



**Draft report of the EURIM - ID-Entity technical briefing meeting,
1000 – 1200 hours, 12 January 2006, Thatcher Room, Portcullis House, Westminster**

1. Introduction

1.1 This meeting was organised jointly by EURIM and the ID Technology Advisory Group (ID-entity) to enable Parliamentarians to question directly representatives of some of the main potential suppliers to the UK ID Cards scheme on the capabilities of the technologies involved. ID-entity members have practical experience in helping deliver similar schemes in Europe, the Far East and North America, from initial application, enrolment, interview and authentication through scalability, speed, stability, security and reliability - including with the large scale use of biometrics.

1.2 The meeting was planned as an informal open panel session with the supplier team taking questions from the floor. Any questions that needed more detailed treatment would be dealt with in break-out sessions with a team member having expertise in that area.

2. Summary of main points

2.1 No leading edge technologies are proposed for use in current ID card proposals; the scheme will use existing available and feasible technologies. What is new is the way in which the component technologies (e.g. biometrics, chip and pin) are being brought together in one scheme, and on a scale that appears to be unprecedented.

2.2 All team members have collaborative experience of delivering systems in non- or partially-consensual environments. The currently stated costs are Home Office costs, net of contributions from revenues from other departments and/or private sector partners, but it is unclear what these are willing to pay in order to receive what levels of service and/or the costs they will incur.

2.3 The business case for an integrated system that brings together a national identity register with comprehensive address information and biometrics for national security, as well as service delivery purposes, depends on a level of co-operation across UK government departments (including funding, management and delivery), that is unprecedented. While Government will invite suppliers to discussions on data sharing before implementation of the scheme, the experience of data sharing in the Criminal Justice between the six criminal justice agencies provides a successful example.

2.4 None of the potential suppliers have had sufficient access to specification of what is intended or who is to be served to be able to provide costings of any reliability. There is no evidence that the potential private sector partners with experience of running supposedly similar operations (e.g. financial services) have been consulted in any more depth.

2.5 Although technological change can bring in the much needed business transformation, often in ways unforeseen in debate, political uncertainties strongly indicate that progress should be incremental, building on what is known to work and testing new developments. It has been said that if HMG were to simply recommend using the Austrian standards for publicly issued service cards and enable the use of shared updating services (as part of the Transformational Government agenda), it could achieve nearly all the claimed service benefits at a fraction of the cost, risk and time.

2.6 There are serious concerns over the people processes involved in the security and accuracy of very large databases to which many departments are expected to have access. Although technical safeguards will be in place, much existing fraud is committed or conceived internally. Authentication by interview and checks with credit reference agencies may help, reinforced by biometrics, but no system can be guaranteed to be 100% secure. The credit agencies do not carry comprehensive information on past addresses. Most carry only information on the addresses in use since the time the individual

first made an application for credit. If they have never applied for credit and are not on the electoral register, there is probably is no address on file to start with. Thus many of the 'socially excluded' in most need of government services are not on file, or only at the location they last registered to vote (if ever).

2.7 The experience of financial services industry security experts on the attitudes and experience of others they met at an open consultation meeting suggest that there is a gulf of understanding between those running systems under regular and sophisticated attack and those who are not under such pressures.