

Author:	Sandy Shaw
Date:	22 September 2004
Programme:	Common Services
Committee Funding:	JCIIE and JCSR
Structure:	3 pages
Document Reference:	CMSS: Shaw2

Core Middleware and Shared Services Studies

Feasibility Study for a JISC National Certificate Issuing Service

Contents

Executive Summary	3
1 Scope	5
2 Purpose	6
3 Background	7
4 Goals	8
5 Constraints	9
6 Observations	10
7 Proposals	11
7.1 Short term: single assurance level	11
7.2 Longer term: multiple assurance levels	11
7.3 Two CAs	12
7.4 Why Not Just One CA?	12
7.5 Registration	13
8 Implications for Stakeholders	15
8.1 E-Science	15
8.2 Institutions	15
8.3 JISC	16
8.4 RAL CA	16
9 Technical Requirements	17
10 Division of Responsibility	20
11 Recommendations	21
Appendix A: Vendor Responses	23
A.1 Pre-Filtering	23
A.2 Initial Contacts	23
A.3 Substantive Proposals	24
A.4 Contacts	29

Executive Summary

The primary requirement for a national X.509 certificate-issuing service comes from e-Science. This demand is forecast to rise from about 1,000 certificates in issue now to 20,000 within 3–5 years. Important secondary requirements for certificates arise from secure e-mail and cross-institutional use of secure web servers, including the forthcoming national deployment of the Shibboleth access-control framework.

At present, the e-Science community issues its own certificates from a CA at Rutherford Appleton Laboratory (RAL) and a network of local and regional RAs around the country. At the outset of this project, it was believed that the RAL CA had reached the limit of its capacity. However, the actual capacity limit is now thought to be an order of magnitude greater, at about 10,000.

This increase in capacity gives more time to implement the report's main proposal, to set up two JISC CAs. One would issue medium-assurance certificates acceptable to e-Science. End users would be registered with it either individually by existing e-Science RAs or (at lower cost) in bulk from existing institutional staff and student databases. Bulk registration would be limited to institutions capable of satisfying the Grid Policy Management Authorities that they operate sufficiently rigorous administrative processes for vetting the identities of their members. The second JISC CA would issue basic-assurance certificates. Current e-Science resources would not accept these certificates (though future ones might). The users of this CA would be registered in bulk from any institution's existing databases, populated using current administrative processes. Optionally, a third CA could be set up to allow self-registration by anyone with a valid UK academic e-mail address, thus lowering the barriers to experimentation with cross-institutional use of certificates (e.g., for secure e-mail).

Potential outsourcing suppliers were approached to determine feasibility and indicative pricing for the services described above. There was general agreement that the proposals are feasible, with prices being quoted on the order of £50,000 for set-up, plus annual costs ranging from £50,000 to £300,000 for 20,000 certificates. Set-up here covers only administrative start-up of the new CAs and excludes the additional cost of developing bespoke software to upload bulk registration data from institutions.

The main recommendations are:

To consider moving towards a system of two JISC CAs, basic and medium assurance, as described above.

Given that the RAL CA has greater capacity than was previously thought, discussion should begin between the JISC, the e-Science community, and RAL CA staff about the future role of the RAL CA.

One option would be for the RAL CA to become the proposed medium-assurance JISC CA, extending its remit beyond e-Science to more general H&FE purposes and working with the Grid Policy Management Authorities to assist the creation of the proposed institutional bulk RAs and their acceptance by e-Science, while working to further increase capacity, possibly by outsourcing some of its mechanical functions. In this approach, the proposed basic-assurance CA could either be set up at RAL as an extension of the existing facility or outsourced.

Alternatively, JISC might request formal bids from outsourcing vendors for its own CAs, in the expectation that the RAL CA would be phased out. Note that if the RAL CA were to continue in operation then the JISC certificates could not be used for e-Science purposes, both because in most circumstances international Grid policy only recognises one CA per country and because of the momentum of existing e-Science CA arrangements.

Regardless of the specific arrangements for actual CA operation, it may be desirable to set up a standing policy body, covering e-Science, JISC and other academic users, which could settle certification policy questions and liaise with international policy bodies.

1 Scope

This report has been produced by the TIES II project, funded by the JISC Shared Services and Middleware Studies programmes, to examine the feasibility and costs of a national CA, either entirely outsourced or operated in-house using licensed commercial software. The contents are a basis for discussion and development rather than a full specification.

2 Purpose

The report has three objectives:

- a) to clarify the requirements for a UK national service that will issue X.509 certificates for use both in e-Science and in other areas of higher education;
- b) to communicate the current understanding of requirements back to stakeholders (JISC, e-Science community, university computing services) with a view to eliciting feedback;
- c) to communicate the requirements to potential service providers, with a view to obtaining feedback on feasibility and indicative pricing.

3 Background

Currently, the communities of interest use and obtain X.509 certificates as follows:

- a) E-Science. Identity certificates are currently required for all Grid applications. UK Grid users obtain medium-assurance certificates from the national CA at Rutherford Appleton Laboratory (RAL) by an enrolment method that requires presentation in person of photo-id to a regional or institutional RA.
- b) Secure web servers. Administrators of secure (SSL) web servers obtain the requisite server certificates using a variety of mechanisms: in e-Science from the RAL CA, in other cases from local institutional CAs and in others still, from commercial CAs, including the discounted GlobalSign certificates offered through UKERNA.
- c) Ad-hoc users. Various small groups use X.509 certificates for teaching and research purposes, for example whilst teaching security principles to undergraduate or postgraduate students on computing-related degrees. Local mechanisms are used and there is no national issuing scheme.

At present, certificates are not widely used for:

- d) Client authentication outside e-Science. Athens Access Management, a proprietary centrally operated system, is the currently deployed mechanism for authentication and authorisation of users of services in the JISC Information Environment (JISC IE).
- e) Secure e-mail. There is very limited use of encryption for content confidentiality. Digitally signed e-mail is used more widely, particularly within closed environments, and is also used within e-Science, although many users use PGP rather than X.509 certificates for this purpose.

Current developments in the library world indicate a possible future requirement for substantial numbers of certificates for applications that require digitally signed forms.

JISC previously funded the TIES project to consider practical issues for the widespread use of X.509 client authentication certificates in UK H&FE (see http://edina.ac.uk/projects/ties/ties_23-9.pdf). That report contains background material about the number of certificates that would be required, the current status of certificate interoperability and usability with standard browsers, certificate profiles, and possible approaches to the problem of distributing revocation information (CRLs and OCSP).

As well as providing a replacement for the Athens system, general use of certificates for client authentication would have aligned JISC IE authentication with the technology currently used in e-Science. However, since the end of the TIES project, JISC has taken a strategic decision to deploy Shibboleth for inter-institutional access control. This offers a more open and standards-based approach than Athens. Because Shibboleth delegates responsibility for authentication to individual origin sites and does not mandate any particular authentication technology, institutions may be encouraged to adopt a simpler local single-signon solution integrated with Shibboleth in preference to the use of X.509 for user authentication, though Shibboleth can work with either. Therefore the number of certificates that a national CA will need to issue is likely to be much smaller than the numbers considered by TIES, which were essentially one for every student in the country. In the short to medium term, the main demand for certificates will continue to come from e-Science students and researchers.

4 Goals

The following goals have been identified:

- a) In order to accommodate the expected growth in the number of UK e-Science participants from about 1,500 now to perhaps 20,000 within 3–5 years, the existing capacity limit of the RAL CA, currently thought to be about 10,000 certificates, must be overcome.
- b) Both end-users and RAs perceive the registration procedures required for medium-assurance certification as burdensome and want them to be simplified.
- c) The RAL CA is expensive to operate (an estimate of £220 per certificate has been published). As the number of certificates has grown since then, the cost per certificate has doubtless reduced somewhat but further reductions will be required to make the numbers indicated in (a) feasible.
- d) As e-Science moves from research to service deployment, plans are emerging to migrate the current Grid Support Centre (which includes the RAL CA) to become a Grid Operations Centre, with a view to its funding and control moving towards JISC, analogously to the previous migration of the network infrastructure from research project to JISC-funded operational service.
- e) JISC and Internet2 expect secure e-mail (S/MIME) to drive increased use of certificates as client software improves in functionality and ease of use. One goal of the OASIS PKI action plan announced in February 2004 is to improve interoperability for secure e-mail, among other PKI applications. See <http://www.oasis-open.org/committees/pki/pkiactionplan.pdf>.
- f) The national CA should be capable of issuing certificates:
 - To all e-Science end users, including the anticipated new participants from HE institutions, research institutes and industry partners;
 - To some or all of staff and students at any institution that decides to use X.509 certificates as its local authentication system (including use with Shibboleth);
 - To all institutions which require server certificates for secure SSL-based cross-institutional communication (such as Shibboleth origin and target servers).

This would be preferable to allowing separate institutional CAs to spring up and would provide a natural source of certificates for trusted communication between servers and end-users at different academic institutions.

- g) Some applications require SSL server certificates from a CA whose root certificate is built into standard browsers, to avoid any need for end users to configure their browsers with a new CA root certificate.

5 Constraints

The following constraints apply:

- a) International e-Science collaboration policy permits only one participating CA per country in most circumstances. That CA must apply registration procedures that guarantee the equivalent of medium-level assurance, which involves verification in person of photo-id. This is necessary to provide the level of reassurance required by owners of high-value e-Science resources (national labs, supercomputers, etc.).
- b) Present e-Science practice assumes there is only one class of certificate. There is no provision for some users to have higher-assurance certificates and others (such as students) to have lower-assurance ones. Some e-Science leaders see a need for multiple levels of assurance (although the real requirement may be for multiple levels of authorisation, with strength of authentication just one factor in the authorisation decision).
- c) Existing e-Science software distributions come pre-configured to accept certificates only from an approved list of national CAs (such as the UK CA operated at RAL). Replacing the UK CA would require negotiation with the teams developing and distributing e-Science software. This would also mean that all resource providers would have to apply this reconfiguration. Existing users, however, should be able to continue using their current certificates for their remaining validity period.
- d) Existing e-Science registration procedures are time consuming and costly, and a lower-cost, more efficient alternative needs to be found. Whilst incorporating certificate registration into institutions' normal, face-to-face staff and student registration procedures would move the work of registration from academic to support staff and potentially allow all users to obtain even the medium-assurance certificates presently required for e-Science at relatively low cost, it is not possible simply to impose change on institutions by fiat.
- e) There is a limit as to how much each institution is prepared to pay for its X.509 certificates (in time and money), and if they are too costly from a national CA then institutions will simply continue to issue their own certificates, or buy them in the commercial market or use alternative authentication mechanisms. To ensure that institutions obtain certificates from the national CA, it may have to be centrally funded.

6 Observations

The goal to simplify registration procedures cannot be easily satisfied while the constraints listed above remain in force. The requirement for personal contact with applicants to verify identity is seen as one of the main burdens, so long as it remains separate from normal student and staff registration. This is because it involves research staff, either as end users or acting as RAs, in time-consuming face-to-face interviews, often involving travel off-site. The problem, therefore, is to reconcile the international e-Science requirement for medium-assurance certification with the constraint that changes in local administrative procedures cannot be externally imposed.

The cost of a PKI increases as the rigour of identity assurance increases. TIES identified two relevant assurance levels: basic assurance for access to JISC IE services, and medium assurance, currently required for e-Science. If agreement could be reached to require medium-assurance certification only for accessing very high value e-Science resources, then the bulk of users could access other resources using basic-assurance certificates.

The basic/medium assurance model was devised to provide broad descriptions of operational practice across a range of industrial and government sectors. In HE, the model has some value, but does not recognise that the processes for staff appointment and student matriculation are similar among institutions, and already provide good assurance of identity in most cases. Indeed, since the institutional photo-id cards issued to staff and students on their induction are currently relied upon for e-Science medium-assurance certification, it could therefore be argued that these induction processes already satisfy a central requirement of medium-assurance certification.

The main inconsistency here is to reject registration based on institutional records while relying indirectly on the photo-id credentials supplied in the course of creating these same records. A second issue is that whereas the UK Grid CA relies on these existing institutional procedures to issue photo-ids to a medium level of identity assurance, it makes no stipulation concerning how they are undertaken, and draws no distinctions between institutions according to the rigour of the induction processes each follows.

Note that some Grid resources already accept local institutional credentials (such as Fermilab, which is reported to use KX509 short-life certificates based on local Kerberos credentials). Local institutional credentials, as used by Shibboleth, may come to be accepted for accessing other e-Science services, in particular lower-value resources, in which case only the minority of users who continue to require medium-assurance certification need undergo the more rigorous registration process. For the short to medium term, however, the requirement for digital certificates for all e-Science services is likely to persist.

Note that while it is possible to deploy a national Shibboleth framework without a national certification authority, the task is made considerably harder, and its integrity is much less assured. In general, a fully managed national certification service is required for all institutional servers that engage in cross-institutional secure communication.

7 Proposals

The following proposals cover issues of assurance level, certification policy, and registration.

7.1 Short term: single assurance level

In the short term, either:

- reduce the cost and increase the longer-term capacity of the RAL CA or
- replace it with a functionally equivalent in-sourced or out-sourced commercial solution issuing medium-assurance certificates in cooperation with the existing e-Science RAs.

Note that during the lifetime of the current RAL CA, the open-source software on which it is built has been modified to improve its performance and scalability. Thus it is possible that further improvements may emerge in the required timeframe. If not, a commercial solution with the required capacity can certainly be obtained.

Either solution above could potentially satisfy all of the short-term ambitions except reducing the burden on RAs, 4(b), and use of certificates for authentication within institutions, 4(f). The restriction in both cases is constraint 5(a), the requirement for medium assurance and face-to-face registration, combined with constraint 5(d), the difficulty of getting institutions to incorporate certificate registration into existing administrative procedures. Note that since the certificate of the existing RAL CA is widely published, and installed in many Grid resources, the transition to any replacement CA may be a non-trivial exercise.

If replacement is undertaken, it should be possible to ensure that new e-Science certificates directly support secure e-mail. The current position is that personal e-Science certificates were intentionally designed not to support secure e-mail. The only officially supported usage is authentication, although extensions in the certificate do permit other uses. It is possible for a technical expert to use the current certificates for secure e-mail, but only by modifying conforming MUA implementations to not check the e-mail address (because the certificates do not contain e-mail addresses).

7.2 Longer term: multiple assurance levels

In the longer term, if the number of e-Science certificates is to grow towards 20,000, and if secure e-mail or local authentication certificates are deployed by some institutions, then registration procedures will have to be simplified to prevent the overall costs and administrative burdens from becoming unsustainable. This would mean that either:

- a) a basic-assurance registration scheme (which could be automated and non face-to-face) would be implemented in addition to the medium-assurance registration offered by e-Science RAs, or
- b) a medium-assurance, face-to-face certificate registration procedure would be integrated with existing face-to-face student and staff registration procedures (matriculation and appointment).

Institutions would have freedom of choice over which certificate registration scheme to adopt.

7.3 Two CAs

The approach proposed is for two CAs, one providing medium-assurance and the other basic-assurance certification.

The medium-assurance CA would be as described in 0 and would be the recognised UK CA for international e-Science purposes. It would be used by:

- e-Science researchers with a genuine need to access Grid resources outside the UK or particularly high-value UK resources, initially by registration with existing e-Science RAs;
- all users at institutions that choose to integrate medium-assurance registration with their normal administrative processes, via the new institutional RAs described in 0(b);
- servers using SSL for secure cross-institutional communication (such as Shibboleth origin and target equipment).

The basic-assurance CA would operate as a general-purpose JISC CA, providing certificates to all other users.

Having more than one CA effectively removes constraint 5(b) and allows multiple levels of assurance. Constraint 5(a) is still satisfied because only the medium-assurance CA would be recognised internationally. To make this work, technical constraint 5(c) must be lifted. However, adding another CA at the same level as the national CAs to the existing list in UK deployments of Grid software is far simpler than removing policy constraint 5(a). Short-term experimental work using the existing RAL CA should be undertaken to find out whether the new CAs can be introduced transparently to existing users.

7.4 Why Not Just One CA?

On general principles, it would be desirable to have a single national CA that issued certificates with both levels of assurance. Relying parties could distinguish these by means of different policy flags embedded in the certificates themselves. However, it is thought unlikely that current e-Science software (Globus) is able to reject certificates that do not contain a particular policy flag. Nor can it be assumed that any modification of the software to support such a feature would be widely distributed in the short term (although a current JISC middleware proposal does suggest including the level of authentication in the Grid authorisation decision-making process).

It has been suggested that if a policy flag marked as critical was included in the basic-assurance certificates then Globus would reject those certificates. This is true. However, it would not then be possible to configure any Globus-based UK e-Science resources to accept basic-assurance certificates, and so all e-Science participants would still need to obtain medium-assurance certificates and the burden on existing RAs would not be reduced. The fundamental problem is due to the current “all or nothing” behaviour of the authentication mechanism, whereas the requirement is to authorise users to different levels based in part on their strength of authentication.

Any proposal for a single UK CA would have to demonstrate that current e-Science software could be configured to discriminate between the different classes of certificate the CA would issue.

7.5 Registration

In the twin CA model, the following mechanisms for certificate registration would be implemented:

- a) Both CAs would support remote RA functions allowing certificates to be registered or revoked by accredited local individuals for small-scale use (e.g., SSL server certificates or teaching).
- b) The existing e-Science institutional and regional RAs would continue operating as at present, using method (a) with the new medium-assurance CA, at least until the vast bulk of e-Science certificates were being registered in one of the other ways listed below.
- c) Some institutions may choose to modify their existing administrative procedures to permit registration with the medium-assurance CA as part of their staff appointment and student matriculation processes. This would involve verifying each applicant's identity to an externally set standard (as defined in the Grid CA CPS) and, as one possibility, including a hardcopy password in the paperwork bundle given to those accepted. This password would allow its holder later to enrol individually with the CA via a secure web connection to obtain their certificate.
- d) Some institutions may retain existing administrative procedures, operating to a lower standard of identity verification acceptable to the basic-assurance CA. In particular, they might continue to use their existing processes for identity verification (for example, presentation of qualifications and official funding letters by students). Handing out passwords for certificate downloading would still be required: the only difference from (c) is not having to do identity verification to external (Grid) standards. Note however that current UK RA practices do accept the photo cards issued by these institutions.
- e) A web-accessible self-registration service could be offered to individual end-users, based on their university assigned e-mail address, similar to services already available from commercial certificate vendors. Note however that the certificate should only contain the authenticated email address and not the user's identity if this is not also authenticated at the same time. This might well be acceptable for experimentation with secure e-mail.
- f) Although a self-registered certificate could in principle offer medium assurance that its holder was the rightful owner of a particular e-mail address, the current UK e-Science CA CP/CPS requires personal Grid certificates to contain a verified real name. If this policy cannot be changed then a third CA would likely be required to issue the self-registered certificates. This would allow relying parties (particularly Grid resources) to reject such certificates based on CA, without having to inspect the contents for policy flags or lack of a real name. As discussed in 0 above, current Grid software (specifically Globus) cannot be simply configured to reject certificates based on content, such as DNs that contain only e-mail addresses.
- g) For the registration of commercially employed members of VOs, existing arrangements involving the presentation of government-issued photo-id to dedicated e-Science RAs will continue to be required.

In cases (c) and (d), users would be registered in bulk with the CA from existing university staff and student databases derived from institutional administrative procedures, as previously investigated by the TIES project. This process should have lower administrative costs than the current e-Science scheme because in-person verification of identity is performed as part of the existing procedure for populating these databases for reasons unconnected with e-Science.

Note that a medium-assurance self-registration service similar to (e) above cannot be provided so long as the definition of medium-assurance involves face-to-face contact. It may be worthwhile discussing relaxations in this area with the Grid authorities, for example telephone or videophone interviews, but rapid change should not be expected.

8 Implications for Stakeholders

There are implications for each of the stakeholders:

- e-Science;
- institutions;
- JISC;
- the RAL CA.

8.1 E-Science

The proposed approach offers a trade-off to UK e-Science. There is the prospect of limiting the burden of face-to-face identity verification on existing e-Science RAs, who are normally academic researchers, to only those cases where it is required by policy: users who need to access international resources from institutions that do not have some other acceptable registration scheme in place. The burden would be offloaded onto institutional administration and computing support staff as numbers grow. The quid pro quo is that to make use of lower-cost, basic-assurance certificates, UK e-Science would have to identify resources it operates (probably small-scale teaching resources initially) where basic-assurance authentication is sufficient and reconfigure those resources to accept basic-assurance certificates in addition to the current medium-assurance ones. There may also be work to accommodate replacement of the RAL CA, and to test the effectiveness of cross-certification.

E-Science may wish to reconsider its requirement for photo-id. As observed in section 0, university photo-id cards currently relied on by e-Science RAs are issued by institutions based on documentary evidence such as employee references and student funding letters. If the cards are acceptable then it makes sense to allow institutions to register users for certification directly using the same evidence. If this argument were accepted then only one CA would be required, the separate medium-assurance registration process, 0(c), could be dispensed with, and all institutional RAs could use the same process, 0(d), a considerable simplification.

8.2 Institutions

The certificate registration processes described in 0(c) and (d) would involve an institution's IT-support staff in secure transmission of bulk extracts from the institution's staff and student databases to a CA. Since each institution's databases are different, this is likely to require some bespoke development work. The institution's administrative staff would need to follow the required identity-verification procedures and might need to merge password letters into the paperwork bundles handed out to new staff and students. At any rate, some confidential method is needed to tie together the student and staff registration process with the key pair generation and certificate issuing process, in order to ensure that the correct person obtains the correct private key and certificate.

Because present arrangements already provide certificates to everyone who currently needs them, local decision-makers are not likely to roll out these new processes spontaneously. However, without new bulk processes, certificate registration will remain small-scale and therefore expensive.

8.3 JISC

If the goals listed in clause 4 are to be fully realised then either:

- e-Science must decide that an automated, non-face-to-face registration procedure such as 0(e), which can be provided centrally, is acceptable for the majority of its UK resources, or
- many institutions must be convinced to undertake the changes described in 0(c) or (d).

The most persuasive arguments for voluntary change are that it would: overcome an obstacle to growth in e-Science numbers, let some academic e-Science staff do more research and less administration, and enable cross-institutional secure e-mail in the longer term. Unfortunately, it cannot be claimed to enable Shibboleth deployment (other than at server level), since Shibboleth was expressly designed to support secure access based on local institutional authentication, including name/password schemes, or even disjoint “islands” of certificates, as exist in the USA.

In the second of the two cases above, the opinion of local decision-makers should be canvassed, and some level of commitment should be secured before procuring the proposed service. This might require incentives more concrete than simple persuasion.

In addition, any change to the present e-Science CA arrangement will require the blessing of (at least) the European-level Grid authorities. This should be sought before proceeding. The authority in question is the EU Grid Policy Management Authority (PMA), which is coordinating Grid authentication activities in Europe. The three large EU FP6 projects (EGEE, DEISA and SEE-GRID) have all agreed to use this single infrastructure. The RAL CA was a founder member of this body, which dates back to the early days of the EU DataGrid project at the end of 2000 (see <http://www.eugridpma.org/>). In turn, the EU Grid PMA is linked into global activities via the Global Grid Forum and the International Grid PMA at <http://www.gridpma.org/>. TERENA operate an independent (trusted third party) repository of CA root certificates and policies (TACAR), also at <http://www.gridpma.org/>.

8.4 RAL CA

At the outset of this project, it was generally believed that the RAL CA would not scale beyond about 1,000 certificates. It is now understood that a technical problem limited the performance and scalability of the original service, but this has since been resolved and numbers up to about 10,000 are now considered feasible.

It should therefore be possible in principle to reduce the cost of the RAL CA, enhance its future capacity towards 20,000 certificates and add extensions along the lines proposed in 0 and 0 to support the longer-term goals, thus providing an in-house alternative to commercial outsourcing. The operators and sponsors of the RAL CA would need to consider whether this course, of becoming a general-purpose higher and further education CA rather than specifically an e-Science CA, is one they wish to pursue, and if so, whether they would prefer to operate an enhanced open source CA or a commercial CA.

9 Technical Requirements

The foregoing discussion leads to the following technical requirements for vendor insourced or outsourced certificate-issuing services, in the short term for e-Science and in the longer term for more general purposes.

- a) *Number of CAs.* Two CAs are proposed (basic and medium assurance) but proposals from vendors for a workable single-CA solution would be welcomed. Because commonly available open-source certificate verification software (openssl, mod_ssl) when configured to accept certificates from one CA will automatically accept certificates from a subordinate CA, it would be tempting to make the medium-assurance CA subordinate to the basic-assurance one, so that resources configured to require basic-assurance certificates would automatically accept medium-assurance ones too. Unfortunately, in that scenario openssl cannot be directly configured to accept only medium-assurance certificates, because to permit verification of the entire certificate chain the resource would also have to include the superior, basic-assurance CA in its list of trusted CAs. It might be possible to work around this by creating an additional, self-signed certificate for the medium-assurance CA (with the same public key) for use in these circumstances, but we have not verified this. Therefore, if there are to be multiple CAs, it may be necessary for them to be at the same level as each other but this has not been conclusively established.
- b) *Certificate acceptance.* It must be possible for holders of medium-assurance certificates to use them wherever a basic-assurance certificate would normally be required. If this cannot be achieved by making one CA subordinate to the other (see above), resources accepting basic-assurance certificates would need to be explicitly configured to also accept medium-assurance certificates. Additionally, some academic sites may require server certificates whose ultimate root certificate is embedded in standard browsers, goal 0(0). If this feature is not available, these applications will continue to use commercial certificates.
- c) *Number of RAs.* This will be not less than one per major research university (50) and not more than one per department at every university (30 x 200 = 6,000). This is such a wide range as to be of little value except to indicate that the supplier must be able to cope with potentially large numbers. Some vendors raised the possibility of delegating some identity verification functions from a single institutional RA to departmental local registration authorities or trusted agents.
- d) *Manual registration.* In the short term, for e-Science, RAs will continue to register users individually using manual procedures.
- e) *Automated registration.* In the longer term, potential suppliers must be able to upload bulk registration information in the order of 10,000 users per RA as a unit, in a standard format to be agreed by the whole community, and process subsequent additions and deletions individually and automatically. During the start-up phase, it may also be necessary to bulk load in the order of 2,000 existing users from the RAL CA.
- f) *Number of certificates.* In the short term, a RAL CA replacement would issue about 5,000 certificates within 1–3 years (factor of five headroom over the current number) and 20,000 in 3–5 years (expected e-Science growth). In the longer term, numbers might grow to the order of every

student at a few universities that choose to use X.509 client certificates as their local authentication mechanism for Shibboleth but do not want to set up a local CA ($10 \times 10,000 = 100,000$) plus some staff at every institution for secure e-mail ($5 \times 30 \times 200 = 30,000$). This is 25% of all UK academic staff (120,000, see <http://www.hesa.ac.uk/holisdocs/home.htm>). This excludes the scenario where every institution decides to use certificates for local authentication, resulting in a need to issue a certificate for every student at every university in the land ($10,000 \times 200 = 2,000,000$). A more reasonable working number for capacity planning purposes looks like 200,000, giving some headroom from the rough estimates above.

For server certificates, the demand for Shibboleth origin certificates will be at least one per institution, say 500, or 1,000 if every institution eventually becomes a Shibboleth target too. Multiplying by 10 target services per institution gives 10,000 (each separate host machine needs its own certificate containing its DNS name).

If BECTA's proposal to use Shibboleth for schools' access to on-line resources is adopted, the additional numbers would be about 5,000 for secondary and independent schools acting as origins only or 50,000 in a worst case where primary schools are included and individual schools all operate one target service machine. There were 25,472 schools in England in 2003, according to DfES' Statistics of Education, Schools in England, of which 3,436 are secondary.

- g) *Type of certificates.* It must be possible to obtain both client and server certificates from the service. The bulk of certificates issued would be client certificates.
- h) *Policies.* Three certificate policies are required, one each for the medium and basic-assurance identity certificates and a third for SSL server certificates, including Shibboleth origins and targets.
- i) *Key usage.* Certificates will be required to support both authentication and signed e-mail (S/MIME). Initially a single key pair is all that will be required. (Note that encrypted email is currently not considered to be a major requirement.)
- j) *Percentage revocation.* The previous TIES project assumed that the number of certificate revocations could be kept below 1% by revoking only in cases of formal disciplinary action, and not for simple key loss. This is because it is assumed that a user can either recover a lost signing key pair, or simply replace it without issuing a revocation. (Note that if encryption is added as a later service, encryption key recovery is usually provided and obviates revocation). This reasoning applies to basic-assurance certificates. Revocation on loss may be required for the medium-assurance certificates, giving a higher proportion of revocations.
- k) *CRL frequency.* At least weekly publishing of CRL updates is required for the basic-assurance (general) service. For the e-Science medium-assurance service, this should be at least as frequent as the existing RAL CA, probably daily.
- l) *CRL distribution.* Mechanisms such as CRL distribution points and delta CRLs should be supported to stop CRLs growing to more than 10Kbytes in size.

- m) *Mobility*. Support for the mobile user, e.g., the ability to fetch a certificate and key from a central store, is a requirement.
- n) *Browsers*. The CA should support the use of all mainstream browsers by both RAs and end users and ideally should be subordinate to a CA embedded as a trusted root in these browsers.
- o) *Private key backup*. The CA's private key must be capable of being backed up and recovered e.g. in case of a catastrophic failure of the hardware running the CA.
- p) *Automated management*. As many of the CA management functions as possible should be automated, so as to reduce human involvement. Examples include: periodic re-issuing of CRLs with the same revoked certificates as in previous lists, backups of the certificate database and directory contents, bulk issuing of certificates to groups of users.
- q) *N from M authority*. Important security functions, such as changing the certification policy, or use of the CA's private key for cross certification, should be configurable so that N from M security officers need to be present to authorise it
- r) *Secure audit*. The CA software should have a tamper proof secure audit trail that records all security relevant actions.

10 Division of Responsibility

An initial question for this report was to consider the relative merits of an insourced or outsourced solution for a certificate issuing service. The apparent choice is between vesting responsibility for management of the technology in an academic agency or in a commercial service supplier.

In practical terms, however, neither scenario provides an entirely realistic choice. The operation of institutional RAs cannot be managed economically or effectively by an external commercial organisation. Equally, an academic authority cannot easily develop the type of secure operating infrastructure or range of technical options that a dedicated PKI supplier can provide. Given the existing demand for medium assurance certificates for end users and server machines, and the anticipated demand for bulk certification at lower assurance levels, the core infrastructure should be capable of accommodating the full range of requirements that may emerge for a national certification service.

The need to balance the division of responsibility for the PKI between the customer and vendor is generally recognised by the suppliers, and the larger of these offers a range of technical options for striking the balance according to customer requirements. In broad terms, it makes sense for an academic authority to take responsibility for the organisation of institutional RAs and the administration of the certificate policy, and the vendor to take responsibility for the core CA functionality.

The RAL CA provides a professional service that satisfies international e-Science requirements but was not designed to accommodate the numbers of end users and the additional service needs now emerging. For example, to enable inter-operation between different Shibboleth federations may require the establishment of pervasive PKI trust relations between many Shibboleth servers which might only be practical where widely-recognised trusted root certification is employed.

The RAL CA, however, is the only academic agency in the UK with experience of PKI operation, with good understanding of the requirements of international e-Science, and with well-established relationships with existing RAs. It would be the preferred academic authority to work with a commercial supplier to deliver a managed PKI service.

11 Recommendations

The recommendations are as follows:

- a) To consider moving towards a system of two JISC CAs, basic and medium assurance, as described above.
- b) Given that the RAL CA has greater capacity than was previously thought, discussion should begin between the JISC, the e-Science community, and RAL CA staff about the future role of the RAL CA.
- c) One option would be for the RAL CA to become the proposed medium-assurance JISC CA, extending its remit beyond e-Science to more general H&FE purposes and working with the Grid Policy Management Authorities to assist the creation of the proposed institutional bulk RAs and their acceptance by e-Science, while working to further increase capacity, possibly by outsourcing some of its mechanical functions. In this approach, the proposed basic-assurance CA could either be set up at RAL as an extension of the existing facility or outsourced.
- d) Alternatively, JISC might request formal bids from outsourcing vendors for its own CAs, in the expectation that the RAL CA would be phased out. Note that if the RAL CA were to continue in operation then the JISC certificates could not be used for e-Science purposes, both because in most circumstances international Grid policy only recognises one CA per country and because of the momentum of existing e-Science CA arrangements.
- e) Regardless of the specific arrangements for actual CA operation, it may be desirable to set up a standing policy body, covering e-Science, JISC and other academic users, which could settle certificate policy questions and liaise with international policy bodies.
- f) The policy issues raised in this report should be resolved before going back to the vendors with a formal request for proposals.
- g) In particular, if the potential cost advantages of moving certificate registration from current e-Science RAs to bulk institutional RAs are to be realised then the support of a critical mass of institutions should be secured before proceeding to implementation. Support would be required from both computing services, which would need to integrate institutional databases with the central CA, and administrators, who would need to review student matriculation and staff appointment procedures.
- h) Similarly, the Grid Policy Management Authorities should be consulted well before any implementation work is begun.
- i) Because the potential outsourcing suppliers produced their price estimates within a limited timescale and without the discipline of having to sign a real contract, it is recommended that the prices are regarded as a floor below which a real bid is unlikely to fall in the short term, rather than a “central case” estimate. That said, PKI market prices have in general been falling over time, so over the longer term further reductions may be expected.
- j) Although **Error! Reference source not found.** contains some discussion of the relative merits of the different companies, it is suggested that to obtain the best outcome from any subsequent procurement exercise, all the vendors should be approached again, including those who did not

respond to our enquiries. All those who did respond (except one) appeared to be potentially suitable, so the field is quite open.

- k) Several vendors proposed variants of a low-cost approach in which there would be only one RA (or a handful of them), which would be used by all (or most) institutions. For security and accountability reasons, it is recommended that the traditional approach of providing a separate RA for each administrative domain (i.e., institution) should be followed, even at somewhat greater expense.

Appendix A: Vendor Responses

During April 2004, a web search identified the following list of potential suppliers for the certificate-issuing service outlined in this document:

Alphatrust, BBN Planet, Bell, Betrusted, Cert. Ireland, Ebizid.com, EDS, Entrust, Equifax, Eurotrust, GTA, GTE, GlobalSign, Identrus, Netscape, TC TrustCenter, Thawte, Trustis, UserTrust, Valicert and Verisign.

A.1 Pre-Filtering

After reviewing the list of potential suppliers with the project’s external consultants, TrueTrust, the following were eliminated:

Alphatrust, Bell, Ebizid	Lack of market presence
Eurotrust	Sold their PKI services business to Verisign on 1/04/04 for about \$10m and are now a sports TV production (!), security and anti-virus company.
GTA	They only issue certificates to “master authorities” and charge £3m/year. Web site dormant since end-2002.
GTE Cybertrust	No longer a going concern; assets sold to Ireland’s Baltimore, themselves now part of USA’s Betrusted.
Netscape	Were advised they don’t offer outsourcing
TC TrustCenter	According to press release on Betrusted website, TC TrustCenter was set up by the big four German banks, is affiliated with Identrus and is now in alliance with Betrusted. Treated as part of Betrusted (see later).
Trustis	Too small (SME)
Valicert	Valicert’s product is a “CA-neutral, Identrus compliant” server that does certificate verification and revocation checking. They don’t offer CA services.

A.2 Initial Contacts

Towards the end of April, each of the remaining companies was contacted by e-mail, at addresses identified from the web search and from previous contacts through TrueTrust. A similar message was sent in each case, briefly stating a requirement for a UK national X.509 certificate-issuing service for H&FE and asking to be put in touch with an appropriate person in the organisation to take the matter further.

The following suppliers were not pursued after these initial contacts:

BBN Planet	BBN is no longer in the CA service business. A part of the company used to do that sort of work, but was sold several years ago.
Cert Ireland	They are now called Certification Europe and don’t offer CA services (they do

	audits of CAs).
EDS	No response.
Entrust	No longer does CA outsourcing. Suggested Betrusted, Trustis and Diginus as third-party possibilities.
Identrus	Umbrella organisation formed by the banks for secure commerce certificates. Their CA service provider is DST, which uses software from Xcert, now part of RSA. Identrus partners include: Baltimore (now Betrusted), IBM (eBX), Kyberpass, Sun (iPlanet), SECUDE (Germany, secure e-mail). They did not respond to us.
Post-Trust	Suggested by Cert. Ireland, no response yet.
Thawte	Stopped responding after initial contacts.

A.3 Substantive Proposals

Six vendors produced substantive responses to an interim version of parts 1–9 of this report: Betrusted, Diginus, Equifax, GlobalSign, UserTrust and Verisign. After initial conference calls to clarify our requirements, Equifax put us in touch with their US parent company, GeoTrust, and Verisign referred us to BT Global Services, a “global affiliate” using Verisign technology.

Each of these six responses is discussed separately below. Five of the six (all except Betrusted) produced indicative commercial proposals. Because the companies produced these within a limited timescale and without the discipline of having to sign a real contract, it is recommended that the prices are regarded as a floor below which a real bid is unlikely to fall, rather than a “central case” estimate. Prices quoted in US dollars are converted to sterling at a rate of \$1.80 to the pound (June 2004) and usually rounded to two significant figures. Euro prices are converted at €1.50 to the pound and similarly rounded.

A.3.1 Betrusted

Betrusted are an approved PKI provider to the US federal government. Other clients include Banks (ABN-AMRO), large telecoms companies (Verizon, Telecom Italia) and health-care providers (OneHealthPort).

Betrusted indicated that options for managed outsourcing based on their (ex-Baltimore) Unicert CA product would be available but believed that further clarification of the basic and medium assurance levels, and more work on options for vetting end-user identities, would be required first.

For basic-assurance registration, both individual and bulk registration by institutional RAs could be supported. For medium assurance, Betrusted suggested that consideration be given to the idea contained in the US government’s PKI Common Policy Framework of trusted agents, who can be delegated by an RA to perform some of the identity verification work. In a university, the trusted agent might be an HR person or administrator. This seems to be similar to the idea proposed by GlobalSign of Local Registration Authorities, in which there would be one RA for an institution, but a local registration authority, trusted by the RA, for each department.

No commercial terms were proposed at this stage.

A.3.2 BT Global Services (Verisign)

BT Global Services are a “global affiliate” (effectively a worldwide franchisee) of Verisign. They use Verisign technology but BT people in the UK provide the service. BT operates a resilient facility with redundant power supplies, disks and a complete warm-standby system in a different city (Belfast). All staff are security-vetted BT employees. The organisation is confident of its ability to handle demanding security applications: BT is supplying PKI services to the two largest UK clearing banks for use in the BACS (Banks Automated Clearing Service) payments system, which handles most salary payments in the UK.

Nothing in the requirements was felt to be a technical problem; they are well used to outsourcing CA functions. The challenges were seen as design of the technical and administrative processes for bulk upload of registration data from institutional RAs and the commercial impact of a possibly large number of RAs. Their pricing normally includes an element per RA; since they normally deal with 2–8 RAs per enterprise, that might become unworkable but they were sure an accommodation could be found. A second-level helpdesk is provided (end users are expected to obtain first-level support from their local institution) and third-level support from Verisign is available if required.

In their standard operational model, the end user applies on-line for a certificate; a local RA later approves this application on-line and e-mail is sent to the user, prompting them to download their certificate. In each case, standard browsers are used, although an ActiveX plug-in (and corresponding firewall hole) is required. If this presents a problem, a work-round is available but the institution would have to pre-configure all their desktop systems with the work-round. The same certificate can be used for both authentication and S/MIME and is normally set to expire after one year. To facilitate secure e-mail applications, a publicly accessible directory is maintained, keyed by e-mail address, from which users’ certificates can be downloaded.

BT saw two ways of incorporating bulk registration data from institutions:

- a) When an individual applies for a certificate, the CA can be configured to query a database held by the RA. A certificate can be issued immediately if the registration data matches.
- b) Alternatively, bulk PCKS#10 registration data could be uploaded from an institutional RA to the CA.

Excluding the cost of developing either bulk system, BT offered the following indicative prices:

No. of users	Set-up (approx.)	Annual licence	Per-user annual cost (excl. set-up cost)
5,000	£24,000	£113,500	£22.70
10,000	£29,000	£146,500	£14.65
25,000	£29,000	£186,500	£7.46
100,000	£29,000	£373,500	£3.74

BT provided a detailed point-by-point response to the interim version of this report.

A.3.3 Diginus

Diginus appear to be a relatively new company, formed by people from the old Post Office Viacode team, which is targeting the UK public-sector market and has deployments within the NHS (NHSIA).

Technically, Diginus use Open CA as their base software but claim to have done a lot of work improving it. They foresee no problem scaling to the level of 20,000 certificates. It would suit them to make our CAs subordinate to their commercial root CA.

Diginus was the only vendor that attempted to propose a single-CA option, in addition to the main two-CAs proposal. Their suggestion was to differentiate between basic and medium assurance certificates from a single CA by using different Organisational Unit names in the Distinguished Name of the certificate subject to indicate whether the registration information came from a basic or medium assurance RA. It is not clear that the Globus software used in e-Science could distinguish the two classes of certificate other than by individual authorisation of acceptable certificates in the gridmap file. However, the choice of single or dual CA option did not affect the commercial terms.

Commercially, there were also two options proposed, depending on whether procurement of certificates would be handled centrally or by individual institutions:

- a) *Central purchase of the CA service and all certificates.* In this option, the supplier relationship with individual institutions is purely at a technical level. In year one, pricing would be £60–80,000 depending on the number of certificates expected (up to 20,000) and in year two onwards, £50,000 for service provision (up to 20,000 certificates) each year.
- b) *Distributed purchase of certificates,* where the supplier must have a commercial and administrative as well as a technical relationship with each RA. This model still assumes central funding of the set-up and running of the CA, at £50,000 in year one and £30,000 p.a. thereafter (no certificates included), but adds £5,000 per year for each separate RA organisation, each to include up to 1,000 certificates.

See the attached letter from Simon Trickett. Note that Diginus was at pains to stress its commercial flexibility.

A.3.4 Equifax (GeoTrust)

Equifax are already involved with (parts of) HMG, providing “SecureMark” client identity certificates at £25 each for various e-government applications, where Equifax is responsible for verifying the identity of the end user. The company is now owned by GeoTrust in the US but retains a separate identity. GeoTrust claims to be the world’s second-largest CA.

The Equifax model of assurance has four levels:

0	No assurance
1	Prove with “reasonable assurance” that an identity exists
2	A genuine identity “probably exists” (this is the bulk of their business)

3	Highest assurance, with face-to-face interview, passports, and multiple sources of documentary ID
---	---

Equifax are a member of tScheme, the UK implementation of the EU digital signature act. Other tScheme approved operators include Betrusted, RBoS TrustAssured, Trustis and BT. tScheme tries to offer common EU legal definitions of assurance levels, as opposed to the banks' Identrus scheme, which offers cash liability up to a given amount per certificate, based on their inspectors' view of each certificate issuer's certificate practices. However, after initial discussions, Equifax decided that since we would not require them to verify end user identities, it would be appropriate to refer us to their parent company, and provider of back-end certificate services, GeoTrust.

The GeoTrust architecture is based on a completely outsourced model. It requires no special browser plug-ins and the format of the generated certificates is configurable. Physical CA operations are located at dual sites in the USA, in highly secure "bunkers" with backup power and air-conditioning.

GeoTrust quoted on the basis of two options:

- a) A shared scheme, the lower-cost option, in which there would effectively be a single RA shared by all institutions. Each institution would have the technical ability to issue or revoke certificates for any other institution's users. Institutions could be bound by contract to register only their own end users but not technically prevented from doing otherwise. This option is priced at \$6,000 (£3,300) for set-up, plus annual hosting fees of \$18,000 (£10,000), plus \$500 (£270) per additional RA (first two free), plus a per-certificate price on the sliding scale in the table below. For example, with 100 institutions sharing one RA and issuing 25,000 certificates, the per-certificate fees would be 25,000 times \$3, i.e., \$75,000 (£42,000). When the \$18,000 (£10,000) hosting fee is added, the grand total would be \$93,000 (£52,000) per annum. In this option, technical support is available only to one designated contact person for the entire community.
- b) A compartmentalised scheme. In this approach, each institution is its own RA and can be technically constrained to issue certificates only within its own organisational domain. This costs more but offers increased security. For this option, the set-up fee and per-certificate pricing are the same as before but a \$400 (£220) monthly fee per institution is added to the running costs. For the example above of 100 institutions and 25,000 certificates, it adds \$40,000 (£22,000) per month, or \$480,000 (£270,000) per year, to the bill, giving a grand total of \$573,000 (£318,000) per annum. In this model, technical support would be available to one designated contact person at each institution.

The per-certificate prices are the same for each option:

Qty	Annual price/unit
1	\$15
500	\$8
1,000	\$7
2,500	\$6

5,000	\$5
10,000	\$4
25,000	\$3
50,000	\$2.25
100,000	\$1.25

Note that in the second option the final price is quite highly geared towards the number of institutions. Our initial discussions with GeoTrust centred on smaller numbers (10–50). They are at pains to stress that the per-institution fee would be negotiable and they would provide a discount if the number reached 100 as in the example above.

A.3.5 GlobalSign

GlobalSign is a European firm (Belgian). Their root certificate comes already embedded in Internet Explorer, Netscape, etc. The firm is involved in Belgium’s national electronic ID card project, Belpic/EID, to issue eight million electronic ID cards with two certificates each, and has undertaken projects in the health-care sector with MedicalNet in Germany and Austria (100 hospitals and 2,500 surgeries) and AstraZeneca in Belgium.

GlobalSign have an existing partnership with UKERNA and therefore have already issued server certificates to some UK universities. Andrew Cormack of UKERNA reports that their, originally 2 year, contract with GlobalSign gives GlobalSign first refusal on any future UKERNA certificate-issuing activity (emphasis on UKERNA as opposed to UK academia in general). Like the other companies, GlobalSign’s proposal included a fixed set-up fee, of €9,000 (£6,000). This would cover both identity and server certificates. The subsequent annual fee is based on the number of certificates of each class in issue (expired and revoked certificates are not counted), on a roughly linear sliding scale:

Annual fee (€)	PersonalSign2	PersonalSign2 Pro	PersonalSign3 Pro	ServerSign
10,000	1,500	750	500	150
12,000	2,000	1,000	700	200
25,000	5,000	2,500	1,700	500
45,000	10,000	5,000	3,500	1,000
100,000	25,000	22,500	9,000	2,500

For our requirements, the Pro versions of the identity certificates, which include the employer organisation name as well as the individual’s name, would be required. PersonalSign2 (Pro) corresponds to what we have been calling basic assurance; PersonalSign3 (Pro) requires the physical appearance of the applicant before the RA and therefore corresponds to what we have been calling medium assurance. ServerSign certificates provide for server identification. It is not clear why the PersonalSign3 certificates should be more expensive, since the additional burden of identity verification falls on the RA, i.e., the customer, rather than GlobalSign. Perhaps there are liability implications. Per-RA pricing was not directly addressed in the GlobalSign proposal.

For 18,000 medium-assurance certificates for e-Science use, the annual cost would be €200,000, or £130,000. In practice, for comparability with the examples previously shown for other vendors, at least some of the total number of certificates would likely be lower-cost basic-assurance ones, and so the overall cost might be less.

One other point to bear in mind about GlobalSign’s proposal is that their existing CAs would issue the certificates. They are not proposing to set up new CAs for this project. For good or ill, it would not be possible to distinguish “academic” certificates from others simply by accepting certificates only from “our” two CAs; anybody with a GlobalSign personal certificate would pass this test, whether or not they were a UK academic.

A.3.6 UserTrust

Since it appears to be a one-man US company (Nick Hales, its president, answers the phone personally), UserTrust is unlikely to be regarded as a suitable supplier for a national service. The company is included here for completeness and because it did respond to our enquiries.

UserTrust was confident of feasibility on the basis of the interim report. Its pricing proposal was \$19 to \$29 per identity certificate, and \$49 to \$69 per SSL server certificate, plus additional start-up costs that would only be defined in response to a formal Request for Proposal from a funding body.

A.4 Contacts

The following contacts were established at the vendors approached:

Betrusted	Russel Weiser, Managing Consultant, rweiser@betrusted.com
BT Global Services	David Shapland, Manager, david.shapland@bt.com Tel: (01344) 863011, Mobile: (07889) 175409 Adrian Hull, Technical, adrian.hull@bt.com Mobile: (07711) 772019
Cert. Europe	Michael Brophy, mbrophy@certificationEurope.com
Diginus	Simon Trickett, simon.trickett@diginus.com Tel: (0845) 456 1234, Mobile: (07968) 730298
EDS	info@eds.com (no response)
Equifax	Lyn Jones, Head of Government Services, Lyn.Jones@equifax.com Tel: (020) 7298 3000, Mobile: (07710) 843936
GeoTrust	Steve Waite, GeoTrust Europe, steve@geotrust.com Tel: (01622) 764789 Chris Bailey, Co-founder and VP Business Development, chris@geotrust.com Mobile: +1 678 595 7999
GlobalSign	Ronald De Temmerman, Business Development Manager ronald.detemmerman@globalsign.net Tel: +32 16 287 285, Switchboard: +32 16 287 123 Johan Sys, General Manager, johan.sys@globalsign.net

UserTrust	Nick Hales, nick@usertrust.com , Tel: +1 801 363 9748
VeriSign	Steven McDonnell, Business Development, SMcDonnell@verisign.com Tel: (0780) 320 8512