Open and Closed Contactless Technologies – Opportunities and Risks in Access Control Applications

Contactless technologies are now an integral part of modern access control applications. More and more users appreciate the level of security, suitability and economic efficiency offered by contactless technologies. Nevertheless, many consumers are still not familiar with some of the most important technical features of Proximity and Smart Card technology, nor with the impact that open or closed technologies and a system's architecture can have on future system expansion.

This article provides an introduction into the background of contactless technologies. Application demands always vary case by case – from simple solutions with low security requirements all the way up to applications with the highest security needs. However the variety of Proximity and Smart Card options available now enables designers to create solutions, in which price, performance and a system's security level are readily customised to individual application requirements.

Advantages of contactless technologies

Users of access control, time management and ticketing applications typically are attracted to the user-friendliness of contactless technology. It offers comparatively low maintenance costs, a longer operating life and reliability in harsh environments – and particularly, hardiness in the presence of dirt or contaminants and resistance to vandalism; conditions that invariably compromise sensitive contact technologies (magnetic, contact chip/dongle). Finally, the high transaction speeds, secure data transfer and convenience of carrying a single device to access multiple applications have become powerfully attractive features engendered in the latest Smart Card Technologies operating at 13,56 MHz.

Proximity and Smart Card technologies

Proximity is typically understood to be a low frequency technology, operating in the 100-500 kHz (mainly 125kHz) bandwidth. Conversely, products using a 13,56 MHz frequency are typically categorized as contactless *Smart Card*. With both frequencies, one finds a variety of tags, e.g. keyring, fob, coin format as well as cards. *Proximity* technology, with read-only function, is still the most common used technology in contactless access control applications today. However, this technology is not based on an ISO standard. *Smart Card* products, in contrast, have grown increasingly popular in access

control because they frequently comply with international standards (ISO14443, ISO 15693), offer enhanced security and provide access to multiple applications.

Profound differences in memory capacity and data transfer speed

Both technologies invariably deploy chips possessing a chip identification number and programmable memory. The serial identification number of a chip is a random, unchangeable and unique number programmed by chip manufacturers. Because of its uniqueness, this serial number is ideally suited for access control and time management applications, since tag holders may be easily yet securely assigned privileges against these numbers.

Memory capacities differ significantly between market offerings of Proximity versus Smart Card. Proximity memory usually tops out around 2 Kbit whereas Smart Card memory can now be as high as 64 Kbit. Because of its larger memory Smart Card can offer significantly enhanced security features, enabling its deployment in the most sensitive settings and applications (e.g. biometric queries). Additionally, Smart Card technology also supports multi-applications; the same card can be used for numerous different applications such as access control, ticketing and other payment or identification queries.

The differences in data transfer speed are even greater between Proximity and Smart Card. The market currently offers Proximity products with transfer rates as high as 4 kbps (kilobit per second). In striking contrast, Smart Card can transfer data as fast as 848 kbps, enabling comparatively huge data transfers in very short intervals.

Open and closed solutions

The most crucial factors (after price) when considering access control or time attendance solutions is the security threshold a site requires and supplier flexibility for providing future system enhancements. System architects must carefully scrutinize any long-term consequences in their selection of a particular contactless technology.

Many chip manufacturers build chips used in transponders and reader devices. Conversely, some other card and reader manufacturers develop proprietary chip technologies utilized only in their own products. This arrangement is referred to as a closed technology; the company is the source for both the chip technology and the assembled cards and readers. Inevitably, this means the products of other manufacturers will be prohibited from interfacing with that technology. Therefore, when system architects integrate products from such suppliers, any future site enhancements or expansions will inevitably be limited to technology produced by the original

manufacturer. Both the architect's and customer's freedom to choose supply sources by quality, functionality or price will have been lost.

Conversely, with Open Proximity technologies, reader and tag manufacturers freely source the chips of other chip suppliers for their own products. If a system works with ID number identification or a user is provided the authority to program their own readers and cards, then those consumers will also be free to choose from whom they purchase their cards and, when expanding their systems, from whom they purchase additional readers.

With Smart Card technology, the chip suppliers are rarely bound in proprietary contracts with the manufacturers of readers and tags. The intention of the existing ISO14443 and ISO15693 standards on 13,56 MHz technology is to ensure the compatibility of chips among different suppliers. Applications working with unique serial number identification particularly benefit most by integrating one of these standards because doing so ensures the availability of a wide range of technology alternatives from the numerous reader and transponder manufacturers who build to those standards. Therefore, when employing Smart Card serial number identification, there is a risk in choosing a non-ISO compatible technology, or deploying a card and reader solution from a provider whose technology constrains your freedom to choose supplier sources in the future.

If the data required in a Smart Card identification system is to be stored in memory, it is also important to learn whether that system's programming authority will reside with the end-user or remain with the card- and reader-supplier. This must be evaluated case-by-case; weighing whether a coding units cost combined with the impact on personnel resources leverages any advantage over the cost, convenience – or inconvenience – of a supplier-maintained archive and authority.

Growing market offers many possibilities

Product development among the world's most important chip technology manufacturers clearly demonstrates a trend toward 13,56 MHz Smart Card technology. Many of them offer ISO-compatible chips, enabling contactless technology consumers to choose among a wide variety of alternatives. Furthermore, increased competition in the chip market has significantly lessened differences in price between Proximity and Smart Card technologies. Particularly telling with Smart Card technology is its growing prevalence in access control, time attendance and payment applications. Notwithstanding cost concerns, it remains a system architect's responsibility to choose the most suitable technology for a given setting, avoiding solutions that might constrain his or his client's independence in a future expansion or system modification.

Idesco product portfolio for all application needs

Founded in 1989, Idesco Oy is both a pioneer and leading innovator in contactless technology and RFID. Idesco specializes in readers, reader modules, cards and tags based on various proximity, smart card and UHF technologies. Its products are deployed globally in access control, factory automation, asset marking and public transportation settings.