

**Cover sheet for proposals**  
**(NB: All sections must be completed)**

**JISC Circular 6/02: JISC programme in authentication, authorisation and accounting**

<b>Name of lead institution/organisation</b>	<b>London School of Economics &amp; Political Science</b>
<b>List project partners (if none, please enter none)</b>	none
<b>Name of proposed project</b>	<b>SECURe</b>
<b>Full contact details for primary contact</b>	
<b>Name:</b>	<b>John Paschoud</b>
<b>Position:</b>	<b>Projects Manager</b>
<b>Email:</b>	<b>j.paschoud@lse.ac.uk</b>
<b>Address:</b>	<b>LSE Library, 10 Portugal Street, London WC2A 2HD</b>
<b>Tel:</b>	<b>020 7955 6129</b>
<b>Fax:</b>	<b>020 7955 7454</b>
<b>Programme area(s) of proposal</b>	
(a) particularly: economics and management of large-scale certificate use, on public-access workstations and with mobile users in typical university environments	
(b) focused on efficient certificate management	
(d) Shibboleth-based cross-domain access management, to include commercial resource suppliers	
<b>Length of project</b>	<b>21 months</b>
(in two semi-autonomous phases of 12 months and 9 months)	
<b>Project start date (earliest start is 1<sup>st</sup> October 2002)</b>	<b>1<sup>st</sup> November 2002</b>
<b>Total cost to the JISC over life of project</b>	<b>£163,500</b>
<b>Cost of proposal to the JISC in each academic year (1 August – 31 July)</b>	
<b>AY 2002/3: £73,100</b>	
<b>AY 2003/4: £90,400</b>	
<b>Outline project description</b>	
This proposal addresses two key strands of the Call, and the wider Sparta requirements for next-generation access management, to achieve:	
(1) An institution-wide deployment of PKI and authentication using personal digital certificates, establishing management approaches to the operation of Certificate Authority services, and several solutions to the problems posed by mobile users and shared workstations.	
(2) Use of the infrastructure created by (1) to enable the development and operational use of Web services and directory components for cross-domain access management, implementing essential 'Shared Services' elements of the JISC Information Environment. Authorisation will be based on extension of the first UK Shibboleth pilot (at LSE) to replace existing access control methods for resources hosted by commercial suppliers such as EBSCO and Elsevier.	
<b>Names and contact details of any additional contacts</b>	
none	

## A. Introduction

This proposal for Project **SECURE** (Secure Environment for Certificated Use of Resources) addresses two key strands of the Call, and the wider Sparta requirements for next-generation access management, to achieve solutions to a range of authentication and authorisation issues, in particular the problems posed by mobile users and the use of shared workstations, via:

- An institution-wide deployment of PKI and authentication using personal digital certificates.
- The creation and operational use of Web services and directory components to enable cross-domain access management, implementing essential ‘shared services’ elements of the JISC Information Environment.

SECURE will build on existing JISC investment in tools and infrastructure, in the ANGEL Project and the pilot installation of Shibboleth software at LSE. Both elements of the project will be fully evaluated, documented and disseminated to the HE/FE community as full-scale models for other institutional deployments of certificate-based authentication and authorisation.

Because the project is seeking to address both short-term management issues, and long-term technical problems (acknowledged as “most challenging” by JISC), it is realistically timetabled over a period of 21 months in total, starting in November 2002.

Inevitably, a number of technical or proprietary terms and acronyms have been used in this proposal, which will be familiar to some (but not all) intended readers of this document. A glossary of these with definitive references where appropriate has been appended.

## B. Project description

### **Background: related work contributing to SECURE**

The SECURE project will make use of previous work (funded internally by LSE) to develop the award-winning LSE For You institutional portal. In addition to providing access to the primary institutional database resources and user profiling data, ‘LSE For You’ is an operational information service that is already frequently used by most members the LSE user community, supporting peaks of up to 10,000 user accesses per day.

Original software developed (and still under development) by the JISC-funded ANGEL Project will be used, and extended where necessary to provide the middleware components between proprietary systems, services and database configurations, and open standards for interoperability with external services and resources. SECURE will also act as a practical testbed for the “UK-HE Roles Namespace” specification (based on the eduPerson LDAP profile) that has been developed by the ANGEL Project.

A number of information resource navigation services for end-users of the LSE Library (both ‘known’ LSE student/staff members, and external users of the Library) will be adapted to use the authentication and authorisation methods implemented by SECURE. Some of these are already using an ANGEL middleware server to manage resource metadata, and it is anticipated that further development of end-user access channels to internal and external

resources managed by the Library will use the same technology, and can therefore contribute to the testing of SECURE by large numbers of users, in real-life situations.

Shibboleth software, developed by the Internet2 Middleware Initiative, will be used as the core of the cross-domain access management required by LSE end-users, extending the small-scale project already funded by JISC at LSE (to pilot and evaluate the installation and configuration of Shibboleth). This will provide JISC (and the Shibboleth development team) with a full-scale institutional trial of the Shibboleth access management model. Commercial resource providers EBSCO and Elsevier have already agreed to participate in trials of Shibboleth, and it is likely that the JISC Data Centre EDINA will also participate. LSE will cooperate with these hosts of information resources (which are already heavily used by LSE Library users), and also with the US universities piloting Shibboleth, to maximise the proportion of resource accesses (driven by genuine user needs) that are mediated using Shibboleth.

Existing components or services for the issue, management and repository of X.509 end-user certificates will be selected. It is likely that a model and software such as that developed by Leeds University in the LURCIS project will be used, but the SECURE project will first evaluate possible alternatives that can be used 'off the shelf' for these functions and will be fully compatible with other components to be used.

The Athens access management service has announced that it will be implementing support for authentication of individual users with X.509 certificates. If possible, SECURE will use these facilities to help outline and test a possible model for transition from the current Athens service to the more sophisticated national infrastructure for F&HE resource access management that is likely to succeed Athens.

The ANGEL Resource Manager (A-RM) already includes facilities, within an enriched collection-level description metadata model, for detailing the licence conditions covering access to (each collection of) resources, and tools for institutional maintenance of such access management metadata, so that it can be used to drive automated decisions on the level of access available to a particular user (i.e. "who can use what, from where").

## **What the SECURE Project will do**

The SECURE project will implement and test a full-scale solution, portable and scaleable to other F&HE institutional environments, to the key problem of achieving fine-grain authorisation of access by all users in an institution to the complete spectrum of relevant information resources. The range of resources must include those under a high degree of institutional control, with relatively high security requirements (such as sensitive staff and student personal data), through to such out-of-domain resources (over which the institution has no direct control) as subscription e-journals to which the institutional library negotiates licensed access for users.

The project will use existing technologies (PKI, X.509 digital certificates, Shibboleth) to implement the necessary authentication infrastructure to support this, on as large a scale as project and institutional resources allow. Ideally this will involve all (approximately 10,000) staff and student members of LSE. This phase of SECURE will focus on documenting and solving the management problems raised by institutional scale deployment of PKI and Certificate Authority services, including appropriate strategies for certificate issue, revocation, and linking the authorisation of certificates with existing registration processes that establish real-world identities of students, staff and other users of campus IT services and managed information resources.

A more experimental element of the SECURE project will explore potential new technologies for solving further problems of fine-grain, cross-domain authorisation, by implementing Web Services to meet the requirements of the newer “shared services” components of the JISC Information Environment, specifically for Resources Directories and Institutional Profiling. It is likely that WSDL, UDDI and SOAP will be relevant protocols, all currently in early stages of adoption to enable a large number of e-commerce developments. Beyond the scope of the ANGEL Project, and included in this strand of SECURE, is further development of the ANGEL Resource Manager (A-RM) server, so that several institutional A-RM servers can inter-operate, offering details of licences held (but not disclosing any commercial or personal confidential information) to other enquiring A-RM servers, so that (for example) a student of institution X may use a workstation in the library of institution Y (e.g. under the terms of the UK Computers Plus scheme), to access resource Z (which she is entitled to do under the licence held by institution X).

‘Mobile users’ pose particular challenges for current access management models. They include those who have exclusive personal use of networked resources via several workstations (such as at home and in an on-campus office), and those who have non-exclusive use of shared workstations (either on-campus, or elsewhere). Schemes such as ‘UK Computers Plus’ (in which LSE is a pilot member) are facilitating the use of managed workstations on the campus of one participating institution, by users who are registered students or staff of another participating institution, creating a further level of complexity.

SECURE will implement a number of potential methods for supporting mobile users, with the intention of testing the viability of supporting a ‘mixed economy’ of co-existing and inter-operable technologies. Subject to initial formative evaluation, these are likely to include a secure certificate-server (possibly based on work done in the Leeds University LURCIS Project), certificates stored on end-user space on network file servers, and (for a limited number of pilot users) key-carrier devices that can be used in both on-campus shared workstations and non-managed workstations off-campus.

All original software components developed within the project will be incorporated in one or more version releases of the ANGEL Server, and will be made available to the F&HE community on an Open Source basis under the GNU General Public Licence. The project will engineer all software produced to ensure that it is interoperable with any standards-compliant external components (such as relational databases, Virtual Learning Environments and Library Management Systems), thus avoiding lock-in to the development path chosen by any specific commercial systems vendor. Where absolutely unavoidable, well-defined and self-contained interfaces will be created to proprietary protocols (or institutional systems configurations that may be specific to LSE), and these will be documented so as to provide a model for future adopters of the software facing similar problems.

The proposed institution-wide scale of the project may appear over-ambitious. However, if institutionally certified (rather than commercially purchased) certificates are used, this can be achieved with a potentially very small incremental cost-per-user (compared to the relatively high once-off cost of setting up Shibboleth components and other servers and infrastructure). This approach will have the benefit of offering LSE as a whole-institution demonstration of the problems, pitfalls and solutions for implementation of the known and necessary technologies of a certificate-based model, including the operation of Certificate Authority (CA) services. The value of this to the community will be not only in the detail of the technologies considered and selected or rejected but in the management and human issues encountered and how they were tackled.

Deliverables to JISC will include a model project plan (based on the 20:20 hindsight gained by our experience during the project) for other HE or FE institutions to follow. Direct impact on the majority of end-users is expected to be minimal - they will merely experience small differences (if any) in their initial sign-on dialogue with the institutional network, and some may notice that the number of subsequent authentication challenges (as they navigate to external access-managed resources) decreases.

A smaller pilot group of users (a few hundred, representing a cross-section of the institutional user profile) will be recruited to trial the use of personal key-carrier devices - 'smart cards', or devices that are functionally compatible (e.g. to PKCS#11) but use an alternative hardware interface such as USB. An early stage of the project will include specification and a competitive procurement process for one or more types of key-carrier device in appropriate quantities. Assessment of the device supplier's willingness and ability to work closely with the project and ensure interoperability of their device with open standards will be a factor in the procurement.

Accessibility of both software and hardware interfaces by all potential users will of course be a consideration in SECURE. LSE employs an Accessibility Officer within the User Support division of IT Services, who is routinely consulted on all changes to user interfaces of online services. Advice and guidance from TechDis is also sought when needed.

An essential element of the Project Plan will be the institutional evaluation, including retrospective costing and cost-benefit analysis, of all independent elements of the new access management infrastructure created by the project, leading to a business decision on which elements should continue to be sustained as fully operational support services for the LSE end-user community.

## **Outline Project Timetable**

### **Phase 1: Institution-wide Authentication Infrastructure**

Phase 1 of SECURE will start in November 2002 and be completed in October 2003, with an evaluation of the costs, benefits and sustainability of the certificate-based authentication infrastructure. An institutional decision will be made based on this evaluation, to rely on using all or some of the facilities created, and to withdraw some or all existing access management methods.

### **Phase 2: Access Management for Cross-domain Resources**

Phase 2 of the project (November 2003 to July 2004) will focus on using the authentication environment created by phase 1 to develop improved authorisation of access to external information resources, offering users the benefit of reduced authentication challenges and implementing 'shared services' identified in models of the JISC Information Environment. During phase 2, longer-term issues arising from management and maintenance of the certificate-based services (such as certificate revocation and key-carrier losses) will also be dealt with and documented.

**Timetable of activities (start-month) & deliverables (due month)**

1	Nov-02	<u>Project Plan</u> ; Audit of existing data/directory resources; Review of parallel projects and case-studies; <u>Specification for key-carrier procurement</u> ; Public SECURE website;
2	Dec-02	Key-carrier procurement; Assessment of alternative products for CA management, key-repository; Implement required directory attributes;
3	Jan-03	<u>Review of parallel projects</u> ; Key-carrier decision & purchase; Recruit key-carrier pilot group;
4	Feb-03	Negotiate Shibboleth access with EBSCO, Elsevier, JSTOR, EDINA and other potential external resource suppliers;
5	Mar-03	Implement CA, issuing, revocation services; Implement key-carrier interfaces;
6	Apr-03	Develop institutional (resource license) profiling service;
7	May-03	
8	Jun-03	Preparation for full rollout of PKI/CA services;
9	Jul-03	
10	Aug-03	<u>Evaluation of infrastructure</u> ; Reporting to JISC & LSE committees
11	Sep-03	Decision by LSE on sustaining PKI infrastructure;
12	Oct-03	Full rollout of PKI/CA services;
13	Nov-03	Design shared-services model;
14	Dec-03	
15	Jan-04	Security evaluation of cross-domain communications;
16	Feb-04	<u>Assessment of key-carrier product(s) and interfaces</u> ;
17	Mar-04	<u>Published JISC IE Shared-services model</u> ; <u>Beta-release of IE shared services</u> to other institutional users;
18	Apr-04	<u>Evaluation of long-term CA issues</u> ; Reporting to JISC & LSE committees
19	May-04	<u>Software package release</u> ;
20	Jun-04	<u>Final evaluation report</u> ;
21	Jul-04	Decision by LSE on full-cost adoption of PKI infrastructure;

**Details of Deliverables**

The following deliverables from SECURE will be made available to JISC, and published for use by the HE/FE community:

Project Plan: will re-assess timetable, detailing responsibilities and dependencies.

Specification for key-carrier procurement: formal document in invitation to tender, re-usable in procurements by other institutions.

Review of parallel projects: findings of research into available literature and online information, from projects worldwide in academic, government and commercial sectors that are dealing with similar technologies and management issues.

Evaluation of infrastructure: costs, benefits, sustainability and security issues; generalised where possible for re-use.

Assessment of key-carrier product(s) and interfaces: comparative evaluation-in-use of technology components that may be selected by other institutions.

Published JISC IE Shared-services model: detailed pre-build design for software components that will implement the current (conceptual) model; comment and review will be actively sought from the community.

Beta-release of IE shared services: Web services components available online to other '.ac.uk' institutional users; software available on beta-test basis to other institutions that wish to implement JISC IE-compatible profiles and directories.

Evaluation of long-term CA issues: report on longer-term management and maintenance issues arising from PKI infrastructure and institutional Certificate Authority services.

Software package release: Web services components available online; software available in packaged and documented form to other institutions that wish to implement JISC IE-compatible profiles and directories.

Final evaluation report: report to JISC and LSE committees, undertaken by a consultant external to the SECURE project.

In addition to the deliverables listed, the project would expect to be liaising with and reporting routinely to JISC Programme Managers on progress, expenditure and joint activities with other relevant projects.

## **Project Governance and Evaluation**

An Operational Working Group comprising representatives from all LSE service departments involved in SECURE, with invited representatives of academic staff and student end-users, will meet monthly (at least in the first 12-month phase of the project) to review progress against the plan and timetable, and authorise changes to the plan where necessary. Records of these meetings will be circulated internally to all interested parties, and can also be made available to specific JISC programme management staff.

An institutional Project Steering Committee to be chaired by the Librarian and Director of Information Services will provide high-level oversight of the project, and will meet once each academic term. A JISC representative will be invited to join the Steering Committee, and invitations will also be made to end-user representatives of LSE staff and students, and to interested parties from at least two other HE/FE institutions, to assist in monitoring the portability of models and tools developed by SECURE.

It is hoped to appoint an independent evaluator of the environment created by SECURE. A nominal budget has been allowed for this, and the Computer Security Research Centre at LSE and the Internet2 Middleware Architecture Committee for Education will be consulted to identify a suitable individual or organisation.

In addition to these formal structures, it is anticipated that LSE staff involved in the project will maintain close contact with, and seek advice from appropriate JISC staff, and liaise with

other relevant JISC projects to ensure that the project is continuing to adopt or develop technical models and standards that will be applicable to the whole of the HE/FE community.

## **Dissemination**

Apart from publication of the formal deliverables, the SECURE project team (and LSE colleagues who are more peripherally involved) will actively seek opportunities to disseminate information and experience from the project, in presentations and publications aimed at appropriate target audiences. All of the key personnel to be involved are experienced speakers and writers, and are active in cross-organisational dialogue with their professional peers.

Previous national and international projects in which LSE has played a lead role have impressive track records of dissemination: The HeadLine Project acted as co-ordinator for events promoting the whole of the JISC eLib Programme to the academic library community. A total of 18 public presentations about LSE For You have been made in the last 6 months in Britain and Europe. The ANGEL Project is currently engaged in organising (at the request of JISC) a national workshop for institutional library and IT service policy-makers dealing with the changing technologies of access management.

SECURE will establish a public Web presence, strongly linked to that of the ANGEL Project. It will also make use of the ANGEL Technology-Watch Web service, and will continue to maintain this public information service after the scheduled termination of ANGEL (in February 2003).

## C. Budget

Project manager	in AY	2002/3	0.4 fte	for	9 months:	£12,000
Database/Webservices developer (BSS)	in AY	2002/3	0.4 fte	for	9 months:	£12,000
ANGEL/Shib developer (Lib)	in AY	2002/3	0.4 fte	for	9 months:	£11,700
LDAP/Exchange systems support (ITS)	in AY	2002/3	0.4 fte	for	9 months:	£12,000
User support/dissemination (ITS or Lib)	in AY	2002/3	0.4 fte	for	9 months:	£11,400
Key-carrier devices (nominal: 500 at £20)	in AY	2002/3				£10,000
Workstation h/w (Shib/Ws dev)	in AY	2002/3				£4,000
Project manager	in AY	2003/4	0.4 fte	for	12 months:	£16,000
Database/Webservices developer (BSS)	in AY	2003/4	0.2 fte	for	12 months:	£8,000
ANGEL/Shib developer (Lib)	in AY	2003/4	0.6 fte	for	12 months:	£23,400
LDAP/Exchange systems support (ITS)	in AY	2003/4	0.2 fte	for	12 months:	£8,000
User support/dissemination (ITS or Lib)	in AY	2003/4	0.6 fte	for	12 months:	£22,800
Server h/w for 1st rollout	in AY	2003/4				£8,000
Dissemination travel	in AY	2003/4				£3,000
Evaluation consultant (nominal: 4days)	in AY	2003/4				£1,200

<b>Total costs requested from JISC</b>	<b>£163,500</b>
(Total in AY 2002/3:	£73,100)
(Total in AY 2003/4:	£90,400)

Institutional support for SECURE will be contributed in the form of senior staff time and all overhead costs for operational management and steering committee activities, hosting of additional Oracle database requirements (including Oracle licensing), standard workstation hardware and software tools used by project staff, and a contribution to anticipated travel costs and staff time for dissemination activities.

## D. Capabilities

The three service departments at LSE that will collaborate to deliver SECURE all have firmly embedded cultures of using project-oriented methods and management to deliver services and change whilst controlling timetables, budgets and quality standards, and in promoting and supporting the use of this approach amongst professional peers. LSE Library recently organised and delivered a one-day training seminar on the use of project management techniques, at the request of the M25 Staff Development Group, which was rated as highly successful by all participants.

The ability of LSE (and of the individual staff to be involved in SECURE) to work effectively within the framework of JISC and similar national project funding bodies can be judged on the records of LSE-led projects such as HeadLine (JISC eLib), ANGEL (JISC IE), and the Charles Booth Online Archive (Research Support Libraries Programme). In all these cases, results have been delivered that were notable in their own right, and also contributed significantly to the national programmes of which they were a part. The project teams involved dealt effectively with adverse circumstances as well as success, and built productive working relationships with teams undertaking other related projects and with funding agency staff.

As a research-led teaching institution, LSE has a highly demanding body of staff and student users of information resources and IT infrastructure, and a corresponding level of competence and responsiveness to user needs is expected of the service departments maintaining these facilities. The impetus to deliver the advanced access management environment proposed by SECURE comes from the requirements of LSE's own users, as well as the changes needed to implement the JISC model of a national Information Environment.

Experience in the technical areas required by SECURE has been gained in the ANGEL Project, the UK pilot of Shibboleth (for which alpha-version software was delivered in July 2002 and is currently being installed at LSE) and from prior work on authentication, authorisation and accounting particularly in the HeadLine and Decomate projects.

## E. Key personnel

The following members of LSE staff will play key roles in SECURE. Other funded posts to deliver the project will be filled by part-time secondment of existing LSE operational or project staff, under their management, thus minimising orientation time at the start of the project and retaining the skills and experience developed after the project has ended.

**Chris Cobb** is Director of Business Systems and Services at LSE. He is a member of the UCISA MISG Committee and a number of DfES consultative and working groups, and is a seasoned Oracle professional with over 12 years in Higher Education. He has been the senior manager responsible for the implementation of 'LSE For You', the institutional information portal that has won UCISA and EUNIS awards for best practice in 2002.

**Christine Cooper** is the Technical Infrastructure Manager in the IT Services Department at LSE and is responsible for the development and operation of the systems and networks which deliver the School's ICT services. She has a strong technical background and considerable project management experience and has been involved in many collaborative projects ranging from the distributed computing environment to the metropolitan area network for Kent. More recently she has been a member of the London MAN Technical Steering Group and is also leading one of the pilot implementations of the UK Computers Plus scheme, which will allow part time students and distance learners to use IT facilities at other institutions.

**John Paschoud** is an Information Systems Engineer and Projects Manager in the LSE Library. He is currently managing the JISC-funded ANGEL Project, involving a consortium led by LSE in partnership with four other universities and the EDINA Data Service. Previously he has managed and undertaken a technical design role in the JISC eLib Programme HeadLine Project, which developed concepts of personal information environments and structured metadata that have contributed to the development of the JISC Information Environment, and he was also responsible for UK participation in the two successful European Decomate projects, from which the software products are now being

commercially marketed as the OCLC iPort system. He has been an IT professional for almost 30 years (including 13 years working in Higher Education), holds a Masters' degree in information systems engineering and is a Chartered Engineer and a Member of the British Computer Society.

**Jean Sykes** is the Librarian and Director of Information Services at LSE, and will act as the senior institutional champion for SECURE, chairing the Steering Committee. Jean was chair of the active M25 Consortium of HE Libraries for two years and has just finished a two-year period as chair of SCONUL (Society of College, National and University Libraries). She is director of the prestigious international social science bibliography, IBSS Online, and has directed a number of successful eLib projects, notably Lamda and M25 Link. She is vice chair of RUGIT (Russell Group of IT Directors) and sits on the Board of the London Metropolitan Network (LMN). Jean also sits on the Steering Committee of the JISC Legal Information Service and, since January 2002, has been a member of the newly established JISC Committee for Content and Services (JCCS).

**Sue Wing** is the User Services Manager in the IT Services Department at LSE. She is responsible for the provision of IT support to academic departments and students. This includes development and support of specialist software applications used in teaching and research, IT training across the School (including computer-based training), IT purchasing, and remote IT support including supporting students connecting to the School's network in Halls of Residence. The LSE's 24 hour IT helpdesk service recently won a UCISA Best Practice award for IT support.

## Appendix A: Glossary

<b>ANGEL</b>	Authenticated, Guided, Networked Environment for Learning'; JISC Information Environment project (Call 5/99); <a href="http://www.angel.ac.uk">http://www.angel.ac.uk</a>
<b>eduPerson</b>	LDAP object class for describing individuals engaged in education; <a href="http://www.educause.edu/eduperson/">http://www.educause.edu/eduperson/</a>
<b>HeadLine</b>	JISC eLib (phase 3) project; <a href="http://www.headline.ac.uk">http://www.headline.ac.uk</a>
<b>Internet2</b>	the Internet2 Project, led by over 190 US universities; <a href="http://www.internet2.edu/">http://www.internet2.edu/</a>
<b>LDAP</b>	Lightweight Directory Access Protocol; defined by a number of publications by the Internet Engineering Task Force, most of which are summarised at <a href="http://www.umich.edu/~dirsvcs/ldap/doc/">http://www.umich.edu/~dirsvcs/ldap/doc/</a>
<b>LSE For You</b>	LSE portal for students and staff; The operational access point for end-users is at <a href="http://www.lse.ac.uk/lseforyou/">http://www.lse.ac.uk/lseforyou/</a>
<b>LURCIS</b>	Leeds User Registration & Certificate Issuing System; JISC Technology Applications Programme project; <a href="http://www.jtap.ac.uk/projects/jtap-595.html">http://www.jtap.ac.uk/projects/jtap-595.html</a>
<b>PKCS#11</b>	Cryptographic Token Interface Standard; an Application Programme Interface; summary of definitive resources at <a href="http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/">http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/</a>
<b>PKI</b>	Public Key Infrastructure; a general term for various management models for dual-key cryptography, including digital certificates;
<b>Shibboleth</b>	a project of Internet2 and the Middleware Architecture for Education; <a href="http://middleware.internet2.edu/shibboleth/">http://middleware.internet2.edu/shibboleth/</a>
<b>SOAP</b>	Simple Object Access Protocol; <a href="http://www.w3.org/TR/SOAP/">http://www.w3.org/TR/SOAP/</a>
<b>UDDI</b>	Universal Description, Discovery and Integration; a particular Web services specification; <a href="http://www.uddi.org/">http://www.uddi.org/</a>
<b>USB</b>	Universal Serial Bus (specification); <a href="http://www.usb.org/">http://www.usb.org/</a>
<b>Web services</b>	generally, machine-to-machine communications using Web protocols; <a href="http://www.w3.org/2002/ws/">http://www.w3.org/2002/ws/</a>
<b>WSDL</b>	Web Services Description Language; <a href="http://www.w3.org/TR/wsdl">http://www.w3.org/TR/wsdl</a>
<b>X.509</b>	Internet Engineering Task Force standard for digital certificates; resources particularly relevant to use in PKI are listed at <a href="http://www.ietf.org/html.charters/pkix-charter.html">http://www.ietf.org/html.charters/pkix-charter.html</a>