

## Despite the Hype, Microchip Implants Won't Deliver Security

Martin Reynolds

Exaggerated media reports suggest that surgically implanted microchips can secure buildings and even help trace kidnap victims. Don't believe it.

## NEWS ANALYSIS

---

### Event

On 16 July 2004, media reports stated that more than 100 employees of the Mexican attorney general's office have received surgical implants containing tracking microchips that control access to secure physical locations. The reports follow an interview in which the attorney general stated that he has had a microchip implanted in his arm to allow access to a crime database and to make it possible for law enforcement authorities to locate him if he is kidnapped.

### Analysis

A microchip surgically implanted in the human body could be used to maintain access control for secure locations. The microchip transmits radio frequency identification (RFID) signals to a reader, and the user opens doors and accesses computer systems simply by placing the body part containing the implant close to the reader. The implants cannot be lost or forgotten, and the devices are difficult to remove and almost impossible to counterfeit.

However, the media reports that the Mexican implants could help locate kidnap victims are almost certainly overblown. The devices' deliberately short range makes them nearly useless for this purpose. The media reports may stem from a clever "disinformation" campaign to discourage kidnapping, which is widespread in Mexico. Gartner believes it is unwise to rely on these devices as a kidnap victim locator — and particularly unwise to announce which body part contains the implant.

Implanted devices are highly unsuitable for virtually all security purposes. Only the body part containing the implant — not the entire employee — is required for access permission, so this approach will not work against people willing to commit bodily harm.

Gartner believes contactless smart cards represent a better means of physical access control than microchip implants. These devices have already been deployed in Japan and Hong Kong as a substitute for cash, allowing users to purchase goods and services such as public transit subway fares. Unlike many other technologies, contactless smart cards cannot be counterfeited, and they are appropriate as a replacement for existing access control systems. They could substitute for the implant devices, and the Mexican government may well shift to nonimplanted technology.

**Recommendations:** Do not implement surgically implanted microchips as a security mechanism. When preparing for new access control systems, consider contactless smart cards instead.

**Analytical Source:** Martin Reynolds, Gartner Research

### Recommended Reading and Related Research

- "U.S. Department of Defense Smart-Card Implementation" — The U.S. military has successfully deployed smart cards for physical security on a large scale. **By Gregg Kreizman and Clare Hirst**
- "Management Update: Prepare for RFID Disillusionment" — In the short term, RFID cannot live up to the promises made for this technology. **By Jeff Woods**

(You may need to sign in or be a Gartner client to access the documents referenced in this FirstTake.)

## REGIONAL HEADQUARTERS

---

Corporate Headquarters  
56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

European Headquarters  
Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

Asia/Pacific Headquarters  
Level 7, 40 Miller Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

Latin America Headquarters  
Av. das Nações Unidas 12.551  
9 andar—WTC  
04578-903 São Paulo SP  
BRAZIL  
+55 11 3443 1509