



**How to secure Video  
Slot Gaming Machines  
using VaultIC™  
Security Modules?**

**driving trust** **inside**  
SECURE

[www.insideseecure.com](http://www.insideseecure.com)

## TABLE OF CONTENTS:

<b>Introduction</b> .....	<b>3</b>
<b>1 What is the architecture?</b> .....	<b>3</b>
1.1 Video slot machines .....	3
1.2 How it works? .....	4
<b>2 Why security is needed?</b> .....	<b>5</b>
2.1 Because it deals with money... ..	5
2.2 Because of operations on Network... ..	5
2.3 Because sensitive information travels on the network .....	5
2.4 Because it deals with valuable data... ..	5
2.5 Attacks .....	6
<b>3 VaultIC solution</b> .....	<b>7</b>
3.1 Inside the VaultIC Module... ..	7
3.2 Example of implementation .....	8
<b>4 Conclusion</b> .....	<b>9</b>
Definitions and abbreviations .....	10
Document Revision History .....	10

## INTRODUCTION

In April 2007 the Nevada Gaming Regulators approved International Game Technology's server-based gaming system following field testing of 20 machines. Since then, the commission has approved other slot makers with server based technology.

The casino gaming industry is undergoing a significant migration from stand-alone slot machines and table games to advanced systems based on modern networking technology. Because it is centrally managed through a single console, casino owners can use a main computer to instantly control and connect all the machines on a casino floor, while tailoring each one to a player's preference. It offers players a way to play the games they want at any location without having to switch machines. It also saves casino owners money on personnel and staffing costs.

But building a network creates security needs, increasing threats of cyber-attacks, fraud and loss of privacy.

VaultIC Security Modules - based on highly secure microcontrollers used in Banking ID markets - can respond to these requirements.

Depending on the size of the data which needs to be secured, the VaultIC Security Modules Family is composed of ATVaultIC200, ATVaultIC400, ATVaultIC420, ATVaultIC440 and ATVaultIC460 can provide an appropriately sized product.

## 1. WHAT IS THE ARCHITECTURE?

### 1.1 Video slot machines

A slot-machine is a gambling machine operated by inserting coins into a slot and often by pulling down on a long handle. Nowadays slot machines are mostly video slot machines, meaning with a video screen (usually touch screen) and a push button to operate it. These computerized machines embed EEPROM where the slot game(s) are stored. Video slots are a modern innovation, with no moving parts at all - instead a graphical representation of one appears on screen. Since the player is essentially playing a computer game, the manufacturers are able to offer more interactive elements, such as advanced bonus games and advanced video graphics.» (source : Wikipedia)

Figure 1-1. Video Slot machine



## 1.2 How it works?

### 1.2.1 Updating games to machines

More than just a video game, server-based video slot machines (also called downloadable slots) are now generic terminals connected to a central server, where different slot games can be downloaded. Slot managers have the ability to remotely change the machine's games, denominations or bonus payouts from the central server, instead of locally by a technician. The «new» slot game is written in the EEPROM. Sometimes all games will already be present in the EEPROM but not enabled. In this case the manager, depending on the rights he has, can change the game by a selection mechanism. This server-based system lets the casino have the ability to switch a game in a few seconds, rather than buying a new slot game.

### 1.2.2 Getting information from machines

In addition to the game configuration, since the slot machine is connected to a local network, casinos can set up management systems in order to log machine events, monitor and report in real-time player-tracking information.

Figure 1-2. Example of Casino Management System



The network architecture permits slot makers to offer different systems with new services, such as slot-accounting and analysis, database marketing, cashless wagering, ticketing... and real-time reporting of all data collected from slot machines. Also, other peripheral devices can be connected to the network (video surveillance, fire-alarm systems...).

The sensitive nature of the data means that security should play a major role in this system. Moreover, the heavy traffic network requires authentication mechanisms.

# 1. WHY SECURITY IS NEEDED?

## 2.1 Because it deals with money...

Casinos make and handle money, a lot of money. Obviously it increases the interest of cheats, thieves, and other malevolent people. Casinos should be vigilant in order to protect their profit and their business. Security guys, video surveillance and complex anti-fraud systems are now part of any casino.

## 2.2 Because of operations on Network...

More than just preventing the system against attackers, authentication mechanisms are mandatory to securely enable Network operations such as:

- **Select / change game:** One early usage of server-based gaming is an easy and fast way to change the game on the slot machine, according to player's preferences: the server has a copy of all the «approved» games so the casino can «push» the game (including graphics and buttons) on to the machines without having to send a technician out to replace the EEPROM. It also offers players a way to play the games they want at any location without having to switch machines. The gaming board would still have to approve the games.
- **Update software applications:** Another security requirement is updating the control software of the Casino Management System (adding services, fixing bugs, upgrading user interfaces...). So the Casino has to identify the machine to update.
- **Download data from machines:** When remote data is required by the server (slot-accounting and analysis, player-tracking, log events...), security mechanisms must be in place to protect the operations and the players. The ability to mutually authenticate and open up secure communication channels between the transmitting and receiving elements of the Network is essential to enable the above types of operation.

## 2.3 Because of operations on Network...

Casino Management Systems include different software modules such as cash desk, table games, player-tracking, surveillance... that deal with private or sensitive information.

For instance, Cash Desk software supports all the Cash Desk Transactions, Slots Transactions, Customer Accounts, credit management... It also permits connections to other software modules such as Player-Tracking.

Player-tracking software manages data concerning the amounts played by Casino Members, such as member profile with detailed history log (gaming date, game, cash in, cash out, win/loss, hours played...), or member search with money won/lost criteria, statistics...

Statistics can also be extracted from slot machines: win, handle, drop, jackpots paid, hopper fills, win percentage, games played... per machine or group of machines.

Customer profiles are also stored in the machines. All this confidential information transits on the Network so it must be secure.

## 2.4 Because it deals with valuable data...

Every game is unique because every game contains various Intellectual Property elements such as graphics, specific code or data, algorithms... This IP is sensitive because it belongs to the game developer and cloning it is considered as fraud. Slot machine makers have to protect this data.

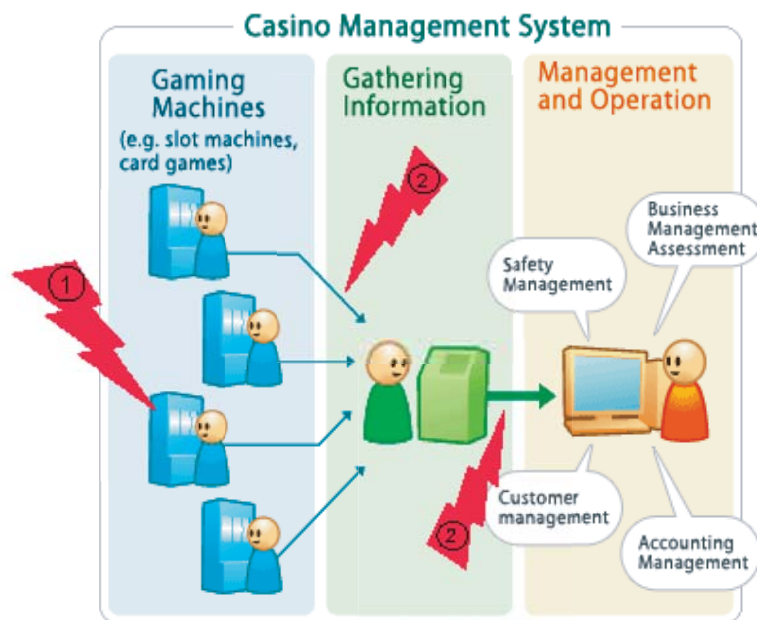
## 2.5 Attacks

Even if they are rare and unlikely due to the high level of difficulty involved, attacks on the system must not be underestimated. Networking technology is inherently less secure than stand-alone machines, and because it deals with money, fraud must be considered as a major threat.

Attacks threats can be listed in two categories: hosting party attacks, which target the slotmachines themselves, and third party attacks, which target the communication links.

- **Hosting party attacks** include hacking, reverse engineering and device cloning. Themachines themselves are targeted (Attack number 1 in Figure 2-1). Cloning IP, physically opening the machine and accessing the gaming board is a threat (fake card, fake data sentto controller...).
- **Third party attacks** include man-in-the-middle attacks, traffic spying, eavesdropping, «fakeslot machine» attacks and authentication snooping. The game is a client/server application, and network traffic can always be sniffed. The communication links aimed at are between themachines and the Casino Controller (Attack number 2 in Figure 2-1).The figure below shows where the threats are in a Casino Management System (The attacks are numbered on the diagram and will be identified with these numbers in the next paragraph).

Figure 2-1. Example of a Casino Management System with threats



### 3. VAULTIC SOLUTION

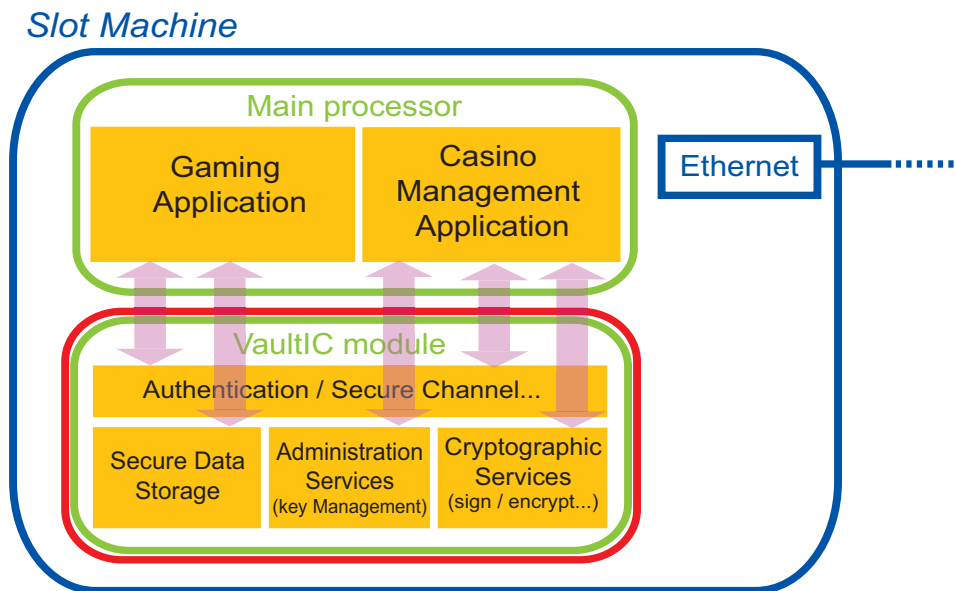
Conscious of all the threats and security issues described above, VaultIC products can provide the required level of security: a solution to prevent the system from unauthorized access and fraud is to embed a VaultIC security module in a Video Slot machine.

#### 3.1 Inside the VaultIC Module...

A VaultIC Module can be considered as a secure box, storing secrets seamlessly and securely. To do this, the secret objects are stored in the secure EEPROM memory of the module, in the form of a dynamic file system. In the gaming case, the file system downloaded by the manufacturer in a VaultIC might be composed as follows:

- **Administrator data:** file system version, private keys. These data allow the Casino Controller to be authenticated to the slot machine and then to upgrade keys, change administration data, update software...
- **Slot data:** identifier, private keys, certificates, IPs. These data allow the Casino Controller to authenticate the slot machine on the Network thereby allowing data to be downloaded from the machine. For more security these data should be unique per chip.
- **Game application data:** IPs. Sensitive data or code are stored in protected records.

Figure 3-1. VaultIC Solution Integration



## 3.2 Example of implementation

Figure 3-2. VaultIC implementation



The example of implementation shown above illustrates how the security modules can bring security to the Network.

### 3.2.1 Identify the slot machine

The VaultIC security modules are secure microcontrollers that embed authentication mechanisms, based on challenge-response algorithms. Then, operations on the Network are secure thanks to the authentication performed between the Casino Controller (or the main server) and the slot machines: for instance, in order to select the right slot machine, the server can authenticate it and change the game on it remotely.

### 3.2.2 Securing the communication

The slot machine can also authenticate the server and then, once both parts are authenticated, they can open a Secure Channel between them. Through it, sensitive information located in the machines (such as player-tracking data) can be conveyed securely on the Network.

### 3.2.3 Several security levels

Depending on who intervenes on the machine, the VaultIC security modules are able to differentiate up to 8 different users according to the rights previously assigned to each one. For instance, the user who downloads data from the machine can be different from the user who upgrades the game software. The VaultIC module will differentiate between these users and permit only the authorised actions for each of them.

### 3.2.4 Securing the IPs

VaultIC Modules embed dedicated hardware for protection against SPA/DPA attacks, advanced protection against physical attack (including active shield), environmental protection systems (voltage, frequency, temperature monitors), light protection and secure management/access protection. Reverse engineering or cloning are then not possible on the VaultIC modules. IPs, intended not to leave the machine, are then protected if stored in the EEPROM of the VaultIC security modules.

Moreover the VaultIC security modules family offers a large choice of EEPROM memory sizes for secure data storage.

### 3.2.5 Against attacks

#### 3.2.5.1 number 1...

The number 1 attack in Figure 2-1 is the least likely but it could result in large losses for slotmakers. However, due to the embedded dedicated hardware in VaultIC for protection against physical attacks, cloning IPs is not possible. Additionally the main server and the VaultIC module have to authenticate each other, so fake data sent to the server will be spotted immediately.

The slot machine, and therefore the secret file system, is then secure and hosting party attacks are warded off.

#### 3.2.5.2 number 2...

In order to authenticate the slot machine on the Casino's Network, a VaultIC module securely stores sensitive data, such as a unique certificate (obviously delivered by a trusted organism, non-duplicated) and a key-pair unique per VaultIC. In this way, each slot machine is unique and considered as genuine by the Casino's Network. Each module can also generate its own key-pair and use it for the strong authentication process performed between both parties.

As a result slot machines will be authenticated on the Network and allowed to make connection and access authorized services. The VaultIC can also authenticate the Network and therefore avoid transferring private data to a «fake» network.

### 3.2.6 And more...

VaultIC security modules can also be used as cryptographic mechanism providers: VaultIC modules can generate the cryptographic primitives needed by the main CPU of the slot machines for different purposes: secure communication using a proprietary protocol in the Casino Management Application, Gaming application...

These primitives include algorithms such as 3DES, AES, RSA up to 4096 bits, DSA up to 2048 bits, ECC up to 384 bits, as well as Public Key Pair Generation, Digital Signature, Encryption /Decryption, Key Wrapping / Unwrapping and HOTP One-Time Password Generation (For more details, please refer to the technical datasheets of the VaultIC products).

Note that these primitives are computed with very good performances thanks to hardware cryptographic engines.

## 4. CONCLUSION

Server-based gaming is the casino technology that is gaining tremendous interest, offering users a much more dynamic and interactive gaming experience. Always concerned about security and fraud, Casino's owners integrate control systems in their local network. This networking of games and control systems creates the need for strong, efficient and reliable security mechanisms to protect the operations and the players. To do this, VaultIC security modules protect the fundamental mechanisms:

- **Mutual authentication:** slot machines and the main server are mutually authenticated to authorize data exchanges.
- **Data Privacy:** the privacy and the confidentiality of the data exchanged between the slot machines and the Casino Controller are protected.
- **Data Integrity:** The slot machine is not physically vulnerable to tampering by malicious users.

For more details about the VaultIC Products Family please contact your local Atmel Sales office.

## DEFINITIONS AND ABBREVIATIONS

<b>AES</b>	Advanced Encryption Standard algorithm as defined in FIPS PUB 197.
<b>Authentication</b>	An identification or entity authentication technique assures one party (the verifier), through acquisition of corroborative evidence, of both the identity of a second party involved, and that the second (the claimant) was active at the time the evidence was created or acquired. (From Handbook of Applied Cryptography).
<b>DES/3DES</b>	Data Encryption Standard algorithm as defined in FIPS PUB 46-3. Triple DES algorithm.
<b>DSA</b>	Digital Signature Algorithm as defined in FIPS PUB 186-2.
<b>ECC</b>	Elliptic Curves algorithm.
<b>EEPROM</b>	Electrically-erasable programmable read-only memory.
<b>RSA</b>	Rivest Shamir Adleman algorithm.
<b>SPA/DPA</b>	Simple Power-Analysis involves visually interpreting power traces, or graphs of electrical activity over time. Differential Power-Analysis is more advanced form of power analysis which can allow an attacker to compute the intermediate values within cryptographic computations by statistically analyzing data collected from multiple cryptographic operations.

## DOCUMENT REVISION HISTORY

- **Rev. TPR0443AX-SMS-09/09**
  1. Official release - Final draft
- **Rev. TPR0443BX-SMS-12/09**
  1. Minor corrections (english).