCard.

Por este motivo consideramos a nossa solução robusta, simples e segura, pois o custo para o atacante em termos de recursos, esforço e tempo para quebrar o nosso sistema, ultrapassa consideravelmente o valor da informação neste guardada, este é o conceito que utilizamos aqui para traduzir a palavra “seguro”. A segurança do sistema poderia ser ainda maior, se fossem considerados aspectos como acessos somente de dentro do Campus, ou com ligações de dentro da rede onde se poderia permitir o uso de VPN's para o estabelecimento de ligações aos sistema WebSecureGrades, no entanto aqui comprometemo-nos somente a disponibilizar um sistema seguro, simples e fácil de usar que constitui uma primeira abordagem à resolução do problema proposto.

## Geração dos Certificados

Para a geração dos certificados das diversas componentes do sistema recorreremos à ferramenta OpenSSL.

Para a geração de Self-Signed Certificates, foram usados os seguintes comandos:

Comando usado para a geração da chave privada:

```
> openssl genrsa -out securegrades.pem 2048
```

Comando usado para exportar a chave e parâmetros públicos específicos do algoritmo RSA para o formato standard PKCS#12:

```
> openssl pkcs12 -export -in securegrades.crt -inkey securegrades.pem -out securegrades.p12
```

Comando usado para a geração de um certificado self-signed que contem a chave pública a distribuir manualmente:

```
> openssl req -new -x509 -key securegrades.pem -out securegrades.crt -days 365
```

Após a geração do certificado de chave privada e pública, foi eliminado de forma segura o ficheiro **pem** que continha o par, chave pública e privada, que continha as chaves no seu interior completamente desprotegidas, referimos isto, porque normalmente os certificados são cifrados com algoritmos simétricos (TripleDES) com uma password do conhecimento do administrador e no nosso caso não existia cifra.

## Segurança das Chaves-Privadas

### Web Server (Máquina Certificação)

A máquina de certificação desempenha no sistema WebSecureGrades o papel da entidade que assina dados em nome de todo o sistema.

Como tal, a assinatura de dados envolve a existência de um par de chaves pública e privada, para as quais foram tomadas algumas medidas de segurança:

- **Chave Pública**

Método de Distribuição: Manual, a chave pública do sistema será sempre instalada manualmente nos sistemas que tenham de comunicar de forma segura com este.

- **Chave Privada**

Armazenamento: No sistema de ficheiros da máquina de certificação, na directoria da aplicação que disponibiliza o webservice de assinatura dos dados relativos a notas de alunos. Somente administradores da máquina têm acesso ao certificado de chave privada e chave pública.

KeyStore da máquina, o certificado encontra-se instalado na KeyStore da LocalMachine, na Location Personal.

Permissões de Acesso: Além do grupo de administradores (que tem *full control* sobre todos os ficheiros da máquina), foi criado o utilizador “educertificator\_svc” que tem permissões para aceder à KeyStore da Local Machine, e obter o certificado de chave privada da Location Personal, com permissões de leitura.

Mais nenhum utilizador, além dos administradores e do “educertificator\_svc” tem permissões de acesso à chave privada. E a conta educertificator\_svc é uma conta de serviço que não permite login na máquina e pode ser usada somente pelo WebServer para adquirir privilégios de acesso.

Nota: O certificado foi instalado inicialmente na máquina, contra a introdução de uma password, por isso, o acesso ao ficheiro que contém a chave privada está protegido por password e só é acessível por administradores. E por outro lado o certificado de chave privada instalado na KeyStore da LocalMachine > Personal, só é acessível por administradores ou pelo user “educertificator\_svc”.

Esta parameterização permite-nos assim obter uma solução segura, no que toca ao armazenamento do certificado de chave privada.

## Configuração do Web Server

### Application Pools

Para a configuração das aplicações no servidor web IIS, foram criados utilizadores específicos para a execução das *Application Pools* de cada aplicação.

#### WebSecureGrades (App Pool)

- Aplicação: /websecuregrades ;
- Utilizador: websecgrades\_service ;  
Permissões Windows: Users, IIS\_USERS.
- Load User Profile : true

#### EduMaterialCertificator (App Pool)

- Aplicação: /edumaterialcertificator ;
- Utilizador: educertificator\_svc ;  
Permissões Windows: Users, IIS\_USERS.
- Load User Profile : true

Tanto os utilizadores dos grupos Users como do IIS\_USERS, têm pouquíssimas permissões no servidor, podendo no caso do primeiro ler ficheiros públicos sem permissões definidas praticamente e no caso do segundo, estes users tem permissões para aceder somente aos ficheiros da pasta **inetpub** do IIS com acesso público.

*Application Pool* com opção **LoadUserProfile** activa, esta opção carrega as permissões do utilizador sobre a qual *Application Pool* se encontra a correr, permitindo de acordo com os acessos definidos, que o utilizador carregue certificados X509 a partir do *filesystem*.

### Web Server (Máquina Certificação)

Na máquina de certificação, foi configurado o *Internet Information Services* da Microsoft para a disponibilização do webservice de assinatura dos dados que contém as notas dos alunos.

Para a disponibilização deste serviço, foi criada no IIS a aplicação “edumaterialcertificator” dentro da qual se encontra o webservice “GradesCertifier.asmx”.

Por questões de segurança, foi criada uma *Application Pool* específica para a aplicação “edumaterialcertificator”, na qual corre somente o código do webservice de assinatura dos dados.

Esta *Application Pool* corre com as mesmas permissões do utilizador “educertificator\_svc” criado para este efeito, por forma a permitir o acesso à keystore onde se encontra o certificado de chave privada, instalado no servidor com password.

## Instalação do Certificado de Chave Privada

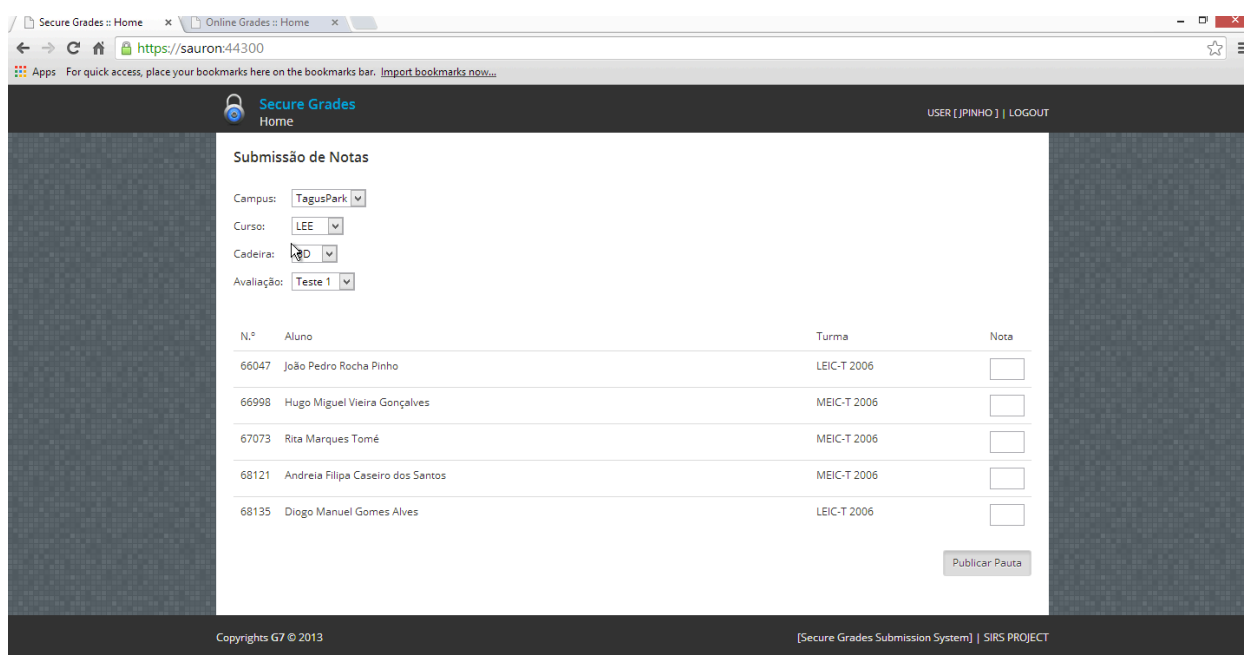
A instalação da chave foi feita, correndo o Wizard de instalação do Windows típico quando se efectua clique duplo sobre um certificado de extensão **p12**.

Após introdução da password que protege o certificado, o certificado foi instalado na Local Machine na directoria Personal da KeyStore do Windows.

Após este processo, via mmc.exe (Management Console) adicionou-se o snap-in de Certificados do Windows, e acedemos ao certificado instalado no passo anterior.

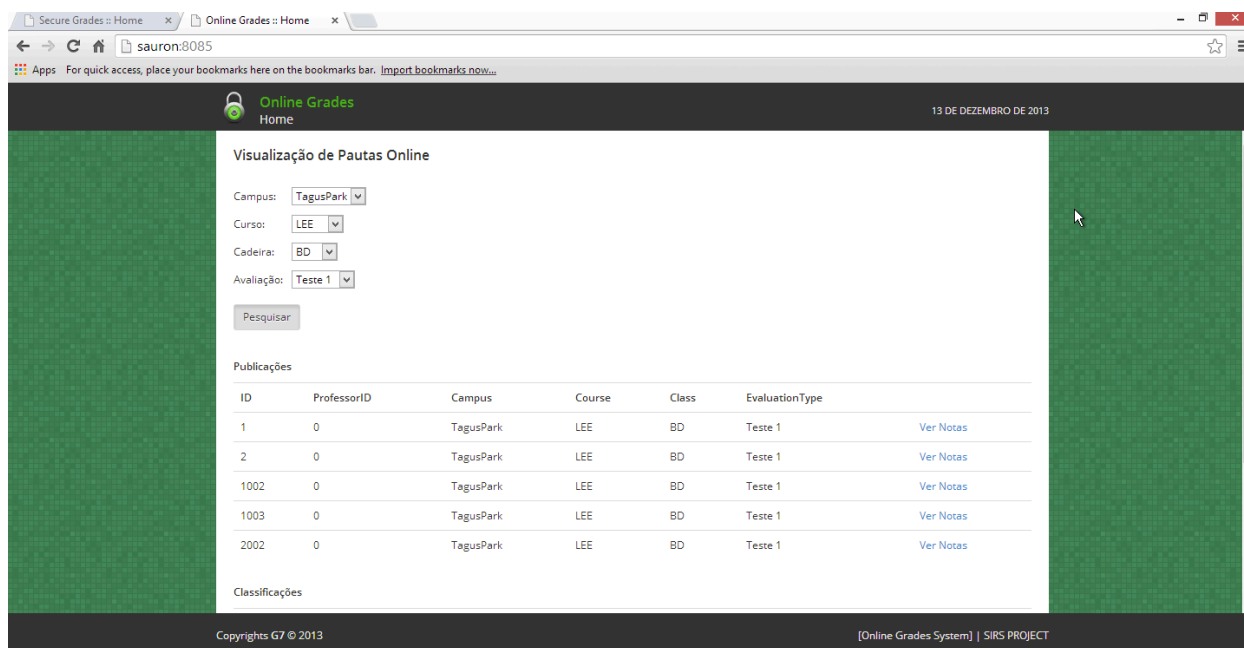
Ai foram configuradas as permissões sobre o certificado, para o qual foram definidos acessos de full control para Administrators e de read para o user “educertificator\_svc”.

## Preview do Sistema



The screenshot shows the 'Secure Grades' web application interface. The top navigation bar includes the application name and a user login/logout option. The main content area is titled 'Submissão de Notas' (Grade Submission). It features a form with dropdown menus for 'Campus' (TagusPark), 'Curso' (LEE), 'Cadeira' (BD), and 'Avaliação' (Teste 1). Below the form is a table with columns for 'N.º', 'Aluno', 'Turma', and 'Nota'. The table lists five students with their respective IDs, names, and class numbers. A 'Publicar Pauta' button is located at the bottom right of the table. The footer contains copyright information for G7 © 2013 and the SIRS PROJECT.

N.º	Aluno	Turma	Nota
66047	João Pedro Rocha Pinho	LEIC-T 2006	
66998	Hugo Miguel Vieira Gonçalves	MEIC-T 2006	
67073	Rita Marques Tomé	MEIC-T 2006	
68121	Andreia Filipa Caseiro dos Santos	MEIC-T 2006	
68135	Diogo Manuel Gomes Alves	LEIC-T 2006	



The screenshot shows the 'Online Grades' web application interface. The top navigation bar includes the application name and the date '13 DE DEZEMBRO DE 2013'. The main content area is titled 'Visualização de Pautas Online' (Online Grade Visualization). It features a form with dropdown menus for 'Campus' (TagusPark), 'Curso' (LEE), 'Cadeira' (BD), and 'Avaliação' (Teste 1), along with a 'Pesquisar' button. Below the form is a table with columns for 'ID', 'ProfessorID', 'Campus', 'Course', 'Class', 'EvaluationType', and a link to 'Ver Notas'. The table lists five publications with their respective IDs, professor IDs, and details. The footer contains copyright information for G7 © 2013 and the SIRS PROJECT.

ID	ProfessorID	Campus	Course	Class	EvaluationType	Ver Notas
1	0	TagusPark	LEE	BD	Teste 1	<a href="#">Ver Notas</a>
2	0	TagusPark	LEE	BD	Teste 1	<a href="#">Ver Notas</a>
1002	0	TagusPark	LEE	BD	Teste 1	<a href="#">Ver Notas</a>
1003	0	TagusPark	LEE	BD	Teste 1	<a href="#">Ver Notas</a>
2002	0	TagusPark	LEE	BD	Teste 1	<a href="#">Ver Notas</a>