Smartcards and the Authentication Market

www.sentrypm.com

Brian McKeon 30/Jan/2004
brian.mckeon@sentrypm.com

MK-WP-191101-2

SENTRY PM

Sentry Project Management Pty Ltd

Introduction

The objective of this article is to discuss the suitability of smartcards as authentication tokens.

The discussions look at the requirements of the authentication market, different authentication methods in use, the trade-offs with each, and the suitability of different technologies. The issue of client PC software and (currently) often low security is also considered. “Did I sign what I was shown?”.

Requirements

Authentication allows you access to a service or information. This implies an authentication agent that is controlling access and some authentication method to be used by you. It is possible for you to have multiple authentication methods to the one agent and these may have different strengths. For example a verbal password or PIN originating from a payphone, a verbal password from your mobile phone (caller ID), a verbal password at a bank branch, a magnetic stripe card, or a micro-processor hardware token such as a smartcard. The authentication agent can use these different strengths to allow access to different services. A PIN might be good enough to see your bank balance but not transfer funds to a newly nominated account. The latter would probably require some stronger authentication.

The points of contact that typically are considered are: “Personal” PC; floating PC; PC Kiosk; PDA; GSM phone; non-SIM cell phone; fixed-line phone; branch office; physical access point.

Current authentication methods are: passwords; software PKI certificates; hardware PKI tokens; software symmetric-key authentication; hardware symmetric-key authentication; voice-print authentication; other biometric authentication; verbal authentication e.g. date of birth etc

Most of the above methods require that the authentication agent know the secret that you know. This is a significant problem for e-signature schemes as it is not clear that an e-signature arose from the "owner", the authentication agent or some related entity could also generate your e-signature.

The current solution to this problem are the PKI schemes where you hold a private key and the authenticating entity has your public key, which is different (but related). You can sign documents with your private key and anyone can verify the e-signature with your public key. An authenticating agent is not a bottleneck. The complexity in PKI arises from setting up a system where people know that a given public key is really yours and not someone else's. This is where the Certifying Authority (CA) plays its role. The book “Digital Signatures” by RSA Press is a good reference and the RSA website, www.rsa.com, is a good introduction to PKI.

The security of the private key is critical and PKI schemes such as Identrus (a scheme proposed by the financial industry, see www.identrus.org) and the US Department of Defence Common Access Card (DOD CAC) require that the private keys will be stored in hardware tokens such as smartcards.

The potential solutions for hardware tokens consist of (I) contact tokens such as smartcards, PCMCIA cards and USB tokens and (II) contactless tokens such as contactless smartcards and keyfobs etc. For PC use, the USB token is initially the most attractive however the USB port is not designed for frequent use (specification 1,500 insertion/removal cycles), still requires software installation, and is not always available on desktop PCs or at an inconvenient location on the PC. Smartcards, both contact and contactless, require a reader but they do offer the opportunity for partnering with financial institutions, telecommunication companies and government agencies to issue the card.

Contactless cards are now becoming available that can perform public key operations over the contactless link however the contactless interface complicates security analysis and the trust of these solutions. As these cards have a smaller market than contact cards, which are being introduced by financial institutions, the price of contactless PKI cards will be an inhibitor. The high cost of contactless readers is another inhibitor. The significant countering factor is the ability of contactless cards to allow a single card that could be used for contactless physical access as well as network access. An alternative is to provide a card with a contactless interface for physical access control and a contact interface for logical network access, allowing the use of lower-cost personal, contact-based, readers.

Smartcards

There are a number of other factors that are driving smartcards that make them an attractive option. Card technology is now standardizing and this has some real benefits for issuers. The availability of standard multi-application platforms such as JavaCard and MULTOS provides:

- multiple sources - reliable supply and good cost control as evidenced by the low-cost card announcements from MasterCard and VISA
- standard application development - multiple sources of applications and ability to move applications between platforms with no changes to the application
- independent security evaluation

Most smartcard technology provides good protection of data to the outside world but it is critical that a multi-application card can clearly show that applications are firewalled. The private keys of a PKI application must not be able to be accessed by an attacker using a logical flaw in a loyalty application, for example.

The DOD CAC has settled on the Global Platform JavaCard however present JavaCard implementations require that a card issuer evaluate the package of card applications that will be running on the card. The flexibility of the JavaCard architecture means that the operation of one application is not clearly insulated from another on the card – hence the need to evaluate the package of applications. The JavaCard would make sense if an issuer required to partner with VISA.

The MULTOS platform is not as flexible as the JavaCard platform but this has allowed much clearer boundaries between applications which have allowed a number of implementations to be approved at the highest ITSEC E6 security standard. There are good opportunities to partner with MasterCard and MasterCard issuers.

The availability of smartcards often raises the question of what else can be done with the cards and card manufacturers are always ready to promote a high-tech (high cost) solution. Customers perceiving that they could store significant amounts of data on the card often drive this. It is important to recognize that a smartcard is an ideal authentication token but is not the place to store data.

- Storing some data in card memory costs are about 10,000 times more than storing the data in a host computer.
- To manage loss of a card, an issuer will typically consider that data should be backed-up on a host computer. If so, why not make the host the primary data source
- Moving data to a third party is about 10,000 times quicker if the data is stored on the host rather than fetching it from a card store.

The conclusion is that data can be stored on the card but only put information that you might need due to some inefficiency of networks, security of essential data such as keys, network transaction cost, transaction speed etc

Issues

Although the Internet has driven the application of interface standards such as PKCS#11 and Microsoft CAPI, there is still no common standard at the card interface level. Even Identrus does not apply a standard here. At present smartcard Interfaces are generally proprietary e.g. Schlumberger Cryptoflex, Gemplus Gemsafe, SecureNet Trusted Net. The ISO7816 standards do define such interfaces but do not define a subset as a standard e-signature token. The WAP WIM standard does and this is a useful starting point (see www.wapforum.org). Even if a standard such as the WIM was adopted there is still the problem of lack of card readers at different desired points of contact. The USB token with a "hardened" socket for longer life is a possible solution here.

The PC client is a complicating factor in e-signature schemes. Although a smartcard can provide a secure signing environment, the user is not clearly aware of just what is being signed. A document that is presented on a screen may not be the document that is actually signed. Some business environments attempt to use only evaluated operating systems and applications but this is rare. The problem is that the software running on the PC client cannot be trusted. Some solutions attempt to present the document being signed via another user interface but, as soon as one such solution became commonplace, it could be subverted as for any other PC software. Another mechanism that is proposed is that the user would re-enter their PIN for each signature however entry of the PIN is typically via the (untrusted) PC so this is not a good solution. It is possible to have PIN entry via the card reader but the added cost is often rejected by issuers. And this still does not answer the issue whereby the document being signed may not be the document that was presented.

Microsoft, Intel and others are attempting to strengthen the PC environment via the Trusted Computing Platform Architecture (TCPA) initiative however this is based on software components having signatures that would be checked when the PC was being started. And it is unlikely that the fast pace of change in the PC software industry would be able to live with this constraint. Most PC users are familiar with the Windows messages to do with installation of software without a trusted signature and still proceed with installation.

These client PC weaknesses mean that it is feasible to attack individual users. However issuance of smartcards is still a useful step for a service operator that was concerned about the possibility of widespread fraud with an internet-based network. Present systems based on passwords mean that an attacker can steal the password and perform fraud at a time of their choosing, at an interface point of their choosing. Systems based on smartcards for authentication mean that an attacker must perform any attacks indirectly via client PCs, and at a time when the smartcard is logged-in, a more difficult proposition. Giving the issuer more time to respond to a trend. The size and speed of the attack has been significantly lessened.

Conclusions

- Smartcards are a familiar format for integration of different functions and are likely to be the dominant form factor for PKI tokens for the next 3-7years until contactless technology matures and there is more cross-over between the physical access control market and the network access market.
- The US DOD Common Access Card is a strong driver of identity card standards and solutions.
- The Identrus PKI scheme is a strong contender for B2B e-commerce and mandates hardware tokens such as smartcards however does not define the card edge inteface.
- Smartcards are an easier migration path from existing identity cards, allowing the printing of pictures etc. In some situations they can allow partnerships with major card issuers.
- Authentication tokens are currently of benefit in environments where the client PC software is well-controlled or where an internet service provider with a base of uncontrolled client PCs runs the risk of significant fraud and can use tokens to slow the size and speed of an attack.

If you have any questions on the content of this whitepaper or have suggestions on further topics, please contact Sentry on support@sentrypm.com.