Acoustic Smart Cards
The Emergence of Ubiquitous Security

Rocky Stefano, CEO

http://www.identita.com

Identita Inc.
207 Edgeley Blvd, Unit #1
Vaughan, Ontario, L4K 4B5
Canada
(905) 738-8999

Edition: January 2005

Abstract

With the ever modernising, technology-driven path industrialised societies are following, smart cards are going to play an ever-increasing role in daily life. Whether it is transportation with radio frequency technology, contact chip payment such as EMV or e-purse, telecommunications with SIM cards or identification with biometrics, standards are on their way. An important area that has not been clearly addressed yet is authentication via sound. New smart card technology, ISO 7816 acoustic smart cards, are aimed at this. It features a reader-less interface based on sound waves and an online security model based on dynamic password hashes. This paper discusses the emergence of acoustic smart cards as a potential new standard for authentication, single sign-on, encryption, e-payment and e-commerce.

1. Introduction

Acoustic smart cards have been developed to address the desperate need for authentication in reader-less environments, such as e-commerce Business to Consumer (B2C) situations. Contact cards (magnetic stripe or chip card), contactless cards (radio frequency smart card) and biometrics provide a wide array of possible answers to transactions and access security requirements where readers are available.

However, when it comes to remote online transactions, such as over the Internet or over telephone networks, most of us will rely on a password or a credit card number to access services and to pay.

Logins, user IDs, passwords, pin, and card numbers, all belong to the family of static passwords. They can be easily stolen, guessed, generated or cracked by specific software. They are a weak method of access in that they expose their users to the largest security concern at the origin of fraud: identity theft.

This publicly recognised lack of trust has two consequences:

- It prevents high value transactions and services to be offered by service providers to consumers,

- Consumers legitimately refuse to rely on static passwords when it comes to financial transactions or privacy-related information.

In spite of the above, these static passwords in B2C e-commerce still persist. This is due to cost and operational issues involved in deploying alternative solutions that require the building of new infrastructures, mainly smart card reader fleets, for this type of transactional environments.

1.1 Dynamic Passwords

An interesting alternative lies with dynamic passwords, widely used in access security such as corporate networks. They are usually generated by calculator type tokens and present an attractive security feature: they can only be used once and therefore prevent identity theft.

Despite their various advantages, such as being multi terminal - they can be entered on the keyboard of a PC or key pad of a telephone or any online terminal - their use has been limited to B2B and corporate environments. The main reason is that they have so far been unable to produce an acceptable format for B2C deployment. It is unlikely that consumers will regularly carry a new product which resembles a calculator or large key fob device. In addition, such devices bear a significant cost per user.

1.2 From tokens to ISO 7816 acoustic smart cards

For years, several companies have worked to bring dynamic password functionality into a card format, as this is understood to be the most deployable for consumers.

However, it is the smart card industry that has successfully integrated the dynamic password capability into its ISO format smart cards. This was possible due to two major advances:

- Progress in miniaturisation and autonomy of extra slim batteries
- The ability to convey data via sound waves.

ISO 7816 format smart cards that support autonomous dynamic password generation and universal sound wave data transmission are now a reality.

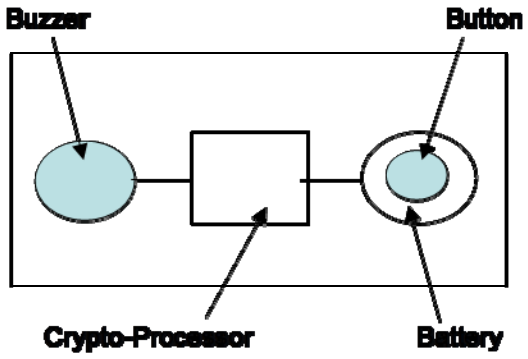
2. Acoustic Smart Card Principles

An acoustic smart card is activated by pressing its pad with one's finger as illustrated in Figure 1.

Upon activation, the chip is powered by a built-in extra slim battery to calculate a dynamic password and attach it with the on-line account number of the registered user.

At each activation, the card generates a new sequence which comprises a static component and a dynamic component. The former is the card user's id, which does not change while the latter is a pseudo random password, which is always different. Activating the card 5 times will generate 5 different passwords. Therefore, as shown in Figure 2, each sequence is unique.

Figure 1. Activation of an acoustic smart card



Online account number	Dynamic password
0000 0000 0000 0001	cefec14f6a8b7af8
0000 0000 0000 0001	273ee481eb293104
0000 0000 0000 0001	8f62910c3024c6a2
0000 0000 0000 0001	467ba050c2d79a00
0000 0000 0000 0001	f279400944ddf20f

Figure 2. Calculation of dynamic passwords by the chip

Once in binary format, the whole sequence is modulated into sound wave frequencies. One frequency is allocated to 0, and another one to 1.

The account number and dynamic password have become a sound which can be very reliably transmitted over the air (Figure 3):

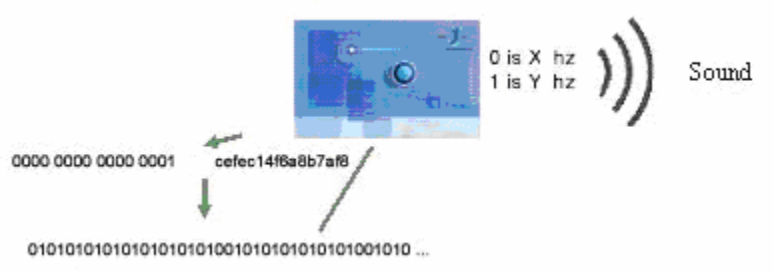


Figure 3. Modulation of account number and dynamic password

The use of sound as a means of transportation for data presents several advantages. The strongest is that any terminal which is equipped with a standard microphone is able to capture the data calculated by the chip and transmit it to a remote server for verification.

3. Acoustic smart card process

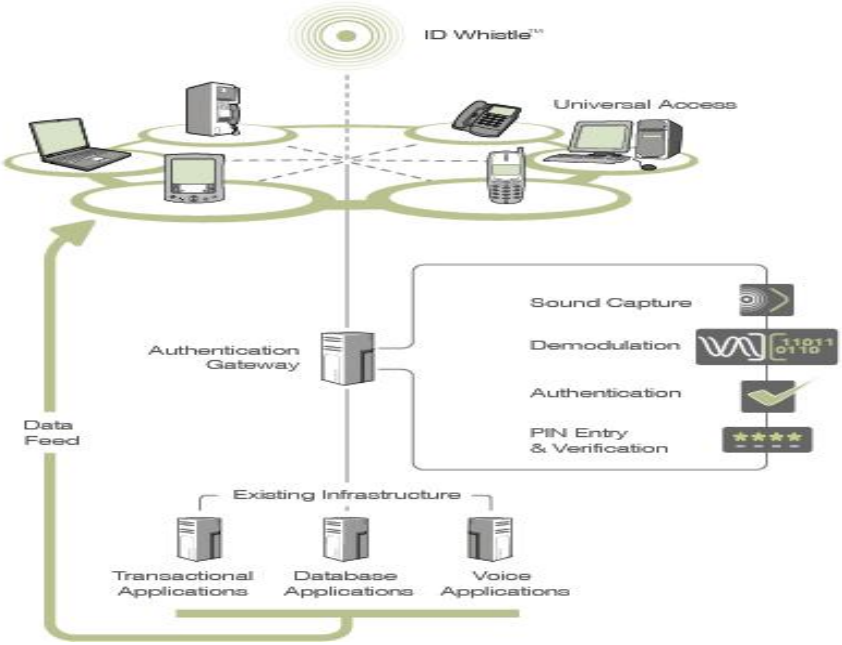
In order to comply with a transaction, authentication is carried out on a PC using an acoustic smart card. The cardholder presents his card in front of the microphone of the PC and activates it.

The sequence generated by the card is captured by the microphone of the PC. Thanks to a plug-in, which was previously downloaded onto the PC by the cardholder, the sound card translates the analog signal back into the initial binary message. This message is then sent electronically through the Internet to an authentication server.

The server has all the necessary information about each account, in order to verify whether the dynamic password sent by a specific card for a specific transaction is an acceptable one.

The authentication process is based on Symmetric Keys held on the card and the authentication server. The whole process as seen in Figure 4 is typically sub-second.

Figure 4. Authentication through PCs



Acoustic smart cards perform authentication through telephones in a smooth and seamless manner. Authentication over the telephone implies the use of an IVR (Interactive Voice Response) system. The IVR system will interact with the cardholder. The analog signal emitted by the smart card will be transmitted directly over PSTN (Public Switched Telephone Network) or GSM (Global System for Mobile Communications) network to the IVR system where it will be translated back into the initial binary message using specific software, and sent to the authentication server for verification.

3.1 Universality

Though acoustic interfaces may at first sight seem “exotic”, it opens a wide door to the smart card industry, as one of the most secure authentication methods available today.

Should the consumer decide to use a PC, PDA, a public telephone or a mobile phone, these terminals are ready to accept authentication based on acoustic smart cards.

Furthermore, although it is difficult to anticipate what the exact capabilities, format and design of new generation terminals are going to be, they will definitely have a microphone to allow voice communication. Acoustic smart cards feature a universal reading mode because it is based on an everlasting capability: the transmission of sound.

3.2 Convergence

If the acoustic smart card's strongest advantage is that it can be used without smart card readers, the parallel is also true. Because of their ISO 7816 format, acoustic smart cards are no different from other cards that are found in our wallets. Their magnetic stripe enables consumers to use them traditionally in reader environments such as an ATM (Automated Teller Machine) or cash register. In time to come, they will also support contact chip transactions in traditional smart card readers. An acoustic smart card is by definition a convergent transactional card ensuring the compliance with new delivery channel requirements while remaining compatible with the traditional ones (Figure 6).

4. Applications

Acoustic smart cards are deemed to have an impact across industries. By providing corporations with a tool to implement an online e-commerce strategy based on cards, acoustic smart cards present the same very appealing features that have made their predecessors so successful in the offline world.

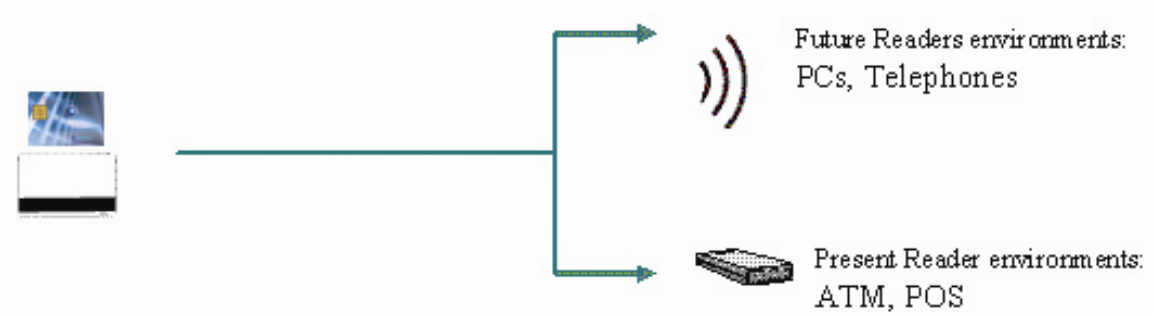


Figure 6. Acoustic Smart Card: a convergent transactional card

If e-commerce is another channel to deliver goods and services, just as retailing is one, it makes sense for existing cards to integrate both. Branding, loyalty and recognition are examples of marketing advantages found in using cards in the delivery of valued added services. In short, acoustic smart cards permit corporations to implement card programs online, just as in their brick and mortar environments which otherwise would have been very difficult to accomplish.

A few examples where acoustic smart cards can contribute to corporations and consumers are given on the following pages.

4.1 e-Banking Cards / e-Payment

The banking industry today relies on PIN/Passwords for accessing consumer-banking services. Given the array of services and the volume of transactions which are involved, the commonly held belief that this level of security access is sufficient is flawed.

Furthermore, Internet banking is still in its early stage of adoption with some banks reporting that only 7 percent of their clientele use online accounts. Banks may protect themselves against fraudulent access by limiting the number of transactions allowed on their websites. This is the case for the few banks that already offer these services. However, increased service means an increased level of secure transaction.

High net-worth individual banking and corporate banking already use the strongest means to authorise access to their accounts remotely. Typically, two factors are used, namely, authentication tokens and digital certificates in smart cards via readers.

It is foreseeable then, that for banks to offer the full spectrum of e-banking and online payment services to their customers, they will have to move one level up in the security ladder.

However, the solutions used to enhance this level of security will probably have to be more operationally acceptable to the public and more easily deployable than the ones used by the two other categories mentioned above.

This is where acoustic smart cards bring a very interesting alternative, by fitting dynamic password generation capability into the existing convenience cards held by consumers. This capability ensures the issuer that the card is present during an online transaction and allows two-factor authentication when combined with a pin.

4.2 Credit Card Payment

What is true for e-banking payments is also true for credit card online payment. Attaching a dynamic password to an online credit card number solves fraudulent issues related to credit cards. By authorizing an online transaction, telephone order or internet order only when the dynamic password has been verified in real time by the issuing bank or a trusted third party, the merchant and the banks are certain that the transaction is initiated by the genuine card holder. The latter is also reassured that no one else can use his card number fraudulently, because only the card he possesses can generate the acceptable dynamic password.

What makes people confident about a transaction in a shop/ATM is that the card has to be present physically to be able to perform the transaction. It protects people from identity theft. When making an online payment today, the card does not have to be present; a card number and expiry date will suffice. It is called a card non-present transaction. Acoustic smart cards allow online credit card transactions to be card-present transactions in every circumstance.

4.3 Telecommunications Card

Even though financial institution applications are the most straight forward applications for acoustic smart cards, the telecommunication industry also has a lot to leverage on.

Not only do acoustic smart cards permit telecom operators to offer secure access to calling card and pre-paid long distance services, they also make it more convenient, since users avoid having to key in too many numbers on the keypad of the telephone.

Secure, faster and more convenient access through phones enables marketing strategies to be implemented in a similar way to those applied by credit cards in targeting specific market segments. It also enables telecom operators to widen the scope of services and the level of value-added services they can sell online.

Acoustic smart cards can also be implemented in a call centre environment thus improving productivity in authenticating, controlling and delivering services or support to callers. Authenticating callers in less than a second can significantly save toll and operator costs since the average process can take 30 to 60 seconds, if not minutes.

4.4 Citizen Card (e-Government) and Health card

Apart from transaction-based operations, acoustic smart cards find wide applications in the area of online identification cards.

The privacy of data is paramount in e-government and online public services. The intimate nature of information, which may be health related or citizen related, requires definite identification before it can be accessed. Any initiative in these fields will encounter the issue of satisfying the privacy and confidentiality requirements by requiring a reliable method of authentication. However, as with most services targeted at a wide consumer base, adoption will be dependent on the level of ease and convenience offered in delivering the service.

Take the example of online access to medical records files. There is no doubt that with the recent HIPAA and PIPEDA legislation coming into effect, medical confidentiality will have to be monitored in a rigorous way. But real adoption will only happen if practitioners and patients are given maximum accessibility to the appropriate files in order to use them efficiently, be it from their home, clinics or overseas/remote areas. This is even truer in emergency cases. Only then will the system be fulfilling the service for which the whole infrastructure has been initially implemented. Once again, acoustic smart cards offer an attractive alternative in these fields.

4.5 Click and Mortar Customer Relationship Management (CRM)

In addition to delivering services, acoustic smart cards can be effectively implemented as a tracking tool in Customer Relationship Management programs. Strong loyalty policy can be implemented by issuing acoustic smart cards to better integrate behaviour pattern monitoring of consumers on-line and off-line.

The improvement of CRM performance will be achieved because of the increase in the volume of secure transactions, due to the use of the card in any circumstance. Secure multi-channel selling is also a tremendous issue for CRM. Acoustic smart card functionality encompasses exchanges and purchases over web sites, call centers and in the retail stores.

4.6 Remote Corporate Network Access

Acoustic smart cards can also be implemented as a means of mobile authentication by corporations that want to provide their executives, managers, clients or suppliers a modern, secure and mobile access device to their corporate networks. Today, a road warrior really isn't a warrior at all. At best, they are carrying critical intellectual property with them on a notebook that can be easily stolen and the information compromised. With an acoustic smart card, every aspect of the laptop would be protected. Logons to the machine and applications on the computer would not function without the use of the card. Files and folders would be encrypted with the card as well and would require the card's acoustic signature including the user's personal pin to decrypt them. Lastly, it would be entirely possible for an organization to require their end users to use their acoustic smart cards to actually turn their laptops on. Much in the same way a BIOS password functions, an acoustic smart card could enable the same functionality.

4.7 Corporate Logon and Single Sign-On Technology

Today, although there is a move to solidify account management and multiple user accounts and passwords on different systems, corporations are wary of providing that "single" login name and password which could potentially give a successful hacker access to all the accounts and programs that a particular logon account has access to. By providing an acoustic smart card associated with a pin we can still consolidate all of these accounts yet offer the safety, security and peace of mind that a card and a pin is still required to access all the specific applications. Our acoustic signature becomes the end user's credentials and their pin is the key to unlocking them.

4.8 Encryption

Successful e-business means more interconnectivity with suppliers and customers than ever before. The benefits can be large, but e-businesses are also potentially far more vulnerable. The right security technology is a must. This means a customised IT security structure that guarantees the confidentiality, authenticity, integrity and traceability of information.

E-mail messages and attachments can be encrypted and/or authenticated with a digital signature. The level of security is comparable to that of documents posted in a secure mailbox and prevents interception or manipulation of your data.

4.9 Digital Rights Management

Today, we have witnessed the virtualization of all media types. From audio to video and entire libraries of books; today's e-culture has changed the way information is accessed and stored. While this cultural evolution is exciting it brings with it several problems. Protecting an original work from being copied and redistributed on the internet is a challenge to say the least. With acoustic smart card technology any DRM system can be tied to the card as a method of authorizing proper use, copy and distribution of any form of copyywritten material.

5. Conclusion

Although the acoustic smart card industry is in its infancy, they could well revolutionize the way we deal with authentication, encryption and authorization in the near future.