

Testimony before the California Research Bureau

Radio Frequency Identification Document Advisory Panel

October 31, 2007

Sacramento, California

**Submitted by Infineon Technologies North America Corp.
Dr. Joerg Borchert, Vice President, Chip Card & Security ICs,
Meg Hardon, Senior Policy Director**

Thank you for inviting Infineon to share its experience and expertise surrounding the use of RFID in identity documents before this panel today. We are grateful for the opportunity to offer comments on data security in the context of ID document systems, as well as our views on the policy issues surrounding the use of RF-enabled ID documents.

As many of you know, Infineon is a global semiconductor company with its US headquarters here in California, providing silicon solutions to the automotive, industrial and communications sectors. Our chip card division, which Dr. Borchert heads in the United States, works with government and private entities worldwide to provide security for ID cards, computers, wireless phones, televisions and set-top boxes, among other products.

We are engaged in this hearing, as we have been engaged in the discussions and debates over proposed legislation here in California, because we believe that RF-enabled technology is unfairly targeted as privacy-invasive. We also believe that legislating technology standards is ultimately destructive of innovation in security technology and privacy protections, and eliminates the many positive benefits RF provides to eliminate counterfeit and fraud.

Infineon has been an active proponent of developing technology-neutral standards for the creation, issuance and management of identity documents. We believe standard protocols for protecting data and privacy are critical to building effective and secure ID card programs. And we do not think that banning/restricting the use of a single technology produces a more privacy-protective ID system.

In addition to our efforts here in California, we have supported the development of best practices for chip-enabled ID cards through the Smart Card Alliance, engaged federal policymakers to initiate government-wide ID management standards, and joined efforts like that of the Center for Democracy and Technology, to develop a set of guidelines or standards that apply to the entire ID management process.

We believe that public confidence in ID documents issued by either the public or private sectors is dependent upon appropriate levels of security to protect the data, and in the case of RF-enabled documents, protect the transmission of the data. There are a wide range of public benefits to RF-enabled ID documents, including reduction of fraud, improved access to information, increased efficiency of transactions, and greater privacy than in existing ID documents.

Dr. Borchert has worked in this field for more than 20 years and will discuss the specifics of ID card data security and provide some examples of applications where technology solutions address vulnerabilities.

Joerg Borchert:

Types of RFID Technologies

Singling out RFID technology as particularly privacy-invasive is the wrong approach to developing best practices around the use of RF technologies on ID documents. There are many RFID TECHNOLOGIES and you cannot compare a tag for identifying a cow with an ID credential developed for the soldier in the field to access his computer. Even the acronym RFID used to widely describe the many RF-enabled documents is misleading because it presumes one kind of technology.

You can see in this illustration that the radio frequencies used in ID applications span a range and include technical characteristics that allow more or less security to be embedded in the RF-enabled chips. Secure RF applications utilize the 13.56 Mhz range for access control and logistics. The International Standards Organization has established standard protocols for the frequency ranges, with those in the shortest read ranges having a higher degree of security.

This graphic presentation of where applications for RF-enabled ID documents fall on the scale of security required and investments made in security, shows that the demand for security increases with the value of the data.

Evolution of Security in ID Documents

The degrees of security in ID products you have just seen are representative of an evolving and complex society where we must authenticate ourselves to access services to which we have rights. Fraud and counterfeit are huge costs to both the public and private sectors in revenue, but also in security. Misrepresentation, theft and ID theft will continue to be threats and companies like Infineon are in a constant race to raise the bar against criminals and terrorists. This is what leads to innovation in document security.

During the past two decades we have seen ID documents evolve from including a signature, to secure paper, to secure ink, pictures, watermarks, holograms, laser engraving and barcodes. The latest innovation is RF security controllers which can bind an electronic biometric to a picture on a card to limit the production and use of fake IDs.

That said, no ID technology is perfect, and any ID document has to establish trust with the card holder in order for that ID to be an effective tool for the issuer and the holder.

Vulnerabilities and Countermeasures

You can see on this slide the list of potential vulnerabilities that are associated with RF-enabled ID Cards, as well as the impact those vulnerabilities can have on the card holder and issuer. In the far right column you will see the solutions to overcome those vulnerabilities. To protect a card's chip from being read surreptitiously, the card can employ basic access control and/or encryption. In the case of the US ePassport, it does both. To prevent tracking a person by the ID number associated with their RF-enabled chip card, the card can employ a random number generator.

However, not every RF-enabled card or application requires every available security measure. The basic premise of ID security, regardless of technology employed, is that the level of protections on the card are commensurate with the level of sensitivity of the data and or the application/use.

Applications

I would like to share with you two examples of RF-enabled ID documents and how they evolved to employ RF for improved efficiency and security.

Counterfeit travel documents have always proved to be a security problem for nations seeking to prevent criminals from entering their country. Well before September 11, 2001, the International Civil Aviation Organization, responsible for the standardization of travel documents worldwide, had taken on the task of reducing the ability of criminals to create counterfeit passports. Their aim was to build another security protocol that would check the authenticity of a passport presented for inspection.

Over a number of years, ICAO developed standards for embedding a secure Contactless microcontroller into passports. The exact data from the data page of a passport would be copied onto a chip, and the chip could be read to compare the data on the passport and the chip. Because passports contain so much personal information, the levels of security and protection required around the chip and the transmission of the data are quite high. They include encryption and basic access controls. While ICAO set the fundamental standards, each nation has also been able to innovate and add additional features or security. The US ePassport was enhanced with additional security to increase the privacy protections of passport holders.

The second application I would like to point out is the electronic driver's license. Many nations have chosen to secure the driver's license with a secure Contactless chip. The motivation for adding an RF-enabled chip to a driver's license have included prevention of counterfeiting, protection of privacy and efficiency in driver's license administration. Other benefits can also be considered, like enabling e-government. An element of some of the e-DLs under development today call for a personal PIN to allow the holder to unlock the chip before it is read, giving access control to the citizen.

Closing Remarks and Questions

There is no absolute security in any ID documents, but there is BETTER security. Societies and communities seeking to protect the security and privacy of their members must stay ahead of the criminals and adversaries and technology is a vital tool to that effort.

The State of California and the chip industry are in the TRUST business when it comes to ID documents. The success of RF-enabled or other secure documents are going to depend upon the public trust.

Also, government or private entities issuing secure IDs are doing so to reduce fraud and all the costs fraud imposes upon citizens and users.

In concluding, I suggest we need to all ask ourselves the following questions.

1. Can California allow itself to fall behind the curve by legislating limits on technology innovation, and setting in stone standards for use in government ID documents?
2. Is CA willing to close out the option for employing the most protected ID documents available?

Thank you to the panel for your attention and I look forward to any questions you may have of me or Ms. Hardon about Infineon and RF-enabled chips for ID documents.