OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication

June 2007

www.oecd.org/sti/security-privacy

OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

This work is published on the responsibility of the Secretary-General of the OECD.

Foreword

The Recommendation on Electronic Authentication and the Guidance for Electronic Authentication have been developed by the OECD Committee for Information, Computer and Communications Policy (ICCP), through its Working Party on Information Security and Privacy (WPISP). The work has been led by Jane Hamilton from Industry Canada with the support of delegates from Australia, France, Hungary, Korea, Norway, the United States, the OECD Secretariat and the Business and Industry Advisory Committee (BIAC) to the OECD. The draft Recommendation was adopted as a Recommendation of the OECD Council on 12 June 2007. The Guidance for Electronic Authentication, was adopted by the ICCP Committee in April and declassified on 12 June 2007 by the OECD Council.

Table of Contents

Preface

Electronic authentication provides a level of assurance as to whether someone or something is who or what it claims to be in a digital environment. Thus, electronic authentication plays a key role in the establishment of trust relationships for electronic commerce, electronic government and many other social interactions. It is also an essential component of any strategy to protect information systems and networks, financial data, personal information and other assets from unauthorised access or identity theft. Electronic authentication is therefore essential for establishing accountability online.

The importance of authentication for electronic government and global electronic commerce was recognised back in 1998 by OECD Ministers at the Ministerial Conference "A Borderless World: Realising the Potential of Global Electronic Commerce" held in Ottawa, Canada.[1] In their "Declaration on Authentication for Electronic Commerce," Ministers outlined a number of actions to promote the development and use of electronic authentication technologies and mechanisms. One important aspect included the need to develop consistent approaches to electronic authentication to facilitate cross-border electronic commerce.

The OECD has carried out several initiatives to support Member countries' efforts to implement the Ministerial Declaration. It has worked in particular to address two important challenges: increasing confidence in authentication processes and operators, and breaking down barriers to the use of authentication across borders. In 1999, a Joint OECD-Private Sector Workshop was organised to foster dialogue among all stakeholders,[2] followed in 2000 by the development of an "Inventory of Approaches to E-Authentication and Certification in a Global Networked Society"[3] and a report on "Progress Achieved in Furtherance of the Ministerial Declaration."[4] More recent work included a 2003 "Survey of Legal and Policy Frameworks for E-Authentication and E-Signatures"[5] and a report on the "Use of Authentication across Borders"[6] completed in 2005.

[1] SG/EC(98)14/FINAL
www.olis.oecd.org/olis/1998doc.nsf/linkto/sg-ec(98)14-final

[2] DSTI/ICCP/REG(99)14/FINAL
www.olis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)14-final

[3] DSTI/ICCP/REG(99)13/FINAL
www.olis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)13-final

[4] DSTI/ICCP/REG(2001)10/FINAL
www.olis.oecd.org/olis/2001doc.nsf/linkto/dsti-iccp-reg(2001)10-final

[5] DSTI/ICCP/REG(2003)9/FINAL
www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp-reg(2003)9-final

[6] DSTI/ICCP/REG(2005)4/FINAL
www.olis.oecd.org/olis/2005doc.nsf/LinkTo/dsti-iccp-reg(2005)4-final

In 2006, building on this work, the ICCP Working Party on Information Security and Privacy (WPISP) prepared a document providing policy and practical guidance for the development, implementation and use of electronic authentication products and services as they relate to the authentication of persons and entities.

The Guidance sets out the context and importance of electronic authentication for electronic commerce and electronic government and provides a number of foundation and operational principles that constitute a common denominator for cross-jurisdictional interoperability. It aims to help Member countries and non-Member economies establish or, as appropriate, amend their approaches to electronic authentication with a view to facilitate cross-border co-operation. The Guidance takes account of work undertaken in other fora, particularly the Asia-Pacific Economic Co-operation's (APEC) work on requirements for cross-jurisdictional authentication services. Selected national approaches to authentication have also been used as an additional input.

The Guidance document served as the basis for the OECD Council Recommendation on electronic authentication which reaffirms the important role of electronic authentication in fostering trust online and the continued development of the digital economy. The Recommendation encourages efforts by Member countries to establish compatible, technology-neutral approaches for effective domestic and cross-border electronic authentication of persons and entities.

Both the Recommendation and the Guidance conclude a work stream initiated in response to the "Declaration on Authentication for Electronic Commerce" adopted by Ministers at the Ottawa Ministerial Conference held on 7-9 October 1998 and serve as a bridge to future OECD work on identity management.

It is anticipated that they will also inform ongoing and future discussions in other international forums such as the Asia Pacific Economic Cooperation (APEC), the United Nations Commission on International Trade Law (UNCITRAL) and national and regional standards organisations.

Recommendation of the Council on Electronic Authentication

Recommendation of the Council on Electronic Authentication

THE COUNCIL,

Having regard to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

Having regard to Rule 18 b) of the Rules of Procedure;

Having regard to the Declaration on Authentication for Electronic Commerce [C(98)177];

Having regard to the Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security [C(2002)131/FINAL] hereinafter the "Guidelines for the Security of Information Systems and Networks";

Having regard to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL];

Recognising that trust is a key condition for many online transactions to take place, and that, within a broader system of measures and strategies, electronic authentication of persons and entities plays an important role in this respect;

Recognising that electronic authentication, which is an essential component of the verification and management of identities online, provides a level of assurance as to whether the other party is who or what it claims to be; and thereby reduces the uncertainty inherent in domestic and cross-border electronic interactions and transactions;

Recognising that effective electronic authentication helps to strengthen systems and network security, as well as privacy by reducing risks such as unauthorised access to personal data, identity theft and data breaches, and by providing additional means of accountability;

Recognising that electronic authentication is an important element in the continued development of governmental and other social and individual activities online, enables the creation of new business opportunities, contributes to the development of electronic commerce, and is a key component of a viable and sustainable Internet;

Recognising finally, that this Recommendation addresses electronic authentication of persons and entities, but does not address other aspects of electronic authentication, such as legal assurance of validity of documents or electronic signatures;

On the proposal of the Committee for Information, Computer and Communications Policy:

RECOMMENDS that Member countries:

- Work towards establishing technology-neutral approaches for effective domestic and cross-border electronic authentication of persons and entities, consistent with the OECD Guidelines for the Security of Information Systems and Networks and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
- Foster the development, provision and use of electronic authentication products and services that embody sound business practices, including technical and non technical safeguards to meet the participants' needs, in particular with respect to security and privacy of their information and identity.
- In both the private and public sectors, encourage business and legal compatibility and technical interoperability of authentication schemas, to facilitate cross-sectoral and cross-jurisdictional online interactions and transactions and to ensure that authentication products and services can be deployed at both national and international levels.
- Take steps to raise the awareness of all participants, including those in non-Member economies, on the benefits of the use of electronic authentication at national and international levels

RECALLS the Guidance on Electronic Authentication [DSTI/ICCP/REG(2006)3/REV3] which may assist Member countries in developing effective and compatible approaches to electronic authentication, both at the national and international levels.

INVITES non-Member economies to take account of this Recommendation.

INSTRUCTS the Committee for Information, Computer and Communications Policy to monitor developments connected with electronic authentication in OECD Member countries and other international forums, and review this Recommendation within three years of its adoption and thereafter as appropriate.

OECD Guidance for Electronic Authentication

OECD Guidance for Electronic Authentication

Introduction

Authentication encompasses a very broad range of things. The work of the OECD however, has focussed on the authentication of persons (natural and legal). OECD began its work on authentication as part of its leading work on electronic commerce. Early on, the OECD recognised that electronic commerce transcends time and geography/location, and sometimes lacked human engagement. As such, the need to properly identify parties to a transaction was seen as essential to building trust in electronic commerce. Today, these issues can be viewed as part of the broader topic of identity management that becomes an essential element of functioning in a digital economy and information society.

Purpose of this Guidance

This guidance document:

- Sets out the context and importance of authentication.
- Defines a set of Principles that provide a framework for the development, implementation and use of authentication products and services as they relate to the authentication of persons and entities. The principles also address cross-border authentication challenges.
- Identifies continuing issues associated with the use of authentication.

The guidance will be useful to OECD Member and non-Member countries in establishing their approaches to authentication and assist those with existing policies to identify and address potential amendments to their approach. While it is understood that Member countries need to comply with the legal provisions in their jurisdiction, the guidance offers a common denominator that opens possibilities for cross-jurisdictional inter-operability.

In addition to offering guidance on electronic authentication that can be referenced by OECD Member countries and non-Member economies, the document also functions as an inventory of instruments and mechanisms that contributed to the work and findings of the WPISP in this area. On this basis, in addition to being a useful tool for individual jurisdictions, it also has utility for ongoing and future discussions in international fora such as APEC's Telecommunications and Information Working Group and Electronic Commerce Steering Group, UNCITRAL and national, regional and international standards organisations among others.

Finally, and while the main purpose of the document is to provide policy and practical guidance for authentication based on OECD work that has been completed to date, it identifies those outstanding issues that the OECD considers should still be addressed, by Member countries and other international fora.

On this basis, this document:

- Ties together some of the results of OECD work to date on authentication.
- Provides a general set of guidance on some of the more complex issues associated with authentication.
- Highlights where further work may be appropriate by OECD or other bodies.

Authentication in Context

Authentication can mean a variety of things depending on the context in which the term is used. An Internet search on the term "authentication" yields a very broad range of definitions, some addressing authentication of persons or other entities, others addressing things, documents and systems. Across these definitions, authentication is accomplished through processes that have various degrees of detail and technical specificity. These processes are aimed at determining whether someone or something is, in fact, who or what it claims to be. As such, effective authentication is a key contributor to the establishment of a trust relationship in a digital environment. For the purposes of this guidance, authentication is defined as:

> *A function for establishing the validity and assurance of a claimed identity of a user, device or another entity in an information or communications system.*

This definition implies two processes and one result:

- A claim related to a person, other entity or thing is presented (claiming process).
- That claim is substantiated (substantiation process).
- As a result, a degree of confidence, or lack thereof, in the claim is generated.

Authentication is not an end, but rather a sub-process in a security system that must work in conjunction with authorisations, rights management, access control and audit processes. Authentication is dependent on substantiating one or more of the following factors: something the claimant knows (*e.g.* a shared secret such as a password), something the claimant has (*e.g.* a token) and something the claimant is (*e.g.* a biometric or set of attributes like height, age and weight). Once a person, other entity or thing has been authenticated (*e.g.* the claim is valid as stated), a variety of things can be enabled. For example, in the case of authenticating an individual, certain rights may be provided to that authenticated individual (authorisation process), along with the responsibilities that may be associated with exercising those rights. Authentication may be bi-directional and offer assurances[7] for both parties to a transaction.

Most often, in the case of authenticating a person, the interest lies in authenticating the person's identity. However, there are circumstances where the interest rests in authenticating an attribute related to a person rather than their identity. For example, in certain online transactions, authentication is employed to

[7] See Appendix B Authentication Assurance Levels.

ensure that Web site visitors are above a certain age prescribed by law. In such cases, the attribute – age (something the customer is), is the main point of the authentication. It is therefore possible to use electronic authentication technologies to authenticate attributes without providing information on identity.

Providing a degree of anonymity can also play an important role to help build trust in online systems. Authentication technologies that do not collect personal information can ensure that information that is not necessary for the transaction in the first place is not collected or used for another purpose in the future. Simply not using authentication at all when it is not needed is another way of contributing to user trust.

While document authentication has long existed through notarisation and its antecedents, new forms of electronic document authentication are also being developed. In the physical world, this may require the presence of the person and the presentation of a credential with both a signature and a photograph. In the online environment, there are a variety of new means of creating digital credentials. Such credentials may be used to authenticate persons (or entities) and they may enable electronic "signing" of documents. The use of electronic signatures for producing legal effect equivalent to handwritten signatures raises several issues which are addressed by the UNCITRAL 2001 Model Law on Electronic Signatures. OECD Member countries support the use of electronic signatures as equivalent to handwritten signatures and advocate technology neutrality in their use.

Even more complexity exists where an automated set of software agents and authentication of systems or machines is introduced. Many legal concepts are predicated on intent between human actors. This then begs the question of how to convey intent and apportion obligation upon transactions that are not human mediated.

In digital environments, authentication raises other complex issues and a range of challenges. Some of the issues relate to how identity is defined and captured in a way that promotes trust in a virtual environment where every aspect needs to be formalised in order to allow for automated processing. While in many respects these issues are the same as in the physical world, the increased level of ambiguity, coupled with serious security threats in the online environment introduces new complexities that must be addressed. The challenges can be considered technological (*e.g.* interoperability, security), legal (*e.g.* legal recognition, liability, privacy) and economic (*e.g.* cost of deployment and of use). There may be significant variance across sectoral implementations which also serve to increase complexity. These challenges are made more difficult by the scale and speed of technological innovations.

A further challenge is the fact that approaches to authentication have emerged on a sectoral or an application-by-application (or service) and proprietary basis. In order to capture some of the economies of scale which may be essential to the economic viability of authentication service providers, commonality among applications needs to be identified. These challenges illustrate the need to adopt a more comprehensive and holistic approach to trust and confidence concerns and to explore secure, privacy enhancing, efficient and convenient approaches to managing identities on-line in order to realise the full benefits of the on-line environment. It is hoped that future OECD work on identity management will facilitate the resolution of some of the issues which have been mentioned above, such as this sectoral, or "silo", approach to authentication.

Authentication mechanisms need to be continually upgraded to keep ahead of new forms of fraud (*e.g.* attackers steal credentials and use them to perpetrate fraud or other crimes). It is therefore desirable for authentication methods to be implemented with the ability to leverage more robust authentication technologies in the future. The growing use of multi-factor authentication, as well as the use of biometrics (*e.g.* iris scanning or finger printing), is an example of this trend.

Viable business models for authentication services are a prerequisite for sustainable development and use of new authentication methods. Such models need to take into account the specific characteristics of the authentication marketplace, where network effects[8] and two-sided market effects[9] are paramount.

It is important to understand the broad complexity of the issues surrounding authentication; both in terms of interrelation with other systems and procedures as well as the variety of uses that may be possible. This broad set of topics has been introduced with the intention of providing some context to this guidance. However, the scope of the principles offered is limited to aspects that flow from OECD work to date on authentication which addressed two of the major challenges of authentication: the confidence in authentication processes and operators, and the challenges relying parties can encounter across borders. To the extent that authentication is a basic component of any identity management process or system, the principles below establish a "bridge" between the OECD authentication work that has now reached a certain degree of maturity and the nascent work on the more general topic of identity management. The history of this work since the "Declaration on Authentication for Electronic Commerce", and a summary of the surveys, reports and workshops that have been carried out by the OECD have been summarised in Appendix A. The list of OECD documents related to authentication since 1998 can be found in the References section at the end of this document.

Importance of Authentication

Businesses, governments and individuals all have sensitive data and assets to protect. Assurance is needed in particular in case of monetary transfers, when legally binding declarations are made or when transactions result in disclosure of personal information. By providing a level of assurance regarding the identity claimed by parties engaged in an online relationship, authentication reduces uncertainty inherent in transactions at a distance, thus fostering trust in electronic interactions, and participates to the broader fight against online threats and criminal activities.

Authentication is an element of a wider system of practices, procedures and technical implementations, that work together to secure information systems, networks and the electronic communications they support. The *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of*

[8] Meaning that the usefulness of a given product increases with the number of participants using the product (*e.g.* the fax machine).

[9] Meaning that the authentication market consists of at least two types of products/services that are complementary (*i.e.* authentication credentials/services and the applications using them). Both are needed for the market to function.

Security[10] recognise the inter-related, inter-dependent nature of these systems and emphasise the need to take a comprehensive and coherent approach to system security if organisational security goals are to be met, policies implemented and a culture of security achieved. Given that authentication forms the basis for most types of access control and for establishing accountability online, it should be viewed as critical building block of information security. In addition, effective authentication contributes to the protection of privacy by contributing to the reduction of risks such as unauthorised access to personal information and identity theft.

More broadly, authentication is a critical tool in achieving trust and online identity protection, which are essential to foster e-commerce and e-government.

Principles for Electronic Authentication

The Principles contained in this document are intended to ensure that authentication products and services embody sound business and market practices, meet the needs of users, aim to achieve interoperability to the extent possible, and are accepted internationally. They function as benchmarks for the development, provision and use of authentication services operating at both the national and international levels. On this basis, the Principles aim to facilitate cross-border electronic communications.

These Principles have been developed with a view towards establishing a consistent approach to evaluating risks inherent in e-transactions and a basis for comparison of mechanisms based on widely different technologies. On this basis, the Principles are intended to promote the compatibility of different authentication schemas. OECD Member countries are encouraged to take the Principles into consideration in their national approaches to electronic authentication. The Principles can also form the basis for voluntary initiatives that are tailored to the requirements of specific industries.

Important Points about the Principles

These Principles identify the functions and responsibilities of participants in authentication systems and provide a framework within which to assess and manage the risks that accompany these responsibilities. The Principles also identify security, privacy, disclosure and complaint-handling matters that need to be taken into account in each stage of the design, development, implementation and assessment of an authentication process.

The Principles are intended to apply to authentication processes used in connection with electronic communications that take place between businesses or governments and other organisations (B2B, B2G and G2G), between organisations and individuals (consumers or citizens – B2C, G2C) and between individuals (C2C).

A range of technical, legal, contractual and commercial relationships can exist between providers of authentication services and users of those services. Many of these relationships are governed by agreements. The Principles contained in this

[10] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.

document are intended to guide the development of these agreements and to apply to the full range of relationships.

The provisions in the various Principles are inter-related and inter-dependent. On this basis, it would be difficult for them to achieve their purpose if they are implemented selectively. Those applying the Principles to define or implement authentication processes are encouraged to exceed the benchmarks that the Principles establish and to expand upon them to address the requirements of their particular security environment or application.

The Principles are expressed at a high level of generality and technological neutrality. A wide variety of authentication technologies and techniques is available and choices should be governed by the nature of the particular communication and the requirements of the participants. The implementation of authentication processes also differs, depending on the business or legal objectives to be met, as well as the characteristics of the environment in which electronic communication takes place, such as security and privacy needs and other legislative or regulatory obligations. These factors define the functionality required of an authentication process and, in some cases, even the type of authentication to be used. Choices will also depend on the degree of deployment of various types of authentication solutions *(i.e.* what solutions or credentials are already present).

The Principles contemplate authentication in its broadest sense but:

- Do not contemplate the authentication of documents.
- Do not include device or domain-level authentication but do have linkages to elements of the Anti-Spam Toolkit developed by the OECD Spam Task Force[11] (*e.g.* authentication applications aimed at reducing spam and harmful e-mail).
- Do not include "authorisation" (which is a separate but related process that refers to verifying the person's or organisation's authority to conduct specified transactions). Typically, decisions concerning authorisation are the purview of the relying party (*i.e.* the entity or person that is relying on the identity assertion to make the authorisation decision).
- Do not address electronic signatures per se (or digital signatures where the authentication is tightly bound to the signed object).

On this basis, it is possible that aspects of authentication, or subjects beyond the scope of these Principles may need to be explored and complementary policy tools developed (by the OECD and other fora) to ensure that the needs of specific users and applications are adequately addressed.

The authentication environment is dynamic and the technologies used will continue to evolve. Although every effort has been made to define Principles that can encompass foreseeable developments, they are open to revision as needed to take into account significant technological advances, changes in market characteristics, and international developments.

[11] Cf. "OECD anti-spam Toolkit", www.oecd-antispam.org.

Concepts and Terminology

These Principles relate to the authentication of electronic communication in its broadest sense. Therefore, the concepts and terms used relate to all participants, actions and techniques comprising all aspects of authentication, whether considered from the technical, legal or business perspective. Each concept or term relates to the others; none should be considered in isolation.

In developing the following, existing definitions were considered, particularly those created by international standards groups such as the International Organization for Standardization (ISO). However, the broad scope of this guidance and its policy orientation resulted in definitions that may not correspond to similar terms used elsewhere in specific contexts or at a technical level.

- **Authentication:** A function for establishing the validity and assurance of a claimed identity of a user, device or another entity in an information or communications system.
- **Assurance:** A process to confirm one of several security goals to protect information and information systems, including authentication, integrity, availability, confidentiality, and accountability. Assurance is not absolute: it is a defined level of confidence. Assurance levels relating to authentication may be approached from various points of view – one of them being risk management practices and the other suitable technological solutions.
- **Attributes:** Information concerning specific types of characteristics of a given identity.
- **Authorisation:** The actions an authenticated person or entity is permitted as a result of authentication. Authorisation may depend on selected attributes of an identity. Decisions concerning authorisation are the purview of relying parties.
- **Credential:** Data that is used to establish the claimed attributes or identity of a person or an entity.
- **Electronic Communication:** An electronic transmission, message or transaction.
- **Electronic Signature:** Data in electronic form in, affixed to, or logically associated with, a data message and used by, or on behalf of a person with the intent to identify that person.
- **Encryption:** The conversion of data (plaintext) into a form called a ciphertext that cannot be easily understood by unauthorised recipients. Decryption is the process of converting encrypted data back into its original form, so it can be understood. Common encryption types include symmetric and asymmetric (public-key) encryption.[12]
- **Identity:** At the operational level, a dynamic set of attributes defining a unique reference to a person or an entity, including where attributes are

[12] The OECD Guidelines for Cryptography Policy are an important reference. The Guidelines recognize the important role encryption plays in helping to ensure the security of data and the protection of privacy in national and global information and communication infrastructures, networks and systems. www.oecd.org/document/11/0,2340,en_2649_201185_1814731_1_1_1_1,00.html.

provided in electronic form, using some sort of credential. The attributes may be context-specific based on the nature of the interaction.

- **Participants:** Individuals or organisations participating in authentication processes. Includes individuals or organisations asserting identity, relying parties, third party authorities providing identity credentials, trust service providers and system certifiers, such as auditors, accreditation bodies, federation governance bodies, government supervisory bodies. Participants may have multiple roles.
- **Relying party:** The entity or person that is relying on an identity credential or assertion of identity to make a decision as to what action to take in a given application context.

In an effort to address the benefits of national and cross-jurisdictional authentication methods, the following foundation and operational principles are offered. The foundation principles constitute guiding principles for the use and implementation of authentication methods, and are inter-related to one another and the operational principles. The operational principles serve as guidance to all users, and in particular to those involved in the design, development and deployment of authentication services and products.

Part A – Foundation Principles

1. Systems Approach

The design, development and implementation of authentication solutions should be seen as a coherent system development process involving all relevant participants at appropriate stages. Particular attention should be paid to the involvement of end users of authentication at the system design stage. Interoperability of authentication solutions should be addressed at this stage as well. Technical and non-technical safeguards should be considered as complementary parts of system design of authentication solutions.

When designing and implementing authentication solutions, overall system security should be a key driver. Threats and challenges introduced by all relevant participants in the data transmission and storage process should be addressed at all stages of system design and development of authentication solutions.

The selection of assurance levels and mechanisms for authentication should be based on a risk assessment of the various system components and of the participant behaviour(s). User friendliness and ease of use should be a leading principle for selecting authentication mechanisms as well as it contributes to fostering trust in online transactions. Security features and ease of use need to be balanced in such a way so as to ensure that overall system security is in place.

2. Proportionality

The degree of responsibility and risk that each participant in the authentication process assumes should be in proportion to the degree of knowledge and control that the participant can reasonably be expected to have and to exercise, as well as to the nature and value of the transaction or communication itself. Since participants can perform multiple functions in varying combinations, the degree of responsibility and risk assumed by any one participant may vary, depending on these functions.

3. Roles and Responsibilities

Participants in authentication processes should be aware of their roles, the functions they are performing and of the responsibilities associated with those functions. Functions and responsibilities should be clearly formulated and disclosed. All participants should act prudently and take reasonable steps to inform themselves of the nature of the authentication process, including its requirements and limitations, to protect information associated with the process, and to manage the risks to which they are exposed.

4. Security and Trust

All participants in authentication processes have the responsibility to contribute to the security and mitigation of risk through sound security practices, as laid out in the OECD Security Guidelines' eighth principle on security management.[13]

All participants in an authentication process should be responsible and accountable for security, in proportion to their roles in that process. Those designing and implementing security and trust services, should bear more responsibility than others for mitigating risk. This includes fostering a global culture of security by building security and trust (*e.g.* privacy protection) features into information systems and technologies. By practicing sound security principles, organisations will contribute towards building trust in the use of technologies that facilitate online transactions. Authentication plays a key role in securing trust in online transactions and e-commerce by establishing reliable access controls and accountability.

5. Privacy

Organisations engaged in the design or operation of authentication processes should comply with the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and with relevant codes of practice, in addition to applicable legislation. This principle is particularly important in the context of cross-border authentication, where privacy laws and regulations may vary.

Those designing and implementing authentication processes should consider how systems can appropriately respect privacy and data protection at every stage of the process. This would involve limiting the collection, use, storage, transfer and disclosure of personal information to the purposes deemed necessary for accomplishing authentication. Where notice is provided to individuals, notice should be accurate, clear, conspicuous and unambiguous. Individual control over personal data by the authentication subject is encouraged even if stewardship of that data is by a public authority or other third party.

The level of authentication (and, by definition the amount of personal information collected for that authentication process) should be in proportion to the nature of the transaction or communication and take into account the degree of

[13] This Principle adopts the OECD Guidelines for the Security of Information Systems and Networks. The complete text of the Guidelines is available at www.oecd.org/dataoecd/16/22/15582260.pdf

importance and sensitivity required. This principle is particularly important in the context of cross-border authentication where privacy laws and regulations can vary.

Authentication offers ways to protect privacy but only if it is used in a manner that is fit for purpose and takes into account the interests of users. There may be a tendency to require the strongest level of authentication for all transactions with a view to protecting systems and their users. However, while a greater amount of personal information may be required to attain the more reliable credential (identity proofing), systems can, and should be designed so as to not expose this information during routine parts of the authentication transaction or the electronic communication.

6. Risk Management

The risks associated with authentication processes for electronic communications should be identified, assessed and managed in a reasonable, fair and efficient manner. The responsibilities of participants concerning risk management should be in proportion to the degree of knowledge, control and power to act that each participant can reasonably be expected to have and to exercise. The ability of participants to identify, assess and manage risks will vary substantially and some types of participants *(e.g.* consumers and small enterprises) may not reasonably be expected to do this to the same extent as other participants. (See Principle 2 – Proportionality)

This principle should also be applied when considering the selection of appropriate assurance levels for various types of applications. The selection of assurance level of authentication should be guided by the likelihood and consequences of identified risks and impacts (*e.g.* misappropriation of identity for all participants).

The selection of assurance levels based on risk analysis should be closely associated with selection of appropriate authentication mechanisms that match the identified risks and impacts with appropriate security features in a cost-effective and efficient manner.

Part B – Operational Principles

1. ***Usability:*** Authentication processes should be effective, efficient, reliable and easy to use and should take into account the interests and requirements of individuals and organisations. Usability should be guided by minimising the risks associated with use.

2. ***Fit for purpose****:* Authentication, like many security related practices and technologies, exists along a continuum of risk. This means that authentication technologies and processes must be considered in the context of an application and be appropriate and proportional to its function and desired use. There should be enough security to address risk in an acceptable fashion, but not be unreasonably burdensome to accomplish the electronic communication. The business requirements for trust are reflected in the assurance level provided and are related to the type of credential used. *(See Appendix B for more information and examples of assurance levels.)* Market-based decisions should be key drivers in determining which authentication technologies should be used**.** Service providers should

consider the level of risk to the system as a whole, the cost of implementation, practicality, overall business benefit and applicable legal requirements.

3. ***Business continuity:*** Establishment of business continuity and incident recovery planning provisions will develop user ***confidence*** and facilitate cross-jurisdictional acceptance of reliable authentication activities or tools**.**

4. ***Education and awareness:*** Effective authentication processes can be an effective deterrent to the theft of online assets and information. Education and awareness of the benefits ***and*** proper uses of authentication are prerequisites for wide penetration of electronic authentication, and critical for continued user trust in networks and information systems. Education campaigns should stress the importance of tools that are user-friendly and yet achieve an appropriate degree of security. Special attention should be paid to consumer and small enterprises education focussing not only on the benefits of authentication, but also the responsibilities and risks associated with its use.

5. ***Disclosure:*** Participants that offer authentication services should disclose information to the other participants to ensure that all participants are aware of the risks and the responsibilities associated with the use of authentication. Appropriate disclosure requires the information to be provided in sufficient detail for the purpose, be in plain language and be conspicuous. All three factors will have a bearing on the knowledge other participants can reasonably be expected to have of the disclosed information.

6. ***Complaints Handling:*** Organisations that utilize authentication processes should make available a complaints-handling process that enables participants to resolve complaints efficiently and effectively and to respond appropriately to non-compliance issues. Complaints handling processes should be visible, accessible, responsive, and objective.

7. ***Independent audit and assessments:*** The use of compliance audits and assessments by independent parties, preferably according to internationally recognised standards, will develop user confidence and facilitate cross-jurisdictional acceptance of services. Each step of the authentication process, from identity proofing to technical or administrative management of the service, influences whether the process is trustworthy and in compliance. Ideally each step in the process should be consistent in its strength and robustness. Accreditation bodies that oversee the requirements for certification and accredit the auditors doing the certification also have an important role to play. Their adherence to generally recognised procedures can also facilitate cross-jurisdictional acceptance of services.

8. ***Cross-jurisdictional approaches:*** National approaches to authentication should ideally allow for foreign-based authentication services to be accepted as long as local requirements, or their equivalent, are met. Such local requirements should not be created or implemented in a discriminatory manner. Consistency in applying standards and general agreement on how to define levels of assurance can facilitate cross-jurisdictional (and cross-sectoral) interoperability. Business, technical and legal inter-operability are necessary for cross-sectoral and cross-jurisdictional transactions. Interoperability needs to be considered at the design stage wherever possible.

9. ***Standards:*** Wide deployment of authentication technologies that may be used in a global context is heavily dependent on standards, both *de facto* and *de jure*. Standards aim at consolidating requirements of suppliers, users, relying parties and government legislative bodies into frameworks that may be used for co-ordinated implementation of authentication schemes. Relevant standards bodies that issue standards important for global interoperability of authentication schemes include: ISO, ITU, ETSI, CEN, ANSI, NIST, OASIS – Liberty Alliance, W3C, IETF and CC (Common Criteria) Multilateral Arrangement.

In order to achieve some degree of interoperability of various authentication schemes, standards should be applied when developing and implementing authentication solutions, in particular considering enrolment procedures, credential deployment, technical capabilities and security of credentials, management of credentials, technical interfaces between authentication solutions and applications, as well as any government supervising procedures for authentication suppliers.

Continuing Issues

The above principles provide a framework to help foster common approaches to authentication in order to foster the use of authentication at national and cross-border levels. However, several issues identified in previous OECD work and in discussions between Member countries, business and the civil society which took place in the OECD Working Party on Information Security and Privacy (WPISP) and Committee for Information, Computer and Communications Policy (ICCP) remain unaddressed. These continuing issues are offered as considerations for the appropriate OECD committee(s) and other international fora, industry and civil society to consider in discussions pertaining to the digital economy and future challenges with identity management.

- The wide variety of existing authentication methods in use could be a source of confusion for users and providers in determining which method best suits their needs. This variety may become a barrier to inter-organisational or cross-border services. International standards could possibly remove some of the complexity currently existing in the authentication marketplace, but wider agreements on assurance levels and authentication methods that may be associated with these are needed in order to establish sustainable solutions, both nationally and at the cross-border level.

- In a globalised marketplace, efforts towards harmonisation of standards are essential to maximise their efficiency. Some efforts in that direction have already achieved results, *e.g.* US-Canadian Government cooperation on "bridge solutions" and the U.S.-EU/ETSI recognition of schemas for defining requirements for certification authorities (PKI services suppliers). Such efforts could be encouraged further and standards-mapping exercises could to be carried out under the auspices of relevant international bodies.

- Differences in the legal treatment and recognition of electronic documents and signatures are still an obstacle to the cross-border use of authentication. While work within international organisations such as UNCITRAL establishes common approaches, additional multilateral work at the practical level is still necessary.

- Mechanisms for recognising foreign authentication services have been developed but there is limited experience in cross-jurisdictional applications. Jurisdictions need some means of assessing the trust framework of their partners. This guidance document and the framework it offers may assist in this regard but more comprehensive work on the issue needs to be carried out.
- Previous OECD work identified the lack of business cases for authentication as an impediment to its wider use. Successes in the marketplace (*e.g.* home banking) could provide elements for such business cases and be leveraged to stimulate the wider adoption of authentication.
- Biometrics and Radiofrequency identification (RFID) are related to authentication as they encompass technology that can further enhance verification methods. It may be valuable to examine the impact of these emerging technologies on the business of authenticating and providing improved online security and identity management.

REFERENCES

OECD documents

The Use of Authentication Across Borders in OECD Countries (Summary of responses, 2005). DSTI/ICCP/REG(2005)4/FINAL
www.olis.oecd.org/olis/2005doc.nsf/LinkTo/dsti-iccp-reg(2005)4-final

Draft OECD Questionnaire for Preparing a Fact-Finding Report to Take Stock of the Current Usage of Authentication Across Borders (2004). DSTI/ICCP/REG(2004)5/FINAL

Summary of Responses to the Survey of Legal and Policy Frameworks for Electronic Authentication Services and E-Signatures in OECD Member Countries (2004). DSTI/ICCP/REG(2003)9/FINAL
www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp-reg(2003)9-final

Survey of Legal and Policy Frameworks for Electronic Authentication Services and E-Signatures in OECD Member Countries (Questionnaire, 2003) DSTI/ICCP/REG(2003)4/REV1

Electronic Authentication: Analysis and Mapping of Key Elements for Establishing Confidence in Certification Services (2002). DSTI/ICCP/REG(2002)4

Electronic Authentication: Framework for Analysis of Key Elements for Establishing Trust in Certification Processes (RD submitted by Canada, 2002) DSTI/ICCP/REG/RD(2002)3

Electronic Authentication: Information Paper on the Work of the APEC eSecurity Task Group - Draft for Discussion Purposes Only (RD submitted by Australia, 2002). DSTI/ICCP/REG/RD(2002)1

Progress Achieved by OECD Member Countries in Furtherance of the Ottawa Declaration on Authentication for Electronic Commerce (2002). DSTI/ICCP/REG(2001)10/FINAL
www.olis.oecd.org/olis/2001doc.nsf/linkto/dsti-iccp-reg(2001)10-final

Revised Inventory of Approaches to Authentication and Certifications in a Global Networked Society (2000). DSTI/ICCP/REG(2000)1/REV1

Questionnaire for the Survey on Form Requirements (2000) DSTI/ICCP/REG(2000)2

Inventory of Approaches to Authentication and Certifications in a Global Networked Society (1999). DSTI/ICCP/REG(99)13/FINAL
www.olis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)13-final

Joint OECD-Private Sector Workshop on Electronic Authentication. Menlo-Park, California, USA. 2-4 June 1999. In co-operation with private sector representatives and with The Stanford Program in Law, Science & Technology, Stanford Law School (1999). DSTI/ICCP/REG(99)14/FINAL including the “Background Paper on Electronic Authentication Technologies and Issues” [DSTI/ICCP/REG(99)6/REV1]
www.olis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)14-final

Proposal by the Delegation of the United Kingdom for Guidelines on Policy for Authentication and Electronic Signatures (1999). DSTI/ICCP/REG/AH(99)1

Discussion Paper on Authentication and Certification (1998). DSTI/ICCP/REG(98)1

OECD Ministerial Declaration on Authentication for Electronic Commerce (1998). DSTI/ICCP/REG(98)9/FINAL
www.olis.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg(98)9-final

Inventory of Approaches to Authentication and Certification in a Global Networked Society (1998). DSTI/ICCP/REG(98)3/REV1

See also:

- Anti-Spam Toolkit: Technical Measures to Combat Spam
  www.olis.oecd.org/olis/2005doc.nsf/linkto/dsti-cp-iccp-spam(2005)3-final

Other resources

International

- UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996)
  www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

- UNCITRAL Model Law on Electronic Signatures with Guide to Enactment (2001)
  www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html

Regional

- EU "Signposts Towards e-Government 2010"
  http://europa.eu.int/information_society/activities/egovernment_research/doc/minconf2005/signposts2005.pdf

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures, Official Journal L 013 , 19 January 2000, p. 0012 - 0020
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

National

- Australian government authentication framework:
  www.agimo.gov.au/infrastructure/authentication/agaf/impguidegovt
  www.agimo.gov.au/infrastructure/authentication/agaf/overview

- Canadian Authentication Principles
  http://strategis.ic.gc.ca/authen

- New Zealand government authentication framework:
  www.e.govt.nz/resources/news/2002/apr-2002/2002042801.html

- United Kingdom: "Registration and Authentication - e-Government Strategy Framework Policy and Guidelines"
  www.govtalk.gov.uk/policydocs/policydocs_document.asp?docnum=654&topic=56&topictitle=Security+Framework&subjecttitle=.

- United States:

  - NIST Special Publication 800 – 63 Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology (NIST), USA
    http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf

  - OMB's E-Authentication Guidance for U.S. Federal Agencies (M-04-04)
    www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf

Non-Governmental

- Center for Democracy and Technology "Authentication Privacy Principles Working Group. Interim Report". 13 May 2003. www.cdt.org/privacy/authentication/030513interim.shtml

- International Chamber of Commerce (ICC): General Usage for International Digitally Ensured Commerce (version II) - GUIDEC II www.iccwbo.org/home/guidec/guidec_two/foreword.asp

APPENDIX A

OVERVIEW OF OECD WORK ON AUTHENTICATION (1998 – 2005)

The Ottawa Ministerial Declaration

On 7-9 October 1998, OECD Ministers adopted the "Declaration on Authentication for Electronic Commerce" at the Ministerial Conference "A Borderless World: Realising the Potential of Global Electronic Commerce" held in Ottawa, Canada.[14] The Declaration recognised the importance of authentication for electronic commerce and outlined a number of actions to promote the development and use of electronic authentication technologies and mechanisms. In particular, Ministers declared their determination to:

- Take a non-discriminatory approach to electronic authentication from other countries.
- Encourage efforts to develop authentication technologies and mechanisms, and facilitate the use of those technologies and mechanisms for electronic commerce.
- Amend, where appropriate, technology or media specific requirements in current laws or policies that may impede the use of information and communication technologies and electronic authentication mechanisms, giving favourable consideration to the relevant provisions of the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996.
- Proceed with the application of electronic authentication technologies to enhance the delivery of government services and programmes to the public.
- Continue work at the international level, together with business, industry and user representatives, concerning authentication technologies and mechanisms to facilitate global electronic commerce.

[14] www.olis.oecd.org/olis/1998doc.nsf/linkto/sg-ec(98)14-final

Inventory of Approaches to E-Authentication and Joint OECD-Private Sector Workshop

As a preparatory step, the OECD ICCP Committee's Working Party on Information Security and Privacy (WPISP) surveyed Member country approaches to authentication and certification on global networks, including laws, policies and initiatives, in both the public and private sectors and at the national, regional and international levels. The resulting 1999 "Inventory of Approaches to Authentication and Certification in a Global Networked Society"[15] provided a useful resource on national approaches in particular on private contractual agreements, technology requirements, standards, and certification authorities.

In addition, the WPISP organised a joint OECD-Private Sector Workshop on Electronic Authentication[16] at Stanford, California, on 2-4 June 1999 to foster the dialogue among all stakeholders and further gather information on approaches to e-authentication. 200 representatives from OECD governments, Asia-Pacific Economic Co-operation (APEC) Telecommunications Working Group, private sector, international organisations, consumer advocacy and user organisations discussed business and government models, approaches of different industry sectors, and issues for implementing electronic authentication including requirements for the international operation of global authentication systems.

Report on Progress Achieved in Furtherance of the Ministerial Declaration

Following the workshop, a Steering Group was established by the WPISP to monitor the implementation of national policies and laws with regards to the objectives of the Ministerial declaration. The group updated in 2000 the "Inventory of Approaches to Authentication and Certifications in a Global Networked Society"[17] to take account of progress made at national level.

This work, along with information from APEC Member economies were integrated in a report on "Progress Achieved by OECD Member Countries in Furtherance of the Ottawa Declaration on Authentication for Electronic Commerce"[18].

The report concluded that progress had been made on issues such as the legal recognition of electronic signatures and the application of authentication technologies to the delivery of government services. The need for compatible approaches and policies among OECD Member governments and business initiatives to establish real international marketplace interoperability of electronic authentication systems was highlighted. The report suggested that additional work could help further identify and address impediments to the global, seamless use of authentication methods.

[15] DSTI/ICCP/REG(99)13/FINAL

[16] Proceedings and background documents can be found in DSTI/ICCP/REG(99)14/FINAL

[17] DSTI/ICCP/REG(2000)1/REV1

[18] DSTI/ICCP/REG(2001)10/FINAL

Survey of Legal and Policy Frameworks for E-Authentication and E-Signatures

In order to help determine how varying legislative, legal and policy frameworks could be bridged to provide for cross-jurisdictional acceptance of authentication services and for legal effect of electronic signatures, the WPISP conducted in 2002-2003 a "Survey of Legal and Policy Frameworks for Electronic Authentication Services and E-Signatures in OECD Member Countries". [19] The questionnaire was designed to be coherent with the survey undertaken in APEC Member economies by the APEC e-Security Task Group.

The information provided by Member countries allowed for the identification of areas where a high degree of consistency existed among Member countries, of areas where only some degree of consistency could be found and of areas showing inconsistencies (cf. Table 1). It also identified the risk that Member countries develop divergent approaches to the recognition of foreign-based authentication services which could stifle cross-border transactions.

Table 1. Findings of the Survey of Legal and Policy Frameworks for Electronic Authentication Services and E-Signatures in OECD Member Countries

High degree of consistency	Some consistency	Inconsistencies
• Legislative/regulatory framework for e-signatures • Licensing/accreditation/approval requirements for authentication services • Technology neutrality • Secure e-government • Approach to "foreign"-based signatures and services • Credential requirements	• Registration processes • Evaluation of services	• Nature of audit requirements • Recognition of foreign authentication services • Technical standards, even if some degree of consistency exists (*e.g.* for PKI)

Report on the Use of Authentication across Borders

On the basis of these findings, the WPISP agreed in October 2003 that a better understanding of the existing cross-border authentication marketplace was necessary to further help bridge national approaches and foster cross-border use of authentication. A survey of current authentication implementations and examples of use of authentication across borders as well as barriers to the use of digital signatures across borders from the supplier/user perspective was conducted in 2004-2005. The survey on "The Use of Authentication across Borders in OECD Countries" [20] also collected information on factors identified as fostering or impeding the national use of authentication technologies and digital signatures.

[19] DSTI/ICCP/REG(2003)9/FINAL

[20] DSTI/ICCP/REG(2005)4/FINAL

The exercise led to identify a number of common themes in Member countries responses (cf. Table 2) but the main finding revealed the need to increase usage rates of effective authentication across borders.

Table 2. Common themes identified in the report on "The Use of Authentication across Borders in OECD Countries"

Common positive themes	**Common negative themes**
• Maturity and robustness of public sector implementations • Maturity of financial sector implementations • Alignment of regulatory frameworks • Non-discriminatory approach to "foreign" signatures and services • Technology neutrality • PKI is alive and well • All categories of users are engaged • All applications described provide evidence of identity but with various methods of authentication	• Challenges and limitation to interoperability • Mechanisms for recognition of foreign authentication services not well developed • Acceptance of credentials as a barrier to interoperability • A range of authentication methods in use leading users to confusion • Lack of information regarding privacy enhancing features • Lack of business cases for authentication • Absence of quantitative data on usage

APPENDIX B

AUTHENTICATION ASSURANCE LEVELS

Assurance levels relating to authentication may be approached from various points of view – one of them being risk management practices and another being suitable technological solutions. Both approaches had been used by Member countries' governments in the policy documents published in recent years.[21]

The risk management approach considers the possible consequences or degree of harm of a security breach following inadequate/failed authentication process. Degrees of harm may be expressed in qualitative (*e.g.* privacy harm) and/or quantitative terms (*e.g.* loss of revenue). Some risks that could be considered include: financial, health, safety and criminal activity. Risks to both the individual and the organisation should be considered.

One could envisage three basic levels of assurance, defined along these lines:

- Low: security breach (*i.e.* misappropriation of e-identity) may lead to moderate losses of an economic or other nature (*e.g.* loss of non-confidential data); a repudiation of transaction based on this type of identification may lead to a moderate pecuniary loss.
- Medium: security breach (*i.e.* misappropriation of e-identity) may lead some losses, but not of a very serious nature; it may cause loss of confidential data; a repudiation of a transaction based on this type of identification may lead to a significant pecuniary loss.
- High: security breach (*i.e.* misappropriation of e-identity) may lead to significant losses; it may cause loss of highly confidential data; a repudiation of a transaction based on this type of identification may lead to a very significant pecuniary loss.

The above scheme provides just one example of many possible assurance level definitions.

The technology approach (suitable authentication mechanisms) considers generic requirements for authentication mechanisms, including associated security procedures. Examples of such requirements may be authentication enrolment procedures (registration procedures), capabilities and security of credentials, deployment procedures for credentials, management of identities associated with credentials, necessary accreditations with certification schemes, etc.

[21] Cf. *e.g.* UK "Registration and Authentication" published in 2002 or the Australian Government e-Authentication Framework (see list of references).

One can envisage assurance levels, defined in agreement with such generic requirements, as follows:

- Basic: single-factor authentication: *e.g.* user name and password issued as a result of a two-channels procedure (i.e. both online and by mail).
- Medium: two-factor authentication: e.g. SMS to mobile phone, token devices with challenge-response protocols, software-based PKI certificates, all issued by a two-channel registration and deployment procedure.
- High: two-factor authentication with very secure registration procedure (such as physical appearance, requirement of legally valid identity credential) and deployment by a two-channel procedure, *e.g.* PKI-certificates on a smart card or secure USB-token, or in a HSM (Hardware Security Module).

Again, the above definitions are offered as just one example of many possible assurance level schemes. Less granulated or more granulated approaches, *i.e.* fewer or several more levels, may be employed. The authentication mechanisms mentioned are provided for illustrative purposes only and should not be interpreted as an exhaustive or exclusive list.

It could be recommended to merge these two approaches into a single, unified approach, where assurance levels defined on the basis of risks posed by a security breach are associated with adequate levels of security in authentication mechanisms.

Any defined authentication level scheme needs to be closely associated with the actual application area (or several areas) it is to be used within. Application areas will constitute the necessary context for precise definitions of losses or consequences and specific selections of appropriate mechanisms for authentication.

Introduction of the concept of federation of identities[22] creates an additional challenge for definitions of assurance levels. Identity federation is a mechanism commonly used to facilitate a single-sign-on feature for users of associated information systems. Single-sign-on may also be facilitated by other mechanisms (*e.g.* common security portals). Defining an assurance level for an authentication mechanism that may be used in a federated environment and/or for single-sign-on purposes requires additional security considerations and a specific risk analysis. Such analysis needs to be targeted at security risks posed by multiple use of one credential against many systems and/or reuse of identity validation information provided by the first system a credential had been used against in other systems. Federated systems introduce a greater level of technical complexity and thus introduce new vulnerabilities in an authentication procedure, as compared to direct authentication against one system. This should also be taken into account in the risk analysis preceding the definition of a unified assurance level scheme.

[22] Cf. Liberty Alliance Project Whitepaper: Personal Identity, March 23, 2006. www.projectliberty.org/about/whitepapers/Personal_Identity.pdf.