Current Trends in IT-Security

–

Pragmatic Approaches

by

Bernhard Esslinger

–

Deutsche Bank AG, Germany

Article for:

ementor

Abstract:

Early PKI projects fell short in getting the critical mass of users subscribed because they were too expensive and to ambigious. Now, beyond the hype, there is a demand for improvement of security step by step rather than for big projects. Now, linking up existing PKI-islands, using S/MIME, introducing single sign-on and rising awareness are hot topics. Our vision, however, remains a globally applicable PKI, based on digital identity cards. Such an infrastructure can be invented in a private-public-partnership – to the benefit of all, businesses, customers, and governments.

1 PUBLIC KEY INFRASTRUCTURE (PKI): FROM TOO AMBIGUOUS EXPECTATIONS TO PRAGMATIC APPLICATIONS AFTER THE HYPE

Business over electronic channels – most prominently the Internet – requires a secure and efficient way to authenticate. Today Online-Banking mostly uses the build-in security of Web browsers (SSL) to do encryption and additionally uses PINs and TANs. The PIN authenticates the customer, the TAN is required to authorize each single transaction. This delivers security at a very high level and is used by most of our customers today all over the world.

Nevertheless for business over the Internet we are missing an authentication mechanism which is very secure and which can be used not only between the customer and a special application but between the customer and almost all applications from different vendors. The lack of authentication is still one of the major barriers to eCommerce. In principle, a public key infrastructure (PKI) is able to solve not only this problem, but also to ensure authenticity, confidentiality, integrity and non-repudiation of electronic data. PKIs are based on advanced mathematical methods developed in the last quarter of the 20th century. Since the technology is mature and elegant, many PKI projects were initiated during the last 5 years, expectations being extremely high.

Today we have to state that most PKI implementations failed in the sense that they could not get sufficiently many users subscribed. In a PKI each user has a secret key and a piece of information, called the public key, that is published in a directory like telephone numbers in a telephone book. Clearly, one needs access to both, the dictionary and the telephone network, in order to make use of the infrastructure. A major problem is that the PKI hype produced a large number of small infrastructures that are not interoperable. We can compare this to a situation in which many non-interoperable telephone networks exist is parallel, and one has to install a new phone and buy a certain directory for nearly each communication partner. Thus, the benefit for a potential user was too low to get him subscribed, and the investment failed.

The major reason for this development was that each company created its own PKI especially for its needs and that the companies were not willing to give up control on their infrastructure.

As a result, the authentication problem over electronic channels is not solved in practice.

2 CONTINUOUS IMPROVEMENTS IN SECURITY VERSUS THE ULTIMATE SOLUTION – A COST EFFICIENT CORPORATE SECURITY E-MAIL SOLUTION

Although there can be no doubt that a PKI would be most desirable, the experiences mentioned in the first section show that such an infrastructure has to be sufficiently large in order to be useful. We expect years rather than months before such an infrastructure will be in place. In the meanwhile it makes sense to think about small, low-cost steps that can improve security, and to integrate and network these steps.

One such step can be the usage of secure e-mail based on S/MIME (Secure Multi-Purpose Internet Mail Extensions). S/MIME is a standard that describes how encryption and a digital certificate can be combined with the message body and its attachments. Since all major messaging programs and Internet browsers are able to process S/MIME, it can be used in today's infrastructure. If a sender wants to authenticate a message, he simply attaches the (digital) signature and his certificate to the original message. Then the recipient can verify the signature if he has access to the corresponding root certificate. Therefore, S/MIME is suitable for communication between employees of different (large) organizations that know each other and have already exchanged a root certificate on a secure (off-line) channel. Each personal certificate can be traced back to this root. In case the sender wants to encrypt a confidential message, he first asks the recipient for his certificate (this is part of each purely signed e-mail). With the help of the recipient's public key included in the certificate, the sender can encrypt the e-mail. S/MIME has the advantage that it is highly standardized and it can easily be implemented. Furthermore, sender and recipient do not need to have access to a common directory as long as they can trace the communication partner back to a trusted root. However, this limits the usage of S/MIME for private clients.

Another measure to improve enterprise security is the implementation of single sign-on (SSO). Employees log-on to the system only once, from any location (roaming). Whenever the user starts an application, the identification is done internally by the system. The major advantage of single sign-on lies in the fact that one password is sufficient to access all applications an employee should work with. This solves the problem of a large number of different applications that require passwords, which often causes confusion (different passwords lengths, expire-dates,…) and makes people start to use weak passwords constructed by some own rules, which are easy to guess. SSO can be easily combined with the use of PKI.

3 LINKING UP EXISTING INFRASTRUCTURES

As mentioned above, getting the critical mass of users subscribed is the crucial success factor for any (security) infrastructure. Therefore, linking up the large number of isolated enterprise PKIs would increase their benefit by far. Since most companies are not willing to accept that another company administrates their security feature, any hierarchic approach is likely to fail. Pure cross-certification on the other hand needs too many contacts. Linking PKIs via 1:n-contacts like it is done by the European bridge-CA initiative (http://www.bridge-ca.com) seems to be a promising and low-cost way to improve the current situation. The European Bridge-CA is a non-profit initiative, open for any business or government organization willing to fulfill the required standards for PKI. This means, loosely speaking, that each company directory contains a link to the bridge-CA that generates and signs a list of participating root certificates – but still each company is responsible for their own directory. Being a founding member of the European bridge-CA initiative, Deutsche Bank uses the bridge-CA and S/MIME for secure communication with business clients. Deutsche Bank is has built up a very cost efficient centralized S/MIME gateway solution for all employees since 2003. This solution combined with the European bridge-CA links up securely a much wider range of business clients with our secure e-mail system, like Siemens, Deutsche Telekom, SAP, IBM. Current business clients using secure e-mail come from Germany, Austria, Italy, Switzerland, Czech Republic, BeNeLux and Great Britain. We'd be happy if Polish companies join the European Bridge-CA too.

In general, interoperability is the key for increasing the benefit of a public key infrastructure. Whenever a new infrastructure is set-up, the architects should have in mind that their infrastructure uses well established standards. Although specially designed solutions might fully meet the needs of the company we would prefer a standard implementation. Proprietary solutions have the disadvantage that it is either impossible or very expensive to link them up with other infrastructures.

4 PRIVATE-PUBLIC-PARTNERSHIPS

In the B2C-market the situation is quite different from the B2B-sector, in which existing PKIs can be linked. The reason is that in B2C nearly no customer can be validated using a root certificate. Each certificate would have to be exchanged off-line in an expensive process. As a consequence, most customers still do not see a benefit for purchasing a certificate. Without a sufficient number of users, no B2C applications are implemented that work with certificates.

In order to overcome this stalemate, a joint public-private effort seems to be most promising. If, for example, all national identity cards were fitted with a chip carrying a digital certificate,

then it would pay to build applications upon this infrastructure, simply because they could be accessed by all potential customers. Such applications could be financial ones, B2C-eCommerce in general or eGovernment. In particular, financial applications seem to be especially qualified since they do not require the exchange of any materialized good.

It is questionable whether independent infrastructures built by banks or insurance companies for their customers, by online shops within the framework of customer retention programs, or by public authorities and social insurance for their purpose will provide a sufficient return on investment. The advantage of the partnership-approach is that one infrastructure can be used for many different purposes – reducing the total cost and increasing potential benefit for each participant. The main requirement here is interoperability. Together with public partners (tax offices in Germany, German social security institution BfA) Deutsche Bank recently launched the db SignaturCard in Germany, to demonstrated feasibility. The signature created with this smartcard is accepted not only in Deutsche Bank's Online Banking but also at the applications of the other partners in the Public-Private-Partnership. So legally binding contracts can be made over the Internet. There is a big amount of work in progress to achieve interoperability. This working group is open for any participant even outside Germany. From our point of view this can be successful only if it is a European approach.

The main advantage of a PKI associated with national ID cards would be that such a 'big-bang-solution' would not have to face the critical mass problem. Furthermore, a PKI issued under the patronage of the government would raise credibility and increase the likelihood that customers adopt the new technique. But also Private-Public-Partnerships where different institutions are allowed to issue smartcards and certificates are a promising approach if interoperability is achieved.

5 RISING AWARENESS

Security people should have a deep understanding of the underlying business and consumer needs. Technique-centric approaches often have to face the problem that they do not take customer's fears seriously enough. As long as customers do not feel comfortable with a system, they will not use it. But defining and promoting high security solutions is not sufficient. Such an approach can even be counterproductive if customers get the feeling that only high security solutions are really secure – meaning, at least in the public perception, that all other solutions are not secure. In the real world, private homes are not build in the same way as bank safes although both should prohibit thieves from break-in. The same principle

applies in the cyber world: If some experts continue to call everything below a ‘cyber-safe’ not secure, then we will either build applications no-one can afford or stay outside any cyber-house in a much less secure environment. The discussion about class-2 or class-3 smart-card readers is a prominent example.

Therefore, a user should be aware of risks on the one hand, and on the other hand be able to take measures to reduce these risks to an adequate level. Certainly, this is not an easy target. But it does neither pay to ignore all risks and try to keep users in total carelessness, nor to overact on risks. People are most likely to feel uncomfortable with risks they cannot estimate, because they do not understand the underlying process. Thus, rising awareness and giving a basic understanding what is really behind eCommerce applications and security features is a crucial step and needs a joint effort of private sector, public authorities and mass media.

One example for rising awareness by giving a better understanding for IT-security is CrypTool (http://www.cryptool.com), an open-source freeware eLearning software, originally developed by Deutsche Bank in cooperation with universities and private companies. CrypTool provides a structured and playful introduction to classical and modern cryptography. It is used for staff training and university education inside many organizations.

6 CONCLUSION

Overall, we see a large potential for the usage of electronic channels for eCommerce as well as eGovernment if the authentication problem can be solved satisfactory. An infrastructure accepted like a national digital identity card would therefore be most desirable. A joint effort will be needed in order to setup such a solution.

In the meantime, one should concentrate on steps that can improve security with reasonable effort, like making use of S/MIME or implementing single sign-on solutions. Last but not least we must rise awareness for security issues, neither ignoring nor over-emphasizing risks. A sensitive handling of consumer’s fears together with educational advertising of customers and employees will be an important step in order to increase security and consumer confidence.