tScheme response to FSA Discussion Paper on Electronic Signatures in e-Commerce

Q45: How do you see the business to business and consumer to business markets for digital certificates developing?

The market for electronic trust services is at present still emerging, and specific services have yet to be defined clearly enough to be marketed aggressively.

There is already a substantial market for server certificates to support SSL (order 100,000 per year), and many businesses have bought such certificates. However, certificates for individuals – whether customers or business employees – have not sold in anything like these numbers. Until businesses and consumers understand more fully how personal digital certificates can be used to remove costs and create new opportunities, they will continue to wait and to watch developments before getting directly involved. Indeed, some will not even be aware that the technically-biased debate which has continued for the past two or three years, with its focus on PKI hierarchies, has anything to offer real businesses in terms of services and applications.

This challenge of market education will be difficult to meet – especially since much of the recent enthusiasm for the internet and e-commerce has waned as quickly as share prices in most dot.com businesses have tumbled. Given these circumstances, rather than attempting to educate all sectors of the business and public communities at the same time, the sensible approach is probably to target specific areas which are further advanced, in terms of their receptivity to the potential opportunities offered by electronic trust services.

In this respect, business communities of interest or supply chains already operate based on established trading relationships, within which a level of trust already exists. Since a focus on specific services and applications relating directly to business needs within these trading groups will be simpler to achieve, these therefore appear to offer one relatively favourable environment for new trust services to flourish. Once established, case studies describing the specific services being used, and their business applications and benefits, can then be made known to a wider business

community to encourage similar initiatives in other areas of the market. Regulatory issues – for instance a requirement for legal signatures in an electronic environment - may well drive particular deployments.

As far as the individual consumer is concerned, there is little incentive to pursue ownership of digital certificates. It will probably be the individual's involvement with digital certificates within a business community of interest – either as an employee or as a customer of a supply chain member company – that will eventually encourage the individual consumer to enter the market to any significant extent. Alternatively, consumers may over time become engaged in transactions which use digital certificates enabled for personal devices, without ever being explicitly aware of this fact. (Very few are aware that certificates are used in SSL, for example).

Q46: Should it be possible for an electronic signature supported by a certificate issued by a third party, which has complied with the non-face to face requirements set out in the JMSLG Guidance Notes, to be relied on by a relevant firm as evidence of identity, sufficient to enter into a relationship with the customer? Does this obviate the need for any further checks to be performed before an account is opened?
Q47: Alternatively, might such a signature require only a reduced number of checks to be performed, for example a single check on the address for fraud purposes, or one check on an address and another on identity?

tScheme does not consider that these questions lie within its principal area of expertise, and so does not wish to enter a response here.

Q48: If an authorised firm can rely on an electronic signature issued by a trust service provider in the UK for the purpose of entering in to a relationship with a customer, should an authorised firm also be able to rely on such a signature

where the certificate is issued by a trust service provider outside the UK? If so, should any additional checks be required, and, if so, in what circumstances?

tScheme does not consider that these questions lie within its principal area of expertise, and so does not wish to enter a response here.

Q49: What identity-related attributes do you believe should be held in or to support the certificate?

Rather than listing the attributes that should be retained it is better to state the requirement that the information must satisfy. This means sufficient information, according to the underlying risks, to locate and identify the subscriber uniquely. However privacy issues may, in specific cases, require that this information is held in support rather than within the certificate.

However there are of course many other certificate types suitable for use in different business contexts, and which could be more anonymous, for example those simply containing or supported by a role-based attribute.

In general, certificates used to introduce an individual to a relying party will need to be more informative than those used to authenticate an individual already known to the relying party by other means. In the latter case, an anonymous identifier is perfectly acceptable, provided that the relying party is willing to accept it. In the former, some combination of name, address, telephone number, email address would be better, provided the subscriber consents to this information appearing in a public directory. (Most users already do so for other services).

Q50: Are there any other material risks arising from the use of electronic signatures that are related to money laundering or to the need to reduce financial crime?

The initial registration of the proposed recipient of a digital certificate is a critically important step in creating the required level of trust in transactions the certificate is later used to support. Service approval of Registration services by an independent trust service self-regulatory body such as *tScheme* ensures that best practice in service management and delivery is being maintained. Service approval will therefore be an important indicator of the level of assurance when relying on the identity represented by a digital certificate.

Accordingly, relying financial parties should not rely solely on digital certificates for authentication but use additional controls commensurate with the risks.

Q51: As regards record keeping, what requirements and arrangements should there be to ensure that years or several decades later it can be shown that a certificate had been properly established, and that it had been checked and found valid at the time of use? What services supporting such verification, if any, need to exist before the acceptance of electronic signatures is allowed?

Proper initial establishment of a certificate is assured by validating the quality of the Registration Authority and its registration policy and processes. *tScheme* is of course designed to approve this type of service to an appropriate standard.

In answer to the second part of the question, many schemes have developed to prove that a certificate has been properly validated by a relying party or its agent. The archives that include audit records would need to be securely time-stamped and stored in compliance with regulatory requirements and where appropriate, in accordance with the organisation's risk management requirements.

When the requirement extends far into the future, certificate expiry dates become a problem, since TSPs commonly use this date to indicate withdrawal of any further interest in or support for a certificate. Long lived reliance issues like these have been extensively discussed in EESSI however.

Q52: Is the ongoing integrity of a digital certificate as important as the identity checks when the certificate is issued?

Yes, but it is easier to assure by use of cryptographic mechanisms of sufficient quality alongside appropriate security measures for ensuring the confidentiality of the key that signed the certificate. (For example don't store keys unprotected on PC disk-drives). Compared with the problem of initial identity checking and subsequent changes of status, this is a relatively straightforward problem to solve. Clearly, there is a requirement that the subscriber inform the certification authority promptly of any changes to the information held in his certificate: but enforcing this is rather hard.

Q53: Are these objectives (i.e. confidence in registration practices, certificate policy, validity, and certification authority practices) reasonable ones? Are there any other key objectives that need to be met?

Yes these issues of confidence are reasonable, and *tScheme* can help meet them. Service approval by *tScheme* as an independent regulatory body relates to the business probity of the trust service provider, the integrity both of the organisation and of the services and management practices defined, and to the method of service delivery.

tScheme does not mandate any aspects of trust service design, nor does its approval warrant fitness for purpose, for example in respect of the approach to record keeping. These are aspects a user or relying party must judge for themselves. *tScheme* can ensure that information is made available by the TSP on which they can base such a judgement. However, *tScheme* service approval does require a satisfactory assessment of the suitability of a TSP's service policy to the service actually being offered. This would relate equally to certificate management and status validation services as to initial certificate issue. Any inconsistencies found during the approval process or in subsequent re-assessments will lead to such approval being refused or potentially withdrawn by *tScheme*.

But there are other important objectives, which fall outside *tScheme*'s remit. Operational issues tend to be paramount, for instance:

(1) The technologies used to verify signatures must be correctly installed and configured to prove that the validation source is authorised on behalf of the CA to act in this capacity

(2) The manner of private key storage must be acceptable and evident to the relying party (possibly from the type of certificate issued or as evidenced by the CA Policy).

(3) The verification software must be compatible with the software used to create signatures, and additionally with the certificate profile(s) used by the CA.

(4) The verification software should be able to successfully retrieve revocation status information for certificates, and should be able to display to users when/how this is happening (and what are the results).

(5) The overall costs of installation, training and operation (signature creation, certification, verification, checking CRLs, timestamping etc) should not be so great as to destroy the business advantages of working electronically, and the security advantages of using electronic signatures.

Q54 – Q58: Relating to the internal procedures of 'authorised firms'.

Q54: Are there any other non-compulsory ways in which authorised firms could use electronic signatures and certificates for the purpose of entering into financial relationships in the confidence that they were complying with the money laundering regulations 1993 and FSA 's money laundering rules?

Q55: Do you support the approach laid out above for ensuring that proper controls and procedures are put in place so that digital certificates of identity can be relied upon for the purpose of entering into financial relationships? Could the approach be improved, and, if so, how?

Q56: Does this approach take sufficient account of the differences between the use of electronic signatures in the business to business and consumer to business sectors?
Q57: In order to ensure that authorised firms have time to develop the processes and controls suggested above, what would be a reasonable time-scale for drawing up guidance in this area?
Q58: How do authorised firms propose to address the risk that a customer does turn out to have been laundering money using an account opened on-line, despite operating whatever controls are recommended?

Although resolving these issues is largely a question for authorised firms, it is worth noting existing standards work and legislation in this area.

For example, most of the confidence issues could be addressed by authorised firms accepting only "advanced electronic signatures" supported by "qualified certificates" (within the meaning of the 1999 EC Directive, amplified by ETSI standards e.g. QCP).

Q59 – Q61: Regarding monitoring and approval/accreditation schemes and information sharing arrangements.
Q59: Are there other key areas issuers should address?
Q60: Are these appropriate tools for the FSA to use? What other tools might it consider adopting?
Q61: What kinds of information, if any, would firms wish the FSA to provide to any accreditation agency, were there to be information sharing arrangements which aimed to reduce regulatory duplication on the part either of the accrediting agency or the FSA?

The issues covered in paragraphs 9.43 to 9.44 of the FSA paper are already the subject of direct focus in the approval criteria defined by *tScheme*.

tScheme is an independent, self-regulatory scheme from which TSP "authorised firms" may wish to seek approval in the promotion of their electronic trust services. Information given to tScheme by TSP and its recognised assessors is treated on a strict non-disclosure basis.

Q62 & Q63: Regarding firms' internal management procedures regarding employees' digital transactions.

Q62: Have firms considered how current operational discretionary powers possessed by authorised signatories will be mapped into the digital world?

Q63: How are firms planning to maintain an audit trail of digital transactions carried out by staff or computers?

Where a TSP applies for *tScheme* approval for a service to corporate customers issuing certificates to employees, aspects such as the ongoing monitoring or control of the use of such certificates is likely to be a key feature of the service offered.

In this case, approval by *tScheme* will depend on a sound assessment that the management controls and restrictions on use of certificates issued are indeed being delivered in the manner described, both through service policy and service implementation.

Q64: What should issuing firms' responsibilities be in this area *(use of digital certificates by consumers)*? What else could be done, and by whom, to aid public understanding?

Where 'authorised firms' (financial institutions whose activities are governed by the FSA) are concerned, the practice of making clear the dispute resolution mechanisms is to be encouraged, no less for digital certificates than for any other of their activities.

NOTE

tScheme is the independent, industry-led self-regulatory body (recognised but not 'sponsored' by DTI as suggested in paragraph 9.53) which has been set up to create strict service criteria and to approve electronic trust services – including qualified certificate services as envisaged by the EC Directive on Electronic Signatures.

tScheme trust service approval will provide a level of assurance to individuals and companies relying on electronic transactions, enabling growth in e-business.