




Laboratório de Instrumentação e Física Experimental de Partículas

Centro de Calculo – Lisboa

Autoridade Certificadora

Criação e operação
de uma autoridade de
registo.

	<p>Autoridade de Certificação do LIP Criação e Operação de uma AR</p>	<p>Versão 1.0 27/10/2004</p>
--	---	----------------------------------

1. Introdução

O Laboratório de Instrumentação e Física Experimental de Partículas (LIP) opera uma autoridade certificadora (AC) que emite certificados digitais para aplicações científicas não comerciais. O objectivo principal da autoridade certificadora do LIP é a emissão de certificados para computação grid.


Este documento descreve o processo de criação e operação de uma autoridade de registo (AR).

2. Considerações iniciais sobre o documento

- Este documento destina-se a:
 - Administradores e operadores da AC;
 - Administradores e operadores das ARs.
- Este documento pode ser actualizado para reflectir alterações nos procedimentos descritos.
- A AC anunciará com antecedência às ARs qualquer alteração aos procedimentos.
- A ultima versão deste documento encontra-se disponível no servidor Web da autoridade certificadora <http://www.lip.pt/ca>.
- A AC do LIP rege-se pelas normas descritas no documento “LIP CA Certificate Policy and Certificate Practice Statement” disponível no servidor Web da autoridade certificadora <http://www.lip.pt/ca>.
- Este documento deve ser considerado uma extensão operacional do documento “LIP CA Certificate Policy and Certificate Practice Statement”, não podendo contrariar as regras aí descritas.
- A leitura deste documento pressupõe o conhecimento anterior do documento “LIP CA Certificate Policy and Certificate Practice Statement”.

3. Considerações iniciais sobre a Autoridade Certificadora do LIP

- A AC emite certificados digitais X.509 para aplicações científicas não comerciais.
- Os certificados emitidos pela AC não dão acesso por si só a qualquer tipo de infra-estruturas ou serviços.
- A AC emite certificados a instituições académicas Portuguesas:
 - Universidades;
 - Centros de investigação públicos ou privados sem fins lucrativos.
- Os certificados podem ser emitidos aos seguintes tipos de entidades ligadas às instituições supra mencionadas.
 - Funcionários, investigadores ou estudantes;
 - Sistemas informáticos ou serviços informáticos;
 - Entidades legais.

	<p>Autoridade de Certificação do LIP Criação e Operação de uma AR</p>	<p>Versão 1.0 27/10/2004</p>
--	---	----------------------------------

4. Definições

- AC: Autoridade Certificadora. Entidade que emite certificados baseados em pedidos que são verificados e aprovados pelas ARs. Uma AC possui um administrador responsável e um ou mais operadores.
- AR: Autoridade de Registo. Entidade que verifica e aprova (ou rejeita) os pedidos de certificados. Uma RA possui um administrador responsável e um ou mais operadores.
- Procedimento de operação da AR: Documento que especifica os detalhes da operação de uma AR. Este documento é especificado pelo administrador da AR e aprovado pelo administrador da AC. O documento em vigor tem de estar disponível no servidor Web da AR.
- Utilizador: A pessoa que efectua um pedido de certificado.
- Entidade: Refere-se a uma pessoa, máquina ou serviço identificada por um certificado.
- Organização: Neste documento refere-se a uma organização “física” onde uma AR opera ou pretende operar. Em princípio a AR de uma dada instituição aprova pedidos de certificados de utilizadores da mesma instituição. Uma instituição é normalmente uma Universidade ou centro de investigação.
- Autoridade local: É a pessoa oficialmente responsável pelo departamento ou unidade que opera uma AR dentro de uma organização, possuindo para tal um mandato oficial da organização. Pode ser por exemplo o director do serviço de informática, centro de cálculo ou departamento de informática.
- DN: Distinguish Name. Nome único num certificado. Cada certificado possui no seu interior dois DNs um que permite saber qual a AC que emitiu o certificado e outro que corresponde ao sistema, serviço ou pessoa o qual o certificado identifica.

5. Nomes e certificados


A AC do LIP emite certificados que possuem um DN com um prefixo de “/C=PT/O=LIPCA/*”. Assinando apenas certificados com este prefixo permite garantir que os certificados emitidos pela AC do LIP não possuem nomes que estejam ou possam vir a estar em conflito com nomes de outros certificados emitidos por outras ACs. Este prefixo define assim o espaço de nomes que a AC do LIP pode assinar.

O certificado da Autoridade Certificadora propriamente dito possui um DN igual a “/C=PT/O=LIPCA/CN=LIP Certification Authority”. Este DN aparece em todos os certificados emitidos identificando assim a AC que os emitiu.

Para além do prefixo existe um formato para os DNs que podem ser usados em certificados emitidos pela AC do LIP. Este formato é o seguinte:

/C=PT/O=LIPCA/O=organização/OU=sub-organização/CN=nome

No DN o componente *organização* corresponde a uma instituição académica com existência legal à qual a pessoa, serviço ou sistema estão ligados. Na

	Autoridade de Certificação do LIP Criação e Operação de uma AR	Versão 1.0 27/10/2004
--	---	--------------------------

maior parte dos casos o componente *organização* deverá identificar também a autoridade de registo, uma vez que cada instituição deverá possuir a sua própria AR.

O componente *sub-organização* refere-se a um grupo, secção, departamento ou centro dentro de uma data organização. O componente *sub-organização* poderá não existir. Este componente existe apenas para simplificar a identificação das entidades certificadas ou a certificar. A AR de uma organização poderá validar certificados para varias *sub-organizações*. Poderá acontecer que uma empresa ou instituição não académica colabore com uma dada instituição académica numa actividade académica ou de investigação, nestes casos podem ser emitidos certificados à instituição não académica. O nome destes certificados deverá conter uma *sub-organização* com um nome que identifique a empresa.

Finalmente o componente *nome* serve para identificar claramente a entidade (pessoa, sistema, serviço). O nome deve ser obténivel do nome real da entidade. No caso de uma pessoa deverá ser o seu nome completo ou parte substancial deste (no mínimo um nome próprio e um nome de família) de forma a minimizar duplicações, caso haja duplicações um número deverá ser acrescentado no fim do nome. No caso de um sistema deverá ser o nome completo do sistema com o domínio DNS. Os nomes não devem conter títulos como Doutor, Dr ou Professor, Prof ou outros.

Exemplos:

Duas pessoas como mesmo nome:

/C=PT/O=LIPCA/O=IST/CN=José Pedro Mendonça

/C=PT/O=LIPCA/O=IST/CN=José Pedro Mendonça 0001

Um sistema no Instituto Superior técnico:

/C=PT/O=LIPCA/O=IST/CN=alfa.ist.utl.pt

Um sistema do LIP no seu centro de Coimbra situado na universidade:


/C=PT/O=LIPCA/O=LIP/OU=Coimbra/CN=ravel.lipc.fis.uc.pt

Um certificado para um servidor/serviço LDAP:

/C=PT/O=LIPCA/O=FEUP/CN=ldap/mars.fe.up.pt

Os caracteres validos num DN são:

‘ ‘ ‘0’ – ‘9’ ‘a’ – ‘z’ ‘A’ – ‘Z’ ‘(’ ‘)’ ‘-’

	Autoridade de Certificação do LIP Criação e Operação de uma AR	Versão 1.0 27/10/2004
--	---	--------------------------

6. Criação de uma AR

6.1. Quem decide quando e onde criar uma AR

A criação de uma AR ocorre geralmente da necessidade por parte de uma instituição de certificados para actividades de computação grid. Também poderá ter origem na necessidade de precaver uma futura necessidade nesta área. É assim da inteira responsabilidade de cada instituição pedir a criação de uma AR quando o assim desejar. Lembra-se que deverá apenas existir uma AR por instituição.

6.2. Como efectuar o pedido de criação de uma AR

Um pedido oficial de criação da AR deverá ser enviado por carta em papel timbrado da instituição requerente e carimbado com o carimbo da instituição, devendo ainda ser assinado por um membro da instituição com autoridade para vincular e representar legalmente a instituição (autoridade local) em relação ao pedido. Esta pessoa poderá ser por exemplo o director do serviço ou centro de informática. O pedido deverá ser efectuado usando a minuta em anexo. Este pedido deverá conter o nome a usar no componente organização e se for caso disso sub-organização juntamente com o contacto do futuro administrador da AR.

6.3. O que é um administrador de uma AR

O administrador da AR é a pessoa que é no dia a dia responsável pelo funcionamento da AR. O administrador é também o ponto de contacto da organização com a autoridade de certificação. Tipicamente poderá ser por exemplo um administrador de sistemas ou professor. O administrador da AR deverá ser sempre um funcionário da organização e possuir bons conhecimentos técnicos sobre certificados X.509 e segurança. O administrador é ainda responsável por:

- definir com a ajuda e aprovação da AC o plano de operação da AR que deverá ficar registado num documento.
- nomear um máximo de dois operadores.

6.4. O que é um operador de uma AR

O operador é quem de facto efectua as verificações de identidade e cancelamento de certificados no dia a dia, pondo assim em prática o plano de operação da AR. Deverão existir dois operadores para redundância em caso de férias ou doença. Mais de dois operadores não é recomendável já que estes terão de aprovar certificados no mesmo espaço e mais do que um operador poderá levar à aprovação de pedidos com nomes duplicados/iguais. A nomeação dos operadores deverá ser enviada por carta em papel timbrado da instituição requerente e carimbado com o carimbo da instituição, devendo ainda ser assinado pelo administrador. Os operadores deverão ser preferencialmente funcionários da organização. O administrador da AR também pode ser operador.

6.5. Como funciona a verificação de um pedido de certificado

Para validar um pedido de certificado a AR deve.

Para um certificado pessoal:


1. Verificar se o nome da organização e sub-organização estão correctos.
2. Verificar se o nome no certificado corresponde ao nome real da pessoa.
3. Para um certificado pessoal verificar se o Email no certificado corresponde ao Email da pessoa.
4. Verificar se a identidade da pessoa corresponde à identidade no documento oficial apresentado pelo (ex. BI ou outro). O documento de identificação a apresentar deverá ser valido e possuir uma fotografia actualizada.
5. Verificar se a pessoa é de facto um membro da organização.
6. Verificar se o documento de registo está correctamente preenchido em particular o “challenge” de verificação de posse da chave privada (ainda não implementado).

Para um certificado de serviço ou servidor:

1. Verificar se o nome da organização e sub-organização estão correctos.
2. Verificar se o nome no certificado corresponde ao nome real do serviço ou sistema. O sistema deve existir.
3. Para um certificado de serviço ou sistema verificar se o nome do servidor no campo DNS do certificado corresponde ao verdadeiro nome DNS do servidor.
4. Verificar se o sistema pertence ou está sobre o controlo da organização.
5. Verificar a identidade de quem pede o certificado.
6. Verificar se a pessoa que pediu o certificado pertence de facto à organização.
7. Verificar se a pessoa que pede o certificado tem legitimidade para o fazer.
8. Verificar se o documento de registo está correctamente preenchido em particular o “challenge” de verificação de posse da chave privada (ainda não implementado).

Para um certificado de serviço ou servidor a verificação de identidade e relação com a organização de quem pede não é necessária caso prove possuir um certificado pessoal verificado e aprovado pela AR.

O requerente deverá dirigir-se à AR com um documento de identificação aceitável e com o formulário de registo devidamente preenchido. Este formulário possui alguma informação sobre o requerente e a sua assinatura. No final a AR deverá igualmente preencher a informação referente ao local e data da verificação e se o pedido de emissão do certificado foi aceite. Este formulário deve ser guardado pela AR.


	<p>Autoridade de Certificação do LIP Criação e Operação de uma AR</p>	<p>Versão 1.0 27/10/2004</p>
--	---	----------------------------------

6.6. O que é o plano de operação

A operação de uma AR está subordinada às regras de operação da AC definidas no seu “Certification Policy and Certification Practice Statement” (CP/CPS). Este documento define de uma forma geral como a AC opera e como as suas subordinadas AR devem efectuar as suas operações de verificação das entidades que pedem certificados, pedem renovação de certificados existentes ou pedem cancelamento. Existe alguma margem de manobra para a operação de uma AR dentro das limitações impostas pelo CP/CPS.

O plano de operação deverá especificar:

- O nome da organização a usar nos certificados.
- O nome de todas as sub-organizações para as quais a AR opera.
- Contacto da AR:
 - Morada postal;
 - Fax;
 - Telefone;
 - Email;
 - Horário de funcionamento.
- Como é verificada a identidade de uma pessoal:
 - Que documento ou documentos são aceites como prova de identidade quando a entidade é uma pessoa:
 - Bilhete de identidade;
 - Passaporte;
 - Carta de condução.
 - É requerida a presença física ou o contacto pode ser telefónico com envio dos documentos de identificação via Fax, neste caso como é obtido o número de telefone e em que moldes são feitos os contactos.
- Como é verificada a identidade de um sistema ou serviço:
 - Que método é usado para verificar que uma maquina existe;
 - Que método é usado para verificar que quem pede o certificado tem o direito de fazer-lo;
 - Como são tratadas eventuais disputas.
- Como é verificada a ligação de uma pessoa à organização:
 - Que tipos de relações com a organização são aceites:
 - Estudantes;
 - Professores;
 - Funcionários em geral;
 - Membros de um dado departamento ou projecto;
 - Investigadores;
 - Pessoal contratado;
 - Etc.

	<p>Autoridade de Certificação do LIP Criação e Operação de uma AR</p>	<p>Versão 1.0 27/10/2004</p>
--	---	----------------------------------

- Que tipo de métodos são usados e aceites para verificar a ligação com a organização:
 - Cartão de estudante;
 - Cartão de funcionário;
 - Declaração;
 - Conhecimento pessoal de um operador da AR;
 - Base de dados da organização;
 - Lista de pessoal ou alunos;
 - Lista telefónica da organização;
 - Etc.
- Como é verificada a ligação de um sistema ou serviço à organização:
 - Que tipos de relações com a organização são aceites:
 - Controle físico da maquina ou serviço;
 - Controle administrativo da maquina ou serviço;
 - Posse legal da maquina ou serviço;
 - Existência da maquina nas instalações da organização;
 - Existência da maquina no domínio DNS da organização;
 - Etc.
 - Que tipo de métodos são usados e aceites para verificar a ligação com a organização:
 - Consulta no DNS;
 - Consulta numa base de dados de sistemas;
 - Consulta com os departamentos ou secções envolvidos;
 - Etc.
- Especificar sanções aplicáveis (se existirem) pela AR aos membros da instituição em a caso do não cumprimento das obrigações definidas na CP/CPS por parte do subscritor.


6.7. Obrigações da uma AR

Em relação à CP/CPS da AC:

- Ler e aceitar as políticas e procedimentos especificados na CP/CPS.
- Acordar com a AC o conjunto de regras de operação e linhas directivas que governam a operação da AR. Estas regras têm de estar de acordo com a CP/CPS.
- Acordar com a AC a comunidade de utilizadores para os quais a AR está autorizada a operar.

Em relação à emissão e revogação de certificados:

- Seguir os procedimentos descritos na CP/CPS e plano de operação da AR para a validação de pedidos.
- Verificar que os requerentes e sujeitos de certificados obedecem aos requisitos expressos nos documentos CP/CPS CPS e plano de operação da AR.
- Autenticar os requerentes e os sujeitos dos pedidos de acordo com as regras descritas nos documentos CP/CPS CPS e plano de operação da AR.

	<p>Autoridade de Certificação do LIP Criação e Operação de uma AR</p>	<p>Versão 1.0 27/10/2004</p>
--	---	----------------------------------

- Verificar que os requerentes estão em posse da chave privada correspondente ao certificado (ainda não implementado).
- Notificar a AR sobre o resultado de cada validação usando um meio seguro (presentemente este processo é implementado através da interface “Web” da AC).

Em relação ao arquivo de dados:

- Manter um registo de todas as validações de pedidos efectuadas.
- Permitir o acesso da AC aos logs e documentos referentes a validações efectuadas.
- Manter um registo dos acordos para disponibilização de informação confidencial aos administradores de sites e organizações virtuais.

Em relação à privacidade:

- Obter e manter o registo apenas da informação essencial para a realização das suas funções.
- Proteger a informação confidencial contra acesso indevido.

Outras obrigações:

- Escolher o seu próprio pessoal e disponibilizar condições para que este opere a AR de acordo com as regras estabelecidas na CP/CPS e plano de operação da AR.