

Discussion Paper

Gaming Technology Reform: Enabling A “Culture of Responsibility”

Prepared by:

Aristocrat Technologies

Gareth Phillips CTO 01/08/04

INDEX

1	INTRODUCTION: "ENABLING A CULTURE OF RESPONSIBILITY"	<u>3</u>	Deleted: 3
2	WHAT DOES THE GAMING NETWORK LOOK LIKE?.....	<u>5</u>	Deleted: 5
3	SECURITY OF GAMING CONTENT	<u>6</u>	Deleted: 6
4	SECURITY OF TRANSACTIONS	<u>6</u>	Deleted: 6
5	THE CHANGING ROLE OF THE REGULATOR IN GAME APPROVALS	<u>7</u>	Deleted: 7
6	PROTECTION AGAINST CRIMINAL ACTIVITY.....	<u>7</u>	Deleted: 7
7	PROMOTING INFORMED PLAYERS	<u>8</u>	Deleted: 8
8	FUN AND ENTERTAINMENT	<u>8</u>	Deleted: 8
9	CONCLUSION.....	<u>9</u>	Deleted: 9
10	SYSTEM SCHEMATIC	<u>10</u>	Deleted: 10

Deleted: 06/09/2004

1 Introduction: “Enabling A Culture of responsibility”

Growth in gaming technology can offer many responsible advantages to players, venues and governments. Modern gaming technology can provide a safer, more enjoyable entertainment experience and as such it is a more useful tool for responsible government policy and regulation.

Aristocrat employs 2085 people that include 1364 in Australia and is an ASX top 100 company. Aristocrat is considered a “clever” company with 402 people employed in global R&D and 251 of these people based in Rosebery, NSW. 171 Australian R&D employees have university degrees including 40 with “Masters” qualifications. R&D expenditure increased from \$28.6 m in 1998 to \$63.1m in 2003 making Aristocrat the sixth largest¹ in R&D expenditure in Australian. In 1998 100% of R&D expenditure was in NSW. This had reduced to 55% by 2003.

We are strongly of the view that the solutions to problem gambling are people-based, not technical and that effective policy must be framed accordingly. The modernisation of gaming technology should not be confused with the extent of gaming proliferation, but rather as the creation of new tools to serve the gaming policy of the day. Indeed, it enables a “culture of responsibility”.

Gaming technology is continually changing in the face of the relentless push of computerisation; essentially the gaming industry is tracking the personal computer industry but maybe ten years behind. Just as personal computers moved from essentially a range of unique manufacturers, (Wang, Commodore, Lisa, Apple, IBM compatible), to today’s “standard” p.c. (Intel and Windows); so gaming machine technology is also moving out of the domain of uniqueness, (Aristocrat, IGT, Alliance WMS etc.), towards an offering based around some form of Gaming Industry standard.

Hand in hand with this “evolution” is the fact that we live in a “linked” world and as p.c. technology starts to come into gaming so does the need to connect them together and create networks.

These networks go beyond the current systems that provide sophisticated monitoring capability within casinos and clubs, to networks that provide the ability to truly link gaming machines together within and across venues. Players will be able to select their favourite games on demand, play tournaments not just against the machine but against other players, communicate within the venue; and to self exclude and more.

However new technology has its own demands particularly with regards to security and regulation. Gaming machines that resemble no more than a network of linked p.c. terminals offer new challenges to the regulatory environment. How do you ensure that such flexible systems have inherent security over the transactions and content; how do you ensure that such systems protect the payers?

¹ Source: Melbourne University

Deleted: 06/09/2004

It is recognised that gaming is the leisure activity of choice for millions of people. New technology is a strong enabler of “a culture of responsibility” while providing a better entertainment experience in that gambling environment.

This briefing paper looks at some of the issues raised by the advent of networks into gaming and poses some questions and possible solutions for the issues and opportunities it brings.

Deleted: 06/09/2004

2 What Does the Gaming Network Look Like?

Gaming systems are migrating towards linked network of essentially p.c. technologies. In computer industry parlance these are described as thin-client or file server technologies. See "System Schematic" at the end of the paper.

Essentially the network consists of a series of computers (i.e. file servers) each with its own distinct mission. Some of the file servers hold game content (games) supplied by each of the content providers whilst other servers hold the "digital certificates" that ensure the content is that which was approved by the regulator. Some of the file servers define the level of services that are provided by the venue; such as service menus; such as drinks; restaurants, hotel accommodation etc. Some of the servers define which players can access the system and what play profiles the system allows for each player.

Games in this environment are said to be "system centric games".

These networks differ from the current systems in a number of significant ways one of which is standardisation. The current systems are a miss-match of proprietary communication protocols unique to a system provider or gaming machine manufacturer, or are based on a unique set of regulations for a particular state or country.

The new networks will be based on standards; standard for protocols; standards for game content; standards for content security; standards for player interface. As with the p.c. industry it is these standards that will allow these networks to exist and function and for game content to be handled in a secure manner.

The Gaming Standards Association (GSA) and the Australian Gaming Association of Machine Manufacturers (AGAMMA) are both in the vanguard of this movement but more needs to be done from the point of view of the policy makers and regulators themselves in supporting and promoting standards and a visionary growth.

Currently, the GSA has three Industry standard initiatives running. The first is to create a standard for the protocol between systems and between the system and the gaming machine. This standard is called BoB (Best of Breed) and the first version of that protocol has just been published. The second standard is the GDS (Gaming Device Standard). This specifies how peripherals such as bill acceptors, coin mechanisms, hoppers etc. are to interface to the p.c. terminals. The GSA has adopted a USB standard for this and expects true "plug and play" peripherals to be available for gaming machines in 2006. The third standard is the GoS (Gaming Operating System) and is an attempt to create a standard for the gaming industry from Win XP and Linux. All three of these initiatives are important to the success of the Industry going forward and in particular by insisting that all manufacturers adopt these standards the Regulators will make the job of regulating the industry more amenable and less technically demanding.

We need further standards and for these the gaming industry can learn from outside sources. In particular it must look at how the music industry is managing to control music

Deleted: 06/09/2004

content on the Internet and how the banking and commercial sector is protecting itself against electronic attacks in the financial sectors

We need the regulators to engage the various experts in these sectors at national level and work with the Gaming Standards Associations to set best practise and standards that we can all use. It is important that we have these new standards in place before there is a proliferation of the new networks. Once a particular method of operation gets regulatory approval it becomes an almost ipso de facto standard and it is this ad-hoc standardisation that we need to ensure doesn't happen.

3 Security of Gaming Content

As mentioned above one of the major issues in the new generation of networks is ensuring that the game content the regulator approved is the only one that the player can play. There are essentially two schemes that can achieve this.

One option consists of holding digital "keys" inside the p.c. based terminals (firmware on the board) such that only game content encrypted for that terminal using the associated digital "keys" can be run on that terminal.

Another option is where the game content has an associated stored digital certificate that has to be downloaded at the same time as the content and it is this certificate which is used to de-encrypt the game in order for it to run.

In either scenario the regulator, or those licensed to manage this process, hold the digital "keys" such that no one can illegally modify or provide game content that can run on the network.

In the latter scheme the regulators can hold the digital certificates either on a secure file server at the venue or even at the premises of the regulator. This is very similar to the system being proposed by the music industry to secure music content on the Internet.

4 Security of Transactions

One of the major issues in such networks is ensuring "live" that each game played is transacted properly and that accordingly the relevant financial transactions are properly processed, recorded, and audited.

The Gaming Industry can learn from the financial institutions that have successfully managed the migration from a paper based system for dealing with financial securities to one now based on electronic data. Their ability to encode data and to audit trail where each security originated from, and was finally deposited to, is necessary to ensure the security of the transactions in the gaming networks.

The lessons learnt by the financial institutes as to how to close down possible financial frauds in electronic networks are there to be exploited. However it will take the regulators

Deleted: 06/09/2004

working on behalf of the Industry to exploit them through the creation and promotion of appropriate security standards.

5 The Changing Role of the Regulator in Game Approvals

Once games become gaming content in linked networks and Gaming machines become p.c. based gaming terminals that are part of the network the current methods of regulatory approvals become redundant.

System centric games can be best tested within, and by, the system itself. Software code inspection within a system centric game becomes impossible as the game content encompasses a number of significant parts of the network and some of the software in question (Windows XP) is not in the public domain.

Game simulations in the 100s of millions become possible using the power of the network and it is this method of “brute force” testing and regression testing that the regulators will need to fall back on along with enforced standards of code development.

The good news here is that such testing methodologies have been in practise for years and there are well established International standards covering the testing of mission critical software that the Industry may adopt.

The role of the regulator then will change in that the content (game) supplier will no longer supply game content (software) to the regulator for code inspection and testing. Instead the content supplier will supply a digital certificate that shows the game content is fit for purpose and has been correctly regression tested on the network. Certification may have taken place at a third party test house, internally by the supplier, or even on the network by the final user.

Once the digital certificate is issued the regulator can use it to test the integrity of that game at any time. The digital certificate is the mark of integrity and test and it is this that the regulator will need to manage and control in the future.

6 Protection Against Criminal Activity

Gaming is renowned internationally as being a target for criminal activity. Criminals are known to physically attack the machine to remove money or gain an advantage. The phenomenon of “money laundering” is also known to afflict the Industry. Network machines will be subject to such abuses although here as well as physical attack we need to be aware of and respond to electronic attack.

Viruses, Trojan horses, denial of service attacks are all common today on the Internet and although gaming networks are private as large customers link their private networks together they could become a target for such activities.

Deleted: 06/09/2004

Security on the network is paramount. Existing expertise and understanding in the commercial and banking industries can provide valuable lessons for the gaming industry. Correct audit trails and the establishment of real time policing polices are required if the industry is to remain clean from crime. Regulators will need to become intrusive into the networks and be able to run electronic audits in real time where ever, and when ever, they wish. The role of the regulator will become that of “cyber cop” across the gaming networks of the future!

For this to occur, regulators must take a key and leading role in engaging experts at the National level and bring to the Industry best practise from around the world.

7 Well Informed Players

An important key to controlling poor player behaviour and excess gambling is to ensure the player is fully informed at all times and to provide mechanisms that allow the player to self exclude if he/she wishes to do so.

Modern networks have the capacity to provide players with continuous “live” access to all of the playing statistics that they may require to ensure they enjoy their gambling experience and do not play to excess.

Through interaction with the system, players can set their own win or loss limits, length of play etc. and the system will automatically dis-able their terminal when these are reached. It is also possible for the system to track players but that requires the player to identify themselves to the system using either loyalty cards, tickets, or some form of pin.

By fully informing the player the gaming networks of the future will help recreational players to maximise their enjoyment and will encourage pathological players to limit their excesses.

8 Fun and Entertainment

Networks of the future will provide the opportunity for players to play against themselves as well as against the basic machine game. This will increase the enjoyment and entertainment factor without necessarily escalating the gambling content. Indeed policy makers may find it appropriate in certain gambling access situations to offer richer entertainment, competition and challenges in their gambling products.

Policy makers will have new tools to apply to their gambling model.

Players can compete against each other for the fun of competing. By the nature of the product there will always be a gambling element involved but the challenge element may prove to be the bigger of the two factors in defining the success of the games themselves.

Deleted: 06/09/2004

9 Conclusion

Linked networks of p.c. terminals will have a place within the international gaming industry of the future. Today, international gaming jurisdictions are pioneering similar new technologies to achieve rapid responsible gaming reform.

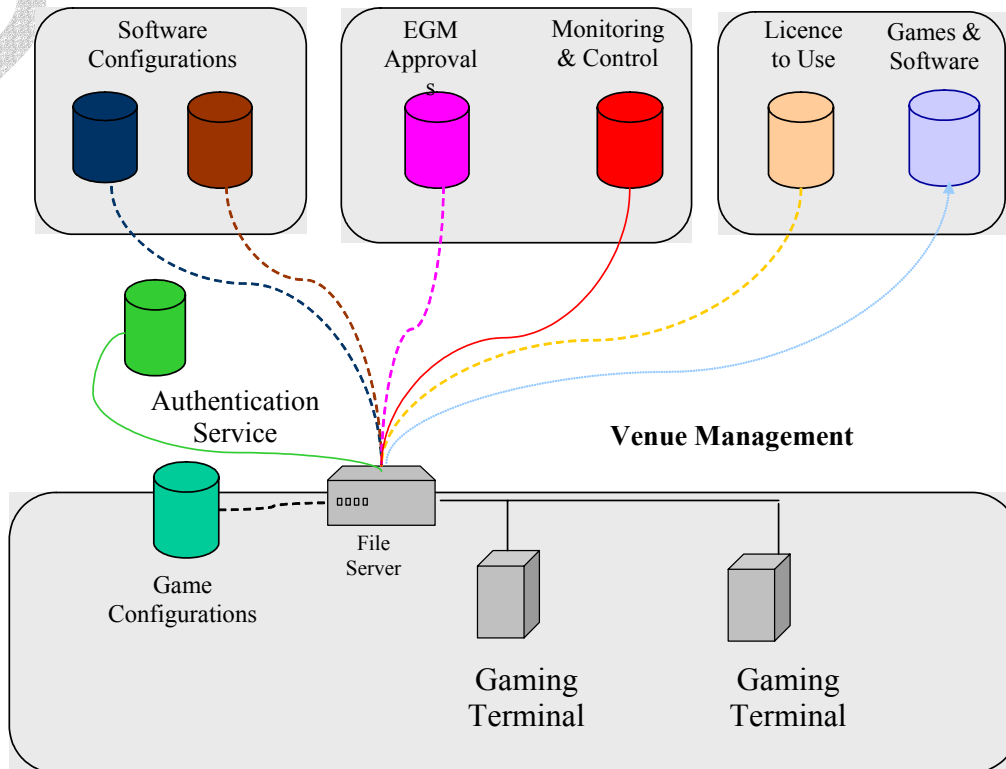
Key to success will be the management of gaming content to ensure that the player is entertained while not exposed to illegal or dubious practises.

To achieve positive reform the regulations and the process where by regulations are applied need to change. Policy makers of the highest calibre need to provide world class leadership in achieving positive reform. We suggest the regulators as a pan-national group leverages the best expertise available in the fields of government and financial security across networks. We also recommend that close contact is established with the music and home entertainment industries who also face the difficult task of retaining security whilst making their content available to the world on the Internet. There are many parallels here which the Gaming Industry may be able to exploit.

Ultimately these networks will benefit the players, venues, community and regulators by providing a more controlled and safer gaming environment, and that is something we all want to achieve.

Deleted: 06/09/2004

10 System Schematic



Deleted: 06/09/2004