

**Disposition of comments received following public consultation (July 2002):**  
**HMG's Minimum Requirements for the Verification of the Identity of Individuals**  
**and**  
**HMG's Minimum Requirements for the Verification of the Identities of Organisations**

This document contains comments received on the two documents detailing HMG's minimum requirements for the verification of the identity of individuals and of organisations. These frameworks were available for comment by the public and industry in general during July 2002. The Office of the e-Envoy wishes to thank all those who contributed to the consultation process for the constructive comments received.

The comments have been broken down into sections: the first section describes those comments that apply to both documents, while subsequent sections list those applying to each of the two documents separately.

We have tried to ensure that the comments cannot be directly attributed either to an organisation or an individual, however they should still be recognisable to those that wrote them.

The documents subject to public consultation comprised:

- *HMG's Minimum Requirements for the Verification of the Identity of Individuals*, v1.1, 12 February 2002.
- *HMG's Minimum Requirements for the Verification of the Identity of Organisations*, v1.1, 12 February 2002.

The documents have been reviewed and re-issued as follows:

- *HMG's Minimum Requirements for the Verification of the Identity of Individuals*, v2.0, January 2003.
- *HMG's Minimum Requirements for the Verification of the Identity of Organisations*, v2.0, January 2003.

## **Both Documents**

Comment	Response
Our question regards the way that the RA will be authorised. This becomes an issue when a certificate is used fraudulently in such a way that loss is incurred. Will there be a further set of guidelines issued for that area or do the Office of the e-Envoy believe the tScheme to be sufficient to cover such events?	No action - we do not currently propose to issue guidelines on authorising RAs: this is currently under the control of tScheme
How do these policies relate to services which we provide to a global community? All of the items used to verify personal identity are parochial in nature	The priority is the UK, but we are working with Europe and elsewhere and exploring cross-certification issues
The availability of higher and higher quality packages i.e. scanner, software and printers which would allow forging of even the “real” (centrally produced and posted) documents means we may need to ensure all those dealing with registrations have training to detect the forgeries. How could we ensure that this was done to a common standard?	Noted. The RA would specify the standard of evidence required to give confidence
In support of verification we already have a Verification Framework which is a well respected and rigid process. Whilst the proposals for Registration Authorities is to establish identity, it is through the Verification Framework that the Department will (where appropriate) need to ‘look behind the scenes’.	Noted
Our interest lies in the overall process and the reality in providing its customers with an electronic identity i.e registration etc. We were unclear as to why the documents make no mention / reference to the Government Gateway, Smart Cards and Entitlement Cards.	Out of scope of this document
We are content with proposals	No action
In themselves each of the documents looks reasonable. Whilst, particularly at the higher levels, there appears to be lots of paper pushing, that is to be expected.	No action

<p>The documents do not specifically state that a level 3 credential would also cover requirements for levels 1 and 2 credentials. Nor does it clearly state that a citizen should have only one of these – yet the citizen will not want a random collection of different verification tokens. In practice many citizens (and organisations) will have no feel for which level of registration might be demanded of them as new transactions come on line and Departments are expected to set the levels required (December 2001 documents). He can, therefore, only guess which 'credential' is likely to be the highest applicable in his circumstances, and if given a choice will tend to gravitate towards a level 3 credential in order to be covered</p>	<p>Sentence added to the end of para 20: "Credentials obtained for Level 2 transactions may also be used for Level 1 transactions, and those obtained for Level 3 transactions may also be used for Level 1 and Level 2 transactions."</p>
<p>We had understood that an individual could define a role at the time of registration with the departmental system (or portal) (December 2001 Registration framework Annex C para 70). We see no reference here to roles as such, and this could be a major issue. An individual may prefer only one credential (and if it is at level 3 so be it) but, unlike an individual, the 'company' registrations (and there may well be many) may legitimately be at many different levels and registered by different sets of people depending upon the transaction type. I.e. accounts people may register for VAT and tax – related services, procurement deals may be handled by sales, personnel officers may register for employment information services, and so on. Within one company, there will be many different people doing different things, and a single company signature for (say, ICI) may not be sensible. This brings a whole raft of management and logistical issues, of course.</p>	<p>An individual may choose to have one or more credential. Individuals within organisations may also have more than one – it is up to the organisation and individual.</p>
<p>A specific role a company or an individual may take on is that of a right of attorney for someone who is ill or unable to cope. It is unclear how such a role might fit into the authentication scheme as outlined here.</p>	<p>Noted. The role of an attorney and how the credentials are used is out of scope of these documents</p>
<p>If a passport or birth certificate etc is major identity document does this preclude applying for these electronically in future? If not it would appear that the use of such documents is, or could be, a circular</p>	<p>Noted. We will need to keep this under review as more services come online</p>

<p>process. Again there is an issue if a document such as a passport is obtained by production of a couple of easily-acquired 'proofs' of identity, which are then re-used together with the document in order to gain even more documents and even greater levels of trust.</p>	
<p>Most official documents require that a fee be paid to obtain them. If the citizen has got to produce a level 3 'credential' (say a passport) how will the fee for obtaining the credential be paid? By the individual or by the authority requiring the document? Will there be three fees one for each level credential?</p>	<p>Noted - out of scope of these documents but will be addressed in subsequent papers</p>
<p>It is not stated in the documents how long a credential will be valid for. This should be identified - for individuals will it be like a passport renewable after 10 years? How might this be retracted – or expired – or modified - as circumstances change? We assume that when an individual who obtained an organisation credential ceases to function in that role the credential ceases to be valid. However, a person who, for example, ceases to be a husband by virtue of leaving the family home must expect that part of his credential to become equally invalid.</p>	<p>The process described is for registration, not for issuing certificates, so this is out of scope of these documents</p>
<p>It states in both documents that records are to be retained for 7 years (para 31 of individuals and para 36 in organisations) but the document does not specify who by or in what form. If it is the RA then surely the citizen must also keep them in case the RA records are defective or wrong, or for any reason the RA 'disappears'. Whilst this is not difficult with say birth certificates etc it might prove difficult with specific (easily forgeable) utility bills. Guidance to the citizen is required on this area. There may be a case for the RA retaining this information indefinitely (or till 10 years after the death of the client, or some such statement) – whilst 7 years is a norm, it may not suit in all circumstances.</p>	<p>The requirement to retain records for 7 years comes from the Treasury Solicitor. The citizen does not need to keep the records, as any problem with the RA would have to be resolved by the CA.</p>

## Individuals

document reference	comment	response
perception of identity	Whilst name, address and DOB are our normal identifiers, they are not always practical (there are scores of John Smiths in the UK alone) and are easy to abuse by fraudsters because verification can be difficult. Biometrics are probably the best tools to quickly verify identity (there is only one human being let alone John Smith with my biometrics) although, of course, they cannot normally confirm that you have a certain name etc but can confirm that you are not registered in another identity. I do though think that it is very important that they are referred to in this document and their value considered.	Out of scope of this document, although we are aware of and do sponsor work on biometrics: we will keep this under review
	I have had a quick look at the paper on Registering Individuals for online services. It gives as an example of a Level 1 transaction online ordering of a publication via a credit card. In order to verify the identity of this person as I understand the proposals we would need name, address, DoB, and then two pieces of independent identity data. If we compare this to say Amazon this seems to be a significant level of additional security. This is likely to be a barrier to uptake and will add to the complexity and cost of service implementation. Have I misread the paper?	The document specifies requirements for RAs issuing a single credential for a range of services, not the requirements for specific service providers. No action
para 21 - definition of identity	I would have thought that UKPS would say that the passport was an official id document, the problem with it is that it is not held by everyone and not all of the resident population in the UK would qualify for one.	Agree that there is no document held by everyone.
para 21 - definition	OeE might want to add a reference to the Entitlement Cards Consultation Paper along the lines of 'The	Noted, but out of scope of these documents.

of identity	Government announced on 5 February that it will be publishing a consultation paper on entitlement cards in the Spring or early Summer. A card scheme would provide widely held card (or set of cards) backed up by an identity database which would provide a means for people to prove their identity more conveniently and to a higher level of assurance than current identity documents. However, even if the Government decided to proceed, a card scheme it is likely to be many years before cards are widely held by the resident population'.	
para 22 - attributes of identity	OeE might want to use the same definition of identity as that adopted by the Cabinet Office-led study on identity fraud. This is consistent with the discussion below (except that this report does not mention biometric information) but it would be worth trying to use the same terminology if possible as the Cabinet Office report will be published in some form either as part of the entitlement cards consultation paper and/or as a separate document.	Out of scope of this document
	If a citizen were to start off with level 1 credentials, and were then to 'upgrade', would his level 1 certificate count towards his level 2 requirement? If so, there is a potential issue about duplication of identity proofs. (i.e. if I use my passport and my utility bill to achieve level 1, it must not be possible to produce a level 1 credential plus my passport and utility bill to achieve level 2 ....)	Sentence added after para 36: "Where existing credentials are used to obtain higher level credentials, the supporting evidence must be additional to that first presented (eg if passport and utility bill were presented to obtain a Level One credential then other proofs of identity must be used to obtain a Level Two credential)." New subparagraph added to para 67: "If the RA does not have sufficient assurance in the registrant's identity then the RA must ensure it uses additional forms of evidence which have not already been presented by the registrant."

para 51 (13) - SAL1 and SAL2 (asylum seekers forms)	these are in the process of being phased out and replaced by an application registration smartcard (which incorporates a photograph and fingerprint - please speak to the Immigration and Nationality directorate for the correct form of words to use about this)	Wording amended following advice from Immigration & Nationality: "Application Registration Card (ARC) issued to people seeking asylum in the UK (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms)"
Para 3.3.2 Examples – No 51 a) 13	From February 2002 Standard Acknowledgement Letters (SAL's) have been replaced by Application Registration Cards (ARC's), as far as we understand these are being rolled out nationwide.	Covered under earlier comment - to be changed
para 3.3.2 Examples - no 51 b) 3	There is a general trend towards providing access and management of accounts on-line –for example some citizens do not receive telephone bills any more, just an email to say there is one available and it can be downloaded from the web and printed (fully or partially), if required. There is a risk that during this process details could be altered. The effect of this for the Department is that we may have to treat some of these types of accounts / bills / statements with suspicion. If we start to exclude them then some citizens are likely to end up without sufficient forms of proof to establish their identity.	Para 3.3.2 b) 3 amended to exclude bills printed from the Internet
	We will need to decide what particular Registration Level is appropriate for each kind of transaction, but the minimum basic level looks OK and I would expect we'd need additional stuff like NI numbers etc.	No action - comment on general implementation
	It will be important for us not to impose additional bureaucratic demands on employers that do not wish to interact with us electronically.	No action - comment on general implementation
	An issue over the retention of information arises, given the pressures to retain the minimum amount of data consistent	No action - comment on general implementation

	with our business needs.	
	There will be some challenges if we adopt remote on-line registration that would permit access to personal information. The need to seek advice from the Information Commissioner should be noted.	No action - comment on general implementation
	It is unlikely that we will routinely ask for original documents to be sent by Special Delivery.	No action - comment on general implementation
	We mustn't forget that consent is required to process and disclose personal data.	No action - comment on general implementation
	We are required to use staff with appropriate levels of skill in undertaking registration. Where does this put the use of temporary staff?	No action - comment on general implementation
	There will be a need to make decisions about the acceptability of evidence and to record the reasons for the decision.	No action - comment on general implementation
	Young people may not have many corroborative documents available to them.	Agreed
	Privacy and security issues are paramount.	No action - comment on general implementation
Para 3.3.2 Examples – No 51 a) 5 & No 51 b) 10	Please change all references to “the Benefits Agency” to read “Department for Work & Pensions”. Also mentions benefit book which DWP is planning to replace by ACT payment / benefit card during 2003.	Changed as requested
	It would aid considerably if the paragraphs in the body of the document could be numbered to correspond to the List of Contents page.	Word processor conversion problem - no action (has been discussed with sender)
	In various parts of the document there is reference to "(see section o)" unfortunately there does not appear to be a section called "o" in the RTF version of the document I downloaded from the Govtalk site yesterday	Word processor conversion problem - no action (has been discussed with sender)
	There are two very useful charts laying out the possible	Tables have been recast to simplify their use,

	permutations for the registration requirements. Would there be an opportunity to combine these charts into one to present a complete picture on one page?	bringing together all the information for a specific registration level in one place
para 56	If third party information is used to verify identity then the citizen should be informed of what information was elicited (except possibly for specifically excluded information). Third parties may be wrong and this MAY be a means of detecting people seeking to obtain spoof identities.(para 56 of individuals). Particular care must be exercised with credit reference agencies as they issue information about all people ever registered at an address unless the citizen has told them not to (a hangover from stated bank checking which is an exemption from the DPA for banks) - a fact most citizens are unaware of!	The issue is for the RA, who must ensure compliance with relevant legislation.
	We are pleased to note that there is commonality in the requirements for identity documentation with other legislation thereby mitigating the concern we expressed in our comments on the December 2001 documents submitted to Mr Framp on 18 January 2002 (B1.4)	Noted
para 4-7	Para 4 – 7 of people document could be clarified and simplified	Noted, but we believe it is sufficiently clear
para 19	Para 19, people document. - ‘ Full details are in the framework, but ..... ‘ A reference should be given.	Footnote reference inserted where Reg+Auth framework is referenced in para 18 and text amended to read "Registration and Authentication Framework"
para 84(a)	Para 84(a) line 3, people document - ‘of’ should be ‘or’.	Changed as requested
para 51 a) 17	Change "certificate of employment in HM forces" to "HM Forces Identity Card"	Changed as requested

## Organisations

document reference	comment	response
registration protocol for level 3 Digital Certificates	document says that care should be taken with Remote Registration where this would give the ability to manipulate personal data. My understanding of the use of DCs is that once registered for a level 3 certificate, that DC could be used as proof of identity to register for access to any system requiring level 3 access. Therefore at the time of registration the RA will not know what eventual use may be made of the DC. Shouldn't the protocol therefore specifically disallow the remote registration for a level 3 DC.	No action - the wording is strong enough, but we will keep this under review
	This appears to rely quite heavily on letters from responsible company officials on headed notepaper to assure that the person chosen to represent the organisation is bona fide and has authority to represent the organisation. We are concerned that this may lead to some kind of infinite recursion - how can the validity of such documents be trusted, both in terms of whether they come from the organisation at all and in terms of whether the unknown person signing these documents either works for the company at all or if they do whether they actually have the authority to grant the authority. For level 3, the document says that the RA should contact this unknown person by phone at a published number to verify their identity, but we believe that for level 3 it would be safer to actually visit the site to speak to the authoriser directly. Even that is not foolproof, and maybe a full identity check on the authoriser should also be required.	Noted: if the RA had any doubts over the representative's authority and identity then the RA should take this further. However we will keep this under review

para 7 - passwords	although passwords appear more secure as they allow a choice from 26 (A-Z) rather than 10 (0-9) characters, PINs are actually more secure since they are much harder to guess. There are mathematical models for this. In the very least it would be good if government were consistent as with time this will look like departments do not have a common approach.	Recommendations follow HMG Infosec guidance from CESG
para 19c	some rationale for export licence work requiring level 3 verification would be useful I can only surmise that this is because it involves transactions outside of the EU, within which there have been recent improvements in law enforcement, but out with are more difficult in terms of both prosecuting and restitution.	Amended to give a different example: a request to gain access to information from the Criminal Records Bureau
page 12 table (after para 38)	there is no explanation of two and three ticks. How more mandatory can you get than given by one tick?	Key to table amended to read "Must be provided. More than one indicates total number of that type of evidence to be provided"
para 69b	the worth of digital certificates varies enormously. Some CAs make no checks at all, simply allowing users to sign up electronically. There needs to be some minimum criteria here for a an existing digital certificate to be accepted. I refer you back to Para 7, many CAs would not meet these requirements so we should not accept their certificates. This is a cross-certification issue.	The document is purely for e-government services. A certificate only has to be accepted if the service provider has confidence in it
	What is an organisation's credential? It is unclear from the document what an organisation credential actually is. Is it for the organisation irrespective of who obtained it? Or is it a credential for the person acting in the defined role (capacity) for the organisation? What use does an organisation credential have? Our understanding of the December 2001 documents indicated that the registration etc was by individual not by organisation. In our	There is no generic organisational credential: a credential is for an individual as a representative of an organisation which has been proved to exist, ie there is proof of: (1) the existence of the organisation; (2) the existence of the individual; and (3) the individual has the authority to act for the organisation. See para 1.1 of the document.

	<p>comments we suggested a simplification of using organisational credentials but are unaware if this has been acted upon. (B1.6 c)) We see nothing in this document which would aid the differentiation of roles and people. (i.e. some things might be signed by the PM's office, and others by Tony Blair as Prime Minister, and others by Tony Blair as MP, and so on. Tony Blair may well have other interests (such as being a father)). Companies also have this problem of separating the actions of the board from the actions of the individuals who comprise it.</p>	
	<p>If, in order to obtain a non-specific company credential, an individual acting as the company contact is identified and authenticated at the appropriate level, will the company credential be revoked should anything happen to that individual? Changes to Company credentials are difficult – whilst the company signatures should last indefinitely, (subject to some renewal / refresh process and a way of dealing with name changes, mergers, takeovers, changes of ownership and nationality, etc) the people 'churn' in a company can be significant. (see confusion on what an organisation credential actually is).</p>	<p>The credential should be revoked, and it is up to the organisation to have it revoked. See the above comment about organisational credentials.</p>