In this issue: A new way forward for an effective identity policy in the UK p. 4

Exclusive: Digital Austria turning mobile p. 14 | Idiocy and eIdentity in the UK p. 20 | Identity management & public service delivery p. 28 | Secure in the cloud p. 34 | UK on the front foot against mobile crime p. 40
Time for governments to grasp the ID nettle?

Nicole Mountain, Channel Director, Security-News.tv

Hello and welcome to the third issue of TheVAULT – Digital.

As an industry, we all know that the technology for secure electronic identification is ready. Did I say ‘ready’? I mean actually up and running in a number of applications. So why is end-user take-up and acceptance so slow? What are the prime reasons why people are still wary of introducing such systems, and what can the Government do to ensure tangible benefits for the end user? Is it time for them to finally ‘grasp the nettle’ that is identification and roll out this theme to the mass population?

In this issue we talk to Guy Herbert, general secretary of the campaign group NO2ID to find out about their hesitancies relating to eID projects in terms of the alleged threat to public privacy and liberty (page 20). We hear the academic point of view from Edgar Whitley, research co-coordinator for the Identity Project at the London School of Economics, to find out his vision for implementing an effective eID solution (page 4), and we get thoughts from technology association Intellect, about identity management and service delivery on page 28. We also talk to Prof. Dr. Posch, CIO for Austria’s Federal Government, about Austria’s success with their eID project and the benefits they have achieved for the country’s citizens (page 14). In addition, we talk to the UK’s Minister for Crime reduction, Alan Campbell, about how the government and industry can work together to ensure safe and secure technology for all (page 40).

Also in this issue we take a look at the subject of ‘Cloud Computing’. We find out about some of the challenges faced with data storage and security as we talk with Google’s Director of Security for Google Apps, Eran Feigenbaum (page 34) and we get input from security experts Infineon Technologies about how some of these challenges can be overcome with trusted computing concepts (page 50).

As usual, we have our special Silicon Trust section, featuring views on card application management systems from Giesecke & Devrient on page 56; the need for smart card based applications by SCM Microsystems (page 78); innovation with Infineon Technologies (page 62); PKI solutions with charismathics (page 72) and a biometrics case study from precise Biometrics (page 84).

Enjoy this issue…

Nicole Mountain
Contents

Cover story
A new way forward for an effective identity policy in the UK
By Dr. Edgar Whitley, Reader in Information Systems in the Department of Management and Research Coordinator of the LSE Identity Project, London, School of Economics

Digital Austria turning mobile
An interview with Prof. Dr. Poehl, Austrian Federal Government

Idiocy and eIdentity in the UK
An interview with Guy Herbert, General Secretary, NO2ID

Identity management & public service delivery
By Carla Baker, Intellect UK

Secure in the cloud
An interview with Eran Feigenbaum, Director of Security for Google Apps

UK on the front foot against mobile crime
An interview with Alan Campbell, Minister for Crime Reduction, UK Home Office

Cloud computing
By Martin Klimke and Tolgahan Yildiz, Infineon Technologies and member of the Silicon Trust

Modern Card Application Management System (CAMS)
By Fabiola Bellersheim, Giesecke & Devrient and member of the Silicon Trust

Fit for ID?
By Peter Stampka, Andreas Karl, Dr. Detlef Houdeau, Infineon Technologies and member of the Silicon Trust

Software protection goes PKI
By Sven Gossel, charismathic

eID for a secure future
By Dietmar Wendling, SCM Microsystems and member of Silicon Trust

Gym access with BIOMATCH™
By Linda Rosdahl, Precise Biometrics and member of Silicon Trust

The Silicon Trust

If you are viewing this publication in PDF format, click on any article title to go directly to the page.
A new way forward for an effective identity policy in the UK

By Dr. Edgar Whitley, Reader in Information Systems in the Department of Management and Research Co-ordinator of the LSE Identity Project, London School of Economics

Dr. Edgar Whitley is a reader in information systems in the Department of Management at the London School of Economics and Political Science and the Research Co-ordinator for the LSE Identity Project. Here Edgar provides Security-news.tv with his vision for an effective identity policy in the UK.
The fate of the UK National Identity Service is increasingly uncertain, facing the dual threats of ‘wise spending reviews’ from the Labour government and immediate cancellation from the two main opposition parties. However, the need to identify, and more importantly authenticate individuals will increase rather than disappear as more and more activities take place online. Politicians and businesses will still be faced with the need for an identity policy that addresses the needs of individuals and organizations. The key question is, what principles such a new policy should adhere to?

Starting from the perspective of business (which can include the ‘service’ side of government as well), one body (the ‘relying party’) needs to know that the other is who they say they are (or have the attributes that they claim to possess) and they need to know the basis of this assertion (i.e. who is the ‘identity service provider’?). Before deciding to interact with the individual, to provide services for them or to allow them access to some of their resources, the relying party takes a commercial decision based on the identity assertion being made. This commercial (risk) decision may include consideration of what is known about the identity service provider, an evaluation of any mediation activities and consideration of liability/repair issues if problems arise.

Identification and authentication

Identity policies seek to address the trust-related issues that arise from identification and authentication interactions. Thus, individuals may need to identify themselves or may wish to confirm that they are over 18 to access particular ‘age-restricted’ resources or services, or may need to confirm that they are entitled to particular government services or benefits. Identification is taken as a process whereby someone’s identity is revealed (‘This is Jo Bloggs’), whilst authentication is a process that results in a person being accepted as authorized to engage in, or perform some activity (‘I am allowed to withdraw money from this bank account’, ‘I am Edgar Whitley’ or ‘I am old enough to buy alcohol’). Identification and authentication are therefore distinct activities with authentication typically undertaken far more frequently than identification.

The individual perspective on identity management is increasingly driven by privacy concerns and consumer choice. Just as it is no longer accepted that the government is necessarily the best (sole) provider of telephone services or water supplies, so it is not necessarily the case that identity services should be driven by the government. This is particularly the case when much of the data used to enroll in an identity scheme will be found in commercial databases held by credit reference agencies and others.
For commercial organizations, particularly those in high assurance environments, there is a particular emphasis on the initial enrolment, which might typically (but not necessarily) be tied to government-issued credentials. In such cases, the enrolment process might be described as ‘identity proofing’ and may also incorporate vetting processes. For other organizations however, this link to nationally-issued credentials is less important. Thus, in the case of age-restricted purchases, the relying party needs to trust that the identity document does confirm that the person satisfies the age requirement but this does not necessarily have to be a government-issued document as many other services providers (banks / schools / mobile phone providers, etc.) might be prepared to stand behind the age-related assertion. For example, a mobile phone company may already restrict access to ‘adult’ sites via its phone internet services based on existing age checking and can use the same processes to allow third parties, such as bars, to confirm that the phone user is over 18.

In other cases, the assertions might be provided by a low-integrity source that is appropriate for that context, so in an online game environment, the attribute that another player has particular powers might be provided by no more reliable authority than the game provider.

Despite these sophisticated requirements the resulting identity policy does not need to follow the same assumptions as the current UK Scheme and there are alternative design choices made in identity policies around the world. Thus, key assumptions underlying the UK Scheme – the collection, storage and use of irrevocable biometrics, the storage of vast quantities of personal data on centralized government databases and a complex legal regime that imposes a series of new duties on individuals to notify the government of changes in their personal circumstances – need to be reconsidered.

Perhaps the most important assumption to question however, is the strong link made between identity cards and passports. This link has existed since the earliest discussion of entitlement cards and has resulted in a single body, the Identity and Passport Service, being responsible for issuing both passports and identity cards.

The initial plan for the roll-out of identity cards was to be closely linked to the issuing / renewal of passports and the link continues with the unsupported assertion that the government was under an international obligation to update its passports and passport-issuing processes to include fingerprint biometric information.

Perhaps the most important limitation of the link between identity cards and passports relates to the principle purpose of a passport, namely to facilitate cross-border travel.

In the UK, passports can be withdrawn from those with a banning order issued in relation to the Football Spectators Act and the Football Disorder Act and there is also discussion that absent parents who fall behind in child maintenance payments should follow suit. These people however, cannot be denied the benefits of an identity card, but will instead be issued with an identification card that is very clearly marked to indicate that it cannot be used to travel within Europe.

The online registration and check-in systems of all participating airlines will presumably have to include a real-time ‘valid for travel’ checking function for UK identity documents.
Perhaps a more significant privacy problem from the link between identity cards and passports arises because the identity card has to satisfy the International Civil Aviation Organization (ICAO) requirements for Machine Readable Travel Documents (MRTDs). These requirements ensure that the documents are usable in a variety of situations from high-tech modern airports to border crossings where online connectivity is limited or non-existent.

This means that the main data about the holder of the card is found in human-readable form on the face of the card. Thus, passport pages typically include details of the holder’s name, place and country of birth, expiry date of the document and details of the issuing authority. Crucially, MRTDs also print the holder’s date of birth on the face of the card. This means that if the identity card is to be used as a basis for determining whether an individual is of the appropriate age to enter or use certain age-restricted products and services, the MRTD requirement automatically discloses their date of birth, which is more detailed than is required to achieve this particular function.

There is no shortage of advice and exemplars that address many of the articulated goals of an effective identity policy:


A corollary of this is that even if more extensive data has been collected, the principle of data minimization should also apply to the data that is disclosed and shared.

To illustrate this point, consider again the example of access to age-restricted services, such as entering a bar. Here the relying party (the bar manager) needs to know that the person buying the drinks is of legal drinking age and that the person claiming this attribute is the person presenting the identity credential.

An identity policy that breaks the link with the passport however, opens up the opportunity for a much more privacy-friendly alternative that adheres to the principle of data minimization recommended by the Home Affairs Committee amongst others. This principle states that organizations ‘should collect only what is essential’, to be stored only for as long as is necessary.

This principle states that organizations ‘should collect only what is essential’, to be stored only for as long as is necessary.

It should also be possible to ensure that control over what information is disclosed remains with the individual.

It should also be possible to ensure that control over what information is disclosed remains with the individual. Thus, the individual could control whether or not to disclose that they are over 18 by requiring the bar manager to first authenticate that he/she is authorized to ask for proof-of-age authentication from bar guests.
This ‘allowed-to-confirm-age’ check can be undertaken in exactly the same way as the proof-of-age check is undertaken. The individual can also control that only confirmation of age data are transferred. This issue of symmetrical checking can be particularly significant for vulnerable groups, such as the elderly greeting someone claiming to be from their electricity company. That person’s identity credentials can be checked in the same way and the householder can decide whether to let them into their property based on whether that person’s identity credential has been issued by their electricity company. The processes underlying such a minimal disclosure process are infinitely scalable and allow for a market of authentication providers to exist, offering differing levels of authentication assurance. For example, those individuals who simply require the ability to confirm that they are able to access age-restricted services do not necessarily need this functionality to be provided by a government-based identification scheme. Instead the age-verification used by the device can be based on, for example, details held by their mobile phone company, bank or even education provider (school, university). This pushes the responsibility for confirming the date of birth of the individual, for example, onto these other organizations but given the relatively low level of risk associated with age-verification services, this is a manageable risk that these companies might be prepared to take.

Despite the challenges an effective identity policy for the UK may face, it should be one based around the needs of citizens and organizations rather than just government. Information and communications technology will play a key role in implementing the policy and the UK is uniquely placed to utilize the best available technology to achieve this goal. 

---

**Inspectron**

ENSURING DOCUMENT INTEGRITY

Track and Trace Solutions: Addressing Today’s Challenges with Tomorrow’s Technologies

Inspectron specialises in the supply and support of Document Integrity and Track and Trace solutions for the security print industry.

Track and Trace Solutions are designed for use with:
- e-Passports
- Smart Cards
- RFID
- Secure Documents

+44 1373 452555 • info@inspectron.com
www.inspectron.com
Digital Austria turning mobile

An interview with Prof. Dr. Posch, Austrian Federal Government

Since 2001, Professor Dr. Posch has been the Chief Information Officer (CIO) for the Austrian Government and has been at the forefront of implementing the country’s eGovernment Platform, ‘Digital Austria’. Security-news.tv spoke with Prof. Dr. Posch to find out more about Austria’s eGov services, the country’s plans for further eID developments and its involvement with the STORK consortium.

Could you tell us a little more about STORK’s activities and what involvement both yourself and the Austrian Government have within the consortium?

Austria has been involved in the preparation regarding the use and development of eID at a European level. On a European level, developments can be seen to have started with the Manchester declaration; where it was agreed that every citizen and business should be enabled with eID that also respects privacy rights. As this developed throughout the years, Europe found that take-up and interoperability were two of the biggest problems in Europe, which is why STORK was initially set up.

Austria was involved in the set up of the STORK project from the beginning, as Austria has a complete infrastructure of eID, which is also reflected in the eGovernment law and the framework as a whole. However, the next and more important step, is to bring that to the user, both within and across the EU member states.

How would you qualify the success in Austria for various eServices?

Most countries will have a criterion that measures the success of certain projects relating to the amount of money available for a task and efficiency etc. Having said this, we observe that eID has two wings – one that you see, which is the card’s external features and the second, which is internal – the background infrastructure. To be able to deploy eID in a seamless way you need an infrastructure which allows individuals to go to their local community and identify themselves, without having to re-register what they have previously registered at the Tax office.
So one of the most important benefits and successes, which can be noted from implementing eID, is that of the back office infrastructure. Just to give you an idea of that, we have a register of inhabitants, which is the basis for identification. And through the effort of eID, the accuracy of this data has increased tremendously. We did have a difference between the social security data and the data on the register of inhabitants, which amounted to something between 10 and 20%, but that has now decreased to less than half percent. And bearing in mind that any such difference causes a huge amount of effort when you have an actual process – here is the big revenue bonus that you get from having an eID solution. But as you can tell, these benefits are not necessarily seen by the citizen, this has nothing to do with whether the citizen uses their card or not, this benefit is purely based on the way that the infrastructure is built.

Then we look at the successes that are actually seen by the citizens, and in Austria we note that there are two most important applications, which are highlighted as successful. The first one is in the social security area – when you visit a doctor, and when you claim money from the social security system to be paid to the doctor – all these processes are now fully automated through eID, there’s no way around it and this is 100% deployed.

The second application is taxes. Austria has in the range of 70%–80% of all tax returns being done electronically, and that’s about the most we can achieve, as you will always have a number of people who refuse to do it electronically. Having implemented the eID effort, the tax system has also provided a much quicker turnaround for citizens – previously, from submitting the tax return to effective payment took approximately 7–8 months, but with the new system it’s within 1–2 weeks! So there you see a tangible benefit for the citizens, which is why of course people are really taking it up. It seems very much like a carrot and stick scenario, in order to get people to start to use these services.

That is the lesson we have learnt – you need some incentive, otherwise you will not attract people. Another incentive is brought through bridging the link between public administration and private sector applications, like banking – and I can happily report that, except for two banks, all the banks in Austria are now accepting the citizen card as a means to do electronic banking.

Has the issue of identity protection been raised amongst the public in terms of these services? This issue has not only been raised, it has been the primary focus from the beginning, even though it makes the citizen card a lot more complex than it perhaps should be. In Austria, because the privacy and the data protection issue demanded that we had a sectorized approach – for example we have a register of cancer illnesses, a register of convicted criminals – we certainly don’t want these registers to be easily aligned with other registers like that of garbage cans, etc. Therefore we have sectors and data protection and privacy issues, which demand that a system be in place, which through technology does not allow the cross over.

These demands resulted in one-way function and cryptology technology, which is within the concept. That lasted about one and a half years, whilst building the concept you find a way together with the data protection issues.
Out of interest, to what extent is it possible to incorporate foreign eID’s into the Austrian Government’s eID processes?

Well, in 2004, we issued an eGovernment law, which is an enabling law that provides a holistic eID concept. Also in 2004, we made some provisions for incorporating non-Austrian eID’s. Eventually we will have the citizen list of inhabitants, which is more or less automatically extended with the identities of non-Austrian residents. So if, for example, you come to Austria with any eID card that has a qualified signature, you could use a different card and still be incorporated into the Austrian system – and this holds true for individuals and for businesses. In 2008, we made an amendment to refine this further so that if we want to incorporate a further foreign eID, we just need to do the paperwork, the technology is already done!

What would you say is next on the agenda in the roadmap for rolling out Austria’s eID schemes across the country?

There is one aspect, which I would say has not been reached full satisfaction, and that is take-up by the citizen.

One reason for this is that there are only 1.7 contacts between an individual and the government per year, and another reason is that technology is, for a number of the public, something people are not really keen to take up. So next on the agenda is simplification.

One way to achieve simplification that we already have on our roadmap is to make it so an individual doesn’t have to install any software on their workstation. As long as the person has a card reader, the card can be recognized through the browser and a plug-in appears automatically when a government service is requested. This is not only true for Austrian cards, but also for other cards, as demonstrated with STORK, for example in Belgium and Portugal. And by the end of this year we will start to implement access to European Commission services with National eID’s, and to do that we need this type of access.

The next avenue we are about to go down, which will be in its first steps this year, is moving further away from physical cards. A physical card needs a card reader and what we plan to use is a mobile phone to generate qualified signatures and the eID is linked to these qualified signatures. So by the end of this new development, citizens will be able to use their mobile phone, after registering it in the appropriate way, to electronically sign documents and perform their eID tasks with government and the private sector applications. This is a major avenue we are starting to go down right now.

If we want to incorporate a further foreign eID, we just need to do the paperwork, the technology is already done!

Next on the agenda is simplification.

It always seems to take longer than people think to introduce and gain mass acceptance in the public domain – What kind of time frame do you expect to see around that?

If we separate two things – one is the readiness of the technology, and in this respect I think the services will be ready by the end of this year, however that doesn’t mean we will necessarily see fast take-up, as that takes time to generate awareness.

Most probably it will be about three or five years before this really infiltrates into all the private sector services, until then it will be a minority that is using eID, and that’s not a specific Austrian feature, that’s the same thing we observe throughout the world.
What do NO2ID see as the main threats towards privacy and liberty with the introduction of a National eID card in the UK?

In my opinion, it is a nationalized identity system that threatens privacy and liberty. Individual privacy and security is threatened by the centralization of personal information in the hands of the state and by linking it all with key identifiers. Privacy is also threatened by the proposed use of such a system to create mechanisms for the passing of information between departments, and (notionally as ‘verification’) to and from private sector organizations, which in turn opens up many more channels for inappropriate use. Liberty is threatened because the scheme potentially gives the state much more power over the individual, both through surveillance, and by giving it (the state) the final say over the validity of a person’s identity and therefore over his / her access to goods, services and own property. Its operation (which would constrain every person’s civic life according to the plans) is wholly in the hands of bureaucracy, which would have powers to penalize citizens without resort to the courts. Independent redress has been made very hard.

As the UK eID project continues to be one of the hot topics of conversation in British politics, Security-news.tv speaks with the UK’s main opposing campaign organization, NO2ID, about the alleged threat to public privacy and liberty, and asks how identity management should be dealt with in a secure, yet public-friendly way.

Idiocy and eIdentity in the UK

An interview with Guy Herbert, General Secretary, NO2ID
The focus on ID cards distracts attention from the centrality in the law and the scheme of the National Identity Register as a catalogue of personal information about individuals and of information sharing across government departments using it. The functions of the Register would be unchanged, and as injurious to privacy and liberty even if no cards were ever issued.

Conversely, it would be entirely possible (in theory), to build a functional eID scheme that did hinge on the card and had no central store of personal data, but that is not contemplated by the Identity Cards Act 2006, which legally requires a central Register in the control of the Home Office.

In an ideal world, what would NO2ID propose as an acceptable solution for the identification scheme?

There’s really no evidence that we need a national identity scheme. Most of the occasions on which government claims it would save citizens trouble are actually occasions on which troublesome demands for ID are imposed by the state; the arguments are therefore circular. The bureaucracy, sometimes deliberately, but more often ignorantly, confuses identity and authentication, authentication and authorization. Officials have a hierarchical, even hieratic understanding of identification, in which there is literally ‘a single source of truth’ and that truth is determined by official approval.

Guy Herbert, General Secretary, NO2ID
It is a mediaeval model of governmentalism, in which the king owns everything and everyone and all the details are kept in a big book. This was done most literal-mindedly in England in the 1080s, when William the Conqueror had what was later called ‘The Domesday Book’, compiled as a survey of his new kingdom. In that model all transactions are ultimately mediated by the state, and identity and privacy are necessarily antagonistic.

NO2ID is enthusiastic about the application of technology to provide authentication with privacy. We see no reason why keys, account cards, age verification and so forth shouldn’t emanate from a wide range of trusted sources and provide only the information or authority that their purpose requires. There’s no reason that identity should be unitary and indivisible. Any good system will provide redundancy, compartmentalization, anonymity and pseudonymity – all of which are needed in practice. All sorts of systems, each tailored to its proper use, are possible. There’s no good reason for them to be unified – on the contrary, it would be dangerous to put all of everyone’s eggs in one basket. For example: It is not necessary to the economic system that the Bank of England is the man-in-the-middle in every transaction. That sort of bureaucratic friction would be a disaster, everyone knows, even without the opportunities for crime and corruption it would create. Anyone who suggested it would be condemned by everyone in finance as a ‘dangerous idiot’. So why is the same sort of idiocy tolerated with regard to identity?

We have likewise from finance, perfectly good examples of working federated identity systems. Distinct payment card systems use the same infrastructure. Separate banks offer card services through shared systems, via chains of authority, not a centralized overseer. Those systems are flexible and respond quickly to threats: one of my identities within it can be cancelled if a card is lost, while another keeps working. No government specified it. It wasn’t the product of an empty theory. It grew to serve its customer’s needs.

In NO2ID’s opinion, what is the best way to safely collect and store personal data?

There isn’t one. What’s good depends on the circumstances and the use. And access must be properly controlled of course. But storage is not the issue here, sharing and transfer is. The technical challenge ought to be to find a good means of minimizing the sharing of personal information and for individuals to exercise control over what happens to their personal information. That is how public security and privacy could be enhanced and preserved by ‘eID’ – if the public, corporate users and solution providers would all reject the Domesday book model, and start to explore what offers the most benefit to individuals, rather than the most convenience to bureaucrats.

What is NO2ID’s opinion on the use of biometrics (fingerprint / iris) for person identification and authentication in government eID schemes? And does that opinion change if biometrics are used in private applications, such as access control for corporate office buildings and so on?

NO2ID is neutral about technology – it is how it is used that matters. Biometrics can certainly be handy for some sorts of access control, but they aren’t a panacea. It is particularly over biometrics that politicians and officials seem to bear out the Arthur C Clarke dictum that “any sufficiently high technology is indistinguishable from magic”, a weak intuition for systems and statistics leads them to think of ‘biometric’ as a synonym for ‘infallible’. And because biometrics are physically part of us, their use feeds the simple-minded bureaucratic model of identity as singular; as one file attaching to a particular body and linking all related facts. That is the danger of biometrics if they are shared. Just like any other shared identifier, they have the power to undermine privacy. And they are hard to hide, since we are always exposing them.

NO2ID would therefore say that of course biometrics can be useful, but that it is with elementary caution that they should be used as confirmation, rather than a sole key in any system, and of course they should be held locally, not shared.
As we know, the UK eID scheme has developed under the Labour Government, which most of the opposition are against. How would you feel if the opposition won in next year’s elections, yet continued with the eID scheme?

We’d feel betrayed, of course. But the simple decision to carry on against all public declarations of policy is highly unlikely.

What is more worrying, is the possibility that a new government will not be sufficiently rigorous in extirpating the scheme, for which there is a powerful internal lobby in Whitehall and that it will end up permitting the principle components of a national register to be built as nominally part of other administrative infrastructure. The Home Office has prepared that route for several years by the decision to abandon the single clean database and instead to incorporate segments of the Register into existing systems maintained by the DWP, the UK Borders Agency and so forth.

The UK National eID scheme is currently being developed on a national basis – how would NO2ID propose to continue the campaign against the scheme if it became a European directive?

Currently it couldn’t be a European directive since national ID cards and related measures are specifically outside the competence of the EU. That could change if the Lisbon treaty comes into effect however.

An EU framework decision would require an escalation of the sort of action required, since it would cease to be directly possible to oppose it in the UK parliament, and the EU parliament has neither great powers, nor great will, to stop such a development. We are committed to staying within the law, but we certainly don’t discount civil disobedience if the UK authorities use policy laundering through the EU to sidestep domestic democratic and legal mechanisms. It is the sort of thing that brings the EU and national governments into disrepute.

That said, a system that had to comply with European standards of data-protection would be a different proposition. It might make a system such as the UK’s current plans impossible, because other member states have more serious attitudes to citizen’s rights and to privacy with which such a scheme would have to comply. It would make the lobbying process more difficult, but we would get new legal tools to challenge ill thought-out legislation. ð
Identity management &
public service delivery

By Carla Baker, Intellect UK

In its recently published policy paper, ‘Reversing the Rise of the Surveillance State’, the UK Conservative Party argues that an over reliance on large centralized databases exposes the public to greater risk. As the paper rightly recognizes, there is a need for an open debate on how governments share, access and use information. However, whatever the outcome of such a debate, governments in the future will need an effective identity management infrastructure that enables public servants, businesses and individuals to access information.
The policy paper references the vulnerability of the Government’s databases and goes on to list the recent high profile data losses in government. There is no doubt that the processes that led to these losses must be reviewed. However, it is important to remember that the majority of these cases were caused by human error and that the databases themselves were not the cause of the data loss. The issue is more about information management and security – how information is stored, who has access to the information and the internal security and governance processes, which organizations have in place for handling information.

Information on citizens will always need to be held by the state – from tax and benefit information, to information held on court and police systems and databases. Information and data held on citizens and the systems used to verify that information are going to be required to deliver world-class services and to enable government to be more cost efficient and effective. For this to work, and to ensure that access to these databases is restricted and granted to those public servants who are authorized to do so, an effective and efficient identity management infrastructure needs to be put in place.

The importance of identity management

‘Identity management’ is a term that has been used to describe activity in a variety of areas; from ID cards, chip and pin, application of biometrics, immigration and prevention of terrorism, to the need for systems that facilitate the public sector reform agenda. This had led to some confusion as to what identity management actually is and why it’s important for the smooth running of society.

Essentially, identity management is the process of monitoring or controlling a sequence of identity interactions. It has come to describe the application of IT business processes in order to ensure that private and public sectors are able to correctly identify a person’s eligibility for the delivery of services.

The high profile media debate on ID cards has muddied the issue about the need for effective identity management systems. The two issues became synonymous with each other and that has caused some confusion. ID cards could provide a single and straightforward mechanism for proving people’s identities. However, in order to understand why an effective identity management infrastructure is required in a modern digital society, we need to separate the issue of ID cards and the rise of databases from the debate. Identity management systems offer real and concrete benefits to citizens and are vital for government and private sector interaction with citizens.

The delivery of public services

Central and local governments are increasingly using technology to ease and improve their interaction with citizens and for the delivery of public services. With more sensitive citizen-government transactions taking place digitally, the need for robust and secure identity management systems has increased. It is these systems that ensure citizens are getting the right benefits and services, as well as protecting against fraud and other criminal activity. Identity management has become a vital aspect in the way we interact with the state, and has become widely recognized as a critical enabler of the public sector reform agenda.

There are numerous government systems that require effective identity management in order to enable citizens to access services and information.
The much publicized and highly praised car tax renewal system provided by the DVLA requires, for example, an identity system that not only can verify personal identities but also the identities of cars (e.g. number plate) and cross-reference the two. ‘Tell Us Once’, the cross government initiative set up by the Department for Work and Pensions (DWP) enables people to advise all government departments and agencies of a birth or a death just once, instead of informing them separately. This can only happen if all government agencies identify the same citizen in the same way.

Opponents of these government systems and services argue that this move has had a negative effect on individuals’ privacy, but as we move towards an increasingly digital world, where people are interacting on a daily basis with applications such as Facebook and Myspace, it could be argued that government should join this digital revolution, but at the same time understand and promote privacy and security implications.

What about the privacy debate?

Identity management systems in a variety of shapes and forms have been around for a number of years. Banks have used online identity systems and ‘chip and pin’ in its dealings with customers, and supermarkets are increasingly using identity systems in their interactions with their customers. Citizens have been giving their information to organizations such as utility companies for years, and as such the provision of personal information is not a new phenomenon. However, the emotive issue of ID cards and concern about the ‘database state’ has distracted government from a more detailed debate about the need for an identity management infrastructure.

When it comes to protection of privacy, there are systems and processes that could be put in place (both technical and on an organizational level) to promote trust in the services that are offered by outlining very clear responsibilities and subsequent liabilities.

Technology systems, for example Privacy Enhancing Technologies, are available that can enable the separation of private information (for example address and date of birth, etc.) with identifying facts. In addition, both government and industry understand that in many circumstances the most basic information will suffice for interactions with citizens. The collection and sharing of data can offer huge benefits to citizens at the same time as protecting privacy but only if the collection of data is conducted in a minimal and secure way.

The future of identity management

Correctly assigning and knowing the identity of people and things is vital in a digital society so that entitlements can be claimed, services delivered, information acquired and transactions processed. A mature debate is needed on the benefits that can be provided to citizens and businesses as well as to the smooth running of government.

Standardizing identity management processes and systems will enable diverse systems and organizations to interoperate, which will lead to greater efficiency and effectiveness in service delivery in the long run. The development of access and role-based identity management systems will enhance privacy and security. The technology industry is making strides in this area, managing access whereby users have access to certain information based on their roles and responsibility and providing audit trails of who has access to what information and when.

Government needs to balance access, transparency and accountability with security and privacy. Promoting the use of secure identity management systems, while at the same time protecting privacy, is a crucial challenge for governments and the technology industry. A mature debate is needed, and one that is separated from the debate about ID cards and databases.
Secure in the cloud

An interview with Eran Feigenbaum, Director of Security for Google Apps

With online data storage becoming increasingly popular in the corporate world, Director of Security for Google Apps, Eran Feigenbaum talks to us about the challenges faced with data storage and security today, and his thoughts on secure computing in the future.

Why is Cloud Computing important in the world of data storage and security?

As computing moves out of the desktop and onto the Internet, worries about security have mounted. If you store data in another company’s servers, in the cloud so-to-speak, how can you be confident that it is safe? I just completed a tour in Europe, including stops in Italy, Germany, France, Belgium and the UK, and will soon travel to Spain and Holland to explain the counterintuitive notion that data can actually be much more secure ‘in the cloud’, than on the desktop.

Cloud computing, when IT software and services are delivered over the web and through a browser, is a paradigm shift, similar to taking your jewellery out of your sock drawer and placing it in the bank. The bank has the economies of scale. It has guards, robust safes, and video surveillance – much more than any security investment you can deploy yourself. The same is true with data. Cloud providers such as Google are equipped to protect millions of users’ data every day. As a customer you get to enjoy these economies of scale at minimal expense. We have over 1000 people dedicated to Google Enterprise, including some of the world’s best security experts who are helping to make sure that your data stays safe.

It’s enough to look at newspaper headlines any day of the week and read about lost data.

It’s enough to look at newspaper headlines any day of the week and read about lost data. Data on USB keys, lost or stolen laptops, MP3 players, etc. A report released last year by Credant Technologies found that London taxi passengers left more than 60,000 hand-held devices in the back of black cabs over a period of six months in 2008. Some 55,843 mobile phones and 6,193 other devices, such as laptops, were forgotten.
What are some of the major challenges faced by businesses when protecting their data and what does the ‘cloud’ offer to overcome these challenges?

Businesses dedicate a lot of time and resources to protecting their data, however this is often wrong. As reported by the IT Policy Compliance Group last year, human error accounts for three quarters of all incidents involving the loss of sensitive data. When I was a Chief Information Security Officer for a major financial services company, I used to tell my team, “make it easy for users to do the right thing and they usually do.” Employees are generally not malicious – they want to work from home as part of getting their work done. Indeed, today’s young employees consider working 9 to 5 and always at the same desk increasingly alien. Allow them to access data anytime and anywhere, while it is still stored and protected in the cloud, and you automatically eliminate many data loss risks.

The cloud offers several other important security advantages. Most organizations take 30–60 days to install security patches on their systems, which is a major concern in its own right. In fact, many companies I talk to admit it’s closer to 3–6 months to install a security patch. This means that traditional IT systems and applications are open to known security vulnerabilities for a very long time. By contrast, we run a very homogeneous computing environment, so when it is time to patch we can do it in a rapid and uniform manner to all of our systems.

And what about the physical security of data centers and the reliability of products?

At Google we replicate users’ data to multiple data centers. If one data center goes out, our infrastructure helps ensure that the data remains secure and accessible. While in Europe, some unfortunate news helped prove my point. I was in Milan when a flood swept the country and knocked out several key data centers. Although it affected a number of local businesses, Google customers saw no disruption of service.

Admittedly, no system is 100% foolproof, or 100% secure. Back in March we had an unfortunate programmatic error that caused a Google Docs sharing problem. However, we were able to respond quickly because it happened in the cloud.

The real question is what do you have in place to minimize the impact of these incidents, and how quickly can you respond if anything goes wrong.

We had an unfortunate programmatic error that caused a Google Docs sharing problem. However, we were able to respond quickly because it happened in the cloud.

To respond quickly because it happened in the cloud. The issue affected less than 0.05% of our users’ documents, and it was corrected without our clients having to do anything. No software to install, no upgrades, no configuration changes, etc. And we worked closely with the affected customers to inform them how it impacted their documents.

From time to time any system will be affected by some security issues. The real question is what people, process, and technologies do you have in place to minimize the impact of these incidents, and how quickly can you respond if anything goes wrong. We designed our systems with security in mind and have a 24 x 7 security team looking at new threats and are able to respond in a rapid manner. I’m confident that they address the sorts of concerns organizations have with their currently in-house managed systems. More than 1.75 million businesses have already signed up for our Google Apps suite, and this number is expanding by an additional 3,000 businesses each day.

And finally, how do you envisage the future of secure computing?

We’re convinced that the future of computing lies in the cloud. Cloud-based solutions are cost efficient, collaborative, and – more often than not – more secure to operate. While in Brussels, I observed that European policymakers are taking note. At least three studies on cloud computing undertaken by the European Commission and its security agency ENISA are in the pipeline, and we also talked about ways to demonstrate to professional and personal users alike how we respect our users’ security and privacy. Instead of seeing security as a negative factor weighing down the transition to cloud computing, I hope I have helped to explain why it should be perceived as a benefit.
In its EU-Passport Specification, the European Commission requires that:

“Every Member State MUST contract an accredited (national) test laboratory to certify functional compliance to the relevant standards on all ISO/OSI layers. Issued certificates MUST be notified to the Commission.”

* Source: European Commission, EU-Passport Specification (EN) 28/06/2006

To meet the European Union’s June 2009 deadline for migration to the EAC standard, e-Passport issuing authorities should seek the right test and certification partner now.

The German Federal Office for Information Security (BSI) has developed a unique e-Passport certification scheme which incorporates all tests of the ISO/OSI layers. The certificate issued by BSI will be published on the BSI website:

www.bsi.bund.de/zertifiz/tr/index_en.htm

The BSI e-Passport certificate
The best way to prove conformity with EU and ICAO standards

HJP Consulting
We are smart card architects

It’s easy when you know how.

HJP – Your global e-Passport and eID card system consultants

ASK US ABOUT OUR REFERENCES
IN EUROPE, THE MIDDLE EAST AND AFRICA
HJP Consulting GmbH | Germany | Phone +49 5251 41776-0
WWW.HJP-CONSULTING.COM

“Don’t waste time going round in circles struggling with test standards and administrative hurdles, go to our website or feel free to contact us.”
UK on the front foot against mobile crime

An interview with Alan Campbell, Minister for Crime Reduction, UK Home Office

The UK Home Office recently announced that they have been working alongside industry members to ensure that criminals don’t take advantage of the contactless technology used in mobile phones, which enables the user to make contactless payments with their mobile. Security-news.tv spoke with the UK’s Minister for Crime Reduction, Alan Campbell, about creating guidelines, and the government’s view on contactless mobile payments in the UK.

In your role as Minister for Crime Reduction, what’s your view on contactless technology and what benefits do you think it could bring to retailers, customers, industry and the country as a whole?

I think contactless payment has huge potential for customers, whether they’re paying for goods or services, because in the future they will be able to do this using their mobile phones. This is a great step forward for consumers, but of course from our perspective, there’s also a risk involved.
We are very keen to be on the front foot with this, to make sure that we have looked at the risk of criminality – cards being misused, or handsets being stolen – before they are rolled out from the schemes that are currently being piloted.

Some people may remember that the first generation of mobile phones led to a state of street crime, where people were sometimes attacked for their mobile phones. What we’re trying to do now, is get ahead of the game – to make sure that when contactless technology is rolled out in mobile phones for payment applications, we have done everything possible to make not only the handset safe, but the end user too.

How do you view the current use of contactless cards in the UK?

There’s a whole range of interesting examples in use at the moment, for example Oyster cards, which people recognize from use on the London Underground. In my opinion, this is the way in which we will see developments in the future. What we’re doing now is talking to the phone companies, telling them that they have a responsibility to look at the risk of criminality and the misuse of this technology and this is why we’ve been working with mobile phone companies and the banking industry, to develop a set of guidelines, so that when this technology is introduced, we’re in a much better place than perhaps we have been in previously.

**Why do you think the government should become involved in a technology that has previously been industry driven?**

Technology is a good thing – it creates new opportunities, however new technology can also create new opportunities for criminals too. I’m concerned for someone who pays a lot of money for this technology, puts money on to their mobile phone and for the loss of that money, should the phone be stolen. But I’m also concerned about what may happen if people think they can take this new phone, with money on it, from perhaps young people, which may also involve violence. I think that we all have a responsibility across the community – including businesses and industry – to make sure that we do everything we can from the outset, to make sure that we don’t get that spike in street crime that mirrors what happened with the introduction of mobile phones.

We’ve talked to industry members extensively about this, both the mobile phone and the banking industry, and I’m delighted that following those discussions they have come forward with a set of guidelines, which will help to make this technology safer. Whether this is a model we can roll out for other technology in the future, we’ll have to wait and see, but I think we’re making real progress.

**listen to this interview online at:**

s-n.tv/channel/audio
Are you just focusing on payment applications at the moment or are you also looking for guidelines on ticketing and access control functionality, because they both have very different security requirements?

We are looking at payment in particular, because what might be a relatively small amount of money that you can spend now (under £10 in the UK), buying your coffee or bun for example, may well be greater in the future — so we’re looking to build in safeguards for that, to make sure that there is a check, such as the current Chip & PIN security check, which is in use across the UK. But of course we’re interested in a whole range of technological advancements and the safety of phones themselves, but it is around the payment issue that we have focused on to date.

I notice that one of the guidelines encourages those who have a contactless payment phone, to add their details to the National Mobile Phone Register, making it easier for stolen phones to be identified and recovered — could you explain what the National Mobile Phone Register is?

We have a National Mobile Phone Register, which people are encouraged to sign up to so that law enforcement agencies can access information, if and when necessary. For example, if your phone is stolen and it is found at some point in the future, it might be that the phone can be returned because the police are able to check who the phone belongs to. If a stolen phone is used for criminal use and the criminal is found with it, law enforcement agencies would be able to check back to see who was responsible for taking the phone in the first instance.

I’m very much in favor of the National Mobile Phone Register because it’s a tool which the law enforcement agencies think is of particular value.

At the moment the register is of course voluntary, but I think there’s a case for creating more publicity about this and saying to people: look, when you buy your mobile phone or you go in to sign your contract for your new generation mobile phone, sign up to the National Mobile Phone Register, because it’s that extra security, that extra safeguard, so that at least criminals will know that if they take it and if they’re carrying it around and they’re stopped, then the Police will be able to check back, know it’s a stolen phone and do something about it.

As we look towards industry and contactless payments, how can the different members of the value chain be encouraged to take ownership of the potential security issues?

I recognize that there are, what appear to be, some conflicting themes in this, in the sense that the whole idea of contactless technology is to make life easier for people. Therefore we have to balance that against the responsibility of individuals for their own security. I also believe that the mobile phone companies and the banks should take some responsibility. All parties have got something to lose from this, but at the same time, something to gain.

We intend to get the message out there that the mobile phone companies and the banks should take some responsibility. All parties have got something to lose from this, but at the same time, something to gain.

We intend to get the message out there that we are on the front foot.

As we look towards industry and contactless payments, how can the different members of the value chain be encouraged to take ownership of the potential security issues?

I think that to some extent we have pushed the industry ourselves, in that we’ve got involved very early — we wouldn’t expect the roll out of this technology much before 2011, so we invited industry members to come and talk with us. And to be honest with you, I think the industry really has stepped up to the plate on this one. The guidelines which have been produced are good guidelines, I think they’re strong guidelines, but the important thing about this is that industry’s being part of this, it’s a real partnership not just between the mobile phone and banking industry, but the police too.
For industry to be involved in actually developing the guidelines themselves means that there’s a much better chance that industry will stick to them. What we don’t want to do is start legislating about what industry should do with regard to these sorts of issues; we want to work in partnership with industry. Major players in the industry have already signed up to this and some haven’t – they’re looking towards their own way of resolving this issue. But what we have certainly managed to achieve is to get industry together to focus on the crime side and the security implications related to the developments and I welcome that as part of their corporate responsibility.

As the father of a teenage daughter who has a mobile phone and who will want the next generation mobile phone, security would be one of those things that I would look at, because I want her to be safe, even before I want the technology to be safe. Therefore, I think that it is important that we get the message out and that people accept their individual responsibility for being safe. We should also publicize the fact that the industry is signed up to this too so people will know what they can expect if anything happens to their technology. And that sends out another message to the criminals, that we’re not just going to sit back and see what happens with this technology; we are actually on the front foot and we’re looking to prevent crime before it happens – a very important part of fighting crime in the future.

Finally, how should the public be educated about contactless mobile usage and perhaps more importantly, who should be responsible for this?

Again, I think there’s a joint responsibility for this. I’m sure the mobile phone industry will want to promote their phones and I’m very happy to talk to them about how we can work together – not just to promote the advantages of this technology, but to promote the security and safety of the technology too.
Since the year 2000, when the Silicon Trust was founded by Infineon Technologies as a marketing program for smart card solutions, the program has developed to be a key partner platform for companies aiming at promoting the use of silicon-based security in a broad variety of applications including Identification, Telecom and Payment. With more than 20 active member companies in 2008, Silicon Trust now forms a strong community of like-minded companies.

Today, the driving force behind the Silicon Trust are the three executive partners: Gemalto, Giesecke & Devrient and Infineon Technologies, supported by the German Federal Office for Information Security (BSI) in the Silicon Trust advisory board. Many other companies along the value chain of silicon-based security participate in Silicon Trust discussions and activities.

A WELL EXECUTED BUSINESS PLATFORM CAN ONLY GROW
Cloud computing

Promises, Technology and Opportunities for the Security Industry

By Martin Klimke and Tolgahan Yildiz, Infineon Technologies and member of the Silicon Trust

The success of cloud computing is hampered by fears relating to its security. Solid security concepts, which are also ready for new and future use cases, are therefore required to secure all parts of the system.

Cloud Computing shifts applications and data storage and is hyped as the next big opportunity for the Internet.

The technology promises the following:
- Cost reduction, by deploying large-scale server infrastructure and centralized maintenance;
- Better and faster scalability, without the need for upfront investment in infrastructure by the customer;
- Less effort, in terms of installation and maintenance for the client, because in many scenarios the Internet browser is used as the application front end;
- To move computing requirements from the client to the server – It is therefore suitable for thin clients with limited performance, making it attractive for portable low-power devices.

The technology is particularly interesting for small and medium-sized companies who often can’t afford their own infrastructure, due to up front investment and maintenance costs. Large corporations, with existing infrastructures, may also adopt this technology to save costs.

Figure 1: Opportunities and challenges that cloud computing and related services pose for enterprises

<table>
<thead>
<tr>
<th>Value Propositions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low cost (lower infrastructure investment, low HW and SW management costs)</td>
</tr>
<tr>
<td>High scalability</td>
</tr>
<tr>
<td>High mobility</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to ensure confidentiality, availability and integrity of the data in cloud</td>
</tr>
<tr>
<td>How to provide secure and mobile access and authentication mechanisms to the cloud services</td>
</tr>
</tbody>
</table>
Market environment

Putting the hype aside, cloud computing is today pretty much in its infancy and the mass deployment of cloud computing faces significant challenges and barriers.

In a recent study, 500 chief executives and IT managers were questioned about their perspectives on cloud computing. And although the benefits of cloud computing in respect to cost savings were acknowledged, 80% said that they leaders recognize the business benefits of cloud computing for making a meaningful difference in their organizations. At the same time, fears about security and control of data are limiting its broad adoption. One of the pressing issues that lies before our industry is addressing these perceived barriers and helping businesses develop a strategy to begin deploying cloud-based services today and build a long-term roadmap to capitalize on the business value of cloud computing in the future.”[1] The conclusion reveals that business and IT leaders recognize the business benefits of cloud computing for making a meaningful difference in their organizations.

“trust existing internal systems over cloud-based systems due to fear about security threats and loss of control of data and systems.” The conclusion of “this global study reveals that business and IT leaders recognize the business benefits of cloud computing for making a meaningful difference in their organizations. At the same time, fears about security and control of data are limiting its broad adoption. One of the pressing issues that lies before our industry is addressing these perceived barriers and helping businesses develop a strategy to begin deploying cloud-based services today and build a long-term roadmap to capitalize on the business value of cloud computing in the future.”[1]

Trusted computing

Trusted computing is based on the work of the Trusted Computing Group (TCG) and the technology is based on a trusted platform module (TPM). The TPM is a security controller that contains a set of functions supporting remote attestation. After the booting process, remote attestation can report on the integrity of a system. This technology has been deployed for some years now, and is implemented in many PCs today.

Trusted Platform Security is gaining new momentum for securing the cloud

One possible approach for ‘Infrastructure as a Service’ (IaaS) are Virtual Desktop Infrastructures (VDI), which enable desktop operating systems and applications to run inside virtual machines that reside on servers in the data center. Users access the virtual desktops and applications from any client, anywhere, and get almost the full amount of features as if the applications were loaded on their local systems, although they are centrally managed.

In “Emerging Technology Analysis: Hosted Virtual Desktops” Gartner estimates that approximately 15 percent of current worldwide traditional professional desktop PCs would migrate to hosted virtual desktops (inside VDIs) by 2014[4]. This would translate to about 66 million connected devices.

This growth projection for virtual desktops does however come with significant challenges for service providers:

• Ensuring confidentiality, availability and integrity of the data in the host;
• Providing secure access and authentication mechanisms to the virtual desktops.
Considering that today, digital identity theft is one of the most dangerous organized crimes in the digital world, the success of desktop virtualization to provide secure access and authentication to the services is critical. Secure HW based access and authentication tokens can be employed in VDIs to provide secure highways to virtual desktops.

Customers are often afraid of the violation of confidentiality by the cloud operators’ personnel and weaknesses in processes. Customers are looking for a means to remotely control security-related processes, or may demand control by independent third parties for critical changes in the cloud platform. In ideal cases this should be possible without the physical presence of a third party and/or the customer.

IaaS research is underway to enhance existing trusted platform concepts for cloud computing platforms\(^2\),\(^3\). Such concepts would enable the customer to remotely verify that the platform has integrity and could even restrict access to a customer’s data by the cloud provider administrator.

**Client side security**

Cloud computing, in combination with a fast cellular network, will provide a push in mobile computing. Convenience will increase the trend for a thin and lightweight product. Security for the mobile client is key, since such devices are more subject to theft. In a recent study it was shown “that a lost or stolen laptop is worth far more than just the hardware.” The study analyzed 138 cases of lost and stolen notebooks and calculates the average cost to be about $49,000.\(^6\)

**In a recent study it was shown “that a lost or stolen laptop is worth far more than just the hardware.”**

Volume encryption, while avoiding the storage of the key on the hard disk is crucial; storing the key in a certified TPM device is the answer to this problem. Additional TPMs can securely store the login credentials and implementing a two-factor authentication process, consisting of a security token plus a pass phrase, can increase security further.

**Security for future mobility – use cases**

As mentioned above, thin, lightweight mobile clients will benefit from cloud computing services, since the need for local storage is greatly reduced and the computing requirements are shifted into the cloud.

The form factor is critical – On one hand, customers prefer small, light devices, while on the other, the small screen real estate limits productivity. One way out would be the use of public terminals in hotels and airport buildings. Since the application and data are in the cloud – leaving security aside – public terminals can be used directly without installation and setup.

In this scenario, the integrity of the public terminal is critical and can be assured by TPM-based platform security. The mobile client acts as an identity provider for the public terminal after having verified the integrity of the public terminal via an encrypted channel between the public terminal TPM and the client TPM.

**Conclusion**

Security is a key requirement for cloud computing in order to gain broader acceptance. Extended trusted computing concepts give the customer greater means of control and security. They will help to strengthen the trust and confidence, which is urgently needed to make this technology a success.

**Source**


\(^6\) In a recent study it was shown “that a lost or stolen laptop is worth far more than just the hardware.”
Modern Card Application Management System (CAMS)

Complex solutions for multi-application smart cards – A project analysis

By Fabiola Bellersheim, Giesecke & Devrient and member of the Silicon Trust

□ Smart health cards or National ID cards are becoming more and more complex, and their functionality is steadily expanding. In the past, smart cards were used exclusively for the secure storage of credentials. Nowadays, smart cards are more powerful, run multiple applications and can be updated in the field. Not only have smart card capabilities improved, but the associated infrastructure has as well. Smart cards are now used in many online applications, particularly in the area of security products. To optimize the use of cards, information (preferably up-to-date) regarding the user status is particularly important to card issuers or application providers. The CAMS – Card Application Management System – offers a wide range of features and functions for administering and controlling smart cards during their entire lifecycle. Although not every eHealth or eID system requires a CAMS, there is a trend towards flexible and scalable systems for managing cards and post-issuance personalization of applications.

This article will give a short overview of the German telematic infrastructure and the involvement of a Card Application Management System. The general functionality of the CAMS, such as personalization orders, card, application and key management is presented.
The German electronic Patient Data Card (eGK)

The rollout of up to 80 million electronic patient data cards will start in Germany at the end of 2009. It will first be an offline rollout of cards, which carry personal and insurance data of the insured. Probably one year later, the online rollout will follow to enable the insured to check his insurance status online and/or update his data each time he visits a healthcare provider. This might be the case when he moves to another place and his address changes. Instead of issuing a new card the new address data can be updated online.

Later on, applications like eEmergency, ePrescription and eSignature can be loaded as well. Besides being a secure storage of data and applications, the cards function as a secure key to the Medical Network in Germany. As the smart cards will be issued by several different health insurance companies, they need to run a card application management system within their respective computer centre in order to fulfill these requirements. This central element controls every function in the card lifecycle – from production, personalization and issuing to ongoing data maintenance during use, up to blocking the card when lost or taken out of service. As such, it interacts with the health insurer’s patient database management systems, image databases, highly secure key management systems and internal or external certificate services, various personalization providers and patient master data services.

Card Application Management System (CAMS)

The main function of the CAMS is the administering and controlling of various status conditions of smart cards and their applications during their entire lifecycle. These status conditions, which are used in CAMS processes, are reflected in the workflow that must be implemented for issuing and using cards.

The CAMS gathers all necessary data and generates symmetric or asymmetric keys.

Usually the workflow starts with an order to produce, personalize and issue either one single card or several million cards. This order includes the links to the data or archives required for personalization. Orders and data from various archives serve as inputs for the CAMS. Desired additional applications can be added in the first personalization or after the issuance of the card. The CAMS gathers all necessary data and generates symmetric or asymmetric keys, which are necessary for card to card and card to server authentication as well as for encryption of data. Typically, the CAMS also connects to certification authorities and applies for certificates. After completing and compiling the card data sets, all required data are transmitted to the personalization module for further processing. These personalization data sets represent the CAMS output, which will be used for the card production at the personalization site. Data, such as the keys and applications, are installed on the smart card. The CAMS receives confirmation after successful personalization of the card or an error message if the card could not be produced and issued. Then CAMS receives and processes numerous messages such as the issuance of the PIN letter or the first use of the card.

Picture 1: Secure Medical Network Germany (“Telematics-Plattform”)
After successful issuance of the cards, the order is archived in the CAMS order database. The card data associated with this order remains linked to the order, but is stored in the card data database.

A ‘normal’ or successful process execution is easy, but as soon as errors occur as a result of interrupted connections, damaged files, incomplete orders, or unsuccessful personalization because of faulty or damaged cards, etc., the order process becomes very complex. A CAMS enables users to remain flexible, monitors the entire workflow and provides support in monitoring the processed orders and resolving open issues. All orders must be processed without interruption to maximize card or order throughput.

After this initial phase, which is governed by order management, the CAMS monitors all cards issued to date. It provides notification when cards or applications on the cards are no longer valid or when they need to be updated. The CAMS PIP (Post Issuance Personalization) feature enables secure connections to the cards to be established using the keys integrated into the cards when they were personalized.

The secure connection prevents the data transmitted between a CAMS and the card from being recorded by hackers.

PIP can be used to transfer additional data or applications onto the card, although the CAMS must first check to determine whether such an update is possible (size, performance). CAMS can quickly establish a secure channel with the card by connecting to a trust center or certification authority (CA). This secure connection prevents the data transmitted between a CAMS and the card from being recorded by hackers. This feature is also used to block cards that have already been issued. A CAMS offers comprehensive control over the use of cards, even after these have been issued. It is capable of expanding or limiting the use of cards depending on the operational requirements.

These kind of Card Application Management Systems are ideal for driving large-scale and complex multi-application smart card rollouts, which are taking place more and more often in the market.
Fit for ID?

Standards, requirements and solutions, for a ten year lifetime

□ Market requirements for National eID card programs

**EU policy for i2010**

In spring 2005, the European Commission (under EC 14351/2005), published a recommendation for the minimum security framework of National eID card programs. EU refers, in this document, to the ICAO 9303 documents.

The reasons are:
- EC does not have the mandate to publish regulations on National eID card programs. Some member states do not have National ID cards in use, such as the UK;
- Citizens typically use their National ID card document for travel within the EU;
- Infrastructure for IT, PKI and data capturing are in place for the biometric passport programs.

The realization of modern government services in Europe is one of the key pillars of the European Union. The program is called ‘i2010’ and addresses eID / eGovernment services. Within this program the authentication and identification of the citizen play important role, as according to various studies from KPMG, Ernst &Young and McKinsey, eID could reduce corruption, increase transparency, increase services and reduce administration costs.
Today eight of the 27 member states currently have an eID card in use, namely Spain (2006), Portugal (2007), Italy (2006), Belgium (2005), Austria (2004), Finland (2002), Sweden (2005) and Estonia (2004).

A new group of standards were deployed under CEN TC 224, called European Citizen Card (ECC), with CEN 15480 and CEN 14980 in spring 2003. These standards define all relevant elements of IAS (identification, authentication and signing). France [Amin08] and Germany have announced that their new National eID programs that start in 2010 will be compliant with these standards. Other member states, like Poland, UK, Bulgaria, Romania and Czech Republic will follow.

Basic requirements for National eID Cards

The following requirements for National eID cards are common in all running and planned programs:

• **Lifetime:** To last a minimum of ten years in most EU member states;

• **Card interface:** ISO / IEC 14443 is mandatory for travel functions and biometrics according to ICAO 9303, contact-based ISO / IEC 7816 or contactless ISO / IEC 14443 for eGovernment services according to CEN TC 224;

• **Memory:** Size dependant on data sets between 32KB and 160 KB EEPROM. Data needs to be compliant with ICAO-biometrics and -MRZ, CEN 15480 and CEN 14980 IAS, including keys, certificates and PIN. Examples are Belgium, start 2004 with 32k EEPROM, Sweden 2005 with 64k EEPROM, Portugal 2007 with 68k EEPROM, Czech Republic expected mid of 2010 with 144k EEPROM and France expected 2nd half of 2010 with 160k EEPROM;

• **Packaging:** Thin, robust and uniform in quality according to the card specification, the application profile and the card production process;

• **Connection between the chip module and antenna:** Must be qualified to last ten years.

Three smart card configurations are used:

• **Dual Interface, hybrid:** In Sweden since 2005; to be expected in France and Poland in 2010;

• **Contact-based:** Belgium, Austria, Estonia, Finland, Spain, Portugal and Italy in use; to be expected in Czech Republic in 2010;

• **Contactless:** Germany will start the issuance in 2010.

Implementation requirements for ID schemes

Standards are fundamental

International standards are the reference for requirements, which component and card developers have to meet in most of the request for proposals (RFPs) and tenders around the world.

Technical standards are as follows: ISO / IEC 14443, ISO / IEC 7816 amongst others. Application standards are as follows: ICAO 9303, CEN 15480, ISO / IEC 18013 amongst others. Test standards include ISO / IEC 10373, amongst others.
Evolution of technology and the value chain for eID schemes

The applications for Smart Cards in National ID schemes have spread worldwide in the last five to six years. The technology has evolved from contact based National ID Card projects, to contactless Driver License solutions and ePassports, as well as dual interface and hybrid National ID cards. This evolution of ID applications has an impact upon the whole value chain that is involved in the production of eID documents.

Additional mandatory requirements

In addition to the international standards, card manufacturers, test institutes and system integrators have their own individual specifications, which are derived from experience and special cultural and national circumstances. The diagram below provides an overview of these additional mandatory requirements.

Optical quality

The optical quality relates to contactless inlays that are visible in the final document, such as a National ID card or Passport. Passport manufacturers often use complete covers equipped with electronics, otherwise known as the ‘eCover’. These combine a contactless inlay with chip module and antenna, with a conventional passport cover sheet. The optical quality of the eCover must be the same as with the conventional cover, without the embedded electronics. However, new processes in eCover production, such as roll-to-roll instead of sheet-by-sheet, inhibit the screening of sheets according to optical quality. For that reason, keeping the optical quality of a long known product with the new requirement for integration of electronics can provide new tasks for contactless inlay developers. In the area of ID cards, you can find the requirement for thin, white contactless inlays. The reason behind it is the design of the card itself, as the card top layers are often transparent to allow the introduction of new security elements in the card. In addition, the contactless inlays need to fulfill very high expectations regarding the surface quality and cleanliness, to allow a clean card design.
Mechanical robustness

The components for passports and ID cards must be very robust in order to survive ten years in a ‘hostile’ environment. The strength is evaluated by the simulation of mechanical, thermal, climatic and chemical stress according to the experience of the card or passport manufacturer. Conventional packages with metal lead frame and plastic molded chip encapsulation meet these requirements today, but the combination with rather conventional contactless inlay processes pushes this technology close to its limits regarding long lifetime in eID applications. Therefore, package developers are working hard on new module designs and materials to increase the lifetime of modules for use in eID cards and passports. Package developers must close the gap between conflicting directions: minimal thickness and robustness.

Minimal thickness of package / contactless inlay

This requirement covers two wishes of card and passport manufacturers:

- The card surface has a better quality, and passports with electronic covers further resemble conventional documents;
- It enables the integration of innovative security and personalization features in ID cards.

This requirement interferes with the demand for high mechanical robustness but it helps to improve optical quality.

Minimum warpage

This requirement refers mainly to electronic passport production. To enable a smooth passport production process, eCovers need to be as flat as conventional paper or fabric-based covers. However, a laminate made from several layers, with drastically different properties can show curling or ‘warpage’ dependant upon the environmental conditions (e.g. temperature, humidity).

For instance, the combination of plastic foils, metal antenna, cotton cover material and coating with acrylic resins is quite challenging in terms of the demand for a flat eCover.

Solutions

Dual Interface – redundant system

To increase the mechanical stability of eID cards, the redundant electrical connection between the chip and ISO- contacts of the module has been introduced. The effectiveness of this technology has been proven over 10 million times in the field. The development of this product was a major milestone in order to meet customer requirements for high-end applications with very low number of field failure rates.

Thin and robust contactless package FTM8

The FTM8 package is today’s solution to achieve a thin and mechanically robust package for a lifetime of ten years and beyond. Due to its design and materials, it is possible to reduce the package thickness to 260µm and at the same time increase its robustness compared to conventional solutions, such as lead frame and mould packages.

The FTM8 overcomes the limitations of existing packages with a flexible carrier tape, round mould body and ultrathin ICs. It is adapted to the requirements for a highly robust and ultra thin package and contactless inlay.
Hybrid cards
A dual interface function can also be realized with a hybrid solution. This means the contactless and the contact-based IC is separately integrated in one card.

There are several advantages by using a hybrid system:
• Proven technologies;
• High assembly yield;
• Easy process integration by using standard equipment;
• Stronger interconnect from contactless module to antenna (e.g. welding) compared to the interconnect technology dual interface module.

Package innovation for the future

“Thin is not enough, robustness is the key!”

With the increasing daily use of contactless chips in ID applications, card users and issuers are becoming more aware of quality and lifetime issues. This is also a driver for the development and integration of additional security features into chip cards. So what is the benefit of even smaller and thinner modules?

As a response to the market needs, a contactless ID package was created – C.I.S. (Chip in Substrate). The C.I.S. is an ultra thin, but highly robust package which also meets the demand for a 10 year lifetime and beyond. Though having a thickness of only 150–180µm (50% of today’s state-of-the-art modules), the robustness of the module is increased to an extent that exceeds today’s standards. Because of the very small dimensions, C.I.S. improves the optical image of the card and allows more flexibility in card design and graphics. The extremely low resulting prelam thickness allows the use of additional layers for thicker foils or security features. C.I.S. is a package that meets the requirement for ‘invisible’ electronic components.
Software protection goes PKI

By Sven Gossel, charismathics

Companies in the digital world do business by selling digital content, such as intellectual property in the form of software, documents or multimedia files, or communicate by exchange of sensitive information. An essential part of their daily business is determined by digital information – so ‘virtual goods / assets’ extend the traditional resources for the production industry. To protect their technological leadership many companies fight against imitators who copy their products or get advantage by knowing sensitive information.
Which merger exists between sensitive information/intellectual property and the Internet? Information can be passed in different ways via the Internet; for example: internally between headquarters and home-work employees or distribution partners, and externally between a company and banks, payment systems, public authorities, patent offices, research institutes or cooperation partners.

Quite often sensitive information is transported unprotected via the Internet so there is a danger that unauthorized persons might misuse them. So each unprotected communication is accompanied by questions such as: will somebody trap or read along this email? What are trustworthy methods for the protection of information? And in general: how can intellectual property be protected?

A PKI binds public keys and private keys to a user's identity for authentication.

Technology public key infrastructure (PKI)

The encryption market raises such questions and develops answers. A very common authentication method for sensitive information is Public Key Infrastructure (PKI): it is a set of hardware, software, people policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates.

A PKI binds public keys and private keys to a user's identity for authentication. For transferring encrypted information the sender requires the public key of the addressee. In doing so, for the sender it is necessary to make sure that this public key really is the right addressee's key and not a fake key by a fraud.

Therefore a digital certificate securing the addressee's authentication is required. For security reasons the private key must not be disclosed to anybody.

Technology software protection

Another target of imitators is the intellectual property such as software. The market offers software based solutions and hardware based protection solutions. A company's protection strategy depends on several factors such as the level of security, flexibility, usability or additional value. The perfect solution includes these different factors combined.

Due to growing Internet access, more and more pirate copies become available all over the world.

Software vendors spend a lot of time and money for software development. Besides, the protection of their development investment is of huge importance. Due to growing Internet access, more and more pirate copies become available all over the world: and they can be easily distributed. The copy has the same quality than the original has. Even self-assigned dealers sell pirate copies very professionally.
Similar to PKI solutions there are keys in the centre of software protection solutions: the level of security increases from serial numbers to keys used for encryption and decryption. The use of license numbers or personalized serial numbers for software protection is weak. Such a number could be distributed freely over the Internet. Another way is to bind a license to a specific PC. This offers a little bit more protection, but increases support efforts. Pure online solutions requiring permanent online access during use of the software are not practicable for many applications. Only the use of a hardware device offers the highest security level and provides mobile and offline usage of a software product.

A perfect licensing and protection solution for software, documents or media requires:
- A secure hardware to store many licenses, which contain cryptographic keys as well as information like expiration time, network floating licenses or pay per use counters;
- Tools that modify documents or software in such a way, that it can be used without hassle, but never stored unprotected. Therefore, the code or data must be never completely in plain in the computer memory. Furthermore, obfuscation, anti-debugging and locking at crack detection increase security.
- A back office integration to simplify logistics and integration in the sales chain and process.

Security of the future

The best security solution combines both worlds: PKI and software protection. Two German companies have set up a technological co-operation that is aimed at merging such expertise and generate an innovative solution. With this partnership, the DRM product range will be boosted by supporting all major identity management standards.

The upcoming USB stick will combine Digital Rights Management with the added security authentication features of a smart card. This product is designed to address the demands for a unique hardware device to serve both software protection and logical access control purposes at the same time.

The unit will show a high level of security, flexibility and usability. The X.509 certificates will be stored in the safest memory area, the smart card chip, which is embedded in the USB-interface based token. The private key is thus kept secret in a tamper-proof unit. And the middleware handles the PKI security, ensuring a 100% complete integration of worldwide common standards like Microsoft Crypto Service Provider (CSP) and PKCS#11 command set. The new solution will run on all common operating systems such as Windows, Linux, and Mac OS X.

This device adds value and security to companies wanting to protect both their applications and laptops by a single secure modern token.
“On the Internet, nobody knows you’re a dog.” A now-famous cartoon of a dog sitting in front of a computer with the above headline appeared in the US magazine The New Yorker. The message being that, on the Internet, you can pretend to be whoever you want to be. It’s true that as we’ve entered this electronic era, proving our identity has become more challenging. And with the threat of terrorism, identity theft, and worldwide fraudulent activity, it has become more important than ever.

Fortunately, governments around the world are addressing these challenges with a number of programs that bring identity into our electronic world. Electronic passports (ePassports), are now being issued in more than 70 countries, leading the way for more secure identity credentialing worldwide.

The use of smart card chip technology in ePassports secures traveler information and protects the holder’s privacy. Now the use of secure smart card technology has also found its way into new identity credentialing projects, such as national eID, driver license, residence permits, voters ID, eHealth cards amongst others. Through these programs, citizens are able to safely prove and protect their identities when traveling, obtaining eServices, conducting government business, and much more.

Why Smart Card Technology?

When you think of smart cards, you should think of security and trust. Both are vital when proving and protecting identity. A smart card contains a secure microcontroller that securely stores and processes all sensitive information. Two kinds of smart cards are generally used today: contact and contactless smart cards. To read the information, contact smart cards need to be inserted into a reader, whereas contactless smart cards only need to be brought close to the reader’s antenna.

Electronic ID and health cards include features of traditional ID cards like images, personal data, signature and others. However, the inclusion of a smart chip provides additional security and enables secure entry to services and applications.

eID for a secure future

Dietmar Wendling, SCM Microsystems and member of the Silicon Trust
Both contact and contactless smart cards and chips have a wide variety of built-in security protections to prevent the leakage of sensitive information by utilizing on board cryptographic engines. The information inside the microprocessor cannot be tampered with, copied, or altered, which is paramount to ending the counterfeiting of IDs. Smart cards often require the use of a PIN in addition to the presence of the card, adding an additional layer of authentication security. Furthermore, the ability to securely store and process digital certificates and biometrics make these chips ideal for identity credentialing.

Electronic National ID Cards

National ID cards are in use in many projects globally. Many European countries, including Croatia, Cyprus, Germany, Greece, Hungary, Luxembourg, the Netherlands, Poland, Serbia, Slovakia, Spain, have compulsory National ID card requirements. Other countries that have non-compulsory National IDs are Canada, Finland, Iceland, France, Sweden, and Switzerland. Denmark, Ireland, Norway and United States don’t have yet national ID cards.

The trend in countries with National IDs now is to move to more secure and advanced electronic identification (eID) systems. Belgium, Finland, Italy, the Netherlands, Germany and Spain are only some of the countries that have planned or already started to deploy eIDs. Germany’s eID program – which will be launched in autumn 2010 – stands out, as it will use the same contactless smart card technology as those used in the latest generation of ePassports.

Another example: Spain is a recognized leader in the electronic National ID movement, and is making steps to ease the use of these cards and add security for its citizens. The Spanish government started to rollout the so-called eDNI cards (for Documento Nacional de Identificación electrónica) in 2006, and has issued around 14 million cards so far. The eDNI can be used for standard cases like obtaining a driver’s license or a passport, collecting a pension and social security benefits. The integrated smart chip allows for further identity uses to the benefit of the cardholder. With the secure card, Spanish citizens can perform eBanking as well as various eGovernment and eAdministration tasks, like requesting a scholarship, making tax payments, carrying out business with private companies, and digitally signing documents.

As users have been slow to utilize the various functions that the cards enable, the Spanish government has set an initiative to push the usage of the eDNI card by distributing free smart card readers to its citizens, which started in October 2009. The goal of the Spanish government’s eDNI initiative is to overcome this hesitancy and help both citizens and the government experience the full benefits of the National ID scheme.

One more example: To allow a Pan-European use of National ID cards, the European citizen card (ECC) project has been launched. With the challenging goal to enable every European citizen in every European country to seamlessly access services. This will be a longer term initiative, as the required EU directives are not yet implemented, and specifications are still not final. Additionally, existing National eID cards might not be fully interoperable with upcoming requirements.

Nevertheless there is a strong trend to use smart card technology for eIDs globally, as it substantially increases the data security, adds convenience and simplifies administration tasks.

Examples outside Europe are the Ivory Coast voter ID card, Indonesia’s driver licence or Venezuela’s ID card, all based on contactless smart chip technology. Guatemala currently launched its eID program and the United Arab Emirates’ eID card migrates from contact to dual interface chip technology.
eHealth Cards

The concept of identity is extremely important in healthcare, where mix-ups can sometimes mean life or death, also fraud happens every day. Now, much in the same way that smart cards are recognized as ideal for electronic national identity cards, smart cards are being used in many country’s rollouts of eHealthcare cards. Austria, France, Germany, Italy and Portugal are some of the countries that are involved in eHealth initiatives.

The German eHealth program is setting a good example for other countries. The program utilizes smart card technology and readers to make their citizens’ identities and medical information secure and private.

In 2003, the Federal Ministry of Health in Germany introduced a law calling for a new eHealth Card, the elektronische Gesundheitskarte (eGK). Because healthcare in Germany is statutory, the eGK eHealth card will ultimately be issued to more than 80 million citizens. This makes the project one of the largest worldwide.

The eGK health card also contains smart card technology. The important feature of the eGK is that the patients are in control of their data and can choose which data are to be stored on his/her eGK card. This includes for example, medical emergency data, such as blood type, allergies or prescriptions. When obtaining medical services, patients insert their cards into a terminal. The card also contains a photo of the patient to allow a visual identity check – this is to cut down on the fraudulent use of medical services. The medical professional must also insert his/her card (Health Professional Card, HPC) and enter a PIN code to prove identity. Only after these actions, can the medical professional access the information stored on the card.

---

Important personal information is always secure, and patients are in control of their own data.

---

A More Secure Future

Our identity is the most important thing we possess, and as the world has progressed into a more electronic one, identity theft, fraud and other threats have rendered our identities vulnerable. ePassports, with their use of smart card technology, accelerated the world on the path to more secure electronic identities, and other electronic identity initiatives have followed. National eID and eHealth card projects are now ramping up worldwide, utilizing smart card technology to make citizens’ identities protected and private. The future holds more smart card-based eID and eHealth projects, as well more identity programs in more markets. We’ll also see an effort to make these systems interoperable, which is a challenge, but still an attainable goal for the long term. In any event, the trend towards the use of smart card technology for secure identity credentialing is one that is sure to continue, ensuring a more secure future for us all.
Gym access with BIOMATCH™

A case study

By Linda Rosdahl, Precise Biometrics and member of Silicon Trust

By implementing fingerprint recognition, a North European Fitness Chain now offers 24-hour access with limited staff. Members can use any of the chain’s gyms. The extended operating hours let each centre keep a larger member base, while keeping prices down with less staff.

The challenge

The Fitness Chain place high value on offering accessibility in several aspects: Their gyms are accessible 24 hours a day, while the reception is manned only a few hours daily. This keeps member prices down but poses high demands on physical access control. It is therefore important that member cards are tied to the individual gym cardholder to avoid unauthorized use. This is achieved through the use of fingerprint biometrics.

How it works

When new gym members sign up, their photos are taken and a template of their fingerprint is stored on their member cards. When accessing gym facilities, members have to use two factors for identification: both the magstripe on the card and the fingerprint template stored on the contactless card. This, together with video surveillance, establishes a secure line of access and the fitness center can be certain that signed members exclusively visit their gyms.

The result

The very core of the Fitness Chain’s successful business concept and market differentiation is their 24-hour gym access and low-cost membership. The biometric access solution is a fundamental part of this business model.

The service level has also increased since staff are available to support members and are not tied to the reception area when on duty.

Future

With a substantial market share in the region, the Fitness Chain’s goal is to double their business within two years. This means that additional tens of thousands of people in Northern Europe are expected to have 24-hour access to their gyms through biometric identification by 2011.
MECHANICAL SPECIFICATIONS

**PDF**
Full page, bleed 367mm x 224mm (+5mm bleed surround)
2/3 page horizontal 167mm x 151mm (+5mm bleed surround)
1/2 page vertical 129.5mm x 180mm (+5mm bleed surround)
1/2 page horizontal 167mm x 112mm (+5mm bleed surround)
Double inside page horizontal 167mm x 150mm (+5mm bleed surround)
Trim size 129.5mm x 112mm (+5mm bleed surround)
Single inside page vertical 129.5mm x 112mm (+5mm bleed surround)
Spread, gutter bleed 10 mm

**DVD BOOKLET**
Full page, bleed 129mm x 176mm (+5mm bleed surround)

**IMPRESSION**

The VAULT is a quarterly English language magazine that provides topical features as well as edited transcripts of interviews previously available from its audio or video broadcasts or downloads and available on security-news.tc.

**Specifications**

- **CPU**: ARM 32-bit Cortex-M3(72MHz)
- **Program Memory**: 128KBytes Flash
- **Data Memory**: 20KBytes SRAM
- **Host Communication**: USB 2.0 (include USB 1.1)
- **Card Communication**: ISO-14443 A/B, Mifare, Felica, ISO-18092, ISO-15693
- **Card Speed**: 106/212/424/848kbps
- **Reading Distance**: Up to 5cm
- **Contact Card**: 1 contact smart card and 1 SAM (2 IST0816)
- **Input Power**: DC5V , 200mA (USB POWER)
- **Dimension**: 68 * 120 * 30(mm)
- **Operating Temperature**: -20 ~ 60 ℃

**Features**

- Full Support of ISO14443 Part 1~Part 4
- Supports Higher Speed of ISO14443 up to 848kbps
- Supports PC/SC Version, Proprietary Version
- Firmware Downloadable
- Multi PC/SC drivers for contactless and contact
- Use NXP PNS12 chip for Mifare and Felica Protocol
- SDK Available with Sample Application
- CE, FCC and RoHS compliant

**Applications**

- Identification System
- Card Issuing System
- Card Operating System Development
- Electronic Payment System
- e-Passport System

**System Development Team**
DUALi Inc.
505, Samsung Techno-park, #471 Wonechon-dong, Youngtong-gu, Suwon, Gyeonggi 443-380, Korea
Tel: 82-31-213-0074  Fax: 82-31-213-0078  URL: www.duali.com  E-mail: hot sunny@duali.com

**DE-620**

**Full Support of ISO14443 Part 1~Part 4**
**Supports Higher Speed of ISO14443 up to 848kbps**
**Supports PC/SC Version, Proprietary Version**
**Firmware Downloadable**
**Multi PC/SC drivers for contactless and contact**
**Use NXP PNS12 chip for Mifare and Felica Protocol**
**SDK Available with Sample Application**
**CE, FCC and RoHS compliant**

**Features**

- Full Support of ISO14443 Part 1~Part 4
- Supports Higher Speed of ISO14443 up to 848kbps
- Supports PC/SC Version, Proprietary Version
- Firmware Downloadable
- Multi PC/SC drivers for contactless and contact
- Use NXP PNS12 chip for Mifare and Felica Protocol
- SDK Available with Sample Application
- CE, FCC and RoHS compliant

**Applications**

- Identification System
- Card Issuing System
- Card Operating System Development
- Electronic Payment System
- e-Passport System

**System Development Team**
DUALi Inc.
505, Samsung Techno-park, #471 Wonechon-dong, Youngtong-gu, Suwon, Gyeonggi 443-380, Korea
Tel: 82-31-213-0074  Fax: 82-31-213-0078  URL: www.duali.com  E-mail: hot sunny@duali.com
Gemalto’s new Common Criteria certified Sealys eTravel operating system:

- **Speeds up border control** with a reading time of less than 3 seconds* in Extended Access Control (EAC) mode
- **Increases ePassport personalization** throughput by leveraging record writing performance

Available on multiple interchangeable microprocessor platforms, the new Sealys eTravel operating system secures your supply chain management.

Gemalto’s Sealys eTravel operating systems are used in more than 21 national ePassport programs worldwide including Côte d’Ivoire, Estonia, Denmark, France, India (diplomatic), Norway, Poland, Portugal, Qatar, Singapore, Slovenia, Sweden and the United States of America.

**Now you know who’s behind.**

* 2.8 seconds for a full EAC transaction with 48 KB of data, RSA 1024 and extended length (EAC tests in September 2008)