ISSN 0961-9348

casg Computer Audit Specialist Group

JOURNAL

VOLUME 8 NUMBER 4 SUMMER 1998

The British Computer Society

Technical Briefings for 1997/98 Season

For more details of all Technical Briefings, and details of costs and registration, contact Jean Brown, on 01803 872775

Technical Briefings (Chargeable Attendance)

Wednesday 30 September 1998	EMU: Business issues, software issues
Tuesday 26 January 1999	Client/server computing: help-desk, configuration, management, asset management, change management
Tuesday 20 April 1999	Benchmarking IT, Systems development, Data centre

Late Afternoon Meetings (Free Attendance)

Tuesday 1 December 1998	UNIX
Tuesday 16 February 1999	NT security
Tuesday 18 May 1999	Forensic Accounting

Followed by the Annual General Meeting.

Contents of the Journal

GUIDELINES FOR POTENTIAL AUTHORS

The *Journal* publishes various types of article.

Refereed articles are academic in nature and reflect the Group's links with the BCS, which is a learned institute governed by the rules of the Privy Council. Articles of this nature will be reviewed by our academic editor prior to publication and may undergo several iterations before publication. Lengthy dissertations may be serialised.

Technical articles on any IS audit, security, or control issue are welcome. Articles of this nature will be reviewed by the editor and will usually receive minimal suggestions for change prior to publication. News and comment articles, dealing with areas of topical interest, will generally be accepted as provided, with the proviso of being edited for brevity. Book and product reviews should be discussed with the appropriate member of the editorial panel prior to submission. All submissions should either be on double spaced, single-sided A4 paper, or on PC format diskette in Microsoft Word, Ami-Pro, or ASCII format. Electronic submission is preferred.

Submissions should be accompanied by a short biography of the author(s) and a good quality monochrome photograph, or electronic image.

Submission Deadlines

Spring Edition	7th February
Summer Edition	7th May
Autumn Edition	7th August
Winter Edition	7th November

The ***Journal*** is the official publication of the Computer Audit Specialist Group of the British Computer Society. It is published quarterly and is free to members.

Letters to the editor are welcome as are any other contributions. Please contact the appropriate person on the editorial panel.

Editorial address:
47 Grangewood,
Potters Bar
Herts, EN6 1SL

Designed and set by Carliam Artwork, Potters Bar, Herts
Printed in Great Britain by Post Script, Berkhamsted, Herts.

EDITORIAL

Summer is here again, the AGM is out of the way and a revitalised committee is preparing the programme for next season. I state these things with some satisfaction because, as editor, I have very little to do with the hard work of preparing the programme, maintaining the membership database (those renewal invoices will be winging their way to you soon), liaising with the BCS and the hundred and one other things that your committee does on your behalf. I spend a few days pleading, bullying, bribing and generally coercing people to supply copy for the *Journal*, another few hours putting it together and then it is the turn of Carliam Artwork, our typesetters and printers, to do the really hard graft. Janet at Carliam is a superb editor, who constantly picks up things that I have missed when supposedly checking the galley proofs and the occasional inconsistency in the papers provided by our contributors. She then organises the printing and distribution, using address labels supplied by Jean Brown, our administrator. The result is a professional *Journal* with just about five minutes of my input. Now that's management for you!

You will notice that we have a new Chairman, John Bevan, who has not only supplied his own column, but also a good explanation of the accreditation process for BS 7799, the new security standard. Both the BCS and our sister group, the London Chapter of ISACA, have put a lot of effort into making the standard workable and I urge you all to get a copy to see how your organisation measures up.

William List, a previous Chairman of this Group, has supplied a paper on the vexed subject of secure communication where he raises the subject of cryptography which leads nicely to our refereed paper from Simon Blake-Wilson and Fred Piper on the role of certification bodies in the administrating of digital signatures. Fred is one of the UK's top cryptographers and this is an area, which is growing in importance. Only recently one of my clients was picking my brains as to how they could be sure of the authenticity of important documents submitted over their Intranet. I suggested the use of digital signatures and, after an initial blank look, they are now pursuing this as a potential solution.

We also have our usual clutch of contributions from our BCS colleagues. Hazel Roberts, our cyber librarian provides details of the latest additions to the BCS/IEE library, while Colin Thompson updates us on our parent body.

The outline programme for next season is on the front cover and you will notice that we are once again running a number of free late afternoon meetings to complement our chargeable Technical Briefings.

Have a good summer. I look forward to seeing many of you at our meetings next season.

John Mitchell

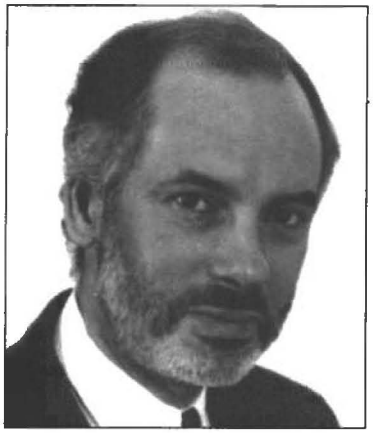
Chairman's Corner

John Bevan

I was elected chairman at the AGM on April 28th. I thought you might like answers to two questions. Will this mean any changes? Who is the new chairman?

I plan to continue the successful policies followed by my predecessor, Alison Webb. The committee are arranging three full day meetings in the coming season, but with a few more late afternoon meetings. We have been encouraged by the numbers who went to the late afternoon meetings on Y2000 and BS 7799 and hope that your support for the shorter format will continue. As before, many meetings are being arranged in collaboration with other groups. I have no specific plans for change elsewhere, although I am open to suggestions. I intend to explore and perhaps develop our group's relationship with the broader BCS, but as yet have little idea where this may lead. Having been on the CASG management committee under three different chairmen I know that any change needs the support of the whole committee, although it may be initiated by one person and not necessarily the chairman.

My background is both long and mixed. I remember nothing of the science that I studied first at university, and little of the Operational Research I did next. I worked for IBM, Logica, and



several computing departments, in programming, analysis, design, support, and consultanty roles, before moving into computer audit in banking. I spent many years here, ending up as an internal audit manager. I started my own business about ten years ago, doing training work initially, adding computer security and audit assignments, some research, IT project QA, system testing, and more recently IS evolution planning. It's good fun, and has taken me into several industrial sectors, roles, and countries that I've not been in before. I am a member of the IIA-UK. Despite the continuing emphasis on auditing I am still married. My wife works as a sculptor and artist. I have two grown-up daughters, one engaged and specialising in IT law - so beware!

Ghost in the Machine - An Analysis of IT Fraud and Abuse

The Audit Commission's latest survey of computer fraud and abuse indicates that computer crime is on the increase.

- survey results from 900 public and private sector organisations show that the percentage of organisations reporting incidents of IT fraud and abuse in 1997 rose to 45 per cent from 36 per cent in 1994
- one-half of all public sector organisations, and one-third of private sector companies, responding to the survey are now affected by IT fraud and abuse

And while key risk areas remain...·

- virus infections are still the single most prevalent form of abuse despite the widespread safeguards available
- all types of organisation reported some form of fraud or abuse
- the percentage of organisations reporting hacking incidents has trebled
- staff in managerial positions commit almost one-quarter of all frauds

...new dangers are emerging.

- the Internet exposes organisations to an increased risk that networks and systems will be accessed improperly, data corrupted and viruses introduced
- telephone systems are a new target for the fraudster

Some organisations have responded positively to the challenges posed...

- prevention is the key and one-quarter of organisations now have anti-fraud strategies compared to none three years ago

...but the overall position shows little improvement.

- frauds or cases of IT abuse often occur because of the absence of basic controls, with one-half of all detected frauds found by accident
- senior management still appears to lack a commitment to improving IT security and cracking down on abuse
- only one-half of computer fraudsters were dismissed or prosecuted

Organisations must renew their efforts in tackling IT fraud and abuse

- local government and the NHS are spending over £1.5 billion on IT
- all organisations are becoming increasingly dependent on IT
- it is essential that risks are recognised, minimised and effective safeguards established

The Internet, and the adaptation of Internet philosophies to internal systems, will be the cornerstone of IT activity in the coming years. The dynamic nature of these technological advances requires careful planning and management to maintain security and contain developing risks

Copies of the update are available from
Audit Commission Publications, Bookpoint Ltd,
39 Milton Park, Abingdon, Oxon OX14 4TD
Telephone 0800 502030

Price is £15.00 or £10.00 for NHS bodies and local authorities.

The Role of Certification Authorities

Simon Blake-Wilson and Fred Piper

Abstract. *Certification Authorities are likely to play a pivotal role in the expansion of the use of public-key cryptography and, in particular, digital signatures. This paper investigates the role of a Certification Authority.*

1 Introduction

Users of any public-key cryptographic system rely on the ability to obtain authentic copies of other users' public keys. Certificates and Certification Authorities provide an attractive solution to this 'public key distribution problem'.

A Certification Authority (abbreviated to CA) issues certificates which bind an entity E and its public key value PK_E. Each certificate consists of a message containing E's identity and PK_E digitally signed by the CA. Anyone in possession of E's certificate and the CA's public key can now obtain an assurance of the authenticity of PK_E by verifying the CA's signature on the certificate.

This solution to the public key distribution problem is attractive because the overhead involved for users is minimized: the distribution of all users' authentic public keys is reduced to the distribution of one CA's authentic public key. However users are required to trust the CA to sign only bona fide certificates.

The current expansion of the use of public-key cryptography and, in particular, digital signatures is leading to a need for CAs. However the role of a CA is complicated by the difficulties inherent in the operation of a CA. These difficulties stem from the stringent requirements involved. As a primary requirement, a CA will need to generate and distribute certificates securely and efficiently. As a secondary requirement, in some applications a CA will also need to be seen to act securely. For example, when certifying signature keys, a CA may become entangled in repudiation disputes and face liability if it is unable to demonstrate the security and validity of its actions. Add to these concerns the additional requirement of a commercial CA to make money.

In this article we provide a brief overview of the role of CAs and the operation of the certification process, focusing on those aspects which effect security. We discuss in turn three questions: How are entities identified and certificates produced? How are certificates distributed? What other services can a CA provide?

2 The Certification Process

The most fundamental task of a CA is to produce certificates. In a typical application, this process will involve the following events:

1. The key pair of the CA is generated.
2. The key pair of E is generated.
3. A certificate for E is requested.
4. E's identity is verified.
5. E's key pair is validated.
6. The CA produces E's certificate.
7. E checks that the certificate is correct.

Although it is clear that each of these events should take place, it is not at all obvious where they will occur in practice. Different applications are likely to require the tasks to be distributed in different ways. Often optimal security will be sacrificed and the practical distribution will differ from the ideal theoretical distribution.

We will discuss each of the events in turn. The composition of each task is described more precisely and the possible locations for the task are discussed from both a theoretical and a practical viewpoint.

Generation of the CA's Key Pair. Certainly a key pair must be generated for the CA if it is going to sign certificates. The key pair of the CA represents a highly attractive target for attack since knowledge of the private key of the CA allows the forgery of any certificate and hence impersonation of any user. Protecting the security of the generation of this key pair is therefore important. Precautions taken are likely to include: the use of a tamper-resistant module to generate the key, the use of a highly secure generation method, the use of highly secure (large) parameters, and possibly the distribution of 'shares' of the private key among several modules so that certificates cannot be created by any one device.

From a theoretical point of view, it is highly desirable that the CA generates its key pair itself. Otherwise the CA will have to trust the key generator not to retain a copy of the private key and produce spoof certificates, and the private key will be extremely vulnerable during its transportation from the key generator to the CA.

In practice it is certainly true that most CAs will generate their own key pair. A possible exception to this might be low level CAs within a certification hierarchy. It is conceivable that these CAs do not possess the hardware resources or the technical expertise to generate their own key pair and that, as a result, the requisite key pair is generated by a higher level CA. However we suggest that this course be avoided where possible due to the possibility of compromise during transfer of the private key as discussed above.

It seems reasonable to mandate that high level CAs must generate their key pairs inside their own tamper-resistant modules and that low level CAs may either generate their key pairs inside their own tamper-resistant modules or collect them from the tamper-resistant modules of higher level CAs.

Generation of E's key pair. Certainly a key pair must be generated for E. Although not as vulnerable to attack as a CA's key pair, compromise of an entity's key pair represents a serious security concern in most applications. A secure generation method should therefore be used to produce each entity's key pair.

In theory it is desirable that only E itself ever has possession of E's secret key. This is particularly pertinent in the case of signature keys; otherwise in the event of a repudiation dispute, E's defence call simply claim that the contested signature was produced by the other party who has accessed its secret signing key. Whatever the use of the key pair, if it is generated by another party, E will have to trust the key generator not to compromise the key, and the key will be

particularly vulnerable during its transportation from the key generator to E. Theoretically therefore we want each entity to generate its own key pair.

However, from a practical standpoint it is often unrealistic to expect that all entities will have the capability to generate their own keys. Since each entity is required to register public keys securely with a CA anyway, and CAs are likely to have a degree of technical sophistication, one obvious solution is for the CA to generate E's key pair, and hand over the secret key SK_E to E during the certification process.

In order to partially eliminate the security concerns this solution raises, the CA (or any other trusted entity) could generate E's key pair on a tamper-proof hardware Security Module that is configured to output keys only to the owner's storage device.

Certificate Request. In some systems, E (or some third party like a Registration Authority; see below) will approach the CA and request that a certificate is issued to E.

In this case, the medium used for the request will effect efficiency. The obvious options are either a paper-based request or an electronic request. Of the two, paper-based requests will be more cumbersome for the CA to handle.

If it is necessary for the CA to maintain a record of the request as evidence, then some sort of proof of the authenticity of the request will be required. Presumably a signature (written or digital) on the request will do the job. Note however, that if E is later required to acknowledge acceptance of the certificate, then it may be more pertinent for the CA to maintain evidence that E has accepted its certificate is valid (step 7).

(Alternatively, in the SET specification [5], E proves the authenticity of the request by including secret information like card number and expiry date. However this technique does not appear to provide as much security as a signature.)

As another possibility, we envisage that in many cases the CA itself will initiate the issuance of E's certificate. This mirrors current scenarios like the issuance of PIN numbers by banks.

Identity Verification. Clearly the CA needs some evidence that PK_E is E's public key before it agrees to issue a certificate to E.

The theoretical model here is simple: E provides the CA with a passport or some other form of identification as well as the public key PK_E. If E already possesses a certified signature key then the CA may instead accept a signature produced using this certified key testifying to the binding between E and PK_E.

In practice the difficulty with this approach is the workload it places on the CA. Often manual or paper-based tasks will be involved and it may be necessary to verify other attributes as well as E's identity.

Instead a third party known as a Registration Authority (abbreviated to RA) may testify to the binding between E and PK_E. One additional advantage of this approach may be that E may register with an authority (such as a bank) with which E has an established trust relationship. Another may be that RAs are run on a local basis so that E does not have to travel so far to register.

However, if the RA and the CA are two different entities, then this creates the problem of transferring evidence of E's registration from the RA to the CA. Again either paper-based or digital routines may be used. Since RAs are designed to remove the need for the CA to rely heavily on paper-based routines, digital routines appear more attractive.

A natural solution therefore is the use of registration certificates. These are certificates signed by the RA rather than the CA which testify to the binding between E and PK_E. Only the CA verifies a registration certificate, and if the certificate is correct, the CA then goes ahead and issues E with a full-blown certificate. Of course, now we have a new problem: who generates the RA's key?! Presumably the security requirements of an RA equate roughly with the security requirements of a low level CA.

A further difficulty associated with separating the roles of RA and CA is that disputes may arise between the two trusted entities in the event of a fake certificate appearing. The CA will probably therefore store registration certificates and produce them as evidence if such a dispute does arise.

The threat of a security breach during the transition from RA to CA means that it is often preferable to combine the roles of CA and RA. In existing (small scale) systems this is usually the case. However in future larger scale systems, this may place an unbearable workload on the CA.

(This means it is desirable that generic system specifications allow either possibility. This is the case with SET [5].)

Key Validation. Ideally the CA (or RA) should check that PK_E really is E's public key. This involves checking that E knows the private key SK_E corresponding to PK_E and checking that PK_E is a valid public key.

These checks have the dual purpose of protecting both E and the CA. They prevent E from mistakenly certifying the wrong key and they guard the CA against liability for certifying an incorrect or invalid key.

One way of checking that E knows SK_E is to have E simply show SK_E to the CA. If the CA has generated E's key pair anyway, this is a sensible solution. However in other circumstances, as we have discussed in step 2, E should avoid telling the CA SK_E if at all possible. An alternative solution in this event is for E to demonstrate knowledge of SK_E by transforming some challenge data, of the CA's choice using SK_E.

In high security applications, this challenge calculation should be performed in the presence of the CA, to prevent an impostor going away and collecting the required response by underhand means. Of course, it is unlikely that E is going to carry a large hardware device to the CA in order to carry out the check. So E will probably store his key on a smart card to transport it to the CA. The whole process is therefore only viable if the smart card has sufficient power to perform the challenge calculation itself.

If this presents a problem, some compromise will have to be made. Either E will be forced to reveal SK_E to the CA, or the CA will be forced to allow E to go away and calculate the response to its challenge (this is essentially the approach taken in SET [5]).

A third possibility is to omit the check altogether. Of course in this case neither E nor the CA receive the desired protection.

The means of checking that PK_E is a valid public key will vary depending on the system for which the key is being certified. For example, if E is certifying a key for a discrete logarithm based system, then it will involve checking that PK_E is a group element of an appropriate order.

Again, this check represents extra work for the CA and some applications may choose to take the risk of omitting it.

Note that both the above checks may also enhance the security of the entire system. Especially in applications like key agreement

and key transport, the security of the system may depend on ensuring that entities always know the private key corresponding to any certified public key or on ensuring that entities are only able to certify valid public keys.

Certificate Production. Once the CA is convinced that PK_E is E's public key, and that E wants to have a certificate testifying to this binding, the CA goes ahead and produces the certificate. Of course, we require the CA to sign the certificates securely.

The other issue is the contents of the certificate. Certainly as a minimum requirement the certificate needs to contain E's identity along with PK_E. It may also include information like:

1. the identity and possibly the public key of the CA.
2. the signature algorithm associated with the C.4's key pair.
3. details of the certification policy and the certification practice statement of the CA (possibly included by reference).
4. the serial number of the certificate (maybe to aid searching of certificate revocation lists; see Section 3).
5. the algorithm associated with E's key pair.
6. the address and affiliation of E.
7. the application for which E's key pair is intended (for example signatures or key establishment).
8. the details of limits on use of key (for example credit limit).
9. the method used to generate the pair (SK_E, PK_E).
10. the validity period for use of the private key (for example the period during which signatures may be created).
11. the validity period for use of the public key (for example the period during which signatures may be verified).
12. the status of certificate (in the case of revocation certificates; see Section 3).

This of course represents only a partial list of some of the possibilities. Since this may lead to overly cluttered certificates, it may in some cases be preferable to defer certain attributes to an associated attribute certificate. See Section 4.

It is desirable in many applications to produce certificates of a standard form. One emerging specification can be found in the standard ISO/IEC 9594-8 [4]. These certificates are commonly known as 'X.509 version 3 certificates'.

Certificate Acceptance. A CA should require some kind of notification that E accepts the certificate it has produced. Again this check protects both E and the CA; E receives additional protection against the mistaken production of a certificate, and the CA receives additional protection against liability if E later disputes the certificate.

As usual the acceptance may be digital or paper-based and some form of signature should be included in the acceptance to prove its authenticity. Either form of acceptance has its problems. On one hand, the processing of a paper-based acceptance will be more onerous for the CA. On the other hand, a digital acceptance signed using SK_E provides evidence only that the holder of SK_E accepts the certificate. If E later claims his certificate has been created by an impostor, such an acceptance will therefore carry little weight as evidence. Ideally therefore a digital acceptance should be signed by E using a (different) previously certified signing key.

Furthermore, the timing of the acceptance presents another problem. Does the CA withhold the certificate until it has received E's acceptance, in which case the user is acknowledging receipt before delivery, or does the CA issue the certificate and then ask for a receipt, in which case there will be a problem if the user does not provide a receipt?

The CA may partially avoid this problem if it can immediately revoke the certificate issued if it does not receive E's acceptance. It may also insist that the validity period for use of the key stated in the certificate begins some time later, so that the certificate is revoked in this event before it becomes valid.

Nonetheless these issues make the acceptance process problematic, and in some applications it is easy to imagine that it will be omitted; for example SET [5] does not include a certificate acceptance process. Of course this may increase the CA's risk of liability.

Whatever the distribution of events in the process of creating certificates that we have outlined in this section, it is likely that a CA will have to provide publicly available security policies. Chokhani and Ford [1] discuss the form these policies might take. They envisage two types of documents: a certificate policy and a certification practice statement. A certification policy contains details of the intended use and scope of a certificate and may differ from certificate to certificate. Each certificate contains a certificate policy. A certification practice statement (abbreviated to CPS) documents the processes undertaken and the methods used by the CA. Thus each CA is likely to have only one CPS, but may issue certificates with many different certificate policies. See [1] for an extensive discussion. Both certificate policies and CPSs assist entities when they decide whether or not to rely on the certificates issued. They also enable CAs to attempt to limit their potential liability by stating clearly the level of trust which they deem should be placed in certificates.

Presumably a CA will also maintain audit trails so that it can check that the methods and procedural controls used are indeed functioning. Provided the audit trails are secure and can be verified by a third party, they may also be used to convince entities that the CA is operating securely -- for example in the case of a dispute, the CA can produce the audit trails in court as worthwhile evidence of the security of its practices and procedures.

The Chokhani-Ford document [1] is part of an initiative known as PKIX [3] created by the Internet Engineering Task Force (IETF) which provides guidelines and standards related to the operation of Internet Public Key Infrastructures. For a further discussion of the certification process we refer the reader to PKIX [3], which describes in detail a variety of possible architectures and protocols. Also relevant is the book of Ford and Baum [2], which investigates in detail the role of CAs in the promotion of electronic commerce.

3 Distribution of Certificates

For the certification process to work, entities need to be able to access and check E's certificate. This is achieved by publicising the CA's public key and distributing E's certificate. In larger systems with more than one CA operating, E may also need to access the keys of other CAs. This is achieved typically by 'cross certification'.

In this section, we discuss these tasks as well as the related issue of key revocation.

Distribution of CA Keys and 'Cross Certification'. Typically, the CA's public key will be given to E at the same time that E gets a certificate.

E will need some assurance at this stage of the authenticity and quality of the CA and hence its public key to protect E against relying on bogus certificates created by a spoof CA. In situations where E

is paying the CA to produce *E*'s own certificate, this assurance will also reassure *E* that it is receiving value for money. The provision of this assurance would appear to require some form of CA accreditation - either in the form of a CA hierarchy, or in the form of a (formal or informal) CA licensing system.

In systems where more than one CA is operating, *E* may also want access to the public keys of the other CAs.

In practice it will be impractical if not impossible for *E* to visit all the other CAs to collect their public keys in person. Instead *E*'s CA may 'cross certify' the public keys of the other CAs.

In this approach, the CA obtains the public keys of the other CAs and gives copies of the keys to *E*, either by handing them over in person, or by issuing special 'authority certificates' binding each CA to its public key.

A related approach is to implement a hierarchy of CAs. Here high level CAs certify low level CAs. Now all *E* needs to verify any entity's certificate is the public key of the 'root' CA and a trail of authority certificates leading to the entity's certificate.

The process of cross certification raises two concerns for the CA.

Firstly, *E*'s certificate can now be checked by users of other CAs. This means that the CA's potential liability is increased. Provided the CA is issuing certificates securely, this should not be a problem, but disputes in other domains may interpret the CA's responsibilities differently. The CA may choose to limit potential problems of this kind by stating in the certificate policy which entities are allowed to rely on *E*'s certificate, and to what extent they may rely on it. If unwarranted reliance is placed on the certificate, the CA may then be able to deny responsibility.

Secondly, the CA can face liability for a certificate issued by another CA because it has implicitly supported the validity of the certificate by cross certifying.

To prevent this problem, the CA may wish to carefully vet the CAs it cross certifies. The vetting procedure may include inspection of the other CA's certificate policies and CPS. Note however that unless the other CA's policies have been independently audited, the CA must still trust the other CA over the accuracy of its policies. Government licensing of C.4s (or licensing of CAs by some other entity) may circumvent this problem.

Alternatively the CA may wish to include a statement in the certificate policy of each authority certificate it issues regarding the limit on the level of trust which it deems should be placed on certificates issued by the other CA. If this level of trust is exceeded, the CA may then be able to deny responsibility. Entities relying on long chains of certificates must then check the certificate policy in each certificate before judging whether its reliance on the relevant public key is justified.

The process of cross certification may also raise similar concerns for *E*. *E* will again need an assurance that each CA is reliable, otherwise *E* may end up relying on worthless certificates.

Distribution of *E*'s Certificate. Provided that the signature mechanism used by the CA is sufficiently strong, forging certificates will not be feasible, and, as a result, the method used to distribute certificates is not a security issue. However, the distribution method will affect the operation of the system. We distinguish essentially two methods: pushing certificates and pulling certificates.

Pushing Certificates, Pushing certificates means that entities are automatically provided with copies of certificates. Either *E* is given its certificate and sends the certificate along with its communications, or the CA itself sends certificates to all users.

On one hand, if *E* distributes its own certificates, the communication overhead *E* bears is increased. On the other hand, if all certificates are sent to all users, then the communication overhead of the CA is increased and each user is required to store all certificates. In systems where storage space is limited or there are a large number of users, this usually means that distribution of all certificates to all users by the CA is impractical. *E* distributing its own certificate to users as required is more viable.

Pulling Certificates. Pulling certificates means that entities request a copy of *E*'s certificate when they need it. Either all certificates are stored in a public directory (not necessarily maintained by the CA), or the CA answers each request separately. These solutions require the CA to be on-line.

The choice between the two approaches, pushing certificates or pulling certificates, will probably be made on an application by application basis, and hybrid solutions may prove popular. At the current time, pushing certificates appears more popular, presumably because it does not require the CA to be on-line. SET [5] is an example of the 'pushing certificates' approach.

In either case, the CA will probably also have to archive old certificates, for example so that signatures can still be verified after the expiry of the certificate or in the event that *E*'s certificate somehow becomes 'lost' (accidentally or deliberately).

Revocation. In most systems, it is unreasonable to expect that the private keys of users will never be compromised. Therefore it is necessary to have a mechanism in place so that users can revoke their certificates.

Since the CA is a trusted entity and is responsible for producing certificates, the burden for maintaining this revocation mechanism usually falls on the CA. In some circumstances this may be advantageous because it also allows the CA to revoke certificates easily; for example if its own key is compromised, or if an entity does not acknowledge receipt of its certificate.

(Note however that the CA does not always have to manage the revocation process. For example, in SET [5], the process is essentially managed by the financial institution authorising payments.)

Both phases of the revocation process represent a security concern: the request phase during which *E* asks for his certificate to be revoked, and the notification phase during which entities are informed of the revocation.

The revocation request mechanism will differ from system to system depending on the potential cost of revoking a perfectly good certificate and on the potential cost of delaying a genuine revocation request.

Presumably, in either case, *E* or some other authorised entity will approach the CA and request that *E*'s certificate is revoked. The request may be paper based, digital, or over the phone. On one hand, if the potential cost of incorrect revocation is high, then the CA will demand that the request is authenticated. On the other hand, if the potential cost of a delayed or ignored revocation request is high, then the CA will be loathe to delay revoking a certificate just because the request has not been authenticated. Similarly the costs involved will also affect which entities are allowed to revoke *E*'s certificate, and for what reasons they are allowed to revoke it. (Examples of entities other than *E* that may be allowed to revoke *E*'s certificate include *E*'s CA, *E*'s employer, etc.)

Whether or not revocation requests should be authenticated and where revocation requests should come from therefore depends on the application concerned. (Note that a request signed using SK_E certainly provides sufficient authentication: in this case either the request really does come from E, or the key really has been compromised!)

The revocation notification mechanism typically takes the form of a certificate revocation list (abbreviated to CRL) - this is simply a list (of the serial numbers) of the revoked certificates. The list is either stored in a public directory maintained by the CA or distributed directly to users. (CRLs are not the only way to run revocation notification mechanisms, but they are by far the most popular way. We do not discuss other techniques explicitly here - in any event all revocation notification mechanisms raise the same concerns as those discussed here.)

Since it is desirable to authenticate the CRL to prevent an adversary revoking valid certificates, either the whole list is signed by the CA, or each revoked certificate is signed individually. Individually signed, revoked certificates are known as 'revocation certificates'. Essentially they contain E's identity, PK_E, and a flag indicating that the certificate has been revoked. They are signed by the CA just like an ordinary certificate.

Managing revocation lists presents a major headache for the CA.

The workload of the CA is increased since it must always be on-line to revoke certificates no matter whether the CRL is stored in a directory or distributed to users.

The potential liability of the CA is also increased, since it faces the possibility of disputes with users over the management of the CRL; either with users who claim the CA did not revoke their key quickly enough, or with users who claim they have relied on a revoked certificate.

CRLs also present a major headache for users.

Each time a user wants to rely on a certificate, it should check the appropriate CRL as well. In many applications, to avoid this overhead, users will only check the CRL periodically. However this approach leaves a window of opportunity in the process which may lead to loss or disputes.

Despite these difficulties, the need for the ability to revoke certificates will nearly always be great enough that CAs and users simply have to face up to CRLs and the revocation process.

4 Other Services

A commercial CA may want to raise revenue by offering additional services. Indeed a CA is a natural candidate to offer a number of other trusted services. In this section, we mention a few possibilities. A brief description of each service is given, and followed by a discussion of whether or not it is desirable from a theoretical point of view for a CA to offer the service.

Timestamping Service. A timestamping service is trusted to testify to the existence of some data at a certain time. The data may consist of, for example, digital signatures or laboratory notes to support patent claims. Typically, the timestamper will append the time T to the data D, and then sign the resulting string. To check the stamp, anyone can now read the time from T and verify the appended signature.

One difficulty inherent in running a timestamping service is the possibility of compromise of the secret timestamping key. This is a worry because it can potentially expose the timestamper to enormous liabilities.

For example, suppose all important signed documents in a system are being timestamped as described above. If the timestamping key is compromised, then entities are able to repudiate all their signatures timestamped at any time, claiming that the signatures were created after the validity period of their signing key and then back-dated using the compromised timestamp key. In this circumstance, the timestamper may be found liable for all the signatures repudiated.

The severity of the compromise of a timestamp key can therefore be much more serious than the severity of the compromise of an entity's key or a CA's key. The effects of the latter are limited to a fixed timeframe (between the compromise of the key and its revocation), but the effects of the former are not time bounded (because the timestamper is able to backdate documents).

One solution is to require that all documents are timestamped by two independent Trusted Third Parties (abbreviated to TTPs). This solution minimises the possibility of the problem occurring, since both TTPs would have to be compromised at the same time. However it doubles the cost of timestamping faced by the user.

The other solution that has been proposed prevents the timestamper's ability to back-date. Essentially the timestamper publishes each timestamp it makes. This can be done reasonably efficiently using authentication trees. In this case however, the workload faced by the timestamper is greatly increased.

Do any additional theoretical drawbacks arise if a CA runs a timestamping service?

Suppose the CA is required to timestamp E's signatures. One reason that signatures are timestamped is to minimise the possibility that a signature is later invalidated by compromise of the corresponding certificate. If the CA and the timestamper are the same, then it increases the likelihood that the timestamp key and the certification key are compromised at the same time. This event could have catastrophic consequences.

From a theoretical point of view, there are therefore some drawbacks to a CA running a timestamping service.

Notary Service. A notary service is a more general service than a timestamping service capable not only of ascertaining the existence of a document at a certain time, but also of vouching for the truth of more general statements at specified points in time.

For example, rather than merely timestamping signatures, it may be desirable to notarise them. The relevant signature is sent to a notary, who checks the signature and appends to it both the time and a statement attesting to the validity of the signature. The notary then signs the entire string. A signature notarised in this way may carry more weight than a timestamped signature if it is later used as evidence in a non-repudiation dispute.

In theory, a CA who acts as a notary agent may run into conflicts of interest. It is clearly undesirable that the CA appear in court to defend itself against liability for a signature and have also to attest to the validity of the signature since it was the notary.

Name Server. The name server is responsible for assigning identities to users in a system. The name server is crucial to security in systems that use public-key cryptography and the certification process because users identities must be unique and unambiguous to prevent users relying on incorrect certificates.

Since the CA (or RA) will already have to testify to the binding

between E and its public key, it seems a natural candidate for the role of name server.

From a theoretical point of view, this situation may facilitate checks that all identities are unique.

Attribute Certificates. In Section 2, it became apparent that a certificate may get fairly lengthy if it lists all E's relevant attributes. To avoid this problem, E may instead have two certificates: one ordinary certificate binding E's identity and PK_E, and one 'attribute certificate' binding E and its other attributes (such as address, affiliation, credit limit, etc.). (Note that E's 'identity' may itself be something; we would usually regard as an attribute - for example in credit card systems, E's 'identity' may be simply E's credit card number.) Of course, a TTP is required to produce attribute certificates.

An additional advantage of the use of attribute certificates is that E can now change attributes like address and affiliation without having to revoke his ordinary key certificate.

The CA is surely the natural candidate to provide attribute certificates.

This situation may save E some time since presumably E can get an ordinary certificate and an attribute certificate at the same time.

Key Generation. Entities who wish to use cryptographic schemes need to generate keys. Frequently key generation procedures are complicated or inefficient and it is convenient for entities to employ a third party to generate keys for them.

Since a CA is a trusted party, and is presumably technically sophisticated, it is a natural candidate to provide key generation services.

Key Escrow. Escrow of keys is another service the CA may want (or be required) to provide. A copy of each key is stored so that it can later be retrieved, if needed, by an authorised entity (typically either the key owner or a law enforcement agency).

Of course escrowing of signature keys is usually undesirable because it complicates non-repudiation disputes. Nonetheless in some situations it may still be necessary - for example it may be required for legal reasons in countries like Japan.

There is no theoretical reason why the CA is not an appropriate party to store escrowed keys.

5 Summary

CAs will certainly play an important role as the use of public-key cryptography increases.

However the operation of a CA is demanding. Add to this the possibility that a CA may need to meet various legal requirements, and may need financial backing to guard against its potential liabilities. Furthermore in different applications, CAs are likely to face different requirements

In this article, we have outlined what some 'natural' requirements might demand of a CA, and how these requirements might affect system security.

We have also outlined some additional services that the CA may want to offer.

References

1. S. Chokhani and W. Ford. *Certificate Policy and Certification Practice Statement Framework.* 1997. Part of IETF PKIX [3].

2. W. Ford and M.S. Baum. *Secure Electronic Commerce.* Prentice Hall. 1997.

3. IETF PKIX. *Public Key Infrastructure (X.509)(pkix).* Details available from: http://vvv.ietf.org/

4. ISO/IEC 9594-8. *Information technology - Open Systems Interconnection - The Directory: Authentication Framework* International Organisation for Standardisation, Geneva, Switzerland, 1995 (earlier version ITU-T Rec. X.509, 1993).

5. SET. *Secure Electronic Transaction Specification.* Available from: http: //www.mastercard. com/

A Requirements of a CA

Based on the discussion in this article, we surmise that a CA will require:

1. A physically secure environment in which to operate.
2. Tamper-resistant modules for its cryptographic processing.
3. The ability to generate key pairs.
4. A random number generator and a pseudorandom number generator.
5. A smart card reader/writer.
6. The ability to check signatures (written or digital).
7. The ability to sign certificates.
8. Software to support all appropriate certificate formats.
9. Clear security policy documents (certificate policies and a CPS; see Section 2).
10. Secure, auditable procedures for producing certificates.
11. Possibly the ability to maintain a directory of certificates and archive certificates.
12. The ability to maintain a certificate revocation list.
13. Possibly the ability to provide 'other services'.
14. Financial backing to cover its potential liabilities.

Simon Blake-Wilson is a post doctoral research fellow at Royal Holloway College, University of London.

Fred Piper is Professor of Mathematics at the same university.

Communications and Security

William List

Introduction

The whole concept of EDI and the Internet relies on the ability to communicate securely. There are very many different computers and different software packages, or versions of packages, all of which handle data differently. The IT and telecommunications industries have therefore invested a substantial amount of time and money in developing the mechanisms to permit the communication to take place. The result is a set of rules that must be complied with if the communication is to be effective. These rules are called protocols or standards.

Security can be applied at different stages in the process of transmission depending on the requirements. Cryptography is a mechanism, which can be applied to achieve some security objectives.

Objective of Communication

The objective of any communication is to be understood by the listener or reader exactly as it was sent.

Subsidiary objectives are that the communication between the parties is secret and provably accurate.

Communications protocols

The Communications protocols can be broadly divided into the following groups:

- Those dealing with physical connections (e.g. plugs, wires, radio waves, etc.). These I will not cover further in this paper.
- Those dealing with the movement of messages over the 'wires'
- Those dealing with the content of the message

All the standards and protocols are specified in great detail and must be implemented with the same rigorous attention to the detail. Even the smallest error in the implementation can cause the communication to fail.

Movement of messages over the 'wires'

These protocols and standards govern the way the messages are transmitted and received so that the recipient receives what the sender sent. They also address all the usual problems encountered in Telecommunications (for example line failures, interference in radio waves, etc).

There are many protocols in this group; all are different, but in most cases the ability to convert from one to another is provided to users in the purchased software or modems. The protocols which are most widely used in UK are:

- X25, in the telephone system,
- X400 (and secure X400), used in government and elsewhere,
- OFTP (ODETTE File Transfer Protocol) used extensively in the EDI community,
- SNA (Systems Network Architecture) which is the main protocol in the IBM mainframe arena.

And for the Internet and Email

- TCP/IP used for the Internet,
- SMTP, for simple mail transfer (this is based on the standard character set and does not cope with signs or normal formatting commands),
- FTP, file transfer protocol for the transfer of files,
- MIME (and others), for compression of attachments to Internet mail.

These protocols cover:

- The structure of addresses for organisations, individuals and devices,
- The structure of the message during transmission - size of message, linkages between parts of one logical message, etc.,
- The interface between a device and a modem - line speed, parity bits, etc.,
- The interface between modems and switching equipment,
- The mechanisms for detecting faults in transmission and the number of retries before failure is accepted,
- The actions to take to deal with the normal telephony events (e.g. engaged numbers, failure to hang up correctly, etc.),
- The identification of the start and end of a session - the period during which one or more messages are sent,
- The identification of routing requirements,
- Many other technical details

Content of the message

This group of protocols and standards govern the way the data in messages is organised and the specific codes etc. used in messages so that the recipient can understand content of the message. These standards are independent of machine, business application and transmission mechanism. A consequence of the need for the content to be standardised is that the sender will usually require to translate the message into the standard form and likewise the recipient will require to translate the message out of the standard form and into a form usable by the recipient's application programs. The oldest example of this in UK is the BACS standard format, which has been used since the 1970's in all financial messages processed through the BACS system.

Today some software packages are using the standard formats to store the data thereby avoiding the need for translations.

Some of the standards used in the commercial world in UK are:

- BACS - for movement of monetary messages to and from BACS,
- SWIFT - for movement of monetary messages internationally,
- EDIFACT - a series of standards for commercial messages,
- TRADACOMS - a series of standards for commercial messages owned by the ANA (Article Number Association) and mainly used in Retail and Distribution.

Note: there are derivatives of the EDIFACT messages created by user groups to meet specific industry sector requirements.

There are no real standards for the movement of word processing documents. Documents created in the latest version of a word processor or under a particular operating system or application suite may not be readable in an earlier version or may only be readable as text (i.e. without formatting). As a courtesy it is sensible to ensure that your documents can be read by the recipient before transmission.

Security of data being transmitted

Security in this context covers confidentiality, completeness and authentication of senders or recipients. Organisations require to take other measures to ensure the availability of their communications capability. It is assumed in this paper that adequate access controls exist in any network to exclude organisations and individuals who should not have access to equipment or systems.

Security may be applied at various stages throughout the process of communication.

As examples:

At the physical level:

- Equipment can be locked up,
- Equipment can be disconnected from the network whilst not in use,
- Confidential data can be physically moved to a networked machine when transmission is to take place,
- Modems can turned off when not in use.

At a physical connection level

- Special wiring can be used to inhibit the placement of listening devices,
- Networks can be swept to locate any listening devices. During transmission
- Transmission failures can be detected (in most software/hardware functionality exists to do this),
- Anonymous messages may be sent (but someone, somewhere is able to identify who sent the message, even if the recipient is not),
- If the security concern is to hide the fact that the transmission occurred between parties it is possible to encrypt the details of the sender and recipient ; but if this message has to be routed through a number of computers then each has to decrypt sufficient to pass the message on.

At the message level

The majority of security procedures applicable to messages are usually performed on the translated messages immediately prior to transmission and checked on receipt prior to the translation into the form necessary for further processing. Care must be taken when applying these measure to ensure that the business objective is fully met.

- A 'hash total' or 'checksum' of (some of) the contents of the message can be created. This is called a MAC in some systems. When the checksum is recomputed on receipt, failure to agree indicates changes since the checksum was applied.
- All or some of the contents of the message can be encrypted.
- A particular form of encryption is used for credit card transactions over the Internet. This is the SET standard. This allows the merchant and the card issuer to only access those parts of the transaction relevant to their processing and inhibits the stealing of credit card numbers electronically.
- The address of the recipient and any cryptographic keys can be confirmed by a Certification Authority.
- A digital signature can be applied to the message. A digital signature is a cryptographic mechanism which computes a result from a combination of the message content and the identity of the sender (an individual or organisation).
- Messages can be sequence numbered.
- Various control totals of message sent or received can be created for comparison with totals generated by business applications to ensure completeness of processing.
- A receipt for a message can be generated. Certain receipts are 'non-repudiation' receipts which means that the recipient cannot subsequently deny receiving the message.

In addition to the measures above, organisations can take steps to prohibit the receipt of unwanted messages. These measures are usually incorporated into a Firewall which is piece of software (or hardware) which examines all incoming messages and rejects unwanted messages. Examples of the restrictions that can be imposed are:

- Only permitting the receipt of messages for selected individuals or departments,
- Not permitting file transfers,
- Not permitting the receipt of software or documents containing macros,
- Rejecting any message containing a (known) virus,
- Rejecting messages from sources known to convey unwanted material (e.g. pornography).

Control of the business process using communications

In addition to the technical controls identified above, organisation will require to maintain their business controls. These may require to be redesigned to take advantage of the technical control introduced and to ensure they constitute an effective control over the

new system. These controls are applied in the business applications, which either creates messages to send or process the received messages.

Examples of business process controls

- Appropriate authorisation of all messages which create a commitment for the organisation.
- Credit checking before acceptance of orders.
- All computers use codes to convey meaning. Controls must exist to ensure that the codes used in the messages are really the ones that mean exactly the same to the recipient.
- Evidence that all messages due to be sent were completely transmitted and all messages received were completely processed by business applications.
- Procedures to notify senders if the business applications cannot process their messages or they are lost.

Cryptography

Cryptography is a mechanism which may be used for three linked but different processes:

- Scrambling a message or document so that only people with the cryptographic keys can read it,
- Providing a unique means of identifying a person or organisation electronically,
- Providing a means of linking a person or organisation uniquely to the contents of a document or message - a digital signature.

A cryptographic mechanism applies a mathematical process to a key (or keys) and the data to be encrypted so that only those with the keys, using the correct mathematical process, can decrypt the information. All cryptography can be broken given sufficient time and effort except for a one off short message using unique keys. Therefore the discussion about strong and weak cryptography is a relative debate about how difficult it is to 'break'. With the greater use of computers, as a general rule, the bigger the key length then the longer it takes to break and the stronger the cryptography, given a competent mathematical process. It is also true that as the power of computers increase what was unbreakable today may well be easy to break in 'N' years time.

There are two basic types of cryptography:

- Symmetric - where both (all) parties who need to read things have the same cryptographic key. For example DES.
- Asymmetric - where there is a public key which is readily available and each person or organisation has their own private key. For example RSV and PPG.

In the case of symmetrical cryptography both parties use the same key and therefore it is necessary to ensure that the keys are distributed securely and kept locked up, if they are in a physical form. This requirement imposes considerable overheads on the systems.

With asymmetrical cryptography each user has a public and a private key. The public key is open to all and the private one never disclosed. The security problem is then whether the public key used really belonged to the user that one expected, and therefore Certification authorities are being created to confirm the genuineness of public keys.

Governments worldwide are concerned that if everyone uses cryptography then their ability to gather intelligence will be diminished. Therefore there are proposals to hold keys in Escrow by Trusted Third Parties, which can be accessed by the authorities after obtaining a warrant. The mechanisms to achieve this were the subject of a consultation paper in spring 1997 and further proposals were published in April 1998.

Conclusion

Today there is an ever increasing use of electronic communication in the World-wide economy. Protocols and standards are used to ensure that recipients understand precisely what is sent to them. All messages require to be in a standard form and this means procedures need to exist to ensure that the computers used in the communication can pass messages to the correct destination without corruption. These protocols are detailed technical procedures.

Cryptography is a mathematical process which can be used to protect the confidentiality of messages, demonstrate they have not been tampered with and identify who sent the message.

Functionality can be provided in software or hardware to ensure that the communication of messages is secure. The precise mechanisms that are appropriate for an organisation need to be determined in the light of the messages being communicated. It is necessary to achieve effective control to ensure that the security of messages before and after transmission is as effective as the security whilst in transit.

Secure Electronic Commerce is possible. To achieve it only requires the effective deployment of the tools available.

The views expressed in this paper are those of the author and do not necessarily represent those of his company, or any professional body. No responsibility can be accepted for any loss, injury or harm suffered by any person or organisation as a result of action or inaction based on this synopsis.

William is a partner of the Kingswell Partnership Ltd, a Fellow of the BCS and a Chartered Accountant. He can be contacted at:
The Kingswell Partnership Ltd, The Forge, Faringdon Road,
Kingston Bagpuize, Oxfordshire OX13 5AG
Tel +44 (0)1865 822010 Fax +44 (0)1865 822011
Email 100416.13@compuserve.com

. . . .and the End Piece to end all End Pieces . . . .
(from The Guardian, 13th May 1998)

In Germany, emergency medical treatment has rescued Werner Hertz from serious injury Mr Hertz, a Munich businessman, was rushed to hospital with his mobile phone inserted in his rectum. He had passed out, naked, on his office floor, Paul Sussman reports in the Big Issue, and only the fortuitous depression of the redial button as he fell, which alerted his wife to "strange gurgling sounds", saved him. Mr Hertz was reticent about the cause of the insertion. "In business," he was only prepared to say, "you must be prepared for every eventuality."

BS 7799 Accredited Certification Scheme

John Bevan

What is the scheme?

Barbara Roche, a minister at the Department of Trade and Industry, launched the new accredited certification scheme for BS 7799 at Infosecurity in April 1998. These notes are based on an April 16th briefing the DTI gave to interested parties, including your new chairman. The scheme will be operational later this year, and has been branded 'c:cure'.

The scheme is intended to allow organisations to benchmark their security against a recognised security standard, removing concerns that might otherwise inhibit more electronic trading between organisations.

The certification scheme has similarities to that for BS 5750 / ISO 9000, involving (for BS 7799):

- certification bodies issuing compliance certificates,
- an accreditation body (UKAS - see references) to accredit certification bodies,
- registered auditors employed by certification bodies to perform compliance audits,
- a register of auditors (run jointly by the BCS and International Register of Certified Auditors), and
- a register of organisations certified as compliant with the standard, run by the scheme manager (BSI/DISC - see references).

The new scheme certifies against the standard BS 7799: Part 2 Specification for Information Security Management Systems, published by the British Standards Institute in February 1998, itself a development of the earlier and better known BS 7799 Part 1 Code of Practice for Information Security Management Systems, published by BSI in 1995. Both must be purchased from BSI (see references).

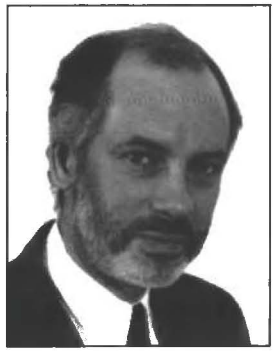
As an article in an earlier edition of this journal indicated was likely, BS 7799 part 2 differs from part 1 in a number of ways, most notably by:

- requiring an organisation seeking certification to perform a risk assessment to select those controls specified in BS 7799 part 2 which it judges are appropriate to its operations, and to record the selection in a Statement of Applicability, and
- envisaging that new or updated security controls will be added by referring to other security standards as they are developed in future.

BS 7799 part 2 addresses the security of all of an organisation's information, not just its IS security. The BCS Security Committee was influential in formulating both the content of the new standard and the certification scheme. The BCS will help operate the BS 7799 auditor register (see later). These notes concentrate on the certification scheme, making only passing reference to the BS 7799 part 2 standard.

What is certified?

BS 7799 part 2 certificates will identify the organisation concerned, and will be in the public domain. An organisation can seek certification for all or part of its organisation, processes, and/or



operations. It is not yet clear how this will be described on the certificate. Certificates will normally be valid for 3 years. Some organisations have already received certificates during a pilot of the certification scheme.

The appointed certification body will review the Statement of Applicability. Organisations may make it available to trading partners, but are not required to do so. It will not be in the public domain.

The standard does not specify what risk assessment method must be used. The appointed certification body will review it. Guidance on risk assessment is published by BSI/DISC (see references).

Scheme Managers

BSI/DISC (part of BSI) are Scheme Managers. They will:

- meet the evolving needs of customers and other interested parties by setting up a Scheme Steering Committee,
- carry out quality control for the scheme as a whole,
- publish lists of accredited service providers,
- publish lists of certificate holders, and
- publish guides (see references).

Who can be a BS 7799 auditor?

Only an accredited certification body, employing registered auditors, can carry out compliance audit work leading to the issue of a BS 7799 certificate.

The following details have been extracted from the BS 7799 Scheme Protocols provided by BSI/DISC for the 16/4/98 DTI briefing, and available free of charge to interested parties from BSI/DISC (see references). Potential applicants should read the Scheme Protocols for the full list of requirements. BSI/DISC reserve the right to vary the protocols from time to time.

There will be auditor training, aptitude, qualification, character and identify checks, certification, and registration processes, as well as interim arrangements during the set up period (but with full compliance required later). The register of auditors will be run jointly by the BCS and the International Register of Certified Auditors (IRCA), and is expected to be in place by September 1998. Qualification will be by examination (syllabus expected to be available in late summer) and interview.

Auditor grades will be:

- Provisional BS 7799 Auditor,
- BS 7799 Auditor, and
- Lead BS 7799 Auditor.

All grades must:

- be educated to degree level or hold a relevant professional or business qualification,
- have successfully completed a 2 day BS 7799 Certification Practices or 5 day BS 7799 Auditor's course,
- pass a BS 7799 Auditor's examination up to one year before applying for registration, and
- possess good inter-personal skills and advanced problem solving abilities exercised within the Information Security and/or IT sectors.

Auditor re-certification will be required every 3 years, with checks on the maintenance of competence, and on having undertaken a minimum of 5 audits in the preceding registration period (3 years). A lead auditor must have participated in 2 out of these 5 or more audits as lead auditor.

All grades must have the following work experience (the periods below may be concurrent):

- 4 or more years full time appropriate general work experience
- 3 or more years of substantial and applied information security work within the scope of BS 7799
- 3 or more years of full time substantial varied and practical work experience of IT, including networks
- 2 or more years awareness and experience of applying relevant technical and procedural standards constituting an Information Security Management System or other similar Management System (e.g. quality systems)

There are other requirements, some being grade dependent. There are requirements for auditors' Continuing Professional Development (CPD). The BCS CASG committee is checking how its meetings and seminars will qualify for BS 7799 CPD.

References

BSI Customer Services, 389 Chiswick High Road, London W4 4AL, or telephone 0181- 996 7000, with a valid credit card to order:

BS 7799 Part 1 *Code of Practice*, 1995, £94.00

BS 7799: Part 2 *Specification for Information Security Management Systems*, 1998, £36.00

c:cure office, BSI/DISC, 389 Chiswick High Road, London W4 4AL, telephone 0181-995 7799, fax 0181-996 6411, e-mail c_cure@bsi.org.uk, for the following BSI/DISC publications:

DISC PD 3000 *Information Security Management - an introduction* £9.50

DISC PD 3001 *Preparing for BS 7799 Certification* £27.50

DISC PD 3002 *Guide to BS 7799 Risk Assessment and Risk Management* £27.50

DISC PD 3003 *Are you ready for a BS 7799 Audit?* £22.50

DISC PD 3004 *Guide to BS 7799 Auditing* £34.50 (for BS 7799 auditors)

Pack 1 Audit/Consultant pack PD 3002 + PD 3004 £55.00

Pack 2 User pack PD 3001 + PD 3002 + PD 3003 £65.00

BS 7799 Scheme Protocols free of charge (for auditor certification & registration, and scheme funding)

The Web site http://www.bsi.org.uk/bsi/disc or http://www.bsi.org.uk/disc gives more information.

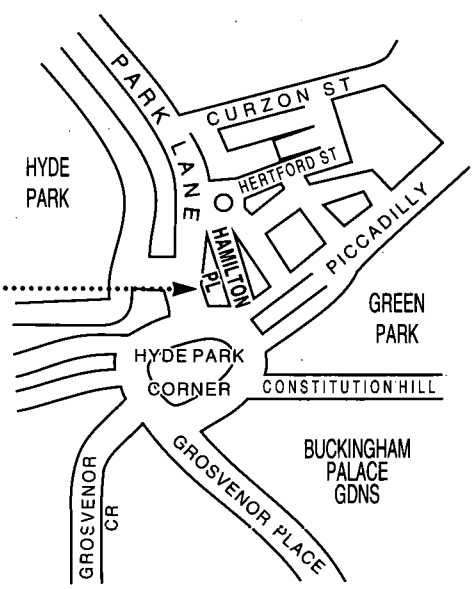
Roger Brockway, UK Accreditation Service (UKAS), 21-47 High Street, Feltham, Middx, TW13 4UN, telephone 0181-917 8400, fax 0181-917 8500

Footnote - CASG participation

If you are a member of the BCS or BCS CASG, and would like to influence the future direction of the BS 7799 standard, the BS 7799 accredited certification scheme, or any other public policy matter of concern to computer auditors, contact the BCS CASG chairman or committee member so that we can do it together and with the BCS. Alternatively you can contact the BCS Security Committee.

Venue for Technical Briefings

Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ



BCS MATTERS

Colin Thompson
BCS Marketing Director

Colin Thompson, BCS Marketing Director, reviews some of the current BCS news items. Requests for further information on these or any other BCS related issues, should be addressed to Customer Services at The British Computer Society, 1 Sanford St Swindon SN1 1HJ or by e-mail to marketing@hq.bcs.org.uk

BCS Registers

Further progress on both the new BCS Registers since my last column. Readers will recall that the Security Register was set up in October last year, with registration restricted to BCS professional members and Companions. There has been a good level of response from members - and from non members making a joint application for membership and registration - and the Register is now available to the public.

More recently, the Society has reviewed the question of the BCS membership restriction, against the background of BS7799 certification and the need to create authoritative listing of competent security practitioners. At the meeting on 23 April, Council approved the removal of that restriction and, in the very near future, we shall be announcing the Register is open to non members. Applicants will, of course have to satisfy the same requirements in respect of competence and experience. They will also be required to commit to the BCS codes of conduct and practice and will be subject to similar disciplinary procedures.

The second new register - the Consultancy Register - has also moved forward and is now open for applications. Unlike the Security Register, this one remains restricted to BCS professional members and there are no plans to change that position. Information packs are available from Customer Services at BCS HQ, or via the BCS Web site.

The Pollard Review

Yet another topic mentioned last time. This review, being chaired by Brigadier Alan Pollard, is looking at the future scope of BCS membership. Alan put an interim report to Council on 23 April suggesting four possible options for the BCS of the future, which he labelled as follows:

Scenario A - The status quo.

Scenario B - A Society with broader-based qualifications.

Scenario C - A Society embracing both qualified and non-qualified members.

Scenario D - A Society catering for members and non-members.

Council expressed a very strong preference for Scenario C, moving in time to Scenario D. Given this guidance, the Working Party will now undertake the further work necessary to produce recommendations by September of this year.

European Computer Driving Licence (ECDL)

The ECDL scheme was officially launched on 11 May at an event at which Deputy President Ian Ritchie presented licenses to the first successful candidates in the UK.

To recap, ECDL is a new Europe-wide qualification for which the BCS is the UK licensing authority. It is designed to enable people to demonstrate their competence in computer skills, with a syllabus broken down into seven modules, each of which must be passed before the ECDL certificate will be awarded:

• Basic concepts of IT • Using the computer and managing files • Word processing • Spreadsheets • Databases • Graphics • Networking

ECDL looks set to become the most widely recognised qualification in the field of work-related computer use. It is currently operating in thirteen countries of Europe with several more being involved in the near future. Overall there are around 100,000 individuals and the BCS now has more than 60 licensed test centres around the country.

IS management Awards

Halifax Share Dealing Limited (HSDL) has won the1998 BCS IS management award. HSDL was set up to deal with the flotation of what was the Halifax Building Society and received the award for the way in which it handled an enormous task, involving 21 million customers, 16 million eligible for shares, 9 million transactions, 75 million letters, and 25 million telephone calls.

As Nigel Horne, the chairman of the awards judging panel said when he presented the award "the Halifax rose to the challenge with the new technology, textbook sponsorship from the Board downwards, massive user involvement, and real-time integration with other systems including external agencies. Not only that they decided to build a totally new business on the back of the opportunity and turn what could have been a £9M cost into a £6M profit for the company."

BCS Publications

The BCS has published the third volume in its Y2K series. The report looks at new issues which have emerged and those previously covered which have developed into major concerns. Subjects covered include:

- information security
- EMU
- current legislation
- general insurance
- personal indemnity
- embedded systems
- data communications

Volume 3 is available individually at £20 or packaged with volumes 1 and 2 at £40 . Both figures are subject to 25% discount for BCS members.

A fourth volume in the Y2K series is planned for later in the year, together with a further report in the EMU series. Other titles in prospect for 1998 include the new Data Protection legislation and e-commerce. Details of all BCS publications are available from Customer Services at BCS HQ.

And Finally.....

News of changes at the top of the BCS. At the April meeting Council approved the following nominations for Honorary Officers:

Ian Ritchie to be President 1998-99

David Hartley to be Deputy President 1998-99

BCS MATTERS

Mike Allen to be Honorary Treasurer 1998-2001 (replacing Gerry Fisher)

John Ivinson to be Vice President Professional and Public Affairs 1998-2001 (replacing Mike Allen)

Frank Moran to be Vice President Branches 1998-2001 (replacing David Holdsworth)

All new Honorary Officers will take office at the end of this year's Annual General Meeting, which will take place in the Playfair Library, Old College, Edinburgh University at 2pm on 22 October 1998.

Library Update

Hazel Roberts - BCS Librarian

Since my last column, the BCS Library has received and added to its book stock many new titles which would be of interest to CASG members. In particular we have received a number of books on the subject of computer security, which includes security and the internet. Other subjects of interest to readers are systems development, disaster recovery, and computer crime.

The BCS Library holds a number of Computer Security journals in its stock: Computer Fraud and Security, Computers and Security and Computers and Law.

To search our library stock it is possible to contact us via the Internet, which is proving to be very handy to members. The Library catalogue can be found at the following address:

http://www.iee.org.uk/Library/Catalogue/Simple-search.html

Unfortunately our Journals catalogue is not available to search as yet on the Internet, but will be in the near future.

Here is a list of all the new books which are now available to borrow or look at within the BCS/IEE Library:

COMPUTER SECURITY

ZETLIN M
The Computer time bomb: how to keep the century date change from killing your organization.
AMA Membership publications
1998
ISBN: 0-8144-2365-5

INTERNET SECURITY

KEEN P G W, BALLANCE C
On-line profits: a manager's guide to electronic commerce
Harvard Business School
1997
ISBN: 0-87584-821-4

MILLER M, ROEHR A J, BERNARD B
Managing the corporate intranet
J. Wiley and Sons
1998
ISBN: 0-471-19978-8

BAYLES D L
Extranets: building the business-to-business web
Prentice Hall
1998
ISBN: 0-13-650912-6

DENNING D E, DENNING P J
Internet besieged: countering cyberspace.
Addison-Wesley and ACM
1998
ISBN: 0-201-30820-7

GONCALVES M
Firewalls Complete
McGraw-Hill
1998
ISBN: 0-07-024645-9

BISAILLON T, WERNER B
TCP/IP with windows NT illustrated
McGraw Hill
1998
ISBN: 0-07-913648-6

SOLOMON J D
Mobile IP: the internet unplugged
Prentice-Hall
1998
ISBN: 0-13-856246-6

LOSHIN P, MURPHY P
Electronic commerce: online ordering and digital money.
Charles River Media
1997
2nd Edition
ISBN: 1-866801-67-3

Hazel Roberts -
BCS Librarian,
IEE/BCS Library
Institution of Electrical Engineers,
Savoy Place,
LONDON,WC2R 0BL
Email: hroberts@iee.org.uk
Telephone: +44 (0)171 344 5449
Fax: +44 (0)171 497 3557
World Wide Web: http://www.iee.org.uk/

Management Committee

CHAIRMAN	**John Bevan**	**Audit & Computer Security Services**	**01992 582439** **john.bevan@virgin.net**
SECRETARY	**Raghu Iyer**	**KPMG**	**0171 311 6023** **raghu.iyer@kpmg.co.uk**
TREASURER	**Andrew Barton**	**Orange plc**	**0171 766 1600** **andrew.barton@orange.co.uk**
MEMBERSHIP SECRETARY	**Jean Brown**		**01803 872775** **100125.66@compuserve.com**
JOURNAL EDITOR	**John Mitchell**	**LHS Business Control**	**01707 851454** **lhs001@aol.com**
SECURITY COMMITTEE LIAISON	**John Bevan**	**Audit & Computer Security Services**	**01992 582439** **john.bevan@virgin.net**
TECHNICAL BOARD LIAISON	**Allan Brown**	**Consultant**	**01803 872775** **100125.66@compuserve.com**
TECHNICAL BRIEFINGS	**Jenny Broadbent**	**Cambridgeshire County Council**	**01223 317256** **jenny.broadbent@finance.cambscnty.gov.uk**
	David Cox	**Lombard North Central plc**	**01737 776286** **dcox@lombard.co.uk**
	Mike Demetriou	**Lombard North Central**	**01737 744111** **mdemetriou@lombard.co.uk**
	Jim Jackson	**Lombard North Central plc**	**0181344 5671** **jjackson@lombard.co.uk**
	Paul Plane	**National Westminster Bank plc**	**0171 726 1000**
	Diane Skinner	**District Audit**	**0117 9001418** **dskinner@district-audit.gov.uk**
	Alison Webb	**Consultant**	**01223 461316** **amwebbcam@aol.com**

Membership Enquiries to:

Jean Brown
Whiddon Lodge
Abbotskerswell
Newton Abbot
Devon
TQ12 5LG

British
Computer
Society

PLEASE RETURN TO
Jean Brown
CASG Membership Secretary
Whiddon Lodge
Abbotskerswell
Newton Abbot
Devon
TQ12 5LG

Membership Application

(Membership runs from July to the following June each year)

I wish to APPLY FOR membership of the Group in the following category and enclose the appropriate subscription.

CORPORATE MEMBERSHIP (Up to 5 members)* £75

* Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal *(see over)*

INDIVIDUAL MEMBERSHIP *(NOT a member of the BCS)* £25

INDIVIDUAL MEMBERSHIP *(A members of the BCS)* £15

BCS membership number: _____

STUDENT MEMBERSHIP (Full-time only and must be supported by a letter from the educational establishment).

Educational Establishment: _____ £10

Please circle the appropriate subscription amount and complete the details below.

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: (Please circle) 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)
SIGNATURE: DATE:

PLEASE MAKE CHEQUES PAYABLE TO "BCS CASG"
AND RETURN WITH THIS FORM TO THE ADDRESS SHOWN ABOVE

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)