iCLASS®

Optimized to make physical access control more powerful, iCLASS® 13.56 MHz read/write contactless smart card technology provides versatile interoperability and supports multiple applications such as biometric authentication, cashless payment and PC log-on security.

Encrypted Communication

The communication between an iCLASS reader and card is encrypted using a secure algorithm so the transaction between the card and reader cannot be "sniffed" and replayed to a reader. The encryption protocol uses a combination of diversified keys, unique 64-bit card serial numbers and mutual card and reader authentication.

Capability to Add Other Applications

The iCLASS chip not only stores HID access control information, it also has memory space available for other applications. iCLASS cards are currently available with 2k bit, 16k, and 32k bit memory capacities, and depending on the amount of memory available and the number of memory areas, iCLASS cards can serve as multi-application credentials that can be used for many purposes.

Since the memory can securely store any kind of information, applications for iCLASS include biometrics, secure computer/network authentication, health record management, time and attendance, digital cash (cafeteria & vending) and many, many more.

Imagine an affordable, single-card, contactless solution that allows you to not only read data securely and quickly, but also to securely write data to the card for many applications.
Patch Antenna

US Industrial, Scientific, and Medical (ISM) band from 902-928 MHz

\[
\frac{\delta f}{f_{\text{res}}} = \frac{Z_0}{2R_{\text{rad}}} \frac{d}{W} = 1.2 \left( \frac{d}{W} \right)
\]
RF Identification

Secure, Sensitive, Low Power Identification Devices

RFID involves contactless reading and writing of data into an RFID tag's nonvolatile memory through an RF signal. Low frequency RFID devices typically consist of a transponder (tag) and reader.

To help you reach the extensive vertical markets that rely on RFID, we offer a complete line of contactless products. Our transponders and readers operate within the 100 to 150 kHz and 13.56 MHz bandwidth ranges. Our RFID chips are suitable for the smallest devices and require few external components, lowering your system costs. Rugged architecture with excellent noise suppression increases reliability and usability in both indoor and outdoor environments.

You can choose from a broad range of read or read/write devices, available as identification ICs on die on wafer, die in tray, die on tape, or micromodule, to complete transponders in plastic packaging with reader, tag and development library.

Key Features

- **Standards based** — You can rely on the fact that Atmel complies to industry-specific standards, such as ISO 11784/85 (FDX-B and FDX-A) for agriculture and ISO 14443 for public transportation applications.

- **Flexible modulation coding options** — The chips can be easily configured to suit a broad array of modulation schemes: FSK, PSK, ASK, Manchester, Bi-phase, NRZ direct coding, and more.
There's a reason why Tadiran batteries were chosen for E-ZPass, the world's best known RFID application

When millions of motorists across the United States flash their E-ZPass at toll booths, they are totally unaware that this pioneering RFID technology is powered by Tadiran lithium batteries. Manufacturers of these electronic toll tags require a battery capable of delivering years of safe, reliable and trouble-free performance under the toughest of environmental conditions, as automotive windshields are subjected to extreme heat, vibration and rapid temperature changes. So they naturally turn to Tadiran.

Tadiran lithium thionyl chloride batteries were also selected by Awarepoint for the medical industry’s first 24/7 RFID asset tracking system. Awarepoint required a battery capable of withstanding extreme autoclave and chemical sterilization temperatures, so they chose Tadiran lithium thionyl chloride batteries that deliver unrivaled performance under the most extreme environmental conditions.

Tadiran batteries feature the highest energy density (1,420 Wh/l), high capacity, and are uniquely able to withstand extreme temperatures (-55°C to +125°C), and offer 20+ year service life due to extremely low self-discharge (less than 1% per year). These batteries are also designed with unique safety features that protect the cell against extreme temperature, pressure, puncture, shock and vibration.

If your RFID application calls for an extended-life battery, don’t settle for anything less than Tadiran, as no one can match our experience and our proprietary manufacturing methods.

Would you like to complete our application questionnaire?
Optimized to make physical access control more powerful, iCLASS® 13.56 MHz read/write contactless smart card technology provides versatile interoperability and supports multiple applications such as biometric authentication, cashless payment and PC log-on security.
**Read/write Functionality for Multi-functional Memory Applications**

iCLASS® was specifically designed to make access control more powerful, more versatile, and more secure. All radio frequency data transmission between the card and reader is encrypted using a secure algorithm. By using industry standard encryption techniques, iCLASS reduces the risk of compromised data or duplicated cards. For even higher security, the card data may also be protected with DES or triple DES encryption. Multiple securely separated application areas are each protected by 64-bit diversified read/write keys which allow complex applications and provide for future expansion.

Security mechanisms such as mutual authentication and encryption are efficiently combined with fast processing and data communication, resulting in transaction times of less than 100 milliseconds for a typical secure e-purse transaction.

**Proven, Reliable Technology**

Offers extremely consistent read range. Unaffected by body shielding or variable environmental conditions.

**Thin**

Can be carried with credit cards in a wallet or purse. Use with a strap and clip as a photo ID badge.

**Photo ID Compatible**

Print directly to the card with a direct image or thermal transfer printer. Slot punch vertically for easy use.

**Long Life**

Passive, no-battery design allows for an estimated minimum 100,000 reads.

**Durability**

Strong, flexible, and resistant to cracking and breaking.

**Options:**

- Magnetic stripe
- External card numbering (inkjet or laser engraving)
- Vertical slot punch
- Custom artwork (text or graphics)
  
  (Please see “How To Order Guide” for a description of the options and associated part numbers.)

**Warranty**

Lifetime warranty. See complete warranty policy for details.

**Base Part Numbers**

- 2000 for 2k bit (256 Byte) card
- 2001 for 16k bit (2k Byte) card with 2 application areas
- 2002 for 16k bit (2k Byte) card with 16 application areas
- 2003 for 32k bit (4k Byte) 16k/2+16k/1
- 2004 for 32k bit (4k Byte) 16k/16 + 16k/1.

**Description**

13.56 MHz contactless smart card.

---

**Features**

**Specifications**

**Typical Maximum Read Range***

- R10 2.0-3.0” (5.0-7.6 cm)
- R30/RW300 2.0-3.5” (5.0-8.9 cm)
- R40/RW400 2.5-4.5” (6.3-11.4 cm)
- RK40/RWK400 3.0-4.0” (7.6-10.1 cm)

*Dependent upon installation conditions.

**Dimensions**

2.127” x 3.375” x 0.033” max. (5.40 x 8.57 x 0.084 cm)

**Weight**

0.20oz (5.7 g)

**Card Construction**

Thin, flexible polyvinyl chloride (PVC) laminate.

**Operating Temperature**

-40° to 158° F (-40° to 70° C)

**Operating Humidity**

5-95% non-condensing

**Operating Frequency**

13.56 MHz

**RF Interface**

As suggested by ISO/IEC:

- 15693 read/write
- 14443B mode - 106 kbps
- 15693 mode - 26 kbps
- 14443 B2 mode - 212 kbps

**Transaction Time**

<100 ms typical

**Baud Rate**

- 14443 B2 mode - 212 kbps
- 15693 mode - 26 kbps

**Memory Type**

EEPROM, read/write

**Multi-application Memory**

2k bit (256 Byte) card – 2 application areas
16k bit (2k Byte) card – 2 or 16 application areas
32k bit (4k Byte) card – 16k bits in 2 or 16 application areas plus 16k bits user configurable.

**Write Endurance**

Min. 100,000 cycles

---

* When customizing cards using Re-Transfer Printers that fuse images to the surface of the card by applying heat and pressure (such as the Fargo HDP5000) we recommend the use of composite cards, which are better able to withstand the higher application temperatures.

---

**HID iCLASS Contactless Smart Card presentation - YouTube**
About 70¢/Card

Fargo FlexIS FPIXT QTY:100

Item#: FPIXT / Brand: fargo
Retail Price: $7.00

Sign in or Register for Guaranteed Lowest Pricing

BUY NOW

Description

Fargo FlexIS FPIXT QTY:100 Description

Specifications

Related Items

CR80.30 (30 Mil) White PVC Cards
- Qty. 500
Item#: 81754
Retail Price: $54.00
Our Price: $38.00

Check to Add

Fargo Backdrop Stand 86102
Item#: 86102
ISO/IEC 15693-1:2010
Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 1: Physical characteristics

Media and price

<table>
<thead>
<tr>
<th>Format</th>
<th>Price</th>
<th>Language</th>
<th>Add to basket</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDF</td>
<td>CHF 50.00</td>
<td>English</td>
<td></td>
</tr>
<tr>
<td>Paper</td>
<td>CHF 50.00</td>
<td>English</td>
<td></td>
</tr>
</tbody>
</table>

Abstract

ISO/IEC 15693-1:2010 defines the physical characteristics of vicinity cards (VICCs). It is used in conjunction with other parts of ISO/IEC 15693.
ISO/IEC 15693 : Vicinity cards

ISO 15693 is an international standard for « Vicinity Cards », i.e. contactless cards operating at the 13.56 MHz frequency, with a maximum operating distance of 1 to 1.5 metres.

The standard

These documents are Final Comittee Drafts. They are not the official documents (which must be purchased from ISO or from your national standardization agency), but are very close to them.

- **15693-1** : Physical characteristics
- **15693-2** : Radio frequency power and signal interface
- **15693-3** : Anticollision and transmission protocol
- **10373-7** : Test methods
Identification cards -
Contactless integrated circuit(s) cards -
Vicinity cards

Part 2:
Radio frequency power and signal interface

1 Scope

This part of ISO/IEC 15693 specifies the nature and characteristics of the fields to be provided for power and bi-directional communications between vicinity coupling devices (VCDs) and vicinity cards (VICCs).

This part of ISO/IEC 15693 shall be used in conjunction with other parts of ISO/IEC 15693.

This part of ISO/IEC 15693 does not specify the means of generating coupling fields, nor the means of compliance with electromagnetic radiation and human exposure regulations which can vary according to country.
6 Power transfer

Power transfer to the VICC is accomplished by radio frequency via coupling antennas in the VCD and in the VICC. The RF operating field that supplies power to the VICC from the VCD is modulated for communication from the VCD to the VICC, as described in clause 7.

6.1 Frequency

The frequency \( (f_c) \) of the RF operating field is 13,56 MHz ±7 kHz.

6.2 Operating field

A VICC shall operate as intended continuously between \( \text{H}_{\text{min}} \) and \( \text{H}_{\text{max}} \).

The minimum operating field is \( \text{H}_{\text{min}} \) and has a value of 150 mA/m rms.

The maximum operating field is \( \text{H}_{\text{max}} \) and has a value of 5 A/m rms.

A VCD shall generate a field of at least \( \text{H}_{\text{min}} \) and not exceeding \( \text{H}_{\text{max}} \) at manufacturer specified positions (operating volume).

In addition, the VCD shall be capable of powering any single reference VICC (defined in the test methods) at manufacturer’s specified positions (within the operating volume).

The VCD shall not generate a field higher than the value specified in part 1 of ISO/IEC 15693 (alternating magnetic field) in any possible VICC position.
7 Communications signal interface VCD to VICC

For some parameters several modes have been defined in order to meet different international radio regulations and different application requirements.

From the modes specified any data coding can be combined with any modulation.

7.1 Modulation

Communications between the VCD and the VICC takes place using the modulation principle of ASK. Two modulation indexes are used, 10% and 100%. The VICC shall decode both. The VCD determines which index is used.

Depending of the choice made by the VCD, a "pause" will be created as described in Figures 1 and 2.

<table>
<thead>
<tr>
<th>Modulation Index</th>
<th>t1</th>
<th>t2</th>
<th>t3</th>
<th>t4</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td>6.0</td>
<td>2.1</td>
<td>0</td>
<td>0.8</td>
</tr>
<tr>
<td>10%</td>
<td>3.0</td>
<td>0.8</td>
<td>4.5</td>
<td>0.3</td>
</tr>
</tbody>
</table>

The clock recovery must be operational after \( t_4 \) max.

\[ y \geq 0.05 \, \text{(a-b)} \]
\[ hf, \, hr \geq 0.1 \, \text{(a-b)} \, \text{max} \]
7.2 Data rate and data coding

Data coding shall be implemented using pulse position modulation.

Two data coding modes shall be supported by the VICC. The selection shall be made by the VCD and indicated to the VICC within the Start of frame (SOF). See 7.3.

8 Communications signal interface VICC to VCD

For some parameters several modes have been defined in order to allow for use in different noise environments and application requirements.

8.1 Load modulation

The VICC shall be capable of communication to the VCD via an inductive coupling area whereby the carrier is loaded to generate a subcarrier with frequency $f_s$. The subcarrier shall be generated by switching a load in the VICC.

The load modulation amplitude shall be at least 10 mV when measured as described in the test methods.

Test methods for VICC load modulation are defined in International Standard ISO/IEC 10373.
8.4.1 Bit coding when using one subcarrier

A logic 0 starts with 8 pulses of 423,75 kHz ($f_c/32$) followed by an unmodulated time of 18,88 µs ($256/f_c$). As shown in Figure 10.

![Figure 10: Logic 0](image)

A logic 1 starts with an unmodulated time of 18,88 µs ($256/f_c$) followed by 8 pulses of 423,75 kHz ($f_c/32$). As shown in Figure 11.

![Figure 11: Logic 1](image)
Passive tags are mostly meant to identify inexpensive objects, and must thus, submit to an economic asceticism that eschews such luxuries. Conventional batteries are far too bulky and expensive to be considered. A conventional radio transmitter or receiver, with the complex and expensive oscillators, mixers, and synthesizers is out of the question. Only inexpensive, low-speed circuitry and simple logic are permitted to us if the tag is to be powered by the pittance of microwatts available at several meters distance from a reader. Instead of a proper transmitter, a switch to change the impedance presented to an antenna must suffice. A single IC is usually the only electrical component to be placed on the tag, and thus, this circuit must be a custom design solely for its specialized application. The expense of creating such an application-specific integrated circuit (ASIC) implies that only large volume usage can provide an economic return to the company responsible for it.

Between these extremes lie semipassive tags, possessed of a battery but bereft of a radio. To date, such tags have typically been constructed for specialized applications with moderate volumes, such as auto tolling, and use fairly conventional fabrication and design approaches, with special attention to duty cycle just as for active tags.

A greatly simplified diagram of the electrical constituents of a passive tag is depicted in Figure 5.1. The radio signal at around 900 MHz from the reader is converted by the antenna into an alternating current, from which the tag must extract both power and information. The tag must then interpret the resulting data, possibly requiring writing data to nonvolatile memory, and modulate the load presented to the antenna in order to change the backscattered signal returning to the reader.

How is power to be extracted from the high-frequency radio signal?  
How can we simultaneously acquire whatever data the reader has sent?  
How do we send back information to the reader?  
How is the resulting chip designed and fabricated?  
How is a completed tag assembled from the chip and other parts?

http://rfid.net/basics/passive/137-uhf-rfid-tags
When the RF input becomes positive, the first diode turns off and the second (output) diode turns on (Figure 5.8). The charge that was collected on the input capacitor travels through the output diode to the output capacitor. The peak voltage that can be achieved is found by adding the voltage across the input capacitor, which we found above, to the peak positive RF voltage and subtracting the turn-on voltage of the output diode:

$$V_{\text{out}} = V_{\text{in}} + V_{\text{RF}} - V_{\text{on}}$$

In the limit where the turn-on voltage can be ignored (e.g. when the input voltage is very large), the output DC voltage is double the peak voltage of the RF signal, from which fact the circuit derives its name. The actual output voltage depends on the amount of current drawn out of the storage capacitor during each cycle, that is on the value of the load resistance (not shown here).

To produce higher output voltages, we can provide additional stages of multiplication to produce a Dickson charge pump. A two-stage configuration is shown in Figure 5.9; in the case of ideal diodes with negligible turn-on voltage, the output would be four times larger than the peak RF input voltage. In general, for N stages we find:

$$V_{\text{DD}} = 2N(V_{\text{in}} - V_{\text{on}})$$

A reasonable approach to estimating the number of stages is to extract an equivalent resistance from the load, given the total power calculated above:

$$V_{\text{in}} = \frac{V_{\text{out}}}{2N}$$

where the input voltage is adjusted to produce the requisite load voltage from equation (5.7). Roughly speaking, the largest resistance that can be matched to the antenna is $Q$ times larger than the radiation resistance of the antenna. For a typical dipole-type antenna, this value is 10–50 Ω, so the largest equivalent resistance that can be optimally matched is around 5 kΩ, assuming the limits on matching mentioned above. (Higher values can be used but at some sacrifice in bandwidth.) We can thus, adjust the number of stages in the charge pump to provide about the right equivalent resistance for the value of $Q$ we expect to achieve in matching.

Several weaker but non-negligible effects are important in arriving at a final design. The area of the diodes has a weak (logarithmic) effect on the turn-on voltage and thus on the efficiency, so one is tempted to make the diodes large. However, the diode capacitance grows linearly with the diode area, and since the equivalent resistance of the charge pump is fixed (by the power and voltage targets, as described above), as the diodes are made larger the capacitor starts to draw a substantial reactive current. The capacitance is also voltage dependent (increasing noticeably as the diodes are turned on), and the variation in capacitance degrades the performance of the matching network, particularly for narrow band, high-Q networks. A charge pump with more stages has smaller capacitance variations because the peak voltage across each diode is closer to the turn-on voltage.
Once we have obtained a low-frequency voltage proportional to the RF power, we need to extract information from it. If the data is, for example, PIE coded, what we need to figure out is how long the signal remains high between pulses: a long RF-high period represents a binary-1 and a short RF-high period represents a binary-0 (see for example Figure 3.7). One simple approach is shown in Figure 5.14. The output of the envelope-detect circuit is directed to a trigger circuit, with an optional current source or other provisions to set the threshold for the trigger. The trigger thus changes state at the beginning of an RF-on pulse, and resets an integrator, which then starts accumulating charge while the voltage is high. The output of the integrator grows linearly with time as long as a signal is applied to its input; on the next rising edge of the RF signal, the integrator output is large if the power was high for a long time, or smaller if the RF-high time was short. That output is applied to a discriminator, which then outputs a 1 or 0 depending on the duration of the RF-high period, just as desired.

Recall that a radio receiver typically includes filtering to select the desired channel, and minimize noise and interference from other transmitters. A passive tag has no such luxurious amenities. Since there is no local RF oscillator or mixer, there is no conversion operation to allow for channel filtering: all received signals at any RF frequency are converted to baseband by the charge pump. The tag antennas provide some frequency selectivity but will generally cover at least the 902–928 MHz ISM band for United States operation. Thus, any transmission in this band, including not only other RFID readers but cordless phones, wireless networks, cell phones and cell basestations, alarm systems, badly grounded spark plug wires, and any other nearby RF radiators all blast right into the IC’s receiver.

Talking Back

Passive tags use modulation of the power scattered by the tag antenna to reply to the reader. In our earlier discussions of backscatter modulation, we imagined a very simple scheme in which the IC simply interrupts current flow through the antenna to modulate the scattered power (see for example Figure 3.15). Let’s take a closer look at how one might modulate the behavior of the antenna and what the consequences are. The three questions we need to address are:

1. How much scattered power can we send back to the reader?
2. What effect do we have on the power absorbed by the (IC) load?
3. How hard is it to implement a given scheme?

Let us first examine the limiting cases of the loads that can be presented to the antenna. These are shown schematically in Figure 5.15. Note that in this and subsequent diagrams, we show an antenna connected to a ground node, which is defined to be at zero voltage. In practice, most tag antennas are symmetric and there is no easy way to define a true “zero” voltage, but the principles are the same, and it is much easier to discuss the problem in this single-ended configuration, rather than the actual balanced or differential connection.

In normal operation, we shall assume that the IC is matched to the antenna: that is, the antenna and IC have been adjusted so that the largest possible power is delivered to the IC. We shall momentarily specify in more detail what this implies about the behavior of the system.

Figure 5.13: Circuit for Extracting RF Envelope and Average Power from Incoming RF Signal; After Curty et al.

Figure 5.14: Simple Demodulation Circuit for Pulse-interval-encoded Data; After Karthaus and Fischer.
Passive tags use modulation of the power scattered by the tag antenna to reply to the reader. In our earlier discussions of backscatter modulation, we imagined a very simple scheme in which the IC simply interrupts current flow through the antenna to modulate the scattered power (see for example Figure 3.15). Let’s take a closer look at how one might modulate the behavior of the antenna and what the consequences are. The three questions we need to address are:

- How much scattered power can we send back to the reader?
- What effect do we have on the power absorbed by the (IC) load?
- How hard is it to implement a given scheme?

Let us first examine the limiting cases of the loads that can be presented to the antenna. These are shown schematically in Figure 5.15. Note that in this and subsequent diagrams, we show an antenna connected to a ground node, which is defined to be at zero voltage. In practice, most tag antennas are symmetric and there is no easy way to define a true “zero” voltage, but the principles are the same, and it is much easier to discuss the problem in this single-ended configuration, rather than the actual balanced or differential connection.

**Figure 5.15: Elements of Simple Backscatter Modulation Schemes. Single-ended Antenna Connections are Shown for Simplicity.**
Tag IC Overall Design Challenges

Now that we’ve touched on the problems presented by the interface to the physical world, let us turn our attention to the logic, memory, and supporting systems that make the tag responsive to its environment. A rough functional layout of a typical passive tag IC is depicted in Figure 5.23. Around half the chip area is taken up by the logic needed to implement the relevant protocol: about 50,000 transistors for an 18000-6C (EPCglobal Class 1 Generation 2) IC.

We’ve looked at the key RF-related challenges in Sections 5.2–5.4 above. The remainder of the chip operates at baseband frequencies and is generally similar to conventional mixed-signal design. However, there are some special challenges peculiar to the RFID world.

The first challenge is, of course, that of cost. The cost of a chip is dominated by its size if yield is reasonably good. Modern IC manufacturing facilities use 200-mm- or 300-mm-diameter wafers. A standard 200-mm-diameter silicon wafer offers a useful area of about 30,000 square millimeters. (This is a bit less than the total surface area: the region within about 3 mm of the wafer edge is usually not useful for processing.) If a single IC has a useful area of around 1 mm², we can get about 22,000 chips from a wafer assuming that 90% of the chips are good (that is, the yield is 90%). In small volumes, it costs about $1000 to purchase a processed wafer, so the cost of these ICs would be roughly $0.05 per chip. The use of 300-mm wafers increases the initial cost for masks, but in high volume the ongoing cost is reduced by 30–40% vs. 200-mm wafer. The actual numbers are influenced by such commercial issues as volume pricing—I don’t pay $1000/wafer if I buy several hundred wafers—but it should be apparent that at 1 square millimeter, the chip cost is a substantial fraction of the $0.05 tag cost goal promulgated by such organizations as EPCglobal. It is imperative to keep the chip as small as possible to minimize IC cost.

![Functional Layout of a Tag IC (After Stewart).](image)
The HID iClass family of 13.56 Mhz Contactless readers and cards was introduced over a decade ago with the primary goal of eliminating some of the security concerns that existed with the older 125Khz Proximity technology. The state-of-the-art iClass technology supported new features such as mutual authentication and Triple DES encryption to improve security and reduce the possibility of card duplication.

The contactless cards themselves utilize an embedded chip technology called "PicoPass" from a French company by the name of Inside Secure http://www.insidesecure.com/. These chips basically consist of a small EEPROM memory and a simple state machine controller that is used to interact with a card reader using the ISO 14443B and ISO 15693 protocols.

All data stored on iClass cards is secured by Authentication Keys. A Key is basically a password used to protect data from being read or changed without authorization. The iClass cards and readers use 64-bit keys (56 key bits plus 8 parity bits). One authentication key is used to protect each of the card’s Application Areas. Two encryption keys are used to support TDES encryption of the transferred data.

Since its introduction, numerous articles have been written by HID and other security industry experts who have all described the technology as "Extremely Secure" and "Difficult to Clone". Those kinds of words are usually interpreted by the hacking community as an open challenge to explore the technology and to identify and exploit any vulnerabilities that are found to exist. As a result, within the last year at
Heart of Darkness - exploring the uncharted backwaters of HID iCLASS™ security

Milosch Meriac, meriac@OpenPCD.de

Abstract—This paper provides detailed information on iCLASS™ reader and key security. It explains the security problems found without revealing the extracted secret keys (DES authentication Key and the 3DES data encryption key for iCLASS™ Standard Security cards).

The chosen approach of not releasing the encryption and authentication keys gives iCLASS vendors and customers an important headstart to update readers and cards to High Security mode in order to stop attackers from forging, reading and cloning iCLASS Standard Security cards.

This paper also explains, how Standard Security and High Security keys were extracted from a RW400 reader without leaving visible traces.

One of the biggest don’ts in card security is to design a card security system which allows copying cards without forcing the attacker to use a card emulator. Out of no apparent reason this implementation flaw exists for HIDs iCLASS cards: Knowing the authentication key results in being able to copy the cards - decrypting 3DES encrypted content is not necessary for that.

IX. RECOMMENDATIONS

- Standard Security Mode is dead. Switch immediately to High Security by asking your local HID vendor for programming cards that will upgrade your Standard Security system to High Security and rotate your existing cards to the new keys at a trusted location only. Make sure that your vendor tells you the new High Security key.
dissipation, and small masses ($10^{15}–10^{17}$ kg), these devices are well suited to such explorations. Their dimensions not only make them susceptible to local forces, but also make it possible to integrate and tightly couple them to a variety of interesting electronic structures, such as solid-state two-level systems (quantum bits, or qubits), that exhibit quantum mechanical coherence. In fact, the most-studied systems, nanoresonators coupled to various superconducting qubits, are closely analogous to cavity quantum electrodynamics, although they are realized in a very different parameter space.

Quantized nanomechanical resonators

The classical and quantum descriptions of a mechanical resonator are very similar to those of the electromagnetic field in a dielectric cavity: The position- and time-dependent mechanical displacement $u(r,t)$ is the dynamical variable analogous to the vector potential $A(r,t)$. In each case, a wave equation constrained by boundary conditions gives rise to a spectrum of discrete modes. For sufficiently low excitation amplitudes, for which nonlinearities can be ignored, the energy of each mode is quadratic in both the displacement and momentum, and the system can be described as essentially independent simple harmonic oscillators.

Spatially extended mechanical devices, such as those in figure 1, possess a total of $3^A$ modes of oscillation, where $A$ is the number of atoms in the structure. Knowing the amplitude and phase of all the mechanical modes is equivalent to having complete knowledge of the position and momentum of every atom in the device. Continuum mechanics, with bulk parameters such as density and Young's modulus, provides an excellent description of the mode structure and the classical dynamics, because the wavelengths (100 nm–10 mm) of the lowest-lying vibrational modes are long compared to the interatomic spacing.

It is natural to make the distinction between nanomechanical modes and phonons: The former are low-frequency, long-wavelength modes strongly affected by the boundary conditions of the nanodevice, whereas the latter are vibrational modes with wavelengths much smaller than typical device dimensions. Phonons are relatively unaffected by the geometry of the resonator and, except in devices such as nanotubes that approach atomic dimensions, are essentially identical in nature to phonons in an infinite medium.

It is an assumption that quantum mechanics should even apply for such a large, distributed mechanical structure. Setting that concern aside for the moment, one can follow the standard quantum mechanical protocol to establish that the energy of each mode is quantized: $E \subset (N \otimes \frac{1}{2})$, where $N \subset 0, 1, 2, \ldots$ is the occupation factor of the mechanical mode of angular frequency $w$. The

Figure 1. Nanoelectromechanical devices. (a) A 20-MHz nanomechanical resonator capacitively coupled to a single-electron transistor (Keith Schwab, Laboratory for Physical Sciences). (b) An ultrasensitive magnetic force detector that has been used to detect a single electron spin (Dan Rugar, IBM). (c) A torsional resonator used to study Casimir forces and look for possible corrections to Newtonian gravitation at short length scales (Ricardo Decca, Indiana University–Purdue University Indianapolis). (d) A parametric radio-frequency mechanical amplifier that provides a thousandfold boost of signal displacements at 17 MHz (Michael Roukes, Caltech). (e) A 116-MHz nanomechanical resonator coupled to a single-electron transistor (Andrew Cleland, University of California, Santa Barbara). (f) A tunable carbon nanotube resonator operating at 3–300 MHz (Paul McEuen, Cornell University).