



# Consulting Services

## Smart Card Security Investigation Service



Analysing fault behaviour in the laboratory

### Your Business Risk

Whether you are building technology or thinking of using new technology in your business, there are always risks to manage. Introducing more security than you need is expensive and can damage your business. But failure to recognise and manage the risks can be fatal for your business and your reputation.

Selecting the right technology and processes to do the job is critical. Achieving the right balance is fundamental to business success.

### Supporting Your Business

Our Smart Card Security Investigation Service applies the skill, experience, innovation and tenacity of the SiVenture analysts to provide support to our clients for the efficient production and implementation, or procurement and integration, of smart card chips, and software.

Involving us in the early stages of your programme will help you to be more productive with:

- Direct improvements in the product's ability to resist hostile attacks by third parties - both physical and logical attacks
- Improvements in the time-to-market of products by early analysis to reveal weaknesses before the final stages of production or implementation
- Development of new defences based on real methods used by attackers
- A risk management strategy based on balancing technical risks and diverse countermeasures in appropriate parts of the operational system



## Flexible Approach

SiVenture uses a range of methods for analysing the strength of chip security, including:

### > Differential Power Analysis

DPA is a non-intrusive method for analysing the power profile of a smart card chip. As it executes its algorithms we can extract the secret keys. This method can be effective with both symmetric cryptography (e.g. DES) and asymmetric cryptography (e.g. RSA).

### > Fault Induction & Differential Fault Analysis

Faults do not always cause an operation to fail - some types of fault can be used to break the security of a product while it continues to operate. For example: if a cryptographic process, such as encryption, can be made to fail in certain ways, then applying mathematical techniques to a correct and an incorrect answer can quickly discover the key.

### > Electromagnetic Emanations Analysis

EMA is a non-intrusive method for analysing the power profile of a smart card chip. As it executes its algorithms, it is sometimes possible to monitor the emissions and derive secret keys.

### > Physical probing and circuit modification

The secret data on a chip may be stored in a secure memory such as EEPROM. However, to be of use, the data must be sent via a bus to some other part of the circuit. A simple attack uses a Focused Ion Beam to connect a large metal pad to each line of the bus, to enable the data to be read or altered. Defences include obscure bus routing techniques and shielding. Our advanced attacks and analysis help to build better defences.

## About SiVenture

For more details about SiVenture and our complete portfolio of smart card consulting and laboratory services, please contact us at: [www.siventure.com](http://www.siventure.com)

Unit 6  
Cordwallis Park  
Clivemont Road  
Maidenhead  
Berkshire  
United Kingdom SL6 7BU

T: +44 (0) 1628 6513 66

F: +44 (0) 1628 6513 65