

ICA 37th Conference: Fourth Session

IT SECURITY TODAY – THE CHALLENGE OF THE REAL TIME GOVERNMENT

Hans Werner Ksica

Austria

And

John Weigelt

Canada

Hans Werner Ksica is the ICA National Representative for Austria. He is Head of IT Organisation and Procurement in the Austrian Federal Ministry of Education, Science and Culture. Hans has been working in IT in government for about 30 years and is a sworn legally certified IT expert. He recently led the ICA Study Group on Security, which was published in July 2003.

John Weigelt, Canada. John is the Senior Director of Architecture of Standards and Engineering in the CIO branch, Treasury Board of Canada. He is responsible for the development of the Government of Canada's Enterprise Architecture and IM and IT standards and he provides support for critical information infrastructure, protection policies.

Hans Werner Ksica, Austria. Good afternoon ladies and gentlemen. We have seen a considerable progress in the adoption of and an increase in the number of PKI users from year to year. The use of smart cards and tokens in governments is moving in step with PKI regulation as they are adopted. Third the employment of biometrics is appearing as a best practice around passports and similar identity systems implementations. This is part of the summary of our Study Group Report. The final report, exclusive to this audience, is a result of the work of the ICA Study Group on Security which was convened in February last year. The group consisted of 9 experts from around the globe and was tasked to present an interim report by October last year. The group has now drafted its final report, which was delivered to the ICA board in July this year. We permanently try to consider three main regulations, to be ready with the very last state of the art and provide latest facts as well. Second, the draft a report, small in pages but clearly arranged in content. Third, to identify the key-player governments in IT security. Our mission was to fulfil this working programme.

Our review covers; country overviews; updates on the latest government solutions in PKI and trusted services and the authorities for authentication and registration; the role of electronic signatures, if in practical use; and what are the legal and financial frameworks. We then discuss smart cards in use or in state of roll out if they are and the latest biometric overviews, analysing successful and unsuccessful field tests. Pointing out successful strategies and plans, selecting best solutions in use or in roll out.

Our schedule. Ten countries provided results to the first overview survey. This was more or less an introduction to us and became a basis for discussion at a first meeting in Salzburg in Austria in June last year. One of the main outcomes from this meeting was a complete structure for the second specific survey including questionnaire, a methodology and a division of the work to follow. The outcome of this survey together with usable results from last Spring brought 14 country results in total, at last a respectable number. We reached the

milestone of an interim report in Singapore last year. The study group held its second meeting in Austria at the same place last year.

We were faced with organising perhaps a difficult stage of work. It was to verify all the collected data. It was to enrich the results of the fact finding period with expert interpretation and we had to develop overviews for comparison. This was followed by a period of crosschecking and drafting with most of the material for a final report.

Summaries and conclusions were completed during the third and final meeting of the Study Group in Ottawa in Canada. It took place at the beginning of March and it was really no early Springtime this year because it was down to -35°c all the time! John Weigelt and his team hosted us with great hospitality, thank you John, once more for this. In the report you will find data results from countries organised in the following structure. Starting with a general analysis of each item, you will be able to compare the country inputs one after the other. Finally, IT strategies are available from these countries. We are happy the questionnaires responses we received were relevant and contained valuable data. Once more, thank you very much to those countries for your contributions. It was great to have your support.

We were not totally successful with a small number of pages, but we were successful with the rearrangement. The main reason for its final size of 106 pages is based on the inclusion of 3 appendices. In our opinion important documents from first Canada, you will hear more on this in a few moments. Second, from the UK – an introduction to the e-Government Strategy Framework Policy and Guidelines. Third, the International Data Corporation (IDC) - State of Technology, an interesting enterprise view called Biometrics Bulletin.

It would be a help if you take some time to visit the corresponding ICA website, go to documents Study Groups Issue 76. You can look it up, go through it or download it as you like. Some of you may remember the intermediate report we gave last year. It told you that besides a number of excellent applications from several countries that really were serving the citizens first. The group selected examples of the best practice, IT Security Solutions. We had the opportunity to discuss this with parts of the staff of Canada's Government On-Line section when we had our meeting there. Their approach to the citizen seemed to the Study Group to be exemplary.

I have tried to reflect briefly on the workings of the study group and its work programme more at less from administration experience and its self and I would like once more to acknowledge all members of the study groups, many of whom are well known experts in the field, and I thank you all for your contributions and support. It was challenging and interesting to work with you in all its stages. Thanks to the ICA Board for trusting our work force. May I invite John Weigelt from Canada to present us with highlights from the Government On-Line Goals in his country? Thank you for your attention.

John Weigelt, Canada. Well thanks very much it is in deed a pleasure to be pointed out as a promising practice I wouldn't say that we are winners of any type of award, we are certainly working hard to deliver the services to Canadians and get something out there that people will be comfortable using. We would like to share what we have done with regard to authentication services because what we feel we have done is unique and we are going to ask you to stretch your minds a bit when you think about certificates, when you think about public infrastructures and how they are employed because we have changed the rules a little bit and we think that changing the rules will help facilitate cross boarder interactions and better comfort with our clients that we all service. I saw this the other day. Our business goals truly its improved quality, programme integrity but privacy is front and centre. When we talk to Canadians privacy is a key aspect is that they are wishing to protect and when we looked at public key infrastructures we found that in some cases there is this misconception that when you use a public infrastructure everything that you touch using that certificate is emblazoned

with your name and whatever particulars and we think about qualified certificates and signing things with qualified certificates this is a concept that, Hey after I signed something you are going to be able to trace my transactions all the way along. We have changed that, that way of doing business. But lets take a step back and say well, why do we need authentication services and how are we going to employ authentication services. We have some hundred plus applications that we hope to put on-line transactional based applications and again seventy percent, over seventy percent indicated that they needed some form of authentication but truly to take a bus you don't necessarily need to tell somebody how old you are, unless your fortunate enough to get discount rates, if you go to a theatre you don't have to tell them who you are for the tickets, and so we look at the range of services that government needs to provide and there is a wide range of services, and some services you don't need to know who you are doing business with, access to public information for example. The access or the ability to obtain paid publications or there is a well defined state of art for doing so, credit card type transactions SSL are not going to change the way of doing business.

When you file your taxes though you want to be given credit for giving us your money, you do not want your neighbour to be given credit for that money that you have given us, so we are going to have to start to know who we are dealing with. Likewise we are going to need some greater assurance in those transactions, better technologies, greater assurance and identity and you see on the right hand side a wide range of technologies everywhere for nothing for just access to publications to secure sockets layer, pins and pass words and finally public key infrastructure. And public key infrastructure has been generally agreed to be one of the strongest levels of assurance, technologies to gain the strongest levels of assurance and we find that when you invest in public key infrastructure you can start to use it for other applications. Our application of PKI allows us the flexibility to use the PKI for lesser assurance applications and we were fortunate we did go on-line with our public key infrastructures September of last year; pretty benign application it was for address changes on-line but it allowed us an opportunity to see how this actually works under real world environments, to see how it scales. There is really no large PKI out there about millions of people and when we started to roll this out we were quite surprised at what it took to start rolling out public key infrastructure to millions of people from a technology perspective, from a business operations perspective and from a business perspective.

So this is our home page for 'epass Canada' and we have a common epass look and feel for all government applications. Now because time is at a premium I am just going to flip through those quickly and get to the summary slide here. So our authentication service, our certificates our meaningless certificates. If you receive one and you are not a business application you can derive no meaning from that certificate. As the distinguished name in the certificate we conclude a meaningless but unique number so that it provides a secure repeatability but it does not bestow identity and that is something that is a challenge I know that when we talk with our colleagues in the Scandinavian nations well saying how do we gain assurance in that. Well the certificate gives us secure repeatability once you have been to our portal to a department then we know when you come back again, when you show that certificate again.

When you access a department using a certificate, the department will receive this number and say well that's fantastic you have gotten one of our epasses but now I need to find out who you are and they will ask you some additional questions; so we do identity proofing as a secondary step. And we can do that identity proofing on a per application basis and that provides us with a great deal of flex ability because when we went to departments and we said well what do want to include in a certificate, name, address, date of birth and we found we could not reach agreement on the formatting of that information, we found that there were different holdings quite a complex challenge this way we were able to deploy the PKI solution and allow the departments to maintain their current data standards.

We allow Canadians to choose one or many epasses just like if you look in your wallet I am sure you will have many different cards in your wallet, likewise you can choose to have many different epasses. You can have many different internet portal or e mail accounts, hotmail, yahoo mail, MSL mail likewise you can choose to have a separate meaningless but unique number, separate user name and pass word for every application for every programme that you get access to on Government On-line. We try to duplicate as much as possible those commonly used services that Canadians were familiar with. Internet banking, Internet portals, passport models things like that. That's the Microsoft passport not the paper passport. Consent base model, the other thing was we found through the studies by reading through studies we found that 40 to 60 percent of clients forget their password and when you look at how individuals deal with government they are not dealing with us everyday they might deal with us once twice a year, some students perhaps more frequently but its not a daily type of occurrence as of yet, we hope that some day it will get there but we are not quite there yet. And so there is a good chance that people will forget their password so we could put in a system like the internet mail accounts and mail back the password but then we lose some of those proof services that we can rely upon with the use of PKI and so what we need to do was create a recovery process some means by which an individual that forgets password can recovery their password, or recover their repeatable credential and so what we have decided to do is use a shared secret process so the users will select from a pull down menu five questions and five answers and when they answer those questions correctly they can recover their profile.

Now on focus testing across Canada people did not really like that they were somewhat concerned about what we were doing with some of those choices and we had a question that said "what is your least favourite vegetable" and the broccoli growers really got mad at us because they thought we were using that information some other way. So things like that it was really, really amusing to see the focus testing, how exactly do people want to recover their passwords what are their choices that they are going to make? Right now, the information resides with the programmes and they have to do that mapping between the meaningless but unique number and the individual programme dealer that they collect at their front door upon the first access. We want to move to a place where when a suitable token exists that we can put that information back into the hands of the client. So that when the department needs to access information we will be able to present them a banner, saying department x needs to access your address, are you okay with releasing that address from your personal token? and then they can be involved without consent decision. But we have not found a token yet that is quite ubiquitous enough so that we can roll out with that type of service.

Now privacy is key. We really want to focus on privacy and security and we believe that privacy and security don't necessarily have to be at the expense of each other. You can have a very private, and a very secure solution. It is just a matter of how you deploy it. We have been looking at the privacy enhancing technologies, and right now we are really focusing on using technologies in a privacy friendly way. After we start to do that, then we can start to look at the privacy enhancing technologies. So our focus testing revealed that people think that the banks do a better job in security than we do but they think we do a better job on privacy, and we want to maintain that level of assurance, that level of trust with our clients. We have some studies that show a direct correlation between the level of voluntary compliance with the taxation act in the level of trust they have in the taxman. We do not want to remove that.

We have implemented a policy for privacy impact assessments, much like we do throughout risk assessments, business impact assessments, legal impact assessments. New programmes are now obliged to do privacy impact assessments for their data and data flows. These are quite detailed reviews of the privacy aspects, privacy elements of applications. They go into individual dataflows, which data element goes where, at what time. This work is based upon

some great work done in the provinces. In other areas we borrowed with pride, adapted it a little for our federal environment, and are moving forward with that. We feel that some of the successes of our secure channel project, our common infrastructure project, are based upon our use of the privacy impact assessment. We had four iterations before we were actually going live with the application to really realise and understand what the privacy impacts were. Again, concerns about privacy.

Other things we looked at and this is not a mark-up of a Canadian card or anything we have planned. This is something, a doodle with PowerPoint so please do not cut and paste. So Canada is doing this, this is the Canada card. We have been looking at cards, and part of the study was to look at card technologies. We conducted some research on token technologies, and what we had concluded was that we did not want to force a single card for across programmes. We wanted to have a common form factor of the card however across programmes so that we could standardise the infrastructure that we used. We looked at International standards, we looked at our friends south of the border to see what they were doing so that we could have interoperability there. With the single form factor based upon the International standard, our smart card token was the result of that debate. Since the study was taken, there is now renewed public policy debate about identity cards and the use of cards within government, and we are still waiting for the final results of that activity.

Biometrics. Some small biometric pilots are in place just to see how the customers, clients' expectations are, what the comfort levels is with this, and we have some applications within government where biometrics are being used. What we concluded, however, is that technology is only a very small part of the solution. You really have to look at the business processes, how you are going to roll this out to individuals, how do you provide a seamless way to access credentials: registration is perhaps one of the most challenging aspects of rolling out public infrastructure. We are fortunate in that we had our taxman go off and do our initial registration, because they maintain a lot of data on their clients. These are repeat clients, they have been there before, still resolving how to register those people that are new to government or that we have not seen before. We believe that you need to have a range of identification options for different programmes based upon what the threat and the risk is. And our solution allows you to have that repeatable secure relationship with your client, and then build upon that through that secondary transaction. We also feel that we have interoperability with other nations by a secondary transaction. We can show you our credential and then associate that information that you require for your transaction as a secondary transaction in a secure way.

But communications are key to dispel those common misconceptions. You know, PKI invades privacy, soft certificates are not good enough for government applications. We really have to start talking this through, seeing how we connect up across borders, and roll out these solutions for the betterment of our clients. I hope I have provided you with a brief snapshot of the PKI initiatives within Canada, and look forward to watching other nations move forward their PKI and public certificate infrastructures to see how we can connect up. This year we are hoping to finalise our cross certification with the United States and start doing some business transactions electronically using PKI across our borders. We are nearing our final stages of that agreement and we hope to be able to talk you more about that once we start doing our business. Thank you very much.