Authentication: International scope and non discrimination in government commerce vs. PKI

DR PAUL R SCHAPPER, DR MERCEDES RIVOLTA AND MR KNUT LEIPOLD

Introduction

In the 1990s as the internet phenomenon generated new ways of undertaking transactions that replace the traditional paper format, countries began to adapt their legal frameworks to give legal status to electronic signatures, digital records and in some cases, digital signatures and 'authentication' technologies.

Digital certificates became an important part of the methodologies used to secure communications on the web, to assure secure internet sessions, to protect confidential documents, and to replace handwritten signatures in many activities that need strong authentication. In many other situations involving electronic transactions, technical advances have developed a range of solutions that do not use digital signatures but which also can be suitable for strong authentication.

These technological developments also provided new ways of undertaking government commerce or procurement, and more and more governments are taking advantage of this potential. With public procurement accounting for up to twenty percent or more of Gross Domestic Product, government policy in this area represents an opportunity to establish new standards of governance not only within government but also more broadly within the economy. This can be especially valuable for developing countries where this technology has the capacity to significantly strengthen the transparency, value-for-money and efficiency of public processes. It is this opportunity that makes e-commerce applications in the public sector, or electronic government procurement (e-GP), hold special interest to multilateral development banks (MDBs) and other international agencies such as the United Nations Commission on International Trade Law (UNCITRAL). The application of this technology to government procurement is now being promoted by the MDBs in terms of a framework of core principles that target these benefits.

This paper discusses the MDB guidelines towards authentication and digital signatures within the context of e-GP and the core principles, and some of the tensions and outstanding issues around these. The MDBs have already initiated discussion on some of the issues around authentication and have created a joint website to facilitate debate.[1]

Electronic Government Procurement

Electronic government procurement is defined as the use of information technology systems, means and networks by governments in order to obtain works, goods, services and consulting services required for the public sector, and to manage their procurement relationship with suppliers and contractors.

To appreciate the issues around authentication in e-GP (or any other form of commerce), it is essential to understand the underlying business framework to which it is being applied. The on-line applications that are being adopted by governments in relation to electronic public procurement are broadly in three parts:

- Electronic tendering (or bidding)
- Electronic purchasing including electronic reverse auctions, and
- Electronic contract management.

These are different technical systems that can stand alone or be combined along some common ground such as performance management and reporting. Most successful government developments are in relation to e-tendering, which

[1] See "Authentication & Digital Signatures in E-Law and Security: A Guide for Legislators and Managers" available in electronic format at http://www.mdb-egp.org, 2004.

Within the public sector however, authentication does not derive from relationship management but from process management or administrative law, or alternatively from legislatively consistent PKI

is often considered to be the easiest part to implement, as it does not require substantial re-engineering of government and business back-office systems. This function commonly advertises government policies, procurement regulations and tendering opportunities and allows businesses to download tender documents and upload bids into an on-line tender box. This function typically does not handle large financial transactions that might be associated with the tenders being advertised and submitted. There can be relatively minor financial transactions where countries charge for document downloads, bid submissions or other levels of participation, for example to cover the costs of the e-GP system. Yet it is with this function, for which identity risk might seem small, that some countries seek to impose strong authentication methodologies.

■ Authentication and Public Administration

There are three broad solution areas for on-line authentication in e-GP (and e-commerce generally). First there have been technological developments, which, of course, gave rise to PKI models based on digital signatures and certificates. Further technological developments have been making other options available such as bionics. Second there is the legislative path where most countries have now implemented laws to give legal status to electronic or digital documents and electronic authentication. Until recently it seemed that lawyers and technologists were evolving some sort of consensus (but by no means unanimous) about on-line authentication. The first of these laws were often not technologically neutral and specified a PKI solution. The weaknesses of this bias has gradually become evident and new laws are now shifting towards technological neutrality.

Finally there is the administrative response to on-line authentication. Here there can often be found a strong polarization between the public and private sectors. Within the private sector, business practice has, to a large degree, ignored developments both in the legislation and in the technology in relation to authentication, and more often relied on traditional processes and risk management. This has been a reflection of the way business actually works, drawing on established alliances and networks. Authentication in B2B commerce usually derives from relationship management, and is unlikely to be dictated by technology or the law.

Within the public sector however, authentication does not derive from relationship management but from process management or administrative law, or alternatively from legislatively consistent PKI. Thus some governments appear to be approaching e-GP authentication via the legal path and specifying PKI processes, while others have adopted a management or administrative path that has no such requirements but instead relies on traditional practice. Examples of this divergence of approach can readily be found, with e-GP in India and Latin America using digital signatures and PKI, while in parts of the USA, Australia and the UK using electronic signatures or simply administrative processes. The MDB e-GP Harmonization Group has developed an Interactive Database in order to provide member countries information on e-GP practices adopted by governments worldwide.[2]

Countries have confronted authentication issues in relation to bid submissions from business. However, as already noted, the e-bidding systems often charge nothing at all and handle no financial transfers. Also, while these systems advertise opportunities and receive bids, they typically do not formalize any contracts on-line. The contract formalization is usually off-line sometimes pending negotiations, due diligence or other procedures. The need for on-line authentication by bidders requires explanation. Under what circumstances would a bidder submit a bid then deny that they did so? And further, do these circumstances actually happen and with what frequency? What are the risks to government?

It is sometimes noted that the risks are indeed high. For example, governments are increasingly accepting tenders from business through the internet, and while at the tender stage there has been no financial transfer, the intellectual property within a high value technology tender or even a construction contract can easily be valued at millions of dollars. Either the business does not compete or it accepts the use of government specified PKI/SSL lodgement technology only some of which might be regarded as having best practice security. But these are issues of security rather than identity.

Some governments claim that they want legal commitment from bidders to address these questions and to hold to their bids, and that a digital signature provides this. However other governments have adopted administrative approaches to these risks, recognising that there

[2] See http://www.mdb-egp.org/data/default.asp, E-GP Interactive Map.

are likely to be administrative or regulatory responses to the threat that bidders will withdraw a bid after tenders have closed. Also, businesses are not anxious to upset government buyers, and a regulation that late bid withdrawal will disqualify a bidder from future bidding, as is the case in some jurisdictions, represents one simple administrative alternative to the attachment of a digital signature. In relation to the potential for the transmission of unauthorized bids, some governments, by requiring a digital signature, are requiring bidders to provide strong evidence that they authorized the bid, while other governments using administrative approaches require bidders to provide strong evidence that they did not authorize a bid should the issue arise. This polarization of government methodology implicitly reflects differences in the management of underlying business risks that have not always been fully analysed.

The MDBs and E-GP

The Asian Development Bank, the Inter-American Development Bank and the World Bank have been harmonizing their approaches to promoting these technological applications in the public sector of developing countries specifically to strengthen governance in this component of government appropriation.

Clearly this technology can strengthen poor governance just as easily as it can enhance good governance, and therefore the guidelines and rules these MDBs have established for developing countries become important. The harmonised approach developed between these Banks has been in recognition of the importance of providing consistent advice and guidance to developing countries in relation to these technological applications.

The MDBs have a significant catalytic role in developing countries in this major area of expenditure through their capacity to attach conditions to the loans, grants and credits that they provide to these countries. The MDBs have an additional legitimate leadership role to play in setting standards and design parameters in relation to e-GP for their borrower countries. The MDBs have responsibilities to their donor countries, other borrower countries and their own governance frameworks to ensure that the processes used by borrowing countries to disperse MDB loans and liabilities meet acceptable public governance standards. This is not new – the MDBs have long imposed basic standards for the management processes of these funds within the traditional paper-based system.

The MDBs have encouraged individual governments to adopt or develop and implement e-GP as a means of promoting good governance, efficiency and technological capacity of their economies and have provided resources to facilitate such processes. No one system has been promoted by the MDBs, but instead they have encouraged governments to find their own path that most closely matches their individual circumstances, recognizing that there is no single "right" solution. It is within these various home grown paths and solutions that the MDBs have defined core principles that need to be incorporated if the systems are to be applied to MDB-sourced funds.

■ E-GP Core Principles

As with traditional paper based procurement, the MDB standards for e-GP rely on a battery of core principles that must be observed. These principles are:

- Transparency
- Non discrimination
- Equality of access
- Open competition
- Accountability
- Security of process

The effective implementation of these core principles implies that such technical requirements must be applied to the electronic procurement systems. These principles must be present in the following procurement systems requirements:

- Bid advertising
- Technological neutrality
- Technical standards for interoperability and security
- Some processes such as ensuring security and good audit trails
- Cost and easy participation

Where executing agencies use e-GP systems operated by a third party under a service contract arrangement, then that third party system must also comply with these requirements. Of particular interest is the approach used by the MDBs around the issue of authentication and how this potentially conflicts with or fits within the core

framework principles.

■ Authentication and E-GP

Like others that have gone before them, the MDBs have encountered problems around the concept of on-line authentication within the context of government procurement that reflect contractual and risk requirements. In fact, although PKI technology has been available for many years and it has legal recognition in most countries, there has not been an intensive use of digital signatures by much of business.

The problems of on-line authentication have of course been extensively documented and will not be revisited here except by way of a summary of a survey conducted by the PKI Forum ("PKI Action Plan", OASIS Public Key Infrastructure Technical Committee, 2004).

That survey attracted a large number of respondents, who identified certain specific issues. The top five obstacles to PKI deployment and usage identified by the survey were:

- Software applications do not support it
- Costs are too high
- PKI is poorly understood
- Too much focus on technology, not enough on need
- Poor interoperability

For public procurement it is important to facilitate participation by as many actual and potential suppliers as possible to encourage real competition, value-for-money and transparency. This means that not only should it be possible for all potential bidders to participate, it should also be procedurally simple and inexpensive. The principle of open access with minimal barriers is a core principle to enhance transparency and reduce malpractice and back door trade restrictions. For this requirement, a certified digital signature can become a barrier for participation at two levels. First for smaller local and regionally based domestic suppliers the processes and costs required to participate in PKI may become a barrier.

At the other extreme, the lack of standards and interoperability can discourage participation by international bidders. Up to now, there are no international agreements about the recognition of digital certificates issued for certification authorities located in different countries reflecting the lack of standards (or too many standards) and interoperability. This is a serious problem because the requirement of personal identification needed for personal certificates. This means that a person needs to go to a registration authority to validate their identification data. This validation requires personal presence. What happens if the person lives in another country? As there are no international agreements between countries and there are no international rules about the international validity of digital certificates, this potentially represents a serious obstacle to the open and ready participation of bidders and thereby conflicts with procurement core principles maintained by the MDBs.

■ MDB E-Tendering Guidelines for Digital Signatures

Facing the obstacles that the use of PKI may represent for the open access and competition, the MDBs have approved processes that establish e-bidding requirements for MDB loans, grants and credits, which are mandatory for electronic government procurement implementation.

It is notable that the MDBs do not require that there be any on-line authentication at all and, as already discussed, some governments indeed do not require on-line authentication for e-GP, except in terms of ordinary administrative processes as is the case for the great bulk of B2B e-commerce today. Where a government insists on digitally certified digital signatures such as PKI, the MDBs have mandated the following requirements to protect the core procurement principles:

- The certification process shall certify bidders for a reasonable period of time (at least one year) and bidders shall not be required to request a certification for each bidding process.
- The certification process shall be kept open permanently, allowing bidders to submit the request for certification at any time in order to allow them to register in advance for future bidding processes.
- The certification process shall allow bidders to take all actions required for their certification within their own countries, without the need to travel abroad.
- The certification process shall accept an electronic signature or a digital certification and signature issued by certifying authorities within the country of the bidder, or the process shall accept submission of on-line or off-line documentation for certifying the authenticity of the bidder representative,

accepting such documentation that can be obtained under commonly used procedures in the country of the bidder (for example, a requirement for notarization in a consulate or embassy would be an unacceptable impost).
- The certification process shall not require bidders to submit mandatory information with origin outside a bidder's own country.

The MDBs do not attempt to develop a model or business case for PKI but leaves that to the countries concerned. These rules represent a compromise between the current state of PKI and business practicalities and do not pretend to resolve PKI weaknesses identified earlier. As such these rules are a defence of the MDB procurement core principles rather than a model for PKI and these agencies have correctly refused to bend their procurement principles to accommodate the technology.

UNCITRAL and E-Commerce

At the same time as these MDBs were establishing their position in relation to on-line authentication, UNCITRAL was revising its position on these and related matters and independently coming to a similar position for e-contract Model Law.

Within the e-commerce environment the idea of non-repudiation has taken on a meaning that connotes both authorization and security of process. The vehicle for non-repudiation has, for some applications, become the certified digital signature. However, from a legal perspective an authorization or signature has never meant to convey assurances of security: the signature was always to convey the idea of intent.

In general the first of the new e-commerce laws enacted by various jurisdictions around the world reflected a certain lack of distinction between the notion of intent and the idea of security or risk management. These laws sometimes defined valid on-line signatures in terms of certified digital signatures and PKI. The UNCITRAL Model Law on E-Signatures was influenced by these developments and is not entirely technologically neutral. As the problems with PKI became evident, the legislation has been shifting towards a technologically neutral position. This is also much more consistent with the way in which B2B interactions generally operate.

A similar approach with regards to authentication has been adopted by UNCITRAL. The Draft Convention on the Use of Electronic Communications in International Contracts, approved at the Thirty-eighth session in Vienna, 4-15 July 2005, aimed at enhancing legal certainty and commercial predictability where electronic communications are used in relation to international contracts. The provisions of the Draft Convention deal with determining a party's location in an electronic environment; the time and place of dispatch and receipt of electronic communications; and the use of automated message systems for contract formation. Other provisions contain criteria establishing the functional equivalence between electronic communications and paper documents - including "original" paper documents - as well as between electronic authentication methods and hand-written signatures. The new Convention will help assure companies and traders around the world that contracts negotiated electronically are as valid and enforceable as traditional paper-based transactions.

The Draft Convention is based on a pure technologically neutral approach. It recognizes the legal validity of the electronic communications, and stipulates that a communication or a contract should not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication. It also adopts an open view with respect to form requirements by considering that nothing in the Convention requires a communication or a contract to be made or evidenced in any particular form. Likewise, it states that where the law has required that a communication or a contract be in writing, or has provided consequences for the absence of written form, those requirements are met by an electronic communication if the information contained therein was accessible so as to be usable for subsequent reference.

With regard to electronic signatures, the Draft Convention has revisited the Electronic Commerce Model Law concept and revised the previous Electronic Signature Model Law approach. It now provides that where the law has required that a communication or contract be signed by a party, or has provided consequences for the absence of a signature, that requirement is met by an electronic communication if:

- A method has been used to identify the party and to indicate that party's approval of the information contained in the electronic communication; and
- That method has been as reliable as appropriate for the purpose for which the

The new Convention will help assure companies and traders around the world that contracts negotiated electronically are as valid and enforceable as traditional paper-based transactions

electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement.[3]

In other words, the Draft Convention allows for the use of any kind of electronic signature, and incorporates the concept of risk by considering the reliability and propriety of the authentication method and the force of the agreements, within which administrative means of authentication may be considered.

In relation to the principles of e-GP, the UNCITRAL Working Group I (Procurement) Report for its sixth session (Vienna, September 2004) recognized that efficient and reliable electronic procurement systems require appropriate controls as regards security, confidentiality and authenticity of submissions, and integrity of data, for which special rules and standards might need to be formulated. In particular, it noted the convenience of guiding principles, which might form a useful basis for any future rules or guidance on the use of electronic communications in the procurement process. The core principles that have been stated by the UNCITRAL Working Group I (Procurement) were the following:

- The means of communication imposed should not present an unreasonable barrier to participation in the procurement proceedings (a principle that would allow a requirement for paper-based or electronic communications in appropriate circumstances);
- There should be appropriate procedures and systems to establish the origin of communications (authenticity);
- The means and mechanisms used should be such as to ensure that the integrity of data is preserved;
- The means used should enable the time of receipt of documents to be established, if the time of receipt were significant in applying the rules of the procurement process (i.e. for submission of requests to participate and for tenders and proposals);
- The means and mechanisms used should ensure that tenders and other significant documents were not accessed by the procuring entity or other persons prior to any deadline, so as to prevent procuring entities' passing information on other tenders to favoured suppliers and to prevent competitors from gaining access to that information themselves (security);
- The confidentiality of information submitted by or relating to other suppliers is maintained.

There was general agreement within the Working Group that the above principles provided a good basis for the formulation of specific rules, standards or guidance on the matter.

As well as being consistent with the MDBs core principles, the UNCITRAL Working Group I (Procurement) Report for its seventh session (New York, April 2005), has suggested that the Secretariat include a provision in an early section of the Procurement Model Law, as a new article 4, promulgating the general principles of functional equivalence and technological neutrality to be observed in various actions taken in the course of the procurement process, such as publication of opportunities and procurement-related information, communication between, for example, procuring entities and suppliers, opening of tenders and holding pre-tender conferences. Such a general provision, it was observed, should eliminate obstacles to, and ambiguities in, the use of electronic means of communication in public procurement under the Model Law and encourage such use by amending all phrases implying a solely paper-based environment, such as "writing", "sealed envelope", "signature" or "record-keeping", without being overly prescriptive or rendering the Model Law more complex.

Discussion and conclusion

These parallel developments by the MDBs and UNCITRAL represent an important shift in the management of on-line authentication as well as a maturing of its understanding. The earlier partial convergence between model law and technology around PKI models for authentication has now dissolved. There is now a convergence between the law and risk management that distances itself from any technology. A further critical development in this regard is the recognition by UNCITRAL that the authentication methodology should be commensurate with risk. This latter development does two things: firstly it opens the door for traditional administrative processes, and secondly requires that the risks implicit within technologies such as PKI be recognised and measured.

These developments now create a tension between the directions of the law (and the MDBs)

[3] Article 9.- Form requirements, subsection 3, (a) and (b).

and the e-GP processes being adopted by some governments. Whereas previously it could have been presumed that business practice was out-of-step with technology and the law, it might now be said that technology (or its application of PKI to e-GP) is out-of-step with model law and business practice. Governments that are locking e-GP into PKI need to be clear about their risks and objectives. With government procurement representing a significant part of the economy and the leadership role of government in many developing countries, care needs to be taken that locking e-GP into PKI does not embed standards that may become superseded and which have unresolved problems of their own. Herein lays a strength of the administrative approach to e-GP authentication over the legal approach.

Also for some applications, PKI with all of its management issues, costs and lack of standards, would seem to add little to security that is not already available within an SSL transmission that has no such problems. The authorization that is supposed to be assured by PKI has been managed by other administrative means by the great bulk of businesses and by some governments, and model law now formally recognises this.

The MDBs have adopted a prudent course by maintaining a technologically neutral position on this issue and focussing instead on the protection of core principles of governance. Within the context of these core principles, the MDBs would be open to considering various options for authentication. UNCITRAL and the MDBs do not suggest that countries close the door on PKI, but that they open the door for other technological and risk management responses including traditional administrative processes that can continue to apply in the e-GP environment. ■

Paul Schapper, BSc, BEc, PhD is a Professorial Fellow for Governance at the Curtin University of Technology (Perth, Western Australia), a member of the Advisory Board of the Commonwealth Centre for E-Governance (India), a member of the Editorial Board of the Journal of Contemporary Issues in Business and Government, and an international consultant.

paul.schapper@iinet.net.au

Mercedes Rivolta, a lawyer and Government Administrator, has been a member of the 1st Qualified Body of Government Administrators since 1987, from Cabinet Chief's Office, Buenos Aires. She is an international consultant in regulation and implementation of Public Key Infrastructure, e-commerce, e-government procurement and digital signatures.

mercedesrivolta@yahoo.com.ar

Knut Leipold is a Senior Procurement Specialist at the World Bank Group, and a member of the Multilateral Development Banks' e-GP Working Group and of the EU's E-Procurement Policy Working Group. He has been actively involved in the development of e-GP policies and in providing support for the adoption of e-GP in low- and middle-income countries.

kleipold@worldbank.org