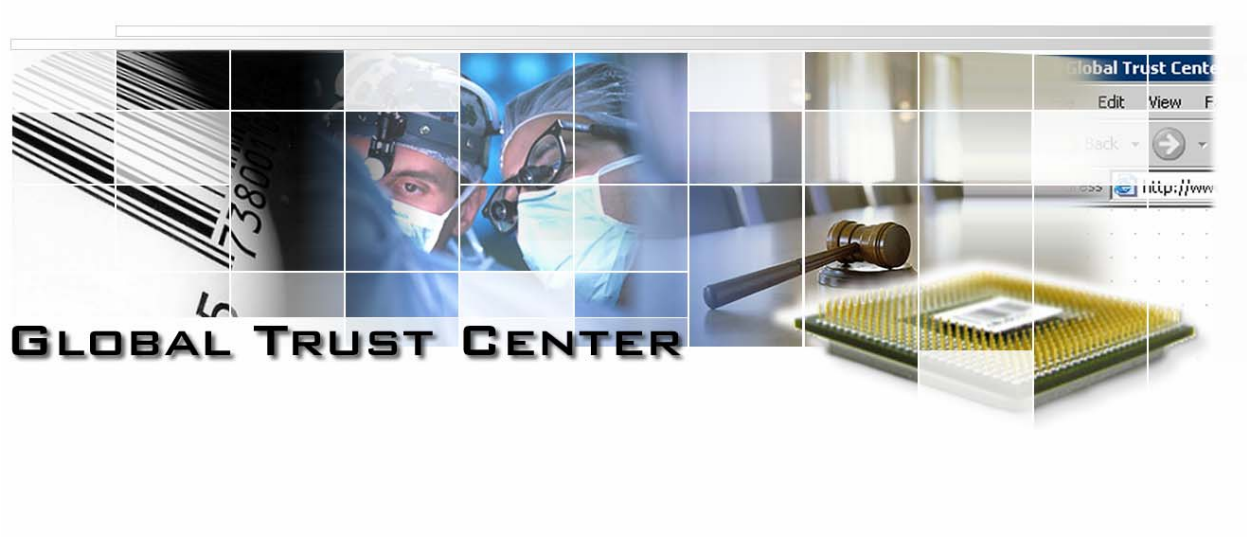
ENABLING TRUST IN THE DIGITAL WORLD

EXPLORING THE MARKET FOR AUTHENTICATION TECHNOLOGIES IN INTERNATIONAL DIGITAL TRANSACTIONS



January 2006

This draft of the final version of the report "Enabling trust in the digital world" is expected to be completed for publication during the 1st quarter of 2006. The full report can be obtained via order through the IKED secretariat (info@iked.org). This free version is an excerpt from the whole document, containing a thorough executive summary and the entire table of contents, giving the interested reader a glimpse of the extensive coverage of the full report.

IKED
INTERNATIONAL ORGANISATION FOR KNOWLEDGE ECONOMY AND ENTERPRISE DEVELOPMENT

EXECUTIVE SUMMARY

The report particularly examines what can be done to enhance trust in the digital world. Electronic transactions are currently taking place in an environment constituted by a technical superstructure and where a lack of time and space, anonymity, antagonistic activities and a sharpening competition is significant. By reflecting on ways to improve the outcomes that appear possible given the evolving trends and the present state of institutions and markets around the world, the study takes the shape of a feasibility study in regard to the option of establishing a Global Trust Center (GTC).[1]

The objectives have been to assess ways in which it will be possible to improve security and enable trust in information economies. At the present time, the issue particularly in focus is the need of strengthening the market for provision of authentication services. Based on the findings, methods are structured for how to put in place more effective cross-recognition and cross-certification of services between jurisdictions, for instance with the aid of a GTC. A fundamental observation concerns the presence of a public good component in a successful strategy for enhancing trust by enabling secure digital transactions.

The report maps and analyses national and international activities in the implementation of authentication services including their legal and regulatory frameworks, security perceptions of relying parties and individual countries, and it describes various strategies employed by countries in the implementation. Different aspects influencing transactions are gathered under the heading of a Global Authentication Framework. This framework may be viewed as a model to advance various processes, issues, institutions and actors that affect the outcome of authentication services in international digital transactions. Market and government failures, technological choice, interoperability aspects, legal systems, governments that provide identification services, etc., all play a role. This report outlines the conclusions and recommendations of those initiatives and provides:

i.) An analysis of varying authentication services which includes;

- A description of the various services in individual countries;
- An analysis of fragmentation, if any, of these services, and;
- Recommendations on possible ways of overcoming fragmentation.

ii.) An analysis of similarities and differences in the legal frameworks and recommending steps involved in moving towards common terminologies and standards where differences in legal frameworks exist;

iii.) Reflections and recommendations on the feasibility and viability of achieving orderly conditions for authentication services as a means to facilitate the use of ICT (information and communication technologies) and electronic commerce globally:

- By defining the regulatory strategies employed by countries in the implementation of authentication services;
- By describing the similarities and differences in the legal frameworks in various countries and steps involved in moving towards common terminologies and standards where differences in legal frameworks are present;
- Analysing perceptions of relying parties and countries to electronic transactions;

[1] See more Appendix A

- Detailing country requirements regarding interoperability with respect to online transactions and digital certificates;
- Description of markets and sector requirements for interoperability, and;
- Exploring how a clearing house structure can be established for the purpose of facilitating dialogue and the application of coordinated solutions on a continuous basis. As part of this study there is the description of a GTC that could facilitate this function.

Scope

The scope of this feasibility study is based on four principle perspectives:

- Organisational aspects: Business models, systems, risk management, etc., constitute this category;
- Legal aspects: Here, regulating bodies and judicial frameworks have been investigated;
- Economic aspects: This topic includes aspects that drive or hinder the development of information economies, and;
- Technological aspects: Different technologies, technological advancements and challenges are included in this group.

Based on those frames, the study includes empirical surveys inclusive of both private and public sector authentication services. Particularly four sectors have been investigated:

i) The governmental sector;
ii) The financial sector;
ii) The e-health sector, and;
iv) The university sector.

Inclusive of transactions between government, business and individual users;

Inclusive of authentication concepts, methods and techniques (making a distinction where legally valid signatures are involved, but being flexible enough to also accommodate solutions that do not use "signatures" in a narrow sense, like PIN-based solutions, for example);

Inclusive of both theoretical as well as empirical aspects of authentication processes, and;

Focused primarily on authentication (although other relevant concepts and models are taken into account).

Methodological approach

The report is based on material gathered through literary reviews as well as interviews with leading actors involved in authentication processes in digital transactions. It examines a limited number of actors and sectors, drawing notably on experience from Australia, the United States, the European Union, (and the individual member countries Austria, Belgium, Denmark, Estonia, Finland, and Sweden), and Hong Kong.

In the empirical investigation, some respondents to a survey questionnaire answered orally whereas others provided information in written form. The questionnaire was structured according to four principle perspectives (see above) and contained questions related to each of the included sectors (see above). The questionnaire is attached to this document as Appendix B.

Finding comparable data covering relevant countries and sectors represented a challenge. Overall, obtaining data on financial and most government sectors was fairly straightforward. However, corresponding information on health and institutions engaged in higher education is hard to come by. While the survey distinguished between the four sectoral aspects through its structure, respondents did not necessarily apply this distinction when answering the questionnaire. An important reason for the mixed levels of data is also due to the broad scope of the project. As a consequence, some respondents have provided feedback on a wide range of authentication methods, used both in private and public sectors on national and transnational levels. The variation in respondents' background, levels of expertise and area of focus, has affected the outcome of the data at hand, although it also increased the richness of the information obtained. Altogether, this has caused some challenges for comparisons. A compilation of the survey responses can be found in Appendix C. Furthermore, some of the material has been acquired from Internet sources.

General observations

Despite the divergent nature of the information received, a number of common themes emerged from the responses that can be useful to the GTC in validating, and further defining, its future programme. The issues associated with authentication have proven greatly relevant and important. The information received will also have utility in terms of allowing the GTC to establish priorities for the various steps ahead.

Based on the theoretical review of concepts and models related to authentication of digital transactions, it was noted that authentication needs to be given a context in order to be useable or meaningful, i.e. authentication is a context-dependant concept. This means that it is the services and products that guide the implementation or level of authentication mechanism – as opposed to the other way around.

It was observed that the implementation of authentication methods needs to be based on risk analysis, i.e. before implementing a security-enhancing technology like authentication; the need for the actual implementation must be reviewed and charted. For this purpose public organisations and standards organisations in some countries[2] have provided national guidelines on how to undertake a risk evaluation process and which techniques to choose in order to meet the required assurance level.

Most respondents agreed on the need for international coordination, which should be based on a national foundation. There is a need for an agreement on terminology throughout national or

[2] Among others; Australia and the United States have guidelines in place, whereas the EU is in the process of developing them.

international levels, technologies and protocols. Also, proper risk evaluation methods need to be developed. Some work is being done by standardisation bodies, however, it would be beneficial to influence their work and coordinate the different standards.

The overall judgment among respondents was that national and international markets are fragmented and that a lack of interoperability causes challenges. Problems with enabling system-to-system communication also decrease user trust in digital transactions. One option to overcome interoperability obstacles is by establishing a global centre for trust issues. A majority of the respondents were positive to the idea of a GTC that promotes standards and protocols for interoperability, and that gathers and organises the available market actors. The opinion was that such an organisation could enhance authentication in transnational transactions, and thereby aid in the enabling of secure digital transactions. As a conclusion, there seems to be support for a GTC, but the opinions on what actions a GTC is to undertake and vision diverge.

Positive

All countries have some cross-sectoral usage. All countries in the survey sample have at least public and financial sector implementations of authentication solutions and most have some sort of cross sectoral usage. Mainly, the financial sector utilises authentication mechanisms for, e.g. banking, tax and government services. Overall, it seems as that technical and legal infrastructures exist, but models and methods for dynamic cooperation in-between service providers appear to be missing.

The financial sector is advanced. In all sample countries, Internet banking is a prominent feature of the financial sector. The most common technologies are based on username and password with Secure Sockets Layer (SSL) technologies, often with enhanced security through hardware tokens (but sometimes software certificates are used). In a few countries, banks are utilising national ID-cards, but these implementations are minor compared to the other established technologies. In some of the countries, banks are collaborating with government bodies on applying authentication solutions.

Existing and similar legal frameworks. A legal framework for authentication services appears to be in place in each country, which provides legal support for electronic signatures. The legal framework has mainly two origins – the ones that are based on the UNCITRAL model law, and the ones that are based on the EU directive (although, Hong Kong is slightly different). EU and Hong Kong are more PKI-oriented whereas the countries based on UNCITRAL (such as Australia and the US) are more technology neutral. All country systems, except in Hong Kong, have non-discriminatory policies, which in brief can be explained as accepting all foreign solutions as long as the services fulfil the national requirements.

PKI for highest assurance. From a legal point of view, PKI is considered to have a great potential. Consequently, it is for instance recommended in cases when strong security is needed. In risk analysis methods, PKI is also popular since it is viewed as enabling risk management processes by allowing for the provision and integration of different levels of security. There exist some large scale implementations of PKI and it is widely deployed around the world. Still, it is not considered to be a great success since it is often argued that the technology has not reached a critical mass of users. Critics say that it is too costly and complex, and that it does not meet the dynamic demands of the market. Given present implementations in combination with national-ID cards and other smart cards, there is an emerging infrastructure in place for development of PKI-oriented services (see, for instance in Hong Kong, Belgium, and Estonia).

A great variety of authentication technologies. Many of the sample countries' citizens utilise some sort of authentication technology when transacting information. In many cases, that particular circumstance could be deployed in other respects as well. For instance, people often have Internet bank accounts,

but the use of digital identities can be developed in connection to other Internet activities as well, e.g. shopping (by credit cards) and income declaration (government services). Service providers are deploying a broad range of different technologies, which could also be used in other regards. However, the strength of the evidence depends on the technology chosen, so this needs to be taken into account when considering developing transaction services. Also, it was suggested among the respondents that there is no apparent need to communicate and deploy a completely new technology. To a GTC, it may therefore be a favourable route forward to act as a broker in-between the existing solutions, as there seems to be a need for bridging in-between these systems and for developing new services. The GTC could also provide a managerial tool that e.g. organises the available technologies according to assurance levels.

The future of authentication services. Both empirical and theoretical findings suggest a positive development of the deployment of authentication services for international transactions. With the enhancement of e-commerce related offerings, the need for secure communications is further accentuated. However, it was implied by the respondents that the market so far has not been characterised by demand-driven offerings, but rather by a supply-driven outline. In the long run, this is not a beneficial situation. Instead of taking the risk of over-heating the market with more services and products, one idea is to invest more efforts in exploring and specifying the demand for authentication mechanisms in markets and sectors. Based on is the presence of an actual demand for security in information transactions, the future of authentication services appears to be bright.

Negative

Fragmentation. The sample countries display differences in the governance of transaction services. For instance, a lack of interdisciplinary interoperability in-between existing systems exists, and the alliances that have taken shape to address the outstanding problems have not yet been successful. From a legal perspective, differences with regard as how to assign liability and compensation are present. From a technical view, numerous standards compete and not one de facto standard have been established. Also, there seem to be discrepancies in terminology, so called semantic fragmentation. From an organisational and economic perspective, the absence of cost/benefit models, risk analysis tools and managerial methods for implementing authentication services were claimed to be obstacles for reaching the potential of digital transactions. Also, tools to overcome fragmentation seem to be much needed – a brokerage house can be one way and/or some form of interoperability protocol, stipulating how standards and techniques should interact.

National Focus. In most countries, the efforts are focused on setting up services that function nationally, as many challenges on this arena still need to be addressed. Despite a number of initiatives and pilots that enable international transactions, no real impact has been achieved. The Internet market is inherently global and citizens and customers are acting on an international basis where they are affected by transnational impulses, which imply a need for an international and inter-organisational structure of digital transactions.

A range of authentication methods in use. The great number of implementations available today may confuse users and service providers as to which technology or method that is fit for their purpose (i.e. which is effective, secure and business-wise sound). Also, risks of technological lock-in of certain technologies that may further enhance market fragmentation exists. One example is that the bank sector in some of the sample countries hesitate to use national PKI solutions due to investments made into other (older and more obsolete) technologies that are already deployed. This supports the idea of a reference tool for risk management in which it is possible to assess the various authentication techniques and the degree to which their attributes address requirements identified by application providers and/or users. Obviously, this is an opportunity for the GTC.

Supply-driven markets. The usage of authentication technologies is growing, but the number of services and technologies provided seem to be higher than the actual demand for them (as was implied by the respondents). Also, many technology and service providers, aided by forward-looking government officials, promote various solutions that may not be demanded by the market. Respondents also indicated that the business case for improving security in digital transactions may be weak in many instances. On the other hand, this may be likely to change in the near future as the awareness of the need for more secure digital transactions of businesses, government authorities and private users is constantly increasing. In addition, private and public sectors seem to be evolving and changing towards enabling more and more Internet-based services. The effect of this change is still hampered by the fact that actors have not found their roles in this new environment.

Political challenges with international organisations. The respondents raised concerns related to the implementation of such an endeavour. The challenge depends on which approach chosen by a GTC and the scope of the project. However a global institution will require heavy funding, time, knowledge, resources and commitment. It was implied that the prospects of such an affair are highly uncertain, furthermore so due to practical challenges with respect to organisational structure, location, funding, political influence, culture and responsibilities. A network-based scenario containing national nodes (both private and public parties) was viewed as a favourable approach according to the respondents, as it could overcome some of the challenges previously listed. Another concern was that in case an organisation reached sufficient coverage, interoperability and technical standards might be enhanced, however, the competition in this area is strong, as such large-scale organisations already exist (e.g. IETF, W3C, OASIS). Some respondents also doubted whether transnational recognition of authentication methods can be improved by such a brokerage organisation, as relevant organisations are well established (e.g. OECD). On the other hand, the problems of assuring secure digital transactions remain, and even though competition in this area might be fierce, the setting up of a GTC contains an inherent public good component. Enabling secure digital transactions will have a (positive) impact on the enhancement of trust in services deployed over global information networks.

Reflections

The information collected in this project is useful in terms of identifying common themes that suggest future areas of work, which could be considered by the GTC. In reflection, these areas relate to:

The analysis suggests that a strong need for coordination of the market of authentication services. The key role of the GTC ought to be a clearing house of various, proprietary authentication systems enabling people with appropriate instruments for authorisation (tokens, smart cards, digital certificates) to achieve interoperable digital transactions in-between users (persons, organisations, government institutions, etc.) devoid of expensive investments in diverse proprietary systems. Other potential roles ought to evolve from the knowledge generated in this area. Furthermore, it is likely that even if the GTC will not take on this responsibility, some other actor or coalition of actors will.

While a number of relevant standards already exist in the marketplace which can be used to support the security and authenticity of electronic transactions, currently no overarching interoperability protocol is present. Such a high-level protocol for interoperability, which could be the key to a positive future development of the market, may be facilitated by the GTC. If the GTC is to be seriously engaged in developing such a protocol this may have important implications for the structure and nature of the organisation. The associated requirements should then preferably be explored in early phases, or in an early pilot.

There seems to be ambiguity in the decision-making process concerning security-enhancing mechanisms in solutions, systems and software. Security managers would benefit from a generic method to explore the actual demands of a system or technique in order to minimise cost and maximise utility so that a high level of cost-efficiency can be assured throughout their organisations. Risk analysis presents such an opportunity to decision-makers. Risk analysis is one of the key processes in defining an appropriate security (and authentication) structure of an enterprise or a government organisation. However, risk analysis in itself is not sufficient to decide which security-enhancing system to choose, it is merely a tool for establishing the state of affairs. On this theme, one possibility is for the GTC to provide recommendations or guidelines on how to select a risk analysis tool, what criteria should be applied and how it may be utilised. Since this process often is the most time-consuming part of conducting a risk analysis, corporations have a rationale to save both time and money. Another time-consuming and equally important task in conducting (quantitative) risk analyses is finding usable statistics to base probabilistic prognoses on. Altogether, this might be an opportunity to explore for the GTC.

From a demand-driven bottom-up perspective, the GTC could engage and involve actors that provide authentication mechanisms which promote interoperability among systems and operators. The GTC could develop methods (e.g. guidelines, best practices, protocol, and templates for developing agreements) to facilitate interoperability, including through acceptance of "foreign" solutions. Such an organisation could thus help to coordinate and facilitate inter-sectoral and inter-governmental contacts and contracts.

Other areas where linkages could potentially be explored include assessing the extent to which authentication can play a dominant role in combating identity theft, the extent to which the use of certain methods of authentication can alter the economic incentives for individuals to steal authentication credentials (e.g. through phishing schemes) and the promotion of authentication as an essential element of the Internet's culture of security.[3]

It has been suggested in literature and in the survey that the GTC should take advantage of existing national systems and standards, as opposed to develop entirely new (technical and/or organisational) solutions. Obviously, the coordinating system needs to be interoperable with other existing systems. However, by designing a new system that is built on top of existing ones, a minimum level of new investments and disturbances can be maintained.

Various observations indicate that today's market for secure digital transactions is fuelled by other forces than demand considerations. For instance, respondents emphasised that the market so far has been characterised by a supply-driven focus which does not represent a sustainable market situation. This situation may hamper market developments, with over investments, costly R&D due to problems in identifying which is the future standard technology and hence reducing possibilities for SMEs to compete, technological lock-in and over heating of services and offerings destroying price signals. One possible avenue forward for the GTC is therefore to locate and arrange the future demand for authentication mechanisms. This imperative observation concerns the presence of a strong demand among multiple actors for the promotion of multi-layered security solutions and risk-driven security-enhancing systems.

Enabling trust is a complex task, the success of which will require time, patience and coordination. All in all, the points made underpin the potential merits of a global brokerage organisation that can

[3] Phishing is a process through which a perpetrator by deceptive means tries to acquire sensitive personal information, such as passwords, user names, credit card numbers, etc. The malevolent actor tries to acquire this information by masquerading as someone trustworthy with a real need for such information and send the requests in an official-looking message.

convey contacts and counselling among the available market actors so as to enhance secure authentication in transnational transactions. This may provide a rationale for establishing a GTC, given that such a body will be in the position to make a significant contribution and improve the situation.

A feasible avenue forward

The overarching objective of the feasibility study is to examine roads ahead that could enhance secure digital transactions by improving the global authentication mechanisms. The proposed idea was a GTC that addresses various challenges for the existing authentication solutions. The analysis has departed from four categories (see below) of challenges and opportunities. For each of these, a number of potential measures to improve the functioning of markets have been found:

i) Legal aspects

- The GTC could improve world markets by providing analysis and recommendations to regulators, existing service and technology providers as well as to potential new endeavours.

ii) Technological aspects

- The GTC could either through partners, joint ventures or by itself develop and improve standards, protocols and technical solutions that aid in improving the functioning of the market. One such solution could be to develop a risk-driven protocol for interoperation in-between authentication systems.
- Analysis and advice on technological solutions can be provided. The GTC can function as a centre of excellence providing trustworthy and independent information on techniques, best practises, standards and solutions.

iii) Economic aspects

- The GTC could help facilitate coordination of supply and demand in order to address market inconsistency that is currently hindering the development of new and improved services and user pick-up of digital solutions. The GTC could also help to facilitate the emergence of a web of trust or a federated identity management structure.
- The GTC could provide analysis of economic consequences on national and international markets and provide rationales for action from key stakeholders. From this knowledge, the GTC can act as global spokesperson on issues related to authentication.

iv) Organisational aspects

- The GTC could help markets by providing and coordinating risk management tools.
- The GTC could provide policy recommendations for private and public entities, both behavioural policies for organisations as well as recommendations for legislations.
- Another important function would be to organise actors and solutions in order to facilitate coordination.
- The GTC could provide information and recommendations on available and successful business models, technologies and standards.

Conclusion

The tentative conclusions of the feasibility study indicate the presence of a gap between the needs for putting in place mechanisms and institutions in support of digital trust, on the one hand, and current and anticipated future driving forces, from the policy and market side alike, for generating such solutions. It is further argued that the notion of putting in place a global trust centre to fill this gap is basically sound.

It appears that the demand for mechanisms supporting trust in digital transactions is dissipated, meets with fragmented market conditions, and is unable to articulate coherent incentives for putting effective solutions in place. Today, the authentication solutions available are primarily supply-driven and there appears to be an over-supply of (foremost technical) solutions around. This may result in technological lock-in, where heavy investments have been made in obsolete technologies, which risks worsening the fragmentation of markets and raise costs to society. At the same time, Internet users are reported to abstain from taking up technology or undertaking actions online due to fear of negative consequences.

Among the responses that do exist, a few international initiatives can be noted. The efforts include networks such as the Liberty Alliance, intergovernmental organisations such as the ITU, IDABC, APEC Tel Group, partnerships between market leaders such as Verisign/Microsoft/RSA/IBM, etc. Still, all of these encounter problems. The reasons apparently include limitations as regards resources, capacity to adjust to changing conditions, ability to meet with market demand, political pressures, competition, etc.

The report concludes that there is a case for the existence of a public good's component in the market for transnational digital transactions. In order to succeed, such an organisation need to take on a role, and adopt an organisation, which enables it to overcome the just-mentioned kinds of problems The study concludes that the notion of GTC, which focuses on enhancing security for transnational electronic transactions and introducing means to develop interoperability, could make a major beneficial contribution. In principle, various alternative models for such a body are conceivable. Different forms display their specific pros and cons pertaining to each alternative. Four alternative paths for the GTC are outlined in the study:

i) Supra- or intergovernmental solution;

ii) Public private partnership (PPP);

iii) Corporation, and;

iv) Loose network.

i) Supra- or intergovernmental solution

This option consists of two paths, whereof analysis suggests that one is more cumbersome than the other to implement. This is a supranational organisation, i.e. an organisation like the WTO, where governments trade certain powers to a higher organisation. In this case, numerous great privacy and political obstacles undermine such an organisation. The intergovernmental approach is slightly different and would incorporate governments to build a web of trust cross-certifying their authentication frameworks. It has the potential to be feasible and it is likely to occur within the EU and, at present, it is an ongoing initiative in the US. It is however more uncertain on an international level, as it incorporates some of the same challenges as applies to a supranational organisation. A more publically oriented organisation would require public resources and political buy-in to proceed, which presumably would be feasible and grant it certain powers. At the same time, such a solution

may be shunned by market actors. Also, by appropriating service provision that market actors should be able to provide, there is a risk that such a body would become too supply-driven. The implications of this option are summarised below:

Supra- or intergovernmental solution	
Pros	*Cons*
Potentially powerful and resourceful Well placed to establish a protocol Clout to back security in digital transactions Favourable position to achieve critical mass Good position to establish a web of trust/federated identity management of at least public organisations High ability to address public goods issues	Too much top-down Supply-driven Lack of flexibility Slow Susceptibility to political problems, e.g. where to locate, who will take final call, turf-battles for influence Expensive Return on investment uncertain

ii) Public private partnership (PPP)

A PPP would aim to gather key stakeholders from across different sectors and representing both public and private entities. It may be relatively easy to establish confidence in this kind of operation, applying both to the market actors and the public sector side. Such a GTC may be in a favourable position to develop matching regulations and technical solutions that meet interoperability requirements. Success in this effort clearly requires public as well as private buy-in. Launching the process would most likely require significant public funding. In order for a PPP to avoid some of the political challenges related to location and influence, however, it may preferably be organised as a network with decentralised national nodes, which could help diffuse costs on a number of participating actors.

Public private partnership (PPP)	
Pros	*Cons*
Demand-oriented Impact on critical mass Cross-sectoral bridging Integrity-preserving Coordination function Can develop protocol Can establish a web of trust/ federated identity management Potential buy-in from key stakeholders Can address public good factor	Limited political powers Uncertain value proposition Competition Lack of ownership and commitment

iii) Corporation

A third option would be to start a private company based on key stakeholders buy-in to the organisation, potentially jointly providing technology through the organisation. It would be more flexible and more market-oriented than the other two alternatives. Launching an endeavour like this would require some sort of venture or seed capital, which could be provided by the actors buying into it. Presumably, it would not get buy-in from governments. There may also be a risk that such a GTC would be viewed as yet another competitor or consultancy firm, and not be perceived as a coordinator of digital transactions.

Corporation	
Pros	*Cons*
Potentially high return on investment Flexible Independence Demand-oriented Business-driven	Less trust from market actors High risk No public buy-in Public good – hard to handle public good Fierce competition from technology and service providers as well as consultancy firms

iv) Loose network

A loose network aims to form a light structure which still exercises sufficient connections to keep the organisation functional around the key actors, presumably represented in the steering committee. Such a body could be relatively flexible, able to focus and responsive as particularly important opportunities arise. The network would observe market developments and gather more knowledge from initiated pilots.

Loose network	
Pros	*Cons*
Low risk Flexibility Independence Small resource requirements	No resources – few results Loss of interest of actors Weak coordination No true ownership

Recommendations

As a point of departure, a feasible action plan for the near future includes the following steps:

1. Decide on strategy	**2. Establish network**	**3. Test phase**	**4. Full launch**
Steering committee meeting	Hold conference	Initiate Pilots	Provide full scale web of trust service or back-up for federated identity management.
Decide organisational form	Create association	Provide knowledge	
Secure financing	Start development of protocol	Develop marketing strategy and tools	
	Develop risk-management tools	Engage key stakeholders	

The key criteria on which to base recommendations are viewed as *relevance of the purpose of the organisation*, *feasibility* and *funding*. The relevance of the organisation is reflected in the value added it can generate through its activities and, in particular, how well it can deliver the public good of interoperability and the ability to facilitate connections between existing actors and solutions. The relevance will furthermore depend on the potential ability of the organisation to generate buy-in from key stake holders and henceforth become a trustworthy actor.

As for the organisational form, this report concludes that a supra- or intergovernmental solution (i) is the best alternative to deal with the legal, economic and organisational aspects on a global level. Crucial to the process is that the GTC achieves appropriate support and sufficient decision-making powers. Naturally, there will be challenges, given the state of the e-political arena, the market, and the speed of the ongoing technological development, however it is of uttermost importance to retain focus on the global tasks the GTC is envisioned to undertake.

Forming an effective public-private partnership (ii) for the technological aspects involved would be less problematic, for a quick start-up, and this kind of structure should have greater chances of incorporating key market actors and other relevant stakeholders. This alternative may, due to this fact, actually be the best positioned to deliver the public good of interoperability, and have the greatest ability to be constantly up-to-date with the latest innovative technical solutions. Evidently, such a strategy requires funding for initiation – both from private and public sectors.

The third option (iii), i.e. a corporate organisational form, may be somewhat faster and "easier" to establish. While running a risk of being too "thin" when it comes to exercising influence, not fully transparent and trustworthy in its objectives, void of value and not being able to properly deliver the public good, there might be some possibility of basing it on incentives to deepen commitments as opportunities develop. The viability of this option must be thought through carefully, however, due to its likely intrinsic difficulties to fulfil the "trust" factor that is a prerequisite for success of the core function of the GTC is set out to carry out.

If options (i) and (ii) are preferred, but present interests lack the initial clout to muster the resources necessary for carrying them out, an option may be for the project, first, to get launched as a network which, from thereon, is gradually enhanced into an association of key stakeholders based on the build-up of several country nodes coordinated under a central function. The respective national actors could bring together their respective interests and experiences while carving out a suitable path towards overall coordination in line with the jointly preferred strategy of the GTC to be followed by a full rollout of the GTC once critical mass of support, commitment and funding is achieved. The board and the associate body would have to have a sufficiently broad geographical and sectoral representation, while avoiding the development of too diverse interests within the network. The intended members should be invited to working group seminars and conferences in order to advance a common approach to the GTC concept and ensure collaboration in making it concrete.

The development of a protocol of risk management tools and the experience of initiated pilot projects represent important building blocks for further advance. Pilots should be advanced not primarily to derive final solutions or strengthen the financial basis of GTC, but rather to accumulate practical experience and to demonstrate the mission and strive of the organisation. Nevertheless, launching such efforts requires a certain, sufficient funding, however, including institutions which would volunteer to support and host certain functions. An appropriate division of labour between the participating parties would have to be worked out. The members will provide the various kinds of experience that is required for the GTC, as well as to help generate the perceived trust which will be a key to GTC success.

In going forward with work that involves promoting an increase in the use of authentication mechanisms, the GTC will need to remain mindful of the fact that there will be a corresponding global increase in the need for users to have ways to manage their digital identities. If the GTC is established and organised so as to address this need, elements of the work would presumably include an assessment of the degree to which federated identity solutions can meet with marketplace demands in this regard, as well as assessments of potential policy issues that these solutions would require. Further, various exchanges, seminars and conferences on the theme of authentication and digital transactions may be needed to boost not only interest in Internet security matters, and an enhanced awareness of Internet related risks and threats, but also to help advance the community of interested parties towards sufficiently common perceptions and perspectives, i.e. establishing more shared concepts. Although numerous such meeting places already exist, there is a need to widen the circle of those engaged, and to bridge the interaction between public sector, industry and academia on this matter. There is also the need to involve consumer groups as the demand side is often been

left out in this context. Some observed arguments in support for this vision of cross-sectoral exchanges on authentication is provided below:

- Trust-enabling methods such as authentication are an agreed topic of importance to Internet's culture of security.
- A limited number of conferences devoted to cross-sectoral interested parties exist.[4]
- Boosting trust by technology as a process (and not a product), which suffices for the need for a meeting place like the suggested conference.
- By having cross-sectoral representation on the conference, there is the possibility of enhancing a market driven by demand.

This report recommends that the GTC is initiated and organised as a combined option of (i) a supra- or intranational organisation covering the legal, economic and organisational aspects on a global level and (ii) a closely connected public-private partnership setup covering the technological aspects. The setup should include a structure for incorporating practically useful pilots organised and tailored to meet the needs of specific sectors or regions. A development in this direction has already been initiated by the Australian group within the steering committee, which has taken the lead in the development of a financial pilot. Currently, demands for new solutions to digital trust are accentuated within the governmental and the financial sectors. Coordination within these domains may be greatly beneficial for enabling a strengthening of joint authentication protocols. Experiences learned from this pilot can serve as inspiration for the development of a future protocol and may show the way towards putting in place other pilots in the future. The provision of good examples and a track-record in promoting efforts which can help create trust will be greatly important for underpinning the formation of an effective GTC.

Important initiatives will have to be taken to examine and advance solutions that can enhance interoperability and support the implementation of cross-cutting solutions. Various initiatives may be needed to advance and explore approaches and methods that can support effective third-party engagement in authentication schemes. Work on the development of an expanded protocol would have to be matched with additional work on risk management tools in order to, concurrently, start planning for marketing strategies and engage private and public actors in tandem.

[4] One example may be the World eID conference, see http://www.strategiestm.com/conferences/we-id/05/

ABSTRACT

Information and communications technologies are offering organisations all over the world unprecedented opportunities to process information and to perform commercial transactions at any location. The market for international electronic transactions has a huge potential, but beneficial results are not a given. Efficient privacy- and security-enhancing techniques that address the specific requirements of users, organisations and governments are still missing. Without the assurance of security and privacy in digital transactions, enabling widespread trust among users, organisations and governments appears challenging.

Addressing these complex issues, this report particularly examines what can be done to enhance trust in the digital world by putting in place better mechanisms to support effective authentication. Electronic transactions are currently taking place in an environment constituted by a technical superstructure and signified by a lack of time and space, anonymity, antagonistic activities and a sharpening competition. Reflecting on ways to improve the outcomes that appear possible given the evolving trends and the present state of institutions and markets around the world, the study also takes the shape of a feasibility study in regard to the option of establishing a "*Global Trust Center*".

The report is based on material gathered through literary reviews and interviews with leading actors involved in authentication processes in digital transactions. It reviews a limited number of actors and sectors, drawing notably on experience from Australia, the United States, the European Union, (and the individual member countries Sweden, Denmark, Finland, Estonia, Belgium, and Austria), and Hong Kong. Various aspects influencing transactions are gathered under the heading of a *Global Authentication Framework*. This kind of framework may be viewed as a model to advance various processes, issues, institutions and actors that affect the outcome of authentication services in international digital transactions. Market and government failures, technological choice, interoperability aspects, legal systems, governments that provide identification services, etc., all play a role.

The main findings of the report include, e.g., that markets are highly fragmented, serious differences in the governance of transaction services amongst countries exist, a lack of interdisciplinary interoperability in-between existing systems is present, and the alliances that have been formed to address the outstanding challenges have not yet had success. In addition, enabling trust is a complex task, the success of which will require time, patience and coordination. Another imperative observation concerns the presence of a strong demand among multiple actors for the promotion of multi-layered security solutions and risk-driven security-enhancing systems.

All in all, these points underpin the need of a global brokerage organisation that is able to convey contacts and counselling among the available market actors and to work on developing interoperability solutions so as to enhance security and efficiency of authentication in transnational transactions. In practice, this could motivate the establishment of a GTC able to make a significant contribution in this respect.

This report recommends that the GTC is initiated and organised as a combined option of (i) a supra- or intranational organisation covering the legal, economic and organisational aspects on a global level and (ii) a closely connected public-private partnership setup covering the technological aspects. The setup should include a structure for incorporating practically useful pilots organised and tailored to meet the needs of specific sectors or regions.

FOREWORD

Information and communications technologies (ICT) are offering organisations all over the world unprecedented opportunities to process information and to perform commercial transactions at any location. The market for international electronic transactions has a great potential, but beneficial results are not a given. Efficient privacy- and security-enhancing techniques that address the specific requirements of users, organisations and governments are still missing. As it seems, without the assurance of security and privacy in digital transactions, enabling widespread trust among users, organisations and governments is impossible.

Addressing these complex issues, this report particularly examines what can be done to enhance trust in the digital world by putting in place better mechanisms to support effective authentication. Electronic transactions are currently taking place in an environment made up by a technical superstructure and signified by a lack of time and space, anonymity, antagonistic activities and a sharpening competition. Reflecting on ways to improve the outcomes that appear possible given the evolving trends and the present state of institutions and markets around the world, the study also takes the shape of a feasibility study in regard to the option of establishing a "*Global Trust Center*".
Jens Sörvik, Andreas Jacobsson and Andreas Mossberg of IKED are thanked for the prime substantive work on the report. Professor Jean-Pierre Briffaut, Institut National des Télécommunications, Paris, Ms. Anna Öhrwall Rönnbäck, Linköping University, and Professor Christina E. Hultmark, Gothenburg University, provided important background reports. Mr. Boyan Kostadinov, graphic design, and Ms. Karin Helene, both IKED, are also thanked for invaluable assistance. The effort has been undertaken under the aegis of an international steering group featuring representatives from different sectors and parts of the world, especially in Europe and in Australia.

December, 2005

Thomas Andersson

TABLE OF CONTENTS

APPENDIX B: EMPIRICAL SURVEY IN THE PROJECT "ENABLING TRUST IN THE DIGITAL WORLD"

QUESTIONS:

APPENDIX C: COMPILATION OF SURVEY RESPONSES IN THE PROJECT "ENABLING TRUST IN THE DIGITAL WORLD"