tScheme and Confidence in Online Identity

tScheme is committed to a realistic, positive vision for the future, where secure online identity management and reliable authentication are the foundations of a networked economy creating enormous potential for prosperity, productivity and convenience. This is why tScheme is determined to promote best practice in the services that address this vision, applying specialist expertise from the fields of cryptography and information security to guard against the threat of online identity theft, impersonation and fraud.

tScheme is an independent regulatory body publishing agreed best practice criteria for secure electronic transaction services. It grants approval to services that meet those strict criteria as shown by independent external assessment, and publishes their details in its secure website Directory of Approved Services. Service users, relying parties, approved service providers and internal service operators all stand to benefit from tScheme's unique contribution to the networked economy. It is government's unique role to lead in the implementation of electronic services that meet the public's high expectations, by mandating service best practice criteria such as those defined and approved by tScheme.

1. Trustworthy Electronic Identity

As the hectic pace of everyday life quickens, pressure mounts to perform tasks more and more efficiently using all the latest tools of modern technology. This is why, despite frequent online security scares both actual and hypothetical, the public Internet continues to grow apace as the most favoured method of communication for both internal and external business transactions. This popularity increasingly extends to transactions between government and its citizens and their businesses.

To develop a truly networked economy however, it is necessary for individuals to possess trustworthy electronic identities that vouch for their real-world identities. Parties to online transactions can then rely upon these identities as they interact over the Internet or across internal networks. An electronic identity needs to be secure enough to ensure that no-one can use it to impersonate another, for example to access valuable online services; and also to facilitate investigation of attempted improper use in support of robust anti-fraud measures.

Through ensuring that the level of electronic identity security is commensurate with the risks – the same proportionate approach that applies in any human situation – the full potential for secure electronic transactions, including the successful delivery of e-government services, can be unlocked for the benefit of all.

tScheme develops and maintains service approval criteria that directly relate to services offering to provide such secure electronic identities. It does this by focusing on the service management processes implemented both at the point of issue – the process by which a real-world identity is validated, verified and then delivered to its owner in the form of an electronic identity; and also at

the point of use – the process by which an electronic identity is authenticated to prove it is being presented by its true owner.

At both points in the process, identity theft and fraudulent transactions are a potential threat unless defended against in identity service design, implementation and operation. However, technology alone cannot address every risk. For example, an electronic identity may have been issued against a bogus National Insurance number; or a fake or assumed birth certificate could have been used to create an entirely fictitious identity. Carefully-guarded access to secure online applications can also fall prey to the fraudulent use of stolen identity credentials: that is, exploiting real identities actually belonging to other individuals – living or dead. All of this has major implications for any organisation, and especially government, wishing to deliver online services in order to take full advantage of the opportunities created by the networked economy.

Where electronic identities are in use for internal transactions within an organisation, problems can arise for example with delegated authority levels, or permitted access to sensitive personal information. Careful role-based segmentation of databases and online procurement applications may be vulnerable to misuse if the service providing for secure electronic transactions dependent on the reliability of online identities is anything less than robust. Audit records too may be forged – it is very difficult to investigate a fraud perpetrated by an insider who has set up fake electronic aliases to create a false identity trail. This has major implications for corporate governance and business continuity objectives.

Looking ahead, the processes implemented by a service to manage an electronic identity over time – where for example future amendments or renewals are required – should also be fully approved against known best practice criteria. This long-term management challenge applies particularly in public services, which span a citizen's identity from cradle to grave.

Increased confidence and assurance can be created, for users and relying parties alike, only through independent assessment of the processes by which electronic identities are created, managed and authenticated – to demonstrate that they are operating in accordance with best practice.

tScheme's dedication to independent regulation ensures that its focus on best practice is flexible, responsive and in line with user and relying party priorities as the networked economy continues on its path of rapid evolution.

tScheme approval may be granted to electronic trust services that continue to meet its best-practice approval criteria. These include digital certificate, PKI-based services, and services providing other forms of secure electronic identity credentials.

2. *tScheme* Approved Service Marks

For any trust service provider or internal service operator to gain the right to display a *tScheme*-Approved Service Mark, a formally-recognised and independently-accredited assessment body must first perform an independent assessment of the service. Such an assessor will have signed a comprehensive agreement with *tScheme* covering the performance of *tScheme* assessments.

Following the completion of a successful service assessment against the relevant *tScheme* approval criteria and the formal granting of approval to a specific service, the trust service provider may indicate this by displaying a Purple (Certificate Service) or Blue (Electronic Identity Service) *tScheme*-Approved Service Mark, as illustrated below, for as long as the service continues to meet all the relevant criteria:

Those selecting an electronic trust service should therefore always look for this *tScheme* Approved Service Mark, and this applies equally in both the public and private sectors. This clearly simplifies service evaluation and selection.

Where only part of the complete secure transaction process is being outsourced in this way – for example outsourcing the generation of digital certificates that the organisation itself then distributes and manages – it is equally important to gain assurance that the integration of the external service into internal operational processes also adheres to best practice. Certificates enabling high value or particularly sensitive transactions must be supported by equally robust processes and procedures if the resulting overall system is to meet expectations.

Thus for an organisation using an external *tScheme*-approved service on which to build its own internal secure transaction processes, extending independent assessment to cover the whole service operation – comprising both outsourced and internal elements – will reveal overall compliance or otherwise to the relevant *tScheme* criteria. If desired, such an organisation can gain the right to display a special Red *tScheme* Approved Service Mark: this can be awarded to such community or closed user group services, to demonstrate its achievement to all its stakeholders – whether citizens, staff, users or suppliers. Such visible adherence to *tScheme* approval criteria sends a strong signal to the outside world that where secure electronic transactions are concerned, best practice is alive and well within the organisation.

3. Best Practice

Best practice comes from the accumulated wisdom and experience of experts. Experts typically share this among themselves, generally having little regard for disseminating it for use by others. Only slowly do those outside the expert circle come to appreciate this body of knowledge. For secure electronic transactions, *tScheme* has successfully undertaken the task of recording best practice in the form of Approval Profiles. These describe the criteria that the processes forming a service must meet in order to be considered appropriately robust.

However, only a minority of these criteria are technical in nature. The majority refer to human and physical factors. For example, does the documentation correctly reflect what the service does? Are its operators correctly selected and trained, bearing in mind their privileged roles as guardians of critical pieces of information? Who has physical access to the most sensitive equipment and files? In other words, the best practice criteria consider the problem of achieving and maintaining security in a holistic manner, from basic equipment to end user training. This reflects real world experience where many more security failures involve, for example, disgruntled staff than the breaking of secret cryptographic keys.

This once again clearly points to the importance of assuring compliance of internal processes to *tScheme* criteria through independent audit or assessment. As well as enhancing management confidence, such evidence of process compliance can be highly relevant to raising public confidence and removing scepticism about electronic security.

Government's desire to embrace the networked economy is well founded. The expectations for the reduction of waste and fraud, and for increased efficiency, greater convenience and so on through the secure online delivery of e-government services are manifestly right. However, the successful

delivery of e-government services depends on the degree of reliance that can be placed on the electronic identity credentials used to access those services. In addition, service take-up still depends on overcoming suspicions on the part of citizens and businesses that the online security risks may be too high.

tScheme offers an effective way to instil confidence and to combat these suspicions through enhanced assurance in service management processes. It is encouraging that e-government services have begun to embrace the *tScheme* approvals regime, simultaneously setting an example for the private sector.

tScheme Summary

tScheme is an independent regulatory body actively supported by a broad coalition of organisations representing service users and relying parties, service providers and technology suppliers from industry, trade bodies, consumer interest groups, UK government and others. All members contribute to the development of *tScheme* through their annual membership subscriptions and by sending delegates to its expert working groups.

tScheme operates as a not-for-profit company limited by guarantee, owned by its members. Its governance ensures its openness, transparency and independence. It is self-funding from membership subscriptions, from fees payable on Grant of approval permitting use of a *tScheme* Mark, and from licence payments for the permitted use of its materials by professional audit bodies or recognised peer schemes.

tScheme provides the independent regulatory environment that avoids the need for the UK Secretary of State for Trade and Industry to invoke legislative powers under Part I of the Electronic Communications Act 2000. *tScheme* also enables the UK government to fulfil certain obligations under the European Directive for a Community Framework on Electronic Signatures.

Through *tScheme*, the UK is demonstrating its leadership in creating an ideal environment for the growth of electronic commerce.

Further details may be found at www.tScheme.org.

***tScheme* Limited**
2nd Floor Russell Square House
10-12 Russell Square
LONDON WC1B 5EE
Tel: 08702 417 497
Fax: 0870 005 6311