Open Smart Card Infrastructure for Europe

v2

Volume 2: **User Requirements**

Part 4: **User Requirements for Cardholder Identification, Authentication and Digital Signatures**

Authors: **Expert Report for eESC TB8 User Requirements**

PREPARED BY: JOHN GILL

DOCUMENT HISTORY

Date	Version	Author/Editor	Comment
12/12/2002	0.1	John Gill / Phil Perry / Ron Bird	Initial Draft
20/12/2002	1.0		Release for Formal Review
23/12/2002	2.0		Final Version
7/1/2003	2.2		Revised Final version

Copyright

Acknowledgement

This report has been written with the help of Phil Perry and Ron Bird. Trailblazer 8 acknowledges the contribution of the wider European IT community and Citizen Groups to its work on User Requirements. Much of this work has been voluntary, but has been produced to the highest professional standards, and we would like to take this opportunity to express our gratitude and appreciation for this work.

*e*Europe Smart Cards Trailblazer 8

*e*Europe Smart Cards Trailblazer 8 on User Requirements is an informal group of participating organisations and individuals working to produce a User Requirements Best Practice Manual for European wide implementations of Smart Card enabled services.

The objective of Trailblazer 8 is to ensure that the user interface, functionality and process of ICT systems employing smart card technology:

- meet identified requirements to support Citizen aspirations,
- are attractive to Citizens,
- and guarantee inclusiveness for all categories of Citizen.

Contact information

For information on *e*Europe Smart Cards Trailblazer 8 (TB 8) please contact:

Philip Perry	Alan Leibert
Secretary, *e*Europe Smart Cards TB 8	Chair, *e*Europe Smart Cards TB 8
philip.f.perry@btopenworld.com	alan@alco.eu.com

For information about this report, please contact:

Dr John Gill
RNIB
Falcon Park
Neasden Lane
London NW10 1RN
Tel +44 20 8438 9071
Fax +44 20 8438 9094
Email john.gill@rnib.org.uk
Web www.tiresias.org

Contents

1 Executive Summary

Consumers want user friendly systems which have the appropriate level of security, but are simple to use. Service providers want to optimise their service level, and to maximise their market penetration through targeted advertising. If service providers do not understand the needs of their consumers, they are likely to find consumers reluctant to use smart card based systems.

Cardholder identification should involve the consent of the user who may wish to withdraw their consent at a later date. Authentication provides the user with a secure way to prove their identity during a transaction, but does not necessarily mean that they are authorised to access a specific service. The use of a digital signature involves the consumer in giving his or her positive consent to the content of an electronic document. However the consumer needs to understand the implications of their actions and how they are legally protected if something goes wrong.

1.1 Recommendations

1. *The consumer must be able to choose the level of identification they provide, in the knowledge of what limitations this will impose on the services they will be able to access.*
2. *The card holder should be able to operate in a pseudo-anonymous mode where they are authenticated to a high level but personal information is not divulged without their consent or after due legal process.*
3. *The cardholder should know what information about him is stored on the card and should be able to decide who else has access to this information.*
4. *Refusal of consent should not be a reason to withhold any service unrelated to that data.*
5. *At the request of the user, extra information could be stored on the card. This information could include the user's preferred interface.*
6. *The authentication system must be of a level appropriate for the application.*
7. *Consumers often have problems in remembering more than one PIN. Passwords are easier to remember than PINs, but are not appropriate for all applications.*
8. *There is no perfect biometric system of identification. Facial imaging has high consumer acceptance, but requires significant processing by the card acceptance device.*
9. *The user should have the facility to choose an alternative to a biometric identification system; this is particularly important for disabled users.*
10. *Consumers need to be educated about the implications of digital signatures.*
11. *When communicating with consumers, consistent non-technical terminology should be used, otherwise consumers will be confused.*
12. *Digital signatures should have a common legal basis internationally, so that consumers are certain of the protection they have in transactions which cross borders.*

2 Introduction

The take-up of smart card based services will be determined by the consumers' perceptions of ease of use and trust in the system. Ease of use will include aspects such as consistency of the user interface as well as the ease of recovering from errors (both by the user and the system). The provision of appropriate instructions and intelligent help will be important; this implies some form of standardisation of terminology.

This report examines some of the aspects which are likely to affect the user's ability or desire to use smart card systems. Users may be customers of a commercial service provider or citizens wanting access to government services, but users will include people with disabilities, older people, people whose primary language is not used by the system, as well as people who are left-handed. These 'minority' groups constitute a significant, if not homogeneous, portion of the general public. Ignoring their needs is likely to have an adverse effect on the take-up of smart card services.

Trust is difficult to measure but will depend on the consumer's understanding of the level of security of their personal information. Perceptions of a system can change suddenly influenced by stories in the media. For instance it would only need a passenger at an airport to claim that their vision has been damaged by an iris scan for there to be widespread reluctance to use the system.

The consumer wants a simple process of identification that does not involve providing more information than is needed for the services they wish to access. The consumer must be able to choose the level of identification they provide, but they must be made aware that this may determine what services they can access. The consumer is likely to be concerned that the information they provide will not be passed to third parties without their permission.

An important aspect is that resources need to be devoted to education of card holders so that they understand how to use systems, understand the implications of their actions, and understand how the law will protect them if something goes wrong.

2.1 Definitions

For the purpose of this report, the following definitions are used:

Advanced electronic signature: An electronic signature which is uniquely linked to the signatory, is capable of identifying the signatory, is created using means that the signatory can maintain under his sole control, and is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Anonymous usage: The citizen has not provided any identification information which can be assured to an acceptable level.

Application: A service which can be used by a cardholder and/or his card proxy with a smart card.

Authentication: Provides users with a secure way to prove their identity, to a known level of assurance, during a transaction. It can also prove the identity of the other participant (card reader and service provider) back to the user.

Authorisation: Permission to carry out a specific task, transaction, or application access at a given time via a given access route (e.g. at 11.45pm from a bus stop via a public kiosk).

Biometrics: A means of identifying the user by their physical characteristics rather than the card. This forms the third part of the "something you hold, something you know, and something about you" authentication paradigm.

Card: A physical object carried by the user that can carry authentication and application data and applications (this may be credit card sized, a mobile phone sim or u-sim, a token or pendant, or even sub-dermally embedded). This forms the first part of the "something you hold, something you know, and something about you" authentication paradigm.

Card holder: A person who can be regarded as the rightful user of a smart card.

Card issuer: The party that issues the card to the card holder or has it issued, and that is responsible for the card management activities during the entire life cycle of the card.

Card provider: The party that on behalf of the card issuer issues the card to the card holder or has it issued.

Certification authority: An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys.

Digital signature: Proving one's positive consent with the content of an information object by electronically signing the contract. Often a feature provided by a PKI infrastructure where it is a cryptographic modification of data providing: origin authentication, assurance of data integrity, and signer non-repudiation.

Electronic Signature: an electronic sound, symbol, or process attached to or logically associated with an electronic document which has been executed or adopted with the intent to sign the document.

Encryption: A means of protecting the confidentiality of information by using a shared secret to convert the information into apparently meaningless data that is difficult to decipher.

Identification: The process by which a potential card user's identity is established in order for the card issuer to issue a card with a defined level of assurance for authentication purposes.

PIN (or password): A shared secret known by both the card holder and the service provider, often a four digit number but can be a longer alphanumeric sequence where the terminal supports this capability. This forms the second part of the "something you hold, something you know, and something about you" authentication paradigm.

Public key infrastructure: A trust based system where sets of Private and Public keys are used to authenticate, digitally sign and encrypt data as necessary. This is a centrally managed system involving a 'trusted third party' rather than a 'peer to peer' system and thus enables secure communication between parties who have never met or exchanged mutual secrets.

Pseudo-anonymous usage: The ability to act in any anonymous manner but with the user's identity assured to a given level by a trusted third party. The service provider allows access based upon the trust model and does not, and cannot, know the user's personal information without their consent or after due legal process.

Qualified certificate: A certificate which is provided by an approved certification service provider.

Qualified electronic signature: An advanced electronic signature, based on a qualified certificate, and created by a secured signature creation device.

Registration authority: An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates.

Signature creation device: A configured software or hardware device to implement the signature creation data.

Third party: Any other party than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data.

3 Consumer and Service Provider Perspectives

Typically the service provider wishes to provide personalisation of the service being offered, both at the portal, and at the application layers. This is often accomplished by maintaining detailed audit records of the user's activities, which are then data mined to drive a personalisation engine.

For example if the user often uses a certain library for books on, say, ethnic issues in society, then the library application may flag up when new books are available in that subject area. Amazon use this technique widely. Often this data is shared with other service providers (or collected centrally at the portal) for use in marketing and sales promotions. The data collected is seen as a business asset that can either be used to differentiate the service or be sold to third parties, often without the user's knowledge or consent.

The user may appreciate this service from a given provider, but may wish this information to be restricted to that provider and not shared with others. Alternatively the user may object to their habits being stored on any given system, or indeed, on any at all.

The key issue is that user permission should be explicitly obtained for the collection of such data where it is not required by statute. Even then it should be clearly explained that such data would be collected. In all cases who will have access, and what it will be used for, should be clearly explained and a non-repudiable record kept of the user's knowledge and consent.

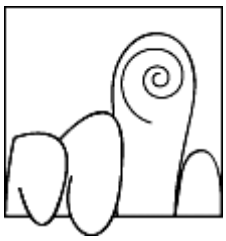
For further information, see TB8 Report on Privacy Code of Conduct (OSCIE Volume 2, Part 2) where the elements of transparency and positive consent are elaborated.

4 Identification

Identity fraud where a person adopts a completely false identity, falsifies part of their identity (for example their age) or adopts the identity of another person is estimated to cost the UK at least 2 billion Euros each year split equally between the public and private sectors.

There are three elements of a person's identity:

(a)



Things which you 'are' i.e. your Biometric identity. These are attributes that are unique to an individual (e.g. fingerprints).

(b)

Things are given to you i.e. your attributed identity. These include full name, date and place of birth.

(c)

Things which happen to you during your life, i.e. your biographical identity. This includes educational qualifications, electoral register entries, and history of interaction with organisations such as banks.

The cardholder needs to be provided with the ability to know what is stored on the card; this may involve going to a special terminal that might be in a public library. The cardholder may authorise some or all of this information to be passed to a service provider or a third party, but they should be given clear information so that they are fully aware of the recipients of this information and to what purposes it will be put.

Information should only be stored on the card with the consent of the user. The level of consent will include full use, anonymous use and no use. The user can withdraw their consent at any time. Refusal of consent should not be a reason to withhold any service unrelated to that data.

4.1 Identifying User at Time of Issue

The card issuer has the responsibility for ensuring that a card is issued to the legitimate user. For anonymous cards, like public transport pre-paid tickets, this may be just the receipt of the money. However in non-anonymous applications there needs to be some check that the person to whom the card is issued is the legitimate user and that the information supplied by the user is correct.

However the issuer should not ask, or demand, information that is not directly pertinent to ascertaining the legitimacy of the user. If the issuer wants extra information for marketing purposes, then it should be clear that providing this information is optional and does not affect the issuing of the card or the terms and conditions relating to the use of the card.

The identification process must support clearly defined levels of assurance in order to maintain interoperability between card schemes and services. These should be as follows:

Level 0 No checks made: No checks on the users identity, used for anonymous services at the discretion of the service provider.

Level 1 Balance of Probabilities: Some form of verifiable ID (e.g. Driving Licence) and proof of address (e.g. Utility bill).

Level 2 Substantial Assurance. As Level 1, but checks made against electoral register and possibly two forms of proof of address rather than one.

Level 3 Beyond Reasonable Doubt: Substantial checks made on ID provided, possibly even involving face to face identification.

Levels 4-8 Not specified at this time. For use in the future.

Clearly these identification rules will need to be centrally set and agreed across national boundaries with the EU. Cultural, political, and procedural differences between countries may require a complex set of equivalences to be drawn when trusting a level of identification indicated on a card. These will need to be clearly explained to the user as will the benefits of higher level identification.

Most importantly it must be left to the user's discretion as to what level of identification assurance they will give. However it must also be clearly explained what the consequences of their decision might be in relation to a given service such as Health Care or some special eGovernment services which will require high assurance. It must also be possible for a user to raise their level of identification assurance by providing an appropriate body with the extra identification proofs required and this should not normally require card re-issue.

4.2 Re-issuing Cards

When a card is lost or stolen, the user requires a fast method of replacing the card. However the issuer needs to ensure that the applicant is the legitimate user. The problem is more complex with multi-application cards where the user has downloaded application modules to the card. In some cases there may be possibilities for crediting the user with the value of some or all the items on the lost card (e.g. in some public transport applications, the transport company has a record of the remaining credit on the card when it was last used).

The card management organisation should keep a record of the applications on a card, even if the user has downloaded extra applications. If the card is stolen, the user should be issued with a new card number.

4.3 Additional Information

At the request of the user, extra information could be stored on the card. This information could be the preferred user interface, qualification for a discount (e.g. a registered disabled person may qualify for reduced fares on public transport), or some information which speeds up the process of accessing a particular service (e.g. connecting and logging onto a text relay service).

There are three types of additional data:

- Data common to all applications
- Application specific data
- Dynamic data (eg card checked by a ticket inspector).

There is a European standard (EN 1332-4) for coding the user's preferred interface on a smart card; such preferences could be large characters on a screen, speech output, or more time for operating a terminal. The coding may be selected by the user at a terminal, such as an ATM, in a similar way to selecting a new PIN. However in other application areas, such as public transport, the coding may have to be put on at time of issue. In other areas a third party may be involved in the process; for instance an audiologist may be involved if the requirement is to code the audio frequency loss of a hearing impaired person so that suitable compensation could be provided by the terminal.

A CEN/ISSS Workshop has produced a report (CWA 13987-1: 2002) on Smart Card Systems: Interoperable Citizen Services: User Related Information (at http://www.uninfo.polito.it/WS_URI/default.htm) which provides guidelines and specifications for designing an open scheme that supports the use of different types of smart card for accessing multiple applications at different types of system terminal.

Qualification for a discount might require an authentication system; for instance a social services department might provide confirmation that a particular individual is registered disabled.

The user may want to store their name and address on the card, but they might want to authorise its access on each occasion. There may be other information that can only be accessed by certain approved types of user (e.g. only medical personnel could access medical insurance information). But for other information (e.g. library borrower number) the user may be happy for unrestricted access such as in a citizen account.

In practice there may have to be restrictions on the amount of additional information stored because of the finite amount of spare memory on the card.

5 Authentication

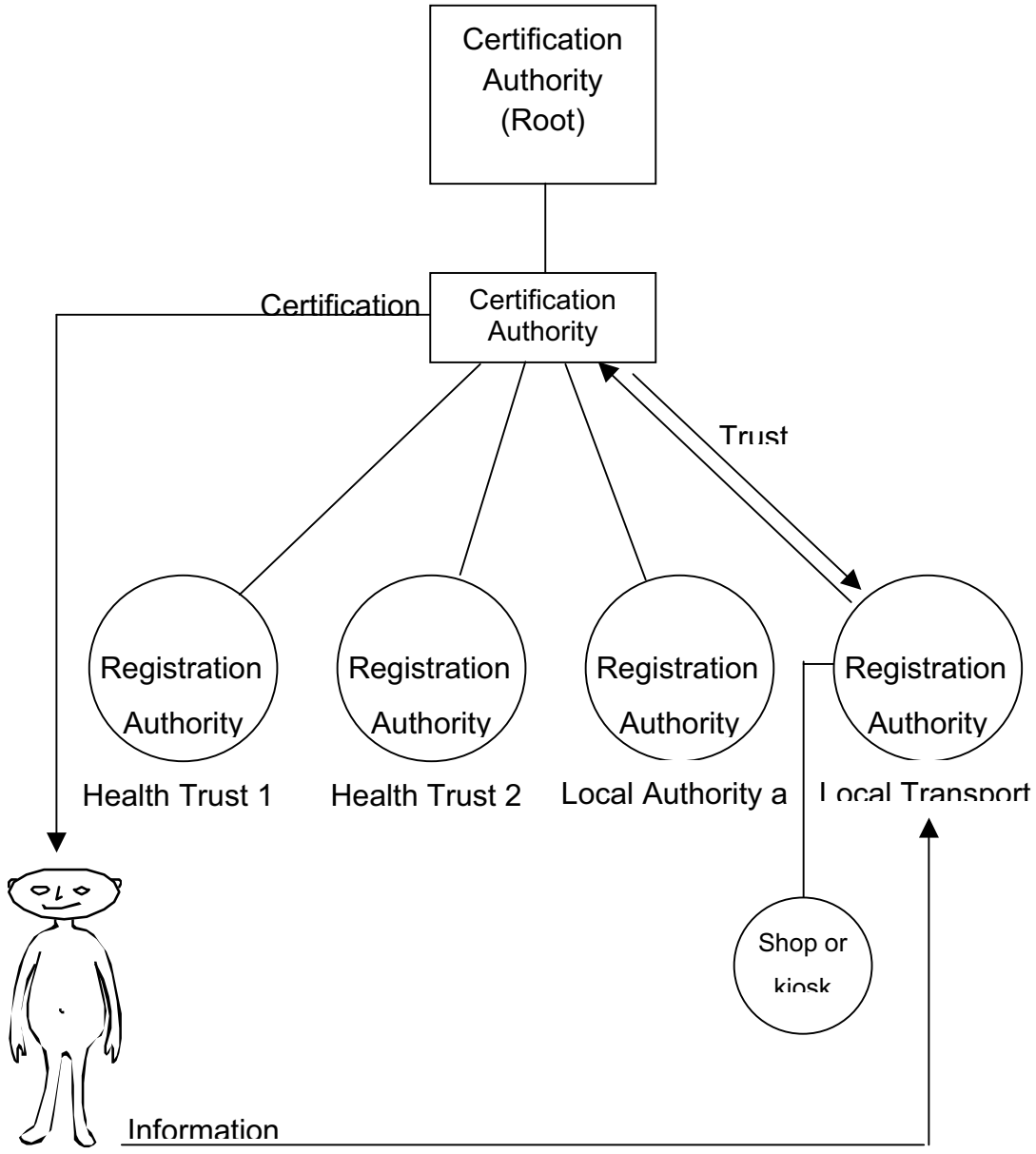
Authentication provides users with a secure way to prove their identity during a transaction. It can also prove the identity of the other participant (card reader and service provider) back to the user. However it is important that the level of authentication is appropriate to the application; users will get frustrated if they are required to provide information which they deem unnecessary.

5.1 Model for Citizen Authentication

In the diagram below the roles of the entities shown are as follows:

- Certification Authority (Root): This entity owns the 'name space' of the PKI domain. For example a <country.gov> name space could contain all government-related services and users for a particular country and each such service or user would have a unique object identifier (UOID) within that name space. Thus a high level object 'police' could exist in many root name spaces, e.g. <police.countryA.gov> and <police.countryB.gov> etc.
- Certification Authority (CA): An entity that is responsible for maintaining a portion of the root name space, e.g. <police.countryA.gov> and for issuing and validating certificates for that portion.
- Registration Authority (RA): An entity trusted by one or more CAs to identify unique objects (e.g. services, users, etc) allocate a UOID and authorise the CA to issue appropriate certificate(s). In the model shown the RA is also trusted by the user to hold their identification data and only share such data with the user's explicit consent. The principle of user choice in selecting a RA which they, the user, trusts is a key principle of this model and inherently requires there to be a fairly wide choice of RA's. Since the RA is then trusted by both the user and the CA, it is the key-stone of the trust model.
- User: The Citizen entrusts identification data to the RA in accordance with the scheme rules for gaining an agreed level of identification for use in Authentication and Authorisation decisions that require a higher level of assurance than that provided by the device (card) on its own.

The interaction of service objects is not shown in the diagram in order to reduce complexity. In summary though, service objects interact at both CA level to check certificate validity and, less frequently, at RA level to validate identification data when authorised by the user.



Using this model, the following Authentication levels can be supported:

Level 0 – Device

This is authentication at the card – terminal level; it identifies the card but only assumes the user. Normally used for high transaction rate, low security services such as access to transport, buildings, library services etc.

Level 1 – User

Level 0 plus a user supplied PIN. The user supplies a PIN, which is checked by the terminal against a PIN stored on the card in an encrypted format. This gives a level of

assurance in the actual user identity. This level requires cryptographic processing. Acceptable for many applications which do not require access to the central portal.

Level 2 – User Verified

As level one but with a second PIN verification (note: this is the same PIN, not an additional second PIN) carried out by the central security database. This provides a check against the PIN on the card being altered. This is the default for applications accessed via the portal.

Level 3 – Enhanced User

As level two but with a second 'proof' – this could be something else the user knows (e.g. mothers maiden name), or biometrics. This level would require strong encryption and digital certification to prove both card and user via PKI.

Level 4 – Application

This is an undefined application specific level of authentication. Any application can require further 'proofs' from the user to check their identity. As per level three this could be communicated via a PKI infrastructure. This level would not be supported directly by the security platform except in so far as it is necessary to record data for audit and non-repudiation purposes. At this level it is entirely the responsibility of the Service Provider to set the level of identification they will accept.

5.2 Identification Assurance Level

Each level will, in addition, have an assurance level indicator. This will reflect the confidence the original Registration Authority (RA) had in the identity of the user. Note that each RA will have a maximum level that they are trusted to allocate by any given service provider, i.e. it is up to the service provider to decide how much they trust the issuing RA.

Level 0	No checks made.
Level 1	Balance of Probabilities.
Level 2	Substantial Assurance.
Level 3	Beyond Reasonable Doubt.
Levels 4-8	Unspecified at this time.

5.3 Authentication Token

Each message from the user should carry an authentication token (data object), digitally signed by the card. The token should contain the following data:

- Authentication Level
- Identification Assurance Level

- Authentication Timestamp
- User identifier
- RA identifier
- Terminal identifier

5.4 Personal identification numbers and passwords

The usual method for authentication has been a four digit personal identification number (PIN). If the system is on-line, then the PIN is stored in the host computer. However for off-line transactions, the PIN has to be stored in an encrypted form on the card.

Many users have problems remembering more than one PIN, so are likely to keep a written record of their PINs (hopefully not written on the back of the card). An alternative is that the user changes all their PINs to be the same number, with the obvious risk that someone else finding out their PIN could then undertake fraudulent transactions with the other applications. It is technically possible to have a common set of authenticators (eg PIN, password, biometric) with the application choosing the level it needs to satisfy its requirements.

The PIN must not be displayed visually or audibly during the transaction. However it is useful to provide a visual (e.g. an 'X') and an audible indication that the user has entered a digit.

People with dyslexia often have problems in remembering a four digit PIN in the correct order, so are likely to prefer alternative biometric systems for authentication. Also some people with an intellectual impairment have problems in not telling other people their PIN.

5.5 Keypads and User Input Devices

For all users, but particularly those who are blind, it is advisable to have a consistent arrangement for the keys including the function keys. However there are two common arrangements for numeric keys – that used for calculators and that for telephones, but devices such as wallets for electronic purses can use either system depending on whether the wallet also includes calculator functionality. This is very confusing for the consumer particularly if they have to use such a device in the back of a taxi at night.

For card reading devices, such as point of sale terminals, the keypads should:

- Use the telephone layout of numeric keys
- Include a tactile dot on number '5'

- Have good visual contrast between the keycaps and the facia
- Used raised keys with concave keycaps
- Have clear visual markings which will survive the anticipated use (with a clear typeface)
- The visual markings should not be obscured by a left-handed user
- Well spaced keys (NB the spacing of the keys is as important as the size of the keys for someone with poor manual dexterity)
- Provide tactual feedback (i.e. a gradual increase in force, followed by a sharp decrease in the force required to activate the key, and a subsequent increase in force beyond this point for cushioning)
- Ideally the keys should be internally illuminated when active

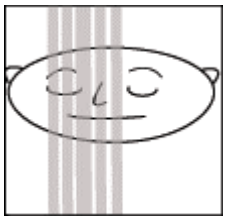
Passwords are easier to remember than PINs so tend to be more secure. Alphanumeric passwords can be input from a numeric keypad but this requires good manual dexterity (as demonstrated by many teenagers sending text messages on their mobile phones). However many elderly people would have the greatest difficulty if restricted to using a numeric keypad, so it would be preferable to provide an alphanumeric keypad (an actual keyboard is easier for the uninitiated than a virtual keypad on a touch screen) if space permits.

Some devices, such as personal digital assistants, can recognise handwritten characters, but these systems give better accuracy if they trained with the individual user. People with a hand tremor can find these systems difficult to use.

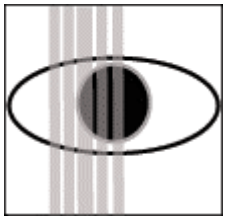
5.6 Biometric Identification Systems

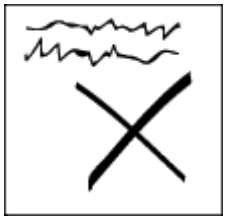
Biometrics permits the automatic identification of an individual based on his or her distinguishing physiological and/or behavioural characteristics. Biometric identification involves comparing with a database of templates to find out who you are, but biometric verification is where the template is compared to the one supplied with your claimed identity. Some biometric systems cannot do identification but can only verify the claimed identity of a person.

Biometric technologies include:

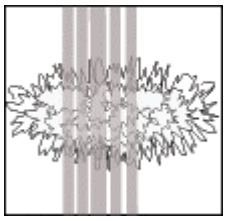

Facial imaging

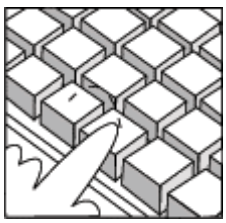

Hand and finger geometry


Iris pattern


Dynamic signature


Voice


Vein geometry


Keystroke


Finger and palm imaging

For the user, it should be easy and comfortable to use the system. Many users would prefer methods which do not require physical contact between the individual and the

device. Consumers need confidence that the system will reliably correctly identify them while not permitting other users access; no current biometric system achieves 100% success in both these aspects.

Depending on cultural background, some users will feel that some biometric systems are a threat to their privacy or unacceptable for some other reason. Therefore designers should be sensitive to these aspects, otherwise consumers could decline to use the services.

It is important that clear instructions are provided on how to use a biometric system. To establish consumer confidence, it may be necessary to provide human assistance for first time users.

Facial recognition can have an unacceptable level of either false positives or false negatives. It is technically best used to say "is this the same person" rather than "who is this person". Thus it is an appropriate technology when used with a secure token such as a smart card. From the users perspective it's non-intrusive nature is a major advantage and users are likely to accept such a system if it can provide a decision quickly, and is seen to be protecting their interests.

Fingerprint systems are good for the low number of false acceptances, but can be problematic for those with damaged fingers or with prosthetic hands. Some users will associate fingerprints with criminal investigations, so may be reluctant to use the system.

Iris recognition is a secure system, but the user has to position their eye in relation to a camera. This can give problems for users who are very tall, very short, or in a wheelchair. There are obvious problems for users who are blind or have a visual prosthesis.

The biometric information can be stored in a central database or on the smart card. Users are likely to have more trust in biometric systems if they are not worried that the personal data on them stored in a central database could be misused.

Users should have the facility to choose an alternative verification system even if it is a PIN. However this choice may be subject to regulatory or legal requirements imposed on the service provider. The user should be advised if the alternative is less secure, but the decision to use an alternative system should be left to the user.

6 Authorisation

Authorisation is the process where the user is allowed to access a given service or data set. Effectively the users current authentication level, time and place of authentication, etc. are checked against the business rules applicable to a given service.

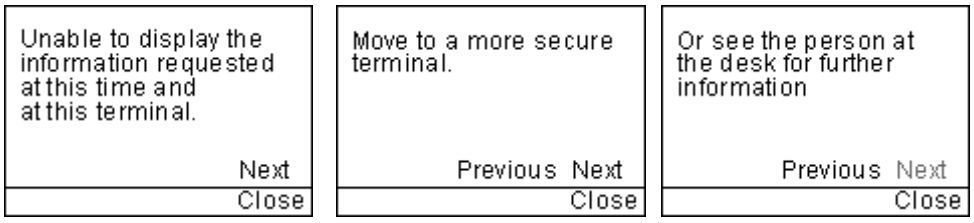
For example health services may require the user to be located at a private workstation in a secure place such as a government building rather than at a kiosk in a public area. Banking services may require the user to be at an ATM and to have authenticated to a given level in the last, say, 2 minutes.

It is important to note that there are three possible responses to an authorisation request:

1. Granted
2. User may access this service but re-authentication is required
3. Refused

Where access is denied the reasons for such denial or request for re-authentication should be clearly explained and help should be provided to advise the user on the actions they should take to remedy this situation.

For example:



7 Digital Signatures

Electronic Signature: an electronic sound, symbol, or process attached to or logically associated with an electronic document which has been executed or adopted with the intent to sign the document.

Digital Signature: A cryptographic modification of data that provides: origin authentication, assurance of data integrity, and signer non-repudiation (when associated with a data unit and accompanied by the corresponding public-key certificate.

A digital signature (not to be confused with a digital certificate), is a form of electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document. It then enables the recipient to ensure that the original content of the message or document is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message was the one actually received means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

For the user it is important that the user interface is simple and consistent. The basic elements are:

1. Identification.
2. Read / check before you sign.
3. Signing.
4. Send.

This could take the form of a message: After you have checked the text, you can now sign. You have to identify yourself with your PIN or password, and press the button "Sign". This has the same meaning as when you sign a paper.

Icons can be useful as long as a significant portion of the potential user population understand their meaning. In general, icons should be used in conjunction with text and not on their own. Icons have advantages for users whose primary language is one not used by the system.

7.1 Advanced Digital Signatures

An advanced electronic signature is one that is uniquely linked to the signatory, and is capable of identifying the signatory. It is created using means that the signatory can maintain under his sole control, and is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

An advanced electronic signature based on a qualified certificate and created by a secure signature creation device can satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data.

7.2 An example of using a Digital Signature

Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

1. You copy-and-paste the contract into an e-mail note.
2. Using special software, you obtain a message hash (mathematical summary) of the contract.
3. You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash. This should be performed by the smart card as a typical 'secure signature creation device'.
4. The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message.

1. To make sure it's intact and from you, your lawyer makes a hash of the received message.
2. Your lawyer then uses your public key to decrypt the message hash or summary.
3. If the hashes match, the received message is valid.

7.3 Informed Consent

Informed consent does not just require that the user presses a key to authorise an action, it also means that the user understands the implications of this action. In practice it may be very difficult to gauge the user's understanding particularly for those whose primary language is not used by the system or those with a cognitive impairment. The service provider has a responsibility to ensure, as far as is reasonably possible, that the user understands the implications of their actions.

7.4 Consumer Protection Legislation

Legislation, in relation to digital signatures, differs from country to country, which leaves the consumer with uncertainty as to their legal protection if something goes wrong. In the first instance, it is essential to have a common legal basis throughout the European Union.

When a transaction or message crosses supra-national boundaries (e.g. a user accesses a service based in the USA, China, etc.) then the lack of these standards means that in the interim, the user must be warned of the risk. It is not sufficient to assume that the user knows, and help should be available to clarify the differences in consumer protection standards.

Whilst common EU standards are being agreed, but have not been implemented, then warnings should also be provided for inter-EU country transactions. Similarly, when new countries join the EU, then warnings will be necessary during their transition phase as their laws are adjusted to the European norm.

8 References and Further Information

Community Framework for Electronic Signatures, Directive 99/93/EC.

Identification and Authentication in eGovernment, Final Report, 2002. (OSCIE Vol. 4 Part 3), eEurope Smart Cards Trailblazer 2,

eGovernment white paper on smart card applications and evolution.- Part 1 Analysis of developments (OSCIE Vol. 1 Part 1), eEurope Smart Cards Trailblazer 10

Electronic Identity White Paper (OSCIE Vol. 4 Part 1), eEurope Smart Cards Trailblazer 1

9 Abbreviations and Acronyms

CA	Certification Authority
CEN	European Committee for Standardisation
CVM	Cardholder Verification Method
eGIF	e-Government Interoperability Framework (UK)
GIF	Global Interoperability Framework (European, eESC)
ISO	International Organisation for Standardisation
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POS	Point of Sale
RA	Registration Authority