



Fundação para a Computação Científica Nacional
Foundation for National Scientific Computing

Serviço de mobilidade e-U Campus Virtual

Termos e condições de utilização

FCCN
Março de 2005



POS_ CONHECIMENTO

Programa Operacional Sociedade do Conhecimento



Portugal em Acção



UNIÃO EUROPEIA
FEDER

ÍNDICE

| | |
|--|----|
| Introdução e enquadramento | 3 |
| Participantes no processo de mobilidade..... | 4 |
| Instituição de origem | 5 |
| Instituição visitada..... | 6 |
| Utilizador em mobilidade | 7 |
| NREN..... | 8 |
| ANEXO 1 – Modelo de <i>accounting</i> | 9 |
| ANEXO 2 – Modelo de suporte | 10 |
| ANEXO 3 – Serviços mínimos | 11 |

INTRODUÇÃO E ENQUADRAMENTO

A rede e-U Campus Virtual é uma iniciativa integrada lançada em 2003 no âmbito do Plano de Acção para a Sociedade da Informação, cuja coordenação técnica é da responsabilidade da FCCN. A e-U envolve Serviços, Conteúdos, Aplicações e Rede de Comunicações Móveis (dentro e fora da Universidade) para utilizadores das instituições aderentes, incentivando e facilitando a produção, acesso e partilha de conhecimento entre estas.

Os principais objectivos da rede e-U Campus Virtual são:

- Fomentar a criação de serviços universitários "on-line";
- Produção e partilha de conteúdos académicos;
- Criação de comunidades do Ensino Superior, com três componentes específicas:
 1. Aposta na criação de Serviços e Conteúdos, disponíveis em qualquer hora, de qualquer lugar;
 2. Massificação da utilização de computadores portáteis ("um para cada", aluno/professor);
 3. Acesso à Internet e Intranet fora e dentro da Universidade.

Este documento tem como objectivo a definição dos termos e condições de participação e utilização para a rede e-U Campus Virtual, nomeadamente para o seu serviço de mobilidade, a aplicar uniforme e igualmente a todos os participantes no processo de mobilidade a saber: utilizador em mobilidade, instituição de origem e instituição visitada.

As disposições constantes neste documento em caso algum se sobrepõem às que resultam da Carta do utilizador da RCTS. Esta política deverá ser seguida por todas as instituições aderentes, quer se apresentem no papel de instituição visitada, quer no papel de instituição de origem, devendo mesmo ser reflectida no documento que seja adoptado internamente para a definição das políticas de utilização desta Rede pelos utilizadores finais.

PARTICIPANTES NO PROCESSO DE MOBILIDADE

Para efeitos do presente documento, são considerados participantes no processo de mobilidade os abaixo definidos:

UTILIZADOR EM MOBILIDADE – Utilizador que visita uma instituição e espera obter os serviços da rede e-U, Campus Virtual.

UTILIZADOR RESIDENTE – Utilizador registado que utiliza os serviços da rede e-U Campus Virtual na sua instituição de origem.

INSTITUIÇÃO DE ORIGEM – Instituição onde o utilizador visitante está registado e para onde são solicitados os pedidos de autenticação locais ou remotos relativos a esse utilizador.

INSTITUIÇÃO VISITADA – A instituição onde o utilizador visitante se encontra e onde espera obter os serviços de mobilidade da rede e-U.

NREN - *National Research and Education Network* – Rede Nacional de Investigação e Ensino. Em Portugal a instituição que gere e opera esta rede (a RCTS) é a FCCN.

INSTITUIÇÃO DE ORIGEM

Ao abrigo da adesão ao e-U, Campus Virtual, a INSTITUIÇÃO DE ORIGEM do UTILIZADOR EM MOBILIDADE, deverá seguir os seguintes procedimentos:

1. Fornecer credenciais válidas para os seus utilizadores autorizados e apenas para estes.
2. Elaborar e divulgar junto dos seus utilizadores um documento que defina uma AUP (Acceptable User Policy) o qual deve incluir, designadamente, a descrição de serviço de mobilidade prestado, as obrigações presentes neste documento com as adaptações que eventualmente se imponham, assim como uma descrição dos contactos e meios de obtenção de informação na instituição sobre questões relativas a esta matéria.
3. Tomar as providências que entenda necessárias e suficientes para que os seus UTILIZADORES EM MOBILIDADE conheçam bem o teor e implicações do documento referido no número anterior
4. Garantir que todos os registos de sessão de autenticação, gerados para um UTILIZADOR EM MOBILIDADE numa INSTITUIÇÃO VISITADA e enviados à INSTITUIÇÃO DE ORIGEM, são armazenados. Durante toda a sessão de autenticação a informação sobre o UTILIZADOR EM MOBILIDADE deve ser mantida o mais correcta e completa possível por forma a permitir a identificação deste, se necessário.
5. Apoiar, técnica e administrativamente, quer os UTILIZADORES RESIDENTES quer os seus UTILIZADORES EM MOBILIDADE numa qualquer INSTITUIÇÃO VISITADA.

INSTITUIÇÃO VISITADA

A INSTITUIÇÃO VISITADA pelo UTILIZADOR EM MOBILIDADE, deverá seguir os seguintes procedimentos:

1. Disponibilizar aos UTILIZADORES EM MOBILIDADE devidamente credenciados e autorizados pela INSTITUIÇÃO DE ORIGEM, pelo menos, os SERVIÇOS MÍNIMOS da rede e-U Campus Virtual.
2. Publicitar, em local adequado, o SERVIÇO DE MOBILIDADE assim como os respectivos termos e condições de utilização. bem como o grau de segurança com que os dados de autenticação são transmitidos.
3. Garantir que o mecanismo de transmissão das credenciais é seguro. Caso isto não seja possível, deve ser garantida a possibilidade ao UTILIZADOR EM MOBILIDADE de iniciar uma sessão segura.
4. Garantir que todos os registos de sessão de autenticação e de sessão de rede, gerados pelo UTILIZADOR EM MOBILIDADE, são armazenados.
5. Enviar informação do início e do fim de sessão para a INSTITUIÇÃO DE ORIGEM. Deve ainda ser tido em conta que toda a informação trocada entre INSTITUIÇÕES (ORIGEM e VISITADA), durante a sessão de autenticação, deve ser a mais correcta e completa possível.
6. Determinar se aplicável, quais os recursos de rede a disponibilizar aos UTILIZADORES EM MOBILIDADE para além dos SERVIÇOS MÍNIMOS estabelecidos para a rede e-U Campus Virtual.
7. Todo o apoio prestado ao UTILIZADOR EM MOBILIDADE deverá ser fornecido pela sua INSTITUIÇÃO DE ORIGEM. Na resposta a uma solicitação de apoio, apenas se deve envolver a INSTITUIÇÃO VISITADA caso se conclua que o eventual problema tem origem nesta, não estando a INSTITUIÇÃO VISITADA obrigada a prestar este apoio.
8. A INSTITUIÇÃO VISITADA poderá bloquear, sempre que tal se justificar, o acesso aos serviços de rede a um UTILIZADOR EM MOBILIDADE, uma instituição ou uma NREN, sendo obrigatória a comunicação à FCCN/CERT.PT (www.cert.pt/) do tipo de bloqueio e das razões que o motivaram. Compete à FCCN/CERT.PT comunicar essa medida e a respectiva motivação à instituição/NREN visada.
9. Caso seja solicitado pelo CERT.PT, deve a INSTITUIÇÃO VISITADA fornecer toda a informação disponível por forma que seja facilitada a identificação da INSTITUIÇÃO DE ORIGEM do UTILIZADOR EM MOBILIDADE envolvido no incidente de segurança.

UTILIZADOR EM MOBILIDADE

O UTILIZADOR EM MOBILIDADE deverá seguir e aceitar os seguintes princípios:

1. O UTILIZADOR é integralmente responsável pela confidencialidade das suas credenciais.
2. Em caso de furto/roubo ou suspeita de perda de confidencialidade das credenciais, é da responsabilidade do UTILIZADOR reportar com a maior brevidade possível esse incidente à sua INSTITUIÇÃO DE ORIGEM, por forma a que sejam canceladas as credenciais em referência e atribuídas novas.
3. Cumprir a AUP fixada e publicitada pela INSTITUIÇÃO VISITADA para a rede e-U Campus Virtual.
4. Todos os UTILIZADORES EM MOBILIDADE devem autenticar-se previamente na sua instituição de origem, por forma a que lhe seja atribuído acesso à rede da INSTITUIÇÃO VISITADA.
5. Os UTILIZADORES EM MOBILIDADE só deverão iniciar tentativas de autenticação depois de certificar que as suas credencias serão transmitidas de forma segura.
6. O UTILIZADOR EM MOBILIDADE deverá estar informado que os recursos de rede que lhe são atribuídos, após a autenticação com sucesso, podem apenas cumprir os parâmetros mínimos definidos para a rede e-U, Campus Virtual não sendo por isso de esperar o mesmo nível de serviço que encontra na sua INSTITUIÇÃO DE ORIGEM.

NREN

No âmbito do serviço de mobilidade e-U Campus Virtual e da rede de mobilidade europeia Eduroam, a FCCN (NREN portuguesa) tem as seguintes responsabilidades:

1. É da responsabilidade da NREN a gestão e manutenção dos servidores de autenticação nacionais.
2. A NREN disponibilizará uma arquitectura de servidores de autenticação nacionais redundante e, concretamente, com mais do que um servidor.
3. A NREN deve ter mecanismos que permitam que a informação relevante recebida pelos servidores de autenticação nacional, e que é reencaminhada para outra instituição se faz de forma inalterada tanto quanto tecnicamente possível.
4. A NREN pode bloquear o acesso à rede aos UTILIZADORES EM MOBILIDADE de uma determinada INSTITUIÇÃO DE ORIGEM nos servidores de autenticação nacionais. Esse bloqueio e suas razões serão comunicadas aos responsáveis pelas instituições intervenientes, designadamente através do CERT.PT.
5. A NREN pode remover uma determinada instituição dos servidores nacionais caso essa instituição incorra deliberadamente no incumprimento da presente AUP.
6. A NREN deve ter mecanismos de monitorização que permitam, designadamente, obter informação sobre o estado dos servidores de autenticação nacional. Os resultados obtidos neste âmbito deverão ser disponibilizados aos interessados, nomeadamente UTILIZADORES EM MOBILIDADE.
7. Não é responsabilidade da NREN garantir a segurança dos dados transmitidos entre um UTILIZADOR EM MOBILIDADE e a sua INSTITUIÇÃO DE ORIGEM. Estes mecanismos devem ser garantidos pelas partes intervenientes no processo, ou seja, o UTILIZADOR EM MOBILIDADE e a sua INSTITUIÇÃO DE ORIGEM.

ANEXO 1 – MODELO DE *ACCOUNTING*

O modelo de confiança entre instituições participantes na rede e-U Campus Virtual, no que se refere à mobilidade de alunos e professores, assenta numa infra-estrutura hierárquica de servidores de autenticação cuja administração é feita de forma distribuída.

Por forma minimizar ou mitigar eventuais problemas segurança inerentes à má utilização de credenciais de utilizadores ou utilização indevida de recursos, importa disponibilizar ferramentas de auditagem, acessíveis aos vários intervenientes no processo de mobilidade, que permitam, caso necessário, identificar de forma inequívoca um determinado utilizador ou instituição.

Este anexo define a informação de registo a transmitir pela INSTITUIÇÃO VISITADA à INSTITUIÇÃO DE ORIGEM na sequência de uma qualquer sessão de utilização por parte de um UTILIZADOR EM MOBILIDADE, assim como as responsabilidades de ambas na retenção desta informação.

Compete à INSTITUIÇÃO VISITADA enviar a informação de *accounting* para a INSTITUIÇÃO DE ORIGEM no início e no fim de cada sessão de um UTILIZADOR EM MOBILIDADE, nomeadamente os registos de *accounting* de *start* e *stop*.

Compete igualmente à INSTITUIÇÃO VISITADA a retenção, por período de 6 meses, dos mesmos registos de autenticação e dos registos de início e fim de sessão de utilização (nível 2 – *accounting* dos *access points*; nível 3 – *accounting* de DHCP).

Compete à INSTITUIÇÃO DE ORIGEM a retenção, por período de 6 meses, dos registos de autenticação e informação de início e fim de sessão dos seus utilizadores.

A INSTITUIÇÃO VISITADA deve garantir, a todo o tempo, a fiabilidade do *logging* de nível 3 para nível 2 e desejavelmente introduzir na infra-estrutura mecanismos de *anti-spoofing* IP.

Os sistemas computacionais das INSTITUIÇÕES VISITADAS E DE ORIGEM, assim como os servidores nacionais de autenticação operados pela FCCN, envolvidos nos registos de *accounting*, terão os seus relógios sincronizados através do NTP – *Network Time Protocol* – utilizando preferencialmente para esse fim os servidores ntp01.fccn.pt e ntp02.fccn.pt.

ANEXO 2 – MODELO DE SUPORTE

Este anexo descreve o modelo de suporte que a NREN fornecerá às instituições ligadas ao projecto e-U Campus Virtual.

1. Os assuntos gerais ou relacionados com a operação da hierarquia de autenticação devem ser enviados para os seguintes contactos:

Correio electrónico: operacao@fccn.pt;
Telefone; +351 21 8 440 101;
Fax: +351 21 8 472 167.

Os serviços prestados são os seguintes:

- Alteração das configurações de acesso afectas a uma instituição (*realms* e servidores de autenticação, *secrets* de RADIUS);
- Remoção de instituição dos proxys nacionais;
- Adição de instituição aos proxys nacionais;
- Coordenação de assuntos técnicos de interesse geral.

2. Os assuntos de segurança devem ser enviados para os seguintes contactos:

Correio electrónico - report@cert.pt;
Telefone: +351 218440177;
FAX: +351 218440185.

Com o objectivo de poder efectuar-se uma comunicação proactiva com as instituições participantes da rede e-U Campus Virtual, estas devem disponibilizar os seguintes dados de contacto:

Instituto Politécnico de Tomar
Gabinete de Informática
Estrada da Serra – Quinta do Contador
249 328207
2300 – 126 Tomar
qi@ipt.pt

Joaquim Pombo
jpombo@ipt.pt

e

Paulo Crispim
pcrispim@ipt.pt

ANEXO 3 – SERVIÇOS MÍNIMOS

Este anexo descreve os SERVIÇOS MÍNIMOS, disponibilizados por todas as instituições da rede e-U Campus virtual, aos quais os UTILIZADORES EM MOBILIDADE devem ter o acesso garantido.

Caso a INSTITUIÇÃO VISITADA disponibilize para os seus utilizadores internos uma classe de serviço superior, é aconselhável que opte por fornecer esse mesmo nível de serviço aos UTILIZADORES EM MOBILIDADE.

De seguida elencam-se os serviços mínimos obrigatórios:

- Serviço IP Público – Atribuição de um endereço IP público a cada UTILIZADOR EM MOBILIDADE;
- Acesso VPN (Virtual Private Network) para fora da INSTITUIÇÃO VISITADA, nomeadamente com as tecnologias IPsec, PPTP, L2TP, sem prejuízo para outras tecnologias existentes ou que venham a existir;
- Acesso a serviços de *messaging*, nomeadamente MSN e skype;
- Serviços de Rede – Acesso de dentro do *hotspot* para fora da INSTITUIÇÃO VISITADA aos seguintes serviços de rede:
 - FTP (porto 20 e 21);
 - HTTP (porto 80);
 - HTTPS (porto 443);
 - IMAP (porto 143);
 - IMAP-SSL (porto 993);
 - POP3 (porto 110);
 - POP3-SSL (porto 995);
 - SMTP e SMTP AUTH (porto 25) pelo menos para os blocos de endereços da RCTS, nomeadamente 139.83.0.0/16; 146.193.0.0/19; 146.193.32.0/19; 146.193.64.0/18; 146.193.128.0/17; 158.162.0.0/18; 158.162.64.0/19; 158.162.96.0/20; 158.162.112.0/21; 158.162.128.0/18; 158.162.192.0/18; 192.12.232.0/24; 192.104.48.0/24; 193.136.0.0/15; 194.117.0.0/20; 194.117.16.0/21; 194.117.32.0/22; 194.117.40.0/22; e 194.210.0.0/16;
 - SSH (porto 22);
 - TELNET (porto 23);
 - SMTPS (porto 465).

FUNDAÇÃO PARA A COMPUTAÇÃO CIENTÍFICA NACIONAL, FCCN, instituição privada sem fins lucrativos declarada de utilidade pública, com sede na Av. do Brasil, n.º 101, em Lisboa, representada pelo Prof. Pedro Veiga e pelo Prof. José Fernandes, na qualidade, respectivamente, de Presidente e Vogal do Conselho Executivo
e

Instituto Politécnico de Tomar, Estrada da Serra Quinta do Contador, 2300 Tomar, representado pelo Professor António Pires da Silva na qualidade de Vice-Presidente

Declaram compreender e aceitar integralmente os termos e condições do Serviço de mobilidade e-U Campus Virtual, acima descritos.

Tomar, 14 de Julho de 2005

(Assinatura)

(Assinatura)

Dados para efeitos do previsto no Anexo 2 – Modelo de Suporte

Nome da instituição Instituto Politécnico de Tomar
Nome de responsável Joaquim Pombo
Endereço Postal Estrada da Serra – Quinta do Contador
Endereço de correio electrónico jpombo@ipt.pt